Index

Note to the reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. Italicized page numbers indicate illustrations.

A
access complexity metric in CVSS, 142–143
access vector metric in CVSS, 142
accesschk tool, 337–339, 337
AccessEnum tool, 338–339
accounts
access, 43–44
default settings, 339–340
ACK scans, 78
Actions on Objectives stage in Cyber Kill Chain model, 17
Active Directory (AD), 331–332
active reconnaissance, 74
code, 88–89, 89
defenses, 90
eavesdropping and packet capture, 81–82
enumeration, 84–88, 85, 87
hosts, 75
network topology, 81, 82
operating system fingerprinting, 77–80, 78–79
packet crafting and inspection, 83–84
services, 75–77
SNMP sweeps, 82–83
tools, 19–20
Acunetix vulnerability scanner, 122
Address Resolution Protocol (ARP) spoofing, 230–231, 230
address space layout randomization (ASLR), 329
administrator credentials, shared, 411
Advanced Exploit Development for Penetration Testers course, 190
adversaries, understanding, 37–38, 38
AFL (american fuzzy lop) fuzzer, 22, 312, 312
AFRINIC site, 68
Aircrack-ng tool
capabilities, 248
description, 22
alarms, 265
AllSigned execution in PowerShell, 366
alteration in DAD triad, 3, 3
american fuzzy lop (AFL) fuzzer, 22, 312, 312
amplification vulnerabilities, DNS, 165, 166
Apiary tool, 43
APK Studio tool
Android application packages, 313
description, 22
mobile devices, 347
APK X tool
Android application packages, 313
description, 22
mobile devices, 347
APNIC site, 68
Apple Remote Desktop (ARD), 203
application layer denial of service attacks, 234
application programming interfaces (APIs)
documentation, 43
enumerating, 87
unprotected, 308
web applications, 302
application vulnerabilities
authentication, 293–299, 294–298
authorization, 299–302, 300
tools, 203
lab exercises, 314–315
overview, 286
review questions, 316–320
summary, 313
testing tools
  DAST, 310–312, 310–312
d debuggers, 312–313
mobile, 313
 overview, 308–309
SAST, 309
unsecure coding practices, 306–308
web applications, 302–305, 304
applications
 enumerating, 86
fingerprinting, 87, 87
unsupported, 153–154, 154
vulnerability scanning, 121–123, 122–124
Approved Service Vendor (ASV), 34
arbitrary code execution, 156, 156
architectural diagrams, 43
ARD (Apple Remote Desktop), 203
ARIN site, 68
Arkin, Ofir, 234
ARP (Address Resolution Protocol) spoofing, 230–231, 230
arpseudo command, 230
arrays, scripting, 368–372
ASLR (address space layout randomization), 329
ASs (authentication servers), 298, 298
asset inventory, 107, 107
ASV (Approved Service Vendor), 34
attacking process, 12–13
attestation of findings, 419–420
authentication
  biometric, 349
  CVSS metric, 143
  multifactor, 413–414, 414
authentication servers (ASs), 298, 298
authentication vulnerabilities
  Kerberos exploits, 298, 299, 298
 overview, 293–294
passwords, 294–295, 294
session attacks, 295–297, 295–297
unvalidated redirects, 297–298
authority factor in social engineering, 267
authorization in penetration testing, 46
authorization vulnerabilities
  directory traversal, 300–301, 300
  file inclusion, 301–302
  insecure direct object references, 299–300
availability
  in CIA triad, 2, 3
  CVSS metric, 144
AXFRs (DNS zone transfers), 70–71

B
back doors
  persistence, 210–211
  vulnerabilities, 307
baiting attacks, 269
banner information, 77
bare-metal virtualization, 168
barriers, bypassing, 265
base scores in CVSS, 146
Bash. See Bourne-again shell (Bash) scripting language
BeEF (Browser Exploitation Framework) tool
  description, 21
  working with, 271–272, 272–273
behaviors in rules of engagement, 38–39
best practices in compliance-based assessments, 49
BGP looking glasses, 72
biometric authentication, 349, 413–414
black box tests, 37
blacklisting, 287
blind SQL injection attacks, 290–291, 290–291
blue-team assessments, 36
Bluejacking, 247
Bluesnarfing, 247
Bluetooth attacks, 247
Bourne-again shell (Bash) scripting language
  comparison operations, 373
  conditional execution, 380–381
  error handling, 395
  for loops, 385–386
overview, 365
string operations, 375–376
variables and arrays, 370
while loops, 389–391
bribery in social engineering, 269
“Bringing Software Defined Radio to the Penetration Testing Community” presentation, 247
Browser Exploitation Framework (BeEF) tool
description, 21
working with, 271–272, 272–273
brute-forcing tools for credentials, 350–351
Brutus tool, 206
budgets, 44–45
buffer overflows
Linux host attacks, 329
overview, 154–155
Burp Proxy, 311, 311
Burp Suite tool, 86, 123
business constraints in vulnerability scans, 109
business processes and practices scoping considerations, 41
bypass, NAC, 233–234
Bypass execution in PowerShell, 367

C

C2C (command-and-control) phase in Cyber Kill Chain model, 16
cache poisoning, DNS, 228, 229, 229
cachedump tool, 205, 348
Cain and Abel tool
description, 21
limitations, 205
password recovery, 350
CAPEC (Common Attack Pattern Enumeration and Classification) list, 62–63
cardholder data environments (CDEs)
penetration tests, 48
regulatory requirements, 6–8
Carnegie Mellon University Software Engineering Institute, 61–62
CAs (certificate authorities), unknown, 164
CAs (confidentiality agreements), 45
CCE (Common Configuration Enumeration), 119
cTLD (country code top-level domain) registries, 67
CDEs (cardholder data environments)
penetration tests, 48
regulatory requirements, 6–8
Censys search engine
description, 20
OSINT data, 61
working with, 73, 74
certificate authorities (CAs), unknown, 164
certificates
enumerating and inspecting, 88
pinning, 44
problems, 164, 165, 164
CERTs (Computer Emergency Response Teams), 61–62
CeWL (Custom Word List Generator)
description, 21
working with, 351
chaining, exploit, 191, 191
change management processes in vulnerability scanning, 128
cheat sheets, 83
chmod command, 365
CIA triad, 2–3, 3
ciphers, insecure, 163, 163
Clark, Ben, 83
cleartext credentials in LDAP, 331–332
clickjacking, 305
client acceptance, 419
cloned websites, 270
cloning, RFID, 248, 249
CMA (Computer Misuse Act), 46
code
analysis and testing, 120–121
arbitrary execution, 156, 156
cross compiling, 207
debugging, 89
decompilation, 88–89, 89
error handling, 306–307, 307
hard-coded credentials, 307
race conditions, 308
scripts and interpreted, 88
source code comments, 306
unprotected APIs, 308
unsigned, 308
code injection attacks, 292
code understanding, 120
cold-boot attacks, 345
command-and-control (C2C) phase in Cyber
Kill Chain model, 16
command injection attacks, 293, 293
comments in source code, 306
Common Attack Pattern Enumeration and
Classification (CAPEC) list, 62–63
Common Configuration Enumeration
(CCE), 119
Common Platform Enumeration (CPE), 119
common services, 240
FTP, 243–244
Samba, 244
SMTP, 242–243
SNMP, 241–242, 242
SSH, 244–245, 245
Common Vulnerabilities and Exposures
(CVE) list
contents, 63
description, 119
Linux kernel exploits, 329
Common Vulnerability Scoring System
(CVSS)
CVSS vector, 145
description, 119
metrics, 142–144
scores, 145–147
Common Weakness Enumeration (CWE)
list, 63
communications. See also reporting
goal reprioritization, 409
importance, 408
paths, 408
results, 13
rules of engagement, 39
triggers, 408–409
comparison operations, 372–373
compiled languages, 367
complexity of passwords, 411–412
compliance-based assessments, 36,
48 50
Computer Emergency Response Teams
(CERTs), 61–62
computer forensics, 407
Computer Misuse Act (CMA), 46
collection section in reports, 417
conditional execution, 379–383, 384
confidentiality agreements (CAs), 45
confidentiality in CIA triad, 2, 3
confidentiality metric in CVSS, 143
configuration files, 43, 75
configuration management systems, 149
Connect scans, 78
contact persons in rules of engagement, 39
containers
host vulnerabilities, 342–345, 343–344
and virtualization, 114–115
content-based blind SQL injection attacks,
290–291, 290–291
continuous monitoring, 126
contracts, 45
cookies, 295–297, 295–297
corporate policy, 106
scan frequency, 107–108, 108
scan target identification, 106–107, 107
country code top-level domain (ccTLD)
registries, 67
covering tracks, 212–213
cPassword attribute, 331, 331
CPE (Common Platform Enumeration), 119
Crack Me If You Can competition, 206
creddump utility, 205
credentialed scans, 115–116, 115
credentials
administrator, 411
brute-forcing tools, 205–206, 350–351
hard-coded, 307
obtaining
cleartext credentials in LDAP,
   331–332
cPassword, 331, 331
DLL hijacking, 335–336
hashes, 333
LSA secrets, 334
LSASS, 334
overview, 348–349
SAM database, 334, 335
service account attacks and
   Kerberos, 332–333
unattended installation, 334
unquoted service paths, 336–337,
   336–337
Windows Credential Manager,
   337–338
Windows kernel exploits, 338
writeable services, 337, 337
offline password cracking, 349–350, 350
tools, 21
   wordlists and dictionaries, 351–352
critical findings, 409
cron jobs, 200–201
cross compiling code, 207
cross-platform exploits in host
   vulnerabilities, 338–340
cross-site request forgery (CSRF/XSRF), 305
Cross-Site Scripting (XSS)
   overview, 172, 172
   reflected, 302–303
   stored/persistent, 303–304, 304
crystal box tests, 36–37
CSRF/XSRF (cross-site request forgery), 305
Custom Word List Generator (CeWL)
   description, 21
   working with, 351
customer commitments in vulnerability
   scanning, 128
CVE (Common Vulnerabilities and
   Exposures) list
   contents, 63
   description, 119
Linux kernel exploits, 329
CVSS. See Common Vulnerability Scoring
   System (CVSS)
CVSS vector, 145
CWE (Common Weakness Enumeration)
   list, 63
Cyber Kill Chain model, 13–17, 14–15
cybersecurity goals, 2–3, 3

D
DAD triad, 3, 3
daemons and services, 210
DAST (dynamic application security testing),
   310–312, 310–312
data
   handling requirements in rules of
      engagement, 38
   isolation in compliance-based
      assessments, 48
   ownership and retention, 46
Data Breach Investigations Report (DBIR)
   overflow issues, 154
   POS systems, 159, 159
   results, 150, 151
database vulnerability scanning, 123, 124
dataflow diagrams, 43
debug modes, 160, 161
debuggers
   common, 312–313
   description, 21–22
   working with, 89
decomposition, code, 88–89, 89
default account settings, 339–340
default passwords, 294, 294
defenses for information gathering, 89–90
delivery phase in Cyber Kill Chain model, 16
denial in DAD triad, 3, 3
denial of service (DoS) attacks, 226,
   234–235, 235
descriptions in scan reports, 139
Deviant Ollam’s site, 264
DHCP (Dynamic Host Configuration
   Protocol) attacks, 227
dictionaries
credentials, 351–352
password attacks, 206–207
difficulty factor in remediation, 126–127
DirBuster tool, 21, 352
direct object references, insecure, 299–300
directories
brute-forcing tools, 351–352
traversal, 300–301, 300
Dirty COW website, 155, 155
disabling plug-ins, 112–113, 113
disclosure in DAD triad, 3, 3
disposition in reports, 417–418
DLLs (Dynamic Link Libraries), hijacking, 335–336
DNS (Domain Name System)
cache poisoning, 228–229, 229
information, 68–70, 70
vulnerabilities, 165, 166
DNS zone transfers (AXFRs), 70–71
Docker containers, 344–345
documentation, 42–43, 42
documented exceptions in vulnerability scan
analysis, 147–148
DOM (Domain Object Model), 305
Domain Name System (DNS)
cache poisoning, 228–229, 229
information, 68–70, 70
vulnerabilities, 165, 166
Domain Object Model (DOM), 305
domains, 67–68
DoS (denial of service) attacks, 226, 234–235, 235
Dot1q, 227
double tagging, 226–227, 226
downgrade attacks
evil twins, 246
SSL, 233, 233
Drozer tool
Android devices and apps, 313
description, 22
exploits, 347
due diligence in compliance-based
assessments, 49
dumpster diving, 266
dynamic application security testing (DAST), 310–312, 310–312
dynamic code analysis, 121
Dynamic Host Configuration Protocol (DHCP) attacks, 227
Dynamic Link Libraries (DLLs), hijacking, 335–336

E
EAR (Export Administration Regulations)
Supplement No 1, 47
eavesdropping, 81–82
echo command, 365
EDGAR (Electronic Data Gathering, Analysis, and Retrieval) system, 66, 67
egress sensors, 264–265
802.1Q trunked interfaces, 226–227, 226–227
Electronic Data Gathering, Analysis, and
Retrieval (EDGAR) system, 66, 67
elicitation in social engineering, 267–268
email addresses, enumerating, 84–85, 85
embedded systems, 169
Empire tool, 23, 198
employees, identifying, 66–67
endpoint vulnerabilities. See server and
endpoint vulnerabilities
engagements
assessment types, 36
classifications, 36–37
overview, 35
rules, 38–40
scoping considerations, 40–42, 40
support resources, 42–45, 42
test control systems, bypassing, 264–265	enumeration, 84
API and interfaces, 87
applications, 86–87
certificates, 88
shares, 86
users, 84–86, 85
web pages and servers, 86
environmental differences, 46–48
error handling
code, 306–307, 307
scripting, 395 397
escalation attacks, 207–208
escape vulnerabilities in virtual machines, 168
/etc/passwd folder, 205
/etc/shadow folder, 205
evil twins, 245–247
exceptions in vulnerability scan analysis, 147–148
executive summaries in reports, 415–416
ExifTool, 65, 65
expiration of certificates, 164
Exploit Database, 188–189
Exploit Writing Tutorials section, 190
exploitation
Apple Remote Desktop, 203
tax essentials, 214–215
exploit development, 189–191, 191
exploit identification, 185–187, 186–187
lab exercises, 215 216
overview, 184
Persistence, 209 211
post-exploit attacks, 204–207, 206
privilege escalation, 207–208
process, 12–13
PsExec, 199
RDP, 202–203
resources, 188–189
review questions, 217–221
RPC/DCOM, 199
scheduled tasks and cron jobs, 200 201
SMB, 201–202, 202
social engineering, 208 209
SSH, 204
summary, 213–214
targets, 184, 184
Telnet, 203

tools, 191
Metasploit, 192–198, 193–194, 196–197
overview, 23
PowerSploit, 198
tracks covering, 212–213
VNC, 203
WinRM, 199–200
WMI, 200, 201
X-server forwarding, 203
exploitation phase in Cyber Kill Chain model, 16
Export Administration Regulations (EAR)
Supplement No 1, 47
exposure factor in remediation, 127
Extensible Configuration Checklist
Description Format (XCCDF), 119
external penetration testing teams, 9

F

facial recognition, 349
false positives in vulnerability scan analysis, 147
fear factor in social engineering, 267
Federal Information Processing Standard (FIPS) 199: Standards, 103–104, 104
Federal Information Security Management Act (FISMA), 103–106, 104
fences, bypassing, 265
File Transfer Protocol (FTP) exploits, 243–244
vulnerabilities, 160, 160
files
filename brute-forcing tools, 351–352
inclusion attacks, 301–302
unsecure permissions, 338 339
financial data, 66, 67
FindBugs tool
description, 22
static analysis of code, 309
findings
attestation of, 419–420
reports, 416–417
findsecbugs tool, 22, 309
fingerprinting
  applications, 87, 87
  operating systems, 77–80, 78–79
Fingerprinting Organizations with Collected Archives (FOCA) tool
  description, 20
  metadata, 65, 66
fingerprints, 349
FIPS (Federal Information Processing Standard) 199: Standards, 103–104, 104
Firefox Tamper Data extension, 310
firewalls, 288–289, 289
firmware
  missing updates, 161–162
  vulnerabilities, 157
FIRST (Forum of Incident Response and Security Teams), 144
FISMA (Federal Information Security Management Act), 103–104, 104
flow control
  conditional execution, 379–383, 384
  for loops, 384–388, 388
  overview, 378–379
  while loops, 389–394, 393
FOCA (Fingerprinting Organizations with Collected Archives) tool
  description, 20
  metadata, 65, 66
follow-up actions, 419
footprinting
  infrastructure and networks, 67–72, 69–72
  location and organizational data, 64–67, 65–67
OSINT, 61–63
  overview, 60–61
  security search engines, 72, 74, 73–74
for loops, 384–388, 388
Forum of Incident Response and Security Teams (FIRST), 144
FTP (File Transfer Protocol)
  exploits, 243–244
  vulnerabilities, 160, 160
FTPS (FTPSecure), 160
Full Disclosure mailing list, 63
full knowledge tests, 36–37
functions, 389–390
fuzzing
  application testing, 311–312, 312
  overview, 121
G
GDB debugger, 21, 312
generic top-level domain (gTLD) registries, 67
German Penal code, 47
Get-Acl command, 339
Get-CachedGPPPassword module, 331
Get-GPPPassword module, 331
Get-NetUser command, 333
GLBA (Gramm-Leach-Bliley Act)
  compliance-based assessments, 50
  description, 102
goal re prioritization in communication, 409
goals-based assessments, 36
Golden Ticket attacks, 205
Google Hacking Database, 188
Gramm-Leach-Bliley Act (GLBA)
  compliance-based assessments, 50
  description, 102
grey box tests, 37
green-team assessments, 36
Group Policy Preferences module, 331
groups, enumerating, 85–86
gTLD (generic top-level domain) registries, 67
guests, virtual, 168–169
H
hacker mind-set, 4–5
handling reports, 417–418
hard-coded credentials, 307
hardware flaws, 157, 158
Hashcat tool
description, 21
password cracking, 349, 350
hashes
acquiring, 333
passwords, 207
Health Insurance Portability and
Accountability Act (HIPAA)
compliance-based assessments, 49–50
description, 102
helpful nature factor in social engineering,
267
High Orbit Ion Cannon (HOIC) tool, 235
HighOn.Coffee Penetration Testing Tools
Cheat Sheet, 83
hijacking Dynamic Link Libraries, 335–336
HIPAA (Health Insurance Portability and
Accountability Act)
compliance-based assessments, 49–50
description, 102
HOIC (High Orbit Ion Cannon) tool, 235
honeypots, 268
horizontal escalation attacks, 208
host vulnerabilities
attacking
cross-platform exploits, 338–340
Linux, 325 330, 326–328, 330
overview, 325
Windows, 331–338, 331, 335–337
credentials, 348–352, 350
exam essentials, 353–354
lab exercises, 354–357
mobile devices, 347–348
overview, 324–325
physical devices, 345–346
remote access, 340–342, 342
review questions, 358–361
summary, 352–353
virtual machines and containers,
342–345, 343–344
hosted virtualization, 168
hosts
enumerating, 75
virtual patching, 168
Hping tool
capabilities, 235
description, 22
packet crafting, 83
HTTP downgrading attacks, 232
HTTP Unbearable Load King (HULK) tool,
235
Hydra tool
credentials, 351
description, 21
SSH attacks, 244–245, 245
Hyper-V, 344
hypervisors, 167, 167

IANA (Internet Assigned Numbers
Authority), 68
icacls command, 339
ICSs (industrial control systems), 169
IDA debugger, 22, 312
If...then...else statements, 379–383, 384
iGoat tool, 347
Immersion tool, 86
Immunity debugger, 21, 312
Impacket tool
description, 23
Python libraries, 86
impact function value in CVSS, 146
impact score in CVSS, 145–146
impersonation in social engineering, 268
in-person social engineering, 267–269
indicators of prior compromise, 409
industrial control systems (ICSs), 169
Inetd modification, 210
information gathering, 11–12
active reconnaissance. See active
reconnaissance
defenses, 89–90
enumeration. See enumeration
exam essentials, 91–92
footprinting. See footprinting
lab exercises, 92–93
overview, 60
review questions, 94–97
summary, 90–91
Information Sharing and Analysis Centers (ISACs), 62
Information Supplement: Penetration Testing Guidance, 8
informational results in vulnerability scan analysis, 148, 149, 148
infrastructure and networks, 67
DNS and traceroute information, 69–70, 70
domains, 67–68
IP ranges, 71, 71–72
routes, 72
WHOIS service, 68, 69
zone transfers, 70–71
injection vulnerabilities
code injection attacks, 292
command injection attacks, 293, 293
DLLs, 335–336
input validation, 287–288
overview, 170–171, 171
SQL, 289–292, 290–291, 414
web application firewalls, 288–289, 289
input
redirecting, 394–395
reflected, 302–303
validation, 287–288
input blacklisting, 287
input whitelisting, 287
insecure ciphers, 163, 163
insecure direct object references, 299–300
insecure protocol use, 160, 160
installation phase in Cyber Kill Chain model, 16
integrity
in CIA triad, 2, 3
CVSS metric, 144
interception proxies, 123, 310–311, 310–311
interfaces, enumerating, 87
internal documentation, 43
internal IP disclosure, 166, 167
internal penetration testing teams, 8–9
Internet Archive, 66
Internet Assigned Numbers Authority (IANA), 68
Internet of Things (IoT), 169–170
Internet Storm Center (ISC), 63
interpreted code
accessible information, 88
Ruby, 367
interrogation in social engineering, 268
interviews in social engineering, 268
IoT (Internet of Things), 169–170
IP addresses
internal disclosure, 166, 167
ranges, 71, 71–72
ISACs (Information Sharing and Analysis Centers), 62
ISC (Internet Storm Center), 63
IT governance in vulnerability scanning, 128
IT service management (ITSM) tool, 125

J
jamming, 249
jobs, scheduled
cron jobs, 209–210
persistence, 209–210
John the Ripper tool
description, 21
password recovery, 350
working with, 206, 206
JPCERT, 62
JTAG debug pins and ports, 346

K
KARMA Attacks Radio Machines
Automatically (KARMA), 245
KDCs (key distribution centers), 298, 298
Kerberoasting, 332–333
Kerberos exploits, 298–299, 298
kernel exploits

Linux, 329–330, 330
vertical escalation, 208
Windows, 337–338
key distribution centers (KDCs), 298, 298
key management testing, 48–49
keyloggers, 339
keys, duplicating, 264
Kismet tool
capabilities, 248
description, 22
wireless traffic capture, 82
knowledge-based authentication, 413–414

L

LACNIC site, 68
LAPS (Local Administrator Password Solution), 411
LaZagne tool, 338
LDAP (Lightweight Directory Access Protocol), 331–332
legal concepts
authorization, 46
contracts, 45
data ownership and retention, 46
environmental differences, 46–48
legal concerns in rules of engagement, 39
lessons learned, 419
licensing limitations in vulnerability scans, 109
lighting, 265
Lightweight Directory Access Protocol (LDAP), 331–332
likeness factor in social engineering, 267
Link Local Multicast Name Resolution (LLMNR) service, 238
Linux host attacks
kernel exploits, 329–330, 330
overview, 325–326
ret2libc, 329
shell upgrade attacks, 328–329
sticky bits, 327, 327
sudo command, 327–328, 328
SUID/SGID programs, 326–327, 326–327
LLMNR (Link Local Multicast Name Resolution) service, 238
local administrator credentials, shared, 411
Local Administrator Password Solution (LAPS), 411
local file inclusion attacks, 301
Local Security Authority Subsystem Service (LSASS), 334
location and organizational data
employees, 66–67
financial data, 66, 67
overview, 64–65
locks, bypassing, 264–265
LockWiki, 264
logs
maintaining, 41
network, 75
scan results reconciliation, 149
LOIC (Low Orbit Ion Cannon) tool, 235
looping operations
for loops, 384–388, 388
while loops, 389–393, 393
Low Orbit Ion Cannon (LOIC) tool, 235
LSA secrets, 334
lsadump tool, 348
LSASS (Local Security Authority Subsystem Service), 334
lsb_release command, 330

M

MAC (Media Access Control) addresses, 230–231
Maltego tool, 20, 72
man-in-the-middle, 229
ARP spoofing, 230, 231, 230
cookies, 296
relay attacks, 231–232
methodology section in reports, 417
MIBs (management information bases), 241
Mimikatz tool
  capabilities, 205
credentials, 348
description, 21, 198
hashes, 333
Kerberoasting, 332
SAM database, 334, 335
Mirai botnet, 170
missing firmware updates, 161–162
missing patches, 151–152, 152
mitigation strategy recommendations
  multifactor authentication, 413–414, 414
open services, 415
overview, 409–410
plain text passwords, 413
shared local administrator credentials, 411
SQL injection, 414
weak password complexity, 411–412
MITRE corporation, 62–63
mobile device management (MDM), 153
mobile devices
  host vulnerabilities, 347–348
  security, 153
testing tools, 313
modification, exploit and payload, 191
module options in Metasploit tool, 197, 197
motion sensors, 265
MOUs (memorandums of understanding), 128
MSAs (master services agreements), 45
multifactor authentication, 413–414, 414
MX records, 70

N

NAC (Network Access Control) bypass, 233–234
name resolution exploits in NetBIOS, 236–240, 237–239
names for certificates, 164
NAT (Network Address Translation) protocol, 166
National Cyber Awareness System Vulnerability Summary, 118, 118
description, 23 remote access vulnerabilities, 341 NDAs (nondisclosure agreements), 45 Nessus scanners
Objectives-based assessments, 36
Offensive Security Metasploit Unleashed documentation, 205
offline password cracking, 349–350, 350
OllyDbg debugger, 22, 312
ongoing scanning, 126
Onion Router, 341
open services, unnecessary, 415
open-source intelligence (OSINT) tools and techniques
CERTs, 61–62
information gathering, 19
MITRE corporation, 62–63
NIST, 62
overview, 60–61
Open Source Security Testing Methodology Manual (OSSTMM), 61, 262
Open Vulnerability and Assessment Language (OVAL), 119
Open Web Application Security Project (OWASP)
Password Storage Cheat Sheet, 207
static code analysis tools, 120, 309
OpenVAS scanners
description, 20
reports, 140, 141
operating systems
fingerprinting, 77–80, 78–79
unsupported, 153–154, 154
operational constraints in vulnerability scans, 109
Osgood, Rick, 190
OSINT. See open-source intelligence (OSINT) tools and techniques
OSSTMM (Open Source Security Testing Methodology Manual), 61, 262
output, redirecting, 394–395
OVAL (Open Vulnerability and Assessment Language), 119
overflows, buffer, 154–155, 329
OWASP (Open Web Application Security Project)
Password Storage Cheat Sheet, 207
static code analysis tools, 120, 309
ownership of data, 46

Packets
capturing, 81–82
crafting and inspecting, 83–84
parameter pollution, 288
pass-the-hash attacks, 231, 333
passive information gathering, 90
passwords
attack forms, 205–207, 206
brute-forcing tools, 350–351
complexity, 411–412
compliance-based assessments, 48
cPassword, 331, 331
hard-coded, 307
offline cracking, 349–350, 350
plain text, 413
vulnerabilities, 294, 295, 294
wordlists and dictionaries, 351–352
WPS, 247
Patator tool
credentials, 351
description, 21
patches, missing, 151–152, 152
patching virtual hosts, 168
paths, communication, 408
payload modification, 191
payload selection, 196
Payment Card Industry Data Security Standard (PCI DSS)
compliance-based assessments, 48–50
overview, 103
penetration testing requirements, 6–8, 34–35
Peach Fuzzer
description, 22
testing environments, 312
Penetration Testing Executing Standard, 61
penetration testing overview
benefits, 5–6
Cyber Kill Chain model, 13–17, 14–15
cybersecurity goals, 2–3, 3
description, 2
exam essentials, 24
external penetration testing teams, 9
hacker mind-set, 4 5
internal penetration testing teams, 8–9
lab exercises, 25
process
attacking and exploiting, 12–13
information gathering and
vulnerability identification, 11–12
overview, 10, 10
planning and scoping, 11
reporting and communicating results,
13
reasons, 5
regulatory requirements, 6–8
review questions, 26–29
summary, 23–24
team selection, 9–10
tools
credential-testing, 21
d_debuggers, 21  22
exploitation, 23
network testing, 22
overview, 17–19
reconnaissance, 19–20
remote access, 23
social engineering, 21
software assurance, 22
vulnerability scanners, 20–21
people category in mitigation strategies, 410
performance work statements (PWSs), 45
perimeter defenses, bypassing, 265
permissions
rules of engagement, 39
unsecure, 338–339
persistence
back doors and Trojans, 210–211
daemons and services, 210
Inetd modification, 210
new users, 211
scheduled jobs and tasks, 209–210
perspectives, scan, 116–117, 117
phantom DLLs, 336
phishing attacks, 269
phpinfo.php page, 186, 186 187
physical devices
cold-boot attacks, 345
JTAG debug pins and ports, 346
serial consoles, 345–346
physical facilities
entering, 262
common controls, 265–266
locks and entry control systems,
264–265
perimeter defenses and barriers, 265
piggybacking and tailgating, 263, 263
exam essentials, 274–275
information gathering, 266
lab exercises, 275–277
overview, 262
review questions, 278–281
scenario, 261
summary, 273–274
piggybacking, 263, 263
pinsets, 44
pivoting, 211–212, 212
plain text passwords, 413
planning and scoping
compliance-based assessments, 48–50
description, 11
guardians. See engagements
tools
exam essentials, 51–52
lab exercises, 52
legal concepts, 45–48
overview, 34
review questions, 53  56
scenario, 261
summary, 50–51
vulnerability scanning, 101–102,
110–111
plug-ins
disabling, 112–113, 113
feeds vulnerability, 118, 118
point-of-sale (POS) system vulnerabilities, 158–159, 159
port/hosts section in scan reports, 140
port scanners, 75–77
POS (point-of-sale) system vulnerabilities, 158–159, 159
post-engagement cleanup, 418
post-exploit attacks, 204–207, 206
PowerShell
comparison operations, 373
conditional execution, 381–382
error handling, 396
for loops, 386–387
overview, 366–367
string operations, 376
variables and arrays, 371
while loops, 391
WinRM, 199
PowerSploit tool
description, 23
Kerberoasting, 333
passwords, 331
working with, 198
presumption of compromise, 6
pretexting in social engineering, 262, 268
prior compromise indicators, 409
prioritizing remediation in vulnerability scanning, 126–127
privilege escalation
Linux host attacks, 326
overview, 155, 155
targets, 207–208
privileged accounts as scoping consideration, 41
problem handling and resolution in rules of engagement, 39–40
process category in mitigation strategies, 410
protocol-based denial of service attacks, 234
proxies
interception, 310–311, 310–311
network, 228
remote access vulnerabilities, 341–342
proxychains, 341–342
Proxychains tool, 23
PsExec tool, 199
purple-team assessments, 36
puts command, 367
pwdump tool, 205, 348
PWSs (performance work statements), 45
Python
comparison operations, 373
conditional execution, 383
error handling, 396–397
for loops, 387–388
I/O redirection, 394
libraries, 86
string operations, 378
variables and arrays, 372
while loops, 392
python-nmap module, 379

Q

Qualys scan reports, 140, 141
QualysGuard
asset maps, 107, 107
scan performance settings, 127, 128
quid pro quo attacks in social engineering, 268

R

race conditions, 308
rainbow tables, 207, 349
RainbowCrack tool, 349
RAML tool, 43
Rapid7 Vulnerability and Exploit Database, 188–189
ratings in Metasploit exploits, 194
RDP (Remote Desktop) exploits, 202–203
real-time operating systems (RTOS), 169
RealVNC tool, 339
reciprocation factor in social engineering, 267
Recon-ng tool, 20, 72
reconciling scan results, 149
reconnaissance and enumeration. See active reconnaissance; enumeration
reconnaissance phase in Cyber Kill Chain model, 15
red-team assessments, 36
Red Team Field Manual (RTFM), 83
redirects
  standard input and output, 394–395
  unvalidated URL, 297–298
reflected XSS attacks, 302–303
registered ports, 75–77
registrars for domains, 67
regulatory requirements
  penetration testing, 6–8
  vulnerability scanning, 102–105, 104
relationships, enumerating, 86
relay attacks, 231–232
remediation in reports, 416–417
remediation workflow, 125–127, 125
remote access vulnerabilities, 340
  Metasploit, 342, 342
  NETCAT and Ncat, 341
  proxies and proxychains, 341–342
  SSH, 340
  tools, 23
remote code execution vulnerabilities, 156, 156
Remote Desktop (RDP) exploits, 202, 203
remote file inclusion attacks, 301
remote login (rlogin), 204
Remote Procedure Call/Distributed Component Object Model (RPC/DCOM) exploits, 199
remote shell (rsh), 204
RemoteSigned execution in PowerShell, 366
repeating traffic, 249–250
replay attacks, 231
reporting, 407
  attestation of findings, 419–420
  client acceptance, 419
  communication
    goal reprioritization, 409
  importance, 408
  paths, 408
  triggers, 408–409
exam essentials, 420–421
follow-up actions, 419
lab exercises, 421
lessons learned, 419
mitigation strategies, 409–415, 414
post-engagement cleanup, 418
reports
  handling and disposition, 417–418
  structuring, 415–417
results, 13
review questions, 422–424
summary, 420
re prioritization of goals, 409
resources
  exploit, 188–189
  rules of engagement, 39
  support, 42–45, 42
Responder tool
  credentials, 202, 202
  description, 23
  NetBIOS name resolution exploits,
    237–239, 238–239
Restricted execution in PowerShell, 366
restricted shells, 328–329
results, reporting and communicating, 13
ret2libc attacks, 329
retention of data, 46
retesting, 419
RFID cloning, 248, 249
RIPE site, 68
risk appetite, 109
risk information section in scan reports,
  140
rlogin (remote login), 204
RockYou dictionary, 206–207
RoE (rules of engagement), 38–40
routes, 72
RPC/DCOM (Remote Procedure Call/ Distributed Component Object Model) exploits, 199
RSA 2011 Recruitment Plan attack, 269
rsh (remote shell), 204
RTFM (Red Team Field Manual), 83
RTOS (real-time operating systems), 169
Ruby
comparison operations, 373
conditional execution, 382
tax error handling, 396
for loops, 387
overview, 367–368
string operations, 377–378
variables and arrays, 371–372
while loops, 392
rules of engagement (RoE), 38–40

S
SAM (Security Accounts Manager)
database, 334, 335
password acquisition, 205
Samba (SMB)
exploits, 244
shares, 86
samrdump tool, 86
sandbox escapes, 342–343
SANS pen-testing blog, 63
SAQ (Self-Assessment Questionnaire), 34–35
Sarbanes-Oxley Act (SOX), 50
SAST (static application security testing), 309
SCADA (supervisory control and data acquisition) systems, 169
scans
Nmap, 78–79, 79–79
target determination, 106–107, 107
templates, 111–112, 112
vulnerability. See vulnerability scanning
SCAP (Security Content Automation Protocol), 119
scarcity factor in social engineering, 267
scheduled jobs and tasks
cron jobs, 200–201
persistence, 209–210
scoping. See planning and scoping
scripting
accessible information, 88
Bash, 365
comparison operations, 372–373
tax error handling, 395–397
exam essentials, 397–398
flow control
conditional execution, 379–383, 384
for loops, 384–388, 388
overview, 378–379
while loops, 389–394, 393
input and output, 394–395
lab exercises, 398
overview, 364–365
PowerShell, 366–367
Python, 368
review questions, 399–403
Ruby, 367–368
string operations, 373–378
summary, 397
variables, arrays, and substitutions, 368–372
SDKs (software development kits), 43
search engines, 72–74, 73–74
search order hijacking DLLs, 336
searches for exploit, 195–196, 196
SearchSploit tool
description, 23
Exploit Database, 188
Secure File Transfer Protocol (SFTP), 160
Secure Shell (SSH)
description, 23
exploits, 244–245, 245
overview, 204
remote access vulnerabilities, 340
for Telnet, 160
Secure Sockets Layer (SSL) protocol,
162–165
downgrade attacks, 233, 233
stripping attacks, 232
Security Accounts Manager (SAM)
database, 334, 335
password acquisition, 205
Security and Privacy Controls for Federal
information Systems and Organizations, 104–105
Security Content Automation Protocol (SCAP), 119

security information and event management (SIEM) systems, 149

security search engines, 72–74, 73–74

selecting penetration testing teams, 9–10

Self-Assessment Questionnaire (SAQ), 34–35

sensitivity levels in scans, 111–114, 112–113

serial consoles, 345–346

server and endpoint vulnerabilities

arbitrary code execution, 156, 156

buffer overflows, 154–155

debg modes, 160, 161

hardware flaws, 157, 158

insecure protocol use, 160, 160

missing patches, 151–152, 152

privilege escalation, 155, 155

unsupported operating systems and applications, 153–154, 154

Server Message Block (SMB)

exploits, 240

overview, 201–202, 202

service account attacks, 332–333

service degradations in vulnerability scanning, 127, 128

service-level agreements (SLAs), 128

service paths, unquoted, 336–337

service principal names (SPNs), 332–333

services

enumerating, 75–77

identifying, 77

session attacks, 295–297, 295–297

Set-ExecutionPolicy command, 367

set group ID (SGID) programs, 326–327, 326–327

SET (Social Engineering Toolkit), 21, 270–271, 271

set user ID (SUID) programs, 326–327, 326–327

severity factor

in remediation, 127

scan reports, 139

SFTP (Secure File Transfer Protocol), 160

SGID (set group ID) programs, 326–327, 326–327

shared local administrator credentials, 411

shares, enumerating, 86

shell upgrade attacks, 328–329

Shodan search engine

description, 20

OSINT data, 61

working with, 73, 73

shoulder surfing, 268

shove keys, 264

side-loading DLLs, 336

SIEM (security information and event management) systems, 149

Sieve application, 347

similarity factor in social engineering, 267

Simple Mail Transfer Protocol (SMTP), 241–243

Simple Network Management Protocol (SNMP)

exploits, 241–242, 242

sweeps, 82–83

SiteList.xml file, 339

SLAs (service-level agreements), 128

SlowLoris tool, 235

SMB (Samba)

exploits, 244

shares, 86

SMB (Server Message Block)

exploits, 240

overview, 201–202, 202

SMBMap scanner, 86

SMS phishing attacks, 269

SMTP (Simple Mail Transfer Protocol), 241–243

SNMP (Simple Network Management Protocol)

exploits, 241, 242, 242

sweeps, 82–83

snmpwalk command, 85, 242, 242

SOAP, 42

social engineering

exam essentials, 274–275

forms, 208–209
lab exercises, 275–277
overview, 262, 266
in-person, 267–269
review questions, 278–281
summary, 273–274
targets, 266–267
tools, 21, 270 272, 271 273
website-based attacks, 270
Social Engineering Framework, 267
Social Engineering Toolkit (SET), 21, 270–271, 271
social networking sites, enumerating, 85
social proof factor in social engineering, 267
Socket Secure Proxy via SSH (SOCKS proxy), 228
software, scanner, 117, 118
software assurance tools, 22
software development kits (SDKs), 43
software security testing
code analysis and testing, 120 121
overview, 119–120
web application vulnerability scanning, 121–123, 122–124
solutions in scan reports, 139
something you know/have/are
authentication, 413–414
SonarQube tool, 22, 309
SOOs (statements of objectives), 45
source code comments, 306
SOWs (statements of work)
description, 45
vulnerability scans, 110
SOX (Sarbanes-Oxley Act), 50
Spanning Tree Protocol (STP) attacks, 227
spear phishing attacks, 269
Spectre vulnerability, 157, 158, 188
SPNs (service principal names), 332–333
SQL injection attacks
remediation, 414
Sqlmap vulnerability scanner
database scans, 123, 124
description, 20
SSH. See Secure Shell (SSH)
SSL (Secure Sockets Layer) protocol, 162–165
downgrade attacks, 233, 233
stripping attacks, 232
standard input and output, redirecting, 394–395
statements of objectives (SOOs), 45
statements of work (SOWs)
description, 45
vulnerability scans, 110
static application security testing (SAST), 309
static code analysis, 120
stealth scans, 114
sticky bits, 327, 327
stored/persistent XSS attacks, 303–304, 304
STP (Spanning Tree Protocol) attacks, 227
stress testing, 234–235, 235
string operations, 373–378
stripping attacks in SSL, 232
substitutions in scripting, 369
sudo command, 327–328, 328
SUID (set user ID) programs, 326–327, 326–327
supervisory control and data acquisition
(SCADA) systems, 169
supplementing network scans, 114–116, 115
supply chain tests, 41
support resources, 42–45, 42
Swagger tool, 43
sweeps, SNMP, 82–83
switch spoofing, 227, 227
SYN floods, 235, 235
Sysinternals toolkit, 199
system criticality in remediation, 126
system-detect-virt command, 344
system ports, 75, 77
tailgating, 263, 263
TamperData interception proxies, 123
Target Corporation data breach, 412

tasks, scheduled

cron jobs, 201–202

persistence, 209–210

TCP SYN scans, 78

teams

external, 9

internal, 8–9

selecting, 9–10

technical constraints in vulnerability scans, 109

technology category in mitigation strategies, 410

Telnet, 160, 203

TGTs (ticket granting tickets), 298–299, 298

THC-Hydra tool, 206

The Open Organization Of Lockpickers (TOOOL) website, 264

theHarvester tool
description, 20, 72

e-mail addresses, 84–85, 85

third-party authorization, 46

threat hunting, 6

ticket granting tickets (TGTs), 298–299, 298

tiger teams, 36

time-based blind SQL injection attacks, 292

time-of-check-to-time-of-use (TOCTTOU) issue, 308

timelines in rules of engagement, 38

timing flags in Nmap, 79

TLS (Transport Layer Security), 162–165, 162–164

TOCTTOU (time-of-check-to-time-of-use) issue, 308

tokens, 87

TOOOL (The Open Organization Of Lockpickers) website, 264

topology, network, 81, 82

TOR router, 341

traceroute information, 69–71, 72

traffic volume-based denial of service attacks, 234

Transport Layer Security (TLS), 162–165, 162–164

trend analysis, 149, 150

triggers, communication, 408–409

Trojans, 210–211

trust in social engineering, 266

try...catch clauses, 395

2011 Recruitment Plan attack, 269

U

UltraVNC tool, 339

unattended installation, 334

Unix shells, 365

unnecessary open services, 415

unprotected APIs, 308

unquoted service paths, 336–337, 336–337

Unrestricted execution in PowerShell, 367

unsecure file/folder permissions, 338–339

unsigned code, 308

unsupported operating systems and applications, 153–154, 154

unvalidated redirects, 297, 298

updates for firmware, 161–162

urgency factor in social engineering, 267

URL redirects, 297–298

USB key drops in social engineering, 268

users

enumerating, 84–86, 85

new, 211

scoping considerations, 41

V

validated redirects, 298

validation of input, 287–288

variables in scripting, 368–372

Veracode, 120, 309

versions, identifying, 77

vertical escalation attacks, 207–208

video surveillance and camera systems, 265

virtual guest issues, 168–169
Virtual local area networks (VLANs), hopping, 226–227, 226–227
virtual machines
escape vulnerabilities, 168
host vulnerabilities, 342–345, 343–344
Virtual Network Computing (VNC), 203
virtual private networks (VPNs), 166
VirtualBox, 344
virtualization
and container security, 114–115
vulnerabilities, 167–169, 167
vishing attacks, 269
VLANs (virtual local area networks), hopping, 226–227, 226–227
VMware, 344
VNC (Virtual Network Computing), 203
VPNs (virtual private networks), 166
VulDB database, 189
vulnerabilities
applications. See application vulnerabilities
host. See host vulnerabilities
identification, 11–12
injection. See injection vulnerabilities
network. See network vulnerabilities
vulnerability scan analysis
common vulnerabilities
Internet of Things, 169–170
network, 161–166, 162–164, 166–167
overview, 150, 151
server and endpoint, 151–160, 152, 154–156, 158–160
virtualization, 167–169, 167
web applications, 170–172, 171–172
exam essentials, 173–174
lab exercises, 174–175, 174–175
overview, 138
reports
CVSS, 142–147
overview, 138–140, 139, 141
result validation
documented exceptions, 147–148
false positives, 147
informational results, 148–149, 148
reconciling, 149
trend analysis, 149, 150
review questions, 176–179
summary, 172–173
vulnerability scanning
barriers, 127 128, 128
configuring and executing
overview, 109
scan perspectives, 116–117, 117
scan sensitivity levels, 111–114, 112–113
scoping, 110–111
supplementing, 114–116, 115
exam essentials, 129–130
lab exercises, 130–131
management requirements
corporate policy, 106 109, 107 108
overview, 102
regulatory environment, 102 105, 104
overview, 101–102
remediation workflow, 125–127, 125
review questions, 132–135
scanner maintenance, 117–118, 118
scanner overview, 20–21
software security testing, 119–123, 122 124
summary, 129

W
W3AF (Web Application Attack and Audit Framework), 20, 86, 352
W3C (World Wide Web Consortium)
standards, 43
WADL (Web Application Description Language), 42
WAFs (web application firewalls), 288–289, 289
watering hole attacks, 270
WDS (Windows Deployment Services), 334
weak password complexity, 411–412
weaponization phase in Cyber Kill Chain model, 15–16
Web Application Attack and Audit Framework (W3AF), 20, 86, 352
Web Application Description Language (WADL), 42
web application firewalls (WAFs), 288–289, 289
web application vulnerabilities, 302
    clickjacking, 305
cross-site request forgery, 305
cross-site scripting, 172, 172, 302–304
    injection attacks, 170–171, 171
scanning, 121–123, 122–124
web pages and servers, enumerating, 86
Web Services Description Language (WSDL), 42–43, 42
web shells, 301–302
WebGoat project, 347
website-based social engineering attacks, 270
well-known ports, 75–77
WEP (Wired Equivalent Privacy), 246
whaling attacks, 269
while loops, 389–394, 393
white box tests
    access, 43–44
    overview, 36–37
white-team assessments, 36
whitelisting, 287
WHOIS service
description, 20
domain database, 68, 69
WiFi Protected Setup (WPS), 246–247
WiFite tool
capabilities, 248
description, 22
WinDBG debugger, 22, 312
Windows Credential Manager, 337–338
Windows Deployment Services (WDS), 334
Windows host attacks on credentials, 331–337, 331, 335–337
Windows kernel exploits, 337–338
Windows Management Instrumentation (WMI), 200, 201
Windows Remote Management (WinRM), 199–200
Windows services, 236–240, 237–239
Wired Equivalent Privacy (WEP), 246
wireless exploits
    evil twins, 245–247
    jamming, 249
    MITM, 245–247
    repeating, 249–250
    RFID cloning, 248, 249
Wireshark capture tool
description, 22
wireless traffic capture, 82
WMI (Windows Management Instrumentation), 200, 201
wmic
    services, 336, 336
    virtual machine attacks, 343, 343–344
WMImplant tool, 200, 200
Wood, Robin, 71
wordlists for credentials, 351–352
World Wide Web Consortium (W3C) standards, 43
WPS (WiFi Protected Setup), 246–247
Write-Host command, 367
writeable services, 337, 337
WSDL (Web Services Description Language), 42–43, 42

X

X-server forwarding, 203
XCCDF (Extensible Configuration Checklist Description Format), 119
Xen Project, 344
XML-based standards, 43
XML documentation, 42, 42
XSS (Cross-Site Scripting)
    overview, 172, 172
Y

YASCA (Yet Another Source Code Analyzer) tool, 22, 309
Yersinia tool, 227, 227

Z

Z-Wave protocol, 246
ZAP (Zed Attack Proxy), 310, 310
Zenmap user interface, 80–81, 82
zero knowledge tests, 37
zone transfers, 70–71

reflected, 302–303
stored/persistent, 303–304, 304