Wireless Intrusion Detection Systems (WIDS) Setup

Objective: Learn how to set up a Wireless Intrusion Detection System (WIDS) to detect unauthorized access points and malicious activity in a wireless network.

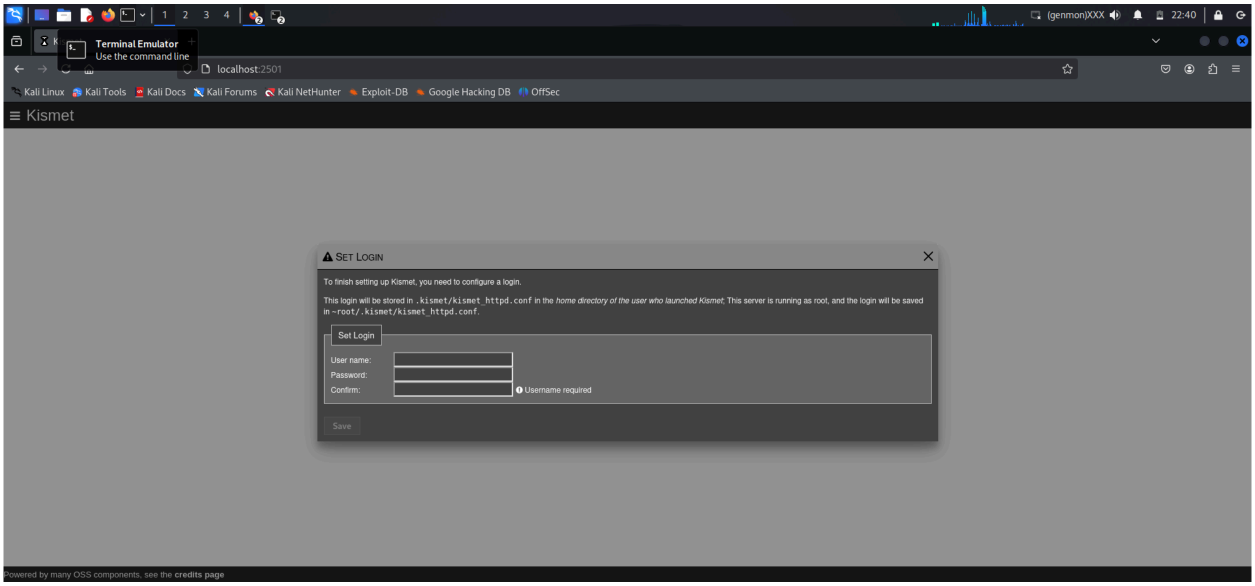
Tools:

- `Kismet` (a wireless network detector, sniffer, and IDS tool).
- Kali Linux or a Linux distribution with wireless tools

Kismet is a tool for sniffing and detecting wireless networks that records and examines network traffic. Numerous wireless network types, including Bluetooth, Zigbee, Wi-Fi (802.11), and others, may be detected by it. The main purposes of Kismet are:

Finding nearby wireless networks: By analyzing radio frequencies, it can find wireless networks, even ones that are concealed.
Wireless data capture: It records packets and data transmitted via wireless networks, which is helpful for security evaluations, network analysis, and troubleshooting.
Finding rogue devices or access points: In wireless settings, it assists in locating illegal devices, access points, or odd activity.

In Kismet, a **data source** refers to the network interface (wireless adapter) that Kismet uses to capture packets. Since i am using an Alfa wireless adapter, i need to configure Kismet to use that adapter as a data source to monitor the wireless network traffic.



SET LOGIN

To finish setting up Kismet, you need to configure a login.

This login will be stored in `.kismet/kismet_httpd.conf` in the *home directory of the user who launched Kismet*; This server is running as root, and the login will be saved in `~root/.kismet/kismet_httpd.conf`.

Set Login

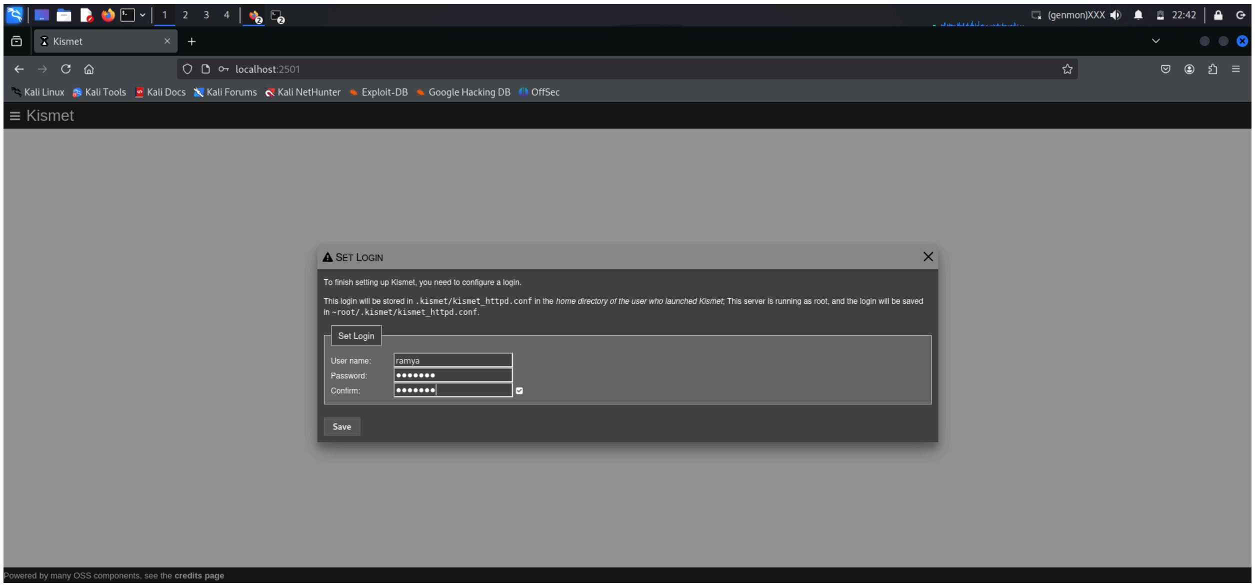
User name:

Password:

Confirm: Username required

Save

Powered by many OSS components, see the **credits page**



SET LOGIN

To finish setting up Kismet, you need to configure a login.

This login will be stored in `.kismet/kismet_httpd.conf` in the *home directory of the user who launched Kismet*; This server is running as root, and the login will be saved in `~root/.kismet/kismet_httpd.conf`.

Set Login

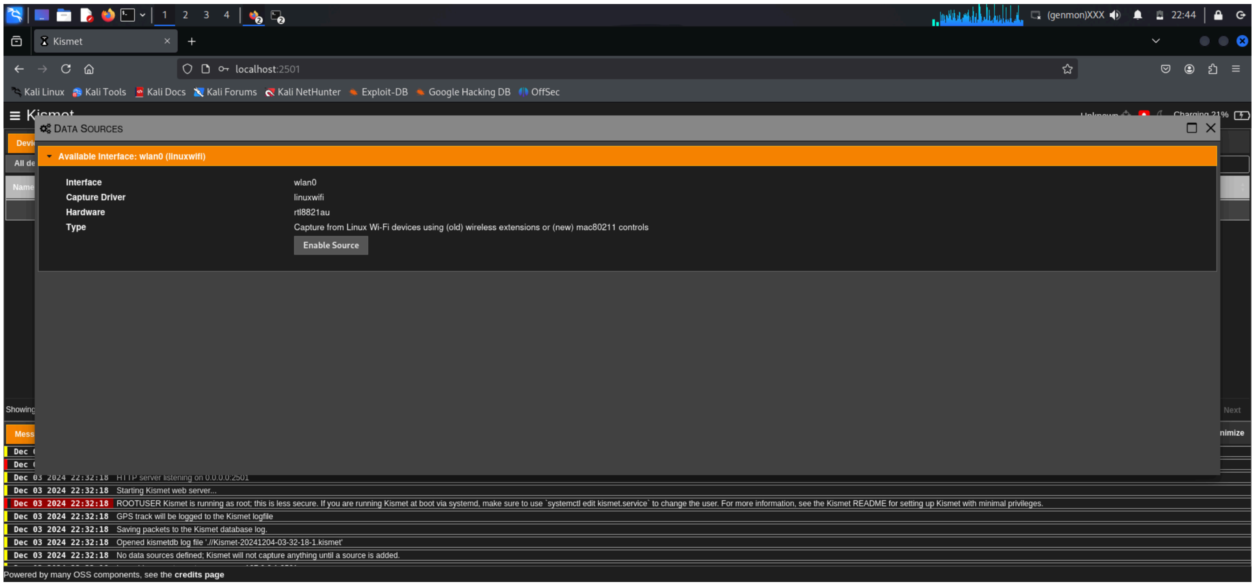
User name: ramya

Password: •••••••

Confirm: ••••••• ☑

Save

Powered by many OSS components, see the **credits page**



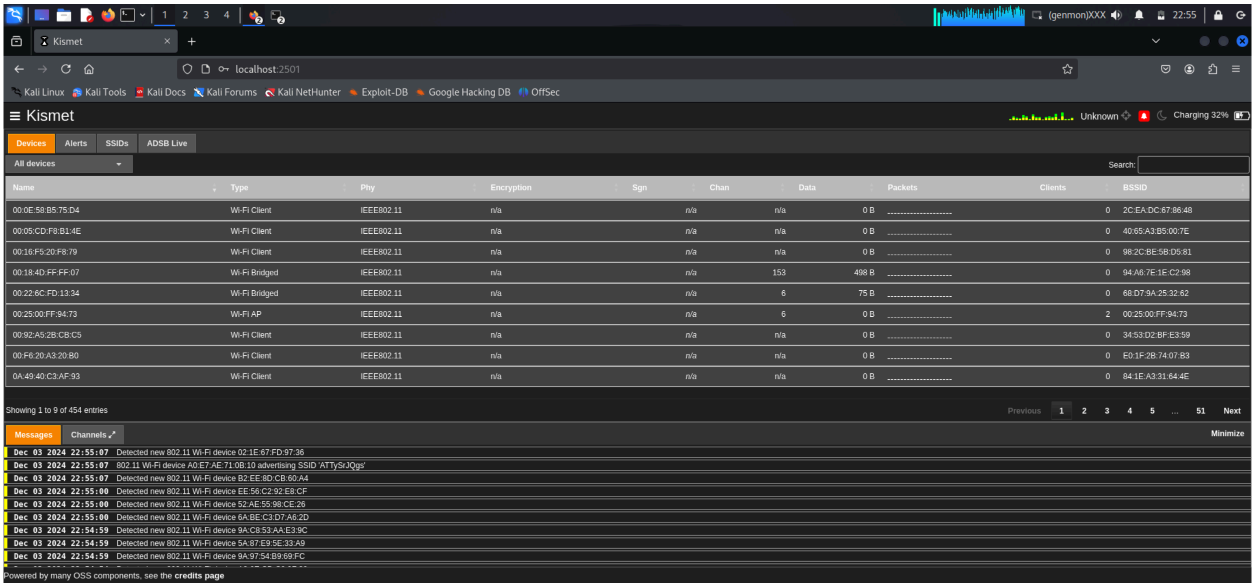
1 2 3 4
(genmon)XXX 22:44
Kismet
localhost:2501
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Kismet
DATA SOURCES

Available Interface: wlan0 (linuxwifi)

Interface	wlan0
Capture Driver	linuxwifi
Hardware	rtl8821au
Type	Capture from Linux Wi-Fi devices using (old) wireless extensions or (new) mac80211 controls

```
Dec 03 2024 22:32:18  HTTP server listening on 0.0.0.0:2501
Dec 03 2024 22:32:18  Starting Kismet web server...
Dec 03 2024 22:32:18  ROOTUSER Kismet is running as root; this is less secure. If you are running Kismet at boot via systemd, make sure to use `systemctl edit kismet.service` to change the user. For more information, see the Kismet README for setting up Kismet with minimal privileges.
Dec 03 2024 22:32:18  GPS track will be logged to the Kismet logfile
Dec 03 2024 22:32:18  Saving packets to the Kismet database log.
Dec 03 2024 22:32:18  Opened kismetdb log file './/Kismet-20241204-03-32-18-1.kismet'
Dec 03 2024 22:32:18  No data sources defined; Kismet will not capture anything until a source is added.
```

Powered by many OSS components, see the **credits page**

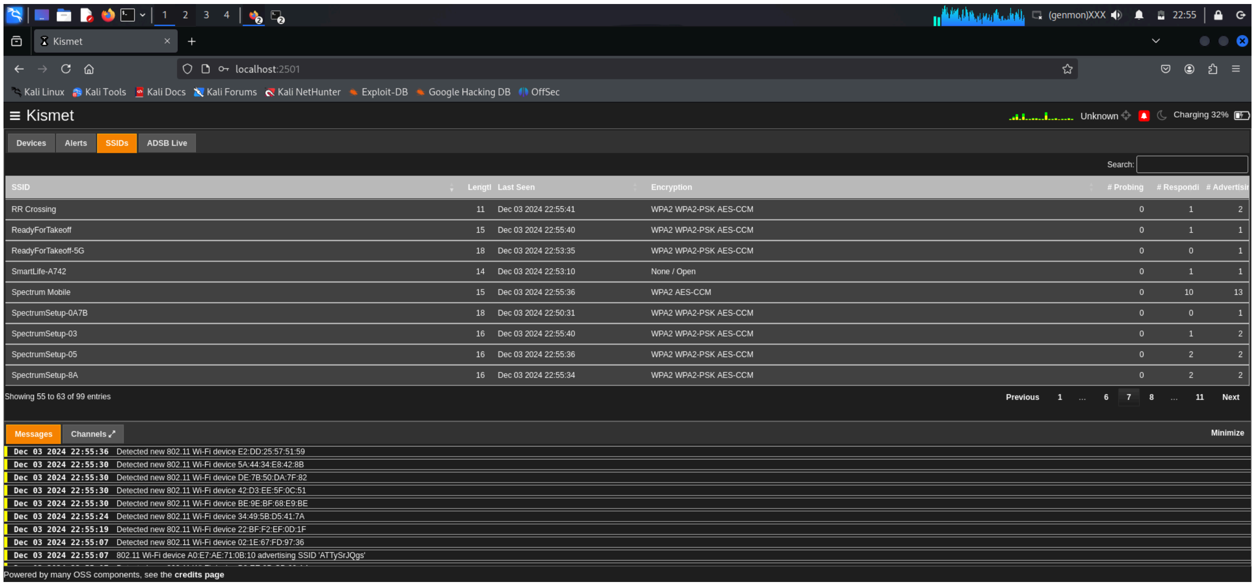


Name	Type	Phy	Encryption	Sgn	Chan	Data	Packets	Clients	BSSID
00:0E:58:B5:75:D4	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B	--------------------	0	2C:EA:DC:67:86:48
00:05:CD:F8:B1:4E	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B	--------------------	0	40:65:A3:B5:00:7E
00:16:F5:20:F8:79	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B	--------------------	0	98:2C:BE:5B:D5:81
00:18:4D:FF:FF:07	Wi-Fi Bridged	IEEE802.11	n/a	n/a	153	498 B	--------------------	0	94:A6:7E:1E:C2:98
00:22:6C:FD:13:34	Wi-Fi Bridged	IEEE802.11	n/a	n/a	6	75 B	--------------------	0	68:D7:9A:25:32:62
00:25:00:FF:94:73	Wi-Fi AP	IEEE802.11	n/a	n/a	6	0 B	--------------------	2	00:25:00:FF:94:73
00:92:A5:2B:CB:C5	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B	--------------------	0	34:53:D2:BF:E3:59
00:F6:20:A3:20:B0	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B	--------------------	0	E0:1F:2B:74:07:B3
0A:49:40:C3:AF:93	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B	--------------------	0	84:1E:A3:31:64:4E

Showing 1 to 9 of 454 entries

```
Dec 03 2024 22:55:07  Detected new 802.11 Wi-Fi device 02:1E:67:FD:97:36
Dec 03 2024 22:55:07  802.11 Wi-Fi device A0:E7:AE:71:0B:10 advertising SSID 'ATTySrJQgs'
Dec 03 2024 22:55:07  Detected new 802.11 Wi-Fi device B2:EE:8D:CB:60:A4
Dec 03 2024 22:55:00  Detected new 802.11 Wi-Fi device EE:56:C2:92:E8:CF
Dec 03 2024 22:55:00  Detected new 802.11 Wi-Fi device 52:AE:55:98:CE:26
Dec 03 2024 22:55:00  Detected new 802.11 Wi-Fi device 6A:BE:C3:D7:A6:2D
Dec 03 2024 22:54:59  Detected new 802.11 Wi-Fi device 9A:C8:53:AA:E3:9C
Dec 03 2024 22:54:59  Detected new 802.11 Wi-Fi device 5A:87:E9:5E:33:A9
Dec 03 2024 22:54:59  Detected new 802.11 Wi-Fi device 9A:97:54:B9:69:FC
```

Powered by many OSS components, see the **credits page**

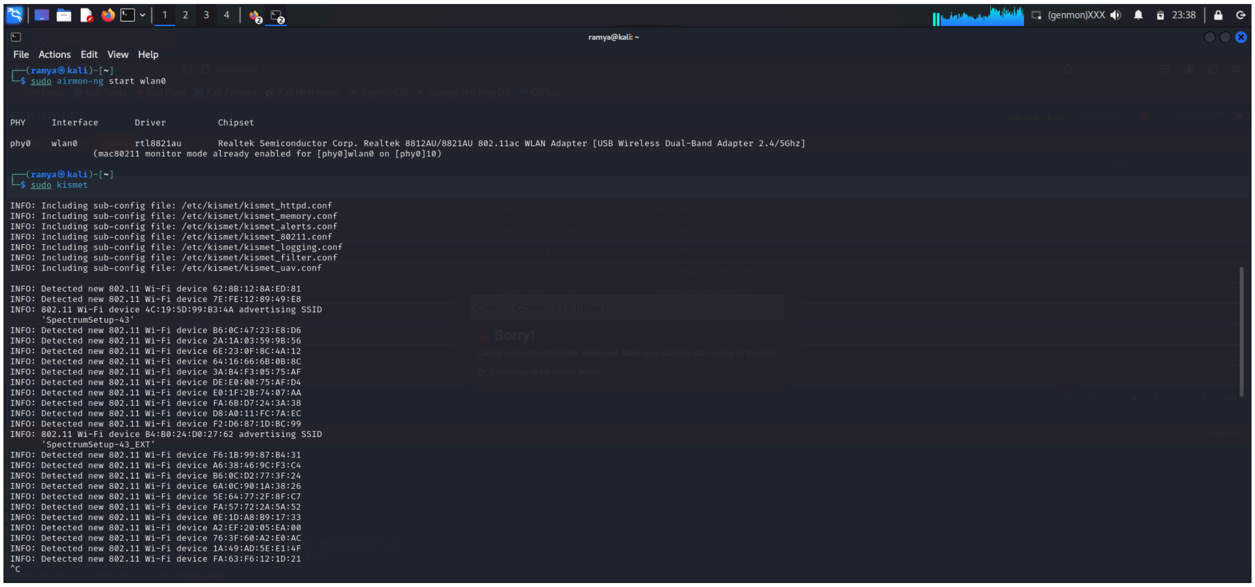


SSID	Lengtl	Last Seen	Encryption	# Probing	# Respondi	# Advertisi
RR Crossing	11	Dec 03 2024 22:55:41	WPA2 WPA2-PSK AES-CCM	0	1	2
ReadyForTakeoff	15	Dec 03 2024 22:55:40	WPA2 WPA2-PSK AES-CCM	0	1	1
ReadyForTakeoff-5G	18	Dec 03 2024 22:53:35	WPA2 WPA2-PSK AES-CCM	0	0	1
SmartLife-A742	14	Dec 03 2024 22:53:10	None / Open	0	1	1
Spectrum Mobile	15	Dec 03 2024 22:55:36	WPA2 AES-CCM	0	10	13
SpectrumSetup-0A7B	18	Dec 03 2024 22:50:31	WPA2 WPA2-PSK AES-CCM	0	0	1
SpectrumSetup-03	16	Dec 03 2024 22:55:40	WPA2 WPA2-PSK AES-CCM	0	1	2
SpectrumSetup-05	16	Dec 03 2024 22:55:36	WPA2 WPA2-PSK AES-CCM	0	2	2
SpectrumSetup-8A	16	Dec 03 2024 22:55:34	WPA2 WPA2-PSK AES-CCM	0	2	2

Showing 55 to 63 of 99 entries

```
Dec 03 2024 22:55:36  Detected new 802.11 Wi-Fi device E2:DD:25:57:51:59
Dec 03 2024 22:55:30  Detected new 802.11 Wi-Fi device 5A:44:34:E8:42:8B
Dec 03 2024 22:55:30  Detected new 802.11 Wi-Fi device DE:7B:50:DA:7F:82
Dec 03 2024 22:55:30  Detected new 802.11 Wi-Fi device 42:D3:EE:5F:0C:51
Dec 03 2024 22:55:30  Detected new 802.11 Wi-Fi device BE:9E:BF:68:E9:BE
Dec 03 2024 22:55:24  Detected new 802.11 Wi-Fi device 34:49:5B:D5:41:7A
Dec 03 2024 22:55:19  Detected new 802.11 Wi-Fi device 22:BF:F2:EF:0D:1F
Dec 03 2024 22:55:07  Detected new 802.11 Wi-Fi device 02:1E:67:FD:97:36
Dec 03 2024 22:55:07  802.11 Wi-Fi device A0:E7:AE:71:0B:10 advertising SSID 'ATTySrJQgs'
```

Powered by many OSS components, see the **credits page**



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

┌──(ramya㉿kali)-[~]
└─$ sudo kismet

INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf

INFO: Detected new 802.11 Wi-Fi device 62:8B:12:8A:ED:81
INFO: Detected new 802.11 Wi-Fi device 7E:FE:12:89:49:E8
INFO: 802.11 Wi-Fi device 4C:19:5D:99:B3:4A advertising SSID
      'SpectrumSetup-43'
INFO: Detected new 802.11 Wi-Fi device B6:0C:47:23:E8:D6
INFO: Detected new 802.11 Wi-Fi device 2A:1A:03:59:9B:56
INFO: Detected new 802.11 Wi-Fi device 6E:23:0F:8C:4A:12
INFO: Detected new 802.11 Wi-Fi device 64:16:66:6B:0B:8C
INFO: Detected new 802.11 Wi-Fi device 3A:B4:F3:05:75:AF
INFO: Detected new 802.11 Wi-Fi device DE:E0:00:75:AF:D4
INFO: Detected new 802.11 Wi-Fi device E0:1F:2B:74:07:AA
INFO: Detected new 802.11 Wi-Fi device FA:6B:D7:24:3A:38
INFO: Detected new 802.11 Wi-Fi device D8:A0:11:FC:7A:EC
INFO: Detected new 802.11 Wi-Fi device F2:D6:87:1D:BC:99
INFO: 802.11 Wi-Fi device B4:B0:24:D0:27:62 advertising SSID
      'SpectrumSetup-43_EXT'
INFO: Detected new 802.11 Wi-Fi device F6:1B:99:87:B4:31
INFO: Detected new 802.11 Wi-Fi device A6:38:46:9C:F3:C4
INFO: Detected new 802.11 Wi-Fi device B6:0C:D2:77:3F:24
INFO: Detected new 802.11 Wi-Fi device 6A:0C:90:1A:38:26
INFO: Detected new 802.11 Wi-Fi device 5E:64:77:2F:8F:C7
INFO: Detected new 802.11 Wi-Fi device FA:57:72:2A:5A:52
INFO: Detected new 802.11 Wi-Fi device 0E:1D:A8:B9:17:33
INFO: Detected new 802.11 Wi-Fi device A2:EF:20:05:EA:00
INFO: Detected new 802.11 Wi-Fi device 76:3F:60:A2:E0:AC
INFO: Detected new 802.11 Wi-Fi device 1A:49:AD:5E:E1:4F
INFO: Detected new 802.11 Wi-Fi device FA:63:F6:12:1D:21
^C
```

In my observation

1.Multiple Wi-Fi Devices: Kismet detected numerous Wi-Fi devices broadcasting various SSIDs (Service Set Identifiers). These include common SSIDs like `NETGEAR00`, `SpectrumSetup-43`, `MyCharterWiFi8b-2G`, `MySpectrumWiFi52-2G`, and `ATTySrJQgs`. It is normal to see various devices in the area.

2.Rouge AP Possibility:

> **SSID Anomalies**: If there is an SSID being advertised by multiple APs (e.g., `SpectrumSetup-43`), it might indicate a misconfiguration or a potential rogue AP (though this isn't always the case). This can happen if a malicious actor is attempting to impersonate a legitimate access point to gain unauthorized access.

3.SSID 'SpectrumSetup-43' and 'SpectrumSetup-43_EXT': The presence of a similarly named extended SSID (`SpectrumSetup-43_EXT`) could be a sign of a legitimate network using a range extender, but it's worth monitoring to ensure it's not a rogue device trying to impersonate a valid network.

4.Devices Advertising the Same SSID: In my logs, several APs appear to advertise the same SSID but have different MAC addresses, such as:

- `SpectrumSetup-43` and `SpectrumSetup-43_EXT` (MAC addresses: 4C:19:5D:99:B3:4A and B4:B0:24:D0:27:62)
- `NETGEAR00` (MAC address: 78:D2:94:6F:6F:E9) and `NETGEAR20` (MAC address: 94:A6:7E:1E:C2:96)

Potential Concerns:

- **SSID Cloning**: Rogue devices may use similar or identical SSIDs to legitimate networks to trick users into connecting. Monitor the MAC addresses associated with these SSIDs for unusual patterns.
- **Monitor Unusual MAC Addresses**: Devices that you don’t recognize or that seem to broadcast unusual SSIDs could be an indication of suspicious activity.