1. Record Nr. UNINA9910824037803321

Autore	Allen Lee (Information security specialist)
Titolo	Kali Linux : assuring security by penetration testing / / Lee Allen, Tedi Heriyanto, Shakeel Ali
Pubbl/distr/stampa	Birmingham : , : Packt Publishing, , 2014
ISBN	1-84951-949-8
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (454 p.)
Collana	Community experience distilled
Disciplina	005.8
Soggetti	Operating systems (Computers) Open source software
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"Master the art of penetration testing with Kali Linus."
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Table of Contents; Preface; Part I: Lab Preparation and Testing Procedures; Chapter 1: Beginning with Kali Linux; A brief history of Kali Linux; Kali Linux tool categories; Downloading Kali Linux; Using Kali Linux; Running Kali using Live DVD; Installing on a hard disk; Installing Kali on a physical machine; Installing Kali on a virtual machine; Installing Kali on a USB disk; Configuring the virtual machine; VirtualBox guest additions; Setting up networking ; Setting up a wired connection; Setting up a wireless connection; Starting the network service; Configuring shared folders Saving the guest machine stateExporting a virtual machine; Updating Kali Linux; Network services in Kali Linux; HTTP; MySQL; SSH; Installing a vulnerable server; Installing additional weapons; Installing the Nessus vulnerability scanner; Installing the Cisco password cracker; Summary; Chapter 2: Penetration Testing Methodology; Types of penetration testing; Black box testing; White box testing; Vulnerability assessment versus penetration testing; Security testing methodologies; Open Source Security Testing Methodology Manual (OSSTMM); Key features and benefits Information Systems Security Assessment Framework (ISSAF)Key features and benefits; Open Web Application Security Project (OWASP) ; Key features and benefits; Web Application Security Consortium Threat Classification (WASC-TC); Key features and benefits; Penetration Testing Execution Standard (PTES); Key features and benefits; General

penetration testing framework; Target scoping; Information gathering; Target discovery; Enumerating target; Vulnerability mapping; Social engineering; Target exploitation; Privilege escalation; Maintaining access; Documentation and reporting; The ethics; Summary
Part II: Penetration Testers ArmoryChapter 3: Target Scoping; Gathering client requirements; Creating the customer requirements form; Deliverables assessment form; Preparing the test plan; Test plan checklist; Profiling test boundaries; Defining business objectives; Project management and scheduling; Summary; Chapter 4: Information Gathering; Using public resources; Querying the domain registration information; Analyzing the DNS records; host; dig; dnsenum; dnsdict6; fierce; DMitry; Maltego; Getting network routing information; tcptraceroute; tctrace; Utilizing the search engine; theharvester MetagoofilSummary; Chapter 5: Target Discovery; Starting off with target discovery; Identifying the target machine; ping; arping; fping; hping3; nping; alive6; detect-new-ip6; passive_discovery6; nbtscan; OS fingerprinting; p0f; Nmap; Summary; Chapter 6: Enumerating Target; Introducing port scanning; Understanding the TCP/IP protocol; Understanding the TCP and UDP message format; Network scanner; Nmap; Nmap target specification; Nmap TCP scan options; Nmap UDP scan options; Nmap port specification; Nmap output options; Nmap timing options; Nmap useful options
Nmap for scanning the IPv6 target

Sommario/riassunto

Written as an interactive tutorial, this book covers the core of Kali Linux with real-world examples and step-by-step instructions to provide professional guidelines and recommendations for you. The book is designed in a simple and intuitive manner that allows you to explore the whole Kali Linux testing process or study parts of it individually.If you are an IT security professional who has a basic knowledge of Unix/Linux operating systems, including an awareness of information security factors, and want to use Kali Linux for penetration testing, then this book is for you.