

---

# Inhaltsverzeichnis

<b>1</b>	<b>Eine Einführung in das Pentesting und in Exploiting-Frameworks</b>	<b>1</b>
1.1	Was ist Pentesting? .....	1
1.2	Die Phasen eines Penetrationstests .....	4
1.2.1	Phase 1 – Vorbereitung .....	5
1.2.2	Phase 2 – Informationsbeschaffung und -auswertung .....	5
1.2.3	Phase 3 – Bewertung der Informationen/Risikoanalyse .....	5
1.2.4	Phase 4 – Aktive Eindringversuche .....	6
1.2.5	Phase 5 – Abschlussanalyse .....	6
1.2.6	Eine etwas andere Darstellung .....	7
1.3	Die Arten des Penetrationstests .....	8
1.4	Exploiting-Frameworks .....	10
1.4.1	Umfang von Exploiting-Frameworks .....	10
1.4.2	Vorhandene Frameworks .....	24
1.5	Dokumentation während eines Penetrationstests .....	30
1.5.1	BasKet .....	31
1.5.2	Zim Desktop Wiki .....	32
1.5.3	Dradis .....	33
1.5.4	Microsoft OneNote .....	36
1.6	Überlegungen zum eigenen Testlabor .....	37
1.6.1	Metasploitable v2 .....	39
1.6.2	MSFU-Systeme .....	40
1.6.3	Testsysteme für Webapplikationsanalysen .....	41
1.6.4	Foundstone-Hacme-Systeme .....	42
1.7	Zusammenfassung .....	43

<b>2</b>	<b>Einführung in das Metasploit-Framework</b>	<b>45</b>
2.1	Geschichte von Metasploit . . . . .	45
2.2	Architektur des Frameworks . . . . .	48
2.2.1	Rex – Ruby Extension Library . . . . .	49
2.2.2	Framework Core . . . . .	51
2.2.3	Framework Base . . . . .	51
2.2.4	Modules . . . . .	52
2.2.5	Framework-Plugins . . . . .	52
2.3	Installation und Update . . . . .	52
2.4	Ein erster Eindruck – das Dateisystem . . . . .	58
2.5	Benutzeroberflächen . . . . .	60
2.5.1	Einführung in die Metasploit-Konsole (msfconsole) . . . . .	60
2.5.2	Armitage . . . . .	69
2.5.3	Metasploit Community Edition . . . . .	72
2.6	Globaler und modularer Datastore . . . . .	76
2.7	Einsatz von Datenbanken . . . . .	78
2.8	Workspaces . . . . .	83
2.9	Logging und Debugging . . . . .	84
2.10	Zusammenfassung . . . . .	86
<b>3</b>	<b>Die Pre-Exploitation-Phase</b>	<b>87</b>
3.1	Die Pre-Exploitation-Phase . . . . .	87
3.2	Verschiedene Auxiliary-Module und deren Anwendung . . . . .	88
3.2.1	Shodan-Suchmaschine . . . . .	89
3.2.2	Internet Archive . . . . .	92
3.2.3	Analyse von der DNS-Umgebung . . . . .	95
3.2.4	Discovery-Scanner . . . . .	98
3.2.5	Portscanner . . . . .	100
3.2.6	SNMP-Community-Scanner . . . . .	102
3.2.7	VNC-Angriffe . . . . .	105
3.2.8	Windows-Scanner . . . . .	109
3.2.9	SMB-Login-Scanner . . . . .	112
3.2.10	Weitere Passwortangriffe . . . . .	113
3.3	Netcat in Metasploit (Connect) . . . . .	120
3.4	Zusammenfassung . . . . .	122

<b>4</b>	<b>Die Exploiting-Phase</b>	<b>123</b>
4.1	Einführung in die Exploiting-Thematik	123
4.2	Metasploit-Konsole – msfconsole	126
4.3	Metasploit Community Edition	139
4.4	Zusammenfassung	145
<b>5</b>	<b>Die Post-Exploitation-Phase: Meterpreter-Kung-Fu</b>	<b>147</b>
5.1	Grundlagen – Was zur Hölle ist Meterpreter?	147
5.2	Eigenschaften	148
5.3	Grundfunktionalitäten	149
5.4	Post-Exploitation-Module und Meterpreter-Skripte	155
5.4.1	Post-Information Gathering	158
5.4.2	VNC-Verbindung	164
5.4.3	Netzwerk-Enumeration	165
5.4.4	Weiteren Zugriff sicherstellen	168
5.5	Timestomp	173
5.6	Windows-Privilegien erweitern	176
5.7	Programme direkt aus dem Speicher ausführen	185
5.8	Meterpreter-Erweiterungsmodule	188
5.9	Pivoting	197
5.9.1	Portforwarding	198
5.9.2	Routen setzen	201
5.9.3	Weitere Pivoting-Möglichkeiten	206
5.10	IRB und Railgun in der Post-Exploitation-Phase	214
5.11	Systemunabhängigkeit des Meterpreter-Payloads	216
5.12	Zusammenfassung	217
<b>6</b>	<b>Automatisierungsmechanismen und Integration von 3rd-Party-Scannern</b>	<b>219</b>
6.1	Ganz nüchtern betrachtet	219
6.2	Pre-Exploitation-Phase	220
6.2.1	Scanning in der Pre-Exploitation-Phase	222
6.2.2	Automatisierte Passwortangriffe	225
6.3	Einbinden externer Scanner	227
6.3.1	Nmap-Portscanner	227
6.3.2	Nessus-Vulnerability-Scanner	232
6.3.3	NeXpose-Vulnerability-Scanner	240
6.4	Armitage	246
6.5	IRB und Ruby-Grundlagen	249
6.6	Erweiterte Metasploit-Resource-Skripte	252

6.7	Automatisierungsmöglichkeiten in der Post-Exploitation-Phase . . . . .	256
6.7.1	Erste Möglichkeit: über die erweiterten Payload-Optionen . . . . .	256
6.7.2	Zweite Möglichkeit: über das Session-Management . . . . .	259
6.7.3	Dritte Möglichkeit: Post-Module . . . . .	259
6.8	Zusammenfassung . . . . .	262
<b>7</b>	<b>Spezielle Anwendungsgebiete</b>	<b>263</b>
7.1	Webapplikationen analysieren . . . . .	263
7.1.1	Warum Webanwendungen analysiert werden müssen . . . . .	263
7.1.2	Wmap . . . . .	265
7.1.3	Remote-File-Inclusion-Angriffe mit Metasploit . . . . .	273
7.1.4	Arachni Web Application Security Scanner Framework und Metasploit . . . . .	275
7.2	Datenbanken analysieren . . . . .	286
7.2.1	MS-SQL . . . . .	287
7.2.2	Oracle . . . . .	294
7.2.3	MySQL . . . . .	306
7.2.4	PostgreSQL . . . . .	311
7.3	Virtualisierte Umgebungen . . . . .	314
7.3.1	Metasploit im Einsatz . . . . .	315
7.3.2	Directory Traversal . . . . .	317
7.4	IPv6-Grundlagen . . . . .	318
7.5	IPv6-Netzwerke analysieren . . . . .	321
7.6	Zusammenfassung . . . . .	327
<b>8</b>	<b>Client-Side Attacks</b>	<b>329</b>
8.1	Sehr bekannte Client-Side-Angriffe der letzten Jahre . . . . .	330
8.1.1	Aurora – MS10-002 . . . . .	330
8.1.2	Browserangriffe automatisieren via browser_autopwn . . . . .	335
8.2	Remote-Zugriff via Cross-Site-Scripting . . . . .	340
8.2.1	XSSF – Management von XSS Zombies mit Metasploit . . . . .	342
8.2.2	Von XSS zur Shell . . . . .	351
8.3	Angriffe auf Client-Software über manipulierte Dateien . . . . .	354
8.4	Ein restriktives Firewall-Regelwerk umgehen . . . . .	355
8.5	Zusammenfassung . . . . .	363

<b>9</b>	<b>Weitere Anwendung von Metasploit</b>	<b>365</b>
9.1	Einen externen Exploit über Metasploit kontrollieren . . . . .	365
9.1.1	Multi-Handler – Fremde Exploits in Metasploit aufnehmen . . . . .	366
9.1.2	Plaintext-Session zu Meterpreter upgraden . . . . .	367
9.2	Pass the Hash . . . . .	369
9.3	SET – Social Engineer Toolkit . . . . .	377
9.3.1	Überblick . . . . .	378
9.3.2	Update . . . . .	379
9.3.3	Beispielanwendung . . . . .	379
9.4	BeEF – Browser-Exploitation-Framework . . . . .	387
9.5	Die Metasploit Remote API . . . . .	391
9.6	vSploit . . . . .	396
9.7	Metasploit Vulnerability Emulator . . . . .	398
9.8	Tools . . . . .	400
9.9	Zusammenfassung . . . . .	403
<b>10</b>	<b>Forschung und Exploit-Entwicklung – Vom Fuzzing zum 0 Day</b>	<b>405</b>
10.1	Die Hintergründe . . . . .	405
10.2	Erkennung von Schwachstellen . . . . .	408
10.2.1	Source-Code-Analyse . . . . .	408
10.2.2	Reverse Engineering . . . . .	409
10.2.3	Fuzzing . . . . .	409
10.3	Auf dem Weg zum Exploit . . . . .	413
10.4	EIP – Ein Register, sie alle zu knechten ... . . . . .	419
10.5	MSFPESCAN . . . . .	420
10.6	MSF-Pattern . . . . .	423
10.7	Der Sprung ans Ziel . . . . .	427
10.8	Ein kleiner Schritt für uns, ein großer Schritt für den Exploit . . . . .	431
10.9	Kleine Helferlein . . . . .	435
10.10	Ein Metasploit-Modul erstellen . . . . .	439
10.11	Immunity Debugger mit Mona – Eine Einführung . . . . .	442
10.12	Die Applikation wird analysiert – Auf dem Weg zum SEH . . . . .	449
10.12.1	Ein (Structured) Exception Handler geht seinen Weg . . . . .	452
10.12.2	Mona rockt die Entwicklung eines Metasploit-Moduls . . . . .	456
10.13	Bad Characters auffinden . . . . .	461

10.14	Command Injection auf Embedded Devices	463
10.14.1	Exploit per Download und Execute	469
10.14.2	Exploit per CMD-Stager	471
10.15	An der Metasploit-Entwicklung aktiv teilnehmen	477
10.16	Zusammenfassung	481
<b>11</b>	<b>Evading-Mechanismen</b>	<b>483</b>
11.1	Antivirus Evading	484
11.2	Trojanisieren einer bestehenden Applikation	488
11.3	Weitere Post-Exploitation-Tätigkeiten	493
11.4	IDS Evading	494
11.4.1	NOP-Generatoren	495
11.4.2	Im Exploit integrierte Evading-Funktionalitäten	497
11.4.3	Evading-Funktionen vorhandener Exploits	499
11.4.4	Erweiterte Evading-Funktionen durch den Einsatz von Fragroute	501
11.4.5	Das IPS-Plugin	509
11.5	Fazit	510
<b>12</b>	<b>Metasploit Express und Metasploit Pro im IT-Sicherheitsprozess</b>	<b>511</b>
12.1	Metasploit Express und Metasploit Pro	512
12.2	Metasploit Express	512
12.3	Metasploit Pro	514
12.4	Zusammenfassung	532
<b>13</b>	<b>Cheat Sheet</b>	<b>535</b>
13.1	Vorbereitungsarbeiten und Bedienung des Frameworks	535
13.1.1	Datastores	535
13.1.2	Datenbankabfragen im Rahmen eines Penetrationstests	536
13.1.3	Workspaces verwalten	536
13.1.4	Logging aktivieren	536
13.1.5	Metasploit-Ergebnisse exportieren	537
13.2	Anwendung eines Moduls	537
13.3	Post-Exploitation-Phase	538
13.3.1	Spuren verwischen	539
13.3.2	Pivoting bzw. in weitere Netzwerke vordringen	539
13.3.3	Lokale Privilege Escalation	540
13.3.4	Domain Privilege Escalation	541

---

13.4	Automatisierungsmechanismen .....	541
13.5	Nmap Cheat Sheet .....	542
13.6	Client-Side Attacks .....	543
13.6.1	Trojanisieren einer bestehenden Applikation und AV Evading .....	543
13.6.2	Ein restriktives Firewall-Regelwerk umgehen .....	544
<b>Anhang</b>		<b>545</b>

---

<b>Literaturverzeichnis und weiterführende Links</b>		<b>547</b>
<b>Schlusswort</b>		<b>561</b>
<b>Index</b>		<b>563</b>