1. Record Nr. UNINA9910813170803321

Autore	Krutz Ronald L. <1938->
Titolo	The CEH prep guide [[electronic resource]] : the comprehensive guide to certified ethical hacking / / Ronald L. Krutz, Russell Dean Vines
Pubbl/distr/stampa	Indianapolis, IN, : Wiley, c2007
ISBN	1-280-97384-6 9786610973842 0-470-23138-6
Descrizione fisica	1 online resource (770 p.)
Classificazione	54.89
Altri autori (Persone)	VinesRussell Dean <1952->
Disciplina	004.16 005.8
Soggetti	Computer security - Testing - Examinations Computer networks - Security measures - Examinations Computer networks - Examinations Computer hackers
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking; About the Authors; Credits; Contents; Foreword; Acknowledgments; Introduction; Exam Eligibility; Part I: The Business and Legal Issues of Ethical Hacking; Chapter 1: Introduction to Ethical Hacking; Terminology; Hacking History; Ethical Hacking Objectives and Motivations; Steps in Malicious Hacking; Hacker and Ethical Hacker Characteristics and Operations; Related Types of Computer Crime; Assessment Questions; Chapter 2: Legality and Ethics; Law and Legal Systems; Computer Crime Penalties; Ethics; Assessment Questions Chapter 3: Penetration Testing for BusinessPenetration Testing from a Business Perspective; Justification of Penetration Testing through Risk Analysis; Management Responsibilities in Risk Analysis Relating to Penetration Testing; Assessment Questions; Part II: The Pre-Attack Phases; Chapter 4: Footprinting; Gathering Information; Locating the Network Range; Assessment Questions; Chapter 5: Scanning; Identifying Active Machines; Identifying Open Ports and Available Services; War Dialing; War Driving and War Walking; Fingerprinting;

Mapping the Network; Assessment Questions
Chapter 6: EnumeratingProtection Rings; Windows Architecture; Windows Security Elements; Enumerating Techniques for Windows; Countermeasures; Assessment Questions; Part III: Attack Techniques and Tools; Chapter 7 System Hacking Techniques; Password Guessing; Privilege Escalation; Password Cracking; Covering Tracks; Countermeasures; Assessment Questions; Chapter 8: Trojans, Backdoors, and Sniffers; Trojans and Backdoors; Sniffers; Assessment Questions; Chapter 9: Denial of Service Attacks and Session Hijacking; Denial of Service/Distributed Denial of Service (DoS/DDoS); Session Hijacking
Assessment QuestionsChapter 10: Penetration Testing Steps; Penetration Testing Overview; Legal and Ethical Implications; The Three Pretest Phases; Penetration Testing Tools and Techniques; Wireless Network Penetration Testing; Social Engineering; Intrusion Detection System (IDS); Assessment Questions; Chapter 11: Linux Hacking Tools; Linux History; Scanning Networks with Linux Tools; Linux Hacking Tools; Linux Rootkits; Linux Security Tools; Assessment Questions; Chapter 12: Social Engineering and Physical Security; Social Engineering; Physical Security; Assessment Questions
Part IV: Web Server and Database AttacksChapter 13: Web Server Hacking and Web Application Vulnerabilities; Web Server Hacking; Web Application Vulnerabilities; Countermeasures; Assessment Questions; Chapter 14:SQL Injection Vulnerabilities; SQL Injection Testing and Attacks; SQL Injection Prevention and Remediation; Automated SQL Injection Tools; Assessment Questions; Chapter 15: Cryptography; Symmetric Key Cryptography; Public Key Cryptosystems; Public Key Certificates; Cryptanalysis; Managing Encryption Keys; Email Security; Electronic Transaction Security; Wireless Security
Disk Encryption

Sommario/riassunto

The Certified Ethical Hacker program began in 2003 and ensures that IT professionals apply security principles in the context of their daily job scopePresents critical information on footprinting, scanning, enumeration, system hacking, trojans and backdoors, sniffers, denial of service, social engineering, session hijacking, hacking Web servers, and moreDiscusses key areas such as Web application vulnerabilities, Web-based password cracking techniques, SQL injection, wireless hacking, viruses and worms, physical security, and Linux hackingContains a CD-ROM that enables read