Index

.vmdk	1:162
.vmsn	1:162
.vmss	1:162
.vmx	1:162
/dev	1:176, 1:183-184, 2:112, 4:74, 5:46-47, 5:64
/etc	1:113, 1:176, 1:178-179, 1:183, 1:193, 1:202, 2:72, 2:113, 2:117, 2:127, 4:5, 4:24-26, 4:31, 4:34, 5:64, 5:66, 6:48
/etc/passwd	1:113, 1:176, 1:183, 4:24-25, 4:31, 4:34, 6:48
/etc/shadow	1:176, 1:183, 4:5, 4:24-26, 4:31, 4:34, 6:48
/lib	1:176, 1:190, 3:27, 3:106, 3:110
/mnt	1:176
/opt	1:176, 1:181, 1:186, 1:199, 3:54
/proc	1:176, 5:46, 5:53
/root	1:176, 1:183, 3:59, 3:97, 5:50, 5:56, 5:59, 5:103-104
/tmp	1:176-177, 1:180, 4:34, 5:64, 6:48
/usr	1:176, 2:72, 4:20, 5:64
/var	1:176, 1:202, 3:58, 3:106, 3:110, 5:66, 5:70
3DES	4:13
802.11	5:125

A

Abel	1:144, 2:5, 2:91
abs	1:9, 1:45, 1:77-78, 1:102, 1:158, 1:164, 1:167, 1:171, 1:175, 1:179, 1:185-187, 1:192, 1:197, 1:201, 1:207, 2:2, 2:46, 2:65, 2:112, 2:119, 2:143-144, 3:56, 3:65, 4:2, 4:65, 4:69, 4:106, 5:9, 5:39, 5:83, 5:95, 6:6
Absolute Reference	1:179
Account harvesting	4:2, 4:76-77, 4:79, 4:81
Acrobat	3:101
Active Directory	4:5, 4:18-20, 4:47, 4:55-56
ActiveX	4:117
Address Resolution Protocol (ARP)	2:103, 2:138, 3:2, 3:28-30, 3:32-33, 3:37,

	3:50, 3:52, 3:57-58, 6:14
ADMIN$	2:132-133, 2:136
Adobe Reader	3:82, 3:101
Advanced Intrusion Detection Environment (AIDE)	5:57
advfirewall	1:63, 6:5
Aircrack-ng	2:75-76
Airdecap-ng	2:76
AirMagnet	2:85
American Registry for Internet Numbers (ARIN)	6:20
AntiVirus (AV)	1:21, 1:48, 1:53, 1:106, 1:121-122, 1:139, 1:142, 3:9, 3:101, 3:104, 3:109, 3:111, 3:113-114, 4:57, 4:67, 4:70, 4:138, 5:9-10, 5:18, 5:56, 5:77
API Hooking	5:36, 5:39
Application Whitelisting	3:89, 3:104, 3:113, 4:70
application.evtx	5:81
apropos	1:205
archive.org	2:46
Armitage	3:81
Arpspoof	3:32-33
Aruba Networks	2:85
ASLEAP	2:80
Assembly	2:119, 3:71, 3:75, 3:109, 3:111, 5:19, 5:101
Assign special privileges	5:86
Assigning Handlers	1:44
ATT&CK Framework	1:82
Attestation Forms	1:84
Aurora	1:135
autorunssc.exe	1:130
AutoStart Entry Points (ASEPs)	1:67-68, 1:132
AutoStart Entry Points (ASEs)	1:67
Avatar	5:52

B

Backdoor	1:50-52, 1:61, 1:101, 1:106, 1:108, 1:112, 1:133, 1:187-188, 1:200, 2:79, 2:138, 3:12, 3:15-16, 3:20-21, 3:34, 3:56, 3:114, 4:64, 5:2, 5:6-7, 5:9-10, 5:14-16, 5:18, 5:22, 5:32-34, 5:41, 5:43, 5:47, 5:92, 5:97,

	5:102, 5:135, 6:13, 6:19, 6:27, 6:31, 6:34-36, 6:41
Backdoor Factory	3:34, 3:114
Badsum	2:117
Baidu	2:44, 2:47
Banner	1:22, 1:26, 1:145, 1:150, 2:58, 2:63, 2:70, 5:109
Banners	1:22, 1:145, 1:150, 2:58, 2:63
Base64	1:65, 1:74, 3:106, 4:25, 4:117
Baselining	1:130, 5:85
bcrypt (Password Hashing)	4:13, 4:28
Bettercap	3:32, 3:34, 3:39, 3:47-48, 3:56
BeyondTrust	2:122
Bind shell	3:83
Binders	5:18
Bing Diggity	2:50
BlackShades	5:9
Bloodhound	2:139
Blowfish	4:13, 4:24-25, 4:33, 5:111-112
Blue Coat	1:147
Blue Pill	5:48
Border Gateway Protocol (BGP)	5:153
Botnet	1:96, 1:121, 4:64, 4:66, 4:131, 4:133, 4:135
Bots	2:51, 2:108, 4:2, 4:59-70, 4:132, 4:138, 5:150
Bridged network	1:166, 4:37, 6:5-6
Browser Exploit Against SSL/TLS (BEAST)	3:46
Browser Exploitation Framework (BeEF)	3:32, 4:2, 4:72, 4:103
BSDI	4:33
btmp	5:70-71
Bugtraq	1:16, 1:81, 5:158-159
Burp Pro	4:78-80, 4:116
Burp Suite	4:89, 4:116

C

C$	2:132-136, 2:140, 2:142, 3:55, 6:49
Cable	1:11, 1:41, 1:94, 1:98, 2:7, 5:150
Cache	1:120-121, 1:131, 2:45-47, 2:51, 2:58, 3:29-30, 3:32-33, 3:37, 3:58, 3:96, 4:38-39, 4:42-43, 4:127-129, 6:14

Cain	1:46
Case Classification	1:89
cat	1:113, 1:183-184, 2:83, 3:9, 3:16, 3:106
cd	1:54, 1:171, 1:175, 1:177-180, 1:182, 1:185, 1:192, 1:197, 1:201-202, 2:140, 3:85, 3:107, 4:21-22, 4:37, 4:39, 4:44, 5:24, 5:63
Center for Internet Security (CIS)	1:75, 5:54
Certificate Authority (CA)	2:22-23, 2:83, 3:41-42, 3:45, 3:57, 5:120
Chain of Custody	1:84
Checkpoint	2:40
chfn	5:33-34
Chief Information Officer (CIO)	1:90, 1:135
Chief Information Security Officer (CISO)	1:90
Chkrootkit	5:55
chmod	3:16
Chrome	2:125, 3:42, 4:107-108, 4:114
chsh	5:33-34
Cisco	2:63, 2:85, 4:135, 4:139, 5:54, 5:153
Cisco Guard	4:139
Citrix	2:118, 4:120
Clear screen	1:170
clearev	5:82
cloak.c	5:71
Cobalt Strike	3:108
Code Caves	3:114
Code Seeker	4:120
CodeSonar	3:95
Command and Control (C2)	1:120, 1:122-123, 4:66, 5:52, 5:101-102
Command history	1:170
Command Injection	4:2, 4:83-86
Common Vulnerabilities and Exposures (CVE)	1:81
Compensation Plan	1:31
Compression Ratio Info-leak Made Easy (CRIME)	3:46
Computer Incident Response Team (CIRT)	1:37
Computer Security Incident Handling Guide	1:15
Conficker	4:61
Confidential	1:145, 2:84, 2:144
configure	1:81, 1:101, 1:128, 1:130, 1:171, 1:175, 1:185,

	1:192-193, 1:197, 1:199-201, 1:205, 2:61, 2:104, 2:122, 2:144, 3:39, 4:11, 4:54, 4:57, 4:103-104, 4:108, 5:14, 5:57, 5:95
Containment	1:2, 1:15, 1:18, 1:81, 1:83, 1:86-102, 1:104, 2:46, 2:65, 2:85, 2:96, 3:59, 3:97, 4:57, 4:70, 4:86, 4:95, 4:109, 4:121, 4:139, 5:59, 5:104, 5:117
Containment Checklist	1:15
Content Addressable Memory (CAM)	3:26
Content Management System (CMS)	5:133-148
cookies	4:83, 4:97-101, 4:105, 4:108, 4:113, 4:115, 4:139, 6:55
Copyrights	1:11
Corroborating Evidence	1:13-14
Counter Hack Challenges	1:37
Country-Specific Cybercrime Laws	1:155
Coverity	3:95
Covert Channel	5:4, 5:94, 5:97-98, 5:100-101, 5:103-104, 5:106, 6:36
Covert_TCP	5:4, 5:97-104
cp	1:171, 1:175, 1:185, 1:187, 1:192, 1:197, 1:201, 3:110, 5:75
CpuHog	4:124
Cracking Modes	4:32
Crazyradio PA USB Stick	2:83
CreateRemoteThread	5:36
Credential Guard	4:45, 4:55, 4:57
Crontab	5:35
crontab	5:35
Cross-Site Scripting (XSS)	4:3, 4:94, 4:97-109, 4:111, 4:117, 4:120, 5:129, 6:55
Crown Jewels	1:136
Cryptcat	3:9
CTRL-C	1:170, 4:34
CTRL-L	1:170
CTRL-R	1:170
CyberCPR	1:92
Cybercrime	1:155
CyberSponse	1:91

D

Dameware	5:9
Data Execution Prevention (DEP)	3:91
Data Loss Prevention (DLP)	2:50, 4:95, 5:102
DefCon	1:16, 5:157
Defense-in-Depth	2:109
Denial-of-Service (DoS)	1:96, 2:7, 2:11, 2:57, 2:81, 2:85, 2:125, 3:80, 4:3, 4:64, 4:68, 4:123-124, 4:131-139, 4:141, 6:14
dig	1:4-5, 1:25, 1:88, 1:97, 1:161, 2:9, 2:19, 2:33-36, 2:50, 2:61, 2:64, 2:75, 3:45, 3:101, 3:114, 4:41-43, 5:24, 5:51, 5:110, 5:125, 5:148, 6:26, 6:44
Digital Millennium Copyright Act (DMCA)	2:9
Disciplines	1:30
Distributed Denial-of-Service (DDoS)	4:68, 4:131-134, 4:138-139
DLL Inject	3:83, 5:36, 5:39
dlllist	5:23, 5:28
DLP Diggity	2:50
DNS attack	3:37, 3:53, 4:131, 5:101
Domain Name Service (DNS)	1:94, 1:107, 1:120-121, 2:2, 2:33-37, 2:54, 2:57, 2:99, 2:102-103, 2:138, 3:4, 3:9, 3:13, 3:28, 3:31, 3:37-39, 3:41, 3:53-55, 3:58, 3:96, 4:3, 4:66, 4:84, 4:102, 4:126-129, 4:131, 5:100-101, 5:122-129, 5:139, 5:153, 6:3, 6:20, 6:22, 6:24, 6:26, 6:44
Domain Password Audit Tool (DPAT)	4:47
Domain Trusts	2:138
DomainToMXrecord_DNS	2:54
DomainToPerson_PGP	2:54
DomainToPhone_Whois	2:54
double dash (--)	4:90
Drive Duplicator	1:98
Drive-By Pharming	4:102
DSL	5:150
Dynamic Host Configuration Protocol (DHCP)	1:193, 3:57

E

Ebowla	3:114
Echo Request	1:195, 2:92, 2:95, 2:103, 4:84, 6:3, 6:8

Edgar database	2:40
Editing shell history	5:68
Egress Traffic	1:120
Eject	1:171, 1:175, 1:185, 1:192, 1:197, 1:201, 6:2
Elasticsearch	5:83
Elasticsearch, Logstash, and Kibana (ELK)	5:83
EmailAddressToEmailAddr_SignedPGP	2:54
Emergency Action plan	1:33
Emergency Communications plan	1:33
Emotet	5:36
EnCase	1:41, 1:153, 3:101
enum	1:49, 2:48, 2:131-133, 2:136-138, 2:141, 3:6, 3:39, 4:78, 6:13, 6:30, 6:46
enumalsgroups	2:141
enumdomusers	2:141
Eradication	1:2, 1:15, 1:18, 1:87, 1:100-101, 1:104-108, 1:112, 2:65, 2:85, 3:97, 4:57, 4:70, 4:86, 4:95, 4:109, 4:121, 5:59, 5:104
Ettercap	3:32, 3:34, 3:39, 3:47-48, 3:56
Event IDs	5:86
Event Logger	5:81
eventquery.vbs	1:72
eventvwr.msc	1:72
Exabeam	5:85
Excel	1:21, 1:28, 1:75, 1:123, 1:128-129, 2:6, 2:10, 2:47-48, 2:50, 2:90, 2:107, 3:101, 3:105, 3:107, 3:114, 4:19, 4:117, 5:18, 5:22, 5:54, 5:81, 5:110
Executive Summary	1:15, 1:116
Explicit Congestion Notification (CC)	2:11, 2:75, 2:105, 3:28, 3:30
Exploit Database	2:44
exploit-db.com	2:44, 3:69
Extensible Authentication Protocol (EAP)	2:73, 2:80-81, 2:84
Extension mechanisms for DNS (EDNS)	4:127, 4:129
External mode	4:32
EyeWitness	2:107

F

fastdump	5:22
fgdump	1:53, 4:52, 6:13

fgets	3:64, 3:71
Fiddler	4:116
File Maker	2:49
File Streaming	5:75
File System Structure	1:176, 5:55
File Transfer Protocol (FTP)	1:146, 1:150-151, 2:58, 2:95, 2:100, 2:103, 2:140, 3:13, 3:28, 3:53, 4:67, 5:126-130, 6:38
Filescan	5:23
filetype:	2:47
FIN	2:100, 2:103
find	1:58, 1:93, 1:123, 1:181, 1:186-187, 1:190-191, 1:203, 2:49, 2:110-112, 3:20, 3:71, 3:73, 3:80, 4:2, 4:21, 4:84-86, 5:25, 5:35, 5:52, 5:101
FiOS	5:150
FireEye	5:58
Firewall	1:48, 1:50, 1:63, 1:81, 1:94, 1:101, 1:107, 1:120, 1:123, 1:137, 1:142-143, 2:23, 2:40, 2:65, 2:96, 2:103, 2:109, 2:117, 2:119, 2:143, 3:17, 3:21, 3:57, 3:85, 4:57, 4:86, 4:95, 4:102, 4:105, 4:120, 5:12, 5:92, 5:101-102, 5:122-129, 5:133-148, 6:5, 6:18
Firewire	3:4
FIRST	1:89, 5:25
First in, First Out (FIFO)	3:18-20
Flame	3:114
Flash	1:13, 2:50, 3:82, 3:101, 4:107, 5:63, 5:110
Flash Diggity	2:50
Flawfinder	3:95
FOCA	2:48-49
Fontanini	5:53
FOR loop	1:70, 2:134
Forcepoint	1:147
Forensics Images	1:35, 1:37, 1:97, 1:100
ForeScout	5:58
Fortify	3:95
free	1:15, 1:37, 1:39, 1:46, 1:70, 1:75, 1:78, 1:91-92, 1:97, 1:108, 1:123, 1:151, 1:155, 1:161, 2:9, 2:18, 2:21, 2:23, 2:25, 2:27, 2:41, 2:48, 2:50, 2:53, 2:57, 2:67, 2:70, 2:90, 2:110, 2:122-123, 2:136, 3:27, 3:36, 3:94-95, 3:107, 4:18, 4:74, 4:106, 4:116-118,

	5:10, 5:19-20, 5:22, 5:24, 5:36, 5:38, 5:46, 5:54-57, 5:83, 5:85, 5:94, 5:137, 5:161-162, 6:9, 6:17, 6:35, 6:37
FreeBSD	2:125, 3:27, 4:33, 4:48
FTK	1:41, 1:153
FTK Imager Lite	1:41, 1:153
Full-Disk Encryption (FDE)	3:7

G

Gcat	1:132, 5:102
gedit	1:67, 1:171, 1:175, 1:182-185, 1:188, 1:192-193, 1:197, 1:201, 3:110-112, 4:53
Generic Route Encapsulation (GRE)	4:68
gets	1:95, 1:97, 1:107, 1:195, 2:49, 3:19, 3:32, 3:48, 3:64, 3:71, 3:77, 3:92, 3:100, 4:92-93, 4:97, 4:102, 4:118, 4:121, 5:100, 5:120, 5:158
getws	3:71
Ghost	3:109-110, 3:112, 5:9, 5:15
GhostRAT	5:9, 5:15
Ghostwriting	3:109-110, 3:112
Global Positioning System (GPS)	2:69, 3:86
Gnu Privacy Guard (GnuPG)	1:35, 1:46
Golang	2:48, 3:39, 3:114
Google Hacking Database (GHDB)	2:44, 2:48
Google Photo	2:41
Google Rapid Response (GRR)	1:39-40
Google's cache	2:46
GrammaTech	3:95
grep	1:171, 1:175, 1:185, 1:192, 1:197, 1:201-203, 2:74, 2:112, 4:108
Group Membership	2:138
Grsecurity	3:90

H

Hacktivism	2:10
Hak5	2:77, 2:83, 3:4, 3:6
Hashcat	4:2, 4:30, 4:35-44, 4:50, 4:56
hashdump (Meterpreter)	4:21-23, 4:31, 4:33, 4:37, 4:44, 4:52, 6:47

HBGary	5:22
head	1:90, 1:115, 1:183
Heartbleed	3:45
Hidden Files	5:35, 5:43, 5:64, 6:37
Hidden Form Elements	4:113
High Orbit Ion Cannon (HOIC)	4:137
History	1:144, 1:170, 1:188, 2:49, 3:101, 4:59, 4:103, 4:117, 5:3, 5:9, 5:41, 5:67-68, 5:73, 5:126, 5:140-142, 6:37
HKEY_CURRENT_USER (HKCU)	1:67
HKEY_LOCAL_MACHINE (HKLM)	1:67, 3:115, 4:46, 4:55
Honeynet	1:23, 5:157
Honeynet Project	1:23, 5:157
Hop Limit	2:91, 2:93
Host Info (HINFO)	2:34
Host-only network	1:166
Hostapd-WPE	2:80-81
HTML5	2:124-125, 3:35, 5:151
Human Interface Device (HID)	2:83, 3:5-6
Hybrid Attack	4:10
Hydan	5:4, 5:109, 5:111-114, 6:54
Hydra	4:8, 5:125-129

I

I Love My Neighbors	2:79
ICMP	1:195, 2:92-93, 2:95, 2:103, 2:105, 4:84, 5:4, 5:90, 5:94-95, 5:97, 5:103, 6:3, 6:8
ICMP IP ID Sequence Generation Algorithm (II)	2:105, 6:25
ICMPCmd	5:94
ICMPShell	5:94
iconv	1:74
Identification	1:2, 1:15, 1:18, 1:43-46, 1:48-49, 1:51-52, 1:54-57, 1:80-81, 1:83-84, 1:87-88, 1:96, 1:104, 1:125, 1:137, 1:151-152, 2:13, 2:18, 2:29, 2:37, 2:42, 2:65, 2:67, 2:70, 2:85, 2:91, 2:95, 2:103, 2:109, 2:119, 2:127, 2:143, 3:44, 3:56, 3:58, 3:97, 4:57, 4:70, 4:81, 4:86, 4:94-95, 4:109, 4:121, 4:139, 5:83, 5:98-99, 5:103, 5:116-117
Identification Checklist	1:15

ifcfg	1:171, 1:175, 1:185, 1:192, 1:197, 1:201
ifconfig	1:171, 1:175, 1:185, 1:192, 1:194, 1:197, 1:201, 1:205, 5:7, 5:34-35, 5:125
imageinfo	5:23
Immunity Debugger	5:20
Impacket	4:20, 4:31, 4:56
Inappropriate Web Access	1:145
Incident Contact List	1:15
Incident Definition	1:12
Incident Handling Step-by-Step	1:1, 1:28
Incremental mode	4:32
inetd	2:113, 2:127, 5:33-34
inetd.conf	2:113, 2:127
info	1:45, 1:171, 1:175-176, 1:185, 1:189, 1:192, 1:197, 1:201, 1:204, 1:208-209, 2:21, 2:45, 2:47, 2:110, 2:147, 3:14, 3:30, 3:33, 3:79, 3:119, 4:118, 4:142, 5:70, 5:163, 6:56-57
info:	2:45, 2:141, 5:23
Insider Threat	1:149-153
InsightIDR	5:85
InsightVM	2:122
InSSIDer	2:3, 2:69-72, 2:88
Instruction Pointer	3:65-66, 3:72-73
Intellectual Property	1:3, 1:11
Interfacing with Law Enforcement	1:25
Internet Assigned Numbers Authority (IANA)	1:52, 2:99
Internet Information Services (IIS)	1:14, 1:31, 1:54, 2:49, 3:82, 4:61-62, 4:94, 4:106, 6:38
Internet Network Information Center (InterNIC)	5:123, 6:22
Internet of Things (IoT)	2:7, 2:12, 2:67, 2:74, 4:30, 5:11, 5:54, 5:151, 5:153
Internet Storm Center (ISC)	1:16, 1:46, 2:6, 5:156
intitle:	2:45, 2:49
Intrusion Detection System (IDS)	1:14, 1:21, 1:48-49, 1:112, 1:137, 1:139, 1:142-143, 1:145, 1:152, 2:3, 2:85-86, 2:95, 2:109, 2:117, 2:119, 2:127, 2:135, 2:143, 3:85-86, 3:97, 4:109, 4:138-139, 5:101-103, 5:123
Intrusion Prevention System (IPS)	1:21, 1:48, 1:101, 1:112, 1:137, 2:3, 2:65, 2:117-119, 2:135, 3:85-86, 3:89, 3:97, 4:57, 4:70, 4:138, 5:58, 5:101-102

inurl:	2:45, 2:49
Invisible Secrets	5:109
IP Don't Fragment Bit (DF)	1:14, 2:75, 2:105, 4:54
IP Initial Time to Live Guess (TG)	2:105
IPAddrToPhone_Whois	2:54
IPC$	2:132-136, 2:142, 3:55
iptables	6:5, 6:47
iTunes	3:82, 3:101

J

Jackit (wireless keystroke injection)	2:83
Java	2:27-28, 2:67, 3:35, 3:46, 3:82, 3:84, 3:93, 3:95, 3:108, 4:74, 4:89, 4:97-101, 4:103, 4:107-108, 4:116, 4:136-137, 5:12, 5:115, 5:151, 6:55
JavaScript	2:27-28, 2:67, 3:35, 3:46, 4:89, 4:97-101, 4:107-108, 4:136-137, 5:151, 6:55
Jikto	4:102
jobs	1:31, 1:141, 1:146, 1:171, 1:175, 1:185, 1:191-192, 1:197, 1:201, 4:34, 5:92, 5:152
John the Ripper (JtR)	4:2, 4:22, 4:30-31, 4:33-35, 4:48, 4:50, 6:13, 6:48
JPCert	5:84-86
Jsteg	5:109
Jump Bag	1:41

K

Kansa	1:129-133
Kerberoasting	4:35, 4:56
Kerberos Authentication TGT Request	5:86
Kerberos Service Ticket Request	5:86
Kernel-Level RootKit	6:34
Kernel-mode rootkit	5:2, 5:7, 5:41, 5:43-46, 5:48, 5:50-51, 5:54-55, 5:57-59, 5:63
Keyboard Skills	1:37
Keystroke logger	2:11, 3:35, 3:86, 5:15
Kibana	5:83
killall	2:113, 5:35, 5:68
Kismet	2:71-72, 2:74-75, 5:124-125

Klocwork	3:95
KODAK	1:136
Kon-boot	3:4, 5:52

L

LANMAN hashes	4:14, 4:45-46
Lanturtle	3:4, 3:7
lastlog	5:70-71
Law Enforcement	1:15, 1:22-25, 1:84, 1:142, 1:146, 1:150, 1:155, 2:11, 2:86, 5:117, 5:122
Leaks	1:45, 1:137, 4:69
Legal Counsel	1:22, 1:25, 1:30, 1:90, 1:153
less	1:28, 1:51, 1:60, 1:93, 1:184, 1:189, 1:196, 2:134, 3:39, 3:64, 4:19
Lessons Learned	1:2, 1:15, 1:18, 1:101-102, 1:115-117, 2:1
LHOST	2:71, 3:106, 3:110, 5:95, 6:47
Link-Local Multicast Name Resolution (LLMNR)	3:7, 3:31-32, 3:52-55, 3:57
link:	2:39, 2:45
Linkcat	3:9
LMHash	4:20, 4:46
Local Administrator Password Solution (LAPS)	4:45, 4:57
Local Security Authority Subsystem Service (LSASS)	4:52-53, 4:63
Local Security Policy	4:47
locate	1:171, 1:175, 1:181, 1:185, 1:192, 1:197, 1:201, 2:8, 2:44, 2:49, 2:60, 2:103, 4:127-128, 4:134
Log Wipers	5:71
Logon Tracer	5:85
Logstash	3:58, 5:83
logwedit.c	5:71
Loki	5:94
long-tail analysis	1:129
lookupnames	2:141
lookupsids	2:141
Low Orbit Ion Cannon (LOIC)	4:136-137
LPORT	3:106, 3:110, 6:47
ls	1:171, 1:175, 1:178, 1:180, 1:184-187, 1:190, 1:192, 1:197, 1:201, 1:204, 2:34, 2:140,

	3:85, 5:35, 5:41, 5:63, 5:68, 6:26, 6:44, 6:54
lsaenumsid	2:141
lsof	1:52, 1:196, 2:112
lusrmgr.msc	1:69

M

Machine Code	3:68, 3:75, 3:77
MacOS X	5:48
Mail eXchanger (MX)	2:34, 5:139
make	1:32, 1:62, 1:84, 1:97, 1:113, 1:170, 1:189, 1:199-200, 1:202, 2:111, 2:113, 2:140, 3:16-18, 3:20, 3:22, 3:39, 3:48, 3:83, 3:93, 3:101, 4:57, 4:69, 5:53, 6:30
Maltego	2:2, 2:53-55
Malware Diggity	2:50
Malware Domain List	1:121
man	1:171, 1:175-176, 1:185, 1:192, 1:197, 1:201, 1:204-205, 3:44, 5:64
Mantech	5:22
marry.c	5:71
Masscan	2:106
McAfee	3:101, 5:56
MD4	4:15, 4:27
MD5	1:92, 1:132, 1:142, 3:45-46, 4:13, 4:18, 4:24-25, 4:27, 4:33, 4:117, 5:95, 5:116, 5:135
mdd	5:22
Media Access Control (MAC)	1:166, 1:194, 2:68, 3:2, 3:26, 3:28-30, 3:32-33, 3:50, 3:57-58, 5:122, 5:125, 6:3
memcpy	3:71
memmove	3:71
Memoryze	5:22
Metamorphic	4:60
Metasploit	1:51, 1:186, 2:107, 2:131, 3:2, 3:71, 3:79-97, 3:110, 3:118, 4:22, 4:53-54, 4:103, 5:9-11, 5:18, 5:52, 5:82, 6:13, 6:32, 6:35, 6:47
Meterpreter	3:84-86, 3:106-108, 3:110, 4:21-23, 4:31, 4:37, 4:52, 5:15, 5:82, 6:35, 6:47
Microsoft Credential Guard	4:45, 4:55, 4:57
Microsoft Local Administrator Password	4:45, 4:57

Solution (LAPS)	
Mimikatz	2:83, 4:31, 4:55-56
Misleading Information	1:139
MITMf	3:32, 3:34-35, 3:56
MITRE	1:81-82
mkdir	1:171, 1:175, 1:180, 1:185, 1:192, 1:197, 1:201
mknod	3:18, 3:20
ModSecurity	4:94, 4:106, 4:120
MongoDB	1:49
Motorola AirDefense	2:85
mount	1:22, 1:165, 1:171, 1:175, 1:185, 1:192, 1:197, 1:201, 2:13, 2:18, 2:48, 2:73, 2:131, 2:137-138, 3:22, 3:29, 3:64, 3:68, 4:28, 4:39, 4:52-55, 4:57, 4:81, 4:123, 4:134-135, 5:15, 5:22, 5:83-84, 5:141, 5:153, 5:156, 5:158
MP3Stego	5:109
MS08-067	4:61
msconfig.exe	1:68
Msfelfscan	3:71, 3:87, 5:46
Msfpescan	3:71, 3:87, 5:46
msfvenom	3:110, 3:116, 5:18
MySQL	1:196

N

NameServer (NS)	2:19, 2:34-35, 3:31, 3:53-54
National Institute of Standards and Technology (NIST)	1:15, 4:27-28, 5:54
National Security Agency (NSA)	5:20, 5:54, 5:81
nbtstat	1:62
nc	1:187, 1:191, 1:203, 2:112, 3:13-18, 3:20, 5:18, 6:51
Ncat	1:131, 3:9, 3:93, 4:14, 4:17, 4:39, 4:94
Near-Future	5:150-151
Nessus	1:108, 2:3, 2:122-126, 2:129, 6:28
net localgroup	1:69, 6:49
net session	1:62, 2:142, 4:57
net sessions	4:57
net start	1:66
net use	1:62, 1:69, 1:113, 2:131-136, 2:142, 4:53, 6:33, 6:49

net user	1:69, 1:113, 2:134, 6:49
net view	1:62, 2:133, 2:136
NetBIOS	1:62-63, 2:131, 2:143, 3:31, 4:19
NetBIOS Name Service (NBT-NS)	3:31
Netcat	1:53, 1:203, 3:2, 3:9-22, 3:24, 3:83, 4:68, 4:132, 5:6, 5:12, 5:18, 5:22, 5:40, 6:13, 6:34-35, 6:51
NetFlow	1:123
NetMon	3:102
NetNanny	1:147
netscan	5:23, 5:25
NetScout AirCheck G2	2:86
netsh	1:63, 6:5
netsh advfirewall	1:63, 6:5
netsh firewall	1:63
netstat	1:51-52, 1:63, 1:131, 1:171, 1:175, 1:185, 1:192, 1:196-197, 1:201, 1:203, 2:110, 2:112, 5:23, 5:25, 5:35, 5:39, 5:53
NetWitness	5:58
Network Address Translation (NAT)	1:123, 1:166, 3:9
Network Operations Center (NOC)	2:41
NeXpose	1:108
Night Dragon	1:135
Nimda	1:83, 4:61
Nmap	1:52, 1:108, 1:199, 2:3, 2:36, 2:90, 2:92-94, 2:103-105, 2:115, 3:9, 3:14, 4:89, 5:123, 5:125-129, 6:13, 6:28-29, 6:45
Nmap Scripting Engine (NSE)	4:89, 6:45
No OPeration (NOP)	3:77, 3:87, 3:111
NOARCHIVE	2:51
NOFOLLOW	2:51
nohup	3:16
NOINDEX	2:51
NOP sled	3:77, 3:87
NOSNIPPET	2:51
nslookup	1:93, 2:33-35, 4:84-85, 6:26, 6:44
NT File System (NTFS)	3:86, 5:3, 5:75-77
NTLM Authentication	5:86
NTLMv1	4:15, 4:33, 4:52, 4:54, 6:30
NTLMv2	3:55, 4:15, 4:52, 4:54
Ntoskrnl.exe	5:47
null character	3:47, 3:75
nvram	1:162

O

Offensive Techniques	1:135
Open Web Application Security Project (OWASP)	4:2, 4:74, 4:89, 4:94, 4:98, 4:108, 4:120
OpenBSD	3:27, 4:33, 6:38
OpenPuff	5:110
OpenSSH	3:44, 6:38
OpenStego	5:110
OpenVAS	1:108, 2:122
OSSEC	5:55, 5:57
Out-Of-Band (OOB)	1:46, 1:92, 2:60, 2:63-65
Outliers	1:131, 3:96
Outlook Web Access (OWA)	2:118

P

packetstormsecurity.org	3:69, 5:71
Pass-the-hash	4:2, 4:52-57
passwd	1:113, 1:171, 1:173, 1:175-176, 1:183, 1:185, 1:192, 1:197, 1:201, 4:21, 4:24-25, 4:31-32, 4:34, 4:48, 5:33-34, 6:48
Password cracking	2:80, 4:2, 4:5-6, 4:8-11, 4:13, 4:16-19, 4:26-28, 4:30-38, 4:40, 4:44-48, 4:52, 5:132, 5:150, 6:13
Password guessing	1:55, 2:63, 2:73-75, 2:134-135, 4:6-8, 4:26, 4:36, 6:13, 6:32
Password Hashing	4:2, 4:13-28, 5:135
Password List (PWL)	2:74, 2:134
Password Protect BIOS	3:7
Patents	1:11
Paterva	2:53-54
Pax	3:90
PBKDF2 (Password Hashing)	4:13, 4:28
PECompact	5:19
pedump	5:23
PeepNtom	2:107
Peer Notification	1:26
Personal Healthcare Information (PHI)	1:24
Personally Identifiable Information (PII)	1:24, 4:95, 5:120
PersonToPerson_PGP	2:54
Phishing	1:21, 1:144, 2:11

phpBB	2:49
pidof	5:35
ping	1:93, 1:171, 1:175, 1:185, 1:192, 1:195, 1:197, 1:201, 2:57, 2:92, 2:94-96, 2:104, 4:84-85, 5:94-95, 5:125, 6:3, 6:5, 6:8
PingChat	5:94
Pluggable Authentication Module (PAM)	4:48
Poison Ivy	5:9, 5:14-15, 5:18
Polymorphic	3:87, 4:60, 4:69, 5:112
Polymorphic Code	3:87
Portmapper	2:103
Positive Skew Analysis	1:129
PowerBleed	3:45
PowerPoint	2:47, 3:101, 3:105
PowerShell	1:65, 1:77, 1:129-130, 1:133, 2:83, 2:137-138, 2:144, 3:6, 3:22, 3:106, 3:108, 4:54, 5:76
PowerShell Empire	2:138
PowerView	2:137
Preparation	1:2, 1:15, 1:18, 1:20-39, 1:41, 1:136, 2:37, 2:42, 2:55, 2:64-65, 2:84, 2:95, 2:109, 2:119, 2:127, 2:143, 3:21, 3:89-90, 3:92, 3:94, 3:96, 4:45, 4:57, 4:70, 4:81, 4:86, 4:94, 4:106-108, 4:120, 4:138, 5:83, 5:103, 5:116
Pretty Good Privacy (PGP)	1:33, 1:35, 1:46, 1:138, 2:54
Privacy	1:22, 1:46, 1:145, 1:150, 5:120
Privacy Law	1:22, 1:150
Private Branch Exchange (PBX)	1:138, 2:64-65
Private VLAN (PVLAN)	2:143, 3:21
Process Explorer	1:75
Process ID (PID)	1:51, 1:63-65, 1:189, 1:196, 2:110, 2:112, 4:21-22, 5:23, 5:25-27
Process Monitor	1:75
ProcessID	1:65, 5:23, 5:26, 5:28
Procurement	1:35
Project Rainbow Crack	4:18
Promiscuous Mode	1:59, 1:166, 3:26, 3:100, 5:43, 5:55
prompt	1:8, 1:66, 1:70, 1:77, 1:88, 1:170, 1:172, 1:174, 1:186, 1:190-191, 1:203, 1:206, 2:35, 2:63, 2:81, 2:110, 2:132, 2:140-142, 3:6, 3:34, 3:39, 3:80, 4:37, 4:107, 5:70, 6:54
Protected Extensible Authentication	2:80, 2:84

Protocol (PEAP)	
ps	1:65, 1:77, 1:113, 1:131, 1:171, 1:175, 1:185, 1:189, 1:192, 1:197, 1:201, 1:203, 2:47, 2:83, 3:58, 3:108, 4:21-22, 5:7, 5:35, 5:41
ps aux	1:189, 1:203
psexec	1:113, 2:131, 4:54, 6:47
pslist	5:23, 5:26-27
Pstree	5:23
Ptunnel	5:94-95, 5:103
Pulsing Zombies	4:134
PUSH	1:13, 1:18, 2:41, 2:100, 2:140, 3:13, 3:67, 3:70, 3:74, 3:76, 3:92, 3:111, 4:81, 5:12, 5:83, 5:92
Pushpin	2:41
pwd	1:171, 1:175, 1:177, 1:179-180, 1:185, 1:187, 1:192, 1:197, 1:201

Q

Quality Assurance (QA)	5:36
Qualys	1:108, 2:122
Quick UDP Internet Connection (QUIC)	5:101
QuickTime	3:82, 4:103

R

RADIUS	2:41, 2:81, 2:84, 4:48
Rainbow	4:17-18, 4:47, 5:135
Rapid7	1:108, 2:61, 2:122
Real Intelligence Threat Analytics	1:123
Real Intelligence/Threat Analytics (RITA)	1:123, 3:96, 5:58
Real Time Incident Response (RTIR)	1:91
reboot	1:163, 1:176, 1:206, 2:111, 5:13, 5:15, 5:45, 5:47, 5:64, 6:16, 6:43
Recon-ng	2:41, 2:50
Recovery	1:2, 1:11, 1:15, 1:18, 1:30, 1:32, 1:90, 1:96, 1:101, 1:105, 1:110-113, 1:115, 2:65, 2:85, 3:97, 4:14, 4:55, 4:57, 4:70, 4:86, 4:95, 4:109, 4:121, 5:59, 5:81, 5:104
Red Canary	1:82
reg query	1:67

regedit	1:67, 4:53
Registration Authority (RA)	3:45
Rekal	1:39, 1:97, 5:22-26, 5:28, 5:30
Rekall	1:39, 5:22-26, 5:28, 5:30
rel	1:171, 1:175, 1:185, 1:192, 1:197, 1:201
related:	2:45
Relative Reference	1:179
Remote Desktop Protocol (RDP)	2:49, 2:107, 2:110, 2:118, 4:8
Remote Procedure Call (RPC)	2:103, 3:91
remove.c	5:71
Remux.py	2:108
Request for Comments (RFC)	1:123, 4:85, 4:127
RESET	1:49, 1:163, 2:100, 2:117, 2:140, 3:39, 4:7, 4:81, 4:120-121, 5:99-100, 5:140, 5:143, 5:146
Responder	1:83, 1:119-120, 1:122, 3:2, 3:4, 3:7, 3:32, 3:53-56, 3:61
Retina	2:122
Return Pointer (RP)	3:67-68, 3:70, 3:73, 3:75-77, 3:87, 3:90-92
Return-Oriented Programming (ROP)	3:91
Reverse HTTP shell	5:4, 5:92
Reverse Shell	3:22, 3:81, 3:83
RFC 1918	1:123, 4:85
RFC 2671	4:127
Ring 0	5:42
Ring 1	1:123, 5:143, 6:38
Ring 3	5:42
RingZero	1:88
robots.txt	2:51
Robtex	2:48
Rootcheck	5:55
RootKit	1:105-106, 4:86, 5:2, 5:6-7, 5:32-48, 5:50-59, 5:63, 6:14, 6:34-35
Rootkit	1:105-106, 4:86, 5:2, 5:6-7, 5:32-48, 5:50-59, 5:63, 6:14, 6:34-35
Rootkit Hunter	5:55
Rooty	5:50-51
Rough Auditing Tool for Security (RATS)	3:95
rpcclient	2:3, 2:131, 2:141
rshd	5:33-34
Rubber Ducky	3:5-7
Run_On_Open	3:105

S

S-Mail	5:109
S/MIME	1:46
Sadmind	4:62
SAINT	2:122
salt	4:15-18, 4:24-27, 4:42-43, 5:135
SAM database	3:86, 4:5
SANS Investigative Forensic Toolkit (SIFT)	1:41
Sasser	4:63
sc query	1:66, 2:111
scanf	3:71
Scanrand	2:106
Scareware	5:16
schtasks	1:71
scrypt (Password Hashing)	4:13, 4:28
SearchDiggity	2:50
secpol.msc	5:36, 6:30
SECRET	1:11, 1:16, 1:34, 1:102, 1:135-136, 1:145, 1:149, 2:74, 4:17, 4:20, 4:31, 5:97, 5:109, 5:111, 5:148
Secure SHell (SSH)	1:106, 1:150, 2:118, 3:28, 3:38, 3:41, 3:44-45, 3:57-58, 3:96, 4:8, 5:10, 5:34, 5:90, 5:95, 5:136, 5:151, 6:50
SecureSafe	1:46-47
Securing the Human	1:21
Security Enhanced Linux (SELinux)	3:90
Security Event Management (SEM)	1:91
Security Information Management (SIM)	1:91, 2:104
Security Onion	5:58
security.evtx	5:81
Sendmail	5:153
Server Message Block (SMB)	1:62-63, 2:3, 2:84, 2:99, 2:131-144, 2:146, 3:53, 3:55, 4:8, 4:52-54, 4:57, 4:61, 4:86, 5:22, 6:33, 6:47
Service Controller (sc)	1:66, 2:111, 2:131
service networking	1:193, 4:37
Service Set Identifier (SSID)	2:68-69, 2:73, 2:75, 2:77-78, 5:124-125
services.msc	1:66, 2:111
Session Tracking	4:113
Set owner User ID (SUID)	3:74
SHA-1	1:142, 5:116

SHA-2	4:24-25, 4:27
SHA1	4:18, 4:28, 4:117
SHA256	1:92, 2:144, 4:13, 4:34
sha256	1:92, 2:144, 4:13, 4:34
Shadow Brokers	5:81
Shared IP ID Sequence Boolean (SS)	2:105
SharpView	2:136-137
ShellShock	4:83
Shodan	2:48, 2:50, 2:57-58
shutdown	1:97, 1:171, 1:175, 1:185, 1:192, 1:197, 1:201, 1:206
SilentEye	5:110
Simultaneous Authentication of Equals (SAE)	2:73
Single Crack	4:32
site:	1:144, 2:16, 2:45, 2:47, 2:144, 3:6, 4:98
Situational Awareness	1:43, 1:80, 2:138
Sleuth Kit	1:41, 3:101
smart_hashdump (Meterpreter)	4:22, 4:31
SMB Security Features	2:144
smbclient	2:3, 2:131, 2:140, 5:76
smbmount	2:131, 4:54
Sniffer	1:46, 1:70, 1:166, 3:26-28, 3:32-33, 3:86, 3:102, 5:43, 5:75, 5:125, 5:128-129, 5:157
Snort	1:14, 1:49, 1:101, 3:102
Social Engineering	1:21, 1:38, 2:39-40, 2:60, 3:47, 4:11, 5:15-16, 5:18, 5:132, 5:141-146, 6:43
Social Engineering (SE)	1:21, 1:38, 2:39-40, 2:60, 3:47, 4:11, 5:15-16, 5:18, 5:132, 5:141-146, 6:43
Social Engineering Toolkit (SET)	5:18
Sophos Anti-Rootkit	5:56
sort	1:122, 1:189, 2:107, 4:53, 4:105, 5:84, 5:117, 5:159, 6:12, 6:21
Source Code Analyzer	3:95
Sourcefire	5:58
sprintf	3:71
SQL Injection (SQLi)	2:48, 4:3, 4:88-95, 4:106, 4:111, 4:117, 4:120, 5:129-130, 5:132-134, 5:136
SQL Slammer	1:83
SQLInject.nse	4:89
sqlmap	4:89
srvinfo	2:141
sshd	1:196, 5:33-34, 5:41, 5:143

SSLStrip	3:32, 3:47-48
SSLStrip+	3:32, 3:48
Starbucks	2:67, 2:77
Stash	3:58, 5:83, 5:109
Static Analysis	3:95
Steganography	1:151, 5:4, 5:108-117
StegExpose	5:115
strcat	3:71
strcpy	3:64, 3:71, 3:75
Stream Control Transmission Protocol (SCTP)	5:101
strncpy	3:64, 3:71, 3:75
Structured Query Language (SQL)	1:83, 3:53, 4:3, 4:88-95, 4:106, 4:111, 4:117, 4:120, 5:27, 5:54, 5:129-130, 5:132-134, 5:136
Stuxnet	3:45, 3:114, 4:61-63, 5:45
su	1:171, 1:174-175, 1:185, 1:192-193, 1:197, 1:201, 3:107, 5:33-34, 5:146, 6:47, 6:52
SubVert	1:135, 4:83, 5:45, 5:48
Successful logon	5:86
SUID	3:74
sumfuq	5:41
Suricata	1:101, 3:102
Survey	1:15, 1:88
Symantec	1:147, 3:101, 4:102
SYN	1:39, 1:49, 1:113, 1:163, 1:183, 1:200, 2:35, 2:47, 2:63, 2:92, 2:100, 2:103-104, 2:106, 2:111, 3:6, 3:16, 3:20, 3:57, 3:64, 3:95, 4:36, 4:41, 4:44, 4:68, 4:88, 4:90-91, 4:133-135, 4:139, 5:27, 5:99-100, 5:121, 5:127, 5:129, 5:136, 5:139-140, 5:147
SYN/ACK	1:49, 2:106, 4:133, 5:100
SYS_execve	5:42, 5:45-46
Sysinternals	1:67, 1:75, 1:113, 1:130, 2:131, 5:77
syslogd	5:35
System Center Configuration Manager (SCCM)	1:128
system.evtx	5:81
systemctl	2:113

T

Tab Completion	1:170
tail	1:129, 1:183
tar	1:171, 1:175, 1:185, 1:192, 1:197-199, 1:201
Task Manager	1:64, 1:73, 1:189, 2:111, 5:13, 5:39
tasklist	1:64-66, 1:113, 5:28
TCP header	2:101, 5:98
TCP Initial Window Size (W, W1-W6)	2:105
TCP IP ID Sequence Generation Algorithm (TI)	2:105
TCP ISN Counter Rate (ISR)	2:105
TCP ISN Greatest Common Denominator (GCD)	2:105
TCP Timestamp Option Algorithm (TS)	2:105
tcpd	5:33-34
tcpdump	1:49, 2:6, 3:27, 3:102
Telnet	1:52, 1:72, 1:93, 2:58, 2:100, 3:10, 3:57, 5:34, 6:50
Tenable	1:108, 2:122-123, 2:126
TGTarget	5:132-148
THC Hydra	4:8
The Sleuth Kit	1:41
Themida	5:19
Thunderbolt	3:4, 4:69
Time Exceeded	2:93, 2:95
Time To Live (TTL)	1:14, 2:91, 2:93, 2:105, 3:33, 4:127, 4:129, 5:98
TippingPoint	5:58
Titan Rain	1:135
Trade Secrets	1:11, 1:136
Trademarks	1:11
Transmission Control Protocol (TCP)	1:14, 1:49, 1:51-52, 1:59, 1:62-63, 1:75, 1:196, 1:203, 2:37, 2:58, 2:92, 2:98-101, 2:103, 2:105-106, 2:110, 2:112, 2:117, 2:119, 2:124, 2:131, 2:143, 3:9, 3:11, 3:13-17, 3:28, 3:32, 3:34, 3:83, 3:85, 3:110, 4:66, 4:68, 4:86, 4:102, 4:133, 4:135-136, 5:4, 5:10, 5:12, 5:23, 5:34, 5:38, 5:40, 5:43, 5:94-95, 5:97-104, 5:123, 5:126, 5:129
Trend Micro	3:101
Tresorit	1:46-47
Tribe Flood Network (TFN)	4:131
Tribe Flood Network 2000 (TFN2K)	4:131

Tripwire	5:7, 5:41, 5:57
Trojan	1:52, 1:88, 1:187, 3:6, 5:2, 5:6-7, 5:9-16, 5:18, 5:22, 5:32, 5:34-35, 5:41, 6:19, 6:27, 6:31, 6:34-36, 6:41
Trojan Horses	5:2, 5:6
Trusted Platform Management (TPM)	4:57
Tunneling	5:4, 5:90, 5:97
Twitter	1:208, 2:41, 2:147, 3:108, 3:119, 4:66, 4:136, 4:142, 5:133-148, 5:163, 6:57

U

UAC (User Account Control)	3:6, 4:22
Unicorn	3:104, 3:107-108
unshadow	4:31, 4:34, 6:48
updatedb	1:181
URG	1:113, 2:55, 2:96, 2:100-101, 4:46, 4:65, 4:126, 5:98, 5:127
US-CERT	5:159
USB Boot	3:4, 3:7
User agent string	1:122, 4:81, 4:104
User Behavioral and Entity Analytics (UBEA)	5:85
User Datagram Protocol (UDP)	1:59, 1:63, 1:75, 1:196, 1:203, 2:37, 2:98-99, 2:102-103, 2:112, 2:131, 2:143, 3:9, 3:11, 3:13-15, 3:28, 3:79, 4:68, 4:126-127, 4:129, 4:136, 5:23, 5:34, 5:38, 5:43, 5:94, 5:98, 5:101, 5:123
useradd	1:171-172, 1:175, 1:185, 1:192, 1:197, 1:201
utmp	5:70-71, 5:81
UUNET	1:83

V

Validation	1:110, 4:54, 4:74
Veil	1:138, 3:104, 3:106, 4:69, 5:18
Veil-Evasion	3:106, 5:18
Virtual Network Computing (VNC)	2:107, 3:80, 3:83, 4:8, 5:2, 5:9-14, 6:34-35, 6:50
Virtual Private Network (VPN)	1:26, 1:150, 3:40, 3:57, 5:122-129
VirtualAllocEx	5:36

VirtualFreeEx	5:36
Vitriol	5:48
vmlinuz	5:47
VMware	1:3, 1:8-9, 1:77, 1:160-168, 4:68, 5:22, 5:48, 6:3, 6:5-6, 6:38
VMware Player	1:161, 1:163-164
VMware Workstation	1:161, 1:163-165
Voice Over Misconfigured Internet Telephones (VOMIT)	1:46
Volatility	1:97, 5:22
vti_inf	1:14

W

War Dialing	2:39, 2:60-62, 2:64
War Driving	2:3, 2:67-74, 2:76-77, 2:79-80, 2:82, 2:84-86
War Room	1:36
WarVOX	2:2, 2:61-62, 2:64
Wayback Machine	2:46
Web Application Attack and Audit Framework (w3af)	4:116
Web Application Firewall (WAF)	4:86, 4:120
Web Proxy	1:120, 1:122, 3:41, 3:52, 3:56, 4:115, 5:92
Web Proxy Auto-Discovery (WPAD)	3:52, 3:56-57
WebGoat	4:74
whatis	1:205
while	1:32, 1:51, 1:61, 1:71, 1:164, 3:9, 3:16, 3:20, 3:80, 3:84, 3:108, 4:85, 5:20
whoami	1:171, 1:174-175, 1:181, 1:185, 1:192, 1:197, 1:201, 6:52
Wi-Fi Protected Access (WPA)	2:73, 2:75-76, 2:80, 2:84, 4:28
WiFi Analyzer for Android	2:70, 2:72
WiFi Pineapple	2:77-79
win32k.sys	5:47
Windows 2000	1:14, 1:60, 2:7, 2:49
Windows Credential Editor (WCE)	4:54
Windows PE	1:63
WinVNC	5:13
Winzip	3:101
Wired Equivalent Privacy (WEP)	2:76
Wireshark	1:46, 2:6, 2:72, 2:76, 3:27, 3:102

wmic	1:65, 1:68, 1:113, 1:127, 2:111, 5:26, 5:28
wmic process	1:65, 2:111, 5:26, 5:28
wmic process list	1:65
wmic startup list	1:68
wmic useraccount list brief	1:113
Word	2:18, 3:101, 3:105-106, 5:18, 5:75, 5:108, 5:111
Wordlist mode	4:32
Wordpad	3:101
WPA Supplicant	2:74
Wrapper	3:13, 3:87, 5:2, 5:18-20
Write Blocker	1:98
WriteProcessMemory	5:36
wtmp	5:70-71, 5:81
wtmped.c	5:71
wzap.c	5:71

X

xinetd	2:113, 2:127, 5:33

Y

Yoda	3:45, 5:19

Z

ZAP Proxy	4:89, 4:116-117
Zenmap	2:90, 2:94
Zigbee	2:82
Zombies	4:134, 4:139
Zone Transfer	2:33-37, 6:3, 6:24, 6:26, 6:44
Zotob	4:63