1. Record Nr. UNINA9910815322503321

Titolo	Network and system security / / edited by John R. Vacca
Pubbl/distr/stampa	Waltham, Mass., : Academic Press, 2014 Waltham, MA : , : Syngress, , 2014
ISBN	0-12-416695-4
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (xxi, 406 pages) : illustrations (some color)
Collana	Gale eBooks
Disciplina	005.8
Soggetti	Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Front Cover; Network and System Security; Copyright Page; Contents; Acknowledgements; About the Editor; Contributors; Introduction; Organization of this Book; 1. Detecting System Intrusions; 1. Introduction; 2. Monitoring Key Files in the System; Files Integrity; 3. Security Objectives; There Is Something Very Wrong Here; Additional Accounts on the System; Timestamps; Hidden Files and Directories; 4. 0day Attacks; Attack Vectors; Vulnerability Window; Discovery; Protection; Ethics; 5. Good Known State; Monitoring Running Processes in the System; Files with Weird Names; 6. Rootkits Kernel-Level RootkitsUserland Rootkits; Rootkit Detection; 7. Low Hanging Fruit; 8. Antivirus Software; 9. Homegrown Intrusion Detection; 10. Full-Packet Capture Devices; Deployment; Centralized; Decentralized; Capacity; Features: Filtered versus Full-Packet Capture; Encrypted versus Unencrypted Storage; Sustained Capture Speed versus Peak Capture Speed; Permanent versus Overwritable Storage; Data Security; 11. Out-of-Band Attack Vectors; 12. Security Awareness Training; 13. Data Correlation; 14. SIEM; 15. Other Weird Stuff on the System; 16. Detection 17. Network-Based Detection of System Intrusions (DSIs)18. Summary; Chapter Review Questions/Exercises; True/False; Multiple Choice; Exercise; Problem; Hands-On Projects; Project; Case Projects; Problem; Optional Team Case Project; Problem; References; 2. Preventing System Intrusions; 1. So, What is an Intrusion?; 2. Sobering Numbers; 3. Know Your Enemy: Hackers versus Crackers; 4. Motives; 5. The Crackers'

Tools of the Trade; Our "Unsecured" Wireless World; 6. Bots; 7. Symptoms of Intrusions; 8. What Can You Do?; Know Today's Network Needs; Network Security Best Practices
9. Security Policies10. Risk Analysis; Vulnerability Testing; Audits; Recovery; 11. Tools of Your Trade; Intrusion Detection Systems (IDSs); Firewalls; Intrusion Prevention Systems; Application Firewalls; Access Control Systems; Unified Threat Management; 12. Controlling User Access; Authentication, Authorization, and Accounting; What the User Knows; What the User Has; Tokens; Time Synchronous; Event Synchronous; Challenge-Response; The User is Authenticated, but is She/He Authorized?; Accounting; Keeping Current; 13. Intrusion Prevention Capabilities; 14. Summary
Chapter Review Questions/ExercisesTrue/False; Multiple Choice; Exercise; Problem; Hands-On Projects; Project; Case Projects; Problem; Optional Team Case Project; Problem; 3. Guarding Against Network Intrusions; 1. Traditional Reconnaissance and Attacks; 2. Malicious Software; Lures and "Pull" Attacks; 3. Defense in Depth; 4. Preventive Measures; Access Control; Vulnerability Testing and Patching; Closing Ports; Firewalls; Antivirus and Antispyware Tools; Spam Filtering; Honeypots; Network Access Control; 5. Intrusion Monitoring and Detection; Host-Based Monitoring; Traffic Monitoring
Signature-Based Detection

Sommario/riassunto

Network and System Security provides focused coverage of network and system security technologies. It explores practical solutions to a wide range of network and systems security issues. Chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes building a secure organization, cryptography, system intrusion, UNIX and Linux security, Internet security, intranet security, LAN security; wireless network security, cellular network security, RFID security, and more. <