



SANS

www.sans.org

SECURITY 511
CONTINUOUS MONITORING
AND SECURITY OPERATIONS

511.6

Capstone:
Design, Detect, Defend

The right security training for your staff, at the right time, in the right location.

<https://t.me/learningnets>

Copyright © 2015, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the SANS Institute.

IMPORTANT-READ CAREFULLY:

This Courseware License Agreement ("CLA") is a legal agreement between you (either an individual or a single entity; henceforth User) and the SANS Institute for the personal, non-transferable use of this courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The 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. 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. **BY ACCEPTING THIS COURSEWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. IF YOU DO NOT AGREE YOU MAY RETURN IT TO THE SANS INSTITUTE FOR A FULL REFUND, IF APPLICABLE.** The SANS Institute hereby grants User a non-exclusive license to use the material contained in this courseware subject to the terms of this agreement. User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, for any purpose without the express written consent of the 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 the SANS Institute.

The SANS Institute reserves the right to terminate the above lease at any time. Upon termination of the lease, user is obligated to return all materials covered by the lease within a reasonable amount of time.

SANS acknowledges that any and all software and/or tools presented in this courseware are the sole property of their respective trademark/registered/copyright owners.

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.

Sec511_6_A13_01



Continuous Monitoring and Security Operations Capstone: Design, Detect, Defend

SANS Security 511.6
Seth Misener (GSE #28) & Eric Conrad (GSE #13)

© 2015, Seth Misener and Eric Conrad
All Rights Reserved
Version A13_01

Continuous Monitoring and Security Operations

1

Welcome to SANS Security 511.6, Capstone: Design, Detect, Defend!

Course Outline

- Day 1: Current State Assessment, SOCs, and Security Architecture
- Day 2: Network Security Architecture
- Day 3: Network Security Monitoring
- Day 4: Endpoint Security Architecture
- Day 5: Automation and Continuous Security Monitoring

Day 6: Capstone: Design, Detect, Defend

Next up: the Design, Detect, and Defend capstone!

Please Get Connected

- Please plug into the network and ensure you have connectivity
- Ensure all VMs are in bridged mode
 - In VMware Player, go to Player -> Removable Devices -> Network Adapter
 - Choose "Bridged" and ensure "Connected" is checked
- Then type the following to ensure you have received a DHCP address:
 - Windows: `c:\> ipconfig`
 - Linux/Unix/OSX: `$ ifconfig`

Please ensure that the cat5 cable you're using has tabs both ends. These often break off, leading to layer 1 problems during the exercise.

Also, ensure that your Ethernet port's link light is on.

You should receive a DHCP address on the 10.5.100.0/23 subnet.

If you would like to use one or more static addresses: please use 10.5.102.X, and ask your instructor for "X" (your last octet). You may then also use 10.5.103.X, 10.5.104.X, etc. Also: ensure your netmask is 255.255.0.0!

Note: if you have VMware Workstation, you may configure bridged networking by going to: VM -> Removable Devices -> Network Adapter -> Settings

In VMware Fusion, it is: Virtual Machine -> Network Adapter -> Settings

Connect to the Scoring Server

- Both Windows and the Sec-511-Linux VM will be needed today
- Type the following from both to verify connectivity:
 - Windows: `C:\> ping 10.5.11.6`
 - Linux: `$ ping 10.5.11.6`
- Then surf to: `https://10.5.11.6`
 - Note the “s” in https!
 - You may use whichever browser/OS is most convenient for you
 - Note: cut and paste will be very helpful!

Please ping from both Linux and Windows to verify connectivity to the scoring server:

```
$ ping 10.5.11.6
```

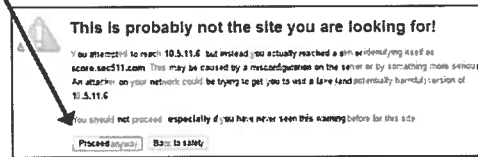
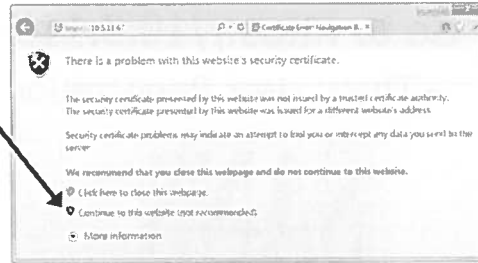
```
C:\> ping 10.5.11.6
```

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

The Sec-511-Linux VM has VMware tools installed, and should support cut and paste. Please test cutting and pasting between Windows and Linux to verify.

Accept the Certificate

- IE: **Continue to this website**
- Chrome: **Proceed anyway**
- Firefox: see notes



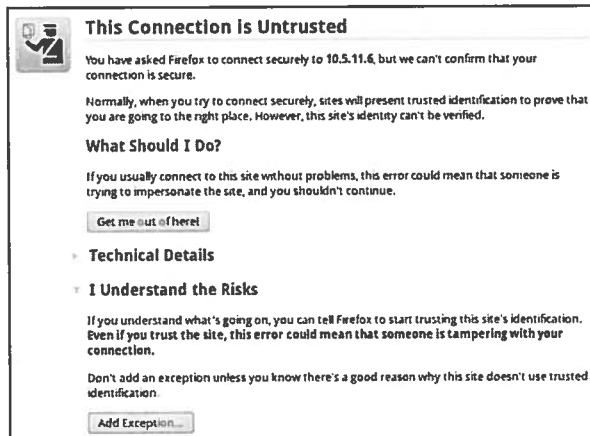
The scoring server is also available at <https://score.sec511.com> (and has a public DNS entry). Any host or VM with Internet access will be able to resolve score.sec511.com and access the server via the name.

The Linux VM has this entry in its `/etc/hosts` file, so you may access <https://score.sec511.com> from Linux, and will not receive a certificate warning.

Your Windows host or VM will not have the hosts file entry, so it will be simplest to use the scoring server's IP address directly: <https://10.5.11.6>.

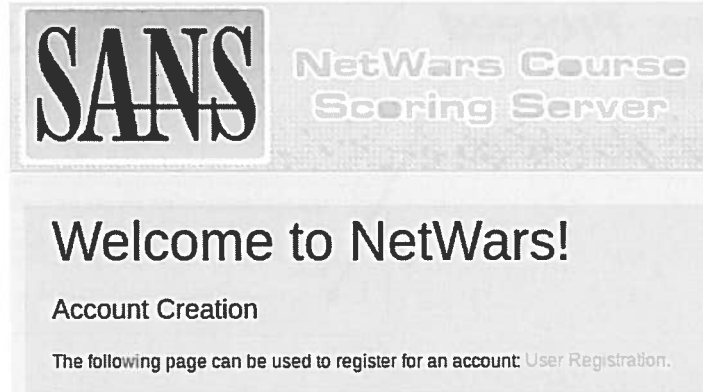
Firefox requires three steps:

1. ***I understand the risks***
2. ***Add Exception***
3. ***Confirm Exception***



Create an Account

- Go to <https://10.5.11.6>
 - Then: User Registration



You should now see the NetWars Scoring Server. Please click on "User Registration."

Create a User

- Choose a username/password
 - Usernames will be publicly posted
 - Please keep it PG-13!
 - And remember the password!
- You will not be able to access questions until the instructor begins the CTF

User Registration

Username:
Apollo Mixed case alphanumeric (A-Z_-.), 4-32 characters

Password:
***** Must be at least 5 characters long

Password Confirmation:
***** Please re-type your password

Register

Continuous Monitoring and Security Operations

7

Choose a username and password.

Your username will be posted on the leaderboard, so please keep it professional.

Also: please choose a good password, and remember it.

You will not be able to access questions until the instructor starts the game. At that point all accounts will be able to access the CTF.

Game Design

- 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
 - “Submit Answers” will only submit answered questions
- New levels unlock when sufficient points have been acquired

Continuous Monitoring and Security Operations

8

Gateway questions will have the following text:

(This question must be answered correctly before proceeding)

Windows Security Logs - (10 pts)

What is the Security Event ID for the error message a “service is marked as an interactive service. However, the system is configured to not allow interactive services”?

(This question must be answered correctly before proceeding)

Short Answer:

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

Game Design II

- There will 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
 - All systems will be on the 10.5.11.0/24 subnet
- These credentials will be used (unless specified otherwise):
 - Username: Student, Password: Security511

The network you will be accessing is 10.5.11.0/24. In other words, every system you access will begin with 10.5.11.*, such as the score server at 10.5.11.6.

The credentials will be the same you use to access the Sec511-Linux-VM, unless otherwise indicated. If a domain is needed to access a Windows system, use SEC511.

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@10.5.11.25:example.txt”

Hints

- Some questions have up to three hints
- Hints deduct points **immediately**
- First hint: deduct 30% available points
 - “Go to workbook section 2-2 (OpenAppID)”
- Second hint: deduct another 30% available points
 - “Begin on step 6, and substitute the /pcap-links directory for analysis.pcap”
- Third hint (deducts all available points for that question):
 - Step-by-step instructions for completing the challenge

Hints are available for many questions. You can use hints in a number of ways. Remember the CTF is designed for learning and/or competing to win. You don't have to do both!

Please keep this in mind: points are deducted immediately!

One way to use hints is strategically: 70% of something is better than zero percent. If you can't answer a question, a hint can provide the necessary boost. The time saved may be critical.

The other way to use hints is to complete steps you may be unable to complete otherwise. You can use hints to complete the entire CTF this way: the final hint is the answer.

Hint Example

- A sample question is worth 10 points
 - You request a hint, which immediately deducts 3 points from your score
 - You then answer the question, winning 10 points, for a net gain of 7 points (10 minus 3)
- Worst-case example (10 point question):
 - Request first (-3 points) and second hint (-3 additional points)
 - If you are still stuck: request the final hint (-4 points), which will provide the answer
 - Then answer the question, for a net gain of 0 points

Once you request a hint for a specific question: it is best to see it through to the end. Assuming a 10-point question, the first hit will deduct 3 points immediately. If you stop there, you will simply be down 3 points.

If you cannot answer the question after the first hint, request the second. Another 30% of question points will be deducted immediately, making you negative 6 points for a 10-point question.

If you still cannot answer the question, request the third hint, which will immediately deduct the final 40% of available points. You will be down 10 points on a 10-point question. Then answer the question winning 10 points, for a net gain of zero points.

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 CTF

Attitude Is Everything

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.

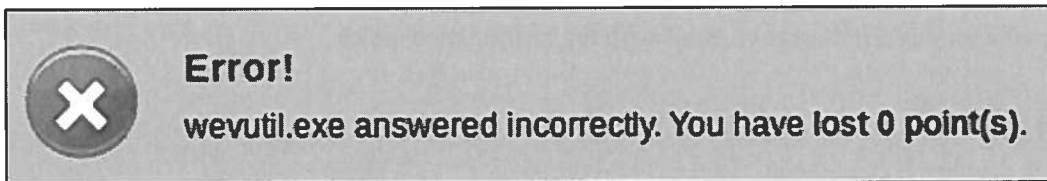
Hints are available at varying costs, from subtle nudge to “here’s how you do it: type this...”

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.

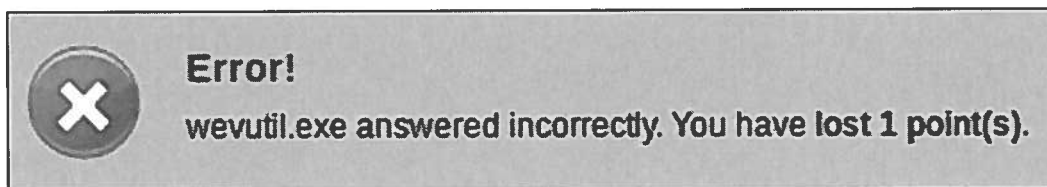
How it Works

- There is no penalty for one wrong answer to a question
- After that, each wrong answer deducts a point from your total
- This is done to
 - Encourage high quality work
 - Discourage blind guessing, brute forcing, etc.

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

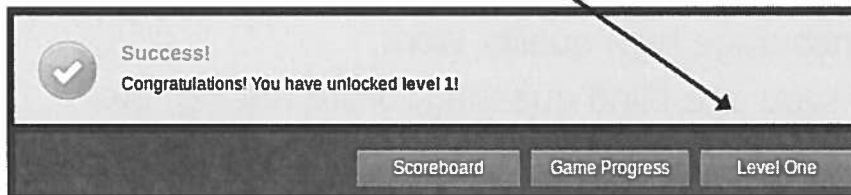
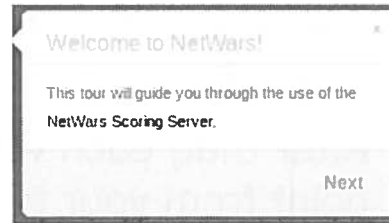


There is a one-point penalty for each incorrect answer after the first:



Once the Instructor Gives the Green Light

- Log into the scoring server
- Take the tour! →
- Then go to "Level One"



Level one will unlock once the instructor begins the game.

You may take the tour to familiarize yourself with the scoring mechanics.

Then go to "Level One."

Flags with SHA1 Answers

- “Flag” answers must be hashed (SHA1)
 - These will have a “Convert to SHA1” option

The screenshot shows a question interface for 'wevutil.exe'. The question asks for the syntax to export the security log to 'cdf.evtx'. Below the question is a 'Flag' input field containing 'wevutil.exe foo bar baz cdf.evtx'. To the right of the input field is a 'Convert to SHA1' link. An arrow points from this link to the 'Converted answer' field, which contains the SHA1 hash: 'fd8582ee2d7ede0493d7f6012f8d4b834c71c6f'.

Continuous Monitoring and Security Operations

15

Hashed answers will always have a “Convert to SHA1” link on the right, which will automatically hash the string entered in the “Flag:” box.

Be very careful with case and spaces with SHA1 answers! A change of a single character will make the answer incorrect. The question will specify case when necessary (for example: Windows commands).

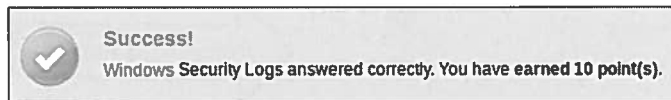
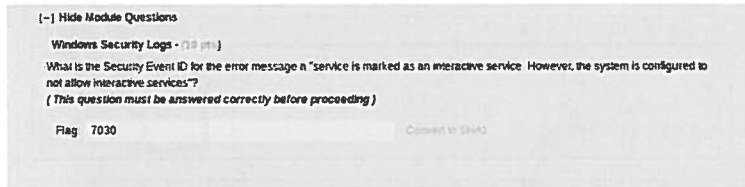
You will need to provide the correct case when you should be able to determine it. For example: Linux is case sensitive, and Linux commands are usually lower case.

The server will generate the error you see below if you enter something that is not a SHA1 hash in a flag question that requires a SHA1 answer. There is no penalty for this error.

Error!
wevutil.exe does not appear to be in the form of a SHA1 hash.

Answering Your First Question

- Answer the first question
 - Enter “7030” and press “Convert to SHA1”
 - Then submit the answer



Continuous Monitoring and Security Operations

16

The first question is:

What is the Security Event ID for the error message a "service is marked as an interactive service. However, the system is configured to not allow interactive services"?

This is a flag question, with a SHA1 hash answer.

We're being generous and giving you the first answer: 7030. Enter that, and press "Convert to SHA1." Then press "Submit Answers".

Yay, points!

It will become more difficult shortly, we promise!

We discussed event 7030 during the 511.5 section *Critical Event 1: Service Creation*

Sysinternals PsExec generates no errors, but Metasploit's generates Event ID 7030

The MIehTND service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

Game Advice

- Read the questions ***very*** carefully
 - Every word counts!
- Inspect your USB carefully
 - The included tools and resources may be hints
- Everything you need to win is in the room
 - Contained in your VM, on the USB, or in a local network resource that will be explicitly referenced
 - Internet access is not needed to complete any challenge
- 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.

Your USB contains a few files that are hints, check it out.

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

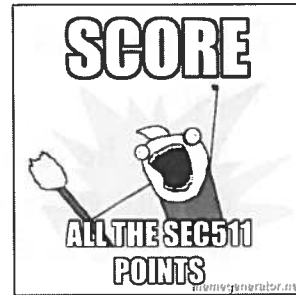
- Please follow the CTF Golden Rule
 - Treat our systems and your competitors as you would like to be treated
- You may only access systems on 10.5.11.0/24 and your own systems
- You may not do any of the following
 - DoS anyone/anything
 - Mess around with layer 2, ARP, etc.
 - Attack or attempt to 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 their rules.

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
- The instructor will then recap the game



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 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: 7030
- 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

Index

Version A13_01

Please let us know if you find any errors in the index. Also, reach out if you have suggestions to improve the index (e.g. keywords that should be added, removed, or have page references added or removed). The easiest way to submit these improvements is to email 511@contextsecurity.com.

Seth Misenaar and Eric Conrad

Index

\$HOME_NET	3:79, 4:86, 4:130
\$TRUSTED	3:77-78
.dll	5:56, 5:145, 6:82
.evt	6:43-44, 6:128, 6:131
.evtx	6:43-44, 6:128, 6:131
.exe	4:121, 5:56, 5:64, 6:104-105
.jar	3:118, 4:49, 6:40
Abnormal	1:140, 1:160, 2:144, 2:164, 3:34, 3:36, 3:41, 4:53, 4:154
Access token	1:112, 2:116, 3:24, 3:139, 4:175, 5:132, 5:152, 5:154-155, 5:157, 5:161
ACT, Application Compatibility Toolkit	5:129-130
ActiveX	1:90, 1:93, 2:94, 2:97
Administrative accounts	3:139, 5:3, 5:95, 5:97-99, 5:101, 5:103, 5:125, 5:137, 6:28, 6:133, 6:143, 6:155, 6:157, 6:159, 6:184
Adobe Reader	1:90, 1:96, 2:94, 2:100, 5:28
ADS, Alternate Data Stream	5:69-70
Adversary Deception	3:3, 3:134-135
Adversary success	1:20, 2:42, 4:20
Alert data	1:27, 2:9, 4:64, 4:82, 4:93
Alexa	3:38, 4:173, 4:175, 6:88
Analysis Methodology	4:3, 4:57, 4:60
Anomaly	3:43, 4:38, 4:43, 4:50-53, 4:81, 4:122, 4:127-130, 4:145, 6:87
Anomaly Detection	3:34, 3:112, 4:50, 4:52-53, 4:128, 4:130, 4:145, 5:49, 6:28
Antimalware	1:52, 1:142, 2:55, 2:146, 3:110, 3:157, 5:4, 5:18, 5:171-172
Antivirus	3:157, 4:21, 4:46-48, 4:55, 4:63, 4:73, 4:115, 4:125, 5:171-172, 6:102
Anubis	3:160
APK	3:160
AppArmor	5:86
Application Inspection	3:95-96, 3:98-99
Application Monitoring	5:48
Application Whitelisting	5:48, 5:62-63, 5:71, 5:77, 5:85, 5:87-88, 5:92, 5:94, 5:182, 6:50
Application Whitelisting, Bypass	5:83
Application Whitelisting, Phase 0: Whitelist Building	5:57, 5:72-76
Application Whitelisting, Phase 1: Targeted Detection	5:77-79
Application Whitelisting, Phase 2: Strict Enforcement	5:80-81
Applocker	5:87-91, 6:132, 6:161-162
APT	3:39, 4:169, 5:164, 6:78, 6:104
argus	4:77, 4:93
ASD Top 35	6:25, 6:38
ASD Top 4	6:26-28, 6:38
ASEPs	5:114
ASEPs, Auto-Start Extensibility Points	1:133, 2:137, 5:3, 5:114-115, 5:117
ASEPs, Registry	5:114, 6:177-182
Asset Inventory	6:52, 6:54, 6:58-59, 6:108
Authentication	5:4, 5:132-133, 5:143-145, 5:152-154, 5:159, 5:162,

	5:168-169, 6:36, 6:84, 6:96, 6:154
Authentication Policy Silos	5:168
Autoruns	1:133, 2:137, 5:3, 5:115, 5:117
awk	4:40, 4:157
Backdoor	1:47-48, 1:107, 2:50-51, 2:111
Base64	4:147, 5:145
Baseline Configuration	5:3, 5:31-34, 5:37-39, 5:41, 5:75, 5:94, 6:75
Baselining	5:42, 5:115, 5:183, 6:51
Behavior	3:10, 3:107-109, 4:49-50, 4:136, 6:104
Bejtlich	1:27, 1:55, 2:9, 2:58, 4:9, 4:11, 4:16, 4:20, 6:5, 6:9, 6:12
BITS, Background Intelligents Transfer Service	5:27, 5:29
Blacklist	1:97, 2:101, 3:44, 3:53-54, 3:56-57, 3:117, 4:44, 4:46, 4:155, 5:167, 5:188, 6:102
Blue Team	4:29
Bogon	3:53-54
Botnet	1:49, 2:52, 4:5, 4:137, 6:89, 6:106, 6:109
Bro	4:30, 4:38-40, 4:43, 4:69, 4:74, 4:89, 4:93, 4:152, 4:155-156, 4:172-173, 4:175-176
Browser	1:82, 1:90-94, 2:86, 2:94-98, 3:18, 3:114-115, 4:151-153, 4:172
Browser attacks	1:92-93, 2:96-97
C2	1:47-48, 1:107, 1:130-131, 1:136, 2:50-51, 2:111, 2:134-135, 2:140, 3:23, 3:26, 3:44-45, 4:3, 4:107, 4:134, 4:141, 6:88-89, 6:176
C2, HTTP	4:148-149
C2, HTTPS	1:119, 1:141, 2:123, 2:145, 3:97, 4:3, 4:141, 4:159-160, 4:162, 4:166, 4:175
C2, HTTPS and X.509	4:55, 4:131-132, 4:162, 4:165, 4:169-175
C2, ICMP	4:143-144
C2, non-HTTPS SSL	4:162, 4:164-165
C2, Persistent Connections	4:138-139
C2, Tor	4:167
Cached Credentials	5:152-153
CAPEX	1:58, 1:153, 2:61, 2:157
Carving	4:3, 4:69-70, 4:74, 4:89
CDM, Continuous Diagnostics and Mitigation	1:24, 6:6, 6:10-13, 6:23
Centralized Logging, Windows	5:175-176, 6:114
Change Detection	5:41-42, 6:96-98
Change Monitoring	5:41-42, 5:183
Ciphertext	4:131
CIS, Center for Internet Security	5:34-35, 5:37, 5:39, 6:124
Cleartext	1:141, 2:145, 5:102, 5:132, 5:145-146, 5:150, 5:162
Client-Side	1:28, 1:60, 1:71-75, 1:77, 1:90, 1:96, 2:3, 2:10, 2:63, 2:74-78, 2:80, 2:94, 2:100, 3:17-18, 3:22, 3:26, 3:76, 3:82, 3:90, 4:108
Content Filter	1:54, 2:57, 3:116-118, 3:120, 3:122, 3:156, 4:140
Content-Type	3:118-119
Correlated Data	1:27, 2:9, 4:64, 4:87
Cost per record	1:11, 2:34
Critical Controls, 1	4:123, 4:135, 5:18, 5:61, 5:96, 6:47, 6:52, 6:74, 6:87, 6:101, 6:108, 6:148
Critical Controls, 10	5:18
Critical Controls, 13	4:135
Critical Controls, 14	6:108

Critical Controls, 19	4:123
Critical Controls, 2	4:123, 4:135, 5:16, 5:61, 6:52, 6:74, 6:101, 6:108, 6:148
Critical Controls, 20	5:7-8
Critical Controls, 3	4:135, 6:47, 6:52, 6:148
Critical Controls, 5	5:8, 5:16, 5:96
Critical Controls, 8	5:61
Critical Controls, 9	4:135
Critical Controls, First Five Quick Wins	5:7-8, 5:16, 5:61, 5:96, 5:194, 6:50-51
Critical Security Controls	1:34, 1:37-40, 1:122, 2:19, 2:126, 4:162, 5:7-8, 5:16, 5:89, 5:94, 6:23-24, 6:148, 6:184
Cuckoo	3:108-109, 3:140
CyberScope	6:18
Daemonlogger	4:68
Data Breach	1:9-11, 2:32-34, 4:19, 5:180
Data Classification	6:32, 6:34
Data compromise	1:69, 1:163, 2:72, 2:167, 3:36, 6:34
Daylight Savings Time	3:58-59, 4:85
DBIR	1:9-10, 1:12-15, 2:32-33, 2:35-37, 2:81, 3:125, 4:19
DDoS	1:48-49, 1:67, 1:100, 2:51-52, 2:70, 2:104
Debug Programs	5:100, 5:105, 5:112, 5:193
Deception Devices	3:3, 3:134-137
Deduction	4:58
Default Deny	1:142, 2:146, 3:51, 3:55, 3:57, 3:60, 6:107
Defensible Network	1:2, 1:26, 2:2, 2:8, 3:163, 4:16, 4:123-125, 4:127-128, 4:138, 4:160, 6:20, 6:30-31, 6:39-40
Detection-Oriented	1:116-117, 2:120-121, 3:74, 5:182
DIACAP	4:8, 6:7-8, 6:18
diff	5:42, 5:115, 6:59, 6:96
Dirty Word List	3:152, 3:154-155, 4:61
Display filters	4:111, 4:119-122, 4:132, 4:167
DITSCAP	4:8, 6:7-8
DLL	3:160, 4:52, 4:87, 4:130, 5:50, 5:56, 5:84, 5:92, 5:145, 5:185, 6:82, 6:161-162
DNS, failed-dns-query	6:93
DNS, Logging	6:86-87, 6:90-93, 6:184
DNS, long-dns-query	6:93, 6:184
DNS, NXDOMAIN	6:93
DOCX	1:79, 1:97, 2:83, 2:101, 3:118, 3:160, 4:44, 4:86, 4:130, 4:163
DoS, Denial of Service	1:46, 1:48, 2:49, 2:51, 3:102, 4:33, 4:117-118
dumpcap	4:68
Dynamic Analysis	3:108-109, 3:118, 3:160
Egress	1:3, 1:142-143, 1:166, 2:4, 2:146-147, 2:170, 3:39, 3:42, 3:44, 3:47, 3:49, 3:55, 3:57, 3:60, 3:97, 3:113, 3:122, 3:162, 5:174-176, 5:182
ELSA	1:3, 1:166, 2:4, 2:170, 4:30, 4:41
Emerging Threats	4:44, 4:83, 4:86-87, 4:130, 4:136
EMET, Enhanced Mitigation Experience Toolkit	5:3, 5:44-46
Enable-PSRemoting	6:173
Entropy	4:34, 4:52, 4:124, 4:127, 4:131-132, 4:163, 4:167, 5:103, 6:88, 6:104-105, 6:135, 6:138, 6:156, 6:181
Event ID 1056, RDP Self-Signed Cert	6:147, 6:162
Event ID 1102, Event Log Cleared	6:145, 6:162
Event ID 2003, Firewall Disabled	6:151, 6:162

Event ID 2005, Firewall Rule	6:103, 6:152
Event ID 4624, Logon	6:153, 6:155
Event ID 4720, User Creation	6:44, 6:142, 6:162
Event ID 4722, User Enabled	6:44, 6:142, 6:162
Event ID 4724, Password Reset	6:142, 6:162
Event ID 4732, User Added to Group	6:44, 6:144, 6:162
Event ID 4738, Account Changed	6:142, 6:162
Event ID 7030, Interactive Service Error	6:21, 6:139-140, 6:162, 7:16, 7:20
Event ID 7045, Service Creation	6:21, 6:135, 6:138, 6:140, 6:149, 6:162
Event IDs, Applocker	5:90-91, 6:161-162
Event IDs, Removable Media	6:149
Event Logs, Critical Windows Events	6:3, 6:127, 6:134, 6:140-141, 6:143, 6:145-146, 6:148-150, 6:153, 6:161, 6:184, 7:16
Event Logs, Damaged	6:129
Event Logs, Windows	6:19, 6:123, 6:129, 6:131, 6:133, 6:164
Event Query, Windows	6:121
Event Viewer	6:120, 6:128-131, 6:142, 6:144, 6:147, 6:149, 6:151
eventvwr	6:120, 6:128, 6:130
EXE	3:160, 4:3, 4:33, 4:52, 4:61, 4:63, 4:73, 4:87, 4:107, 4:116-117, 4:121-122, 4:130, 4:178, 5:56, 6:105, 6:162
EXE, MZ	4:33, 4:72, 4:118-120, 4:130
EXE, PE	4:73, 4:87, 4:118, 4:120, 4:130
EXE, This program cannot be run in DOS mode	4:33, 4:117-119
EXE, This program must be run under Win32	4:118, 4:120
EXE, This program must be run under Win64	4:118
EXE, Transfer	4:3, 4:125, 4:127, 4:130, 4:178
Executable	1:79, 2:83, 4:116, 4:125, 4:127, 5:66-69, 5:72, 5:75-76, 5:78, 5:84, 6:102
Exfiltration	1:101, 1:131, 1:141, 1:143, 2:105, 2:135, 2:145, 2:147, 3:15, 3:25, 3:36, 3:42-45, 3:58-61, 3:68-69, 3:81, 3:83, 3:89-90, 3:94, 3:100-102, 3:110, 3:122
Exploitation	1:44-45, 1:70, 1:75, 1:93, 1:99, 1:107, 1:118, 1:127, 1:131, 2:47-48, 2:73, 2:78, 2:97, 2:103, 2:111, 2:122, 2:131, 2:135, 3:15, 3:22, 3:90, 3:137, 5:94, 5:113, 5:132
Extracted data	4:64, 4:69
False Negative	4:125
False Positive	3:66, 3:81, 3:86, 3:102, 3:140, 4:24, 4:52, 4:129-130, 5:77-79, 5:186, 6:40
File Analysis	3:157, 3:160
File Carving	4:70, 4:74
File Integrity Monitoring	5:42, 5:63, 5:179, 5:183
File-format	1:90, 1:96-97, 2:94, 2:100-101, 4:65, 4:115, 5:187
FIPS 199	6:33
Firewalls	1:54, 2:57, 3:64, 3:74, 3:87, 3:92-95, 3:97-102, 3:116, 3:146, 3:156, 3:162
Flash	1:90, 1:93-94, 2:94, 2:97-98, 5:26, 6:26
Flow Data	1:26, 2:8, 3:30-33, 3:41, 3:143, 3:162, 4:77
Forensics	1:155, 2:159, 3:107, 3:125, 3:154, 4:34, 4:61, 5:42, 5:49, 5:73, 5:84, 5:185-186, 6:129
Forward Proxy	3:116, 3:122-123
Framework	1:37, 1:94, 1:111, 1:122, 2:98, 2:115, 2:126, 3:96, 3:152, 4:39, 5:188, 6:8, 6:174
GeoIP	3:33, 3:40, 3:53-54, 3:56
Get-WinEvent	6:21, 6:43-44, 6:140, 6:142, 6:144-145, 6:147, 6:149,

	6:151, 6:162
grep	4:5, 4:30, 4:37, 4:75-76, 4:152, 4:154, 4:156-157, 4:176, 6:68-69, 6:92
Group Policy	5:24, 5:38, 5:87-88, 5:110, 5:126, 5:139, 5:175, 6:114-115, 6:123
Hanlon's Razor	4:49, 6:40
HIDS, Host Intrusion Detection System	1:9, 2:32, 5:172, 5:179-184
HIPS, Host Intrusion Prevention System	5:172, 5:179-182, 5:184, 6:36
HKLM\Security\Policies\Secrets	5:105
HoneyAdmins	3:139
Honeyclients	3:140
Honeynets	3:135, 3:137
Honeypots	3:3, 3:134-139
HoneyRobots.txt	3:139
HoneySAT	3:139
HoneyTable	3:139
HoneyTokens	3:4, 3:165
HoneyUsers	3:139
HTTP GET	4:36, 4:109, 6:105
HTTP POST	1:135-136, 2:139-140, 4:147-148
Hunt team	1:31, 1:117, 1:163, 2:13, 2:121, 2:167, 3:8-10, 3:126-127, 3:130-131, 4:7, 4:11-13, 4:178, 5:188, 7:12
Hunt Teams	1:31, 1:84, 1:117, 1:163, 2:13, 2:88, 2:121, 2:167, 3:8-10, 3:39, 3:126-127, 3:130-131, 4:7, 4:11-13, 4:178, 5:188, 7:12
Hypothesis Management	4:60
ICMP	1:141, 2:145, 3:32, 3:48-50, 4:52, 4:110, 4:138, 4:141-145
ICMP 0:0, Echo Reply	4:144
ICMP 8:0, Echo Request	4:52, 4:142, 4:145, 7:4
IDS Frontends	1:60, 1:62-64, 2:63, 2:65-67, 4:3, 4:30-34, 4:66, 4:83, 4:113
Impersonation Level	5:154-157, 5:161
Inbound Filtering	3:29, 3:53
Incident Response	1:8-9, 1:39, 1:155, 1:157, 2:31-32, 2:159, 2:161, 4:13, 4:103, 4:138, 4:140, 5:42, 5:186
Indicator Identification	3:152
Indicators	1:129-130, 2:133-134, 3:151-155
Indicators of Compromise	3:155, 5:186
Interactive Logon	5:153, 5:159, 5:169, 6:155
Internal SI Firewalls	3:146, 3:162
Inventory, Active Scanning	6:52, 6:54-58, 6:64, 6:108
Inventory, Passive Discovery	4:30, 4:93, 6:54, 6:63-64, 6:66-69
Invisibility	3:78
IPFIX	3:30-32, 3:41, 3:143, 3:162, 4:77
IRC	1:102, 1:128, 2:106, 2:132, 3:48, 3:52, 3:70, 3:77, 3:97, 3:101, 4:39, 4:53, 4:67, 4:73, 4:141, 5:83, 5:87
IRC C2	3:97, 3:101, 4:141
ISCM, Information Security Continuous Monitoring	6:6, 6:8, 6:14-16
JAR	3:106, 3:118, 3:160, 4:49, 6:40
Java	1:90, 1:93-95, 2:94, 2:97-99, 3:114, 3:118, 3:160, 5:22, 5:26, 5:28, 5:46, 6:26, 6:78
JavaScript	1:93, 2:97, 3:114, 3:160
Joe Sandbox	3:160

Kansa	5:188-189
Kill Chain	1:129-130, 2:133-134, 3:151-152, 3:154
LanMan Hash	5:139-140
Layer 3	1:56, 1:121, 2:59, 2:125, 3:30, 3:33, 3:53, 3:55-57, 3:93, 3:95, 3:97-98, 3:144, 4:108, 4:127
Layer 4	1:56, 2:59, 3:30, 3:33, 3:55, 3:57, 3:93, 3:95, 3:97, 4:108
Layer 7	1:33, 1:56, 1:121, 2:18, 2:59, 2:125, 3:33, 3:43-45, 3:50, 3:93, 3:95, 3:98-99, 3:101, 4:65, 4:79, 4:108, 6:100
LiveSSP	5:147, 5:150, 5:162, 5:168
Log data	1:27, 2:9, 3:43, 4:64, 6:19, 6:129
Log files	4:8, 6:5, 6:129
Log Monitoring	5:39, 5:183, 6:112, 6:127, 6:132
Log Review	1:9, 2:32, 5:179
Log Settings, Windows	6:122, 6:124
Logon Types, Type 10	5:153, 6:155
Logon Types, Type 11	5:152-153
Logon Types, Type 2	5:153, 5:157, 5:159, 5:169, 6:155
Logon Types, Type 3	3:50, 5:111, 5:153, 6:156, 6:159-160
Logon Types, Type 4	5:153
Logon Types, Type 7	5:147, 5:153, 7:8, 7:14
Long Tail Analysis	5:188-189, 6:41-44, 6:167, 6:181, 6:184
LSA Secrets	5:105
lsass.exe	5:64
LUA Buglight	5:130
M-Trends	1:8, 1:14-15, 1:84, 1:126, 1:135, 1:138, 2:31, 2:36-37, 2:88, 2:130, 2:139, 2:142, 3:125, 5:163
Malvertising	1:77, 1:83, 2:80, 2:87
Malware Detonation Devices	1:26, 1:54, 2:8, 2:57, 3:3, 3:64, 3:106-107, 3:140, 4:125
MBSA, Microsoft Baseline Security Analyzer	6:79-82
Memory Analysis	5:185-186, 5:188
Metadata	1:27, 2:9, 4:64, 4:79, 4:87, 5:57, 6:129
Metasploit	1:111, 1:138-139, 2:115, 2:142-143, 4:47, 4:132, 4:165, 5:163, 6:136, 6:138-139, 6:146, 6:157-158
Meterpreter	1:111-112, 2:115-116, 4:117, 4:164-165, 5:161, 6:133, 6:141, 6:145-146, 6:157
Microsoft Account	5:144, 5:147-150
Microsoft Office	1:90, 1:96-97, 2:94, 2:100-101, 5:34-35, 6:26
Mimikatz	5:48, 5:56, 5:92, 5:150, 5:160-168
Minnow	1:87-88, 2:91-92
Mobile application	3:95
Mobile device	1:38, 1:44, 1:86-88, 2:47, 2:90-92, 3:10, 3:114, 4:110, 5:6, 5:13, 5:21
ModSecurity	3:3, 3:72
MSSP	1:9, 1:148, 1:153-155, 1:159, 2:32, 2:152, 2:157-159, 2:163
NAT	3:33-34
Nation-State	1:68, 2:71
ndiff	6:59
NetFlow	1:26, 2:8, 3:30-33, 3:41, 3:143, 3:162, 4:77
netsniff-ng	4:30, 4:66, 4:68
Network Logon	5:111, 5:153, 6:156, 6:159-160
NGFW	1:26, 1:54, 2:8, 2:57, 3:3, 3:64, 3:74, 3:87, 3:92-95, 3:97-102, 3:116, 3:156, 4:108, 6:89, 6:107

ngrep	4:30, 4:37, 4:75-76
NIDS	3:3, 3:74-77, 3:80-84, 3:86-87, 4:15, 4:17, 4:30-31, 4:38, 4:43, 4:51, 4:93, 5:179
NIPS	3:3, 3:74, 3:86-90, 5:179
nmap	3:38, 4:30, 4:145, 6:56, 6:58-59
Non-Encrypted HTTPS	4:160-161
NSRL RDS	5:57, 5:72-76
NT Hash	5:136, 5:138, 5:140-141, 5:143-144, 5:159, 6:156
NTFS Permissions	5:99-100, 5:108-110
Obfuscation	3:160, 4:147
Offense informs defense	3:149, 6:24
OpenAppId	3:3, 3:96-97, 3:104, 7:10
OpenVAS	6:76
OPEX	1:58, 1:153, 2:61, 2:157
OSSEC	4:93, 5:183
Outbound connections	3:35-36, 3:38, 3:41, 6:106
Outbound Filtering	3:29, 3:55-57
Outsource	1:148, 1:152-155, 1:159, 2:152, 2:156-159, 2:163, 3:67
p0f	6:3, 6:64-65, 6:71
PAC	3:114-115
Packet capture, Full	1:62-63, 2:65-66, 3:30, 4:32, 4:66-68, 4:93
Packet Data	1:62-63, 1:112, 2:65-66, 2:116, 3:30, 3:130-132, 4:32, 4:66-68, 4:93
PADS, Passive Asset Database	4:93, 6:64
Pass the pass	5:162
Pass-the-Hash	5:136, 5:139, 5:159, 5:161, 6:155-160
Password Hashes	5:132, 5:135-136, 5:141, 5:157, 5:161, 6:96
Passwords Hashes, Ntds.dit	5:141
Passwords Hashes, SAM	5:139, 5:141
Patching	1:75, 2:78, 3:64, 3:66, 3:68, 5:15-17, 5:21-23, 5:26, 5:31, 5:66, 5:94, 6:31, 6:51, 6:78, 6:184
PDF	1:72, 1:74, 1:79, 1:97, 2:75, 2:77, 2:83, 2:101, 3:119, 3:160, 4:108, 6:26
Perfect Solution Fallacy	4:55, 4:155
Perimeter SI Firewall	3:3, 3:47, 3:58
Persistence	1:108, 1:110, 1:112, 1:116, 1:131, 1:133, 2:112, 2:114, 2:116, 2:120, 2:135, 2:137, 3:121, 5:4, 5:113-114, 5:184-185, 5:191, 6:176
Persistence, registry	6:176
Persistence, service	5:114
persistent.pl	4:139-140, 6:106
Phish	1:12, 1:72-74, 1:80-81, 1:87, 2:75-77, 2:81, 2:84-85, 2:91, 3:152
Phishing	1:12, 1:72-74, 1:80-81, 1:87, 2:75-77, 2:81, 2:84-85, 2:91, 3:152
Pivoting	1:102, 1:127, 1:137, 2:106, 2:131, 2:141, 6:153, 6:155, 6:160
Plugin	1:93-94, 2:97-98, 5:161
Ponemon	1:11, 2:34
Port Scan	6:58
Post-Exploitation	1:99, 1:107, 1:118, 1:127, 1:131, 2:103, 2:111, 2:122, 2:131, 2:135, 3:15, 3:23, 3:137, 5:132, 5:184
PowerShell Remoting	5:188, 6:173-174
PPT	1:85, 1:97, 2:89, 2:101, 3:160, 5:140

PPTX	1:85, 1:97, 2:89, 2:101, 3:160
PRADS	4:30, 6:64, 6:66-69
PRADS, Passive Real-Time Asset Database	4:30, 6:64, 6:66-69
Prevention-Oriented	1:54, 2:57, 3:74
Privilege escalation	1:112, 2:116, 4:13, 4:93, 5:109, 6:46
Process Monitor	5:127-128
Protected Users	5:168, 6:160
Protocol Behavior	4:43, 4:49
Proxies	3:57, 3:112-114, 3:116, 3:121-123, 3:140, 4:139, 4:147, 6:100-106
PSExec	1:138-139, 2:142-143, 4:132, 5:160, 6:133-139, 6:157-159, 7:16
Rainbow Tables	5:136
Red Team	1:39, 4:29
Redline	5:186-187
Registry keys	4:8, 5:127, 6:5, 6:41, 6:167, 6:176, 6:179, 6:181
Remote Interactive	5:153, 6:155
Reputation	3:41, 3:45, 3:56, 3:98, 3:120-122, 4:50-51, 5:163
Response-Driven	1:120, 2:124
Restricted Admin Mode RDP	5:168
Reverse HTTP	1:112, 2:116, 4:139, 6:106
Reverse HTTPS	1:112, 2:116, 6:106
RFC 1918	3:53-54
Risk Informed	1:122, 2:126
Risk Management	1:37, 1:122, 2:126, 6:8, 6:12, 6:14, 6:18
RMF, Risk Management Framework	6:9
Router	1:38, 3:29-30, 3:34, 3:41-45, 3:47, 3:143, 6:97-98
RTF	1:79, 1:97, 2:83, 2:101
Salts	5:102, 5:136-138, 5:140, 5:159, 6:156-157
SANCP	4:93
Sandbox	1:26, 2:8, 3:108-109, 3:118, 3:140
SCAP, Security Content Automation Protocol	5:39, 6:18, 6:74-76
SCCM, System Center Configuration Manager	5:27-29, 5:68
Scheduled Tasks	5:114
SCM, Security Compliance Manager	5:38
SCUP, System Center Updates Publisher	5:28-29
Security Onion	1:60-61, 2:63-64, 4:28-30, 4:93, 4:99, 4:178, 6:66
SeDebugPrivilege	5:100, 5:105, 5:112, 5:165, 5:193
Sensor Placement	4:100-102
Sensor, Design	4:91, 4:93
Sensor, DMZ	3:75, 4:102
Sensor, External	4:102
Sensor, NSM	4:92, 4:99-100
Sensor, Security Onion	4:30, 4:93, 4:99, 4:178
Sensor, Umbrella	4:101-102
Service Accounts	5:104-105, 6:155
Service Logon	5:153
Service-side	1:44-45, 1:70, 1:75, 2:47-48, 2:73, 2:78, 4:110
Set-ExecutionPolicy	6:170-171
sFlow	3:30
Sguil	1:60, 1:62-64, 2:63, 2:65-67, 4:3, 4:30-34, 4:66, 4:83, 4:113
Shell	1:48, 1:64, 1:107, 1:111, 2:51, 2:67, 2:111, 2:115, 6:84, 6:101, 6:118-119, 6:133, 6:141

Shellcode	1:135, 2:139, 4:32, 4:34, 5:44
SI Firewall	3:3, 3:47-48, 3:58-61, 3:92-95, 3:97-99, 3:146-147, 3:162
SID	5:154
SIEM	1:26, 1:54, 1:147, 2:8, 2:57, 2:151, 3:3, 3:125-128, 3:132, 4:30, 4:41, 4:63, 5:49-50, 5:57, 5:183, 6:109
Signature Evasion	4:47
Signature Matching	4:43-44, 4:46, 4:131
SiLK	4:77
Situational Awareness	1:29, 2:11, 6:46
Sniffing	1:67, 2:70, 4:92-94, 4:97, 4:99, 6:56, 6:64
Sniffing, Hubs	4:95
Sniffing, Port Mirror/SPAN Port	4:94-96, 4:98, 4:101, 4:128, 4:178
Sniffing, Port Overload	4:97-98
Sniffing, Taps	4:94-95, 4:97-98
Sniffing, Virtual	4:94, 4:99
Snorby	4:30-31
Snort	3:3, 3:78-79, 3:96, 3:104, 4:30, 4:38, 4:40, 4:43, 4:68, 4:80, 4:84-85, 4:145
Snort Frontends	1:60, 1:62-64, 2:63, 2:65-67, 4:3, 4:30-34, 4:66, 4:83, 4:113
SOC	1:145-161, 2:149-165, 5:10, 5:92
Social Engineering	1:12, 1:71, 1:77, 2:74, 2:80-81, 3:17, 5:113
SP 800-117	6:75
SP 800-137	6:8, 6:14-17, 6:23
SP 800-37	6:8
Spam	1:46, 1:67, 2:49, 2:70, 3:67, 4:86, 6:103, 6:109-110
Splash Proxy	3:121
Splunk	4:30, 4:41
Spoofed	3:41
SQL Injection	3:10, 3:14-16
SRP, Software Restriction Policies	5:87-88
SSH	1:141, 2:145, 3:95, 3:101, 4:39, 4:139-140, 4:144, 6:84
SSL	1:112, 2:116, 3:39, 4:39, 4:159-167, 4:173, 4:175, 5:54-55, 5:68, 6:147
SSO, Single Sign-On	5:135, 5:143-145, 5:147, 6:156
SSP, Security Service Provider	1:148, 2:152, 5:4, 5:143-145, 5:147, 5:162
Stage 2	1:133, 2:137, 4:3, 4:13, 4:107, 4:115-118, 4:128-129, 6:27
Statistical Data	4:64, 4:81
STIGs, Security Technical Implementation Guides	5:39-40
Strategic Web Compromise	1:84, 2:88
String data	4:64, 4:75-76, 4:89
strings, command	4:5, 4:61, 4:75-76, 4:89, 4:117, 4:152, 4:154, 4:157
Suricata	4:30, 4:38, 4:40, 4:43, 4:145
Sysmon	5:3, 5:49-57, 5:59
Sysmon, syntax and configuration	5:3, 5:49, 5:51-53
Tagged data	4:84-86
Target Breach	1:13, 2:35, 3:26, 4:21-25, 4:142, 5:180
TCP/21, FTP	3:93, 3:95, 4:22-23, 4:39, 4:79, 5:68, 6:101
TCP/22, SSH	1:141, 2:145, 3:95, 3:101, 4:39, 4:139-140, 4:144, 6:84
TCP/3389, RDP	5:152, 5:157, 5:168, 6:110, 6:132-133, 6:146-147, 6:152, 6:162
TCP/443, HTTPS	1:112, 2:116, 3:39, 4:39, 4:159-167, 4:173, 4:175, 5:54-

	55, 5:68, 6:147
TCP/6667, IRC	3:97, 3:101, 4:39, 4:53, 4:141
TCP/80, HTTP	1:45, 1:112, 1:121, 1:135-136, 2:48, 2:116, 2:125, 2:139-140, 3:39, 3:42, 3:95, 4:39, 4:44, 4:79, 4:138, 4:141, 4:147-148, 4:154, 4:159-167, 4:175, 5:68, 5:145
tcpflow	4:77
Teensy	1:85, 2:89
Threat Intelligence	1:128, 2:132, 3:4, 3:98, 3:106, 3:120, 3:149-150, 3:153, 3:157, 5:185
ThreatExpert	3:160
ThreatTrack	3:160
Time synchronization	3:57, 4:91, 4:103-104
Time Zone	4:104
TLS	1:112, 2:116, 4:13, 4:117, 4:160, 4:162-165, 4:167, 4:169
True Positive	4:24, 4:130, 5:77-78
tshark	4:35, 4:37, 4:77-78, 4:80, 4:152, 4:175
tspkg	5:162
TTPs	1:128, 2:132, 3:150
Tunnel	1:141, 2:145, 3:53, 4:139-141, 4:143-144, 4:162, 4:166, 6:40, 6:102, 6:106
Two-Factor Authentication	5:133, 5:169
UAC, User Account Control	5:120-121, 5:123-127, 6:182
UDP/123, NTP	3:57, 4:91, 4:103
UDP/53, DNS	3:13, 3:39, 3:51, 3:115, 4:52, 4:141, 5:68, 6:86-90, 6:93, 6:184
UDP/69, TFTP	5:68
URL Analysis	3:156, 3:159-160
USB	1:77, 1:85, 1:141, 2:80, 2:89, 2:145, 4:110, 5:68, 6:43, 6:129, 6:148-149, 6:162, 6:172, 6:180, 7:17
User Rights, Windows	5:99-100, 5:108, 5:111, 5:154, 5:193
User Visibility	3:98
User-Agent	4:3, 4:40, 4:107, 4:151-155, 4:157, 4:178
UTC	1:9, 1:129, 2:32, 2:133, 4:103-104
Virtual Patching	3:64, 3:66, 3:68
VirusTotal	3:157-159, 5:50, 5:57, 5:115, 5:166
Visibility	1:121, 1:132-133, 1:160, 2:125, 2:136-137, 2:164, 3:44-45, 3:78, 3:90, 3:98, 3:101, 3:142, 4:178, 5:180, 6:15
VLAN ACLs	3:142, 3:144-146, 5:180
VNC	1:112, 2:116, 5:157, 6:139
VPN	1:34, 1:65, 1:141, 2:19, 2:27, 2:68, 2:145, 2:171, 3:35, 3:166, 4:135, 4:138-139, 4:162, 4:180, 5:195, 6:40, 6:47, 6:61, 6:102, 6:108, 6:185-186
Vulnerability assessment	1:38, 4:8, 6:82
Vulnerability Scanning	3:16, 5:20, 6:3, 6:47, 6:58, 6:73-74, 6:76
Watering Hole	1:77, 1:84, 2:80, 2:88, 3:17-22, 5:121
WDigest	5:145-147, 5:150, 5:162, 5:165, 5:168
Web Application Firewall	1:26, 2:8, 3:3, 3:63-64, 3:66-70
wecutil	6:119
Wepawet	3:160
wevutil	6:128
WFAS, Windows Firewall with Advanced Security	5:175-177, 6:132, 6:150-151, 6:162
Whitelist Integrity	5:65

Windows Event Collector	6:119
Windows Remoting	6:118, 6:173
winrm	6:118, 6:173
Wireshark	1:60, 1:63-64, 2:63, 2:66-67, 4:32, 4:35-36, 4:65, 4:68, 4:70, 4:81, 4:119-122, 4:132, 4:143, 4:161, 4:164, 4:167
WMF	1:79, 1:97, 2:83, 2:101
WPAD	3:114-115
WSUS, Window Server Update Services	4:124, 5:23-29
X.509	4:55, 4:131-132, 4:162, 4:165, 4:169-175
XLS	1:97, 2:101, 3:160, 5:70
XLSX	1:97, 2:101, 3:160, 5:70
XOR	1:135, 2:139, 4:147
Zero-copy	4:68
Zero-day	6:78
Zone.Identifier	5:69-70