INDEX

Numbers
0-day attacks
  overview, 165–172
  exercise, 172
  recommendations, 172–173
2-step authentication, 43–44

A
active authentication, 36
address space layout randomization (ASLR), 170
advanced persistent threats (APTs), xxii
Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, 206
AI-powered fuzzers, 169
air gapping, 134
AirHopper, 81
ambushes, 126
animal behavior, xxviii
anomaly detectors, 51–53
anti-privilege, 26–27
antivirus software, 134
APT28, 148
APT29, 148
Armed Services Vocational Aptitude Battery test (ASVAB), 178–179
art of estimating distance, 8
The Art of War (Sun Tzu), xxv
attack sensing and warning (AS&W) indicators, 157
attack vectors
  overview, 15–18
  exercise, 23
  finding, 20–22
  recommendations, 23–24
  threat modeling, 18–22
attribution
  overview, 113–117
  approaches to, 116–117
  exercise, 118
  recommendations, 118–119
Aurora Panda, 142
authentication, 34–35, 43–44

B
baiting, 93. See also social engineering attacks
bandwidth usage, 155
Bansenshūkai scrolls
  overview, xxi, xxv
  correct mind, xxvii
  double-sealed passwords, 41
  guarding, 15
  identification methods, 34
  mapping networks, 1
  Teikairon scroll, 42
  time-scheduled events, 49–51
behavior heuristics, 101
BitWhisper, 81
black-box aptitude battery, 179–180
BLACKCOFFEE remote access
trojan, 142
"block suspicious" policies, 197
blue teams, 74, 170
Border Gateway Protocol (BGP)
gateways, 8
BoringSSL open source project, 171
bridges and bridging
overview, 79–80
exercise, 82
network boundary bridging, 80–82
recommendations, 83
bring your own device (BYOD)
policies, 93, 197

call sign techniques
overview, 147–150
exercise, 150
recommendations, 150–151
Castle Theory thought exercises.
See exercises
challenge-response authentication.
See matched pairs
Chaos Monkey exercise, 135
chassis-case locks, 87
checksums, 59
Chinese APT17, 142
clock signals, 58
cognitive biases, 116–117
command and control (C2)
communications
overview, 139–143
exercise, 144
recommendations, 144–145
communication connections, 2
continuous authentication, 36
correct mind, xxvii
countersigns. See matched pairs
COZYBEAR, 148
culture of excellence, 180–181
Cummins, Antony, xxiii, xxvii
cyber attacks
overview, 131–134
exercise, 136–137
recommendations, 137–138
safeguards from, 134–136
cyber fire drills, 134–135
cyber insurance, 134
cyber intelligence (CYBINT), 116
Cyber Kill Chain framework, 206
cyber threat intelligence
(CTI), 208
cybersecurity industry
issues in, xxiii, 175–181
recruitment, 175–181

D
data flow diagrams (DFDs), 19
Democratic National Committee hack, 148–149
denial and deception (D&D), 171
Department of Defense’s DLAB
(Defense Language Aptitude
Battery) test, 179–180
Deputy Dog, 142
detect function, 18
device port locks, 87
devices
bring your own device (BYOD)
policies, 93, 197
device port locks, 87
network maps and, 2
out-of-band devices, 43
digital litter, 156
digital tailgating, 94
disconnect defense, 171–172
disqualifiers, 180
distance estimating, 8
distributed denial of service (DDoS)
attacks, 161
double-sealed passwords
overview, 41–43
2-step authentication, 43–44
development, 44–45
exercise, 46
recommendations, 46
egress points, 74  
elliptic-curve Diffie-Hellman (ECDH), 74  
employees  
Overview, 175–181  
Exercise, 181  
human resource departments  
and, 103, 177  
isues and behavior, 175–181  
recommendations, 181–182  
encrypted traffic, 74  
encryption, 59  
exercises  
0-day attacks, 172  
attack vectors, 23  
attribution, 118, 188  
brides and bridging, 82  
call sign techniques, 150  
Chaos Monkey exercise, 135  
command and control (C2) communications, 144  
cyber attacks, 136–137  
double-sealed passwords, 46  
employees, 181  
fire attacks, 136–137  
forensics, 127  
guarding, 23  
hiring talent, 181  
hours of infiltration, 53  
identification methods, 38  
implants, 111  
infiltration, 53, 162  
insider threats, 105  
light discipline, 157  
litter discipline, 157  
live capture, 127  
locks, 89  
mapping networks, 12–13  
network boundary bridging, 82  
network mapping, 12–13  
noise discipline, 157  
opportunities, 162  
recruitment, 181  
security operations centers (SOCs), 191  
sensors, 75  
social engineering attacks, 95–96  
supply chain attacks, 111  
tactics, techniques, and procedures (TTPs), 210  
talent, 181  
time tracking, 61  
time-scheduled events, 53  
tools, 68  
trust, 199  
wm agents, 105  
xenophobic security, 30  
zero-day attacks, 172  
zero-trust threat management, 199  
false alerts, 157  
FANCYBEAR, 148  
Faraday cages, 82  
feedback, 189  
FEIB Hermes ransomware, 133  
file sizes, 155  
fire attacks  
Overview, 131–134  
exercise, 136–137  
recommendations, 137–138  
safeguards from, 134–136  
fire drills, 134–135  
firewalls, 93–94, 134  
FizzBuzz problem, 178  
forensics  
Overview, 124–125  
confronting live threats, 125–127  
exercise, 127  
recommendations, 127–128  
FSB, 148  
Fujibayashi, xxv  
fushi-kamari, 122  
fuzzers and fuzzing, 169  
Google, 171  
Group Policy Objects (GPO), 28, 134
GRU, 148–149
GSMem, 81
guarding
  overview, 15–18
  exercise, 23
  finding attack vectors, 20–22
  recommendations, 23–24
  threat modeling, 18–22
Gunpo Jiyoshu scroll, xxvi, 41, 132, 139–140, 147, 201–202. See also Yoshimori Hyakushu

H
Hanzō, Hattori, xxiv, xxvi
Hideyoshi, Toyotomi, 64
hiring talent
  overview, 175–181
  exercise, 181
  recommendations, 181–182
honey ambushes, 126
host intrusion detection systems (HIDS), 134
hours of infiltration. See also attribution; infiltration
  overview, 49–51
  anomaly detectors, 51–53
  exercise, 53
  recommendations, 54–55
human intelligence (HUMINT), 116
human resource departments, 103, 177
hunt teams, 170

I
identification methods. See also attribution
  overview, 33–37
  authentication, 34–35
  exercise, 38
  matched pairs, 34–35, 37–38
  open disguise, 34
  recommendations, 38–39
  spoofing, 36
identify function, 17
imaging, 124–125
imitation, 123
implants
  overview, 107–109
  exercise, 111
  protections from, 109–110
  recommendations, 111–112
indicators of compromise (IoC), 206
infiltration
  overview, 159–162
  exercises, 53, 162
  hours of, 49–55
  infiltration, 163
  in-nin mode of, xxvii, 34
  recommendations, 54–55, 163
  yo-nin mode of, xxvii, 34
information gathering, xxviii, 6–9
information sharing and analysis center (ISAC), 199
in-nin mode of infiltration, xxvii, 34
insider threats
  overview, 99–102
  approach to, 102–104
  exercise, 105
  recommendations, 105–106
insurance policies, 134
intelligence collection, 6–9
Internet of Things (IoT), 134
interoperability, 27–29
interview capability assessments, 179
intrusion prevention systems (IPS), 134
inward-facing sensors, 75

J
jump boxes, 20
Just Enough Administration (JEA), 66
Just in Time (JIT) administration, 66

K
Kahneman, Daniel, 95
kamaritsuke technique, 203–204
Kayser, Richard, 58
kokoro, xxii

L
light discipline
  overview, 153–157
exercise, 157
recommendations, 158
Link Layer Discovery Protocol (LLDP), 81
links, 2
litter discipline
overview, 153–157
exercise, 157
recommendations, 158
live capture
overview, 124–125
confronting live threats, 125–127
exercise, 127
recommendations, 127–128
live threats, 125–127
living-off-the-land attacks, 65–66
Lockheed Martin, 206
locks
overview, 85–87
defeating, 87–88
exercise, 89
improvement of, 88–89
recommendations, 89
lucky days, 50. See also time-scheduled events

M
malware attacks, 133
mapping networks
overview, 1–6
accuracy, 5
challenges, 6–9
details, 3–5
examples, 3–4
exercise, 12–13
intelligence collection, 6–9
process, 9–12
recommendations, 13
testing, 12
topology, 11
Masashige, Kusunoki, 41
Masatake, Natori Sanjuro, xxiv, xxvi
matched pairs, 34–35, 37–38
Microsoft, 66, 142
military recruiting, 178
Minami, Yoshie, xxiii
minomushi, 100, 103
mirroring, 124
MITRE, 206
multifactor authentication, 35
multitenant clouds, 93

N
National Institute of Standards and Technology (NIST) Cybersecurity Framework, 17
net, 8
Netflix, 135
network access controls (NACs), 28, 81
network boundary bridging
overview, 79–80
exercise, 82
recommendations, 83
network mapping
overview, 1–6
accuracy, 5
challenges, 6–9
details, 3–5
examples, 3–4
exercise, 12–13
intelligence collection, 6–9
process, 9–12
recommendations, 13
testing, 12
topology, 11
network segmentation, 143
Network Time Protocol (NTP), 59
night attacks, 50. See also time-scheduled events
ninjutsu, xxv

NIPRnet, 197
Nmap, 6, 155
Nobunaga, Oda, 64
nodes, 2
noise discipline
  overview, 153–157
  exercise, 157
  recommendations, 158
Nonce, 59
non-promiscuous mode, 9
no-operation (NOP), 156

O
open disguise, 34
open source intelligence (OSINT), 116
Open Systems Interconnection (OSI) model, 29
opportunities
  overview, 159–162
  exercise, 162
  recommendations, 163
out-of-band devices, 43

P
packet captures (PCAP), 10
packet frequency, 155
passive mapping, 8
passive sensors, 75
passwords
  overview, 41–43
  2-step authentication, 43–44
  development, 44–45
  exercise, 46
  recommendations, 46
patents, xxiv
payloads, 155
pen testing, 74
“permit any-any” conditions, 161
phishing, 93. See also social engineering attacks
physical security, 72–73, 87–88. See also locks
ping, 8
Plug and Play (PnP) standard, 28
power locks, 87
PowerShell, 66
pretexting, 93. See also social engineering attacks
privilege, 26–27
Privilege Access Management (PAM), 66
procedures. See tactics, techniques, and procedures (TTPs)
promiscuous mode, 9
protect function, 17–18
purple teams, 74
Pyramid of Pain. See tactics, techniques, and procedures (TTPs)

R
randomization, 170
ransomware attacks, 133
recommendations
  0-day attacks, 172–173
  attack vectors, 23–24
  attribution, 118–119
  bridges and bridging, 83
  call sign techniques, 150–151
  command and control (C2)
    communications, 144–145
cyber attacks, 137–138
double-sealed passwords, 46
employees, 181–182
fire attacks, 137–138
forensics, 127–128
guarding, 23–24
hiring talent, 181–182
hours of infiltration, 54–55
identification methods, 38–39
implants, 111–112
infiltration, 54–55, 163
insider threats, 105–106
light discipline, 158
litter discipline, 158
live capture, 127–128
locks, 89
mapping networks, 13
network boundary bridging, 83
network mapping, 13
noise discipline, 158
opportunities, 163
recruitment, 181–182
security operations centers (SOCs), 191–192
sensors, 76
social engineering attacks, 96
supply chain attacks, 111–112
tactics, techniques, and procedures (TTPs), 211
talent, 181–182
time tracking, 61
time-scheduled events, 54–55
tools, 68–69
trust, 200
worm agents, 105–106
xenophobic security, 30–31
zero-day attacks, 172–173
zero-trust threat management, 200
recovery function, 18
recruitment
overview, 175–181
exercise, 181
human resource departments
and, 103, 177
recommendations, 181–182
red teams, 74
“remote viewing” controls, 143
remote work, 93
respond function, 18
ringed architecture, 26
routers, 3
sabotage malware, 133
Saku’un, Ogasawara, xxvi
schematics, 5
security controls, 68–69
security logs, 51–53
security operations centers (SOCs)
overview, 175–181
exercise, 191
recommendations, 191–192
segmentation, 143
SELinux OS, 171
sensors
overview, 71–72
exercise, 75
improvement of, 73–75
inward-facing sensors, 75
passive sensors, 75
recommendations, 76
togiki sensors, 75
use of, 72–73
Wi-Fi sensors, 72–73
Shamoon malware, 59
Shamoon virus, 133
shielded glass, 82
shinobi, xxiv, xxvii
Shinobi Hiden scrolls, xxvi
shinobi-gaeshi, 16, 22
Shiyoshu scroll. See Gunpo fiyoshu scroll
Shōninki, xxvi, 49, 63, 165–167
signal intelligence (SIGINT), 116
single-factor authentication, 35
size of packets, 155
sneakernet, 81
social engineering attacks
overview, 91–92
defenses against, 94–95
exercise, 95–96
recommendations, 96
software-based “mapping” tools, 6
spoofing, 36
spreadsheets, 5
STRIDE, 21
strong authentication, 35
STUXNET, 168
Sun Tzu, xxv
supply chain attacks
overview, 107–109
exercise, 111
protections from, 109–110
recommendations, 111–112
SWIFT financial attack, 133

tachisuguri isuguri, 41–42
tactics, techniques, and procedures (TTPs), xxii
overview, 201–208
cyber threat intelligence (CTI),
208–210
exercise, 210
recommendations, 211
tailgating, 94
talent
  overview, 175–181
  exercise, 181
  human resource departments
  and, 103, 177
  recommendations, 181–182
TechNet website, 142
technical detection techniques, 101
  See tactics, techniques, and
  procedures (TTPs)
Teikai ron scroll, 42. See also
  Bansenshūkai scrolls
  TEMPEST controls, 82
tethering locks, 87
Thinking, Fast and Slow (Kahneman), 95
threat intelligence, 208
threat modeling, 18–22
tiger traps, 126–127
  “time bomb” viruses, 133
time tracking
  overview, 57–58
  exercise, 61
  importance of, 58–60
  recommendations, 61
time-scheduled events
  overview, 49–51
  development, 51–53
  exercise, 53
  recommendations, 54–55
timestamps, 59
togiki sensors, 75
tools
  overview, 63–65
  exercise, 68
  living-off-the-land attacks, 65–66
  recommendations, 68–69
  securing, 66–67
traps, 126–127
trust
  overview, 195–199
  exercise, 199
  recommendations, 200
two-factor authentication, 35
two-step authentication, 43–44
U
Unified Modeling Language (UML), 20
unique properties and
  characteristics, 29
uramittsu no jutsu, 8, 9
US Department of Defense (DoD), 189, 197
US military, 178
USB ports, 22, 81
W
Wi-Fi access points, 81
Wi-Fi sensors, 72–73
Windows, 66, 142
wipe-and-forget responses, 123
wiper malware attacks, 133
Wireshark, 156
wiring diagrams, 5
work-feedback loops, 189
worm agents
  overview, 99–102
  approach to, 102–104
  exercise, 105
  recommendations, 105–106
X
xenophobic security
  overview, 25–29
  exercise, 30
  interoperability, 27–29
  privilege, 26–27
  recommendations, 30–31
  unique properties and
  characteristics, 29
Y
yabumi, 140
yo-nin mode of infiltration, xxvii, 34
Yoshimori Hyakushu, xxvi, 1, 49, 123,
  161, 175–177, 202. See also Gunpo
  Jiyoshu scroll
zero-day attacks
  overview, 165–172
  exercise, 172
  recommendations, 172–173

zero-trust threat management
  overview, 195–199
  exercise, 199
  recommendations, 200