1. Record Nr. UNINA9910813995003321

| | |
|---|---|
| Autore | Allen Lee (Information security specialist) |
| Titolo | Advanced penetration testing for highly-secured environments |
| Pubbl/distr/stampa | Birmingham : , : Packt Publishing, , [2016]<br>©2016 |
| ISBN | 1-78439-202-2 |
| Edizione | [Second edition /] |
| Descrizione fisica | 1 online resource (428 p.) |
| Collana | Community experience distilled |
| Soggetti | Penetration testing (Computer security)<br>Computer networks - Security measures<br>Computer security - Management<br>Computer networks |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di contenuto | Cover; Copyright; Credits; About the Authors; About the Reviewer; www.PacktPub.com; Table of Contents; Preface; Chapter 1: Penetration Testing Essentials; Chapter 2: Preparing a Test Environment; Chapter 3: Assessment Planning; Chapter 4: Intelligence Gathering; Chapter 5: Network Service Attacks; Chapter 6: Exploitation; Chapter 7: Web Application Attacks; Chapter 8: Exploitation Concepts; Chapter 9: Post-Exploitation; Chapter 10: Stealth Techniques; Chapter 11: Data Gathering and Reporting; Chapter 12: Penetration Testing Challenge; Index; Methodology defined; Example methodologies<br>Abstract methodologySummary; Introducing VMware Workstation; Installing VMware Workstation; Network design; Understanding the default architecture; Creating the switches; Putting it all together; Summary; Introducing advanced penetration testing; Before testing begins; Planning for action; Installing LibreOffice; Effectively managing your test results; Introduction to the Dradis framework; Summary; Introducing reconnaissance; DNS recon; Gathering and validating domain and IP information; Using search engines to do your job for you; Creating network baselines with scanPBNJ; Summary<br>Web Application Attack and Audit framework (w3af)Introduction to browser plugin HackBar; Reader challenge; Summary; Buffer overflows - |

a refresher; 64-bit exploitation; Introducing vulnserver; Fuzzing tools included in Kali; Social Engineering Toolkit; Fast-Track; Reader challenge; Summary; Rules of Engagement; Data gathering, network analysis, and pillaging; Pivoting; Reader challenge; Summary; Lab preparation; Stealth scanning through the firewall; Now you see me, now you don't - avoiding IDS; Blending in; PfSense SSH logs; Looking at traffic patterns; Cleaning up compromised hosts
Miscellaneous evasion techniquesReader challenge; Summary; Record now - sort later; Old school - the text editor method; Dradis framework for collaboration; The report; Reader challenge; Summary; Firewall lab setup; The scenario; The virtual lab setup; The challenge; The walkthrough; Reporting; Summary; Penetration testing framework; Penetration Testing Execution Standard; Pre-engagement interactions; Intelligence gathering; Threat modeling; Vulnerability analysis; Exploitation; Post exploitation; Reporting; Final thoughts; Why VMware Workstation?; VMnet0; VMnet1; VMnet8; Folders
Installing Kali Linux

Sommario/riassunto

Employ the most advanced pentesting techniques and tools to build highly-secured systems and environments About This Book Learn how to build your own pentesting lab environment to practice advanced techniques Customize your own scripts, and learn methods to exploit 32-bit and 64-bit programs Explore a vast variety of stealth techniques to bypass a number of protections when penetration testing Who This Book Is For This book is for anyone who wants to improve their skills in penetration testing. As it follows a step-by-step approach, anyone from a novice to an experienced security tester can learn effective techniques to deal with highly secured environments. Whether you are brand new or a seasoned expert, this book will provide you with the skills you need to successfully create, customize, and plan an advanced penetration test. What You Will Learn A step-by-step methodology to identify and penetrate secured environments Get to know the process to test network services across enterprise architecture when defences are in place Grasp different web application testing methods and how to identify web application protections that are deployed Understand a variety of concepts to exploit software Gain proven post-exploitation techniques to exfiltrate data from the target Get to grips with various stealth techniques to remain undetected and defeat the latest defences Be the first to find out the latest methods to bypass firewalls Follow proven approaches to record and save the data from tests for analysis In Detail The defences continue to improve and become more and more common, but this book will provide you with a number or proven techniques to defeat the latest defences on the networks. The methods and techniques contained will provide you with a powerful arsenal of best practices to increase your penetration testing successes. The processes and methodology will provide you techniques that will enable you to be successful, and the step by step instructions of information gathering and intelligence will allow you to gather the required information on the targets you are testing. The exploitation and post-exploitation sections will supply you with the tools you would need to go as far as the scope of work will allow you. The challenges at the end of each chapter are designed to challenge you and provide real-world situations that will hone and perfect your penetration testing skills. You will start with a review of several well respected penetration...