Index

Numbers
007Shell, covert channel exploits, 248
3DES (Triple DES) encryption, 78–79, 88
3G hot spots, 412
4G hot spots, 412
802.11. See Wi-Fi
802.11i, 418
802.3 (Ethernet), 45

A
access control
   Android OS, 444–446
   Apple iOS, 446
   cloud computing, 495
   mobile device, 442–443
   physical. See physical security
access control lists (ACLs), 381, 470
access points
   broadcasting SSID, 413
   client misassociation attacks on, 428
   honeypot attacks on, 428–429
   misconfiguration problem with, 428
   rogue access point attacks, 426–427
   wireless antennas and, 414–415
   wireless network, 411–412
account hijacking, cloud security threat, 490
ACK flag, 134–135, 136–137
ACK scanning, 143–144
ACK sequence numbers, TCP/IP session hijacking, 344
ACK tunneling, defying detection by firewall, 479
AckCmd, 248, 479
ACLs (access control lists), 381, 470
active fingerprinting, of OS, 146–147
active information gathering, footprinting, 106
active online attacks, 198–199, 202–203
active session hijacking attacks, 335–336
active sniffing, 256
active wireless network attacks, 425
ad hoc attacks, on Wi-Fi, 427
administrator accounts, Windows OS, 60–61, 163–164
administrators
   application, 361
   server and network, 360
ADS (Alternate Data Streams), covering tracks, 216–217
adware, 227, 237
AES (Advanced Encryption Standard), 79
AES-256 encryption, Apple iOS, 446
AH (Authentication Header), IPSec, 90
aircrack-ng
   breaking WEP, 420–421
   brute-force attacks, 425
   wireless tool for lab testing, 572
aireplay-ng, 420
AirMagnet, 430
AirMon, 453
AirPcap
   breaking WEP, 421–422
   hardware tool for lab testing, 573
   sniffing wireless networks, 260
algorithms
   asymmetric, 80–86
   cryptography and, 77
   symmetric, 77–79
   types of hashing, 87
ALog reader, pentesting Android, 453
alteration, breaking CIA triad, 16
Alternate Data Streams (ADS), covering tracks, 216–217
alternate sites, business continuity/disaster recovery, 27–28
Amitis, Trojan-creation tool, 243
analysis and tracking phase, incident response, 24
AnDOSid, pentesting Android, 451
Android OS
   with 83 percent of market share, 441
   common problems, 447–448
   countermeasures, 454–455
customized versions of, 445–446
design of, 444–446
overview of, 443–444
pentesting, 450–454
storage encryption on, 442
vulnerabilities, 62
Android runtime (ART), 445
Android Updates, 445
Angry IP Scanner, 570
Anna Kournikova computer worm, 5, 291
anomaly-based IDS, 464–465
anonymity, pentesting Android, 454
Anonymous hacking group, 6, 8
Anonymous logon group, Windows, 165
antennas, wireless, 414–416
antimalware applications
DoS/DDoS protection, 323
installing for lab testing, 569
mobile device countermeasures, 455
antivirus applications
installing for lab testing, 569
Phatbot terminating, 243
polymorphic/metamorphic viruses
unidentifiable to, 230
virus detection and elimination, 229
web browser integration with, 295
AOKP (Android Open Kang Project), 445
Apache Server, 361–362, 367
App Scanner, pentesting Android, 452
Apple iOS
with 14 percent of market share, 441
common problems, 447–448
countermeasures, 454–455
overview of, 446–447
Apple iOS vs. Android, application provenance, 446
application administrators, 361
application content, web applications, 369
application developers, web applications, 361
Application layer, OSI model
overview of, 46
session hijacking at, 334
SNMP functioning at, 178
application proxy firewalls, 56, 58–59
application services, Android OS, 445
application-level attacks, 310–314
application-level firewalls, 469
application-level hijacking
cross-site scripting, 338–341
man-in-the-browser attacks, 338
man-in-the-middle attacks, 338
predicting session tokens, 338
session fixation attacks, 341
session sniffing, 337
web apps, 336–337
applications
executing, 213–217
mobile device countermeasures, 455
security testing of, 554
session hijacking and web, 336–337
sources of Android OS, 445
tools for building lab, 570–571
web. See web servers/applications
AppThwack, testing security in cloud, 496
architecture, cloud security controls, 494–495
archived copies of website, footprinting, 110
Archive.org, 110
archiving, 63–64
ARP (Address Resolution Protocol) requests, and
MAC addresses, 55
ARP poisoning
overview of, 343
pentesting mobile devices with, 450
preventing, 273
sniffing switched networks, 271–272
ART (Android runtime), 445
AS (authentication server), Kerberos, 211–212
Assange, Julian, 307
association, defined, 414
asymmetric (public key) cryptography
authenticating certificate, 83
building PKI structure, 85–86
how it works, 81–82
how you know who owns key, 82–83
overview of, 80–81
PKI system, 83–85
attacks
defined, 13
threats. See threats
attributes, protecting cookie, 379–380
auditing, disabling to cover tracks, 215–216
auditipol command, disabling auditing, 216
authentication
biometric, 515–516
certificate, 83
cryptography for, 75–76
as defense against session hijacking, 352
on Microsoft platforms, 209–213
multifactor, 198
with SNMPv3, 178
technologies, 418
web application, 368
wireless modes of, 416–417
Authentication Header (AH), IPSec, 90
authentication server (AS), Kerberos, 211–212
authorization, before pen testing, 556–557
automated penetration testing, vs. manual, 561–562
availability
balancing security with, 308
breaking CIA triad, 16
cloud security controls, 495
preserving CIA triad, 15–16
awareness, as line of defense, 519

B

B0CK, exploiting covert channels, 248
Back Orifice 2000 (BO2K), 243–246
backdoors
attacker access via, 246–247
executing applications via, 213–214
planting, 214–215, 561
system administrators using, 287
back-end resources, DoS attacks on, 308
backups
business continuity/disaster recovery via, 28
overview of, 63–64
securing, 519
bandwidth
defined, 414
protecting from DoS/DDoS attacks, 323
wireless networks and, 411
banner grabbing
countermeasures to, 151
identifying services running on ports, 470
overview of, 149–151
as web server/application vulnerability, 373
basic service set identification (BSSID), 414, 423
bastion host, firewall configuration, 468
bat2com, creating viruses, 233
batch execution, in SQL injection attacks, 392
batch group, Windows, 165
BCP (business continuity plan), 26–29
Beast, Trojan-creation tool, 243
BeEF (Browser Exploitation Framework), 200–201
best evidence, defined, 30
best practices, reporting security incident, 32
binary conversion, vs. hexadecimal, 49–50
biometrics, 515–516
black box pen tests, 14–15
black hole filtering, 324
Blackberry. See also mobile device security, 441
black-box testing, 551
black-hat hackers, 9, 11
blacklists, 392, 404
BlazeMeter, 496
blind hijacking, 341, 345
blind SQL injection, 401–402, 403
blind testing, 552
blocked scans, 144
Blowfish, 79
bluejacking attack, 433
Bluepot, 433
Bluesnarfer tool, 572
bluesnarfing attack, 433
Bluetooth, creating test setup, 568
Bluetooth, hacking. See also Wi-Fi, hacking
current developments in, 4
overview of, 431–432
threats, 432–433
as vulnerability in Mac OS X, 62
BO2K (Back Orifice 2000), 243–246
bolllards, protecting facilities, 517, 518
boot-sector (or system) viruses, 229, 230
Bothyl, Adam, hacker, 5
botnets
DDoS attacks and, 318
defensive strategies, 323–324
rental of, 307
tools for creating, 318–319
bots, 318
bricked systems, caused by phlashing, 310
bring your own device (BYOD), problems with,
440–441, 448–449
broad network access, cloud computing, 487
broadcast domains, 55
browser defects, spyware delivery via, 236
Browser Exploitation Framework (BeEF), 200–201
browser-based web applications, 363–364
brute-force attacks
on cryptographic systems, 88
on directory services, 162
in exploitation phase, 560
in password cracking, 198
on session ID in session hijacking, 333
in syllable attacks, 198
on WPA/WPA2 keys, 425
Brutus, password cracking with, 377–378, 571
BSSID (basic service set identification), 414, 423
buffer overflow attacks
  as DoS attacks, 314
  heap and stack, 314–315
  NOP sled, 317
  smashing stack, 315–316
  on web servers/applications, 370–371
building a lab. See lab, building
Burp Suite
  man-in-the-middle attacks, 200–201
  pentesting Android, 453
  testing web applications, 383
bus topology, 40–41
business closure, from social engineering, 286
business continuity plan (BCP), 26–27
BusinessWire, competitive analysis data, 117
BYOD (bring your own device), problems with, 440–441, 448–449

C
C functions, buffer overflow vulnerability, 314
C2DM (cloud-to-device messaging), Android OS, 445
cabling
  at Physical layer of OSI model, 45
  protecting server rooms, 518
Cain & Abel
  breaking WEP, 420
  sniffer tool for lab testing, 572
CAM tables, and MAC flooding, 270–271, 274–275
cameras, physical security, 517, 518
CAN-SPAM Act, 227
capture button, sniffers, 257
CAs (certificate authorities), 82–85
case locks, 519
Catch Me If You Can movie, social engineering in, 285
categories, malware, 227–228
cavity (file-writing) viruses, 231
CCTV Scanner, pentesting Android, 452
CEH credential, Code of Conduct and Ethics, 11–12
ceiling, securing physical area, 516–517
CER (crossover error rate), biometric accuracy, 515
certificate authorities (CAs), 82–85
chain of custody, evidence, 30–31
Check Point FireWall-1, 470
choke points
  firewall services at, 467
  gates as physical, 511
chosen plaintext/cipher-text attacks, on cryptographic systems, 89
CIA (confidentiality, integrity, and availability)
  triad, 15–17
cipher locks, physical access control, 513
cipher text
  in asymmetric algorithms, 80
  how cryptography works, 77
  PKI system, 83–85
  in symmetric algorithms, 77
ciphers, weaknesses in web applications, 380
cipher-text-only attacks, on cryptographic systems, 89
circuit-level gateway firewall, 469
circumstantial evidence, 30
Cisco IOS devices, mitigating MAC flooding, 274
CLI (command-line interface), Wireshark tools using, 264
client misassociation attack, on Wi-Fi, 428
client-based web applications, 364
clients, DoS attacks against specific, 308
client-server relationship, 360–361, 364–365
client-side technologies, 365, 394
climate control, server rooms, 518
cloud technologies
  Android OS, 445
  cloud computing attacks, 490–494
  controls, 494–495
  forms of cloud services, 488–489
  overview of, 365–366, 486
  review, 496–497
  review answers, 546–547
  review questions, 498–500
  testing, 495–496
  threats, 489–490
  types of cloud solutions, 487–488
  understanding, 486–487
  understanding cloud computing, 485–487
cloud-to-device messaging (C2DM), Android OS, 445
cluster viruses, 231
CNBC, competitive analysis data via, 117
code injection, session fixation attack, 341
Code of Ethics, 11–12, 33
cold sites, 27
collision domains, 55
columns, database, 395
command injection, in session hijacking, 334
command-line interface (CLI), Wireshark tools using, 264
communication channels, disaster and recovery, 29
community cloud, 488
CommView, wireless traffic analysis, 430
companion (camouflage) viruses, 231
competitive analysis, in footprinting, 118–119
complex passwords, risk mitigation for WEP/WPA, 425
compliance, cloud security controls, 495
components
Android OS, 444–446
web application, 367–368
computer crime
collecting evidence. See evidence collection incident response for. See incident response
con artists, social engineers as, 283
concatenating strings of texts, evading detection via, 404
conclusive evidence, 30
confidentiality
CIA triad and, 15–16
Code of Ethics for, 11
ethical hacker responsibility for, 10, 13
as primary goal of encryption, 75
construction kits, Trojan, 246
contactless cards, securing physical area, 515
contacts, social networking countermeasures, 292
containment phase, incident response, 24
contracts
contents of, 555–556
ethical hacker responsibility for, 9–10
getting help of lawyer, 10
before starting testing activities, 13
controls
cloud security, 494–495
defense in depth, 520
physical security, 503–505
convenience vs. security analysis, 14
cookies
protecting, 379
safely using, 367–368
session hijacking and, 337
web server/application session management issues, 379
corroborative evidence, 30
counterfeit devices, as Android OS vulnerability, 62
countermeasures
banner grabbing, 151
identity theft, 297–298
mobile device security, 454–455
social networking, 291–293
covering your tracks
Alternate Data Streams, 216–217
data hiding, 216
disabling auditing, 215–216
in hacking process, 18
overview of, 215
cover channels
defined, 239
tools to exploit, 247–248
Trojans as biggest users of, 247
 crackers, executing applications via, 214
CRC32 (Cyclic Redundancy Check), WEP vulnerability, 419
Creator group, Windows, 165
Creator owner group, Windows, 165
credentials, threats to cloud security, 490
credit card information, hacking of, 5, 296
Creeper project, virus, 228
crossover error rate (CER), biometric accuracy, 515
cross-site request forgery (CSRF), against cloud, 491–492
cross-site scripting. See XSS (cross-site scripting)
crying wolf, defying detection by IDS, 476
cryptanalysis
attacks against cloud, 494
defined, 73
Cryptcat, tool for lab testing, 571
cryptography
applications of, 89–94
applied, 76
asymmetric. See asymmetric (public key) cryptography
encryption and, 73
evolution of, 75–76
hashing, 86–88
history of, 73–75
how it works, 77
issues with, 88–89
overview of, 72–73
review, 94
review answers, 528–529
review questions, 95–97
symmetric, 77–79
cryptoviruses, 232
CSRF (cross-site request forgery), against cloud, 491–492
customized Android versions, 445
CyanogenMod, Android, 446
cybercrime
  current developments in, 4–5
  DoS attacks, 307
  famous hacks over time, 5–6
  generic examples of, 6–7
DDoS (distributed denial-of-service) attacks
  against cloud, 490, 494
  as cybercrime, 7
  overview of, 317–319
tools, 320–322
web servers/applications vulnerable to, 371
deauthentication attack, on WPA/WPA2, 424–425
debriefing and feedback phase, incident response, 24
decimal, hex/binary vs., 50
decision-making, reporting security incident, 32
decoys, honeypots as, 473–474
defacement, website, 374–375
default passwords
  avoiding, 405
  obtaining, 207
  obtaining information through, 162
default scripts, causing attacks, 378
defense in depth
  physical security and, 519
  session hijacking protection, 352
defensive strategies, DoS, 323–324
degaussing, hard drives/magnetic media, 508–509
deliverables, in contract content, 556
demilitarized zone (DMZ)
  firewall configuration, 468–469
  honeypots as decoys in, 473–474
Department of Energy (DoE), SQL injection attack on, 391
DES (Data Encryption Standard), 78, 88
descynchronizing connections, 342
design
  Android OS, 444–446
  cloud security controls, 494–495
  flawed web server/application, 369–370
  viruses, 228
  vulnerabilities of web servers/applications, 369–370
destructive Trojans, 240
detection
  difficulty of social engineering, 283
  viruses and, 229
Dev@Cloud, 496
developers, Android OS security and, 443
device drivers, authentication of, 76
devices, network, 53–55
dial-up, as backup to existing technologies, 131
dictionary attacks, 198
differential backups, 63
dig command, 175–176
digital certificates, 83, 86
digital rights management (DRM), 446–447
digital signatures
in asymmetric cryptography, 81–83
creating with digital certificates, 86
creating/verifying with hash function, 81–82
mobile device security via, 442
digital trespassing, as cybercrime, 6
direct evidence, 30
directional (Yagi) antenna, 415
directory services
brute-force attacks on, 162
and LDAP enumeration, 182–183
directory traversal attacks, web servers, 381–383
DirecTV dish, 416
disaster recovery plan (DRP), 26–29
disclosure
breaking CIA triad, 16
Code of Ethics for, 11
discoverable mode, Bluetooth, 431
Dish Network dish, 416
disruption (loss), breaking CIA triad, 16
distributed computing, SETI programs, 206
distributed databases, 395
distributed denial-of-service attacks. See DDoS
(distributed denial-of-service) attacks
Distributed Network Attack (DNA), password cracking, 205–206
DMZ (demilitarized zone)
firewall configuration, 468–469
honeypots as decoys in, 473–474
DNA (Distributed Network Attack), password cracking, 205–206
DNS (Domain Name System)
attacks against cloud, 494
overview of, 53
querying with nslookup, 119–120
TCP 53 port for, 169
UDP 53 port for, 169
working with zone transfers, 162
DNS spoofing, 343, 351–352
documentation, planning disaster and recovery, 29
DoE (Department of Energy), SQL injection attack on, 391
Domain attribute, cookies, 380
Domain Name System. See DNS (Domain Name System)

DoS (denial-of-service) attacks. See also DDoS
(distributed denial-of-service) attacks
in active session hijacking, 335
against cloud, 490, 494
as cybercrime, 7
defensive strategies, 323–324
defying detection by IDS, 475
jamming attacks on WLANs, 428
overview of, 306, 371
pentesting Android, 451–452
pen-testing considerations, 324
review, 324–325
review answers, 537–538
review questions, 326–329
targets, 308
tools for, 319–320
understanding, 306–308
WEP vulnerability to, 419
DoS (denial-of-service) attacks, types of
application-level, 310
buffer overflow, 314–317
fraggle, 310
ICMP flood, 309
land, 310
permanent DoS, 310
ping of death, 309–310
service request floods, 308
smurf, 310
SYN attack/floods, 309, 311–314
tear drop, 310
DoSHTTP, DoS tool, 319
double-blind testing, 552
drivers, installing for lab testing, 569
drives
disabling for protection, 519
encrypting, 506–507
wiping, 508
DRM (digital rights management), 446–447
DroidSheep, pentesting Android, 451
DroidSQLi, pentesting Android, 453
Dropbox, as cloud computing, 487
dropboxes, breaching wireless networks with, 427
DRP (disaster recovery plan), 26–29
dsniff, sniffer, 259
dSploit Scripts, pentesting Android suites, 454
due diligence, cloud security and, 491
DumpSec, enumeration tool for lab testing, 571
dumpster diving
as cybercrime, 7
preventing, 294
social engineering via, 121
thwarting for discarded media, 508
duration, penetration test, 555
dynamic content, in cross-site scripting, 339–341
dynamic pages, in directory traversal attacks, 382
dynamic ports, 51
dynamic SQL, thwarting SQL injection, 404

E

EAP wireless authentication, 418
Easy Packet Blaster, pentesting Android, 451
eavesdropping, social engineering and, 120, 293
EC Council (International Council of Electronic
Commerce Consultants), 10, 11–12
Echosec, social engineering via, 115–116, 292
e-commerce, cryptography in, 75
economic loss, from social engineering, 285
EDGAR (Electronic Data-Gathering, Analysis,
and Retrieval) system, 117
education, as line of defense, 519
egress filtering, as DoS/DDoS prevention, 323
Egyptian hieroglyphics, 74–75
EIP (Extended Instruction Pointer) value, 315–317
Electronic Data-Gathering, Analysis, and
Retrieval (EDGAR) system, 117
elimination, virus, 229
EliteWrap, distributing Trojans, 246
Elk Cloner virus, 229
e-mail
cloud computing for, 487
in footprinting process, 117–118
law enforcement agencies and sniffing, 258
performing enumeration on, 162
SNMP enumeration, 184–186
in social engineering via phishing, 120–121
spyware delivery via attachments, 236
embezzlement, as cybercrime, 7
employee profile, gathering job posting data, 117
Encapsulating Security Payload (ESP), IPSec, 90
encryption
in Apple iOS, 446
cryptography and, 73
as defense against session hijacking, 352
defying detection by IDS, 477
Egyptian hieroglyphics, 74–75
mandating by law, 507
physically securing drives, 506–508
weaknesses in web applications, 380
encryption, wireless
methods of, 417
mobile device, 442, 505–506
mobile device countermeasures, 455
protocols, 417
risk mitigation for WEP/WPA, 425
WEP, 418–422
WPA, 422–425
encryption viruses, 230, 231
entryways, protecting, 517–518
enum4linux command, 181–182
enumeration
in hacking process, 17–18
LDAP and directory service, 182–184
Linux, 180–182
NTP, 184
review, 187–188
review answers, 532
review questions, 189–191
as second phase of ethical hacking, 101–102
SMTP, 184–186
SNMP, 178–180
tools for building lab, 571
understanding, 161–163
Unix, 180–182
in vulnerability analysis phase, 559
Windows, 163–167
error messages
acquiring target in SQL injection attacks via, 398
extracting information from, 403
suppressing detailed, 374, 402
thwarting SQL injection by disabling, 405
in web servers and applications, 374
escalation of privilege, in hacking process, 18
ESP (Encapsulating Security Payload), IPSec, 90
EssentialNetTools, TamoSoft, 186
/etc/passwd file, Linux user account, 168
EtherApe, sniffer, 260
ethical hacking, introduction to
business continuity plans, 26–28
chain of custody, 30–31
code of conduct and ethics, 11
conflicting views about hackers, 3
current developments, 4–5
early days of hacking, 3–5
ethics and the law, 33–34
evidence types, 29–30
evidence-collection techniques, 29
evasion and growth of, 7–8
exam objectives, 1
as fun vs. criminal activity, 5–7
hacking methodologies, 17–21
incident response, 21–26
overview of, 2–3
penetration testing, 11–17
recovering from security incident, 31–32
recovering systems, 28–29
reporting security incident, 32–33
responsibilities of, 9–11
review, 34–35
review answers, 526–527
review questions, 36–38
role of ethical hacker, 9
rules of evidence, 31
steps of, 100–102
types of hackers, 9
vulnerability research and tools, 21

evasion
firewalls. See firewalls
honeypots, 473–474
IDS, 462–466, 475–477
overview of, 462
review, 480–481
review answers, 544–546
review questions, 482–484
testing firewalls, 479–480
testing IDS, 480

event-viewing tools, lab testing, 572
Everyone group, Windows, 165
evidence collection, 29–31
evolution, of hacking, 4–8
executive level report, on security incident, 33
executives, as targets of social engineers, 286
Expires attribute, cookies, 380
exploitation
pentesting mobile devices, 450
phase of penetration testing, 560
post-exploitation phase, 560–561
exploits, defined, 13
EXPN command, SMTP enumeration, 185–186
Extended Instruction Pointer (EIP) value, 315–317
Extensible Markup Language (XML), 493, 494
extensions, signs of host system intrusions, 466
exterior, building for physical defense, 520
external factors, and reports, 562–563
extortion, DoS attacks for, 307

F
Facebook
gathering information using, 288–289
people search utility, 297
social engineering via, 114
FaceNiff, pentesting Android, 451
Fakegina keylogger, 248
false ceilings, securing physical area, 516
false rejection rate (FRR), biometric accuracy, 515
false walls, securing physical area, 516
FAR (false acceptance rate), biometric accuracy, 515
fault tolerance, business continuity/disaster recovery, 27
FDDI (Fiber Distributed Data Interface), ring topology, 42
Federal Information Security Management Act (FISMA), 2002, 34
fences, securing physical area, 511
Fiber Distributed Data Interface (FDDI), ring topology, 42
file (multipartite) viruses, 230, 232
file integrity checker, 46
File Transfer Protocol. See FTP (File Transfer Protocol)
file-allocation tables, cluster viruses altering, 231
files, signs of host system intrusions, 465–466
file-writing (cavity) viruses, 231
filters, Wireshark, 263–264
FIN flag, 137, 139–141
FIN scan, 140–141
financial fraud, embezzlement as, 7
financial services
current developments in hacking/cybercrime, 4–5
in footprinting process, 116
researching data on companies via, 117
Fing, pentesting Android, 450
finger command, Linux/Unix enumeration, 178, 180–181
finger scan systems, biometrics, 516
fingerprinting. See OS fingerprinting
fire suppression, server rooms, 518
Firekiller 2000, distributing Trojans, 246
Firesheep, session hijacking, 337
Firewalk, determining firewall configuration, 470–472
firewalking, determining firewall configuration, 470–472
firewalls
- blocking ping requests, 134–135
- blocking scans, 144
- bypassing, 479–481
- configurations, 468–469
- determining configuration with firewalking, 470–472
- determining configuration with nmap, 472–473
- evading with fragmenting, 144
- identifying, 470
- for mobile devices, 473
- overview of, 56–57, 467–468
- setting up security, 58–59
- testing, 479–480
- types of, 469

FISMA (Federal Information Security Management Act), 2002, 34

flags
- defying detection by IDS, 476–477
- TCP, 136–137

flash drives, physical security of, 507–508
flawed web design, web servers/applications, 369–370

floors, securing physical area, 516–517
folders, signs of host system intrusions, 465–466

footprinting
- competitive analysis in, 118–119
- email, 117–118
- as first step of ethical hacking, 17, 100–101
- information gathering via, 113–116, 160
- as intelligence gathering, 557–558
- job sites and job postings, 116–117
- location and geography in, 112–113
- network information gathering in, 119–120
- other phases of ethical hacking, 101–102
- overview of, 100
- pen testing mobile devices via, 449
- public and restricted websites, 111–112
- review, 121–122
- review answers, 529–530
- review questions, 123–125
- search engines, 108–111
- as social engineering phase, 120–121, 285
- terminology, 106–107
- threat modeling via in-depth, 557–558
- threats introduced by, 107
- understanding, 102–106
- forwards, web server/application attacks from unvalidated, 376–377

fragile attack, as DoS attack, 310

fragmentation attacks
- on Android devices, 448
- defying detection by firewalls, 478
- defying detection by IDSs, 476
- web servers/applications vulnerable to, 372
- fragmenting packets, preventing detection, 144
- fragroute command, 144
- fragtest command, 144
- frames, securing door, 512
- fraud, as cybercrime, 7
- freeware, spyware delivery via, 236
- FRR (false rejection rate), in biometric accuracy, 515
- FTP (File Transfer Protocol)
  - easy sniffing of, 259
  - TCP 21 port for, 169
  - Trojans, 240
- vulnerable to man-in-the-middle attack, 200
- full backups, 63
- full-open scans, 135
groups
- capturing user, 162–163
- Linux, 169
- security identifiers for Windows, 166–167
- storing information in SAM, 167
- Windows, 164–165

GSM (Global System for Mobile Communications), 414
guest account, Windows OS, 163

H

hack value, 13
hackers
- ethical hackers vs., 10
- evolution of, 3–8
- methodologies of, 17–21
Hackode, pentesting Android suites, 454
hactivism, DoS attacks based on, 307
half-open (stealth) scan, 135–136
hand geometry systems, biometrics, 516
handler (master computer), DDoS attack setup, 318–319
HAPs (hardware access points), 411
hard drives
- creating test setup, 568
- physical security of portable, 506–507
Hard-disk killer, Trojan-creation tool, 243
hardening
- network against sniffing, 273
- thwarting SQL injection, 404–405
- as vulnerability in Windows, 61
hardware
- Android OS, 444
- gathering job posting data, 117
- planning disaster and recovery, 29
- protocol analyzers, 258
- tools for lab testing, 573–574
hardware access points (HAPs), 411
hash function, 81–82, 86–88
hash injection attacks, 202–203
hashing
- passwords, 203
- process of, 86–88
- rainbow tables attacks using precomputed, 203–205
- salting to strengthen password, 210
HAVAL, hashing algorithm, 87
HAVING command, error messages, 403
heap, in buffer overflow attacks, 314–315
help desk personnel, social engineering, 286
hex coding, evading detection via, 404
hexadecimal values
- MAC addresses broken down into, 54
- reading sniffer output in IP addresses, 269–270
- vs. binary, 49–50
HFS (Hierarchical File System), Mac OS X, 216
hidden field, session ID embedded in, 336
hiding data, 216–217
HIDS (host-based intrusion detection system), 463
high-availability architecture, business continuity/disaster recovery, 27
high-interaction honeypots, 474
history, of cryptography, 73–75
hoaxes, 232
Home Depot, tarnished through social media, 290
honeynets, 474
honeypots
- Bluetooth, 433
- purposes of, 473
honeypot attacks, on Wi-Fi, 428–429
horizontal privilege escalation, 212
host, firewalking, 470
host system intrusions, signs of, 465–466
host-based intrusion detection system (HIDS), 463
hostname, using Ping via, 133
hot sites, 28, 29
hot spots, 412, 414
Hping2/hping3
- checking for live systems, 134–135
- checking status of ports, 137
- ICMP flood attacks, 309
- scanner for lab testing, 571
- web servers/applications vulnerable to, 371–372
HP’s Performance Insight, detecting sniffing attacks, 275
HTTP (HyperText Transport Protocol)
- easy sniffing of, 258
- header response, 341
- listener, IIS, 363
- and SOAP, 494
- TCP 80 port for, 169
- tunneling, defying detection by firewall, 479
HTTP Injector tool, pentesting Android, 453
HTTP Tool, pentesting Android, 453
HttpOnly attribute, cookies, 379
HTTPRecon, fingerprinting website, 374
HTTPPrint, identifying sites, 374
HTTPS, 367
HTTP . sys file, 363
hubs, switches vs., 56
human beings
art of hacking, 120–121
power of social engineering and nature of, 284
HUMINT (human intelligence), penetration testing, 558
hybrid attacks, password cracking via, 198
hybrid cloud, 488
hybrid topologies, 42–43

IaaS (Infrastructure as a Service) model, cloud, 365, 489
ICMP (Internet Control Message Protocol), 133–134
ICMP Backdoor, 247
ICMP flood attack, 309, 371–372
ICMP tunneling, 479
ICMP_TIME_EXCEEDED message, nmap, 472
ID Serve, providing information about web server, 373
IDEA (International Data Encryption Algorithm), 79
identity theft, 75, 296–298
idle scans, 142–143
IDS (intrusion detection system)
detection methods, 464–465
evading, 144, 403–404
firewalls as form of, 467
inner workings of, 462–463
overview of, 57
role of, 462
signs of intrusion, 465–466
testing, 480
thwarting session hijacking via, 352
thwarting SQL injection via, 403, 404
types of, 462
IEEE 802.11 standard, 411–413
ignorance, social engineers preying on, 283
IGRP (Interior Gateway Routing Protocol), 45
IIS (Internet Information Server)
countering banner grabbing, 151
overview of, 362–363
used by web applications, 367
IIS Lockdown, 151
IKS Software Keylogger, 248
illegal material, and cybercrime, 7
IM (Instant Messaging), spyware delivery via, 236
IMAP (Internet Message Access Protocol), 259
incident response
business continuity plan, 26–28
overview of, 21–22
phases of, 22–25
plans, 25–26
policies, 22
recovering from security incident, 31–32
recovering systems, 28–29
reporting security incident, 32
team, 25
incident response policies (IRPs)
in incident response plans, 25
overview of, 22
reporting security incident via, 32
Incognito, pentesting Android, 454
incorporation, virus, 229
incremental backups, 63
industrial, scientific, and medical (ISM) band, 414
inference
overview of, 288
using corporate espionage, 119
information
data-diddling of, 7
gathering in SQL injection attack, 402–403
leakage caused by footprinting, 107
sharing too much on social media, 289–291, 296
social networking countermeasures, 292–293
unauthorized destruction/alteration of, 7
Infrastructure as a Service (IaaS), cloud, 365, 489
ingress filtering, countering DoS/DDoS attacks, 323
initial sequence number (ISN), 343
initialization vectors (IVs), 419–420
input strings, evading detection via, 404
input validation
SQL injection attack from flawed/absent, 391
thwarting SQL injection using, 392, 404
web server/application attacks from flawed/absent, 375
insertion attack, defying detection by IDS, 475
insider attacks, 555
inSSIDer tool, 426, 572
Instagram, social engineering via, 114
Instant Messaging (IM), spyware delivery via, 236
integrity
  breaking CIA triad, 16
  cryptography used for information, 75
  preserving CIA triad, 15–16
Intelsis, people search utility, 113, 298
intellectual property, Code of Ethics for, 11
intelligence gathering, in penetration testing, 557–558
Interactive group, Windows, 165
Interceptor-NG, pentesting Android, 451
interference, Wi-Fi and, 411
interior controls, as third layer of physical defense, 520
Interior Gateway Routing Protocol (IGRP), Network layer of OSI, 45
International Council of Electronic Commerce Consultants (ECCouncil), 10, 11–12
International Data Encryption Algorithm (IDEA), 79
Internet
developments in hacking/cybercrime, 4–5
evolution of hacking, 4
footprinting, 107
mobile device security issues, 447
preventing threats, 294–296
using SSL to exchange data over, 93–94
Internet Control Message Protocol. See ICMP (Internet Control Message Protocol)
Internet Information Server. See IIS (Internet Information Server)
Internet Message Access Protocol (IMAP), 259
Internet Protocol security. See IPsec (Internet Protocol security)
Internet Protocol v6 (IPv6), 273
Internet Relay Chat (IRC), spyware delivery, 236
intrusion detection system. See IDS (intrusion detection system)
intrusion prevention system. See IPS (intrusion prevention system)
intrusions
  signs of, 465–466
testing web applications with Burp Suite, 383
investigation phase, incident response, 23
investments, researching, 117
IP address(es)
  defying detection by firewall, 478–479
  DNS and, 53
  finding website, 104–105
  importance of, 53
  looking for live hosts via ping sweeps, 134
  at Network layer of OSI model, 45
  routers and, 54
  smurf attack spoofing, 310
  using Ping via, 133
IP fragmentation, web server/application vulnerability, 372
IP ID (identification number), idle scans, 142–143
IP spoofing
defying detection by firewall, 477
leading to prison time, 346
overview of, 341–342
IP subsetting, 49
IP Tool, pentesting Android, 450
iPlanet Web Server, Oracle, 367
IPS (intrusion prevention system)
detecting/preventing network anomalies, 353
IDS vs., 465
overview of, 57
IPsec (Internet Protocol security)
as cryptographic technology, 90
defending against session hijacking, 352
hardening network against sniffing, 273
working with, 90–92
IPv6 (Internet Protocol v6), 273
IRC (Internet Relay Chat), spyware delivery, 236
iris recognition, biometrics, 516
IRPs (incident response policies)
in incident response plans, 25
overview of, 22
reporting security incident via, 32
ISM (industrial, scientific, and medical) band, 414
ISN (initial sequence number), 343
isolation
  Apple iOS, 446
  mobile device security via, 442
ISPs (Internet Service Providers), 54
IT audits, by ethical hackers, 15
IVs (initialization vectors), 419–420

J
jailbreaking, 446–447
jamming attacks, on Wi-Fi, 428
JavaScript, in XSSs, 339–340
Jerusalem virus, 230
JiWire, wireless traffic analysis, 429
job site/postings, footprinting process, 116–117
John the Ripper tool, 571
Jolt2, DoS tool, 319
JPS Virus Maker, 233–234
Juniper device, mitigating MAC flooding, 274
JXplorer, searching LDAP directory, 183

K

Kali Linux
  breaking WEP with, 420–422
  cracking WPA with, 423
  testing with, 63
  using Firewalk script with, 472
KDC (key distribution center), Kerberos, 211–212
Kerberos, 211–274
key pair, CA generating, 85
keyboard dynamics, biometrics, 516
KeyGrabber tool, 574
keyloggers
  active online attacks via, 202
  executing applications via, 214
  malware programs installing, 225
  planting in post-exploitation phase, 561
  types of keystroke recorders, 248
keys
  asymmetric algorithm, 80–86
  cryptosystem, 76
  how cryptography works, 77
  symmetric algorithm, 78–79
KisMAC, 426
Kismet
  pentesting mobile devices, 449
  tool for lab testing, 572
  wardriving with, 426
  wireless traffic analysis, 430
known plaintext attacks, on cryptographic systems, 89

L

L0phtCrack tool, passwords, 571
lab, building
  build process, 566–567
  creating test setup, 568–569
  enumeration tools, 571
  evaluating tools for, 566
  hardware tools, 573–574
  installation process, 569
  installing tools, 570
  installing virtualized OS, 570
  logging/event-viewing tools, 572
  password-cracking tools, 571
  reasons for, 566
  scanner tools, 570–571
  sniffers, 572
  what you will need, 567–568
  wireless tools, 572
Lacroix, Cameron, hacker, 5
laminated windows, 517
Lan Manager (LM) hash, storing information in SAM, 167, 209–210
LAN Turtle tool, 573
land attack, as DoS attack, 310
LanDroid, pentesting Android, 450
LAN-to-LAN wireless networks, 412
large-storage-capacity hard drives, securing, 506–507
last-in, first-out (LIFO) access, 314
launch, of virus, 229
law enforcement, reporting security incident to, 32
lawful interception (LI), or wiretapping, 258
layers, web application, 366–367
LDAP (Lightweight Directory Access Protocol), 170, 182–183
LEAP (Lightweight Extensible Authentication Protocol), wireless authentication, 418
least privilege
  mobile device security via isolation, 442
  thwarting SQL injection, 404–405
legal issues
  creating/using malware, 225–226
  with data, 507
  getting advice of lawyers on, 17
  laws, regulations and directives, 33–34
  permission from client to perform enumeration, 162
  purchasing lock-picking tools, 515
  sniffing, 258
  of social engineering, 286
legally permissible rule of evidence, 31
Let Me Rule, Trojan-creation tool, 243
LexisNexis, for competitive analysis data, 117
LFM (log file monitor) IDS, 463
LI (lawful interception), or wiretapping, 258
LIFO (last-in, first-out) access, 314
Lightweight Directory Access Protocol (LDAP), 170, 182–183
Lightweight Extensible Authentication Protocol (LEAP), wireless authentication, 418
limited discoverable mode, Bluetooth, 432
Link Extractor, 111
LinkedIn, 114, 297
Linux OS
   Android based on, 443
   banner grabbing tools, 150–151
   finding MAC address, 55
   macof MAC flood attacks, 270
   packet sniffing with tcpdump, 264–266
   passive fingerprinting of, 148–149
   using Kali Linux, 63
   vulnerabilities of, 62–63
   wireless penetration tools, 431
Linux OS enumeration
   commonly exploited services, 170–172
   DNS zone transfers, 174–176
   finger command, 178
   NULL sessions, 173–174
   services/ports of interest, 169–170
   SuperScan, 174
   Unix and, 180–182
   users, 168–169
live systems, checking for
   in targeted environment, 130–131
   using hping3, 134–135
   using ping, 133–134
   using wardialing, 131–132
LM (Lan Manager) hash, storing information in SAM, 167, 209–210
LNS tool, finding ADS streamed files, 217
LoadStorm, testing security in cloud, 496
local service account, in Windows, 164
location, footprinting data on, 112–113
lock screens, physical security via, 504
locks, securing physical area, 513–515, 519
log file monitor (LFM) IDS, 463
log file readers, pentesting Android, 453
logging tools, lab testing, 572
logic bombs, 230, 231
logic function, web applications, 369
Logic layer, web applications, 366
logon
   physical security via, 503
   web server/application attacks from insecure, 368, 377–378
logout
web application, 369
web server/application session management, 379
LOIC (Low Orbit Ion Cannon)
in action, 320–322
creating botnets, 318
DDoS tool, 320
pentesting Android, 451
Loki, exploiting covert channels, 247
long-lived sessions, web servers/applications, 379
low-interaction honeypots, 474
LulzSec, 8

M

MAC (media access control) address, 54–56
MAC flooding, 270–271, 274–275
Mac OS, vulnerabilities of, 61–62
MAC spoofing, 272, 427
macof MAC flood, Linux, 270
macro viruses, 230–231
maintenance, thwarting SQL injection, 404
malicious activity
   1980s hackers engage in, 4
   abusing cloud services via, 491
   current developments in hacking/cybercrime, 4–5
   ethical hackers using same tactics as, 13
   malicious code, as cybercrime, 7
Maltego, 116, 151
malware
   adware, 237
categories of, 227–228
executing applications via, 214
mobile device countermeasures, 455
mobile device security issues, 442–443, 447
overt and covert channels used by, 247–249
overview of, 224–226
ransomware, 238
removing in mopping up phase of pen testing, 563
review, 249–250
review answers, 533–534
review questions, 251–253
scareware, 237
social engineering via Trojans, 293
spyware, 236–237
strict laws against, 226–227
Trojans. See Trojans
viruses. See viruses
worms, 234–236
Management Information Base (MIB), 178–180
man-in-the-browser attacks, 338–339
man-in-the-middle attacks. See MitM (man-in-the-middle) attacks
mantraps, securing physical area, 511–513
manual penetration testing, 561–562
mapping networks, 152–153
Marshmellow, Android OS, 442, 505
master boot record (MBR), boot-sector viruses infecting, 230
master computer (handler), DDoS attacks, 318–319
Matchstick Men movie, social engineering in, 285
MBR (master boot record), boot-sector viruses infecting, 230
McKinnon, Gary, 5
MD2 (Message Digest 2), hashing algorithm, 87
MD4 (Message Digest 4), hashing algorithm, 87
MD5 (Message Digest 5), hashing algorithm, 87
MD6 (Message Digest 6) hashing algorithm, 87
measured service, cloud computing, 487
mechanical locks, physical access control, 513
Medusa, password-cracking tool, 571
Melissa virus, 5, 231
membership registration sites, databases in, 395
memory, buffer overflow attacks on, 314–317
mesh topology, 42–43
<META> tag, code injection attacks, 341
metadata, 364–365
metamorphic viruses, 230
MIB (Management Information Base), 178–180
MicroSD cards, mobile device encryption, 505
Microsoft Hyper-V, building lab with, 569
Microsoft Proxy Server firewall, 470
Microsoft Windows OS
Apple devices not playing well in, 62
common vulnerabilities of, 60–61
finding MAC address, 55
Microsoft Windows OS enumeration
commonly exploited services, 170–172
DNS zone transfers, 174–176
groups, 164–165
NULL sessions, 173–174
overview of, 163
PsTools suite, 177
security identifiers, 166–167
services and ports of interest, 169–170
storing information in SAM file, 167
SuperScan, 174
users, 163–164
Minipwner tool, 573
misconfiguration
attacks on web servers/applications, 375
on Wi-Fi, 428
MitM (man-in-the-middle) attacks
application-level hijacking via, 341
on cryptographic systems, 89
in exploitation phase, 560
as passive online attacks, 200–201
pentesting mobile devices via, 450
performing, 347–351
as session hijacks, 346
TCP packet sequence numbers in, 47–48
Mitnick, Kevin, 346
mnemonics, OSI layers, 46
mobile apps, 363–364
mobile device security
Android OS, 443–446
Apple iOS, 446–447
approaches to, 442–443
countermeasures, 454–455
cryptography in, 75
firewalls for, 473
goals of, 441–442
OS models and architectures, 440–441
overview of, 440
pentetration testing, 449–450
pentetration testing using Android, 450–454
physical theft, 505–506
problems, 447–449
review, 435–436
review answers, 544
review questions, 457–460
use of locks, 519
modems, 131–132
modules, Apache web server/IIS, 363
monitoring, session hijacking process, 334
mopping up phase, penetration testing, 563
moral obligation, social engineers prey on victim's, 283
Morris, Robert T., Jr., as first hacker, 4–5
MSN Sniffer, 260
multifactor authentication, 198
multihomed firewall configuration, 468
multipartite (or file) viruses, 230, 232
multiple access points, wireless networks, 412, 429–430
multi-tenant environments, threats to cloud security, 491
Myspace, people search utility, 297

N

NAT (Network Address Translation), routers using, 54
nature, securing physical area, 509
NBNS (NetBIOS Name Service), 170
nbstat command, 171–172
NBTScan, for lab testing, 571
Nessus Vulnerability Scanner, 130, 380
NetBIOS, 171, 174
NetBIOS Name Service (NBNS), 170
NetBIOS Session Service (SMB over NetBIOS), port for, 170
Netcat
  for Android, 451
  enumeration tool for lab testing, 571
  planting backdoors, 215
  port redirection, 248–249
  providing information about web server, 374
Netcraft
  banner grabbing with, 150
  finding information about URLs, 111
  providing information about web server, 374
NETGEAR device, mitigating MAC flooding, 274–275
NetScan tools, 571
NetScanTools Pro, 186
netstat, detecting open ports, 241
NetStumbler, 426, 572
NetWitness NextGen, sniffer, 260
Network Address Translation (NAT), routers using, 54
network cards, 411
Network Discovery tool, pentesting Android, 450
Network group, Windows, 165
Network Handbook, pentesting Android, 450
network interface cards (NICs), 54
network intrusion detection system. See NIDS (network intrusion detection system)
Network layer, OSI model
  IP subnetting, 49
  overview of, 45

routers at, 54
  session hijacking at, 334
network mappers, 152–153
Network News Transfer Protocol (NNTP), 258
network scans, 129
network security, 58–59
network service account, Windows, 164
network session hijacking, 344
network sniffing, against cloud, 494
Network Time Protocol (NTP), and enumeration, 184
network topologies
  bus, 40–41
  hybrid, 42–43
  mesh, 42–43
  overview of, 40
  ring, 41
  star, 42
networking tools, pentesting tools for Android, 450–451
NetworkMiner, lab testing tool, 572
networks
  administrator interaction with web servers, 360
  attacks caused by footprinting, 107
  attacks on mobile devices, 441
  defending against session hijacking, 352
  DoS attacks against specific, 308
  firewalls, 56–59
  information gathering on, 104–105, 119–120, 558
  intrusions, 6, 466
  proxies, 56
  routers and switches, 53–56
Nexpose, 130, 496
NICs (network interface cards), 54
NIDS (network intrusion detection system)
  detecting sniffing attacks, 275
  overview of, 463
  targeting with DoS attack, 475
NirSoft Suite, 571
Nmap
  defying detection by firewall, 478
  defying detection by IDS, 476
  detecting Trojans and viruses, 240–241
  determining firewall configuration, 472–473
  FIN scan with, 141
  fragmenting packets, 144
  how it works, 141
  importance in CEH exam, 133–134
NULL scan with, 141
OS detection with, 146–147
pinging with, 133
port scanning with, 129
providing information about web server, 374
as scanner for lab testing, 570
stealth or half-open scan with, 139
as vulnerability scanner, 152
Xmas tree scan with, 140
NNTP (Network News Transfer Protocol), 258
nondiscordable mode, Bluetooth, 432
nonpairing mode, Bluetooth, 432
nonrepudiation
cryptography in, 76
symmetric cryptography lacking, 78
non-repudiation, supporting CIA triad, 16–17
nontechnical (or non-electronic) attacks
password cracking, 199
social engineering, 282
NOP sled, buffer overflow attack, 317
nslookup command, DNS, 119–120, 175–176
NT LAN Manager (NTLM), 167, 209–210
NTFS volumes, 217
NTLM (NT LAN Manager), 167, 209–210
Ntop tool, 572
NTP (Network Time Protocol), in enumeration, 184
NULL scan, 141–142
NULL sessions, exploiting, 173–174
numbers
decoding SID, 166–167
TCP packet sequence, 47–48
TCP/IP port, 50–52
password cracking via, 199
precomputed hashes/rainbow tables, 203–205
on WPA/WPA2, 424
OIDs (object identifiers), recognizing MIB elements, 179
omnidirectional antennas, 415
OmniPeek, sniffer, 259
on-demand self-service, cloud computing, 486
OneDrive, cloud computing, 487
one-way hash function, 81–82
online habits, changing, 295
Open Signal tool, wireless traffic analysis, 429–430
open source
information gathering via footprinting, 106
Linux OS, 63
Open Web Application Security Project (OWASP), 380, 448
open-source intelligence (OSINT), 558
OpenSSL, web application encryption, 380
open-system authentication, Wi-Fi, 416
operating systems. See OSs (operating systems)
OphCrack tool, 571
opinion evidence, defined, 30
OPM (Office of Personal Management), threats to cloud security, 490
Oracle VM VirtualBox, building lab, 569
Orbot, pentesting Android, 454
order by statement, in SQL injection attack, 398
organization data, in footprinting, 105–106
Orweb, pentesting Android, 454
OS fingerprinting
active, 146–147
overview of, 145–146
passive, 147–149
OS X, Apple iOS based on, 446
OSI (Open Systems Interconnection) model
attacks caused by footprinting, 107
overview of, 44–46
session hijacking in, 334
TCP/IP suite mapping to, 47–48
OSINT (open-source intelligence), 558
OSs (operating systems)
Android, 62, 444
Apple iOS. See Apple iOS
choosing for test setup, 568
finding information in footprinting, 105
Linux, 62–63
Mac OS, 61–62
Microsoft Windows, 60–61

Obfuscated code, evading detection via, 404, 476
object identifiers (OIDs), recognizing MIB elements, 179
object identifiers, recognizing MIB elements, 179
objective, pre-engagement interactions, 553–554
object-oriented programming databases, 395
Office 365, cloud computing for, 487
Office of Personal Management (OPM), threats to cloud security, 490
offline attacks
e xtracting hashes from system, 203
overview of, 203
output, reading sniffer, 266–270
outside attacks, pre-engagement interactions, 555
overt channels, 239
OWASP (Open Web Application Security Project), 380, 448

P
p0f tool, Linux, 148–150
P2P (Peer-to-Peer Networks), spyware delivery via, 236
PaaS (Platform as a Service), cloud, 366, 489
Packet Capture tool, pentesting Android, 450
packet capture, with sniffers. See sniffers
packet crafters, 137
Packet Generator, pentesting Android, 451
packet sequencing, implementing TCP hijacking, 344–345
packet sniffing, 199–200
packet-filtering firewalls, 57, 469
PacketShark, pentesting Android, 451
Padding Oracle On Downgraded Legacy Encryption (POODLE) attack, 381
PageXchanger for IIS, 151
pairing mode, Bluetooth, 432
palm scan systems, biometrics, 516
Parabolic Antenna tool, lab testing, 574
parabolic grid antennas, 415–416
Paranoid Android, 446
parties involved, pre-engagement interactions, 553–554
passive fingerprinting, OSs, 146–147
passive information gathering, footprinting, 106
passive online attacks
man-in-the middle, 200–201
overview of, 199
packet sniffing, 199–200
password cracking, 198
replay attack, 201–202
passive session hijacking attack, 335–336
passive snifing, 256
passive wireless network attacks, 425
passphrases, identity theft protection, 297
passwd file, Linux, 168
password cracking
as active online attack, 202–203
of cloud services, 491
of database server, 396
in distributed network attack, 205–206
in exploitation phase, 560
as offline attack, 203–205
as passive online attack, 199–202
performing, 377–378
risk mitigation for WEP/WPA, 425
techniques, 198–199
understanding, 196–198
password guessing
as active online attack, 202
obtaining password via, 207
password-cracking backdoors, 247
password-protected screensavers, 504
passwords
adding additional security measures to, 504
avoid saving of, 296
biometric authentication replacing, 515
capturing in post-exploitation phase, 561
cybercrime of stealing, 6
Linux user account, 168
mobile device countermeasures, 454–455
mobile device security issues, 447
in multifactor authentication, 198
physical security via, 503
SNMP, 179
social networking and, 289
social networking countermeasures, 292–293
storing information in SAM, 167
as vulnerability in Windows, 61
web server/application issues, 377–378, 379
working with, 503
patches
creating test setup, 568
installing for lab testing, 569
mobile device security issues, 447
as vulnerability in Windows, 60
Path attribute, cookies, 380
Patriot Act, malware and, 226–227
pattern matching, IDS signature detection, 464
PBXs (private branch exchanges), wardialing, 132
PDF printer, for lab testing, 569
PDF viewer, for lab testing, 569
PDQ Deploy, planting backdoors, 214
peer CA, 85
penetration (pen) testing
alternative methods of testing, 550–552
Android OS, 450–454
automated vs. manual, 561–562
building lab for. See lab, building
contact contents for, 555–556
evaluating necessity of, 19–20
evasion, 479–480
exploitation, 560
footprinting phase, 100–101
frameworks, 549
gaining permission, 556
IDS, 480
intelligence gathering, 557–558
of mobile devices, 449–454
mopping up, 563
Penetration Testing Execution Standard, 552–553
permissions/contracts before, 13
post-exploitation, 560–562
pre-engagement interactions, 553–555
reporting, 562–563
review, 563–564
security in cloud, 495–496
tests within, 20–21
threat modeling, 558–559
vulnerability analysis, 559–560
web applications, 383–384
penetration testers
ethical hackers as, 2, 12–17
prerequisites for, 10
role of, 19–21
Penetration Testing Execution Standard. See PTES
(Penetration Testing Execution Standard).
People Search, 297
people search utilities, 113
Performance Insight, detecting sniffing attacks, 275
perimeter, building physical defense, 520
permanent DoS attack, 310
permissions
black hats functioning without, 11
ethical hacker responsibility for, 9–10
Linux group, 169
mobile device access control via, 443
before starting testing activity, 13, 556–557
web applications, 369
white hats functioning with, 11
personally identifiable information. See PII
(personally identifiable information)
personally owned devices, in workplace, 440–441, 448–449
PGP (Pretty Good Privacy), 79, 92–93
phases, social engineering, 285
Phatbot, Trojan-creation tool, 243
phishing, social engineering, 120–121, 293–294
phlashing, permanent DoS, 310
phone taps, firewalls acting as, 467
PhoneSweep wardialing program, NIKSUN, 132
physical access, spyware delivery via, 236
Physical layer, OSI model, 45
physical security
biometrics, 515–516
contactless cards, 515
data storage, 506–509
defense in depth, 519–520
doors and mantraps, 511–513
education and awareness, 519
entryways, 517–518
fences, 511
gates, 511
locks, 513–515
mobile device issues, 505–506
other items to consider, 519
overview of, 502
physical penetration test of, 554
review, 520–521
review answers, 547–548
review questions, 522–524
securing physical area, 510
server rooms and networks, 518
simple controls, 503–505
walls, ceilings, and floors, 516–517
windows, 517
picks, lock, 514
PII (personally identifiable information)
footprinting causing threats to, 107
preventing, 393
preventing threats when posting, 296
SQL injection attacks stealing, 391
PIN code problem, WPS, 422–423
pin-and-tumbler locks, physical access control, 513
ping of death, as DoS attack, 309–310
ping utility
checking for live systems via, 133–134
checking for live systems via hping, 134–135
gaining information about target’s network, 119
ping sweeps, 134
pivot points, wardialing, 132
PKI (public key infrastructure), 83–86
plain text/clear text
in asymmetric algorithms, 80
how cryptography works, 77
PKI system, 83–85
plaintext attacks – PsTools suite

in symmetric algorithms, 77
understanding hashing, 86–88
plaintext attacks, WEP vulnerability, 419
plans, incident response, 25–26
planting backdoors, 18
Platform as a Service (PaaS), cloud, 366, 489
PlugBot, creating botnets, 318
points of failure, disaster and recovery plans, 29
Poison Ivy, creating botnets, 318
poison null byte attacks, scripting errors, 378
policies
BYOD, 448
capturing settings in enumeration phase for, 163
firewall configuration via security, 467
hardening network against sniffing, 273
incident response. See IRPs (incident response
policies)
lack of social engineering security, 283
strong password, 503
PoliteMail tool, 117
polycarbonate acrylic windows, 517
polymorphic viruses, debut of, 230
POODLE (Padding Oracle On Downgraded
Legacy Encryption) attack, 381
poorly written/questionable scripts, causing
attacks, 378
POP (Post Office Protocol), sniffing of, 258
pop action, program stack, 314–315
pop-up blockers, social engineering prevention,
294
port mirroring, sniffing switched networks,
272–273
Port Scanner, pentesting Android, 450
port scanning
checking status of ports, 135–137
detecting Trojans and viruses, 240–241
determining type/brand of firewalls, 470
overview of, 129
portables, securing, 519
portals, as mantraps, 513
ports
checking status of, 135–137
hardening network by securing, 273
knowing for exam, 169–170
redirecting, 248–249
TCP/IP, 50–53
tracking usage with TCPView, 242–243
using Firewalk, 471
using netstat to detect open, 241
positive pressure, server rooms, 518
post exploitation, pentesting mobile devices, 450
Post Office Protocol (POP), sniffing of, 258
Poulsen, Kevin Lee (Dark Dante), hacker, 5
power outages
mesh topology and, 42–43
star topology and, 42
preinstalled applications, Android OS, 445
Presentation layer, OSI model, 46, 366
preservation rule of evidence, 31
Pretty Good Privacy (PGP), 79, 92–93
primary (default) groups, Linux, 169
printers, physical protection of, 519
privacy
Code of Ethics for, 11
ethical hacker responsibility for, 10
footprinting causing loss of, 107
with SNMPv3, 178
social engineering impacting loss of, 285
social networking countermeasures, 293
private branch exchanges (PBXs), wardialing, 132
private browsing, preventing threats, 295
private cloud, 488
private keys, 80–86, 93
privilege escalation, on Microsoft platforms,
211–212
processes, running Windows, 164
process-hiding backdoor, 247
promiscuous client attacks, Wi-Fi, 428
promiscuous mode, detecting sniffing
attacks, 275
proper identification rule of evidence, 31
protocol anomaly detection, IDS, 465
protocol listeners, IIS, 363
protocols, subject to sniffing, 258–259
proxies
overview of, 56
pentesting tools for Android OS, 453
providing anonymity for scanning party,
153–154
setting up web browser to use, 154–155
testing web applications with Burp Suite,
383
proxy Trojans, 240
proxy-based firewalls, 469
pseudonymous footprinting, 106–107
PSH flag, 137, 139–140
Psiphon, pentesting Android, 453
pspv.exe tool, 208
PsTools suite, planting backdoors, 214
PTES (Penetration Testing Execution Standard).
contents of contract, 555–556
 gaining permission, 556–557
 intelligence gathering, 557–558
 pre-engagement interactions, 553
 seven stages of, 552–553
 threat modeling, 558–559
 working with, 553
 public cloud, 488
 public information, intelligence gathering for, 558
 public key infrastructure (PKI), 83–86
 public keys
   in asymmetric cryptography, 80–86
   CA publication of, 85
   Pretty Good Privacy using, 92–93
 public places, access to sensitive information in, 295
 public profiles, avoiding on social networks, 293
 public websites, in footprinting process, 111–112
 push action, program stack, 314–315
 push messaging, Android OS, 445
 pwdump command, extracting hashes, 203
 Pwn Pad, 430, 573
 Pwn Phone, 430, 573
 Pwnie Express, 430

R

RA (Registration Authority), CA as, 85
rack-mounted servers, server rooms, 518
radio frequency ID (RFID), physical access
control, 515
RADIUS (Remote Authentication Dial-In User
Service), 417–418
rainbow table attacks, 203–205
RainbowCrack, 571
RAM, creating test setup, 568
range
   extending Bluetooth device, 432
   wireless networks and, 411
ransomware, 7, 238
rapid elasticity, in cloud computing, 487
Raspberry Pi, 427, 573
RATs (Remote Access Trojans), 240
RC2 symmetric algorithm, 79
RC4 symmetric algorithm, 79
RC5 symmetric algorithm, 79
RC6 symmetric algorithm, 79
RCPT TO command, SMTP enumeration, 186
reaper virus, 228
Reaver, tool for lab testing, 572
receptionists, as targets of social engineers, 286
reconnaissance, ethical hacking. See footprinting
records (rows), database, 395
recovery
   DRP. See disaster recovery plan (DRP)
   as incident response phase, 24
   RECUB (Remote Encrypted Callback Unix
   Backdoor), Trojan-creation tool, 243
   red team, pentester, 557
   redirects, web server/application attacks from
   unvalidated, 376–377
   redundancy
     disaster and recovery plans for, 28–29
     mesh topology providing high, 42–43
     ring topology providing, 42
reflected XSS attacks, 340
registered ports, 51–52
Registration Authority (RA), CA as, 85
relational databases, 395
Relay service, SMTP, 186
relevance rule of evidence, 31
reliability rule of evidence, 31
religious law, ethics and, 33
Remote Access Trojans (RATs), 240
Remote Authentication Dial-In User Service
(RADIUS), 417–418
Remote Encrypted Callback Unix Backdoor
(RECUB), Trojan-creation tool, 243
Remote Procedure Call (RPC), TCP 135 port, 169
remote wiping, 449, 455
RemoteExec, planting backdoors, 214
repair phase, incident response, 24
replay attack, 201–202
replication, 229
reporting
  in penetration testing, 562–563
  as responsibility of ethical hacker, 14
  security incident, 32
reputation filtering, protection from botnets, 324
researching, viruses, 233–234
resource pooling, cloud computing, 487
response phase, incident response, 23
responsibilities, ethical hacker, 9–10
Restorator, distributing Trojans, 246
Restricted group, Windows, 165
restricted websites, footprinting, 111–112
retina pattern systems, biometrics, 516
revenue, footprinting and loss of, 107
reversal testing, 552
reverse proxy, protecting from DoS/DDoS attacks, 323
reverse SSH tunneling, breaching wireless networks, 427
Reverse World Wide Web (WWW) Tunneling Shell, 248
RFC 3704 filtering, protecting from botnets, 323
RFID (radio frequency ID), physical access control, 515
rights, Linux group, 168
Rijndael, 79
ring topologies, 41
RIP (Routing Information Protocol), 45
RIPE-MD, hashing algorithm, 87
risk
cloud controls managing, 495
contract content stating perceived, 555
increased wireless network, 410
mobile device security, 440–441
reporting security incident, 32
rlogin keystrokes, Telnet, 258
rogue access point attacks, Wi-Fi, 426–427
root CA, 85
root directory, directory traversal attacks, 382
rooting device, Android, 444
rootkits, 227
Rosetta stone, 74
router throttling, protecting from DoS/DDoS, 323
routers
  evading with fragmenting, 144
  firewalls acting as, 467
  firewalls working in conjunction with, 468
  overview of, 53–54
Routing Information Protocol (RIP), 45
rows (records), database, 395
RPC (Remote Procedure Call), TCP 135 port, 169
rpcinfo command, Linux/Unix, 181
RST flag
  ACK scanning and, 143
  defined, 137
  defying detection by IDS with, 477
  full-open scans, 138
  idle scans, 142–143
  stealth or half-open scans, 138–139
rule-based attacks, password cracking via, 198
rules
  of engagement, 13–14, 558
  of evidence, 31
  firewall, 467
for strong passwords, 197–198
runtime, Android application, 444–445

S
SaaS (Software as a Service), cloud, 366, 488–489
SAM (Security Accounts Manager)
  authentication on Microsoft platforms, 209–210
  how passwords are stored within, 209–210
  user and group information stored in, 167
  sample scripts, and scripting errors, 378
  sandboxing, access control via, 444
  SandroProxy, pentesting Android, 453
  sanitation methods, 508, 509
  SAPs (software access points), 411–412
  Saran Wrap, Trojans, 246
  Sarbanes–Oxley Act (SOX or SarBox), 2002, 34
  satellites, footprinting location data, 112
save capture function, sniffers
  overview of, 257–258
  reading captured output, 267–270
  Wireshark, 262
scalar objects, MIB, 179
scale, DoS attacks vs. DDoS attacks, 317–318
scans, social media, 290–291
scanner, testing web applications with Burp Suite, 383
scanners, lab testing tools, 570–571
scanning
  ACK scans, 143–144
  banner grabbing, 149–151
  checking for live systems, 130–135
  checking status of ports, 135–137
  ethical hacking and, 101
  FIN scans, 137–138
  full-open scans, 135
  idle scans, 142–143
  network mapping, 152–153
  NULL scans, 141–142
  OS fingerprinting, 145–149
  pentesting mobile devices, 449
  pentesting tools for Android, 452–453
  review, 155
  review answers, 530–531
  review questions, 156–158
  as second phase of ethical hacking, 17
stealth or half-open scans, 135–136
techniques used in, 161
types of, 129–130
types of information learned by, 130
UDP scans, 144–145
understanding, 128–129
using proxies, 153–155
in vulnerability analysis phase, 559
vulnerability scanners, 129–130, 151–152
when scan is blocked, 144
Xmas tree scans, 136–137

scareware, 237, 284
Schneier, Bruce, 79
scope, pre-engagement interactions, 553
screened subnet, firewall configuration, 468
screensavers, physical security, 504
script kiddies, 9
scripting errors, in attacks on web servers/
applications, 378
search engines, in footprinting, 108–111
SEC (Securities and Exchange Commission), 117
secondary evidence, 30
secondary groups, Linux, 169
secrecy, in cryptography, 75
sector-specific data, intelligence gathering for, 558
Secure attribute, cookies, 379
Secure Hash Algorithm-0 (SHA-0), 87
Secure Hash Algorithm-1 (SHA-1), 87
Secure Hash Algorithm-2 (SHA-2), 87
Secure Shell (SSH), hardening network, 273
Secure Sockets Layer. See SSL (Secure Sockets Layer)

Securities and Exchange Commission (SEC), 117
security
cryptography. See cryptography
early Internet not designed for, 4
footprinting. See footprinting
network, 58–59
in pentesting, 13
preserving CIA triad when planning, 16
of private cloud, 488
vs. convenience analysis, 14
security film windows, 517
security identifiers (SIDs), 166–167
security policies, and social engineering, 283
security software disablers, Trojans as, 240
Self group, Windows, 165
SENA adapter, in test setup, 568
Senna spy, Trojan construction kit, 246
sequencer, Burp Suite, 383

SERP (search engine results page), footprinting, 108
server administrators, and web servers, 360
Server Mask, countering banner grabbing, 151
server rooms and networks, securing, 318
server validation, 425
server-side technologies
SQL injection and, 394
understanding web applications, 365
Service group, Windows, 165
service hijacking, against cloud, 490, 494
service packs, Windows vulnerability, 60
service providers
planning for disaster and recovery, 28
as threat to cloud security, 491
service request flood, as DoS attack, 308
service set identifier. See SSID (service set identifier)

service-level agreements (SLAs), 27, 29

services
commonly exploited, 170–171
and ports of interest, 169–170
protecting from DoS/DDoS attacks by
degradation, 323
protecting from DoS/DDoS attacks by
disabling, 323

session desynchronization, session hijacking, 334

session fixation attack, 341

session hijacking
active and passive attacks, 335–336
defensive strategies, 352–353
DNS spoofing, 351–352
in exploitation phase, 560
key concepts, 341–343
man-in-the-middle attack, 346–351
network, 344–346
overview of, 332
pentesting tools for Android, 451
review, 353–354
review answers, 539–540
review questions, 355–358
in session fixation attack, 341
spoofing vs. hijacking, 334
TCP packet sequence numbers in, 47–48
types of application-level, 337–341
UDP, 352
understanding, 332–334
web apps and, 336–337
session ID prediction, session hijacking, 334
session IDs
  session hijacking at application level, 336–337
  session management issues, 379
  types of session hijacking, 333
  understanding, 334
Session layer, OSI model, 46
session management, web servers and
  applications, 378–379
session riding (or CSRF), against cloud, 491–492
session sniffing, 337
session splicing, 476
session tokens, 334, 338
session tracking, web applications, 369
SETI (Search for Extraterrestrial Intelligence)
  project, 206
SETI@home project, 206
SFind tool, 217
SHA-0 (Secure Hash Algorithm-0), 87
SHA-1 (Secure Hash Algorithm-1), 87
SHA-2 (Secure Hash Algorithm-2), 87
shared key authentication, Wi-Fi, 416–417
SharesFinder, pentesting Android, 451
Shark, creating botnets, 318
Shark for Root, pentesting Android, 451
sheep-dip system, researching viruses, 233–234
shell viruses, 232
Shodan search engine, 297, 374
Short Message Service (SMS), pentesting mobile
devices, 450
shoulder surfing, 121, 293
showmount command, Linux/Unix, 181
shredding, physical security via, 508
side channel attacks, on cloud, 492–493
SIDs (security identifiers), 166–167
signature wrapping attacks, on cloud, 493
signature-based IDS, 464
Simple Mail Transfer Protocol. See SMTP (Simple
  Mail Transfer Protocol)
Simple Network Management Protocol. See SNMP
  (Simple Network Management Protocol)
Simple Object Access Protocol (SOAP), 493, 494
site survey tools, wireless networks, 426
Skyhook, wireless traffic analysis, 429
Slammer worm, SQL, 234–235
SLAs (service-level agreements), 27, 29
slaves (zombies), DDoS attack setup, 318–319
SlimROM, Android, 445
smart cards, supplementing passwords, 504
smartphones
  Android OS. See Android OS
  Apple iOS. See Apple iOS
bring your own device issues, 448–449
hacking with Pwn Phone, 430
smashing stack, buffer overflow attacks, 315–316
SMB over NetBIOS (NetBIOS Session Service),
  port for, 170
SMB over TCP (or Direct Host), port for, 170
Smith, David L., hacker, 5
SMS (Short Message Service), pentesting mobile
devices, 450
SMTP (Simple Mail Transfer Protocol)
  easy sniffing of, 258
  enumeration with, 162, 184–186
  TCP 25 port for, 169
smurf attacks, 310
sniffers
  on the defensive, 273
detecting attacks, 275
  overview of, 256
in passive session hijacking attacks, 335
reading output, 266–270
review, 275–276
review answers, 534–536
review questions, 277–280
switched network, 270–275
tcpdump, 264–266
tools, 259–260, 572
understanding, 256–258
using, 259
Wireshark, 260–264
sniffing, session hijacking process, 334, 352
SNMP (Simple Network Management Protocol)
  enumeration with, 162, 178–179
  MIB used as codebook by, 179–180
  UDP 161 and 162 ports for, 170
SNScan, 180
SOAP (Simple Object Access Protocol), 493, 494
SOASTA CloudTest, 495–496
social engineering
  commonly employed threats, 293–296
  on cryptographic systems, 89
  as cybercrime, 6
  footprinting as, 107, 120–121
  identity theft as, 296–298
  impact of, 285–286
  on mobile devices, 442
  phases of, 285
  power of, 284
  pre-engagement interactions, 554
  review, 298–299
review answers, 536–537
review questions, 300–303
social networking as, 287–291
social networking countermeasures, 291–293
targets of, 286–287
understanding, 282–283
why it works, 283–284

social networking
  countermeasures for, 291–293
  in footprinting process, 113–116
  gathering information via, 287–291
  strengthening your accounts from, 289–291

software
  adware installed with, 237
  encryption weaknesses in web applications, 380
  gathering job posting data, 117
  malicious. See malware
  mobile device security issues, 447
  spyware installed with, 237
  tools for building lab, 570–571

Software as a Service (SaaS), cloud, 488–489
software piracy, as cybercrime, 7
software updates
  installing for lab testing, 569
  mobile device countermeasures, 455
solar film windows, 517
solid state drives (SSDs), problems with, 509
Sony Corporation, SQL injection attack on, 391
Source IP reputation filtering, protection from botnets, 324
source routing, 342
SPAN (Switched Port Analyzer) port, sniffing switched networks, 272–273
sparse-infector viruses, 231
spear phishing, 121
Spector Pro keylogger, 248
SPI (stateful packet inspection), in ACK scanning, 142–143
Spider tool, testing web applications, 383
Spikeo, people search utility, 113, 297
spoofing
  DNS, 343
  IP, 341–342
  MAC, 427
  pentesting mobile devices, 450
  vs. session hijacking, 334
spyware
  active online attacks via, 202
  defined, 227
  methods of infection, 236–237
SQL injection
  altering data with, 399–401
  anatomy of, 396–399
  blind, 401–402
  against cloud, 494
  countermeasures, 404–405
  database vulnerabilities, 394–396
  evading detection mechanisms, 403–404
  information from error messages and, 403
  information gathering and, 402–403
  introduction, 390–392
  lack of input validation allowing, 375
  overview of, 390
  pentesting tool for Android, 453
  prerequisites for, 390
  results of, 392–393
  review, 405
  review answers, 541–542
  review questions, 406–408
  web application anatomy and, 393–394

SQL Slammer worm, 234–235
SQLite Editor, pentesting Android, 453
sqlmapchik, pentesting Android, 453
SQLPing 3.0, 396
SQLRecon, 396
SSDs (solid state drives), problems with, 509
SSH (Secure Shell), hardening network, 273
SSID (service set identifier)
  access points broadcasting, 413
  changing default, 413
  open system authentication for Wi-Fi and, 416
  rogue access point attack on, 427
  wireless traffic analysis, 429–430
SSL (Secure Sockets Layer)
  defending against session hijacking, 352
  hardening network against sniffing, 273
  POODLE attack using, 381
  at Presentation layer of OSI model, 46
  securing information, 93–94
SSL Strip, 200–201, 451
Stacheldraht, DDoS tool, 320
stack
  buffer overflow attacks and, 314–315
  smashing, 315–316
  standard windows, 517
star topology, 42
stateful packet inspection (SPI), in ACK scanning, 142–143
SYN flag
- checking status of ports, 136–137
- passive fingerprinting of OS, 147–149
- performing idle scan, 142–143
SYN packet, TCP/IP suite, 47–48
SYN scan, 138–139
SYN sequence numbers, TCP/IP session hijacking, 344
SYN-ACK response
- passive fingerprinting of OS, 147–149
- performing idle scan, 142–143
- performing stealth or half-open scan, 138–139
SYN attack/floods exploiting, 309
TCP three-way handshake and, 47–48
Sysinternals Suite, for lab testing, 571
SYSKEY, improving security of SAM, 209
Syslog, pentesting Android, 453
system (boot-sector) viruses, 229, 230
system account, processes in Windows, 164
system administrators
- as targets of social engineers, 286
tendency to use backdoor accounts, 287
system fundamentals
- backup/archiving, 63–64
DNS, 53
- exam objectives, 39
hexadecimal vs. binary, 49–50
IP subnetting, 49
IPS and IDS, 57
network devices, 53–57
network security, 58–59
network topologies, 40–44
- operating systems, 60–63
OSI model, 44–46
review, 64–65
review answers, 527–528
review questions, 66–69
TCP/IP ports, 50–53
TCP/IP suite, 47–48
System group, Windows, 165
system hacking
- active online attacks, 202–203
authentication on Microsoft platforms, 209–213
covering tracks, 215–217
distributed network attacks, 205–206
executing applications, 213–214
in hacking process, 18
offline attacks, 203–205
options for obtaining passwords, 207–208

statefull firewalls
- multilayer inspection, 469
packet filtering, 57
- preventing port scans, 143
stateless, defined, 367
stealing session ID, in session hijacking, 333
stealth (half-open) scan, 135–136
Stealth Tool, hiding Trojans, 246
stolen equipment attack, 555
stolen session. See session hijacking
stored XSS attacks, 339–340
strong passwords
- physical security via, 503
- rules for, 197–198
Stunnel, 381
Stuxnet virus, 6, 45
subdomains
- defined, 111
- footprinting restricted websites, 111–112
- revealing with Netcraft tool, 111
subnetting, IP, 49
subordinate CA, 85
suicide hackers, 9
suites, pentesting Android, 454
SuperScan
- enumeration tool for lab testing, 571
- enumeration utilities of, 174
- scanner for lab testing, 570
Svechinskaya, Kristina Vladimirovna, 6
switched networks, sniffing
- ARP poisoning, 271–272
- MAC flooding, 270–271
- MAC spoofing, 272
- mitigating MAC flooding, 274–275
- port mirror or SPAN port, 272–273
Switched Port Analyzer (SPAN) port, sniffing
- switched networks, 272–273
switches
- broadcast domains/collision domains, 55–56
- nbstat, 171–172
- nmap, 141
- overview of, 54–55
tcpdump, 266
syllable attacks, password cracking via, 198
symbols, Egyptian hieroglyphic, 74–75
symmetric cryptography, 77–79
SYN attack/flood
- as DoS attack, 309
- performing, 311–314
- web servers/applications vulnerable to, 372
overview of, 194, 196
passive online attacks, 199–202
password cracking, 196–199, 208–209
as phase of ethical hacking, 102
planting backdoors, 214–215
previous phases of ethical hacking, 194–196
review, 217–218
review answers, 532–533
review questions, 219–221
system integrity verifier, 463
system knowledge, in contract content, 556
system weaknesses, penetration testing, 558
tcpdump, sniffer
defined, 259
packet sniffing in Linux, 264–266
sniffer tool for lab testing, 572
TCP/IP ports, 50–53
TCP/IP suite, 47–48, 333
TCPView, 242–243, 571
teams, incident response, 25
teardrop attack, as DoS attack, 310
technology
evolution of hacking in response to, 4
little impact on social engineering, 283
Teflon Oil Patch, distributing Trojans, 246
telephone calls, law enforcement and sniffing, 258
Telnet
banner grabbing with, 149–151
easy sniffing of, 258
enabling in modern Windows, 149
TCP 23 port for, 169
vulnerable to man-in-the-middle attack, 200
telnet command, SNMP enumeration, 185
tension wrenches, lock picking, 514
terminal Server User group, Windows, 165
terminology
footprinting, 106–107
wireless, 414
terrorism, and social engineering, 285
testing. See penetration (pen) testing
TFN2K, DDoS tool, 320
TGS (ticket-granting server), Kerberos, 211–212
TGT (ticket-granting ticket), Kerberos, 211–212
The Italian Job movie, social engineering in, 285
Onion Router (Tor), 154–155
theft of access, as cybercrime, 6
THE-SCAN wardialing program, 132
threats. See also vulnerabilities
Bluetooth, 432–433
BYOD, 448–449
caused by footprinting, 107
cloud security, 489–490, 491–493
defined, 13
mobile device, 441
modeling in penetration testing, 558–559
social engineering, 283, 293–294
web servers/applications. See web servers/
applications, common flaws/attack methods
Wi-Fi. See Wi-Fi, threats
three-way handshake, TCP, 47–48
thumbprint, as one-way hash value, 87
ticket-granting server (TGS), Kerberos, 211–212
ticket-granting ticket (TGT), Kerberos, 211–212
time to live values. See TTL (time to live) values
  in contract content, 555–556
  intelligence gathering for, 558
timeline of security incident, reporting, 32
timing, of penetration test, 555
TOE (target of evaluation), 13
tokens, supplementing passwords with, 504
ToneLoc wardialing program, 132
tools
  creating botnets, 318
  creating Trojans, 243–245
  DDoS, 320
  DoS, 319
  enumeration, 571
evaluating when building lab, 566
  exploiting covert channels, 247–248
  hardware, 573–574
  installing, 570
  lock-picking, 514–515
  logging/event-viewing, 572
  password-cracking, 571
  scanner, 570–571
  sniffer, 259–260, 572
  wireless, 572
topologies, network, 40–44
Tor (The Onion Router), 154–155
Tracert utility
  finding IP address for website, 104–105
  footprinting using, 103
  gaining information about target’s network, 120
traffic analysis, targeted Wi-Fi networks, 429–430
traffic filters, firewalls as, 468
traffic sniffing, 560
training
  as line of defense in security, 519
  in preventing social engineering, 292–293
  as social engineering countermeasure, 283–284
Transmission Control Protocol. See TCP
  (Transmission Control Protocol)
Transport layer, OSI model, 46
triage phase, incident response, 23
Trinoo, DDoS tool, 320
Triple DES (3DES) encryption, 78–79, 88
Tripwire, 217, 463
TRK (Trinity Rescue Kit), 213, 571
Trojan Construction Kit, 246
Trojan Man, 246
Trojans
  active online attacks via, 202
  backdoors, 246–247
  behaviors of, 238–239
  BO2K, 244–245
  construction kits, 246
defined, 227
detecting, 240–243
distributing, 245–247
social engineering via, 284, 293
  systems of behaviors, 238–239
tools for creating, 243–245
types of, 240
  unknowing victims of, 239–240
  using covert and overt channels, 239, 247
trust
  ethics and the law, 33
  social engineers preying on victim’s, 114, 283, 284
trusted root CA, 85
TTL (time to live) values
  determining firewall configuration with
    Firewalk, 470–471
  determining firewall configuration with
    Nmap, 472–473
  firewalking and, 470
  passive fingerprinting of OS, 147–149
Twitter
  gathering information using, 288–289
  social engineering via, 114
TwoFish symmetric algorithm, 79
  type mismatch, and error messages, 403

U

UAC (User Account Control), 60
Ubertooth One, for lab testing, 573
Ubuntu, overflowing CAM tables in, 271
UD100 Bluetooth adapter, extending range, 432
UDP (User Datagram Protocol)
  in fraggle attack, 310
  port numbers, 169–170
  in session hijacking, 352
  SNMP functioning with, 178
  at Transport layer of OSI model, 46
  UDP-based scans, 144–145
UDPFlood, DoS tool, 319
UID, Linux user account, 168
uniform resource identifier (URI), and web applications, 367
Universal Resource Locators. See URLs (Universal Resource Locators)
Unix OS enumeration, 180–182
unsafe site warning, heeding, 295
unvalidated redirects and forwards, attacks on web servers/applications, 376–377
updates
Android Updates, 445
lab testing, 569
mobile device, 447, 455
test setup, 568
as vulnerability in Windows, 60
upload bombing, from scripting errors, 378
UPnP Scanner, pentesting Android, 451
URG flag
defined, 137
marking data as urgent, 477
performing Xmas tree scan, 139–140
URI (uniform resource identifier), and web applications, 367
URLs (Universal Resource Locators)
defying detection by firewall using IP address instead of, 478–479
in directory traversal attacks, 382–383
footprinting, 110–111
session IDs embedded in, 336
U.S. Army, SQL injection attack on, 391
U.S. Communications Assistance for Law Enforcement Act, 1994, 34
U.S. Computer Fraud and Abuse Act, 34, 226
U.S. Electronic Communications Privacy Act, 1986, 34
U.S. Kennedy - Kassebaum Health Insurance and Portability Accountability Act (HIPAA), 1966, 34
U.S. Medical Computer Crime Act, 1984, 34
U.S. military files, 2002 hacking of, 5
U.S. National Information Infrastructure Protection Act, 1996, 34
U.S. Privacy Act, 1974, 34
USA Freedom Act, 227
USB (Universal Serial Bus)
password theft, 207–208
physical security of external drives, 506–507
USB Rubber Ducky
hardware tool for lab testing, 573
stealing passwords, 208
User Account Control (UAC), 60
User Datagram Protocol. See UDP (User Datagram Protocol)
user-installed applications, Android OS, 445
usernames
cybercrime of stealing, 6
Linux, 168
users
Android OS security for, 443–444
interaction with web servers, 360
Linux, 168–169
removing accounts in mopping up phase, 563
SQL injection attacks on current, 399
as targets of social engineers, 286
vs. administrative account, 60
Windows, 163–167

V

validation
of certificates by CAs, 85
input. See input validation
VBA (Visual Basic for Applications), macro viruses using, 230–231
Vega web application scanner, 384
vehicles, protecting facility against, 517
verbal agreements, never accepting from client, 14
version information, SQL injection attacks, 398
versions, SNMP, 178
vertical privilege escalation, 212
virtual machines. See VMs (virtual machines)
virtual private networks (VPNs), hardening network with, 273
virtualization
advantages for testing, 566–567
software options for building lab, 569
viruses
creating, 232–233
defined, 227
detecting, 240–243
kinds of, 230–232
overview of, 228
researching, 233–234
understanding, 228–230
as vulnerability in Mac OS X, 61–62
as vulnerability in Windows, 61
Visual Basic for Applications (VBA), macro viruses using, 230–231
VMs (virtual machines)
creating test setup, 568
installing/configuring for lab, 570
in side channel attacks on cloud, 493
VMware Player, building lab, 569
VMware Workstation, building lab, 569
voice recognition, biometrics, 516
voiding warranty, by jailbreaking, 447
VPNs (virtual private networks), hardening network with, 273
VRFY command, SMTP enumeration, 185
vulnerabilities
Android OS, 62
bus topology, 42
cryptographic, 88–89
defined, 13
topology, 58–59
Linux OS, 62–63
Mac OS, 61–62
mobile device, 447–448
web servers/applications, 369–374
WEP, 419
Windows OS, 60–61
WPA, 422–423
WPA/WPA2, 424–425
vulnerability analysis phase, penetration testing, 559–560
vulnerability research, 21
vulnerability scanning, 129–130, 151–152

W

Wabbit virus, 229
WAITFOR DELAY command, blind SQL injection, 402
walls, securing physical area, 516–517
WAPs (wireless access points), hardening networks, 273
warballooning attacks, 426
warchalking, 426
warded locks, 513
wardialing, 131–132
wardriving attacks, 426, 429
warflying attacks, 426
warm sites, 27
warning banners, physical security via, 504–505
warranty, voiding via jailbreaking, 447
warwalking attacks, 426
WaveStumbler, 426
web applications, pentesting tools for Android, 453
web browsers
preventing session hijacking, 352
preventing social engineering, 294
preventing threats, 294–295
setting to use proxy, 154–155
web applications based on, 363–364
web servers/applications
Apache, 361–362
client/server and, 364–365
cloud technologies, 365–366
cookies, 367–368
databases linked to web applications, 395
DoS attacks against, 308
exploring client-server relationship, 360–361
IIS, 362–363
individuals interacting with, 360–361
layers of web applications, 366–367
methods of attacking, 375–384
overview of, 360–361
review, 384
review answers, 540–541
review questions, 385–388
session hijacking, 336–337
SQL injection and, 393–394
testing web applications, 383–384
vandalizing, 374–375
variations of, 363–364
web application components, 368–369
web servers, 361–363
web servers/applications, common flaws/attack methods
cross-site scripting, 376
directory traversal attacks, 381–383
encryption weaknesses, 380–381
input validation, 375–376
insecure logon systems, 377–378
misconfiguration, 375
protecting cookies, 379–380
scripting errors, 378
session management issues, 378–379
unvalidated redirects and forwards, 376–377
web servers/applications, vulnerabilities
banner grabbing, 373
buffer overflow, 370–371
DDoS attack, 371–372
DoS attack, 371
error messages, 374
flawed web design, 369–370
using ID Serve, 373–374
vandalizing web servers, 374–375
web services, signature wrapping attacks on, 493
web-based attacks, on mobile devices, 441
webcams, footprinting location data, 113
websites
footprinting public/restricted, 111–112
spyware delivery via, 236
wifi tool, wireless traffic analysis, 429
well-known ports, 51–52
WEP (Wired Equivalent Privacy) encryption
breaking, 419–420
cracking with Kali Linux, 420–422
defined, 417
overview of, 418–419
problems/vulnerabilities, 419
RC4 algorithm in, 79
risk mitigation, 425
white box pen tests, 15
white-box testing, 551
white-hat hackers, 9, 11
whitelists, thwarting SQL injection, 392, 404
whitespace, evading detection via liberal use of, 404
Whois tool, 119
WhoReadMe utility, 117
Wi-Fi
authentication modes, 416–417
at Data Link layer of OSI model, 45
overview, 410–411
as vulnerability in Mac OS X, 62
wireless standards in use, 412–413
Wi-Fi, hacking
authentication technologies, 418
choosing right wireless card, 430–431
fine print, 411–412
locating wireless networks, 429–430
mitigating WEP and WPA cracking, 425
overview of, 410, 425
preventing threats to, 295
review, 433–434
review answers, 542–543
review questions, 435–437
sniffing with Wireshark, 260–264
SSID, 413
terminology, 414
understanding wireless networks, 410
WEP encryption, 418–422
wireless antennas, 414–416
wireless encryption mechanisms, 417
WPA encryption, 422–425
Wi-Fi, pentesting tools for Android, 453–454
Wi-Fi, threats
ad hoc, 427
client misassociation, 428
honeypot attacks, 428–429
jamming attacks, 428
MAC spoofing, 427
misconfiguration, 428
performing traffic analysis, 429–430
promiscuous client, 428
rogue access points, 426–427
wardriving, 426
ways to locate wireless networks, 429–430
WiFi Pineapple
hardware tool for lab testing, 573
as wireless honeypot, 429
Wi-Fi Protected Access. See WPA (Wi-Fi Protected Access) encryption
WifiKill, pentesting Android, 453
Wifite, 424–425, 453
Wigle Wifi Wardriving, 429, 454
WikiLeaks, 307
windows, securing physical area, 517
Windows OS. See also Microsoft Windows OS
creating virus in Notepad, 233
disabling auditing in Security Log, 216
enumeration, 163–167
iPhone. See also mobile device security, 441
WinDump, sniffer, 259, 572
Wink, people search utility, 113
WinSSLMiM, 381
wire reinforced windows, 517
Wired Equivalent Privacy. See WEP (Wired Equivalent Privacy) encryption
wireless access points (WAPs), hardening
networks, 273
wireless adapters, creating test setup, 568
wireless antennas, 414–416
wireless card
breaking WEP, 420–421
choosing right, 430–431
in promiscuous client attacks, 428
in wardriving attacks, 426
wireless connections, mobile device security issues, 447
wireless LANs (WLANs), accessing, 413
wireless networks. See Wi-Fi
wireless tools, for building lab, 572
Wireshark
  overview of, 260–264
  reading captured output of, 267–270
  as sniffer, 259, 572
  wireless traffic analysis, 430
Wit, Jan de, hacker, 5
WLANs (wireless LANs), accessing, 413
worms
defined, 227
first Internet, 5
functions of computer, 235–236
overview of, 234
SQL Slammer worm, 234–235
Stuxnet, 4
WPA (Wi-Fi Protected Access) encryption
attacking, cracking, 424–425
cracking, 422–424
defined, 417
overview of, 422
risk mitigation, 425
WPA2 encryption
attacking, cracking, 424–425
defined, 417
overview of, 424
risk mitigation, 425
WPA2 Enterprise, 417, 424
WPA2-Personal, 424
WPScan, pentesting Android, 452–453
wrapper programs, distributing Trojans, 245–246

X
Xamarin Test Cloud, 496
Xmas tree scan, 136–137
XML (Extensible Markup Language), 493, 494
Xprobe, banner grabbing with, 150
XSS (cross-site scripting)
  application-level hijacking via, 339–340
  against cloud, 494
  against web server, 376

Y
Yagi (directional) antenna, 415
Yagi Antenna tool, 573

Z
Zabasearch, people search utility, 113, 297
Zanti (for mobile phones), 454, 570
Zenmap scanner, 571
zero day threat/vulnerability, 13
zeroization, cryptographic processes and, 508
Zimmermann, Philip, 93
Zombam.B, Trojan-creation tool, 243
zombies
  DDoS attack setup, 318–319
  performing idle scan, 142–143
  zone transfers, DNS, 174–176