

# Metasploit: The Penetration Tester's Guide

Kennedy, David

ISBN-13: 9781593272883

## Table of Contents

Foreword; Preface; Acknowledgments; Special Thanks; Introduction; Why Do a Penetration Test?; Why Metasploit?; A Brief History of Metasploit; About This Book; What's in the Book?; A Note on Ethics; Chapter 1: The Absolute Basics of Penetration Testing; 1.1 The Phases of the PTES; 1.2 Types of Penetration Tests; 1.3 Vulnerability Scanners; 1.4 Pulling It All Together; Chapter 2: Metasploit Basics; 2.1 Terminology; 2.2 Metasploit Interfaces; 2.3 Metasploit Utilities; 2.4 Metasploit Express and Metasploit Pro; 2.5 Wrapping Up; Chapter 3: Intelligence Gathering; 3.1 Passive Information Gathering; 3.2 Active Information Gathering; 3.3 Targeted Scanning; 3.4 Writing a Custom Scanner; 3.5 Looking Ahead; Chapter 4: Vulnerability Scanning; 4.1 The Basic Vulnerability Scan; 4.2 Scanning with NeXpose; 4.3 Scanning with Nessus; 4.4 Specialty Vulnerability Scanners; 4.5 Using Scan Results for Autopwning; Chapter 5: The Joy of Exploitation; 5.1 Basic Exploitation; 5.2 Exploiting Your First Machine; 5.3 Exploiting an Ubuntu Machine; 5.4 All-Ports Payloads: Brute Forcing Ports; 5.5 Resource Files; 5.6 Wrapping Up; Chapter 6: Meterpreter; 6.1 Compromising a Windows XP Virtual Machine; 6.2 Dumping Usernames and Passwords; 6.3 Pass the Hash; 6.4 Privilege Escalation; 6.5 Token Impersonation; 6.6 Using ps; 6.7 Pivoting onto Other Systems; 6.8 Using Meterpreter Scripts; 6.9 Leveraging Post Exploitation Modules; 6.10 Upgrading Your Command Shell to Meterpreter; 6.11 Manipulating Windows APIs with the Railgun Add-On; 6.12 Wrapping Up; Chapter 7: Avoiding Detection; 7.1 Creating Stand-Alone Binaries with MSFpayload; 7.2 Evading Antivirus Detection; 7.3 Custom Executable Templates; 7.4 Launching a Payload Stealthily; 7.5 Packers; 7.6 A Final Note on Antivirus Software Evasion; Chapter 8: Exploitation Using Client-Side Attacks; 8.1 Browser-Based Exploits; 8.2 Using Immunity Debugger to Decipher NOP Shellcode; 8.3 Exploring the Internet Explorer Aurora Exploit; 8.4 File Format Exploits; 8.5 Sending the Payload; 8.6 Wrapping Up; Chapter 9: Metasploit Auxiliary Modules; 9.1 Auxiliary Modules in Use; 9.2 Anatomy of an Auxiliary Module; 9.3 Going Forward; Chapter 10: The Social-Engineer Toolkit; 10.1 Configuring the Social-Engineer Toolkit; 10.2 Spear-Phishing Attack Vector; 10.3 Web Attack Vectors; 10.4 Infectious Media Generator; 10.5 Teensy USB HID Attack Vector; 10.6 Additional SET Features; 10.7 Looking Ahead; Chapter 11: Fast-Track; 11.1 Microsoft SQL Injection; 11.2 Binary-to-Hex Generator; 11.3 Mass Client-Side Attack; 11.4 A Few Words About Automation; Chapter 12: Karmetasploit; 12.1 Configuration; 12.2 Launching the Attack; 12.3 Credential Harvesting; 12.4 Getting a Shell; 12.5 Wrapping Up; Chapter 13: Building Your Own Module; 13.1 Getting Command Execution on Microsoft SQL; 13.2 Exploring an Existing Metasploit Module; 13.3 Creating a New Module; 13.4 The Power of Code Reuse; Chapter 14: Creating Your Own Exploits; 14.1 The Art of Fuzzing; 14.2 Controlling the Structured Exception Handler; 14.3 Hopping Around SEH Restrictions; 14.4 Getting a Return Address; 14.5 Bad Characters and Remote Code Execution; 14.6 Wrapping Up; Chapter 15: Porting Exploits to the Metasploit Framework; 15.1 Assembly Language Basics; 15.2 Porting a Buffer Overflow; 15.3 SEH Overwrite Exploit; 15.4 Wrapping Up; Chapter 16: Meterpreter Scripting; 16.1 Meterpreter Scripting Basics; 16.2 Meterpreter API; 16.3 Rules for Writing Meterpreter Scripts; 16.4 Creating Your Own Meterpreter Script; 16.5 Wrapping Up; Chapter 17: Simulated Penetration Test; 17.1 Pre-engagement Interactions; 17.2 Intelligence Gathering; 17.3 Threat Modeling; 17.4 Exploitation; 17.5 Customizing MSFconsole; 17.6 Post Exploitation; 17.7 Attacking Apache Tomcat; 17.8 Attacking Obscure Services; 17.9 Covering Your Tracks; 17.10 Wrapping Up; Configuring Your Target Machines; Installing and Setting Up the System; Booting Up the Linux Virtual Machines; Setting Up a Vulnerable Windows XP Installation; Cheat Sheet; MSFconsole Commands; Meterpreter Commands; MSFpayload Commands; MSFencode Commands; MSFcli Commands; MSF, Ninja, Fu; MSFvenom; Meterpreter Post Exploitation Commands; Colophon; Updates;