

## A

Access Control	5–91, 1–231
Access Control entries (ACE)	5–96
Access Control list (ACL)	5–32
Discretionary Access Control (DAC)	2–30
Linux	6–108
Discretionary Access Control List (DACL)	
Active Directory	5–119
NTFS	5–96
Windows	5–96
GrSecurity	6–112
Internet Information Services (IIS)	5–235
List-based Access Control	2–30
Maintenance Access Control	2–32
Mandatory Access Control (MAC)	2–30, 6–108
Network Access Control (NAC)	1–107
Port-level access control	1–108
Registry	5–118
Revocation	2–32
Role-Based Access Control (RBAC)	2–30, 6–112
Ruleset-based access control	2–30
Security Access Token (SAT)	5–29, 5–35, 5–123
SELinux	6–108
System Access Control List (SACL)	5–296
auditing	5–296
Token-based Access Control	2–30
Access This Computer from the Network	5–127
Account	
Administration	2–32
Administrative accounts	5–176
Guest account	W–5–31, 5–174
Local management	5–26
Lockout	5–165
Microsoft	5–47
Organizational	5–47
System	6–64
System	6–64
User	6–61
User account control (UAC)	5–181
Accountability	2–28
ACE → Access control entries	
ACL → Access control list	
Active defense	3–202
attack back	3–207
attribution	3–206
deception	3–205
harbinger distribution (ADHD)	3–225
legal warning	3–208
techniques	3–211
tools	3–224
types	3–203
Active Directory (AD)	532
Administrator	5–107
Authentication Protocols	5–35
Being in the domain—book5	33
Contains	5–33
Cross-Forest Trust	5–40, 5–43
Delegation of Authority	5–121
Distribution group	5–105
Domain Controller	5–32
Multi-master Replication	5–32
Read-only (RODC)	5–33
Federation services (ADFS)	5–47
Forest	5–40
Multi-master replication	5–32
Permission	5–119
Security group	5–105
Trust	5–42
Two-way transitive trust	5–41
Users & computers	5–105
AD → Active Directory	
Address (network)	1–86
Address resolution protocol (ARP)	1–84
Cache poisoning	1–83
Address space layout randomization (ASLR)	6–104
AddRoundKey	4–74
ADFS → Active Directory Federation Services	
ADHD → Active Defense Harbinger Distribution	
Administrative accounts	5–176
Administrative GPO templates → Group Policy Ob-	
ject	
Administrative shares	5–111
Advanced Encryption Standard (AES)	1–176
Advanced Encryption Standard → AES	
Advanced packaging tool (APT)	6–14, 6–249
Advanced persistent threats (APT)	1–16, 2–161
common defense model	2–178
exploitation process	2–172
maturity level	2–171
remediation	2–181
security measures	2–177
AES (Advanced Encryption Standard)	4–73
algorithm	4–74
AGULP	5–103
AH → IPsec Authentication header	
Air gap	1–54
aircrack-ng	W–1–43
aireplay-ng	W–1–43
airmon-ng	W–1–43
airodump-ng	W–1–43
ALE → Annualized Loss Expectancy	
Alien vault	6–124
Alternate ports	3–131
Android	6–26
pay	6–28
security	6–28
Annualized Loss Expectancy (ALE)	4–210
ALE & SLE	4–210
Ansible	6–91
Apache2Syslog	3–181
AppArmor	6–115
Application gateway (proxy firewall)	3–70
Application server mode (RDP)	5–242
Application whitelisting	3–142
Application-specific integrated circuit (ASIC)	3–111

AppLocker .....	5-178
AppX package .....	5-179
APT → Advance packaging tool .....	
Architecture of the system .....	1-7
ARM devices .....	5-20
ARP → Address resolution protocol .....	
Artillery (active defense) .....	3-226
ASIC → Application-specific integrated circuit .....	
ASLR → Address space layout randomization .....	
Asymmetric encryption → Cryptography .....	
Asymmetric key cryptosystem → Cryptosystem .....	
Asymmetric key exchange .....	4-28
Attack	
against routers .....	1-18
against switches .....	1-20
definition .....	3-37
pentest .....	3-37
process (pentest) .....	3-39
Attack back (offensive) .....	3-207
Attacker activities .....	2-94
Attribution (offensive) .....	3-206
Audit object access .....	5-295
Audit policies .....	5-294
auditd .....	6-171
Auditing	
log .....	3-168
what should be logged .....	5-299
auditpol.exe .....	5-295
aureport .....	6-173
ausearch .....	6-173
Australian Defense Signal Directorate (DSD) ....	2-93
Authentication .....	2-28
attacks .....	1-228
cryptography .....	4-16
Form-based .....	1-228
HTTP .....	1-228
Multi-factor .....	6-97
Authentication Header → IPsec Authentication	
header .....	
Authorization .....	2-28
Automatic demotion guest .....	5-175
Automation .....	5-264
autrace .....	6-173
Availability (CIA) .....	2-9
awk .....	6-166
Azure .....	5-252
backup .....	5-77
Azure Active Directory (MAAD) .....	5-45, 5-253
admin .....	5-256
management .....	5-46
single sign on (SSO) .....	5-48

## B

Backgr. Intelligent Transfer Service (BITS) .....	5-72
Backup	
files and directories .....	5-129
for security .....	5-76

third-party solutions .....	5-79
Bare metal hypervisor .....	1-50
Baseline	
Documentation .....	2-66
endpoint .....	3-130
system .....	3-129
Baseline (policy) .....	2-71
Baselining an environment .....	3-19
Bash → Shell .....	
Bastille .....	6-95
BCP → Business continuity plan .....	
Beartrap .....	3-227
Bell-LaPadula .....	6-109
Binary disk image .....	5-80
bindhshell (infected on port 465) .....	6-234
Biometrics .....	2-50
Birthday attack .....	4-84
Bitlocker .....	5-131
options .....	5-134
recovery .....	5-136
BITS → Backgr. Intelligent Transfer Service .....	
Blackbox diagram .....	1-7
Block cipher .....	4-8
Bluebugging .....	1-171
Bluejacking .....	1-171
Bluesnarfing .....	1-171
Bluesniff .....	1-171
Bluetooth .....	1-169
pairing .....	1-173
protecting .....	1-174
security .....	1-171
versions .....	1-170
Bootp/DHCP (port) .....	1-147
Bourne → Shell .....	
BPDU → Bridge protocol data unit .....	
Bridge protocol data unit (BPDU) .....	1-20
Bridged network .....	1-46
btm linux log .....	6-131
Buffer overflow .....	2-143
defense .....	2-144
Built-in auditing .....	1-56
Built-in commands 🚩 .....	6-181
Burp .....	1-234
Business continuity .....	1-64
Cloud .....	1-64
Business continuity plan (BCP) .....	4-172
BCP vs DRP .....	4-179
components .....	4-173
planning lifecycle .....	4-174
what is .....	4-175
Business impact analysis (BIA) .....	4-185
BYOD → Device .....	5-13

## C

C shell → Shell .....	
cain .....	5-130
Cain & abel .....	W-2-14, W-2-16, 2-83

CALs .....	5-15	Conceptual design .....	1-7
Carrier sense multiple access/collision detection (CSMA/CD) .....	1-23	Confidentiality (CIA) .....	2-9
cat .....	6-36	Confidentiality attack (offense) .....	2-186
CCB → Change control board .....		Confidentiality in transit .....	4-91
CCMP → Counter Mode CBC-MAC Protocol .....		Configuration management .....	2-20
CD Filesystem .....	5-94	Change control .....	2-20
CDFS → CD Filesystem .....		tools .....	6-88
CDP → Cisco Discovery Protocol .....		Container .....	6-239
Center for internet security (CIS) .....	6-230	cgroups 🚀 .....	6-240
hardening guides .....	6-230	Container vs VM .....	6-243
Central logging .....	6-150	Docker .....	6-242
Certificate Revocation list (CRL) .....	4-120	LXC vs Docker .....	6-241
Limitation .....	4-120	Namespace .....	6-240
cfengine .....	6-90	Containment → Incident Handling .....	
cgroups → Container .....		Content discovery .....	1-60
Chain of custody .....	4-159	Control System Entity Relationship Diagram ...	2-109
Change control → Configuration management .....		Controlling access .....	2-29
Change control board (CCB) .....	5-283	ConvertTo-HTML .....	W-5-63
Change detection analysis .....	5-313	Convincing the organization .....	2-63
chef .....	6-92	Cookies .....	1-216
chgrp .....	6-59	non-persistent .....	1-218
chmod .....	6-57	Copy-Item .....	W-5-68
chown .....	6-59	Copyright .....	2-80
chroot .....	6-236	Counter Mode CBC-MAC Protocol (CCMP) ...	1-176
chroot (problems) .....	6-238	bluetooth .....	1-176
chrootkit .....	6-234	wireless .....	1-183
CIA (Confidentiality - Integrity - Accessibility) ...	2-9	CPNI → UK Center for the protection of national in- frastructure .....	
CIDR (network notation) .....	3-26	Creator Owner Group → NTFS .....	
CIFS → Shared message block (SMB) .....		Critical application analysis → Disaster Recovery Plan .....	
Cipher, ciphertext .....	4-8	Critical Security Controls (CSC) .....	2-91
CIS → Center for internet security .....		Core eval test .....	2-100, 101
Cisco Discovery Protocol Manipulation .....	1-20	Denial of Service (DoS) .....	2-93
Civilian penetration tester .....	2-93	Effectiveness measures .....	2-102
Classic init .....	6-78	ERD (Entity Relationship Diagram) .....	2-109
Cloud		Key points .....	2-96
Business continuity .....	1-64	Project guiding principles .....	2-96, 97
Cloud Service Provider (CSP) .....	1-64	Sample .....	2-104
Data .....	1-60	Understanding the controls .....	2-98
Defense .....	3-158	What are .....	2-99
Clustering .....	4-8	CRL → Certificate Revocation List .....	
CNSS 4009 (pentest) .....	3-37	Cron .....	6-84
Codes .....	4-8	Cross-Forest Trust → Active Directory .....	
Cold boot attack .....	5-135	Cross-site request forgery (XSRF) .....	1-15
Cold site .....	4-195	router .....	1-18
Collection of patches .....	5-64	Cross-site scripting (XSS) .....	1-15
Collision .....	1-23	Cryptanalysis .....	4-8
Communication flow .....	1-7	Analytic .....	4-83
Communication Plan → Disaster recovery plan .....		Differential .....	4-83
CompanyConfidential .....	6-109	Differential linear .....	4-83
Compare-Object .....	W-5-47	Linear .....	4-83
Complexity infrastructure layers .....	1-55	Statistical .....	4-83
compmgmt.msc .....	5-26	techniques .....	4-83
Computational complexity .....	4-62	Cryptanalysts .....	4-7
Computer activists .....	1-17	Cryptogram .....	4-8
Computer attacker activities .....	2-94	Cryptographers .....	4-7
		Cryptography .....	4-8

algorithms	4-8, 4-14
Arbitrary substitution	4-22
Asymmetric encryption	4-32
Caesar cipher	4-20
challenge	4-15
concept	4-61
core components	4-9
Decryption	4-9
Diffie-Hellman	4-29
Digital signature	4-37
Discrete logarithm	4-65
Frequency analysis	4-23
goals	4-16
Key Length	4-79
key length	4-79
Key Server	4-13
Keys	4-11
Keyspace	4-11
Non-repudiation	4-16
Permutation	4-24
Rotation substitution	4-20
Symmetric encryption	4-18
XOR	4-19
Cryptology	4-7
Cryptosystem	4-10
Asymmetric key	4-31
Elliptic Curve Cryptosystem (ECC)	4-66, 4-78
Symmetric key	4-27
Types	4-26
CSC → Critical Security Controls	
csh → Shell	
CSMA/CD → Carrier sense multiple access/collision detection	
CSP → Cloud service provider	
CSRF → Cross-site request forgery	
Current branch 🌈 → Windows servicing branch	
cut	6-156
Cyber	
criminals	1-16
espionage	1-16
Cygwin	6-16

## D

DAC → Access Control	
DAC → Discretionary Access Control	
DACL → Discretionary Access Control List	
DAD → Log collection	
DAM → Database activity monitoring	
Damage assessment procedures → Disaster Recovery Plan	
Data classification	2-26
Data diode	3-71
Data dispersion	1-61
Data flow	1-27
Data fragmentation	1-61
Data Loss Prevention (DLP)	1-60, 5-266
Data migration to the cloud	1-61

Data normalization	3-86
Data security	1-60
Database activity monitoring (DAM)	1-61
dc.exe	5-204
DC3	2-93
Debug	
Privilege	5-130
Traces	3-168
Deception (offensive)	3-205
Decloack (active defense)	3-228
Decoy	
IPs	3-219
ports	3-220
servers (active defense)	3-205
Decryption → Cryptography	
Default domain policy	5-160
Defense-in-depth	2-5
information centric	2-16
protecting enclaves	2-15
uniform	2-14
vector oriented	2-17
Denial of Service	2-93
Router	1-18
Wifi	1-196
Departement of Energy (DoE)	2-93
Departement of homeland security (DHS)	2-93
DES	4-68
Double-DES	4-71
in the middle attack	4-71
Triple-DES	4-72
Design network	
final	1-32
Device	
ARM	5-20
Bring your own device (BYOD)	5-13
Driver rollback	5-83
Log	3-168
Mobile Security	6-25
Network → Network device	
Wireless popular devices	1-164
df	6-42
DHCP spoofing	
switch	1-20
DHS → Departement of homeland security	
Dictionary attack → Password	
Diffie-Hellman → Cryptography	
dir	W-5-65
Direct evidence	4-161
Direct memory access (DMA)	1-55
Directed broadcasts	1-102
Disaster recovery	1-64
Disaster Recovery Plan (DRP)	4-172, 4-177, 4-196
activation	4-198
cloud	1-64
Communication Plan	4-192
Critical application analysis	4-188
Damage assessment procedures	4-194
Lifecycle	4-174

Mangement awareness	4-182
planning lifecycle	4-174
Planning mistakes	4-199
Planning process	4-181
Risk assessment	4-183
Scenario identification	4-184
Site planning	4-195
Steps	4-178
Virtual machine	1-41
Discrete logarithm → Cryptography	
Discretionary Access Control (DAC)	2-30
Linux	6-108
Discretionary Access Control List (DACL)	
Active Directory	5-119
NTFS	5-96
Registry	5-118
Windows	5-96
Disgruntled employee	
router	1-19
DLL injection	W-5-15, 5-130
DLP → Data Loss Prevention	1-60
DMA → Direct memory access	
dmesg linux log	6-131
DN (Distinguished name)	4-115
DNS → Domain Name Service	
Docker → Container	
Documentation baseline → baseline	
DoE → Departement of Energy	
Domain (location type)	5-218
Domain Controller → Active Directory	
Domain GPO → Group Policy Object	
Domain Name Service (DNS)	
Bogus entries	3-222
False entries (offensive)	3-205
TCP/UDP port	5-214
UDP port	1-147
DoS → Denial of Service	
Dos commands	6-35
dropmyrights.exe	5-181
DRP → Disaster Recovery Plan	
DSD → Australian Defense Signal Directorate	
dsniff	1-82
Dumpster diving	3-43
dumpuser.exe	5-170
Duo (multifactor authentication)	6-97
Dynamic loading (modules)	6-106

## E

EAP → Extended Authentication Protocol	
EAPoL → Extended Authentication Protocol over Lan	
Eavesdropping	3-43
wifi	1-192
ECC → Cryptosystem	
ECN → Explicit Congestion Notification	
Elliptic Curve Cryptosystem → Cryptosystem	
Encapsulated security Payload (IPsec)	4-97

Encryption	4-9
AES → AES	
Asymmetric → Cryptography	
Full disk encryption	4-107
Full volume encryption key (FVEK)	5-132
Hard disk encryption 🚩	6-46
Irreversible	2-35
Local encryption key managment	5-259
Object storage	1-60
On-the-fly	4-107
One-way	4-34
Reversible	2-35
Symmetric → Cryptography	
Virtual machine snapshot	1-60
Volume storage	1-60
Entity Relationship Diagram → Critical Security Controls	
EOI (Event of interest)	6-209
EOI → Event of interest	
ER Diagram → Critical Security Controls	
Eradication → Incident Handling	
ESP → IPsec Encapsulating Security Protocol	
Ethernet	1-23
packet	1-80
Ethical hacking	3-36
Ettercap	1-81
Event	4-140
Event of interest (EOI)	3-76
Evidence	4-160-162
Exchange online	5-252
Explicit Congestion Notification → TCP	
Exploit	
definition	3-37
pentest	3-37
Export-CSV	W-5-60
Extended Authentication Protocol	
over Lan (EAPoL)	1-180
Extended Authentication Protocol (EAP)	1-179
Extended C shell → Shell	

## F

FAT	5-94
FAT32	5-94
FC.exe	5-313
Features (server)	5-200
Federal reserve	2-93
Federation Services → Active Directory Federation Services	
Fedora	6-14
FIC → File integrity checking	
File	
\$	5-111
Absolute file permission 🚩	6-50
Activity monitoring	1-61
File integrity checking (FIC)	3-138, 139, 6-213
File permission 🚩	6-51
History	5-86

Sharing	
Hidden	5-111
Storage → Filesystem	
Symbolic file permission 🚩	6-50
Filesystem	1-59, 5-94
Logical file system 🚩	6-39
noexec	6-111
nosuid	6-44
Physical file system 🚩	6-40
Resilient File System (ReFS)	5-95
Fill	W-5-59
Find	6-36
Finger	2-122
port	1-139
Fingerprint	3-27
Firewall	
benefits	3-62
default rule	3-63
Egress	3-64
Endpoint	3-136
endpoint	3-136
firewalld	6-224
Host-based 🚩	6-222
Ingress	3-64
iptables	6-220, 6-222
example	6-222
Linux	6-218
Locate	1-29
locate	1-29
next-generation	3-65
Rules 🚩	5-220
types	3-65
types, endpoint	3-137
why?	3-61
Windows	5-216
Fixing the problem	2-19
Forensic snapshots	5-305
content	5-307
Forest → Active Directory Cross-Forest	
Format-List	W-5-58
Frame	1-23, 1-80
freeotp	6-97
FTP	
control (port)	1-139
data (port)	1-139
Full disk encryption	4-107
Full volume encryption key → Encryption	
FVEK → Encryption	

## G

Gatekeeper 🍏	6-20
Gateway (unidirectional)	3-72
GCHQ → UK Gov. communications HQ	
GET	1-215
Get-FileHash	W-5-70
Get-Process	W-5-57, 5-266
Get-Service	W-5-63, 5-204

Get-WinEvent	W-5-75
Get-WmiObject	W-5-70
getmac.exe	5-273
Global Catalog (GC)	5-40
Global Catalog Server	5-40
Global groups	5-34
Gnome	6-87
Google authenticator	6-97
GPA → GPG Assistant	
GPG	W-4-23, 4-106
Establishing a key	4-108
functions	4-110
GPG Assistant (GPA)	W-4-23
GPMC → Group Policy Management Console	
GPO → Group Policy Object	
gradm commands	6-113
graylog2	6-128
grep	6-36, 6-154
Options	W-3-3
Group Policy Management Console (GPMC)	5-51, 5-161
Group Policy Object (GPO)	5-50, 5-162
Account Lockout Policy	5-165
Administrative templates	5-159, 5-167
Anonymous access	5-170
Domain GPO	5-160
Local GPO	5-156
Management console	
→ Group Policy Management Console	
Password	5-163
Push scripts	5-278
Security options	5-166
Servicing Branch	5-70
Settings checklists	5-162
User account control (UAC)	5-182
Windows Update	5-70
GrSecurity	6-110
commands	6-113
PaX (memory protection)	6-111
Role-Based Access Control (RBAC)	6-112
Guest account	5-174
Guideline	2-72

## H

Hactivist	1-17
Harden linux	6-95
scripts	6-229
sysctl	6-101
Hardening	1-99
Hardening router → Router	
Hardening switch → Switch	
Hash	2-36
Collision	4-35
Function	4-34
Length	W-4-43
MD2	4-34
MD4	4-34



MD5 .....	4-34, 4-80
NT/MD4 .....	5-39
Secure Hash Standard (SHS) .....	4-34
Strong hash .....	2-41
Headers (false) .....	3-218
HIDS (Host-based intrusion detection system) ..	3-146
advantage .....	3-147
challenges .....	3-148
future .....	3-150
network monitoring .....	3-146
overview .....	3-144, 3-146
HIPS (Host-based intrusion prevention system)	
advantages .....	3-153
application behavior monitoring .....	3-155
future .....	3-154-157
overview .....	3-152
recommendations .....	3-156
Histograms .....	4-43
Hololens .....	5-13
Honey badger (active defense) .....	3-229
HoneyCreds .....	3-215
Honeynets .....	3-213
Honeypot .....	3-212, 3-232
active defense .....	3-205
advantages .....	3-234
checklist/summary .....	3-240
classification .....	3-236
deployment .....	3-238
offensive .....	3-212
production .....	3-213
research .....	3-213
Honeytokens .....	3-213
IDS .....	3-87
HOST ID .....	1-86
Hot site .....	4-195
Hotfixes .....	5-63
hping3 .....	W-3-34, 3-20
flags commandline .....	3-21
options .....	W-3-35
HTML .....	1-214
Forms .....	1-215
HTTP .....	1-212
Authentication .....	1-228
HTTPS (port) .....	1-139
Port .....	1-139
Hub .....	1-77
Hub vs Switch .....	1-79
Hybrid attack → Password .....	
Hybrid identity management .....	5-255
Hypervisor → Virtual machine .....	

## I

I need to ask your mother .....	5-39
ICACLS.exe .....	5-96
ICMP → Internet Control Message Protocol .....	
ICMPv6 .....	1-133
Identification → Incident Handling .....	

Identity .....	2-28
IDS .....	3-74
What is not .....	3-75
wireless networks .....	3-105
IE Protected mode .....	5-183
IEEE .....	
802.11ac .....	1-178
802.11b .....	1-178
802.11g .....	1-178
802.11i .....	1-179
802.11n .....	1-178
802.15.4 .....	1-175
802.1x .....	1-108, 1-180
IKE (Internet key exchange) .....	4-101
Incident .....	4-140
Incident Handling .....	4-138
Containment .....	4-148
Eradication .....	4-149
Identification .....	4-146
Legal .....	4-155
legal .....	4-155
Lessons .....	4-151
mistakes .....	4-152
steps .....	4-143
Incident Response .....	
Cloud .....	1-66
inetd.conf .....	6-94
Information centric → Defense-in-depth .....	
Information management .....	1-59
Information system contingency plan .....	4-190
init classic .....	6-78
Innocent infringement (copyright) .....	2-80
Input attacks .....	2-140
Integrity .....	
CIA .....	2-9
cryptography .....	4-16
hash .....	4-36
Integrity Check Value (ICV, IPsec) .....	4-97
tools .....	6-214
Inter-domain replication .....	5-40
International Telecom Union (ITU) .....	4-118
Internet Control Message Protocol (ICMP) ....	1-112,
1-133	
header .....	1-134
checksum .....	1-134
code .....	1-135
type .....	1-134
Internet Explorer (IE) .....	5-183
Internet zone .....	5-186
Restricted site zone .....	5-188
Security .....	5-183-189
Smartscreen filter .....	5-189
Trusted sites zone .....	5-188
Internet Information Services (IIS) .....	5-230
access control .....	5-235
IUSR .....	5-235
log .....	5-238
Secure Socket Layer (SSL) .....	5-235

security	5-230
Server Nano	5-232
Transport Layer Security (TLS)	5-235
URLSCAN	5-237
Internet protocol (IP)	1-123
IP & OSI model	1-131
IP address	1-86
IP Spoofing	2-125
IP version 4 → IPv4	
IP version 6 → IPv6	
Internet security association and key managment pro- tocol (ISAKMP)	4-101
Internet zone → Internet explorer	
Intractable problems	4-62
Intune	5-253
iOS	6-26
security	6-29
IP → Internet protocol	
ipconfig	5-112
ipconfig.exe	5-273
IPS (Intrusion prevention system)	3-107
what is not	3-108
IPsec	4-96, 5-225
Authentication header (AH)	4-97
command line	5-226
configure and manage	5-225
Encapsulating Security Protocol (ESP)	4-97
group policy	5-227
header	4-97
modes	4-100
port	5-214
types	4-97
iptables → Firewall	222
IPv4	1-124
header	1-126
IPv4 vs IPv6	1-125
IPv6	1-125
addresses (self-assignment)	6-103
features	1-130
hardening	6-103
header	1-129
translation	1-130
tunneling	1-130
IR → Incident Response	
Irreversible encryption	2-35
ISAKMP → Internet security association and key managment protocol	
ISNs (TCP handshake)	1-140
ISO (OSI)	1-116
ITU → International telecommunication union	
IUSR → Internet Information Services	5-235

## J

Jailed environments	3-216
John the ripper	2-49
Files	W-2-4
Options	W-2-3

## K

KDC → Kerberos Key Distribution Center	
Kerberos	2-33, 5-36
Brute-force cracking	5-37
example	5-38
Kerberos vs NTLM	5-172
Key Distribution Center (KDC)	5-36
port	5-212
Supported protocols	5-36
Kernel	
Loadable kernel modules (LKM)	6-105
Kernel 🚩	6-38
Key escrow	4-116
Keybox	6-98
kismet	1-32, 1-82
Kiwi	3-181
korn shell → Shell	
ksh shell → Shell	

## L

Labeled security protection	6-109
Lan Manager (LM)	5-39, 5-173
LASSO (Log tool, windows)	3-181
lastb	6-131
Law	
Civil law	4-156
Criminal law	4-156
Law of negligence	4-156
Law of torts	4-156
LDAP → Lightweight Directory Access Protocol	
Least privilege	1-25, 2-29
NTFS	5-101
Least significant bits	4-49
Legacy pairing → Bluetooth	
Legal → Incident Handling	
Lessons → Incident Handling	
Lightweight Directory Access Protocol (LDAP)	6-73
LDAPS port	5-32, 5-212
Linux	6-73
OpenLDAP	6-73
Port	5-32, 5-212
Linux	
commands	6-35
configuration managment	6-86
containers → Container	
distribution	6-12
File permissions	6-50
hard disk encryption	6-46
Linus Torvalds	6-13
Locking out linux	6-72
marketshare	6-7
superuser	6-62
system accounts	6-64
unified key setup	6-46
user accounts	6-61
vserver	6-245
List-based Access Control	2-30



# SEC401 – Security Essentials Bootcamp Style

LKM → Kernel Loadable Module) .....	
Local accounts windows (management) .....	5–26
Local encryption key managment → Encryption .....	
Local security policy .....	5–51
Log .....	3–168
aggregation correlation .....	6–121
Alert .....	3–168
analysis tools .....	3–181
Collection	
DAD (Tool, windows) .....	3–181
consolidation .....	5–303
correlation .....	3–179
Debug traces .....	3–168
Exclusive analysis .....	3–140
files .....	3–168
linux .....	6–131
forwarding .....	3–172
how helps .....	3–196
Inclusive analysis .....	3–140
Message .....	3–168
Monitoring .....	3–140, 3–168
annual tasks .....	3–195
daily tasks .....	3–190
monthly tasks .....	3–193
program .....	3–185
quarterly tasks .....	3–194
real-time tasks .....	3–189
strategy .....	3–184
weekly tasks .....	3–192
OpenSSH .....	3–181
Parsing	
Command-line (CLI) .....	6–153
parsing .....	6–153
reports (the best) .....	3–176
SEC .....	3–181
SELinux .....	6–131
server (build) .....	3–172
SIEM .....	3–166-181
overview .....	6–121
size .....	5–301
standards .....	3–173
Stunnel .....	3–181
tools .....	3–183
wrapping options .....	5–301
LOGalyze (Log tool, linux) .....	6–129
Logical design .....	1–7
Logical location of data .....	1–59
Logical topology .....	1–22
login.defs .....	6–67
Logon	
Other Domain .....	5–42
Logon locally → Privilege .....	
Logon through remote desktop services .....	5–127
LogPP .....	3–181
logrhythm .....	6–125
logrotate .....	6–147
logrotate.conf .....	3–172
logstash .....	6–127

Long term servicing branch .....	5–70
ls .....	6–182
LSB (Least significant bit) .....	4–49
LSPP (Labeled security protection profile) .....	6–109
LUKS (Linux unified key setup) .....	6–46
LXC → Container .....	
Lync .....	5–252
Lynis (linux audit tool) .....	6–96

## M

MAAD → Azure active directory .....	
MAC address .....	1–86
MAC flooding (switch) .....	1–20
Machines become files → Virtual machine .....	
macOS .....	6–18
iCloud Keychain .....	6–20
Sandboxing .....	6–21
security .....	6–20
Maillog (log tool, linux) .....	6–131
Maintaining state (app) .....	1–232
Maintenance Access Control .....	2–32
Malicious insider (router) .....	1–19
man .....	6–36
Mandatory Access Control (MAC) .....	2–30
SELinux .....	6–108
Mannerisms .....	2–50
Matrix (risk managment) .....	4–206
Maximum tolerable downtime (MTD) .....	4–186
mbsaccli.exe .....	5–260, 5–290
MCS (Multi-category security) .....	6–109
md5sum .....	W–4-43
Mean downtime .....	4–189
Meet-in-the-middle attack .....	4–71
Message digests .....	4–34
Messages (linux log) .....	6–131
Metasploit .....	3–47
Microsoft account .....	5–47
Microsoft Azure Active Directory (MAAD) → Azure active directory .....	
Microsoft Baseline Security Analyzer (MBSA) W–5-28, 5–286	
Microsoft cloud computing .....	5–251
Microsoft resource kits .....	5–268
Microsoft security compliance manager .....	5–151
Microsoft Security Configuration and Analysis ..	5–153
Microsoft security update guide .....	5–67
Middleware tier .....	1–30
Minimizing packages .....	6–87
Minix .....	6–13
Mirrored site .....	4–195
Mission statement .....	2–64
Mitnick .....	2–117
Lessons learned .....	2–138
MixColumns .....	4–74
MLS (Multi-category security) .....	6–109
Mobile Device Security → Device .....	
modinfo .....	6–105

modprobe	6–105
Monitoring web-application	1–235
more	6–36
Mounted drives	6–40
MPLS (Multi-protocol label switching)	4–94
MPROTECT	6–111
MS Cloud service (categories)	5–251
mstsc.exe	5–244
MTD	4–186
Multi-category security (MCS)	6–109
Multi-factor authentication	1–228
Azure	5–46
SSL	6–97
Multi-level security (MLS)	6–109

## N

NAC (Network access control)	1–107
Namespace 🐳 → Containers	
Nature of trust	5–42
NBT (port)	1–147
nbtstat.exe	5–210, 5–273
ncpa.cpl	W–1–17
NDA (Non-disclosure agreement)	2–80
Need to know	2–29
Nessus	3–31
Net flow	1–27
net.exe	W–5–30, 5–26, 5–109, 5–170
share	5–109
NET.ID	1–86
NetBios	5–210
port	5–214
netcat	W–1–37, 3–218
netsh.exe	5–226
netstat	6–187, 6–189
netstat.exe	5–273
Network access control (NAC)	1–106
Network adapter bindings	5–209
Network architecture design	1–27
Network configuration tools	5–274
Network design	
final	1–32
goals	1–30
Network device	1–77
Security	3–58, 1–74
Network level authentication	5–246
Network location types	5–218
Network mapping	3–22
Network protocol	1–114
Network security devices → Network device	
NFS (port)	1–147
nftables	6–226
NIDS (Network intrusion detection system)	3–78
advantages	3–87
analyse encrypted traffic	3–92
anomaly analysis	3–82
challenges	3–89
cost	3–96

devel	3–104
key points	3–103
performance limitations	3–94
rules and signature criteria	3–80
signature	3–93
signature analysis	3–79
topology limitations	3–90
NIPS (Network intrusion prevention system)	3–109
challenges	3–112
devel	3–113
passive analysis	3–115
referenced architecture	3–116
NIS (Sun's network information service)	2–122
NIST (pentest)	3–37
NLA (Network level authentication)	5–246
nmap	3–23
host specification	3–25
options	W–3–6
scripting engine (NSE)	W–3–13
no_magic_root	6–72
nodev	6–44
noexec → Filesystem	
Non-disclosure agreement (NDA)	2–80
Non-repudiation → Cryptography	
nosuid → Filesystem	
Notification and activation (Disaster recovery)	4–193
NOVA (active defense)	3–230
NSA (National security agency)	2–93
NSD → Network device security	
NSE (nmap scripting engine)	3–51
NTFS	
Creator Owner Group	5–99
Discretionary Access Control List (DACL)	5–96
Filesystem	5–94
owner	5–99
permissions & shares	5–113
NTLM	5–39
NTLMv1	5–172
NTLMv2	5–173
NTLMv2	2–45
NTP (port)	1–147
ntrights.exe	5–124
ntSyslog	3–181
Null user session	5–170

## O

Oakley	4–101
Object storage	1–59
Object storage encryption → Encryption	
OCSP (Online Certificate Status Protocol)	4–120
OEM license	5–8
Off-boarding (access)	2–32
Offense	3–202
Offensive operation	2–185
Office	
365	5–253
best practice	5–255

mobile .....	5-253
online .....	5-253
ollydbg .....	5-130
On-premises directory synchronization .....	5-46
On-the-fly encryption .....	4-107
One-time passwords → Password .....	
One-way encryption .....	4-34
Onedrive .....	5-252
Online Certificate Status Protocol (OCSP) .....	4-120
OpenSCAP .....	6-254
audit tool .....	6-255
base .....	6-255
daemon .....	6-255
timony .....	6-255
workbench .....	6-255
Organized crime .....	1-16
OS	
Guest OS → Virtual machine .....	
Host OS → Virtual machine .....	
OS command injection .....	2-141
defenses .....	2-142
OS identification .....	3-27
oscap anaconda addon .....	6-255
OSI model .....	1-118, 1-131
Layer 3 .....	1-112
Layer 4 .....	1-112
OSI model vs TCP/IP .....	1-118
OSSEC	
HIDS 🚩 .....	6-216
log .....	3-181
Out-File .....	W-5-63, W-5-69
Out-GridView .....	W-5-62
Outlook.com .....	5-253
Owner group .....	5-99

## P

Package management 🚩 .....	6-247
Packages minimizing .....	6-87
Packet	
firewall .....	3-66
inspection (deep vs shallow) .....	3-85
misrouting (router) .....	1-18
sniffing (router) .....	1-18
PAM (Pluggable authentication modules) .....	6-68
pam_cracklib .....	6-71
pam_tally .....	6-72
pam_unix .....	6-71
Partitions .....	6-40
Passive fingerprinting .....	3-104
Passwd file .....	6-65
Password	
Attack .....	2-38, 2-43
Brute-force .....	2-43
Dictionary .....	W-2-3, 2-43
Hybrid .....	2-43
Incremental .....	W-2-3
Single .....	W-2-3

User information .....	W-2-3
Wordlist .....	W-2-3, 2-43
Group Policy Object (GPO) .....	5-163
Linux	
Aging .....	6-67
Hardening .....	6-70, 71
One-time password .....	2-50
Policy .....	2-48
Rainbow table .....	2-43, 2-46
Prevention .....	2-45
Salt .....	2-45
Strength of hash .....	2-41
Patch .....	5-63
Patch management system (third party) .....	5-74
Path	
Windows .....	5-277
PatientRecord .....	6-109
PaX (memory protection) .....	6-110
GrSecurity .....	6-111
Paxctld .....	6-110
pc-sort=pepu .....	6-192
PC Refresh .....	5-84
PC Reset .....	5-84
PCI 🚩 .....	6-96
PEAP (wifi) .....	1-194
Peer review (secure web app) .....	1-222
Pentest .....	3-36
approach .....	3-41
techniques .....	3-43
terms and definitions .....	3-37
Permission .....	5-123
Active Directory .....	5-119
Delegation of Authority .....	5-121
Other Domain .....	5-42
Shared folder .....	5-108
Permission behavior .....	6-54
folders permission .....	6-54
Philippe Oechslin .....	2-46
Physical design .....	1-7
Physical location of data .....	1-59
Physical topology .....	1-22
ping .....	1-135
pipe .....	6-209
PKI (Public key infrastructure) .....	4-112
lifecycle .....	4-115
problems .....	4-126
SSL .....	4-124
Pluggable authentication modules (PAM) .....	6-68
Policy	
baseline .....	2-66
creation .....	2-77
general .....	2-68
in general .....	2-68
mission statement .....	2-64
Password .....	2-48
penalties .....	2-78
statement .....	2-75
table of content .....	2-73

type of policies .....	2-76
vs procedure .....	2-67
Port .....	5-216
137-139 .....	1-147
161-162 .....	1-147
67-68 .....	1-147
802.11a .....	1-178
20 .....	1-139
21 .....	1-139
22 .....	3-172
23 .....	1-139
25 .....	1-139
42 .....	5-214
47 .....	5-215
50 .....	5-214
51 .....	5-214
53 .....	1-147, 5-214
67 .....	1-147
68 .....	1-147
69 .....	1-147
79 .....	1-139
80 .....	1-139
88 .....	5-212
123 .....	1-147
135 .....	5-212
137 .....	5-214
138 .....	5-214
139 .....	5-212, 5-214
161 .....	1-147
162 .....	1-147
389 .....	5-32, 5-212
443 .....	1-139, 5-215
445 .....	5-216
500 .....	5-214
514 .....	3-172
636 .....	5-32, 5-212
1433 .....	5-214
1434 .....	5-214
1512 .....	5-214
1723 .....	5-215
2049 .....	1-147
3268 .....	5-212
3269 .....	5-212
3389 .....	5-214, 5-246
4500 .....	5-214
5985 .....	5-265
5986 .....	5-265
closing 🚪 .....	6-94
forwarding .....	1-109
switch .....	1-109
knocking .....	3-132
scan .....	3-22
translation .....	3-131
Port-level access control .....	1-108
POSIX .....	6-18
POSIX ACL .....	6-52
Post (html) .....	1-215
PowerShell	

Remote port .....	5-265
Snapshot .....	5-309
Powershell .....	W-5-29, 5-265
commands .....	W-5-47, W-57
Register .....	5-115
remoting .....	5-265
variable .....	W-5-59
PPTP (port) .....	5-215
Pre-computation attack	
Prevention .....	2-45
Pre-computation attack → Password Rainbow table ..	
Pre-scale image Steganography .....	4-49
Preparation (Incident Handling) .....	4-144
Previous version (FS, restore) .....	5-86
Private (location type) .....	5-218
Private (network section) .....	1-29
Private network .....	4-91
Privilege .....	5-123
Access to RAW memory .....	5-2
Dangerous 🚩 .....	5-124
Debug programs .....	5-29, 5-130
Elevation .....	6-63
Least privilege .....	2-29, 5-101
List 🚩 .....	5-124
Logon locally .....	5-127
Other Domain .....	5-42
Privileges .....	5-123
Procedure (general) .....	2-69
Process Hacker .....	W-5-2
Protected enclave .....	1-25
Protected enclaves	
defense-in-depth .....	2-15
Protocol (IPv4 header) .....	1-127
Proxy (firewall) .....	3-70
Privilege	
Least privilege .....	1-25
ps .....	6-191
Public (location type) .....	5-218
Public Key Infrastructure (PKI) .....	4-112
puppet .....	6-89, 6-98
PUT (HTTP) .....	1-213
pwd .....	6-36

## Q

qradar .....	6-126
Qualitative risk	
assessment .....	4-213
vs quantitative risk assessment .....	4-213
QualysGuard .....	3-31
Quantitative risk assessment .....	4-213

## R

R2 .....	5-15
R3 .....	3-7
RANDMMAP .....	6-111

Rate limiting	6–103
RBAC → Access Control	
rc.d	6–94
RDP (Remote desktop protocol)	5–242
best practice	5–249
port	5–214, 5–246
RDP/TLS	5–247
Read only (Domain Controller)	5–33
Read only (FS load option)	6–44
Real evidence	4–161
Reconnaissance	3–7
Reconstitution of business (define)	4–191
Recovery (Incident Handling)	4–150
Point Objective	4–189
Time Objective	4–189
window	4–189
Red-team exercise	3–36
Redfang	1–171
Referenced architecture (NIPS/NSD)	3–116
Refresh PC	5–84
ReFS Filesystem	
reg.exe	5–115
regdmp.exe	5–269
regedit.exe	5–115
regfind.exe	5–269
Register powershell	5–115
Registry	5–115
Discretionary Access Control List (DACL)	5–118
share permissions	5–116
regsvc.exe	5–116
Remote access (types)	4–95
Remote assistance	5–245
Remote desktop protocol (RDP)	5–246
Remote desktop service	5–242
Remote PowerShell (port)	5–265
Remote registry service	5–116
Remote wipe	5–255
Reset PC	5–84
Restart-Service	W–5-63
Restore point	5–81
Restricted site zone → Internet Explorer	
Retail license	5–8
Reversible encryption	2–35
Revocation → Access Control	
RFC 2401	4–96
RFC 4120	2–33
RFC 826	1–84
rhosts	2–124
Rights mangment services (RMS) & DLP	5–256
Rijndael	4–73
Risk	2–8, 3–9, 4–207
Risk (mitigation)	1–56
Risk assessment	4–183
Risk key	4–208
Risk management	
business case	4–215
matrix	4–206
process (steps)	4–205

questions	4–209
Risk mitigation	
Virtual machine	1–56
rkhunter	6–233
ro (FS load option)	6–44
robocopy	5–88
RODC (Read-only Domain Controller)	5–33
Rogue AP	1–198
ROI	3–8
Role-Based Access Control (RBAC)	2–30
GrSecurity	6–112
Roles (server)	5–200
Root (linux FS)	6–39
Rootkit detectors	6–232
ROSI	3–8
ROT-13	4–20
Rotation of duties	2–29
route.exe	5–273
Router	1–77
attacks	1–18
Border	1–31
Hardening	1–99
hardening	1–99, 1–105
Insider threat	1–19
Internal threat	1–19
Router (advertisements)	6–103
Routing	1–88
Routing table	1–19
poisoning	1–19
RPC (port)	5–212
rpcinfo	2–122
RPM package	6–14
RPO (Recovery point objective)	4–189
RSA (Rivest-Shamir-Adleman)	4–77
RST Bit (router)	1–19
RTO (Recovery time objective)	4–189
Ruleset-based access control	2–30
runas.exe	5–181
runlevels	6–78

## S

SACL → Access Control	
SAFER+	1–171
SaltStack (configuration managment, linux)	6–93
SamHain (HIDS, linux)	6–215
Sandboxing 🍏	6–21
SAT → Security Access Token	5–29
sc.exe	5–204
SCA (Security configuration and analysis)	5–153, 5–284
scanport	3–22
SCAPTimony (audit tool)	6–255
Scheduling task	5–280
Schema and Configuration Naming Context	5–40
schtasks.exe	5–280
SCW (Security configuration wizard)	5–206
scwcmd.exe	5–208

SDN (Software-defined network)	1–25	set-gid	6–54
secedit.exe	W–5-42, 5–155, 5–285	set-uid	6–54
Secure boot	5–138	SHA	4–34
Secure coding (web app)	1–224	SHA-1/SHA-2	4–81
Secure hash	4–34	sha1sum	W–4-43
Secure Shell (SSH)	1–104	sha256sum	W–4-43
key	6–97	Shadow file	6–66
key managment	6–98	Share administrative	5–111
multi-factor	6–97	Share folders (how)	5–109
port	3–172	Share hidden	5–111
Secure simple pairing → Bluetooth		Share permissions & NTFS share	5–113
Secure Socket Layer (SSL)	4–122, 1–219	Shared folder permission	5–108
Internet Information Services (IIS)	5–235	Shared message block (SMB)	5–108
PKI	4–124	Sharepoint online	5–252
port	5–215	Shell	6–33
SSL/TLS	1–219	Bash	6–34
VPN	4–102	Bourne	6–34
Secure WLAN (steps)	1–200	C	6–34
Securing services	5–199	csh	6–34
Security (understanding)	6–179	Examples	6–34
Security Access Token (SAT)	5–29, 5–35, 5–123	Extended C	6–34
Security access token (SAT)	W–5-8, 5–29	korn	6–34
Security as a service	1–62	ksh	6–34
Security configuration and analysis (SCA)	5–153, 5–284	Powershell → Powershell	
Security configuration wizard (SCW)	5–206	Secure Shell (SSH) → Secure Shell	
Security Event Log	5–294	tcsh	6–34
Security ID numbers (SID)	5–27	ShiftRows	4–74
S-1-1-0 (Everyone)	5–27	showmount	2–122
S-1-5-11 (Authenticated Users Group)	5–27	SHS → Hash	4–34
S-1-5-32-544 (Local Admin Group)	5–27	SID (Security ID numbers)	5–27
Security policy	2–62	SIEM → Log	
Security templates	5–149	Signature → Cryptography Digital Signature	
sed	6–161	Single Loss Expectancy (SLE)	4–210
Segmentation	1–25	ALE & SLE	4–210
Select-Object	W–5-60	Single Sign-on	5–42
Selective ACK (tcp option)	1–142	Azure	5–48
SELinux	6–108	Single Sign-on (SSO)	2–32
Log	6–131	Skype	5–252
Mandatory Access Control (MAC)	6–108	SLE → Single Loss Expectancy	
Separation of duties	2–29	Small business server	5–14
Server core	5–16	Smartscreen filter → Internet Explorer	
Server manager	5–200	SMB → Server message block	
Server message block (SMB)	5–94	SMTP (port)	1–139
Port	5–212	Snapshot	
Server Nano	5–17	forensic	5–305
Internet Information Services (IIS)	5–232	PowerShell	5–309
servermanagercmd.exe	5–202	Snapshot encryption → Encryption	
Service		snare	3–181
disable	5–203	sniffer	1–80
securing	5–199	examples	1–82
Servicing branches	5–70	Sniffing (authorization)	1–83
Session attacks (app)	1–234	SNMP (Simple network managment protocol)	1–147
Session ID	1–232	port	1–147
hacking	1–233	snmp-check	W–3-15
Session tracking (app)	1–232	snort	1–82, 3–98
set	5–277	Rules	3–101
Set-ExecutionPolicy	W–5-70	snort (rules)	W–3-22
		SO:C1	6–109



# SEC401 – Security Essentials Bootcamp Style

SO:C1,C3 .....	6–109
SO:C2 .....	6–109
SO:C3 .....	6–109
SO:CO .....	6–109
SOC .....	5–14
Social engineering .....	3–44
Defense .....	3–46
Types .....	3–45
Software restriction policies .....	5–180
Software-defined network (SDN) .....	1–25
Sort-Object .....	W–5-67
Source routing .....	1–101, 6–102
SoX Linux .....	6–96
Spanning port .....	3–90
Spanning tree (switch) .....	1–20
Spear phishing .....	2–174
splunk .....	6–123
Sprawl managment .....	1–56
SQL injection .....	2–145
defense .....	2–147
SQL Sever (port) .....	5–214
SRP .....	5–180
SSH → Secure Shell .....	
SSL → Secure Socket Layer .....	
SSO → Single Sign-on .....	
SSP → Bluetooth .....	
Standard (policy) .....	2–70
Stateful (firewall) .....	3–68
Steganography .....	W–4-2, 4–40
detection .....	4–49
Injection .....	4–46
New file .....	4–48
types .....	4–45
Sticky bit .....	6–55
Stored procedures (SQL) .....	2–147
STP attack (switch) .....	1–20
Strength of a password hash → Password .....	
Stunnel .....	3–181
su .....	6–36
su/sudo .....	6–63
SubBytes .....	4–74
Substitution .....	
cryptography .....	4–22
steganography .....	4–47
sudo .....	6–36, 6–99
SUID .....	6–44
SUID/SGID programs .....	6–56
Superuser .....	6–62
Surface hub .....	5–13
Switch .....	1–77
attacks .....	1–20
Hardening .....	1–106
hardening .....	1–106
Hub vs Switch .....	1–79
sniffing .....	1–83
SYN Flooding Attack→ TCP SYN Flooding .....	
Symmetric encryption → Cryptography .....	
Symmetric key cryptosystem → Cryptosystem .....	
SYN flood → TCP .....	
sysctl command .....	6–101
sysctl hardening .....	6–101
Sysinternals .....	5–276
Syslog .....	
facility codes .....	6–140
format linux .....	6–139
linux .....	6–138
port .....	3–172
RFC .....	3–173
rSyslogd .....	6–146
security .....	6–142
severity levels .....	6–141
Syslog-ng .....	3–181
syslog-ng .....	6–145
System Access Control List (SACL) .....	5–296
auditing .....	5–296
System accounts .....	6–64
System level objectives .....	1–15
System restore .....	5–81
system-v style init .....	6–78
systemd .....	6–80
commands .....	6–81
pro/con .....	6–82
<b>T</b>	
tail .....	6–205
Take ownership .....	5–128
takeown.exe .....	5–100
Tarpits .....	3–221
TCP .....	1–112, 1–138
closing .....	1–143
connection .....	1–140
Handshake .....	1–140
Header .....	
Explicit Congestion Notification (ECN) ..	1–141
Windows scale .....	1–142
header .....	1–141
Initial sequence numbers .....	4–124, 1–140
Maximum segment size (MSS) .....	1–142
options .....	1–142
reset attack .....	1–19
SYN Flooding .....	1–19, 20, 2–122, 2–129
TCP/IP .....	
packets .....	1–120
TCP/IP vs OSI .....	1–118
tcpdump .....	1–82, 1–151
tcpdump (options) .....	W–1-29
tcsh → Secure Shell .....	
telnet .....	1–104
Telnet (port) .....	1–139
telnet (router) .....	1–104
telnet attack (switch) .....	1–20
TFTP .....	1–147
chroot .....	6–236
port .....	1–147
Threat .....	3–10, 4–207

T

tail	6–205
Take ownership	5–128
takeown.exe	5–100
Tarpits	3–221
TCP	1–112, 1–138
closing	1–143
connection	1–140
Handshake	1–140
Header	
Explicit Congestion Notification (ECN)	1–141
Windows scale	1–142
header	1–141
Initial sequence numbers	4–124, 1–140
Maximum segment size (MSS)	1–142
options	1–142
reset attack	1–19
SYN Flooding	1–19, 20, 2–122, 2–129
TCP/IP	
packets	1–120
TCP/IP vs OSI	1–118
tcpdump	1–82, 1–151
tcpdump (options)	W–1–29
tcsh → Secure Shell	
telnet	1–104
Telnet (port)	1–139
telnet (router)	1–104
telnet attack (switch)	1–20
TFTP	1–147
chroot	6–236
port	1–147
Threat	3–10, 4–207



agents	1–15
definition	3–37
enumeration	1–15
external	3–12
internal	3–13
types	3–11
Threeway handshake (TCP)	1–140
Timestamp (TCP option)	1–142
TKIP (Temporal key integrity protocol)	1–183
wireless	1–183
TLS	4–122, 1–219
Internet Information Services (IIS)	5–235
Token-based Access Control	2–30
Tools logs	3–183
top	6–197, 6–201–203
TopSecret	6–109
TPC	
Piggy-backed	1–140
TPE Trusted Path Execution	6–110
TPM	5–131
Tractable problems	4–62
Traffic class (IPv6 header)	1–129
Translation (IPv6)	1–130
Transport mode (IPsec)	4–100
Tripwire	6–214
Trust	5–42
Trusted Path Execution (TPE)	6–110
Trusted platform module	5–133
Trusted sites zone → Internet Explorer	
Trustlink	5–42
TTL (IPv4 header)	1–127
Tunnel mode (IPsec)	4–100
Tunneling (IPv6)	1–130
Twofish	4–73
Type 1 hypervisor	1–50

## U

UAC → Account	
Ubuntu	6–14
UDP	1–146
header	1–148
use	1–147
UEFI secure boot	5–138
UK Center for the Protection of National Infrastructure (CPNI)	2–93
UK Gov. communications HQ (GCHQ)	2–93
umask	6–57
unc path	5–111
Unclassified	6–109
Underground market hotfixes	5–10
Undirectional gateway	3–72
Update	5–69
Update rollup	5–64
Update vs upgrade	5–69
Upgrade	5–69
upstart	6–79
URLSCAN (IIS)	5–237

US-CERT	2–93
User account control (UAC)	5–181
useradd	6–67
Users 🐼	6–61
utmp (linux log)	6–131

## V

Valuable data	1–7
Vector (threat)	3–11
Verifying policy compliance	5–283
Vertical markets → Wireless	
Virtual administrator	1–53
Virtual machine	1–37
Disaster Recovery Plan (DRP)	1–41
Guest OS	1–37
Host OS	1–37
Host-only network	1–46
Hypervisor	1–39, 1–51
introspection	1–51
Layers of infrastructure complexity	1–55
Machines become files	1–52
NAT	1–46
Patch	1–56
Resource sharing	1–55
Risk mitigation	1–56
Snapshot encryption → Encryption	
software	1–40
Trust zones	1–56
Type	1–39
Virtual sprawl	1–52
Virtualization security	1–49
VLAN	1–14, 1–106
hopping (switch)	1–20
VM	
escape tactics	1–49
network options	1–46
VM & containers	6–243
Volume storage	1–59
Encryption	1–60
VPN	4–92
advantage	4–93
breakdown	4–94
SSL	4–102
types	4–95
Vulnerability	3–14, 4–207
assessment	6–253
axioms)	3–16
definition)	2–37
Microsoft	5–63
scan)	3–28, 3–30

## W

WaaS	5–69
wbadmin	5–77
Webapp	

monitoring .....	1-235
securing .....	1-222
vulnerability .....	1-227
Whitelisting .....	1-25
whoami.exe .....	5-28, 29, 5-123
Wifi	
misconceptions .....	1-185, 1-189
security risks .....	1-191
Windows	
as a service .....	5-69
client edition (CE) .....	5-7
Computer Management .....	5-26
DLL injection → DLL Injection .....	
embedded .....	5-19
End of sales .....	5-9
End of support .....	5-9
Custom .....	5-10
Extended .....	5-10
Mainstream .....	5-9
firewall → Firewall .....	
IoT .....	5-19
licensing .....	5-8
logging (configure) .....	5-292
OS classes .....	5-6
OS clients .....	5-7
phone .....	5-11
best practices .....	5-12
platforms .....	5-8
server .....	5-14
backup .....	5-77
roles .....	5-18
Servicing branch .....	5-70
update .....	5-68
Windows Event Viewer logs .....	5-292
Windows Management Instrumentation (WMI) .	W-5-70
Windows Server Update Services (WSUS) .....	5-71
Wireless	
Advantages .....	1-167
Evil twin .....	1-194
IDS .....	3-105
Masquerading .....	1-194
Network mapping mitigation .....	2-34
Network scan .....	3-32

Popular devices .....	1-164
Security risks .....	1-191
Steps for securing .....	1-200
TKIP (Temporal key integrity protocol) ....	1-183
Vertical markets (wireless) .....	1-165
WEP .....	W-1-45
WPA/WPA2 .....	1-201
Wireshark .....	W-1-51, 1-82
WMI (Windows Management Instrumentation) .	W-5-70
wmic.exe .....	5-273
Workgroups .....	5-22
benefits .....	5-24
drawbacks .....	5-25
World writable directory .....	6-55
WSUS → Windows Server Update Services .....	
wtmp (linux log) .....	6-131

## X

X.509 .....	4-118
Xbox one .....	5-13
xfce .....	6-87
xinetd.conf .....	6-94
XNU .....	6-18
XOR → Cryptography XOR .....	
XSRF → Cross-site request forgery .....	
XSS (Cross-site scripting) .....	1-15
xxd .....	W-3-27

## Y

YUM package .....	6-14
-------------------	------

## Z

Zeroday .....	3-14
Zigbee .....	1-175
Zigbee (security) .....	1-176
Zombie .....	1-18
ZPHA (Zero Power High Availability) .....	3-110