

## Table of Contents

<b>Windows Event Logs Table .....</b>	<b>2</b>
<b>Get-WinEvent .....</b>	<b>5</b>
AppLocker.....	6
EMET .....	6
Sysmon.....	6
Windows Defender .....	6
<b>Bro.....</b>	<b>8</b>
<b>Tshark.....</b>	<b>9</b>
<b>Linux.....</b>	<b>10</b>
awk .....	10
checksum tools .....	10
cut.....	10
file.....	11
grep.....	11
head .....	11
sed .....	12
sort.....	12
wc .....	13
xxd .....	13
<b>Index.....</b>	<b>14</b>
A .....	14
B.....	15
C.....	15
D .....	16
E.....	17
F.....	18
G .....	18
H .....	18
I.....	19
J .....	19
K.....	19
L.....	20
M .....	20
N .....	20
O .....	21
P.....	21
R.....	22
S.....	22
T.....	24
U .....	25
V .....	25
W .....	25
X.....	25
Z.....	26

# Windows Event Logs Table

Log Name	Provider Name	Event IDs	Description
System		7045	A service was installed in the system
System		7030	...service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
System		1056	Create RDP certificate
Security		7045, 10000, 10001, 10100, 20001, 20002, 20003, 24576, 24577, 24579	Insert USB
Security		4720	A user account was created
Security		4722	A user account was enabled
Security		4724, 4738	Additional user creation events
Security		4728	A member was added to a security-enabled global group
Security		4732	A member was added to a security-enabled local group
Security		4740, 4767	User account locked out, unlocked
Security		4624, 4647	Successful logon, user initiated logoff
Security		4625	Logon failure
Security		4778, 4779	RDP reconnected, disconnected

Security		4800, 4801	Workstation locked, workstation unlocked
Security	Logon types	2	Interactive
Security	Logon types	3	Network (i.e. mapped drive)
Security	Logon types	4	Batch (i.e. schedule task)
Security	Logon types	5	Service (i.e. service startup)
Security	Logon types	7	Unlock (i.e. unattended workstation with password protected screen saver)
Security	Logon types	8	Network Cleartext (Most often indicates a logon to IIS with "basic authentication")
Security	Logon types	10	Remote Desktop
Security	Logon types	11	Logon with cached credentials
Security		1102	Clear Event log
Application	EMET	2	EMET detected ... mitigation and will close the application: ...exe
Firewall		2003	Disable firewall
Microsoft-Windows-AppLocker/EXE and DLL		8003	(EXE/MSI) was allowed to run but would have been prevented from running if the AppLocker policy were enforced
Microsoft-Windows-AppLocker/EXE and DLL		8004	(EXE/MSI) was prevented from running.
Microsoft-Windows-WindowsDefender/Operational		1116	Windows Defender has detected malware or other potentially unwanted software

Microsoft-Windows- WindowsDefender/Operational		1117	Windows Defender has taken action to protect this machine from malware or other potentially unwanted software
---	--	------	--

# Get-WinEvent

View all events in the live system Event Log:

```
Get-WinEvent -LogName system
```

View all events in the live security Event Log (requires administrator PowerShell):

```
Get-WinEvent -LogName security
```

View all events in the file example.evtx, format list (fl) output:

```
Get-WinEvent -Path example.evtx | fl
```

View all events in example.evtx, format GridView output:

```
Get-WinEvent -Path example.evtx | Out-GridView
```

Perform long tail analysis of example.evtx:

```
Get-WinEvent -Path example.evtx | Group-Object id -NoElement | sort count
```

Pull events 7030 and 7045 from system.evtx:

```
Get-WinEvent -FilterHashtable @{Path="system.evtx"; ID=7030,7045}
```

Same as above, but use the live system event log:

```
Get-WinEvent -FilterHashtable @{logname="system"; id=7030,7045}
```

Search for events containing the string "USB" in the file system.evtx:

```
Get-WinEvent -FilterHashtable @{Path="system.evtx"} | Where {$_.Message -like "*USB*"}
```

'grep'-style search for lines of events containing the case insensitive string "USB" in the file system.evtx:

```
Get-WinEvent -FilterHashtable @{Path="system.evtx"} | fl | findstr /i USB
```

Pull all errors (level=2) from application.evtx:

```
Get-WinEvent -FilterHashtable @{Path="application.evtx"; level=2}
```

Pull all errors (level=2) from application.evtx and count the number of lines ('wc'-style):

```
Get-WinEvent -FilterHashtable @{Path="application.evtx"; level=2} | Measure-Object -Line
```

## AppLocker

Pull all AppLocker logs from the live AppLocker event log (requires Applocker):

```
Get-WinEvent -logname "Microsoft-Windows-AppLocker/EXE and DLL"
```

Search for live AppLocker EXE/MSI block events: "(EXE) was prevented from running":

```
Get-WinEvent -FilterHashtable @{{logname="Microsoft-Windows-Applocker/EXE and DLL";  
id=8004}}
```

Search for live AppLocker EXE/MSI audit events: "(EXE) was allowed to run but would have been prevented from running if the AppLocker policy were enforced":

```
Get-WinEvent -FilterHashtable @{{logname="Microsoft-Windows-Applocker/EXE and DLL";  
id=8003}}
```

## EMET

Pull all EMET logs from the live Application Event log (requires EMET):

```
Get-WinEvent -FilterHashtable @{{logname="application"; providername="EMET"}}
```

Pull all EMET logs from a saved Application Event log (requires EMET):

```
Get-WinEvent -FilterHashtable @{{path="application.evtx"; providername="EMET"}}
```

## Sysmon

Pull all Sysmon logs from the live Sysmon Event log (requires Sysmon and an admin PowerShell):

```
Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational"
```

Pull Sysmon event ID 1 from the live Sysmon Event log

```
Get-WinEvent -FilterHashtable @{{logname="Microsoft-Windows-Sysmon/Operational";  
id=1}}
```

## Windows Defender

Pull all live Windows Defender event logs

```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Windows  
Defender/Operational"}
```

Pull Windows Defender event logs 1116 and 1117 from the live event log

```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Windows  
Defender/Operational";id=1116,1117}
```

Pull Windows Defender event logs 1116 (malware detected) and 1117 (malware blocked) from a saved evtx file

```
Get-WinEvent -FilterHashtable @{path="WindowsDefender.evtx";id=1116,1117}
```

# Bro

*Bro is an open-source network security platform that illuminates your network's activity in detail, with the stability and flexibility for production deployment at scale.*

*Bro reduces incoming packet streams into higher-level events and applies customizable scripts to determine the necessary course of action. This simple design allows you to configure an array of real-time alerts, execute arbitrary programs on demand, and log data for later use.*

Run bro against a pcap, create bro log files in the current directory. Some of following logs files may be created, depending on the pcap content:

```
conn.log dns.log
files.log http.log
irc.log packet_filter.log
ssl.log weird.log
```

```
$ bro -r /pcaps/virut-worm.pcap
```

Carve executables from a file:

```
$ sudo bro -r /pcaps/virut-worm.pcap /opt/bro/share/bro/file-extraction/extract.bro
$ ls -la /nsm/bro/extracted
```

Carve multiple file types: exe, txt, jpg, png, html and "other" (uses the extension .xxx):

```
$ sudo bro -r /pcaps/virut-worm.pcap /opt/bro/share/bro/file-extraction/extract-all.bro
$ ls -la /nsm/bro/extracted
```

Display x.509 issuer subjects:

```
$ bro -C -r /pcaps/normal/https/alexa-top-500.pcap
$ cat ssl.log | bro-cut issuer_subject
```



# Tshark

*TShark is a network protocol analyzer. It lets you capture packet data from a live network, or read packets from a previously saved capture file, either printing a decoded form of those packets to the standard output or writing the packets to a file. TShark's native capture file format is pcap format, which is also the format used by tcpdump and various other tools.*

*Without any options set, TShark will work much like tcpdump. It will use the pcap library to capture traffic from the first available network interface and displays a summary line on stdout for each received packet.*

Read a pcap file:

```
$ tshark -r /pcaps/zeus-gameover-loader.pcap
```

Read a pcap, don't resolve names (layers 3 or 4):

```
$ tshark -nr /pcaps/zeus-gameover-loader.pcap
```

Read a pcap, use the display filter "http.request.method==GET":

```
$ tshark -r /pcaps/zeus-gameover-loader.pcap -R "http.request.method==GET"
```

Read a pcap, show TCP SYN packets not sent to port 80, don't resolve names:

```
$ tshark -r /pcaps/zeus-gameover-loader.pcap -n -R "not tcp.port==80 and tcp.flags == 0x0002"
```

Print TCP conversations in a pcap:

```
$ tshark -n -r /pcaps/virut-worm.pcap -q -z conv,tcp
```

Print HTTP User-Agents in a pcap:

```
$ tshark -nr /pcaps/normal/http/normal-user-agent.pcap -R "http.user_agent" -Tfields -e http.user_agent
```

Print X.509 certificates in a pcap:

```
$ tshark -r /pcaps/normal/https/alexa-top-500.pcap -T fields -R "ssl.handshake.certificate" -e x509sat.printableString
```

# Linux

## awk

Print the length of each line of a file (/etc/passwd in this case), followed by the line itself:

```
$ cat /etc/passwd | awk '{print length, $0;}'
```

Print the 2nd field from a file using the string 'Mozilla/' as a delimiter:

```
$ cat /var/log/apache2/access.log | awk -F "Mozilla/" '{print $2}'
```

Print the last period delimited field

```
$ cat domains.txt | awk -F "." '{print $(NF)}'
```

## checksum tools

Generate the MD5 checksum of a file:

```
$ md5sum /etc/passwd
```

Generate the SHA1 checksum of a file. The three following commands are equivalent:

```
$ sha1sum /etc/passwd  
$ shasum /etc/passwd  
$ shasum -a1 /etc/passwd
```

Generate the SHA-256 checksum of a file:

```
$ shasum -a256 /etc/passwd
```

Generate the SHA-512 checksum of a file:

```
$ shasum -a512 /etc/passwd
```

## cut

Cut the 2nd field from a file, using the space as a delimiter:

```
$ cat /var/log/dpkg.log | cut -d ' ' -f2
```

Cut the 6th field from a file, using the colon as a delimiter:

```
$ cat /etc/passwd | cut -d: -f6
```

Cut the 2nd and 3rd field from a file, use the comma as a delimiter:

```
$ cat /labs/honeytokens/pilots.csv | cut -d, -f2-3
```

Cut beginning at the 7th field, to end of line, using the space as a delimiter:

```
$ cat /var/log/dpkg.log | cut -d' ' -f7-
```

Cut the 6th field, using the double-quote (") as a delimiter, and escaping it to treat it as a literal character:

```
$ cat /var/log/apache2/access.log | cut -d\" -f6
```

Cut the beginning at the 11th character, to end of line:

```
$ ifconfig | cut -c11-
```

## file

Determine the file type, using the file's magic bytes:

```
$ file /usr/local/bin/*
```

## grep

Search for lines containing the string "bash", case sensitive:

```
$ grep bash /etc/passwd
```

Search for lines containing the string "bash", case insensitive:

```
$ grep -i bash /etc/passwd
```

Search for lines that do not contain the string "bash", case insensitive:

```
$ grep -vi bash /etc/passwd
```

Search for lines containing the string "root", case sensitive, plus print the next 5 lines:

```
$ grep -A5 root /etc/passwd
```

## head

Print the first 10 lines of a file:

```
$ head -n 10 /etc/passwd
```

## sed

grep for lines containing "Mozilla", then change "Mozilla" to "MosaicKilla":

```
$ grep Mozilla /var/log/apache2/access.log | sed "s/Mozilla/MosaicKilla/g"
```

grep for lines containing "Mozilla", then delete all characters up to and including "Mozilla":

```
$ grep Mozilla /var/log/apache2/access.log | sed "s/^.*Mozilla//g"
```

grep for lines containing "Mozilla", then delete all characters that precede "Mozilla":

```
$ grep Mozilla /var/log/apache2/access.log | sed "s/^.*Mozilla/Mozilla/g"
```

## sort

The following examples will run strings on a file, search for user-agent (ignore case), and use various sort options

Simple alphabetic sort (may include duplicates)

```
$ strings /pcaps/fraudpack.pcap | grep -i user-agent | sort
```

Sort and unique lines. The two following sets of commands are equivalent:

```
$ strings /pcaps/fraudpack.pcap | grep -i user-agent | sort -u  
$ strings /pcaps/fraudpack.pcap | grep -i user-agent | sort | uniq
```

Get a numeric count of each unique entry:

```
$ strings /pcaps/fraudpack.pcap | grep -i user-agent | sort | uniq -c
```

Get a numeric count of each unique entry, perform a numeric sort of that count:

```
$ strings /pcaps/fraudpack.pcap | grep -i user-agent | sort | uniq -c | sort -n
```

Sort and unique lines, print the length of each unique line followed by the line itself, perform a reverse numeric sort of that count:

```
$ strings /pcaps/fraudpack.pcap | grep -i user-agent | sort -u | awk '{print length, $0}' |  
sort -rn
```

Sort on the the second comma separated field

```
$ cat /bonus/alexa/top-1m.csv sort -t, -k2
```

## WC

Determine number of lines in a file (the flag is the letter "l", not the number one):

```
$ wc -l /etc/passwd
```

## xxd

xxd creates a hexdump, or converts a hexdump into binary. A lot of malware hex-encodes web traffic or malicious payloads (such as DOS executables) in order to avoid signature matching. Useful hex patterns to look for are 4d5a90 (the magic bytes for a DOS executable: "MZ<90>"), and "DOS mode" (444f53206d6f6465, see commands below).

xxd cannot natively handle percent-encoded hex, such as "%63%67%69%2D%62%69%6E", but can if the percent signs are removed (see below).

Convert the string "DOS mode" to hex, grouped in sets of 4 hex characters (default):

```
$ echo -n "DOS mode" | xxd
0000000: 444f 5320 6d6f 6465          DOS mode
```

Convert the string "DOS mode" to hex, ungrouped:

```
$ echo -n "DOS mode" | xxd -g0
0000000: 444f53206d6f6465          DOS mode
```

Convert the hex string "444f53206d6f6465" to binary:

```
$ echo 444f53206d6f6465 | xxd -r -p
DOS mode
```

Use sed to remove the percent signs from the percent-encoded hex string "%63%67%69%2D%62%69%6E", then translate to binary:

```
echo "%63%67%69%2D%62%69%6E" | sed "s/\%/g" | xxd -r -p
cgi-bin
```

# Index

\$HOME_NET	2:78, 3:85, 3:129
\$TRUSTED	2:76-77
.dll	4:57, 4:146, 5:79
.evt	5:40-41, 5:125, 5:128
.evtx	5:40-41, 5:125, 5:128
.exe	3:2, 3:33, 3:52, 3:60, 3:62, 3:72-73, 3:106, 3:115-118, 3:120-121, 3:126, 3:129, 3:175, 4:57, 4:65, 5:101-102
.jar	2:117, 3:49, 5:37
<b>A</b>	
Abnormal	1:145, 1:165, 2:33, 2:35, 2:40, 2:136, 3:53, 3:151
Access token	1:118, 2:23, 2:154, 3:172, 4:133, 4:153, 4:155-156, 4:158, 4:162
ACT, Application Compatibility Toolkit	4:130-131
ActiveX	1:96, 1:99
Administrative accounts	2:154, 4:2, 4:96, 4:98-100, 4:102, 4:104, 4:126, 4:138, 5:25, 5:130, 5:142, 5:154, 5:156, 5:158, 5:184
Adobe Reader	1:96, 1:102, 4:27
ADS, Alternate Data Stream	4:70-71
Adversary Deception	2:3, 2:149-150
Adversary success	1:44, 3:20
Alert data	1:8, 3:63, 3:81, 3:92
Alexa	2:37, 2:129-130, 2:134-135, 3:170, 3:172, 5:85
Analysis Methodology	3:2, 3:56, 3:59
Anomaly	2:42, 3:38, 3:43, 3:50-53, 3:80, 3:121, 3:126- 129, 3:142, 5:84
Anomaly Detection	1:37, 2:33, 2:111, 3:50, 3:52-53, 3:127, 3:129, 3:142, 4:50, 5:25
Antimalware	1:57, 1:147, 2:109, 2:172, 4:3, 4:17, 4:173- 174
Antivirus	1:38, 2:172, 3:21, 3:46-48, 3:62, 3:72, 3:114, 3:124, 4:173-174, 5:99
APK	2:175
AppArmor	4:86
Application Inspection	2:94-95, 2:97-98
Application Monitoring	4:2, 4:7, 4:47
Application Whitelisting	4:47, 4:63-64, 4:72, 4:78, 4:85, 4:87-88, 4:93, 4:95, 4:184, 5:47
Application Whitelisting, Bypass	4:84
Application Whitelisting, Phase 0: Whitelist Building	4:58, 4:73-77
Application Whitelisting, Phase 1: Targeted Detection	4:78-80
Application Whitelisting, Phase 2: Strict Enforcement	4:81-82

Aplocker	4:87-91, 5:129, 5:160, 5:162
APT	2:38, 3:166, 4:165, 5:75, 5:101
argus	3:76, 3:92
ASD Top 35	5:22, 5:35
ASD Top 4	5:23
ASEPs	4:115
ASEPs, Auto-Start Extensibility Points	1:39, 1:138, 4:2, 4:115-116, 4:118
ASEPs, Registry	4:115, 5:177-182
Asset Inventory	3:86, 5:49, 5:51, 5:55-56, 5:105
Authentication	4:3, 4:133-134, 4:144-146, 4:153-155, 4:160, 4:163, 4:169, 4:171, 5:33, 5:81, 5:93, 5:153
Authentication Policy Silos	4:169
Autoruns	1:138, 4:2, 4:116, 4:118
awk	2:130, 2:135, 3:40, 3:154

## B

Backdoor	1:52-53, 1:113
Base64	3:144, 4:49, 4:146, 5:139
Baseline Configuration	4:2, 4:30-33, 4:36-38, 4:40, 4:76, 4:95, 5:72
Baselining	4:41, 4:116, 4:185, 5:48
Behavior	2:9, 2:106-108, 3:49-50, 3:133, 5:101
Bejtlich	1:8, 1:60, 3:9, 3:11, 3:16, 3:20, 5:5, 5:9, 5:11
BITS, Background Intelligents Transfer Service	4:26, 4:28
Blacklist	1:103, 2:43, 2:52-53, 2:55-56, 2:116, 3:44, 3:46, 3:152, 4:168, 4:190, 5:99
Blue Team	1:37, 3:29, 6:3
Bogon	2:52-53
Botnet	1:54, 3:5, 3:134, 5:86, 5:103, 5:106
Bro	3:30, 3:38-40, 3:43, 3:68, 3:73, 3:88, 3:92, 3:149, 3:152-153, 3:169-170, 3:172-173
Browser	1:88, 1:96-100, 2:17, 2:113-114, 3:148-150, 3:169
Browser attacks	1:98-99

## C

C2	1:52-53, 1:113, 1:135-136, 1:141, 2:22, 2:25, 2:43-44, 2:136, 3:3, 3:106, 3:131, 3:133, 3:138, 5:85-86
C2, HTTP	3:145-146
C2, HTTPS	1:125, 1:146, 2:96, 3:3, 3:138, 3:156-157, 3:159, 3:163, 3:172, 5:103
C2, HTTPS and X.509	2:124-125, 3:45, 3:159, 3:162, 3:166-172
C2, ICMP	3:140-141
C2, non-HTTPS SSL	3:159, 3:161-162
C2, Persistent Connections	3:135-136
C2, Tor	3:164
Cached Credentials	4:153-154
CAPEX	1:63, 1:158
Carving	3:2, 3:68-69, 3:73, 3:88
CDM, Continuous Diagnostics and Mitigation	5:6, 5:10-11, 5:20
Centralized Logging, Windows	4:177-178, 5:111
Change Detection	4:40-41, 5:93-95

Change Monitoring	4:40-41, 4:185
Ciphertext	2:124
CIS Critical Security Controls	1:17, 1:128, 3:159, 4:6-7, 4:15, 4:89, 4:95, 4:97, 4:194, 5:20-21, 5:47-48
CIS Critical Security Controls, 1	3:122, 3:132, 4:62, 5:44, 5:49, 5:71, 5:84, 5:98, 5:105
CIS Critical Security Controls, 10	3:132
CIS Critical Security Controls, 14	5:105
CIS Critical Security Controls, 2	4:7
CIS Critical Security Controls, 3	4:7
CIS Critical Security Controls, 5	4:7
CIS Critical Security Controls, 8	3:132, 4:62
CIS Critical Security Controls, First Five Quick Wins	4:6-7, 4:97, 4:194, 5:47-48
CIS, Center for Internet Security	1:17, 1:128, 3:102, 3:122, 3:132, 3:159, 4:6-7, 4:15, 4:33-34, 4:36, 4:38, 4:95, 4:97, 4:194, 5:21, 5:47-48, 5:121
Cleartext	1:146, 4:103, 4:133, 4:146-147, 4:151, 4:163, 4:169
Client-Side	1:9, 1:65, 1:76-80, 1:82, 1:96, 1:102, 2:16-17, 2:21, 2:25, 2:75, 2:81, 2:89, 3:107
Command-Line Auditing	4:48, 5:138, 5:162
Content Filter	1:59, 2:115-117, 2:119, 2:121, 2:171, 3:137
Content-Type	2:117-118
Correlated Data	1:8, 3:63, 3:86
Cost per record	1:32
Cuckoo Sandbox	2:107-108, 2:155

## D

Daemonlogger	3:67
Data Breach	1:30-32, 1:35, 4:182
Data Classification	5:29, 5:31
Data compromise	1:74, 1:168, 2:35, 5:31
Daylight Savings Time	2:57-58, 3:84, 3:104
DBIR	1:30-31, 1:33-35, 1:83, 2:140, 3:19
DDoS	1:53-54, 1:72, 1:106
Debug Programs	4:101, 4:106, 4:113, 4:193
Deception Devices	2:3, 2:149-152
Deduction	3:57
Default Deny	1:147, 2:50, 2:54, 2:56, 2:59, 5:104
Defensible Network	1:7, 2:178, 3:16, 3:122-124, 3:126-127, 3:135, 3:157, 5:17, 5:27-28, 5:36-37
Detection-Oriented	1:122-123, 2:73, 4:184
DIACAP	3:8, 5:7-8
diff	4:41, 4:116, 5:56, 5:93
Dirty Word List	2:167, 2:169-170, 3:60
Display filters	2:125, 3:110, 3:118-121, 3:164
DITSCAP	3:8, 5:7-8
DLL	2:175, 3:52, 3:86, 3:129, 4:49, 4:51, 4:57, 4:92-93, 4:146, 4:187, 5:79, 5:160, 5:162
DNS, failed-dns-query	5:90
DNS, Logging	5:83-84, 5:87-90, 5:184



DNS, long-dns-query	5:90, 5:184
DNS, NXDOMAIN	5:90
DOCX	1:85, 1:103, 2:117, 2:175, 3:44, 3:85, 3:129, 3:160
Domain Generation Algorithms (DGA)	2:136-137
Domain Shadowing	2:137
DoS, Denial of Service	1:51, 1:53, 2:101, 3:33, 3:116-117
dumpcap	3:67
Dynamic Analysis	2:107-108, 2:117, 2:175
<b>E</b>	
Egress	1:3, 1:147-148, 1:171, 2:38, 2:41, 2:43, 2:46, 2:48, 2:54, 2:56, 2:59, 2:96, 2:112, 2:121, 2:177, 4:176-178, 4:184
ELK, Elasticsearch, Logstash, Kibana	2:138
ELSA	1:3, 1:171, 3:30, 3:41
Emerging Threats	3:44, 3:82, 3:85-86, 3:129, 3:133
EMET, Enhanced Mitigation Experience Toolkit	1:37, 1:39, 4:2, 4:43-45, 5:161-162
Enable-PSRemoting	5:173
Entropy	2:2, 2:124-134, 3:34, 3:52, 3:123, 3:126, 3:160, 3:164, 4:104, 5:85-86, 5:101-102, 5:132, 5:135, 5:155, 5:181
Event ID 1056, RDP Self-Signed Cert	5:146, 5:162
Event ID 1102, Event Log Cleared	5:144, 5:162
Event ID 2003, Firewall Disabled	5:150, 5:162
Event ID 2005, Firewall Rule	5:100, 5:151
Event ID 4624, Logon	5:152, 5:154
Event ID 4688, Process Creation	4:48, 5:138, 5:162
Event ID 4720, User Creation	5:41, 5:141, 5:162
Event ID 4722, User Enabled	5:41, 5:141, 5:162
Event ID 4724, Password Reset	5:141, 5:162
Event ID 4732, User Added to Group	5:41, 5:143, 5:162
Event ID 4738, Account Changed	5:141, 5:162
Event ID 7030, Interactive Service Error	5:18, 5:136-137, 5:162, 6:16, 6:20
Event ID 7045, Service Creation	5:18, 5:132, 5:135, 5:137, 5:148, 5:162
Event IDs, Applocker	4:90-91, 5:160, 5:162
Event IDs, Removable Media	5:148
Event Logs, Critical Windows Events	5:3, 5:124, 5:131, 5:137-138, 5:140, 5:142, 5:144-145, 5:147-149, 5:152, 5:160-162, 5:184, 6:16
Event Logs, Damaged	5:126
Event Logs, Windows	5:120, 5:126, 5:128, 5:130
Event Query, Windows	5:118
Event Viewer	5:117, 5:125-128, 5:141, 5:143, 5:146, 5:148, 5:150
eventvwr	5:117, 5:125, 5:127
EXE	2:175, 3:2, 3:33, 3:52, 3:60, 3:62, 3:72-73, 3:86, 3:106, 3:115-116, 3:120-121, 3:129, 3:175, 4:57, 5:102, 5:162
EXE, MZ	3:33, 3:71, 3:117-119, 3:129
EXE, PE	3:72, 3:86, 3:117, 3:119, 3:129

EXE, This program cannot be run in DOS mode	3:33, 3:116-118
EXE, This program must be run under Win32	3:117, 3:119
EXE, This program must be run under Win64	3:117
EXE, Transfer	3:2, 3:124, 3:126, 3:129, 3:175
Executable	1:85, 3:115, 3:124, 3:126, 4:67-70, 4:73, 4:76-77, 4:79, 4:92, 5:99
Exfiltration	1:107, 1:136, 1:146, 1:148, 2:14, 2:24, 2:35, 2:41-44, 2:57-60, 2:67-68, 2:80, 2:82, 2:88-89, 2:93, 2:99-101, 2:109, 2:121
Exploitation	1:49-50, 1:75, 1:80, 1:99, 1:105, 1:113, 1:124, 1:132, 1:136, 2:14, 2:21, 2:89, 2:152, 4:95, 4:114, 4:133
Extracted data	3:63, 3:68

## F

Fallacies	1:38-39, 3:152
False Negative	3:124
False Positive	2:65, 2:80, 2:85, 2:101, 2:126, 2:129-130, 2:155, 3:24, 3:52, 3:128-129, 4:78-80, 4:188, 5:37
File Analysis	2:172, 2:175
File Carving	3:69, 3:73
File Integrity Monitoring	4:41, 4:64, 4:181, 4:185
File-format	1:96, 1:102-103, 3:64, 3:114, 4:189
FIPS 199	5:30
Firewalls	1:59, 2:63, 2:73, 2:86, 2:91-94, 2:96-101, 2:115, 2:161, 2:171, 2:177
Flash	1:96, 1:99-100, 4:21, 4:25, 5:23
Flow Data	1:7, 2:29-32, 2:40, 2:158, 2:177, 3:76
Forensics	1:160, 2:106, 2:140, 2:169, 3:34, 3:60, 4:41, 4:50, 4:74, 4:92, 4:187-188, 5:126
Forward Proxy	2:115, 2:121-122
Framework	1:100, 1:117, 1:128, 2:95, 2:167, 3:39, 4:190, 5:8, 5:174
freq.py	2:2, 2:132-138, 5:86

## G

GeolP	2:32, 2:39, 2:52-53, 2:55
Get-WinEvent	4:48, 5:18, 5:40-41, 5:137-138, 5:141, 5:143-144, 5:146, 5:148, 5:150, 5:161-162
grep	2:129, 2:135, 3:5, 3:30, 3:37, 3:74-75, 3:149, 3:151, 3:153-154, 3:173, 5:65-66, 5:89
Group Policy	4:23, 4:37, 4:87-88, 4:111, 4:127, 4:140, 4:177, 5:111-112, 5:120

## H

Hanlon's Razor	3:49, 5:37
HIDS, Host Intrusion Detection System	1:30, 4:174, 4:181-186
HIPS, Host Intrusion Prevention System	4:174, 4:181-184, 4:186, 5:33
HKLM\Security\Policies\Secrets	4:106
HoneyAdmins	2:154
Honeyclients	2:155

Honeynets	2:150, 2:152
Honeypots	2:3, 2:149-154
HoneyRobots.txt	2:154
HoneySAT	2:154
HoneyTable	2:154
HoneyTokens	2:3, 2:180
HoneyUsers	2:154
HTTP GET	3:36, 3:108, 5:102
HTTP POST	1:140-141, 3:144-145
Hunt team	1:12, 1:123, 1:168, 2:7-9, 2:17, 2:141-142, 2:145-146, 3:7, 3:11-13, 3:175, 4:190, 6:12
Hunt Teams	1:12, 1:90, 1:123, 1:168, 2:7-9, 2:17, 2:38, 2:141-142, 2:145-146, 3:7, 3:11-13, 3:175, 4:190, 6:12
Hypothesis Management	3:59
<b>I</b>	
ICMP	1:146, 2:31, 2:47-49, 3:52, 3:109, 3:135, 3:138-142
ICMP 0:0, Echo Reply	3:141
ICMP 8:0, Echo Request	3:52, 3:139, 3:142, 6:4
IDS Frontends	1:65, 1:67-69, 3:2, 3:30-34, 3:65, 3:82, 3:112
Impersonation Level	4:155-158, 4:162
Inbound Filtering	2:28, 2:52
Incident Response	1:29-30, 1:37, 1:160, 1:162, 3:13, 3:102, 3:135, 3:137, 4:41, 4:188
Indicator Identification	2:167
Indicators	1:134-135, 2:166-170
Indicators of Compromise	2:170, 4:188
Interactive Logon	4:154, 4:160, 4:171, 5:154
Internal SI Firewalls	2:161, 2:177
Inventory, Active Scanning	5:49, 5:51-55, 5:61, 5:105
Inventory, Passive Discovery	3:30, 3:92, 5:51, 5:60-61, 5:63-66
Invisibility	2:77
IPFIX	2:29-31, 2:40, 2:158, 2:177, 3:76
IRC	1:108, 1:133, 2:47, 2:51, 2:69, 2:76, 2:96, 2:100, 3:39, 3:53, 3:66, 3:72, 3:138, 4:84, 4:87
IRC C2	2:96, 2:100, 3:138
ISCM, Information Security Continuous Monitoring	5:6, 5:8, 5:12-14
<b>J</b>	
JAR	2:105, 2:117, 2:175, 3:49, 5:37
Java	1:96, 1:99-101, 2:113, 2:117, 4:21, 4:25, 4:27, 4:45, 5:23, 5:75
JavaScript	1:99, 2:113
Joe Sandbox	2:175
<b>K</b>	
Kansa	4:190-191
Kill Chain	1:134-135, 2:166-167, 2:169

## L

LanMan Hash	4:140-141
Layer 3	1:61, 1:127, 2:29, 2:32, 2:52, 2:54-56, 2:92, 2:94, 2:96-97, 2:159, 3:107, 3:126
Layer 4	1:61, 2:29, 2:32, 2:54, 2:56, 2:92, 2:94, 2:96, 3:107
Layer 7	1:16, 1:61, 1:127, 2:32, 2:42-44, 2:49, 2:92, 2:94, 2:97-98, 2:100, 3:64, 3:78, 3:107, 5:97
LiveSSP	4:148, 4:151, 4:163, 4:169
Log data	1:8, 2:42, 3:63, 5:16, 5:126
Log files	3:8, 5:5, 5:126, 6:9
Log Monitoring	4:38, 4:48, 4:185, 5:16, 5:109, 5:124, 5:129
Log Review	1:30, 4:181
Log Settings, Windows	5:119, 5:121
Logon Types, Type 10	4:154, 5:154
Logon Types, Type 11	4:153-154
Logon Types, Type 2	4:154, 4:158, 4:160, 4:171, 5:154
Logon Types, Type 3	2:49, 4:112, 4:154, 5:155, 5:158-159
Logon Types, Type 4	4:154
Logon Types, Type 7	4:148, 4:154, 6:8, 6:14
Long Tail Analysis	1:38, 4:190-191, 5:38-41, 5:167, 5:181, 5:184
LSA Secrets	4:106
lsass.exe	4:65
LUA Buglight	4:131

## M

M-Trends	1:29, 1:34-35, 1:90, 1:140, 1:143, 2:140, 3:19, 4:164
Malvertising	1:82, 1:89
Malware Detonation Devices	1:7, 1:59, 2:2, 2:63, 2:105-106, 2:155, 3:124
MBSA, Microsoft Baseline Security Analyzer	5:76-79
Memory Analysis	4:187-188, 4:190
Metadata	1:8, 3:63, 3:78, 3:86, 4:58, 5:126
Metasploit	1:117, 1:143-144, 2:125, 3:47, 3:162, 4:164, 5:133, 5:135-136, 5:145, 5:156-157
Meterpreter	1:117-118, 3:116, 3:161-162, 4:49, 4:162, 5:130, 5:138-140, 5:144-145, 5:156
Microsoft Account	4:145, 4:148-151
Microsoft Office	1:96, 1:102-103, 4:33-34, 5:23
Mimikatz	4:47, 4:57, 4:93, 4:151, 4:161-170
Minnow	1:93-94
Mobile application	2:94
Mobile device	1:49, 1:92-94, 2:9, 2:113, 3:109, 4:5, 4:12, 4:20
ModSecurity	2:2, 2:71
MSSP	1:30, 1:153, 1:158-160, 1:164

## N

NAT	2:32-33
Nation-State	1:73
ndiff	5:56
NetFlow	1:7, 2:29-32, 2:40, 2:158, 2:177, 3:76

netsniff-ng	3:30, 3:65, 3:67
NetWars	1:12, 1:15, 1:172, 2:181, 3:177, 4:196, 5:186, 6:6, 6:12
Network Logon	4:112, 4:154, 5:155, 5:158-159
NGFW	1:7, 1:59, 2:2, 2:63, 2:73, 2:86, 2:91-94, 2:96-101, 2:115, 2:171, 3:107, 5:86, 5:104
ngrep	3:30, 3:37, 3:74-75
NIDS	2:2, 2:73-76, 2:79-83, 2:85-86, 3:15, 3:17, 3:30-31, 3:38, 3:43, 3:51, 3:92, 4:181
NIPS	2:2, 2:73, 2:85-89, 4:181
Nirvana fallacy	1:38
nmap	2:37, 3:30, 5:53, 5:55-56
Non-Encrypted HTTPS	3:157-158
NSA	1:36-37, 4:16, 4:38, 5:16, 5:129, 5:154, 5:159, 5:161
NSRL RDS	4:58, 4:73-77
NT Hash	4:137, 4:139, 4:141-142, 4:144-145, 4:160, 5:155
NTFS Permissions	4:100-101, 4:109-111

## O

Obfuscation	3:144, 5:139
Offense informs defense	2:164, 5:21
OpenAppId	2:2, 2:95-96, 2:103, 6:10
OpenVAS	5:73
OPEX	1:63, 1:158
OSSEC	3:92, 4:185
Outbound connections	2:34-35, 2:37, 2:40, 5:103
Outbound Filtering	2:28, 2:54-56
Outsource	1:153, 1:157-160, 1:164, 2:66

## P

pOf	5:2, 5:61-62, 5:68, 5:164
PAC	2:113-114
Packet capture, Full	1:67-68, 2:29, 3:32, 3:65-67, 3:92
Packet Data	1:67-68, 1:118, 2:29, 2:145-147, 3:32, 3:65-67, 3:92
PADS, Passive Asset Database	3:92, 5:61
Pass the pass	4:163
Pass-the-Hash	4:160, 4:162, 5:154-159
Password Hashes	4:133, 4:136-137, 4:142, 4:158, 4:162, 5:93
Passwords Hashes, Ntds.dit	4:142
Passwords Hashes, SAM	4:140, 4:142
Patching	1:80, 2:63, 2:65, 2:67, 4:7, 4:14, 4:16, 4:20-22, 4:25, 4:30, 4:67, 4:95, 5:28, 5:48, 5:75, 5:184
PDF	1:36, 1:77, 1:79, 1:85, 1:103, 2:118, 2:175, 3:107, 5:23
Perfect Attacker Fallacy	1:39
Perfect Solution Fallacy	1:38-39, 3:152

Perimeter SI Firewall	2:2, 2:46, 2:57
Persistence	1:37, 1:39, 1:114, 1:116, 1:118, 1:122, 1:136, 1:138, 2:120, 4:3, 4:16, 4:114-115, 4:186-187, 4:195, 5:176
Persistence, registry	1:39, 5:176
Persistence, service	4:115
persistent.pl	3:136-137, 5:103
Phish	1:77-79, 1:83, 1:86-87, 1:93, 2:167
Phishing	1:77-79, 1:83, 1:86-87, 1:93, 2:167
Pivoting	1:108, 1:132, 1:142, 5:152, 5:154, 5:159
Plugin	1:99-100, 4:162
Ponemon	1:32
Port Scan	5:55
Post-Exploitation	1:105, 1:113, 1:124, 1:132, 1:136, 2:14, 2:22, 2:152, 4:133, 4:186
PowerShell Remoting	4:190, 5:173-174
PPT	1:91, 1:103, 2:175, 4:141
PPTX	1:91, 1:103, 2:175
PRADS	3:30, 5:61, 5:63-66
PRADS, Passive Real-Time Asset Database	3:30, 5:61, 5:63-66
Prevention-Oriented	1:57, 1:59, 2:73
Privilege escalation	1:118, 3:13, 3:92, 4:110, 5:43
Process Monitor	4:128-129
Protected Users	4:169, 5:159
Protocol Behavior	3:43, 3:49
Proxies	2:56, 2:111-113, 2:115, 2:120-122, 2:155, 3:136, 3:144, 5:97-103
PSEXec	1:143-144, 2:125, 4:161, 5:130-136, 5:138, 5:156-158, 6:16

## R

Rainbow Tables	4:137
Red Team	3:29
Redline	4:188-189
Registry keys	3:8, 4:128, 5:5, 5:38, 5:167, 5:176, 5:179, 5:181
Remote Interactive	4:154, 5:154
Reputation	1:37, 2:40, 2:44, 2:55, 2:97, 2:119-121, 3:50-51, 4:164
Response-Driven	1:126
Restricted Admin Mode RDP	4:169
Reverse HTTP	1:118, 3:136, 5:103
Reverse HTTPS	1:118, 5:103
RFC 1918	2:52-53
Risk Informed	1:128
Risk Management	1:128, 5:8, 5:11-12
RMF, Risk Management Framework	5:9
Router	2:28-29, 2:33, 2:40-44, 2:46, 2:158, 5:94-95
RTF	1:85, 1:103

## S

Salts	4:103, 4:137-139, 4:141, 4:160, 5:155-156
-------	---

SANCP	3:92
Sandbox	1:7, 2:107-108, 2:117, 2:155, 2:175
SCAP, Security Content Automation Protocol	4:38, 5:71-73
SCCM, System Center Configuration Manager	4:26-28, 4:69
Scheduled Tasks	2:138, 4:115
SCM, Security Compliance Manager	4:37
SCUP, System Center Updates Publisher	4:27-28
Security Onion	1:65-66, 3:28-30, 3:92, 3:98, 3:142, 3:175, 5:63
SeDebugPrivilege	4:101, 4:106, 4:113, 4:166, 4:193
Sensor Placement	3:99-101
Sensor, Design	3:90, 3:92
Sensor, DMZ	2:74, 3:101
Sensor, External	3:101
Sensor, NSM	3:91, 3:98-99
Sensor, Security Onion	3:30, 3:92, 3:98, 3:142, 3:175
Sensor, Umbrella	3:100-101
Service Accounts	4:105-106, 5:154
Service Logon	4:154
Service-side	1:49-50, 1:75, 1:80, 3:109
Set-ExecutionPolicy	5:170-171
sFlow	2:29
Sguil	1:65, 1:67-69, 3:2, 3:30-34, 3:65, 3:82, 3:112
Shell	1:53, 1:69, 1:113, 1:117, 5:81, 5:98, 5:115-116, 5:130, 5:140
Shellcode	1:140, 3:32, 3:34, 4:43
SI Firewall	2:2, 2:46-47, 2:57-60, 2:91-94, 2:96-98, 2:161-162, 2:177
SID	4:155
SIEM	1:7, 1:59, 1:152, 2:3, 2:138, 2:140-143, 2:147, 3:30, 3:41, 3:62, 4:50-51, 4:58, 4:185, 5:106
Signature Evasion	3:47
Signature Matching	2:124, 3:43-44, 3:46
SiLK	3:76
Situational Awareness	1:10, 5:2, 5:43
Sniffing	1:72, 3:91-93, 3:96, 3:98, 5:53, 5:61
Sniffing, Hubs	3:94
Sniffing, Port Mirror/SPAN Port	3:93-95, 3:97, 3:100, 3:127, 3:175
Sniffing, Port Overload	3:96-97
Sniffing, Taps	1:37, 3:93-94, 3:96-97
Sniffing, Virtual	3:93, 3:98
Snort	2:2, 2:77-78, 2:95, 2:103, 3:30, 3:38, 3:40, 3:43, 3:67, 3:83-84, 3:142
Snort Frontends	1:65, 1:67-69, 3:2, 3:30-34, 3:65, 3:82, 3:112
SOC	1:150-166, 4:9, 4:93
Social Engineering	1:76, 1:82-83, 4:114
SP 800-117	5:72
SP 800-137	5:8, 5:12-15, 5:20
SP 800-37	5:8
Spam	1:51, 1:72, 2:66, 3:85, 5:100, 5:106-107
Splash Proxy	2:120
Splunk	3:30, 3:41

Spoofed	2:40
SQL Injection	2:9, 2:13-15
SRP, Software Restriction Policies	4:87-88
SSH	1:146, 2:94, 2:100, 3:39, 3:136-137, 3:141, 5:81
SSL	1:118, 2:38, 3:39, 3:156-164, 3:169-170, 3:172, 4:55-56, 4:69, 5:146
SSO, Single Sign-On	4:136, 4:144-146, 4:148, 5:155
SSP, Security Service Provider	1:153, 4:3, 4:144-146, 4:148, 4:163
Stage 2	1:138, 3:13, 3:115-116, 3:127, 5:24
Statistical Data	3:63, 3:80
STIGs, Security Technical Implementation Guides	4:38-39, 4:44
Strategic Web Compromise	1:90
String data	3:63, 3:74-75, 3:88
strings, command	3:5, 3:60, 3:74-75, 3:88, 3:116, 3:149, 3:151, 3:154
Suricata	3:30, 3:38, 3:40, 3:43, 3:142
Sysmon	4:2, 4:50-58, 4:60
Sysmon, syntax and configuration	4:2, 4:52-54

## T

Tagged data	3:83-85
Tailored Access Operations (TAO)	1:36
Target Breach	1:33, 2:25, 3:21-25, 3:139, 4:182
TCP/21, FTP	2:92, 2:94, 3:22-23, 3:39, 3:78, 4:69, 5:98
TCP/22, SSH	1:146, 2:94, 2:100, 3:39, 3:136-137, 3:141, 5:81
TCP/3389, RDP	4:153, 4:158, 4:169, 5:107, 5:129-130, 5:145-146, 5:151, 5:162
TCP/443, HTTPS	1:118, 2:38, 3:39, 3:156-164, 3:169-170, 3:172, 4:55-56, 4:69, 5:146
TCP/6667, IRC	2:96, 2:100, 3:39, 3:53, 3:138
TCP/80, HTTP	1:50, 1:118, 1:127, 1:140-141, 2:38, 2:41, 2:94, 3:39, 3:44, 3:78, 3:135, 3:138, 3:144-145, 3:151, 3:156-164, 3:169, 3:172, 4:69, 4:146
tcpflow	3:76
Teensy	1:91
Threat Intelligence	1:133, 2:3, 2:97, 2:105, 2:119, 2:164-165, 2:168, 2:172, 4:187
ThreatExpert	2:175
ThreatTrack	2:175
Time synchronization	2:56, 3:90, 3:102-104
Time Zone	3:103
TLS	1:118, 3:13, 3:116, 3:157, 3:159-162, 3:164, 3:166
True Positive	2:129, 3:24, 3:129, 4:78-79
tshark	3:35, 3:37, 3:76-77, 3:79, 3:149, 3:172
tspkg	4:163
TTPs	1:133, 2:165



Tunnel	1:146, 2:52, 3:136-138, 3:140-142, 3:159, 3:163, 5:37, 5:99, 5:103
Two-Factor Authentication	4:134, 4:171

## U

UAC, User Account Control	4:121-122, 4:124-128, 5:182
UDP/123, NTP	2:56, 3:90, 3:102
UDP/53, DNS	2:12, 2:38, 2:50, 2:114, 2:136, 3:52, 3:138, 4:69, 5:83-87, 5:90, 5:184
UDP/69, TFTP	4:69
URL Analysis	2:171, 2:174-175
USB	1:82, 1:91, 1:146, 3:109, 4:69, 5:40, 5:126, 5:148, 5:162, 5:172, 5:180, 6:17
User Rights, Windows	4:100-101, 4:109, 4:112, 4:155, 4:193
User Visibility	2:97
User-Agent	3:3, 3:40, 3:106, 3:148-152, 3:154, 3:175
UTC	1:30, 1:134, 3:102-103

## V

Virtual Patching	2:63, 2:65, 2:67
VirusTotal	2:172-174, 4:51, 4:58, 4:116, 4:167
Visibility	1:127, 1:137-138, 1:165, 2:43-44, 2:77, 2:89, 2:97, 2:100, 2:157, 3:175, 4:182, 5:13
VLAN ACLs	2:157, 2:159-161, 4:182
VNC	1:118, 4:158, 5:136
VPN	1:17, 1:25, 1:38, 1:70, 1:146, 1:172, 2:34, 2:181, 3:132, 3:135-136, 3:159, 3:177, 4:196, 5:37, 5:44, 5:58, 5:99, 5:105, 5:185-186
Vulnerability assessment	3:8, 5:79
Vulnerability Scanning	2:15, 4:19, 5:2, 5:44, 5:55, 5:70-71, 5:73

## W

Watering Hole	1:82, 1:90, 2:16-21, 4:122
WDigest	4:146-148, 4:151, 4:163, 4:166, 4:169
Web Application Firewall	1:7, 2:2, 2:62-63, 2:65-69
wecutil	5:116
WFAS, Windows Firewall with Advanced Security	4:177-179, 5:129, 5:149-150, 5:162
Whitelist Integrity	4:66
Windows Event Collector	5:116
Windows Remoting	5:115, 5:173
winrm	5:115, 5:173
Wireshark	1:65, 1:68-69, 2:125, 3:32, 3:35-36, 3:64, 3:67, 3:69, 3:80, 3:118-121, 3:140, 3:158, 3:161, 3:164
WMF	1:85, 1:103
WPAD	2:113-114
WSUS, Window Server Update Services	3:123-124, 4:22-28

## X

X.509	2:124-125, 3:159, 3:162, 3:166-172
XLS	1:103, 2:175, 4:71
XLSX	1:103, 2:175, 4:71

XOR	1:140, 3:144
<b>Z</b>	
Zero-copy	3:67
Zero-day	1:37, 4:16, 5:75
Zone.Identifier	4:70-71