Security Vulnerability Analysis Of A Wireless Network With Wpa2 Encryption Using Cain And Abel

Ofonime Dominic Okon[1]
Department Of Electrical/Electronic and Computer Engineering
University of Uyo, Akwa Ibom State Nigeria

Ekpedeme John[2]
Department Of Electrical/Electronic and Computer Engineering
University of Uyo, Akwa Ibom State Nigeria

Henshaw Jumbo [3]
Department of Computer Engineering Heritage Polytechnic, Eket
Akwa Ibom State Nigeria
henshawjumbo@yahoo.com

***Abstract*— In this paper, security vulnerability analysis of a wireless network with WPA2 encryption using Cain and Abel is presented. Security vulnerability analysis of a wireless network entails a study explicitly conducted using penetration testing tools and observation to detect security lapses or flaws in the network which can be exploited. The penetration testing was conducted on a small case study wireless network set up comprising of MTN Router, two laptops, along with some mobile phones. The results show that Cain and Abel was able to view the network traffic and also resolve the domain name server of both source and destination IP addresses with the time of communication between them in real-time. However, Cain and Abel was not able to capture and save the displayed traffic for further analysis. Also, Cain and Abel was able to initiate a man-in-the-middle attack through ARP poisoning using. Spoofing of mac-address was effectively carried out by Cain and Abel during the ARP poisoning session. This attack compromised the integrity and availability of the needed information. In addition, Cain and Abel was used to sniff the wireless devices connected to the network and also expose their wireless passwords. This attack compromised all the 3 aspects of the confidentiality, integrity and availability (CIA) triad. In all, the study shows that Cain and Abel tool can be effective in conducting security vulnerability analysis of a wireless network with WPA2 encryption, especially for the three security concerns considered in this work.**

Keywords— Cybersecurity, Wireless Network, WPA2 Encryption, Vulnerability Analysis, Cain and Abel Software

1.0 Introduction

Today, in virtually every aspect of human activity, wireless network has an application [1,2,3,4]. When compare with the wired and fiber optic networks [5,6, 7, 8,9, 10,11, 12,13, 14, 15, 16,17,18] with their high bandwidth specifications, the wireless technologies have dominated because of each of deployment. Moreover, beyond the terrestrial applications [19,20], wireless technologies are increasingly being used for satellite and deep space communications [21,21,22,23]. These diverse applications have placed wireless network among the most widely research area. The original basic challenges associated with wireless networks are limited bandwidth [24,25,26,27,28], signal propagation loss [29,30, 31,32,33,34,35,36], rain fading [37,38, 39, 40, 41, 42, 43, 44,45], multipath fading [46,47, 48,49,50], diffraction loss [51, 52, 53,54, 55,56], among others. However, today, the emergence of the wireless internet has given birth to increased dependency on online presence for individuals and organizations who aim to achieve progress in several areas like business transaction, access to information, data storage and distribution etc. This implies that lots of data are generated and transmitted daily. The safely and security of these data in storage and in-transit has become a burning issue [57, 58, 59, 60] and this has prompted the Institute of Electrical and Electronics Engineers (IEEE) to create several encryption techniques such as Wireless equivalence privacy (WEP) and WIFI Protected Access (Version 1 and 2) (WPA and WPA2) in a bid to ensure that data integrity is not compromised [61, 62, 63, 64, 65, 66, 67]. Unfortunately, as the number of users increases, the number of cyber-attackers has also increased [68,69,70,71] and data security has become critical since several vulnerabilities in the encryption are being detected and exploited to cause data breach in the network [72,73,74,75]. Accordingly, in this paper, experimental research was carried out to conduct a performance analysis of some of the cybersecurity tools in a case study wireless network with WPA2 encryption [76,77,78,79,80]. In the course of this research, a case study Wireless Lan was setup, then the needed tools were selected, and the diverse functionalities of the selected tools are tested. Finally, the result, recommendation and conclusion of the paper are presented.

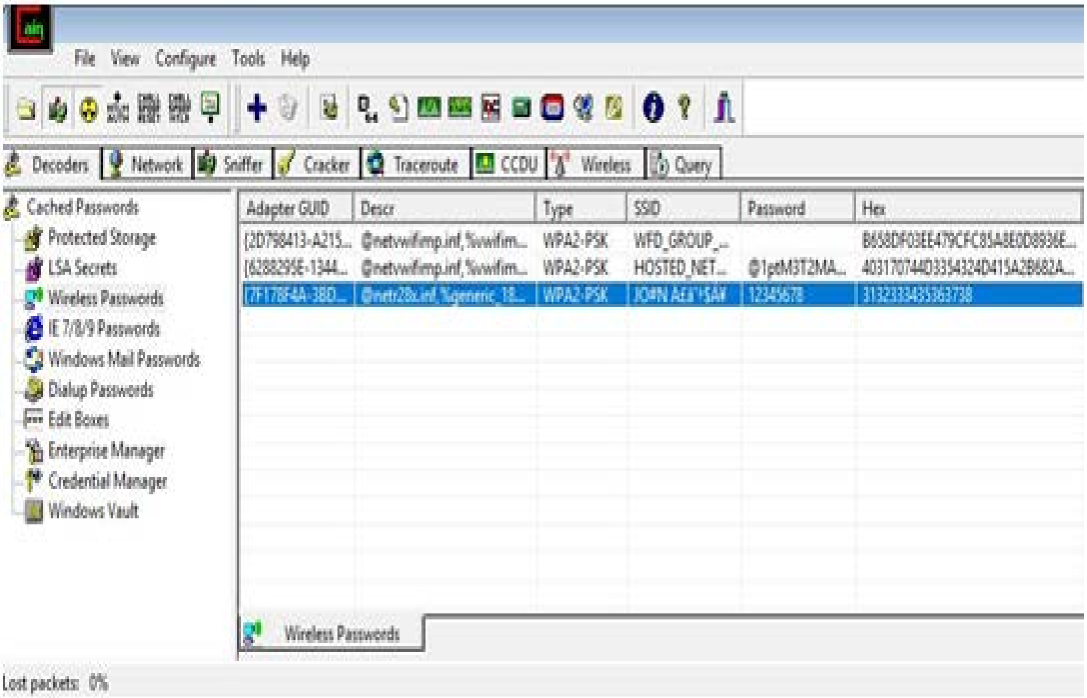
2.0 Methodology

Security vulnerability analysis of a wireless network entails a study explicitly conducted using penetration testing tools and observation to detect security lapses or flaws in the network which can be exploited. Accordingly, the focus of this paper is to conduct security vulnerability analysis of a wireless network with WPA2 encryption using Cain and Abel wireless network security testing software tool [81,82,83,84]. First, brief description of the Cain and Abel tool is presented along with the procedure for its installation. Subsequently, the following three wireless network security vulnerability issues for a wireless network with WPA2 encryption were analyzed using the Cain and Abel tool;

i. Password Decryption/Cracking
ii. Man-in-the-Middle Attack (ARP poison)
iii. Packet capturing/Intrusion detection

2.1 Description and Installation of Cain and Abel

Cain and Abel is a Windows Operating System-based password recovery software which employs several techniques to collect password hashes. It can collect the hash from the network, or extract it from the local machine. It employs several techniques such as dictionary attacks, brute force, and many other cryptanalysis techniques to decrypt passwords. It also sniffs the network for data, records VoIP conversations, and possesses other characteristics/functions more sophisticated than simple password cracking. The interface of Cain and Abel tool showing an exposed WIFI password is shown in **Figure 1**.



Adapter GUID	Descr	Type	SSID	Password	Hex
{2D798413-A215...	@netvwifimp.inf,%wifim...	WPA2-PSK	WFD_GROUP_...		B658DF03EE479CFC85A8E0D8936E...
{6288295E-1344...	@netvwifimp.inf,%wifim...	WPA2-PSK	HOSTED_NET...	@1ptM3T2MA...	403170744D3354324D415A2B682A...
{7F178F4A-38D...	@netr28x.inf,%generic_18...	WPA2-PSK	JO#N AÉä°$AV	12345678	3132333435363738

Figure 1 Cain and Abel Interface

In order to use the Cain & Abel tool, first there is need to download it and one option is to go to the download page at www.oxid.it/cain.html. After downloading the Cain and Abel self-installing executable package, run it and follow the installation instructions to complete the installation process. The detailed installation procedure of Cain and Abel is given as follows:

1. First, open your Web browser and search for Cain and Abel IDS.exe, your search engine will come up with a website that offers free download.
2. Download the Cain & Abel installation file via this link: https://win10fix.com/goto/cain-and-abel/download/
3. When the download is completed, double-click on the executable file to begin the installation and follow the instructions as presented by the self-installing file.
4. Click on the icon that appears on the desktop to launch the software on your PC

Note: Windows Defender and any other antivirus will immediately detect the Application as a virus, hence, you will need to deactivate all antivirus from your PC or you install it in a virtual box.

2.2 The security vulnerability concerns considered

In this study, the penetration testing was conducted on a small case study wireless network set up comprising of MTN Router, two laptops, along with some mobile phones. The following three wireless network security vulnerability issues for a wireless network with WPA2 encryption were analyzed using the Cain and Abel tool;

i. Password Decryption/Cracking
ii. Man-in-the-Middle Attack (ARP poison)
iii. Packet capturing/Intrusion detection

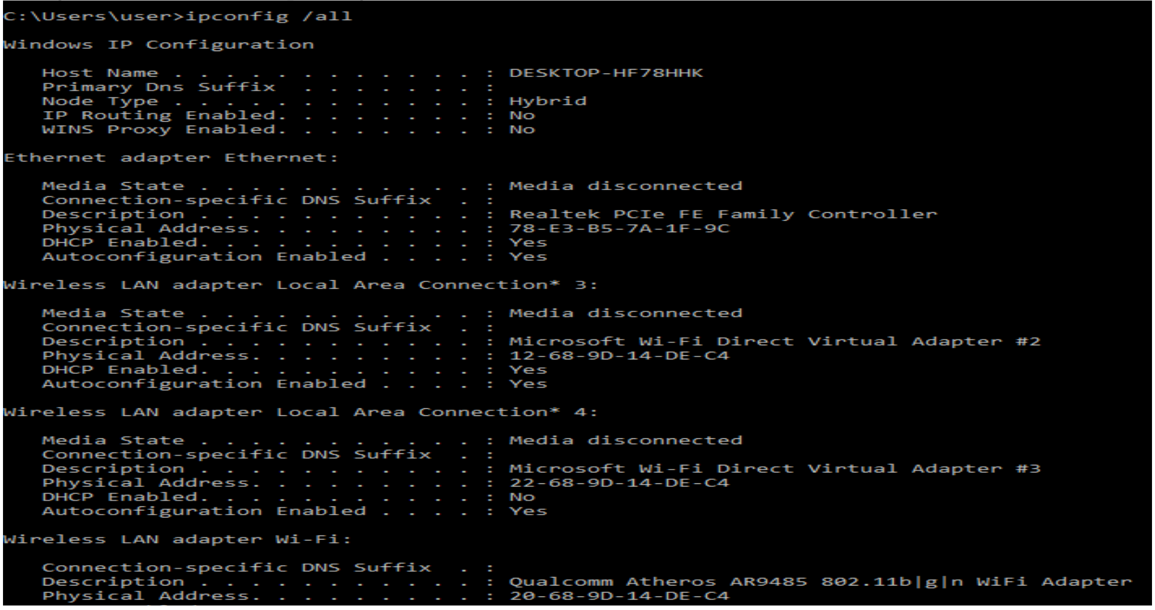
2.2.1 Password Decryption/Cracking using Cain and Abel software

Password decryption and cracking in this context is the exposure of password from encrypted packet. Essentially, it means using Cain and Abel software to decode the wireless network passwords that are stored in Windows operating system. In this paper, password decryption and cracking was carried out on Cain and Abel based on the following procedure:

Step 1: Launch the Cain and Abel software in a desktop system. At this point the Cain and Abel software has been downloaded and installed on the system.

Step 2: Discover all the MAC addresses on the system using the command prompt Windows IP Configuration command, "ipconfig /all"

First, the MAC address of the specific network card to be used for the sniffing need to be obtained. Accordingly, for Windows operating system, in a situation where there are more than one network card in the system, the MAC address of all the network cards can be obtained using the Command Prompt and typing "ipconfig /all" on the command line, as shown in Figure 2.

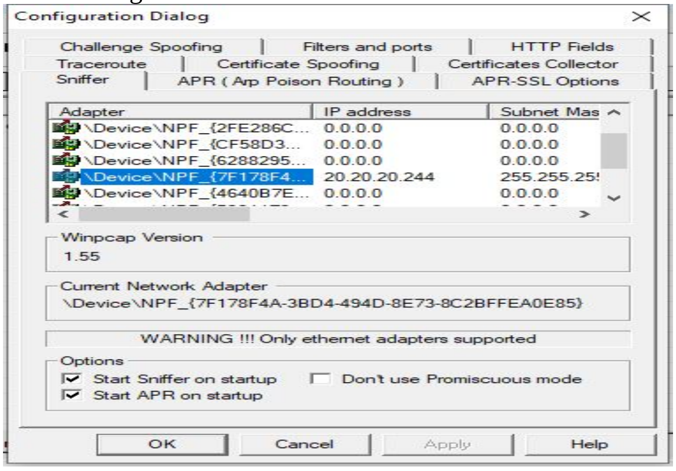


```
C:\Users\user>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-HF78HHK
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 78-E3-B5-7A-1F-9C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 12-68-9D-14-DE-C4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : 22-68-9D-14-DE-C4
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros AR9485 802.11b|g|n WiFi Adapter
   Physical Address. . . . . . . . . : 20-68-9D-14-DE-C4
```

Figure 2. The screenshot of the output of the "ipconfig /all" command on the command prompt

Step 3: Select the specific network interface

After launching the Cain and Abel software, launch the configuration dialog box from the Cain and Abel interface main menu. On the configuration dialog box the specific network interface which is already identified is selected, as shown in Figure 3.



Adapter	IP address	Subnet Mas
\Device\NPF_{2FE286C...	0.0.0.0	0.0.0.0
\Device\NPF_{CF58D3...	0.0.0.0	0.0.0.0
\Device\NPF_{6288295...	0.0.0.0	0.0.0.0
\Device\NPF_{7F178F4...	20.20.20.244	255.255.25!
\Device\NPF_{4640B7E...	0.0.0.0	0.0.0.0

Winpcap Version
1.55

Current Network Adapter
\Device\NPF_{7F178F4A-3BD4-494D-8E73-8C2BFFEA0E85}

WARNING !!! Only ethernet adapters supported

Options
☑ Start Sniffer on startup
□ Don't use Promiscuous mode
☑ Start APR on startup

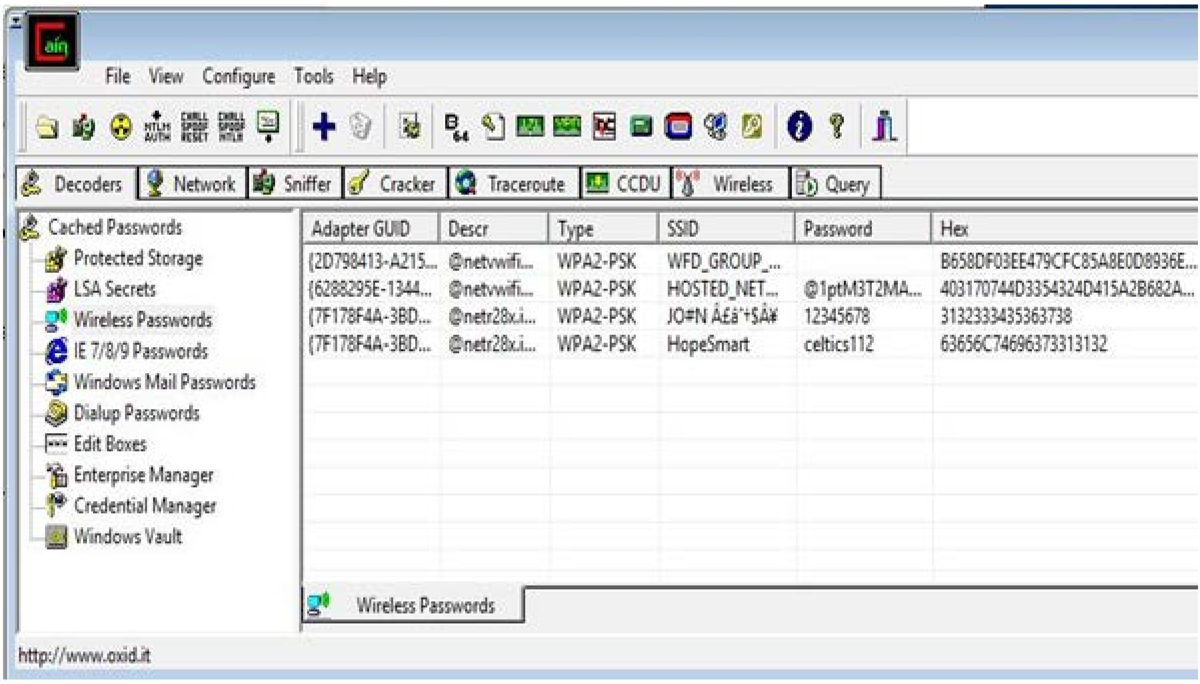
Figure 3 Select the targeted wireless interface

Step 4: Obtain and decode the wireless network passwords along with their encryption type and their SSID

This is achieved by selecting the Decoders tab and the select the Wireless Passwords on the left-hand side of the navigation menu that will appear when Decoders tab is selected. Next click on the + button on the toolbar.

At this point, the software begins to probe the wireless interface for all the wireless devices on the network and the click on the + button on the toolbar enables the software to dump the identified and decoded wireless network passwords along with their encryption type and their SSID on the decoders dialogue box as shown in Figure 4.

The result from the probe shows that the software was able to discover all the wireless devices connected to the case study wireless network and was also able to decrypt their respective wireless passwords.



Adapter GUID	Descr	Type	SSID	Password	Hex
{2D798413-A215...	@netvwifi...	WPA2-PSK	WFD_GROUP_...		B658DF03EE479CFC85A8E0D8936E...
{6288295E-1344...	@netvwifi...	WPA2-PSK	HOSTED_NET...	@1ptM3T2MA...	403170744D3354324D415A2B682A...
{7F178F4A-3BD...	@netr28x.i...	WPA2-PSK	JO#N Å£á˜+$Å¥	12345678	3132333435363738
{7F178F4A-3BD...	@netr28x.i...	WPA2-PSK	HopeSmart	celtics112	63656C74696373313132

Figure 4

Decrypted Wireless Password

2.2.2 Man-in-the-Middle Attack (ARP poison) using Cain and Abel software

This is a form of Man-in-the-middle attack that is made possible by exploiting the insecure nature of Address resolution protocol (ARP). Devices using ARP can accept frequent update which makes it possible for the malicious devices to force another device on the network to update its ARP cache with new values by sending ARP reply packet to the unsuspecting device. The device's correct IP address will then be matched with the attacker's mac-address. At this stage, the attacker can comfortably listen/communicate with other devices on the network disguising as the genuine host and can also exploit the exposed packet information.

Step 1 **Open the Cain & Abel** software and navigate to the MAC address scanner dialogue box on Cain & Abel Open Cain & Abel by double clicking its icon on the desktop.

On the Cain & Abel interface click on "Sniffer" tab (as shown in Figure 5(a)) and then on the toolbar click on "Start/Stop Sniffer" button (as shown in Figure 5(b)). Then, click on the + button (as shown in Figure 5(c)). At this point, the MAC address scanner dialogue box in Cain & Abel software will open

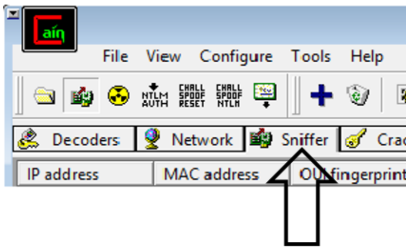


Figure 5(a) "Sniffer" tab

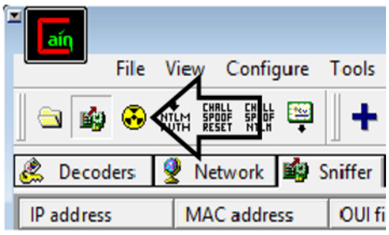


Figure 5(b) "Start/Stop Sniffer" button

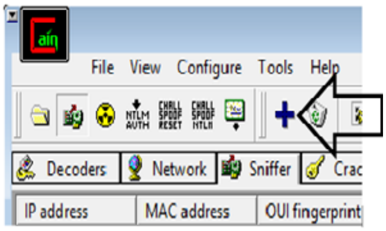
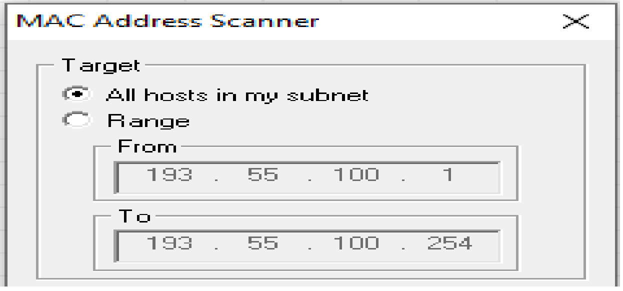


Figure 5(c) the + button

Step 2: Scan the network for list of target IP addresses

Set the range of target IP addresses on the MAC address scanner dialogue box. As shown in Figure 6, the range of target IP addresses is 193:55:100:1 to 193:55:100:254. Then select the "All Tests" checkbox on the MAC address scanner dialogue box as shown in Figure 6.



MAC Address Scanner

Target

● All hosts in my subnet

○ Range

From

193 . 55 . 100 . 1

To

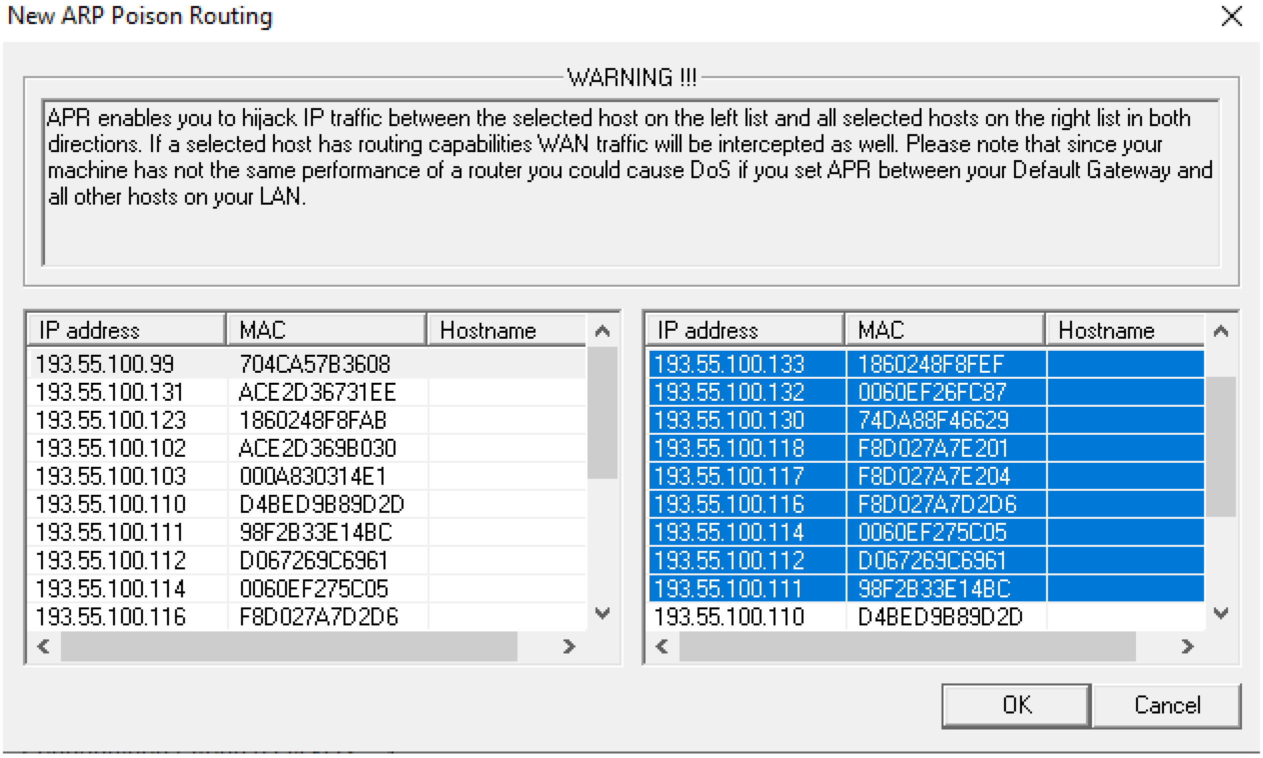
193 . 55 . 100 . 254

Figure 6 Screenshot showing how Cain and Abel uses the mac-address scanner feature to scan and discover all the usable IP-address host range in the wireless network.

The screenshot of the Poison Routing window is presented in Figure 7 and it presents the option of selecting the targeted **victim's** IP address and the network's gateway address with their corresponding mac-addresses.

Initiate the ARP poisoning requestor operation by clicking on the "Start/Stop APR" button, as shown in Figure 5(b).

The screenshot showing that the attacker has successfully implemented the attack is shown in Figure 8, w where you will notice that the traffic from the victim's PC are re-routed through the PC with IP address of 193:55:100:99 and corresponding MAC address of 704CA5783608. From this stage, the PC with IP address of 193:55:100:99 and corresponding MAC address of 704CA5783608 can monitor the victim's internet activities and the information can be used for subsequent attacks.



New ARP Poison Routing

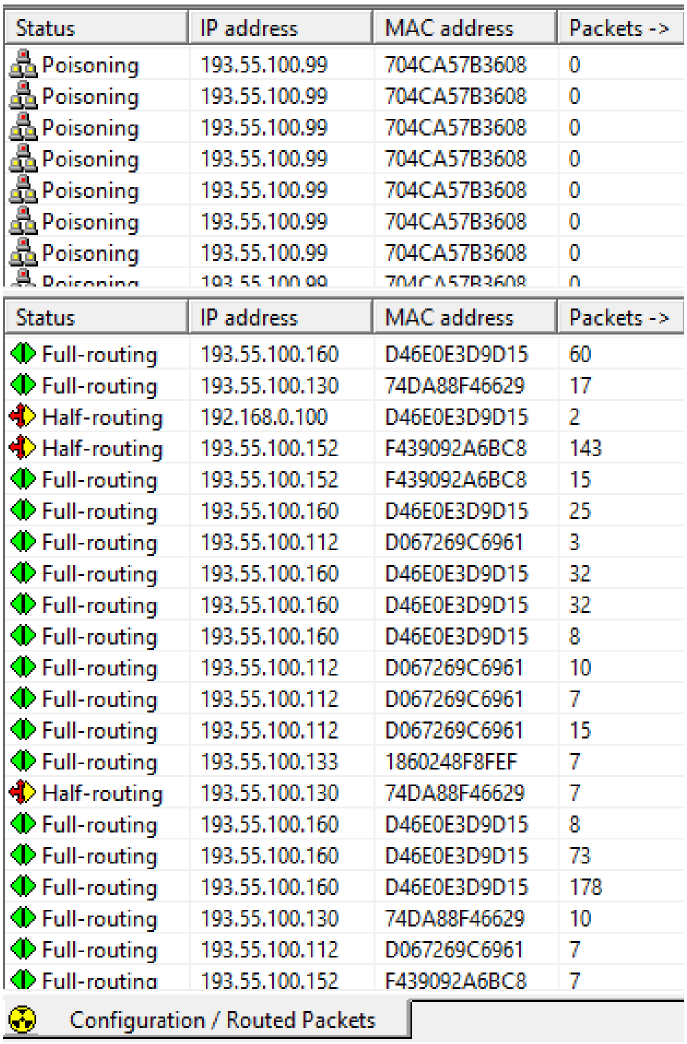
WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
193.55.100.99	704CA57B3608	
193.55.100.131	ACE2D36731EE	
193.55.100.123	1860248F8FAB	
193.55.100.102	ACE2D369B030	
193.55.100.103	000A830314E1	
193.55.100.110	D4BED9B89D2D	
193.55.100.111	98F2B33E14BC	
193.55.100.112	D067269C6961	
193.55.100.114	0060EF275C05	
193.55.100.116	F8D027A7D2D6	

IP address	MAC	Hostname
193.55.100.133	1860248F8FEF	
193.55.100.132	0060EF26FC87	
193.55.100.130	74DA88F46629	
193.55.100.118	F8D027A7E201	
193.55.100.117	F8D027A7E204	
193.55.100.116	F8D027A7D2D6	
193.55.100.114	0060EF275C05	
193.55.100.112	D067269C6961	
193.55.100.111	98F2B33E14BC	
193.55.100.110	D4BED9B89D2D	

Figure 7: The screenshot of the Poison Routing window for **selecting the victim's IP-address**



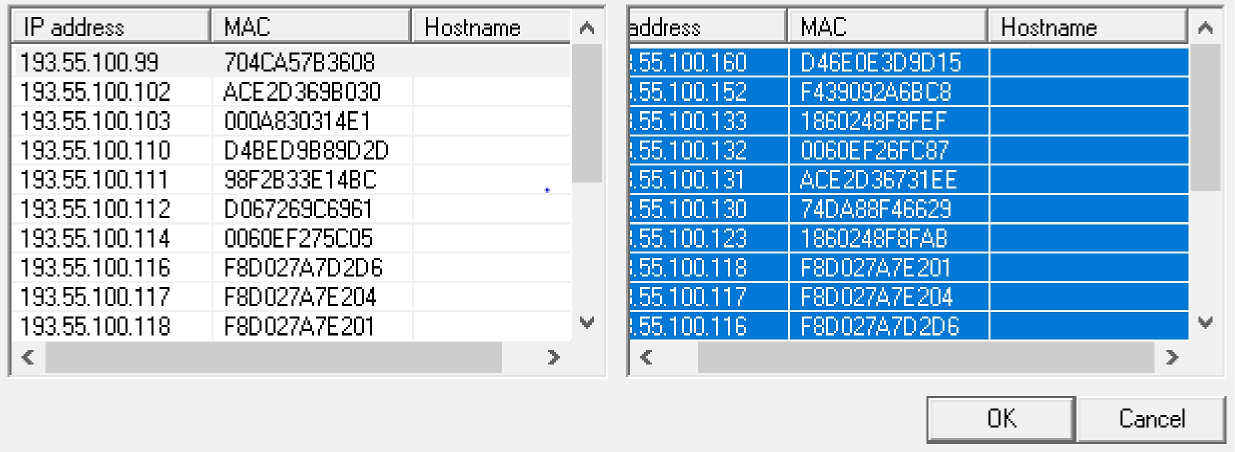
Status	IP address	MAC address	Packets ->
Poisoning	193.55.100.99	704CA57B3608	0
Poisoning	193.55.100.99	704CA57B3608	0
Poisoning	193.55.100.99	704CA57B3608	0
Poisoning	193.55.100.99	704CA57B3608	0
Poisoning	193.55.100.99	704CA57B3608	0
Poisoning	193.55.100.99	704CA57B3608	0
Poisoning	193.55.100.99	704CA57B3608	0
Poisoning	193.55.100.99	704CA57B3608	0

Status	IP address	MAC address	Packets ->
Full-routing	193.55.100.160	D46E0E3D9D15	60
Full-routing	193.55.100.130	74DA88F46629	17
Half-routing	192.168.0.100	D46E0E3D9D15	2
Half-routing	193.55.100.152	F439092A6BC8	143
Full-routing	193.55.100.152	F439092A6BC8	15
Full-routing	193.55.100.160	D46E0E3D9D15	25
Full-routing	193.55.100.112	D067269C6961	3
Full-routing	193.55.100.160	D46E0E3D9D15	32
Full-routing	193.55.100.160	D46E0E3D9D15	32
Full-routing	193.55.100.160	D46E0E3D9D15	8
Full-routing	193.55.100.112	D067269C6961	10
Full-routing	193.55.100.112	D067269C6961	7
Full-routing	193.55.100.112	D067269C6961	15
Full-routing	193.55.100.133	1860248F8FEF	7
Half-routing	193.55.100.130	74DA88F46629	7
Full-routing	193.55.100.160	D46E0E3D9D15	8
Full-routing	193.55.100.160	D46E0E3D9D15	73
Full-routing	193.55.100.160	D46E0E3D9D15	178
Full-routing	193.55.100.130	74DA88F46629	10
Full-routing	193.55.100.112	D067269C6961	7
Full-routing	193.55.100.152	F439092A6BC8	7

Figure 8: The screenshot showing the **Arp Poisoning in action and results**

2.2.3 Packet capturing/Intrusion detection using Cain and Abel software

Intrusion Detection is the detection of unauthorized users and suspicious activities in a network. It is analysed concurrently with packet capturing because intrusion cannot be detected without first capturing the packet. In this research, Packet capturing was achieved by repeating the procedure shown in Figure 6 to show the list of active IP-Address before selecting the IP-Address whose packet I wanted to capture and monitor for intrusion , for the purpose of this research, all the IP-Address was chosen as shown Figure 9.

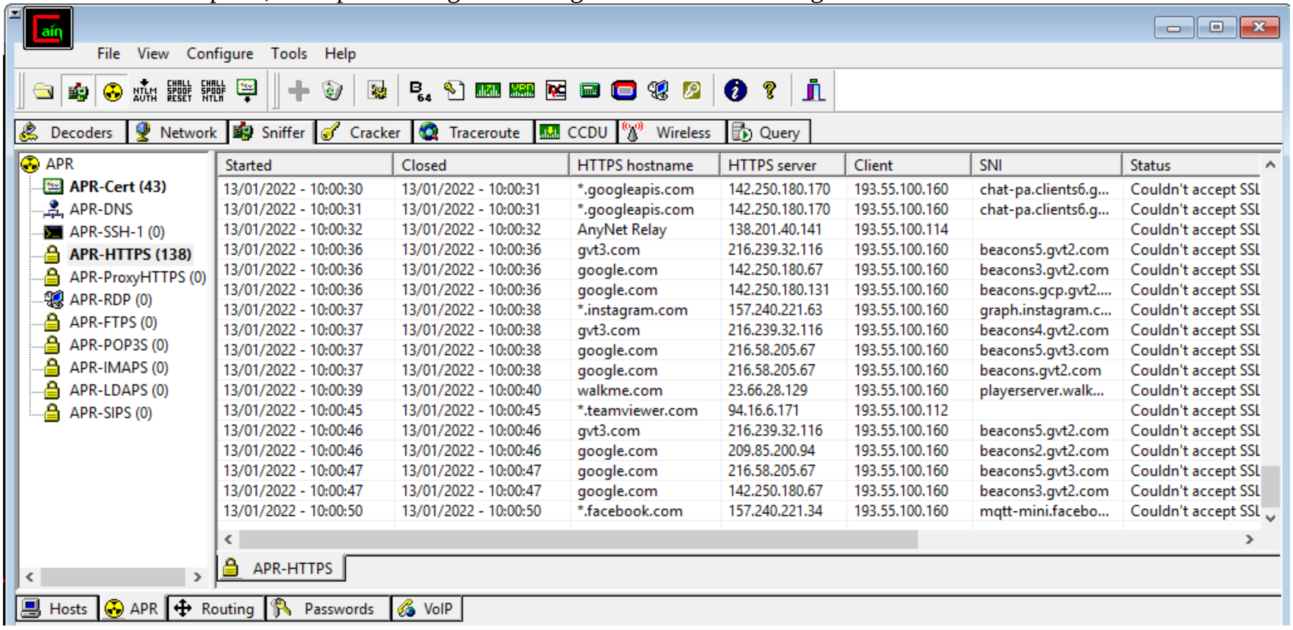


IP address	MAC	Hostname
193.55.100.99	704CA57B3608	
193.55.100.102	ACE2D369B030	
193.55.100.103	000A830314E1	
193.55.100.110	D4BED9B89D2D	
193.55.100.111	98F2B33E14BC	
193.55.100.112	D067269C6961	
193.55.100.114	0060EF275C05	
193.55.100.116	F8D027A7D2D6	
193.55.100.117	F8D027A7E204	
193.55.100.118	F8D027A7E201	

address	MAC	Hostname
.55.100.160	D46E0E3D9D15	
.55.100.152	F439092A6BC8	
.55.100.133	1860248F8FEF	
.55.100.132	0060EF26FC87	
.55.100.131	ACE2D36731EE	
.55.100.130	74DA88F46629	
.55.100.123	1860248F8FAB	
.55.100.118	F8D027A7E201	
.55.100.117	F8D027A7E204	
.55.100.116	F8D027A7D2D6	

Figure 9: Selecting the targeted IP-Address

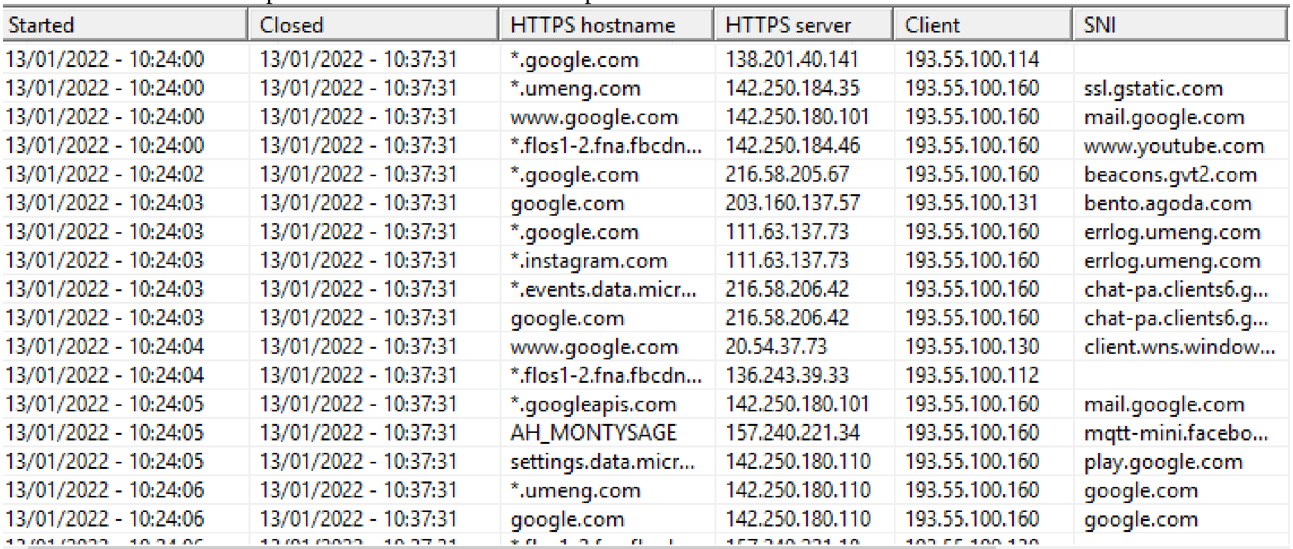
After selecting the targeted IP-address, I proceeded to click on the **ARP-HTTPS** option, this option brought a catalogue of all the traffic generated in the network in real-time which enabled me to monitor the network for any Intrusion as shown in Figure 10 below



Started	Closed	HTTPS hostname	HTTPS server	Client	SNI	Status
13/01/2022 - 10:00:30	13/01/2022 - 10:00:31	*.googleapis.com	142.250.180.170	193.55.100.160	chat-pa.clients6.g...	Couldn't accept SSL
13/01/2022 - 10:00:31	13/01/2022 - 10:00:31	*.googleapis.com	142.250.180.170	193.55.100.160	chat-pa.clients6.g...	Couldn't accept SSL
13/01/2022 - 10:00:32	13/01/2022 - 10:00:32	AnyNet Relay	138.201.40.141	193.55.100.114		Couldn't accept SSL
13/01/2022 - 10:00:36	13/01/2022 - 10:00:36	gvt3.com	216.239.32.116	193.55.100.160	beacons5.gvt2.com	Couldn't accept SSL
13/01/2022 - 10:00:36	13/01/2022 - 10:00:36	google.com	142.250.180.67	193.55.100.160	beacons3.gvt2.com	Couldn't accept SSL
13/01/2022 - 10:00:36	13/01/2022 - 10:00:36	google.com	142.250.180.131	193.55.100.160	beacons.gcp.gvt2....	Couldn't accept SSL
13/01/2022 - 10:00:37	13/01/2022 - 10:00:38	*.instagram.com	157.240.221.63	193.55.100.160	graph.instagram.c...	Couldn't accept SSL
13/01/2022 - 10:00:37	13/01/2022 - 10:00:38	gvt3.com	216.239.32.116	193.55.100.160	beacons4.gvt2.com	Couldn't accept SSL
13/01/2022 - 10:00:37	13/01/2022 - 10:00:38	google.com	216.58.205.67	193.55.100.160	beacons5.gvt3.com	Couldn't accept SSL
13/01/2022 - 10:00:37	13/01/2022 - 10:00:38	google.com	216.58.205.67	193.55.100.160	beacons.gvt2.com	Couldn't accept SSL
13/01/2022 - 10:00:39	13/01/2022 - 10:00:40	walkme.com	23.66.28.129	193.55.100.160	playerserver.walk...	Couldn't accept SSL
13/01/2022 - 10:00:45	13/01/2022 - 10:00:45	*.teamviewer.com	94.16.6.171	193.55.100.112		Couldn't accept SSL
13/01/2022 - 10:00:46	13/01/2022 - 10:00:46	gvt3.com	216.239.32.116	193.55.100.160	beacons5.gvt2.com	Couldn't accept SSL
13/01/2022 - 10:00:46	13/01/2022 - 10:00:46	google.com	209.85.200.94	193.55.100.160	beacons2.gvt2.com	Couldn't accept SSL
13/01/2022 - 10:00:47	13/01/2022 - 10:00:47	google.com	216.58.205.67	193.55.100.160	beacons5.gvt3.com	Couldn't accept SSL
13/01/2022 - 10:00:47	13/01/2022 - 10:00:47	google.com	142.250.180.67	193.55.100.160	beacons3.gvt2.com	Couldn't accept SSL
13/01/2022 - 10:00:50	13/01/2022 - 10:00:50	*.facebook.com	157.240.221.34	193.55.100.160	mqtt-mini.facebo...	Couldn't accept SSL

Figure 10 Catalogue of generated traffic

Figure 11 below shows all the website visited by all the network clients. The data captured included client and Https server address, session start/closing time and the resolved DNS of the visited sites.



Started	Closed	HTTPS hostname	HTTPS server	Client	SNI
13/01/2022 - 10:24:00	13/01/2022 - 10:37:31	*.google.com	138.201.40.141	193.55.100.114	
13/01/2022 - 10:24:00	13/01/2022 - 10:37:31	*.umeng.com	142.250.184.35	193.55.100.160	ssl.gstatic.com
13/01/2022 - 10:24:00	13/01/2022 - 10:37:31	www.google.com	142.250.180.101	193.55.100.160	mail.google.com
13/01/2022 - 10:24:00	13/01/2022 - 10:37:31	*.flos1-2.fna.fbcdn...	142.250.184.46	193.55.100.160	www.youtube.com
13/01/2022 - 10:24:02	13/01/2022 - 10:37:31	*.google.com	216.58.205.67	193.55.100.160	beacons.gvt2.com
13/01/2022 - 10:24:03	13/01/2022 - 10:37:31	google.com	203.160.137.57	193.55.100.131	bento.agoda.com
13/01/2022 - 10:24:03	13/01/2022 - 10:37:31	*.google.com	111.63.137.73	193.55.100.160	errlog.umeng.com
13/01/2022 - 10:24:03	13/01/2022 - 10:37:31	*.instagram.com	111.63.137.73	193.55.100.160	errlog.umeng.com
13/01/2022 - 10:24:03	13/01/2022 - 10:37:31	*.events.data.micr...	216.58.206.42	193.55.100.160	chat-pa.clients6.g...
13/01/2022 - 10:24:03	13/01/2022 - 10:37:31	google.com	216.58.206.42	193.55.100.160	chat-pa.clients6.g...
13/01/2022 - 10:24:04	13/01/2022 - 10:37:31	www.google.com	20.54.37.73	193.55.100.130	client.wns.window...
13/01/2022 - 10:24:04	13/01/2022 - 10:37:31	*.flos1-2.fna.fbcdn...	136.243.39.33	193.55.100.112	
13/01/2022 - 10:24:05	13/01/2022 - 10:37:31	*.googleapis.com	142.250.180.101	193.55.100.160	mail.google.com
13/01/2022 - 10:24:05	13/01/2022 - 10:37:31	AH_MONTYSAGE	157.240.221.34	193.55.100.160	mqtt-mini.facebo...
13/01/2022 - 10:24:05	13/01/2022 - 10:37:31	settings.data.micr...	142.250.180.110	193.55.100.160	play.google.com
13/01/2022 - 10:24:06	13/01/2022 - 10:37:31	*.umeng.com	142.250.180.110	193.55.100.160	google.com
13/01/2022 - 10:24:06	13/01/2022 - 10:37:31	google.com	142.250.180.110	193.55.100.160	google.com

Figure 11 Captured information

3. Discussion of Results

Packet Capturing/Intrusion detection

Cain and Abel was able to view network traffic and also resolve the Domain name server of both source and destination IP addresses with the time of communication between them in real-time. However, Cain and Abel was not able to capture and save the displayed traffic for further analysis.

Man-in-the-middle Attack

Cain and Abel was able to initiate a man-in-the-middle attack through ARP poisoning using. Spoofing of mac-address was effectively carried out by Cain and Abel during the ARP poisoning session. This attack compromised the integrity and availability of the needed information.

Password Cracking

Cain and Abel was used to sniff other wireless devices connected to the network and also expose their wireless passwords. This attack compromised all the 3 aspects of the confidentiality, integrity and availability (CIA) triad.

4. Conclusion

Security vulnerability analysis of a wireless network with WPA2 encryption using Cain and Abel wireless network security testing software tool is presented. First, first, brief description of the Cain and Abel tool is presented along with the procedure for its installation. Subsequently, password decryption/cracking, man-in-the-middle attack (ARP poison) and packet capturing/intrusion detection, which are among the most popular wireless network security vulnerability issues were analyzed for a wireless network with WPA2 encryption using the Cain and Abel tool. The results show that for the wireless network with WPA2 encryption, Cain and Abel tool is able to identify and execute each of the three security vulnerability issues considered in the study.

References

1. Hammerla, N. Y., Halloran, S., & Plötz, T. (2016). Deep, convolutional, and recurrent models for human activity recognition using wearables. *arXiv preprint arXiv:1604.08880*.
2. Ronao, C. A., & Cho, S. B. (2016). Human activity recognition with smartphone sensors using deep learning neural networks. *Expert systems with applications*, *59*, 235-244.
3. Anietie Bassey, **Simeon Ozumba** & Kufre Udofia **(2015).** An Effective Adaptive Media Play-out Algorithm For Real-time Video Streaming Over Packet Networks. European. ***Journal of Basic and Applied Sciences*** *Vol, 2(4).*
4. Kalu, C., **Ozuomba, Simeon**. & Udofia, K. **(2015).** Web-based map mashup application for participatory wireless network signal strength mapping and customer support services. ***European Journal of Engineering and Technology,*** *3 (8)*, 30-43.
5. Essiambre, R. J., & Tkach, R. W. (2012). Capacity trends and limits of optical communication networks. *Proceedings of the IEEE*, *100*(5), 1035-1055.
6. Lam, C. F., Liu, H., Koley, B., Zhao, X., Kamalov, V., & Gill, V. (2010). Fiber optic communication technologies: What's needed for datacenter network operations. *IEEE Communications Magazine*, *48*(7), 32-39.
7. DeCusatis, C. (Ed.). (2013). *Handbook of fiber optic data communication: a practical guide to optical networking*. Academic Press.
8. **Ozuomba Simeon** and Chukwudebe G. A**.(2011) ;** *"Performance Analysis Of Timely-Token Protocol With Variable Load Of Synchronous Traffic"* ***NSE Technical Transactions , A Technical Journal of The Nigerian Society Of Engineers,*** Vol. 46, No. 1 Jan – March 2011, PP 34 – 46.
9. **Ozuomba Simeon** and Chukwudebe G. A.**(2003)** *An improved algorithm for channel capacity allocation in timer controlled token passing protocols, The Journal of Computer Science and its Applications* ***(An international Journal of the Nigerian Computer Society (NCS))*** *Vol. 9, No. 1 , June 2003 , PP 116 124*
10. Kalu C. , **Ozuomba Simeon,** Onoh G.N. **(2013)** Dynamic Threshold limited timed token (DTLTT) Protocol ***Nigerian Journal of Technology (NIJOTECH)*** Vol. 32. No. 1. March 2013, pp. 266-272.
11. **Kalu, S. Ozuomba, G. N. Onoh (201**1) ANALYSIS OF TIMELY-TOKEN PROTOCOL WITH NON-UNIFORM HEAVY LOAD OF ASYNCHRONOUS TRAFFIC. Electroscope Journal Vol. 5 No. 5 (2011)
12. **Ozuomba Simeon ,** Chukwudebe G. A. and Akaninyene B. Obot **(2011); "***Static-Threshold-Limited On-Demand Guaranteed Service For Asynchronous Traffic In Timely-Token Protocol " Nigerian* ***Journal of Technology (NIJOTECH)*** Vol. 30, No. 2 , June 2011 , PP 124 – 142
13. Kalu, C., **Ozuomba, Simeon**., & Anthony, U. M. **(2015).** STATIC-THRESHOLD-LIMITED BuST PROTOCOL. ***European Journal of Mathematics and Computer Science*** *Vol, 2(2).*
14. **Ozuomba Simeon** and Chukwudebe G. A. **(2004)** *A new priority scheme for the asynchronous traffic in timer-controlled token passing protocols, The Journal of Computer Science and its* ***Applications (An international Journal of the Nigerian Computer Society (NCS))*** *Vol. 10, No. 2 , December 2004 , PP 17 -25*
15. **Ozuomba, Simeon,** Amaefule, C. O., & Afolayan, J. J. **(2013).** Optimal Guaranteed Services Timed Token (OGSTT) Media Access Control (Mac) Protocol For Networks That Support Hard Real-Time And Non Real-Time Traffic. ***Nigerian Journal of Technology (NIJOTECH)*** *32*(3), 470-477
16. **Kalu C., Ozuomba S., and Mbocha C.C. (2013)** Performance Analysis of Static- Threshold-Limited On-Demand Guaranteed Services Timed Token Media Access Control Protocol Under Non Uniform Heavy Load of Asynchronous Traffic. *NSE Technical Transactions, A Technical Journal of the Nigerian Society of Engineers,* Vol. 47, No. 3 July – Sept 2013,
17. Constance Kalu, Simeon Ozuomba and **Umoren Mfonobong Anthony** (2015) Performance Analysis of Fiber Distribution Data Interface Network Media Access Control Protocol Under-Uniform Heavy load of Asynchronous Traffic. European Journal of Basic and Applied Sciences. Vol 2 No. 4
18. Constance Kalu, Simeon Ozuomba and **Umoren Mfonobong Anthony** (2015) Static-Threshold-

Limited Bust Protocol, European Journal of Mathematics and Computer Science, Vol. 2 N0. 2

19. **Ezenugu, I. A** and Ezeh, Ikechuwu H (2019) "Application Of Regular Falsi Algorithm In The Determination Of The Optimal Path Length For Terrestrial Fixed Point Microwave Line Of Sight Communication Link" **Journal of Multidisciplinary Engineering Science Studies (JMESS) ISSN: 2458-925X Vol. 5 Issue 9 pp3711 - 3721**
20. Ono, M. N., Obot, A. B., & **Ozuomba, Simeon. (2020).** ENHANCED BISECTION ITERATION METHOD APPLIED IN FADE MARGIN-BASED OPTIMAL PATH LENGTH FOR FIXED POINT TERRESTRIAL MICROWAVE COMMUNICATION LINK WITH KNIFE EDGE DIFFRACTION LOSS. ***International Multilingual Journal of Science and Technology*** *(IMJST) Vol. 5 Issue 6, June – 2020*
21. **Ezenugu, I. A (2014)**, "Evaluation Of Required Receiver Antenna Gain And Dimension For Analog And Digital Satellite Tv Transmission Link" **Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 2458-9403 Vol. 1 Issue 5, pp 12755-12758**
22. Dike Happiness Ugochi and **Ezenugu, I. A (2019) "**Analysis of Antenna Point Loss In Satellite Communication Link**" Science and Technology Publishing (SCI & TECH) ISSN: 2632-1017 Vol. 3 Issue 10 pp 643 - 648**
23. **Simeon, Ozuomba (2014)** "Fixed Point Iteration Computation Of Nominal Mean Motion And Semi Major Axis Of Artificial Satellite Orbiting An Oblate Earth." ***Journal of Multidisciplinary Engineering Science and Technology (JMEST)*** *Vol. 1 Issue 4, November – 2014*
24. **Simeon, Ozuomba. (2017).** "Determination Of The Clear Sky Composite Carrier To Noise Ratio For Ku-Band Digital Video Satellite Link" ***Science and Technology Publishing*** *(SCI & TECH) Vol. 1 Issue 7, July – 2017*
25. Simeon, Ozuomba. (2016). Evaluation Of Bit Error Rate Performance Of Multi-Level Differential Phase Shift Keying. Evaluation, 1(8). ***International Multilingual Journal of Science and Technology*** *(IMJST) Vol. 1 Issue 8, August – 2016*
26. **Ezenugu, I. A (2014)**, "Analytical Computation Of The Error Probability Of Coherent M-Ary Frequency Shift Key Modulation Scheme" **Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 2458-9403 Vol. 1 Issue 5, pp 12759-12763**
27. **Ezenugu, I. A** and Dike Happiness Ugochi (2020) "Performance Analysis Of M-Ary Amplitude Shift Keying Digital Modulation Scheme "***Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 2458-9403 Vol. 7 Issue 11, pp 13667 - 13672***
28. **Ezenugu, I. A** and Dike Happiness Ugochi (2021) "Analytical Models For The Computation Of Error Probability Of Multi-Level Phase Shift Keying Modulation Scheme "***British Journal of Computer, Networking and Information Technology ISSN: 2689-5315 Volume 4, Issue 1, 2021 pp. 13-20.*** **www.abjournals.org**
29. **Ozuomba, Simeon. (2019).** EVALUATION OF OPTIMAL TRANSMISSION RANGE OF WIRELESS SIGNAL ON DIFFERENT TERRAINS BASED ON ERICSSON PATH LOSS MODEL. ***Science and Technology Publishing*** *(SCI & TECH) Vol. 3 Issue 12, December - 2019*
30. Kalu Constance, **Ozuomba Simeon**, Umana, Sylvester Isreal (2018). Evaluation of Walficsh-Bertoni Path Loss Model Tuning Methods for a Cellular Network in a Timber Market in Uyo. ***Journal of Multidisciplinary Engineering Science Studies*** *(JMESS) Vol. 4 Issue 12, December - 2018*
31. Constance, Kalu, **Ozuomba Simeon**, and Ezuruike Okafor SF**. (2018).** Evaluation of the Effect of Atmospheric Parameters on Radio Pathloss in Cellular Mobile Communication System. Evaluation, 5(11). ***Journal of Multidisciplinary Engineering Science and Technology*** *(JMEST) Vol. 5 Issue 11, November - 2018*
32. Njoku Chukwudi Aloziem, **Ozuomba Simeon**, Afolayan J. Jimoh **(2017)** Tuning and Cross Validation of Blomquist-Ladell Model for Pathloss Prediction in the GSM 900 Mhz Frequency Band , ***International Journal of Theoretical and Applied Mathematics***
33. **Ozuomba, Simeon,** Johnson, E. H., & Udoiwod, E. N. **(2018).** Application of Weissberger Model for Characterizing the Propagation Loss in a Gliricidia sepium Arboretum. ***Universal Journal of Communications and Network, 6(2), 18-23.***
34. **Ozuomba, Simeon,** Enyenihi, J., & Rosemary, N. C**. (2018).** Characterisation of Propagation Loss for a 3G Cellular Network in a Crowded Market Area Using CCIR Model. ***Review of Computer Engineering Research***, 5(2), 49-56.
35. Akaninyene B. Obot , **Ozuomba Simeon** and Afolanya J. Jimoh **(2011); "***Comparative Analysis Of Pathloss Prediction Models For Urban Macrocellular"* ***Nigerian Journal of Technology (NIJOTECH)*** Vol. 30, No. 3 , October 2011 , PP 50 – 59
36. K.M. Udofia (2019)COMPARATIVE ANALYSIS OF OPTIMAL TRANSMISSION RANGE OF Ka-BAND COMMUNICATION LINK BASED ON DIFFERENT DEGREES OF URBANIZATION IN CCIR PATH LOSS MODEL
37. I. E afahakan, k. M. Udofia, and M. A. Umoren (2016) Analysis of Rain Rate and Rain Attenuation for Earth-space Communication Links Over Uyo - Akwa Ibom State, *Nigerian Journal of Technology (Nijotech), Vol. 35 No. 1, January 2016, pp.* 137 – 143
38. M. C. Uko, M. A. Umoren, and J. Enyenihi, (2016) Effect of Shadowing and Multipath Fading on The Area Spectral For Cell-Edge Users In Heterogeneous Networks, *Nigerian Journal of Technology (NIJOTECH), Vol 35, No.21, April 2016, pp 409-414*
39. Ononiwu, Gordon, Simeon Ozuomba, and Constance Kalu. (2015). Determination of the dominant fading and the effective fading for the rain zones in the ITU-R P. 838-3 recommendation. *European Journal of Mathematics and Computer Science Vol, 2(2).*
40. Kalu, C., Ozuomba, Simeon. & Jonathan, O. A. (2015). Rain rate trend-line estimation models and

web application for the global ITU rain zones. *European Journal of Engineering and Technology, 3 (9)*, 14-29.

41. Simeon, Ozuomba. (2016) "Comparative Analysis Of Rain Attenuation In Satellite Communication Link For Different Polarization Options." *Journal of Multidisciplinary Engineering Science and Technology (JMEST) Vol. 3 Issue 6, June - 2016*
42. Udofia Kufre. M., Ogungbemi Emmanuel Oluropo (2017)Determination and Comparative Analysis of Refractivity Profile and Fade Depth for Microwave Links in Lagos International Journal of Information and Communication Sciences 1 (3), 59-62
43. O.A. Jonathan, K.M. Udofia, C. Kalu (2016) Empirical Models for Estimation of Rain Rate in the Fifteen ITU Rain Zones Mathematical and Software Engineering 2 (2), 85-9
44. Ono, M. N., Obot, A. B., & Ozuomba, Simeon. (2020). ENHANCED BISECTION ITERATION METHOD APPLIED IN FADE MARGIN-BASED OPTIMAL PATH LENGTH FOR FIXED POINT TERRESTRIAL MICROWAVE COMMUNICATION LINK WITH KNIFE EDGE DIFFRACTION LOSS. *International Multilingual Journal of Science and Technology (IMJST) Vol. 5 Issue 6, June – 2020*
45. M. Emenyi, K. Udofia, O.C. Amaefule (20017) Computation of optimal path Length for terrestrial line of sight microwave link using Newton–Raphson algorithm Software Engineering 5 (3), 44-50
46. Johnson, Enyenihi Henry, **Simeon Ozuomba**, and Kalu Constance. **(2019).** Development of model for estimation of radio refractivity from meteorological parameters. ***Universal Journal of Engineering Science*** 7(1), 20-26.
47. **Simeon, Ozuomba,** Kalu Constance, and Ezuruike Okafor SF**. (2018).** "Analysis of Variation in the Vertical Profile Of Radio Refractivity Gradient and its impact on the Effective Earth Radius Factor." ***International Multilingual Journal of Science and Technology*** *(IMJST) Vol. 3 Issue 11, November - 2018*
48. **Ozuomba, Simeon**, Henry Johnson Enyenihi, and Constance Kalu **(2018)** "Program to Determine the Terrain Roughness Index using Path Profile Data Sampled at Different Moving Window Sizes." ***International Journal of Computer Applications*** *975: 8887.*
49. Egbe Jesam Nna, **Ozuomba Simeon**, Enyenihi Henry Johnson **(2017)** Modelling and Application of Vertical Refractivity Profile for Cross River State. ***World Journal of Applied Physics*** 2017; 2(1): 19-26
50. Eunice, Akinloye Bolanle, and **Simeon Ozuomba (2016)** "Evaluation of the Distribution of Terrain Roughness Index for Terrestrial Line of Site Microwave Links in Uyo Metropolis." ***Mathematical and Software Engineering*** 2.1 (2016): 9-18
51. Dialoke, Ikenna Calistus, **Ozuomba Simeon**, and Henry Akpan Jacob. **(2020)** "ANALYSIS OF SINGLE KNIFE EDGE DIFFRACTION LOSS FOR A FIXED TERRESTRIAL LINE-OF-SIGHT MICROWAVE COMMUNICATION LINK." ***Journal of Multidisciplinary Engineering Science and Technology*** *(JMEST) Vol. 7 Issue 2, February - 2020*
52. Imoh-Etefia, Ubon Etefia, **Ozuomba Simeon**, and Stephen Bliss Utibe-Abasi. **(2020).** "Analysis Of Obstruction Shadowing In Bullington Double Knife Edge Diffraction Loss Computation." ***Journal of Multidisciplinary Engineering Science Studies*** *(JMESS) Vol. 6 Issue 1, January – 2020*
53. **Simeon, Ozuomba,** Ezuruike Okafor SF, and Bankole Morakinyo Olumide **(2018).** Development of Mathematical Models and Algorithms for Exact Radius of Curvature Used in Rounded Edge Diffraction Loss Computation. Development, 5(12). *Journal of Multidisciplinary Engineering Science and Technology (JMEST) Vol. 5 Issue 12, December - 2018*
54. **Ozuomba, Simeon,** Constant Kalu, and Henry Johnson Enyenihi. **(2018)** "Comparative Analysis of the Circle Fitting Empirical Method and the International Telecommunication Union Parabola Fitting Method for Determination of the Radius of Curvature for Rounded Edge Diffraction Obstruction." **Communications on Applied Electronics (CAE)** *7: 16-21.*
55. Oloyede Adams Opeyemi, **Ozuomba Simeon,** Constance Kalu **(2017)** Shibuya Method for Computing Ten Knife Edge Diffraction Loss. ***Software Engineering*** 2017; 5(2): 38-43
56. C.H. Amadi, C. Kalu, K. Udofia (2020) Modelling of Bit Error Rate as a Function of Knife Edge Diffraction Loss Based on Line of Sight Percentage Clearance International Journal of Engineering & Technology 5 (1), 9-24
57. Simeon O., Joseph, A., & Ezeh, G. N. (2022) Smart Phone Security Threats And Risk Mitigation Strategies. *People, 72,* 84. *Journal of Multidisciplinary Engineering Science Studies (JMESS)* Vol. 8 Issue 7, July – 2022: http://www.jmess.org/wp-content/uploads/2022/09/JMESSP13420874.pdf
58. Gutiérrez-Martínez, J., Núñez-Gaona, M. A., & Aguirre-Meneses, H. (2015). Business model for the security of a large-scale PACS, compliance with ISO/27002: 2013 standard. *Journal of digital imaging*, *28*, 481-491.
59. Seanosky, J., Jacques, D., & Kumar, V. (2016). Security and Privacy in Bigdata Learning Analytics: An Affordable and Modular Solution. In *Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16')* (pp. 43-55). Springer International Publishing.
60. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In *AMIA annual symposium proceedings* (Vol. 2017, p. 650). American Medical Informatics Association.
61. Alblwi, S., & Shujaee, K. (2017). A survey on wireless security protocol WPA2. In *Proceedings of the international conference on security and management (SAM)* (pp. 12-17). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
62. Kwon, S., & Choi, H. K. (2020). Evolution of Wi-Fi protected access: security challenges. *IEEE Consumer Electronics Magazine*, *10*(1), 74-81.

63. Adam, M. M. E., & Abdallah, A. G. E. (2015). WIFI SECURITY. *International Journal Of Advances in Engineering and Management (IJAEM)*, *2*(2), 143-149.

64. Sakib, A. N., Jaigirdar, F. T., Munim, M., & Akter, A. (2011). Security improvement of WPA 2 (Wi-Fi protected access 2). *IJEST*, *3*(1).

65. Ahmed, S., Sakib, A. N., & Rahman, S. (2012). WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis. *Global Journal of Computer Science and Technology*, *12*(6), 83-89.

66. Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A., & Shrawne, S. (2012). Vulnerabilities of Wireless Security protocols (WEP and WPA2). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *1*(2), 34-38.

67. Bhatnagar, R., & Birla, V. K. (2015). Wi-Fi security: A literature review of security in wireless network. *IMPACT: IJRET*, *3*(5), 23-30.

68. Rusi, T., & Lehto, M. (2017). Cyber threats mega trends in cyber space. In *ICMLG 2017 5th International Conference on Management Leadership and Governance. Academic Conferences and Publishing Limited* (p. 323).

69. Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smart phones. *Journal of Information Systems Technology and Planning*, *5*(14), 40-60.

70. Shabut, A. M., Lwin, K. T., & Hossain, M. A. (2016, December). Cyber attacks, countermeasures, and protection schemes—A state of the art survey. In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)* (pp. 37-44). IEEE.

71. Singh, J. (2014). Cyber-attacks in cloud computing: A case study. *International Journal of Electronics and Information Engineering*, *1*(2), 78-87.

72. Schneider, D. (2012). The state of network security. *Network Security*, *2012*(2), 14-20.

73. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

74. Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (e-health) systems. *Journal of medical systems*, *40*, 1-12.

75. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International journal of critical infrastructure protection*, *25*, 36-49.

76. Chyrun, L., Chyrun, L., Kis, Y., & Rybak, L. (2020). Information System for Connection to the Access Point with Encryption WPA2 Enterprise. In *Lecture Notes in Computational Intelligence and Decision Making: Proceedings of the XV International Scientific Conference "Intellectual Systems of Decision Making and Problems of Computational Intelligence"(ISDMCI'2019), Ukraine, May 21–25, 2019 15* (pp. 389-404). Springer International Publishing.

77. Khasawneh, M., Kajman, I., Alkhudaidy, R., & Althubyani, A. (2014). A survey on Wi-Fi protocols: WPA and WPA2. In *Recent Trends in Computer Networks and Distributed Systems Security: Second International Conference, SNDS 2014, Trivandrum, India, March 13-14, 2014, Proceedings 2* (pp. 496-511). Springer Berlin Heidelberg.

78. Nussel, L. (2010). The evil twin problem with WPA2-enterprise. *SUSE Linux Products GmbH*.

79. Radivilova, T., & Hassan, H. A. (2017, September). Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise. In *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)* (pp. 1-4). IEEE.

80. Tsitroulis, A., Lampoudis, D., & Tsekleves, E. (2014). Exposing WPA2 security protocol vulnerabilities. *International Journal of Information and Computer Security*, *6*(1), 93-107.

81. Fahmy, S., Nasir, A., & Shamsuddin, N. (2012, June). Wireless network attack: Raising the awareness of Kampung WiFi residents. In *2012 International Conference on Computer & Information Science (ICCIS)* (Vol. 2, pp. 736-740). IEEE.

82. Kadam, S. P., Mahajan, B., Patanwala, M., Sanas, P., & Vidyarthi, S. (2016, March). Automated Wi-Fi penetration testing. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 1092-1096). IEEE.

83. Kaur, S., & Singh, H. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY A DESCRIPTIVE REVIEW OF DIFFERENT PENETRATION TESTING TOOLS AND METHODS.

84. Gandarilla, H. (2018). Safeguarding personal health information: case study. In *Information Technology-New Generations: 15th International Conference on Information Technology* (pp. 3-6). Springer International Publishing.