INDEX

Symbols
# prompt, 11
$ prompt, 11

A
access controls lists (ACLs), 94–95, 98–101
acl directive, 99
ad blocking, 105–116
    in Brave, 108
    browser plug-ins, 181–182
    in Google Chrome, 106–107
    in Mozilla Firefox, 107–108
    with Pi-Hole, 108–116
    configuring, 109–113
    configuring DNS on endpoints, 115–116
    using, 113–114
Adblock Plus, 106, 181–182
add-ons (extensions), 106
adduser command, 11
Advanced Package Tool (APT), 10–11, 127
 -aG (add group) parameter, 12
Airport Extreme base station, 137
Airport Time Capsule, 137
allowlists, 60, 98, 100
Amazon Alexa, 183
Amazon Web Services, 7
anonymize_headers directive, 97
antivirus farms, 120
AnyDesk, 68
Apache Traffic Server, 93
 -A parameter, 37, 39–40, 50
APT (Advanced Package Tool), 10–11, 127
asset lists
    creating, 56–57
    defined, 55
    MAC address filtering, 60
    network segmentation, 30
    Squid proxy, 93
    static IP addressing, 58
    template, 56
ASUS RT-AC5300 wireless router, xxii, 59, 59, 60, 61, 62–64
attack surface reduction
    configuring iptables, 39, 41
    defined, 34
    disabling IPv6, 48, 54, 111
    guest networks, 65
    Squid proxy, 95
    static IP addressing, 59
    third-party VPNs, 68
auth directive, 77, 80
Authy, 180
Automox, 128–130
Avast, 120–122

B
Backblaze, 143–144, 146
backup strategies, 131–147
    cloud backup solutions, 142–144
      Backblaze, 143–144, 146
      Carbonite, 144, 146
duplication, 138–142
    considerations, 141–142
    creating local backups, 139–140
    creating network backups, 140
    restoring backups, 141
    onsite vs. offsite, 133–134
restoring backups, 146
backup strategies *(continued)*
schedules, 133
storage, 134
testing backups, 146
Time Machine, 137–138, 146
types of backup, 132–133
virtual machine snapshots, 145–146
what to back up, 134
Windows Backup, 134–135
Windows Backup and Restore, 135–137, 146
basic input/output system (BIOS)
bootable USBs, 7
UEFI vs., 7
blacklists, 114
blocklists, 110
bogon networks, 48
bootable USBs
creating physical systems
on macOS, 6–7
on Windows, 6
defined, 6
using, 7
Brave, 108
broadcast address, 19
browser plug-ins, 181–183
Adblock Plus, 181–182
Ghostery, 182
HTTPS Everywhere, 182–183
brute-force attacks, 178

C
CA. See certificate authority
caching
defined, 92
disabling for specific sites, 101
Squid proxy, 93, 101
Can You Block It, 116
Carbonite, 143, 144, 146
CCMP (Counter Mode CBC-MAC Protocol), 63
CentOS Linux, 2
certificate authority (CA)
overview of, 69
setting up, 71–73
CIDR notation, 19
cipher directive, 77, 80
ClamAV, 122–124
CLI (command line interface)
utilities, 10
client directive, 73, 75
cloud backup solutions, 142–144
Backblaze, 143–144, 146
Carbonite, 144, 146
collection-status parameter, 141
collision domain, 26
command line interface (CLI)
utilities, 10
Command Prompt, 10
Common Name, 72–73, 75, 79
cnbytes tool, 38
CONNECT parameter, 95, 99
conrate tool, 38
cookies, 106
Counter Mode CBC-MAC Protocol (CCMP), 63
Crontab utility, 123, 140
cryptominers, 106
--ctstate argument, 38
curl tool, 42

data exfiltration, 151
data tables, 169
default gateway, 19
default route, 78, 84
defense-in-depth architecture, xx, 44
deluser command, 12
denylists, 60, 98–100
deny parameter, 99
DFIR Training, 184
DHCP. See Dynamic Host Configuration Protocol
dhcp-option directive, 77
differential backups, 132–133, 135
Diffie-Hellman key exchange, 74
digital certificates, 69
creating client certificate, 74–75
creating server certificate and key, 72–75
setting up certificate authority, 71–72
distributions, defined, 2, 127
dist-upgrade command, 15
Domain Name System (DNS)
  ad blocking, 108–110, 114–116
  configuring OpenVPN, 77
  configuring Wireguard, 85–86
  defined, 108
  Faster Than Light, 111, 112
  firewalls, 41
  identifying DNS server, 85
  testing VPNs, 89
dotted quad notation, 17
-D parameter, 37, 42
dpkg utility, 165
draw.io, 20
Dropbox, 28, 142, 174
dstdomain directive, 99
Dualcomm ETAP, 151
duplicity, 138–142
  considerations, 141–142
  creating local backups, 139–140
  creating network backups, 140
  restoring backups, 141
Dynamic Host Configuration Protocol (DHCP), 2
  ad blocking, 114–115
  checking IP addresses, 18, 30
  creating asset lists, 56
  disabling IPv6, 55
  static IP addressing, 57–59
E
EasyRSA
  installing, 70
  overview of, 69
easyrsa import-req command, 73
ECDSA key fingerprint, 14
endpoint detection and response (EDR) platforms, 162
endpoints (hosts). See also virtual private networks
defined, xx
firewalls, 33–34, 44
hostnames, 12
network devices, 26–27
network segmentation, 28, 31
static IP addressing, 57, 59
wireless authentication, 64–65
ETAP-2003, xxii
Etcher utility, 6–7
EternalBlue vulnerability, 48
ETOPEN ruleset, 158–159
--exclude argument, 141
ExpressVPN, 68
extensions (add-ons), 106
external hard drives, 134–138, 143–144
F
Faster Than Light (FTL) DNS, 111, 112
Fedora Linux, 2
file transfer, 22–23
find command, 102
fingerprinters, 106
firewalls, xxii, 33–51
  common protocols to block, 49
  configuring in OpenVPN, 78–79
  configuring in Wireguard, 84–85
defined, 33
iptables, 33, 35–44
  configuring, 38–42
  creating rules, 37–38
  installing, 36–44
  logging behavior, 43–44
pfSense, 33–34, 44–49
  creating rules, 48–49
  hardening, 47–48
  installing, 44–47
testing, 48–49
types of, 34–35
  hardware firewalls, 34
  host-based firewalls, 33, 34–35
  packet-filtering firewalls, 34
  perimeter firewalls, 34
  software firewalls, 34
  stateful firewalls, 34
  stateless firewalls, 34
Uncomplicated Firewall, 70, 84–85
--flush parameter, 40
Forcepoint, 93
forward chains, 35–36, 37, 39, 40
-F parameter, 40, 42
FreeBSD Unix, 44
FROM command, 169
FTL (Faster Than Light) DNS, 111, 112
full backups, 132–135
  duplicity, 138–140
  storage, 134
testing, 146
full backups (continued)
Windows Backup, 135
Windows Backup and Restore, 135–137

G
gen-dh argument, 74
Ghostery, 182
Google Authenticator, 180
Google Chrome
   ad blocking, 106–107
   incognito mode, 107
Google Chromecast, 28
Google Drive, 28, 142
Google Home, 183
Google Titan Key, 180
government information and identification, xix
Grafana, 153–154
group directive, 77, 80
guest networks, 28, 60–65

H
hardware firewalls, 34
hashing, 124–125
Have I Been Pwned service, 179
heuristics, 120
hexadecimal (hex), 19
h flag, 22
host-based firewalls, 33, 34–35
hostname command, 12–13, 163
hostnames
   asset lists, 56
   changing, 12–13
   checking, 12
   defined, 12
hosts. See endpoints; virtual private networks
HTTP
   firewalls, 42, 47
   Squid proxy, 109
http_access allow localnet directive, 95
http_access deny all directive, 95–96
http_access directive, 99
http_deny directive, 97
HTTPS
   firewalls, 42, 47
   Squid proxy, 95
HTTPS Everywhere, 182–183
hubs, 26
hypervisors
   creating Ubuntu virtual machines, 3–5
   defined, 3
   VirtualBox, 4–5, 8
   VMware Fusion, 4
   VMware Fusion Player for macOS, 4
   VMware Player for Windows, 3–4
   VMware Workstation, 3–4

I
icanhazip, 42
ICMP. See Internet Control Message Protocol
IDSs (intrusion detection systems), 151, 153
include directive, 99
incremental backups, 132–133, 138, 140
input chains, 35, 37, 39, 40, 42–43
intellectual property, xix
Intel Next Unit of Computing (NUC), 44, 154–155
Internet Control Message Protocol (ICMP)
   firewalls, 41
   output chains, 35
internet of things (IoT), 2, 183
   network maps, 22
   network segmentation, 25, 27–28, 31, 61
   wireless network security, 53, 61
Internet Protocol (IP). See also IP addresses
   defined, 17
   versions of, 17
Internet Protocol version 6 (IPv6). See also IP addresses
   disabling, 48, 54–55, 111
   ip6tables, 36
   overview of, 17
intranets, 27, 62
intrusion detection systems (IDSs), 151, 153
IoT. See internet of things
IP. See Internet Protocol
ip6tables, 36
IP addresses
  checking, 18–19
  on Linux, 19
  on Mac, 19
  on Windows, 18–19
  defined, 17
  dynamic, 57
  overview of, 17–18
  RFC1918 addresses, 48
  routers, 27
  static, 56–59, 69
-I parameter, 37
iptables firewall, 33, 35–44
  configuring, 38–42
  creating rules, 37–38
  installing, 36–44
  logging behavior, 43–44
  policy chains, 35–37, 39–43
  testing, 49–51
  VPs, 70
iptables-persistent tool, 36, 43
IPv6. See Internet Protocol version 6

J
  -j parameter, 38

K
  Kali Linux, 2
  key-direction directive, 80
  keyspace, 178
  Kibana, 161

L
  LANs (local area networks), 47, 53–55, 58
  Linux, 1–23
    configuration options, 9
    creating cloud-based systems, 7–8
    creating physical systems, 5–7
    creating virtual machines, 2–5
    hypervisors, 3
    VirtualBox, 4–5
    VMware Fusion, 4
    VMware Fusion Player for macOS, 4
    VMware Player for Windows, 3–4
    VMware Workstation, 3–4
  finalizing installation, 8–9
  hardening system, 9–16
  capturing VM configurations, 16
    defined, 9–10
    installing system packages, 10–11
    securing remote access, 13–16
    user management, 11–13
    operating systems, 2–8
    overview of, 2
    patches and updates, 126–127
  local area networks (LANs), 47, 53–55, 58
  loopback addresses, 38

M
  MAC addresses
    asset lists, 56–57
    filtering, 56, 59–60, 59
    network devices, 26–27, 55–56
    network maps, 21
  malware, 117–130
    Automox, 128–130, 129, 130
    Avast, 120–122, 121
    ClamAV, 122–124
    Microsoft Defender, 118–119
    patches and updates, 125–128
      Linux, 126–127
      macOS, 126–127
      Windows, 126
    tools, 119
      antivirus farms, 120
      heuristics, 120
      signatures, 120
    VirusTotal, 124–125
  manage_agents script, 162, 165–166
  managed switches, xxii, 28–29
  -m argument, 38
  metadata, 92–93
  MFA (multifactor authentication), 179–180
  Microsoft Authenticator, 180
  Microsoft Azure, 7
  Microsoft Defender, 118–119
  Microsoft Visio, 20
  mirror ports. See switch port analyzers
modems
   disabling IPv6, 55
network maps, 20–21
Mozilla Firefox, 107–108
multifactor authentication (MFA), 179–180

N
Nano, 14
NAS (network attached storage), xxi, 134, 137
NAT (network address translation), 17–18, 36, 54
netfilter command, 43
Netgate 1100 pfSense+, 44
Netgate 2100 Base pfSense+, 44
Netgear GS308E switch, xxii, 28–29
Netgear Nighthawk series routers, 54
Netgear SG-3100, xxii, 44, 57, 58
Netgear Switch Discovery Tool (NSDT), 30
network address translation (NAT), 17–18, 36, 54
network attached storage (NAS), xxi, 134, 137
network devices, 26
   hubs, 26
   limiting, 54–60
      creating asset lists, 56–57
      MAC address filtering, 59–60
      static IP addressing, 57–59
   routers, 27
   switches, 26–27
network maps
   creating, 20–22
   keeping up-to-date, 21
network monitoring and detection, 149–175
Security Onion, 153–175
   installing, 155–161
osquery, 166–172
   using as SIEM tool, 172–175
Wazuh, 161–166, 171–172
switch port analyzers, 152–153
traffic access points, 150–151
network segmentation, 25–31
   defined, 27
   Ethernet segmentation, 29–31
   logical segmentation, 28
network devices, 26
   hubs, 26
   routers, 27
   switches, 26–27
physical segmentation, 27
trust zones, 27–29, 31
wireless networks, 60–62
Network Time Protocol (NTP), 159
network topology, 17
   checking IP addresses, 18
      on Linux, 19
      on Mac, 19
      on Windows, 18–19
   creating network maps, xx–xxi, 20–22
   defined, xx
   transferring files, 22–23
NGINX, 93
Nmap tool, 49–50
NordVPN, 68
   -N parameter, 43
NSDT (Netgear Switch Discovery Tool), 30
NTP (Network Time Protocol), 159
NUC (Intel Next Unit of Computing), 44, 154–155

O
offsite backups, 133–134
1Password, 180
onsite backups, 133–134
OpenSSH, 79, 85
OpenVPN
   configuring, 76–82
      firewall, 78–79
      starting VPN, 79
      VPN client, 79–82
   creating client certificate, 74–75
   creating server certificate and key, 72–75
   creating VPNs with, 70–82
   EasyRSA, 69–70
   overview of, 68–69
   setting up certificate authority, 71–72
   openvpn --gen-key secret command, 74
organizational fields, 71
osquery, 159, 166–172
  defined, 153
  Fleet, 167–171
  installing on Linux, 168
  installing on macOS, 167–168
  installing on Windows, 167
  using, 168–171
output chains, 35, 37, 39, 40–43
P
-p 445 argument, 50
packet-filtering firewalls, 34
passwd command, 12
passwords and passphrases, 177–179
  changing default, 30, 178
  disallowing password authentication, 14
  password breach detection, 179
  password managers, 178
  remote access security, 13–14
  strong, 47, 177–178
  user management, 11–12
  wireless authentication, 62–63, 65
patches and updates, 125–128
  Linux, 126–127
  macOS, 126–127
  Windows, 126
perimeter firewalls, 34
personal identifiable information (PII), xix, 92, 100–101
P flag, 22
pfSense firewall, xxii, 44–49
  creating rules, 48–49
  DNS settings, 116
  hardening, 47–48
  installing, 44–47
    on Linux, 45–46
    on Mac, 45
    on Windows, 45
  testing, 49–51
  VPNs, 70
PHI (protected health information), xix
Pi-Hole, 77, 91
  ad blocking, 108–116
  configuring, 109–113
  configuring DNS on endpoints, 115–116
  using, 113–114
PII (personal identifiable information), xix, 92, 100–101
PKI (public key infrastructure), 69, 71–72
policy chains, 35–37, 39–43
potentially unwanted applications (PUAs), 123
PowerShell, 10
-P parameter, 39, 40
PPPoE, 46
--protect-args argument, 22
protected health information (PHI), xix
proxies, 91–104
  overview of, 91–92
Squid proxy
  blocking and allowing domains, 98–100
  configuring, 93–97
  configuring devices to use, 97
  defined, 91
  disabling caching for specific sites, 101
  protecting personal information, 100–101
  reports, 101–104
  testing, 98
PUAs (potentially unwanted applications), 123
public key infrastructure (PKI), 69, 71–72
R
-R argument, 37
Red Hat Linux, 2
redirect-gateway directive, 77
relational databases, 168
--remove-source-files argument, 22
request_header_access directive, 100
restore command, 141
RFC1918 addresses, 48
r flag, 22
root users. See superusers
routers
  disabling IPv6, 55
  overview of, 27
rsync command, 22–23, 73
Rufus utility, 6
rulesets, 34

S
SAE (Simultaneous Authentication of Equals), 63
Safe_ports directives, 95
Sanders, Chris, 184
SANS, 184
SARG (Squid Analysis Report Generator), 101–104
Secure Copy Protocol (SCP), 23
Secure File Transfer Protocol (SFTP), 23
secure shell (SSH), 13–16
firewalls, 39–40, 48, 78
installing, 11
SSH key pairs, 13–16
creating, 13–14
disabling root login, 14–15
disallowing password authentication, 14
duplicity backups, 140
login information, 15–16
passphrase, 13, 23
public key file, 13–14
remote login, 15–16
security information and event management (SIEM) tools
defined, 173
using Security Onion as, 172–175
Security Onion, 153–175
defined, 153
Grafana, 153–154
installing, 155–161
completing installation, 157–161
from ISO file, 155–156
manually, 155–156
Kibana, 161
minimum specifications, 154
osquery, 159, 166–172
defined, 153
installing on Linux, 168
installing on macOS, 167–168
installing on Windows, 167
using, 168–171
Strelka, 153, 159
suricata, 153
using as SIEM tool, 172–175
Wazuh, 159, 161–166
defined, 153
installing on Linux, 165–166
installing on macOS, 164–165
installing on Windows, 162–164
using, 171–172
zeek, 153, 158–160
SELECT command, 169
server argument, 73, 75
Server Message Block (SMB), 48–49
SFTP (Secure File Transfer Protocol), 23
SIEM tools. See security information and event management tools
signatures, 120
Simultaneous Authentication of Equals (SAE), 63
small networks, defined, xx
SMB (Server Message Block), 48–49
snapshots
defined, 16
removing old, 16
taking in VirtualBox, 16
taking in VMware, 16, 145–146
so-allow script, 164–165, 167–168
social media trackers, 106
software firewalls, 34
SPANs. See switch port analyzers
-s parameter, 39
split tunneling, 86
SQL (Structured Query Language), 168–169
Squid Analysis Report Generator (SARG), 101–104
Squid proxy, 91–104
blocking and allowing domains, 98–100
configuring, 93–97
configuring devices to use, 97
declared, 91
disabling caching for specific sites, 101
Pi-Hole and, 109
protecting personal information, 100–101
Index

reports, 101–104

testing, 98

SSH (secure shell). See secure shell

SSID, 63, 65

stateful firewalls, 34

stateless firewalls, 34

static leases, 56–59, 69

Strelka, 153, 159

Structured Query Language (SQL), 168–169

subnet mask, 19

subnets, 27

sudo command, 10–11

superusers (root users), 10–11

   disabling root login, 14–15

   securing remote access, 13

suricata, 153

switches
   managed, 28–29

   overview of, 26–27

switch port analyzers (SPANs; mirror ports)

   configuring, 152–153

   defined, 152

system images, 136

system repair discs, 136

T

tail command, 98

TAPs. See traffic access points

TCP. See Transmission Control Protocol

Teamviewer, 68

Temporal Key Integrity Protocol (TKIP), 62

Terminal, 10

TFPT (Trivial File Transfer Protocol), 174

Time Machine, 137–138, 146

tls-auth directive, 77, 80

traffic access points (TAPs), 150–151

   defined, xxii, 150

   intrusion detection systems and, 151

   placement, 150, 151

Transmission Control Protocol (TCP)

   common protocols to block, 49

   firewalls, 37–39, 41

   VPNs, 76

Trivial File Transfer Protocol (TFPT), 174

trust zones, 27–29, 31

tuples, 169

two-factor authentication (2FA), 179–180

U

Ubiquiti, xxii

Ubuntu Linux

   configuration options, 9

   creating cloud-based systems, 7–8

   creating physical systems, 5–7

   creating virtual machines, 2–5

   hypervisors, 3

   VirtualBox, 4–5

   VMware Fusion, 4

   VMware Fusion Player for macOS, 4

   VMware Player for Windows, 3–4

   VMware Workstation, 3–4
downloading, 2
editions of, 2

finalizing installation, 8–9

hardening system, 9–16

   capturing VM configurations, 16

   defined, 9–10

   installing system packages, 10–11

   securing remote access, 13–16

   user management, 11–13

overview of, 2

patches and updates, 126–127

Uncomplicated Firewall, 70, 78, 84–85

Wireguard, 82

u flag, 22

umask command, 83

Uncomplicated Firewall (UFW), 70, 78, 84–85

Unified Extensible Firmware Interface (UEFI), 6

update command, 127

upgrade command, 127

User Datagram Protocol (UDP)

   common protocols to block, 49

   defined, 38
User Datagram Protocol (UDP)
(continued)
output chains, 41
VPNs, 76
user directive, 77, 80
user management and security, 11–12,
177–183
adding users, 11–12
adding users to sudo group, 12
browser plug-ins, 181–183
deleting users, 12
internet of things, 183
multifactor authentication,
179–180
passwords and passphrases, 11–12,
177–179
resetting, 12
sudo privileges, 12
Ubuntu Linux, 11–13
usermod command, 12

V
VDI format, 5
verify parameter, 141
VHD format, 5
VirtualBox
creating Ubuntu virtual machines,
4–5
finalizing installation, 8
taking snapshots, 16
virtual local area networks (VLANs)
defined, 28
network segmentation, 28–31, 30
virtual machines (VMs)
capturing configurations, 16
taking snapshots in
VirtualBox, 16
taking snapshots in VMware,
16, 145–146
creating, 2–5
hypervisors, 3
VirtualBox, 4–5
VMware Fusion, 4
VMware Fusion Player for
macOS, 4
VMware Player for Windows,
3–4
VMware Workstation, 3–4
defined, xxi
finalizing installation, 8
host system, xxi
virtual private networks (VPNs), 67–89
drawbacks of third-party VPNs and
remote access services, 68
functions of, 67–68
input chains, 35
OpenVPN
creating VPNs with, 70–82
EasyRSA, 69
overview of, 68–69
testing, 89
Wireguard
creating VPNs with, 82–89
overview of, 69
VirusTotal (VT), 124–125
VLANs. See virtual local area networks
VMDK format, 5
VMs. See virtual machines
VMware Fusion, 4
VMware Fusion Player for macOS, 4
VMware Player for Windows, 3–4
VMware Snapshot Manager, 16,
145–146
VMware Workstation, 3–4
VPNs. See virtual private networks
VT (VirusTotal), 124–125
Vultr, 7–8

W
WannaCry ransomware, 48
Wazuh, 159, 161–166
defined, 153
installing on Linux, 165–166
installing on macOS, 164–165
installing on Windows, 162–164
using, 171–172
webcam covers, 180, 183
WEP (Wired Equivalent Privacy), 62
wg pubkey command, 83
WhatIsMyIP.com, 89
whitelists, 114
Wi-Fi Protected Access (WPA), 62–63
Wi-Fi Protected Access preshared key
(WPA-PSK), 63
Wi-Fi Protected Access version 2
(WPA2), 63
Wi-Fi Protected Access version 3  
(WPA3), 63
Windows Backup, 134–135
Windows Backup and Restore, 
135–137, 146
Wired Equivalent Privacy (WEP), 62
Wireguard
  configuring, 83–89
  firewall, 84–85
  identifying DNS server, 85
  starting VPN, 85
  VPN client, 85–89
  creating VPNs with, 82–89
  installing, 82
  overview of, 69
  setting up key pairs, 83
wireless authentication, 62–65
  WEP, 62
  WPA/WPA2, 62–63
  WPA3, 63–65
wireless network security, 53–65
  2.4 GHz and 5 GHz wireless 
bands, 60
  configuring wireless
    authentication, 62–65
    WEP, 62
    WPA/WPA2, 62–63
    WPA3, 63–65
disable IPv6, 54–55
hiding SSID, 65
limiting network devices, 54–60
  creating asset lists, 56–57
  MAC address filtering, 59–60
  static IP addressing, 57–59
network segmentation, 60–62
upgrading hardware, 54
wireless routers, xxii
WPA (Wi-Fi Protected Access), 62–63
WPA2 (Wi-Fi Protected Access 
version 2), 63
WPA3 (Wi-Fi Protected Access 
version 3), 63
WPA-PSK (Wi-Fi Protected Access 
preshared key), 63
X
  XProtect, 119
Y
  Yubikey, 180
  yum utility, 157
Z
  zeek, 153, 158–160
  Zenmap tool, 49–50