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

(TANDATANGAN PENULIS)

(TANDATANGAN PENYELIA)

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

MUHAMAD SYAHRUL AZHAR B. SANI
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 : . 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 lindungan 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 dibangun 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

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ACRONYM	DESCRIPTION
[A]	
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]	
BSD	Berkeley Software Distribution
[C]	
Cat	Category
CD-ROM	Compact Disk Read Only Memory
CGI	Common Gateway Interface
CIS	Cerberus Internet Scan Program
[D]	
DDos	Distributed Denial of Service
DDR	Double Data Rate
DIDS	Distributed Intrusion Detection System
DMZ	Demilitarized Zone

DNS	Domain Name Services
[E]	
E-COMMERCE	Electronic Commerce
E-BUSINESS	Electronic Business
E-MAIL	Electronic Mail
[F]	
FTP	File Transfer Protocol
[G]	
GHz	Giga Hertz
GUI	Graphic User Interface
[H]	
HDD	Hard Disk Drive
HIDS	Host Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over Secure Socket Layer
[I]	
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
Inc.	Incorporate
IP	Internet Protocol
IT	Information Technology
[K]	
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
[S]	
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
[T]	
TCP	Transmission Control Protocol
[U]	
UDP	User Datagram Protocol
UTP	Unshielded Twisted-Pair
[V]	
VPN	Virtual Private Network
[W]	
WBS	Work Breakdown Structure
[X]	
XP	Extreme Programming

LIST OF APPENDICES

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