

# Inhaltsverzeichnis

<b>1</b>	<b>Eine Einführung in das Pentesting und in Exploiting-Frameworks</b>	<b>13</b>
1.1	Was ist Pentesting? .....	13
1.2	Die Phasen eines Penetrationstests .....	16
1.2.1	Phase 1 – Vorbereitung .....	17
1.2.2	Phase 2 – Informationsbeschaffung und -auswertung .....	17
1.2.3	Phase 3 – Bewertung der Informationen/Risikoanalyse .....	17
1.2.4	Phase 4 – Aktive Eindringversuche .....	18
1.2.5	Phase 5 – Abschlussanalyse .....	18
1.2.6	Eine etwas andere Darstellung .....	19
1.3	Die Arten des Penetrationstests .....	20
1.3.1	Kurze Darstellung der einzelnen Testarten .....	20
1.4	Exploiting-Frameworks .....	22
1.4.1	Umfang von Exploiting-Frameworks .....	22
1.4.2	Bestehende Frameworks .....	36
1.5	Dokumentation während eines Penetrationstests .....	42
1.5.1	BasKet .....	43
1.5.2	Zim Desktop Wiki .....	44
1.5.3	Dradis .....	45
1.6	Überlegungen zum eigenen Testlabor .....	51
1.6.1	Metasploitable .....	53
1.6.2	MSFU-Systeme .....	54
1.6.3	Testsysteme für Webapplikationsanalysen .....	54
1.6.4	Foundstone-Hacme-Systeme .....	55
1.7	Zusammenfassung .....	56

<b>2</b>	<b>Einführung in das Metasploit-Framework</b>	<b>59</b>
2.1	Geschichte von Metasploit	59
2.2	Architektur des Frameworks	62
2.2.1	Rex – Ruby Extension Library	63
2.2.2	Framework Core	65
2.2.3	Framework Base	65
2.2.4	Modules	66
2.2.5	Framework-Plugins	66
2.3	Installation und Update	66
2.3.1	BackTrack Linux	67
2.3.2	Metasploit auf Windows-Systemen installieren	74
2.3.3	Update von Metasploit	78
2.4	Ein erster Eindruck – das Dateisystem	81
2.5	Benutzeroberflächen	83
2.5.1	Metasploit-GUI(s)	84
2.5.2	Armitage – seit Version 3.6.0	86
2.5.3	Metasploit-CLI – Command Line Interface	89
2.5.4	Einführung in die Metasploit-Konsole (msfconsole)	91
2.6	Globaler und modularer Datastore	100
2.7	Einsatz von Datenbanken	103
2.7.1	Datenbankabfragen im Rahmen eines Penetrationstests	106
2.8	Workspaces	108
2.9	Logging und Debugging	109
2.10	Zusammenfassung	111
<b>3</b>	<b>Die Pre-Exploitation-Phase mit Metasploit</b>	<b>113</b>
3.1	Die Pre-Exploitation-Phase	113
3.2	Verschiedene Auxiliary-Module und deren Anwendung	114
3.2.1	Shodan-Suchmaschine	115
3.2.2	Internet Archive	119
3.2.3	Analyse von DNS-Systemen	122
3.2.4	Discovery-Scanner	125
3.2.5	Portscanner	126
3.2.6	SNMP-Community-Scanner	129
3.2.7	VNC-Angriffe	132
3.2.8	Windows-Scanner	136
3.2.9	SMB-Login-Scanner	138
3.2.10	Weitere Passwortangriffe	140

---

3.3	Netcat in Metasploit .....	145
3.4	Zusammenfassung .....	148
<b>4</b>	<b>Die Exploiting-Phase</b>	<b>149</b>
4.1	Einführung in die Exploitingthematik .....	149
4.2	Metasploit-CLI – msfcli .....	151
4.3	Metasploit-Konsole – msfconsole .....	156
4.3.1	Session-Management .....	167
4.4	Zusammenfassung .....	170
<b>5</b>	<b>Meterpreter-Kung-Fu – Die Post-Exploitation-Phase</b>	<b>171</b>
5.1	Grundlagen – Was zur Hölle ist Meterpreter? .....	171
5.2	Eigenschaften .....	172
5.3	Grundfunktionalitäten .....	173
5.4	Meterpreter- und Post-Exploitation-Skripte .....	179
5.4.1	Post-Information Gathering .....	182
5.4.2	VNC-Verbindung .....	188
5.4.3	Netzwerk-Enumeration .....	189
5.4.4	Weiteren Zugriff sicherstellen .....	193
5.5	Timestomp .....	198
5.6	Privilege-Escalation auf Windows-Systemen .....	201
5.7	Meterpreter-Erweiterungsmodule .....	203
5.7.1	Incognito – Token Manipulation .....	204
5.8	Pivoting .....	212
5.8.1	Portforwarding .....	212
5.8.2	Routen setzen .....	216
5.8.3	Advanced Pivoting .....	221
5.9	Systemunabhängigkeit des Meterpreter-Payloads .....	229
5.10	Zusammenfassung .....	231
<b>6</b>	<b>Automatisierungsmechanismen</b>	<b>233</b>
6.1	Ganz nüchtern betrachtet .....	233
6.2	Pre-Exploitation-Phase .....	234
6.2.1	Scanning in der Pre-Exploitation-Phase .....	236
6.2.2	Automatisierte Passwortangriffe .....	239

---

6.3	Exploitation-Phase – db_autopwn .....	242
6.3.1	Nmap-Portscanner .....	244
6.3.2	Nessus-Vulnerability-Scanner .....	250
6.3.3	NeXpose-Vulnerability-Scanner .....	263
6.4	Armitage .....	270
6.5	Post-Exploitation-Phase .....	273
6.6	Zusammenfassung .....	277
<b>7</b>	<b>Spezielle Anwendungsgebiete</b>	<b>279</b>
7.1	Webapplikationen analysieren .....	279
7.1.1	Warum Webanwendungen analysiert werden müssen .....	279
7.1.2	Wmap .....	281
7.1.3	Remote-File-Inclusion-Angriffe mit Metasploit .....	288
7.1.4	Nikto und Metasploit .....	291
7.1.5	Arachni Web Application Security Scanner Framework und Metasploit .....	294
7.2	Datenbanken analysieren .....	308
7.2.1	MS-SQL .....	308
7.2.2	Oracle .....	317
7.2.3	MySQL .....	329
7.2.4	PostgreSQL .....	334
7.3	Virtualisierte Umgebungen .....	337
7.3.1	Directory Traversal .....	338
7.4	Zusammenfassung .....	339
<b>8</b>	<b>Client-Side Attacks</b>	<b>341</b>
8.1	Sehr bekannte Client-Side-Angriffe der letzten Jahre .....	342
8.1.1	Aurora – MS10-002 .....	342
8.1.2	Browserangriffe automatisieren via browser_autopwn .....	348
8.2	Remote-Zugriff via Cross-Site-Scripting? .....	353
8.2.1	XSSF – Management von XSS Zombies mit Metasploit .....	354
8.2.2	Von XSS zur Shell .....	363
8.3	Trojanisieren einer bestehenden Applikation .....	367
8.4	Angriffe auf Client-Software über manipulierte Dateien .....	374
8.5	Ein restriktives Firewall-Regelwerk umgehen .....	378
8.6	Antivirus Evading .....	383
8.7	Zusammenfassung .....	389

---

<b>9</b>	<b>Weitere Anwendung von Metasploit</b>	<b>391</b>
9.1	Einen externen Exploit über Metasploit kontrollieren . . . . .	391
9.1.1	Multi-Handler – Fremde Exploits in Metasploit aufnehmen . . . . .	392
9.1.2	Plaintext-Session zu Meterpreter upgraden . . . . .	393
9.2	Pass the Hash . . . . .	395
9.2.1	db_autopwn in Kombination mit Pass the Hash . . . . .	399
9.3	SET – Social Engineer Toolkit . . . . .	401
9.3.1	Überblick . . . . .	402
9.3.2	Update . . . . .	404
9.3.3	Beispielanwendungen von SET . . . . .	405
9.3.4	SET automatisiert . . . . .	412
9.3.5	SET-Webinterface . . . . .	413
9.4	BeEF . . . . .	414
9.5	Tools . . . . .	421
9.6	Zusammenfassung . . . . .	424
<b>10</b>	<b>Forschung und Exploit-Entwicklung – Vom Fuzzing zum 0 Day</b>	<b>425</b>
10.1	Die Hintergründe . . . . .	425
10.2	Erkennung von Schwachstellen . . . . .	428
10.2.1	Source-Code-Analyse . . . . .	428
10.2.2	Reverse Engineering . . . . .	429
10.2.3	Fuzzing . . . . .	429
10.3	Auf dem Weg zum Exploit . . . . .	433
10.4	EIP – Ein Register, sie alle zu knechten . . . . .	438
10.5	MSFPESCAN . . . . .	439
10.6	MSF-Patterns . . . . .	443
10.7	Der Sprung ans Ziel . . . . .	446
10.8	Ein kleiner Schritt für uns, ein großer Schritt für den Exploit . . . . .	451
10.9	Kleine Helferlein . . . . .	455
10.10	Ein Metasploit-Modul erstellen . . . . .	463
10.11	IRB – Ruby Interpreter Shell . . . . .	466
10.12	Zusammenfassung . . . . .	470

<b>11</b>	<b>Metasploit Express und Metasploit Pro im IT-Sicherheitsprozess</b>	<b>471</b>
11.1	Metasploit Express und Metasploit Pro . . . . .	472
11.2	Metasploit Express . . . . .	472
11.3	Metasploit Pro . . . . .	476
	11.3.1 Installation . . . . .	482
	11.3.2 Anwendungsbeispiel . . . . .	485
11.4	Zusammenfassung . . . . .	500
	<b>Schlusswort</b>	<b>501</b>
	<b>Literaturverzeichnis und weiterführende Links</b>	<b>503</b>
	<b>Stichwortverzeichnis</b>	<b>519</b>