Metasploit [the penetration tester's guide /

Kennedy, David (
1982-)

No Starch Press,
2011

Monografía

"The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, documentation is lacking and the tool can be hard to grasp for first-time users. Metasploit: A Penetration Tester's Guide fills this gap by teaching you how to harness the Framework, use its many features, and interact with the vibrant community of Metasploit contributors. The authors begin by building a foundation for penetration testing and establishing a fundamental methodology. From there, they explain the Framework's conventions, interfaces, and module system, as they show you how to assess networks with Metasploit by launching simulated attacks. Having mastered the essentials, you'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, devastating wireless attacks, and targeted social engineering attacks. Metasploit: A Penetration Tester's Guide will teach you how to: Find and exploit unmaintained, misconfigured, and unpatched systems Perform reconnaissance and find valuable information about your target Bypass anti-virus technologies and circumvent security controls Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery Use the Meterpreter shell to launch further attacks from inside the network Harness standalone Metasploit utilities, third-party tools, and plug-ins Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to make your own networks more secure or to put someone else's to the test, Metasploit: A Penetration Tester's Guide will take you there and beyond"--

"The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, documentation is lacking and the tool can be hard to grasp for first-time users. Metasploit: A Penetration Tester's Guide fills this gap by teaching you how to harness the Framework, use its many features, and interact with the vibrant community of Metasploit contributors. The authors begin by building a foundation for penetration testing and establishing a fundamental methodology. From there, they explain the Framework's conventions, interfaces, and module system, as they show you how to assess networks with Metasploit by launching simulated attacks. Having mastered the essentials, you'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, devastating wireless attacks, and targeted social engineering attacks. Metasploit: A Penetration Tester's Guide will teach you how to: Find and exploit unmaintained, misconfigured, and unpatched systems Perform reconnaissance and find valuable information about your target Bypass anti-virus technologies and circumvent security controls Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery Use the Meterpreter shell to launch further attacks from inside the network Harness standalone Metasploit utilities, third-party tools, and plug-ins Learn how to write

your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to make your own networks more secure or to put someone else's to the test, Metasploit: A Penetration Tester's Guide will take you there and beyond"--

https://rebiunoda.pro.baratznet.cloud:28443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMTc4NjY1MTc

Título: Metasploit Recurso electrónico] the penetration tester's guide by David Kennedy [and others]

Editorial: San Francisco, CA No Starch Press 2011

Descripción física: xxiv, 299 p. il

Mención de serie: EBSCO Academic eBook Collection Complete

Nota general: Incluye índice

Contenido: 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; 1: The Absolute Basics of Penetration Testing; The Phases of the PTES; Pre-engagement Interactions; Intelligence Gathering; Threat Modeling; Vulnerability Analysis; Exploitation; Post Exploitation; Reporting; Types of Penetration Tests; Overt Penetration Testing; Covert Penetration Testing; Vulnerability Scanners; Pulling It All Together; 2: Metasploit Basics; Terminology; Exploit; Payload ShellcodeModule; Listener; Metasploit Interfaces; MSFconsole; MSFcli; Armitage; Metasploit Utilities; MSFpayload; MSFencode; Nasm Shell; Metasploit Express and Metasploit Pro; Wrapping Up; 3: Intelligence Gathering; Passive Information Gathering; whois Lookups; Netcraft; NSLookup; Active Information Gathering; Port Scanning with Nmap; Working with Databases in Metasploit; Port Scanning with Metasploit; Targeted Scanning; Server Message Block Scanning; Hunting for Poorly Configured Microsoft SQL Servers; SSH Server Scanning; FTP Scanning; Simple Network Management Protocol Sweeping Writing a Custom ScannerLooking Ahead; 4: Vulnerability Scanning; The Basic Vulnerability Scan; Scanning with NeXpose; Configuration; Importing Your Report into the Metasploit Framework; Running NeXpose Within MSFconsole; Scanning with Nessus; Nessus Configuration; Creating a Nessus Scan Policy; Running a Nessus Scan; Nessus Reports; Importing Results into the Metasploit Framework; Scanning with Nessus from Within Metasploit; Specialty Vulnerability Scanners; Validating SMB Logins; Scanning for Open VNC Authentication; Scanning for Open X11 Servers; Using Scan Results for Autopwning 5: The Joy of ExploitationBasic Exploitation; msf> show exploits; msf> show auxiliary; msf> show options; msf> show payloads; msf> show targets; info; set and unset; setg and unsetg; save; Exploiting Your First Machine; Exploiting an Ubuntu Machine; All-Ports Payloads: Brute Forcing Ports; Resource Files; Wrapping Up; 6: Meterpreter; Compromising a Windows XP Virtual Machine; Scanning for Ports with Nmap; Attacking MS SQL; Brute Forcing MS SQL Server; The xp_cmdshell; Basic Meterpreter Commands; Capturing Keystrokes; Dumping Usernames and Passwords; Extracting the Password Hashes Dumping the Password HashPass the Hash; Privilege Escalation; Token Impersonation; Using ps; Pivoting onto Other Systems; Using Meterpreter Scripts; Migrating a Process; Killing Antivirus Software; Obtaining System Password Hashes; Viewing All Traffic on a Target Machine; Scraping a System; Using Persistence; Leveraging Post Exploitation Modules; Upgrading Your Command Shell to Meterpreter; Manipulating Windows APIs with the Railgun Add-On; Wrapping Up; 7: Avoiding Detection; Creating Stand-Alone Binaries with MSFpayload; Evading Antivirus Detection; Encoding with MSFencode; Multi-encoding

Detalles del sistema: Forma de acceso: World Wide Web

ISBN: 9781593274023 1593274025 9781593272883 159327288X

Autores: Kennedy, David (1982-)

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es