CONTENTS IN DETAIL

Acknowledgments

Introduction

How to Use This Book: What to Expect

Recommended (But Not Required) Knowledge

Recommended Hardware

Summary

1: Getting Started with a Base Linux System and Network Map

Linux Operating Systems

#1: Creating an Ubuntu Virtual Machine

Hypervisor Options

VMware Workstation and VMware Player for Windows

VMware Fusion and VMware Fusion Player for macOS

VirtualBox

#2: Creating a Physical Linux System

Bootable USB on Windows

Bootable USB on macOS

Using the Bootable USB

#3: Creating a Cloud-Based Linux System

Finalizing the Linux Installation

Hardening Your Ubuntu System

#4: Installing System Packages

#5: Managing Linux Users

#6: Securing Remote Access

Generating SSH Keys

Remote Login with SSH

#7: Capturing VM Configurations

Taking Snapshots in VMware

Taking Snapshots in VirtualBox

Network Topology

#8: Checking Your IP Address

On Windows

On a Mac

On Linux

#9: Creating a Network Map

#10: Transferring Files

Summary

2: Architecting and Segmenting Your Network

Network Devices

Hubs

Switches

Routers

Creating Trust Zones

Physical Segmentation

Logical Segmentation

#11: Segmenting Your Network

Ethernet Segmentation

Summary

3: Filtering Network Traffic with Firewalls

Types of Firewalls

iptables

#12: Installing iptables

iptables Firewall Rules

Configuring iptables

Logging iptables Behavior

pfSense

#13: Installing the pfSense Firewall

Hardening pfSense

pfSense Firewall Rules

#14: Testing Your Firewall

Summary

4: Securing Wireless Networks

#15: Disabling IPv6

#16: Limiting Network Devices

Creating an Asset List

Static IP Addressing

MAC Address Filtering

#17: Segmenting Your Network

#18: Configuring Wireless Authentication

WEP

WPA/WPA2

WPA3

Summary

5: Creating a Virtual Private Network

Drawbacks of Third-Party VPNs and Remote Access Services

OpenVPN

EasyRSA

Wireguard

#19: Creating a VPN with OpenVPN

Set Up the Certificate Authority

Create the OpenVPN Server Certificate and Key

Configure OpenVPN

#20: Creating a VPN with Wireguard

Installing Wireguard

Set Up the Key Pairs

Configure Wireguard

Test Your VPN

Summary

6: Improving Browsing and Privacy with the Squid Proxy

Why Use a Proxy?

#21: Setting Up Squid

Configuring Squid

Configuring Devices to Use Squid

Testing Squid

Blocking and Allowing Domains

Protecting Personal Information with Squid

Disabling Caching for Specific Sites

Squid Proxy Reports

Summary

7: Blocking Internet Advertisements

Browser-Level Ad Blocking

#22: Blocking Ads in Google Chrome

#23: Blocking Ads in Mozilla Firefox

#24: Controlling Brave’s Privacy Settings

#25: Blocking Ads with Pi-Hole

Configure Pi-Hole

Using Pi-Hole

Configure DNS on Your Endpoints

Summary

8: Detecting, Removing, and Preventing Malware

Microsoft Defender for Windows

Choosing Malware Detection and Antivirus Tools

Antivirus Farm

Signatures and Heuristics

#26: Installing Avast on macOS

#27: Installing ClamAV on Linux

#28: Using VirusTotal

#29: Managing Patches and Updates

Windows Update

macOS Software Update

Linux Updates with apt

#30: Installing Automox

Installing Automox

Using Automox

Summary

9: Backing Up Your Data

Backup Types

Devising a Backup Schedule

Onsite and Offsite Backups

What to Back Up and What Storage to Use

#31: Using Windows Backup

#32: Using Windows Backup and Restore

#33: Using macOS Time Machine

#34: Using Linux duplicity

Creating Local Backups with duplicity

Creating Network Backups with duplicity

Restoring duplicity Backups

Additional duplicity Considerations

Cloud Backup Solutions

Backblaze

Carbonite

Virtual Machine Snapshots

Testing and Restoring Backups

Summary

10: Monitoring Your Network with Detection and Alerting

Network Monitoring Methods

Network Traffic Access Points

Switch Port Analyzers

#35: Configuring a SPAN Port

Security Onion

#36: Building a Security Onion System

Installing Security Onion

#37: Installing Wazuh

Installing Wazuh on Windows

Installing Wazuh on macOS

Installing Wazuh on Linux

#38: Installing osquery

Installing osquery on Windows

Installing osquery on macOS

Installing osquery on Linux

A Network Security Monitoring Crash Course

Using osquery

Using Wazuh

Using Security Onion as a SIEM Tool

Summary

11: Tips for Managing User Security on Your Network

Passwords

Password Managers

Password Breach Detection

Multifactor Authentication

Browser Plug-ins

Adblock Plus

Ghostery

HTTPS Everywhere

Internet of Things Considerations

Additional Resources

Summary

Index