Analyze the Delay Time by Data Mining for Network Intrusion Prevention System Using Bro

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

By

Kaled Hussain Azrane

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)

KALED HUSSAIN AZRANE
(800293)

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)

ANALYZE THE DELAY TIME BY DATA MINING FOR NETWORK INTRUSION PREVENSION SYSTEM USING BRO

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)

Tarikh
(Date) : 28/4/09.

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 important for using the network are increased day by day, and the important for the security for these networks are more important. To implement secure network, the network administrator use several type of security systems and software tools, the most focus systems used in this area are the firewalls and the intrusion detection and prevention systems. There are many features developed every year for these systems and there are many studies done to evaluate and develop these systems, this thesis focus on evaluate the performance for one of famous open free source intrusion detection and prevention system, which is Bro IDS, the thesis will test the performance for Bro in different situations to determine which conditions make Bro work with the minimum delay time for the packets, the thesis will use the data mining tool which it SPSS, to analyse the effects for the main policies on the delay time for the packets when the Bro work as intrusion prevention system.

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, big brother, other brothers, wife, and my three kids 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. Where they 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,

big brother, other brothers, wife,

and kids who lovely encouraged

and supported me through all my study.

The motivation for all I do.

CONTENTS

LIST OF FIGURES

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

CHAPTER ONE

INTRODUCTION

1 INTRODUCTION

Network security is not just about keeping people out of our network. Network security also provides access into our network in the way we want to provide it, allowing people to work together. Strong network security opens up pathways to let authorized people in to our business, regardless of where they are located physically or what kind of connection they have. To improve that and to detect unwanted attacks or even threads, we have to use Network Intrusion Detection System (NIDS). In general, Intrusion Detection System (IDS) is the process of monitoring for and identifying attempted unauthorized system access or manipulation. Most network administrators do IDS all the time without realizing it. Security administrators are constantly checking system and security log files for something suspicious. An antivirus scanner can be considered as IDS when it checks files and disks for known malware. An IDS is tool that can monitor host system changes or sniff network packets off the wire looking for signs of malicious intent.

The upgrading of computer security solutions is non-trivial: many types of intrusion exist, which are diverse in method of action and are constantly evolving. Programs and tools designed to disrupt or damage computer systems are collectively termed malware. The 'infection' of a computer network by malware can result in loss of confidentiality, integrity and availability of data, systems and services. Protection

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 [Electronic Version] 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* 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 Genration of Network Security*. Indianapolis,USA: Cisco Press.

Caruso, L. C., Guuindani, 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

Cisco. (2007). Understanding Delay in Packet Voice Networks [Electronic Version] from http://www.cisco.com/warp/public/788/voip/delay-details.html.

Crothers, T. (2003). *Implementing Intrusion Detection Systems*. Indiana: Wiley Publishing, Inc.

Dries, J. (2001). An Introduction to Snort: A Lightweight Intrusion Detection System [Electronic Version] from http://www.informit.com/articles/article.aspx?p=21777.

Graham, J. M. (2000). Interaction Effects: Their Nature and Some Post Hoc Exploration Strategies [Electronic Version] from http://ericae.net/ft/tamu/interaction.pdf.

Greensmith, J. (2007). *The Dendritic Cell Algorithm*. University of Nottingham.

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 Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'02).

Jeong, Y., Jeon, J., Ryu, J., & Seo, D. (2006). *A Developing of Signature-based Network Security Tester for NGSS.* Paper presented at the 8th IEEE International Conference Advanced Communication Technology, ICACT

Kim, Y., Jung, B., Lim, J., & Kim, K. (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.

Korenek, J., & Kobiersky, P. (2007). *Intrusion Detection System Intended for Multigigabit Networks.* Paper presented at the Design and Diagnostics of Electronic Circuits and Systems, DDECS.

Koziol, J. (2003). *Intrusion Detection with Snort*: Sams Publishing.

Lauf, A. P. (2007). *Hybrids: Embeddable Hybrid Intrusion Detection System.* Vanderbilt University.

Lippmann, R., Haines, J., Fried, D., Korba, J., & Das, K. (2000). *The 1999 DARPA Off-Line Intrusion Detection Evaluation*: Lincoln Laboratory MIT.

Lussi, C. (2008). *Signature-based Extrusion Detection.* Swiss Federal Institute of Technology Zurich.

Maxwell, S., & Delaney, H. (2004). *Designing Experiments and Analyzing Data* (2nd ed.): Lawrence Erlbaum Associates.

May, C., 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., & Levitt, K. (1994). Network Intrusion Detection. *IEEE Network, 8*(4), 26-41.

Newman, D., Manalo, K., & Tittel, E. (2004). CSIDS Exam Cram 2 [Electronic Version] 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 [Electronic Version] from http://www.snort.org/docs/stream5-model-Aug032007.pdf.

NSSlabs. (2008). Gigabit Intrusion Detection Systems (IDS) [Electronic Version] from http://www.nsslabs.com/white-papers/gigabit-intrusion-detection-systems-ids.html.

NSSLabs. (2008). Intrusion Prevention Systems (IPS) [Electronic Version] from http://nsslabs.com/white-papers/intrusion-prevention-systems-ips.html.

Oksuz, A. (2007). *Unsupervised Intrusion Detection System.* Technical University of Denmark.

Papini, D. (2008). *An Anomaly based Wireless Intrusion Detection System.* Technical University of Denmark.

Perdisci, R. (2006). *Statistical Pattern Recognition Techniques for Intrusion Detection in Computer Networks: Challenges and Solutions.* Universita degli Studi di Cagliari, Cagliari, Italy.

Pfleeger, C., & Pefleeger, S. (2007). *Security in Computing* (4th ed.). USA: Pearson Education, Inc.

Pipa, D. (2008). *Intrusion Detection and Prevention: Immunologically Inspired Approaches.* University of London.

Puketza, N. (2000). *Approches to Computer Security: Filtering. Testing, and Detection.* University of California Davis.

Rehman, R. (2003). *Intrusion Detection Systems with Snort* (1st ed.). New Jersey Printice Hall PTR.

Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks [Electronic Version] from http://www.snort.org/docs/lisapaper.txt.

Safiee, M. (2007). *An Intrusion Detection System (IDS) For Internet Network.* Universiti Teknologi Malaysia.

Schwartz, D., Stoecklin, S., & Yilmaz, E. (2002). *A Case-Based Approach to Network Intrusion Detection.* Paper presented at the 5th IEEE International Conference on Information Fusion.

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

Snyder, J. (2008). Six Strategies for Defense-in-depth: Securing the Network from the Inside Out [Electronic Version] 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 Universitat Munchen.

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

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.

Tenhunen, T. (2008). *Implementing An Intrusion Detection System In The Mysea Architecture.* Naval Postgraduate School, Monterey, California.

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

Vallentin, M. (2006). *Transparent Load-Balancing for Network Intrusion Detection Systems.* Technische Universitat Munchen.

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

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

Wan, T., & Yang, X. (2001). *IntruDetector: A Software Platform for Testing Network Intrusion Detection Algorithms.* Paper presented at the 17th Annual IEEE Computer Security Application Conferance.ACSAC.

Wu, Y., 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

Yaacob, N. (2003). *Utilizing Snort in the analysis of intrusion Detection System.* University Utara Malaysia, Kedah.

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

Zanero, S. (2006). *Unsupervised Learning Algorithms for Intrusion Detection.* Politecnico Milano University, Milano.