

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 (/)

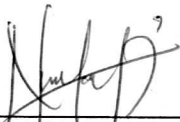
_____ SULIT

(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

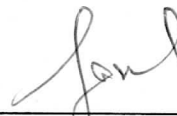


(TANDATANGAN PENULIS)

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**

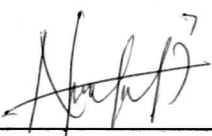
DECLARATION

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

: 

(NOOR IDHAM BIN SULAIMAN)

Date : 25/6/10

SUPERVISOR

: 

(DR. MOHD. FAIZAL ABDOLLAH)

Date : 25/6/10

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 Ubuntu 9.10.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	i
	DEDICATION	ii
	ACKNOWLEDGEMENTS	iii
	ABSTRACT	iv
	ABSTRAK	v
	TABLE OF CONTENTS	vi
	LIST OF TABLE	xiv
	LIST OF FIGURES	xv
	LIST OF ABBREVIATIONS	xx
CHAPTER 1	INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statement	4
	1.3 Objective	5
	1.4 Scope	5
	1.5 Project Significance	6
	1.6 Expected Output	6
	1.7 Conclusion	7

CHAPTER 2 LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1	Introduction	8
2.2	Literatures Review	9
2.2.1	Domain	9
2.2.2	Keyword	9
2.2.2.1	Intrusion Detection System (IDS)	9
2.2.2.2	Centralized intrusion detection system (IDS)	9
2.2.2.3	Distributed intrusion detection system (IDS)	10
2.2.3	Previous Research	10
2.2.3.1	Past Similar Research	11
2.2.3.1.1	Methodology	11
2.2.3.1.1.1	Computer System Security Management model	11
2.2.3.1.1.2	Intrusion Detection System Methodology	13
2.2.3.1.2	System/Project	15
2.2.3.1.2.1	Centralized IDS	15
2.2.3.1.2.2	Distributed IDS	16
2.2.3.1.2.3	Testing Intrusion Detection System	17
2.3	Proposed Solution	19
2.3.1	Project Methodology	19
2.3.1.1	Reference of selected methodology	20
2.3.1.1.1	Prototyping Model	20

	2.3.1.2 Prototyping Model IDS	21
2.4	Project Schedule and Milestones	23
2.5	Conclusion	24
CHAPTER 3	ANALYSIS	
3.1	Introduction	25
3.2	Problem analysis	26
	3.2.1 Network Architecture	26
	3.2.1.1 Hardware	27
	3.2.1.1.1 Switch	27
	3.2.1.1.2 Router	27
	3.2.1.1.3 Server	28
	3.2.1.2 Software	28
	3.2.1.2.1 NMON	28
	3.2.1.2.2 Snort	29
	3.2.1.2.3 NTOP	29
	3.2.1.2.4 HTOP	30
	3.2.1.2.5 TOP	31
	3.2.2 Logical and Physical Design	31
	3.2.2.1 Logical Design	32
	3.2.2.1.1 Centralized IDS	32
	3.2.2.1.2 Distributed IDS	33
	3.2.2.2 Physical Design	35
3.3	Requirement Analysis	36
	3.3.1 Quality of Data	36
	3.3.1.1 Raw Packet	36
	3.3.1.2 Data collection technique	36

	3.3.1.3 Data collection flow	37
	3.3.1.4 Command for Snort	39
	3.3.1.6 Data captured format	41
	3.3.1.7 Data Output Format	43
3.4	Conclusion	46
CHAPTER 4	DESIGN	
4.1	Introduction	47
4.2	Possible Scenarios	48
	4.2.1 Network traffic In Centralized IDS	48
	4.2.2 Network traffic In Distributed IDS	49
	4.2.3 Read Logs/Alert	50
	4.2.4 Flow Centralized IDS	51
	4.2.5 Flow Distributed IDS	53
4.3	Conclusion	54
CHAPTER 5	IMPLEMENTATION	
5.1	Introduction	55
5.2	Network Configuration Management	55
	5.2.1 Configuration Environment Setup	56
	5.2.2 Version Control Procedure	59
5.3	Hardware Configuration Management	64
	5.3.1 Hardware Setup	64
5.4	Development Status	66
	5.4.1 Result Schedule	66
	5.4.2 Distributed IDS	67
	5.4.2.1 Normal Packet Output Using TOP	67

5.4.2.1.1	VLAN 3	67
5.4.2.1.2	VLAN 11	70
5.4.2.1.3	VLAN 35	73
5.4.2.1.4	VLAN 43	74
5.4.2.2	Running Packet with Alert	77
5.4.2.2.1	VLAN 11	77
5.4.2.2.1	VLAN 35	80
5.4.2.2.3	VLAN 43	81
5.4.2.2.4	VLAN 3	84
5.4.3	Centralized IDS	87
5.4.3.1	Running Packet with Alert	87
5.4.3.1.1	VLAN 35	87
5.4.3.1.2	VLAN 3	88
5.4.3.1.3	VLAN 11	91
5.4.3.1.4	VLAN 43	94
5.5	Conclusion	95
CHAPTER 6	TESTING	
6.1	Introduction	96
6.2	Test Plan	96
6.2.1	Test Organization	97
6.2.2	Test Environment	97
6.2.3	Test Schedule	97
6.3	Test Strategy	99
6.3.1	Classes of test	99
6.4	Test Design	100
6.4.1	Test Data	100

6.5	Test Result and Analysis	100
6.5.1	Distributed IDS	100
6.5.1.1	Normal Packet Output Using TOP	100
6.5.1.1.1	VLAN 21	100
6.5.1.1.2	VLAN 35	103
6.5.1.1.3	VLAN 37	106
6.5.1.1.4	VLAN 38	108
6.5.1.2	Running Packet with Alert	111
6.5.1.2.1	VLAN 21	111
6.5.1.2.2	VLAN 35	114
6.5.1.2.3	VLAN 37	116
6.5.1.2.4	VLAN 38	119
6.5.2	Centralized IDS	122
6.5.2.1	Running Packet with Alert	122
6.5.2.1.1	VLAN 21	122
6.5.2.1.2	VLAN 35	125
6.5.2.1.3	VLAN 37	127
6.5.2.1.4	VLAN 38	129
6.5.2.2	Running Normal Packet	130
6.5.2.3	Running Packet with alert	131
6.6	Conclusion	133

CHAPTER 7 CONCLUSION

7.1	Observations on Weaknesses and Strengths	134
7.1.1	Strengths	134
7.1.2	Weaknesses	135
7.2	Propositions for Improvement	135

7.3	Contribution	135
7.4	Conclusion	136
REFERENCES		137
BIBLIOGRAPHY		139
APPENDICES		140

LIST OF TABLE

TABLE	TITLE	PAGE
5.1	Device Configuration Details	57
5.2	Device Configuration Details	59
5.3	Version Control Procedure Old Raw Packet	59
5.4	Version Control Procedure New Raw Packet	62
5.5	Hardware Setup	64
5.6	Result Schedule	66
6.1	Test Schedule	98
6.2	Summary Table	133

LIST OF FIGURES

DIAGRAM	TITLE	PAGE
2.1	Computer System Security management Model	11
2.2	Intrusion Detection System Methodology	13
2.3.	Prototyping Model	20
2.4	Prototyping Model IDS	21
3.1	NMON	28
3.2	Snort	29
3.3	NTOP	29
3.4	HTOP	30
3.5	TOP	31
3.6	Centralized IDS	33
3.7	Distributed IDS	34
3.8	Physical Design Centralized IDS	35
3.9	Physical Design Distributed IDS	35
3.10	Step to capture network traffic In Centralized IDS	37
3.11	Step to capture network traffic In Distributed IDS	38
3.12	Packet Run in Snort	41
3.13	Log/Alert Run in Snort	42
3.14	Memory in HTOP	43
3.15	CPU in HTOP	43
3.16	CPU in TOP	44

3.17	Memory in TOP	45
4.1	Step to capture network traffic In Centralized IDS	48
4.2	Step to capture network traffic In Distributed IDS	49
4.3	Read Log/Alert	50
4.4	Logical Design Centralized IDS	51
4.5	Logical Design Distributed IDS	53
5.1	Logical Design Distributed IDS	56
5.2	Logical Design Centralized IDS	58
5.3	Performance CPU in VLAN 3	67
5.4	Performance Memory in VLAN 3	68
5.5	Performance I/O in VLAN 3	69
5.6	Performance Disk Utilization in VLAN 3	69
5.7	Performance CPU in VLAN 11	70
5.8	Performance Memory in VLAN 11	71
5.9	Performance Memory in VLAN 11	71
5.10	Performance Disk Utilization in VLAN 11	72
5.11	Performance CPU in VLAN 35	73
5.12	Performance Memory in VLAN 35	73
5.13	Performance CPU in VLAN 43	74
5.14	Performance Memory in VLAN 43	75
5.15	Performance I/O in VLAN 43	75
5.16	Performance Disk Utilization in VLAN 43	76
5.17	Performance CPU in VLAN 11 with Alert	77
5.18	Performance Memory in VLAN 11 with Alert	78
5.19	Performance I/O in VLAN 11 with Alert	78
5.20	Performance Disk Utilization in VLAN 11 with Alert	79
5.21	Performance CPU in VLAN 35 with Alert	80

5.22	Performance Memory in VLAN 35 with Alert	81
5.23	Performance Memory in VLAN 35 with Alert	81
5.24	Performance Memory in VLAN 43 with Alert	82
5.25	Performance I/O in VLAN 43 with Alert	83
5.26	Performance Disk Utilization in VLAN 43 with Alert	83
5.27	Performance CPU in VLAN 3 with Alert	84
5.28	Performance Memory in VLAN 3 with Alert	85
5.29	Performance I/O in VLAN 3 with Alert	85
5.30	Performance Disk Utilization in VLAN 3 with Alert	86
5.31	Performance CPU in VLAN 35 with Alert in Centralized	87
5.32	Performance Memory in VLAN 35 with Alert in Centralized	88
5.33	Performance CPU in VLAN 3 with Alert in Centralized	88
5.34	Performance Memory in VLAN 3 with Alert in Centralized	89
5.35	Performance I/O in VLAN 3 with Alert	90
5.36	Performance Disk Utilization in VLAN 3 with Alert	90
5.37	Performance CPU in VLAN 11 with Alert in Centralized	91
5.38	Performance Memory in VLAN 11 with Alert in Centralized	92
5.39	Performance I/O in VLAN 11 with Alert	92
5.40	Performance Disk Utilization in VLAN 11 with Alert	93
5.41	Performance CPU in VLAN 43 with Alert in Centralized	94
5.42	Performance Memory in VLAN 43 with Alert in Centralized	95
6.1	Performance CPU in VLAN 21	100
6.2	Performance Memory in VLAN 21	101

6.3	Performance I/O in VLAN 21	102
6.4	Performance Disk Utilization in VLAN 21	102
6.5	Performance CPU in VLAN 35	103
6.6	Performance Memory in VLAN 35	104
6.7	Performance I/O in VLAN 35	104
6.8	Performance Disk Utilization in VLAN 35	105
6.9	Performance CPU in VLAN 37	106
6.10	Performance Memory in VLAN 37	106
6.11	Performance I/O in VLAN 37	107
6.12	Performance Disk Utilization in VLAN 37	108
6.13	Performance CPU in VLAN 38	108
6.14	Performance Memory in VLAN 38	109
6.15	Performance I/O in VLAN 38	110
6.16	Performance Disk Utilization in VLAN 38	110
6.17	Performance CPU in VLAN 21 with Alert	111
6.18	Performance Memory in VLAN 21 with Alert	112
6.19	Performance I/O in VLAN 21 with alert	112
6.20	Performance Disk Utilization in VLAN 21 with Alert	113
6.21	Performance CPU in VLAN 35 with Alert	114
6.22	Performance Memory in VLAN 35 with Alert	114
6.23	Performance I/O in VLAN 35 with Alert	115
6.24	Performance Disk Utilization in VLAN 35 with Alert	116
6.25	Performance CPU in VLAN 37 with Alert	116
6.26	Performance Memory in VLAN 37 with Alert	117
6.27	Performance I/O in VLAN 37 with Alert	118
6.28	Performance Disk Utilization in VLAN 37 with Alert	118
6.29	Performance CPU in VLAN 38 with Alert	119

6.30	Performance Memory in VLAN 38 with Alert	120
6.31	Performance I/O in VLAN 38 with Alert	120
6.32	Performance Disk Utilization in VLAN 38 with Alert	121
6.33	Performance CPU in VLAN 21 with Alert in Centralized	122
6.34	Performance Memory in VLAN 21 with Alert in Centralized	123
6.35	Performance I/O in VLAN 21 with Alert	123
6.36	Performance Disk Utilization in VLAN 21 with Alert	124
6.37	Performance CPU in VLAN 35 with Alert in Centralized	125
6.38	Performance Memory in VLAN 35 with Alert in Centralized	125
6.39	Performance I/O in VLAN 35 with Alert	126
6.40	Performance Disk Utilization in VLAN 35 with Alert	127
6.41	Performance CPU in VLAN 37 with Alert in Centralized	127
6.42	Performance Memory in VLAN 37 with Alert in Centralized	128
6.43	Performance CPU in VLAN 38 with Alert in Centralized	129
6.44	Performance Memory in VLAN 38 with Alert in Centralized	129
6.45	Performance CPU in Centralized	130
6.46	Performance Memory in Centralized	131
6.47	Performance CPU in Centralized with Alert	131
6.48	Performance Memory in Centralized with Alert	132

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.