1. Record Nr. UNINA9910464798203321

Autore	Jaswal Nipun
Titolo	Mastering metasploit : write and implement sophisticated attack vectors in Metasploit using a completely hands-on approach / / Nipun Jaswal ; cover image by Aniket Sawant
Pubbl/distr/stampa	Birmingham, England : , : Packt Publishing Ltd, , 2014 ©2014
ISBN	1-78216-223-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (378 p.)
Collana	Community Experience Distilled
Disciplina	005.8
Soggetti	Computers - Access control Computer networks - Security measures Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: Approaching a Penetration Test Using Metasploit; Setting up the environment; Preinteractions; Intelligence gathering / reconnaissance phase; Presensing the test grounds; Modeling threats; Vulnerability analysis; Exploitation and post-exploitation; Reporting; Mounting the environment; Setting up the penetration test lab; The fundamentals of Metasploit; Configuring Metasploit on different environments; Configuring Metasploit on Windows XP/7; Configuring Metasploit on Ubuntu Dealing with error statesErrors in the Windows-based installation; Errors in the Linux-based installation; Conducting a penetration test with Metasploit; Recalling the basics of Metasploit; Penetration testing Windows XP; Assumptions; Gathering intelligence; Modeling threats; Vulnerability analysis; The attack procedure with respect to the NETAPI vulnerability; The concept of attack; The procedure of exploiting a vulnerability; Exploitation and post-exploitation; Maintaining access; Clearing tracks; Penetration testing Windows Server 2003; Penetration testing Windows 7; Gathering intelligence

Modeling threatsVulnerability analysis; The exploitation procedure; Exploitation and post exploitation; Using the database to store and fetch results; Generating reports; The dominance of Metasploit; Open source; Support for testing large networks and easy naming conventions; Smart payload generation and switching mechanism; Cleaner exits; The GUI environment; Summary; Chapter 2: Reinventing Metasploit; Ruby - the heart of Metasploit; Creating your first Ruby program; Interacting with the Ruby shell; Defining methods in the shell; Variables and data types in Ruby; Working with strings
The split functionThe squeeze function; Numbers and conversions in Ruby; Ranges in Ruby; Arrays in Ruby; Methods in Ruby; Decision-making operators; Loops in Ruby; Regular expressions; Wrapping up with Ruby basics; Developing custom modules; Building a module in a nutshell; The architecture of the Metasploit framework; Understanding the libraries' layout; Understanding the existing modules; Writing out a custom FTP scanner module; Writing out a custom HTTP server scanner; Writing out post-exploitation modules; Breakthrough meterpreter scripting; Essentials of meterpreter scripting
Pivoting the target networkSetting up persistent access; API calls and mixins; Fabricating custom meterpreter scripts; Working with RailGun; Interactive Ruby shell basics; Understanding RailGun and its scripting; Manipulating Windows API calls; Fabricating sophisticated RailGun scripts; Summary; Chapter 3: The Exploit Formulation Process; The elemental assembly primer; The basics; Architectures; System organization basics; Registers; Gravity of EIP; Gravity of ESP; Relevance of NOPs and JMP; Variables and declaration; Fabricating example assembly programs; The joy of fuzzing
Crashing the application

Sommario/riassunto

A comprehensive and detailed, step by step tutorial guide that takes you through important aspects of the Metasploit framework. If you are a penetration tester, security engineer, or someone who is looking to extend their penetration testing skills with Metasploit, then this book is ideal for you. The readers of this book must have a basic knowledge of using Metasploit. They are also expected to have knowledge of exploitation and an indepth understanding of object-oriented programming languages.