1. Record Nr. UNISALENTO991003243739707536

Autore	Harrington, Jan L.
Titolo	Network security [electronic resource] : a practical approach / Jan L. Harrington
Pubbl/distr/stampa	Amsterdam ; Boston : Elsevier : Morgan Kaufmann Publishers, c2005
ISBN	9780123116338 0123116333
Descrizione fisica	xv, 365 p. : ill. ; 24 cm.
Disciplina	005.8
Soggetti	Computer networks - Security measures Computernetwerken Computerbeveiliging Réseaux d'ordinateurs - Sécurité - Mesures Electronic books.
Lingua di pubblicazione	Inglese
Formato	Risorsa elettronica
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references (p. 344-345) and index.
Nota di contenuto	Chapter 1: In the Beginning -- Chapter 2: Basic Security Architecture -- Chapter 3: Physical Security -- Chapter 4: Information Gathering -- Chapter 5: Gaining and Keeping Root Access -- Chapter 6: Spoofing -- Chapter 7: Denial of Service Attacks -- Chapter 8: Malware -- Chapter 9: User and Password Security -- Chapter 10: Remote Access -- Chapter 11: Wireless Security -- Chapter 12: Encryption -- Appendix A: The TCP/IP Protocol Stack -- Appendix B: TCP and UDP Ports -- Appendix C: Security Update Sites -- Glossary -- Index.
Sommario/riassunto	Network Security is a comprehensive resource written for anyone who plans or implements network security measures, including managers and practitioners. It offers a valuable dual perspective on security: how your network looks to hackers who want to get inside, and how you need to approach it on the inside to keep them at bay. You get all the hands-on technical advice you need to succeed, but also higher-level administrative guidance for developing an effective security policy. There may be no such thing as absolute security, but, as the author clearly demonstrates, there is a huge difference between the protection offered by routine reliance on third-party products and what you can

achieve by actively making informed decisions. Youll learn to do just that with this books assessments of the risks, rewards, and trade-offs related implementing security measures. + Helps you see through a hacker's eyes so you can make your network more secure. + Provides technical advice that can be applied in any environment, on any platform, including help with intrusion detection systems, firewalls, encryption, anti-virus software, and digital certificates. + Emphasizes a wide range of administrative considerations, including security policies, user management, and control of services and devices. + Covers techniques for enhancing the physical security of your systems and network. + Explains how hackers use information-gathering to find and exploit security flaws. + Examines the most effective ways to prevent hackers from gaining root access to a server. + Addresses Denial of Service attacks, "malware," and spoofing. + Includes appendices covering the TCP/IP protocol stack, well-known ports, and reliable sources for security warnings and updates.