## Index

### A

AAA (authentication, authorization, and auditing), 98–99
aboutface.com, 148
access management
  AAA (authentication, authorization, and auditing), 98–99
  about, 97–98
  JumpCloud, 103–108
  principle of least privilege (PoLP), 99–101
  single sign-on (SSO), 101–103
ACLU (American Civil Liberties Union), 78
Active Directory (AD), 170
Address Resolution Protocol (ARP), 33
administrative privileges, controlled use of, 240–241
AFGSC (Air Force Global Strike Command), 173
agentless agents, 61
agents, 61–65
Aharoni, Mati (administrator), 205
Air Force Global Strike Command (AFGSC), 173
AM (asset management), 98
American Civil Liberties Union (ACLU), 78
Angular, 150
Anonymous, 78
application layer (Wireshark), 89
application logs, 111
AppLocker, 238
APT28, 78
apt-get dist-upgrade command, 219
apt-get update command, 219
ARP (Address Resolution Protocol), 33
asset management (AM), 98
assets, discovering vulnerable, 134–135
atomic rules, 60
audit logs, 246–248
auditing and logging, 156
Auditpol /set
  /Category:System
  /failure:disable command, 115
Auditpol /set
  /Category:System
  /failure:enable command, 114
authentication, 155
authentication, authorization, and
auditing (AAA), 98–99
authority, as a fundamental guide to
human behavior, 188, 189
Autoruns utility, 27
availability, in the CIA triad, 102

B
BackTrack, 205
BareTail, 116–117
baseline, 118–119
Bills, Robert (Master Sergeant), 173
blacklisting, 238
blue teamers, 125–126
Blue/Black Screen of Death (BSOD), 19
Bluetooth networks, 68
Brush, Douglas (cybersecurity
expert), 1
BSOD (Blue/Black Screen of Death), 19
Burp Suite, 156–163

C
cache, 7
cache poisoning, 7
Caïldini, Robert (professor), 188, 190
canonical name, 154
capture, 89–92
Center for Internet Security (CIS)
about, 31
controls and best practices,
  235–248
CentOS, 59, 61
certificate, 16
Chrome, Incognito mode in, 80
CIA triad, 102
Cid, Daniel (author), 57
CIS (Center for Internet Security)
about, 31
controls and best practices, 235–248
CIS Control 6, 109
“CIS Controls Implementation Guide
for Small- and Medium-Sized
Enterprises (SMEs),” 41
CLI (command-line interface), 112
client-owned networks, creating, 76
client-side exploit, 135
Clonezilla, 179–185
Closed port state, 34
Closed/filtered port state, 35
cmdlet, 113
CNAME (Domain Name Aliases), 154
colors, 92–93
command-line interface (CLI), 112

commands
  apt-get dist-upgrade, 219
  apt-get update, 219
  Auditpol /set
    /Category:System
    /failure:disable, 115
  Auditpol /set
    /Category:System
    /failure:enable, 114
  cp, 232
Get-EventLog -ComputerName
  PC1 -LogName System, 115
ipconfig, 4–5
ipconfig /all, 6
ipconfig /displaydns, 7
ipconfig /flushdns, 7
ipconfig /release, 6
ipconfig /renew, 6
netstat, 10–11, 13
netstat -ano, 121–122
ping, 3
sudo, 47
sudo add-apt-repository
ppa: mrazavi/openvas, 48
sudo apt-get install, 48
sudo apt-get install
python-software-properties, 47
sudo apt-get install
sqlite3, 47
sudo apt-get update, 48
sudo apt-get upgrade -y, 47
sudo openvas-nvt-sync, 48
/var/ossec/bin/ossec-control restart, 64
Common Vulnerability Scoring System (CVSS), 45
comparing hosts to _inf files, 178–179
composite rules, 60
Computer Fraud and Abuse Act (1984), 126
confidentiality, in the ICA triad, 102
configuration management
about, 165–166, 173–179
Clonezilla, 179–185
Configuration Manager, 237
configuring
Burp Suite Community, 157–161
Windows workstations, 241–246
Conrad, Eric (author), 236
consensus, as a fundamental guide
to human behavior, 188, 190
consistency, as a fundamental guide
to human behavior, 188, 189
Continuous Vulnerability Management, as a top six CISv7 basic control, 239–240
Controlled Use of Administrative Privileges, as a top six CISv7 basic control, 240–241
control-plane policing (CoPP), 22–23
CoPP (control-plane policing), 22–23
cp command, 232
creating
client-owned networks, 76
Clonezilla Live images, 182–184
Clonezilla Live USBs, 180–181
managed networks, 76–78
Metasploit projects, 133
site and scans, 53
systems in JumpCloud, 105–106
users in JumpCloud, 104
cross-site scripting (CSS), 157
cryptojacking, 167
CSS (cross-site scripting), 157
CVSS (Common Vulnerability Scoring System), 45
D
Damn Vulnerable Web App (DVWA), 144–146
Dashlane, 193
data link layer (Wireshark), 87
Data Protection Manager, 237
database, as a Syslog server component, 118
Davidoff, Sherri (CEO), 83
DC (domain controller), 44
Debian Linux, 128
default gateway, 6
DEFCON Social Engineering Capture the Flag (CTF), 188
defense in depth, 155–156
DeMeyer, Zavh, 103
Desktop Central, 168–172
DHCP (Dynamic Host Configuration Protocol), 6, 237
Diamond, Deidre (speaker), 191
discovering vulnerable assets, 134–135
Django, 150
DNS (Domain Name System), 7, 153–155
DNS spoofing, 7
DNS zone, 154–155
DNSdumpster, 151, 152–153
domain controller (DC), 44
Domain Name Aliases (CNAME), 154
Domain Name System (DNS), 7, 153–155
Donut day, 106–107
Doom (video game), 28–29
DuckDuckGo search engine, 81
DVWA (Damn Vulnerable Web App), 144–146
Dynamic Host Configuration Protocol (DHCP), 6, 237

E
802.11 standard, 67–70
Elastic search-Logstash-Kibana (ELK), 59
enabling Windows Master Control Panel, 28
encryption, 156
endpoint, 36
Endpoint Protection, 237
engine, 46
epmap/loc-srv service, 11–12
EternalBlue, 166–167
exception handling, 156
Expert Info tool (Wireshark), 94–95
exploit, 135
Extensible Markup Language (XML), 66
extracting keys for agents, 64

F
Federal Communications Commission (FCC), 67
Federal Desktop Core Configuration, 101
filter operators, 93
Filtered port state, 34
filters, 92–93
fingerprinting, 34
firewall, 122
firmware, 206
Foss, Greg (researcher), 189
Franz, Josh (security consultant), 98
FTP Bounce, 34

G
Gateway network, 74
Get-EventLog -ComputerName PC1 -LogName System command, 115
Git, 203
GitHub, 203
God mode (Doom game), 28–29
Google, 79–80, 115, 117
Gorbachev, Mikhail (Soviet Union General Secretary), 190
graphic user interface (GUI), 110
Greenbone Networks, 46
Greenbone Security Manager (GSM), 46
guest operating system, 207
GUI (graphic user interface), 110

H
hacktivist organizations, 78
Hadnagy, Chris (author)
about, 190
The Science of Human Hacking, 192
Hamachi, 72–78
hardware assets, inventory and control of, 236–238
Hashcat, 230–233
hashes, 230
Hawkins, Michael (security supervisor), 193
Health Insurance Portability and Accountability Act (HIPAA), 58
host operating system, 207
hosts
  comparing to _inf files, 178–179
  defined, 2
hotspot, 69
HTTP traffic, intercepting using
  Burp Suite, 161–162
HTTPS (Hypertext Transfer Protocol
  over TLS/SSL), 12
Hub-And-Spoke network, 74
human behavior, fundamentals
  guiding, 188–189
Hypertext Transfer Protocol over
  TLS/SSL (HTTPS), 12
hypervisor, 206–207

I
IANA (Internet Assigned Numbers
  Authority), 11
ICMP (Internet Control Message
  Protocol) echo request, 2, 9, 21–22
identity management (IM), 98
IEEE (Institute of Electrical and
  Electronics Engineers Standards
  Association), 67
IETF (Internet Engineering Task
  Force), 122
IM (identity management), 98
incident response (IR) plan, 58
Incognito mode, 80
inspection, 93–96
inSSIDer, 70–71
installable agents, 61
installing
  Burp Suite Community, 157–161
  Desktop Central, 168–169
  Desktop Central agents,
    170–172
Hamachi, 75
Linux OS Ubuntu 18.04 on
  Windows machines, 199–203
Metasploit, 128–135
Metasploit Community, 129–130
Nexpose Community, 51–52
7-Zip, 212–218
VM Workstation, 208–211
VMware Workstation Pro
  evaluation, 140
Wireshark, 84
Institute of Electrical and Electronics
  Engineers Standards Association
  (IEEE), 67
integrity, in the CIA triad, 102
Internet Assigned Numbers
  Authority (IANA), 11
Internet Control Message Protocol
  (ICMP) echo request, 2, 9, 21–22
Internet Engineering Task Force
  (IETF), 122
Internet of Things (IoT), 115
Internet Protocol (IP), 4
Inventory and Control of Hardware
  Assets, as a top six CISv7 basic
  control, 236–238
Inventory and Control of Software
  Assets, as a top six CISv7 basic
  control, 238–239
IoT (Internet of Things), 115
IP (Internet Protocol), 4
IP address, 3, 154, 237
IPConfig, 4–7
ipconfig /all command, 6
ipconfig command, 4–5
ipconfig /displaydns
  command, 7
ipconfig /flushdns command, 7
ipconfig /release command, 6
ipconfig /renew command, 6
IPv4 address, 115, 154
IPv6 address, 115
IR (incident response) plan, 58
ISO image, 47
J
John the Ripper, 229–230
JumpCloud, 103–108

K
Kali Linux
about, 128, 205–206
Hashcat, 230–233
John the Ripper, 229–230
Kismet, 227–228
MacChanger, 225–226
Maltego, 222–223
Nikto, 226–227
optimizing, 219–221
Recon-ng, 223–225
Sparta, 225
tools, 221–233
virtualization, 206–218
WiFite, 228–229
Keeper, 193
Kennedy, David (founder of
   TrustedSec and DerbyCon),
   190–191, 196
keyboard shortcuts (Wireshark), 86
keys, extracting for agents, 64
Kimball, Matt (analyst), 23
Kismet, 227–228
Klotz, Lt, General, 173

creating a managed network, 76–78
creating a site and scan, 53
creating Metasploit projects, 133
creating systems in JumpCloud,
   105–106
creating users in JumpCloud, 104
discovering vulnerable assets,
   134–135
enabling Windows Master Control
   Panel, 28
installing 7-Zip and using Kali
   Linux in VMware Workstation,
   212–218
installing and configuring Burp
   Suite Community, 157–161
installing and using Hamachi, 75
installing Desktop Central, 168–169
installing Desktop Central agents,
   170–172
installing Metasploit Community,
   129–130
installing Nexpose Community,
   51–52
installing the Linux OS Ubuntu
   18.04 on a Windows machine,
   199–203
installing VM Workstation, 208–211
installing VMware Workstation
   Pro evaluation, 140
IPConfig, 4–5
MTR (My TraceRoute), 23–24
NetStat, 13
NSLookup, 7–8
PathPing, 23
Ping (Packet InterNet Groper), 4
playing Metasploiter in VMware
   Pro, 141–143
PSR (Problem Steps Recorder), 20
PuTTY, 14–16
RELI, 18–19
reporting, 54
reviewing logs using Windows PowerShell, 113–114
securing and configuring a
Windows workstation, 241–246
Sysinternals, 25–26
Tracert, 9–10
using Burp Suite to intercept HTTP traffic, 161–162
validating targets, 151–153
Windows security logs, 111–112
Zenmap and Wireshark, 89–90
LastPass, 193
Lee, James (author), 165
leet speak, 13
LIDS (log-based intrusion detection system), 57–61
lifecycle
patch management, 166
of vulnerability management, 44
looking, as a fundamental guide to human behavior, 188, 189–190
Linux, Tracert and, 9
Linux Ubuntu 18.04, installing on Windows machines, 199–203
Lizard Squad, 78
LLC (Logical Link Control) layer (Wireshark), 87
log analysis, 65–66
log management
about, 109–110
BareTail, 116–117
SolarWinds Kiwi, 120–124
Syslog, 117–119
Windows Event Viewer, 110–112
Windows PowerShell, 112–115
log-based intrusion detection system (LIDS), 57–61
Logical Link Control (LLC) layer (Wireshark), 87
LogMeIn, 74
logs, reviewing using Windows PowerShell, 113–114
Long, Johnny (computer security expert), 165
loopback address, 3
Lyon, Gordon (author), 32

M
MAC (Media Access Control)
address, 33
MAC filtering, 69–70
MAC layer (Wireshark), 87
MacChanger, 225–226
Mac/Unix, Tracert and, 9
Maintenance, Monitoring, and
Analysis of Audit Logs, as a top six CISv7 basic control, 246–248
Maltego, 222–223
Malware Archaeology, 247
managed networks, creating, 76–78
ManageEngine Desktop Central, 168
management software, as a Syslog server component, 118
MD5 sum hash, 50–51
Media Access Control (MAC)
address, 33
Mesh network, 74
Metasploit Community, installing, 129–130
Metasploit Framework
about, 13, 125–126
creating projects, 133
gaining access, 135–139
installation, 128–135
Metasploitable2, 139–144
Meterpreter, 146
reconnaissance, 127–128
vulnerable Web services, 144–146
Metasploitable2, 139–144
MeteorJS, 150
Meterpreter, 146
MHTML file type, 21
Microsoft Management Console (MMC), 174–176
Microsoft TechNet, 24
Microsoft Windows
about, 17–18
MTR (My TraceRoute), 23–24
PathPing, 21–23
PSR (Problem Steps Recorder), 19–21
RELI, 18–19
Security Configuration and Analysis Configuration (SCA) tool, 174–176
Security Configuration Toolkit, 179
Sysinternals, 24–28
middleware, 148
Mitnick, Kevin (social engineer), 187
MMC (Microsoft Management Console), 174–176
Monero, 167
Moore, HD (Metasploit developer), 125
Morpho, 78
MTR (My TraceRoute), 23–24
multifactor authentication, 98
Mutilldae web application, 144

N
name servers (NS), 154
National Institute of Standards and Technology (NIST), 45, 101
National Security Agency (NSA), 166
National Vulnerability Database (NVD), 45
NetStat, 10–13
netstat -ano command, 121–122
netstat command, 10–11, 13
NetStumbler, 70
network analyzer, 83
network layer (Wireshark), 88
network mapping, 32–34
network scanning
about, 32
network mapping, 32–34
operating systems, 38
port scanning, 34–35
services running, 36–38
Network Vulnerability Tests (NVT), 46
networking and security tools
about, 1
IPConfig, 4–7
NetStat, 10–13
NSLookup, 7–8
Ping (Packet InterNet Groper), 1–4
PuTTY, 14–16
Tracert, 9–10
Nexpose Community, 50–55, 146
Nikto, 226–227
NIST (National Institute of Standards and Technology), 45, 101
Nmap
about, 31–32, 128
network mapping, 32–34
operating systems, 38
port scanning, 34–35
services running, 36–38
Zenmap, 39–41
nonrepudiation, 99
Notmyfault utility, 25, 28
NotPetya malware, 167
NS (name servers), 154
NSA (National Security Agency), 166
NSLookup, 7–8
NVD (National Vulnerability Database), 45
NVT (Network Vulnerability Tests), 46

O
OMP (OpenVAS Management Protocols), 46
Open port state, 34
Open Source Security (OSSEC)
about, 57
agents, 61–65
log analysis, 65–66
log-based intrusion detection system (LIDS), 57–61
Open Systems Interconnection (OSI) model, 84, 86–89
Open Web Application Security Project (OWASP), 129
Open/filtered port state, 35
open-source intelligence (OSINT), 192
OpenVAS (Open Vulnerability Assessment System), 46–50
OpenVAS Management Protocols (OMP), 46
OpenVAS Manager, 46
OpenVAS scanner, 46
OpenVAS Transfer Protocol (OTP), 46
operating systems
about, 38
LogMeIn and, 74–75
Operations Manager, 237
optimizing Kali Linux, 219–221
Orchestrator, 237
OSI Layer 8
about, 187
education, 193–195
human attacks, 192
human nature, 188–191
Social Engineer Toolkit, 195–203
OSI (Open Systems Interconnection) model, 84, 86–89
OSINT (open-source intelligence), 192
OSSEC (Open Source Security)
about, 57
agents, 61–65
log analysis, 65–66
log-based intrusion detection system (LIDS), 57–61
OSSEC Alert Data panel (ELK), 65
OSSEC Alerts Over Time panel (ELK), 65
OTP (OpenVAS Transfer Protocol), 46
OWASP (Open Web Application Security Project), 129

P
parsing, 119
password hygiene, 194
password manager, 193
patch management
about, 165–166
Clonezilla, 179–185
lifecycle of, 166
PathPing, 21–23
Payment Card Industry (PCI), 58
penetration testers, 125
personal package archive (PPA), 48
phishing, 192
physical layer (Wireshark), 87
Ping (Packet InterNet Groper), 1–4
ping command, 3
playing Metasploiter in VMware Pro, 141–143
PoLA (principle of least authority), 99
PoLP (principle of least privilege), 99–101
Port 20, 36
Port 21, 36
Port 22, 36
Port 23, 36
Port 25, 36
Port 53, 36
Port 80, 36
Port 110, 36
Port 123, 37
Index

Port 135, 11–12
Port 143, 37
Port 161, 37
Port 443, 12, 37, 48
Port 445, 37
Port 465, 37
Port 1433, 37
Port 3389, 37
Port 4444, 13
Port 31337, 13
port scanning, 34–35
ports. See also specific ports
defined, 11
overview of, 36–37
states of, 34
used by Kiwi Syslog Server, 120
PostgreSQL database, 128
PowerShell, 146
PPA (personal package archive), 48
predictive policing, 78
presentation layer (Wireshark), 89
principle of least authority (PoLA), 99
principle of least privilege (PoLP), 99–101
probe packets, 32
Process Explorer utility, 24, 26
PsExec utility, 24–25, 28
PsKill utility, 26
PsList utility, 26
PsLoggedOn utility, 27
PSR (Problem Steps Recorder), 19–21
PuTTY, 14–16
pwned, 107

R
Rapid7, 50, 125, 128, 141
Raw connection type (PuTTY), 15
Reagan, Ronald (U.S. President), 190
receiver, for wireless communication, 68
reciprocity, as a fundamental guide to human behavior, 188–189
Recon-ng, 223–224
red teamers, 125–126
RELI, 18–19
remote exploit, 135
Reporters Without Borders, 78
Request for Comments (RFC), 122
reviewing logs using Windows PowerShell, 113–114
Rlogin connection type (PuTTY), 15
Roberts, Chris (security strategist), 156
round-trip time (RTT), 22
router, for wireless communication, 68
Ruby, 128
Ruby on Rails, 150
rules
creating in Kiwi Syslog Server, 124
on firewalls, 122
type of, 60

S
SANS, 126, 236
SCA (Security Configuration and Analysis) tool, 174–176
scarcity, as a fundamental guide to human behavior, 188, 189
SCCM (System Center Configuration Manager), 237, 239
The Science of Human Hacking (Hadnagy), 192
Scope of Management (SOM), 169
SDelete utility, 27–28
SDLC (software development lifecycle), 148, 150
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, as a top six CISv7 basic control, 241–246
Secure Shell (SSH), 14
securing Windows workstations, 241–246
security and networking tools about, 1
IPConfig, 4–7
NetStat, 10–13
NSLookup, 7–8
Ping (Packet InterNet Groper), 1–4
PuTTY, 14–16
Tracert, 9–10
Security Configuration and Analysis (SCA) tool (Microsoft), 174–176
Security Configuration Toolkit (Microsoft), 179
security logs, 111–112
separation of duties (SoD), 101
Serial connection type (PuTTY), 15
Service Manager, 238
service set identifier (SSID), 69
services running, 36–38
session layer (Wireshark), 89
SET (Social Engineer Toolkit), 195–203
7-Zip, 212–218
Shadow Brokers hackers group, 166
shell, 112
Shodan, 153
single sign-on (SSO), 101–103
single-factor authentication, 98
Skoudis, Ed (speaker), 165
small office of home office (SOHO), 69
SMEs (subject-matter experts), 31, 67
SMTP mail exchange (MX), 154
sniffer, 83
SOA (Start of Authority), 154
Social Engineer Toolkit (SET), 195–203
social engineering, 188
SoD (separation of duties), 101
software assets, inventory and control of, 238–239
software development lifecycle (SDLC), 148, 150
software glue, 148
Software Restriction Policies (SRP), 238
SOHO (small office of home office), 69
SolarWinds Kiwi, 120–124
SOM (Scope of Management), 169
Sparta, 225
Spitzner, Lance (director of SANS Security Awareness), 193
splats, 19
SQL injection (SQLi), 146
SRP (Software Restriction Policies), 238
SSH (Secure Shell), 14
SSH connection type (PuTTY), 15
SSH key, 16
SSID (service set identifier), 69
SSO (single sign-on), 101–103
star icons (OpenVAS), 48–49
Start of Authority (SOA), 154
Stealth, 34
strings, 117
Strobe scan, 34
subject-matter experts (SMEs), 31, 67
sudo add-apt-repository ppa:mrazavi/openvas command, 48
sudo apt-get install command, 48
sudo apt-get install python-software-properties command, 47
sudo apt-get install sqlite3 command, 47
sudo apt-get update command, 48
sudo apt-get update -y command, 47
sudo apt-get upgrade -y
command, 47
sudo command, 47
sudo openvas-nvt-sync
command, 48
SYN scan, 34, 35
Sysinternals, 24–28
Syslog, 117–119
Syslog Listener, as a Syslog server
component, 118
syslog server, 118
System Center Configuration
Manager (SCCM), 237, 239
system logs, 111
systems, creating in JumpCloud,
105–106

T
tailored access operation (TAO), 78
targets, validating, 151–153
Task Manager, 26
tcp string, 92
Telnet, 137
Telnet connection type (PuTTY), 15
three-way handshake, 88
Top Alerts Per Agent panel (ELK), 65
tor (The Onion Router), 78–81
Total/Terrorism Information
Awareness, 78
traceroute tool, 9
Tracert, 9–10
transmitter, for wireless
communication, 68
transport layer (Wireshark), 88
troubleshooting Microsoft Windows,
17–29
two-factor authentication, 98

U
Unfiltered port state, 34
uniform resource locator (URL), 3
United States Computer Emergency
Readiness Team, 239
URL (uniform resource locator), 3
users, creating in JumpCloud, 104

V
validating targets, 151–153
Vanilla scan, 34
/var/ossec/bin/ossec-control
restart command, 64
Verizon Data Breach, 110
virtual machine, 207
Virtual Machine Manager, 238
virtual private network (VPN), 72–78
VirtualBox, 61
virtualization, 206–218
vishing, 192
VM Workstation, installing, 208–211
VMware, 139–140
VMware Workstation Pro
hypervisor, 140
voice phishing, 192
VPN (virtual private network), 72–78
vulnerability management
about, 43–46
continuous, 239–240
Nexpose Community, 50–55
OpenVAS (Open Vulnerability
Assessment System), 46–50
vulnerable Web services, 144–146

W
WannaCry ransomware, 166–167
WannaMine malware, 167
Wantegrity, 193–194
Wanteigrity, 193–194
WAP (wireless access point), 68
WARRIOR PRIDE, 78–79
Wayback Machine, 148
Web application security
about, 147–148
Burp Suite, 156–163
Defense in Depth, 155–156
Domain Name System (DNS), 153–155
information gathering, 151–153
Web development, 148–151
Web development, 148–151
websites
aboutface, 148
BareTail, 116
Burp Suite Community Edition, 157
“CIS Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs),” 41
Clonezilla, 180
creating, 53
Desktop Central, 168
DNSdumpster, 152
inSSIDer, 70
JumpCloud, 103
Kali image, 211
Malware Archaeology, 247
Metasploit, 128
Microsoft TechNet, 24
OSSEC, 61
Rapid7, 141
SANS, 236
7-Zip, 212
Shodan, 153
Statistica, 79
The Tor Project, 80
Ubuntu, 197
Verizon Data Breach, 110
VM Workstation, 208
VMware Workstation Pro, 140
Wantegrity, 193
Wayback Machine, 148
whatismyp, 161
Whois, 151
WinMTR, 23
Wireless Network Watcher, 71
Wireshark, 84, 89
Zenmap, 40
whitelisting, 238
Whois, 151–152
Wi-Fi hotspot, 69
Wi-Fi Protected Access version 2 (WPA2), 69
WiFite, 228–229
Wild West Hacking Fest (WWHF), 165
Windows (Microsoft)
about, 17–18
MTR (My TraceRoute), 23–24
PathPing, 21–23
PSR (Problem Steps Recorder), 19–21
RELI, 18–19
Security Configuration and Analysis (SCA) tool, 174–176
Security Configuration Toolkit, 179
Sysinternals, 24–28
Windows Event Viewer, 110–112
Windows Lock Screen policy, 107
Windows Master Control Panel, 28–29
Windows PowerShell, 112–115
Windows security logs, 111–112
Windows Server Update Services (WSUS), 168
Windows Subsystem for Linux (WSL), 195–196
wireless access point (WAP), 68
wireless communication
about, 67
802.11 standard, 67–70
Hamachi, 72–78
inSSIDer, 70–71
Tor (The Onion Router), 78–81
Wireless Network Watcher, 71–72
Wireless Network Watcher, 71–72
wireless personal area networks (WPANs), 68
Wireshark
about, 83–86
capture, 89–92
filters and colors, 92–93
inspection, 93–96
Open Systems Interconnection (OSI) model, 86–89
WPA2 (Wi-Fi Protected Access version 2), 69
WPANs (wireless personal area networks), 68
WSL (Windows Subsystem for Linux), 195–196
WSUS (Windows Server Update Services), 168
Wu, Magen (senior associate), 165–166
WWHF (Wild West Hacking Fest), 165
X
XMAS, 34
XML (Extensible Markup Language), 66
Y
YII, 150
Z
Zenmap, 32, 39–41, 89–90, 136
ZoomIt utility, 27