CONTENTS IN DETAIL

FOREWORD TO THE FIRST EDITION **xv**

ACKNOWLEDGMENTS **xix**

SPECIAL THANKS **xxi**

INTRODUCTION **xxiii**

Why Do a Penetration Test? xxiv
Why Metasploit? xxiv
About This Book xxiv
What's New to This Edition xxvi
A Note on Ethics xxvii

1
THE ABSOLUTE BASICS OF PENETRATION TESTING **1**

The Phases of the PTES 2
  Preengagement Interactions 2
  Intelligence Gathering 2
  Threat Modeling 2
  Vulnerability Analysis 3
  Exploitation 3
  Post Exploitation 3
  Reporting 4
Types of Penetration Tests 4
  Overt 4
  Covert 5
Vulnerability Scanners 5
Installing Kali, Metasploit, and Metasploitable 5
Wrapping Up 6

2
METASPLOIT FUNDAMENTALS **7**

Terminology 8
  Exploit 8
  Payload 8
  Shellcode 8
  Module 8
  Listener 8
Metasploit Interfaces 9
  MSFconsole 9
  Resource Scripts 10
  Armitage and Cobalt Strike 10
Metasploit Utilities 11
  MSFvenom 11
  NASM Shell 12

Metasploit Pro 13
Wrapping Up 13

3
INTELLIGENCE GATHERING 15

Passive Information Gathering 16
Whois Lookups 16
Netcraft 17
DNS Analysis 18
Active Information Gathering 18
Port Scanning with Nmap 19
Port Scanning with Metasploit 25
Targeted Scanning 26
Scanning for Server Message Block 26
Hunting for Poorly Configured Microsoft SQL Servers 28
Scanning for S3 Buckets 29
Scanning for SSH Server Version 29
Scanning for FTP Servers 30
Sweeping for Simple Network Management Protocol 31
Writing a Custom Scanner 32
Wrapping Up 34

4
VULNERABILITY ANALYSIS 35

The Basic Vulnerability Scan 36
Scanning with Nexpose 37
Configuring Nexpose 37
Importing Reports into Metasploit 40
Running Nexpose in MSFconsole 40
Scanning with Nessus 42
Configuring Nessus 42
Creating Scans 43
Creating Scan Policies 44
Viewing Reports 44
Importing Results into Metasploit 45
Nessus Scanning in Metasploit 46
Specialty Vulnerability Scanners 48
Validating SMB Logins 48
Finding Scanners for Recent Exploits 49
Wrapping Up 50

5
THE JOY OF EXPLOITATION 51

Basic Exploitation 52
Searching for an Exploit 52
searchsploit 53
info 54

Selecting an Exploit 56
show payloads 57
show targets 58
set and unset 58
setg and unsetg 59
save 59
exploit 59
Exploiting a Windows Machine 60
Exploiting an Ubuntu Machine 63
Wrapping Up 65

6
METERPRETER 67

Compromising a Windows Virtual Machine 67
Port Scanning with Nmap 68
Brute-Forcing MySQL Server Authentication 68
Uploading User-Defined Functions 69
Basic Meterpreter Commands 70
Capturing Screenshots 71
Finding Platform Information 71
Capturing Keystrokes 71
Extracting Password Hashes 72
Passing the Hash 74
Mimikatz and Kiwi 75
Privilege Escalation 77
Lateral Movement Techniques 80
Token Impersonation 80
DCSync and Golden Ticket Attacks 82
Other Useful Meterpreter Commands 84
Enabling Remote Desktop Services 84
Viewing All Traffic on a Target 84
Scraping a System 85
Establishing Persistence 85
Manipulating Windows APIs with Railgun 88
Pivoting to Other Systems 90
Wrapping Up 90

7
AVOIDING DETECTION 91

Creating Stand-Alone Binaries with MSFvenom 92
Encoding with MSFvenom 94
Packing Executables 96
Custom Executable Templates 97
Launching Payloads Stealthily 98
Evasion Modules 99
Developing Custom Payloads 101
Generating Executables from Python Files 104
Wrapping Up 105

8
SOCIAL ENGINEERING 107

Updating and Configuring the Social-Engineer Toolkit 108
Spear-Phishing Attacks 109
    Setting Up an Email Server 109
    Sending Malicious Email 110
    Phishing with Gophish 112
Web Attacks 113
    Username and Password Harvesting 113
    Tabnabbing 116
    Bypassing Two-Factor Authentication 116
Infectious Media Generation Attacks 117
Wrapping Up 119

9
CLIENT-SIDE ATTACKS 121

Browser-Based Exploits 122
    Finding Exploits in Metasploit 123
    Automating Exploitation with AutoPwn2 125
    Finding Even More Recent Exploits 126
File-Format Exploits 126
    Exploiting Word Documents 126
    Sending Payloads 128
Wrapping Up 129

10
WIRELESS ATTACKS 131

Connecting to Wireless Adapters 132
Monitoring Wi-Fi Traffic 132
Deauth and DoS Attacks 133
Capturing and Cracking Handshakes 135
Evil Twin Attacks 136
Sniffing Traffic with Metasploit 138
Harvesting Credentials with the Wi-Fi Pineapple 139
Wrapping Up 143

11
AUXILIARY MODULES 145

Exploring Auxiliary Modules 145
Searching for HTTP Modules 148
Creating an Auxiliary Module 149
    Writing the Module 149
    Running the Module 151
    Debugging the Module 153
Wrapping Up 154

12
PORTING EXPLOITS TO THE FRAMEWORK 155

Assembly Language Basics 156
    EIP and ESP Registers 156

The JMP Instruction Set . . . 156
NOPs and NOP Slides . . . 156
Disabling Protections . . . 156
Porting Buffer Overflows . . . 157
Stripping Existing Exploits . . . 159
Configuring the Exploit Definition . . . 160
Testing the Base Exploit . . . 161
Implementing Features of the Framework . . . 162
Adding Randomization . . . 163
Removing the NOP Slide . . . 163
Removing the Dummy Shellcode . . . 164
Porting an SEH Overwrite Exploit . . . 166
Wrapping Up . . . 171

13
BUILDING YOUR OWN MODULES 173

Getting Command Execution on MS SQL . . . 173
Enabling Administrator-Level Procedures . . . 174
Running the Module . . . 175
Exploring the Module Code . . . 176
Creating a New Module . . . 178
Editing an Existing Module . . . 178
Running the Shell Exploit . . . 180
Defining the Exploit . . . 180
Uploading PowerShell Scripts . . . 181
Running the Exploit . . . 183
Wrapping Up . . . 184

14
CREATING YOUR OWN EXPLOITS 185

The Art of Fuzzing . . . 186
Downloading the Test Application . . . 186
Writing the Fuzzer . . . 186
Testing the Fuzzer . . . 187
Controlling the Structured Exception Handler . . . 190
Hopping Around Restrictions . . . 192
Getting a Return Address . . . 194
Including Backward Jumps and Near Jumps . . . 197
Adding a Payload . . . 198
Bad Characters and Remote Code Execution . . . 198
Wrapping Up . . . 201

15
A SIMULATED PENETRATION TEST 203

Preengagement Interactions . . . 204
Intelligence Gathering . . . 204
Threat Modeling . . . 205
Exploitation . . . 206
Executing the Exploit . . . 207
Establishing Persistence . . . 207

Post Exploitation . . . 208
Scanning the Linux System . . . 209
Identifying Vulnerable Services . . . 211
Attacking Apache Tomcat . . . 212
Attacking Obscure Services . . . 214
Covering Your Tracks . . . 215
Wrapping Up . . . 217

16
PENTESTING THE CLOUD 219

Cloud Security Basics . . . 220
Identity and Access Management . . . 220
Serverless Functions . . . 221
Storage . . . 222
Docker Containers . . . 223
Setting Up Cloud Testing Environments . . . 225
Container Takeovers . . . 226
Escaping Docker Containers . . . 229
Kubernetes . . . 231
Wrapping Up . . . 231

A
CONFIGURING YOUR LAB ENVIRONMENT 233

x86 and AMD64 . . . 234
ARM and Apple Silicon . . . 235
Installing Kali Meta Packages . . . 236

B
CHEAT SHEET 239

MSFconsole . . . 239
Meterpreter . . . 240
MSFvenom . . . 242
Meterpreter Post Exploitation . . . 242

INDEX 245