CONTENTS IN DETAIL

PREFACE **xv**

A Note on the Book's Exercises . . . xvi
Who This Book Is For . . . xvi
What's in the Book? . . . xvi

ACKNOWLEDGMENTS **xix**

1
AN INTRODUCTION TO CYBERSECURITY **1**

What Is Cybersecurity? . . . 2
Cybersecurity and Privacy . . . 2
What Cybersecurity Isn't . . . 3
Black Hats vs. White Hats . . . 4
Types of Black Hats . . . 4
Types of White Hats . . . 6
Exercise: Learning More About Cybersecurity and Threats . . . 10
Conclusion . . . 11

2
ATTACK TARGETS ON THE INTERNET **13**

How the Internet Works. . . . 14
TCP/IP: The Backbone of the Internet . . . 15
Public vs. Private Networks. . . . 16
How the Internet Looks to a Black Hat . . . 17
The Black Hat Attack Methodology . . . 18
Reconnaissance . . . 18
Weaponization. . . . 19
Delivery . . . 19
Exploitation and Installation . . . 20
Command and Control, and Attack on Objectives . . . 20
How Black Hats Find You . . . 21
Example 1: The Merger . . . 21
Example 2: Social Media Hunting . . . 21
How to Hide from Black Hats. . . . 22
The Internet Is Open . . . 22
The Internet Is Public . . . 23
The Internet Is Forever . . . 24
Exercise: Analyzing Your Network . . . 25
Network Command Line Tools . . . 25
Using Shodan . . . 31
Conclusion . . . 34

3
PHISHING TACTICS 35

What Is Phishing? 36
An Obvious Phish 36
Not All Phishing Is Obvious 37
Using Details for a More Convincing Phish 37
Vishing and Other Non-Email Phishing 38
How to Protect Yourself Against Phishing 38
How Black Hats Trick You with URLs 39
Typosquatting 39
Complex URLs and Redirects 40
Modifying DNS Records 40
Hoaxes 41
Why Black Hats Love Phishing 42
Think Twice to Avoid Phishing 42
Take an Alternate Route 43
Listen to Your Spidey Sense 43
Exercise: Analyzing a Phishing Email 43
Phishing Email Indicators 44
Header Analysis 46
URL Analysis 50
Conclusion 53

4
MALWARE INFECTIONS 55

What Is Malware? 56
Types of Malware 56
Viruses 56
Worms 57
Trojans 59
Ransomware 59
Spyware and Adware 60
Rootkits and Bootkits 60
Polymorphic Malware 61
How Black Hats Deploy Malware 62
How to Defend Against Malware 63
Exercise: Analyzing Malware and Managing Antivirus Settings 65
Analyzing Malware in Attachments 66
Reviewing Antivirus Settings 70
Conclusion 74

5
PASSWORD THEFTS AND OTHER ACCOUNT ACCESS TRICKS 75

Authentication 76
Types of Authentication 76
Multi-Factor Authentication 80
Authorization 81
Mandatory Access Control 82
Rule-Based Access Control 82
Role-Based Access Control 82
Attribute-Based Access Control 83

Discretionary Access Control 84
Accounting 84
Logging 85
Auditing. 86
Indicators of Attack 87
Exercise: Setting Up Accounts in Windows 10 and macOS 89
Windows 10 89
Access Control on macOS 98
Conclusion 101

6
NETWORK TAPPING 103

The Basics of Network Design 104
Attacking Your Network 106
How Black Hats See Your Traffic 106
Man-in-the-Middle Attacks 108
Denial of Service 110
Distributed Denial of Service. 110
Defense Against Network Attacks. 112
Firewalls 113
Intrusion Detection Systems 115
Intrusion Prevention Systems 116
Exercise: Setting Up Your Firewall 117
Windows 117
macOS 122
Conclusion 124

7
ATTACKS IN THE CLOUD 125

How Cloud Computing Works 126
Software as a Service 127
Platform as a Service. 127
Infrastructure as a Service 127
Security as a Service 128
Attacking the Cloud 128
Web Application Attacks 129
Defending the Cloud 133
Exercise: Performing SQL Injection on the Damn Vulnerable Web Application 134
Installing Docker and the DVWA. 134
Listing Users 137
Finding Database Table Names 138
Finding Passwords 139
Conclusion 139

8
WIRELESS NETWORK PIRATING 141

How Wireless Networks Work. 142
Wireless Standards 144
Wireless Security 145

Wireless Authentication 145
Wireless Encryption 146
Wireless Attacks 147
Rogue Access Points 147
Disassociation Attacks 148
Jamming 149
Setting Up a Wireless Network with Security in Mind 149
Exercise: Secure Your WAP 151
Setting Up Your Access Point 151
Setting Up Wireless Security 152
Enabling Filtering 154
Conclusion 156

9
ENCRYPTION CRACKING 157

What Is Cryptography? 158
What We Encrypt 158
Early Cryptography 159
Substitution Ciphers 159
Transposition Ciphers 160
Modern Cryptography 160
Symmetric Cryptography 161
Asymmetric Cryptography 163
Validating Public Keys 164
Hashing 166
What Happens When You Visit a Website? 167
How Black Hats Steal Your Keys 168
Cryptanalysis 169
Asymmetric Algorithm Attacks 170
Protecting Your Keys 170
How Black Hats Break Hashes 171
Salting Your Hashes 172
Exercise: Encrypting and Hashing Files 172
Encrypting and Hashing a File in Windows 10 172
Protecting Files Using macOS 174
Using ssh-keygen to Generate a Public Key (Windows 10 or macOS) 176
Conclusion 177

10
HOW TO DEFEAT BLACK HATS 179

What's the Worst That Could Happen? 180
Risks 180
Threats 182
Controls 183
Risk Management Programs 184
Putting It All Together 186
Exercise: Conducting a Risk Analysis 187
Farewell and Good Luck 188

INDEX 189