

INDEX

Italicized page numbers indicate definitions of terms.

Symbols

- * (asterisk/wildcard), 114
- @ (at sign), 37
- ~ (tilde), 175

A

- access control, 75, 81, 83, 94, 98, 101
 - least privilege, 83
 - privilege creep, 83
 - separation of duties, 83
- accounting, 75, 84, 101
- Advanced Encryption Standard (AES), 163, 174
- Advance Research Projects Agency, (ARPA), 14
- AES. *See* Advanced Encryption Standard (AES)
- alert, 9
- antivirus programs, 63
- Apple, 89
 - macOS, 70, 89, 98
 - account management, 98
 - exercise: Encrypting and Hashing Files, 172
 - file sharing, 100
- APT. *See* black hats, types
- ARPA. *See* Advance Research Projects Agency (ARPA)
- attack on objectives, 20
- attack techniques
 - denial of service (DoS), 110
 - distributed denial-of-service (DDoS), 110
 - DNS amplification attack, 111
 - man-in-the-middle, 108

- network tap, 107
- ping flood, 110
- Smurf, 110
- sniffing, 106
- vampire tap, 107

- Attribute-Based Access Control, 83, 84
- auditing, 86, 88, 92
- authentication, 76–81, 89–91, 98, 101
 - biometric, 79, 89
 - crossover error rate, 79
 - false acceptance rate, 79
 - false rejection rate, 79
 - fingerprint, 79, 90
 - Type 1, 76
 - Type 2, 78
 - Type 3, 78
 - Type 4, 80
 - Type 5, 80
 - verification code, 77
- authorization, 75, 81–83, 89, 98, 101

B

- backup, 9
- black hats, 4
 - types, 4
 - Advance Persistent Threats (APT), 6
 - hacktivists, 5
 - organized criminals, 5
 - script kiddies, 5
 - state actor, 5–6
 - vs. white hats, 4
- Bluetooth, 90
- broadcast addresses, 111
- brute force, 76

C

- CA. *See* certificate authority (CA)
- CAC. *See* Common Access Card (CAC)
- CAPTCHA, 80
- certificate authority (CA), 165–166
- certificates, 77
- certutil tool, 173
- CIA triad, 2
 - availability, 2
 - confidentiality, 2
 - integrity, 2
- cipher, 158–162, 166, 169
- ciphertext, 158
- CISA. *See* Cybersecurity and Infrastructure Security Agency (CISA)
- CKC. *See* Lockheed Martin Cyber Kill Chain (CKC)
- cloud computing, 126–128
 - cloud services
 - Infrastructure as a Service (IaaS), 127
 - Platform as a Service (Paas), 127
 - Security as a Service (SECaaS), 128
 - Software as a Service (Saas), 127
 - attacks
 - buffer overflow, 130
 - SQL injection, 131
 - XML injection, 132
- collisions, 171
- Common Access Card (CAC), 78
- command and control, 20
- controls, 183
 - Administrative, 184
 - Compensating, 184
 - Corrective, 184
 - Detective, 184
 - Preventative, 184
- cryptanalysis, 169–170
 - differential analysis, 169
 - integral analysis, 170
 - meet-in-the-middle, 169
 - side-channel attack, 170
- cryptography, 157–159
 - Alice and Bob, 158
 - asymmetric algorithm attacks, 170
 - asymmetric algorithms, 164
 - asymmetric cryptography, 163
 - asymmetric key, 161
 - attacks, 168
 - block ciphers, 162
 - Caesar Cipher, 160
 - connecting to a website, 167
 - cryptanalysis, 161
 - cryptographic algorithms, 158
 - data at rest, 158
 - data in transit, 158
 - data in use, 158
 - Enigma Machine, 160
 - hashing, 161, 164, 166, 171
 - digest size, 167
 - hashing algorithms, 167
 - hashing attacks, 171
 - initialization vector, 170
 - private key, 163, 168
 - private key cryptography, 161
 - protecting encryption keys, 170
 - public key, 163–165, 167
 - certificate authorities, 165–166
 - webs of trust, 165
 - salt, 172
 - Scytale, 160
 - session key, 170
 - single key cryptography, 161
 - stream cipher, 162
 - substitution, 159
 - substitution cipher, 159
 - symmetric cryptography, 161
 - symmetric key, 161, 168
 - symmetric key cryptography, 163
 - transposition, 159
 - transposition ciphers, 160
 - validating public keys, 164
 - waterfall effect, 166
 - what it is, 158
 - work factor, 161
- crypto-mining malware, 129
- cybersecurity, 2–3
 - career, 6
 - privacy, 2
- Cybersecurity and Infrastructure Security Agency (CISA), 10

D

DAC. *See* Discretionary Access Control (DAC)
databases, 7
Data Encryption Standard (DES), 162
 Triple DES, 162, 169
decryption, 158
defense in depth, 81
delivery, 19
demilitarized zone (DMZ), 112
DES. *See* Data Encryption Standard (DES)
digital certificate, 78, 165
Discretionary Access Control (DAC), 82, 84
DMZ. *See* demilitarized zone (DMZ)
Domain Name Service (DNS), 23

E

EAP. *See* Extensible Authentication Protocol (EAP)
ECC. *See* Elliptical Curve Cryptography (ECC)
Elliptical Curve Cryptography (ECC), 164
encryption, 78, 157–163, 165, 167–172, 174–177
 file encryption, 159
 transport encryption, 159
exploit, 3
exploitation and installation, 20
Extensible Authentication Protocol (EAP), 146

F

File Transfer Protocol (FTP), 63, 88
filtering, 154
 MAC address filtering, 155
 port filtering, 154
 URL filtering, 155
firewall, 88, 113
 hardware firewall, 113
 software firewall, 113
 packet-filtering, 113
 stateful inspection firewall, 114
firmware, 109
forensic analysis, 9
FTP. *See* File Transfer Protocol (FTP)

G

Google, 170
 Drive, 84
gray hats, 4

H

hacker, 4
hacking, 3, 5

I

IDS. *See* intrusion detection system (IDS)
IEEE. *See* Institute of Electronic and Electrical Engineers (IEEE)
ifconfig command, 29
incident, 8–9
 incident responders, 8–9
Indicators of Attack (IoA), 87
InfraGard, 11
Institute of Electronic and Electrical Engineers (IEEE), 144
internet service providers (ISPs)
intrusion detection system (IDS), 115
 heuristics, 116
 signatures, 116
intrusion prevention system (IPS), 116
IoA. *See* Indicators of Attack (IoA)
IP address, 15, 88
ipconfig command, 26–27
IPS. *See* intrusion prevention system (IPS)
IP spoofing, 107
IP suite. *See* TCP/IP
ISPs. *See* internet service providers (ISPs)

J

Joe Sandbox, 51–52, 68, 71

L

LAN. *See* local area network (LAN)
Linux, 9, 63–64
local account, 93
local area network (LAN), 105
Lockheed Martin Cyber Kill Chain (CKC), 18–20
logs, 9
logging, 85

M

MAC. *See* Mandatory Access Control (MAC)

malware, 4, 8–9, 55–65, 88

- malware analysis, 8
- types
 - polymorphic malware, 61
 - ransomware, 59, 87
 - rootkits and bootkits, 60
 - spyware and adware, 60
 - trojans, 59
 - viruses, 56
 - worms, 57

man command, 124

Mandatory Access Control (MAC), 82–84

MD5. *See* Message Digest 5

mesh network, 144

Message Digest 5, 167

Microsoft, 182

- OneDrive, 84
- Windows, 10, 70, 89
 - sharing a folder, 94
 - Exercise-Encrypting/Hashing a File, 172
- Windows accounts
 - setup, 89
- Windows Hello, 89
- Windows Hello Fingerprint, 90
- Windows Hello PIN, 90
- Windows Security, 89

MIMO. *See* Multiple-In Multiple-Out (MIMO)

modem, 16

MS-ISAC. *See* Multi-State Information Sharing and Analysis Center (MS-ISAC)

multi-factor authentication, 80

Multiple-In Multiple-Out (MIMO), 144

Multi-State Information Sharing and Analysis Center (MS-ISAC), 11

N

NAT. *See* Network Address Translation (NAT)

National Institute for Cybersecurity Education (NICE), 10

National Institute of Standards and Technology (NIST), 10

network, 2, 7–8

- networking, 7

Network Address Translation (NAT), 17

NICE. *See* National Institute for Cybersecurity Education (NICE)

NIST. *See* National Institute of Standards and Technology (NIST)

nodes, 16

non-repudiation, 2, 164, 183

NSFNET, 14

nslookup command, 27, 31

O

openssl tool, 175

operational security (OPSEC), 22

P

packet, 105

packet switching, 14

password, 76, 91

- cognitive, 76
- dictionary attack, 77
- security question, 76
- strength, 76

penetration testing, 3

- penetration testers, 10

Personal (or PSK) mode, 145

ping command, 27, 31

PGP. *See* Pretty Good Privacy (PGP)

plaintext, 158

port scan, 106

Pretty Good Privacy (PGP), 165

privacy, 3

- cybersecurity, 2

private network, 16

proxy server, 105

public network, 16

R

rainbow table, 171

RC4, 169

reconnaissance, 18

risk, 180–182, 184–188

- acceptance, 182
- avoidance, 182

- calculating, 180
- conducting a risk analysis, 187
- management, 181, 184, 186
- mitigate, 182
- risk register, 185
- transfer, 182
- risk management, 8
- Rivest–Shamir–Adleman, 164, 170
- role-based access control, 82–83
- router, 16
- rule-based access control, 82
 - implicit deny, 82

S

- SANS, 11
- scanning, 19
- Secure Hashing Algorithm 1 (SHA-1), 167
- security information and event management (SIEM), 87
- security kernel, 81
- Security Key, 91
- Security Operations Center (SOC), 6
- security plan, 180
- server
 - web, 168
- Service Set Identifier (SSID), 142
- SHA-1. *See* Secure Hashing Algorithm 1 (SHA-1)
- SHA-2, 167
- SHA-3, 167
- shasum command, 175
- Shodan, 21
- SIEM. *See* security information and event management (SIEM)
- smart card, 77
- sniffing, 19
- social engineering, 35–38, 77
 - hoax, 41
 - phishing, 36
 - spear phishing, 37
 - typosquatting, 40
 - vishing, 38
- SOC. *See* Security Operations Center (SOC)
- ssh-keygen command, 176
- SSID. *See* Service Set Identifier (SSID)
- STRIDE, 182

- switch flipping, 3
- Syslog, 85

T

- TCP/IP, 15
- Temporal Key Integrity Protocol (TKIP), 146
- threats, 9, 180, 182–185, 188
- tracert command, 28, 30
- Trusted Platform Module (TPM), 78

V

- VeraCrypt, 172
- vulnerability, 3, 9
 - zero-day, 4

W

- WAF. *See* web application firewall (WAF)
- WAN. *See* wide area network (WAN)
- WAP. *See* Wireless Access Point (WAP)
- weaponization, 19
- web application firewall (WAF), 115
- webs of trust, 165
- WEP. *See* Wired Equivalent Privacy (WEP)
- white hats, 4, 6
 - types, 6
 - chief information security officer (CISO), 7
 - computer forensic analysts, 9
 - cybersecurity analyst, 6
 - cybersecurity architects, 7
 - cybersecurity consultants, 7
 - incident responders, 8
 - penetration testers, 10
 - threat hunters, 9
 - vulnerability managers, 9
- wide area network (WAN), 105
- Wi-Fi Protected Access (WPA), 146
- Wired Equivalent Privacy (WEP), 146, 169
- Wireless Access Point (WAP), 142
- wireless attacks
 - disassociation, 148
 - jamming, 149
 - rogue access points, 147

wireless substandards

802.11a, *144*

802.11ac, *145*

802.11ax, *145*

802.11b, *144*

802.11g, *144*

802.11n, *144*

WPA. *See* Wi-Fi Protect Access (WPA)