UNIVERSITY OF MALAYA

EVALUATING INTRUSION DETECTION SYSTEMS IN A UNIX-BASED ENVIRONMENT

MAZNI ZAMBRI

WGC97012

This dissertation is submitted to the
Faculty of Computer Science and Information Technology, University of Malaya
in fulfillment of the requirements for the degree of
Masters of Software Engineering.

2003

Abstract

An intrusion detection system is an essential security component of any computing or network resource. Its function is to verify that an intrusive activity has occurred within the target system. However, as with any security technology, it has its limitations. The reality is that intruders are always a step ahead of the security measures of the target system and will likely find a loophole.

Even if a computing infrastructure is equipped with an intrusion detection system, it does not mean that the intrusion detection system will detect 100% of the malicious activities that occur. There is a need for the security personnel to be made aware of the strengths and weaknesses of their running intrusion detection systems in order to keep vigilant of potential attacks and to undertake countermeasures to known weaknesses. Evaluation of intrusion detection systems provides for this need.

The main purpose of evaluations is to determine the performance of intrusion detection systems which reveals their strengths and weaknesses. Evaluations are beneficial in terms of helping to focus effort on eliminating current weaknesses, documenting existing technologies and guiding research.

This dissertation describes the evaluation on intrusion detection systems using publicly available test data sets and open source intrusion detection systems. The performance of the selected intrusion detection systems is measured and performance ranking conferred based on their detection rates. In addition, this dissertation also highlights the weaknesses of previous evaluations to improve future evaluations.

Acknowledgements

I would like to thank my research supervisor, Pn. Azwina Mohd. Yusof, for guiding my dissertation and providing me with valuable ideas. I would also like to thank my brothers and parents for their assistance and encouragement.

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Full Phrase
ASIM	Automated Security Management System
BSM	Basic Security Module
CAPI	Common Application Programming Interface
CGI	Common Gateway Interface
CMDS	Computer Misuse Detection System
DARPA	Defense Advanced Research Projects Agency
DARPA-LL	Massachusetts Institute of Technology's Lincoln Laboratory, under Defense Advanced Research Projects Agency (DARPA) sponsorship
DES	Data Encryption Standard
DIDS	Distributed Intrusion Detection System
DoS	Denial of Service
GB	Gigabyte
GHz	Gigahertz
GSS-API	Generic Security Services Application Program Interface
HTML	Hypertext Markup Language
ICMP	Internet Control Message Protocol
ID	Intrusion Detection
IDS(s)	Intrusion Detection System(s)
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISS	Internet Security Systems
MB	Megabyte
Mhz	Megahertz
NIDS(s)	Network-based Intrusion Detection System(s)
OS	Operating System
PID	Process Identification
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
R2L	Remote to Local
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
RPC	Remote Procedure Protocol
SAIC	Science Applications International Corporation
SANS	SysAdmin, Audit, Network, Security
SLIP	Serial Line Internet Protocol
SMB	Server Message Block Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
U2R	User to Root
UID	User Identification