SpringerBriefs in Computer Science

For further volumes:
http://www.springer.com/series/10028

Xinming Ou • Anoop Singhal

Quantitative Security Risk Assessment of Enterprise Networks

Springer

Xinming Ou
Computing and Information Sciences
Kansas State University
Manhattan, Kansas
USA
xou@ksu.edu

Anoop Singhal
Computer Security Division
National Institute of Standards
and Technology (NIST)
Gaithersburg, Maryland
USA
psinghal@nist.gov

ISSN 2191-5768 e-ISSN 2191-5776
ISBN 978-1-4614-1859-7 e-ISBN 978-1-4614-1860-3
DOI 10.1007/978-1-4614-1860-3
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2011941356

If you cannot measure it, you cannot improve it.

— Lord Kelvin

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.

Acknowledgements

The authors Anoop Singhal and Ximming Ou would like to thank their colleagues who reviewed drafts of this document and contributed to its development. This material is based upon work supported by U.S. National Science Foundation under grant no. 1038366 and 1018703, AFOSR under Award No. FA9550-09-1-0138, and HP Labs Innovation Research Program. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation, AFOSR, or Hewlett-Packard Development Company, L.P.

Contents

Acronyms

CVSS	Common Vulnerability Scoring System
NVD	National Vulnerability Database
MulVAL	Multi-host, multi-step Vulnerability Analysis Language
CERT	Computer Emergency Response Team