

# Contents

Preface.....	i
Notes and Disclaimer.....	iii
Introduction.....	v
Penetration Testing Teams vs Red Teams.....	vi
Summary.....	ix
1 Pregame - The Setup.....	1
Assumed Breach Exercises.....	3
Setting Up Your Campaign.....	3
Setting Up Your External Servers.....	4
Tools of the Trade.....	7
Metasploit Framework.....	7
Cobalt Strike.....	8
PowerShell Empire.....	12
dnscat2.....	15
p0wnedShell.....	21
Pupy Shell.....	21
PoshC2.....	21
Merlin.....	22
Nishang.....	22
Conclusion.....	22
2 Before the Snap - Red Team Recon.....	23
Monitoring an Environment.....	24
Regular Nmap Diffing.....	24
Web Screenshots.....	25
Cloud Scanning.....	27
Network/Service Search Engines.....	28
Manually Parsing SSL Certificates.....	30
Subdomain Discovery.....	32
Github.....	35
Cloud.....	37
Emails.....	41
Additional Open Source Resources.....	42
Conclusion.....	43
3 The Throw - Web Application Exploitation.....	44
Bug Bounty Programs.....	45
Web Attacks Introduction - Cyber Space Kittens.....	47
The Red Team Web Application Attacks.....	48
Chat Support Systems Lab.....	49
Cyber Space Kittens: Chat Support Systems.....	51
Setting Up Your Web Application Hacking Machine.....	51
Analyzing a Web Application.....	52
Web Discovery.....	52

Cross-Site Scripting XSS.....	53
Blind XSS .....	59
DOM Based XSS.....	60
Advanced XSS in NodeJS.....	61
XSS to Compromise .....	67
NoSQL Injections .....	68
Deserialization Attacks.....	72
Template Engine Attacks - Template Injections.....	77
JavaScript and Remote Code Execution.....	86
Server Side Request Forgery (SSRF).....	89
XML eXternal Entities (XXE) .....	94
Advanced XXE - Out Of Band (XXE-OOB).....	96
Conclusion.....	98
4 The Drive - Compromising the Network.....	99
Finding Credentials from Outside the Network.....	100
Advanced Lab.....	104
Moving Through the Network.....	104
Setting Up the Environment - Lab Network.....	105
On the Network with No Credentials.....	106
Responder .....	107
Better Responder (MultiRelay.py).....	109
PowerShell Responder.....	111
User Enumeration Without Credentials.....	111
Scanning the Network with CrackMapExec (CME).....	112
After Compromising Your Initial Host.....	113
Privilege Escalation.....	115
Privilege Escalation Lab.....	119
Pulling Clear Text Credentials from Memory.....	120
Getting Passwords from the Windows Credential Store and Browsers .....	123
Getting Local Creds and Information from OSX.....	126
Living Off of the Land in a Windows Domain Environment .....	128
Service Principal Names.....	128
Querying Active Directory .....	129
Bloodhound/Sharphound.....	134
Moving Laterally - Migrating Processes.....	139
Moving Laterally Off Your Initial Host .....	141
Lateral Movement with DCOM.....	143
Pass-the-Hash.....	146
Gaining Credentials from Service Accounts.....	148
Dumping the Domain Controller Hashes.....	151
Lateral Movement via RDP over the VPS.....	153
Pivoting in Linux.....	155
Privilege Escalation.....	156
Linux Lateral Movement Lab.....	159

Attacking the CSK Secure Network .....	160
Conclusion .....	172
5 The Screen - Social Engineering.....	173
Building Your Social Engineering (SE) Campaigns.....	174
Doppelganger Domains .....	174
How to Clone Authentication Pages.....	175
Credentials with 2FA .....	176
Phishing .....	177
Microsoft Word/Excel Macro Files .....	178
Non-Macro Office Files - DDE .....	183
Hidden Encrypted Payloads.....	184
Exploiting Internal Jenkins with Social Engineering .....	185
Conclusion.....	190
6 The Onside Kick - Physical Attacks .....	191
Card Reader Cloners.....	192
Physical Tools to Bypass Access Points.....	193
LAN Turtle (lanturtle.com).....	194
Packet Squirrel.....	201
Bash Bunny .....	203
Breaking into Cyber Space Kittens.....	203
QuickCreds.....	206
BunnyTap .....	206
WiFi .....	208
Conclusion.....	210
7 The Quarterback Sneak - Evading AV and Network Detection.....	211
Writing Code for Red Team Campaigns.....	212
The Basics Building a Keylogger .....	212
Setting up your environment .....	212
Compiling from Source.....	213
Sample Framework .....	213
Obfuscation.....	217
THP Custom Droppers .....	220
Shellcode vs DLLs.....	221
Running the Server.....	221
Client.....	222
Configuring the Client and Server.....	222
Adding New Handlers .....	223
Further Exercises.....	223
Recompiling Metasploit/Meterpreter to Bypass AV and Network Detection .....	224
How to Build Metasploit/Meterpreter on Windows: .....	225
Creating a modified Stage 0 Payload:.....	226
SharpShooter.....	228
Application Whitelisting Bypass.....	230

Code Caves.....	232
PowerShell Obfuscation.....	233
PowerShell Without PowerShell:.....	236
HideMyPS .....	237
Conclusion.....	239
8 Special Teams - Cracking, Exploits, and Tricks.....	240
Automation .....	241
Automating Metasploit with RC scripts .....	241
Automating Empire .....	242
Automating Cobalt Strike.....	243
The Future of Automation .....	243
Password Cracking.....	243
Gotta Crack Em All - Quickly Cracking as Many as You Can.....	247
Cracking the CyberSpaceKittens NTLM hashes: .....	247
Creative Campaigns.....	251
Disabling PS Logging.....	252
Windows Download File from Internet Command Line.....	252
Getting System from Local Admin.....	253
Retrieving NTLM Hashes without Touching LSASS.....	254
Building Training Labs and Monitor with Defensive Tools .....	254
Conclusion.....	255
9 Two-Minute Drill - From Zero to Hero.....	256
10 Post Game Analysis - Reporting .....	262
Continuing Education.....	267
About the Author.....	270
Special Thanks.....	271