1. Record Nr. UNINA9910823417103321

Titolo	How to cheat at securing a wireless network / / Chris Hurley ... [et al.]
Pubbl/distr/stampa	Rockland, Mass., : Syngress Media, c2006
ISBN	1-281-07833-6 9786611078331 0-08-050822-7
Edizione	[1st edition]
Descrizione fisica	1 online resource (481 p.)
Collana	How to Cheat
Altri autori (Persone)	HurleyChris
Disciplina	621.3845
Soggetti	Computer networks - Security measures Wireless communication systems - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Front Cover; Securing a Wireless Network; Contents; Chapter 1. Introduction to Wireless: From Past to Present; Introduction; Exploring Past Discoveries That Led to Wireless; Exploring Present Applications for Wireless; Exploring This Book on Wireless; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 2. Wireless Security; Introduction; Enabling Security Features on a Linksys WRT54G 802.11g Access Point; Enabling Security Features on a D-Link DI-624 AirPlus 2.4 GHz Xtreme G Wireless Router with Four-Port Switch; Enable Wi-Fi Protected Access Enabling Security Features on Apple's Airport Extreme 802.11g Access PointEnabling Security Features on a Cisco 1100 Series Access Point; Enabling Security Features on Wireless Clients; Understanding and Configuring 802.1X RADIUS Authentication; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 3. Dangers of Wireless Devices in the Workplace; Introduction; Intruders Accessing Legitimate Access Points; Intruders Connecting to Rogue Wireless Access Points; Intruders Connecting to WLAN Cards; Summary; Solutions Fast Track; Frequently Asked Questions Chapter 4. WLAN Rogue Access Point Detection and MitigationIntroduction; The Problem with Rogue Access Points; Preventing and Detecting Rogue Access Points; IEEE 802.1x Port-based

Security to Prevent Rogue Access Points; Using Catalyst Switch Filters to Limit MAC Addresses per Port; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 5. Wireless LAN VLANs; Introduction; Understanding VLANs; VLANs in a Wireless Environment; Wireless VLAN Deployment; Configuring Wireless VLANs Using the IOS: A Case Study; Broadcast Domain Segmentation; Primary (Guest) and Secondary SSIDs
Using RADIUS for VLAN Access ControlSummary; Solutions Fast Track; Frequently Asked Questions; Chapter 6. Designing a Wireless Network; Introduction; Exploring the Design Process; Identifying the design methodology; Understanding Wireless Network Attributes from a Design Perspective; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 7. Wireless Network Architecture and Design; Fixed Wireless Technologies; Developing WLANs through the 802.11 Architecture; Developing WPANs through the 802.15 Architecture; Mobile Wireless Technologies; Optical Wireless Technologies; Summary Solutions Fast TrackFrequently Asked Questions; Chapter 8. Monitoring and Intrusion Detection; Introduction; Designing for Detection; Defensive Monitoring Considerations; Intrusion Detection Strategies; Conducting Vulnerability Assessments; Incident Response and Handling; Conducting Site Surveys for Rogue Access Points; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 9. Designing a Wireless Enterprise Network: Hospital Case Study; Introduction; Introducing the Enterprise Case Study; Designing a Wireless Solution; Implementing and Testing the Wireless Solution
Lessons Learned

Sommario/riassunto

Wireless connectivity is now a reality in most businesses. Yet by its nature, wireless networks are the most difficult to secure and are often the favorite target of intruders. This book provides the busy network administrator with best-practice solutions to securing the wireless networkWith the increased demand for mobile connectivity and the decrease in cost and in the time required for installation, wireless network connections will make up 20% of all corporate network connections by the end of 2006. With this increase in usage comes a commensurate increase in the network's