

Frank Neugebauer

Penetration Testing mit Metasploit

Eine praktische Einführung

Frank Neugebauer
metasploit@pentestit.de

Lektorat: René Schönfeldt
Copy-Editing: Ursula Zimpfer, Herrenberg
Herstellung: Frank Heidt
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: Media-Print Informationstechnologie, Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-89864-739-7

1. Auflage 2011
Copyright © 2011 dpunkt.verlag GmbH
Ringstraße 19 B
69115 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

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?	3
1.6	Haftungsausschluss	4
1.7	Danksagung	4
2	Die Testumgebung	5
2.1	VMware-Server 2.0.2 installieren	6
2.2	Virtuelle Maschinen erstellen	8
2.2.1	Windows XP mit Metasploit und Nmap	9
2.2.2	Backtrack mit Nessus und NeXpose installieren	10
2.3	Das Testumfeld für Webapplikationen	20
2.3.1	Damn Vulnerable Web Application (DVWA)	20
2.3.2	Badstore Online Shop	23
2.3.3	Hacme Bank von Foundstone	24
2.4	Die Metasploit »Vulnerable VM«	27
2.5	Debian 5.0 (Lenny) in einer virtuellen Umgebung	27
2.6	Das Netzwerk und die Firewall	29
2.6.1	Das Netzwerk	29
2.6.2	Die Firewall	30
2.7	Zusammenfassung	33

3	Das Metasploit-Framework	35
3.1	Die Metasploit-Framework-Architektur	35
3.2	Metasploit-Module	36
3.2.1	Exploits	36
3.2.2	Payloads	37
3.2.3	Encoder	38
3.2.4	NOPs	39
3.2.5	Auxiliary	39
3.3	Metasploit-Konsole (msfconsole)	40
3.4	Metasploit-Client (msfcli)	49
3.5	Das grafische User-Interface (msfgui)	51
3.6	Die Cygwin Shell	54
3.7	Zusammenfassung	56
4	Metasploit für Pentester	57
4.1	Informationsbeschaffung	58
4.1.1	Portscanning	58
4.1.2	Dienste erkennen	63
4.1.3	Passwörter sniffen	65
4.1.4	Ein einfacher TCP-Scanner im »Eigenbau«	67
4.2	Verwundbare Systeme erkennen	68
4.2.1	Schwachstellenscans mit Nessus	69
4.2.2	Schwachstellenscans mit NeXpose	76
4.3	Schwachstellen ausnutzen	81
4.3.1	Grundlagen	81
4.3.2	Manuelles Vorgehen	85
4.3.3	Automatisiertes Vorgehen	89
4.4	Post-Exploitation	92
4.4.1	Metasploit Privilege Escalation	94
4.4.2	Keylogger, Hashdump und Winenum	95
4.4.3	Spuren verwischen und Zugriff verwalten	98
4.5	Zusammenfassung	105

5	Anwendungsszenarien	107
5.1	Die Schwachstelle im E-Mail-Server Exim4 ausnutzen	108
5.2	Die Schwachstelle im Samba-Dienst ausnutzen	110
5.3	Die Schwachstelle im Windows-Druckerwarteschlangendienst ausnutzen	112
5.4	Die Microsoft-LNK-Lücke ausnutzen	115
5.5	Die Internet-Explorer-Schwachstelle (CSS Recursive Import)	119
5.6	Die Schwachstellen im Adobe Reader ausnutzen	124
5.7	Ein trojanisches Pferd für Linux erstellen	128
5.7.1	Das trojanische Pferd anfertigen	129
5.7.2	Das trojanische Pferd auf dem Client-PC einsetzen	132
5.8	Eine Hintertür für das MacBook	134
5.9	Virenschutzprogramme umgehen	138
5.9.1	Grundlagen zu msfpayload und msfencode	139
5.9.2	Den Trojaner erstellen	141
5.9.3	Den Trojaner in den Wirt einbetten	143
5.9.4	Wird unser Trojaner von Virenschutzprogrammen erkannt? 145	
5.9.5	Das Zielsystem angreifen 146	
5.10	Webseiten prüfen mit Nikto und Metasploit	148
5.11	SET – das Social Engineering Toolkit	154
5.12	Das Browser Exploitation Framework (BeEF)	165
5.12.1	BeEF installieren und konfigurieren	165
5.12.2	Metasploit Browser Exploit mit BeEF	168
5.12.3	Metasploit SMB Challenge Theft	171
5.13	Karmetasploit	172
5.13.1	Was ist Karmetasploit?	173
5.13.2	Die virtuelle Umgebung vorbereiten	173
5.13.3	Karmetasploit auf dem Notebook installieren	176
5.13.4	Der Angriff	179
5.13.5	Schlussfolgerungen und Bemerkungen	183
5.14	Windows-7-UAC-Bypass	184
5.14.1	Benutzerrechte in einer Meterpreter-Session erlangen	186
5.14.2	Windows 7 (64 Bit) angreifen und Rechte eskalieren	187
5.14.3	Gegenmaßnahmen	189
5.15	Zusammenfassung und Schlussfolgerungen	189

6	Das kommerzielle Produkt Metasploit Pro im Vergleich	191
6.1	Die einzelnen Komponenten von Metasploit Pro	192
6.2	Metasploit Pro im Testnetzwerk einsetzen	195
6.3	Zusammenfassung	199
6.3	Schlusswort	200

Anhang

A.1	Metasploit-Konsole, Hilfe (msfconsole)	203
A.2	Metasploit-Client (msfcli)	205
A.3	NeXpose-Modul	205
A.4	nexpose_scan	206
A.5	Meterpreter-Kommandos	206
A.6	Meterpreter-Module	209
A.7	db_autopwn	209
A.8	Sessions	210
A.9	msfencode	210
A.10	Liste der verfügbaren Encoder	211
A.11	Befehlsübersicht sendEmail	211
A.12	Karmetasploit-Skript (karma.rc)	212
A.13	Nessus-Hilfe	214
A.14	Metasploit »Vulnerable VM« – Nutzerinformationen	215
A.15	Nikto-Hilfe	217

Stichwortverzeichnis

219