

The Art Of Offensive Scripting

Rocky

The Art Of Offesnsive Scripting

© 2024 by Codelivly. All rights reserved

No part of this ebook may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

For permission requests, don't hesitate to get in touch with the author at:

Rocky
Email: rocky@codelivly.com
Website: www.codelivly.com

The content of this ebook is provided for educational and informational purposes only. While the author has made every effort to ensure the accuracy of the information provided, neither the author nor the publisher assumes responsibility for errors, omissions, or contrary interpretations of the subject matter.

This page was left blank intentionally

Contents

Introductions	16
Getting Started with Scripting	28
Python for Offensive Security	70
Bash Scripting for Offensive Security	101
Advanced Scripting Techniques	126
Integrating Scripting with Other Tools	167
Utilizing APIs for Offensive Scripting	205
Combining Scripting with Task Automation Tools	223
Vulnerability Scanning and Fuzzing	241
Projects	280

Table of contents

Introduction..... 23
Whom This Book Is For ?..... 25
Setting Up Your Scripting Environment..... 27
Why Kali Linux?..... 28
Downloading and Installing Kali Linux..... 29
Installing Gedit: Your Scripting Text Editor..... 30
Organizing Your Workspace..... 32
Running and Testing Your Scripts..... 33
Ready to Get Started?..... 34
Chapter 1: Getting Started with Scripting..... 35
Difference Between Scripting and Programming..... 36
Common Uses of Scripting in Hacking..... 36
Benefits of Learning Scripting for Hackers..... 37
Choosing the Right Scripting Language..... 39
Why Choosing the Right Language Matters..... 39
Popular Scripting Languages in Hacking..... 40
Factors to Consider When Choosing a Language..... 42
Why We'll Focus on Python and Bash..... 43
Introduction to Python Scripting..... 44
Getting Started with Python Scripting..... 45
1. Installing Python..... 45
2. Running Your First Python Script..... 46
3. Understanding Python Syntax..... 46
4. Basic Python Concepts for Scripting..... 47
Practicing Your Python Skills..... 48
Introduction to Bash Scripting..... 49
Getting Started with Bash Scripting..... 50
1. Writing Your First Bash Script..... 50
2. Basic Bash Scripting Concepts..... 51
3. Scripting Best Practices..... 53
Practicing Your Bash Skills..... 54
Key Concepts in Scripting for Offensive Security..... 55
Variables and Data Handling..... 57

Variables in Scripting: The Basics..... 57
Python Variables..... 58
Bash Variables..... 59
Handling Data in Python..... 60
Handling Data in Bash..... 61
Practical Applications in Offensive Security..... 62
File and Directory Manipulation..... 63
Why File and Directory Manipulation Matters..... 63
Basic File Operations in Python..... 64
Navigating and Manipulating Directories in Python..... 65
File and Directory Manipulation in Bash..... 67
Practical Applications in Offensive Security..... 68
Handling File Permissions..... 69
Network Interaction Basics..... 70
What Is Network Interaction?..... 70
Why Network Interaction Is Important in Offensive Scripting..... 71
Getting Started with Basic Networking Concepts..... 71
Interacting with Networks Using Python..... 72
Interacting with Networks Using Bash..... 73
Practical Tips for Network Interaction..... 74
Hands-On: Your First Offensive Script..... 75
Project Overview: A Simple Port Scanner..... 75
What is a Port Scanner?..... 76
Why Create Your Own Port Scanner?..... 76
Project Goals..... 77
Part 1: Building a Simple Port Scanner in Python..... 77
Python Script Outline..... 77
Part 2: Building a Simple Port Scanner in Bash..... 79
Bash Script Outline..... 79
Script Walkthroughs..... 80
Next Steps..... 81
Chapter 2: Python for Offensive Security..... 81
Python Basics: The Building Blocks..... 82
Getting Comfortable with Python: A Few Tips..... 85
Writing Your First Python Script..... 85
Getting Started: Your Scripting Toolkit..... 85
Step 1: Opening Gedit and Creating a New File..... 86

Step 2: Writing Your First Lines of Code....86
Step 3: Saving and Running Your Script....86
Step 4: Adding More Functionality....87
Step 5: Troubleshooting and Debugging....88
Libraries and Tools for Offensive Python Scripting....88
Getting Started with Python Libraries....89
1. Requests: For HTTP Requests and Web Interaction....89
2. Scapy: For Network Packet Manipulation....90
3. Beautiful Soup: For HTML Parsing and Web Scraping....90
4. Paramiko: For SSH Connections....91
5. Subprocess: For System Interaction....92
6. PyInstaller: For Creating Standalone Executables....93
Network Programming with Python....93
Why Network Programming?....94
Getting Started with Sockets....94
Understanding Protocols....96
Building a TCP Server....96
Network Programming Use Cases in Offensive Security....98
File Handling and Automation....99
Getting Started with File Handling in Python....99
Opening a File....100
Reading from a File....100
Writing to a File....101
Appending to a File....101
File Handling with Error Checking....102
Automation with File Handling....102
Combining File Handling with Bash Scripting....103
Creating Simple Exploits....104
What is an Exploit?....104
The Building Blocks of an Exploit....104
Example: A Simple Buffer Overflow in Python....105
Writing Your First Exploit: Exploiting a Simple Service....106
Exploiting Web Vulnerabilities with Python....107
Bash Scripting for Exploits....109
Practice Makes Perfect....110
Hands-On Project: Building a Custom Python Tool....110
Why Build Your Own Tool?....111

What Are We Building?....111
Setting Up Your Environment....111
Step 1: Plan Your Tool....111
Step 2: Write the Basic Script....112
Step 3: Adding Features and Functionality....113
Step 4: Testing Your Tool....115
Step 5: Improving and Expanding....117
Chapter 3: Bash Scripting for Offensive Security....118
Why Bash?....118
Getting Started with the Command Line....119
What is a Bash Script?....119
Basic Bash Scripting Concepts....120
1. Variables:....120
2. Comments:....121
3. Conditionals:....121
4. Loops:....121
5. Functions:....122
6. Handling Files:....122
Putting It All Together....123
Writing Your First Bash Script....124
Getting Started: Your First Script....124
Step 1: Open Your Text Editor....125
Step 2: Write Your Script....125
Step 3: Save and Close the File....126
Step 4: Make the Script Executable....126
Step 5: Run Your Script....126
Expanding Your Script....126
Why This Matters....127
What's Next?....128
Automating Tasks with Bash....128
Getting Started with Automation....128
Step 1: The Plan....129
Step 2: Writing the Script....129
Step 3: Understanding the Script....130
Step 4: Running Your Script....131
More Automation Examples....131
Scheduling Automation: Using Cron Jobs....132
Why Automating Tasks is a Game-Changer....133

Using Bash for System Enumeration..... 133
Why Use Bash for Enumeration?..... 134
Common Enumeration Tasks You Can Automate with Bash..... 134
Creating a Basic System Enumeration Script..... 134
Step 1: Plan the Script..... 135
Step 2: Write the Script..... 135
Step 3: Understanding the Script..... 136
Step 4: Make the Script Executable and Run It..... 137
Advanced Enumeration Techniques..... 138
Practical Example: Enumerating Services with Netstat..... 138
Adding to Your Script:..... 138
Hands-On Project: Automating Reconnaissance with Bash..... 140
Project Overview..... 140
Step 1: Planning the Script..... 140
Step 2: Writing the Script..... 141
Step 3: Understanding the Script..... 143
Step 4: Making the Script Executable and Running It..... 143
Enhancing Your Script..... 144
Chapter 4: Advanced Scripting Techniques..... 146
Error Handling and Debugging..... 149
Getting Started with Error Handling..... 150
Advanced Error Handling: Making Your Scripts Bulletproof..... 151
Debugging Techniques: Finding and Fixing Bugs..... 153
Scripting for Stealth and Evasion..... 154
The Importance of Stealth and Evasion..... 155
Advanced Techniques for Stealthy Scripting..... 156
Timing Attacks with Precision:..... 156
Obfuscation and Encryption:..... 156
Blending in with Legitimate Traffic:..... 157
Command and Control (C2) Channels:..... 158
Evading Endpoint Security:..... 159
Adaptive and Responsive Behavior:..... 159
Misleading and Manipulating Logs:..... 160
Putting It All Together: A Stealthy Network Recon Script..... 160
Parsing and Manipulating Data..... 162
Getting Started with Parsing Data..... 163
Parsing Text Data with Python..... 164
Reading and Splitting Text:..... 164

Working with Structured Data:..... 165
Using Regular Expressions for Complex Parsing:..... 165
Manipulating Data..... 166
Filtering Data:..... 166
Modifying Data:..... 167
Combining Data:..... 168
Parsing and Manipulating Data with Bash..... 168
Reading and Filtering Text with Bash:..... 168
Modifying Text with sed:..... 168
Combining Data with Bash:..... 168
Practical Example: Parsing and Analyzing Logs..... 169
Python Script:..... 169
Bash Script:..... 170
Multithreading and Parallel Processing..... 170
When to Use Multithreading vs. Parallel Processing..... 171
Advanced Multithreading in Python..... 171
Advanced Parallel Processing with Python's multiprocessing Module..... 173
Advanced Techniques and Best Practices..... 175
Advanced Parallel Processing in Bash..... 176
Advanced Network Scripting..... 178
Understanding Advanced Network Scripting..... 178
Socket Programming: Beyond the Basics..... 178
Working with Different Protocols..... 180
Handling Asynchronous Network Tasks..... 182
Handling Network Latency and Timeouts..... 184
Building and Analyzing Custom Packets with Scapy..... 185
Hands-On Project: Creating an Advanced Port Scanner..... 187
Project Overview..... 187
Step 1: Setting Up Your Environment..... 188
Step 2: Basic Structure of the Scanner..... 188
Step 3: Introducing Multithreading for Speed..... 190
Step 4: Advanced Packet Crafting with Scapy..... 191
Step 5: Enhancing Error Handling and Stealth..... 193
Chapter 5: Integrating Scripting with Other Tools..... 196
Extending Capabilities with Nmap..... 197
Using Python to Automate and Extend Nmap Scans..... 197
Extending with Bash for Quick and Powerful Automation..... 201
Practical Use Cases and Tips:..... 203

Project 1: Advanced Host Discovery with Python..... 204
Project 2: Vulnerability Assessment with Nmap and Bash..... 206
Project 3: Service Enumeration and Banner Grabbing with Python..... 209
Leveraging Metasploit with Scripting..... 211
Integrating Metasploit with Python: Automating Exploits and Beyond..... 211
Troubleshooting Connection Issues with Metasploit RPC..... 215
Common Errors.....215
Step-by-Step Troubleshooting..... 215
Check the Connection Settings:.....216
Verify Network Accessibility:..... 216
Review SSL Settings:..... 216
Examine Metasploit Logs:.....216
Adjust Connection Retry Parameters:.....217
Ensure Correct Permissions:..... 217
Practical Use Cases for Scripting with Metasploit:.....217
Project 1: Automated Exploit Finder.....218
Project 2: Custom Metasploit Auxiliary Module with Ruby.....220
Project 3: Automating Post-Exploitation with Metasploit and Python.....223
Project 4: Automating Social Engineering with Metasploit.....225
Integrating Scripting with Burp Suite..... 229
Getting Started with Burp Suite API and Extender..... 229
Automating Burp Suite with Python: Initiating and Managing Scans..... 230
Extending Burp with Custom Scripts: Real-Time Request Modification.....233
Practical Applications of Scripting with Burp Suite..... 236
Project 1: Automating Scans with Burp Suite.....237
Project 2: Real-Time Request Modification with Custom Headers.....241
Project 3: Automating Repetitive Actions Using Burp Macros.....243
Project 4: Automating Intruder Attacks with Custom Payloads.....244
Chapter 6: Utilizing APIs for Offensive Scripting..... 248
Introduction to REST APIs..... 249
Understanding REST Architecture and HTTP Methods..... 249
Using Python’s requests Library to Interact with APIs..... 250
Practical Example: Exploiting an API Vulnerability.....251
Automating Tasks with REST APIs Using Advanced Scripting..... 253
Accessing and Consuming APIs with Python..... 255
Understanding RESTful APIs and Python's requests Library.....255
Basic API Request with Python..... 256

Advanced API Consumption: Authenticating and Handling Errors..... 257
Practical Offensive Scripting: Automating Reconnaissance with APIs..... 259
Practical Use: Creating a Custom API Client with Error Handling and Retrying.. 261
Automating Reconnaissance and Data Collection..... 263
Advanced Reconnaissance Automation with Python..... 264
Detailed Explanation:..... 270
Extending the Script: Additional Automation Features..... 270
Chapter 7: Combining Scripting with Task Automation Tools..... 271
Using Cron Jobs for Scheduled Execution..... 273
What is Cron?..... 273
Understanding Cron's Syntax..... 273
Step-by-Step: Setting Up Your First Cron Job..... 274
Making Your Cron Jobs More Robust..... 274
Advanced Scheduling with Cron..... 275
Troubleshooting Cron Jobs..... 276
Leveraging Cron for Offensive Security..... 277
Automating Workflows with Jenkins..... 277
What is Jenkins?..... 278
Getting Started with Jenkins..... 278
Creating Your First Jenkins Pipeline..... 279
Step-by-Step Guide to Creating an Offensive Security Pipeline:..... 279
Integrating Jenkins with Nmap..... 282
Leveraging Jenkins with Metasploit..... 282
Advanced Jenkins Integrations for Offensive Security..... 283
Triggering Scripts with System Events..... 284
What Are System Events?..... 285
Using inotify to Monitor File Events..... 285
Using systemd to Automate Script Execution..... 287
Using Udev Rules for Device-Based Triggers..... 288
Chapter 8: Vulnerability Scanning and Fuzzing..... 290
Common Tools and Approaches..... 291
Automated vs. Manual Scanning..... 292
Using OpenVAS for Vulnerability Scanning..... 292
Setting Up OpenVAS..... 292
Automating OpenVAS with Python..... 293
Automating OpenVAS with Bash..... 294
Handling Results..... 295

Scheduling Scans with Cron Jobs....296
Advanced Scanning with Nessus....297
Setting Up Nessus....297
Automating Nessus with Python....297
Automating Nessus with Bash....300
Scheduling Nessus Scans with Cron Jobs....302
Handling and Parsing Results....302
Integrating Nmap for Vulnerability Detection....303
The Power of Nmap with Scripting....304
Getting Started with Nmap and Python....304
Automating Nmap with Bash....308
Integrating Nmap with Other Tools for Advanced Scanning....312
Getting Started with OWASP ZAP Fuzzer....313
Introduction to OWASP ZAP Fuzzer....314
Setting Up OWASP ZAP for Fuzzing....315
Automating OWASP ZAP Fuzzing with Python....315
Automating OWASP ZAP Fuzzing with Bash....319
Advanced Fuzzing Techniques....321
Advanced Fuzzing with AFL (American Fuzzy Lop)....322
Getting Started with AFL....322
Advanced AFL Usage: Automating AFL with Python....324
Advanced AFL Usage: Automating AFL with Bash....325
Leveraging AFL for Complex Scenarios....326
Automating Fuzzing with Python....327
Setting Up the Environment....328
Automating AFL Fuzzing with Python....328
Using Radamsa for Input Mutation....331
Combining Python with Custom Fuzzing Logic....332
Hands-On Project: Building a Custom Vulnerability Scanner....334
Project Overview....334
Setting Up Your Environment....335
Step-by-Step Implementation....335
Breaking Down the Code....339
Running the Scanner....340
Chapter 9: Projects....341
#1. Gaining a Web Shell....341
What is a Web Shell?....342

Prerequisites....342
Creating a Basic Web Shell in Python.... 342
Creating a Basic Web Shell in Bash....345
Combining Python and Bash for Enhanced Web Shells.... 347
Defensive Measures and Mitigations.... 349
#2. Reverse Shells....350
What is a Reverse Shell?.... 350
Basic Reverse Shell in Python.... 351
Basic Reverse Shell in Bash....353
Advanced Reverse Shell Techniques.... 354
Practical Considerations....355
#3. Automated Password Cracking.... 355
Automating Password Cracking with Python....356
Automating Password Cracking with Bash.... 358
Dictionary vs. Brute Force Attacks.... 360
Enhancing Password Cracking Techniques.... 360
#4. Malware Analysis Automation.... 361
Automating Static Analysis with Python....362
Automating Dynamic Analysis with Python and Bash....365
Automating Malware Analysis with Bash.... 366