UNIVERSITI TEKNOLOGI MARA

SYSTEMATIC MONITORING ATTACK REPULSION TOTAL DETECTION (SMART) DETECTION

KHAIRUNNISA HALIM AZMAN
2009447762

Thesis submitted in partial fulfillment of the requirements
for the degree of
Bachelor of Science (Hons) in Data Communication and Networking
Faculty of Computer and Mathematical Science

April 2011

ACKNOWLEDGMENT

First of all, I would like to pay my gratitude to the Almighty, Allah S.W.T for giving me the will and strength in completing my final year project. Thank you for giving me the guidance and courage in order to complete this research.

A special thanks to Pn Zolidah Kasiran my supervisor for her patience and guidance and Cik Shasarida Bidin who is the senior engineer at Sapura Secured Technologies (SST) for her support and guidance throughout the whole process in completion of this project. This project could not be accomplished without their advice and encouragement.

A million of thanks go to my beloved family for their moral and financial support in completing this project. Not to forget, my fellow friends and others who have contributed direct or indirectly towards the completion of this research. Thank you very much and may Allah SWT bless you all.

ABSTRACT

Nowadays, we commonly used internet connections in our daily life activities such as communicating with friends and families, paying bills, retrieve information, downloading software and so on. Even some of the organizations and company also used internet connections for business purposes such as communicate with client, exchanging document and etc. However, the activities that have been mentioned earlier may cause threats to intrude into user computer and run silently behind it. This situation may pose a problem to the user because the intruders can stealth the information in user computer such as password, company confidential data and other business documentation. Currently, an intrusion detection system (IDS) is an important component for protecting information resources. It is similar to burglar alarms in the physical world which it monitors for intrusions and alert designated parties when suspicious activity is detected. The main objective of this project is to implement this IDS technology in Sapura Secured Technology (SST) network so that the network administrator of SST will be alert if there have any threats that try to intrude into their network. To successfully achieve our objective, we followed the guideline that we set in the methodology as well as following the timeline that has been stated strictly. This system is hopefully can overcome the possible threat of current network at SST such as IP Spoofing and Virus Attack.

TABLE OF CONTENT

CHAPTER 1
INTRODUCTION

Network based on TCP/IP protocols had become a part of our life. We use them for our daily life activities such as to retrieve information, communicate with customers or friends, paying bills and etc. There are never ending usage for internet and as it increases the security for user computer also increase similarly. However, the protection for the network only has a little progress. This might cause a problem because there is still a lot of security problems occur in the enterprise as well as the private network nowadays. (Allix, 2007)

Today's most popular intrusion protection is firewall. However, firewall will become defenseless when it comes to errors in configuration, ambiguous security policies, insider attacks and also data-driven attacks through allowed services. Taking the chance from this situation, many of the providers started to commercial their intrusion detection tools to help the users affectively protecting their network as well as others digital asset such as anti-viruses.

There are two general approaches to detect intrusions in the network which is misuse detection and anomaly detection. Attempt to detect known attacks against computer system are the character of misuse detection meanwhile anomaly detection uses the knowledge of user's normal behavior to detect attempted attacks. (Ghosh et al, 2000)