AN INTRUSION DETECTION SYSTEM (IDS) FOR INTERNET NETWORK

MOHAMAD FAUZAN BIN SAFIEE

A project report submitted in partial fulfilment of the
Requirements for the award of the degree of
Master of Engineering (Electrical - Electronic and Telecommunication)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

MAY 2007

To my beloved wife, mum and all my siblings
thanks a lot for your patience and prayer for my success.
Al-Fatihah to my late father.

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my thesis supervisor, Dr. Sharifah Hafizah bt. Syed Ariffin, for encouragement, guidance, critics and friendship. I am also very thankful to Assoc. Prof. Liza bt. Abdul Latif and my friend Br. Muhammad Sadry bin Abu Seman for their guidance, advices and motivation. Without their continued support and interest, this thesis would not have been the same as presented here.

I am also indebted to Ministry of Defence (MINDEF) for funding my Master study. Librarians at UTM and MINDEF also deserve special thanks for their assistance in supplying the relevant literatures.

My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family members especially my beloved wife.

ABSTRACT

An Intrusion Detection System (IDS) is detects and blocks unwanted attacks to the civilian or the military systems. These attacks can be an internal attack or external attack. The traffic or the normal networks is heterogeneous where else the military network has more homogeneous traffic. Even though the internet security includes firewall and other system security it usually failed to filter out the unwanted attack to the system and allows system breakdown and system failures. The major problems in developing the IDS method is the evolving growth of the internet topology and the growth of the internets users which makes the modeling of the network with attack free data is difficult. Real world test has shown overwhelming numbers of false alarms of attack and little success in filtering them out. This project is to analysis the network with data free attacks in a simulator that involved self-similar traffic that ideally represents the internet traffic modeling as well as the Poisson traffic modeling for the non peak hours periods. With templates of data free attacks a system will reduce the complexity in detecting the attacks during peak hours and non peak hours. The network system was simulated in NS-2 simulator.

ABSTRAK

Sistem Pengesanan Pencerobohan (SPP) ini mengesan dan menyekat serangan yang tidak diingini kepada sistem orang awam atau tentera. Serangan ini boleh dilaksanakan samada serangan secara dalaman atau luaran. Bagi aliran trafik rangkaian biasa, ia adalah berbentuk pelbagai jenis yang mana rangkaian tentera aliran trafiknya lebih berbentuk sama jenis. Walaupun ia dilengkapi dengan sistem keselamatan internet termasuk 'firewall' dan sistem keselamatan yang lain, yang mana kebiasaannya ia gagal untuk menapis serangan yang tidak dikehendaki kepada sistem dan menyebabkan sistem terganggu dan gagal beroperasi. Masalah utama dalam membangunkan kaedah bagi sistem ini ialah perkembangan dalam topologi internet dan juga pengguna internet yang mana permodelan rangkaian ini lebih sukar untuk serangan data bebas. Ujian sebenar yang dilaksanakan ia menyatakan bahawa masalah ini berpunca kerana banyak serangan-serangan palsu dilakukan ke atas sistem ini dan ia tidak berupaya untuk menapis semua serangan tersebut. Projek ini bertujuan menganalisis rangkaian dalam simulator dengan serangan data bebas yang mana melibatkan trafik 'self-similar' yang menunjukkan permodelan trafik internet dan sebaik-baiknya permodelan trafik 'Poisson' digunakan bagi luar jangka waktu puncak. Dengan templet serangan data bebas, sistem akan mengurangkan kesulitan dalam mengesan serangan semasa waktu puncak dan luar waktu puncak. Sistem rangkaian ini disimulasikan dalam perisian 'NS-2 Simulator'.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACK	-	acknowledgement
AF	-	Assured Forwarding
ATM	-	Asynchronous Transfer Mode
BE	-	Best-effort
CBR	-	Constant Bit Rate
CBS	-	Committed Burst Size
CIR	-	Committed Information Rate
CPU	-	central processing unit
DiffServ	-	Differentiated Services
DES	-	Discrete Event Simulation
DNS	-	Domain Name Server
DoS	-	Denial of Service
DSCP	-	Differentiated Service Code Point
EF	-	Expedited Forwarding
HIDS	-	host-based intrusion detection system
IDS	-	Intrusion Detection System
IntServ	-	Integrated Service
IP	-	Internet protocol
ISP	-	Internet service provider
FARIMA	-	(fractional) autoregressive integrated moving average
FTP	-	File transfer protocol
GUI	-	graphical user interface
HTTP	-	Hypertext transfer protocol
LAN	-	Local Area Network
MPEG4	-	
NIDES/STAT	-	statistical anomaly detection engine/algorithm

NIDS	-	network-based intrusion detection system
NNTP	-	network news transfer protocol
NS-2	-	Network Simulator, version 2
PDF	-	probability distribution function
PHB	-	Per Hop Behavior
QoS	-	Quality of Service
RED	-	Random Early Dropping
RFC	-	Request For Comment
RNG	-	random number generators
RTT	-	round-trip times
RULE	-	Rule-based detection engine
SLA	-	Service Level Agreement
SMTP	-	simple mail transfer protocol
TBF	-	Token Bucket Filter
TCA	-	Traffic Conditioning Agreement
TCP	-	transmission control protocol
UDP	-	user datagram protocol
URL	-	uniform resource location
VLL	-	Virtual Leased Line
VoIP	-	Voice over Internet protocol
WAN	-	Wide Area Network
WRR	-	Weighted Round Robin
WWW	-	World Wide Web

LIST OF SYMBOLS

Gbps	-	Giga bits per second
KB	-	Kilobyte
Kbps	-	Kilobit per second
Mbps	-	Megabit per second

CHAPTER 1

INTRODUCTION

1.1 Overview

In the context of physical security, intrusion detection systems mean tools used to detect activity on the boundaries of a protected facility. When we commit to physically protecting the premises on which our staff work and which house our information processing equipment, we should carry out an exhaustive risk analysis and, where the threat requires, consider installing a perimeter intrusion detection system (IDS).

The simplest IDS are a guard patrol. Guards who walk on the corridors and perimeter of a facility are very effective at identifying attempts of break-in on the premises. If anything goes wrong, they will either raise the alarm or attempt to challenge the intruder. Of course, the most obvious shortcoming of a guard patrol is that the patrol cannot be at all points of the facility at the same time.

This leads to the next simplest IDS and that is video monitoring. Video camera can be place at locations in the facility where all points in the perimeter can be monitored simultaneously. If there is an intrusion attempt it will be detected and the alarm will be raise by the person in charged with monitoring the video an alarm.

IDS are designed to function like a burglar alarm on your house where these systems should record suspicious activity against the target system or network, and should alert the information security manager or support staff when an electronic

break-in is underway. The biggest downfall with IDS products is the necessary level of customization ‘of the box’. Without significant amounts of customization, the IDS will produce a large number of false-positive alerts. A false positive is created when the IDS alerts the support staff to an event that will not have an impact on the target system. For example, a Code Red attack against and Apache Web server will not work, but the IDS may still sound the alarm.

1.2 Problem Statement

The major problems in developing the IDS method is the evolving growth of the internet topology and the growth of the internets users which makes the modelling of the network with attack free data is difficult. Real world test has shown overwhelming numbers of false alarms of attack and little success in filtering them out.

1.3 Objective

Objective of this thesis are:

(a) To analysis the network with data free attacks in that involved the complex Internet Traffic as well as data traffic for the peak hours and non peak hours periods for the peak packet and average packet received.

(b) To analysis the network with attacks in that involved the complex Internet Traffic as well as data traffic for the peak hours and non peak hours periods for the peak packet and average packet received.

1.4 Scopes of Work

The scopes of this project consist of:

(a) Discussion about the concept and application of intrusion detection system (IDS).

(b) Study on self-similar traffic which represent the Internet traffic source and Poisson traffic modelling which represent voice traffic in the analysis.

(c) Simulate the attacks during peak hours and non peak hours in Network Simulator, version 2 (NS-2) simulator.

(d) Analyses the result to determine the performance of Internet network and propose the proactive action to solve the weakness that going happened.

1.5 Thesis Organization

This thesis has the following structure. Chapter 2 give some literature review background information. Chapter 3 discusses the methodology simulation and analysis that to be used. Then, Chapter 4 explains the simulation and analysis. Finally, Chapter 5 concludes the thesis and gives possible directions for future research.