

Inhaltsverzeichnis

1	Einleitung	1
1.1	Was ist das Metasploit-Framework?	2
1.2	Ziel des Buches	2
1.3	Wer sollte dieses Buch lesen?	3
1.4	Was erwartet Sie in diesem Buch?	3
1.5	Was behandelt das Buch nicht?	4
1.6	Haftungsausschluss	4
1.7	Danksagung	4
2	Die Testumgebung	7
2.1	VirtualBox 4.1 und phpVirtualBox installieren	8
2.2	Virtuelle Maschinen erstellen	13
2.2.1	Backtrack 5 als VMware-Image nutzen	14
2.2.2	Nexpose und Metasploit Community in virtuelle Umgebungen integrieren	19
2.2.3	Windows 7 mit Metasploit und Nmap	24
2.3	Das Testumfeld für Webapplikationen	25
2.3.1	Damn Vulnerable Web Application/DVWA	27
2.3.2	Badstore Online Shop	29
2.3.3	Hacme Bank von Foundstone	30
2.4	Die Metasploit »Vulnerable VM«	33
2.5	Debian 5.0 (Lenny) in einer virtuellen Umgebung	34

2.6	Das Netzwerk und die Firewall	35
2.6.1	Die Netzwerkadapter	35
2.6.2	Ein einfaches Testnetzwerk	37
2.6.3	Die erweiterte Netzwerkkonfiguration mit Firewall	37
2.6.4	Die Firewall	39
2.7	Zusammenfassung	43
3	Das Metasploit-Framework	45
3.1	Die Metasploit-Framework-Architektur	45
3.2	Metasploit-Module	46
3.2.1	Exploits	46
3.2.2	Payloads	47
3.2.3	Encoder	48
3.2.4	NOPs	49
3.2.5	Auxiliary	49
3.3	Metasploit-Konsole (msfconsole)	50
3.4	Metasploit-Client (msfcli)	59
3.5	Das grafische User-Interface (msfgui)	62
3.6	Armitage – (noch) eine grafische Oberfläche für das Framework	64
3.7	Metasploit Community	66
4	Metasploit für Pentester	69
4.1	Informationsbeschaffung	70
4.1.1	Portscanning	70
4.1.2	Dienste erkennen	77
4.1.3	Passwörter sniffen	79
4.1.4	Ein einfacher TCP-Scanner im »Eigenbau«	80
4.2	Verwundbare Systeme erkennen	82
4.2.1	Schwachstellenscans mit Nessus	82
4.2.2	Schwachstellenscans mit Nmap	89
4.3	Schwachstellen ausnutzen	95
4.3.1	Grundlagen	95
4.3.2	Manuelles Vorgehen	98
4.3.3	Automatisiertes Vorgehen	103

4.4	Post-Exploitation	106
4.4.1	Metasploit Privilege Escalation	107
4.4.2	Keylogrecorder, Hashdump und Winenum	108
4.4.3	Pass-the-Hash und Token-Manipulation	112
4.4.4	Spuren verwischen und Zugriff verwalten	118
4.5	Zusammenfassung	131
5	Anwendungsszenarien	133
5.1	Die Schwachstelle im E-Mail-Server Exim4 ausnutzen	134
5.2	Die Schwachstelle im Samba-Dienst ausnutzen	136
5.3	Die Schwachstelle im Windows-Druckerwarteschlangendienst ausnutzen	138
5.3.1	Ermittlung der Hosts im Netzwerksegment	139
5.3.2	Vulnerability-Scan durch Nexpose Community	140
5.3.3	Ausnutzen der Schwachstellen	143
5.4	Die Microsoft-LNK-Lücke ausnutzen	145
5.5	Die Internet-Explorer-Schwachstelle (CSS Recursive Import)	149
5.6	Die Schwachstellen im Adobe Reader ausnutzen	154
5.7	Ein trojanisches Pferd für Linux erstellen	158
5.7.1	Das trojanische Pferd anfertigen	159
5.7.2	Das trojanische Pferd auf dem Client-PC einsetzen	162
5.8	Eine Hintertür für das MacBook	164
5.9	Virenschutzprogramme umgehen	168
5.9.1	Grundlagen zu msfpayload und msfencode	169
5.9.2	Den Trojaner erstellen	172
5.9.3	Wird unser Trojaner von Virenschutzprogrammen erkannt?	174
5.9.4	Das Zielsystem angreifen	175
5.9.5	Alternative Methoden	177
5.10	Webseiten prüfen mit Nikto und Metasploit	180
5.11	SET – das Social-Engineer Toolkit	186
5.12	Das Browser Exploitation Framework (BeEF)	195
5.12.1	BeEF installieren und konfigurieren	196
5.12.2	BeEF über das Metasploit-Plug-in steuern	200
5.12.3	Zusammenfassung	204

5.13	Karmetasploit	205
5.13.1	Was ist Karmetasploit?	205
5.13.2	Die virtuelle Umgebung vorbereiten	206
5.13.3	Karmetasploit auf dem Notebook installieren	208
5.13.4	Der Angriff	212
5.13.5	Schlussfolgerungen und Bemerkungen	216
5.14	Windows-7-UAC-Bypass	217
5.14.1	Benutzerrechte in einer Meterpreter-Session erlangen	218
5.14.2	Windows 7 (64 Bit) angreifen und Rechte eskalieren	220
5.14.3	Gegenmaßnahmen	221
5.15	In lokale Netzwerke über das Internet eindringen	222
5.15.1	Das Szenario	222
5.15.2	Den Angriff vorbereiten	223
5.15.3	In das lokale Netzwerk eindringen	227
5.15.4	Das lokale Netzwerk erkunden	230
5.15.5	Den Dateiserver penetrieren	232
5.15.6	Die anderen Hosts im Netzwerk übernehmen	234
5.15.7	Schlussfolgerungen und Gegenmaßnahmen	236
5.16	Wie kommt der Keylogger auf die Webseite?	237
5.16.1	Das Szenario	237
5.16.2	Den Angriff vorbereiten	239
5.16.3	Den Angriff ausführen	242
5.16.4	Eine XSS-Schwachstelle im Online-Shop ausnutzen	243
5.16.5	Zusammenfassung und Gegenmaßnahmen	248
5.17	Zusammenfassung und Schlussfolgerungen	249
6	Das kommerzielle Produkt Metasploit Pro im Vergleich	251
6.1	Die einzelnen Komponenten von Metasploit Pro	252
6.2	Metasploit Pro im Testnetzwerk einsetzen	255
6.3	Zusammenfassung	261
6.4	Schlusswort	263
Anhang		
A.1	Metasploit-Konsole, Hilfe (msfconsole)	267
A.2	Metasploit-Client (msfcli)	268
A.3	NeXpose-Modul	269

A.4	nexpose_scan	269
A.5	Meterpreter-Kommandos	270
A.6	Meterpreter-Module	272
A.7	Sessions	274
A.8	msfvenom	275
A.9	msfencode	276
A.10	Liste der verfügbaren Encoder	276
A.11	Befehlsübersicht sendEmail	277
A.12	Karmasploit-Skript (karma.rc)	278
A.13	Nessus-Hilfe	280
A.14	Metasploit »Vulnerable VM« – Nutzerinformationen	281
A.15	Nikto-Hilfe	282
A.16	Verwenden des Net User- und des Net Group-Befehls	283
A.17	Der Execute Befehl	284

Stichwortverzeichnis**285**