NETWORK ANALYSIS AND THREATS DETECTION SYSTEM

MUHAMMAD ‘AMMAR BIN AZMAN

NETWORK ANALYSIS AND THREATS DETECTION SYSTEM

MUHAMMAD ‘AMMAR BIN AZMAN

This report is submitted in partial fulfilment of the requirements for the Bachelor of Computer Science (Computer Networking) With Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2017

DECLARATION

I hereby declare that this project report entitled

NETWORK ANALYSIS AND THREATS

DETECTION SYSTEM

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

STUDENT : _____ Date: _____

(MUHAMMAD ‘AMMAR BIN AZMAN)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Networking) With Honours.

SUPERVISOR : _____ Date: _____

(MR. MUHAMAD SYAHRUL AZHAR BIN SANI)

DEDICATION

To my beloved parents who inspired me,
for their prayers and
all of the support they have given and
always standing beside me.

To my supervisor
for encouraging, motivating and
believing in me

ACKNOWLEDGEMENTS

First of all, I would like to be grateful to Allah S.W.T by reason of giving me chance to finish my final year project in fixed period and giving me a good health. Without His power, I was unable to finish my final year project in expected time.

I would like to express my deepest appreciation to all those who provided me the possibility to complete this final year project. A special gratitude I give to my project supervisor, Mr. Muhamad Syahrul Azhar Sani, for the guidance, encouragement and helped me to coordinate my project especially in writing this report. Without his guide, this project cannot be done properly like this.

Furthermore, I would like to show my appreciation to my parents for giving me moral support and my friends also went through the final year project and helped me whenever I needed them and enriched my work with their valuable suggestions.

ABSTRACT

Network Analysis and Threats Detection System is a computer system that can be uses to analyse the network traffic and also to detect the threats which can affect the network performance. Generally, it using visual basic and all configuration by using the software VB.Net language. Nowadays, the attackers are growing smarter and their techniques more creative with many way to attack the computer. This system is use to analyse and detect the threats, this is effective way of improving an organization's network security. The organization can take early action to prevent or to denying the attacker to access to their network. The methodology chosen is Prototyping Model. The Prototyping Model is which a prototype is produce, tested, and then modify until an acceptable prototype is finally achieved from which the complete system can be developed. For the significant contribution, this project being conducted was to analyse the traffic and performance in the network based on port and protocol that always uses. At the end of the project, admin will know the condition of the network performance and relationship between the threats. So that admin can take action to improve the network to prevent the threats.

ABSTRAK

Analisis rangkaian dan Pengesan Ancaman adalah satu sistem komputer yang boleh digunakan untuk menganalisis trafik rangkaian dan juga untuk mengesan ancaman yang boleh menjejaskan prestasi rangkaian. Secara umumnya, sistem ini menggunakan Visual Basic dan semua perisian dalam bahasa VB.Net. Pada masa kini, serangan dan teknik yang semakin meningkat lebih bijak dan teknik mereka lebih kreatif dengan banyak cara untuk menyerang komputer. Sistem ini digunakan untuk menganalisis dan mengesan ancaman ini adalah cara yang berkesan untuk meningkatkan keselamatan rangkaian dalam organisasi. Organisasi boleh mengambil tindakan awal untuk mencegah atau menafikan penyerang itu untuk mengakses kepada rangkaian mereka. Metodologi dipilih adalah Prototyping Model. Prototyping Model adalah prototaip yang menghasilkan, diuji, dan kemudian mengubah suai sehingga prototaip diterima dan dicapai dengan sistem lengkap yang boleh dibangunkan. Sumbangan projek ini adalah untuk menganalisis trafik dan prestasi dalam rangkaian berdasarkan port dan protokol yang sering di gunakan untuk menyerang. Pada akhir projek, pentadbir akan tahu keadaan prestasi rangkaian dan hubungan antara ancaman. Jadi pentadbir yang boleh mengambil tindakan awal untuk meningkatkan keselamatan rangkaian untuk mencegah daripada ancaman.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Introduction

Human nowadays is always keeping the usage of internet to the maximum all the time. While the usage of internet and network is keep expanding and demanding from time to time but the resources to keep it stabilize and fulfilling the demand is running low.

Network Analysis and Threat Detection System is a computer system that can be uses to analyses the network traffic and also to detect the threats which can affect the network performance. A Network Analysis and Threat Detection System or known as NATD comprises of a PC, information or a system site that appears of being a part of a system that is really isolated and monitored, and which appears to contain information or a resource of value to threats.

Network Analysis and Threat Detection System are collect data only when someone interacting with them. Besides that, NATD require minimal resources, even on a big system. This system get their value from threats using them. If the hacker or vulnerable does not collaborate or use the NATD, then it has little value.

Low-Interaction has limited interaction. It works by imitating working frameworks and administrations running on them. The fundamental focal points are that it is extremely basic, simple to set up and manage. It postures insignificant dangers as there are no genuine Operating Systems (OS). Besides, it logs only limited information and designed to capture previously known attacks. Examples: Specter and KFSensor.

Medium-Interaction is more sophisticated than low-interaction one but it is still emulating a complete OS. It emulated more complicated services. The advantages are low risk of penetration and better interaction performance (Girdhar & Kaur, 2012). The disadvantages are capture only activity that directly interact with them and do not emulate a complete real OS. Examples: Honeypot and MWCollect.

High-Interaction involves real OS and applications. The main advantage of using this system is that data obtained about the attack is in awesome detail as it captures all the activities. This helps us to capture the observation about the attack behaviours that we will never predict. Examples of the high-interaction are Symantec Decoy Server and Honeynets.

In 2013, vandalism had increased hugely especially in the private district. They are hosted by third party website provider that did not provide any security control measure. Their daily activity had been disrupted by DDoS (Distributed Denial of Service) that occur in the local ISP and also compassionated some of the clients. The statistics attack (Mycert.org.my, 2017) reported incidents is shown as in Figure 1.1.

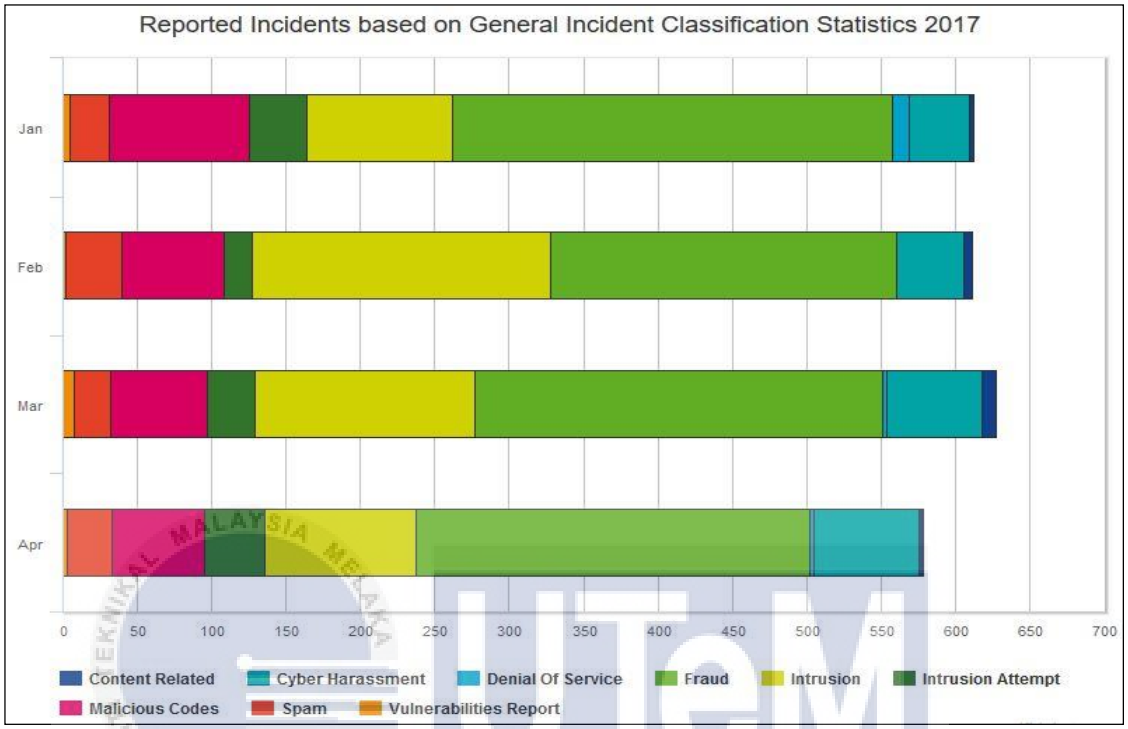

Figure 1.1: Reported Incidents Statistics 2017

Therefore, based on the statistics from MyCERT in 2017 in Figure 1.1 in March, the total incidents had been increased and the reported the highest attack occurs in March. Many of the people in this world are growing more intelligent. For this reason, the security control needs to be more effective to detect and defence the network. Much software is provided to detect and defence the network from the attack. The administration needs to understand the operation of the software so that they can understand the attack detected and able to make a decision to protect the network.

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	5	9	2									18
Cyber Harassment	41	45	64	71									221
Denial of Service	11	0	3	3									17
Fraud	296	233	274	265									1068
Intrusion	98	201	148	101									548
Intrusion Attempt	39	19	32	41									131
Malicious Codes	94	68	65	62									289
Spam	26	38	24	30									118
Vulnerabilities Report	5	2	8	3									18
	612	611	627	578									2428

Figure 1.2: Reported Incidents Statistics 2017

Figure above shows the current statistics of reported incidents of attack in 2017. At first four months, the fraud attack was the highest incidents occurred in 2017. The second highest attack in 2017 is intrusion in network. For this reason, we must prevent the attack from increase month by month. The administrator understanding when using detection or prevention software is important so that the administrator will be able to alert when the threats or attacks try to encounter the network. This statistics table and graph from the trusted Malaysia Cybersecurity website (https://www.mycert.org.my/assets/graph/pdf/2017-1.pdf). Network Analysis and Threats Detection System is software that detects a lot of different types of intrusions. In this project, Network Analysis and Threats Detection System will be used to overcome the problem.

1.2 Problem Statement

Nowadays, many way or technic uses by attacker to attack the network. It will affect the machine performance and make the network down. Besides that, false alarm always happens in many threats detection systems. False alarm regularly occurs when an attack is detected but actually there is no attack. So, some of the administrator faced some problem with the issues. The problem with this issue is in tables below.

Table 1.1: Problem Statement 1

PS	Problem Statement
PS1	Attackers nowadays more creative to attack the computer or server to affect the network performance.

PS1: Attackers nowadays more creative to attack the computer or server to affect the network performance

Network Analysis and Threats Detection System will create and detect the way to prevent the attackers from attacks the computer. But administrator need to take the action that the administration needs to decide.

Table 1.2: Problem Statement 2

PS	Problem Statement
PS2	Administrator has difficulty to know the way attacker attacks the network.

PS1: Administrator has difficulty to know the way attacker attacks the network

Network Analysis and Threats Detection System will create and analysing the attacker techniques to gain the network by port and protocol. This way administrator will know which port the attackers uses.

Table 1.3: Problem Statement 3

PS	Problem Statement
PS3	Network always slow and down because of suspicious activity inside the network.

PS1: Network always slow and down because of suspicious activity inside the network

Network Analysis and Threats Detection System will create the best way to detect the most traffic use inside the network. The highest traffic uses consider are suspicious activity. Administrator need to take the manual action to block the suspicious activity to prevent the network.

1.3 Project Question

Project question (PQ) are constructed and shown as below. It was to identify the problem statement that being discussed in Table 1.4.

Table 1.4: Summary of Project Question

PS	PQ	Project Question
PS1	PQ1	Attackers attack the computer or server to affect the network performance?
PS2	PQ2	How administrator identifying which protocols attacker uses to attacks the network?
PS3	PQ3	What are the ways administrator need to maintain the performance of the network inside the organization?

PQ1: Attackers attack the computer or server to affect the network performance?

This project question is to investigate the network attack that NATD can analyze and the behavior of the attack and relationship between the network performance.

PQ2: Administrator has difficulties to identifying which protocols attacker uses to attacks the network?

This project question is to analyse the port and protocols that attackers uses to attack the network that ca be use to Network Analysis and Threats Detection System (NATD).

PQ3: Administrator has difficulties to identifying how attacker flooding their network?

This project question is to analyse port ICMP, TCP and UDP which the attackers always use to attack the network.

1.4 Project Objective

This project objectives (PO) are developed based on the previous section which is the project question (PQ) The Project Objective (PO) is shown in Table 1.5.

Table 1.5: Project Objectives

PS	PQ	PO	Project Objectives
PS1	PQ1	PO1	To investigate about the attacks and the performance of the network that user connected
PS2	PQ2	PO2	To analyse the packet inside the network by identifying port and protocol uses.
PS3	PQ3	PO3	To identify the threats in the network based on protocols especially ICMP, TCP and UDP that effect the network performance.

PO1: To investigate about the attacks and the performance of the network that user connected.

In order to create the detection system, we must first understand about the network attacks and the behavior of attacks and the network performance.

PO2: To analyse the packet inside the network by identifying port and protocol uses.

After understand the attack and the way to detect, the next step is to analyse the network by identifying the port and protocol. The analyses also including what are inside the packet that user communication from source and destination.

PO3: To identify the threats in the network based on protocols especially ICMP, TCP and UDP.

After analyse the packet form ports and protocols, next step is to analyse the threats that attacks the network based on the most popular protocols that attackers uses. There are ICMP, TCP and UDP.

1.5 Project Scopes

The scopes of this project are:

1. This project will be focus on for administration uses.
2. This project focus on the port and protocol which attackers always uses.
3. The Network Analysis and Threats Detection System is used in Windows OS (Operating System)
4. All communications with the system are considered malware or threats, as there's no reason for legitimate users to access the computer.

1.6 Project Contribution

Project contribution are shown as below in Table 1.6

Table 1.6: Project Contribution

PS	PQ	PO	PC	Project Contribution
PS1	PQ1	PO1	PC1	Attackers and network performance
PS2	PQ2	PO2	PC2	Analysis the packet by port and protocol
PS3	PQ3	PO3	PC3	Threats analysis based on ICMP,TCP,UDP

PC1 : Attack and network performance

After study about the attack and network performance, it will be easy to know how network performance if there some attackers inside the network.

PC2: Analysis the packet by port and protocol

After that, NATD will provide an analyses for administrator about the packet inside the network traffic.

PC3: Provide an accurate tools to identify the attack

After the analyses the packet, this system will find the way to analyses the threats based on the most popular protocols that attackers uses. It will provide an accurate tools to administrator to identify the attack.

1.7 Thesis Organization

This report consists of seven chapters which is Chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Design, Chapter 5: Implementation, Chapter 6: Testing and lastly Chapter 7: Project Conclusion.

Chapter I: Introduction

This chapter will explain and summarize about the problem statement, project question, project objective, project scope, project contribution and thesis organization.

Chapter II: Literature Review

This chapter will explain and summarize about the related work of the previous work about the types of attack and Threats Detection System. It also will explain about the proposed solution or further project that will be done.

Chapter III: Methodology

This chapter will explain and summarize about the project methodology. It will explain briefly every phase that available on the methodology. This chapter will also include project schedule and milestone.

Chapter IV: Design