

**TESTING AND ANALYZE TYPE OF SCANNING TOOLS BASED ON  
THRESHOLD AT ANOMALY DETECTION**

NURUL AFIQAH BINTI IBRAHIM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## BORANG PENGESAHAN STATUS TESIS\*

JUDUL: TESTING AND ANALYZE TYPE OF SCANNING TOOLS BASED ON THRESHOLD AT ANOMALY DETECTION

SESI PENGAJIAN: 2010/2011

Saya NURUL AFIQAH BINTI IBRAHIM

mengaku membenarkan tesis PSM ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek 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 termaktub di dalam AKTA RAHSIA RASMI 1972)

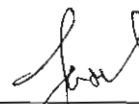
\_\_\_\_\_ TERHAD

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

/ \_\_\_\_\_ TIDAK TERHAD



(TANDATANGAN PENULIS)



(TANDATANGAN PENYELIA)

KM 4434 Jln Samarinda 6,  
Taman Samarinda,  
78000 Alor Gajah  
Melaka

DR. MOHD FAIZAL BIN ABDOLLAH

Tarikh: 7/7/2011

Tarikh: 7/7/2011

CATATAN: \* Tesis ini dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)

\*\*Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

TESTING AND ANALYZE TYPE OF SCANNING TOOLS BASED ON  
THRESHOLD AT ANOMALY DETECTION

NURUL AFIQAH BINTI IBRAHIM

This report is submitted in partial fulfillment of the requirements for the  
Bachelor of Computer Science (Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
UNIVERSITI TEKNIKAL MALAYSIA MELAKA  
2011

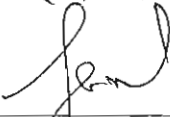
## DECLARATION

I hereby declare that this project report entitled  
**TESTING AND ANALYZE TYPE OF SCANNING TOOLS BASED ON  
THRESHOLD AT ANOMALY DETECTION**

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

STUDENT :   
(NURUL AFIQAH BINTI IBRAHIM)

DATE: 7/7/2011

SUPERVISOR:   
(DR. MOHD FAIZAL BIN ABDOLLAH)

DATE: 7/7/2011

## DEDICATION

To my beloved parent, thank you for giving me opportunity to further my study until  
finish

Thank you to my supervisor for helping me also guide me from the beginning until  
the end of this project

Thank you to all my lecture for teach me and you all are the great teacher

Thank to all my friend and being my good friend

## ACKNOWLEDGEMENTS

I would like to thank Dr. Mohd Faizal Bin Abdollah for giving assistant to complete this project successfully.

I would also like to thank my beloved parents who have been giving me support and motivation throughout my project.

Thank you also to my entire friend, have fun together.

Last but list my UTeM Taekwondo family (UTeM Tae Kwon Do Chill!!!) especially my Instructor Sir Michael Bong always gives full support, motivation and advice in what I doing. Love you all.

## ABSTRACT

This project focuses on testing and analyzes threshold with 15 type of scanning tool. Anomaly – based intrusion detection cooperates with snort threshold. There are two primary methods of detection used by IDS's, signature and anomaly. This project only focuses on Anomaly detection. Beside that Snort is a famous intrusion detection system in field of open source software analyze by Basic Analysis and Security Engine (BASE). This test is the way to prevent and care the networks, by using scanning tool to detect what port is open or close. Then change the threshold to test any changes or find specific threshold that valid for specific attack because right now everything is at fingertips, easy and all source already have then helped of any kind of software to make more easier for hacker or somebody try to come into network because, scanning port is first way to attack and make strategy.

## ABSTRAK

Projek ini memberi tumpuan kepada ujian dan analisis threshold dengan menggunakan 15 jenis alat pengimbas. Anomaly- pengesanan pencerobohan bekerjasama dengan Snort. Terdapat dua jenis utama signature dan anomaly. Projek ini hanya memberi tumpuan kepada kepada pengesanan anomaly. Selain itu Snort terkenal sebagai sistem pengesanan pencerobohan dalam bidang perisian sumber terbuka dianalisis oleh Analisis Asas dan Keselamatan Engine. Ujian ini adalah cara untuk mengesan bahagian yang terbuka atau tertutup. Kemudian menukar threshold untuk menguji apa – apa perubahan atau mencari threshold tertentu yang sesuai untuk serangan yang khusus kerana semuanya di hujung jari, mudah bagi dan semua sumber kemudian dibantu dengan jenis perisian untuk memudahkan kerja bg seorang penggodam atau seseorang yang cuba memasuki sesebuah rangkaian kerana imbasan adalah langkah pertama bagi permulaan strategi.



## TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	i
	DEDICATION	ii
	ACKNOWLEDGEMENTS	iii
	ABSTRACT	iv
	ABSTRAK	v
	TABLE OF CONTENTS	vi
	LIST OF TABLES	ix
	LIST OF FIGURES	x
	LIST OF APPENDIX	xii
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	
	1.1 Project Background	1
	1.2 Problem Statements	2
	1.3 Objective	2
	1.4 Scope	3
	1.5 Project Significant	3
	1.6 Expected Output	3
	1.7 Conclusion	4
<b>CHAPTER II</b>	<b>LITERATURE REVIEW AND PROJECT METHODOLOGY</b>	
	2.1 Introduction	5
	2.2 Literature Review	6
	2.2.1 Domain	6

	2.2.2	Keyword	6
	2.2.3	Previous Research	8
	2.3	Proposed solution	9
	2.3.1	Project Methodology	9
	2.4	Project Schedule	11
	2.5	Conclusion	12
<b>CHAPTER III</b>		<b>REQUIREMENT ANALYSIS</b>	
	3.1	Introduction	13
	3.2	Problem analysis	14
	3.2.1	Network Architecture	14
	3.2.2	Logical and Physical Design	14
	3.2.2.1	Physical Design	15
	3.2.2.2	Logical Design	15
	3.3	Requirement analysis	16
	3.3.1	Quality of Data	16
	3.4	Conclusion	17
<b>CHAPTER IV</b>		<b>DESIGN</b>	
	4.1	Introduction	18
	4.2	Project Overview	19
	4.2.1	Experiment Process	20
	4.2.2	Default Threshold	
		Experiment	21
	4.2.3	Modify Threshold	
		Experiment	22
	4.3	Security Requirement	23
	4.4	Conclusion	23
<b>CHAPTER V</b>		<b>IMPLEMENTATION</b>	
	5.1	Introduction	24
	5.2	Network Configuration Management	25
	5.2.1	Configuration Environment	
		Setup	25

	5.2.2	Version Control Procedure	31
5.3		Hardware Configuration Management	32
	5.3.1	Hardware Setup	32
5.4		Development Status	34
	5.4.1	Scanning Attack	34
5.5		Conclusion	50
<b>CHAPTER VI</b>		<b>TESTING</b>	
6.1		Introduction	51
6.2		Test Plan	51
	6.2.1	Test Schedule	51
6.3		Test Design	52
6.4		Test Result and Analysis	52
6.5		Conclusion	60
<b>CHAPTER VII</b>		<b>CONCLUSION</b>	
7.1		Observation on Weaknesses and Strengths	61
7.2		Proposition for Improvement	63
7.3		Contribution	64
7.4		Conclusion	64

**LIST OF TABLES**

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	Project Milestone of PSM I	11
5.1	Device Configuration Detail	26
5.2	Version Control Procedure	31
5.3	Hardware Setup	32
6.1	Threshold 10 second	52
6.2	Threshold 20 second	53
6.3	Threshold 30 second	54
6.4	Threshold 40 second	55
6.5	Threshold 50 second	56
6.6	Threshold 60 second	57
6.7	Summarization Alert of Scanning Tool Based Threshold Setting	58
6.8	First Total Alert in One Second	59

## LIST OF FIGURES

DIAGRAM	TITLE	PAGE
2.1	Waterfall Model	9
3.1	Physical Network Design	15
3.2	Logical Network Design	15
4.1	Project Overview	19
4.2	Experiment Process	20
4.3	Default Threshold Experiment	21
4.4	Modify Threshold Experiment	22
5.1	Testing and analyze scenario	25
5.2	Advanced Port Scanner 1.3 Interface	35
5.3	Alert for Advanced Port Scanner 1.3	35
5.4	BurnSoft Portscan Interface	36
5.5	Alert for BurnSoft Portscan	36
5.6	FreePortScanner 2.7 Interface	37
5.7	Alert for FreePortScanner 2.7	37
5.8	IP PIG Port Scanner 1.0 Interface	38
5.9	Alert for IP PIG Port Scanner 1.0	38
5.10	NetworkActiv Port Scanner 4.0 Interface	39
5.11	Alert for NetworkActiv Port Scanner 4.0	39
5.12	NetBrute Interface	40
5.13	Alert for NetBrute	40
5.14	Network Scanner Interface	41
5.15	Alert for Network Scanner	41
5.16	Nmap (Network Mapper) Interface	42

5.17	Alert for Nmap (Network Mapper)	42
5.18	Network Studio Remote Port Scanner1.32 Interface	43
5.19	Alert for Network Studio Remote Port Scanner1.32	43
5.20	Ping Scanner Pro Interface	44
5.21	Alert for Ping Scanner Pro	44
5.22	P-Ping Tool 2.6 Interface	45
5.23	Alert for P-Ping Tool 2.6	45
5.24	Reconport Scanner Interface	46
5.25	Alert for Reconport Scanner	46
5.26	Shark Network Tool Professional 2.20 Interface	47
5.27	Alert for Shark Network Tool Professional 2.20	47
5.28	Superscan 4.0 Interface	48
5.29	Alert for Superscan 4.0	48
5.30	Very Simple Network Scanner Interface	49
5.31	Alert for Very Simple Network Scanner	49

**LIST OF APPENDIX**

<b>APPENDIX</b>	<b>TITLE</b>	<b>PAGE</b>
<b>A</b>	<b>Domain Name Server (DNS)</b>	<b>68</b>
<b>B</b>	<b>Web Server (ISS7)</b>	<b>70</b>
<b>C</b>	<b>Mail Sever (hMailServer)</b>	<b>72</b>
<b>D</b>	<b>Snort Installation and Configuration</b>	<b>74</b>
<b>E</b>	<b>AcidBase Installation and Configuration</b>	<b>77</b>
<b>F</b>	<b>Snort.conf</b>	<b>81</b>
<b>G</b>	<b>Threshold.conf</b>	<b>101</b>
<b>H</b>	<b>Port mirroring @ SPAN configuration</b>	<b>104</b>
<b>I</b>	<b>Gantt Chart</b>	<b>107</b>

## CHAPTER I

### INTRODUCTION

#### 1.1 Project Background

These projects focus more on testing and analyzes threshold with scanning tool. Network traffic has “Attacker”, “Victim” host and also use SNORT as detector. The “Attacker” is 15 type of scanning tool for get better result. This project only focuses on anomaly detection. Anomaly-based intrusion detection cooperates with snort threshold. Furthermore it can analyze and find suitable threshold setting for every scanning tool. Alerts are any sort of user notification of an intruder activity. When IDS detect an intruder, it has to inform security administrator by alerts. Alerts may be in the form of pop-up windows, logging to a console, sending e-mail and so on. Alerts are also stored in log files or databases where admin can be viewed later on by security experts’ example for this project use Basic Analysis and Security Engine (BASE). This test will know type or performance of “attacker” either faster or slow attacker.

There are two primary methods of detection used by IDS’s, signature and anomaly. This project focuses on Anomaly detection. Anomaly detection module is constructed by using frequent episode rule. Snort is a famous intrusion detection system in the field of open source software. Snort is a lightweight network intrusion detection system, which is written with C language. Besides the Snort is simple, short and has good programming style. Testing Intrusion Detection Systems (IDS) to ensure the most malicious attacks are detected is a cornerstone of these systems, but there is no standardized method to execute these tests. Running live exploitations is not always a viable option especially



when the rule set isn't finalized, and clients are often nervous about the use of "hacker tools" on these networks. Solid understanding very important for the default behavior and how it may be insufficient in performing host discovery and search out security holes and scan for open network services.

## 1.2 Problem Statements

Intrusion detection systems fall into two basic categories: signature-based intrusion detection systems and anomaly detection systems. Intruders have signatures, like computer viruses, that can be detected using scanning tool. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity. Anomaly-based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers. So, this project use Anomaly-based intrusion detection cooperates with snort threshold.

## 1.3 Objective

- To study threshold technique used by anomaly detection in snort
- To identify a threshold as wrote rules for specific attack
- To test and validation of the threshold in term of accuracy and time

## 1.4 Scope

It just for proof-of-concept with testing and analyze. Testing and analyze type of scanning tools based on threshold at anomaly detection and only do this test in Local Area Network environment.

## 1.5 Project Significant

This project is the way to prevent and care the networks, by using scanning tool to detect what port is open or close. Moreover study threshold technique used by anomaly detection in snort. Then change the snort threshold to test any changes or find specific threshold that valid for specific attack.

## 1.6 Expected Output

This project proved from the fact that knows Nmap is the best security scanner from another type of security scanner that test for network. Then clarify the suitable category of each scanning tool base on time at snort threshold. Beside that the output will get more information about scanning type, duration time detection, category attacker and total host discovery that only focus only anomaly detection.

## 1.7 Conclusion

This chapter gives full understanding about the project, that very important for this project as a guide for what that want to achieve. Besides that, to know what to do and beware not out of topic. Next in Chapter 2 focus more on literature review and project methodology where more information details phase by phase. On that time decide the project schedule and produce of project time line or Gantt chart.

## CHAPTER II

### LITERATURE REVIEW AND PROJECT METHODOLOGY

#### 2.1 Introduction

Developing any new project, the initial step should take is doing researches and study so that he or she can identify information, ideas and methods that relevant to his or her project. This theoretical base for research, one thing can determine the true of his or her project. Develop a new project, the researchers are very important because all the information from the research about the project is used as a guideline to develop a new project and execute it successfully. This chapter discusses and studies on Literature Review and Methodology about the project, the research will be done by reference to books, articles, online journals about the existing systems that are available in market nowadays. Literature review will take part in the discussion on researches that already done before by others debates based on the selected area of study. Besides that, including the searching, collecting, identifying, analyzing and drawing conclusion through several kinds of researches. All these things are mainly gather from journals, articles, books, web pages and technical reports. Meanwhile, project methodology will discuss on the steps involve to undergo the experiment. All the approach that have been used in previous researches is justify and describe on how it will being applied in this project.

## 2.2 Literature Review

### 2.2.1 Domain

The domain is based on rules Computer and Network Security and that means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. This analyze it already categorize only for BITC student and it criteria is network infrastructure, design and network security.

### 2.2.2 Keyword

- **IDS**

An intrusion detection system (IDS) is software that automates the intrusion detection process and monitors network traffic also monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. The software that use is Snort.

- **Anomaly Detection**

The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. This project use anomaly-based detection to represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time. Mirashe et al. (2010), give example, a profile for a network might show that Web activity comprises an average of 13% of network bandwidth at the Internet border during typical workday hours. Then use statistical methods to compare the characteristics of current activity to thresholds

related to the profile, such as detecting when Web activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly. Profiles can be developed for many behavioral attributes, such as the number of e-mails sent by a user, the number of failed login attempts for a host, and the level of processor usage for a host in a given period of time.

- **Scanning Tool**

These tools allow attacks to survey and analyze system characteristics. These tools can determine the OS used by network devices, and then identify vulnerabilities and potential network ports to use for an attack. Some tools can also perform slowly timed surveys of a target system in order to not trigger an IDS.

- **Thresholding**

Event thresholding can be used to reduce the number of logged alerts for noisy rules. There are 3 types of thresholding: (SNORT User Manual, 2009).

- **LIMIT**

Alerts on the 1st m events during the time interval, and then ignores events for the rest of the time interval.

- **THRESHOLD**

Alerts every m times we see this event during the time interval.

- **BOTH**

Alerts once per time interval, after seeing m occurrences of the event, and then ignores any additional events during the time interval.

### 2.2.3 Previous Research

#### i. Techniques

- **Anomaly detection using Snort**

Anomaly detection is a critical issue in Network Intrusion Detection Systems (NIDSs). Anomaly detection identifies attacks based on the deviations from the established profiles of normal activities. Activities that exceed thresholds of the deviations are detected as attacks. Misuse detection has low false positive rate, but cannot detect new types of attacks. Anomaly detection can detect unknown attacks, under a basic assumption that attacks deviate from normal behavior. Currently, many NIDSs such as Snort (Snort Home Page, 2010) are rule-based systems, which employ misuse detection techniques. (Jiong, Z et al, 2006).

- **Technique for selecting static threshold value from a minimum standard features in detecting fast attack**

Threshold Verification Technique for Network Intrusion Detection System, (Faizal M et al., 2009) focusing on detecting fast attack based on the connection made by attacker on a single victim. Mc Hugh also provide further evidence by stating that anyone can attack Internet site using readily made available intrusion tools and exploit script that capitalize on widely known vulnerabilities. (McHugh J et al., 2000). Hence, the increasing number of the exploit tools may have influence on the number of novice attackers on the internet (McHugh J, 2001). An attack can be divided into five phases which are reconnaissance, scanning, and gaining access, maintaining access and covering tracks. The first two phases is an initial stage of an attack and it does involve scanning and probing network traffic for information on the vulnerabilities of the targeted machine. This initial stage of attack can be categorized into two which are fast attack and slow attack; (Lazarevic A et al., 2003) defined fast attack as an attack that uses a large amount of packet or connection within a few second. Meanwhile a slow attack is defined as an

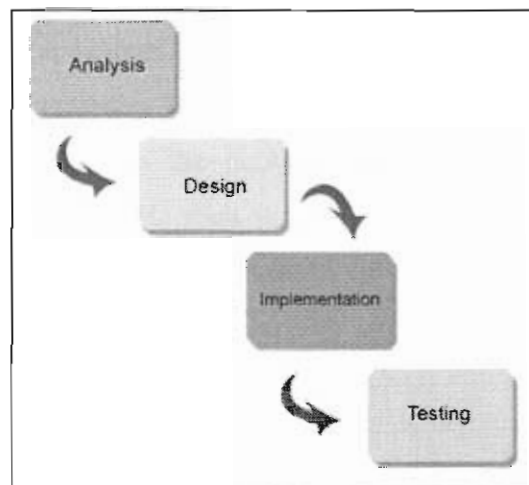
attack that takes a few minutes or a few hours to complete. (Wenke Lee, 1999).

## ii. Experimental Tools

This research is to specify fast attack and slow attack of 15 type of scanning tool base on it threshold setting.

## 2.3 Proposed solution

### 2.3.1 Project Methodology



**Figure 2.1: Waterfall Model**

The project goes through several phases for developing this project which are analysis, design, implementation, and testing.

- **Analysis Phase**

The project can start after the title is already approved and can proceed to the next step to study the previous research and acts as guidance and reference on how to construct the project. Very important to know project topology in order to avoid the project is out of track and follow the objective.