

530.6 Hands-On: Secure the Flag Challenge

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020



© SANS Institute 2019
Copyright © 2019 Eric Conrad, Justin Henderson, Ismael Valenzuela. All rights reserved to Eric Conrad, Justin Henderson, Ismael Valenzuela, and/or SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

SANS

Hands-On: Secure the Flag Challenge



© 2019 Eric Conrad, Justin Henderson, & Ismael Valenzuela | All Rights Reserved | Version E01_02

Welcome to SANS Security 530.6, Capstone: Design, Detect, Defend!

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

Teams

Work in teams

- Between two and five people

Winning teams are multithreaded

- Always work different angles
- Do not "monotask"

Have regular meetings

- Review what you have
- Compare notes
- Adjust and plan your next steps

Please work in teams as we recommend that you normally do when working on the blue team. This allows you to combine skill sets and viewpoints to assess the data better. We recommend at least two people and no more than five. We find that more than five becomes overkill in this environment. People start getting left out.

Have each person record his findings and steps. But make sure that you have regular meetings to compare notes and make sure that you are working together. This is VERY important.

Connect to the Scoring Server

- Your instructor will provide you the URL to the scoreboard
- It will look similar to this:
`https://dtf01.sec530.com`
 - Note the “s” in https!
 - You may use whichever browser/OS is most convenient for you
 - Note: Cut and paste will be very helpful!

Make sure you connect to the URL provided by your instructor!

The ability to cut and paste will be *quite* useful as you enter flags into the scoring server.

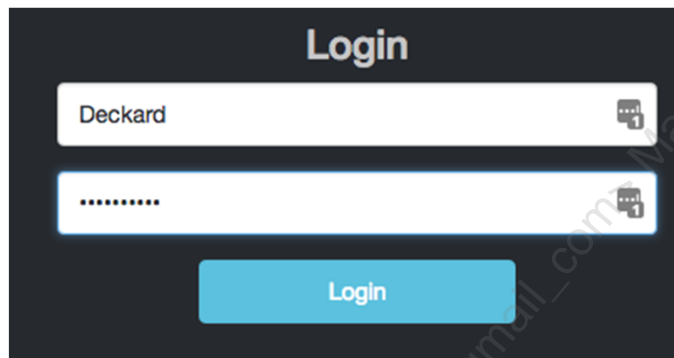
The Sec-530-Linux VM has VMware tools installed and should support cut and paste. Please test cutting and pasting between Windows and Linux to verify.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

Create an Account

Start by clicking on **Register**

- Create an account and then "Login"



Login

Deckard

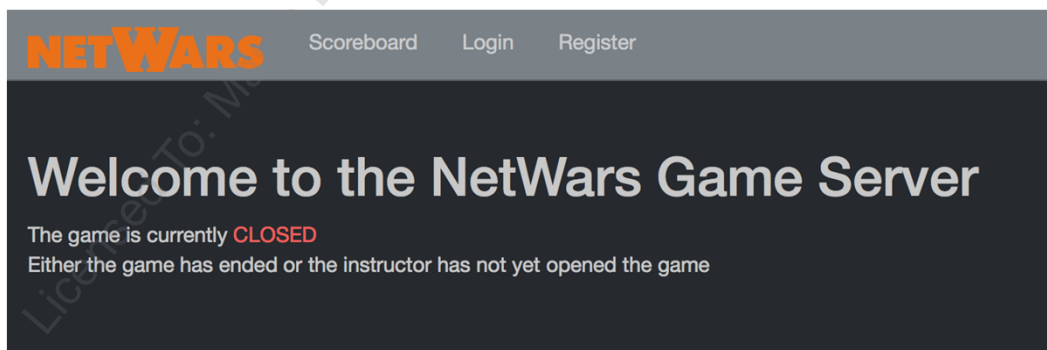
.....

Login

You should now see the NetWars Course Scoring Server. Please click on "Register."

Choose a username and password. Your password must be at least 10 characters long.

You may register an account and log in before (or after) the game begins. If you register before: the game will show "CLOSED". It will open once the instructor begins the game.



NETWARS Scoreboard Login Register

Welcome to the NetWars Game Server

The game is currently **CLOSED**
Either the game has ended or the instructor has not yet opened the game

Create and/or Join a Team!

Form a team by clicking on "Teams"

- See notes for details

The screenshot shows a dark-themed interface titled "Teams". At the top, it explains that users can join teams and play as a group, and that joining a team will result in losing current progress. Two bullet points provide details: "New Team: You will start with a clean progress with no questions answered" and "Join Existing Team: Your progress will be that of the team. All progress will be among your team. The maximum team size is 5." Below this, a message states: "You are currently playing as an individual - to change your avatar click the image on the top right corner of the page". The interface is divided into two main sections: "Join Team" and "Create Team". The "Join Team" section includes a warning that individual progress will be lost and that a team name and password are required. It features input fields for "Team Name" and "Team Password", both with asterisks indicating they are required, and a blue "Join Team" button. The "Create Team" section includes a warning that the new team will have the same progress as the current user or team and that team members will need to supply a name and password. It also features input fields for "Team Name" and "Team Password", both with asterisks, and a blue "Create Team" button.

Speak with your fellow classmates and form a team. The maximum team size is 5.

One teammate should create the team and supply a password that will be shared by all teammates. Creative team names are encouraged!

Each individual should then join the team. Please note the caveats on the team page:

- You can create a new team. The new team will have the same progress as your current user or team. To join the team users will need to supply the team name and password.
- When you join a team, your individual progress will be lost. You need to provide the team name and a team password.

Game Design I

There are multiple levels

- And multiple “missions” per level
- You may attempt missions in any order

Some questions are gateway questions

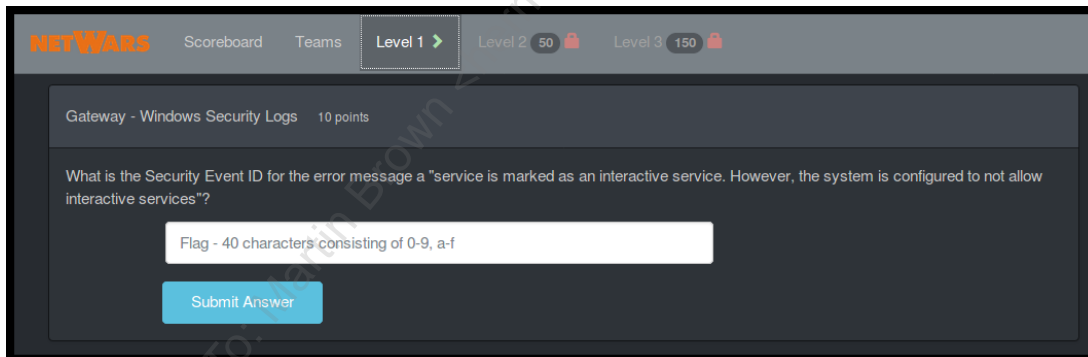
- Correct answer unlocks more questions

Other questions are grouped

- You may answer some of these, and leave others blank

New levels unlock when sufficient points have been acquired

Gateway questions will begin with "Gateway -":



More questions will unlock once the gateway question is answered correctly.

Game Design II

- There will be a number of network resources referenced in questions
 - For example, log files, event logs, web interfaces, etc.
- You may be directed to access a system or copy a log file via the network
- These credentials will be used (unless specified otherwise):
 - Username: Student, Password: Security530

The credentials will be the same ones you use to access the Sec530-Linux-VM unless otherwise indicated.

If a network resource is required to answer a question, the question will give specific directions. For example, “Use scp to copy a log file from student@example.sec530.com:example.txt.”

Attitude Is Everything

- Today's goals:
 - Put everything we have learned this week into hands-on practice
 - Learn
 - Have fun while competing to win
- Hints can be used strategically and/or to complete every challenge
- **Anyone** may complete the entire DTF

We designed the NetWars capstone to be enjoyable for all: from management to the hands-on experienced hunt teamer with years of experience in the trenches.

Hints are available at varying costs, from subtle nudge to “here’s how you do it: type this...”

The capstone provides an opportunity to learn and/or an opportunity to compete. You may choose the “no hints” method to maximize points, the “more hints” method to maximize learning or a combination of the two methods.

How It Works

There is no penalty for one wrong answer to a question

- After that, each wrong answer deducts a point from your total
- Up to a maximum of 3 points per question

This is done to

- Encourage high-quality work
- Discourage blind guessing, brute forcing, etc.

Do not reload the page immediately after a wrong answer

- Some browsers will auto-resubmit old (bad) answers!

There is no penalty for one wrong answer to a question:

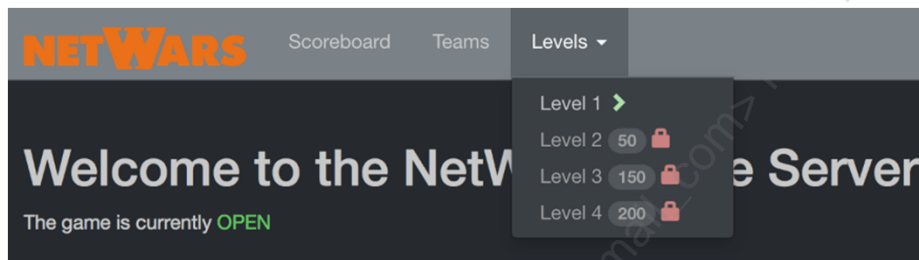


There is a one-point penalty for each incorrect answer after the first:



Once the Instructor Gives the Green Light

- If you have not already done so
 - Create an account and log in to the scoring server
 - Form and join a team
- Then go to “Level 1”



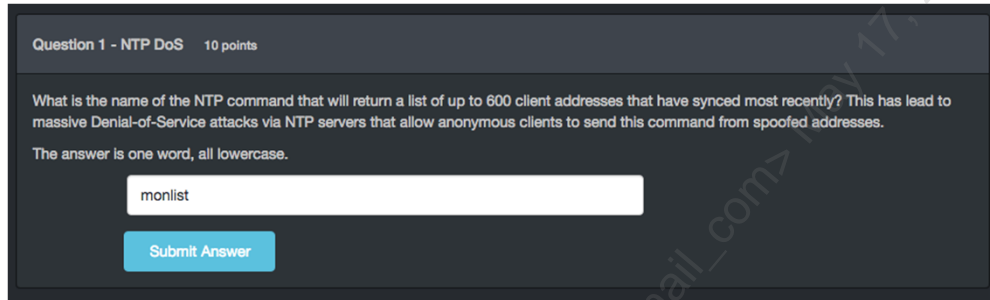
You will be able to enter answers once the instructor begins the game.

Then go to “Level1.”

Answering Your First Question

Answer the first question

- Enter “monlist” and press “Submit Answer”
- Then submit the answer



Question 1 - NTP DoS 10 points

What is the name of the NTP command that will return a list of up to 600 client addresses that have synced most recently? This has led to massive Denial-of-Service attacks via NTP servers that allow anonymous clients to send this command from spoofed addresses.

The answer is one word, all lowercase.

Submit Answer

The first question is:

What is the name of the NTP command that will return a list of up to 600 client addresses that have synced most recently? This has led to massive Denial-of-Service attacks via NTP servers that allow anonymous clients to send this command from spoofed addresses.

We're being generous and giving you the first answer: monlist. Enter that, and press "Submit Answers."

Yay, points!

It will become more difficult shortly, we promise!

Game Advice

Read the questions **very** carefully

- Every word counts!

Inspect your USB carefully

- The included tools and resources may be hints

If the challenge states that it is based on specific files, then use those files, plus related tools

- Do not add unrelated data to the challenge!

It may go without saying but **read the questions carefully!** Students often lose points due to carelessness.

Most of the challenges are based directly on previous labs. If you are stuck, flip through the lab workbook. This is one of the reasons we placed all of the labs in a dedicated book.

More Ground Rules

- Please follow the DTF Golden Rule
 - Treat our systems and your competitors as you would like to be treated
- You may not do any of the following
 - DoS anyone/anything
 - Mess around with layer 2 attacks, ARP, etc.
 - Attack or attempt to exploit any servers, any infrastructure, other student systems, etc.

Please play according to the rules. They are designed to ensure maximum learning and enjoyment for everyone!

The instructor reserves the right to dismiss any student who does not comply with the rules.

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020

Declaring a Winner

We will play until roughly
2:00 PM

- Assuming a 9:00 AM start time

The winner is the player who either:

- Scores all the points
- Has the most points when the game ends



Today will be a lot more free-flowing than days 1 through 5. You may take breaks or lunch whenever you'd like.

The game will last roughly 5 hours, or 9:00 AM to 2:00 PM, assuming a normal conference start time.

Any Questions?

- The game is about to begin
 - If you have any last-minute questions, now is the time to ask
- We provided the first answer: monlist
- After that, it's up to you!



If you have any questions, please ask them now!

Otherwise, let the games begin!



[1] http://kidvskat.wikia.com/wiki/File:1-1_-_Let_The_Games_Begin.png

This page intentionally left blank.

Licensed To: Martin Brown <hermespa56@gmail_com> May 17, 2020

Index

10.0.0.0/8	2:46, 2:82, 3:69
172.16.0.0/12	2:46, 3:69
192.168.0.0/16	2:46, 2:82, 3:69
4over6	2:105
6in4	2:105-106
6over4	2:105
6rd	2:105
6to4	2:105-106, 2:109-110
802.1X	1:100, 1:115, 1:124, 1:184, 2:21, 5:28, 5:35, 5:54-56, 5:59-62, 5:64

A

Abel	1:130, 1:167, 2:66, 2:117, 4:87-88, 4:95
Access-denied Assistance	4:108, 4:110
Active Directory Rights Management (ADRM)	4:85
Active Flow	1:177
Address Resolution Protocol (ARP)	1:35, 1:120, 1:126-131, 2:96, 2:99, 2:104, 3:166, 6:13
African Network Information Center (AFRINIC)	2:61, 2:73
ALLTQ	2:127
Alternate Data Streams (ADS)	4:80, 4:84, 4:86, 4:89
Alternate Queueing	2:127
Always On VPN	3:124, 3:126
American Registry for Internet Numbers (ARIN)	2:61, 2:73
Android	1:11, 1:93-94, 1:100, 2:23, 2:123, 3:99, 4:131-132, 4:134-136
AppArmor	4:177, 4:183
Apple iOS	2:23
Apple OS	2:23
Application Container	4:131, 4:133
Argus	2:53
ARP Cache Poisoning	1:35, 1:126-127, 1:129
ARPANET	1:23, 1:30, 1:151
arpwatch	1:131
Asia-Pacific Network Information Centre	2:47, 2:61, 2:73

(APNIC)

attack surface	1:26, 1:51, 1:58, 1:77, 1:79-82, 2:88, 3:16, 4:69, 4:119, 4:148, 4:158, 4:176, 5:29, 5:42, 5:135, 5:137, 5:150
Attack Surface Analysis	1:77, 1:79-82
Audit Object	4:53
Audit Policies	1:16, 5:2, 5:114-115, 5:117, 5:132
auditd	5:128-130, 5:132, 5:170
Auditing	1:64, 1:81, 2:2, 2:16, 2:26, 2:29, 2:31, 4:35, 4:41, 4:44, 4:53-54, 4:116, 4:134, 4:138, 4:143, 4:151, 4:163, 4:168-170, 4:182, 5:19, 5:21, 5:24, 5:48, 5:119-120, 5:128-130, 5:139, 5:169-170, 5:172, 5:175
auditpol.exe	5:117
Automated Installation Kit (AIK)	5:156
Autonomous System (AS)	1:8, 1:168, 2:12
AutoSecure	2:16, 2:18-19
Azure Information Protection (AIP)	4:85-89, 4:91, 4:105, 4:124, 4:139, 4:159, 4:187
Azure Rights Management (ARM)	4:85, 4:89
Azure Rights Management Connector (ARMC)	4:89

B

Background Intelligent Transfer Service (BITS)	5:153
Banners	1:119, 1:159, 2:6, 2:164, 2:171, 5:160-162, 5:164, 5:175
Bcrypt	1:158
Bejtlich	1:25-26, 1:47, 1:152
Bind	1:130, 1:135, 2:23, 2:47, 4:177, 5:104
BIOS	1:12, 1:18, 3:102, 4:66, 5:137-139, 5:147, 5:149
BitLocker	4:68, 4:70, 4:72, 4:122
Blue team	1:25, 1:49, 3:33, 3:119, 6:2
bogon	1:186, 2:2, 2:46-48, 2:51, 2:54
BOOTP	1:152, 2:19
Bring Your Own Device (BYOD)	1:47, 1:80, 4:127-131, 4:137, 5:6
Bro	1:170, 2:53, 3:35, 3:42, 3:44-47, 3:49, 3:55-59, 3:61
Broken Windows Theory	1:54, 1:91

C

Cain	1:130
CanaryTokens.org	5:173
CAPTCHA	4:22, 4:25
Captive Portal	1:107, 5:54, 5:62, 5:65, 5:68
Carrier-Grade NAT (CGN)	2:61
Center for Internet Security (CIS)	1:140, 2:23-24, 2:26, 2:29, 5:53, 5:68, 5:136, 5:150, 5:154
CentOS	2:23, 4:173-174, 4:177, 4:179, 5:125, 5:128
Central Intelligence Agency (CIA)	1:42, 1:96
Certificate Authorities (CA)	3:51, 3:54, 3:163, 3:169-170, 3:176, 4:130, 5:30-35
Certificate Authority Authorization (CAA)	3:170, 3:179
Certificate Revocation List (CRL)	3:160
Certificate Transparency Monitoring	3:171
CertSpotter	3:171
CHAINS	2:11, 2:67, 2:123-125
Chrome	1:78, 1:114, 2:23, 3:166, 3:171, 5:164
Cisco Catalyst	2:26
Cisco Discovery Protocol (CDP)	1:35, 1:84, 1:121, 1:152, 2:19
Cisco Firewall	2:26
Cisco Router	1:36, 2:24, 2:26-27, 2:33, 2:67, 2:122
Cisco Switch	1:123, 1:130, 1:153, 1:159-161, 2:17, 2:26, 2:35, 2:37, 5:56
ClamAV	2:148
Classification	1:15, 1:77, 1:85, 1:183, 2:120, 2:138, 3:78, 3:81, 4:2, 4:75, 4:77-86, 4:88-91, 4:95, 4:102, 4:104-105, 4:107, 4:109, 4:124, 4:138-139, 4:150, 4:159, 4:163, 4:170, 4:187
Classless Inter-Domain Routing (CIDR)	2:46, 2:61
Client Configuration TooKit (CCTK)	5:147
Clifford Stoll	1:25
Cloud Access Security Broker (CASB)	4:170
Communications Intelligence (COMINT)	1:166
community string	2:22, 2:33-35, 2:37
Computer Emergency Response Team (CERT)	1:30
Conficker	1:33
Content Addressable Memory (CAM)	1:106, 1:122-124, 1:127, 2:96
Content filtering	2:138-139, 2:150
Content Routing	4:22, 4:26

Content Service Switches (CSS)	2:26
Control Groups (CGroups)	4:174, 4:179
Credential Rotation	1:16, 5:2, 5:14, 5:16, 5:20, 5:24
Cuckoo	1:25, 3:99
Cuckoo's Egg	1:25

D

darknet	1:186, 2:2, 2:50-54
Data breach	1:38, 3:93, 4:40, 4:46-47, 4:61, 4:72, 4:122, 4:163, 4:169
Data Breach Investigation Report (DBIR)	1:38
Data diode	5:101
Data Egress Analysis	1:77
Data Encryption	1:15, 4:2, 4:50, 4:61-64, 4:69, 4:72, 4:167
Data Expiration	4:83, 4:90
Data Governance	4:75, 4:107, 4:138, 4:163, 4:169, 4:171
Data Loss Prevention (DLP)	1:15, 2:136, 3:6, 4:2, 4:75, 4:77, 4:82, 4:84-85, 4:95-105, 4:107, 4:121-122, 4:138-139, 4:159, 4:163, 4:170, 4:187, 5:91, 5:93
Data Masking	4:40, 4:44-45
Data Protection Policies	4:124
Data Remanence	4:167, 4:171
Database Activity Monitor (DAM)	4:41-48, 4:73, 4:76, 4:91, 4:105, 4:139, 4:159, 4:187
Database Firewall (DBF)	4:37, 4:41-45, 4:47, 4:96
Database Logging	4:35
Database Monitoring	4:2, 4:34, 4:41, 4:47
DB2	2:23, 4:41
DDOS Scrubbing	3:153-156
Debian	2:23, 5:160
Deep Packet Inspection (DPI)	3:6-7, 3:13, 3:117, 4:7
Defense Information Systems Agency (DISA)	2:16-17, 2:20-23, 2:54
Defensible Network Architecture	1:26
Defensible Networks	1:25-26, 1:152
Denial of Service (DoS)	1:122, 1:160-161, 1:166, 2:43-44, 2:67, 2:84, 2:88, 2:109, 3:27, 3:74, 3:148, 3:169, 4:25, 4:155, 4:179, 5:78-79, 5:82, 5:145, 6:13
Desired State Configuration (DSC)	5:139

Destination IP	1:164, 2:66, 3:68
Destination Port	1:164, 3:8, 3:12, 3:68
Detonation	1:40, 2:116, 2:149-150, 2:174, 3:2, 3:90-98, 3:100-102, 3:104-106, 3:129, 3:139, 3:156, 3:161, 3:176-177, 3:180, 3:184, 5:12, 5:43, 5:87
DHCP Fingerprinting	5:57-58, 5:60, 5:62, 5:65
DHCP starvation	1:132-134
Diamond Model	1:63, 1:68
Diffie-Hellman (DH)	3:175
Direct Memory Access (DMA)	4:69, 5:140
DirectAccess	2:62, 3:126
Distributed Denial-of-Service (DDOS)	3:2, 3:6, 3:141-145, 3:150-156, 3:184, 4:12
dnstwist	2:163
Docker	2:23, 2:107, 3:55, 4:56, 4:133, 4:173-182
Docker Content Trust	4:180
Docker Hub	4:180
Domain Name Service (DNS)	1:40, 1:54, 1:87, 1:106-107, 1:133, 2:41, 2:63, 2:83, 2:85, 2:88, 2:99, 2:105, 2:132, 2:157, 2:159, 2:161, 3:6, 3:8-9, 3:15, 3:25, 3:37, 3:40, 3:51, 3:53, 3:56, 3:61, 3:69, 3:73, 3:115, 3:126, 3:151-153, 3:163, 3:166, 3:170, 4:12, 4:165, 5:54, 5:62, 5:76, 5:86, 5:111, 5:137, 5:168
Domain-based Message Authentication, Reporting, and Compliance (DMARC)	2:161-162
DomainKeys Identified Mail (DKIM)	2:159-162
DShield	2:51, 5:171
Due Diligence	4:157, 4:168, 4:171, 5:150
Duplicate Address Detection (DAD)	2:79
Dynamic Access Control (DAC)	4:79, 4:104, 4:109-113, 4:115, 4:118, 4:124
Dynamic ARP Inspection (DAI)	1:130
Dynamic Host Configuration Protocol (DHCP)	1:35, 1:49, 1:106, 1:124, 1:130, 1:132-135, 2:74-75, 2:85, 3:37, 4:70, 4:145, 4:165, 5:54-55, 5:57-60, 5:62, 5:65

E

Electric Fence	5:66, 5:83
Encapsulating Security Payload (ESP)	3:110, 5:38
Encrypted File System (EFS)	4:64
Encryption	1:15, 1:40, 1:71, 1:81, 1:109-110, 1:115-116,

	1:128, 1:141, 1:155, 1:157-158, 2:19, 2:38, 2:50, 2:90, 2:137, 2:155, 2:159, 2:174, 3:2, 3:6, 3:13, 3:37, 3:58, 3:73, 3:109-113, 3:128, 3:158-159, 3:161-165, 3:172-175, 3:179, 3:182, 4:2, 4:13, 4:50, 4:61-69, 4:71-73, 4:86, 4:88, 4:91, 4:96, 4:99, 4:103, 4:105, 4:113, 4:122-123, 4:125, 4:133, 4:137, 4:139, 4:143-144, 4:159, 4:163, 4:166-167, 4:181, 4:187, 5:8, 5:26-29, 5:32, 5:36, 5:38, 5:40-42, 5:92, 5:101-102, 5:104, 5:106-107, 5:140, 5:144
End-to-End Encryption	3:162, 3:164, 4:13, 5:28
Enumeration	5:145, 5:168
Evebox	3:83
Extended Interior Gateway Protocol (EIGRP)	2:10-12, 2:25, 2:83
Extensible Key Management (EKM)	4:63
Exterior Gateway Protocol (EGP)	2:10

F

Fear Uncertainty and Doubt (FUD)	1:145, 5:6
ff02::16	2:83
ff02::1:2	2:83
ff02::1:3	2:83
ff02::5	2:83
ff02::6	2:83
ff02::7	2:83
ff02::8	2:83
ff02::9	2:83
ff02::a	2:83
ff02::c	2:83
ff05::1:3	2:83
ff0x::101	2:83
ff0x::fb	2:83
File Classification Infrastructure (FCI)	4:78, 4:81, 4:83-85, 4:89, 4:104, 4:124
File Properties	4:79, 4:83-84, 4:86, 4:107
File Server Resource Manager (FSRM)	4:78, 4:80
File Transfer Protocol (FTP)	1:152, 2:133, 3:12, 3:35, 3:51-54, 5:95
FileVault	4:72
FILTER	1:26, 1:31, 1:74, 1:84, 1:100, 1:116, 1:135, 1:160, 1:170, 1:173-174, 1:184, 1:186, 2:2,

	2:7, 2:21, 2:46-48, 2:54, 2:81, 2:93-94, 2:107, 2:109-110, 2:116, 2:118, 2:122, 2:124-125, 2:127, 2:129, 2:136, 2:138-139, 2:149-150, 2:156-157, 2:161, 2:172, 3:5-7, 3:11, 3:13, 3:16-17, 3:34, 3:45, 3:89, 3:104, 3:115, 3:126, 3:154, 4:24, 4:82, 5:18, 5:47-48, 5:51, 5:73, 5:78, 5:83, 5:98, 5:101, 5:104, 5:106-107, 5:121, 5:137, 5:139, 5:170
Fingerbank	5:58
Firefox	2:23
Firewall Logging	5:51, 5:119
Flexible Authentication Secure Tunneling (FAST)	4:113
Flowbits	3:76
fprobe	1:169, 1:175
Full Disk Encryption (FDE)	4:62-63, 4:65-69, 4:72, 4:143, 5:140
Fully Qualified Domain Name (FQDN)	3:11, 3:16-17, 3:115, 5:76

G

Generic Routing Encapsulation (GRE)	1:27, 1:168, 2:14, 2:105, 3:153
Geolocation	3:6, 3:11, 3:16, 3:101, 3:118-119
Google Auth	3:122
GRE	1:2, 1:7, 1:20, 1:24, 1:26-27, 1:38, 1:45, 1:49, 1:51, 1:57, 1:65, 1:71, 1:73, 1:77, 1:82, 1:87, 1:89, 1:111-112, 1:139, 1:162, 1:168-170, 1:174, 2:14, 2:17, 2:24, 2:29, 2:42, 2:44, 2:50-51, 2:67, 2:81, 2:90, 2:105, 2:108, 2:119-120, 2:139, 2:141, 2:161-163, 2:165, 3:11, 3:17, 3:22, 3:31, 3:58, 3:78, 3:80, 3:89, 3:95, 3:98, 3:109, 3:136, 3:153, 3:164-165, 3:167, 3:175, 4:7, 4:18, 4:23-25, 4:41, 4:43, 4:46-47, 4:52, 4:58, 4:75, 4:82, 4:85, 4:88, 4:90, 4:96, 4:98, 4:101, 4:120, 4:123, 4:137, 4:148, 4:153, 4:168, 4:177-178, 4:182, 5:4, 5:17, 5:19, 5:62, 5:84, 5:94, 5:101-102, 5:109-111, 5:121, 5:134, 5:137, 5:159, 5:175, 6:5, 6:10
Group Managed Service Accounts (GMSA)	5:23

H

Hardening	1:14, 1:16, 1:31, 1:35, 1:49, 1:121, 2:17, 2:19, 2:37, 3:147, 3:179, 4:149, 4:152-153, 4:158, 4:177-178, 5:2, 5:8, 5:135-136, 5:138, 5:140, 5:147-150
Hardware Security Module (HSM)	4:63, 4:164
Hashed Message Authentication Code (HMAC)	1:157-158, 2:11, 3:121, 5:41
High Availability (HA)	1:56, 2:127, 2:129, 3:124
HMAC-SHA-256	2:11
Honeypot	5:166-168, 5:173, 5:175
HoneyTokens	5:169, 5:171, 5:173-175
Honeytokens Against Leveraging OSINT (HALO)	5:174
Host-based Firewall	1:16, 1:18, 1:83, 2:129, 3:127, 5:2, 5:47-49, 5:51, 5:73, 5:78, 5:104, 5:108, 5:137
HOTP	3:121
HSTS Preloading	3:167, 3:179
HTTP Public Key Pinning (HPKP)	3:168-169, 3:173, 3:179
HTTP Strict Transport Security (HSTS)	3:165-168, 3:173, 3:178-179, 4:22
Hypervisor	1:73, 1:165, 4:141-154, 4:156-159, 4:162, 4:166, 4:174, 4:187, 5:93

I

IBM AIX	2:23
ICMP flooding	2:8, 3:144
Identity Access Management (IAM)	3:131, 3:137, 3:139
IIS	1:162, 2:23, 3:9, 3:36, 4:37, 5:31, 5:136, 5:162-163
Industrial Control System (ICS)	1:53, 1:80, 1:103, 1:116
Infrastructure-as-a-service (IaaS)	1:171, 1:178, 4:161-163, 4:165, 4:167
Intermediate System-to-Intermediate System (IS-IS)	2:10
International Standards Organizations (ISO)	1:12, 1:45, 1:63, 2:128
Internet Content Adaptation Protocol (ICAP)	2:148-150, 4:96, 4:98
Internet Control Message Protocol (ICMP)	1:168, 2:5, 2:8, 2:14, 2:98, 2:116, 2:122, 3:79, 3:144, 5:39, 5:149, 5:168
Internet Engineering Task Force (IETF)	2:89

Internet Explorer	2:23, 5:164
Internet of Things (IoT)	1:29, 1:37, 1:39, 1:80, 1:104, 1:114, 2:123, 2:145, 3:141-142, 5:57
Internet Worm	1:24, 1:30
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	2:105
Intrusion Detection System (IDS)	1:15, 1:27, 1:83, 1:131, 1:166, 1:172, 2:51-52, 2:60, 2:112, 3:26, 3:31, 3:33, 3:35-37, 3:39-40, 3:43, 3:61, 3:65, 3:67, 3:72-74, 3:76-78, 3:80-81, 3:89, 3:93, 3:95, 3:161, 3:174, 3:176-177, 4:5, 4:42, 4:96-98, 4:104, 4:146-147, 4:165, 5:55, 5:63, 5:93
Intrusion Prevention System (IPS)	1:83, 1:106-107, 2:60, 2:67, 2:112, 3:27, 3:36, 3:74-75, 3:77, 3:81, 3:89, 3:152, 3:154, 3:176-177, 4:7, 4:11, 4:97-98, 4:104, 4:164-165
IP Fragmentation	1:27
ipchains	2:123-124
ipfawdm	2:124
IPsec	1:27, 1:54, 2:5, 2:90, 3:110, 3:116, 5:28, 5:35-40, 5:42, 5:51
IPv6	1:14, 1:78, 1:84, 1:167-168, 1:186, 2:2, 2:9, 2:58-85, 2:87-90, 2:92-112, 2:114, 2:158, 2:171-173, 5:143

J

Jump Box	1:15, 2:174, 3:2, 3:131, 3:134-136, 3:139, 3:156, 3:184
Juniper	2:23-24, 2:26-27, 2:47, 2:87

K

Kali	3:33, 5:125, 5:168
Kerberos	2:23, 2:40, 3:36, 4:111-114, 5:38, 5:104, 5:144
Kill Chain	1:63, 1:65-66
Kon-boot	4:66, 4:103
Kubernetes	2:23, 3:55, 4:175, 4:181

L

LanMan (LM)	1:65, 1:158, 5:141, 5:144
Latin America and Caribbean Network Information Centre (LACNIC)	2:61, 2:73
Layer 2 Tunneling Protocol (L2TP)	3:108, 3:110
layer 7	1:12, 1:18, 1:40, 2:132, 3:5, 3:7-8, 3:11, 3:22, 3:70
Layer 8	1:96, 2:162
Link Layer Discovery Protocol (LLDP)	1:84
Link-local Multicast Name Resolution (LLMN)	2:83
Linux	1:18-19, 1:78, 1:98-99, 1:129, 1:152, 1:169, 1:177, 2:23, 2:53, 2:71, 2:77, 2:79-81, 2:84-85, 2:93-94, 2:97, 2:100-102, 2:111, 2:123-125, 3:29, 3:33, 3:79, 3:99, 3:112, 3:122, 3:136, 3:147, 3:172, 4:17, 4:56-57, 4:67, 4:137, 4:155, 4:173-174, 4:176-178, 4:183, 5:17-19, 5:32, 5:34, 5:47-48, 5:50, 5:64, 5:92-93, 5:114, 5:124-125, 5:128-132, 5:138-141, 5:146, 5:149, 5:169-170, 6:3, 6:7
Linux Containers (LXC)	4:173-174
Linux Permissions	4:56
Local Administrator Password Solution (LAPS)	5:21
Lockdown	4:122, 4:151-153, 5:49
Log Agents	5:91, 5:101-103, 5:107, 5:125, 5:132
Log rotation	5:101, 5:107
Logging	1:27, 1:59, 1:81, 1:83, 1:86, 1:115, 1:119, 1:150, 1:153, 1:165, 1:172-174, 1:178, 1:180, 1:184, 2:6, 2:19, 2:54, 2:127, 2:141, 2:171-172, 3:6, 3:19, 3:36, 3:43, 3:51, 3:54, 3:72-73, 3:100, 4:15, 4:28, 4:35, 4:41, 4:46, 4:53, 4:116, 4:137, 4:143, 4:152, 4:163, 4:182, 5:9, 5:51, 5:75, 5:77, 5:79, 5:82-83, 5:85, 5:94, 5:108, 5:114, 5:119-120, 5:123-125, 5:128-130, 5:132, 5:135, 5:166, 5:169, 5:175

M

MAC Authentication	5:55-57, 5:59-60, 5:62, 5:65
MAC Spoofing	1:122, 1:124, 1:127, 1:131, 5:57
Maintenance Operation Protocol (MOP)	1:152
malwr.com	3:98-99
Man-in-the-Middle (MitM)	1:107, 1:115, 1:127, 1:133, 1:150, 2:7, 2:9, 2:11, 2:13, 2:42, 2:110, 3:6, 3:163-166, 5:26, 5:37, 5:104, 5:141, 5:149
Managed Security Service Provider (MSSP)	1:38
Managed Service Account (MSA)	5:22-23
MANGLE	2:125
Maximum Segment Size (MSS)	1:27, 3:148, 5:149
Maximum Transmission Unit (MTU)	1:27, 1:54, 5:96
MD5	1:155-156, 1:158, 2:11-12, 2:36, 2:38, 3:52, 3:54, 3:58, 3:172, 5:41
Media Access Control (MAC)	1:35, 1:100, 1:106-107, 1:116, 1:120, 1:122- 131, 1:134-135, 1:184, 2:21, 2:70, 2:74-79, 2:96, 3:37, 3:102, 4:145, 5:54-57, 5:59-60, 5:62, 5:65, 5:67
Metadata	2:106-107, 2:156, 3:25, 3:36-38, 3:40, 3:56-57, 3:60, 3:67-68, 3:70, 3:72-73, 3:76, 3:83-84, 3:93, 4:165, 5:174
Metasploit	1:35, 1:98, 1:100, 2:34, 2:43, 2:97, 2:104, 5:164-165
Meterpreter	1:35, 1:98, 5:19
MICCMAC	1:26
mick-mack	1:26
Micro Core and Perimeter (MCAP)	5:73, 5:75-76, 5:80
Microsoft Development Toolkit (MDT)	5:156
Microsoft Point-to-Point Encryption (MPPE)	3:109-110
Mirai	3:142
mirror	1:83, 1:172, 3:27-30, 3:62, 3:80, 3:85, 3:106, 3:129, 3:139, 3:156, 3:161, 3:177- 180, 3:184, 4:42, 4:145, 4:147, 4:165, 5:12, 5:43, 5:87, 5:111
Mobile Device Management (MDM)	1:15, 4:2, 4:123-124, 4:131-134, 4:136-137, 4:139
Modern Honey Network (MHN)	5:167
ModSecurity	4:15, 4:18, 4:29, 5:162
MongoDB	2:23

monlist	2:43-44, 3:152, 6:11, 6:15
Morris Worm	1:24, 1:30
Mozilla	2:23, 5:164-165
MSo8-067	1:33
MTU	1:27, 1:54, 5:96
Multi-tenancy	4:164, 4:166, 4:171
Multicast Listener Discovery (MLD)	2:103
Mutual TLS (mTLS)	5:30, 5:42-43, 5:153
MySQL	2:23, 3:36, 4:6, 4:41, 4:46

N

National Institute of Science and Technology (NIST)	1:45-46, 1:48, 1:63, 1:69, 2:42, 2:92, 2:112, 2:117, 4:129, 4:167, 5:14-15
National Security Agency (NSA)	1:23, 1:33, 1:51, 5:104
Neighbor Discovery Protocol (NDP)	2:97, 2:100, 2:102, 2:104
Netfilter	2:124
NetFlow	1:83, 1:87, 1:165, 1:167-169, 1:174-176, 2:17, 4:145, 5:101, 5:121
Network Access Control (NAC)	1:16, 1:70, 1:100, 1:124, 1:184, 3:127, 5:2, 5:28, 5:40, 5:53-56, 5:58-68, 5:77, 5:79, 5:82
Network Access/Admission Control (NAC)	1:16, 1:70, 1:100, 1:124, 1:184, 3:127, 5:2, 5:40, 5:53-56, 5:58-68, 5:77, 5:79, 5:82
Network Address Translation (NAT)	1:23, 1:106, 2:46, 2:61, 2:87-89, 2:105, 2:125, 3:32, 3:96, 3:110, 5:38
Network Attached Storage (NAS)	4:142-143, 5:93
Network Attack Surface	1:77, 1:79-80, 1:82
Network Control Protocol (NCP)	1:151
Network Intrusion Detection System (NIDS)	1:83, 3:25, 3:65-67, 3:72, 3:74-75, 3:77, 3:79-81, 4:165, 5:15
Network Policy Server (NPS)	5:64
Network Security Monitoring (NSM)	1:15, 1:25-26, 1:47, 1:50, 1:54, 1:87, 1:165, 1:172, 1:178, 2:53, 2:174, 3:2, 3:25-27, 3:33-36, 3:40-41, 3:62, 3:64, 3:72-73, 3:79, 3:84-85, 3:87, 3:106, 3:129, 3:139, 3:156, 3:161, 3:177, 3:180, 3:184, 4:137, 4:146-147, 4:164-165, 5:12, 5:43, 5:82, 5:87
Network Tap	1:83, 1:172, 3:27-28, 3:30-31, 3:62, 3:85, 3:106
Network Time Protocol (NTP)	1:186, 2:2, 2:18, 2:25, 2:40-44, 2:47, 2:54,

	2:83, 3:15, 3:152, 5:95, 6:11
Network Visibility Analysis	1:77, 1:83
Next-Generation Firewall (NGFW)	1:15, 1:105, 1:107, 2:112, 2:116, 2:174, 3:2, 3:5-6, 3:8, 3:10-11, 3:13-14, 3:19, 3:21-23, 3:62, 3:67, 3:85, 3:95, 3:104, 3:106, 3:129, 3:139, 3:152, 3:154, 3:156, 3:161, 3:174, 3:176, 3:179-180, 3:184, 4:5, 4:7, 4:10-11, 4:13, 4:96, 4:98, 4:104, 4:121, 4:124, 4:165, 4:170, 5:12, 5:43, 5:71-72, 5:74-76, 5:80, 5:82, 5:87, 5:91
NFdump	1:176
NFsen	1:175-176
Nipper	1:119, 2:16, 2:26-28
Nipper-ng	2:16, 2:26-28
NIST 800-63B	5:14-15
Nmap Scripting Engine (NSE)	2:35, 2:44, 2:103
Normalization	4:14, 4:18, 4:29
Nortel	2:26-27
NotPetya	1:33-34
nprobe	1:175, 1:177
ntopng	1:175, 1:177
ntpdc	2:43-44
Number Resource Organization (NRO)	2:47

○

Object Access	4:53, 5:119
Office of Strategic Services (OSS)	1:42, 1:56
OneDrive	4:68
Online Certificate Status Protocol (OCSP)	3:160
Open Shortest Path First (OSPF)	1:71, 2:10-12, 2:25
Open Systems Interconnection (OSI)	1:12, 1:31, 1:40, 1:49, 1:86, 1:116, 2:5, 2:132
Open Web Application Security Project (OWASP)	1:81, 4:10-11
OpenVPN	2:105, 3:113
Optical Character Recognition (OCR)	4:82
Optimized Link State Routing Protocol (OLSR)	2:84
Oracle	2:23, 4:41
Organizational Unique Identifier (OUI)	1:106, 3:102, 5:55-57
OSPFv2	2:11

OWASP Top 10	4:11
--------------	------

P

Packet Assembler/Disassembler (PAD)	1:91, 1:152
Pafish	3:102-103
Palo Alto	2:23
Parser Return Code (PRC)	1:59
Password Auditing	5:19, 5:24
Password Policies	5:16-18, 5:24
patch Tuesday	1:55
Path MTU Discovery (PMTUD)	1:27
Path Vulnerabilities	5:146
Payment Card Industry Data Security Standard (PCI DSS)	1:41
PBKDF2	1:155-158
pcap	1:87, 2:35, 2:44, 2:127, 3:33-34, 3:45, 3:49, 3:52, 3:57, 3:81, 5:66
Perfect Forward Secrecy (PFS)	3:174-176
PF_RING	1:177, 3:43, 3:45
pfSense	2:124, 2:127-129
Pivot	1:31, 1:33, 1:49, 1:68, 1:83, 1:91, 1:139, 1:164, 2:118, 3:32, 3:41, 3:61, 3:80-82, 3:84, 3:179, 5:50, 5:143
Planes of Authorization	5:71
Platform-As-A-Service (PAAS)	4:71, 4:141, 4:161
PMTUD	1:27
Point-to-Point (PPP)	1:27, 1:159, 3:108-109, 3:111-112
Point-to-Point Tunneling Protocol (PPTP)	3:108-111, 3:116
poison PDF	1:40
PowerShell	1:105, 3:92, 3:136, 4:39, 4:45, 4:53, 4:58, 4:68, 4:79-80, 4:82, 4:87, 4:89, 4:118, 4:120, 5:22-23, 5:35, 5:38, 5:48, 5:50, 5:58, 5:98, 5:105, 5:114, 5:138-139, 5:146, 5:148, 5:155
Priority routing	5:101
Privilege Attribute Certificate (PAC)	4:111
protocol 41	2:105-106, 2:108, 2:112
Protocol Data Units (PDUs)	1:12
Protocol Visibility Analysis	1:77, 1:84
Proxy	1:24, 1:78, 1:105, 2:3, 2:88, 2:133-138, 2:140-152, 2:154-155, 2:157, 2:159, 2:163-

164, 2:166-167, 2:169, 3:3, 3:6-7, 3:23, 3:36, 3:43, 3:47, 3:62, 3:85, 3:94, 3:106, 3:119, 3:129, 3:139, 3:150, 3:152, 3:156, 3:169, 3:176, 3:180, 3:183-184, 4:10, 4:12-13, 4:15, 4:29, 4:42, 4:44, 4:96, 4:104, 4:170, 5:12, 5:43, 5:71, 5:87, 5:91, 5:111, 5:160, 5:162, 5:164

ProxyCannon	3:119
PSExec	1:33
Public Key Infrastructure (PKI)	3:109, 3:111, 3:159, 3:164, 4:64, 4:85, 5:32-35, 5:42
Pulledpork	3:75, 3:78

Q

Quality of Service (QoS)	2:66, 2:127, 3:28, 5:66
Qualys SSL Labs	3:173
Quarantine	2:161, 2:163, 2:167, 3:95, 5:63
QUIC	1:49, 1:54-56, 1:58, 1:78, 1:107, 1:131, 1:149, 2:10, 2:20, 2:61-62, 2:128, 2:137-138, 2:140, 3:11, 3:14-15, 3:22, 3:33, 3:83, 3:97, 4:12, 4:28, 4:81, 4:157, 4:161-162, 4:164-165, 4:173, 4:176, 5:19, 5:38, 5:49, 5:108, 5:154, 5:157, 5:167, 5:171, 5:173, 5:175
quintillion	2:70, 2:72, 2:79, 2:96, 2:99

R

RADIUS	1:115, 3:36, 5:54, 5:64
Rate-limiting	2:166
Recursive DNS Server (RDNSS)	2:85
Red Herring	1:16, 5:2, 5:159, 5:175
Red team	1:25, 1:49, 1:77, 1:93-94, 1:97, 2:7, 2:59, 3:33
Request for Comments (RFC)	1:151, 1:167, 2:46, 2:51, 2:63-64, 2:66, 2:68, 2:72-73, 2:79, 2:82, 2:85, 2:87, 2:89-90, 2:105, 2:107, 3:65, 3:69, 3:148, 3:170, 4:113, 5:92, 5:96
Reverse Proxy	2:134, 2:142, 3:150, 3:152, 3:169, 4:10, 4:12-13, 4:15, 4:29, 4:42, 4:44, 5:160,

	5:162, 5:164
RFC 3164	5:92, 5:96
RFC 4941	2:79
RFC 6106	2:85
RFC 6434	2:90
RFC 791	2:66
RFC4301	2:90
RIPv1	2:10
RIPv2	2:10
robots.txt	4:27
rogue DHCP	1:132-135
Round Robin Database Tool (RRDTool)	1:176
Router Advertisement Daemon (radvd)	2:81, 2:85
Routing Information Protocol (RIP)	2:10-11, 2:83
Rule Counter	3:12

S

S4U2Self	4:114
Sabotage	1:42, 1:55-56
Sandbox	1:40, 1:105, 2:136, 3:6, 3:90-91, 3:94, 3:96, 3:99-100, 3:103, 5:82
ScreenOS	2:26
SCRYPT	1:155-158
Secrets	1:81, 3:92, 3:132, 4:181, 5:15
Secure SHell (SSH)	1:94, 1:150-151, 1:154, 1:159, 2:13-14, 2:18, 2:24, 2:122, 2:126, 3:6, 3:13, 3:21, 3:51, 3:54, 3:72, 3:104, 3:108, 3:112, 3:116, 4:152, 4:154, 5:65, 5:75-76, 5:108, 5:141
Secure Socket Tunneling Protocol (SSTP)	3:108, 3:111
Secure Sockets Layer (SSL)	2:105, 2:137, 2:148, 3:6, 3:9, 3:13, 3:17, 3:25, 3:35, 3:40, 3:51, 3:54, 3:57-60, 3:111-117, 3:125-126, 3:129, 3:159, 3:166, 3:169, 3:172-174, 3:176-179, 4:13-14, 4:98- 99, 4:130, 4:153, 4:181, 5:12, 5:29, 5:31, 5:36, 5:43, 5:87
Security Access Token (SAT)	4:111, 5:171
Security Information and Event Management (SIEM)	1:16, 1:135, 1:153, 1:171, 3:19, 3:37-38, 3:40, 3:58, 3:81-82, 3:84, 3:100, 4:46, 4:53, 4:165, 5:2, 5:77, 5:82-87, 5:89, 5:100, 5:105, 5:107, 5:110, 5:112, 5:114, 5:166, 5:170

Security Onion	1:170, 2:53, 3:33-34, 3:40-41, 3:75, 3:81, 3:83-84, 3:177
Security Operations Center (SOC)	1:53, 1:59, 1:126, 4:168
Security Operations Fundamentals	1:26
Security Pendulum	5:134
Security Technical Implementation Guide (STIG)	2:16, 2:20-23, 5:150
Segmentation Gateway	1:16, 5:2, 5:72-74, 5:76-80
Self-Defeating Network	1:26
SELinux	4:174, 4:177, 4:183
Sender Policy Framework (SPF)	2:157-159, 2:161-162
Server Message Block (SMB)	1:31, 1:33, 2:71, 3:94, 4:119, 4:142, 5:50, 5:65, 5:141-142, 5:144
Set-Group Identification (SGID)	4:57, 4:178
Set-User Identification (SUID)	4:57, 4:178
Shared Responsibility	4:71, 4:163, 4:171
Signals Intelligence (SIGINT)	1:166
Signed Certificate Timestamp (SCT)	3:171
SiLK	1:175, 2:50, 2:53
Silk Road	2:50
Simple Network Management Protocol (SNMP)	1:126, 1:152, 1:154-155, 1:186, 2:2, 2:13, 2:22, 2:28, 2:33-38, 2:53-54, 2:56, 4:152, 5:55, 5:61, 5:91
Simple Network Time Protocol (SNTP)	2:40
Simple Service Discovery Protocol (SSDP)	2:83, 5:137
Single Packet Authorization (SPA)	5:28, 5:40-41
Slowloris	3:149
SMTP Proxy	2:3, 2:154-155, 2:157, 2:159, 2:163-164, 2:166-167, 4:104
Smurf attack	2:8
Snort	1:170, 2:53, 2:106-107, 3:26, 3:33, 3:45, 3:61, 3:67-72, 3:74-75, 3:79, 3:81, 4:97
Software-As-A-Service (SAAS)	4:71, 4:161
Solid Detection	5:82-83
SonicWALL	2:26
Source IP	1:106, 2:88, 3:68, 3:118, 3:146, 3:151, 4:47
Source Port	3:68
Split-Tunneling	3:123, 3:126
SQL Server Report Service (SSRS)	4:37, 4:44-45
Squid	2:88, 2:148-149, 3:36, 5:165
SSL Offloading	4:13-14
sslstrip	3:165-166
Stateless Address Auto Configuration	2:59-60, 2:74-77, 2:79, 2:85, 2:96

(SLAAC)

Statement of Health (SoH)	5:64-65
Storage Area Network (SAN)	4:142-143, 5:93
Suricata	1:165, 1:170, 1:172-173, 2:53, 2:106, 3:33, 3:36, 3:40, 3:45, 3:58, 3:60-61, 3:72-73, 3:75, 3:83
Switched Port ANalyzer (SPAN)	1:83, 3:28
SYN Cookie	3:147-148
SYN Flood	3:146-148, 3:150, 3:154
Syslog	1:59, 1:131, 1:135, 1:153-154, 3:36, 4:182, 5:91-98, 5:100-103, 5:106-107, 5:111-112, 5:124-127
Sysmon	1:165, 3:38, 3:41, 5:100, 5:121-123, 5:128, 5:132

T

T-Pot	5:167
Tailored Access Operations (TAO)	1:51
Teredo	2:105, 2:107
The Onion Router (TOR)	2:50
thresholds.conf	3:76
Tomcat	2:23, 3:36, 4:6
Total Cost of Ownership (TCO)	1:38, 1:66
TOTP	3:121
Transport Layer Security (TLS)	1:36, 1:71, 1:78, 2:105, 3:8-9, 3:13, 3:15, 3:51, 3:54, 3:57-60, 3:73, 3:109, 3:111-115, 3:126, 3:159, 3:161, 3:166, 3:172-174, 3:176-177, 3:179-180, 4:13, 4:152, 5:14, 5:28-30, 5:35-36, 5:40, 5:42-43, 5:92, 5:101, 5:106, 5:153
Trusted Platform Module (TPM)	4:65, 4:67-70
Type 0	1:155, 2:22, 2:36
Type 5	1:155-156, 1:158, 2:13, 2:22, 2:36
Type 7	1:155, 2:13
Type 8	1:155-158, 2:22
Type 9	1:155-158

U

Ubuntu	1:98, 1:169, 1:177, 2:23, 2:77-78, 2:93, 2:101, 3:73, 4:173-174, 4:177, 5:125-126, 5:128, 5:149, 5:161
Unique Local Address (ULA)	2:71-73, 2:78, 2:82, 2:85
USB keyboard	1:95, 1:97-99
User-agents	3:37, 5:164, 5:175

V

Variable Trust	5:9, 5:82-83, 5:132
Veracrypt	4:67, 4:72
Virtual Local Area Network (VLAN)	1:31, 1:49, 1:70, 1:100, 1:115, 1:120, 1:125, 1:139-140, 1:142-147, 1:184, 2:118, 2:129- 130, 4:144, 4:146, 5:54, 5:60-62, 5:73
Virtual Machine Identification	3:102-103
Virtual Machine Masking	3:103
Virtual patching	4:14, 4:23-24
Virtual Private Network (VPN)	1:27, 1:56, 1:80, 1:165, 1:170, 2:73, 2:105, 2:146-147, 3:101, 3:109-114, 3:116-117, 3:120, 3:122-129, 4:98, 4:119, 5:4, 5:12, 5:27, 5:36, 5:38, 5:43, 5:77, 5:87
Virtual Trunking Protocol (VTP)	1:144-145
Virtualbox	3:135
VLAN hopping	1:120
VM Escape	3:135, 4:148-149, 4:156, 4:166
VMware	1:18, 1:73-74, 2:23, 2:128, 3:135, 4:132, 4:142, 4:144-147, 4:149, 4:151-152, 4:157, 4:174, 6:3
Voice over IP (VoIP)	1:36
Volume Shadow Copy Service (VSS)	4:54-55
Volumetric Attack	3:143-145

W

WAF Detection	4:28
Web Application Firewall (WAF)	1:15, 2:134, 2:142, 3:150, 3:154, 4:2, 4:10- 30, 4:48, 4:73, 4:76, 4:91, 4:96, 4:104- 105, 4:139, 4:153, 4:159, 4:187, 5:162
Web Proxy	1:105, 2:3, 2:133-138, 2:140-148, 2:150-

	152, 3:3, 3:6-7, 3:23, 3:62, 3:85, 3:106, 3:129, 3:139, 3:156, 3:180, 3:183-184, 4:12, 4:96, 4:104, 4:170, 5:12, 5:43, 5:71, 5:87, 5:111, 5:164
Web Vulnerability Scanner	4:23, 5:162
WebLabyrinth	4:27
Websockets	4:19
Whitecap	3:79
Whitelisting	1:116, 2:140, 2:151, 3:10-11, 3:19, 3:22, 3:77, 3:104, 3:116, 4:21, 4:137, 5:120
Windows	1:16, 1:18, 1:33, 1:40, 1:54, 1:67, 1:78-79, 1:83, 1:87, 1:91, 1:98, 1:105, 1:129, 1:140-141, 1:152, 1:158, 2:23, 2:36, 2:40, 2:62, 2:76-77, 2:80-81, 2:85, 2:93, 2:97-98, 2:100-102, 2:110-111, 2:129, 3:8-9, 3:51, 3:53, 3:79, 3:92, 3:99-100, 3:104, 3:109-111, 3:114, 3:122, 3:126, 3:133-136, 3:147, 3:172, 4:17-18, 4:37, 4:51-55, 4:57-58, 4:64, 4:66-70, 4:72, 4:78, 4:80-86, 4:89-91, 4:104, 4:108, 4:110, 4:113-114, 4:116, 4:119, 4:122, 4:124, 4:134-135, 4:137, 4:148, 4:151-152, 4:155, 4:161, 4:165, 4:167, 4:174, 5:17-19, 5:21-23, 5:32, 5:34-35, 5:37-39, 5:42, 5:47-51, 5:56-57, 5:59, 5:64, 5:76, 5:93, 5:96, 5:98-100, 5:102-105, 5:107-108, 5:112, 5:114-122, 5:124, 5:132, 5:135-142, 5:144-146, 5:148-149, 5:153, 5:156, 5:164-165, 5:169-171, 5:173, 6:3
Windows Deployment Services (WDS)	4:70, 5:156
Windows Domain Isolation	5:37
Windows Event Forwarding	4:53, 5:104-105, 5:112
Windows Information Protection (WIP)	4:124, 4:134-136
Windows Management Instrumentation Command (WMIC)	1:33
Windows Permissions	4:51
Windows Server Update Services (WSUS)	1:141, 5:153, 5:157
Wireshark	1:84, 2:107, 3:174, 3:178
Worm	1:24, 1:30, 1:33-34, 1:54, 2:9, 2:13-14, 2:51-52
Wormhole	2:9, 2:13-14

X

X-Forwarded-For (XFF) 2:135

Z

Zero Trust 1:16, 1:61, 1:63, 1:69-70, 1:74, 1:86, 5:1-2,
5:5-11, 5:14, 5:16, 5:26, 5:28, 5:32, 5:38,
5:40, 5:42, 5:47-48, 5:51, 5:53, 5:65, 5:68,
5:70-72, 5:76, 5:114, 5:132

Zero Trust Model 1:61, 1:63, 1:69, 1:74, 1:86, 5:7, 5:70, 5:76

Licensed To: Martin Brown <hermespaul56@gmail.com> May 17, 2020