

PERFORMANCE EVALUATION IN REAL-TIME
NETWORK INTRUSION DETECTION SYSTEM
USING SNORT

A Thesis submitted to
College of Arts and Sciences (Applied Sciences)
in partial fulfillment of the requirements for the degree
Master of Science (Information Technology)
Universiti Utara Malaysia

By
Ausama A. Majeed

All rights reserved, ©. November, 2008

TIC
5104.59
m233p
2008



KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

AUSAMA A. MAJEED
(88937)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

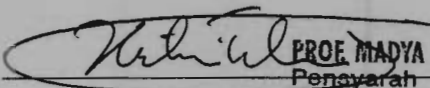
PERFORMANCE EVALUATION IN REAL-TIME NETWORK
INTRUSION DETECTION SYSTEM USING SNORT

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan
dan meliputi bidang ilmu dengan memuaskan.
*(that the project paper acceptable in form and content, and that a satisfactory
knowledge of the field is covered by the project paper).*

Nama Penyelia Utama
(Name of Main Supervisor): **ASSOC. PROF. HATIM MOHAMED TAHIR**

Tandatangan
(Signature)

: 
PROF. Madya HATIM MOHAMED TAHIR
Penyarah
Bidang Sains Gunaan
Kolej Sastera & Sains
Universiti Utara Malaysia

Tarikh
(Date)

: 17/11/08

PERMISSION TO USE

In present this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copy of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by me supervisor or, in their absence by the Dean of Research and Postgraduate Studies. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia FOR any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part should be addressed to:

Dean of Research and Postgraduate Studies

College of Arts and Sciences

Universiti Utara Malaysis

06010 UUM Sintok

Kedah Darul Aman

Malaysia

ABSTRACT

The growing numbers of Internet threats increasingly inspire the need of applying a defence in depth concepts to protect worldwide computer systems from being intruded for grabbing information. Crucially, the defence in depth includes multiple pieces of software and hardware working together to provide the desired protection. Purposefully, one component of this approach is names as Network Intrusion Detection System (NIDS) and its affiliation tool of the Snort IDS. However, to ensure that such an implementation is taking the row into reliable succession, the systems have to be examined to provide the decision makers with assurance about the way of reducing risks. Therefore, the criteria in achieving an effective NIDS, this system should not degrade overall network performance. Fruitfully, some experiments are designed and implemented using the simulation test-bed methodology with the interference of the Snort which measured by end-to-end delay-time. Introducing this software through the engine is going to be highlighted and discussed as a method of Intrusion Detection Systems testing performance at a basic level in order to ensure unaffected network traffic. Moreover, this will play a role to provide some information as if the IDS is efficiently capable to detect intrusions while maintaining network performance.

ACKNOWLEDGMENT

All praise is due to Allah, Most Gracious, and Most Merciful. Without whose help and mercy, I would not have reached this far.

It would not have been possible for me to complete the course of my master without encourage and support of my family. My first expression of gratitude goes to my parents, brothers, wife, and my two sons whose gave me the strength to complete this course.

I must convey my gratitude to my supervisor, Assoc. Prof. Hatim Mohamad Tahir for his support, guidance, critical remarks, and advices throughout this study. Also, I want to thank the people who contributed significantly to my work, and my deepest gratitude goes to all of them. Assoc. Prof. Dr. Ang Chooi Leng, Dr. Maznah Mat Kasim, Norhayati Bt Yusof, and Yuhaniz Ahmad provided me with many hours of discussion and led me to ways of conducting data analysis.

I would like to thank my colleagues and friends to many moments of insight, inspiration, laughter, and support throughout my completion of the program.

DEDICATION



I would like to dedicate this thesis to my parents,
brothers, wife, and sons who lovely encouraged
and supported me through all my study.

The motivation for all I do.



CONTENTS

PERMISSION TO USE	ii
ABSTRACT.....	iii
ACKNOWLEDGMENT.....	iv
DEDICATION.....	v
CONTENTS	vi
LIST OF FIGURES	ix
ABBREVIATIONS.....	x
CHAPTER ONE: INTRODUCTION	1
1.1 Background.....	1
1.2 Problem Statements	3
1.3 Research Questions	4
1.4 Research Objectives	5
1.5 Assumptions	5
1.6 Scope and Limitations	6
1.7 Significant of Study	7
1.8 Definition of key Terms	8
1.9 Organization of the Thesis	10
CHAPTER TWO: LITERATURE REVIEW	11
2.1 Introduction	11
2.2 Defense In-Depth	12
2.3 Intrusion Detection System (IDS)	13
2.3.1 Network-Based Intrusion Detection Systems (NIDSs)	14
2.3.2 Host-Based Intrusion Detection Systems (HIDSs)	16
2.3.3 Distributed Intrusion Detection Systems (DIDS)	17
2.4 Intrusion Prevention Systems	18
2.5 IDS Detection Approaches	19
2.5.1 Misuse Detection IDS	20

2.5.2	Anomaly Detection IDS	21
2.6	Types of Computer Attacks Commonly Detected by IDSs.....	22
2.6.1	Scanning Attacks	23
2.6.2	Denial of Service Attacks	24
2.6.3	Penetration Attacks	24
2.7	General Architecture of a Network Intrusion Detection System.....	25
2.8	Snort: Network Intrusion Detection System	28
2.8.1	The Packet Sniffer.....	30
2.8.2	Preprocessors	31
2.8.3	The Detection Engine	32
2.8.4	Logging and Alerting System	33
2.8.5	Output Modules	33
2.9	Snort Preprocessors Options	34
2.10	Advantages and Disadvantages of Snort	39
2.11	Related Work	40
2.12	Summary.....	44
 CHAPTER THREE: RESEARCH METHODOLOGY		 45
3.1	Introduction	45
3.2	Problem Definition	46
3.3	The Simulation Model Design	46
3.4	The Simulation Model Configuration	47
3.5	The Experiments Design	50
3.6	The Experiments Conduct	50
3.7	The Results Analysis & Evaluation	51
3.8	Summary	53
 CHAPTER FOUR: FINDING AND ANALYSIS OF DATA		 55
4.1	Introduction	55
4.2	Application to Research Questions	56
4.3	Data Set Collected	56
4.4	Method of Analysis.....	57

CHAPTER FIVE: CONCLUSIONS	68
5.1 Summary of the Analysis Method	68
5.2 Conclusions	69
5.3 Future Works	71
REFERENCES	73
Appendix A	79
Appendix B	85
Appendix C	87
Appendix D	95

LIST OF FIGURES

Figure 1.1	Typical Location for an IDS	2
Figure 2.1	NIDS Schema	15
Figure 2.2	HIDS Schema	16
Figure 2.3	DIDS Schema	18
Figure 2.4	General Architecture of NIDS	26
Figure 2.5	Snort Architecture	29
Figure 2.6	Snort's Packet-Sniffing Functionality	30
Figure 2.7	Snort's Preprocessor	31
Figure 2.8	Snort's Detection Engine	32
Figure 2.9	Snort Alerting Component	33
Figure 2.10	Key Element of a Secure Network Implementation	40
Figure 3.1	Simulation Test-Bed Model	45
Figure 3.2	Intrusion Detection Simulated Network	47
Figure 3.3	Colasoft Packet Player Interface	49
Figure 3.4	Wireshark Interface	49

ABBREVIATIONS

ASCII	American Standard Code For Information Interchange
CGI	Common Gateway Interface
CPU	Central Processing Unit
DIDS	Distributed Intrusion Detection System
DNS	Domain Name Service
DOS	Denial of Service
FIN	Freedom to Innovate Network
FTP	File Transfer Protocol
GNU	Government of National Unity
HIDS	Host Intrusion Detection System
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
LAN	Local Area Network
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
OS	Operating System
RFC	Request For Comments
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Sequential Query Language
SSH	Secure Shell
SYN	Synchronize
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

The contents of
the thesis is for
internal user
only

traffic containing known attacks and malicious traffic, which is quite difficult to obtain and verify prior to use.

This study allowed Snort to use the basic logging system to track the alerts and detection reports. Such logs are quite difficult to read carefully and analyze and can be time consuming. Snort provides several more user friendly options for logging of the engine alerts. However, when using these advanced options, how will they affect the processing performance as well as the detection abilities of the Snort system?

These are some topics to be considered in future research projects. Each provides specific questions that could be answered following a similar methodology used for this study.

REFERENCES

- Anderson, J. R. (1980). *Computer security threat monitoring and surveillance*.
- Anttila, J. (2004). *Intrusion Detection in Critical E-business Environment*. Helsinki University of Technology, Finland.
- Archibald, N., Ramirez, G., & Rathaus, N. (2005). *Nessus, Snort, & Ethereal Power Tools : Customizing Open Source security Application*. USA: Syngress Publishing, Inc.
- Asarcikli, S. (2005). *Firewall Monitoring Using Intrusion Detection Systems*. Izmir Institute of Technology, Izmir.
- Attig, M., & Lockwood, J. (2005). *SIFT:Snort Intrusion Filter for TCP*. Paper presented at the 13th IEEE Symposium on High Performance Interconnects.
- Axelsson, S. (2006). *Understanding Intrusion Detection Through Visualization*. USA: Springer.
- Bace, R., & Mell, P. (2001). *Intrusion Detection Systems*. Retrieved 8 September, 2008, from <http://www-cse.ucsd.edu/classes/fa01/cse221/projects/group10.pdf>
- Baker, A. R., Caswell, B., & Poor, M. (2004). *Snort 2.1 Intrusion Detection* (2nd ed.). USA: Syngress Publishing, Inc.
- Baker, A. R., & Esler, J. (2007). *Snort IDS and IPS Toolkit*. Burlington: Syngress Publishing, Inc.
- Balzarotti, D. (2006). *Testing Network Intrusion Detection Systems*. Politecnico di Milano, Italy.
- Beale, J., & Foster, J. C. (2003). *Snort 2.0 Intrusion Detection*. USA: Syngress Publishing.
- Capite, D. D. (2007). *Self-Defending Networks : The Next Generation of Network*

- Security*. Indianapolis, USA: Cisco Press.
- Caruso, L. C., Guindani, G., Schmitt, H., neycalazans, & Moraes, F. (2007). *SPP-NIDS - A Sea of Processors Platform for Network Intrusion Detection Systems*. Paper presented at the 18th IEEE/IFIP International Workshop on Rapid System Prototyping(RSP07).
- Chang, Y.-K., Tsai, M.-L., & Chung, Y.-R. (2008). *Multi-Character Processor Array for Pattern Matching in Network Intrusion Detection System*. Paper presented at the 22nd IEEE International Conference on Advanced Information Networking and Applications, AINA 2008. .
- Chiu, C.-H., Lin, J.-F., Lee, J.-J., & Lei, C.-L. (2007). *A High-Performance Clustering Scheme with Application in Network Intrusion Prevention System*. Paper presented at the IEEE International Symposium on Communications and Information Technologies. ISCIT '07 Sydney.
- Cisco. (2007). Understanding Delay in Packet Voice Networks. Retrieved 4 July, 2008, from <http://www.cisco.com/warp/public/788/voip/delay-details.html>
- Crothers, T. (2003). *Implementing Intrusion Detection Systems*. Indiana: Wiley Publishing, Inc.
- Debar, H., Dacier, M., & Wespi, A. (1999). Towards a Taxonomy of Intrusion Detection Systems. *Elsevier*.
- Dries, J. (2001). An Introduction to Snort: A Lightweight Intrusion Detection System. Retrieved 4 September, 2008, from <http://www.informit.com/articles/article.aspx?p=21777>
- Graham, J. M. (2000). Interaction Effects: Their Nature and Some Post Hoc Exploration Strategies. Retrieved 25, July, 2008, from <http://ericae.net/ft/tamu/interaction.pdf>

- Guerrero, J. H., & Cardenas, R. G. (2005). An example of communication between security tools: Iptables - Snort. *ACM*, 39(3), 34 - 43
- Hutchings, B. L., Franklin, R., & Carver, D. (2002). *Assisting Network Intrusion Detection with Reconfigurable Hardware*. Paper presented at the 10th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'02).
- Jeong, Y., Jeon, J., Ryu, J., & Seo, D. (2006, 20-22 Feb.). *A Developing of Signature-based Network Security Tester for NGSS*. Paper presented at the 8th IEEE International Conference Advanced Communication Technology, ICACT 2006.
- Kim, Y.-H., Jung, B.-H., Lim, J.-D., & Kim, K.-Y. (2007). *Processing of Multi-pattern Signature in Intrusion Detection System with Content Processor*. Paper presented at the 6th IEEE International Conference on Information, Communications & Signal Processing, 2007
- Korenek, J., & Kobiersky, P. (2007, 11-13 April). *Intrusion Detection System Intended for Multigigabit Networks*. Paper presented at the IEEE Design and Diagnostics of Electronic Circuits and Systems, DDECS 07.
- Koziol, j. (2003). *Intrusion Detection with Snort*: Sams Publishing.
- Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). The 1999 DARPA Off-Line Intrusion Detection Evaluation. *Lincoln Laboratory MIT*.
- Maxwell, S. E., & Delaney, H. D. (2004). *Designing Experiments and Analyzing Data* (2nd ed.): Lawrence Erlbaum Associates.
- May, C. J., Hammerstein, J., Mattson, J., & Rush, K. (2006). *Defense-in-Depth: Foundations for Secure and Resilient IT Enterprises*: Carnegie Mellon University.

- McHugh, J., Christie, A., & Allen, J. (2000). Defending Yourself: The Role of Intrusion Detection Systems. *Software, IEEE* 17(5).
- Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network Intrusion Detection. *IEEE Network*, 8(4), 26-41.
- Newman, D., Manalo, K. M., & Tittel, E. (2004). CSIDS Exam Cram 2. Retrieved 4 September, 2008, from <http://www.informit.com/articles/article.aspx?p=174342&seqNum=1>
- Northcutt, S., & Novak, J. (2003). *Network Intrusion Detection* (3rd ed.): New Riders.
- Novak, J., & Sturges, S. (2007). Target-Based TCP Stream Reassembly. Retrieved 25 July, 2008, from <http://www.snort.org/docs/stream5-model-Aug032007.pdf>
- NSSLabs. (2008). Gigabit Intrusion Detection Systems (IDS) Retrieved 10 August, 2008, from <http://www.nssslabs.com/white-papers/gigabit-intrusion-detection-systems-ids.html>
- NSSLabs. (2008). Intrusion Prevention Systems (IPS) Retrieved 1st September, 2008, from <http://nssslabs.com/white-papers/intrusion-prevention-systems-ips.html>
- Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in Computing* (4 ed.). USA: Pearson Education, Inc.
- Puketza, N. J. (2000). *Approches to Computer Security: Filtering, Testing, and Detection*. University of California, Davis.
- Rehman, R. U. (2003). *Intrusion Detection Systems with Snort* (1st ed.). New Jersey Printice Hall PTR.
- Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. Retrieved 5 July 2008, from <http://www.snort.org/docs/lisapaper.txt>
- Schwartz, D. G., Stoecklin, S., & Yilmaz, E. (2002). *A Case-Based Approach to Network Intrusion Detection*. Paper presented at the 5th IEEE International

Conference on Information Fusion, 2002

Smith, C. L. (2003). *Understanding Concepts in the Defence in Depth Strategy*. Paper presented at the 37th Annual IEEE International Carnahan Conference on Security Technology.

Snort. (2008). Snort Users Manual 2.8.2. Retrieved 25 July, 2008, from http://www.snort.org/docs/snort_htmanuals/htmanual_282

Snyder, J. Six Strategies for Defense-in-depth: Securing the Network from the Inside Out. Retrieved 10 July, 2008, from http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Defense-in-depth.pdf

Sommer, R. (2005). *Viable Network Intrusion Detection in High-Performance Environments*. Technische University Munchen, Germany.

Song, H., Sproull, T., Attig, M., & Lockwood, j. (2005, 24-26 Aug.). *Snort Offloader: A Reconfigurable Hardware NIDS Filter*. Paper presented at the IEEE International Conference on Field Programmable Logic and Applications, 2005.

Sourdis, I., Dimopoulos, V., Pnevmatikatos, D., & Vassiliadis, S. (2006). *Packet Pre-filtering for Network Intrusion Detection*. Paper presented at the 2006 ACM/IEEE symposium on Architecture for networking and communications systems California,USA.

Thomas, T. (2004). *Network Security: first-step*. Indianapolis: USA: Cisco Press.

Wagoner, R. (2007). *Performance Testing an Inline Network Intrusion Detection System Using Snort*. Morehead State University, Morehead.

Wan, T., & Yang, X. D. (2001, 10-14 Dec). *IntruDetector: A Software Platform for Testing Network Intrusion Detection Algorithms*. Paper presented at the 17th

Annual IEEE Computer Security Application Conferance.ACSAC2001.

Wu, Y.-S., Foo, B., Mei, Y., & Bagchi, S. (2003). *Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS*. Paper presented at the 19th Annual IEEE Computer Security Applications Conference (ACSAC 2003).

Yaacob, N. A. b. (2003). *Utilizing Snort in the Analysis of Intrusion detection system*.
Unversiti Utara Malaysia, Kedah.

Zamboni, D. (2001). *Using Internal Sensors for Computer Intrusion Detection*.
Purdue University, Purdue