

Inhaltsverzeichnis

	Geleitwort	1
	Vorwort	9
1	Eine Einführung in das Pentesting und in Exploiting-Frameworks	13
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	Vorhandene 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
1.5.4	Microsoft OneNote	48
1.6	Überlegungen zum eigenen Testlabor	49
1.6.1	Metasploitable v2	51
1.6.2	MSFU-Systeme	52
1.6.3	Testsysteme für Webapplikationsanalysen	52
1.6.4	Foundstone-Hacme-Systeme	54
1.7	Zusammenfassung	55

2	Einführung in das Metasploit-Framework	57
2.1	Geschichte von Metasploit	57
2.2	Architektur des Frameworks	60
2.2.1	Rex – Ruby Extension Library	61
2.2.2	Framework Core	63
2.2.3	Framework Base	63
2.2.4	Modules	64
2.2.5	Framework-Plugins	64
2.3	Installation und Update	64
2.3.1	Kali Linux	65
2.4	Ein erster Eindruck – das Dateisystem	70
2.5	Benutzeroberflächen	72
2.5.1	Einführung in die Metasploit-Konsole (msfconsole)	73
2.5.2	Armitage	82
2.5.3	Metasploit Community Edition	85
2.6	Globaler und modularer Datastore	88
2.7	Einsatz von Datenbanken	91
2.7.1	Datenbankabfragen im Rahmen eines Penetrationstests ...	94
2.8	Workspaces	96
2.9	Logging und Debugging	97
2.10	Zusammenfassung	99
3	Die Pre-Exploitation-Phase	101
3.1	Die Pre-Exploitation-Phase	101
3.2	Verschiedene Auxiliary-Module und deren Anwendung	102
3.2.1	Shodan-Suchmaschine	103
3.2.2	Internet Archive	106
3.2.3	Analyse von der DNS-Umgebung	109
3.2.4	Discovery-Scanner	112
3.2.5	Portscanner	114
3.2.6	SNMP-Community-Scanner	116
3.2.7	VNC-Angriffe	119
3.2.8	Windows-Scanner	123
3.2.9	SMB-Login-Scanner	126
3.2.10	Weitere Passwortangriffe	127
3.3	Netcat in Metasploit (Connect)	134
3.4	Zusammenfassung	136

4	Die Exploiting-Phase	137
4.1	Einführung in die Exploiting-Thematik	137
4.2	Metasploit-Konsole – msfconsole	140
4.2.1	Session-Management	150
4.3	Metasploit Community Edition	153
4.4	Zusammenfassung	158
5	Die Post-Exploitation-Phase: Meterpreter-Kung-Fu	161
5.1	Grundlagen – Was zur Hölle ist Meterpreter?	161
5.2	Eigenschaften	162
5.3	Grundfunktionalitäten	163
5.4	Meterpreter- und Post-Exploitation-Skripte	169
5.4.1	Post-Information Gathering	172
5.4.2	VNC-Verbindung	178
5.4.3	Netzwerk-Enumeration	179
5.4.4	Weiteren Zugriff sicherstellen	182
5.5	Timestomp	187
5.6	Windows-Privilegien erweitern	189
5.7	Programme direkt aus dem Speicher ausführen	198
5.8	Meterpreter-Erweiterungsmodule	201
5.8.1	Incognito – Token Manipulation	202
5.9	Pivoting	210
5.9.1	Portforwarding	211
5.9.2	Routen setzen	214
5.9.3	Weitere Pivoting-Möglichkeiten	219
5.10	Systemunabhängigkeit des Meterpreter-Payloads	227
5.11	Zusammenfassung	228
6	Automatisierungsmechanismen und Integration von 3rd-Party-Scannern	229
6.1	Ganz nüchtern betrachtet	229
6.2	Pre-Exploitation-Phase	230
6.2.1	Scanning in der Pre-Exploitation-Phase	232
6.2.2	Automatisierte Passwortangriffe	234
6.3	Einbinden externer Scanner	237
6.3.1	Nmap-Portscanner	237
6.3.2	Nessus-Vulnerability-Scanner	242
6.3.3	NeXpose-Vulnerability-Scanner	252
6.4	Armitage	257
6.5	IRB und Ruby-Grundlagen	260

6.6	Erweiterte Metasploit-Resource-Skripte	264
6.6	Automatisierungsmöglichkeiten in der Post-Exploitation-Phase	268
6.6.1	Erste Möglichkeit: über die erweiterten Payload-Optionen	268
6.6.2	Zweite Möglichkeit: über das Session-Management	271
6.6.3	Dritte Möglichkeit: Post-Module	272
6.7	Zusammenfassung	275
7	Spezielle Anwendungsgebiete	277
7.1	Webapplikationen analysieren	277
7.1.1	Warum Webanwendungen analysiert werden müssen	277
7.1.2	Wmap	279
7.1.3	Remote-File-Inclusion-Angriffe mit Metasploit	286
7.1.4	Arachni Web Application Security Scanner Framework und Metasploit	288
7.2	Datenbanken analysieren	300
7.2.1	MS-SQL	300
7.2.2	Oracle	308
7.2.3	MySQL	320
7.2.4	PostgreSQL	325
7.3	Virtualisierte Umgebungen	328
7.3.1	Metasploit im Einsatz	329
7.3.2	Directory Traversal	331
7.4	IPv6-Grundlagen	332
7.4.1	Konfigurationsgrundlagen	334
7.5	IPv6-Netzwerke analysieren	335
7.6	Zusammenfassung	341
8	Client-Side Attacks	343
8.1	Sehr bekannte Client-Side-Angriffe der letzten Jahre	344
8.1.1	Aurora – MS10-002	344
8.1.2	Browserangriffe automatisieren via browser_autopwn ...	349
8.2	Remote-Zugriff via Cross-Site-Scripting	354
8.2.1	XSSF – Management von XSS Zombies mit Metasploit ..	356
8.2.2	Von XSS zur Shell	365
8.3	Angriffe auf Client-Software über manipulierte Dateien	368
8.4	Ein restriktives Firewall-Regelwerk umgehen	369
8.5	Zusammenfassung	377

9	Weitere Anwendung von Metasploit	379
9.1	Einen externen Exploit über Metasploit kontrollieren	379
9.1.1	Multi-Handler – Fremde Exploits in Metasploit aufnehmen	380
9.1.2	Plaintext-Session zu Meterpreter upgraden	381
9.2	Pass the Hash	383
9.2.1	Pass the Hash automatisiert	387
9.3	SET – Social Engineer Toolkit	391
9.3.1	Überblick	392
9.3.2	Update	393
9.3.3	Beispielanwendung	393
9.4	BeEF – Browser-Exploitation-Framework	401
9.5	Die Metasploit Remote API	406
9.6	vSploit	410
9.7	Tools	413
9.8	Zusammenfassung	416
10	Forschung und Exploit-Entwicklung – Vom Fuzzing zum 0 Day	417
10.1	Die Hintergründe	417
10.2	Erkennung von Schwachstellen	420
10.2.1	Source-Code-Analyse	420
10.2.2	Reverse Engineering	421
10.2.3	Fuzzing	421
10.3	Auf dem Weg zum Exploit	425
10.4	EIP – Ein Register, sie alle zu knechten	430
10.5	MSFPESCAN	431
10.6	MSF-Pattern	435
10.7	Der Sprung ans Ziel	438
10.8	Ein kleiner Schritt für uns, ein großer Schritt für den Exploit	443
10.9	Kleine Helferlein	447
10.10	Ein Metasploit-Modul erstellen	450
10.11	Immunity Debugger mit Mona – Eine Einführung	454
10.11.1	Mona-Grundlagen	455
10.12	Die Applikation wird analysiert – Auf dem Weg zum SEH	461
10.12.1	Ein (Structured) Exception Handler geht seinen Weg	465
10.12.2	Mona rockt die Entwicklung eines Metasploit-Moduls ..	468

10.13	Command Injection auf Embedded Devices	473
10.13.1	Exploit per Download und Execute	478
10.13.2	Exploit per CMD-Stager	480
10.14	An der Metasploit-Entwicklung aktiv teilnehmen	486
10.15	Zusammenfassung	490
11	Evading-Mechanismen	491
11.1	Antivirus Evading	492
11.2	Trojanisieren einer bestehenden Applikation	496
11.3	Weitere Post-Exploitation-Tätigkeiten	501
11.4	IDS Evading	502
11.4.1	NOP-Generatoren	503
11.4.2	Im Exploit integrierte Evading-Funktionalitäten	505
11.4.3	Evading-Funktionen vorhandener Exploits	507
11.4.4	Erweiterte Evading-Funktionen durch den Einsatz von Fragroute	509
11.4.5	Das IPS-Plugin	517
11.5	Fazit	517
12	Metasploit Express und Metasploit Pro im IT-Sicherheitsprozess	519
12.1	Metasploit Express und Metasploit Pro	520
12.2	Metasploit Express	520
12.3	Metasploit Pro	522
12.3.1	Anwendungsbeispiel	527
12.4	Zusammenfassung	541
13	Cheat Sheet	543
	Literaturverzeichnis und weiterführende Links	553
	Schlusswort	567
	Stichwortverzeichnis	569