

Contents

1	The Evolution of Penetration Testing, Red Teaming, and Bug Bounties	1
	Into the Abyss	1
	The Uncharted Territory	2
	The AI Crash Course	2
	Into the Breach	3
	Culmination	5
	Next Steps	5
	Industry Overview	5
	What Are Penetration Testing, Red Teaming, and Bug Bounties?	6
	Why Are These Disciplines Important?	6
	How Have They Evolved Over Time?	6
	The Early Days and Evolution of Penetration Testing	7
	The Rise of Red Teaming	9
	The Emergence of Bug Bounty Programs	10
	The Convergence of Penetration Testing, Red Teaming, and Bug Bounties	11
	The Future of Penetration Testing, Red Teaming, and Bug Bounties	12
	The Increasing Use of AI and ML in Penetration Testing, Red Teaming, and Bug Bounties	13
	Test Your Skills	15
2	Introduction to Red Teaming	17
	What Is Red Teaming?	17
	The Importance of Red Teaming	18
	Identifying Critical Vulnerabilities	18
	Challenging Assumptions	18
	Emulating Industry-Specific Threats	19
	Red Team Frameworks and Methodologies	20

	MITRE ATT&CK Framework	20
	Unified Kill Chain	20
	TIBER-EU	21
	CBEST	21
	Red Team Engagements	22
	Full-Scope	22
	Objective-Based	23
	Adversary Emulation (Scenario-Based)	24
	Purple Team	24
	Tabletop	25
	Red Team Challenges	26
	Leveling Up Other Teams	26
	Lack of Findings	27
	References	28
	Test Your Skills	30
3	Red Team Infrastructure	33
	An Overview of Red Team Infrastructure	34
	Command and Control	34
	C2 Communication Channels	36
	Redirectors	37
	Command and Control Setup	37
	Test Your Skills	60
4	Modern Red Team Methodology and Tools	63
	Planning	64
	Rules of Engagement	64
	Kickoff Call	65
	Communication	65
	Reconnaissance	65
	Autonomous System Number (ASN)	65
	Certificate Transparency	66
	Proxying Traffic	66

Domain Name Service	71
Metadata	78
Username Collection	79
Software Discovery	81
Leaked Data	81
Initial Access	81
Password Spraying	82
Mobile Device Management (MDM)	87
Social Engineering and Physical Access	88
Payload Preparation	88
Web Application Vulnerabilities	95
Persistence	96
Lateral Movement	97
Obtaining Credentials	97
Gathering Domain Information	97
Kerberoasting	99
Active Directory Certificate Services	100
SCCM Abuse	104
Post-Exploitation	105
Reporting	105
Test Your Skills	107
5 Social Engineering and Physical Assessments	109
Phone Pretexting: Let's Dial into Your Target	110
Reconnaissance	110
Preparing Pretext	111
Execution	113
Spear Phishing: Time to Reel In Your Target	115
Infrastructure	116
Formulating Your Email or Instant Message	128
Execution	130

Can You Hear Us from the Inside?	131
Remote Reconnaissance	131
Badge Cloning	132
Onsite Reconnaissance	139
Social Engineering in Person	140
Physical Building Bypasses	140
Test Your Skills	144
6 Advanced Post-Exploitation Techniques.....	147
An Overview of Post-Exploitation	148
Evaluating Detection and Response Capabilities and Understanding the Impact of a Breach	148
Improving Blue Team Capabilities	149
How to Maintain Access, Use Persistence Mechanisms, and Create Backdoors	152
Types of Backdoors	153
Reverse Shells vs. Bind Shells	160
Patching Binaries to Include a Backdoor	165
Avoiding Detection Using Code Obfuscation	167
System-Level Backdoors	170
Kernel-Level Backdoors	174
Hardware and Firmware Backdoors	178
Scheduled Jobs and Tasks	179
New Users	180
Command and Control (C2) and Covert Channels	180
How DNS Tunneling Works	181
HTTP/HTTPS Tunneling	183
Nontraditional Protocols	183
Additional C2 Techniques and Tools	183
How to Perform Lateral Movement	186
Post-Exploitation Scanning	186
Legitimate Utilities and Living Off the Land	189

PowerShell for Post-Exploitation Tasks	189
PowerSploit and Empire	190
BloodHound	193
Windows Management Instrumentation for Post-Exploitation Tasks	193
Sysinternals and PsExec	194
Windows Remote Management (WinRM) for Post-Exploitation Tasks	195
Living-Off-the-Land Bins, Libraries, and Useful Scripts	195
Post-Exploitation Privilege Escalation	197
How to Cover Your Tracks	198
Steganography	198
Test Your Skills	202
7 Active Directory and Linux Environments	207
Active Directory Fundamentals	208
Centralized Data Repository and High Availability	208
Security	209
Active Directory Architecture	211
AD Trust Relationships	213
Key Active Directory Protocols and Services	216
Microsoft Entra ID and Azure	223
Active Directory Attack Techniques	229
How to Set Up the Lab	229
AD Recon and Enumeration	231
Password Spray and ASREPROast	239
Useful LDAP Queries for Windows Active Directory Assessments	242
BloodHound Is Awesome	246
Using Responder for Credential Harvesting in Active Directory Environments	247
Using Secretsdump to Extract Credentials	253
Using Lsassy to Extract Credentials from LSASS	256
Using DonPAPI to Target the Windows Data Protection Application Programming Interface (DPAPI)	257

	ADCS Reconnaissance and Enumeration with Certipy and BloodHound.	259
	Exploitation Using Certipy.	261
	Abusing Discretionary Access Control Lists (DACLS) and Access Control Entries (ACEs)	262
	The Golden SAML Attack.	263
	Microsoft Entra Connect (Azure AD Connect) Sync Account Takeover	265
	Microsoft Entra Privileged Identity Management (PIM) Abuse	266
	Advanced Linux Environment Attack Techniques	267
	A Quick Refresher on How Buffer Overflows Work	267
	How to Exploit Buffer Overflows	267
	Examples of Vulnerable Code	270
	Bypassing No-Execute (NX) Stack with Return-Oriented Programming (ROP).	273
	Bypassing NX with ROP.	275
	Test Your Skills	277
	Project 7-1	280
8	The Future of Red Teaming Beyond the AI Revolution	281
	Understanding the Current State of AI in Red Teaming	282
	Creating AI-Powered Offensive Security Tools	283
	LangChain, Prompt Templates, LangSmith, LangGraph, and LlamaIndex	289
	Examining Fine-Tuned Uncensored AI Models.	297
	Understanding Retrieval-Augmented Generation (RAG) for Red Teaming	299
	Vector Embeddings	300
	Vector Database Storage	302
	User Query Processing.	305
	Semantic Search and Document Retrieval	305
	Context Preparation for LLMs or SLMs	308
	Response Generation and Post-Processing and Refinement.	311
	Red Teaming AI and Autonomous Systems	313
	Keeping Pace with Rapidly Evolving Technologies.	322
	Test Your Skills	324

9	Introduction to Bug Bounty and Effective Reconnaissance	327
	Understanding Bug Bounty Programs	328
	Types of Bug Bounty Programs	329
	Attack Surface Management vs. Bug Bounties	331
	Vulnerability Disclosure Programs (VDPs) vs. Bug Bounties	332
	Getting Started: Preparing Yourself as an Ethical Hacker in Bug Bounty Programs	333
	Understanding the Scope and Rules of Engagement	334
	Exploring Effective Reconnaissance	336
	Active vs. Passive Reconnaissance	336
	Understanding OSINT	337
	Leveraging DNS for Recon	339
	Identifying Technical and Administrative Contacts	342
	Identifying Cloud vs. Self-Hosted Assets	344
	Social Media Scraping	348
	Cryptographic Flaws	348
	Obtaining Sensitive Information About External and Internal Hosts Using Certificate Transparency	353
	Leveraging Password Dumps	355
	Recon from File Metadata	358
	Strategic Search Engine Analysis/Enumeration	360
	Website Archive/Caching	361
	Public Source-Code Repositories, Secrets, and Other Sensitive Information	362
	Performing Reconnaissance with Recon-ng	363
	Shodan	369
	Amass, Maltego, and Other OSINT Tools	371
	Using Generative AI and the Gorilla Large Language Model to Interact with Tools Like Amass	372
	Using Open-Interpreter to Interact with Recon Tools	373
	Performing Active Reconnaissance	377
	Creating Your Own Scanner Using Python	380

Exploring the Different Types of Enumeration	382
Using BloodHound for a Bug Bounty	394
Packet Inspection and Eavesdropping	395
Understanding the Art of Performing Vulnerability Scans	396
Understanding the Types of Vulnerability Scans	396
Challenges to Consider When Running a Vulnerability Scan	398
Performing Web Application and API Recon	401
Directory and File Brute-Forcing	401
API Recon	404
Communicating Your Findings and Creating Effective Bug Bounty Reports	407
Test Your Skills	410
Exercises	412
10 Hacking Modern Web Applications and APIs	415
Overview of Web Application-Based Attacks, the OWASP Top 10 for Web Applications, and OWASP Top 10 for LLM Applications	416
The HTTP Protocol	416
Understanding Web Sessions	425
OWASP Top 10 for Web Applications	427
OWASP Top 10 for LLM Applications	428
Building Your Own Web Application Lab	429
Understanding Business Logic Flaws	430
Understanding Injection-Based Vulnerabilities	432
Hacking Databases and Exploiting SQL Injection Vulnerabilities	433
Command Injection Vulnerabilities	448
Lightweight Directory Access Protocol (LDAP) Injection Vulnerabilities	449
Exploiting Authentication-Based Vulnerabilities	451
Brute-Forcing Credentials	451
Understanding Session Hijacking	452
Understanding Redirect Attacks	458
Taking Advantage of Default Credentials	458

Exploiting Kerberos Vulnerabilities	459
Exploiting Authorization-Based Vulnerabilities	461
Understanding Parameter Pollution	461
Exploiting Insecure Direct Object Reference (IDOR) Vulnerabilities	462
Understanding Cross-Site Scripting (XSS) Vulnerabilities	463
Reflected XSS Attacks	465
Stored XSS Attacks	466
XSS Evasion Techniques	470
XSS Mitigations	471
Understanding Cross-Site Request Forgery and Server-Side Request Forgery Attacks	472
Server-Side Request Forgery Attacks	475
Exploiting an SSRF Vulnerability Using WebSploit Labs	477
Understanding Clickjacking	480
Exploiting Security Misconfigurations	480
Exploiting Directory Traversal Vulnerabilities	480
Understanding Cookie Manipulation Attacks	482
Exploiting File Inclusion Vulnerabilities	482
Local File Inclusion Vulnerabilities	482
Remote File Inclusion Vulnerabilities	483
Exploiting Insecure Code Practices	484
Comments in Source Code	484
Lack of Error Handling and Overly Verbose Error Handling	484
Hard-Coded Credentials	484
Race Conditions	485
Unprotected APIs	485
Hidden Elements	488
Lack of Code Signing	488
Using Additional Web Application Hacking Tools	488
Test Your Skills	493

11 Automating a Bug Hunt and Leveraging the Power of AI	497
Traditional Bug Hunting Methods	498
Limitations of Manual Bug Hunting	499
AI-Powered Automation in Bug Hunting	500
AI Capabilities of Bug Bounty Platforms	508
A Comprehensive View of an Organization's External Risk Exposure	509
Vulnerability Prioritization Using AI	510
AI-Created Scanner Templates	512
AI Model Training, Fine-Tuning, and RAG for Bug Bounties	516
Deploying AI Models	516
Fine-Tuning AI Models	517
Using RAG and AI Agents for Bug Bounty Hunting	519
Tool Calling	520
Challenges of Using AI for Bug Bounty Hunting	521
Censored Models and Guardrails	521
Hallucinations or Confabulations	522
Test Your Skills	523
Answers to Multiple-Choice Questions	527
Index.....	541