

## Hacking mit Post Exploitation Frameworks

Angriffe verstehen und vorbeugen, Awareness herstellen

# DAS INHALTS- VERZEICHNIS

» Hier geht's  
direkt  
zum Buch

# Inhalt

<b>Vorwort</b> .....	<b>IX</b>
Geleitwort von Marco Krempel .....	X
Geleitwort von Felix Noack .....	XI
<b>1 Über dieses Buch</b> .....	<b>1</b>
1.1 Orientierung und Begriffsbestimmung .....	1
1.2 Ziel des Buches .....	2
1.3 Wer soll das Buch lesen? .....	4
1.4 Was erwartet Sie in diesem Buch? .....	5
1.5 Wie ist das Buch aufgebaut? .....	7
1.6 Was Sie noch wissen sollten .....	9
1.7 Etwas zur verwendeten Sprache und Gendergerechtigkeit .....	10
1.8 Ein Wort zu Penetrationstests und Angriffsmethoden .....	11
<b>2 Eine eigene Testumgebung aufbauen</b> .....	<b>15</b>
2.1 Desktop-Virtualisierung .....	16
2.1.1 VMware Workstation Pro und Player .....	16
2.1.2 VirtualBox von Oracle .....	17
2.1.3 VirtualBox auf Ubuntu installieren .....	18
2.2 Server-Virtualisierung .....	19
2.2.1 Proxmox VE .....	19
2.2.2 Virtualisierung mit XCP-NG .....	21
2.3 Virtuelle Maschinen erstellen .....	24
2.3.1 Kali Linux aus Image-Datei in VirtualBox importieren .....	24
2.3.2 Ubuntu VM in VMware Workstation Player erstellen .....	26
2.3.3 Windows 11 als VM in Proxmox einrichten .....	27
2.3.4 Einen Linux Container in Proxmox erstellen .....	31
2.3.5 Netzwerkeinstellungen in virtuellen Maschinen .....	33
2.4 Die Übungsumgebung .....	34
2.5 Kontrollfragen .....	40

<b>3</b>	<b>Die Post Exploitation Frameworks anwenden</b>	<b>43</b>
3.1	Das Metasploit Framework	44
3.1.1	Das Metasploit Framework installieren	44
3.1.2	Ein Schnellstart ins Metasploit Framework	47
3.1.3	Metasploit-Generator für Payloads	48
3.1.4	Ein Szenario für den Schnelleinstieg	50
3.1.5	Post Exploitation mit Metasploit	54
3.1.6	Zusammenfassung und Fazit	56
3.1.7	Kontrollfragen zum Metasploit Framework	57
3.2	Das Post Exploitation Framework Empire	58
3.2.1	Das Empire Framework installieren	59
3.2.2	Aufbau und Funktionsweise des Empire Frameworks	62
3.2.3	Das Empire Framework nutzen – einfaches Szenario	64
3.2.4	Im Empire Framework die Kommunikation über einen Cloud-Dienst einrichten	74
3.2.5	Die grafische Nutzeroberfläche Starkiller	80
3.2.6	Zusammenfassung und Fazit	87
3.2.7	Kontrollfragen zum Empire Framework	87
3.3	Das Post Exploitation Framework Koadic	89
3.3.1	Aufbau und Funktionsweise von Koadic	89
3.3.2	Installation und erste Schritte mit Koadic	90
3.3.3	Handhabung von Koadic	92
3.3.4	Ein erstes Szenario mit Koadic	93
3.3.5	Wichtige Kommandos und Hilfsmittel	97
3.3.6	Ein erweitertes Szenario mit Koadic	99
3.3.7	Zusammenfassung und Fazit	109
3.3.8	Kontrollfragen zum Koadic Framework	109
3.4	Das Post Exploitation Framework Merlin	111
3.4.1	Aufbau und Funktionsweise von Merlin	111
3.4.2	Installation des Servers	112
3.4.3	Agenten im Windows-PC einrichten	113
3.4.4	Merlin – Bedienung und Grundlagen	114
3.4.5	Ein Szenario mit Merlin	116
3.4.6	Zusammenfassung und Fazit	126
3.4.7	Kontrollfragen zum Merlin Framework	127
3.5	Das Post Exploitation Framework Covenant	128
3.5.1	Aufbau und Bestandteile von Covenant	129
3.5.2	Covenant installieren	130
3.5.3	Ein Szenario mit Covenant	133
3.5.4	Zusammenfassung und Fazit	152
3.5.5	Kontrollfragen zu Covenant	153
3.6	Das Post Exploitation Framework Sliver	154
3.6.1	Aufbau und Bestandteile von Sliver	155
3.6.2	Sliver installieren	157
3.6.3	Sliver – ein einfaches Szenario zur Einführung	160

3.6.4	DNS-Tunneling mit Sliver .....	168
3.6.5	Zusammenfassung und Fazit .....	173
3.6.6	Kontrollfragen zu Sliver .....	174
3.7	Das Mythic Framework für Red Teams .....	175
3.7.1	Aufbau und Bestandteile von Mythic .....	176
3.7.2	Mythic installieren .....	178
3.7.3	Agents und C2-Profiles installieren .....	180
3.7.4	Ein einfaches Szenario mit Mythic .....	180
3.7.5	Ein Szenario mit dem Mythic Agent „Apollo“ .....	186
3.7.6	Zusammenfassung und Fazit .....	192
3.7.7	Kontrollfragen zu Mythic .....	192
3.8	Das Post Exploitation Framework Havoc .....	194
3.8.1	Aufbau und Bestandteile von Havoc .....	194
3.8.2	Havoc installieren .....	197
3.8.3	Ein Szenario mit Havoc .....	200
3.8.4	Zusammenfassung und Fazit .....	208
3.8.5	Kontrollfragen zu Havoc .....	209
<b>4</b>	<b>Gegenmaßnahmen .....</b>	<b>211</b>
4.1	Allgemeine Maßnahmen zur Stärkung der IT-Sicherheit .....	212
4.2	Schwachstellenscanner .....	217
4.2.1	Kommerzielle Lösungen .....	217
4.2.2	Der Open-Source-Schwachstellenscanner von Greenbone .....	221
4.3	Einbrüche erkennen und verhindern .....	228
4.3.1	Kommerzielle Lösungen auf dem Markt .....	229
4.3.2	Snort - die quelloffene IDS/IPS-Lösung .....	231
4.4	Netzwerkmonitoring .....	240
4.4.1	Kommerzielle SIEM-Lösungen .....	241
4.4.2	Wazuh - eine Open-Source-SIEM-Lösung .....	243
4.5	Kontrollfragen zum Kapitel Gegenmaßnahmen .....	252
<b>5</b>	<b>Lösungen zu den Kontrollfragen .....</b>	<b>255</b>
5.1	Lösungen zu den Kontrollfragen in Kapitel 2 .....	255
5.2	Lösungen zu den Kontrollfragen in Abschnitt 3.1 .....	257
5.3	Lösungen zu den Kontrollfragen in Abschnitt 3.2 .....	258
5.4	Lösungen zu den Kontrollfragen in Abschnitt 3.3 .....	259
5.5	Lösungen zu den Kontrollfragen in Abschnitt 3.4 .....	260
5.6	Lösungen zu den Kontrollfragen in Abschnitt 3.5 .....	261
5.7	Lösungen zu den Kontrollfragen in Abschnitt 3.6 .....	262
5.8	Lösungen zu den Kontrollfragen in Abschnitt 3.7 .....	264
5.9	Lösungen zu den Kontrollfragen in Abschnitt 3.8 .....	265
5.10	Lösungen zu Kontrollfragen im Kapitel 4 .....	266

<b>Anhang</b> .....	<b>269</b>
A.1 Module und deren Bedeutung .....	269
A.2 Im Buch verwendete One-Liner .....	273
A.3 Nützliche Skripte und Tools .....	274
<b>Schlusswort</b> .....	<b>279</b>
<b>Index</b> .....	<b>281</b>