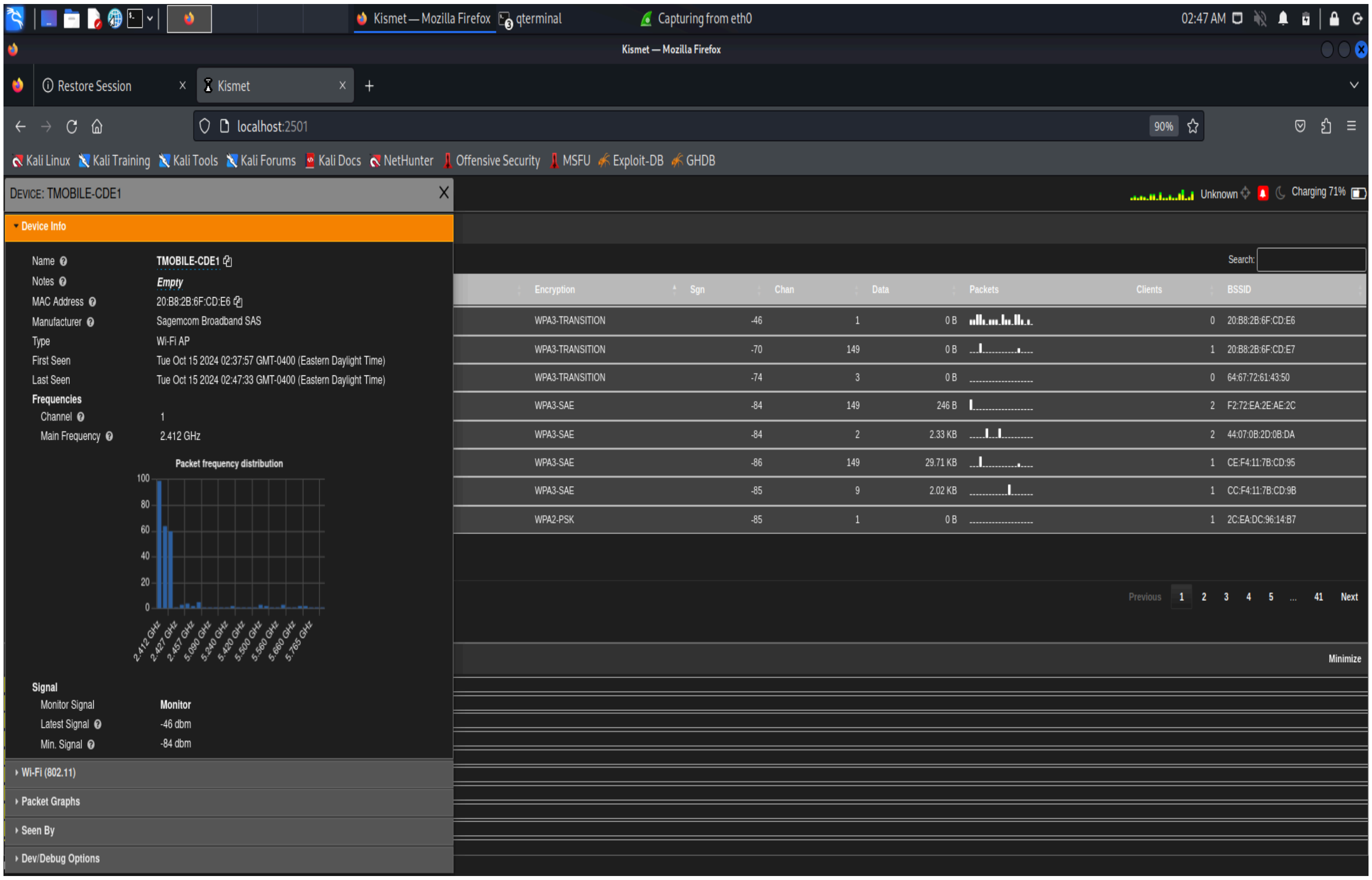
Wireless Intrusion Detection Systems (WIDS) Setup

Tools Required:

- **Kismet** (Wireless IDS, sniffer, and network monitoring tool)
- **Kali Linux** (or any Linux distribution with wireless tools)



DEVICE: TMOBILE-CDE1

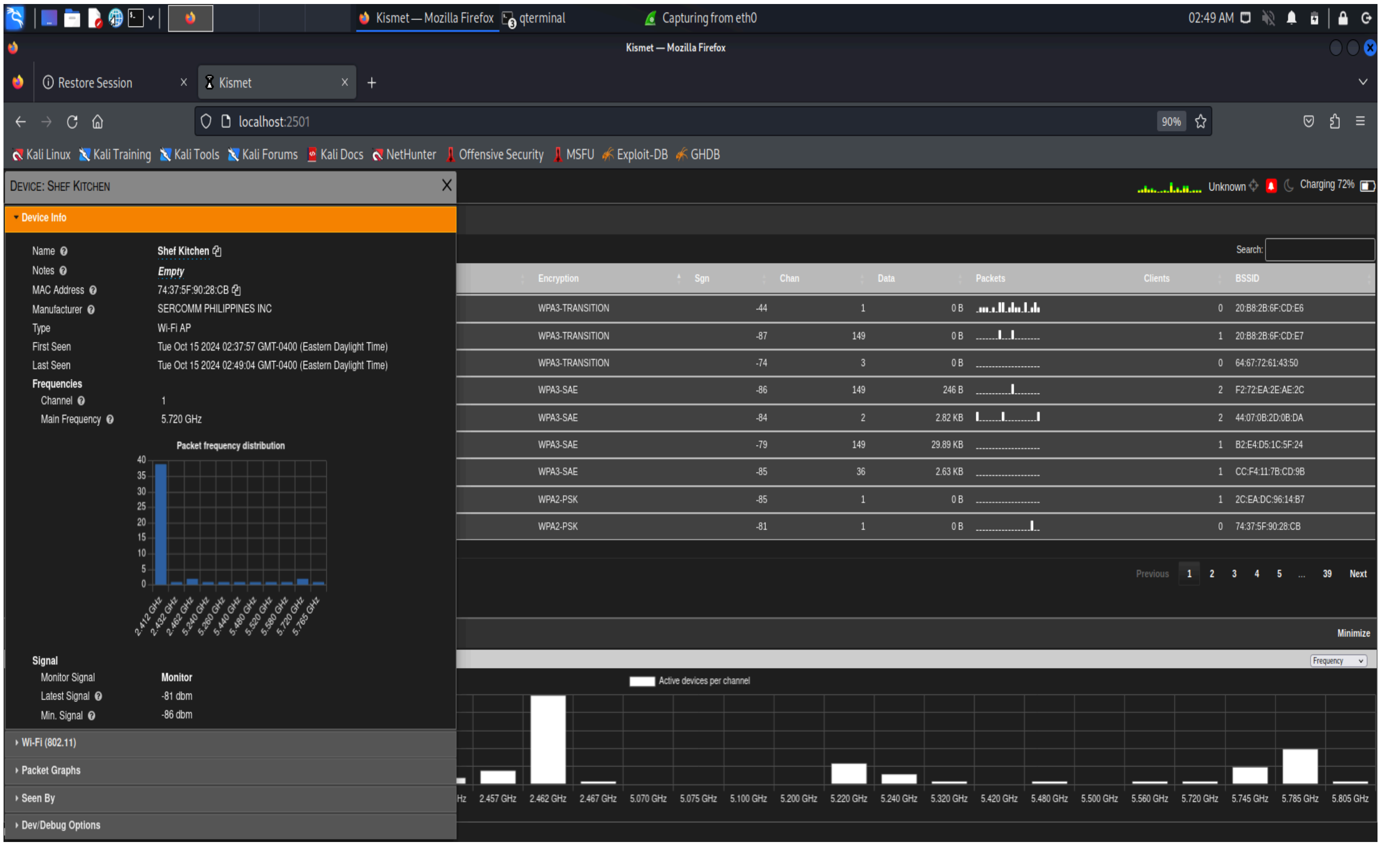
Device Info

Name: TMOBILE-CDE1
Notes: *Empty*
MAC Address: 20:B8:2B:6F:CD:E6
Manufacturer: Sagemcom Broadband SAS
Type: Wi-Fi AP
First Seen: Tue Oct 15 2024 02:37:57 GMT-0400 (Eastern Daylight Time)
Last Seen: Tue Oct 15 2024 02:47:33 GMT-0400 (Eastern Daylight Time)

Frequencies
Channel: 1
Main Frequency: 2.412 GHz

Signal
Monitor Signal: **Monitor**
Latest Signal: -46 dbm
Min. Signal: -84 dbm

Encryption	Sgn	Chan	Data	Packets	Clients	BSSID
WPA3-TRANSITION	-46	1	0 B		0	20:B8:2B:6F:CD:E6
WPA3-TRANSITION	-70	149	0 B		1	20:B8:2B:6F:CD:E7
WPA3-TRANSITION	-74	3	0 B		0	64:67:72:61:43:50
WPA3-SAE	-84	149	246 B		2	F2:72:EA:2E:AE:2C
WPA3-SAE	-84	2	2.33 KB		2	44:07:0B:2D:0B:DA
WPA3-SAE	-86	149	29.71 KB		1	CE:F4:11:7B:CD:95
WPA3-SAE	-85	9	2.02 KB		1	CC:F4:11:7B:CD:9B
WPA2-PSK	-85	1	0 B		1	2C:EA:DC:96:14:B7



DEVICE: SHEF KITCHEN

Device Info

Name	Shef Kitchen
Notes	*Empty*
MAC Address	74:37:5F:90:28:CB
Manufacturer	SERCOMM PHILIPPINES INC
Type	Wi-Fi AP
First Seen	Tue Oct 15 2024 02:37:57 GMT-0400 (Eastern Daylight Time)
Last Seen	Tue Oct 15 2024 02:49:04 GMT-0400 (Eastern Daylight Time)
Frequencies	
Channel	1
Main Frequency	5.720 GHz

Signal	
Monitor Signal	**Monitor**
Latest Signal	-81 dbm
Min. Signal	-86 dbm

Wi-Fi (802.11)

Packet Graphs

Seen By

Dev/Debug Options

Search:

Encryption	Sgn	Chan	Data	Packets	Clients	BSSID
WPA3-TRANSITION	-44	1	0 B		0	20:B8:2B:6F:CD:E6
WPA3-TRANSITION	-87	149	0 B		1	20:B8:2B:6F:CD:E7
WPA3-TRANSITION	-74	3	0 B		0	64:67:72:61:43:50
WPA3-SAE	-86	149	246 B		2	F2:72:EA:2E:AE:2C
WPA3-SAE	-84	2	2.82 KB		2	44:07:0B:2D:0B:DA
WPA3-SAE	-79	149	29.89 KB		1	B2:E4:D5:1C:5F:24
WPA3-SAE	-85	36	2.63 KB		1	CC:F4:11:7B:CD:9B
WPA2-PSK	-85	1	0 B		1	2C:EA:DC:96:14:B7
WPA2-PSK	-81	1	0 B		0	74:37:5F:90:28:CB

General Analysis:

1. **Device Info**: The selected device is an access point with the name "Shef Kitchen." It is manufactured by **Sercomm Philippines Inc.**, as indicated by the OUI (Organizationally Unique Identifier) associated with the MAC address 74:37:5F:90:28:CB.
2. **Frequency Information**:
   - The device operates on **Channel 1** with a frequency of **5.720 GHz**.
   - It appears to broadcast on **multiple frequency bands**, but its primary signal is on the **2.4 GHz** band (Channel 1).
3. **Signal Strength**:
   - **Monitor Signal**: -81 dBm (the signal strength detected by your monitoring interface).
   - **Minimum Signal**: -86 dBm (historically the weakest detected signal from this device).
   - These values suggest the access point is somewhat distant or obstructed since signals closer to 0 dBm are stronger.
4. **Encryption and Security**:

  - This AP supports a combination of WPA2 and WPA3 encryption protocols:
    - **WPA3-TRANSITION**: An AP using both WPA2 and WPA3 simultaneously to provide backward compatibility for older devices.
    - **WPA3-SAE**: WPA3's more secure handshake method (Simultaneous Authentication of Equals).
    - **WPA2-PSK**: Traditional WPA2 with Pre-Shared Key, still in use by some networks.
  - Security-wise, the presence of **WPA3** is good, as it's the most current standard.

Network Information:

- **SSID**: The network is named "Shef Kitchen."
- **BSSID**: The MAC address of the AP is **74:37:5F:90:28**
  .
- **Channels**: The AP is seen operating primarily on **Channel 1** in the 2.4 GHz band and **5.720 GHz** in the 5 GHz band.

Packet Traffic:

- **Packets Sent**: It looks like some packet data has been captured:
  - 246 B (Bytes) on channel 149.
  - **3 KB** on channel 36 (perhaps suggesting client activity or beacon frames).
  - Most other devices show very little packet data, indicating that they may be inactive or not transmitting much data.

Additional Observations:

- The **device list** shows several nearby access points, each broadcasting on different channels and frequencies, with encryption schemes ranging from WPA3 to WPA2.

Weak Encryption (WPA2-PSK)

- While WPA2-PSK (Pre-Shared Key) is a widely used encryption protocol, it is vulnerable to **brute force and dictionary attacks** if weak passwords are used. Attackers could capture the WPA2 handshake and try to crack the key using common wordlists .
- **Threat**: If any of the networks are using weak or default passwords with WPA2-PSK, they could be compromised by attackers capturing the handshake and performing offline cracking.

Potential Rogue Access Points

- There could be unauthorized or rogue access points that are imitating legitimate networks, particularly if an attacker has set up an AP with a **duplicate SSID**. This is especially dangerous for networks with WPA2-PSK because users could unknowingly connect to the rogue AP.
- **Threat**: Users connecting to a rogue AP could have their traffic intercepted or manipulated through a **man-in-the-middle (MITM) attack**, exposing sensitive information such as credentials, personal data, or internal network traffic.

4. Unprotected Management Frames

- If **802.11w (Protected Management Frames - PMF)** is not enabled, management frames such as deauthentication and disassociation frames are unprotected. Attackers can use these vulnerabilities to **disrupt network traffic** via deauthentication attacks.
- **Threat**: The networks can be vulnerable to **WiFi jamming and deauthentication attacks**, which can force clients off the network or even capture handshakes to use in offline cracking attempts.

5. Weak Signal and Signal Interference

- Some networks show **weak signals** (-81 dBm or weaker), which could indicate that the devices or APs are far away or have poor signal quality. Poor signal strength might be exploited by attackers to perform **denial-of-service (DoS) attacks** through **jamming** or by simply overwhelming the network with noise.
- **Threat**: The presence of **multiple devices on the same or overlapping channels** (e.g., multiple devices on Channel 149) can lead to **channel congestion**, which attackers could exploit to perform jamming attacks and disrupt legitimate communication.

6. Unsecured Devices or Open APs

- While the screenshot doesn’t explicitly show any **open access points**, any unsecured networks (open or using WEP) would present a high-security risk.
- **Threat**: Open APs can be easily accessed by attackers, who can conduct **MITM attacks**, inject malicious traffic, or gain unauthorized access to internal network resources.

7. Legacy Devices Using WPA2

- Some devices may still rely on **WPA2-SAE**, even though they are part of networks transitioning to WPA3. These devices, depending on their implementation, might not support advanced features like **protected management frames (PMF)** or strong cryptographic algorithms.

- **Threat**: Devices with **outdated firmware** or **poor WPA2 implementations** can be vulnerable to exploits like **KRACK (Key Reinstallation Attacks)**, which target WPA2 vulnerabilities.

Mitigation Strategies:

1. **Use WPA3 with SAE (without transition mode)**: For sensitive networks, ensure WPA3-SAE is used exclusively without fallback to WPA2. This limits the risk of attacks targeting WPA2 vulnerabilities.
2. **Enable 802.11w (Protected Management Frames)**: Ensure that 802.11w is enabled to protect against deauthentication and disassociation attacks. This can prevent attackers from easily disrupting your network traffic.
3. **Monitor for Rogue APs**: Use a Wireless Intrusion Detection System (WIDS) to regularly monitor for rogue APs with the same or similar SSIDs. Ensure your clients are configured to connect only to authorized networks.
4. **Strong Passwords**: Ensure all WPA2/3-PSK networks use strong, complex passwords. This will help mitigate brute-force or dictionary-based attacks on captured handshakes.
5. **Update Firmware**: Regularly update the firmware of routers and APs to protect against known vulnerabilities like KRACK, and ensure that security features like WPA3 and PMF are properly implemented.
6. **Reduce Channel Congestion**: Spread devices across different channels, particularly in the 5 GHz band, to avoid interference and channel saturation. This can help mitigate jamming attacks.