1.	Record Nr.	UNINA9910784790303321
	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;

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