ISSN 2707-1898 (print)
ISSN 2786-9172 (online)
Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2025.02.106
Article received 08.08.2025 р.
Article accepted 30.10.2025 р.
UDC 004.056.5:004.7

Correspondence author
@ Luay Abdulwahid Shihab
luaay.abdulwahid@uobasrah.edu.iq

Luay Abdulwahid Shihab*, *Hazim N. Waheeb
University of Basrah, Basrah, Iraq

ANALYSIS OF COMPUTER NETWORK SECURITY AGAINST PACKET INTERCEPTION: A CASE STUDY OF THE COLLEGE OF NURSING

Society has enjoyed technological developments, especially in the field of information, one of which has developed currently is the internet. In its use, the networks used by the public are LAN cables or Wi-Fi (without cables), attacks from irresponsible parties, namely hackers who can exploit important user data, intercept data such as passwords and change user data. This research discusses the evaluation of the security level of Wi-Fi facilities at University of Basrah compus,basrah, Governorate, Iraq using the Aircrack-ng, Kismet and ettercap applications. Aircrack-ng is a Wi-Fi hacking tool that is used to detect and identify open wireless signals. Kismet is alternative software whose function is exactly the same as Aircrack-ng. Ettercap is a packet sniffer tool used to analyse network protocols and audit network security, which also has the ability to block traffic on LAN networks, steal passwords, and carry out active eavesdropping on common protocols. In this research, two stages were carried out, the first was to identify the existence and security of the Wi-Fi used using Kismet software. The second stage carried out a packet sniffing attack using Ettercap software as a security testing step at the University of Basrah compus, basrah, Governorate, Iraq.

Keywords: analysis of computer, network security, against packet interception.

Introduction

A router is a tool used to connect several networks. According to [1]. Network security is very important to pay attention to, networks connected to the internet are basically unsafe and can always be exploited by hackers, both on cable and wireless networks. According to [11]. Packet Sniffing / Sniffer is an attack method by monitoring all packets passing through a communications medium, be it cable or wireless media.

University of Basrah compus,basrah, Iraq has Wi-Fi which does not rule out the possibility of attacks on the network. Based on interviews conducted at PGRI University, West Sumatra with one of the staff in the ICT room, information was obtained that PGRI West Sumatra University distributes both cable and wireless network services. The distribution of the Wi-Fi network in building A, building B, building C, and building D, and also obtained information regarding the security of the Wi-Fi network at the University of Basrah compus,basrah, Governorate, Iraq does not yet know the security of the network.

According to [19] Network Security is the process of preventing and identifying unauthorized use of a computer network. According to [3]. Wireless Fidelity (Wi-Fi) is a technology that allows a number of computers to be connected in a network without cables, aka wireless local area network (WLAN). According to [7] a router is a tool used to connect several networks. According to [1]. Packet sniffing is a technique for monitoring every packet that crosses a network, and is a piece of software or hardware that monitors all traffic that crosses a network. According to [16] Kali Linux is a Linux distribution system that was developed with a focus on penetration testing tasks according to [4].

Types of attack threats

There are several types of attacks that can occur on networks, particularly wireless networks (Wi-Fi), as detailed by [14] in their research Network Security Analysis in Internet Facilities (Wi-Fi) against attacks. Packet Sniffing is classified below;

1. Packet sniffer: A packet sniffer is a tool that can intercept and record network traffic. A packet sniffer can capture protocol data units (PDU), decode them, and analyse their contents as they move via a network. Wireshark is a packet sniffer designed to recognise a variety of network protocols. Wireshark may additionally display encapsulation results and fields in the PDU [14]. An attack method called a packet sniffer entail intercepting and tracking every packet sent over a communication channel, be it a wireless or cable network. After the transmitted packets are obtained, they are rearranged so that an unauthorised party can unlawfully extract the data that was sent by one party. This is made feasible by the fact that nearly all Ethernet connections are broadcast connections, which means that packets sent by a host will be received by all computers in the network group. The fundamental nature of packet sniffing – a passive approach that requires only the ability to listen from the attacker – makes it difficult to defend against this interference [2].

2. Denial of service (Dos): Valuable network resources include computers and databases, as well as services provided by the organization that owns the network. Most network users take advantage of these services so that their work becomes efficient. If this service cannot be used for certain reasons, it will of course cause a loss of productivity. It is difficult to predict the cause of a denial of service. The following are examples of causes of denial of service:

a) It is possible that the network may not function due to being flooded with traffic.

b) There is a possibility that a virus will spread and cause the computer system to become slow or even paralyzed.

c) The possibility that the device protecting the network is damaged.

3 Review of literature

Previous research is used to be used as consideration and it is hoped that it can help in creating new techniques. The research made by the author is not 100 % the result of his own work, but the author took the basics from several studies from several other authors related to this research, one of which is research from [5]. analyses the Network Security in Internet Facilities (Wi-Fi) against Packet Sniffing Attacks, this research focuses on security testing against sniffing attacks which aim to record all important data from the target so that important data such as usernames and passwords can be retrieved.

Computer networks have two data transmission media, namely cable and wireless. University of Basrah compus,basrah, Governorate, Iraq is one of the State-Owned Enterprises (BUMN) that has wireless network facilities (Wi-Fi). Wi-Fi networks are very vulnerable to threats of attack, because the communication that occurs is open. A good security system is needed to maintain the security of user data to avoid attacks carried out by irresponsible people.

Another research that the author took was from [6] entitled Application of the ISSAF and OWASP Version 4 Methods for Testing Web Server Vulnerabilities where this research aims to test attacks on web servers using the ISSAF and OWASP methods where one of these methods is used by the author to use. test against their own servers. Through this self-test, web server owners will find out where the vulnerabilities of the existing system are. One of these self-test methods is a penetration test. This method is the same as hacking activity but is carried out legally. In this research, the penetration test implementation method that will be used is ISSAF (Information Systems Security Assessment Framework) and OWASP version 4. IKIP PGRI Madiun as an educational institution has had its own web server since 2010. Based on an interview with the web server manager of IKIP PGRI Madiun, since the first time the web server went online until now the web server has been hacked several times a year and a penetration test has never been carried out on the web server. Testing and analysis conducted using the ISSAF method indicate that the IKIP PGRI Madiun web server system remains vulnerable to unauthorised access and the takeover of administrator privileges. Similarly, the use of the OWASP version 4 method reveals that the implementation of authentication, authorization, and session management is inadequate. As well as research from [15] carried out penetration tests on Wireless LANs to evaluate the level of network security by also applying the ISSAF method as a framework in this research.

Wireless Local Area Network (WLAN) is a network that is widely used in several institutions to provide joint access to information. Wireless network security is a major concern for network managers to maintain the quality of the network system. To see the quality of network security, it is necessary to evaluate the security system in the network. One method that can be used to evaluate is penetration testing of the network [15]. Penetration testing is the act of testing a system by simulating forms of attacks on the system so that the level of vulnerability is known. Testing with this method will of course carry risks that can affect the system. Attacks carried out against the system can be detrimental to the testing target and for the perpetrator it is certainly an act of violation if there is no agreement on the action to be taken and the consequences of that action. Therefore, to apply it to institutions, there needs to be good planning and preparation so as not to harm each party. This research uses the case of University of Basrah compus, basrah, Governorate, Iraq as an institution that is used as an object for implementing a WLAN security evaluation model with penetration testing.

At this moment, network security is a critical issue that requires attention; networks connected to the internet are inherently insecure and can be abused by hackers, both wired and wireless LAN networks. When data is transferred, it must pass through numerous terminals before reaching its destination, which allows other unscrupulous users to intercept or modify it [10]. The security system for networks connected to the Internet must be carefully established and understood in order to properly secure network resources and minimise hacker threats.

Ettercap is a packet sniffer programme for analysing network protocols and auditing network security. It can block traffic on LAN networks, steal passwords, and perform active eavesdropping on popular protocols. Meanwhile, Aircrack-ng is a Wi-Fi hacking tool that detects and identifies open wireless signals infiltrating the network. The design of a wireless sensor network involves a number of factors to be considered. Of the most important we have Fault tolerance, Scalability, Production cost, Operating environment, Hardware restrictions, Network topology, Transmission medium and power consumption [7]. Wireless sensor networks have been the subject of study for some time, mainly due to technological innovations introduced by the advance in micro-electro-mechanical systems, wireless communications and digital electronics [8]. In particular, within organizational contexts, processes have been improved, automated, or transformed to reduce production costs and eliminate repetitive tasks – crucial measures for operational efficiency. Examples include package classification for shipping, automated production chains, or continuous monitoring of core business assets such as physical devices, crops, or manufactured products [9].

Currently University of Basrah compus, basrah, Iraq has implemented a wired and wireless computer network as a medium for exchanging data / information on public or commercial services, personnel and other important information. There are two networks installed within University of Basrah campus namely [18].

1. Installed in a new building which contains TU, Cashier, Administration, Public Services and KesKam rooms / offices using a cable network.

2. Installed at the TelNav Office which is connected to the University of Basrah campus which uses a cable network and there are two access points as a wireless network

Based on the description above, the author is interested in learning how to secure a network. Therefore, the author took material regarding internet network security for the research paper title "Analysis of Network Security in Internet Facility (Wi-Fi) against Packet Sniffing Attacks".

2. METHODOLOGY

2.1. Time and Place of Research

The research was carried out from March 2024 to June 2024 at University of Basrah compus, Basrah, Governorate, Iraq.

2.2. General Profile

The University of Basrah is highly esteemed among the universities in Iraq. The university comprises several colleges offering several specialisations in the fields of science, literature, engineering, and medicine. Notably, the institution of Medicine holds the distinction of being the oldest institution within the university [13].

The University of Basrah is seeking to procure Internet services for the academic year (2023–2024) based on the following requirements and specifications:

1. Internet service with a minimum speed of 300 megabits per second, accessible 24/7.

2. The minimum requirement for the number of actual addresses is 24 addresses (4IPv).

3. Cash services (FNA, GCC) are provided at no cost and are accessible to anyone.

4. The duration of the preparation phase is 12 months.

5. The company is accountable for supplying the essential equipment for delivering the Internet service via the site's optical cable, ensuring high performance and quality, and offering an alternate connection.

6. The corporation commits to uphold and substitute the devices used for providing the Internet service in the event of any harm.

7. The company needs to be able to establish connections with the internal department sites (Al-Farouq Complex) situated on the right side.

Currently University of Basrah compus, basrah, Governorate, Iraq has implemented wired and wireless computer networks as a medium for exchanging data/information on public or commercial services, personnel, military and other important information.

2.3. Research Materials and Tools

In this study, the research material is based on the basic theory of computer network security taken from various literature such as books, articles in softcopy and hardcopy form.

2.4. Thinking Framework and Flowchart

In explaining a problem, the framework of thought or research flow is presented to facilitate understanding of the research. This method is presented in the research flow diagram (Fig. 1).

In accordance with the research flow diagram above, this research was carried out in several stages.

a. Prepare literature, books, ebooks and articles to support research.

b. Fulfill research licensing requirements / procedures provided by KesKam (Safety and Security) at University of Basrah compus,basrah, Governorate, Iraq, because not all places / locations are allowed to enter except certain employees who are entitled.

c. Look for information on existing data, configuration of LAN and Wi-Fi cable networks installed throughout University of Basrah compus, Basrah, including location, SSID, BSSID, encryption used, channels.

d. Prepare the hardware and software needed to support the implementation of the research.

e. Stepping to carry out an attempted attack on the LAN cable and Wi-Fi network to obtain information about its security.

f. Draw conclusions to decide on a suggestion that can be used to secure LAN and Wi-Fi cable networks from the user's perspective.

2.5. Stages of Software Installation and Configuration

1. Install Aircrack-ng software on Windows 7

– double click on the netstumblerinstaller_0_4_0.exe file for installation, then follow the next commands by clicking i agree, next and install until finished;

– configure the network device connected to the laptop on Aircrack-ng by clicking on the device option, as in Fig. 2 following:

After seeing image 3.2. It turns out that the network adapter device connected to the author's laptop does not support it, because the Aircrack-ng software can only run perfectly on Windows XP and cannot run perfectly on Windows 10. Then the author replaced it with in SSIDer software as an alternative to the Aircrack-ng software for Windows 10

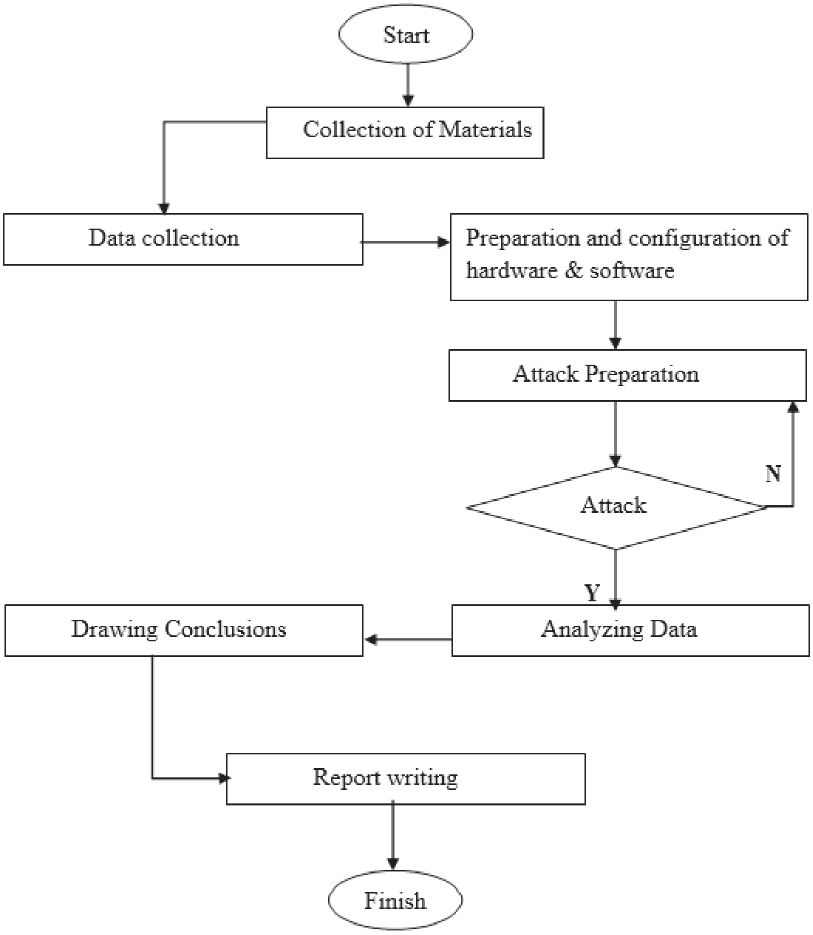
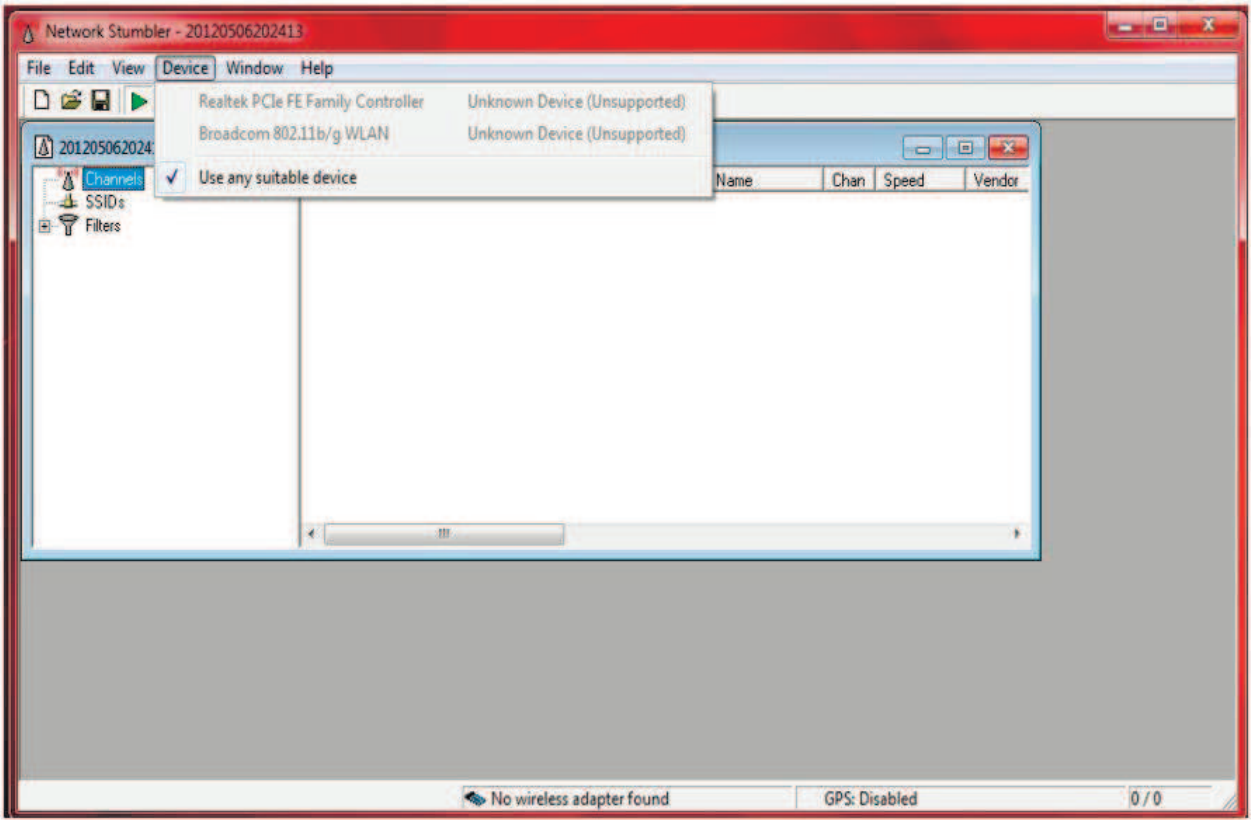


Fig. 1. Research Flow Chart


Network Stumbler - 20120506202413
File
Edit
View
Device
Window
Help
Realtek PCIe FE Family Controller
Unknown Device (Unsupported)
Broadcom 802.11b/g WLAN
Unknown Device (Unsupported)
✓ Use any suitable device
201205062024
Channels
SSIDs
Filters
Name
Chan
Speed
Vendor

No wireless adapter found

GPS: Disabled

0 / 0

Fig. 2. Configure the network adapter device in Aircrack-ng software

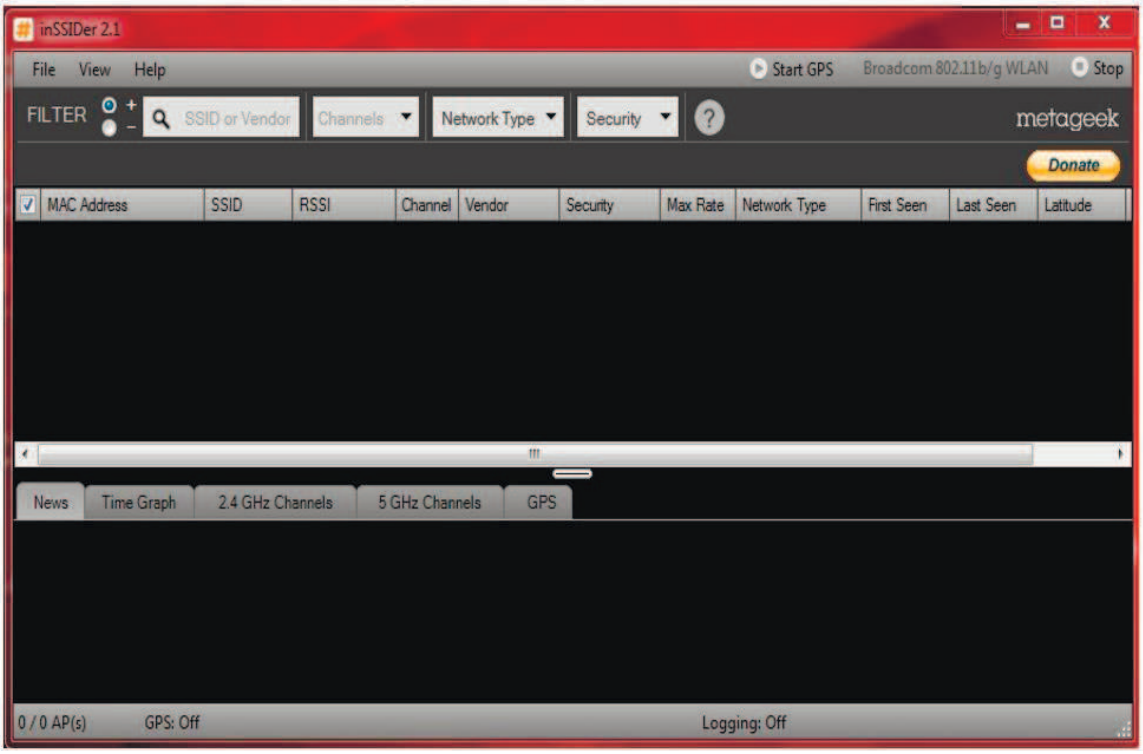
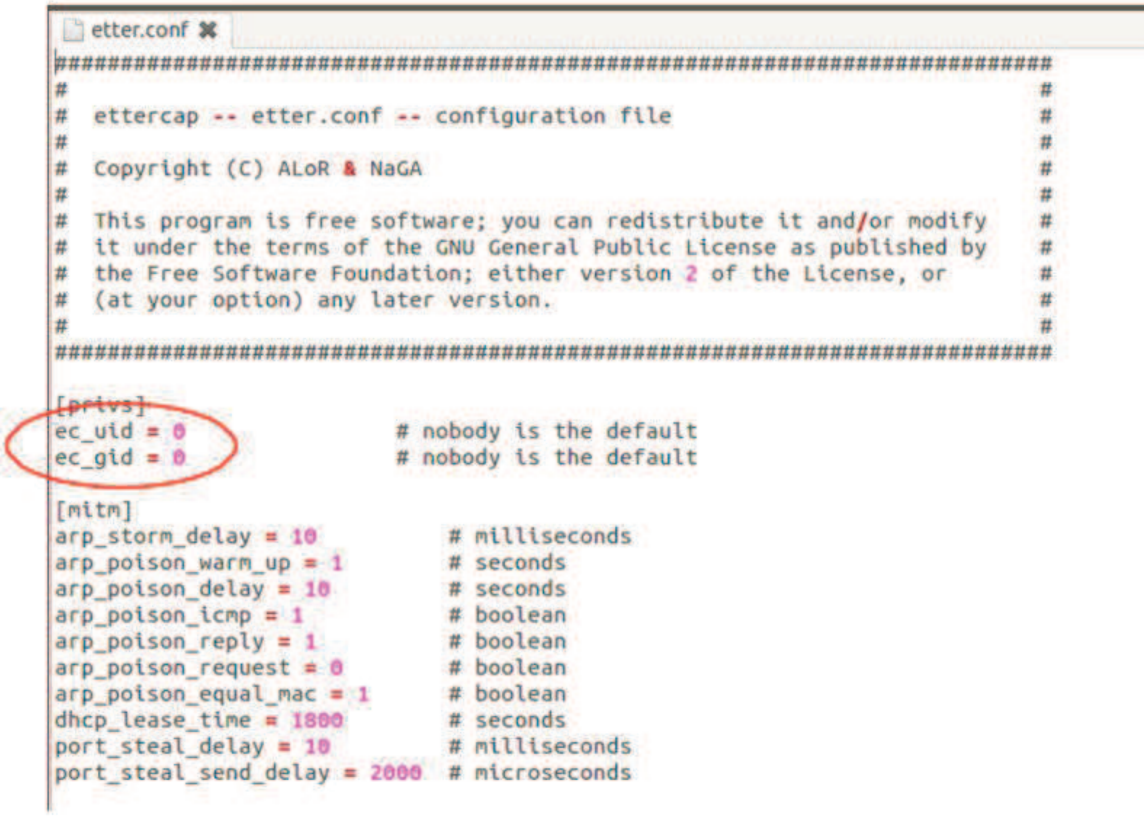


Fig. 3. Display of in SSIDer software on Windows 7

2. Installing Ettercap software on Ubuntu 23.10

- First update the index package first via the terminal with the specific command:
- Then install ettercap-gtk deb package with the specific command:
- The next step is setting the etter.conf file with the specific command.
- Then change the contents of the etter.conf file to configure the ettercap software so that it can run properly on a secure SSL connection.



```
etter.conf
############################################################################
#                                                                          #
#  ettercap -- etter.conf -- configuration file                            #
#                                                                          #
#  Copyright (C) ALoR & NaGA                                               #
#                                                                          #
#  This program is free software; you can redistribute it and/or modify    #
#  it under the terms of the GNU General Public License as published by    #
#  the Free Software Foundation; either version 2 of the License, or       #
#  (at your option) any later version.                                     #
#                                                                          #
############################################################################

[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
arp_poison_request = 0        # boolean
arp_poison_equal_mac = 1      # boolean
dhcp_lease_time = 1800        # seconds
port_steal_delay = 10         # milliseconds
port_steal_send_delay = 2000  # microseconds
```

Fig. 4. *Etter.conf* file configuration display 1

In Fig. 4 an Ettercap configuration which aims to be able to carry out tasks as attacking software cleanly or without other users knowing, by changing the $privs$ section to 0.

The command above is an ettercap configuration which aims to carry out the attack so that it can run well on a secure SSL and https network connection, so the author must ensure that the $redir\_command\_on$ script in $etter.conf$ is active.

2.6. Security Testing Techniques

Security testing aims to gain awareness of security issues in wired and wireless networks (wireless LAN).

a. The author tries to identify the existence and security used by the target Wi-Fi using in SSIDer software.

b. After knowing the existence and security used by the target Wi-Fi, the author logs in to get a connection with the target Wi-Fi.

c. Security testing steps, after getting a connection with the target Wi-Fi, the author tries to carry out a Packet Sniffing attack on Wi-Fi and cable networks using Ettercap software, the attack will be successful if data transfer is not protected by security such as SSL, IP Sec, WEP, WPA and WPA2. Because the data obtained is encrypted.

2.7. Stages of Attack

1. The author looks for positions where attacks are permitted.

Fig. 5 is a location plan where the author conducted research on a new building at University of Basrah campus, the numbers written above are representative of several rooms, here is the explanation:

a. Room 1 contains the Service Employee Room, Service Assistant Manager and Safety and Security Assistant Manager.

b. Room 2 has rooms for Financial Administration Employees, Cashiers and Accounting & Budget Assistant Managers.

c. Rooms 3 and 4 contain rooms for Administrative Employees, Assistant Manager for Treasury & PKBL, Assistant Manager for Personnel & General Affairs, Assistant Manager for Commercial and Business Development.

d. Room 5 contains the Finance, Commercial, Personnel & General Manager’s Room.

e. Room 6 contains the Operations & Engineering Manager’s Room.

f. Room 7 contains the Employee Room, Assistant Manager for Academic Operations and Assistant Manager for General Engineering & Equipment.

g. Room 8 is a meeting room that the author uses as a research area, in which there is a switch and ADSL provider modem.

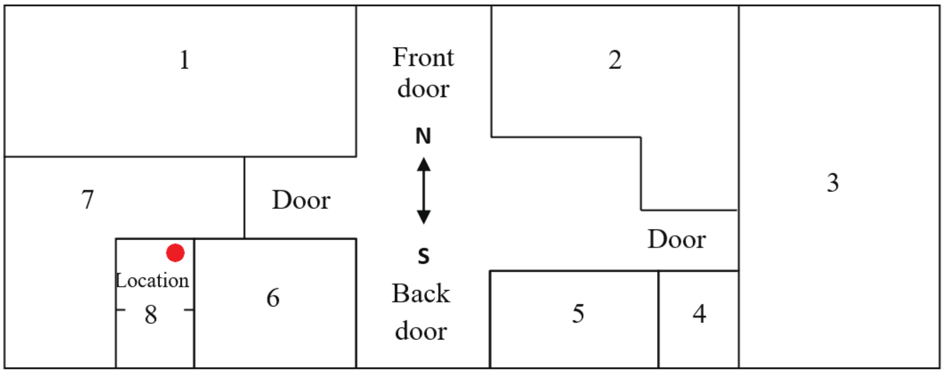


Fig. 5. Position of permitted attack places / locations in new buildings

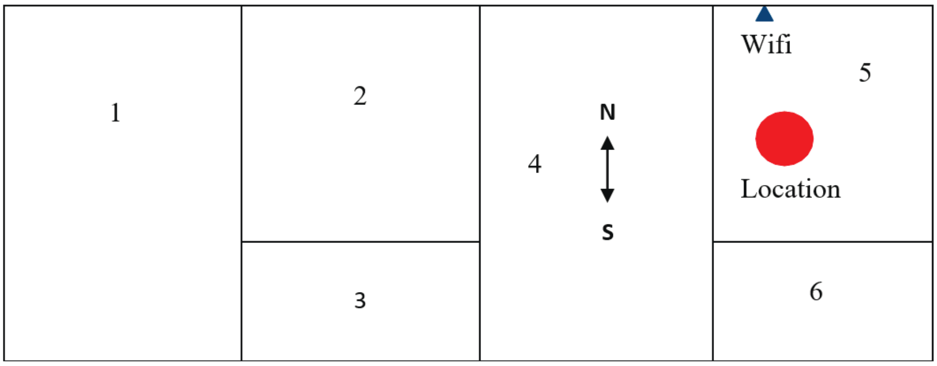


Fig. 6. Position of permitted attack locations / locations in TelNav buildings and terminals

Fig. 6 is a location plan where the author conducted research on the Telecommunications and Navigation building at University of Basrah compus, basrah, the numbers written above are representative of several rooms, here is the explanation:

a. Room 1 is the server room.

b. Room 2 is the Electronics and Electrical Employees room.

c. Room 3 is the room for the Assistant Manager of Electronics and Electrical.

d. Room 4 is the server room.

e. Room 5 is a computer network monitoring room which the author uses as a place for research.

f. Room 6 is the warehouse.

2. Identifying Wi-Fi security using Kismet software. The author runs Kismet software on Windows 7 and automatically

It will automatically display information about the existence of Wi-Fi complete with SSID name, $MAC\ address$, $RSSI$, $vendor$, $channel\ used$, $network\ type$ and $security$ used.

3. Using the ettercap software, one may do packet sniffing on both Wi-Fi and cable networks.

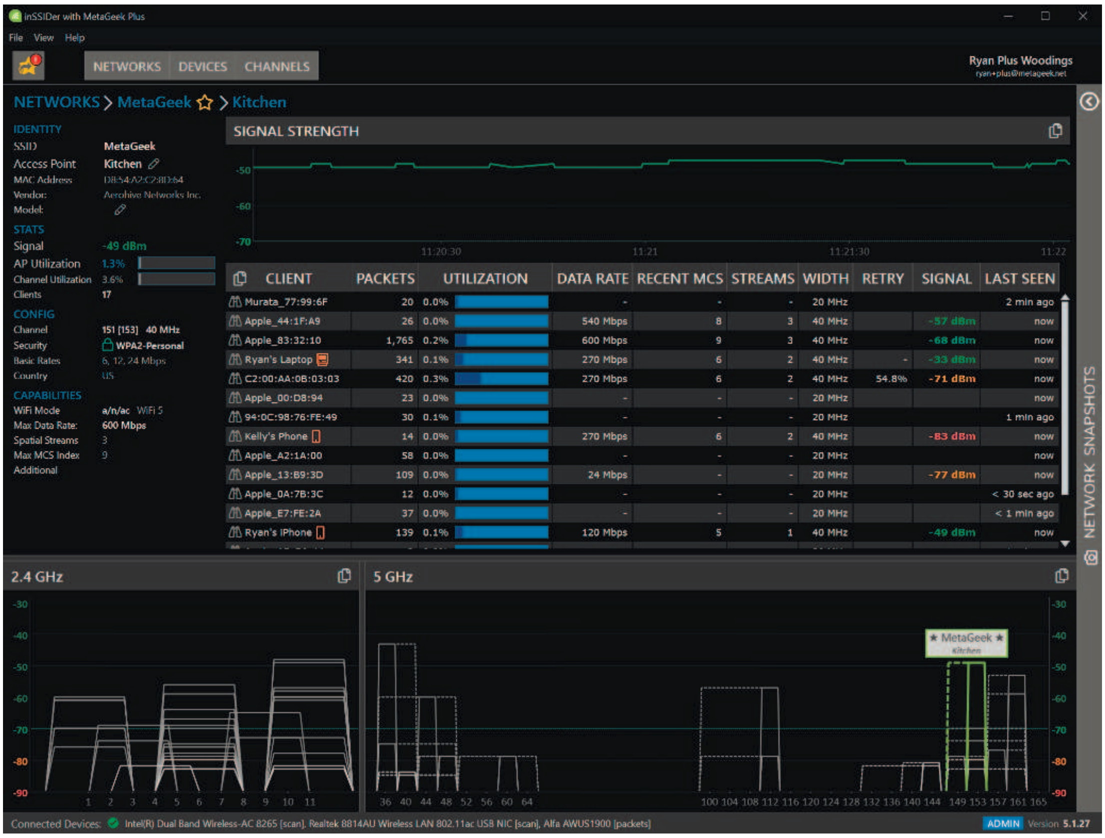
The steps taken are:

- The author's first step is to activate the ettercap software via the terminal with a command (Fig. 4).
- Then the second step, click on the sniff menu toolbar, select unified sniffing, then select device eth1/device Wi-Fi so that it can run on a Wi-Fi / Wi-Fi network and select device eth0/device LAN Card so that it can run on a wired network.

Fig. 8 is the display of Ettercap software that is already running / entering the Wi-Fi network, there is some information, namely the IP address of the attacker registered on the Wi-Fi network, if a configuration error occurs it will also be displayed as in the image above.

Fig. 9 is the display of the ettercap software that is already running / entering the LAN cable network.

– The third step, click host to search for the target host, select scan host.



IDENTITY
SSID MetaGeek
Access Point Kitchen
MAC Address D8:54:A2:C2:8D:64
Vendor: Aerohive Networks Inc.
Model:

STATS
Signal -49 dBm
AP Utilization 1.3%
Channel Utilization 3.6%
Clients 17

CONFIG
Channel 151 [153] 40 MHz
Security WPA2-Personal
Basic Rates 6, 12, 24 Mbps
Country US

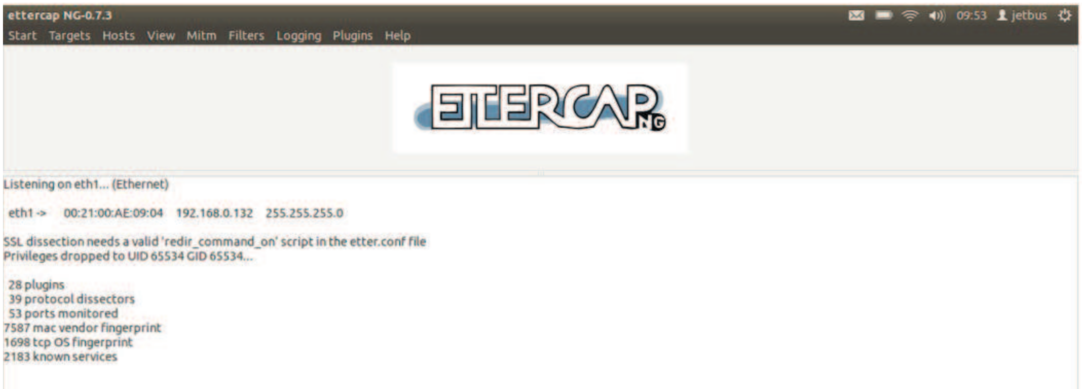
CAPABILITIES
WiFi Mode a/n/ac WiFi 5
Max Data Rate: 600 Mbps
Spatial Streams 3
Max MCS Index 9
Additional

CLIENT	PACKETS	UTILIZATION	DATA RATE	RECENT MCS	STREAMS	WIDTH	RETRY	SIGNAL	LAST SEEN
Murata_77:99:6F	20	0.0%	-	-	-	20 MHz			2 min ago
Apple_44:1F:A9	26	0.0%	540 Mbps	8	3	40 MHz		-57 dBm	now
Apple_83:32:10	1,765	0.2%	600 Mbps	9	3	40 MHz		-68 dBm	now
Ryan's Laptop	341	0.1%	270 Mbps	6	2	40 MHz	-	-33 dBm	now
C2:00:AA:0B:03:03	420	0.3%	270 Mbps	6	2	40 MHz	54.8%	-71 dBm	now
Apple_00:D8:94	23	0.0%	-	-	-	20 MHz			now
94:0C:98:76:FE:49	30	0.1%	-	-	-	20 MHz			1 min ago
Kelly's Phone	14	0.0%	270 Mbps	6	2	40 MHz		-83 dBm	now
Apple_A2:1A:00	58	0.0%	-	-	-	20 MHz			now
Apple_13:B9:3D	109	0.0%	24 Mbps	-	-	20 MHz		-77 dBm	now
Apple_0A:7B:3C	12	0.0%	-	-	-	20 MHz			< 30 sec ago
Apple_E7:FE:2A	37	0.0%	-	-	-	20 MHz			< 1 min ago
Ryan's iPhone	139	0.1%	120 Mbps	5	1	40 MHz		-49 dBm	now

Connected Devices: Intel(R) Dual Band Wireless-AC 8265 [scan], Realtek 8814AU Wireless LAN 802.11ac USB NIC [scan], Alfa AWUS1900 [packets]

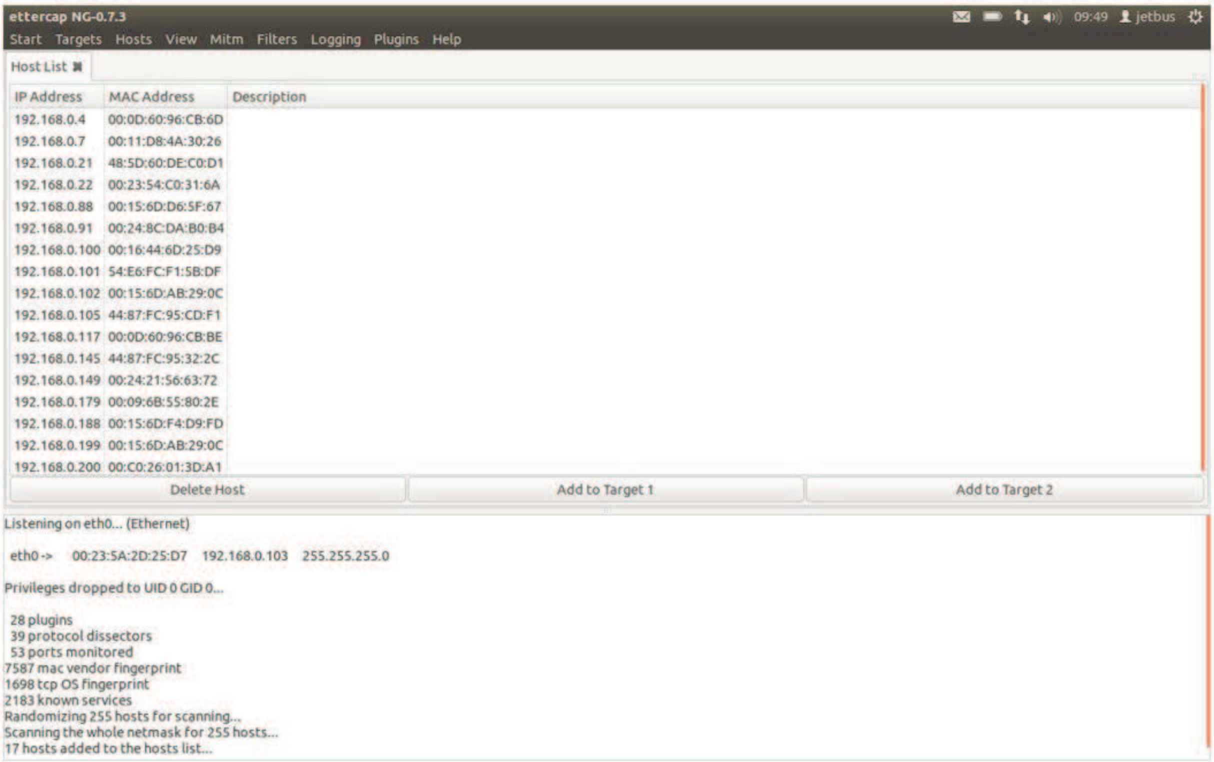
Version 5.1.27

Fig. 7. Kismet software display when identifying Wi-Fi



```
Listening on eth1... (Ethernet)

 eth1 ->    00:21:00:AE:09:04   192.168.0.132   255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

 28 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
```

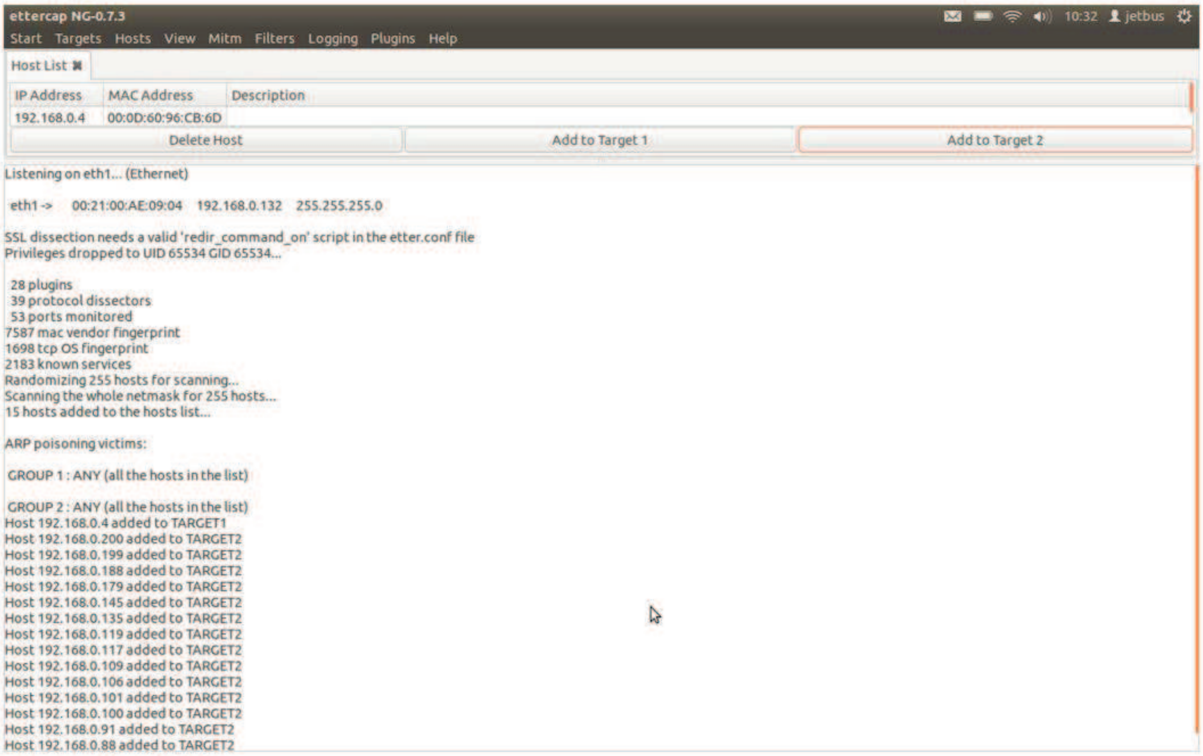
Fig. 8. Second step display for device eth1



IP Address	MAC Address	Description
192.168.0.4	00:0D:60:96:CB:6D	
192.168.0.7	00:11:D8:4A:30:26	
192.168.0.21	48:5D:60:DE:C0:D1	
192.168.0.22	00:23:54:C0:31:6A	
192.168.0.88	00:15:6D:D6:5F:67	
192.168.0.91	00:24:8C:DA:B0:B4	
192.168.0.100	00:16:44:6D:25:D9	
192.168.0.101	54:E6:FC:F1:5B:DF	
192.168.0.102	00:15:6D:AB:29:0C	
192.168.0.105	44:87:FC:95:CD:F1	
192.168.0.117	00:0D:60:96:CB:BE	
192.168.0.145	44:87:FC:95:32:2C	
192.168.0.149	00:24:21:56:63:72	
192.168.0.179	00:09:6B:55:80:2E	
192.168.0.188	00:15:6D:F4:D9:FD	
192.168.0.199	00:15:6D:AB:29:0C	
192.168.0.200	00:C0:26:01:3D:A1	

```
Listening on eth0... (Ethernet)

 eth0 ->    00:23:5A:2D:25:D7   192.168.0.103   255.255.255.0

Privileges dropped to UID 0 GID 0...

 28 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
17 hosts added to the hosts list...
```

Fig. 9. Second step display for device eth0



IP Address	MAC Address	Description
192.168.0.4	00:0D:60:96:CB:6D	

```
Listening on eth1... (Ethernet)

 eth1 ->    00:21:00:AE:09:04   192.168.0.132   255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

 28 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
15 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Host 192.168.0.4 added to TARGET1
Host 192.168.0.200 added to TARGET2
Host 192.168.0.199 added to TARGET2
Host 192.168.0.188 added to TARGET2
Host 192.168.0.179 added to TARGET2
Host 192.168.0.145 added to TARGET2
Host 192.168.0.135 added to TARGET2
Host 192.168.0.119 added to TARGET2
Host 192.168.0.117 added to TARGET2
Host 192.168.0.109 added to TARGET2
Host 192.168.0.106 added to TARGET2
Host 192.168.0.101 added to TARGET2
Host 192.168.0.100 added to TARGET2
Host 192.168.0.91 added to TARGET2
Host 192.168.0.88 added to TARGET2
```

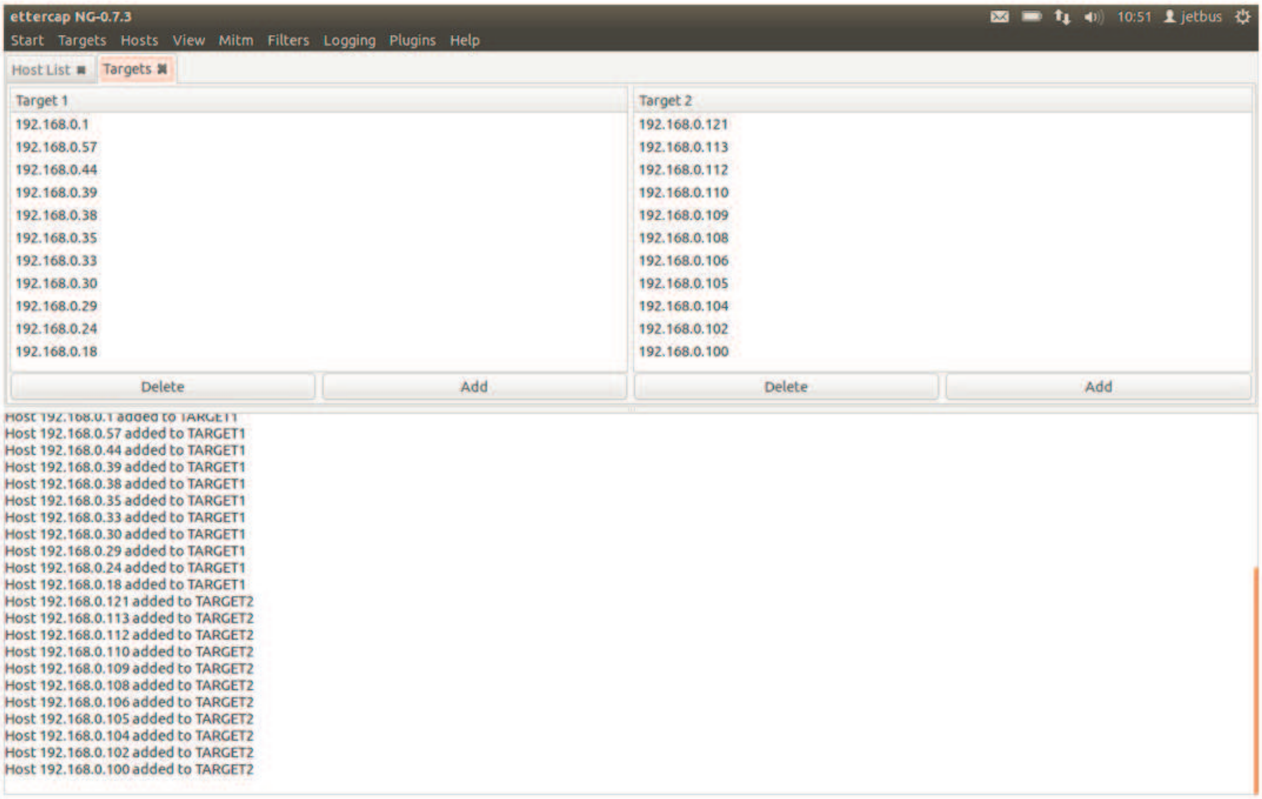
Fig. 10. The display of the third step scans the target host

Fig. 10 – is what the Ettercap software displays when scanning a host, it contains information about the IP Address of the host connected to the Wi-Fi network and cable network.

– The fourth step selects the target host.

Fig. 11 is a step to select the host that will be the target of attack, there are two classifications of targets, namely target 1 is the main target to be attacked, target 2 is an alternative target if target 1 does not get results.

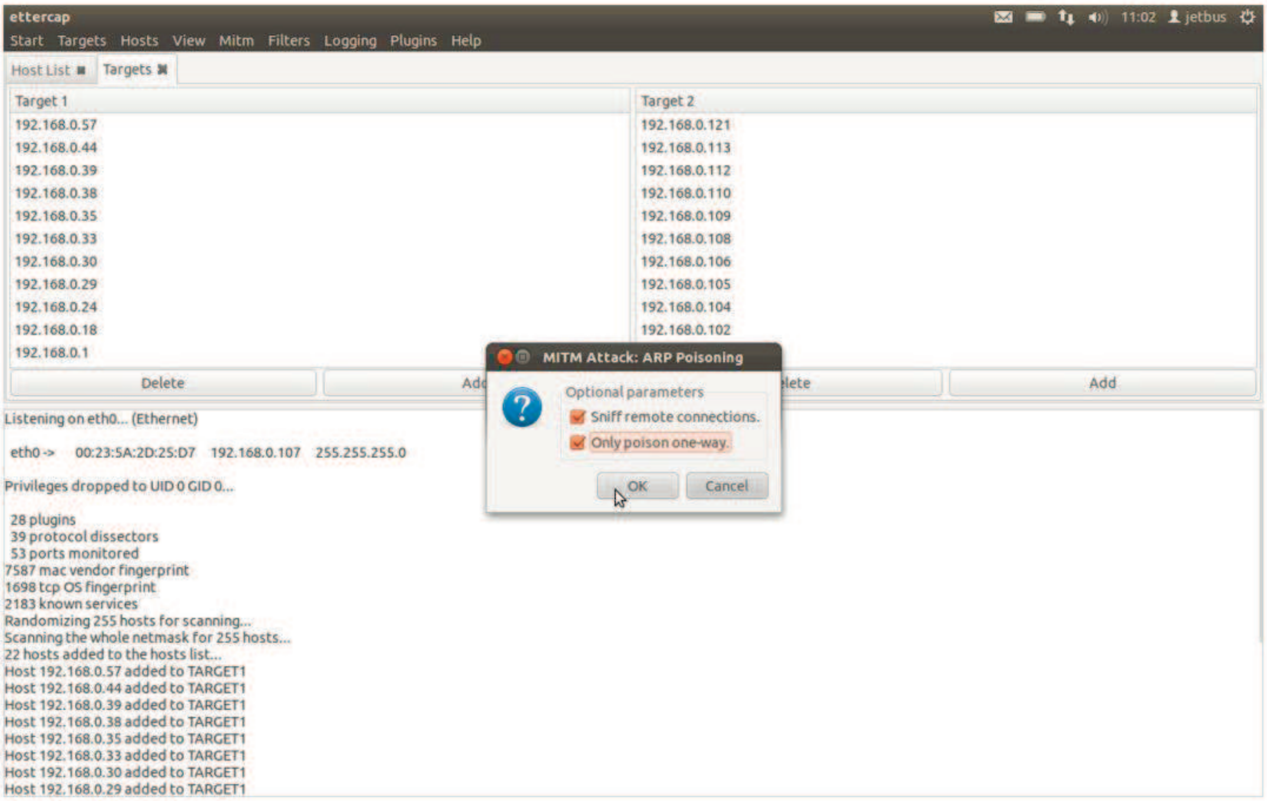
– Proceed to the fifth step and click on MITM Attack to initiate an attack. Choose ARP poisoning, enable sniffing of distant connections, and pick the option to poison just one-way. This will execute ARP poisoning on the host that the author has already registered as targets 1 and 2.



Target 1	Target 2
192.168.0.1	192.168.0.121
192.168.0.57	192.168.0.113
192.168.0.44	192.168.0.112
192.168.0.39	192.168.0.110
192.168.0.38	192.168.0.109
192.168.0.35	192.168.0.108
192.168.0.33	192.168.0.106
192.168.0.30	192.168.0.105
192.168.0.29	192.168.0.104
192.168.0.24	192.168.0.102
192.168.0.18	192.168.0.100

```
Host 192.168.0.1 added to TARGET1
Host 192.168.0.57 added to TARGET1
Host 192.168.0.44 added to TARGET1
Host 192.168.0.39 added to TARGET1
Host 192.168.0.38 added to TARGET1
Host 192.168.0.35 added to TARGET1
Host 192.168.0.33 added to TARGET1
Host 192.168.0.30 added to TARGET1
Host 192.168.0.29 added to TARGET1
Host 192.168.0.24 added to TARGET1
Host 192.168.0.18 added to TARGET1
Host 192.168.0.121 added to TARGET2
Host 192.168.0.113 added to TARGET2
Host 192.168.0.112 added to TARGET2
Host 192.168.0.110 added to TARGET2
Host 192.168.0.109 added to TARGET2
Host 192.168.0.108 added to TARGET2
Host 192.168.0.106 added to TARGET2
Host 192.168.0.105 added to TARGET2
Host 192.168.0.104 added to TARGET2
Host 192.168.0.102 added to TARGET2
Host 192.168.0.100 added to TARGET2
```

Fig. 11. The fourth step displays selecting the Target Host


ettercap
11:02 jetbus
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
Targets
Delete
Add
Delete
Add
MITM Attack: ARP Poisoning
OK
Cancel

Target 1	Target 2
192.168.0.57	192.168.0.121
192.168.0.44	192.168.0.113
192.168.0.39	192.168.0.112
192.168.0.38	192.168.0.110
192.168.0.35	192.168.0.109
192.168.0.33	192.168.0.108
192.168.0.30	192.168.0.106
192.168.0.29	192.168.0.105
192.168.0.24	192.168.0.104
192.168.0.18	192.168.0.102
192.168.0.1	

Optional parameters

☑ Sniff remote connections.

☑ Only poison one-way.

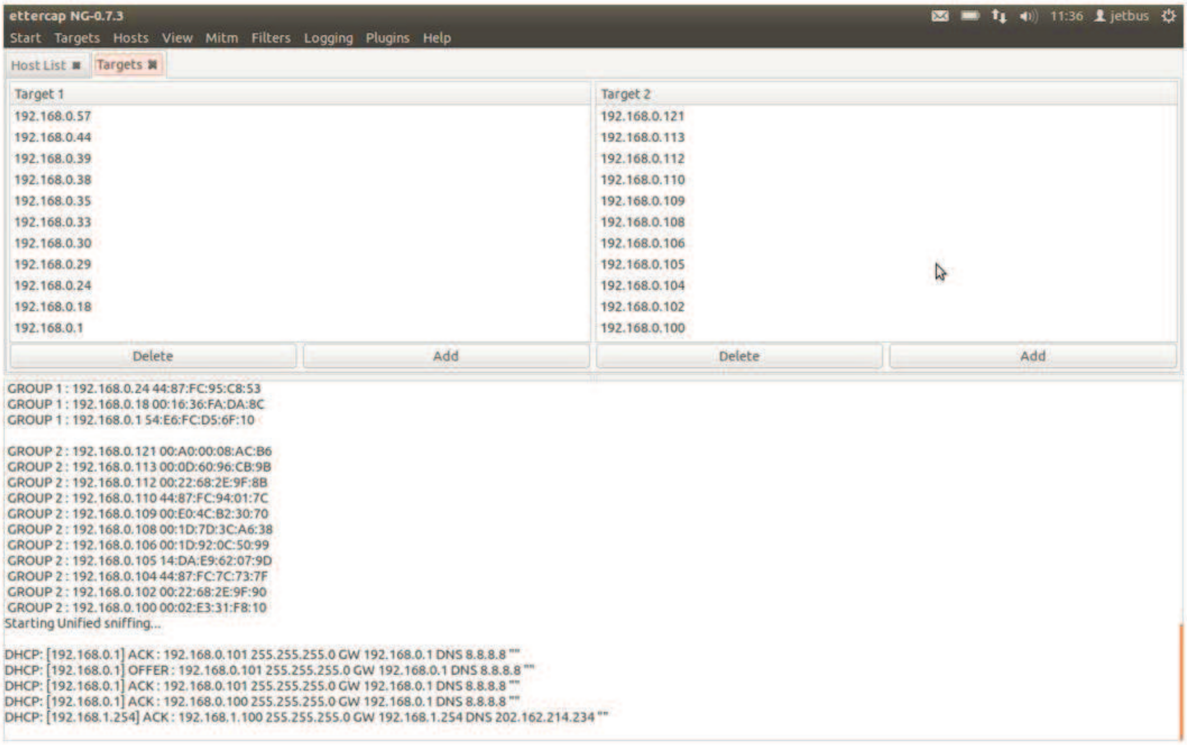
```
Listening on eth0... (Ethernet)

 eth0 ->   00:23:5A:2D:25:D7   192.168.0.107   255.255.255.0

Privileges dropped to UID 0 GID 0...

 28 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
22 hosts added to the hosts list...
Host 192.168.0.57 added to TARGET1
Host 192.168.0.44 added to TARGET1
Host 192.168.0.39 added to TARGET1
Host 192.168.0.38 added to TARGET1
Host 192.168.0.35 added to TARGET1
Host 192.168.0.33 added to TARGET1
Host 192.168.0.30 added to TARGET1
Host 192.168.0.29 added to TARGET1
```

Fig. 12. Display of the fifth step to carry out a Packet Sniffing attack

Fig. 12 is a display of the steps to carry out a packet sniffing attack, the author selects ARP Poisoning and ticks sniff remote connections and only poison one-way so that he can record the user and password of the target's email and DNS account.

– Then in the sixth step, click start, select start sniffing

Fig. 13 is an example of the display of the results of a packet sniffing attack on Ettercap software which has recorded the target host accessing DNS from Google.



Target 1	Target 2
192.168.0.57	192.168.0.121
192.168.0.44	192.168.0.113
192.168.0.39	192.168.0.112
192.168.0.38	192.168.0.110
192.168.0.35	192.168.0.109
192.168.0.33	192.168.0.108
192.168.0.30	192.168.0.106
192.168.0.29	192.168.0.105
192.168.0.24	192.168.0.104
192.168.0.18	192.168.0.102
192.168.0.1	192.168.0.100

```
GROUP 1 : 192.168.0.24 44:87:FC:95:C8:53
GROUP 1 : 192.168.0.18 00:16:36:FA:DA:8C
GROUP 1 : 192.168.0.1 54:E6:FC:D5:6F:10

GROUP 2 : 192.168.0.121 00:A0:00:08:AC:B6
GROUP 2 : 192.168.0.113 00:0D:60:96:CB:9B
GROUP 2 : 192.168.0.112 00:22:68:2E:9F:8B
GROUP 2 : 192.168.0.110 44:87:FC:94:01:7C
GROUP 2 : 192.168.0.109 00:E0:4C:B2:30:70
GROUP 2 : 192.168.0.108 00:1D:7D:3C:A6:38
GROUP 2 : 192.168.0.106 00:1D:92:0C:50:99
GROUP 2 : 192.168.0.105 14:DA:E9:62:07:9D
GROUP 2 : 192.168.0.104 44:87:FC:7C:73:7F
GROUP 2 : 192.168.0.102 00:22:68:2E:9F:90
GROUP 2 : 192.168.0.100 00:02:E3:31:F8:10
Starting Unified sniffing...

DHCP: [192.168.0.1] ACK : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 8.8.8.8 ""
DHCP: [192.168.0.1] OFFER : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 8.8.8.8 ""
DHCP: [192.168.0.1] ACK : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 8.8.8.8 ""
DHCP: [192.168.0.1] ACK : 192.168.0.100 255.255.255.0 GW 192.168.0.1 DNS 8.8.8.8 ""
DHCP: [192.168.1.254] ACK : 192.168.1.100 255.255.255.0 GW 192.168.1.254 DNS 202.162.214.234 ""
```

Fig. 13. Display of packet sniffing attacks

3.RESULTS AND DISCUSSION

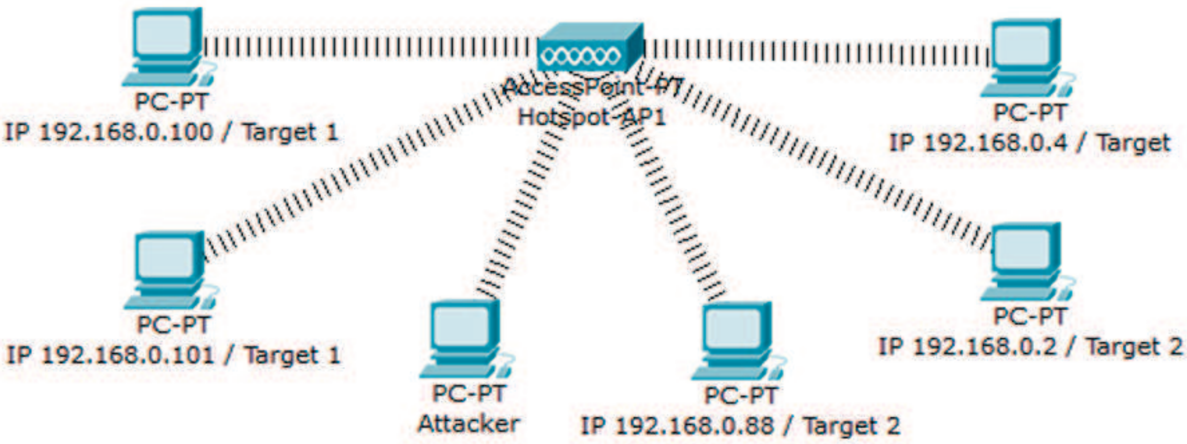
Analysis needs to be carried out to find out how safe the level of security that has been implemented in a cable or wireless network is. As we know, the level of security does not only come from existing hardware and software but the important role of humans/users who carry out the configuration and from designing the network itself.

Network Security installed within **University of Basrah campus** in general still needs improvement as proven by the Wi-Fi not using security or open. Apart from that, there are still many employees who are still unfamiliar with what is called computer network security.

Analysis of research results

Identifying Wifi: This experiment aimed to detect the presence of Wi-Fi by gathering comprehensive information about the network, including its kind and the security measures employed. This is done to make it easier for attacks to gain a connection with the existing Wi-Fi network. In this experiment the author found that Wi-Fi in the Basrah campus area was not secured / open.

Packet Sniffing: This experiment was carried out to obtain important information regarding the account username, password, intended DNS access and other information. This is intended so that attackers can access the internet illegally for personal gain which can result in losses to users on the network. In this experiment, information regarding the target's DNS access was successfully obtained and the author also obtained the email username and password from one of the targets. Thus, the author can state that it is not safe because all activities can be easily recorded and easily stolen.



PC-PT
IP 192.168.0.100 / Target 1
AccessPoint-PT
Hotspot-AP1
PC-PT
IP 192.168.0.4 / Target
PC-PT
IP 192.168.0.101 / Target 1
PC-PT
Attacker
PC-PT
IP 192.168.0.88 / Target 2
PC-PT
IP 192.168.0.2 / Target 2

Fig. 14. Attack simulation display

The image above is an illustration of a scenario where the attacker carries out an attack by grouping targets into two groups, namely target 1 and target 2, which functions when the main target or target 1 does not carry out any activity, the attack will move to target 2 and vice versa until the attacker can record all the activities that occur. walk.

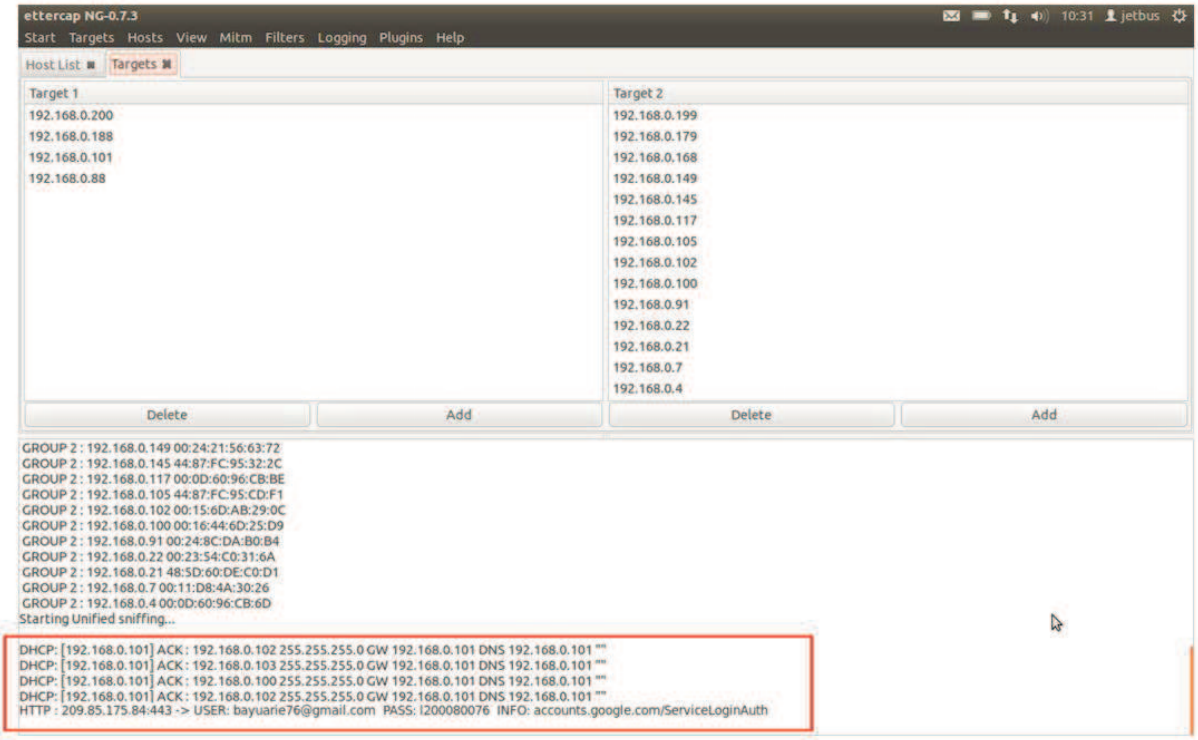
Because during research several times during working hours the author did not find any activity that accessed accounts and passwords, the author carried out two scenarios, namely:

First scenario with the following steps:

1. The author creates several new accounts and passwords.

2. Try logging into the account using the office computer.

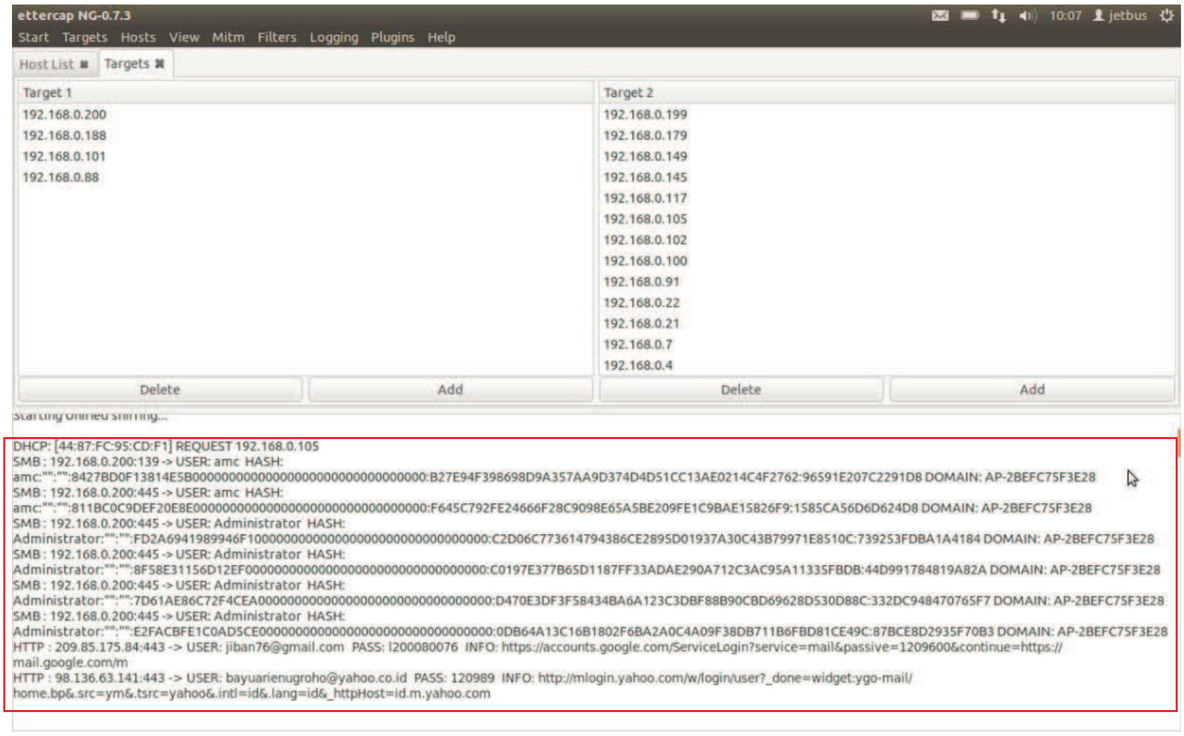
3. The author recorded the activities that occurred using *Ettercap* software.



Target 1	Target 2
192.168.0.200	192.168.0.199
192.168.0.188	192.168.0.179
192.168.0.101	192.168.0.168
192.168.0.88	192.168.0.149
	192.168.0.145
	192.168.0.117
	192.168.0.105
	192.168.0.102
	192.168.0.100
	192.168.0.91
	192.168.0.22
	192.168.0.21
	192.168.0.7
	192.168.0.4

```
GROUP 2 : 192.168.0.149 00:24:21:56:63:72
GROUP 2 : 192.168.0.145 44:87:FC:95:32:2C
GROUP 2 : 192.168.0.117 00:0D:60:96:CB:BE
GROUP 2 : 192.168.0.105 44:87:FC:95:CD:F1
GROUP 2 : 192.168.0.102 00:15:6D:AB:29:0C
GROUP 2 : 192.168.0.100 00:16:44:6D:25:D9
GROUP 2 : 192.168.0.91 00:24:8C:DA:B0:B4
GROUP 2 : 192.168.0.22 00:23:54:C0:31:6A
GROUP 2 : 192.168.0.21 48:5D:60:DE:C0:D1
GROUP 2 : 192.168.0.7 00:11:D8:4A:30:26
GROUP 2 : 192.168.0.4 00:0D:60:96:CB:6D
Starting Unified sniffing...

DHCP: [192.168.0.101] ACK : 192.168.0.102 255.255.255.0 GW 192.168.0.101 DNS 192.168.0.101 ""
DHCP: [192.168.0.101] ACK : 192.168.0.103 255.255.255.0 GW 192.168.0.101 DNS 192.168.0.101 ""
DHCP: [192.168.0.101] ACK : 192.168.0.100 255.255.255.0 GW 192.168.0.101 DNS 192.168.0.101 ""
DHCP: [192.168.0.101] ACK : 192.168.0.102 255.255.255.0 GW 192.168.0.101 DNS 192.168.0.101 ""
HTTP : 209.85.175.84:443 -> USER: bayuarie76@gmail.com  PASS: l200080076  INFO: accounts.google.com/ServiceLoginAuth
```

Fig. 15. Results of Packet Sniffing attacks on Wi-Fi



Target 1	Target 2
192.168.0.200	192.168.0.199
192.168.0.188	192.168.0.179
192.168.0.101	192.168.0.149
192.168.0.88	192.168.0.145
	192.168.0.117
	192.168.0.105
	192.168.0.102
	192.168.0.100
	192.168.0.91
	192.168.0.22
	192.168.0.21
	192.168.0.7
	192.168.0.4

```
Starting Unified sniffing...

DHCP: [44:87:FC:95:CD:F1] REQUEST 192.168.0.105
SMB : 192.168.0.200:139 -> USER: amc  HASH:
amc:"":"":8427BD0F13814E5B00000000000000000000000000000000:B27E94F398698D9A357AA9D374D4D51CC13AE0214C4F2762:96591E207C2291D8 DOMAIN: AP-2BEFC75F3E28
SMB : 192.168.0.200:445 -> USER: amc  HASH:
amc:"":"":811BC0C9DEF20E8E00000000000000000000000000000000:F645C792FE24666F28C9098E65A5BE209FE1C9BAE15826F9:1585CA56D6D624D8 DOMAIN: AP-2BEFC75F3E28
SMB : 192.168.0.200:445 -> USER: Administrator  HASH:
Administrator:"":"":FD2A6941989946F100000000000000000000000000000000:C2D06C773614794386CE2895D01937A30C43B79971E8510C:739253FDBA1A4184 DOMAIN: AP-2BEFC75F3E28
SMB : 192.168.0.200:445 -> USER: Administrator  HASH:
Administrator:"":"":8F58E31156D12EF000000000000000000000000000000000:C0197E377B65D1187FF33ADAE290A712C3AC95A11335FBDB:44D991784819A82A DOMAIN: AP-2BEFC75F3E28
SMB : 192.168.0.200:445 -> USER: Administrator  HASH:
Administrator:"":"":7D61AE86C72F4CEA00000000000000000000000000000000:D470E3DF3F58434BA6A123C3DBF88B90CBD69628D530D88C:332DC948470765F7 DOMAIN: AP-2BEFC75F3E28
SMB : 192.168.0.200:445 -> USER: Administrator  HASH:
Administrator:"":"":E2FACBFE1C0AD5CE00000000000000000000000000000000:0DB64A13C16B1802F6BA2A0C4A09F38DB711B6FBD81CE49C:87BCE8D2935F70B3 DOMAIN: AP-2BEFC75F3E28
HTTP : 209.85.175.84:443 -> USER: jiban76@gmail.com  PASS: l200080076  INFO: https://accounts.google.com/ServiceLogin?service=mail&passive=1209600&continue=https://
mail.google.com/m
HTTP : 98.136.63.141:443 -> USER: bayuarienugroho@yahoo.co.id  PASS: 120989  INFO: http://mlogin.yahoo.com/w/login/user?_done=widget:ygo-mail/
home.bp&.src=ym&.tsrc=yahoo&.intl=id&.lang=id&_httpHost=id.m.yahoo.com
```

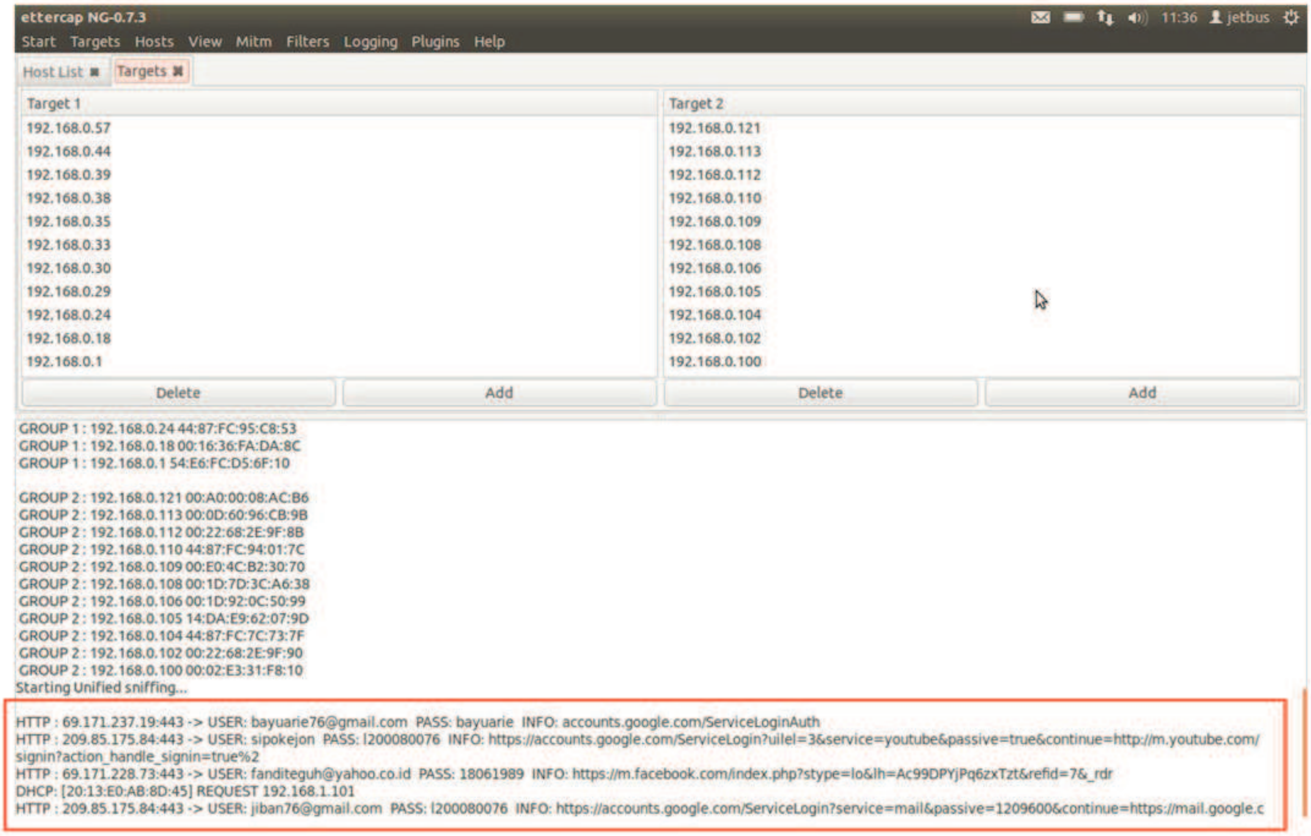
Fig. 16. Results of Packet Sniffing attacks on cable networks at the University of Basrah campus

Fig. 15, it can be explained that the software can record several activities which are marked with red rectangles, namely in lines 1 to 4 where message communication is taking place between computers and computers in one network to ensure that they are still connected in one network but are not connected by other computer users. This means that the user does not communicate, but the computer automatically sends the message itself, which is called ACK (Acknowledgement). Then the last line explains that one of the client computers accessed the recorded Google Mail account.

Fig. 16 can explain that in lines 1 to 13 in the red rectangle file sharing is taking place between the server and client but the recorded message is encrypted so the author cannot describe it. Meanwhile, in lines 14 to 17 there are two client computers that are logging in to a Google Mail account and Yahoo Mail account.

Second scenario: The author changes the password and randomizes several new accounts and passwords.

Fig. 17 explained that accounts whose passwords were changed and several accounts and passwords that were scrambled could be recorded. From the analysis of the results obtained, the author obtained a discussion of the University of Basrah compus, Basrah and found several reasons why the Wi-Fi at the **TelNav** Office was not provided with security or was open, here are the reasons:



Target 1	Target 2
192.168.0.57	192.168.0.121
192.168.0.44	192.168.0.113
192.168.0.39	192.168.0.112
192.168.0.38	192.168.0.110
192.168.0.35	192.168.0.109
192.168.0.33	192.168.0.108
192.168.0.30	192.168.0.106
192.168.0.29	192.168.0.105
192.168.0.24	192.168.0.104
192.168.0.18	192.168.0.102
192.168.0.1	192.168.0.100

```
GROUP 1 : 192.168.0.24 44:87:FC:95:C8:53
GROUP 1 : 192.168.0.18 00:16:36:FA:DA:8C
GROUP 1 : 192.168.0.1 54:E6:FC:D5:6F:10

GROUP 2 : 192.168.0.121 00:A0:00:08:AC:B6
GROUP 2 : 192.168.0.113 00:0D:60:96:CB:9B
GROUP 2 : 192.168.0.112 00:22:68:2E:9F:8B
GROUP 2 : 192.168.0.110 44:87:FC:94:01:7C
GROUP 2 : 192.168.0.109 00:E0:4C:B2:30:70
GROUP 2 : 192.168.0.108 00:1D:7D:3C:A6:38
GROUP 2 : 192.168.0.106 00:1D:92:0C:50:99
GROUP 2 : 192.168.0.105 14:DA:E9:62:07:9D
GROUP 2 : 192.168.0.104 44:87:FC:7C:73:7F
GROUP 2 : 192.168.0.102 00:22:68:2E:9F:90
GROUP 2 : 192.168.0.100 00:02:E3:31:F8:10
Starting Unified sniffing...

HTTP : 69.171.237.19:443 -> USER: bayuarie76@gmail.com  PASS: bayuarie  INFO: accounts.google.com/ServiceLoginAuth
HTTP : 209.85.175.84:443 -> USER: sipokejon  PASS: l200080076  INFO: https://accounts.google.com/ServiceLogin?uilel=3&service=youtube&passive=true&continue=http://m.youtube.com/
signin?action_handle_signin=true%2
HTTP : 69.171.228.73:443 -> USER: fanditeguh@yahoo.co.id  PASS: 18061989  INFO: https://m.facebook.com/index.php?stype=lo&lh=Ac99DPYjPq6zxTzt&refid=7&_rdr
DHCP: [20:13:E0:AB:8D:45] REQUEST 192.168.1.101
HTTP : 209.85.175.84:443 -> USER: jiban76@gmail.com  PASS: l200080076  INFO: https://accounts.google.com/ServiceLogin?service=mail&passive=1209600&continue=https://mail.google.c
```

Fig. 17. Results of Packet Sniffing attacks on cable networks in new buildings

1. Wi-Fi installed in the civil defence room is a facility for visitors or service users, while waiting students can access the internet easily and for free.

2. The Wi-Fi installed at the TelNav Office is the main Wi-Fi, if one day you want to add more Wi-Fi, it is not difficult to configure it.

The essence of the two discussions above is the Wi-Fi installed at University of Basrah compus, Basrah is used as a public facility, not for commercial purposes, so it is not provided with security measures such as WEP, WPA, WPA2 and others so that service users can easily and quickly connect to the internet.

Solutions to Prevent Packet Sniffing Attacks

After conducting research, the author has prepared several recommended solutions to improve network security from attacks, such as what the author did to analyse network security that can be implemented by University of Basrah compus, Basrah, such as:

1. Differentiate between the office Wi-Fi/LAN network and Wi-Fi for service user facilities, so that when an attacker attack using the Packet Sniffing technique, they cannot penetrate the office Wi-Fi/LAN network. Technically, the above solution can be applied by resetting the subnetting, for office Wi-Fi/LAN, for example 6 hosts for employee LAN switch1, IP 7 hosts for employee LAN switch2 and for public Wi-Fi for 24 hosts.

Fig. 18 explained that by differentiating the network IP, packet sniffing attacks cannot enter another network to intercept ongoing data traffic, because in the system packet sniffing runs at layer 2.

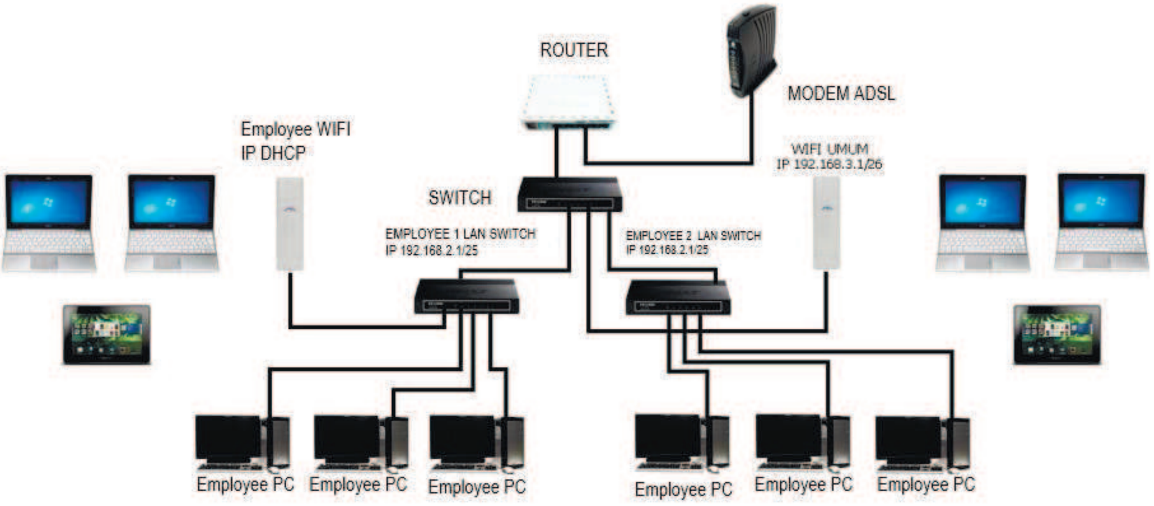


Fig. 18. Differences between office and public internet networks

Binding IP and MAC Address

One method that can be used to overcome ARP

Spoofing on a network is by binding IP and MAC addresses. This method works by registering every user connected to the network at the gateway. Each user has an IP address and MAC address tied to it so that the gateway will not send the wrong packet to the user. By using this method, ARP Spoofing can be prevented.

Use WPA2-PSK and Radius encryption security in the room area to secure the office $Wi - Fi$ network so that the signal doesn't go too far and only employees know.

Alternative Solution to Prevent Packet Sniffing Attacks for Linux Users (As Client and Server)

Actually, you can easily prevent Arp Spoofing by changing the arp table from dynamic to static. However, it is not enough to just create a static arp table between Mac Address and IP, because the technique of creating a static arp table can only prevent arp spoofing scenarios. If an attacker is spoofing the gateway, of course the client arp table and gateway arp table must be made static too, with the help of $ArpOn$ we can prevent the attacker from spoofing using this mode.

Conclusion

Based on the data analysis and attack attempts, it can be concluded that the LAN network security system including wired and wireless networks in University of Basrah compus,basrah, Governorate, Iraq still needs improvement, as demonstrated by:

1. $inSSIDer$ app detects open Wi-Fi security.

2. Packet sniffing attacks that can record and display usernames and passwords using the Ettercap application.

Recommendations

From the description of the conclusions, the above advantages and disadvantages can be lessons and references for the future. Suggestions to consider for the future include:

1. It is necessary to divide the network to differentiate networks for the public and networks for employees so that attacks do not occur through the public Wi-Fi network by irresponsible people to obtain important information that passes through the employee's computer network.

2. The need for WPA2-PSK security as initial Wi-Fi security in order to minimize packet sniffing attacks before they occur.

AUTHOR'S NOTE

The author declares that there is no conflict of interest regarding the publication of this article. The author confirmed that the paper was free of plagiarism.

References

1 Ansari, S., Rajeev, S. G., & Chandrashekar, H. S. (2003). Packet sniffing: A brief introduction. IEEE Potentials, 21(2), 17–19. https://doi.org/10.1109/MP.2002.1166620

2 Anu, P., & Vimala, S. (2017). A survey on sniffing attacks on computer networks. International Conference on Intelligent Computing and Control (I2C2), 1–5. https://doi.org/10.1109/I2C2. 2017.8321914

3 Bakare, B., & Minah-Eeba, W. (2019). A comprehensive review of wireless fidelity (Wi-Fi) technology in Nigeria. *IOSR Journal of Electronics and Communication Engineering*, 13(3), 37–42. https://doi.org/10.9790/2834-1303023742

4. Das, R., & Tuna, G. (2017). Packet tracing and analysis of network cameras with Wireshark. Proceedings of the 2017 International Symposium on Digital Forensics and Security (ISDFS), 1–6. https://doi.org/10.1109/ISDFS.2017.7916510

5. Fatimah, T. M., & Pernanda, A. Y. (2022). Wi-Fi network security analysis against packet sniffing attacks at Universitas PGRI Sumatera Barat. *JURTEII: Jurnal Teknologi Informasi*, 1(2), 7–11.

6. Fajaryanto, A., Dirgahayu, T., & Prayudi, Y. (2015). Implementation of the ISSAF and OWASP version 4 methods for web server vulnerability testing. *NERO Scientific Journal*, 1(3), 190–197.

7. Huai, S., & Zhongsheng, W. (2020). Research and implementation of future network router. *International Journal of Advanced Network, Monitoring and Controls*, 5(1), 10–22. https://doi.org/10.21307/ijanmc-2020-012

8. Shihab, L. A. (2022). Study and evaluation of wireless sensor networks performance. *Webology*, 19(1).

9. Shihab, L. A. (2025). Real time attack prevention for industrial IoT network. *Journal of Machine and Computing*, 5(4).

10. Nazir, R., Laghari, A., Kumar, K., David, S., & Ali, M. (2021). Survey on wireless network security. *Archives of Computational Methods in Engineering*, 29(5). https://doi.org/10.1007/s11831-021-09631-5

11. Paravathi, C., Roshini, D., & Nayak, S. S. (2014). Packet sniffing. *International Journal of Engineering and Management Research*, 14(1), 71–76.

12. Prabadevi, B., & Nagamalai, J. (2018). A review on various sniffing attacks and its mitigation techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, 12(3), 1117–1125. https://doi.org/10.11591/ijeecs.v12.i3.pp1117-1125

13. Qadeer, M., Iqbal, A., Zahid, M., & Siddiqui, M. (2010). Network traffic analysis and intrusion detection using packet sniffer. International Conference on Communication Software and Networks (ICCSN), 313–317. https://doi.org/10.1109/ ICCSN. 2010.104

14. Rahman, R., & Tomar, D. (2018). Security attacks on wireless networks and their detection techniques. In Advances in Information Communication Technology and Computing (pp. 185–201). Springer. https://doi.org/10.1007/978-981-13-0396-8_13

[15]. Rusdan, M., Manurung, D., & Genta, F. (2020). Evaluation of wireless network security using information system security assessment framework (ISSAF): Case study of PT. Keberlanjutan Strategis Indonesia. *Test Engineering and Management*, 83, 15714–15719.

16. Surarapu, P., Mahadasa, R., Vadiyala, V. R., & Baddam, P. R. (2023). An overview of Kali Linux: Empowering ethical hackers with unparalleled features. *Journal of Emerging Technologies*, 1, 171–180.

17. Sadkhan, S. B., & Abbas, N. (2013). Privacy and security of wireless communication networks. In Mobile networks and cloud computing convergence for progressive services and applications (pp. 58–78). IGI Global.

18. University of Basrah (n. d.). Official website. Retrieved from https://www.uobasrah.edu.iq

19. Xiao, M., & Guo, M. (2020). Computer network security and preventive measures in the age of big data. *Procedia Computer Science*, 166, 438–442. https://doi.org/10.1016/j.procs.2020. 02.068

Луай Абдулвахід Шихаб, Хазім Н. Вахіб

Університет Басри, м. Басра, Ірак

АНАЛІЗ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПРОТИ ПЕРЕХОПЛЕННЯ ПАКЕТІВ: КЕЙС КОЛЕДЖУ СЕСТРИНСЬКОЇ СПРАВИ

Суспільство отримало значні переваги від технологічного розвитку, особливо у сфері інформації, однією з найважливіших складових якого є інтернет. Користувачі інтернету застосовують як дротові (LAN), так і бездротові мережі (Wi-Fi). Однак існує загроза атак з боку недобросовісних осіб – хакерів, які можуть отримати доступ до важливих даних користувачів, перехоплювати інформацію (наприклад, паролі) та змінювати дані.

У цьому дослідженні здійснено оцінювання рівня безпеки Wi-Fi у кампусі Університету Басри (м. Басра, провінція Басра, Ірак) із використанням програм Aircrack-ng, Kismet та Ettercap. Aircrack-ng – це інструмент для зламу Wi-Fi, який застосовують для виявлення та ідентифікації відкритих бездротових сигналів. Kismet є альтернативним програмним забезпеченням із подібним функціоналом. Ettercap – це інструмент для перехоплення пакетів, що використовується для аналізу мережевих протоколів та аудиту безпеки мереж; він також може блокувати трафік у LAN-мережах, викрадати паролі та здійснювати активне прослуховування загальновживаних протоколів.

Дослідження містило два етапи. Перший – ідентифікація наявності та рівня безпеки Wi-Fi за допомогою програмного забезпечення Kismet. На другому етапі було здійснено атаку з перехопленням пакетів за допомогою програмного забезпечення Ettercap як метод перевірки безпеки Wi-Fi у кампусі Університету Басри.

Ключові слова: аналіз комп'ютерної мережі, мережева безпека, перехоплення пакетів.

Інформація про авторів:

Luay Abdulwahid Shihab, Assistant Professor in College of Nursing.
Email: luaay.abdulwahid@uobasrah.edu.iq

Hazim N. Waheeb, Assistant teacher, department of community health nursing in College of Nursing.
Email: hazim.waheeb@uobasrah.edu.iq

Цитування за ДСТУ: Шихаб Л. А., Вахіб Х. Н. Аналіз безпеки комп'ютерної мережі проти перехоплення пакетів: кейс Коледжу медсестринства. *Український журнал інформаційних технологій*. 2025, т. 7, № 2. С. 106–119.

Citation APA: Shihab, L. A., & Waheeb, H. N. (2025). Analysis of computer network security against packet interception: A case study of the College of Nursing. *Ukrainian Journal of Information Technology*, 7(2), 106–119. https://doi.org/10.23939/ujit2025.02.106