

2
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

Perpustakaan Universiti Malaya



A511294870

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	vii
List of Tables	viii
List of Abbreviations	ix
1 Introduction.....	1
1.1 Intrusion Detection Systems	1
1.2 Evaluations of Intrusion Detection Systems	2
1.3 The Objectives and Benefits of Evaluating Intrusion Detection Systems	3
1.4 Research Objectives and Contributions	3
1.5 Research Methodology	4
1.6 Research Scope	5
1.7 Dissertation Organisation.....	6
2 Background	8
2.1 Computer Security	8
2.1.1 What is Computer Security?	8
2.1.2 Why Computer Security?.....	9
2.1.3 Computer Security Today	10
2.1.4 Approaches to Secure Computing.....	11
2.1.5 Computer Security and Software Engineering.....	19
2.2 Unix.....	21
2.2.1 Definitions.....	21
2.2.2 An Overview of the Unix Operating System	22
2.3 Security in Unix	25
2.3.1 Unix Security Issues	27
2.3.2 Enhancing Unix Security	31
2.3.3 Similarities and Differences Between Windows NT and Unix	36
2.4 Intrusion Detection.....	38
2.4.1 What is Intrusion Detection?.....	38
2.4.2 Why Intrusion Detection?	39
2.4.3 The Evolution of Intrusion Detection: An Overview.....	39
2.4.4 Technology Overview of Intrusion Detection Systems	42
2.4.5 Methods Used in Intrusion Detection Systems	45
2.4.6 Organisation of Intrusion Detection Systems	50
2.4.7 Intrusion Detection Architecture.....	53
2.5 Intrusion Detection in Unix	58
2.5.1 Monitor Log Files	58
2.5.2 Use Commands that Run at a Specified Times to Your Benefit.....	59
2.5.3 Examine the Filesystem	60
2.6 Summary	62
3 Evaluating Intrusion Detection Systems.....	63
3.1 Previous Evaluations of IDSs	63
3.1.1 NSS Group 2001 [NSS 2001].....	63
3.1.2 The 1998 DARPA-LL Evaluations [Lippmann 2000].....	64
3.1.3 The 1999 DARPA-LL Evaluations [Lippmann 2000a].....	65

3.2	Selection of IDS tool for the evaluation	66
3.2.1	Why Snort?	67
3.2.2	What is Snort?	67
3.2.3	Snort Architecture	68
3.3	Test Objective	69
3.4	Test Scope	70
3.5	Test Requirements	71
3.5.1	Hardware Requirements	71
3.5.2	Software Requirements	72
3.6	Summary	73
4	Test Design	74
4.1	Overview of Tests	74
4.2	Test Data	75
4.2.1	Attack Descriptions for the Test Data Sets	76
4.2.2	The Test Data Sets	84
4.3	Steps to Testing	88
4.3.1	Construction of Suitable Test Environment	88
4.3.2	Implementation of Tests	91
4.3.3	Gathering of Results	91
4.3.4	Evaluation of Results	91
4.4	Summary	92
5	Test Implementation	93
5.1	Configuring Snort	93
5.1.1	Specifying the Snort Rulesets	95
5.2	Resulting Configurations	97
5.3	Testing the 4 Configurations of Snort	98
5.4	Example of a Test Run	98
5.5	Summary	102
6	Test Results	103
6.1	Test Data Set 1 (1998 Learning Data Week 6)	103
6.1.1	Summary of Results from Test Data Set 1	104
6.2	Test Data Set 2 (1998 Learning Data Week 7)	105
6.2.1	Summary of Results from Test Data Set 2	106
6.3	Test Data Set 3 (1999 Test Data Week 1)	107
6.3.1	Summary of Results from Test Data Set 3	109
6.4	Test Data Set 4 (1999 Test Data Week 2)	110
6.4.1	Summary of Results from Test Data Set 4	114
6.5	Overall Test Result Summary	115
6.6	Summary	116
7	Test Evaluation	117
7.1	IDS Performance	117
7.1.1	Snort 1.7 Custom	117
7.1.2	Snort 1.7 Full	118
7.1.3	Snort 1.8.3 Full	118
7.1.4	Snort 1.8.3 Custom	119
7.2	Performance Ranking	119

7.3	Limitations of Previous Research	120
7.3.1	Limitations of the NSS Group 2001 Evaluation	120
7.3.2	Limitations of the 1998 DARPA-LL Evaluation	120
7.3.3	Limitations of the 1999 DARPA-LL Evaluation	121
7.4	Summary	122
8	Summary and Conclusion	123
	References	126
	Appendix A: Attacks in Test Data Set 1	133
	Appendix B: Attacks in Test Data Set 2	134
	Appendix C: Attacks in Test Data Set 3	135
	Appendix D: Attacks in Test Data Set 4	143
	Appendix E: Snort Rulesets	155
	Appendix F: Result Form for Test Data Set 1	158
	Appendix G: Result Form for Test Data Set 2	160
	Appendix H: Result Form for Test Data set 3	161
	Appendix I: Result Form for Test Data Set 4	163
	Appendix J: Sample Snort Configuration File	166

List of Figures

Figure 2.1: Hacker Capabilities [Cisco Systems 2000]	10
Figure 2.2: Example Access Matrix.....	14
Figure 2.3: The Evolution of Intrusion Detection Systems	42
Figure 2.4: High Level Depiction of Audit Trail Processing.....	45
Figure 2.5: High Level Depiction of On-the-Fly Processing.....	46
Figure 2.6: Profiling Normal Behaviour	48
Figure 2.7: Abnormal Behaviour Signature Method	49
Figure 2.8: Pattern Matching Method of Intrusion Detection.....	50
Figure 2.9: Intrusion Detection System Components.....	51
Figure 2.10: Intrusion Detection Architectural Schema	54
Figure 3.1: Snort Architecture	69
Figure 4.1: Test Overview	74
Figure 4.2: Attacks in Test Data Set 1	84
Figure 4.3: Attacks in Test Data Set 2	85
Figure 4.4: Attacks in Test Data Set 3	86
Figure 4.5: Attacks in Test Data Set 4	87
Figure 5.1: Snort Pre-Run Screen	99
Figure 5.2: Snort Post-Run Screen.....	100
Figure 5.3: SnortSnarf Output.....	101

List of Tables

Table 2.1: Similarities and Differences Between Windows NT and Unix	37
Table 2.2: Pros and Cons of Network-Based Intrusion Detection Systems.....	43
Table 2.3: Pros and Cons of Host-Based Intrusion Detection Systems.....	44
Table 4.1: Description of the Denial of Service Attacks	76
Table 4.2: Description of the User to Root Attacks.....	78
Table 4.3: Description of the Remote to Local Attacks.....	80
Table 4.4: Description of the Probe Attacks	82
Table 4.5: Description of the Data Attack(s)	84
Table 6.1: Results of Testing the Snort Configurations with Test Data Set 1	103
Table 6.2: Summary of Results from Testing Snort with Test Data Set 1.....	105
Table 6.3: Results of Testing the Snort Configurations with Test Data Set 2	106
Table 6.4: Summary of Results from Testing Snort with Test Data Set 2.....	106
Table 6.5: Results of Testing the Snort Configurations with Test Data Set 3	107
Table 6.6: Summary of Results from Testing Snort with Test Data Set 3.....	110
Table 6.7: Results of Testing the Snort Configurations with Test Data Set 4	111
Table 6.8: Summary of Results from Testing Snort with Test Data Set 4.....	114
Table 6.9: Summary of the Overall Test Results	115

List of Abbreviations

<u>Abbreviation</u>	<u>Full Phrase</u>
ASIM	Automated Security Management System
BSM	Basic Security Module
CAPI	Common Application Programming Interface
CGI	Common Gateway Interface
CMD5	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