

## TESIS^ APPROVAL STATUS FORM

JUDUL: INTRUSION DETECTION SYSTEM (IDS) FOR DETECTING NETWORK THREATS AND VULNERABILITIES  
SESI PENGAJIAN: 2004/2005 I

Saya LEE YEW LOON  
(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 adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
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

Lee.  
(TANDATANGAN PENULIS)

Muhamad Syahrul Ashar B. Sami  
(TANDATANGAN PENYELIA)

Alamat tetap : 154-C, JALAN RAJA LAUT, 50350 KUALA LUMPUR

MUHAMAD SYAHRUL ASHAR B. SAMI

Nama Penyelia

Tarikh : 20/10/04

Tarikh : 20/10/04

CATATAN: \*\* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

**INTRUSION DETECTION SYSTEM (IDS)  
FOR DETECTING NETWORK THREATS AND VULNERABILITIES**

LEE YEW LOON

This report is submitted in partial fulfillment of the requirements for the  
Bachelor of Information and Communication Technology (Computer Network)

FACULTY OF TECHNOLOGY AND COMMUNICATION TECHNOLOGY  
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA  
2004

## ADMISSION

I admitted that this project title name of  
**INTRUSION DETECTION SYSTEM (IDS)**  
**FOR DETECTING NETWORK THREATS AND VULNERABILITIES**

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

STUDENT : Lee. Date : 20/10/04  
(LEE YEW LOON)

SUPERVISOR : Encik Muhamad Syahrul Azhar Bin Sani Date : 20/10/04  
(ENCIK MUHAMAD SYAHRUL AZHAR BIN SANI)

## **DEDICATION**

Specially dedicated to  
my beloved parents, sister and brother who have  
encouraged, guided and inspired me throughout my journey of education

## ACKNOWLEDGEMENTS

This PSM report was being accomplished with the generous help of a great many people, who contributed time, energy, ideas, suggestions, reviews and a great deal of encouragement.

Firstly, I would like to express my appreciation to KUTKM for providing me a well-planned semester. My utmost gratitude goes to my academic supervisor, Encik Muhamad Syahrul Azhar Bin Sani who has providing me a detailed information regarding to PSM via email, telephone and personal meeting. I appreciated the words of guidance and support. He relentlessly bombarded me with hundred of questions, making me aware of the learning process and forcing me to experiment with various methods of conversing knowledge into the implementing system and have eventually smoothen the process of brainstorming and system design.

Highest salute to my beloved parents: Lee Fiang Kew and Tan Chong Hong for their support, love, patience and guidance.

Special thanks are due to all of the lecturers in KUTKM for their invaluable feedbacks, tireless assistances, advices and management behind the scenes. Without their cooperation, the PSM is not being able to go through smoothly.

Finally, to the many friends who have shared in this experience with me from the start. Thank you for being there unconditionally, always with a smile and a good story to share.

## ABSTRACT

Intrusion Detection System (IDS) is a relatively new addition to the field of computer security. It is concerned with software that can distinguish between legitimate users and malicious users of a computer system and make a controlled response when an attacker is detected. The project proposed is mainly for the purpose to detect any network vulnerabilities and threats by providing an extra layer of security to SCS Computer System Sdn. Bhd. where the company is currently using only firewall for security protection. Network Intrusion Detection System (NIDS) has been selected to be used in the project implementation. NIDS provides a layer of defense which monitors network traffic for predefined suspicious activity or patterns, and alert system administrators when potential hostile traffic is detected. There are various commercial NIDS in market, but they may have complex deployment and high monetary cost. The project was designed to address these issues. The purpose of research, particularly literature reviews is to collect data. Through this literature review, scope of project and user requirements can be retrieved whether how big the project is. Prototyping Model has been chosen as a methodology for this project and will be implemented along the system development process to ensure the objectives of the project can be fulfilled. The project proposed is planned to develop IDS technology on the Linux platform. The IDS is using misuse detection which is based on signature recognition. A combination of five primary software packages will be included in the system development for enhancing the IDS usage. With these powerful technologies, the system is not only expected to be workable, but also highly efficient in terms of execution speed and response time. This IDS project will contribute effort to users. In addition to identifying attacks and suspicious activity, IDS data can be used to identify security vulnerabilities and weaknesses.

## ABSTRAK

*Intrusion Detection System (IDS)* atau dinamakan sebagai Sistem Pengesan Penceroboh merupakan sesuatu tambahan kawalan baru dalam alam komputer masa kini. Ia merupakan perisian yang dapat mengenali antara pengguna yang sah dan pengguna yang merupakan penceroboh dan memberikan isyarat sekiranya penceroboh dikesan. Projek ini adalah bertujuan untuk mengesan kelemahan dan penceroboh rangkaian Syarikat *SCS Computer System Sdn. Bhd.* dengan memberikan kawalan tambahan kepada rangkaian tersebut memandangkan syarikat ini hanya menggunakan *firewall* sahaja sebagai perlindungan kawalan. *Network Intrusion Detection System (NIDS)* telah dipilih untuk digunakan dalam pembangunan projek ini. NIDS memberi kawalan tambahan dengan mengesan dan memerhati trafik rangkaian dan memberi isyarat kepada pengguna apabila terdapat aktiviti-aktiviti yang disyaki dikesan. Terdapat banyak jenis NIDS yang komersial dalam pasaran tetapi NIDS yang komersial ini mengenakan bayaran yang mahal dan juga ada yang memerlukan pemasangan atau pembangunan yang rumit. Projek yang dibangunkan ini dapat menyelesaikan masalah yang demikian. Tujuan untuk membuat penyelidikan seperti penyelidikan literatur adalah untuk mengumpul maklumat bagi menetapkan skop projek dan keperluan pengguna. Model Prototaip telah dipilih sebagai metodologi projek ini dan akan digunakan dalam sepanjang proses pembangunan projek bagi memastikan objektif projek dicapai. Projek ini dicadang untuk dibangunkan dengan menggunakan *Linux*. Pembangunan IDS ini adalah dengan menggunakan *misuse detection* dimana pengesanan pencerobohan adalah berdasarkan pengenalan *signature*. Pergabungan 5 perisian pakej akan digunakan bagi pembangunan sistem. Dengan penggunaan teknologi-teknologi canggih, sistem ini bukan saja akan dapat berjalan dengan baik bahkan juga efektif dalam kelajuannya. Projek IDS ini dipercayai akan memberi pelbagai sumbangan kepada pengguna dalam aspek mengesan penceroboh rangkaian, aktiviti-aktiviti yang disyaki dan juga kelemahan sesuatu rangkaian komputer.

## TABLE OF CONTENTS

CONTENT	PAGE
TESIS^ APPROVAL STATUS FORM	
INTRUSION DETECTION SYSTEM (IDS)	
FOR DETECTING NETWORK THREATS AND	
VULNERABILITIES	i
ADMISSION	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT	v
ABSTRAK	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	xii
LIST OF FIGURES	xiii
LIST OF ACRONYMS	xv
LIST OF APPENDICES	xix
CHAPTER I INTRODUCTION	1
1.1 Project Introduction	1
1.2 Problem Statement	2
1.3 Project Objectives	3
1.4 Project Scope	4
1.5 Proposed Solution	5
1.6 Project Significance	6
1.6.1 Project Contribution	6



1.7	Expected Output	7
1.8	Conclusion of Chapter I	7
CHAPTER II LITERATURE REVIEW		8
2.1	Introduction	8
2.1.1	Significance of Literature Review	8
2.2	Fact And Finding	9
2.2.1	Research Case	9
2.2.1.1	IDS Concepts	10
2.2.1.2	IDS Criteria	11
2.2.1.3	Passive and Reactive System	17
2.2.1.4	Misuse and Anomaly Detection	17
2.2.2	Review of Past Similar Research	17
2.2.3	Comparison of IDS and Firewall	24
2.2.4	Result of Past Research	25
2.3	Conclusion of Chapter II	26
CHAPTER III PROJECT PLANNING AND METHODOLOGY		28
3.1	Introduction	28
3.2	High-Level Project Requirements	29
3.2.1	Project Facilities Requirements	29
3.2.2	Software Requirements	29
3.2.3	Hardware Requirements	31
3.3	Project Development Approach	32
3.3.1	Prototyping Model	32
3.3.1.1	Planning Phase	33
3.3.1.2	Analysis Phase	34
3.3.1.3	Design Phase	35
3.3.1.4	Implementation Phase	37
3.3.1.5	Integration and Testing Phase	37
3.3.1.6	Operation and Maintenance Phase	37
3.3.2	Methodology Justification	38

3.4	Task Planning	39
3.4.1	Project Milestones	39
3.4.2	Work Break Down Structure (WBS)	40
3.4.3	Gantt Chart	40
3.5	Conclusion of Chapter III	40
CHAPTER IV ANALYSIS RESEARCH		41
4.1	Introduction	41
4.2	Analysis of Current System	42
4.2.1	Main Business	43
4.2.2	Business Process	43
4.3	Problem Analysis	44
4.4	Analysis of To Be System	46
4.4.1	Functional Requirements	47
4.4.2	Software Requirements	48
4.4.2.1	Primary Software Requirements	49
4.4.2.2	Additional Software Requirements	52
4.4.3	Hardware Requirements	54
4.4.4	Network Requirements	55
4.4.5	Implementation Requirements	56
4.5	Conclusion of Chapter IV	56
CHAPTER V DESIGN		57
5.1	Introduction	57
5.2	Raw Data/Pilot Review	58
5.3	System Architecture	61
5.3.1	Webmin Login Module	64
5.3.2	IDS Sensor Tuning Module	64
5.3.3	Network Packets Capturing Module	65
5.3.4	Packets Processing Module	65
5.3.5	Alert Storing Module	65
5.3.6	Alert Viewing Module	65
5.4	Proposed System Design	66

5.4.1	IDS Decomposition Diagram	67
5.4.2	IDS Context Data Flow Diagram	68
5.4.3	IDS Data Flow Diagram 0	69
5.4.4	Data Flow Diagram For Activity 1	70
5.4.5	Data Flow Diagram For Activity 2	70
5.4.6	Data Flow Diagram For Activity 3	70
5.4.7	Data Flow Diagram For Activity 4	70
5.4.8	Data Flow Diagram For Activity 5	71
5.4.9	Data Flow Diagram For Activity 6	71
5.5	Input/Output Specification	72
5.6	IDS User Interface	75
5.7	IDS Placement Design	78
5.8	Conclusion of Chapter V	81
CHAPTER VI IMPLEMENTATION		82
6.1	Introduction	82
6.2	Software Configuration Management	83
6.2.1	Configuration Environment Setup	83
6.2.1.1	Linux OS Installation	83
6.2.1.2	MySQL Installation	84
6.2.1.3	Installing and Configuring Apache With PHP	84
6.2.1.4	Installing and Setting Up Snort and The Snort Rules	85
6.2.1.5	Setting Up Snort Database In MySQL	85
6.2.1.6	Installing and Configuring ACID	85
6.2.1.7	Installing and Configuring Webmin	87
6.2.1.8	Installing Additional Packages	88
6.2.1.9	Network Configuration	88
6.2.2	Version Control Procedure	90
6.3	Hardware Configuration Management	90
6.3.1	Hardware Setup	90
6.4	Security	91
6.4.1	Security Policies and Plan	91
6.5	Development Status	92

6.6	Conclusion of Chapter VI	93
CHAPTER VII TESTING		94
7.1	Introduction	94
7.2	Test Plan	94
7.2.1	Test Organization	95
7.2.2	Test Environment	95
7.2.3	Test Schedule	96
7.3	Test Strategy	97
7.3.1	Classes of Tests	98
7.4	Test Design	100
7.4.1	Test Description	101
7.4.2	Test Data	101
7.5	Test Case Results	102
7.6	Conclusion of Chapter VII	103
CHAPTER VIII PROJECT CONCLUSION		105
8.1	Observation on Weaknesses and Strengths	105
8.2	Propositions For Improvement	106
8.3	Conclusion	107
BIBLIOGRAPHY		108
APPENDICES		111

**LIST OF TABLES**

<b>TABLE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
3.1	System Development Software	30
3.2	Project Management Software	30
3.3	Hardware Requirement	31
5.1	Partitioning Strategies	58
5.2	Commands and Functionalities	59
5.3	Simple IDS Signature	60
5.4	IDS Signature For DNS	60
5.5	Input and Output Specification	72
7.1	Hardware and Software For Test Environment	96
7.2	IDS Test Schedule	97
7.3	Test Data of IDS Rulesets	102
7.4	Satisfaction Scale	103

## LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	NIDS Network	13
2.2	HIDS Network	15
2.3	DIDS Network	16
2.4	Dragon Squire IDS Topology	19
2.5	Dragon Sensor IDS Topology	21
3.1	Prototyping Model Methodology	33
3.2	Conceptual IDS Topology	36
4.1	Functional Requirements of IDS	47
5.1	Architecture for IDS Security Posture	62
5.2	The IDS Architecture	66
5.3	Decomposition Diagram of IDS	67
5.4	Context Data Flow Diagram	68
5.5	Data Flow Diagram 0	69
5.6	System Distributed Diagram for IDS	71
5.7	Webmin Login Interface	75
5.8	Servers Interface	76
5.9	Rule Sets Interface	76
5.10	Rule Sets Editing Interface	77
5.11	ACID Interface	78
5.12	SCS Company's Network Diagram	79
5.13	IDS Placement for SCS Company's Network	80
6.1	ACID Initial Setup Page	86
6.2	ACID Setup Page	86

6.3	ACID Homepage	87
6.4	IDS Architecture of SCS Company's Network	89
7.1	Top-down Models	98

## LIST OF ACRONYMS

ACRONYM	DESCRIPTION
<b>[A]</b>	
ACID	Application Under Testing
ADODB	ActiveX Database Object
AJK	Ahli Jawatan Kuasa
API	Application Programming Interface
ASP	Active Server Pages
ATA	Advance Technology Attachment
AUT	Application Under Testing
<b>[B]</b>	
BSD	Berkeley Software Distribution
<b>[C]</b>	
Cat	Category
CD-ROM	Compact Disk Read Only Memory
CGI	Common Gateway Interface
CIS	Cerberus Internet Scan Program
<b>[D]</b>	
DDos	Distributed Denial of Service
DDR	Double Data Rate
DIDS	Distributed Intrusion Detection System
DMZ	Demilitarized Zone



DNS	Domain Name Services
<b>[E]</b>	
E-COMMERCE	Electronic Commerce
E-BUSINESS	Electronic Business
E-MAIL	Electronic Mail
<b>[F]</b>	
FTP	File Transfer Protocol
<b>[G]</b>	
GHz	Giga Hertz
GUI	Graphic User Interface
<b>[H]</b>	
HDD	Hard Disk Drive
HIDS	Host Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over Secure Socket Layer
<b>[I]</b>	
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
Inc.	Incorporate
IP	Internet Protocol
IT	Information Technology
<b>[K]</b>	
KB	Kilo Byte
KUTKM	Kolej Universiti Teknikal Kebangsaan Malaysia

**[M]**

MAC	Media Access Control
Mac	Macintosh
MB	Mega Byte
Mb/s	Mega Bit per Second
Mbps	Mega Bit per Second
MD5	Message-Digest Algorithm number 5
ME	Millenniums
MHz	Mega Hertz

**[N]**

NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NFR	Network Flight Recorder
NT	New Technology

**[O]**

OS	Operating System
OSI	Open Systems Interconnection

**[P]**

PC	Personal Computer
PHP	Hypertext Preprocessor
PID	Process Identifier
PSM I	Projek Sarjana Muda Satu
PSM II	Projek Sarjana Muda Dua

**[R]**

RAD	Rapid Application Development Model
RAM	Random Access Memory
RHN	Red Hat Network
RICS	Regulated Information Compliance Systems
RJ45	Registered Jacks 45

ROBO	Remote Office Branch Office
rpm	Remote Package Manager
RSA	Rivest Shamir Adleman public key encryption algorithms
<b>[S]</b>	
SCS	Singapore Computer System
SDLC	System Development Life Cycle
SDM	Systems Development Method
Sdn Bhd	Sendirian Berhad
SDRAM	Synchronous Dynamic RAM
SDSI	Stateful Signature Inspection
SMB	Server Message Block
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SQL	Structured Query Language
SVGA	Super Video Graphics Array
<b>[T]</b>	
TCP	Transmission Control Protocol
<b>[U]</b>	
UDP	User Datagram Protocol
UTP	Unshielded Twisted-Pair
<b>[V]</b>	
VPN	Virtual Private Network
<b>[W]</b>	
WBS	Work Breakdown Structure
<b>[X]</b>	
XP	Extreme Programming

## LIST OF APPENDICES

<b>APPENDIX</b>	<b>TITLE</b>	<b>PAGE</b>
A	Project Milestones	112
A.1	PSM I (BITU 3973) Milestones	112
A.2	PSM II (BITU 3983) Milestones	115
B	Work Break Down Structure (WBS)	118
B.1	Identification of PSM I Activities	118
B.1.1	Work Break down Structure for PSM I	119
B.2	Identification of PSM II Activities	120
B.2.1	Work Break down Structure for PSM II	121
C	Gantt Chart	122
D	Installation and Configuration User Guide	123
D.1	Redhat Linux Installation	123
D.2	Zlib Installation	125
D.3	LibPcap Installation	125
D.4	MySQL Installation and Configuration	125
D.5	Apache Web Server Installation and Configuration	127
D.6	Snort Installation and Configuration	127
D.7	Setting up the database in MySQL	129
D.8	JPGraph Installation	129
D.9	ADODB Installation	129
D.10	ACID Installation and Configuration	130
D.11	Webmin Installation and Configuration	131
D.12	NET_SSLeay Installation and Configuration	132
E	IDS User Guide	133

F	Development Status	147
G	Test Description	150
H	Test Case Results	172
H.1	Linux OS Test Case – UT01	172
H.2	MySQL Server Test Case – UT02	173
H.3	Apache Web Server and PHP Test Case – UT03	176
H.4	Snort Test Case – UT04	177
H.5	ACID, JPGraph and ADODB Test Case – UT05	178
H.6	Webmin and Net_SSLeay Test Case – UT06	180
H.7	System Integration Test Summary	181
H.8	IDS Functionality Test Case – FT01	184
H.9	Security Test Case – SET01	189
H.10	Resource Usage Test Case – RUT01	190
H.11	Stress Test Case – STT01	191
H.12	IDS Comparison Test Case	193
H.13	Firewall Test Case – FWT01	196
I	Testing On IDS	201
I.1	IDS Testing Using Blade Informer	201
I.2	IDS Testing Using Cerberus Internet Scanner	207
I.3	IDS Testing Using SuperScan	208
I.4	IDS Testing Using Nmap	211
J	Intrusion Detection Rule	213
J.1	Network Flight Recorder (NFR) Rule	213
J.2	Snort Rule	214
K	Example of IDS Security Network Design	215
L	Others	217

## CHAPTER I

### INTRODUCTION

#### 1.1 Project Introduction

In today's world, everyone is increasingly dependent on the ability to have instant access to information. The explosion of the internet, along with wireless and broadband technologies, allows companies and individuals, unprecedented "Real Time" access to vast amounts of information. Network security has been an issue almost since computers have been networked together. Since the evolution of the internet, there has been an increasing need for security systems. One important type of security software that has emerged since the evolution of the internet is Intrusion Detection Systems (IDSs). It is the art of detecting inappropriate, incorrect, or anomalous activity on a network. Intrusion detection is needed in today's networking environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in network system. An IDS actually is the high-tech equivalent of a burglar alarm that configured to monitor access points, hostile activities, and known intruders. The simplest way to define an IDS might be to describe it as a specialized tool that knows how to read and interpret the contents of log files from routers, firewalls, servers, and other network devices. Many researches have been made regarding IDS to build a most reliable security defense and to detect various patterns of intruders.

The IDS is suitable for any types of organizations for protecting the network and system security. From this project proposed, SCS Computer System Sdn. Bhd.

will be chosen as a study case. The main reason of choosing this company is because the current network of SCS Computer System Sdn. Bhd. is running without any IDS approaches. There is only a firewall implemented to protect the entire network of the company.

Methodology that will be using for this project is Prototyping Model. This methodology is being chosen to ensure that the objective of the project can be archive and is important in building fast, better, more reliable, better quality systems. "Prototyping Model involves the process of developing a fast testing or experiment system to evaluate by the end user (Laudon & Ladon, 1996a)." Prototyping Model is a system development methodology based on building and using a model of a system for designing, implementing, testing, and installing the system. The Prototyping Model consists of 6 primary phases which are planning, analysis, design, implementation, integration and testing and operation and maintenance.

## 1.2 Problem Statement

Undeniable, one of the well-known strategies nowadays is that many of the organizations will protect their network or system using firewall. The most common misconception is that a firewall will secure an organization computer facility and additional steps need not to be taken. A firewall is just one component of an effective security model. As refer to SCS Computer System Sdn. Bhd., additional components or layers should be added to provide an effective security model within the company. Using only firewall may not secure enough as most of the intruders nowadays are genius enough to break through the firewall easily and access to the network or database system.

Threats and vulnerabilities in SCS Computer System Sdn. Bhd. networking environment are also constantly increasing. There are people or groups who have the potential to compromise the network system. These may be a curious teenager, a

disgruntled employee, or espionage from a rival company or a foreign government. The hacker has become a nemesis not only SCS Company but to many others companies.

Backdoor programs such as Trojan are increasing from time to time. The techniques used to intrude are constantly improving. This may cause serious problem in the network environment as well as the computing environment. The personal or SCS Company's secret data may not secure and may be fall into the hacker's hand.

### **1.3 Project Objectives**

From the project's point of view, the primary objective of proposing this project theme is to detect network threats and vulnerabilities. The objectives are stated as below:

- i. To setup an effective network security for monitoring 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.
- ii. To protect data and systems integrity by preventing outsiders to access critical files or authentication databases except by authorized systems administrators.
- iii. To provide an extra layer of protection for a system by placing IDS before or after a firewall monitoring access from the internet through the sensitive data ports of the secured system and detect whether unknown