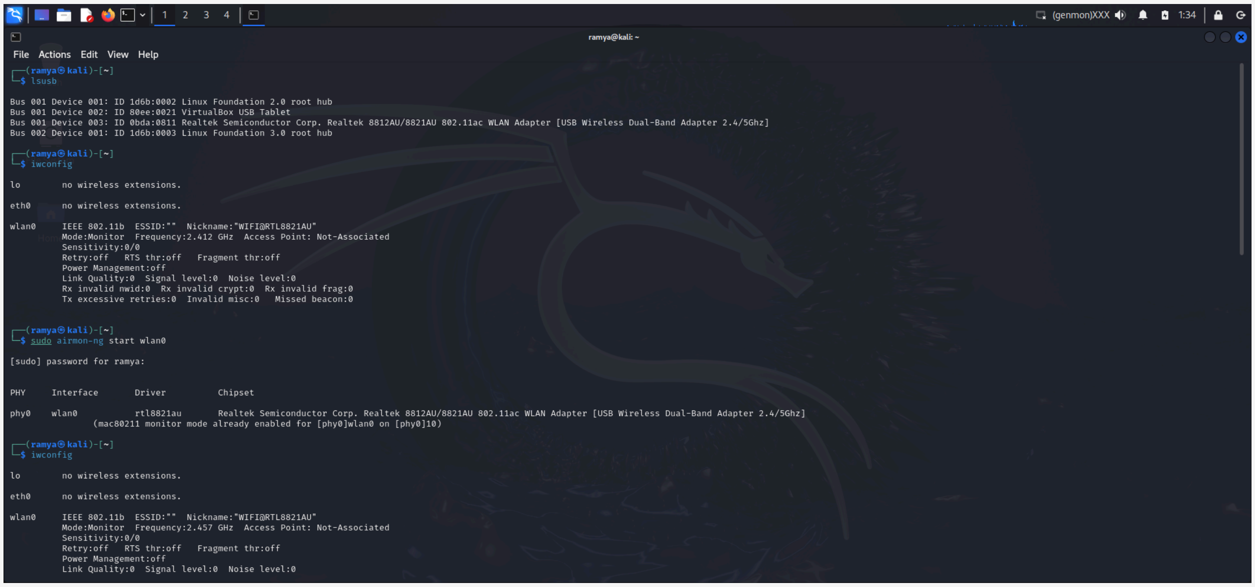
Wireless Network Scanning and Information Gathering

Step1: install alfa drivers in kali linux

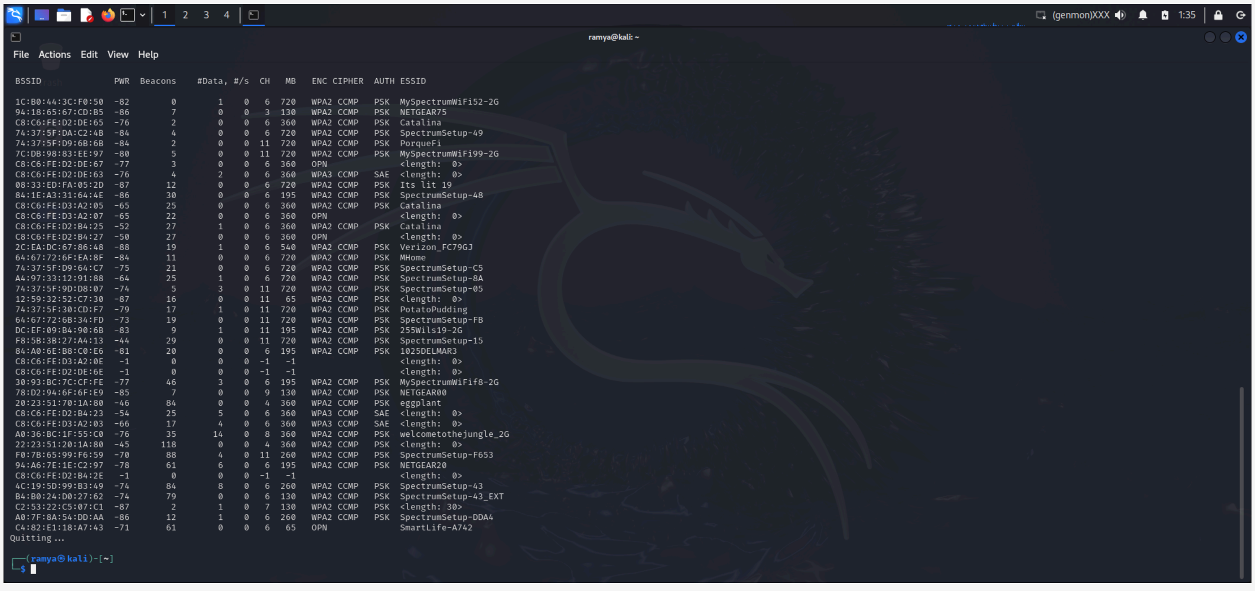
STEP 2: enable monitor mode

1. **Enable Monitor Mode:**
   - Use `airmon-ng` to enable monitor mode on your wireless interface.

2. **Scan Wireless Networks:**
   - Use `airodump-ng` to scan for nearby wireless networks.



```
┌──(ramya㉿kali)-[~]
└─$ lsusb

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 001 Device 003: ID 0bda:0811 Realtek Semiconductor Corp. Realtek 8812AU/8821AU 802.11ac WLAN Adapter [USB Wireless Dual-Band Adapter 2.4/5Ghz]
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

┌──(ramya㉿kali)-[~]
└─$ iwconfig

lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11b  ESSID:""  Nickname:"WIFI@RTL8821AU"
          Mode:Monitor  Frequency:2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0


┌──(ramya㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

[sudo] password for ramya:


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]
                (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]10)

┌──(ramya㉿kali)-[~]
└─$ iwconfig

lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11b  ESSID:""  Nickname:"WIFI@RTL8821AU"
          Mode:Monitor  Frequency:2.457 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
```



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

 1C:B0:44:3C:F0:50  -82        0        1    0   6  720   WPA2 CCMP   PSK  MySpectrumWiFi52-2G
 94:18:65:67:CD:B5  -86        7        0    0   3  130   WPA2 CCMP   PSK  NETGEAR75
 C8:C6:FE:D2:DE:65  -76        2        0    0   6  360   WPA2 CCMP   PSK  Catalina
 74:37:5F:DA:C2:4B  -84        4        0    0   6  720   WPA2 CCMP   PSK  SpectrumSetup-49
 74:37:5F:D9:6B:6B  -84        2        0    0  11  720   WPA2 CCMP   PSK  PorqueFi
 7C:DB:98:83:EE:97  -80        5        0    0  11  720   WPA2 CCMP   PSK  MySpectrumWiFi99-2G
 C8:C6:FE:D2:DE:67  -77        3        0    0   6  360   OPN              <length:  0>
 C8:C6:FE:D2:DE:63  -76        4        2    0   6  360   WPA3 CCMP   SAE  <length:  0>
 08:33:ED:FA:05:2D  -87       12        0    0   6  720   WPA2 CCMP   PSK  Its lit 19
 84:1E:A3:31:64:4E  -86       30        0    0   6  195   WPA2 CCMP   PSK  SpectrumSetup-48
 C8:C6:FE:D3:A2:05  -65       25        0    0   6  360   WPA2 CCMP   PSK  Catalina
 C8:C6:FE:D3:A2:07  -65       22        0    0   6  360   OPN              <length:  0>
 C8:C6:FE:D2:B4:25  -52       27        1    0   6  360   WPA2 CCMP   PSK  Catalina
 C8:C6:FE:D2:B4:27  -50       27        0    0   6  360   OPN              <length:  0>
 2C:EA:DC:67:86:48  -88       19        1    0   6  540   WPA2 CCMP   PSK  Verizon_FC79GJ
 64:67:72:6F:EA:8F  -84       11        0    0   6  720   WPA2 CCMP   PSK  MHome
 74:37:5F:D9:64:C7  -75       21        0    0   6  720   WPA2 CCMP   PSK  SpectrumSetup-C5
 A4:97:33:12:91:88  -64       25        1    0   6  720   WPA2 CCMP   PSK  SpectrumSetup-8A
 74:37:5F:9D:D8:07  -74        5        3    0  11  720   WPA2 CCMP   PSK  SpectrumSetup-05
 12:59:32:52:C7:30  -87       16        0    0  11   65   WPA2 CCMP   PSK  <length:  0>
 74:37:5F:30:CD:F7  -79       17        1    0  11  720   WPA2 CCMP   PSK  PotatoPudding
 64:67:72:6B:34:FD  -73       19        0    0  11  720   WPA2 CCMP   PSK  SpectrumSetup-FB
 DC:EF:09:B4:90:6B  -83        9        1    0  11  195   WPA2 CCMP   PSK  255Wils19-2G
 F8:5B:3B:27:A4:13  -44       29        0    0  11  720   WPA2 CCMP   PSK  SpectrumSetup-15
 84:A0:6E:B8:C0:E6  -81       20        0    0   6  195   WPA2 CCMP   PSK  1025DELMAR3
 C8:C6:FE:D3:A2:0E   -1        0        0    0  -1   -1                    <length:  0>
 C8:C6:FE:D2:DE:6E   -1        0        0    0  -1   -1                    <length:  0>
 30:93:BC:7C:CF:FE  -77       46        3    0   6  195   WPA2 CCMP   PSK  MySpectrumWiFif8-2G
 78:D2:94:6F:6F:E9  -85        7        0    0   9  130   WPA2 CCMP   PSK  NETGEAR00
 20:23:51:70:1A:80  -46       84        0    0   4  360   WPA2 CCMP   PSK  eggplant
 C8:C6:FE:D2:B4:23  -54       25        5    0   6  360   WPA3 CCMP   SAE  <length:  0>
 C8:C6:FE:D3:A2:03  -66       17        4    0   6  360   WPA3 CCMP   SAE  <length:  0>
 A0:36:BC:1F:55:C0  -76       35       14    0   8  360   WPA2 CCMP   PSK  welcometothejungle_2G
 22:23:51:20:1A:80  -45      118        0    0   4  360   WPA2 CCMP   PSK  <length:  0>
 F0:7B:65:99:F6:59  -70       88        4    0  11  260   WPA2 CCMP   PSK  SpectrumSetup-F653
 94:A6:7E:1E:C2:97  -78       61        6    0   6  195   WPA2 CCMP   PSK  NETGEAR20
 C8:C6:FE:D2:B4:2E   -1        0        0    0  -1   -1                    <length:  0>
 4C:19:5D:99:B3:49  -74       84        8    0   6  260   WPA2 CCMP   PSK  SpectrumSetup-43
 B4:B0:24:D0:27:62  -74       79        0    0   6  130   WPA2 CCMP   PSK  SpectrumSetup-43_EXT
 C2:53:22:C5:07:C1  -87        2        1    0   7  130   WPA2 CCMP   PSK  <length: 30>
 A0:7F:8A:54:DD:AA  -86       12        1    0   6  260   WPA2 CCMP   PSK  SpectrumSetup-DDA4
 C4:82:E1:18:A7:43  -71       61        0    0   6   65   OPN              SmartLife-A742
Quitting ...

┌──(ramya㉿kali)-[~]
└─$ 
```

1. **Identify Key Information:**
   - Document the following for each detected network:

- SSID (network name)
- BSSID (MAC address)
- Encryption type (WEP/WPA/WPA2)
- Signal strength
- Channel

Date: 12/1/2024
Time: 10:37PM
Location: Pasadena ,CA

---

1. Introduction

This report lists the wireless networks detected during the scan using `airodump-ng`. The networks are categorized based on their **BSSID**, **Channel**, **Encryption Method**, and **SSID**. The purpose of this scan is to analyze the security posture of nearby wireless networks and to reflect on how this data can be used in network security assessments.

---

2. Detected Networks and Their Characteristics

Network Name (SSID)	BSSID	Channel (CH)	Signal Strength (PWR)	Encryption Method (ENC)	Ciphers (CIPHER)	Authentication Method (AUTH)
MySpectrumWiFi52-2G	1C:B0:44:3C:F0:50	6	-82	WPA2	CCMP	PSK
NETGEAR75	94:18:65:67:CD:B5	3	-86	WPA2	CCMP	PSK
Catalina	C8:C6:FE:D2:DE:65	6	-76	WPA2	CCMP	PSK
SpectrumSetup-49	74:37:5F:DA:C2:4B	6	-84	WPA2	CCMP	PSK
SpectrumSetup-8A	A4:97:33:12:91:88	6	-64	WPA2	CCMP	PSK

MySpectrumWiFi99-2G	7C:DB:98:83:EE:97	11	-80	WPA2	CCMP	PSK
Its lit 19	08:33:ED:FA:05:2D	6	-87	WPA2	CCMP	PSK
SpectrumSetup-F653	F0:7B:65:99:F6:59	11	-70	WPA2	CCMP	PSK

these are some my networks in my home surroundings.

3. Analysis of Network Security Posture

From the list of detected networks, we can observe various types of encryption and authentication mechanisms:

WPA2 Networks:

- Most of the detected networks use **WPA2** encryption, which is currently a common but somewhat outdated security protocol.
- **WPA2 with CCMP (AES)** is a strong encryption cipher used by these networks.
- These networks also use **PSK (Pre-Shared Key)** authentication, meaning that the networks are secured by a shared password.

WPA3 Networks:

- A few networks detected use **WPA3** encryption, such as the network with ESSID **Catalina** (BSSID: C8:C6:FE:D2:DE:63).
- **WPA3** offers improved security compared to WPA2 by implementing stronger encryption algorithms and protections against offline dictionary attacks.

Open Networks (No Encryption):

- Some networks detected are open (no encryption), such as the network with ESSID **SmartLife-A742** (BSSID: C4:82:E1:18:A7:43).
- These networks do not require any form of authentication or password to connect, which makes them highly vulnerable to attacks.

4. Reflections on Network Security Assessment

Vulnerabilities in WPA2 Networks:

- **Weak Passwords**: Networks using WPA2-PSK can be vulnerable to brute-force or dictionary attacks if weak passwords are used. Tools like **Aircrack-ng** can be used to capture handshake data and attempt to crack weak passwords.
- **Offline Attacks**: WPA2-PSK is vulnerable to offline dictionary attacks once a handshake is captured, which is why using a complex password is critical for securing these networks.

WPA3 Advantages:

- **Increased Security**: WPA3 provides enhanced security features like **Simultaneous Authentication of Equals (SAE)**, which is resistant to offline dictionary attacks. However, WPA3 is still not universally supported on older devices.
- **Future Security**: While WPA3 improves security significantly, it is not yet fully adopted across all devices and networks, making some WPA2 networks still common.

Open Networks:

- **Data Interception**: Open networks (those without encryption) are highly vulnerable to data interception and Man-in-the-Middle (MITM) attacks. Anyone within range can easily connect and intercept data without any encryption.
- **Exploiting Open Networks**: These networks are often used by attackers for **Evil Twin** attacks, where the attacker sets up a rogue AP with the same SSID to capture users' traffic and credentials.

Use in Penetration Testing:

- This information can be used for penetration testing by identifying weaknesses in the encryption and authentication protocols.
- Open networks can be targeted for sniffing traffic, while WPA2 networks can be tested for weak passwords or vulnerabilities in the handshake process.
- WPA3 networks provide a more secure target but are still vulnerable if users fall back on weaker configurations or fail to properly implement the protocol.

---

5. Recommendations for Improving Network Security

- **Switch to WPA3**: If possible, upgrade networks to use **WPA3** for better security.

- **Enforce Strong Passwords**: Use strong, random passwords with a mix of uppercase letters, numbers, and special characters to protect WPA2-PSK networks from brute-force attacks.
- **Avoid Open Networks**: Avoid using open networks for sensitive tasks, and consider encrypting communication using tools like **VPNs**.
- **Monitor for Rogue Access Points**: Continuously monitor for rogue APs using tools like **airodump-ng** to prevent **Evil Twin** attacks.

---

6. Conclusion

This scan has revealed a mix of WPA2, WPA3, and open networks in the vicinity. These findings emphasize the need for network owners to adopt stronger encryption standards like **WPA3**, enforce strong passwords, and avoid open networks to mitigate security risks. By understanding the vulnerabilities present in wireless networks, network administrators can take proactive steps to secure their environments and reduce the likelihood of unauthorized access or attacks.