1. Record Nr. UNINA9910816736803321

Autore	Beale Jay
Titolo	Snort 2.0 intrusion detection / / Jay Beale, James C. Foster
Pubbl/distr/stampa	Rockland, : Syngress Oxford, : Elsevier Science, c2003
ISBN	1-281-05609-X 9786611056094 0-08-048100-0
Edizione	[1st edition]
Descrizione fisica	1 online resource (559 p.)
Altri autori (Persone)	FosterJames C
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Front Cover; Snort 2.0 Intrusion Detection; Copyright Page; Contents; Chapter 1. Intrusion Detection Systems; Introduction; What Is Intrusion Detection?; A Trilogy of Vulnerabilities; Why Are Intrusion Detection Systems Important?; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 2. Introducing Snort 2.0; Introduction; What Is Snort?; Snort System Requirements; Exploring Snort's Features; Using Snort on Your Network; Security Considerations with Snort; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 3. Installing Snort; Introduction A Brief Word about Linux DistributionsInstalling PCAP; Installing Snort; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 4. Snort: The Inner Workings; Introduction; Snort Components; Decoding Packets; Processing Packets 101; Understanding Rule Parsing and Detection Engines; Output and Logs; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 5. Playing by the Rules; Introduction; Understanding Configuration Files; The Rule Header; The Rule Body; Components of a Good Rule; Testing Your Rules; Tuning Your Rules; Summary; Solutions Fast Track Frequently Asked QuestionsChapter 6. Preprocessors; Introduction; What Is a Preprocessor?; Preprocessor Options for Reassembling

Packets; Preprocessor Options for Decoding and Normalizing Protocols; Preprocessor Options for Nonrule or Anomaly-Based Detection; Experimental Preprocessors; Writing Your Own Preprocessor; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 7. Implementing Snort Output Plug-Ins; Introduction; What Is an Output Plug-In?; Exploring Output Plug-In Options; Writing Your Own Output Plug-In; Summary; Solutions Fast Track; Frequently Asked Questions Chapter 8. Exploring the Data Analysis ToolsIntroduction; Using Swatch; Using ACID; Using SnortSnarf; Using IDScenter; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 9. Keeping Everything Up to Date; Introduction; Applying Patches; Updating Rules; Testing Rule Updates; Watching for Updates; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 10. Optimizing Snort; Introduction; How Do I Choose What Hardware to Use?; How Do I Choose What Operating System to Use?; Speeding Up Your Snort Installation; Benchmarking Your Deployment; Summary; Solutions Fast Track
Frequently Asked QuestionsChapter 11. Mucking Around with Barnyard; Introduction; What Is Barnyard?; Preparation and Installation of Barnyard; How Does Barnyard Work?; What Are the Output Options for Barnyard?; But I Want My Output Like ""This""; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 12. Advanced Snort; Introduction; Policy-Based IDS; Inline IDS; Summary; Solutions Fast Track; Frequently Asked Questions; Index; GNU GENERAL PUBLIC LICENSE; TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION; END OF TERMS AND CONDITIONS
SYNGRESS PUBLISHING LICENSE AGREEMENT

Sommario/riassunto

The incredible low maintenance costs of Snort combined with its powerful security features make it one of the fastest growing IDSs within corporate IT departments. Snort 2.0 Intrusion Detection is the first book dealing with the Snort IDS and is written by a member of Snort.org. Readers will receive valuable insight to the code base of Snort and in-depth tutorials of complex installation, configuration, and troubleshooting scenarios. The primary reader will be an individual who has a working knowledge of the TCP/IP protocol, expertise in some arena of IT infrastructure, and is