AN ANALYSIS OF INTRUSION DETECTION SYSTEM

FAZILAH BT FUZI

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2011

BORANG PENGESAHAN STATUS TESIS

JUDUL: **AN ANALYSIS OF INTRUSION DETECTION SYSTEM**

SESI PENGAJIAN: **SEMESTER 2010/2011**

Saya **FAZILAH BT FUZI**
(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 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: Kg Chicha Menyabong
Sering 16150 Kota Bharu
KELANTAN

Tarikh : 7/7/11

(TANDATANGAN PENYELIA)

EN MOHD ZAKI BIN MAS'UD
Nama Penyelia

Tarikh : _____

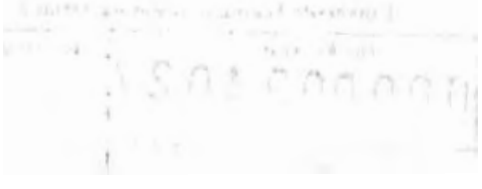
CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

AN ANALYSIS OF INTRUSION DETECTION SYSTEM

FAZILAH BT FUZI

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
2011



DECLARATION

I hereby declare this project report entitled

AN ANALYSIS OF INTRUSION DETECTION SYSTEM

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

STUDENT : _____ Date: _____

(FAZILAH BT FUZI)

SUPERVISOR : _____ Date: _____

(MR. ZAKI BIN MAS'UD)

DEDICATION

Dear Allah, I devoted my life for Allah and May my life is under His guidance.

Dear my parents thank you for your sacrifice and love.

Dear Teacher, thank you for your sacrifice and knowledge. May your knowledge are blessed.

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

To my supportive friends and my supervisor, thank you so much for assist and help.

ACKNOWLEDGEMENTS

Bismillahirrahmanirrahim

First of all the rest of my life, Alhamdulillah, Thanks to Allah SWT, whom with His willing give me the opportunity to complete this Final Year Project, Projek Sarjana Muda which is title Wireless An Analysis of Intrusion Detection System. This final year project report was prepared for Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), importantly for final year student to complete the undergraduate program that leads to the degree of Bachelor of Computer Science. This report is based on the methods given by the university.

I would like to express my appreciation to UTeM for providing me a well-planned semester. Mu utmost gratitude goes to my academic supervisor, Encik Zaki Bin Mas'ud who has providing me me detailed information regarding to PSM and very appreciated the words of guidance and supports.

Highest salute to my beloved parents: Fuzi Bin Mamat and Sakilah Bt Md Zain for their supports, love, patience and guidance.

Special thanks are due to all of the lecturers in UTeM for their invaluable feedbacks, tireless assistance, advices and management behind scenes.

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

Firstly, I would like to express my deepest thanks to, Mr. Othman bin Mohd, a lecturer at FTMK, UTeM and also assign, as my supervisor who had guided be a lot of task during semester session 2010/2011. I also want to thanks the lecturers and technicians of FTMK for their cooperation during I complete the final year project that had given valuable information, suggestions and guidance in the compilation and preparation this final year project report.

Deepest thanks and appreciation to my parents, family, special mate of mine, and others for their cooperation, encouragement, constructive suggestion and full of support for the report completion, from the beginning till the end. Also thanks to all of my friends and everyone, that has been contributed by supporting my work and helps myself during the final year project progress till it is fully completed.

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. This project is about the Intrusion Detection System using Snort and Sax2 to give security for wireless network. In this project, the capabilities of Snort and Sax2 will be discussed. A detailed explanation of how to install Snort and Sax2, including the installation and configuration of Snort for use as an IDS. 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 alerts 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 purpose of research, particularly literature review is to collect data. Through this literature review, scope of project and user requirements can be retrieved whether how big the project is. The project methodology that will be going to use in this project is Systems Development Life Cycle (SDLC) approach. The IDS developed consists of weaknesses and strength in its functionality. This software is configured using Linux operating system and MySQL server as database. Overall this implementation of security will give more benefit and information's to users that want to monitor their network.

ABSTRAK

Intrusion Detection System (IDS), adalah tambahan yang relatif baru di bidang keselamatan computer. Hal ini berkaitan dengan peranti lunak yang dapat membezakan antara satu yang sah, pengguna dan pengguna yang berniat jahat dalam system computer. Projek ini adalah tentang Intrusion Detection System menggunakan perisian Snort dan Sax2 untuk memberikan keselamtan bagi rangkaian. Projek ini adalah tentang Intrusion Detection System menggunakan snort dan Sax2 untuk memberikan keselamatan bagi rangkaian. Dalam projek ini, kemampuan Snort dan Sax2 akan I bahas. Penjelasan terperinci tentang cara memasang Snort dan Sax2, termasuk pemasangan dan kongfigurasi Snort untuk digunakan sebagai IDS. NIDS telah dipilih untuk digunakan dalam pelaksanaan projek. NIDS menyediakan lapisan pertahanan yang memantau lalu lintas rangkaian untuk aktiviti-aktiviti yang mencurigakan standard atau pola-pola, dan tanda-tanda pentadbir sistem ketika lalu lintas bermusuhan berpontensi dikesan. Ada pelbagai NIDS komersial di pasaran, tetapi mereka mungkin mempunyai penyebaran yang kompleks dan kos kewangan yang tinggi. Tujuan kajian ini adalah untuk mengumpul data melalui pustaka, ruang lingkup keperluan projek dan pengguna boleh diambil seberapa besar projek tersebut. Metodologi projek yang akan digunakan dalam projek ini adalah Pembangunan Life Cycle (SDLC) pendekatan. IDS dibangunkan terdiri dari kelemahan dan kekuatan dalam fungsinya. Peranti lunak ini dikongfigurasikan menggunakan sistem operasi Linux dan pelayan MySQL sebagai pengkalan data. Secara keselamatan akan memberikan keuntungan yang lebih dan maklumat bagi pengguna yang ingin memantau rangkaian mereka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Project Background

This project will be focusing on performance comparison between Intrusion Detection System (IDS) software and also log analysis for the intrusion detection system. As we all know Intrusion Detection has been define by Mukherjee, Heberlein, & Levitt, (1994) as "the problem of identifying individuals who are using computer system without authorization (i.e., 'the crackers') and those who have legitimate access to the system but are abusing their privilages (i.e., 'inside threat')".

So Intrusion Detection Systems (IDSs) evolves into critical component secure network architecture. Therefore, this project is to compare the performances of two categories of Intrusion Detection System in order to see which types of Intrusion Detection System (IDSs) will give the best result in monitoring and detecting all of the threads.

This project also will be focusing on log analysis that will be generated by these Intrusion Detection Systems software. As we all know, log analysis is one of the most overlooked aspects of intrusion detection. Nowadays we see every desktop with an anti-virus, companies with multiple firewalls and even simple end-users buying the latest security related tools but unfortunately there are only a small amount of people who cares about their tools.

Nowadays, security of network has been an issue almost since computers have been networked together. An increasing need for security system since the evolution of internet. Intrusion Detection Systems (IDSs) is one of important types of security software since of internet evolution which is art of detecting inappropriate, incorrect or anomalous activity on a network. Today's, network environment needs the intrusion detection because it is impossible to keep pace with the current and potential threats and vulnerabilities in network systems.

Actually, IDS also 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 IDS might be to describe it as a specialized tool that knows how to read and interrupt the contents of log files from routers, firewalls, servers and other network devices.

Many researchers have been made regarding IDS to build a most reliable security defences and to detect various patterns of intruders. The IDS is suitable for any types of organization for protecting the network and system security.

1.2 Problem Statement(s)

Many studies had been done in order to test the performance not only on Host Intrusion Detection System but also Network Intrusion Detection System base but mostly all of these studies will focus on the Network Intrusion Detection System software and Host Intrusion Detection System. The most popular software based on is Snort, Bro, Ossec, and so on.

As we all know, Snort is currently the most popular open source Intrusion Detection System software and the advantages of Snort also numerous such as it can perform content matching and searching, perform protocol analysis and it also can be used to detect many types of attacks. It also can be install on lots of platform such as Windows, Linux, Solaris and many more. A lot of attacks can be stop or prevent earlier if the administrator cared to monitor their logs.

Nowadays, one of the well-known strategies is that many of the organization and network structure will be protect their network or system using firewall. The most common misconception is that a firewall will secure an organization computer security and additional steps not be taken. A firewall is just one component of an effective security model. Besides that, using only firewall may not secure enough as most of intruders nowadays are genius to break through the firewall easily and access to the network or database employee and so on. The hacker has become a nemesis in companies. The personal data may not secure and may be fall into the hacker's hand.

1.3 Objective

Intrusion detection system faced many weaknesses in system especially in identifying the suitable and appropriate threshold to distinguish between the normal and abnormal network traffic. 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 compare which IDS software are the best in order to detect the intrusions when implement in a real-time Intrusion Detection System.

ii. Comparison of IDS based on signature, sensor, alerts and logs.

iii. Recommend the network IDS based on the analyzer parameter such as sensor, alerts and signature.

1.4 Scope

The scope for this project is mainly to implement an IDS using Linux platform. There is a conceptual topology that will be implemented as stated early.

i. The scope of the project is to compare the performance in real time environment between IDS hereafter in order to fine the best software of IDS in order to detect the intrusions and also to watch and monitor the log file.