DEVELOPING A WIRELESS PENETRATION TESTING TOOL IN LINUX PLATFORM

NOR ARLIZA BINTI ABDULLAH

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

FACULTY OF INFORMATION TECHNOLOGY AND COMMUNICATION
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2013

DECLARATION

I hereby declare that this project report entitled

DEVELOPING A WIRELESS PENETRATION TESTING TOOL IN LINUX PLATFORM

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

STUDENT : _________________________ Date: _______________
(NOR ARLIZA BINTI ABDULLAH)

SUPERVISOR : _________________________ Date: _______________
(DR.WAHIDAH BINTI MD SHAH)

DEDICATION

Alhamdulillah and praise to Allah S.W.T, with His will, I able to complete this project successfully. This dissertation is dedicated to my beloved parents Hj. Abdullah bin Ahmad and Hjh. Shuaini binti Suib who have supported me all the way since the beginning of my study and always supporting me. I also want to thank my supervisor Dr.Wahidah binti Md Shah for the guidance and encouragement for me during conducting this project.

ACKNOWLEDGEMENT

Firstly, I would like to express my gratitude to God for all the understanding during these three years in gathering and compiling this project. I also would like to thank my parents for keep praying and supporting and never let me give up in my study. I also would like to thank my *Projek Sarjana Muda* supervisor, Dr.Wahidah binti Md Shah for sacrificing her valuable time to assist me and thanks for her comments, motivations and idea and encouragement during this semester. I also would like to thank my classmates who encourage me to accomplish this project and willing to help if their help is needed.

Finally, I would like to thank and appreciate all individuals who directly or indirectly took part in making this project successful.

ABSTRACT

Wireless Local Area Network (WLAN) has been popular and more preferred by the users compared to wired ones. This is because wireless has more advantages compared to wired technology such as more cost effective and mobility issue. The disadvantage of using wireless technology is it has high risk of the threat. This research is focused on wireless fidelity (wifi) keys. There are three encryption types for wireless security which are Wired Equivalent Protocol (WEP), Wireless Protected Access (WPA) and Wireless Protected Access 2 (WPA2). This project was proposed to help to carry out wifi penetration testing. This penetration testing was conducted to determine wireless vulnerabilities in these three encryption types and to study the differences between them. The contribution of this project is to guide to carry out penetration testing and as an exposure on how the attack had been done by the crackers.

ABSTRAK

Rangkaian tanpa wayar telah menjadi popular dan menjadi pilihan oleh pengguna berbanding rangkaian dengan wayar. Ini kerana rangkaian tanpa wayar memberi lebih banyak faedah jika dibandingkan dengan teknologi rangkaian dengan wayar seperti ia lebih murah dan tidak membataskan pergerakkan. Kelemahan penggunaan rangakaian tanpa wayar adalah ia lebih berisiko. Kajian ini tertumpu kepada kekunci rangkaian tanpa wayar. Terdapat tiga jenis enkripsi untuk rangkaian tanpa wayar iaitu *Wired Equivalent Protocol (WEP), Wireless Protected Access (WPA),* dan *Wireless Protected Access 2 (WPA2).* . Projek ini telah dicadangkan untuk membantu memudahkan ujian penembusan rangkaian tanpa wayar. Ujian penembusan ini dijalankan bertujuan utuk mengenalpasti kelemahan yang ada pada ketiga-tiga jenis enkripsi ini serta mengkaji perbezaan di antara ketiga-tiga jenis enkripsi ini. Sumbangan projek ini adalah untuk member panduan untuk menjalankan ujian penembusan dan mendedahkan bagaimana serangan keatas rangkaian dilakukan oleh penggodam.

TABLE OF CONTENTS

CHAPTER 5 TESTING AND ANALYSIS

CHAPTER 6 CONCLUSION

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advance Encryption Standard
AP	-	Access point
BSSID	-	Broadcast service set identifier
CCMP	-	Cipher Block Chaining Message Authentication Code Protocol
CIA	-	Confidentiality Integrity Authentication
CPU	-	Central Processing Unit
EAP	-	Extensible Authentication Protocol
GUI	-	Graphical user interface
GTK	-	Group Temporal Key
ICV	-	Integrity check value
ISP	-	Internet Service Provider
IV	-	Initialization vector
IEEE	-	Institute of Electrical and Electronics Engineer
MAC	-	Media access control
MPDU	-	Medium Access Control Protocol Data Unit
MSDU	-	Medium Access Control Service Data Unit
MIC	-	Message Integrity Code
OS	-	Operating system
PC	-	Personal computer

PMK	-	Pair Master Key
PSK	-	Pre-Shared Key
PRNG	-	Pseudo Random Number Generator
RADIUS	-	Remote Authentication Dial-In User Service
RAM	-	Random Access Memory
SDLC	-	System Development Life Cycle
SSID	-	Service set identifier
TKIP	-	Temporal key Integrity Protocol
TLS	-	Transport Layer Security
WAP	-	Wireless access points
WEP	-	Wired Equivalent Privacy
WPA	-	Wireless Protected Access
WPA2	-	Wireless Protected Access version 2
Wifi	-	Wireless Fidelity
WLAN	-	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Introduction

Two decades years back, it was hardly anyone heard of wireless internet. Nowadays, our technology devices mostly are wireless network-enabled devices. In wireless local area network (WLAN), big issues are associated with the security problems. According to Choi,M.K., et. al, the wireless signal of WLAN is broadcast in all directions through the air using radio frequencies [8]. The risk of interception is higher than compared with wired network and unauthorized people can easily capture the data transmitted illegally by exploit wireless vulnerability. Thus, wireless network is not a really secure connection. Referring to H,Halapacz, he stated that WLANs are increasingly used because of mobility, affordable prices for wireless devices, and convenience issue [10]. To test our wireless network security, we need to carry out penetration testing. Penetration testing or pen-test is an alternative to determine wifi network security by stimulating an attack from malicious outsiders which is unauthorized access. Before this, the penetration testing is carried out with command lines entered manually one by one.

Since there are a lot of commands, it will be inconvenient to enter manually. Therefore, this project is developed to ease the testing. The wide range of wifi usage emphasizes importance of having a secure network. In order to secure the network, mostly encryptions are likely to be used are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA/WPA2). This encryption will allow the data transmitted within network being encrypted. Security also interrelated with the security key or password. The password strength is determined by password complexity. The stronger the user's password strength caused difficulty for attacker to break the key. The Backtrack Linux distribution is built for computer security enthusiasts and pen-tester. This tool is developed using scripting language. This project is developed to study the vulnerability of wifi security encryption. Then, this project also developed to study the different of encryption mechanism used in WEP and WPA2. This bash script allowed few commands typed manually to be executed automatically. All the detail is discussed in this chapter.

1.2 Problem Statements

1. Lack of information on factors that lead to vulnerability of the wifi security mechanism which cause difficulty to ensure their wifi security on top level

The vulnerability in the encryption mechanisms can be deployed to penetrate the network. Lack of information on factors that cause it leads to the penetration testing.

2. Lack of information on the difference between WEP and WPA2

Difficulty to differentiate between WEP and WPA2 encryption because of lack of information. The mechanisms used in these encryption types vary in a few aspects such as key length. The effectiveness of the mechanisms can only be known once the testing are done.

3. Difficulty using command lines entered manually to carry out this penetration testing for checking their wifi security purpose.

Entering each command lines manually cause difficulty. If there is even small mistake in the command line, the command might be fail to be executed. So this project is developed to ease to carry out penetration testing.

Table 1.1: Problem Statement

No	Problem Statement
RP1	Lack of information on factors that lead to vulnerability of the wifi security mechanism which cause difficulty to ensure their wifi security on top level.
RP2	Lack of information on the difference between WEP and WPA2.
RP3	Difficulty using command lines entered manually to carry out this penetration testing for checking their wifi security purpose.

Table 1.2 : Research Problem

RP	RQ	Research questions
RP1	RQ1	What are the factors that cause vulnerability of wireless security mechanism?
RP2	RQ2	What are the differences of mechanism used in WEP and WPA2 ?
RP3	RQ3	How to ease the users to carry out the penetration testing for their wireless networks in more convenient way rather than enter each command line manually?

1.3 Objectives

This project embarks on the following objectives:

1. To study the vulnerability of wifi security encryption type which is not exposed to the users such as weakness of encryption algorithm.

2. To discover the differences of encryption mechanism in WEP and WPA2.

3. To develop a penetration tool for wireless penetration testing which assist user to carry out the testing.

Table 1.3: Objective

RP	RQ	RO	Objectives
RP1	RQ1	RO1	To study the vulnerability of wifi security encryption type which is not exposed to the users such as weakness of encryption algorithm.
RP2	RQ2	RO2	To discover the differences of encryption mechanism in WEP and WPA2.
RP3	RQ3	RO3	To develop a penetration tool for wireless penetration testing which assist user to carry out the testing

1.4 Scope

The scope for this project includes:

This project focuses on wireless LAN security. The users of this project are network administrator. Since they have been exposed to ethical work and company policy, it can prevent them from doing unethical thing. This project is a creation of bash script in Linux operating system. This tool will only work if it meets the all the requirement. In this section, all software and project requirement are described. For example, this system worked if wireless adapter used that support aircrack suite.

1.4.1 Software

i) Virtual machine software (VMWareWorksation)

Virtual machine enables users to set up multiple virtual machine (VMs). It allowed multiple virtual machines to be used concurrently along with the actual machine. Each virtual machine can execute its own operating system, such as Linux, Solaris and Microsoft Windows. VMware Workstation allows one physical machine to run multiple operating systems simultaneously. This software is developed and sold by VMWare.Inc.

ii) Backtrack operating system

In order to install Backtrack operating system, it needs a USB with minimum space of 4GB. The tool will be developed in Backtrack Linux operating system. Backtrack is a penetration testing Linux distribution which is your one-stop shop for learning penetration testing. Backtrack Linux is designed with the purpose of using it in penetration testing. In this operating system, bash script created contain all commands necessary for wireless penetration testing.

1.4.2 Hardware

i) Laptop

The laptop used in this project has been installed 3 GB random access memory (RAM), with 32-bit architecture. This laptop running on windows 7 platform with the processor Intel® Core ™ 2 Duo processor T6600 central processing unit (CPU) running at cpu minimum 2.20 GHz .

ii) Wireless access point

Wireless access point (APs or WAPs) are specially configured nodes on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of WLAN radio signals and support Wi-Fi wireless communication standards.

iii) USB wifi adapter (AZTEC Wireless-N WL568USB Adapter)

This wifi dongle is Wireless N WL568USB speed up to 300Mbps makes it ideal for video streaming, online gaming and internet calls. This adapter is used because it has chipset that can support packet injection. It supports 64/128-bit strength WEP encryptions, as well as WPA/WPA2 encryptions and mechanisms encryption to prevent outside intrusion and protect your personal information from being exposed. The device is easy to install or use.

1.5 Expected Output

The expected results from this project are to help to carry out wifi penetration testing using bash script. Other than that, this project also expected to expose about the vulnerability of the wifi security mechanism. Other than that, this tool can also help to set up the wifi setting in security aspect.

1.6 Report Organization

This chapter consists of project background, problem statements, objectives, scope of this project and expected output from this project. Then, in chapter 2, related previous works is discussed. Analysis of current problem and proposed solution also is included in chapter 2. In chapter 3, methodology used for this project is explained in detail. Chapter 4 is discussed about design and implementation. All hardware and software requirement are stated in this chapter. In chapter 5, analysis and testing are done. All the steps on how to analyze are described in detail here. In chapter 6, the limitations, contributions, and future works are discussed there.

1.7 Conclusion

As a conclusion, the expectation output from this project is to resolve all the problems stated and the objectives achieved within the time allocated. In this chapter, three objectives, scope of the project, and the software and hardware used are identified. Chapter 2 is discussed about the related previous works, analysis of current problem and proposed solution for the problems identified.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

A literature review is a text description of the literatures related to any particular topic. It is also a survey of existing writing within the scope. It gives an overview of what has been said, what hypothesis, and methodology used. The purpose of this literature review is to extract some valuable knowledge through summary, classification and comparison of prior research studies. In this chapter, all problems relevant to the wifi security are discussed. The purpose was to determine the vulnerability of wifi security mechanism which is not really exposed to us.