T.R.
ERCIYES UNIVERSITY
GRADUATE SCHOOL OF NATURAL OF AND APPLIED SCIENCES
DEPARTMENT OF COMPUTER ENGINEERING

DEVELOPING A METHOD TO PROTECT ATTACKS IN WIRELESS NETWORKS

Prepared by
Muntasser HAMZAH

Supervisor
Asst. Prof. Dr. Celal ÖZTÜRK

MSc Thesis

July 2017
KAYSERİ

T.C
ERCIYES UNIVERSITY
GRADUATE SCHOOL OF NATURAL OF AND APPLIED SCIENCES
DEPARTMENT OF COMPUTER ENGINEERING

DEVELOPING A METHOD TO PROTECT ATTACKS IN WIRELESS NETWORKS

(MSc Thesis)

Prepared by
Muntasser HAMZAH

Supervisor
Asst. Prof. Dr. Celal ÖZTÜRK

July 2017
KAYSERİ

SCIENTIFIC ETHICS DECLARATION

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Muntasser HAMZAH

SUITABILITY FOR GUIDE

The MSc thesis entitled **"Devoloping a Method to Protect Attacks in Wireless Networks"** has been prepared in accordance with Erciyes University Graduate Education and Teaching Institute Thesis Preparation and Writing Guide.

Prepared by

Muntasser HAMZAH

Supervisor

Yrd. Doç. Dr. Celal ÖZTÜRK

Chairman of the Department of Computer Engineering

Prof. Dr. Derviş KARABOĞA

ACCEPTANCE AND APPROVAL PAGE

This study entitled "**Developing A Method To Protect Attacks In Wireless Networks**" prepared by **Muntasser HAMZAH** under the supervision of **Assist. Prof. Dr. Celal ÖZTÜRK** was accepted by the jury as MSc. Thesis in Computer Engineering Department.

.../.../ 2017

JURY:

Supervisor: Yrd. Doç.Dr. Celal ÖZTÜRK .....

Juror : Yrd. Doç. Dr. Günyaz Ablay .....

Juror : Yrd.Doç.Dr. Selçuk ÖKDEM .....

APPROVAL:

That the acceptance of this thesis has been approved by the decision of the Institute's Board of Directors with the 18/07/2017 date and 2017/30-51. numbered decision.

.....19../..07../ 2017

Prof. Dr. Mehmet AKKURT

Director of the Institute

ACKNOWLEDGEMENTS

First, I would like to thank Allah, for having made everything possible by giving me strength and courage to do this work.

Special thanks to my supervisor Asst. Prof. Dr. CELAL ÖZTÜRK for his time, patience, and supporting during the development of this project, it has been an honor for me to work with him.

I would like to extend my thanks the Government and the people of Turkey for their hospitality, generosity and a very good handling with me.

Finally, I would like to extend my thanks to my parents, my wife, my children and all friends.

TABLE OF CONTENTS

DEVELOPING A METHOD TO PROTECT ATTACKS IN WIRELESS NETWORKS

CHAPTER 2

MATERIALS AND METHODOLOGY

CHAPTER 3

EXPERIMENTAL STUDIES

CHAPTER 4

DISCUSSION, CONCLUSION, AND RECOMMENDATIONS

LIST OF TABLES

LIST OF FIGURES

KABLOSUZ AĞLARA YAPILAN SALDIRILARA KARŞI KORUYUCU BİR YÖNTEMİN GELİŞTİRİLMESİ

Muntasser HAMZAH

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüsek Lisans Tezi, July 2017
Danışman: Yrd. Doç. Dr. Celal ÖZTÜRK

ÖZET

Ortadaki adam saldırısı, servis dışı bırakma ve oturum çalma vb. kablosuz ağlara yapılan saldırılar göstermektedir ki, hiç bir açık ağ sızıntılara karşı tam güvenli değildir. Kablosuz ağlar özellikle yarı-açık dinamik değişken topolojilere sahip olmaları, kooperatif algoritmalar kullanmaları, merkezi izleme ve yönetim noktası eksiklikler gibi özeliklerinden dolayı kesin olarak savunmalıdırlar denilemez. Ayrıca kablolu ağlar için geliştirilmiş birçok saldırı tespit yöntemi kablosuz ağlara uygulanamamaktadır.

Saldırıları tespit etmek zorlu bir araştırma problemidir. Bu tez çalışmasında ilk olarak kablosuz ağların açıkları incelenmiştir, ağ ele geçirme denemelerinden ve bilgi sızdırma çabalarina karşı saldırıların nasıl tespit edilebileceği üzerine çalışılmıştır.

Tez çalışması kapsamında iki yeni uygulama önerilmiştir, ilk olarak saldırı tespit edildiğinde arayüz üzerinden saldırganın IP ve MAC bilgisini içeren alarm verme ve saldırganın IP ve MAC adresini engelleme uygulaması geliştirilmiştir. İkinci yönten ise yöneticinin bilgisayarı dışındaki tüm IP'leri engelleme ve bütün MAC adreslerini kapatma uygulamasıdır, böylece hiç kimse yönlendiriciye erişemeyecek, bilgi toplayamayacak ve ağı tarayamayacaktır.

Anahtar Kelimeler: Kablosuz ağlar, Ağ saldırıları, Ağ güvenliği ve koruma

DEVOLOPING A METHOD TO PROTECT ATTACKS IN WIRELESS NETWORKS

Muntasser HAMZAH

Erciyes University, Graduate School of Natural and Applied Sciences
M. Sc. Thesis, July 2017
Supervisor: Asst. Prof. Dr. Celal ÖZTÜRK

ABSTRACT

The attacks to several major wireless networking like Man-in-the-Middle (MITM), Denial of Services (DOS) and Session Hijacking, have shown that no open network is safe from intrusions. Wireless network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the attack detection techniques developed on a fixed wired network are not applicable in wireless network.

Detect attacks is a challenging research problem. This research first examines the vulnerabilities of a wireless networking, the reason why there is a need for attacks detection, and how to have attacks detection from the first attempt to hack network and intrusion to information.

We proposed two new applications, the first application to detect the attack and give an alarm, through the interface contains the IP and Mac attacker, and the gives a block to the IP and Mac attacker. The second application is protecting by giving a block to all IPs except for the administrator's computer, and closing all MACs addresses, so that no one can access the router, sniffing work, gathering information and scanning the network.

Key Words: Wireless Network, Attacks to networks, Network Security and protection.

INTRODUCTION

Communications, as a system, have security challenges (either infrastructure or services) like a great challenge posed by the information technology resources. The presence of the same technical, organizational, and human barriers in an attempt to meet this challenge should be noted.

The protection of information in the event of a breach is necessary, though not sufficient in itself, where the degree of exposure increases once the stage of information processing and storage is reached. Hasty rush and unregulated security tools hinder use, harm the operations, and adversely affect the performance of IT systems. For example, protecting data encryption during the transition process is useless if it will be stored at a later date in the non-security. Similarly, the establishment of a security system, such as "firewall" will be remembered if it is allowed for connections that exceed the value of this system.

Such lack of awareness and information security were not given the importance and necessary attention due to illegal software usage to such a high level compared to other countries. Institutions cannot understand the importance of the matter before the beginning of a nuisance. However, because of the complexity and diversity of the threats, it has not seen enough of this technology to be used in many different security technologies.

Two applications are designed to develop a way for protection against attackers in wireless networks. The applications are coded by using the Python programming language for Kali Linux System because it has already been pre-installed in it. Also, the program will depend on the ARP to send the corrupt packets to the modem. After that,

the modem sends back the report that contains the IP of the attackers. By then, the software have already block it.

ARP (Address Resolution Protocol) is a widely used communications protocol for resolving Internet layer addresses into link layer addresses. The basic principle behind the ARP deception is to exploit the lack of documentation in the ARP protocol by sending spoofed ARP messages on the local network [1].

One goal of ARP cache poisoning is to put the attacker in position to capture and log network information. Intruders have several tools for listening on the LAN and logging data for later analysis [2] [3].

The applications intercept packets that can be read, sniffed, or changed before sending on to the victim. The goal of the project is to detect listening and sniffing, and attempts to a penetration of the wireless network and the wired network.

By means of two methods, the first to detect attack attempt, give an alarm, through the GUI show the attacker information, IP and MAC, and give it block by sending it to the router. The second way is to exclude the administrator's IP, and give a block to all IPs, thus ensuring that no user can access the router.

Both methods are explained in detail in the following chapters.

2.4 GHz vs. 5GHz Techniques:

The wireless network tools typically use radio signals either 2.4 GHz or 5 GHz ranges.

Interference

2.4 GHZ band faces further intervention from the 5GHz signal because of two things:

The main issue is that there are many wireless devices that operate at 2.4 GHz, like cordless phones, baby directors, and games radio controlled, amateur radio, microwaves, etc., and lots of existing wireless networks that may be close to you, like

your neighbors or people in your home complex. A much smaller number of devices and networks currently using 5GHz [4].

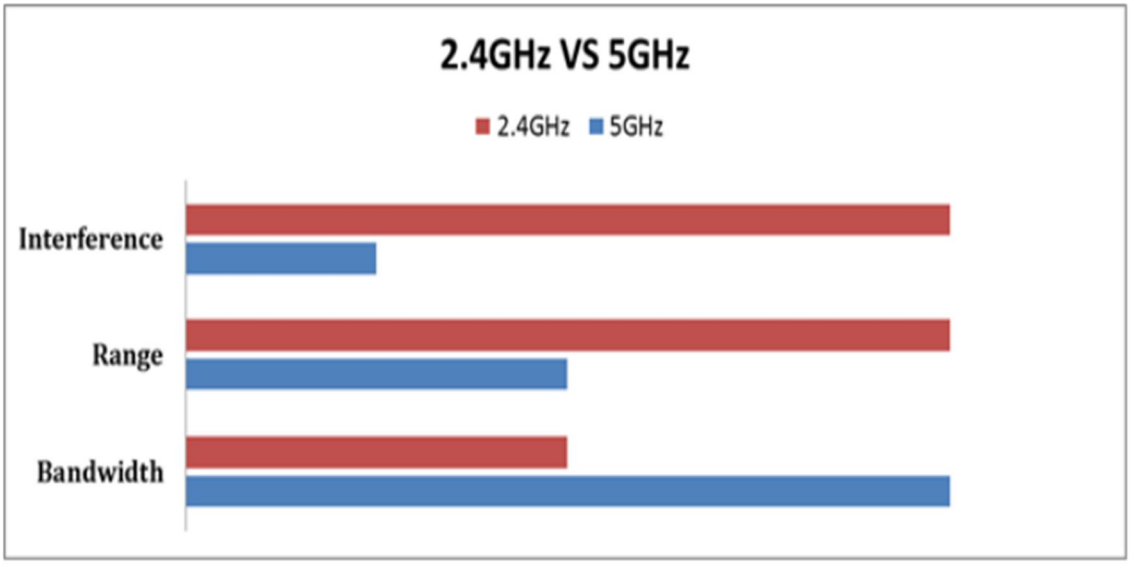

Figure 1. 2.4 GHz vs. 5GHz Techniques (from Google)

In addition, the 2.4GHz band has only three non-overlapping channels (channels 1, 6 and 11) of these different devices to work, examined with 23 band 5GHz channels. The appearance of more channels makes it simple to find the channel that has not obtained used by anyone other in the area [5].

Range

Many external influences that affect how the wireless network, making it impossible to predict what the scope will achieve in site. Some materials in the walls and tiles, pipes can greatly affect effective stream group [3].

High frequency (5GHz) radio waves lose more than one pass through the walls of power, etc. air from the lowest frequency (2.4GHz L) waves. Since the broadcast is sent to essentially the same power source, 2.4GHZ wireless networks usually have the widest range of 5GHz networks, group for each of the bands can be significantly increased through the use of high-gain special directional antennas, top-of-the-line routers become with this already, if you want to expand your wireless network for all

activities of the area of your Wi-Fi, it can be beneficial to consider upgrading the router [2].

Speed

The main difference between 2.4GHZ and 5GHz is the data transfer speed, which may also be described as bandwidth. Where 5GHz allow network connections much faster than 2.4GHZ's. If high-bandwidth applications, such as video, are transferred through your wireless network, 5GHz is by far the best choice [3].

Wireless Networks Standards:

Three generations of standards for wireless networks have emerged so far and in a chronology: 802.11, g 802.11, and 802.11b. The focus was on the faster speed of data transfer. These three generations did not take the issue of security well enough, which made wireless networks more vulnerable to security threats [6].

IEEE Computer Society are working on a new version of a standard with special security Wireless networks, which had been covered by standards 802.11i [7].

Table standards are be shown in table 1 and table 2

Table 1. 802.11 network PHY standards

Release date	Standard	Frequency	Modulation
Jun 1997	802.11	2.4 GHz	DSSS, FHSS
Sep 1999	802.11a	5 GHz	OFDM
Sep 1999	802.11b	2.4 GHz	DSSS
Jun 2003	802.11g	2.4 GHz	OFDM
Oct 2009	802.11n	2.4/5 GHz	OFDM

Table 2. 802.11 network PHY standards

IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Operates at 5 GHz (less popular)	Operates at 2.4GHz radio spectrum	Combine the feature of both standards (a, b)	Its purpose is to improve network throughput over the two previous standards—802.11a and 802.11g
54 Mbps (theoretical speed)	11 Mbps (theoretical speed) - within 30 m Range	100-150 feet range	600 feet range
15-20 Mbps (Actual speed)	4-6 Mbps (actual speed)	54 Mbps Speed	54 Mbps Speed
50-75 feet range	100 -150 feet range	2.4 GHz radio frequencies	2.4/5 GHz radio frequencies
More expensive	Most popular, Least Expensive	Compatible with 'b'	
Not compatible with 802.11b	Interference from mobile phones and Bluetooth devices		

Wireless Network Working:

Transfer of data through a wireless network involves three separate elements the radio signals, the data format, and the construction of the network. Each of these elements is independent of the other two, so one must define all three when creating a new network. This is in terms of OSI source model, operating radio signals in the physical layer, and controlling many of the upper layer's forms of data. The wireless LAN components are a simple mode of operation [8].

So, after the energy delivery to access the network, equipped with wireless card devices points and while all in the operating mode, the following occurs:

1- The entry point is sent to the network electronic pulses on declaring itself regular intervals.

2- These pulses devices are picked up. They contain important information that helps devices to respond and create the same connection. The most important part in this information is known as (Service Set Identifier), which is known simply as (SSID). It is what distinguishes a wireless network from another.

3- Impulses referred to the channels that are working on wireless network and their features to protect the exchange of letters encoded within the wireless network using the encryption system known simply as (WEP). However, this encryption system suffers from several weaknesses that an attacker can exploit to enter the system and threaten the wireless network [6].

Wireless access point topologies

IEEE 802.11 operates in the three following modes [9]:

1- AP-based topology (Infrastructure Mode)

2- Peer-to-Peer topology (Ad-hoc Mode)

3- Point-to-Multipoint bridge topology

1- AP-based topology (Infrastructure Mode):

The client communicates through Access Point, also BSA-RF coverage provided by an AP, as ESA-It consists of 2 or more BSA and ESA cell includes 10-15% overlap to allow roaming [10].

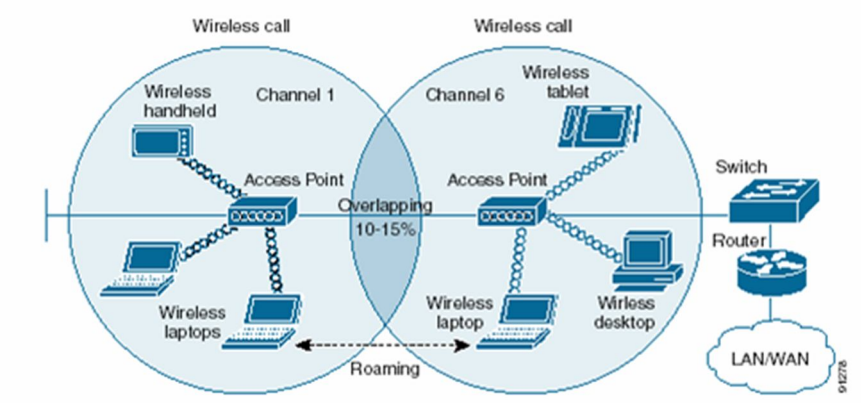

Figure 2. AP-based topology

2- Peer-to-Peer topology (Ad-hoc Mode)

The Client devices in a cell can communicate instantly with the others. It is beneficial for setting up of a wireless network speedily and simply.

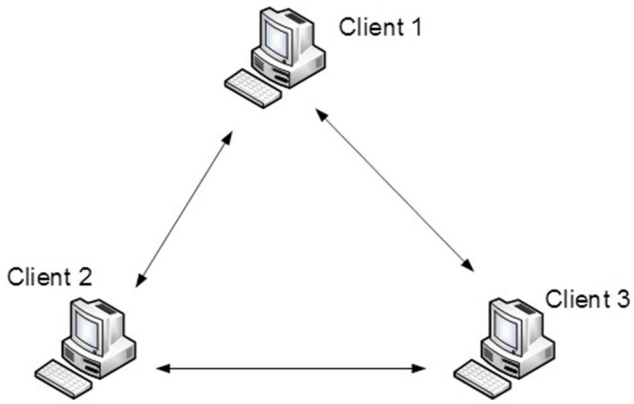

Figure 3. Peer-to-Peer topology

3- Point-to-Multipoint bridge topology:

This is used to connect a LAN (Local Area Network) in one building to LANs (Local Area Networks) in other buildings even if the buildings are miles apart. Certain statuses receive a clear line of view between buildings. The line-of-sight range different based on the kind of wireless bridge-whist and antenna utilized as well as the environment al efficiency [11].

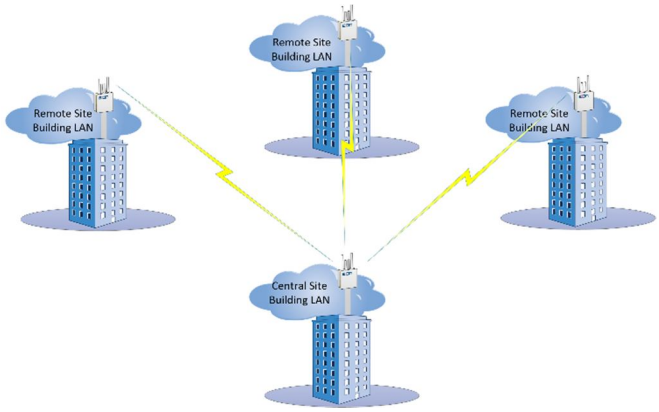

Figure 4. Point-to-Multipoint bridge topology

General Information:

Wi-Fi Security is to prevent unauthorized access or computers that use wireless disabled communication networks [12].

1- **Service Set Identifier (SSID)** is the primary name associated with an 802.11 wireless local area network (WLAN) containing home networks and public hotspots. Client devices utilize the name to name and connect wireless networks. On LAN Wi-Fi networks, a broadband router or broadband modem stores the SSID and allows administrators to change it. Routers can broadcast the name to help wireless clients find the network.
2- **Wired Equivalent Privacy (WEP)**: is a standard network protocol that adds security to Wi-Fi and other 802.11 wireless networks. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.
3- **Wireless Protected Access (WPA)**: is a security technology for Wi-Fi wireless computer networks. WPA increases on the authentication and encryption characteristics of WEP (Wired Equivalent Privacy)[13].

Hotspot:

Hotspot is a way to permit users to access specific network resources but does not give encrypted traffic. Upon Logging on, users can use almost any Web browser (either HTTP or HTTPS protocol), so they are not required to install additional software. Gateway, accounting and uptime, and the amount of traffic utilized by every client can also send this information to the RADIUS server. The Hotspot system might limit the deciding each particular user time, the total amount of traffic, uptime and some other features [12].

The Hotspot system aims to provide authentication system within the local area network (for LAN users to access the Internet), but it might as well be utilized to authorize access from external networks to get access to local resources (like authentication gateway to the outside world's access to the network). It is possible to permit users access to certain web pages without authenticate using the walled field feature [13].

CHAPTER 1

GENERAL INFORMATION

1.1. Security in wireless networks

This phase involves a deep understanding of the problem of the study, and the past research conducted in the same area. Literature Review is compiled through the collection of information.The main goal of the study is to provide the highest possible level of protection for the network and prevent any threats or attacks trying to access and damage it, and this is via performed the development of a new method to protect the network from any attackers.

Users can within the geographical network to a wireless network, open scale, non-encrypted sniff or capture and record, traffic, and unauthorized access to internal network resources, as well as on the internet, and then use the information necessary to disrupt performance or unlawful acts and resources.

Firstly, it is useful to describe the types of security threats and attacks. There are currently materially different networks, data networks and network simultaneously consists of a switch. The current data network consists of existing guidance on the computers, and the information can be obtained from a private source, like Trojan horse, planted in routers programs. A synchronized network which is made up of the keys does not buffer the data, therefore is not threatened by the attackers. Therefore, there is an emphasis on security in data networks like the internet and different networks that link to the internet. With a wireless network, one should consider the security procedures that will protect resources from unauthorized person. A summary will be provided of the reference model and the fundamental principles of the OSI network security through a review of wireless security in the context of IEEE 802.11 n WLAN protocol [14].

1.2. Characteristics of Security in Wireless Networks:

There will be a description of five security systems related to wireless networks like Confidentiality, Authentication, Integrity, Non-Repudiation, and Availability. and assessed later in the connection of wireless networks which have to be addressed when designing wireless networks:

1.2.1. Confidentiality

Confidentiality is a assure that the information did not reach unauthorized individuals, processes or devices unauthorized access to this information (protection from unauthorized detect of information).

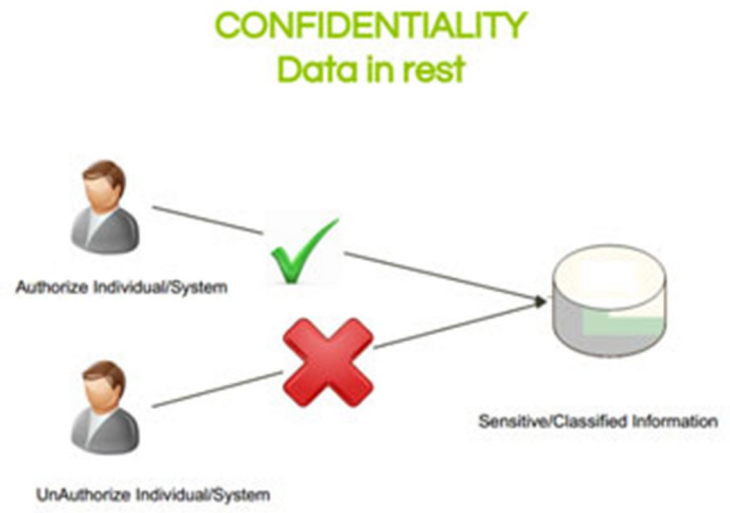

Figure 5. Confidentiality

1.2.2. Authentication

A security measure is to ensure the correct of the call, the message or the source or means to check the correct of a person to receive a particular classification of information or check the source of this information.

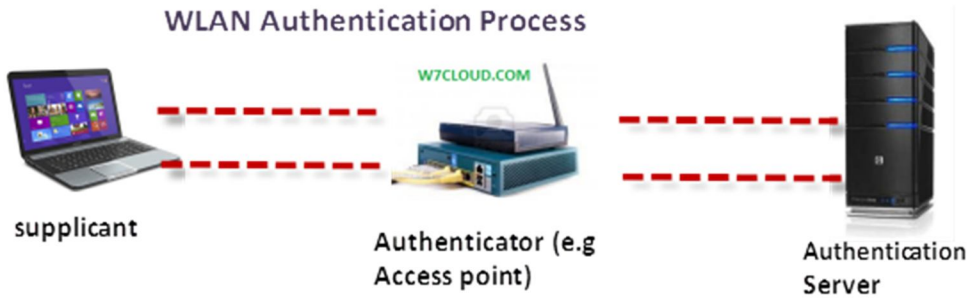

Figure 6. Authentication

1.2.3. Integrity

The quality of any information system reflects the validity and reliability of the operating system, the logical integration of the tools, software that provides protection tools and the extent of harmony IT infrastructure with the stored data.

Figure 7. Integrity

1.2.4. Non-Repudiation

Secure access to data and information services when needed by authorized person.

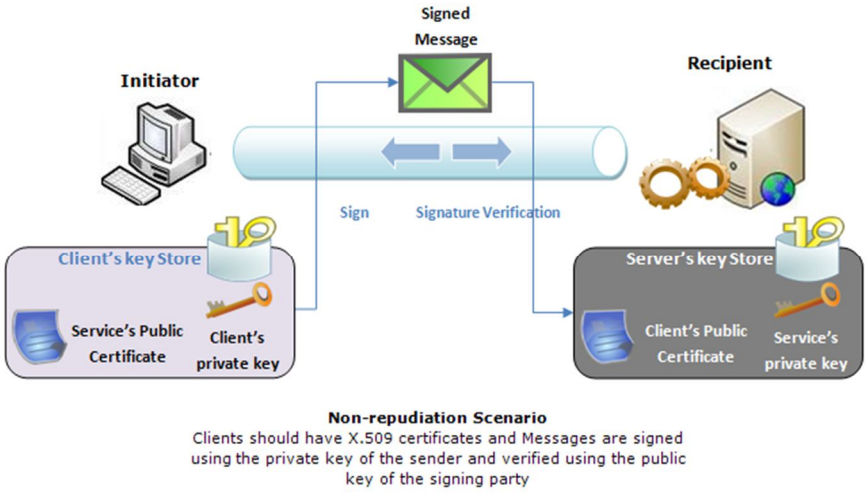

Figure 8. Non-Repudiation

1.2.5 Availability

Confirmation is that the data sender has got proof of the arrival of the data to the consignee and that the future has got to prove to the sender personal rejection, which prevents the possibility of any of the parties that he has dealt with this data.

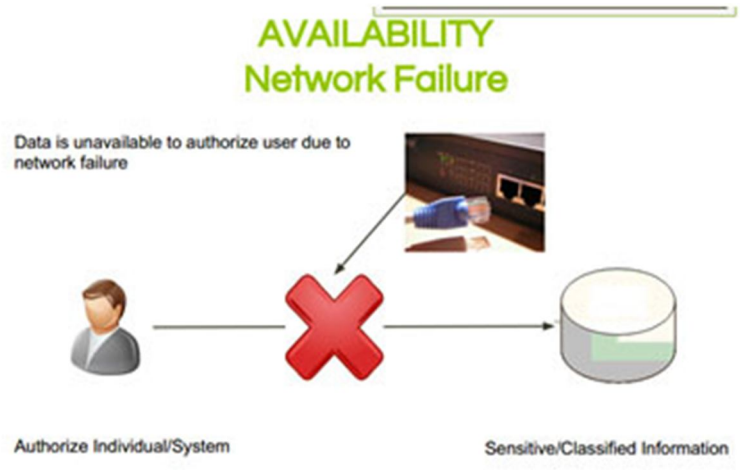

Figure 9. Availability

Supposedly, good designer for wireless networks is to think about how to set up each of these security features for networks. For example, encryption has prepared the mystery within the link level or within applications or services based on the Internet Protocol IP, and may send its SSID or a group. It may choose Identity using a protocol, IEEE

820.1X and can also be used gates or simple filter MAC addresses and physical and other fixed tools.

1.3. Types of attacks

The following are some types of attacks that can result from ARP Spoofing [15]:

1- Man-in-the-Middle (MIM).

2- Denial of Services (DOS).

3- Session Hijacking.

1.3.1. Man-in-the-Middle (MIM)

This considers an attack active eavesdropping. The MITM (Man-in-the-Middle) works by creating links to the devices of the victim and the transfer of messages between them. In these cases, the victim believes they communicate directly with another when in fact the communication flows through the host's performance attack. The end result is that the attacker host can not only intercept sensitive data but can also inject and manipulated in the data stream to get more control over his victims.

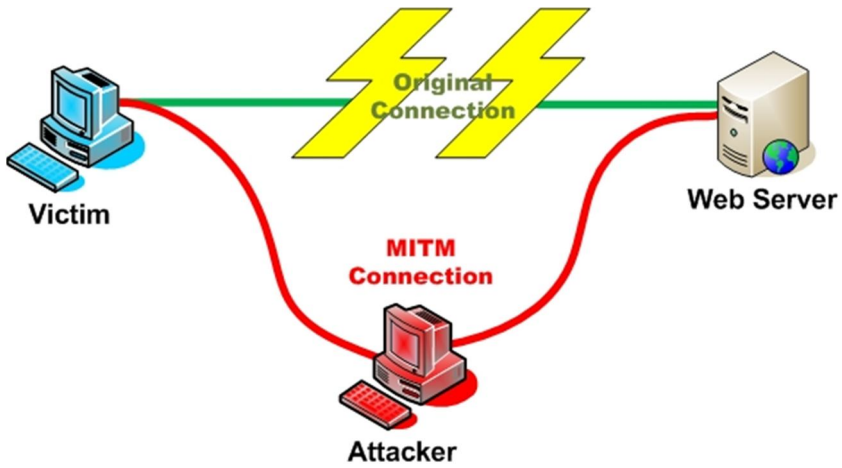

Figure 10. Man-in-the-Middle (MIM)

1.3.2. Denial of Services (DoS):

DoS is an attack when the system receives many requests, and cannot return communication with the requestors. The system then utilizes resources waiting for the

handshake to complete it. Finally, the system cannot respond to more requests requisition it without service.

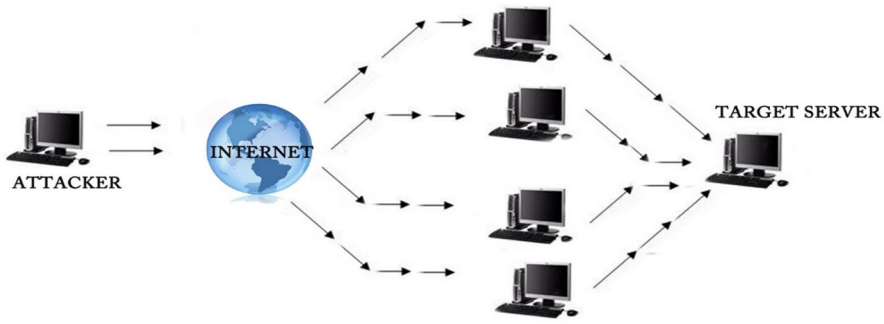

Figure 11. Denial of Services (DOS)

1.3.3. **Session Hijacking:**

Session Hijacking is the action of getting control of a user session after successfully getting an allowed session ID. Session hijacking includes an attack using obtained session id to grab control the legitimate user's web application session, while that application is yet in progress. Session hijacking gets a position in the transport layer from the network layer of OSI model.

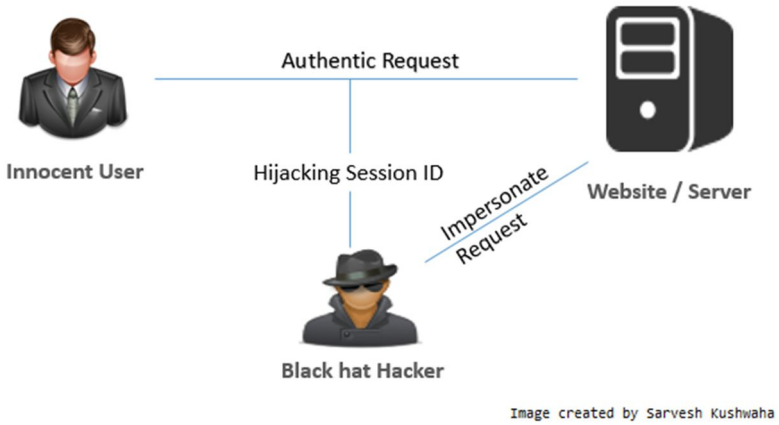

Figure 12. Session Hijacking

1.4. Sniffing

Sniffing is eavesdropping on the network and packet sniffer is a piece of Programs that grab all of the flow of traffic to and from the PC connected Network. It is available for several platforms in both the commercial and open source differences. Sniffers are also engines to other programs. Storming detection systems (IDS) use sniffers to match packets against the rule set aimed at knowing anything harmful or strange [14].

Sniffer software allows users to view all network traffic more than any network interface connected to the host machine. Sniffer program can watch TCP, IP, UDP, ICMP, ARP, and RARP. Sniffer also lets one see the port specified password for monitor HTTP, FTP, Telnet, etc.

Also, a sniffer can grab anything sent across the LAN, including:

- User IDs and passwords
- Web pages being visited
- Email messages
- Files shared using the Network File System
- Chat sessions
- DNS queries

1.4.1.Types of Sniffing

1.4.1.1. Passive Sniffing

Sniffing worked on a hub is known as passive sniffing. In Passive Sniffing, data is sent over the LAN to each device connected to the LAN. Thus, the smell will be able of collecting data posted to and any from another system on the local network [14].

1.4.1.2. Active Sniffing

When sniffing is performed on a switched network, it is known as active sniffing. Looking for a MAC address associated and sending only the data required to connect to the switch. Therefore, the sniffer will be able to see the data in and out of his machine

only. And all other information of interest that flows on the LAN is unavailable to smell [14].

1.4.2. Detection of Sniffers

1.4.2.1. The DNS Test

Creating is created is several false TCP connections on a network section, expecting a badly written sniffer to pick up on those connections and resolve IP addresses of the non-existent hosts. Some packet sniffers work reverse DNS lookups for packets it captures. When reverse DNS lookup happens a sniffer detection device sniffs the lookup request to see if the victim is the one requesting resolution of the nonexistent host.

1.4.2.2. The Ping Test

This method relies on a problem in the target machine kernel. An ICMP echo request can be constructed with the IP address of the machine suspected of hosting a sniffer but with a deliberately mismatched MAC address. An ICMP echo packet is sent to the target with the correct destination IP address, but a spurious destination hardware address. Most systems will disregard this packet since its hardware address information is incorrect. But in some Linux, NetBSD (Berkeley Software Distribution) and NT systems, since the NIC is in illegitimate mode, the sniffer will grab this packet of the network as a legitimate packet and respond accordingly. If the victim in question replies to the request, it becomes known it is in illegitimate mode. Smart attackers are of course informed of this, can update their sniffers to filter out such packets as the NIC itself would have had it not been in illegitimate mode [15].

1.4.2.3. The ICMP Ping Latency Test

The ICMP (Internet Control Message Protocol) into this method pings the victim and sees the round-trip time (RTT), from there. Hundreds of false TCP connections on a network segment are created at a lightning rate. The sniffer is expected to deal with those packets at the rate which will improve latency victim organ network. Then the victim has pinged once again and compared with the RTT this time with the first time. After series of experiments and percentages, it can be concluded whether sniffer is indeed running on the target.

1.4.2.4. The ARP Test

An ARP request is sent out to the victim beside all correct information except a false destination hardware address. A device that is not in diverse form would never notice the packet since it was not destined to them, therefore it wouldn't return. If a device is in diverse form, the ARP request would be seen and the kernel would process it and return. Through the device replying, it becomes known it is in diverse form.

In this project, work has been done on IP and Mac Address in order to protect the network from attack and penetrate through the address resolution protocol (ARP) when it is doing its job within the network. Therefore, it is important to know how it works and how the attackers can circumvent it and penetrate the network through it. As such, it becomes possible to enter into the heart of the project and to find out the mechanism and the algorithm that are designed to strengthen and protect the network.

1.5 Address Resolution Protocol (ARP):

ARP is a protocol used by the IP network layer to map IP addresses to hardware addresses that are used by the data link layer. ARP works at the network layer as part of the OSI link layer and is utilized when IP is utilized over the Ethernet.

Table 3. Format of ARP packet

Attribute	Size
destination address	6byte
source address	2byte
ARP request/replay	2byte
type	28byte
fill	18byte

There are two types of addresses that are used to uniquely identify a host:

1.5.1.MAC Address

It is identified by various names hardware address, LAN address also physical address, or Network Interface Card (NIC) address. Every computer’s network interface card is

selected a globally unique six-byte address by the company that manufactured the card. This is the source physical address utilized by the host network interface. When a host sends out an IP packet, it utilizes this source address and it receives all packets that meet its own hardware address or the broadcast address. This Ethernet address, typically the 48-bit address, is a link layer address, based on the network interface card managed.

1.5.2. IP Address

IP operates at the network layer and is free of the hardware address. The IP address of a host is a 32-bit address specified to a host and is either static or dynamically specified by Dynamic Host Configuration Protocol (DHCP).

When an Ethernet frame is broadcast from one device on a LAN to another, the 48-bit MAC address is utilized to define the interface for that the frame is designed. The device driver does not ask the destination IP address of the IP datagram for the resolution of the address.

1.6 Literature Review

There are Various researchers have given a good job and try to prevent the attacks in ARP, until the present, there are numerous solutions for ARP attacks to prevent the ARP cache poisoning attacks, also provides the solution for security of ARP, still, these solutions have some shortcomings that cannot be permitted by the network communication tool, these solutions, and their shortcomings [17].

Note that the subject has been in the works by researchers in the field of network security, the following is a summary of these studies:

ARP Spoofing attacks remain as one of serious security threats on the local area network.

According to the study [18], the author proposes a mechanism query process ARP which is compatible with Mac and IP addresses current list on ARP protocol. This can provide effective protection against the attacks of the ARP spoofing by allowing operating systems independent implementation of the process of verifying the

association the IP/MAC exact by following protocol RFC826, using the shape of the current package ARP.

Continue to focus on the IP/MAC mapping query mechanism within the local network, the characteristics of networking to determine the management mechanism of the hosts at the LAN. The specified host's administration in the network can be utilized to ensure network security and they can also be utilized to build a management mechanism that can be utilized to connect all hosts on the LAN. ARP is created to operate without problems in general environments. However, as it does not have security measures facing malicious attacks, an attacker can impersonate another host utilizing ARP spoofing or access critical information.

As stated in [19] this design detects ARP attacks through real-time monitoring of the ARP cache record and a routing trace and protects the hosts from attackers through ARP Link Model Control which changes from dynamic to static. In addition, it can resolve problems like host position, man-in-the-middle attack, and the block of the host. the proposed scheme does not require an ARP protocol change or multiple encryption algorithms, further, it does not cause high system load.

Despite the various solutions offered according to this study, new attack techniques can still cause new security problems, since the ARP protocol has some fundamentals vulnerabilities. Hence, further investigations on solving the basic security vulnerabilities of the ARP protocol are required. Still, the data link layer performance and security problems are not sufficiently addressed yet. The problem was found in the link between IP protocol and Ethernet protocol. Those two protocols are not completely suitable and not created to work correctly with each other.

As stated in [20] the current design of the identifying architecture may utilize the main issue of the problem, while weak principles in using MAC address were named. This link needs to be improved to increase the performance and security in the data link layer. It is proposed to make a reduction on the naming architecture design. In this scheme, Layer 3 address is utilized as a flat address for both Layer 2 and Layer 3 instead of utilizing fixed media access control (MAC) addresses. Further, this architecture decreases the function of ARP in the unicast data traffic.

As given in [21], to avoidance the issues of certain 2 protocols, a scheme of adaptive routing protocol is proposed to depend on Cuckoo search algorithm (ARP-CS). ARP-CS technique ensures road protection service quality which is the most objective of transportation systems. It utilizes two main procedures to deal with the different density of VANET. When the network density is low a geography-based routing approach is performed. in addition, a topology-depend routing protocol is performed. It is worth seeing that this protocol can apply the two procedures at once based on the network density. The test results here show that the proposed method outperforms the exiting routing protocols. Sniffers pose huge threats in the monitoring and verification of traffic on the internet. It is essential for the effective work of computer networks in any organization. Sniffer helps network monitoring, as well as the seizure of passwords used in communications telnet, login and FTP. It examines and sniffs travel package through a network without changing them. Sniffer translates packets captured and allows network administrators to understand, analyze and retrieve useful information from the package content. In addition to being a boon for the organization, it is also used sniffers pirates for indulging in malicious acts of piracy and account systems other users.

As mentioned in [22], the focus is on the development and implementation of a new sniffer named Analyzer that explores briefly the protocols used in the packet analysis. The results of the implementation Analyzer create the encrypted database of the beam front and displays the front end displays appropriate information according to the user's wishes.

The analyzer is an application that can be used in the field of network security. The network can be a local network or the internet. The point of the design of cash is the purpose for which it is used. Depending on the intention of the user, the tool can act as a management tool for the maintenance of networks or wicked purposes by the attackers to get unauthorized access to remote hosts. Message listening tools inhalation is impossible to detect because they are passive in nature, this is the only collect data.

The attacker usually makes the performance of the ARP protocol’s stateless characteristics to carry on the ARP beguilement and causes great harm to the security of networks. The research method and prevention policies of the ARP Spoofing as stated in [23] introduce the commonly used ARP spoofing methods such as internal/external

network sniffing, the interception and malicious attacks. It presents the Matching IP design, Data monitor design, Echo time design, ARP reply analysis design, software tools detecting design as well as the new method of ARP cache updating.

To fundamentally solve the ARP Spoofing is more complex and needs to consider integrating the technology and the management in the actual network environment to minimize the risks posed by ARP Spoofing. Many people and companies trust wired connections, way more than wireless. A man dressed like an electrician with a strange box of wires and tools should never be underestimated.

According to the study [24], it proposes a concept of the device for not detectable interception (and modification) of the transmitted information through the Ethernet network. To prevent data leakages, like technologies as SSL, SSH, VPN, and others for privacy should be used. Even with developed prototype hardware, somebody can remotely sniff confidential information, examine network for vulnerable machines with common tools for analysis, do some basic DoS attacks, use unsecured (not protected by password) network resources (SAMBA, FTP, proxy) and of course internet access (upload successfully captured data).

There is no unique and stable method for these types of attacks. So, the need of that kind of method is still an open issue. As stated in [25] for that type of ideal solution some conditions should be considered and it should be widely available, easy to implement and it should follow all the basic aspects of network layer principles. Furthermore, it also should be backward compatible to address resolution protocol (ARP). An ideal solution should use minimum cryptographic function so that its performance is good enough.

In [26] MAC address, ARP cache poisoning will create the entries constant and the attackers will not be able of applying ARP spoofing in the network. This entry is made utilizing windows command quickly like ARP-sip_address mac_address. But, this method is not suitable for big networks as it would be very complicated for the network administrator to manage and update these tables throughout the network.

As given in [27] offers a secure version of ARP that gives security against ARP poisoning. every host has a public/private key pair certificate by a local trusted performance on the LAN, which operates as a Certification Committee. The Messages are digitally signed by the sender. hence, preventing the injection of fake or snooping information.

According to the [28] New modified techniques are proposed which could efficiently secure our ARP against the attacker and protect important data from being sniffed both internally and externally. The efficiency of these methods has been shown mathematically without any major impact on the performance of the network. The main idea behind how these methods work and proceed to achieve its task has been explained with the help of flow chart and pseudo codes. With the help of various tools ARP cache is being monitored systematically and if any malicious activity is encountered, it is intimidated to the administrator immediately.

As mentioned in [29] focuses on comparing various techniques that are utilized to protect the users from these attacks by providing practical notes based on a network parameters time, and scalability and highlighted the valid method, in the end, to fight the attacks at a superior level. Moreover, in [30] Network intrusion detection systems (NIDS) usually rely on accurate string matching techniques. Depending on the selection of algorithm, implementation and the frequency with which it is applied, this model matching will enhance a performance bottleneck. also, to increasing network activities and traffic, NIDS can get the benefit of high-level string matching algorithms. it has been describing the effectiveness of a significantly quicker method to model matching in the open source NIDS Snort.

As stated in [31] give the solution and implementation features of it in a flows-based networking subsystem. the solution includes two sections a "bump in the stack" flows module and the split-up Stream with a driver and user-level application. also, presented the algorithm that is done by the module and utilizes to stop ARP cache poisoning anywhere possible and to detect and raise alarms otherwise. it has been then discussing some limitations with our approach and present some preliminary performance figures for our implementation.

As given in [32] it has been analyzing the ways that SSL stripping can be utilized by attackers and present a countermeasure against such attacks. it has leveraged the browser's history to create a security profile for each visited website. Any profile contains information about the exact use of SSL at each website and all future connections to that site are verified against it. It has shown that SSL stripping attacks can prevent with accepted overhead, without help from web servers or trusted third parties.

As stated in [33] It has been considering three critical and unique attack models, namely dynamic pharming, deceptive captive portal and SSLStrip attacks, and it is shown that there is no single defense solution except SSLock. it has conducted employability analysis which further justifies the proposal in terms of its high unit rate. SSLock is the just method that is practical and light-weight for application trade, opt-in and zero-initialization for service providers, and privacy-preserving for generic users.

According to the [34] The attacks can be detected by the protocol, if a client receives a reply from a website without every protocol header or just only HTTP header. Its principal drawback is that it is a client-side detection system and can just be utilized to detect the SSL stripping attack.

Anticap, as stated in [35] the ARP reply and check it with the MAC address before stored in the ARP cache. If this MAC address is determined to be different from the already cached one then it detects whether that address is still alive. If that MAC address is found to be alive then this new update is ignored and it is also added to the list of banned MAC addresses. Its weakness is that it trusts that the ARP entry already cached is the allowed one which creates a critical condition of a race among the attacker and the victim. If somehow, the host cache is updated with faked ARP entry before the actual host could update, the allowed user gets banned under such circumstances.

AntiSniff application, as stated in [36] It has been operated by sending a set of nicely made packets in a particular request to a victim system, sniffing the results and performing the timing tests against the victim. By measuring the timing results and observing the victim responses on the network, it can be determined if the victim is in promiscuous mode.

As given in [37] It is a non-cryptographic method. In MR-ARP if any new IP, MAC binding request happens then the genuineness of that request is verified by voting and if more than 50% response comes into the service of that binding then only the binding is accepted. If no reply will come then it has considered this binding as true that's why any other node is not voting against the node and the binding will be accepted. This requirement can be satisfied in the Ethernet, but maybe not be correct in the wireless LAN network because of the traffic rate agreement based on the signal-to-noise ratio (SNR).

The flaw is that some of the solutions have no backward compatibility option, some of them utilize cryptography to exchange encrypted data which is not achievable because it takes a long time in encrypting the packets and few of them utilizes the server middleware-based solution what has the large flaw that a single crash of server that may lead to failing in communication.

Table 4. Comparisons of Different ARP Prevention Methods

Scheme	Method	Advantages / Disadvantages
Static Cache entries [25]	Utilize of static ARP cache entries.	Simple method but not appropriate for big networks.
S-ARP [26]	Signed ARP messages utilizing public-private keys.	the fiasco of third-party leads to failure of the whole network.
ARP Watch [27]	Observes the traffic and operate alerts based on the rule.	Free but produce high number of alarms thus increasing work of the admin.
ARP Guard [28] [29]	Sniffing and generating alarms based on the rule.	Seems to be good but costly.
Dynamic Detection Approach based on Snort [30]	Sniffing and generating alarms based on the rules.	Free but increases the work of admin by generating high number of alarms.
Middleware Approach [31]	Block unsolicited replies and generating alarms based on the rule set.	Not a practical approach as it requires changes on all the hosts.
HProxy [32]	Client-side recognition method for SSL striping attack.	Does not give any protection only detects.
HTTPSLock [33]	Protocol validator that will redirect the user to an error page in case of bogus certificate.	Depend on client-side detection.
Anticap and Antidote [34]	Mechanism used to block ARP replies.	Blocks ARP reply having MAC Receiver different from the one in the cache but suitable only for specific Kernel.
AntiSniff [35]	Detecting the node currently running in loose mode.	Detects the node but requires constant monitoring and scanning.
MR - ARP [36]	Extended version of ARP to prevent attacks based on the concept of voting.	Might not be valid in 802.11 networks due to auto rate fallback.

In this project, the following tools and requirement are used:

1- Kali Linux system. (2 computer)
2- Python programming language.
3- WinBox
4- VirtualBox
5- Mikrotik Router
6- Widows (computer)
7- Access point
8- UTP wire

CHAPTER 2

MATERIALS AND METHODOLOGY

2.1. Introduction

The application has been designed for the purpose of protecting a particular system or certain building belonging to government or any other agency from the process of penetration and espionage when such process is not permitted on the operations of illicit penetration testing. This application is designed for PCs, workstations or services. However, in the future it can be modified to work on Mobile. It can, through mobile, run the application to protect.

2.2. The Materials Used in Project

The two applications are developed to detect any threats or attacks against the networks, prevention of these malicious ways of the access to the router.

Today the damage of the thing being moved within the Internet is a packet. That packet within the internet can be carrying a different set of data, and such data is possible to be, for example, massages and content of the message. For instance, such transfer happens when data moves from one computer to another through e-mail.

Before talking about or entering into the subject of penetration, there should be a simple overview of the communications taking place and how, through a router, computers can be connected with one another and in ranges of different IPs. For example, if there are two computers and each computer carries a range of different IPs, here comes the task of the router is to guide any work routing process.

What is the problem today in the field of large networks? Note that there are many penetrating programs and operations also being used to attack networks and penetration testing. For instance, if a computer has Mac system and is connected to another computer on a network, the IPs will automatically be recorded through a protocol called ARP. This process will basically tell Mac that it wants to link to the network but does not have IP, so it will require Mac to provide the IP to start the binding process.

ARP is very important in connection of two computers, whether they are from the same range of IP or two different range, but connect themselves through several routers or one router. The ARP is the one that gives the IP network address, it cannot connect any computer to any network [38].

Nowadays, it is important to note that there are a lot of applications and programs that do scanning, sniffing, and spoofing within the process of penetration and reconnaissance which is the first process in which an attacker gathers the information that could enable the attacker to enter the network, because it will recognize the weaknesses and doors points that can be accessed as well as the IP of users who are in the network. It is known that it is not the normal user who has the right to know all these information [39].

Since the ARP can obtain all the IPs, it is very easy to manipulate the owner's information. Each owner has a computer with Mac fixed. But this Mac can change on the computers.

For example, the protection is present within the network and the network consists of four computers, computer dedicated to employee information technology, another director, another supervisor, and another student. Naturally it is the powers of the Director which are much more than the student and the rest of the staff. If it is assumed that seven of the director powers to manager and a user put Mac student instead of Mac manage, there will be higher demand for the validity of this process. For instance, in the case of a breakout, there would be a lot of issues and sabotage within the network.

So, there is a need to make networks more secure, not in this case only, but there are plenty of cases in which problems happen after obtaining the IP through many special infiltration programs as mentioned.

What are the methods used by the hackers in the penetration process? To answer this question, understand, it is important to know how connection to the internet occurs. Whichs can be occur either via Ethernet cable or Wi-Fi. Wi-Fi is more dangerous because it is possible for a hacker to be outside the building or close to it while attacking and the hacker will be completely unknown. The first step in attacking is a reconnaissance or the gathering of information through the use of applications to obtain such information. Most of these applications use a protocol or technical ARP [40].

Experienced hackers always use reconnaissance process mentioned earlier for information that will enable access to the router. When they get to the router, they can manipulate the entire network.

The applications will block IP and MAC attacker, who will not be able to connect to the router again. The attacker can use the ARP but cannot access the entire router.

2.3. The Components in the Applications

2.3.1. Kali Linux

Among the most updated and greatest of all versions is Kali. It is popular Backtrack Linux penetration testing distribution. Kali has been kept in a format very similar to Backtrack due to the works of the creators of the Backtrack series. This makes anyone who is familiar with the older Backtrack platform use the system conveniently.

Kali was developed from scratch and updated to have most features rich Ethical Hacking/Pentesting distribution available. Kali is able to operate on more hardware devices, thereby increasing the options for computer security penetration testing.

Security testing tools are over 300 in Kali. Attention was given to eliminate redundancy. So, many tools from Backtrack were eliminated. The user can access the tools quickly as they are clearly visible in the menu. Moreover, all the tools are very well organized in

the interface. Kaldi's tools can be used by a user the same was a hacker would do. This is done to test the security of the system. This is to taint the user so a potential hacker can be detected [41].

Moreover, the Python language is very easy with many applications. It is very well built. The language is high quality high-level o.o.p (object-oriented programming). The system processes the same way as many libraries that will help the designer or developer in his work. Moreover, it has been dedicated to penetrating the libraries as well as for protection at the same time as possible to work out many tests in order to determine the offices that are possible to be used in the application.

2.3.2. Python

The aim of Python is to provide dynamic language that are easy and understandable. Its name sound comical and it should be.

Python sets the difference between data groups in terms of string and number. What is meant by string is characters or words or even whole text. For numbers, they could be natural or floating. Substantial work has been performed by Python community. They managed to adopt and approach to almost all issues. The material is open source on the net [42].

After selecting the programming language, Python, one must choose the system that the application will work with.

If a single System, Windows or Mac, is used, all private libraries inauguration should be in Python. Moreover, the penetration testing programs should also be included. Therefore, a long time is needed. The Linux system is called Kali Linux and is dedicated to penetrating and to examine. This make is a ready environment for the application. It contains many programs that are used to penetrate, spy on, examine. This makes the designer or developer know how much power to apply for defensive strength and the face of these programs as well as prevent any penetration from happening in the future. So why not choose the second system and the installation of all these programs and testing tools which automatically found in Cali Linux, as well as even the language

of Python automatically be down 2.7 edition. After choosing the language, one should also select any library to analyze the packet and data within the network. One can also listen to anything happening within the network. Upon extensive search, one would find that there is a very nice library, a library of scapy.

2.3.3. Scapy

Through Scapy, one is able to send, sniff, and knows the nature of network packets. The program can facilitate the creation of tools to investigate as well as attack networks.

That is, Scapy is a handy program with a lot of impact power. It can understand and deal with packets of different types of programs, send them to the wire, seize them, and correspond with them. Most classical tasks can be handled by Scapy with ease such as tracerouting, unit tests, probing, scanning, network discovery, or attacks [43].

Library of Scapy provide us with so many things and resources used in the analysis of the process packets for any possible disclose in any case of a request ICMP or any case of a request convergence or any other case of TCP or UDP. It can show in full detail and also can display the packets that have been sent and the number of packets. In the library, you can see all the movements and things that occur within the network. After selecting the library in Scapy and the application targets the network of state of the ARP protection for most of the giant software such as Nmap, Ettercap which is the basis of its work depends on the ARP and it will use part of the ARP from a library of Scapy, because this library provides follow-up to the ARP.

Next comes the sniffing process or listen to any user who requests the ARP within the network. In this case, the application for any user working ARP will show the IP and the MAC detection. The application will determine if the person intends to attack the network because of what he wants to get, such as all the information inside the computer. Such an action is not valid or allowed for such a user.

If there is no sniffing, the application will return to search again, or it will find a user who works ARP within the network. The application will obtain IP and Mac of the attacker. The application will order the block on the attacker to prevent him from

entering the router. In case the attacker enters the router, they can act as the owner and stop all users from entering the router. The attacker can also remove and tamper with important information within the router.

2.3.4. Nmap

What is known as Nmap (Network Mapper) is an open and free source utilized to determine and secure networks. Nmap is considered helpful by several systems and network administrators to perform tasks like network inventory, managing service upgrade schedules, monitoring host, and service uptime.

Fresh IP packets are utilized in unfamiliar ways by Nmap to discover what hosts are available on the network, what services those hosts are offering, what operating systems they are operating, what system of packet filters/firewalls are in utilize and several other functions. Nmap is programmed to scan huge networks. It was created to quickly scan huge networks but works well against single hosts. It also works against single and tiny networks. Further, Nmap is harmonious with and works fine on all major computer operating systems as well as on official binary packages that are available for Linux, Windows, and Mac OS [44].

2.4. The Methodology of Application I

The final flow chart of the suggestion system is shown in figure 13. The purpose is to protect any network using the application by every user that the application is tied with the network so that the process of convergence process detects any illegal possible attack that occurs within the network.

Server type is chosen as the mikrotik because it is more popular after Cisco in the world in terms of internet use. It has been used heavily whether in Iraq or the Arab world.

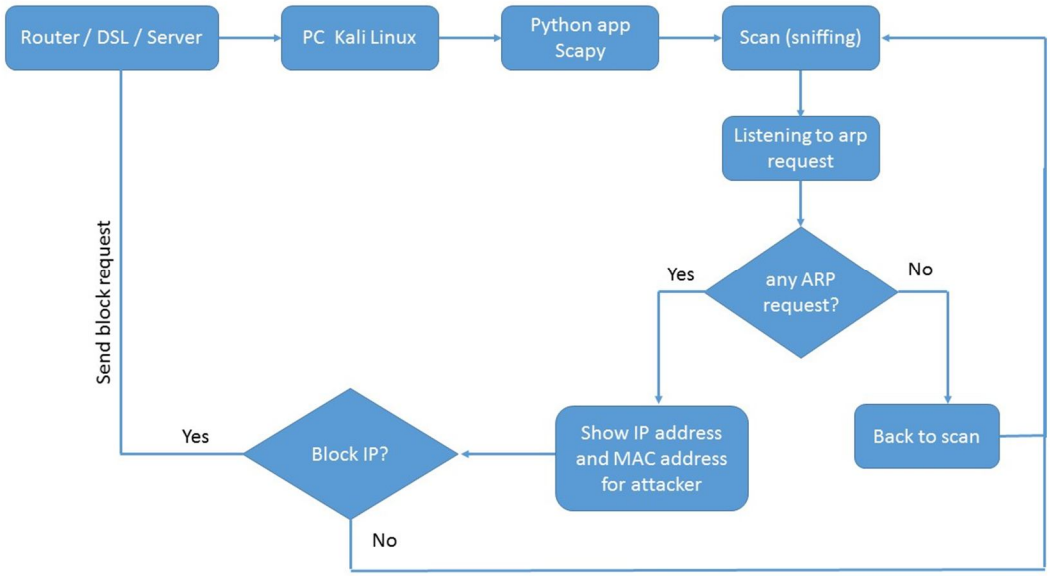

Figure 13. The First Application flowchart

The second main issue in the application is the environment which will be designed. It is known that there are three types of key systems which are windows, Mac, and Linux. A server system will possibly be one of these systems. The appropriate language for this thing, Python, is be used. They Multiplatform, meaning it supports all platforms, for example, if the application is designed for Linux, it is possible to be used in Windows and Mac, and the meaning of the designer more accuracy is not specified in a specific system.

2.5. The Methodology of Application II

The final flow chart of the suggestion system is shown in figure 14. The purpose is to protect and prevent any atttack against network, which will be uses by the admin. The application is aske to send command to block all ports detecting scan requests and ARP request or access to router within the network.

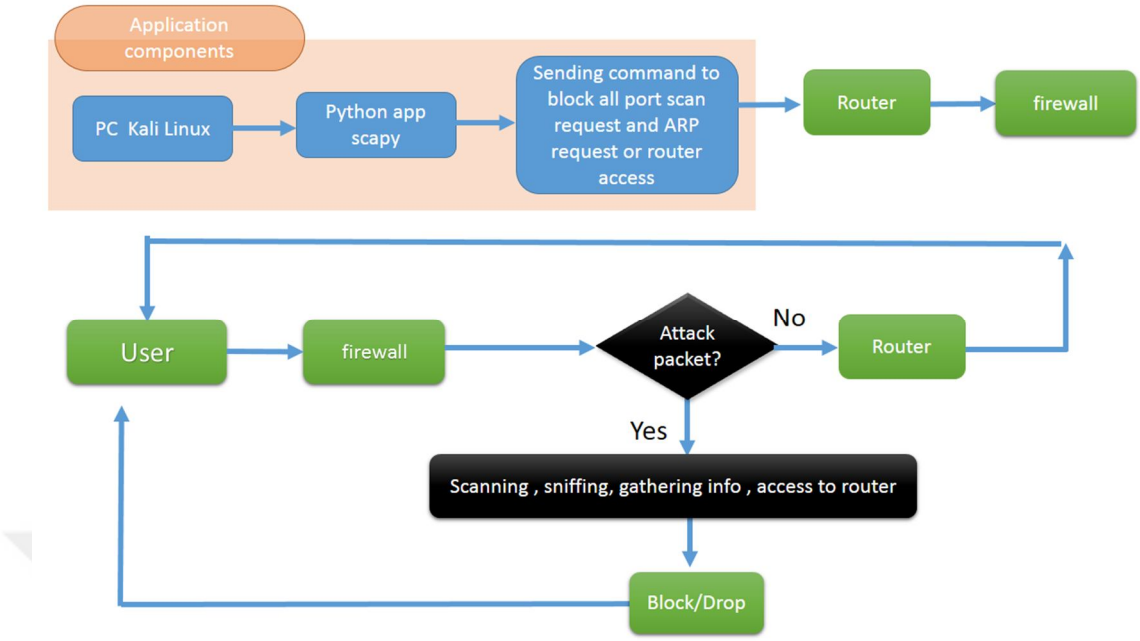

Figure 14. The Second Application flowchart

The main differences between of the two applications is, the first application works to detect the attacker and send an alarm or notice to the supervisor, and is known the supervisor is human being can not stay all the time monitoring the traffic within the network, There is an intelligence in the second application and processes from the first moment of running and thus there is a kind of simulation between the devices, which reduces the effort on the supervisor and also closes all doors to the attacker, who cannot collect the information, which is considered the first step in the attacks.

CHAPTER 3

EXPERIMENTAL STUDIES

3.1. Introduction

It should be noticed that before the implementation and uncovering, the attacker could have entered the network and access a lot of information. can be done through the use of Nmap. It would be possible to see the penetration tools used by this program and how the attacker can access significant amount of information when using such program.

To explain the proposed, it is important to know that there is something called scanning and gathering information spoofing and poisoning. It is possible for others to take advantage of this situation. When entering the field of networking and a specific network, the most dangerous thing to face is an internal attacker as opposed to an outside the attacker because the latter will need to work set-ups in order to enter the network as it is downright in front of a firewall and a lot of barriers must be surpassed in order to for the outside attacker to be able to penetrate the network. Internal attacker already exists within the network and knows the password and many more about the network.

To protect against such attacks, the presence of a defense plan is required. Such a plan defends the network and protects existing users within the network from any person who attempts to penetrate Mann as being MITM (Man-in-the-middle attack) or poisoning or spoofing or ARP [45].

There is a question about the nature of ARP and the router as well as the possible use by any user. Why should attacks of spoofing or poisoning or MITM be allowed? The network should be available only for authenticated users.

When using in the Nmap program, the reconnaissance that get in Ethical hacking which they call passive attack (called passive Attack any sense attacking positive non-harmful, the attacker reconnaissance and gather information without the process of attack and penetration carried out, only the gathering of information) gathers the information. For example, it should be asked how many open computers there are and how many ports are open and what kinds of existing systems there are. All of these things should be known by the attacker in order to see where the weaknesses through which the attacker can penetrate the network or through any important weapon used to penetrate [46].

So, the answer becomes obvious now to the question above, what already allows the attacker to reach this stage. When it is revealed that the case is spoofing and the attacker had arrived, took all the information, and the potentially broke to some user information, it is important to stop him.

The application in the first step is to give warning as an alert that there is a person who uses ARP as it is also known that ARP is used between computers and the internet and there is no problem with that. However, when the normal user within the network using ARP of course this user cannot use it, for example, a person or an ordinary employee in taking Internet Company and uses it in his work but enters the network and gathering information. It is important to know the reason.

To protect the network from such cases, this application is designed to support the process of listening the network. If convergence for all users is heard out, the application will reveal the process and thus work to block possible attacks. The application will work through private IP as well and will possibly identify and stop the attacker who can be an engineer in the same company or a stranger person.

Thus, the concept of the main application is to prevent any case of attacks to gather possible information that occur in the network for all kinds of attacks that have been mentioned earlier. When the attacker is crossing the reconnaissance phase and gathering

information, the application will cut off the road from the beginning to prevent anyone trying to do the process of collecting information or reconnaissance. The application will detect and block access to the router. The application will provide general protection for the network as a whole. It will also prevent even passive attacks even if the attack is not harmful to the network [47].

Note that there are a lot of programs that reveal the attacks that happened. The application does disclose the attack before entering the network and accessing the information. In other words, the function of the application is prevention, not treatment because the treatment is possible to take a long time. For instance, in the event of an attack, there will be a need to reset IP users and check into any possibility that private information has been stolen the users such as bank accounts or important documents. As such, prevention is better than cure.

3.2. The Proposed Algorithm (Application I)

The detailed algorithm steps can be explained as the following:

Output: Attacker Information (IP, MAC)

Step1: Include a set of libraries that will be used in the application.

Step2: Create function working on the implementation of GUI, then set up three labels, the first to information attacker and the second of IP Address and third Mac Address.

Step3: Function working on the implementation of ssh connection.

Step4: Create function for ssh connection.

Step5: Set up a dictionary and that the idea is to save the two variables or values and including the application that will store IP and Mac.

Step6: Create a function that will monitor any ARP condition that occurs within the network, take the argument on the packet, and obtain information of the attacker (IP, MAC).

Step7: Create a taste function that works inside on sniffing. This sniffing is running the arp _monitor, and the presence of the filter to see only the ARP with all information inside the packet.

First, call Python necessary libraries and the application would work out as follows:

Tkinter: this library is used to call up images

Scapy: is a library that operates on the basis of the application.

Paramiko: is a library that is used in order to set up ssh connection.

In step 2, The function is working on the implementation of GUI that will start when any ARP operation is running inside the network when the application is running.

Then set up three labels, the first is to information attacker and the second of IP Address and third to Mac Address determine the characteristics of each label in terms of name label and background color, font size, font type foreground color of the label. Late, these characteristics are grouped and located inside the window and through the identification of values of the X and the Y.

In step 3, The function is working on the implementation of ssh. Here, one can take the argument (IP, port, username, password, command), and send it through ssh.

After that, it defines a variable root1 which is equal to that order so as to set up a new window through which the attacker can be identified and the IP and Mac are named victor, to quantify information, and identify the offer value and longer and be non-telescoping zoom. The process then determines the background color which is white which exists from the application.

Then set up labels and determine the characteristics of label in terms of label name (Done Successfully!) and background color, font size, font type foreground color of the label. All of these characteristics are grouped and locate the label inside the window and through the identification of values the X and the Y.

After that, a button bears the name of Block Host starts working by simply pressing it implementing Mikrotik function to send it forward with information to the router via the SSH connection as mentioned above in order to give block the attacker. It is also specifying the name and background color and font size, and it includes the function name and the Select button from the site by giving the values of x and y.

The work also bears the name of a second button (cancel) to cancel orders and get out of the program. It is also specifying the name and background color and font size, and it includes an end to the work of the application and determine the location of the button by giving x and y values.

In step 4, SSH function will take (host, port, username, password, command), and this was taken from a library of paramiko or Python libraries, to be used to send the command instead of the user.

Note that the error does not appear in the application interface but only in terminal because it should appear for the developer and not for the user as it is part of the work of the developer.

In step 5, Set up a dictionary and that the idea is to save the two variables or values and including the application that will store IP and Mac. The dictionary takes two values for the key variable it will be regarded as a key IP and Mac as a variable or can specifically does vice versa.

Because in the case of the sniffing the application will offer many things to any components of the packet. What the application only wants is the value of IP and Mac attacker who works ARP, then select the two values using a dictionary which will get the IP and Mac attacker of the packet only.

IPs can change depending on DHCP assignments when our devices are connected to the network, it is important to defragment these IPs because they are not considered as an attacker and they are using ARP.

In step 6, This function will work to monitor any ARP condition that occurs within the network taking the argument and the packet. If there is ARP within this packet, Kali Linux and the sniffing are used to listen on the network, which will be located where the router and the Kali Linux are. A computer and telephone as well as another computer will all be monitored. It is where the packet data are. The data is sent from the router to the first computer and the second computer and other devices, as well as the rest of the devices when the transmitter in the process transmits information.

It is known as the OSI especially in physical layers. It is in the wireshark program and appears on the packet format. Permission must be given to monitor the packet.

Now it is known that within the network there is the packet but the question here does the application require the packet and all its contents?

Of course not, because in the case of work sniffing for the computer and for a three-way second, there will be massive amounts of data needed. One thing is important, that is, to listen to the application and to have knowledge of all these quantities of data from the ARP Act, which is only follow-up or the word ARP control through the network.

Why has this function been created? In order to use it within the sniffing and the function of all codes to contain and be called only by summoned function.

Why is sniffing needed for this function? It requires that the function returns the packet. How is the packet returned? When the program is told to return, it will return based on the process of the return of the packet again.

And the function used to know first whether there is ARP in the packet. From the use of ARP and the working of ARP, and if the router or computer where the Kali Linux or PC Windows or Access Point work, ARP should be excluded because they do not consider the hackers of the network in this case.

Two variables have been identified, namely IP and Mac, meaning that all the packets want to know is the IP address of the packet and Mac that worked ARP and the rest of the stuff in the packet does not need to be known. The last thing is to obtain information of the attacker.

The question is raised again for a second time because if IP is in the dictionary (the database), the key must be a value with the key. If the Mac is not in dictionary (database), then the question is whether the Ethernet is in the packet because the packet is obtained through Ethernet and this is the last point of contact with the network. Any means will be going down to the second layer. As mentioned earlier, the second layer can get too many things. Then the question again is whether there is Ethernet in the packet. If the Mac does not exist with the IP as mentioned above, the key is the IP and application also needs a Mac so complete the first value in the dictionary (the database). The Ethernet own hardware is a Mac. Otherwise, if they exist in the dictionary (the database) and taken directly, then the IP is in the dictionary (database) should get its own Mac, and then get an attacker IP Information and Mac, the myInfo_ip2 equal to the value of IP, and then returns the value of IP and Mac.

In step 7, Create Taste function that is inside. It does the sniffing. This sniffing is running the ARP _monitor, and the presence of the filter to see only the ARP and all the information inside the packet, then Storage zero and the Count 10.

The results are presented and shows how the attacker was prevented through the process of checking the information obtained by the attacker before and after the discovery as well as after the attacker was blocked inside the router through the application which is designed and worked on in the following examples:

3.3. Application I

1. The application start by VirtualBox Contain kali linux as shown in figure 15:

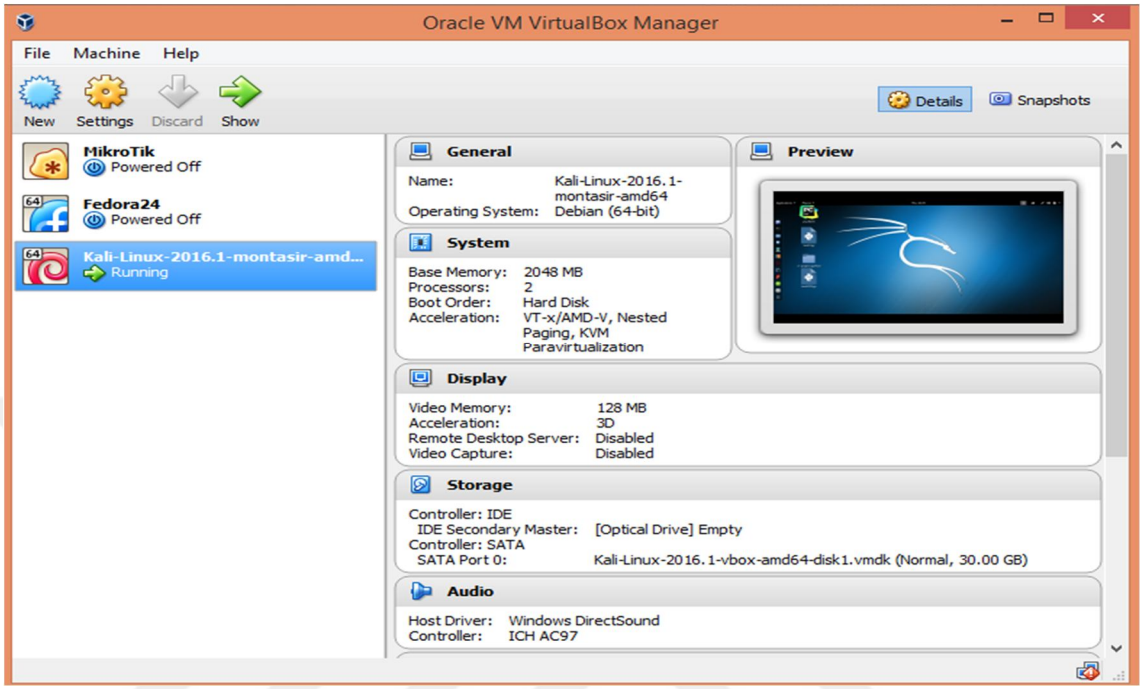

Figure 15. VirtualBox Contain kali linux

2- Run the application as shown in figure 16:

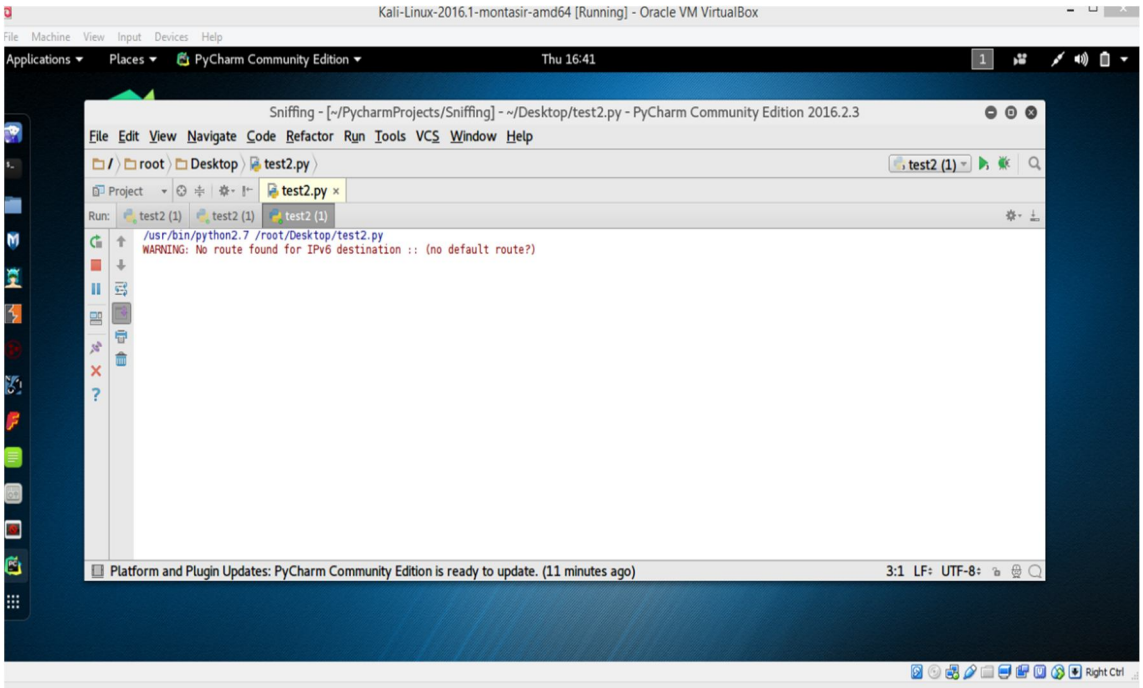

Figure 16. A screen of running the application

3- Then the application will detect the attacker by giving attacker information (IP and MAC) through an interface .As shown below in figure 17:

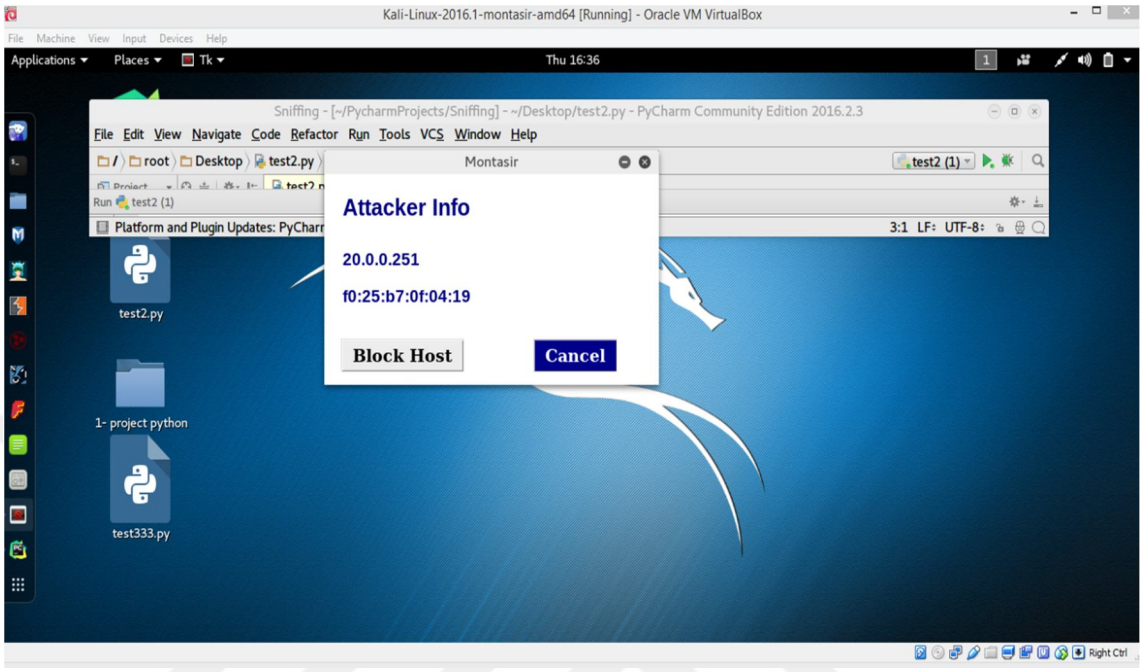

Figure 17. Attacker information (IP and MAC)

4- Another interface will show that the attacker has been blocked and sent his information to the router or the main server, to block it in its firewall. As shown below in figure (18):

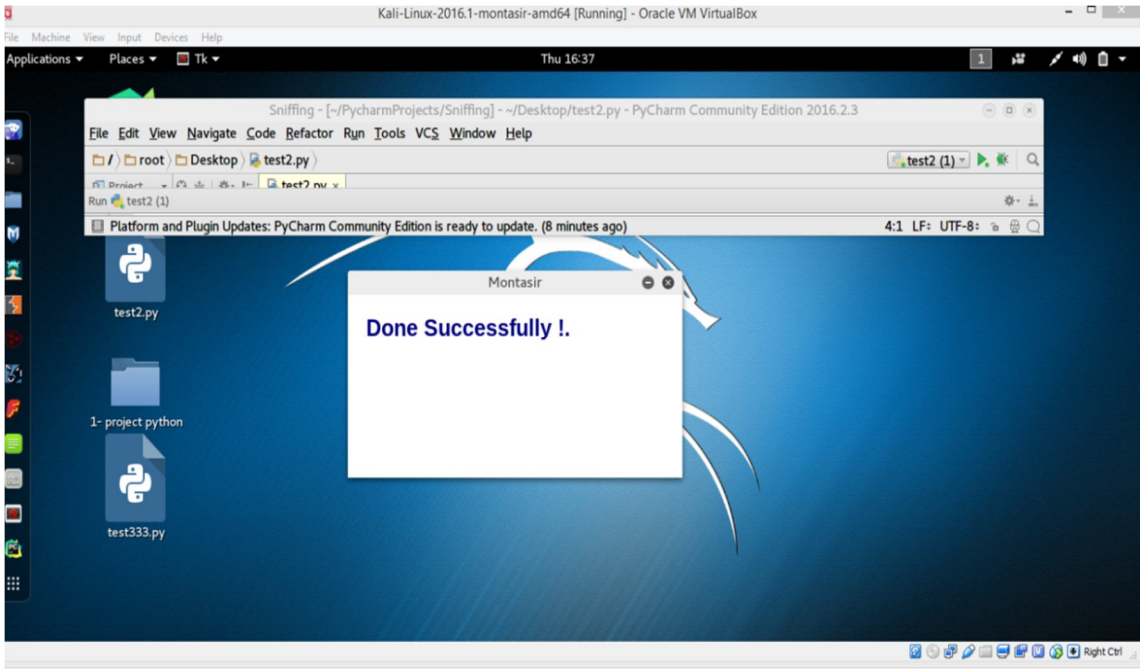

Figure 18. The command succeeds

5- Enter the main interface of the microtek, through the interface to the Linux, through the IP of the router that is specified in the selection process. shown in the figure 19:

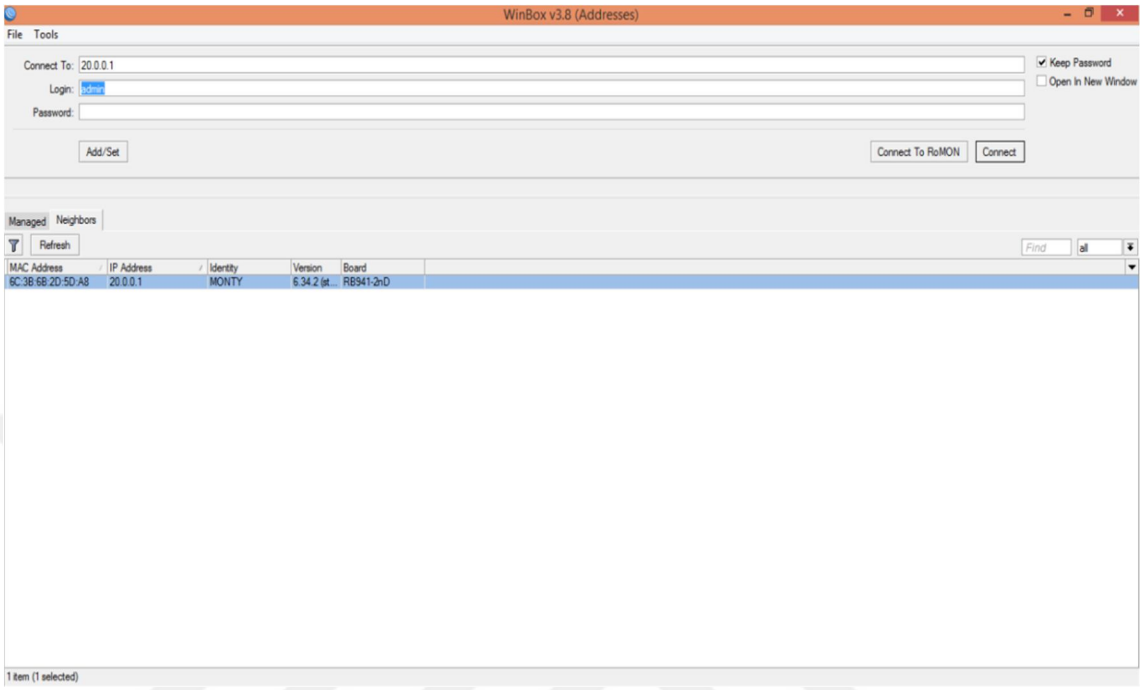

Figure 19. The main interface of the microtek

6- Listing then to the firewall list, show how to block the attackers within the router by the application, as shown in the figure 20:

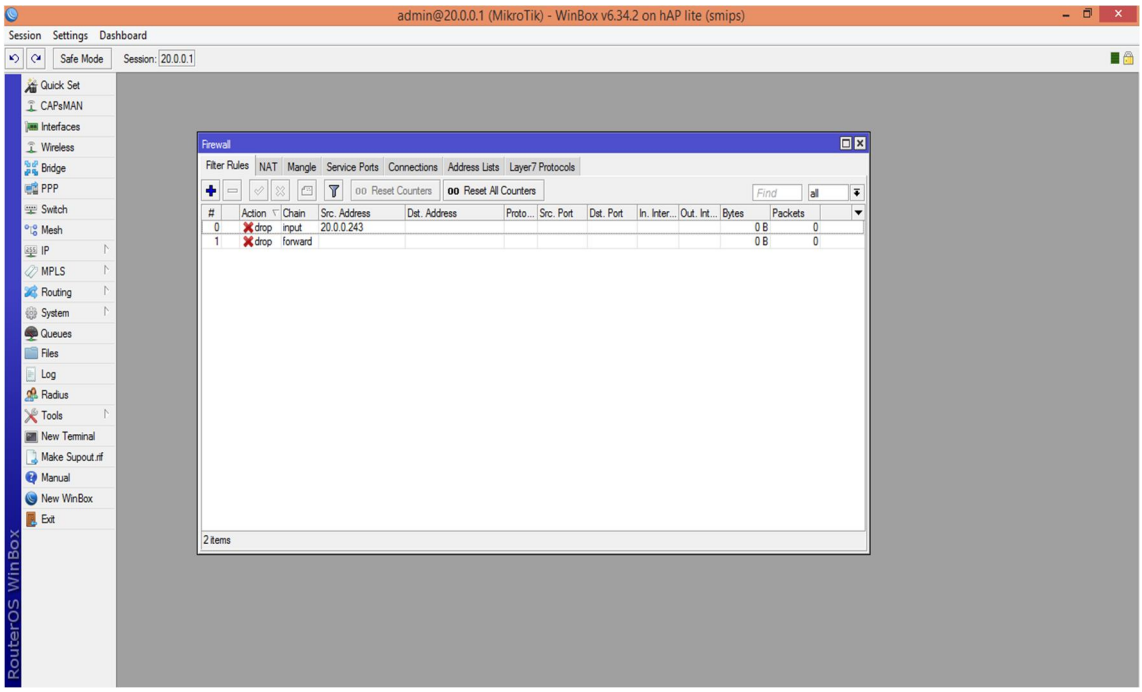

Figure 20. The firewall list

The results show that how to prevent the attacker through the information that will be obtained about the attacker before and after detection. The results also show how to block the attackers within the router by the application, as shown in the following examples:

3.3.1. Scan a single IP address

Nmap 20.0.0.1

Table 5. The results for Nmap 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). Not shown: 994 closed ports Port State Service 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 80/tcp open http 2000/tcp open cisco-sccp 8291/tcp open unknown MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). All 1000 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.3.1.1. Detect OS and services

Nmap –A 20.0.0.1

Table 6.The results for Nmap –A 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). Not shown: 994 closed ports Port State Service VERSION 21/tcp open ftp MikroTic router ftpd 6.34.2 22/tcp open ssh MikroTic routerOS sshd (protocol 2.0) | ssh-hostkey: | 1024 b1:a6:f1:53:35:b2:8c:a0:2a:bb:5d:f4:e2:9a:28:48 (DSA) | 2048 8a:e6:7a:98:83:93:58:62:27:2a:ef:a9:a9:2b:e0:28 (RSA) 23/tcp open telnet Linux telneted 80/tcp open http MikroTic router config ftpd | http-robots.txt: 1 disallowed entry | / | http.titel: routerOS router configuration page 2000/tcp open bandwidth-test MikroTic bandwidth-test server 8291/tcp open winbox MikroTic winbox MAC Address: 6C:3B:6B:2D:5D:A8 (unknown) Devise type: general purpose Running: Linux 2.6.x|3.x OS CEP: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 OS details: Linux 2.6.32 - 3.10 Network Disance: 1 host Service Info: Host: MONTY; OSs : Linux , RouterOS; Device: router ; CEP: cpe:/o: mikrotic: routeros, cpe:/o:linux:linux_kernel TRACEROUTE HOP RTT ADDRESS 1 1.27 ms 20.0.0.1	Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). All 1000 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown) Too many fingerprinter mach this host to give specific OS details Network Disance: 1 host TRACEROUTE HOP RTT ADDRESS 1 1.27 ms 20.0.0.1

3.3.1.2. Scan all 65,535 ports

Nmap – p – 20.0.0.1

Table 7.The results for Nmap – p – 20.0.0.1 before and after using the application

Before Block	**After Block**
Nmap scan report foe 20.0.0.1 Host is up (0.0027s latency). Not shown: 65527 closed ports Port State Service 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 80/tcp open http 2000/tcp open cisco-sccp 8291/tcp open unknown 8728/tcp open unknown 8729/tcp open unknown MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.00076s latency). All 65535 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.3.1.3. Scan a single port

Nmap – p 20.0.0.1

Table 8.The results for Nmap – p 20.0.0.1 before and after using the application

Before Block	**After Block**
Nmap scan report foe 20.0.0.1 Host is up (0.0079s latency). Port State Service 22/tcp open ssh MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.0079s latency). Port State Service 22/tcp filtered ssh MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.3.1.4. Detect remote services (server / daemon) version numbers

Nmap – sV 20.0.0.1

Table 9.The results for Nmap – sV 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). Not shown: 994 closed ports Port State Service VERSION 21/tcp open ftp MikroTic router ftpd 6.34.2 22/tcp open ssh MikroTic routerOS sshd (protocol 2.0) 23/tcp open telnet Linux telneted 80/tcp open http MikroTic router config ftpd 8291/tcp open unknown MAC Address: 6C:3B:6B:2D:5D:A8 (unknown) Service Info: Host: MONTY; OSs : Linux , RouterOS; Device: router ; CEP: cpe:/o: mikrotic: routeros, cpe:/o:linux:linux_kernel	Nmap scan report foe 20.0.0.1 Host is up (0.00089s latency). All 1000 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.3.1.5. Scan a host for UDP services (UDP scan)

Nmap – sU 20.0.0.1

Table 10. Showing the results for Nmap – sU 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.00077s latency). Not shown: 999 closed ports Port State Service 67/udp open | filtered dhcps MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.035s latency). All 1000 scanned ports on 20.0.0.1 are open | filtered MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.3.1.6. Scan 100 most common ports (Fast)

Nmap – F 20.0.0.1

Table 11. The results for Nmap – F 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0023s latency). Not shown: 95 closed ports Port State Service 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 80/tcp open http 2000/tcp open cisco-sccp MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.00090s latency). All 1000 scanned ports on 20.0.0.1 are filtered MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.4. The Proposed Algorithm (Application II)

The Detailed algorithm steps can be explained as the following:

Output: Attack packets

Input: IP Admin

Step1: Include a set of libraries that will be used in the application.

Step 2: Create function working on the implementation of GUI, its contain on one label for IP admin, and two buttons the first one for protect and the second one for stop and exit from application.

Step3: Function working on the implementation of ssh connection.

Step4: Create function for ssh connection.

Step5: Send command to block all IPs ranges except the IP admin computer.

Step6: Create a function that will monitor any ARP condition that occurs within the network, take the argument on the packet, and obtain information of the attacker (IP, MAC).

Step7: Create a taste function that works inside on sniffing. This sniffing is running the Arp _monitor, and the presence of the filter to see only the ARP with all the information inside the packet.

3.5. Application II

In the second application, when the application is running, the interface will appear as shown in the figure below (figure 21). The interface contains a label. The administrator put its own IP in order to be excluded from the block. Then, the application gives a block to all the range from the IPs with the exception of the administrator's IP.

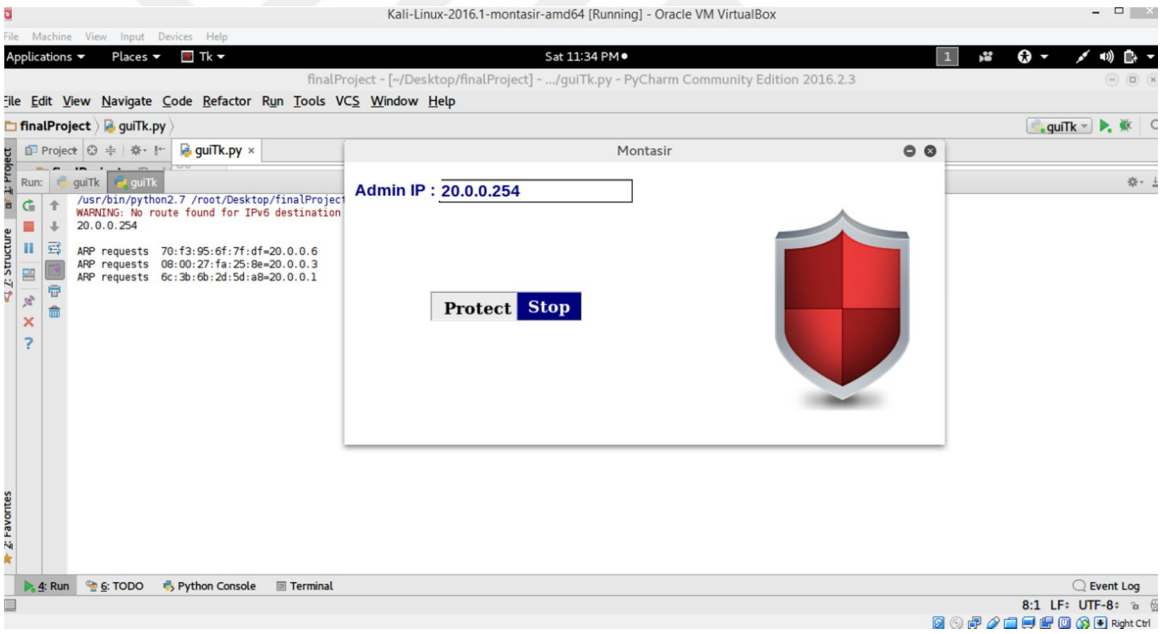

Figure 21. The Second Application Running

Therefore, we ensure that the users can not attempt to use Sniffing, scanning or gathering information. The router interface can not be accessed through the browser, from any computer except the computer administrator. As shown in Figure 22, 23.

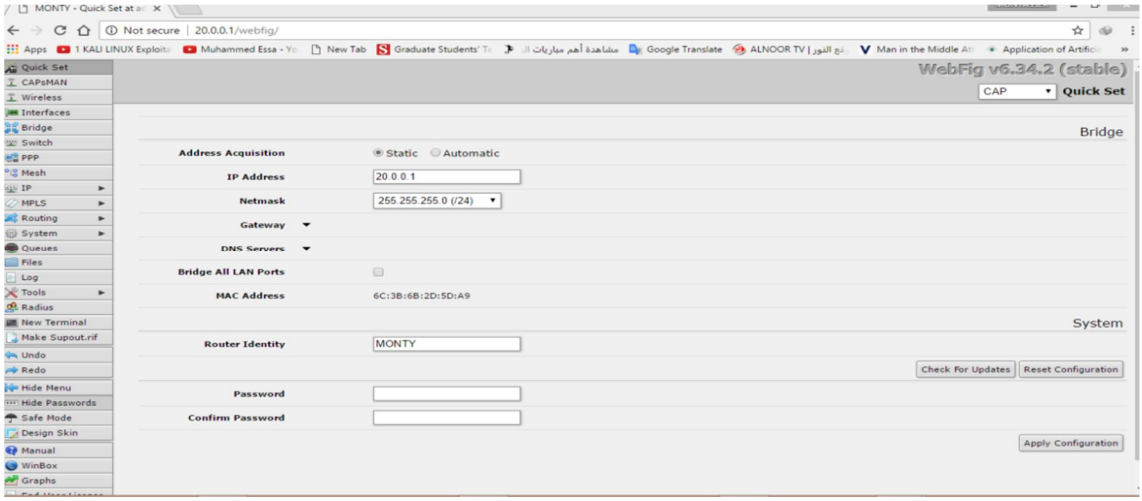

Figure 22. The router interface browser before block

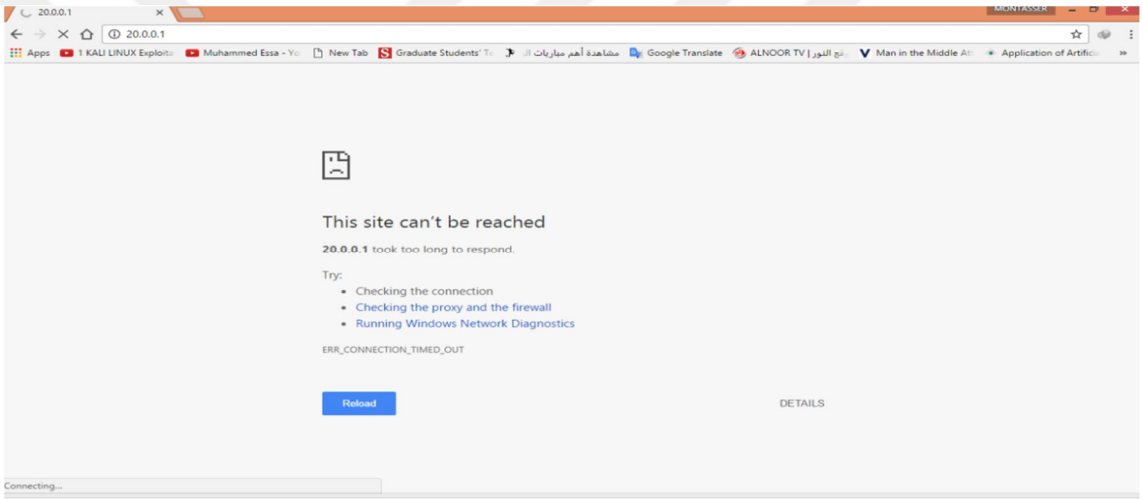

Figure 23. The router interface browser after block

3.5.1 Scan a single IP address

Nmap 20.0.0.1

Table 12. The results for Nmap 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). Not shown: 994 closed ports Port State Service 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 80/tcp open http 2000/tcp open cisco-sccp 8291/tcp open unknown MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). All 1000 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.5.2 Detect OS and services

Nmap –A 20.0.0.1

Table 13. The results for Nmap –A 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). Not shown: 994 closed ports Port State Service VERSION 21/tcp open ftp MikroTic router ftpd 6.34.2 22/tcp open ssh MikroTic routerOS sshd (protocol 2.0) | ssh-hostkey: | 1024 b1:a6:f1:53:35:b2:8c:a0:2a:bb:5d:f4:e2:9a:28:48 (DSA) | 2048 8a:e6:7a:98:83:93:58:62:27:2a:ef:a9:a9:2b:e0:28 (RSA) 23/tcp open telnet Linux telneted 80/tcp open http MikroTic router config ftpd | http-robots.txt: 1 disallowed entry | / | http.titel: routerOS router configuration page 2000/tcp open bandwidth-test MikroTic bandwidth-test server 8291/tcp open winbox MikroTic winbox MAC Address: 6C:3B:6B:2D:5D:A8 (unknown) Devise type: general purpose Running: Linux 2.6.x|3.x OS CEP: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 OS details: Linux 2.6.32 - 3.10 Network Disance: 1 host Service Info: Host: MONTY; OSs : Linux , RouterOS; Device: router ; CEP: cpe:/o: mikrotic: routeros, cpe:/o:linux:linux_kernel TRACEROUTE HOP RTT ADDRESS 1 1.27 ms 20.0.0.1	Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). All 1000 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown) Too many fingerprinter mach this host to give specific OS details Network Disance: 1 host TRACEROUTE HOP RTT ADDRESS 2 1.27 ms 20.0.0.1

3.5.3 Scan all 65,535 ports

Nmap – p – 20.0.0.1

Table 14. The results for Nmap – p – 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0027s latency). Not shown: 65527 closed ports Port State Service 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 80/tcp open http 2000/tcp open cisco-sccp 8291/tcp open unknown 8728/tcp open unknown 8729/tcp open unknown MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.00076s latency). All 65535 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.5.4 Scan a single port

Nmap – p 20.0.0.1

Table 15. The results for Nmap – p 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0079s latency). Port State Service 22/tcp open ssh MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.0079s latency). Port State Service 22/tcp filtered ssh MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.5.5. Detect remote services (server / daemon) version numbers

Nmap – sV 20.0.0.1

Table 16. The results for Nmap – sV 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0020s latency). Not shown: 994 closed ports Port State Service VERSION 21/tcp open ftp MikroTic router ftpd 6.34.2 22/tcp open ssh MikroTic routerOS sshd (protocol 2.0) 23/tcp open telnet Linux telneted 80/tcp open http MikroTic router config ftpd 8291/tcp open unknown MAC Address: 6C:3B:6B:2D:5D:A8 (unknown) Service Info: Host: MONTY; OSs : Linux , RouterOS; Device: router ; CEP: cpe:/o: mikrotic: routeros, cpe:/o:linux:linux_kernel	Nmap scan report foe 20.0.0.1 Host is up (0.00089s latency). All 1000 scanned ports on 20.0.0.1 are filtered. MAC Address: 6C:3B:6B:2D:5D:A8 (unknown)

3.5.6. Scan a host for UDP services (UDP scan)

Nmap – sU 20.0.0.1

Table 17. The results for Nmap – sU 20.0.0.1before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.00077s latency). Not shown: 999 closed ports Port State Service 67/udp open | filtered dhcps MAC Address: 6C:3B: 6B:2D:5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.035s latency). All 1000 scanned ports on 20.0.0.1 are open | filtered MAC Address: 6C:3B: 6B:2D: 5D:A8 (unknown)

3.5.7. Scan 100 most common ports (Fast)

Nmap – F 20.0.0.1

Table 18. The results for Nmap – F 20.0.0.1 before and after using the application

Before Block	After Block
Nmap scan report foe 20.0.0.1 Host is up (0.0023s latency). Not shown: 95 closed ports Port State Service 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 80/tcp open http 2000/tcp open cisco-sccp MAC Address: 6C:3B: 6B:2D: 5D:A8 (unknown)	Nmap scan report foe 20.0.0.1 Host is up (0.00090s latency). All 1000 scanned ports on 20.0.0.1 are filtered MAC Address: 6C:3B: 6B:2D:5D:A8 (unknown)

CHAPTER 4

DISCUSSION, CONCLUSION, AND RECOMMENDATIONS

4.1. Discussion

In this section, the results are discussed. The features and importance of the application that are recognized through the applied examples in the previous chapter will also be noted. It has been shown that when the applications are not operated and there is an attack to the network, a lot of information might be compromised, which is the first step is for any attacker who wants to attack and penetrate a network. If the attacker obtains the information, he will find out about the weaknesses of the network and the gaps that can be used to penetrate the network, which is called information gathering. Of course, this all happens when the attacker is outside the network. If the attacker is inside, he might attempt to access the router and the main server and do some tampering after obtaining the information.

When the first application is operated, the attacker will be discovered immediately and prevented from taking any information by blocking him and instructing the router that this attacker must be blocked and stopped immediately. As such, the application will prevent the attack after the first attack step. Therefore, it can be concluded that the application uncovered and handled the attacker immediately before information gathering can be compromised and used as a gap against the network.

While the second application is running the application will give a block to all the range of the IPs except to the admin IP, so that no users can reach to the router, a scanning or Sniffing or gathering information of the network.

As such, and after the applications are operated and results are seen and discussed, it can be said that a new and successful applications have been designed. The applications are able to defend the network against any internal or external attack.

4.2. Conclusion

It has been argued that any secure network will have the vulnerability that an attacker could exploit. This is especially true for wireless networks. Attacks detection can be complement intrusion prevention techniques (encryption, authentication, protected MAC, protected routing, etc.) to increase the network security. However, new techniques should be developed to make attack detection work better for the networking environment.

Through continuing investigation, this thesis study has shown two new applications for better detection and prevention of attacks in wireless networks. The packet analysis and anomaly detection should be done locally in each connect in the network. Moreover, attacks detection should get the place in all networking layers in an integrated cross-layer manner. We proposed our applications to network attacks in the ARP detection model.

For ARP detection model, we studied the effectiveness and scalability of our application for building ARP detection models and for other layers of networking.

In conclusion, the main purpose of this thesis is to study and characterize between the different solutions of address resolution protocol and discuss the limitations of these present solutions. We have designed two new applications to detect and prevent attacks against networks.

4.3. Recommendations

For future development and expansion of this research, the following points are planned:

i) It can be developed to work on Mobile devices. It can, through mobile, the application will run to protect. Integrate the protect part using mobile monitor (m- monitoring) technology.

ii) Further developments will be made to cover other protected services of the security of networking.

iii) New methods will be developed to detect attacks on networks based on UDP or ICMP or TCP instead of ARP.

REFERENCES

1. Bruschi, D., Ornaghi, A. and Rosti, E., 2003, December. S-ARP: a secure address resolution protocol. *In Computer Security Applications Conference, 2003. Proceedings. 19th Annual* (pp. 66-74). IEEE.

2. Abad, C.L. and Bonilla, R.I., 2007, June. An analysis on the schemes for detecting and preventing ARP cache poisoning attacks. *In Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on* (pp. 60-60). IEEE.

3. Nam, S.Y., Kim, D. and Kim, J., 2010. Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks. **IEEE communications letters, 14**(2), 187-189.

4. Farooq, J. and Soler, J., 2017. Radio communication for communications-based train control (CBTC): a tutorial and survey. **IEEE Communications Surveys & Tutorials**.

5. Holt, A. and Huang, C.Y., 2010. *802.11* Wireless Networks: Security and Analysis. Springer Science & Business Media,436 pp.

6. Sohrabi, K., Gao, J., Ailawadhi, V. and Pottie, G.J., 2000. Protocols for self-organization of a wireless sensor network. **IEEE personal communications, 7**(5), 16-27.

7. Gast, M., 2005. 802.11 Wireless Networks: The Definitive Guide. "O'Reilly Media, Inc.".

8. Karygiannis, T. and Owens, L., 2002. Wireless network security. NIST special publication, *800*, p.48.

9. Dargie, W. and Poellabauer, C., 2010. Fundamentals of Wireless Sensor Networks: Theory and Practice. John Wiley & Sons.

10. Jardosh, A.P., Papagiannaki, K., Belding, E.M., et al. 2009. Green WLANs: on-demand WLAN infrastructures. **Mobile Networks and Applications, 14**(6), 798-814.

11. Grosse, R., 1996. International technology transfer in services. **Journal of International Business Studies, 27**(4), 781-800.

12. Plósz, S., Farshad, A., Tauber, M., Lesjak, C., Ruprechter, T. and Pereira, N., 2014, September. Security vulnerabilities and risks in industrial usage of wireless communication. *In* ***Emerging Technology and Factory Automation (ETFA), 2014 IEEE*** (pp. 1-8). IEEE.

13. Khan, S. and Pathan, A.K., 2013. *Wireless networks and security*. Berlin: Springer.

14. Liu, Y., Dong, K., Dong, L. and Li, B., 2008. Research of the ARP spoofing principle and a defensive algorithm. **International Journal of Communications**, *4*.

15. Trabelsi, Z. and El-Hajj, W., 2009, September. ARP spoofing: a comparative study for education purposes. *In 2009 Information Security Curriculum Development Conference* (pp. 60-66). ACM.

16. Hoque, N., Bhuyan, M.H., Baishya, R.C., Bhattacharyya, D.K. and Kalita, J.K., 2014. Network attacks: Taxonomy, tools and systems. **Journal of Network and Computer Applications, 40**, 307-324.

17. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. **Journal of Network and Computer Applications, 36**(1), 42-57.

18. Nam, S.Y., Jurayev, S., Kim, S.S., Choi, K. and Choi, G.S., 2012. Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN. ***EURASIP*** **Journal on Wireless Communications and Networking,** 1, 89.

19. Song, M.S., Lee, J.D., Jeong, Y.S., Jeong, H.Y. and Park, J.H., 2014. DS-ARP: a new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments. **The Scientific World Journal**.

20. Alzubaidi, W.K., Cai, L. and Alyawer, S.A., 2012. Enhance the security and performance of IP over ethernet networks by reduction the naming System Design. **Int. J. Comput. Netw. (IJCN), 4**(5).

21. Ramakrishnan, B., Sreedivya, S.R. and Selvi, M., 2015. Adaptive routing protocol based on cuckoo search algorithm (ARP-CS) for secured vehicular ad hoc network (VANET). **International Journal of computer networks and applications (IJCNA), 2**(4), 173-178.

22. Khokhar, V., Khan, S., Muppuri, P. and Ahlawat, P., Sniflyzer: A Network Sniffer.

23. Singh, K. and Sharma, S., ARP Spoofing and ARP Poisoning: Proof of Concept and Mitigation.

24. Zharinov, R., Virovlyanskiy, D. and Shvedov, Y., 2013, November. Undetectable interception of network traffic on lan technologies. *In Open Innovations Association (FRUCT), 2013 14th Conference of* (pp. 169-174). IEEE.

25. More, S.R., Bhatt, D.V. and Menghani, J.V., 2017. Recent Research Status on Erosion Wear–An Overview. *Materials Today:* **Proceedings, 4**(2), 257-266.

26. Whalen, S., 2001. An introduction to ARP spoofing. Online document.

27. Bruschi, D., Ornaghi, A. and Rosti, E., 2003, December. S-ARP: a secure address resolution protocol. *In Computer Security Applications Conference, 2003. Proceedings. 19th Annual* (pp. 66-74). IEEE.

28. Kaur, I. and Miglani, S.G., 2013. Detection and prevention of ARP cache poisoning (Doctoral dissertation).

29. Kaur, G. and Malhotra, J., 2015. Comparative Investigation of ARP Poisoning Mitigation Techniques using Standard Testbed for Wireless Networks. **International Journal of Computer Applications, 121**(13).

30. Coit, C.J., Staniford, S. and McAlerney, J., 2001. Towards faster string matching for intrusion detection or exceeding the speed of snort. *In DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings* (Vol. 1, pp. 367-373). IEEE.

31. Tripunitara, M.V. and Dutta, P., 1999. A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning. *In Computer Security Applications Conference, 1999. (ACSAC'99) Proceedings. 15th Annual* (pp. 303-309). IEEE.

32. Nikiforakis, N., Younan, Y. and Joosen, W., 2010, July. HProxy: Client-side detection of SSL stripping attacks. *In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 200-218). Springer Berlin Heidelberg.

33. Fung, A.P. and Cheung, K.W., 2010, April. SSLock: sustaining the trust on entities brought by SSL. *In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security* (pp. 204-213). ACM.

34. Singh, J., Dhariwal, S. and Kumar, R., 2017, A Detailed Survey of ARP Poisoning Detection and Mitigation Techniques.

35. Goyal, V. and Tripathy, R., 2005. An efficient solution to the ARP cache poisoning problem. *In Australasian Conference on Information Security and Privacy* (pp. 40-51). Springer Berlin Heidelberg.

36. Nam, S.Y., Kim, D. and Kim, J., 2010. Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks. **IEEE communications letters, 14**(2), 187-189.

37. Ramachandran, V. and Nandi, S., 2005, December. Detecting ARP spoofing: An active technique. In ***International Conference on Information Systems Security*** (pp. 239-250). Springer Berlin Heidelberg.

38. Nenovski, B. and Mitrevski, P.,2015, Real-World ARP Attacks and Packet Sniffing, Detection and Prevention on Windows and Android Devices. *The 12th International Conference for Informatics and Information Technology* (CIIT 2015), (pp. 187-191).

39. Shezan, F.H., Afroze, S.F. and Iqbal, A., 2017, January. Vulnerability detection in recent Android apps: An empirical study. *In Networking, Systems and Security (NSysS), 2017 International Conference on* (pp. 55-63). IEEE.

40. Tripunitara, M.V. and Dutta, P., 1999. A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning. *In Computer Security Applications Conference, 1999. (ACSAC'99) Proceedings. 15th Annual* (pp. 303-309). IEEE.

41. Joshi, D., Dwivedi, V.V. and Pattani, K.M., 2017. De-Authentication attack on wireless network 802.11 i using Kali Linux. *International Research Journal of Engineering and Technology (IRJET),* (pp.1666-1669).

42. Duffy, C., 2015. Learning Penetration Testing with Python. Packt Publishing Ltd.

43. Biondi, P., 2005. Scapy: explore the net with new eyes. Technical report, EADS Corporate Research Center, **http://www.secdev.org.**

44. Shaw, D., 2015. Nmap Essentials. Packt Publishing Ltd.

45. Deng, H., Li, W. and Agrawal, D.P., 2002. Routing security in wireless ad hoc networks. **IEEE Communications magazine, 40**(10), 70-75.

46. Pearce, M., Zeadally, S. and Hunt, R., 2013. Virtualization: Issues, security threats, and solutions. **ACM Computing Surveys (CSUR), 45**(2), 17.

47. Mason, R., 2017, January. Introductory Programming Courses in Australasia in 2016. *In Proceedings of the Nineteenth Australasian Computing Education Conference,* ACM. (pp. 81-89).

CURRICULUM VITAE

Name and surname: Muntasser HAMZAH

Nationality: İraq

Birth date and place: 16/ 11/ 192 Bağdat

Marital status: Married

Cell phone: 0 531 989 90 22

E-mail: montaser_hamza@yahoo.com

Correspondence Address: Fevzi Çakmak Mah. Sivas Cad. Alçılar Apt. 67/16 Kocasinan/KAYSERİ

EDUCATION

Degree	Institution	Date of graduation
MSc	Erciyes University	----------
License	Diyala University Collage	2008
High school	Laila Achaily	1997

FOREIGN LANGUAGE

Arabic

English