1.

Record Nr.	UNINA9910790494203321
Autore	Singh Abhinav
Titolo	Metasploit penetration testing cookbook [[electronic resource]] : over 70 recipes to master the most widely used penetration testing framework / / Abhinav Singh
Pubbl/distr/stampa	Birmingham, : Packt Pub., 2012
ISBN	1-62198-904-6 1-281-09013-1 9786613775498 1-84951-743-6
Edizione	[1st edition]
Descrizione fisica	1 online resource (269 p.)
Disciplina	005.8
Soggetti	Computers - Access control Penetration testing (Computer security) Computer networks - Security measures - Testing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"Quick answers to common problems." Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: Metasploit Quick Tips for Security Professionals; Introduction; Configuring Metasploit on Windows; Configuring Metasploit on Ubuntu; Metasploit with BackTrack 5 - the ultimate combination; Setting up the penetration testing lab on a single machine; Setting up Metasploit on a virtual machine with SSH connectivity; Beginning with the interfaces - the ""Hello World"" of Metasploit; Setting up the database in Metasploit; Using the database to store penetration testing results Analyzing the stored results of the databaseChapter 2: Information Gathering and Scanning; Introduction; Passive information gathering 1.0 - the traditional way; Passive information gathering 2.0 - the next level; Port scanning - the Nmap way; Exploring auxiliary modules for scanning; Target service scanning with auxiliary modules; Vulnerability scanning with Nessus; Scanning with NeXpose; Sharing information with the Dradis framework; Chapter 3: Operating System-based

Vulnerability Assessment and Exploitation; Introduction; Exploit usage quick tips

Penetration testing on a Windows XP SP2 machineBinding a shell to the target for remote access; Penetration testing on the Windows 2003 Server; Windows 7/Server 2008 R2 SMB client infinite loop; Exploiting a Linux (Ubuntu) machine; Understanding the Windows DLL injection flaws; Chapter 4: Client-side Exploitation and Antivirus Bypass; Introduction; Internet Explorer unsafe scripting misconfiguration vulnerability; Internet Explorer CSS recursive call memory corruption; Microsoft Word RTF stack buffer overflow; Adobe Reader util.printf() buffer overflow

Generating binary and a shellcode from msfpayloadBypassing client-side antivirus protection using msfencode; Using the killav.rb script to disable antivirus programs; A Deeper look into the killav.rb script; Killing antivirus services from the command line; Chapter 5: Using Meterpreter to Explore the Compromised Target; Introduction; Analyzing meterpreter system commands; Privilege escalation and process migration; Setting multiple communication channels with the target; Meterpreter filesystem commands; Changing file attributes using timestomp; Using meterpreter networking commands

The getdesktop and keystroke sniffingUsing a scraper meterpreter script; Chapter 6: Advanced Meterpreter Scripting; Introduction; Passing the hash; Setting up a persistent connection with backdoors; Pivoting with meterpreter; Port forwarding with meterpreter; Meterpreter API and mixins; Railgun -- converting Ruby into a weapon; Adding a DLL and function definition to Railgun; Building a ""Windows Firewall De-activator"" meterpreter script; Analyzing an existing meterpreter script; Chapter 7: Working with Modules for Penetration Testing; Introduction; Working with scanner auxiliary modules

Working with auxiliary admin modules

Sommario/riassunto

Over 80 recipes to master the most widely used penetration testing framework