# CONTENTS IN DETAIL

**ACKNOWLEDGMENTS** **xvii**

**INTRODUCTION** **xix**

How to Use This Book: What to Expect . . . xx
Recommended (But Not Required) Knowledge . . . xxi
Recommended Hardware . . . xxi
Summary . . . xxiii

**1**
**GETTING STARTED WITH A BASE LINUX SYSTEM AND NETWORK MAP** **1**

Linux Operating Systems . . . 2
**#1: Creating an Ubuntu Virtual Machine** . . . 2
Hypervisor Options . . . 3
VMware Workstation and VMware Player for Windows . . . 3
VMware Fusion and VMware Fusion Player for macOS . . . 4
VirtualBox . . . 4
**#2: Creating a Physical Linux System** . . . 5
Bootable USB on Windows . . . 6
Bootable USB on macOS . . . 6
Using the Bootable USB . . . 7
**#3: Creating a Cloud-Based Linux System** . . . 7
Finalizing the Linux Installation . . . 8
Hardening Your Ubuntu System . . . 9
**#4: Installing System Packages** . . . 10
**#5: Managing Linux Users** . . . 11
**#6: Securing Remote Access** . . . 13
Generating SSH Keys . . . 13
Remote Login with SSH . . . 15
**#7: Capturing VM Configurations** . . . 16
Taking Snapshots in VMware . . . 16
Taking Snapshots in VirtualBox . . . 16
Network Topology . . . 17
**#8: Checking Your IP Address** . . . 18
On Windows . . . 18
On a Mac . . . 19
On Linux . . . 19
**#9: Creating a Network Map** . . . 20
**#10: Transferring Files** . . . 22
Summary . . . 23

**2**
**ARCHITECTING AND SEGMENTING YOUR NETWORK 25**

Network Devices . . . 26
Hubs . . . 26
Switches . . . 26
Routers . . . 27
Creating Trust Zones . . . 27
Physical Segmentation . . . 27
Logical Segmentation . . . 28
**#11: Segmenting Your Network** . . . 28
Ethernet Segmentation . . . 29
Summary . . . 31

**3**
**FILTERING NETWORK TRAFFIC WITH FIREWALLS 33**

Types of Firewalls . . . 34
iptables . . . 35
**#12: Installing iptables** . . . 36
iptables Firewall Rules . . . 37
Configuring iptables . . . 38
Logging iptables Behavior . . . 43
pfSense . . . 44
**#13: Installing the pfSense Firewall** . . . 45
Hardening pfSense . . . 47
pfSense Firewall Rules . . . 48
**#14: Testing Your Firewall** . . . 49
Summary . . . 51

**4**
**SECURING WIRELESS NETWORKS 53**

**#15: Disabling IPv6** . . . 54
**#16: Limiting Network Devices** . . . 55
Creating an Asset List . . . 56
Static IP Addressing . . . 57
MAC Address Filtering . . . 59
**#17: Segmenting Your Network** . . . 60
**#18: Configuring Wireless Authentication** . . . 62
WEP . . . 62
WPA/WPA2 . . . 62
WPA3 . . . 63
Summary . . . 65

**5**
**CREATING A VIRTUAL PRIVATE NETWORK 67**

Drawbacks of Third-Party VPNs and Remote Access Services . . . 68
OpenVPN . . . 68
EasyRSA . . . 69
Wireguard . . . 69

**#19: Creating a VPN with OpenVPN** . . . . . . . . . . 70
Set Up the Certificate Authority . . . . . . . . . . 71
Create the OpenVPN Server Certificate and Key . . . . . . . . . . 72
Configure OpenVPN . . . . . . . . . . 76
**#20: Creating a VPN with Wireguard** . . . . . . . . . . 82
Installing Wireguard . . . . . . . . . . 82
Set Up the Key Pairs . . . . . . . . . . 83
Configure Wireguard . . . . . . . . . . 83
Test Your VPN . . . . . . . . . . 89
Summary . . . . . . . . . . 89

**6**
**IMPROVING BROWSING AND PRIVACY WITH THE SQUID PROXY 91**

Why Use a Proxy? . . . . . . . . . . 92
**#21: Setting Up Squid** . . . . . . . . . . 93
Configuring Squid . . . . . . . . . . 93
Configuring Devices to Use Squid . . . . . . . . . . 97
Testing Squid . . . . . . . . . . 98
Blocking and Allowing Domains . . . . . . . . . . 98
Protecting Personal Information with Squid . . . . . . . . . . 100
Disabling Caching for Specific Sites . . . . . . . . . . 101
Squid Proxy Reports . . . . . . . . . . 101
Summary . . . . . . . . . . 104

**7**
**BLOCKING INTERNET ADVERTISEMENTS 105**

Browser-Level Ad Blocking . . . . . . . . . . 106
**#22: Blocking Ads in Google Chrome** . . . . . . . . . . 106
**#23: Blocking Ads in Mozilla Firefox** . . . . . . . . . . 107
**#24: Controlling Brave's Privacy Settings** . . . . . . . . . . 108
**#25: Blocking Ads with Pi-Hole** . . . . . . . . . . 108
Configure Pi-Hole . . . . . . . . . . 109
Using Pi-Hole . . . . . . . . . . 113
Configure DNS on Your Endpoints . . . . . . . . . . 115
Summary . . . . . . . . . . 116

**8**
**DETECTING, REMOVING, AND PREVENTING MALWARE 117**

Microsoft Defender for Windows . . . . . . . . . . 118
Choosing Malware Detection and Antivirus Tools . . . . . . . . . . 119
Antivirus Farm . . . . . . . . . . 120
Signatures and Heuristics . . . . . . . . . . 120
**#26: Installing Avast on macOS** . . . . . . . . . . 120
**#27: Installing ClamAV on Linux** . . . . . . . . . . 122
**#28: Using VirusTotal** . . . . . . . . . . 124
**#29: Managing Patches and Updates** . . . . . . . . . . 125
Windows Update . . . . . . . . . . 126
macOS Software Update . . . . . . . . . . 126
Linux Updates with apt . . . . . . . . . . 127

**#30: Installing Automox** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 128
Installing Automox. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 128
Using Automox . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 129
Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 130

## 9
## BACKING UP YOUR DATA 131

Backup Types . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 132
Devising a Backup Schedule . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 133
Onsite and Offsite Backups . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 133
What to Back Up and What Storage to Use . . . . . . . . . . . . . . . . . . . . . . . 134
**#31: Using Windows Backup** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 134
**#32: Using Windows Backup and Restore** . . . . . . . . . . . . . . . . . . . . . . 135
**#33: Using macOS Time Machine** . . . . . . . . . . . . . . . . . . . . . . . . . . . 137
**#34: Using Linux duplicity** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 138
Creating Local Backups with duplicity . . . . . . . . . . . . . . . . . . . . . . . . 139
Creating Network Backups with duplicity . . . . . . . . . . . . . . . . . . . . . . 140
Restoring duplicity Backups . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 141
Additional duplicity Considerations . . . . . . . . . . . . . . . . . . . . . . . . . . 141
Cloud Backup Solutions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 142
Backblaze . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 143
Carbonite. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 144
Virtual Machine Snapshots . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 145
Testing and Restoring Backups . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 146
Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 147

## 10
## MONITORING YOUR NETWORK WITH DETECTION AND ALERTING 149

Network Monitoring Methods . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 150
Network Traffic Access Points . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 150
Switch Port Analyzers . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 152
**#35: Configuring a SPAN Port** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 153
Security Onion. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 153
**#36: Building a Security Onion System** . . . . . . . . . . . . . . . . . . . . . . . . 154
Installing Security Onion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 155
**#37: Installing Wazuh** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 161
Installing Wazuh on Windows . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 162
Installing Wazuh on macOS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 164
Installing Wazuh on Linux . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 165
**#38: Installing osquery** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 166
Installing osquery on Windows . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 167
Installing osquery on macOS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 167
Installing osquery on Linux . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 168
A Network Security Monitoring Crash Course . . . . . . . . . . . . . . . . . . . . . . 168
Using osquery . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 168
Using Wazuh . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171
Using Security Onion as a SIEM Tool. . . . . . . . . . . . . . . . . . . . . . . . . . 172
Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 175

## 11
## TIPS FOR MANAGING USER SECURITY ON YOUR NETWORK 177

Passwords . . . . . . . . . . 177
    Password Managers . . . . . . . . . . 178
    Password Breach Detection . . . . . . . . . . 179
Multifactor Authentication . . . . . . . . . . 179
Browser Plug-ins . . . . . . . . . . 181
    Adblock Plus . . . . . . . . . . 181
    Ghostery . . . . . . . . . . 182
    HTTPS Everywhere . . . . . . . . . . 182
Internet of Things Considerations . . . . . . . . . . 183
Additional Resources . . . . . . . . . . 184
Summary . . . . . . . . . . 184

## INDEX 185