SOFTWARE COMPARISON HOST BASED INTRUSION DETECTION SYSTEM

MOHD ALIFF BIN ABDUL RAHMAN

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2011

SOFTWARE COMPARISON HOST BASED INTRUSION DETECTION SYSTEM

MOHD ALIFF BIN ABDUL RAHMAN

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

BORANG PENGESAHAN STATUS TESIS*

JUDUL: SOFTWARE COMPARISON HOST BASED INTRUSION DETECTION SYSTEM

SESI PENGAJIAN: 2010/2011

Saya MOHD ALIFF BIN ABDUL RAHMAN
(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: No 54 Kg Sg Pinang,
Palekbang, 16040 Tumpat,
Kelantan.

Tarikh : 5/7/2011

(TANDATANGAN PENYELIA)

Prof. Madya Dr Rabiah Binti Ahmad

Tarikh : 5/7/2011

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

DECLARATION

I hereby declare this project report entitled

SOFTWARE COMPARISON HOST BASED INTRUSION DETECTION SYSTEM

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

STUDENT : _____ Date: 5/7/2011

(MOHD ALIFF BIN ABDUL RAHMAN)

SUPERVISOR : _____ Date: 5/7/2011

(PROFESSOR MADYA DR RABIAH BINTI AHMAD)

DEDICATION

This work is dedicated to my beloved family and siblings, especially my beloved parents, Tuan Zaharah Binti Tuan Yusoff and Abdul Rahman Bin Mat who always encourage me.

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

ACKNOWLEDGEMENTS

First of all I would like to thank Allah because of His kindness and bless, I finally able to finish up my PSM with successful, Alhamdulillah. Here I would like to take this chance to express my appreciation to UTeM for providing me a well-planned semester. Most gratitude goes to my Projek Sarjana Muda supervisor, Prof. Madya Dr Rabiah Binti Ahmad for her kindness and providing me detailed information regarding to PSM and very appreciated the words of guidance and supports.

I also would like to give a big appreciation to both of my parents who always giving me advices and morale support and without their concern, it is very impossible for me to finish up my project. Also special thanks to all of the lecturers in FTMK for their advice and feedbacks when assist me in my project.

And finally, to my beloved friends who have shared their ideas with me from the beginning of the PSM and willing to give lots of co-operation and suggest the solution for the problem. 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 is a type of security management system for computers and networks. An IDS system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). IDS use vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network. This project will be focusing on performance comparison between Host IDS hereafter (HIDS) software and also detection for the intrusion detection system. Host Intrusion Detection becomes an important key element in the security approach in order to protect the network. So the performance of this Host Intrusion Detection software must be very high in order to perform the real time intrusion detection. The word real time here means that the software must be able to detect the intrusion activities before any damage can be happen to the network system and also the services. This project will compare the performances between Snort and also Ossec in order to see which types of Intrusion Detection System (IDSs) will give the best result in monitoring and detecting all of the threads. We also will be focusing on detection that will be generated by these Intrusion Detection Systems software. The objectives of the project is to compare, monitor and also to understand the log files and the result from the project will be used to select the best Host IDS.

ABSTRAK

"Intrusion Detection System" adalah sejenis sistem keselamatan pengurusan untuk komputer dan rangkaian. "IDS" akan mengumpul dan menganalisa maklumat dari pelbagai kawasan dalam sebuah komputer atau rangkaian untuk mengenalpasti kesalahan dari segi keselamatan yang mungkin, yang meliputi baik gangguan (serangan dari luar organisasi) dan penyalahgunaan (serangan dari dalam organisasi). "IDS" menggunakan teknologi imbasan (juga disebut sebagai "scanning"), yang merupakan teknologi yang dibangunkan untuk mengimbas keselamatan dari sebuah sistem komputer atau rangkaian. Projek ini akan menumpukan pada perbandingan prestasi antara perisian "Host IDS" yang juga disebut (HIDS) dan juga kemampuan untuk mengesan sebarang pencerobohan. "Host IDS" menjadi kunci elemen yang sangat penting dalam pendekatan keselamatan untuk melindungi rangkaian. Oleh sebab itu prestasi perisian "Host IDS" perlulah tinggi bagi mengesan sebarang pencerobohan pada masa sebenar (Real-Time). "Real-Time" di sini bermaksud perisian tersebut harus dapat mengesan kegiatan pencerobohan sebelum apa-apa kerosakan boleh berlaku pada sistem rangkaian dan juga perkhidmatan. Projek ini akan membandingkan prestasi antara "Snort" dan juga "Ossec" dalam rangka untuk melihat jenis "Intrusion Detection System" (IDS) mana yang akan memberikan hasil yang terbaik dalam memantau dan mengesan aktiviti pencerobohan. Projek ini juga akan memfokuskan pada pengesanan yang akan dihasilkan oleh perisian "Intrusion Detection Systems". Tujuan utama projek ini adalah untuk membandingkan, memantau dan juga untuk memahami fail-fail log dan hasil dari projek ini akan digunakan untuk memilih perisian "Host IDS" yang terbaik.

TABLE OF CONTENTS

CHAPTER II LITERATURE REVIEW AND PROJECT METHODOLOGY

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION	WORD/DESCRIPTION
IDS	Intrusion Detection System
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
DNS	Domain Name System
DOS	Denial Of Service
FTP	File Transfer Protocol
SSH	Secure Shell
GNU GPL	GNU General Public License
ICT	Information and Communication Technologies
LAN	Local Area Network
MAC	Media Access Control
OS	Operating System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol

CHAPTER I

INTRODUCTION

1.1 Project Background

Using internet through multi-computer devices in a certain corporation put various files, data, and any other valuable information in danger of intruder's attacks. So, Network Security becomes a large and growing area of concern between corporations whiles accessing internet. Meanwhile and up to now, there is no mechanism that can promise to totally secure a network, therefore, network administrators deploy a variety of perimeter and host-based tools such as firewalls, intrusion detection system, patch and version managers, and anti-virus tools in order to deal with the constant threats and maintain an acceptable level of security. These tools form an integrated line of defence against network attacks.

This project will be focusing on performance comparison between Host IDS hereafter (HIDS) software and also how the Intrusion Detection System will react on several attack after they been launch to test the performance of Intrusion Detection System.

The term "Intrusion Detection" implies discovering attacks and threats throughout an enterprise, and responding to those discoveries. Some of the automated responses typically include notifying a security administrator via a console, e-mail, pager; stopping the offending session; shutting the system down; turning off down Internet links; disabling users; or executing a predefined command procedure. Clearly Defined: "Intrusion Detection" is more than just a coded application.

An effective Intrusion Detection system needs to limit false positives—incorrectly identifying an attack when there is none. At the same time it needs to be effective at catching attacks. Figuratively speaking, Intrusion Detection is like a surveillance camera and alarm system all rolled into one. False alarms are distracting and reduce the effectiveness of an Intrusion Detection system. Failing to catch a break-in reduces its value even further. To detect new types of attacks an Intrusion Detection tool must have a way to be quickly updated. This is particularly challenging since updates of attack detection scenarios need to be more frequent than typical product release upgrade cycles of three to nine months. In fact, to be effective probably requires updating the software to new detection procedures on a regular basis[13] .

This project also will be focusing on how these Host IDS will handle attack that comes from several sources. Attacks such as network attack and social engineering attack will be launch directly to the servers that contain Intrusion Detection System software that has been selected to monitor the servers from any outsider and insider attacks that can harm and damage the whole files and network system itself.

1.2 Problem Statements

A few years ago, hacking took a lot of time and study. While expert hackers still abound, the Internet has entered a new era. Using almost any search engine, average Internet users can quickly find information describing how to break into systems; for example, simply searching for key words like hacking, password cracking, and Internet security. Thousands of sites publish step-by-step instructions as to how to break into Windows NT systems, Web Servers, UNIX systems, etc. The sites often include tools that automate the hacking process. In many cases the tools have easy to use graphical interfaces.

For instance, a tool called "crack" automatically attempts to guess UNIX passwords. A similar tool called L0phtcrack breaks Windows NT passwords. A software probe called SATAN discovers vulnerable systems in a network and reports on the specific holes that can be exploited. What does all this mean? Almost anyone with the motivation to break into systems can quickly obtain the technology to do so without having to become an expert hacker. Attacks come from both the inside and the outside.

Many studies had been done in order to test the performance not only on Network Intrusion Detection System but also Host Intrusion Detection System base but mostly all of this studies only focusing on the Network Intrusion Detection System software and only test whether they can detect only network attacks and not the social engineering attacks.

Snort is one of the most popular and most well known software based on Network Intrusion Detection System and the good things about this software is it is open source software and it's free.

One other major problem with Host Intrusion Detection System is false positive and false negative. False positive is when an alarm is generated for an event that is not malicious and false negative is when a malicious event goes undetected.

Usually false negative is more serious because it mean malicious event occur on host and cannot be detected. So that's why this project will look at the log file because there is nobody that watching or monitoring all of the information these tools generate or even worse who is watching our mail server or authentication log and web server? A lot of attacks can be stop or prevent earlier if the administrator cared to monitor their logs.

1.3 Objective

Host Intrusion Detection becomes an important key element in the security approach in order to protect the network. So the performance of this Host Intrusion Detection software must be very high in order to perform the real time intrusion detection. The word real time here means that the software must be able to detect the intrusion activities before any damage can be happen to the network system and also the services.

Objectives that will be achieved at the end of this project are :

- To compare which Host IDS are the best in order to detect the attacks when implement in a real-time Intrusion Detection System.

- To compare the performance of which HIDS software are able to consistently operate in all circumstances when there is an attack launch on the network.

- To analyze and evaluate the capabilities of HIDS from data collected.

- To find out which Host IDS is better when detecting network attack and social engineering attack.

1.4 Scope

The scope of the project is to compare the performance in real time environment between two Host Intrusion Detection System hereafter (HIDS) in order to fine the best software of HIDS in order to detect the intrusions that were cause by network attack for example FTP Brute Force Attack, Open Port Scanner, SSH Brute Force Attack and also to monitor whether this two HIDS can detect the attack that come from social engineering attack for example Trojan Horse, Network Monitoring, E-Mail Attachment and many more attack.

From the result, the administrator will know exactly and understand the log file by correlated the bad events, correlated the good events, and also to look for unusual pattern that are not in the bad and good list for the intrusion detection system.

The whole test activities will be conduct in an isolated local area network (LAN) that will be detailed explain on the next chapter because the test will be conduct to test the HIDS software whether they can perform in normal environment where there are no attack occur to the network and also will be test in stress environment where there will be a lots of attack to the specific host in the network.

1.5 Project Significance

The project significance will be focusing on the users that want to implement the Host Intrusion Detection System (HIDS) software on their network system because from this project, the users are able to choose and select the best software that will be comparing in this project based on their detection on attacks that will be launch to the host.

Users or the Administrator also can protect the network and more importantly the servers that has been setup on the current network by the hacker or attacker whether insider or outsider attacker that want to brake or damage the whole system by launching the selected attack directly to the specific host on the network whether they want to get the information illegally or they just want to test the security of the network.

By looking at the logs from the Host IDS, administrator also can monitor and watch the whole network system activities and by doing that, the administrator or user can easily understand what happened on the network based on the detection and also based on the logs file system that has been generated by the Host Intrusion Detection System (HIDS) software.

1.6 Expected Output

The expected output that will be achieved after carrying out the project is will be able to identify which types of Host Intrusion Detection System (HIDS) software are better not only in terms of performance on the network but also the abilities of the Host Intrusion Detection System (HIDS) software in detecting all kind of attacks that will be perform in order to test both Host Intrusion Detection System (HIDS) software.

Both Host Intrusion Detection System (HIDS) software also will be test by perform lots of attack. The type of attack that will be use to test both software are network attack and also social engineering attack. So by perform those attacks, we want to see whether these Host Intrusion Detection System (HIDS) software can detect that kind of attack or not.

1.7 Conclusion

With the explosion of Internet connectivity and the pervasive access every day users have to both internal and external networks, experts have seen a tremendous rise in attacks and corporate and government networks. At the same time the complexity of our enterprises has increased rapidly. Many organizations report that they have more computer systems than users. Add to this the diversity of operating system platforms, routers, network protocols, applications, web servers, databases, etc., and we can quickly see why trying to spot an attack becomes extremely difficult. Without sophisticated tools, it's nearly impossible.

For the summary, this chapter discusses about the introduction of the projects to be developed. The introduction to the project including project objectives, project scope, the significant of this project, the expected output from this project and also the problems that enabled this project.

Next chapter will be Literature Review and Project Methodology that discuss about methodologies, techniques, software and hardware that is being used in other research or in this project.