Preface

At present, enterprise networks constitute the core component of information technology infrastructures in areas such as power grids, financial data systems and emergency communication systems. Protection of these networks from malicious intrusions is critical to the economy and national security. To improve the security of these information systems, it is necessary to measure the amount of security provided by different networks' configurations. The objective of this book is to give an overview of the techniques and challenges for security risk analysis of computer networks. A standard model for security analysis will enable us to answer questions such as "are we more secure than yesterday or how does the security of one network configuration compare with another". Also, having a standard model to measure network security will bring together users, vendors and researchers to evaluate methodologies and products for network security.

An essential type of security risk analysis is to determine the level of compromise possible for important hosts in a network from a given starting location. This is a complex task as it depends on the network topology, security policy in the network as determined by the placement of firewalls, routers and switches and on vulnerabilities in hosts and communication protocols. Traditionally, this type of analysis is performed by a red team of computer security professionals who actively test the network by running exploits that compromise the system. Red team exercises are effective, however they are labor intensive and time consuming. There is a need for alternate approaches that can work with host vulnerability scans.

In this book, we will present a methodology for security risk analysis that is based on the model of attack graphs and the Common Vulnerability Scoring System (CVSS). Attack graphs illustrate the cumulative effect of attack steps, showing how individual steps can potentially enable an attacker to gain privileges deep within the network. CVSS is a risk measurement system that gives the likelihood that a single attack step is successfully executed. In this book we present a methodology to measure the overall system risk by combining the attack graph structure with CVSS. Our technique analyzes all attack paths through a network, providing a probabilistic metric of the overall system risk.

http://www.springer.com/978-1-4614-1859-7

Quantitative Security Risk Assessment of Enterprise Networks

Ou, X.; Singhal, A.

2011, XIII, 28 p., Softcover
ISBN: 978-1-4614-1859-7