

# **METASPLOIT**

## **The Penetration Tester's Guide**

**by David Kennedy,  
Jim O'Gorman, Devon Kearns,  
and Mati Aharoni**



**no starch  
press**

San Francisco

**METASPLOIT.** Copyright © 2011 by David Kennedy, Jim O’Gorman, Devon Kearns, and Mati Aharoni

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

15 14 13 12 11      1 2 3 4 5 6 7 8 9

ISBN-10: 1-59327-288-X

ISBN-13: 978-1-59327-288-3

Publisher: William Pollock

Production Editor: Alison Law

Cover Illustration: Hugh D’Andrade

Interior Design: Octopod Studios

Developmental Editors: William Pollock and Tyler Ortman

Technical Reviewer: Scott White

Copyeditor: Lisa Theobald

Compositors: Susan Glinert Stevens

Proofreader: Ward Webber

Indexer: BIM Indexing & Proofreading Services

For information on book distributors or translations, please contact No Starch Press, Inc. directly:

No Starch Press, Inc.

38 Ringold Street, San Francisco, CA 94103

phone: 415.863.9900; fax: 415.863.9950; [info@nostarch.com](mailto:info@nostarch.com); [www.nostarch.com](http://www.nostarch.com)

Library of Congress Cataloging-in-Publication Data

A catalog record of this book is available from the Library of Congress.

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

# BRIEF CONTENTS

Foreword by HD Moore .....	xiii
Preface .....	xvii
Acknowledgments .....	xix
Introduction .....	xxi
Chapter 1: The Absolute Basics of Penetration Testing .....	1
Chapter 2: Metasploit Basics .....	7
Chapter 3: Intelligence Gathering .....	15
Chapter 4: Vulnerability Scanning.....	35
Chapter 5: The Joy of Exploitation.....	57
Chapter 6: Meterpreter.....	75
Chapter 7: Avoiding Detection .....	99
Chapter 8: Exploitation Using Client-Side Attacks.....	109
Chapter 9: Metasploit Auxiliary Modules .....	123
Chapter 10: The Social-Engineer Toolkit.....	135
Chapter 11: Fast-Track.....	163
Chapter 12: Karmetasploit .....	177
Chapter 13: Building Your Own Module.....	185

Chapter 14: Creating Your Own Exploits .....	197
Chapter 15: Porting Exploits to the Metasploit Framework.....	215
Chapter 16: Meterpreter Scripting.....	235
Chapter 17: Simulated Penetration Test.....	251
Appendix A: Configuring Your Target Machines .....	267
Appendix B: Cheat Sheet .....	275
Index .....	285

# CONTENTS IN DETAIL

<b>FOREWORD by HD Moore</b>	<b>xiii</b>
-----------------------------	-------------

<b>PREFACE</b>	<b>xvii</b>
----------------	-------------

<b>ACKNOWLEDGMENTS</b>	<b>xix</b>
------------------------	------------

Special Thanks .....	xx
----------------------	----

<b>INTRODUCTION</b>	<b>xxi</b>
---------------------	------------

Why Do A Penetration Test? .....	xxii
Why Metasploit? .....	xxii
A Brief History of Metasploit .....	xxii
About this Book .....	xxiii
What's in the Book? .....	xxiii
A Note on Ethics .....	xxiv

<b>1</b>	
<b>THE ABSOLUTE BASICS OF PENETRATION TESTING</b>	<b>1</b>

The Phases of the PTES .....	2
Pre-engagement Interactions .....	2
Intelligence Gathering .....	2
Threat Modeling .....	2
Vulnerability Analysis .....	3
Exploitation .....	3
Post Exploitation .....	3
Reporting .....	4
Types of Penetration Tests .....	4
Overt Penetration Testing .....	5
Covert Penetration Testing .....	5
Vulnerability Scanners .....	5
Pulling It All Together .....	6

<b>2</b>	
<b>METASPLOIT BASICS</b>	<b>7</b>

Terminology .....	7
Exploit .....	8
Payload .....	8
Shellcode .....	8
Module .....	8
Listener .....	8
Metasploit Interfaces .....	8
MSFconsole .....	9
MSFcli .....	9
Armitage .....	11

Metasploit Utilities .....	12
MSFpayload .....	12
MSFencode .....	13
Nasm Shell .....	13
Metasploit Express and Metasploit Pro .....	14
Wrapping Up .....	14

### **3**

## **INTELLIGENCE GATHERING**

### **15**

Passive Information Gathering .....	16
whois Lookups .....	16
Netcraft .....	17
NSLookup .....	18
Active Information Gathering .....	18
Port Scanning with Nmap .....	18
Working with Databases in Metasploit .....	20
Port Scanning with Metasploit .....	25
Targeted Scanning .....	26
Server Message Block Scanning .....	26
Hunting for Poorly Configured Microsoft SQL Servers .....	27
SSH Server Scanning .....	28
FTP Scanning .....	29
Simple Network Management Protocol Sweeping .....	30
Writing a Custom Scanner .....	31
Looking Ahead .....	33

### **4**

## **VULNERABILITY SCANNING**

### **35**

The Basic Vulnerability Scan .....	36
Scanning with NeXpose .....	37
Configuration .....	37
Importing Your Report into the Metasploit Framework .....	42
Running NeXpose Within MSFconsole .....	43
Scanning with Nessus .....	44
Nessus Configuration .....	44
Creating a Nessus Scan Policy .....	45
Running a Nessus Scan .....	47
Nessus Reports .....	47
Importing Results into the Metasploit Framework .....	48
Scanning with Nessus from Within Metasploit .....	49
Specialty Vulnerability Scanners .....	51
Validating SMB Logins .....	51
Scanning for Open VNC Authentication .....	52
Scanning for Open X11 Servers .....	54
Using Scan Results for Autopwning .....	56

### **5**

## **THE JOY OF EXPLOITATION**

### **57**

Basic Exploitation .....	58
msf> show exploits .....	58
msf> show auxiliary .....	58

msf> show options .....	58
msf> show payloads .....	60
msf> show targets .....	62
info .....	63
set and unset .....	63
setg and unsetg .....	64
save .....	64
Exploiting Your First Machine .....	64
Exploiting an Ubuntu Machine .....	68
All-Ports Payloads: Brute Forcing Ports .....	71
Resource Files .....	72
Wrapping Up .....	73

## 6

### METERPRETER

75

Compromising a Windows XP Virtual Machine .....	76
Scanning for Ports with Nmap .....	76
Attacking MS SQL .....	76
Brute Forcing MS SQL Server .....	78
The xp_cmdshell .....	79
Basic Meterpreter Commands .....	80
Capturing Keystrokes .....	81
Dumping Usernames and Passwords .....	82
Extracting the Password Hashes .....	82
Dumping the Password Hash .....	83
Pass the Hash .....	84
Privilege Escalation .....	85
Token Impersonation .....	87
Using ps .....	87
Pivoting onto Other Systems .....	89
Using Meterpreter Scripts .....	92
Migrating a Process .....	92
Killing Antivirus Software .....	93
Obtaining System Password Hashes .....	93
Viewing All Traffic on a Target Machine .....	93
Scraping a System .....	93
Using Persistence .....	94
Leveraging Post Exploitation Modules .....	95
Upgrading Your Command Shell to Meterpreter .....	95
Manipulating Windows APIs with the Railgun Add-On .....	97
Wrapping Up .....	97

## 7

### AVOIDING DETECTION

99

Creating Stand-Alone Binaries with MSFpayload .....	100
Evading Antivirus Detection .....	101
Encoding with MSFencode .....	102
Multi-encoding .....	103
Custom Executable Templates .....	105
Launching a Payload Stealthily .....	106

Packers .....	107
A Final Note on Antivirus Software Evasion .....	108

## **8**

### **EXPLOITATION USING CLIENT-SIDE ATTACKS 109**

Browser-Based Exploits .....	110
How Browser-Based Exploits Work .....	111
Looking at NOPs .....	112
Using Immunity Debugger to Decipher NOP Shellcode .....	112
Exploring the Internet Explorer Aurora Exploit .....	116
File Format Exploits .....	119
Sending the Payload .....	120
Wrapping Up .....	121

## **9**

### **METASPLOIT AUXILIARY MODULES 123**

Auxiliary Modules in Use .....	126
Anatomy of an Auxiliary Module .....	128
Going Forward .....	133

## **10**

### **THE SOCIAL-ENGINEER TOOLKIT 135**

Configuring the Social-Engineer Toolkit .....	136
Spear-Phishing Attack Vector .....	137
Web Attack Vectors .....	142
Java Applet .....	142
Client-Side Web Exploits .....	146
Username and Password Harvesting .....	148
Tabnabbing .....	150
Man-Left-in-the-Middle .....	150
Web Jacking .....	151
Putting It All Together with a Multipronged Attack .....	153
Infectious Media Generator .....	157
Teensy USB HID Attack Vector .....	157
Additional SET Features .....	160
Looking Ahead .....	161

## **11**

### **FAST-TRACK 163**

Microsoft SQL Injection .....	164
SQL Injector—Query String Attack .....	165
SQL Injector—POST Parameter Attack .....	166
Manual Injection .....	167
MSSQL Bruter .....	168
SQLPwnage .....	172
Binary-to-Hex Generator .....	174
Mass Client-Side Attack .....	175
A Few Words About Automation .....	176



<b>12</b>	<b>KARMETASPLOIT</b>	<b>177</b>
Configuration .....		178
Launching the Attack .....		179
Credential Harvesting .....		181
Getting a Shell .....		182
Wrapping Up .....		184
<b>13</b>	<b>BUILDING YOUR OWN MODULE</b>	<b>185</b>
Getting Command Execution on Microsoft SQL .....		186
Exploring an Existing Metasploit Module .....		187
Creating a New Module .....		189
PowerShell .....		189
Running the Shell Exploit .....		190
Creating powershell_upload_exec .....		192
Conversion from Hex to Binary .....		192
Counters .....		194
Running the Exploit .....		195
The Power of Code Reuse .....		196
<b>14</b>	<b>CREATING YOUR OWN EXPLOITS</b>	<b>197</b>
The Art of Fuzzing .....		198
Controlling the Structured Exception Handler .....		201
Hopping Around SEH Restrictions .....		204
Getting a Return Address .....		206
Bad Characters and Remote Code Execution .....		210
Wrapping Up .....		213
<b>15</b>	<b>PORTING EXPLOITS TO THE METASPLOIT FRAMEWORK</b>	<b>215</b>
Assembly Language Basics .....		216
EIP and ESP Registers .....		216
The JMP Instruction Set .....		216
NOPs and NOP Slides .....		216
Porting a Buffer Overflow .....		216
Stripping the Existing Exploit .....		218
Configuring the Exploit Definition .....		219
Testing Our Base Exploit .....		220
Implementing Features of the Framework .....		221
Adding Randomization .....		222
Removing the NOP Slide .....		223
Removing the Dummy Shellcode .....		223
Our Completed Module .....		224
SEH Overwrite Exploit .....		226
Wrapping Up .....		233

<b>16</b>	<b>METERPRETER SCRIPTING</b>	<b>235</b>
Meterpreter Scripting Basics .....		235
Meterpreter API .....		241
Printing Output .....		241
Base API Calls .....		242
Meterpreter Mixins .....		242
Rules for Writing Meterpreter Scripts .....		244
Creating Your Own Meterpreter Script .....		244
Wrapping Up .....		250
<b>17</b>	<b>SIMULATED PENETRATION TEST</b>	<b>251</b>
Pre-engagement Interactions .....		252
Intelligence Gathering .....		252
Threat Modeling .....		253
Exploitation .....		255
Customizing MSFconsole .....		255
Post Exploitation .....		257
Scanning the Metasploitable System .....		258
Identifying Vulnerable Services .....		259
Attacking Apache Tomcat .....		260
Attacking Obscure Services .....		262
Covering Your Tracks .....		264
Wrapping Up .....		266
<b>A</b>	<b>CONFIGURING YOUR TARGET MACHINES</b>	<b>267</b>
Installing and Setting Up the System .....		267
Booting Up the Linux Virtual Machines .....		268
Setting Up a Vulnerable Windows XP Installation .....		269
Configuring Your Web Server on Windows XP .....		269
Building a SQL Server .....		269
Creating a Vulnerable Web Application .....		272
Updating BackTrack .....		273
<b>B</b>	<b>CHEAT SHEET</b>	<b>275</b>
MSFconsole Commands .....		275
Meterpreter Commands .....		277
MSFpayload Commands .....		280
MSFencode Commands .....		280
MSFcli Commands .....		281
MSF, Ninja, Fu .....		281
MSFvenom .....		281
Meterpreter Post Exploitation Commands .....		282
<b>INDEX</b>		<b>285</b>