

CONTENTS IN DETAIL

FOREWORD by HD Moore	xv
-----------------------------	-----------

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

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

Who This Book Is For	xx
What This Book Isn't	xx
Why Use Go for Hacking?	xxi
Why You Might Not Love Go	xxi
Chapter Overview	xxii

1	
GO FUNDAMENTALS	1

Setting Up a Development Environment	1
Downloading and Installing Go	2
Setting GOROOT to Define the Go Binary Location	2
Setting GOPATH to Determine the Location of Your Go Workspace	2
Choosing an Integrated Development Environment	3
Using Common Go Tool Commands	6
Understanding Go Syntax	10
Data Types	10
Control Structures	14
Concurrency	16
Error Handling	17
Handling Structured Data	18
Summary	20

2	
TCP, SCANNERS, AND PROXIES	21

Understanding the TCP Handshake	22
Bypassing Firewalls with Port Forwarding	23
Writing a TCP Scanner	23
Testing for Port Availability	24
Performing Nonconcurrent Scanning	25
Performing Concurrent Scanning	26
Building a TCP Proxy	32
Using io.Reader and io.Writer	32
Creating the Echo Server	35
Improving the Code by Creating a Buffered Listener	37
Proxying a TCP Client	39
Replicating Netcat for Command Execution	40
Summary	44

3	HTTP CLIENTS AND REMOTE INTERACTION WITH TOOLS	45
HTTP Fundamentals with Go		46
Calling HTTP APIs		46
Generating a Request		48
Using Structured Response Parsing		48
Building an HTTP Client That Interacts with Shodan		51
Reviewing the Steps for Building an API Client		51
Designing the Project Structure		52
Cleaning Up API Calls		53
Querying Your Shodan Subscription		54
Creating a Client		58
Interacting with Metasploit		59
Setting Up Your Environment		59
Defining Your Objective		61
Retrieving a Valid Token		62
Defining Request and Response Methods		63
Creating a Configuration Struct and an RPC Method		64
Performing Remote Calls		64
Creating a Utility Program		67
Parsing Document Metadata with Bing Scraping		68
Setting Up the Environment and Planning		69
Defining the metadata Package		71
Mapping the Data to Structs		72
Searching and Receiving Files with Bing		73
Summary		76
4	HTTP SERVERS, ROUTING, AND MIDDLEWARE	77
HTTP Server Basics		78
Building a Simple Server		78
Building a Simple Router		79
Building Simple Middleware		80
Routing with the gorilla/mux Package		81
Building Middleware with Negroni		83
Adding Authentication with Negroni		86
Using Templates to Produce HTML Responses		88
Credential Harvesting		90
Keylogging with the WebSocket API		93
Multiplexing Command-and-Control		98
Summary		102
5	EXPLOITING DNS	103
Writing DNS Clients		104
Retrieving A Records		104
Processing Answers from a Msg struct		106
Enumerating Subdomains		107

Writing DNS Servers	117
Lab Setup and Server Introduction	118
Creating DNS Server and Proxy	121
Summary	130

6 INTERACTING WITH SMB AND NTLM 131

The SMB Package	132
Understanding SMB	132
Understanding SMB Security Tokens	133
Setting Up an SMB Session	134
Using Mixed Encoding of Struct Fields	135
Understanding Metadata and Referential Fields	138
Understanding the SMB Implementation	139
Guessing Passwords with SMB	146
Reusing Passwords with the Pass-the-Hash Technique	147
Recovering NTLM Passwords	150
Calculating the Hash	150
Recovering the NTLM Hash	150
Summary	151

7 ABUSING DATABASES AND FILESYSTEMS 153

Setting Up Databases with Docker	154
Installing and Seeding MongoDB	154
Installing and Seeding PostgreSQL and MySQL Databases	156
Installing and Seeding Microsoft SQL Server Databases	157
Connecting and Querying Databases in Go	158
Querying MongoDB	158
Querying SQL Databases	160
Building a Database Miner	161
Implementing a MongoDB Database Miner	164
Implementing a MySQL Database Miner	166
Pillaging a Filesystem	170
Summary	172

8 RAW PACKET PROCESSING 173

Setting Up Your Environment	174
Identifying Devices by Using the pcap Subpackage	174
Live Capturing and Filtering Results	175
Sniffing and Displaying Cleartext User Credentials	178
Port Scanning Through SYN-flood Protections	180
Checking TCP Flags	180
Building the BPF Filter	181
Writing the Port Scanner	182
Summary	185

9	WRITING AND PORTING EXPLOIT CODE	187
Creating a Fuzzer		188
Buffer Overflow Fuzzing		188
SQL Injection Fuzzing		192
Porting Exploits to Go		196
Porting an Exploit from Python		197
Porting an Exploit from C		201
Creating Shellcode in Go		213
C Transform		213
Hex Transform		214
Num Transform		214
Raw Transform		215
Base64 Encoding		215
A Note on Assembly		216
Summary		216
10	GO PLUGINS AND EXTENDABLE TOOLS	217
Using Go's Native Plug-in System		218
Creating the Main Program		219
Building a Password-Guessing Plug-in		222
Running the Scanner		224
Building Plug-ins in Lua		225
Creating the head() HTTP Function		226
Creating the get() Function		227
Registering the Functions with the Lua VM		229
Writing Your Main Function		230
Creating Your Plug-in Script		231
Testing the Lua Plug-in		232
Summary		232
11	IMPLEMENTING AND ATTACKING CRYPTOGRAPHY	233
Reviewing Basic Cryptography Concepts		234
Understanding the Standard Crypto Library		235
Exploring Hashing		235
Cracking an MD5 or SHA-256 Hash		236
Implementing bcrypt		237
Authenticating Messages		239
Encrypting Data		242
Symmetric-Key Encryption		242
Asymmetric Cryptography		245
Brute-Forcing RC2		252
Getting Started		252
Producing Work		255
Performing Work and Decrypting Data		257
Writing the Main Function		258
Running the Program		260
Summary		261

12		
WINDOWS SYSTEM INTERACTION AND ANALYSIS		263
The Windows API's <code>OpenProcess()</code> Function		263
The <code>unsafe.Pointer</code> and <code>uintptr</code> Types.		266
Performing Process Injection with the <code>syscall</code> Package.		268
Defining the Windows DLLs and Assigning Variables		270
Obtaining a Process Token with the <code>OpenProcess</code> Windows API.		271
Manipulating Memory with the <code>VirtualAllocEx</code> Windows API		273
Writing to Memory with the <code>WriteProcessMemory</code> Windows API		274
Finding <code>LoadLibraryA</code> with the <code>GetProcessAddress</code> Windows API		275
Executing the Malicious DLL Using the <code>CreateRemoteThread</code> Windows API.		275
Verifying Injection with the <code>WaitforSingleObject</code> Windows API.		276
Cleaning Up with the <code>VirtualFreeEx</code> Windows API.		277
Additional Exercises		278
The Portable Executable File		279
Understanding the PE File Format		279
Writing a PE Parser		280
Additional Exercises		289
Using C with Go		290
Installing a C Windows Toolchain.		290
Creating a Message Box Using C and the Windows API.		290
Building Go into C		291
Summary		293
13		
HIDING DATA WITH STEGANOGRAPHY		295
Exploring the PNG Format		296
The Header		296
The Chunk Sequence.		297
Reading Image Byte Data		298
Reading the Header Data		298
Reading the Chunk Sequence		299
Writing Image Byte Data to Implant a Payload		302
Locating a Chunk Offset.		302
Writing Bytes with the <code>ProcessImage()</code> Method		302
Encoding and Decoding Image Byte Data by Using XOR		307
Summary		312
Additional Exercises		312
14		
BUILDING A COMMAND-AND-CONTROL RAT		315
Getting Started		316
Installing Protocol Buffers for Defining a gRPC API.		316
Creating the Project Workspace		317
Defining and Building the gRPC API		317
Creating the Server		319
Implementing the Protocol Interface		319
Writing the <code>main()</code> Function		322
Creating the Client Implant		323

Building the Admin Component	325
Running the RAT.	326
Improving the RAT	326
Encrypt Your Communications	327
Handle Connection Disruptions.	327
Register the Implants	327
Add Database Persistence	328
Support Multiple Implants.	328
Add Implant Functionality.	329
Chain Operating System Commands.	329
Enhance the Implant's Authenticity and Practice Good OPSEC	329
Add ASCII Art	329
Summary	330

INDEX