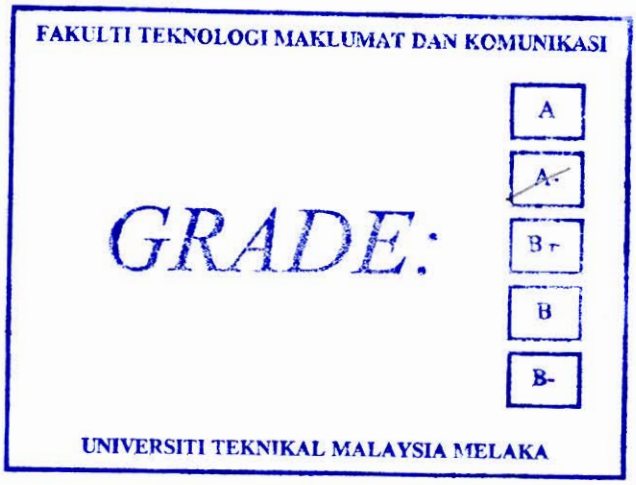
EVALUATING KISMET AND WIFI MANAGER AS WIRELESS IDS

ALIMAN BIN SELAMAT



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS

JUDUL: EVALUATING KISMET AND WIFI MANAGER AS WIRELESS IDS

SESI PENGAJIAN: 2010/2011

Saya, ALIMAN BIN SELAMAT

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: Km4343 PT6663
Jln Samarinda 9, Tmn Samarinda
Pengkalan, 78000 Alor Gajah
Melaka

Tarikh : 05.07.2011

(TANDATANGAN PENYELIA)

MR OTHMAN BIN MOHD

Tarikh : 05-07-2011

EVALUATING KISMET AND WIFI MANAGER AS WIRELESS IDS

ALIMAN BIN SELAMAT

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
2011

DECLARATION

I hereby declare this project report entitled

EVALUATING KISMET and WIFI MANAGER as WIRELESS IDS

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

STUDENT : _____ Date: 05.07.2011

(ALIMAN BIN SELAMAT)

SUPERVISOR : _____ Date: 05.07.2011

(MR. OTHMAN BIN MOHD)

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

Bismillahirrahmanirrahim

Alhamdulillah, Thanks to Allah SWT, whom with His willing give me the opportunity to complete this Final Year Project which is title Evaluating Kismet and Wifi Manager as Wireless IDS. 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, Mr. Othman bin Mohd, 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

This project is about the Wireless IDS using Kismet and Wifi Manager to give security for wireless network. In this project, the capabilities of both Kismet and Wifi Manager will be discussed. A detailed explanation of how to install Kismet and Wifi Manager, including the installation and configuration for use as an IDS will follow. Kismet and Wifi Manager will monitor the wireless network within range and provide alert if there is possible threat occur limited to the rules. This software is configured using Ubuntu 10, and Window Server 2003 operating system and MySQL server as database. The traditional project management has been used as the methodology. Overall this implementation of security will give more benefit and information's to users that want to monitor their wireless network.

ABSTRAK

Projek ini adalah tentang mengkaji keupayaan Kismet dan Wifi Manager sebagai alat keselamatan rangkaian untuk memberikan keselamatan bagi rangkaian tanpa wayar. Dalam projek ini, kemampuan kedua-dua Kismet dan Wifi Manager akan dibahas. Penjelasan terperinci tentang cara instalasi Kismet dan Wifi Manager, termasuk pemasangan dan konfigurasi Kismet dan Wifi Manager untuk digunakan sebagai IDS. Kismet dan Wifi Manager akan memantau rangkaian tanpa wayar yang berada dalam liputan dan memberikan peringatan jika ada ancaman yang berlaku terbatas pada kemampuan Kismet dan Wifi Manager. Perisian ini dikonfigurasikan menggunakan Ubuntu 10, Windows Server 2003 sistem operasi dan pelayan MySQL sebagai database. Pengurusan projek tradisional telah digunakan sebagai metodologi. Secara keseluruhan pelaksanaan keselamatan akan memberikan keuntungan dan maklumat yang berguna bagi pengguna yang ingin memantau rangkaian tanpa wayar mereka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ABBREVIATION	DESCRIPTION
AP	Access Point
ARP	Address Resolution Protocol
CCPM	Critical Chain Project Management
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial of Service
FTP	File Transfer Protocol
GNU GPL	GNU General Public License
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
LAN	Local Area Network
LAWN	Local Area Wireless 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
WBS	Work Breakdown Structure
WIDS	Wireless Intrusion Detection System
WDS	Wireless Distribution System
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Project Background

Wireless technology has emerged as a very popular alternative to wired technology in recent years and has become more readily available for computer networks anywhere, whether it is for a home, an office, or any size of business. Wireless technology is another way of connecting a number of computers without using wired. Wireless technology uses radio frequency to connect wirelessly, so there is greater freedom to connect computers from anywhere in a home or an office network.[1]

In a WLAN, a device called an AP, or key point, connects multiple computers to the network. The access point usually has a small antenna attached, which allows the device to transmit data back and forth over radio signals. These radio signals can travel up to 300 feet. With an outdoor access point with larger antennas, a signal can travel up to 30 miles to serve public places such as college and high school campuses, airports, and many other outdoor venues. The basic configuration of a WLAN is not much different from a regular LAN, except that the network uses radio waves instead of wires and cables. By adopting the use of radio waves, the range of communication is much farther than with infrared rays with much less interference.[2]

Because WLAN uses radio waves, there is the potential that a third party could attempt to access or intrude into networks illegally. To prevent such intrusions,

one of the tools available for use is a WIDS. These wireless IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs. Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures [3] or on anomalies in the traffic. [4]

This "Evaluating Kismet and Wifi Manager as Wireless IDS" is project that discusses the capabilities of both Kismet and Wifi Manager to work as IDS for wireless network. This project will show the prove of concept for wireless technologies, outline the key security threats for wireless networking, specifically focusing on intrusion detection systems for WLAN 802.11 networking and the need for them to be included as part of an overall security solution.

1.2 Problem Statements

An intrusion is somebody attempting to break into or misuse your system. The word "misuse" is broad, and can reflect something severe as stealing confidential data to something minor such as misusing your email system for spam.[5] Unlike traditional wired networks where network packets are transmitted along physical wires, wireless technologies use the air as the physical media when sending and receiving data packets.[6] Air being the physical media where wireless packets traverse, opens up whole new opportunities for anyone within the vicinity (either of the wireless client or the wireless access point) with the right devices and software to be able to capture those packets.

Air being the physical media where wireless packets traverse, opens up whole new opportunities for anyone within the vicinity (either of the wireless client or the wireless access point) with the right devices and software to be able to capture those packets. In order to capture wireless packets, the sniffing station will have to be equipped with the appropriate hardware and software. The hardware required will depend on the wireless network being targeted and they come in the form of a

wireless network interface card.[7] Table 1.1 and 1.2 shows the research problem and research question occur during research.

Table 1.1 shows the research problems in this project.

RP	Research Problem
RP 1	There are many hardware and software currently in the market can be used to capture wireless packets.
RP 2	There are lack of WIDS implementation

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

RP	RQ	Research Question
1	1	How to choose the better hardware and software for monitoring wireless packets?
2	2	What is the capability of WIDS?

1.3 Objectives

The main objectives of this project are:

- To monitor wireless packet using Kismet and Wi-Fi Manager.
- To analyze and evaluate the capabilities of Kismet and Wi-Fi Manager.
- To choose the best WIDS.

From the research problem and research question, the research objectives have been create to overcome the problem and question as shown in Table 1.3.

Table 1.3 shows the research problems, research questions, and research objectives.

RP	RQ	RO	Research Objective
1	1	1	To monitor wireless network using Kismet and Wi-Fi Manager.
2	2	2	To analyze and evaluate the capabilities of Kismet and Wi-Fi Manager as WIDS
2	2	3	To choose the best WIDS.

1.4 Scope

Scope of this project will be involved data capturing at Experiment Technique Lab, Faculty of Information and Communication, Universiti Teknikal Malaysia Melaka. The operating system for main server is Windows server 2003 and for Kismet server is Ubuntu 10.10. The software used is Kismet-2011-01-R1 and will be configuring as kismet server. The hardware Linksys WRT54GL will be used as drone in order to monitoring and capturing the wireless packets. Data capturing duration will held from 14 March 2011 until 25 March 2011.

1.5 Project Significance

Describe the capabilities of Kismet and Wi-Fi Manager to produce better output in detection of intrusion and vulnerabilities in wireless network.

1.6 Expected Output

Performance of WIDS in wireless network will be analyzed in this project and a report will be generated to show the result of this project.

1.7 Conclusion

Wireless intrusion detection systems are an important addition to the security of wireless local area networks. While there are drawbacks to implementing a wireless IDS, the benefits will most likely prove to outweigh the downsides. With the capability to detect probes, DoSs, and variety of 802.11 attacks, in addition to assistance with policy enforcement, the benefits of a wireless IDS can be substantial. Of course, just as with a wired network, an IDS is only one part of a greater security solution. WLANs require a number of other security measures to be employed before an adequate level of security can be reached, but the addition of a wireless IDS can greatly improve the security posture of the entire network. With the immense rate of wireless adoption, the ever-increasing number of threats to WLANs, and the growing complexity of attacks, a system to identify and report on threat information can greatly enhance the security of a wireless network.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

This chapter will discuss details about the literature review and project methodology. The purpose of this chapter is to conduct the research about the other systems or applications that are similar to the system that will be developed. All aspect is studied in order to develop a system that is more effective. Furthermore, the discussion is also including the methodologies, techniques, hardware and software that being used in other research. The comparison between them is analysed to highlight the differences thus determine the better solutions for this project.

2.2 Literature Review

Literature review is about the investigating and analysing the current systems that are similar and applied same technology with the system that will be implementing. Moreover, a literature review is a body of text that aims to review the critical points of current knowledge and methodological approaches on a particular topic. Literature reviews are secondary sources, and as such it does not report any new or original experimental work.