

## BORANG PENGESAHAN STATUS TESIS

JUDUL: ANALYSIS OF VOIP ATTACKS

SESI PENGAJIAN: 2011/2012

Saya, GAN HOCK SENG

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:  
Lot 1356 Jalan Besar Guchil 4,  
18020 Kuala Krai,  
Kelantan.

Tarikh : 28-8-2012

\_\_\_\_\_  
(TANDATANGAN PENYELIA)  
ENCIK ERMAN HAMID

Tarikh : \_\_\_\_\_

**ANALYSIS OF VOIP ATTACKS**

**GAN HOCK SENG**

**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  
2012**

## DECLARATION

I hereby declare this project report entitled  
Analysis of VoIP Attacks

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

STUDENT

:  Date: 28-8-2012  
(GAN HOCK SENG)

SUPERVISOR

: \_\_\_\_\_ Date: \_\_\_\_\_  
(ENCIK ERMAN HAMID)

## DEDICATION

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

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

## ACKNOWLEDGEMENTS

Thanks to all beings that support me to finish this research, whom with His willing give me the opportunity to complete this Final Year Project which is title Analysis type of VoIP attacking. This final year project report was prepared for Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), basically for student in final year to complete the undergraduate program that leads to the degree of Bachelor of Computer Science. This report is based on the methods given by the university.

Firstly, I would like to express my deepest thanks to, Encik Erman Hamid, a lecturer at FTMK, UTeM and also assign, as my supervisor who had guided be a lot of task during my project research. I also want to thanks the lecturers and technicians of FTMK for their cooperation during I complete the final year project that had given valuable information, suggestions and guidance in the compilation and preparation this final year project report.

Deepest thanks and appreciation to my parents, family, special mate of mine, and others for their cooperation, encouragement, constructive suggestion and full of support for the report completion, from the beginning till the end. Also 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 until it is fully completed.

## ABSTRACT

VoIP security tools such as protocol analyzers, vulnerability assessment utilities and security monitoring utilities are among the common tools in a security professional's arsenal. Such tools have reached a high level of dependence among security professionals for evaluating potential vulnerabilities in such areas as operating systems, device configuration, networking protocols and applications. However, these tools have their limitations, such as where they are applied, how they are implemented and how they are maintained and updated. Furthermore, while such tools are fairly robust for more mature technology, it remains difficult to develop comprehensive security tools for emerging technology. Voice over Internet Protocol is an example of such an emerging technology. This paper explores the known VoIP-related vulnerabilities and tests several of the more popular open source and commercial VoIP security tools with the intention of demonstrating the gap that exists between vulnerability and test the best IDS for VoIP system. Understanding this gap will help to identify what issues need to be addressed in the future development of VoIP system security.

## ABSTRAK

Keselamatan VoIP adalah penting dalam mengelakan belaku pencorohohan dan kerosakan pada sistem. Alat-alat seperti penganalisa protokol VoIP, kelemahan taksiran utiliti dalam memantau keselamatan adalah antara pekara biasa dalam menjaga keselamatan sistem. Alat tersebut telah mencapai tahap yang tinggi bagi menilai keselamatan dan kelemahan yang berpotensi dalam bidang-bidang seperti sistem operasi, konfigurasi peranti, protokol rangkaian dan aplikasi. Walau bagaimanapun, alat ini mempunyai hadnya, seperti mana mereka digunakan, bagaimana ia dilaksanakan dan bagaimana mereka dipelihara dan dikemaskinikan. Selain itu, untuk mencari alat tasiaran VoIP yang terbaik bagi menguji kelemahan sistem. Ia masih sukar untuk membangunkan alat keselamatan yang komprehensif untuk teknologi baru muncul. Voice over Internet Protokol adalah satu contoh teknologi yang kian berkembang dari masa ke semasa. Tesis ini akan meneroka beberapa jenis pencorobohan VoIP dengan menggunakan beberapa ujian alat ceroboh VoIP yang lebih popular bagi mrngenapasti keselamatan VoIP yang baik. Dalam tesis ini juga akan menguji IDS yang terbaik untuk sistem VoIP. Memahami lebih dalam lagi dalam keselamatan VoIP dan akan membantu untuk mengenal pasti isu-isu yang perlu ditangani dalam pembangun masa hadapan dalam sistem keselamatan VoIP.

## TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	ADMISSION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF ABBREVIATIONS	xiii
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objective	3
	1.4 Scope	4
	1.5 Project Significance	5
	1.6 Expected Output	6
	1.7 Conclusion	6



<b>CHAPTER II</b>	<b>LITERATURE REVIEW AND PROJECT METHODOLOGY</b>	
2.1	Introduction	8
2.2	Literature Review	9
2.2.1	Domain	10
2.2.2	Keyword	11
2.2.3	Previous Research	11
2.2.4	Type of VoIP Attacks	12
2.2.5	Software	19
2.3	Proposed Solution	22
2.3.1	Project Methodology	22
2.4	Project Schedule and Milestone	25
2.5	Conclusion	27
<b>CHAPTER III</b>	<b>ANALYSIS</b>	
3.1	Introduction	28
3.2	Problem Analysis	29
3.2.1	Network Architecture	29
3.2.2	Logical and Physical Design	31
3.3	Requirement Analysis	33
3.3.1	Quality of Data	33
3.3.2	Software Requirement	37
3.4	Conclusion	45
<b>CHAPTER IV</b>	<b>DESIGN</b>	
4.1	Introduction	46
4.2	Possible Scenarios	47
4.2.1	Scenario A	47
4.2.2	Scenario B	51
4.3	Security Requirement	70
4.4	Conclusion	71

<b>CHAPTER V</b>	<b>IMPLEMENTATION</b>	
5.1	Introduction	72
5.2	Network Configuration Management	73
5.3	Configuration Environment Setup	73
	5.3.1 Linux and Windows OS Installation	73
	5.3.2 Installing and Setting Up Snort and the Snort Rules	74
	5.3.3 Installing and Configuring 3CX Phone System	75
	5.3.4 Installing and Configuring the Sax2 IDS	76
	5.3.5 Network Configuration	77
5.4	Hardware Configuration Management	79
	5.4.1 Hardware Setup	79
5.5	Security	80
	5.4.1 Security Policies and Plan	80
5.5	Development Status	80
5.6	Conclusion	81
<b>CHAPTER VI</b>	<b>TESTING</b>	
6.1	Introduction	82
6.2	Test Plan	83
	6.2.1 Test Organization	83
	6.2.2 Test Environment	83
	6.2.3 Test Schedule	85
6.3	Test Strategy	86
	6.3.1 Classes of Test	86
6.4	Test Design	89
	6.4.1 Test Description	89
	6.4.2 Test Data	89
6.5	Test Results and Analysis	91

6.6	Conclusion	103
<b>CHAPTER VII</b>	<b>PROJECT CONCLUSION</b>	
7.1	Introduction	104
7.2	Observation on Weaknesses and Strengths	104
7.2.1	Inviteflood tool	104
7.2.2	CommView tool	105
7.2.3	Cain tool	106
7.2.4	Nmap Scan tool	107
7.2.5	RTPinject	108
7.2.6	IDS for VoIP	109
7.3	Propositions for Improvement	110
7.4	Contribution	111
7.5	Conclusion	111
	<b>REFERENCES</b>	112
	<b>BIBLIOGRPHY</b>	114
	<b>APPENDICES</b>	115

**LIST OF TABLES**

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Research Problems	3
1.2	Research Questions	3
2.1	The project milestone for PSM I	25
2.2	The project milestone for PSM II	26
6.1	Hardware and Software	84
6.2	Test Schedule	85
6.3	Network Connectivity Test	87
6.4	Compare the IDS system for VoIP attacks	91
6.5	Compare the Eavesdropping attack	94
6.6	Compare the SIP authentication tools	96
6.7	Compare the best Injection attacks tools	98
6.8	Compare the Dos attacks tools	100
6.9	Comparison of the VoIP attack tools	102

## LIST OF FIGURES

<b>FIGURE</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	System Development Life Cycle approach	23
3.1	Network Topology	30
3.2	Logical Network Design	31
3.3	Physical Network Design	32
3.4	Sax2 IDS during real-time monitoring	34
3.5	Snort IDS during real-time monitoring	34
3.6	Alert detected	35
3.7	Sax2 IDS Log File	36
3.8	Snort IDS Log File	36
3.9	VoIP 3CX Phone System	37
3.10	VoIP 3CX Phone System Activity Log	38
3.11	VoIP 3CX Soft phone for Windows	39
3.12	Softphone for Tablet PC and Smart Phone	39
3.13	Snort System Architecture	43
4.1	Scenario A Network Design	48
4.2	Snort VoIP rule file	48
4.3	Snort rule for VoIP	49
4.4	Snort system process for generate the Alert	49
4.5	Sax2 IDS detecting the attacker	50
4.6	Snort Detection the attacker	50
4.7	Zenmap Port scan tool	51
4.8	SMAP tool	52
4.9	Injection of RTP packet	53
4.10	Injecting the audio file to the VoIP network	53
4.11	Sax2 IDS detect the attacker	54

4.12	Example of the invite flood attack flow	55
4.13	inviteflood attack tool in Linux base	55
4.14	arpspoof tool	56
4.15	Sax2 IDS detect the ARP spoofing attack	57
4.16	iaxflood tool for flooding	57
4.17	Sax2 was detect the iaxflood packet	58
4.18	UDP Flooder tool	59
4.19	Example of RTPFlood attack	59
4.20	Dictionary password	60
4.21	SIP packet	61
4.22	SIP packet that ready to crack	61
4.23	Successful crack the password	62
4.24	Attack using SIPCrack	62
4.25	Make a calling to the Smartphone	63
4.26	VoIPong tool	64
4.27	VoIPong start sniffing	64
4.28	VoIP conversations media files	64
4.29	RTP files that have capture by Wireshark	65
4.30	RTP packet	65
4.31	Audio File that already can play	66
4.32	Mac Address Scanner result	66
4.33	IP Address and their Mac	67
4.34	Man-in-the-middle attack	68
4.35	Communication between 2 user	68
4.36	Captured VoIP RTP packet	69
4.37	The RTP packet that have be capture	70
4.38	Commview media player	70
5.1	Snort VoIP rule file	75
5.2	Management Consoler	76
5.3	Security Policy	77
5.4	IDS Architecture Implementation	78
6.1	Snort IDS rules set	90
6.2	Sax2 IDS rules set	90

6.3	IDS application that have detecting the attack	92
6.4	Show Nmap scan tool	93
6.5	The RTP packet	95
6.6	Cain tools for crack SIP authentication	97
6.7	Successful crack the password	97
6.8	Injecting the audio file to the VoIP network	99
6.9	Sax2 IDS detect the attacker	99
6.10	Compare the Dos attack tools with bandwidth	101
6.11	IP address conflict	102
6.12	Comparison of the VoIP attack tools	103

## ABBREVIATIONS

<b>ABBREVIATION</b>	<b>DESCRIPTION</b>
AP	Access Point
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial of Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
LAN	Local Area Network
MAC	Media Access Control
MB	Megabytes
NIC	Network Interface Card
OS	Operating System
PERT	Program Evaluation and Review Technique
PRGA	Pseudo Random Generation Algorithm
QoS	Quality of Service
RAM	Random Access Memory
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSID	Service Set Identifier
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network



**LIST OF ATTACHMENTS**

<b>ATTACHMENTS</b>	<b>TITLE</b>	<b>PAGE</b>
A	Gantt chart	117
B	Software Installation	118

## CHAPTER I

### INTRODUCTION

#### 1.1 Project Background

Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Voice over Internet Protocol (VoIP) has seen rapid implementation over the past few years.

A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service. This paper deals with VoIP communication security and various techniques of VoIP attacks. We also try to find effective methods to prevent or mitigate these attacks. At the end, we provide a real example of a VoIP attack.

The paper focuses solely on Session Initiation Protocol (SIP) which is the most frequently used signal protocol these days. Voice over Internet Protocol is without any doubts a step ahead in communication technologies. But similarly to other technologies, there should be certain specific rules and security measures otherwise the technology does not work.

This project will be focusing on how these IDS software will detect the attacking comes from several types of VoIP attacks. Attacks such as Information Gathering, Eavesdropping, Attacking Authentication, VoIP Media Manipulation and Denial Of Service. This 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 network system itself.

## 1.2 Problem Statements

Security continues to be an issue and an obstacle to implementing VoIP for many individuals and companies. Especially in cases where many calls deal with sensitive or confidential information. Of course, VoIP is subject to the same sorts of attacks as data networks, example denial-of-service (DoS) attacks that can bring down your VoIP service.

VoIP conversations in on their calls can hackers listening by capture the packet, and the data packets can easily be intercepted by hacker to record the calls. Most of the organizations which have implemented VoIP are either unaware or ignore the security issues with VoIP and its implementation. Like every other network, a VoIP network is also susceptible to abuse. Network Security becomes a large and growing area of concern between corporations whiles accessing internet.

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.

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.

Table 1.1 shows the research problems in this project.

<b>RP</b>	<b>Research Problem</b>
<b>RP 1</b>	<b>There are many hardware and software currently in the market can be used to detect the attacking.</b>
<b>RP 2</b>	<i>There are lack of VoIP IDS implementation</i>

Table 1.2 shows the research problems and research questions in this project.

<b>RP</b>	<b>RQ</b>	<b>Research Question</b>
<b>1</b>	<b>1</b>	<b>How to choose the better hardware and software for monitoring VoIP network?</b>
<b>2</b>	<b>2</b>	<i>What is the capability of VoIP attacking and detecting system?</i>

### 1.3 Objective

This project will analysis and examine some real world attack vectors and discover how hacker can assist us pretesting VoIP. In this project will go to protocol level details of the basics, though it is strongly encouraged to understand the protocols used in VoIP networks.

We will also set-up an attacker to compromise the VoIP being established to better understand some VoIP security issues. And this project wills various enumeration techniques followed by demonstration of few VoIP attacks and compare

the type of attacking. Also type of hacking the VoIP over wireless and wired connection. Using intrusion detection system (IDS) where it can identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system and can kill the process that try to access to network or VoIP system.

When there are any suspicious patterns occurs the system will make an alert, and then it depends to the admin that handle the system either wants to kill or ignore the process.

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

- I. Setup a VoIP Network.
- II. Analysis type of attacking to VoIP and compare it.
- III. Analysis the best system that can detect the attacker (Snort and Sax2 IDS).
- IV. To compare which IDS are the best in order to detect the attacks when implement in a real-time Intrusion Detection System.

#### **1.4 Scope**

The scope of the project is to analysis the attacking of VoIP phone system. Compare type of the attacking in real time environment. Compare Intrusion Detection System for VoIP System, in order to fine the best software to detect the intrusions that were cause by network attack for example Denier Of Service, Open Port Scanner, Eavesdropping (Sniffing) and many more attack.

From the result, the administrator will know exactly and understand type of attacking and the VoIP intrusion detection system 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 conducted in an isolated local area network (LAN) that will be detailed explained in the next chapter because the test will be conducted to test the IDS software whether they can perform in a normal environment where there are no attacks occur to the network and also will be tested in a stress environment where there will be a lot of attacks to the specific host in the network.

Scope of this project will be involved setting up a VoIP in a LAN network. The operating system for the server is Windows Server. The hardware Linksys Access point will be used.

- I. Setup a VoIP in LAN network.
- II. Attack the VoIP network.
- III. Detect the hacker using IDS Software.

## **1.5 Project Significance**

The project significance will be focusing on the analysis type of attacking and describing the capabilities of Snort and Snort2 IDS to produce better output in detection of intrusion and vulnerabilities in a VoIP network.

In order for users that want to implement the VoIP Phone System and Intrusion Detection System for VoIP software on their network system because from this project, the users are able to choose and select the best software that will be compared in this project based on their detection on attacks that will be launched to the host.

Users or the Administrator also can protect the network and more importantly the servers that have been set up on the current network by the hacker or attacker whether insider or outsider attacker that want to break 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.

## **1.6 Expected Output**

The expected output that will be achieved after carrying out the project is will be able to identify types of attacking to VoIP system and comparing. Analysis the best system that can detect the attacker using (Snort and Sax2 IDS). Will be analysed in this project and a report will be generated to show the result of this project. Intrusion Detection System software also will be test by perform lots of attack. The type of attack that will be used to test software are network attack. So by perform those attacks.

## **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.