1. Record Nr. UNINA9910254849503321

Autore	Wang Lingyu
Titolo	Network Security Metrics / / by Lingyu Wang, Sushil Jajodia, Anoop Singhal
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-66505-7
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XIV, 207 p. 110 illus., 63 illus. in color.)
Disciplina	005.8
Soggetti	Computer security Computer communication systems Data encryption (Computer science) Systems and Data Security Computer Communication Networks Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references at the end of each chapters.
Nota di contenuto	1 Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks -- 2 Refining CVSS-based network security metrics by examining the base scores -- 3 Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs -- 4 k-Zero day safety: Evaluating the resilience of networks against unknown attacks -- 5 Using Bayesian Networks to Fuse Intrusion Evidences and Detect Zero-day Attack Paths -- 6 Evaluating the network diversity of networks against zero-day attacks -- 7 Metrics suite for network attack graph analytics -- 8 A Novel Metric for Measuring Operational Effectiveness of a Cybersecurity Operations Center.
Sommario/riassunto	This book examines different aspects of network security metrics and their application to enterprise networks. One of the most pertinent issues in securing mission-critical computing networks is the lack of effective security metrics which this book discusses in detail. Since “you cannot improve what you cannot measure”, a network security metric is essential to evaluating the relative effectiveness of potential network

security solutions. The authors start by examining the limitations of existing solutions and standards on security metrics, such as CVSS and attack surface, which typically focus on known vulnerabilities in individual software products or systems. The first few chapters of this book describe different approaches to fusing individual metric values obtained from CVSS scores into an overall measure of network security using attack graphs. Since CVSS scores are only available for previously known vulnerabilities, such approaches do not consider the threat of unknown attacks exploiting the so-called zero day vulnerabilities. Therefore, several chapters of this book are dedicated to develop network security metrics especially designed for dealing with zero day attacks where the challenge is that little or no prior knowledge is available about the exploited vulnerabilities, and thus most existing methodologies for designing security metrics are no longer effective. Finally, the authors examine several issues on the application of network security metrics at the enterprise level. Specifically, a chapter presents a suite of security metrics organized along several dimensions for measuring and visualizing different aspects of the enterprise cyber security risk, and the last chapter presents a novel metric for measuring the operational effectiveness of the cyber security operations center (CSOC). Security researchers who work on network security or security analytics related areas seeking new research topics, as well as security practitioners including network administrators and security architects who are looking for state of the art approaches to hardening their networks, will find this book helpful as a reference. Advanced-level students studying computer science and engineering will find this book useful as a secondary text.