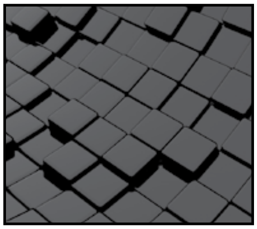

Kali Linux Penetration Testing Bible

Gus Khawaja

WILEY

Copyright © 2021 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-71908-3
ISBN: 978-1-119-71964-9 (ebk)
ISBN: 978-1-119-71907-6 (ebk)

Manufactured in the United States of America

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2021904285

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. Linux is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

About the Author

Gus Khawaja is an expert in application security and penetration testing. He is a cybersecurity consultant in Montreal, Canada, and has a depth of experience working with organizations to protect their assets from cyberattacks. He is a published author and an online instructor in the field of cybersecurity.

About the Technical Editor

Corey Ball is a cybersecurity expert with more than 10 years of IT and cybersecurity leadership experience. He specializes in penetration testing APIs, web applications, and networks. He currently has more than 10 cybersecurity certifications including the OSCP, CISSP, CISM, and CCISO. Corey is a cybersecurity career mentor for Cybrary and the author of the upcoming book *Hacking APIs*. He has a bachelor of arts in English and philosophy from CSU Sacramento.

Acknowledgments

I have been fortunate to share my knowledge and expertise with my audience through Wiley. I hope this knowledge will make you the best expert in your career as a penetration tester.

I am especially grateful to my family who supported me to deliver 18 full chapters of this book. A full year of nonstop writing takes a lot of guts, but it's here for you, so take advantage of it.

I am blessed that I have background experience in programming that helped me a lot in my career as a penetration tester and as an application security expert. You will realize that these days, having skills in web application architecture will allow you to master this career.

Finally, I would like to thank Wiley's team members who supported me during the journey of writing this amazing book. Without this support, this book would never have seen the light of day!

Contents at a Glance

Introduction		xx
Chapter 1	**Mastering the Terminal Window**	**1**
Chapter 2	**Bash Scripting**	**49**
Chapter 3	**Network Hosts Scanning**	**65**
Chapter 4	**Internet Information Gathering**	**89**
Chapter 5	**Social Engineering Attacks**	**105**
Chapter 6	**Advanced Enumeration Phase**	**125**
Chapter 7	**Exploitation Phase**	**161**
Chapter 8	**Web Application Vulnerabilities**	**199**
Chapter 9	**Web Penetration Testing and Secure Software Development Lifecycle**	**231**
Chapter 10	**Linux Privilege Escalation**	**257**
Chapter 11	**Windows Privilege Escalation**	**273**
Chapter 12	**Pivoting and Lateral Movement**	**305**
Chapter 13	**Cryptography and Hash Cracking**	**319**
Chapter 14	**Reporting**	**345**
Chapter 15	**Assembly Language and Reverse Engineering**	**353**
Chapter 16	**Buffer/Stack Overflow**	**369**

Chapter 17 Programming with Python 389

Chapter 18 Pentest Automation with Python 411

Appendix A Kali Linux Desktop at a Glance 427

Appendix B Building a Lab Environment Using Docker 467

Index 477

Contents

Introduction **xx**

Chapter 1 **Mastering the Terminal Window** **1**
Kali Linux File System 2
Terminal Window Basic Commands 3
Tmux Terminal Window 6
Starting Tmux 6
Tmux Key Bindings 7
Tmux Session Management 7
Navigating Inside Tmux 9
Tmux Commands Reference 9
Managing Users and Groups in Kali 10
Users Commands 10
Groups Commands 14
Managing Passwords in Kali 14
Files and Folders Management in Kali Linux 15
Displaying Files and Folders 15
Permissions 16
Manipulating Files in Kali 19
Searching for Files 20
Files Compression 21
Manipulating Directories in Kali 23
Mounting a Directory 23
Managing Text Files in Kali Linux 24
Vim vs. Nano 26
Searching and Filtering Text 27

Remote Connections in Kali 29
- Remote Desktop Protocol 29
- Secure Shell 30
- SSH with Credentials 30
- Passwordless SSH 32

Kali Linux System Management 34
- Linux Host Information 36
- Linux OS Information 36
- Linux Hardware Information 36
- Managing Running Services 38
- Package Management 39
- Process Management 41

Networking in Kali Linux 42
- Network Interface 42
  - IPv4 Private Address Ranges 42
  - Static IP Addressing 43
- DNS 45
- Established Connections 46
- File Transfers 47

Summary 48

Chapter 2 Bash Scripting 49

Basic Bash Scripting 50

Printing to the Screen in Bash 50

Variables 52
- Commands Variable 54

Script Parameters 54

User Input 56

Functions 56

Conditions and Loops 57
- Conditions 58
- Loops 60
  - File Iteration 61

Summary 63

Chapter 3 Network Hosts Scanning 65

Basics of Networking 65
- Networking Protocols 66
  - TCP 66
  - UDP 67
  - Other Networking Protocols 67
- IP Addressing 69
  - IPv4 69
  - Subnets and CIDR 69
  - IPv6 70
  - Port Numbers 71

Network Scanning 72
Identifying Live Hosts 72
Ping 73
ARP 73
Nmap 73
Port Scanning and Services Enumeration 74
TCP Port SYN Scan 75
UDP 75
Basics of Using Nmap Scans 76
Services Enumeration 77
Operating System Fingerprinting 79
Nmap Scripting Engine 80
NSE Category Scan 82
NSE Arguments 84
DNS Enumeration 84
DNS Brute-Force 85
DNS Zone Transfer 86
DNS Subdomains Tools 87
Fierce 87
Summary 88

Chapter 4 Internet Information Gathering 89
Passive Footprinting and Reconnaissance 90
Internet Search Engines 90
Shodan 91
Google Queries 92
Information Gathering Using Kali Linux 94
Whois Database 95
TheHarvester 97
DMitry 99
Maltego 99
Summary 103

Chapter 5 Social Engineering Attacks 105
Spear Phishing Attacks 105
Sending an E-mail 106
The Social Engineer Toolkit 106
Sending an E-mail Using Python 108
Stealing Credentials 109
Payloads and Listeners 110
Bind Shell vs. Reverse Shell 111
Bind Shell 111
Reverse Shell 112
Reverse Shell Using SET 113
Social Engineering with the USB Rubber Ducky 115
A Practical Reverse Shell Using USB Rubber Ducky and PowerShell 117

Generating a PowerShell Script 118
Starting a Listener 118
Hosting the PowerShell Script 119
Running PowerShell 120
Download and Execute the PS Script 120
Reverse Shell 121
Replicating the Attack Using the USB Rubber Ducky 122
Summary 122

Chapter 6 Advanced Enumeration Phase 125
Transfer Protocols 126
FTP (Port 21) 126
Exploitation Scenarios for an FTP Server 126
Enumeration Workflow 127
Service Scan 127
Advanced Scripting Scan with Nmap 128
More Brute-Forcing Techniques 129
SSH (Port 22) 130
Exploitation Scenarios for an SSH Server 130
Advanced Scripting Scan with Nmap 131
Brute-Forcing SSH with Hydra 132
Advanced Brute-Forcing Techniques 133
Telnet (Port 23) 134
Exploitation Scenarios for Telnet Server 135
Enumeration Workflow 135
Service Scan 135
Advanced Scripting Scan 136
Brute-Forcing with Hydra 136
E-mail Protocols 136
SMTP (Port 25) 137
Nmap Basic Enumeration 137
Nmap Advanced Enumeration 137
Enumerating Users 138
POP3 (Port 110) and IMAP4 (Port 143) 141
Brute-Forcing POP3 E-mail Accounts 141
Database Protocols 142
Microsoft SQL Server (Port 1433) 142
Oracle Database Server (Port 1521) 143
MySQL (Port 3306) 143
CI/CD Protocols 143
Docker (Port 2375) 144
Jenkins (Port 8080/50000) 145
Brute-Forcing a Web Portal Using Hydra 147
Step 1: Enable a Proxy 148
Step 2: Intercept the Form Request 149
Step 3: Extracting Form Data and Brute-Forcing with Hydra 150

Web Protocols 80/443 151
Graphical Remoting Protocols 152
RDP (Port 3389) 152
RDP Brute-Force 152
VNC (Port 5900) 153
File Sharing Protocols 154
SMB (Port 445) 154
Brute-Forcing SMB 156
SNMP (Port UDP 161) 157
SNMP Enumeration 157
Summary 159

Chapter 7 Exploitation Phase 161
Vulnerabilities Assessment 162
Vulnerability Assessment Workflow 162
Vulnerability Scanning with OpenVAS 164
Installing OpenVAS 164
Scanning with OpenVAS 165
Exploits Research 169
SearchSploit 171
Services Exploitation 173
Exploiting FTP Service 173
FTP Login 173
Remote Code Execution 174
Spawning a Shell 177
Exploiting SSH Service 178
SSH Login 178
Telnet Service Exploitation 179
Telnet Login 179
Sniffing for Cleartext Information 180
E-mail Server Exploitation 183
Docker Exploitation 185
Testing the Docker Connection 185
Creating a New Remote Kali Container 186
Getting a Shell into the Kali Container 187
Docker Host Exploitation 188
Exploiting Jenkins 190
Reverse Shells 193
Using Shells with Metasploit 194
Exploiting the SMB Protocol 196
Connecting to SMB Shares 196
SMB Eternal Blue Exploit 197
Summary 198

Chapter 8 Web Application Vulnerabilities 199
Web Application Vulnerabilities 200
Mutillidae Installation 200
Apache Web Server Installation 200

Firewall Setup 201
Installing PHP 201
Database Installation and Setup 201
Mutillidae Installation 202
Cross-Site Scripting 203
Reflected XSS 203
Stored XSS 204
Exploiting XSS Using the Header 205
Bypassing JavaScript Validation 207
SQL Injection 208
Querying the Database 208
Bypassing the Login Page 211
Execute Database Commands Using SQLi 211
SQL Injection Automation with SQLMap 215
Testing for SQL Injection 216
Command Injection 217
File Inclusion 217
Local File Inclusion 218
Remote File Inclusion 219
Cross-Site Request Forgery 220
The Attacker Scenario 221
The Victim Scenario 222
File Upload 223
Simple File Upload 223
Bypassing Validation 225
Encoding 227
OWASP Top 10 228
Summary 229

Chapter 9 Web Penetration Testing and Secure Software Development Lifecycle 231

Web Enumeration and Exploitation 231
Burp Suite Pro 232
Web Pentest Using Burp Suite 232
More Enumeration 245
Nmap 246
Crawling 246
Vulnerability Assessment 247
Manual Web Penetration Testing Checklist 247
Common Checklist 248
Special Pages Checklist 248
Secure Software Development Lifecycle 250
Analysis/Architecture Phase 251
Application Threat Modeling 251
Assets 251
Entry Points 252
Third Parties 252

Trust Levels 252
Data Flow Diagram 252
Development Phase 252
Testing Phase 255
Production Environment (Final Deployment) 255
Summary 255

Chapter 10 Linux Privilege Escalation 257
Introduction to Kernel Exploits and Missing Configurations 258
Kernel Exploits 258
Kernel Exploit: Dirty Cow 258
SUID Exploitation 261
Overriding the Passwd Users File 263
CRON Jobs Privilege Escalation 264
CRON Basics 265
Crontab 265
Anacrontab 266
Enumerating and Exploiting CRON 266
sudoers 268
sudo Privilege Escalation 268
Exploiting the Find Command 268
Editing the sudoers File 269
Exploiting Running Services 270
Automated Scripts 270
Summary 271

Chapter 11 Windows Privilege Escalation 273
Windows System Enumeration 273
System Information 274
Windows Architecture 275
Listing the Disk Drives 276
Installed Patches 276
Who Am I? 276
List Users and Groups 277
Networking Information 279
Showing Weak Permissions 282
Listing Installed Programs 283
Listing Tasks and Processes 283
File Transfers 284
Windows Host Destination 284
Linux Host Destination 285
Windows System Exploitation 286
Windows Kernel Exploits 287
Getting the OS Version 287
Find a Matching Exploit 288
Executing the Payload and Getting a Root Shell 289
The Metasploit PrivEsc Magic 289

Exploiting Windows Applications 293
Running As in Windows 295
PSExec Tool 296
Exploiting Services in Windows 297
Interacting with Windows Services 297
Misconfigured Service Permissions 297
Overriding the Service Executable 299
Unquoted Service Path 299
Weak Registry Permissions 301
Exploiting the Scheduled Tasks 302
Windows PrivEsc Automated Tools 302
PowerUp 302
WinPEAS 303
Summary 304

Chapter 12 Pivoting and Lateral Movement 305
Dumping Windows Hashes 306
Windows NTLM Hashes 306
SAM File and Hash Dump 307
Using the Hash 308
Mimikatz 308
Dumping Active Directory Hashes 310
Reusing Passwords and Hashes 310
Pass the Hash 311
Pivoting with Port Redirection 312
Port Forwarding Concepts 312
SSH Tunneling and Local Port Forwarding 314
Remote Port Forwarding Using SSH 315
Dynamic Port Forwarding 316
Dynamic Port Forwarding Using SSH 316
Summary 317

Chapter 13 Cryptography and Hash Cracking 319
Basics of Cryptography 319
Hashing Basics 320
One-Way Hash Function 320
Hashing Scenarios 321
Hashing Algorithms 321
Message Digest 5 321
Secure Hash Algorithm 323
Hashing Passwords 323
Securing Passwords with Hash 324
Hash-Based Message Authenticated Code 325
Encryption Basics 326
Symmetric Encryption 326
Advanced Encryption Standard 326
Asymmetric Encryption 328
Rivest Shamir Adleman 329

Cracking Secrets with Hashcat 331
Benchmark Testing 332
Cracking Hashes in Action 334
Attack Modes 336
Straight Mode 336
Combinator 337
Mask and Brute-Force Attacks 339
Brute-Force Attack 342
Hybrid Attacks 342
Cracking Workflow 343
Summary 344

Chapter 14 Reporting 345
Overview of Reports in Penetration Testing 345
Scoring Severities 346
Common Vulnerability Scoring System Version 3.1 346
Report Presentation 349
Cover Page 350
History Logs 350
Report Summary 350
Vulnerabilities Section 350
Summary 351

Chapter 15 Assembly Language and Reverse Engineering 353
CPU Registers 353
General CPU Registers 354
Index Registers 355
Pointer Registers 355
Segment Registers 355
Flag Registers 357
Assembly Instructions 358
Little Endian 360
Data Types 360
Memory Segments 361
Addressing Modes 361
Reverse Engineering Example 361
Visual Studio Code for C/C++ 362
Immunity Debugger for Reverse Engineering 363
Summary 368

Chapter 16 Buffer/Stack Overflow 369
Basics of Stack Overflow 369
Stack Overview 370
PUSH Instruction 370
POP Instruction 371
C Program Example 371
Buffer Analysis with Immunity Debugger 372
Stack Overflow 376
Stack Overflow Mechanism 377

Stack Overflow Exploitation 378
Lab Overview 379
Vulnerable Application 379
Phase 1: Testing 379
Testing the Happy Path 379
Testing the Crash 381
Phase 2: Buffer Size 382
Pattern Creation 382
Offset Location 382
Phase 3: Controlling EIP 383
Adding the JMP Instruction 384
Phase 4: Injecting the Payload and Getting a Remote Shell 386
Payload Generation 386
Bad Characters 386
Shellcode Python Script 387
Summary 388

Chapter 17 Programming with Python 389
Basics of Python 389
Running Python Scripts 390
Debugging Python Scripts 391
Installing VS Code on Kali 391
Practicing Python 392
Python Basic Syntaxes 393
Python Shebang 393
Comments in Python 393
Line Indentation and Importing Modules 394
Input and Output 394
Printing CLI Arguments 395
Variables 395
Numbers 395
Arithmetic Operators 397
Strings 397
String Formatting 397
String Functions 398
Lists 399
Reading Values in a List 399
Updating List Items 399
Removing a list item 400
Tuples 400
Dictionary 400
More Techniques in Python 400
Functions 400
Returning Values 401
Optional Arguments 401

Global Variables 402
Changing Global Variables 402
Conditions 403
if/else Statement 403
Comparison Operators 403
Loop Iterations 404
while Loop 404
for Loop 405
Managing Files 406
Exception Handling 407
Text Escape Characters 407
Custom Objects in Python 408
Summary 409

Chapter 18 Pentest Automation with Python 411
Penetration Test Robot 411
Application Workflow 412
Python Packages 414
Application Start 414
Input Validation 415
Code Refactoring 417
Scanning for Live Hosts 418
Ports and Services Scanning 420
Attacking Credentials and Saving the Results 423
Summary 426

Appendix A Kali Linux Desktop at a Glance 427
Downloading and Running a VM of Kali Linux 428
Virtual Machine First Boot 428
Kali Xfce Desktop 429
Kali Xfce Menu 430
Search Bar 430
Favorites Menu Item 430
Usual Applications 432
Other Menu Items 433
Kali Xfce Settings Manager 433
Advanced Network Configuration 435
Appearance 436
Desktop 439
Display 441
File Manager 442
Keyboard 445
MIME Type Editor 447
Mouse and Touchpad 448
Panel 449
Workspaces 450
Window Manager 451

Practical Example of Desktop Customization 454
Edit the Top Panel 454
Adding a New Bottom Panel 454
Changing the Desktop Look 457
Installing Kali Linux from Scratch 458
Summary 466

Appendix B Building a Lab Environment Using Docker 467
Docker Technology 468
Docker Basics 468
Docker Installation 468
Images and Registries 469
Containers 470
Dockerfile 472
Volumes 472
Networking 473
Mutillidae Docker Container 474
Summary 475

Index 477

Introduction

Kali is a popular Linux distribution used by security professionals and is becoming an important tool for daily use and for certifications. Penetration testers need to master Kali's hundreds of tools for pentesting, digital forensics, and reverse engineering. *Kali Linux Penetration Testing Bible* is a hands-on guide for getting the most from Kali Linux for pentesting. This book is for working cybersecurity professionals in offensive, hands-on roles, including red teamers, white-hat hackers, and ethical hackers. Defensive specialists will also find this book valuable, as they need to be familiar with the tools used by attackers.

This comprehensive pentesting book covers every aspect of the art and science of penetration testing. It covers topics like building a modern Dockerized environment, the basics of bash language in Linux, finding vulnerabilities in different ways, identifying false positives, and practical penetration testing workflows. You'll also learn to automate penetration testing with Python and dive into advanced subjects like buffer overflow, privilege escalation, and beyond.

By reading this book, you will:

- Gain a thorough understanding of the hundreds of penetration testing tools available in Kali Linux.
- Master the entire range of techniques for ethical hacking so you can be more effective in your job and gain coveted certifications.
- Learn how penetration testing works in practice and fill the gaps in your knowledge to become a pentesting expert.
- Discover the tools and techniques that hackers use so you can boost your network's defenses.

What Does This Book Cover?

This book goes deep into the subject of penetration testing. For established penetration testers, this book fills all the practical gaps, so you have one complete resource that will help you as your career progresses. For newcomers to the field, *Kali Linux Penetration Testing Bible* is your best guide to how ethical hacking really works.

Chapter 1: Mastering the Terminal Window

This chapter outlines the in and outs of the Linux system Terminal window and covers how to manage the file system like the pros. You will learn how to manage users and groups inside Kali, and you will see how to manipulate files and folders during your engagements and much more.

Chapter 2: Bash Scripting

Bash scripting is an essential skill for a penetration tester. In this chapter you will learn how to start to use programming principles such as variables, functions, conditions, loops, and much more.

Chapter 3: Network Hosts Scanning

This chapter teaches you how to conduct network scans like professionals. You will learn first about the basics of networking, and then you will delve deep into the port scanning techniques.

Chapter 4: Internet Information Gathering

This chapter discusses the passive information gathering phase in penetration testing. You will be introduced to how to deal with advanced search engine queries. Also, you will learn how to use Shodan and other tools to get the job done.

Chapter 5: Social Engineering Attacks

This chapter focuses on how to take advantage of human weakness to exploit organizations. You will learn about how to send phishing emails and steal credentials. On top of that, you will see how to use the Social Engineer Toolkit as a penetration tester. Finally, you will see how USB Rubber Ducky operates in similar SE attacks.

Chapter 6: Advanced Enumeration Phase

This chapter reviews how to handle the enumeration phase in a penetration testing engagement. Enumeration means collecting the necessary information that will allow us to exploit the specific service (e.g., FTP, SSH, etc.).

Chapter 7: Exploitation Phase

This chapter discusses some actual attacks and shows you how to get inside the systems. In the previous chapters, you had all the information about each service, and in this one, we will take this step further and exploit the vulnerabilities.

Chapter 8: Web Application Vulnerabilities

This chapter focuses on the basics of web application vulnerabilities. The goal is to allow you test web applications with ease during your engagements. Every company has a website these days, and it's crucial to understand this topic from A to Z.

Chapter 9: Web Penetration Testing and Secure Software Development Lifecycle

In this chapter, you will mainly learn about the methodology of web application penetration testing and how to use Burp Suite Pro. Finally, you will see how to implement a secure software development lifecycle (SSDLC) in an organization.

Chapter 10: Linux Privilege Escalation

This chapter focuses mainly on Linux operating system privilege escalation. The techniques in this chapter will allow you to gain root privileges on a compromised Linux OS.

Chapter 11: Windows Privilege Escalation

This chapter describes how to get administrator privileges on the compromised Windows OS. First you will learn about how to enumerate the Windows OS, and then you will see how to exploit the Windows system with practical examples.

Chapter 12: Pivoting and Lateral Movement

This chapter describes how to use the pivoting techniques to move laterally on the compromised network. In this chapter, you will learn how Windows hashes work under the hood and how to reuse admin credentials to get the job done.

Chapter 13: Cryptography and Hash Cracking

This chapter describes how to crack hashes during your engagements using Hashcat. Before starting on the cracking topic, you will learn about the basics of cryptography including hashing and encryption.

Chapter 14: Reporting

This chapter explains how to present professional penetration testing reports. Also, you will learn how to evaluate accurately the severity of your findings.

Chapter 15: Assembly Language and Reverse Engineering

This chapter will introduce you to the concept of reverse engineering using the assembly language. You will learn about the basics of the assembly language including registers, assembly instructions, memory segments, and much more.

Chapter 16: Buffer/Stack Overflow

This chapter will use what you learned in the previous chapter to exploit the stack using the buffer overflow technique.

Chapter 17: Programming with Python

This chapter discusses the basics of Python version 3. This programming language is the choice of hackers, so you should learn it too.

Chapter 18: Pentest Automation with Python

This chapter focuses on the automation of the penetration testing phases using the Python language. You will see a complete practical example that can use in your career.

Appendix A: Kali Linux Desktop at a Glance

This appendix focuses on how to manage the interface of the Kali Linux desktop environment. You will learn how to handle this operating system with ease and customize it to your liking.

Appendix B: Building a Lab Environment Using Docker

This appendix will delve deep with Docker, and you will see how images and containers work in practice. Both Docker and hypervisor technologies facilitate the creation of a live lab so we, penetration testers, can have fun with it.

Companion Download Files

As you work through the examples in this book, you may choose either to type in all the code manually or to use the source code files that accompany the book. All the source code used in this book is available for download from `www.wiley.com/go/kalilinuxpenbible`.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

How to Contact the Author

We appreciate your input and questions about this book! Email the author at `gus.khawaja@guskhawaja.me`, or message him on Twitter at `@GusKhawaja`.