BORANG PENGESAHAN STATUS TESIS*

JUDUL : PERFORMANCE COMPARISON BETWEEN CENTRALIZED AND DISTRIBUTED IDS

SESI PENGAJIAN : 2009/2010

Saya NOOR IDHAM BIN SULAIMAN
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_________ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_________ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_________ TIDAK TERHAD

(TANDATANGAN PENULIS)
Alamat tetap: No 696, Lot 113,
KG Pulau Kapas Demit,
16150, Kota Bharu, Kelantan.

Tarikh : 18 Julai 2010

(TANDATANGAN PENYELIA)
DR.MOHD FAIZAL BIN ABDOLLAH

Tarikh : 18 Julai 2010

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

PERFORMANCE COMPARISON BETWEEN CENTRALIZED AND DISTRIBUTED IDS

NOOR IDHAM BIN SULAIMAN

This report is submitted in partial fulfillment of the requirements for the
Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2010

DECLARATION

I hereby declare that this project report entitled

PERFORMANCE COMPARISON BETWEEN CENTRALIZED AND DISTRIBUTED IDS

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENTS : ______________________ Date : 25/6/10

(NOOR IDHAM BIN SULAIMAN)

SUPERVISOR : ______________________ Date : 25/6/10

(DR. MOHD. FAIZAL ABDOLLAH)

DEDICATION

To my dearest parents, your love support are my greatest, for continues love, and motivation.

To my helpful lecturer, thank you for being respective and critical, and challenging me to be a better student and for the guidance from the beginning until the end of the final project.

To my dear friends, thank you for all encourage, sacrifice and support that had been given to me to finish my study and final project.

ACKNOWLEDGEMENTS

Throughout the period of doing this project, I received a lot of encouragements from many of my close associates. Firstly, I would like to express my sincere gratitude to my project supervisor, Dr. Mohd Faizal Bin Abdollah for the guidance, support, motivation and help throughout this project.

I also would like to express my most appreciation and apologies to all my family member for their endless support, encouragement and love through, who over the duration has been neglected even ignored, during my deepest concentrations.

Finally, I would like to thank you all of my friends for their help and motivation as they never been disappointed of giving me their fruitful thoughts and ideas throughout the project.

ABSTRACT

This project is focusing on Intrusion Detection System (IDS). IDS have two types which is Centralized IDS and Distributed IDS. This project will make a comparison between them to determine which will give the best result in term of performances. The performances that will be measured in this project are CPU, Memory, I/O, Disk Utilization and Alert. There is a new data and old data in Distributed IDS and Centralized IDS. The old data and the new data have four types of VLAN that had divided from Centralized IDS which each of them will be tested and analyzed. The performances on Centralized IDS also will be tested same as Distributed IDS but in different way. It is require an equipment or software such as TOP, HTOP and NMON to make an analysis. TOP and HTOP has capability to analyzed the used of CPU and Memory, while NMON has the capability to analyzed CPU, Memory, I/O and Disk Utilization. The important software for this project is Snort. Snort will be used to detect an alert in the conducted data. The Snort can detect the alert but not to avoid it. The operating system that had been used in this project is Ubuntu 9.04 and Ubuntu 9.10.

ABSTRAK

Projek ini fokus kepada Intrusion Detection System (IDS). IDS terbahagi kepada dua jenis iaitu Centralized IDS dan Distributed IDS. Dalam projek ini IDS digunakan adalah untuk membuat perbandingan diantara Centralized IDS dan Distributed IDS yang mana lebih bagus dari aspek prestasi. Antara prestasi yang akan dinilai di dalam projek ini ialah CPU, Memory, I/O, Disk Utilization dan Alert. Didalam Distributed IDS dan Centralized IDS terdapat dua jenis data iaitu data lama dan data baru. Didalam data lama terdapat empat jenis VLAN yang telah dipecahkan daripada Centralized IDS dan setiap VLAN yang telah dipecahkan akan diuji prestasinya untuk membuat analisa. Begitu juga dengan data baru, terdapat empat jenis VLAN yang telah dipecah daripada Centralized IDS. Centralized IDS juga akan diuji prestasinya sama dengan Distributed IDS cuma cara untuk jalankan data didalam Centralized IDS sedikit berbeza. Untuk menguji prestasi IDS, projek ini memerlukan alat prestasi atau perisian untuk membuat analisa. Antara perisian yang digunakan didalam projek ini ialah TOP, HTOP dan NMON. Setiap perisian yang digunakan mempunyai keupayaan sendiri untuk membuat analisa. Seperti TOP dan HTOP ia mempunyai keupayaan untuk membuat analisa bagi penggunaan CPU dan Memory. Manakala bagi NMON pula ia mempunyai keupayaan untuk membuat analisa untuk CPU, Memory, I/O dan Disk Utilization. Perisian yang paling penting didalam projek ini ialah snort ia digunakan untuk mengesan alert didalam data yang dijalankan. Snort hanya boleh mengesan alert dan tidak boleh mencegah alert. Sistem operasi yang digunakan didalam projek ini ialah Ubuntu 9.04 dan Ubuntun 9.10.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIX	-	Advanced Interactive Executive
ATM	-	Asynchronous Transfer Mode
CPU	-	Central Processing Unit
DoS	-	Denial of Service
FTMK	-	Fakulti Teknologi Maklumat dan Komunikasi
FE	-	Fast Ethernet
GUI	-	Graphical User Interface
HIDS	-	Host Intrusion Detection Systems
HP	-	Hewlett-Packard
IDS	-	Intrusion Detection System
I/O	-	Input/Output
IPS	-	Intrusion Prevention System
IOS	-	Internetwork Operating System
IP	-	Internet Protocol
IPv6	-	Internet Protocol version 6
Lab	-	Laboratory
NIDS	-	Network Intrusion Detection Systems
NIPS	-	(Network Intrusion Prevention Systems
NMON	-	Nigel Monitoring
PC	-	Personal Computer
PoE	-	Port of Entry
RAP	-	Roving Analysis Port
ROC	-	Receiver Operating Characteristic
RAD	-	Rapid Application Development Model

RAM	-	Random Access Memory
SDLC	-	System Development Life Cycle
SDM	-	Systems Development Method
Span Port	-	Spanning Port
SPAN	-	Switched Port Analyzer
TCP	-	Transmission Control Protocol
UNIX	-	UNiplexed Information and Computing System
UK	-	United Kingdom
VLAN	-	Virtual LAN
VPN	-	Virtual Private Network
VNC	-	Virtual Network Computing
Win	-	Windows
WWW	-	World Wide Web

CHAPTER I

INTRODUCTION

1.1 Project Background

An Intrusion Detection System (IDS) is a system for detecting misuse of network or computer resources. An IDS will have a number of sensors it utilizes to detect intrusions. Example sensors may be:

- A sensor to monitor TCP connection requests.
- Log file monitors.
- File integrity checkers.

The IDS system is responsible for collecting data from its sensors and analyzing this data to give the security administrator notice of malicious activity on the network. IDS technologies are commonly divided into NIDS (Network Intrusion Detection Systems) and HIDS (Host Intrusion Detection Systems).Newer NIDS also attempt to act as NIPS (Network Intrusion Prevention Systems).

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

i. **There are several ways to categorize IDS:**

- Misuse detection vs. anomaly detection: in misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.
- Network-based vs. host-based systems: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.
- Passive system vs. reactive system: in a passive system, the IDS detect a potential security breach, log the information and signal an alert. In a reactive system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.
- Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.