1. Record Nr. UNINA9910451850903321

Autore	Allen Lee (Information security specialist)
Titolo	Advanced penetration testing for highly-secured environments [[electronic resource]] : the ultimate security guide : learn to perform professional penetration testing for highly-secured environments with this intensive hands-on guide / / Lee Allen
Pubbl/distr/stampa	Birmingham, U.K., : Packt Pub., 2012
ISBN	1-62198-905-4 1-280-67747-3 9786613654403 1-84951-775-4
Descrizione fisica	1 online resource (414 p.)
Collana	Open source : community experience distilled
Disciplina	005.8
Soggetti	Computer security - Testing Penetration testing (Computer security) Computer networks - Security measures Computer networks Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: Planning and Scoping for a Successful Penetration Test; Introduction to advanced penetration testing; Vulnerability assessments; Penetration testing; Advanced penetration testing; Before testing begins; Determining scope; Setting limits - nothing lasts forever; Rules of engagement documentation; Planning for action; Installing VirtualBox; Installing your BackTrack virtual machine; Preparing the virtual guest machine for BackTrack Installing BackTrack on the virtual disk imageExploring BackTrack; Logging in; Changing the default password; Updating the applications and operating system; Installing OpenOffice; Effectively manage your test results; Introduction to MagicTree; Starting MagicTree; Adding nodes; Data collection; Report generation; Introduction to the Dradis

Framework; Exporting a project template; Importing a project template; Preparing sample data for import; Importing your Nmap data; Exporting data into HTML; Dradis Category field; Changing the default HTML template; Summary
Chapter 2: Advanced Reconnaissance TechniquesIntroduction to reconnaissance; Reconnaissance workflow; DNS recon; Nslookup - it's there when you need it; Default output; Changing nameservers; Creating an automation script; What did we learn?; Domain Information Groper (Dig); Default output; Zone transfers using Dig; Advanced features of Dig; DNS brute forcing with fierce; Default command usage; Creating a custom wordlist; Gathering and validating domain and IP information; Gathering information with whois; Specifying which registrar to use; Where in the world is this IP?; Defensive measures Using search engines to do your job for youSHODAN; Filters; Understanding banners; Finding specific assets; Finding people (and their documents) on the web; Google hacking database; Metagoofil; Searching the Internet for clues; Metadata collection; Extracting metadata from photos using exiftool; Summary; Chapter 3: Enumeration: Choosing Your Targets Wisely; Adding another virtual machine to our lab; Configuring and testing our Vlab_1 clients; BackTrack - Manual ifconfig; Ubuntu - Manual ifconfig; Verifying connectivity; Maintaining IP settings after reboot; Nmap - getting to know you
Commonly seen Nmap scan types and optionsBasic scans - warming up; Other Nmap techniques; Remaining stealthy; Shifting blame - the zombies did it!; IDS rules, how to avoid them; Using decoys; Adding custom Nmap scripts to your arsenal; How to decide if a script is right for you; Adding a new script to the database; SNMP: A goldmine of information just waiting to be discovered; SNMPEnum; SNMPCheck; When the SNMP community string is NOT ""public""; Creating network baselines with scanPBNJ; Setting up MySQL for PBNJ; Starting MySQL; Preparing the PBNJ database; First scan; Reviewing the data Enumeration avoidance techniques

Sommario/riassunto

Learn to perform professional penetration testing for highly-secured environments with this intensive hands-on guide with this book and ebook.