

CONTENTS IN DETAIL

ACKNOWLEDGMENTS	xvii
------------------------	-------------

INTRODUCTION	xix
---------------------	------------

Core Concepts of Offensive Security	xx
Ethical Implications of Red Teaming	xxi
Red Team Operations	xxii
What You'll Need to Follow Along	xxiii
How This Book Is Organized	xxiv

0	
TOOLS OF THE TRADECRAFT	xxvii

PART I: OFFENSIVE SECURITY DEVELOPMENT 1

1	
WEB APPLICATION EXPLOITS	3

Considering OST Best Practices	4
Building a Basic Phishing Page	5
Using Bootstrap and Font Awesome CSS for a Modern-Looking Site	5
Importing JavaScript Libraries via CDNs	6
Adding a Navigation Bar	8
Creating a Credential-Harvesting Form	11
Handling Credentials with JavaScript	13
Capturing Credentials Server-Side with PHP	16
Saving Credentials Without a Database	20
Creating a MySQL Database for Credential Storage	24
Building a Phishing Website with Database Credential Storage	28
Capturing Credentials with JavaScript	32
Exploring Common Tools for Phishing	37
The wget Tool	37
The goclone Tool	40
AI, LLMs, and ChatGPT	41
EAPHammer Captive-Portal Attacks	44
Summary	46
Going Further	47

2	
AUTHENTICATION ATTACKS	49

Creating a Target Application	50
Adding Authentication with PHP	50
Preventing SQL Injection	51

Implementing a Login Response	52
Following Best Practices for Credential Storage	54
Dissecting Requests with DevTools and Proxies	55
Identifying Data with Web Developer Tools	55
Intercepting Requests with a Web Proxy	56
Handling Proxied Requests with Python	57
Sending a Transparent Proxy Response	59
Building a Proxy Server	60
Brute-Forcing Credentials	64
Building the Login Request Script	64
Sending Authentication Data with Python	65
Automating the Brute-Force Behavior	67
Running a Brute-Force Attack	69
Creating a Web Application Password-Spraying Tool	70
Building the Password-Spraying Tool	70
Running the Password-Spraying Attack	73
Creating an SMB Brute-Forcing Attack Tool	73
Implementing the SMB Connection in Python	74
Validating Successful Authentication to SMB Shares	76
Automating the Brute-Force Attack for SMB Targets	77
Running a Brute-Force Attack Against SMB	79
Creating an SMB Password-Spraying Tool	80
Implementing a Password-Spraying Loop for SMB Targets	80
Running a Password Spray Against SMB	82
Common Tools for Authentication Attacks	83
Burp Suite	83
CrackMapExec	88
Spray Wrapper	92
Summary	95

3 CUSTOM MALWARE DEVELOPMENT AND DISTRIBUTION 97

Writing a Simple Program in Go	98
Setting Up the File-Reading Functionality	98
Setting Up the File-Writing Functionality	102
Combining the Reading and Writing Programs	103
Command Execution with the os Library	106
File Encryption with Go	110
Building the Encryption Tool	110
Building the Decryption Tool	116
Writing Custom Ransomware	120
Defining the Encrypt() and Decrypt() Functions	121
Scaffolding the Ransomware Logic	123
Defining the doEncrypt() and doDecrypt() Functions	125
Running the Ransomware Program	132
Writing a C2 Server in Python	133
Writing a C2 Implant	139
AI Malware Development	147
Summary	153

PART II: OFFENSIVE SECURITY ENGINEERING

155

4

AUTOMATING OFFENSIVE SECURITY INFRASTRUCTURE DEPLOYMENT

157

Tools and Technologies for Automation	158
AWS for Attack Infrastructure	159
Creating an AWS Service Account	161
A Terraform Primer	164
Terraform Server Instantiation	164
Terraform Network Access Control Lists	166
Terraform EC2 Instance Creation	167
Terraform Deployment	169
A Serverless Framework Primer	172
Boilerplate Serverless Application	173
Serverless Python Deployment Dependencies	174
Serverless Flask API Code	176
Serverless Framework Deployment	176
Summary	178

5

APPLYING NETWORK FUNDAMENTALS TO C2 IMPLEMENTATION

179

The OSI Model	180
Simple Target Network	180
Active Directory Target Network	182
Command-and-Control Network Flows	184
Bind Connections	185
Reverse Connections	185
Exploitation with the Metasploit Framework	186
Executing a Bind Shell	187
Executing a Reverse Shell	188
The Implications of Connection Directionality	189
Summary	190

6

REVERSE VPN TUNNELING

191

Reverse VPN Topology	191
Compromising a Server for Reverse VPN Tunneling	192
Using Reverse VPN Tunnel Path Topology	193
Configuring an EC2 Instance with Terraform	193
Accessing the Reverse VPN Server Instance	195
Simulating a Dropbox with Vagrant	195
Configuring OpenVPN with PiVPN	197
Selecting OpenVPN Configuration	197
Configuring OpenVPN Service and DNS	198
Setting OpenVPN Encryption Strength	199
Setting OpenVPN Post-Installation Configurations	200

Generating a VPN Certificate	200
Establishing a Reverse VPN Tunnel	202
A Note on Automation	203

7
MANAGING INFRASTRUCTURE FOR OFFENSIVE SECURITY OPERATIONS **205**

The Evolution of Infrastructure Operations	206
Getting Started with Salt Project	206
Configuring the Salt Project Terraform Server	207
Installing Salt Project	209
Configuring the Salt Fingerprint and IP Address	210
Linking the Minions to the Master	211
Running a Salt Project Command	212
Working with Salt States	212
Creating a Salt State	213
Observing Desired State	214
Salt Project as a C2 Server	219
Summary	219

PART III: OFFENSIVE SECURITY IN THE REAL WORLD **221**

8
EXPLOITATION WITH METASPLOIT **225**

Gaining Access: Configuring a C2 Server with Terraform	226
Spinning Up Metasploit on a C2 Server	229
Setting Up the Exploit Callback	230
Exploiting the Target	231
Maintaining Access: Establishing Persistence with Metasploit	233
Disabling Windows Defender	234
Generating a Meterpreter Payload	235
Configuring Persistence Options	236
Using the Metasploit Cleanup Automation Resource	239
Acting on the Objective: Extracting Credentials with Mimikatz	239
Summary	241

9
DEPLOYING A DROPBOX **243**

Configuring a Reverse VPN Dropbox	245
Using Empire on a C2 Server	246
Configuring Empire	248
Preparing an Empire C2 Stager	249
Post-Exploitation via Python Impacket	250
Deploying the Empire Stager	252
Establishing Persistence via Empire	252
Summary	254

10		
PHISHING ATTACK WITH C2 REDIRECTORS		255
Preparing Your Custom C2 Implant and Server		256
Implementing C2 Redirectors via the Serverless Framework		259
Creating an AWS Lambda Redirector in Python		260
Deploying the Redirector to AWS Lambda		262
Configuring a Custom C2 Server and Implant		263
Configuring Gophish		264
Creating the Gophish Service Account		265
Installing Gophish and Configuring Program Permissions		265
Setting Up an SSH Proxy to the Gophish Admin Panel		266
Configuring the Gophish Admin Panel		268
Creating and Launching a Gophish Campaign		269
Cloning a Landing Page		270
Creating a Phishing Email Template		273
Configuring an SMTP Sending Profile		276
Executing the Campaign		278
Phishing Payload Execution		280
Receiving a Custom Simple C2 Callback		282
Red Team Infrastructure in the Real World		283
11		
MULTIPLAYER C2 CONFIGURATION		285
teamserv for Cobalt Strike and Armitage		286
Starting the Metasploit Database and teamserv		286
Connecting to teamserv with Armitage		287
Interacting with teamserv		288
Multiplayer Mode for Sliver C2		289
Installing Sliver C2		290
Configuring Multiplayer Mode		291
Getting a Callback with Sliver C2		293
Other Multiuser C2 Tool Kits		295
Conclusion		295
RESOURCES		297
INDEX		299