Wireless Network Scanning and Information Gathering

Objective: Learn how to scan for wireless networks, gather essential information, and analyze the available wireless access points (APs) using various tools.

Tools:

1. Kali Linux or any Linux distribution with wireless network tools.
2. Aircrack-ng suite.
3. A wireless adapter that supports monitor mode.

1. This will display a list of nearby wireless networks with the following details:
    a. **BSSID**: The MAC address of the access point (AP).
    b. **PWR**: Signal strength (in dBm).
    c. **Beacons**: Number of beacon frames sent by the AP.
    d. **#Data**: Data packets sent from or to the AP.
    e. **CH**: The channel the network is operating on.
    f. **MB**: Maximum speed supported by the AP.
    g. **ENC**: The encryption type (e.g., WEP, WPA, WPA2).
    h. **CIPHER**: The cipher used for encryption (e.g., TKIP, CCMP).
    i. **AUTH**: Authentication mechanism (e.g., PSK).
    j. **ESSID**: The SSID or network name.
2. Leave airodump-ng running for a few minutes to capture all available networks.

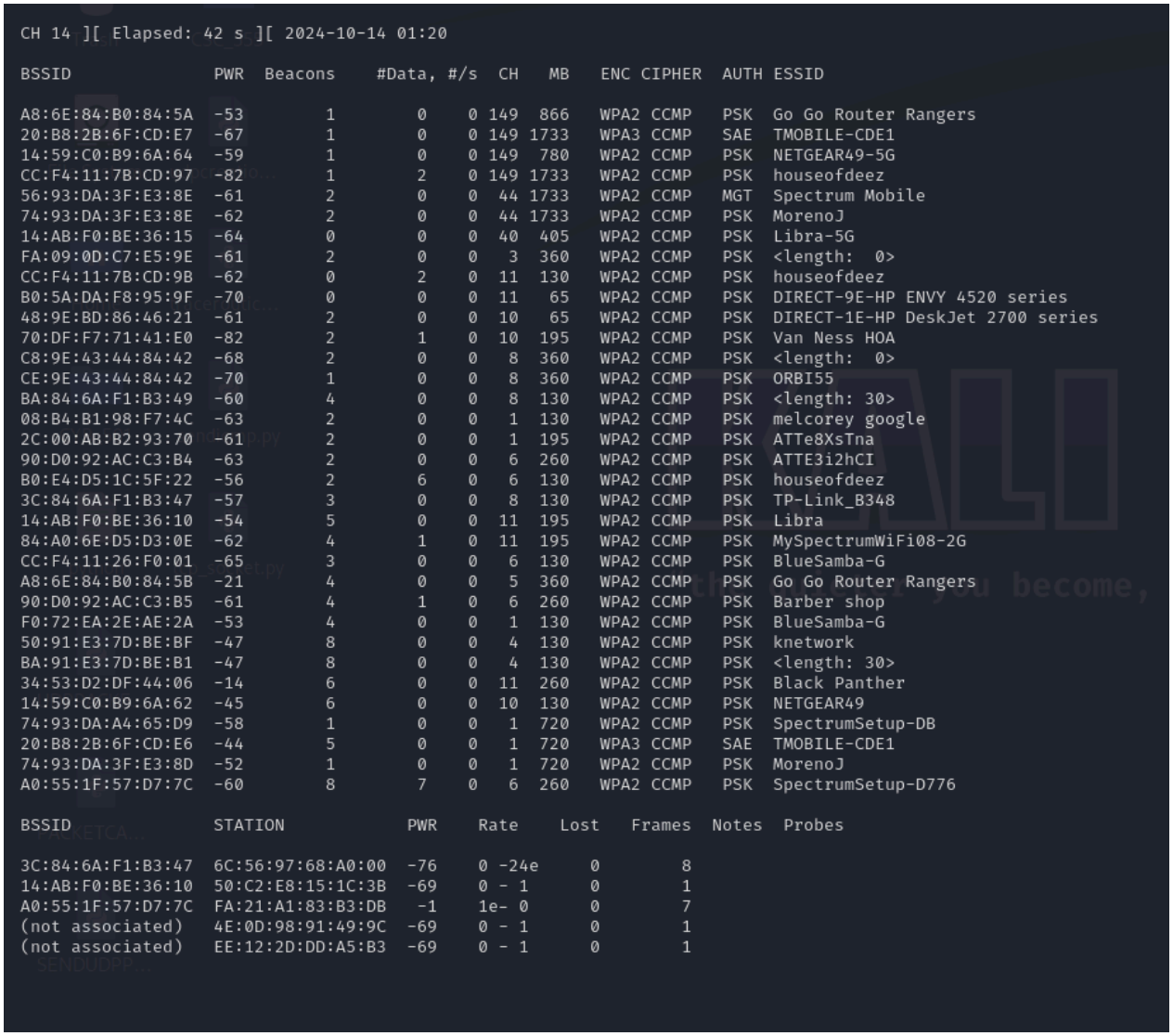
3. Identify Key Information

For each detected network, gather the following key information:

1. **SSID**: The network name (ESSID).
2. **BSSID**: The unique MAC address of the access point.
3. **Channel**: The channel the network is operating on.
4. **Encryption Type**: The encryption protocol (WEP, WPA, WPA2).
5. **Signal Strength (PWR)**: Measured in dBm, lower values indicate stronger signals (e.g., -50 dBm is stronger than -80 dBm).

pause the airodump-ng output by pressing Ctrl + C.


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
515 NetworkManager
640 wpa_supplicant
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]
(monitor mode enabled)
(root kali)-[~]
sudo airodump-ng wlan0
Warning: Detected you are using a non-UNICODE terminal character encoding.



```
CH 14 ][ Elapsed: 42 s ][ 2024-10-14 01:20

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

A8:6E:84:B0:84:5A  -53        1        0    0 149  866   WPA2 CCMP   PSK  Go Go Router Rangers
20:B8:2B:6F:CD:E7  -67        1        0    0 149 1733   WPA3 CCMP   SAE  TMOBILE-CDE1
14:59:C0:B9:6A:64  -59        1        0    0 149  780   WPA2 CCMP   PSK  NETGEAR49-5G
CC:F4:11:7B:CD:97  -82        1        2    0 149 1733   WPA2 CCMP   PSK  houseofdeez
56:93:DA:3F:E3:8E  -61        2        0    0  44 1733   WPA2 CCMP   MGT  Spectrum Mobile
74:93:DA:3F:E3:8E  -62        2        0    0  44 1733   WPA2 CCMP   PSK  MorenoJ
14:AB:F0:BE:36:15  -64        0        0    0  40  405   WPA2 CCMP   PSK  Libra-5G
FA:09:0D:C7:E5:9E  -61        2        0    0   3  360   WPA2 CCMP   PSK  <length:  0>
CC:F4:11:7B:CD:9B  -62        0        2    0  11  130   WPA2 CCMP   PSK  houseofdeez
B0:5A:DA:F8:95:9F  -70        0        0    0  11   65   WPA2 CCMP   PSK  DIRECT-9E-HP ENVY 4520 series
48:9E:BD:86:46:21  -61        2        0    0  10   65   WPA2 CCMP   PSK  DIRECT-1E-HP DeskJet 2700 series
70:DF:F7:71:41:E0  -82        2        1    0  10  195   WPA2 CCMP   PSK  Van Ness HOA
C8:9E:43:44:84:42  -68        2        0    0   8  360   WPA2 CCMP   PSK  <length:  0>
CE:9E:43:44:84:42  -70        1        0    0   8  360   WPA2 CCMP   PSK  ORBI55
BA:84:6A:F1:B3:49  -60        4        0    0   8  130   WPA2 CCMP   PSK  <length: 30>
08:B4:B1:98:F7:4C  -63        2        0    0   1  130   WPA2 CCMP   PSK  melcorey google
2C:00:AB:B2:93:70  -61        2        0    0   1  195   WPA2 CCMP   PSK  ATTe8XsTna
90:D0:92:AC:C3:B4  -63        2        0    0   6  260   WPA2 CCMP   PSK  ATTE3i2hCI
B0:E4:D5:1C:5F:22  -56        2        6    0   6  130   WPA2 CCMP   PSK  houseofdeez
3C:84:6A:F1:B3:47  -57        3        0    0   8  130   WPA2 CCMP   PSK  TP-Link_B348
14:AB:F0:BE:36:10  -54        5        0    0  11  195   WPA2 CCMP   PSK  Libra
84:A0:6E:D5:D3:0E  -62        4        1    0  11  195   WPA2 CCMP   PSK  MySpectrumWiFi08-2G
CC:F4:11:26:F0:01  -65        3        0    0   6  130   WPA2 CCMP   PSK  BlueSamba-G
A8:6E:84:B0:84:5B  -21        4        0    0   5  360   WPA2 CCMP   PSK  Go Go Router Rangers
90:D0:92:AC:C3:B5  -61        4        1    0   6  260   WPA2 CCMP   PSK  Barber shop
F0:72:EA:2E:AE:2A  -53        4        0    0   1  130   WPA2 CCMP   PSK  BlueSamba-G
50:91:E3:7D:BE:BF  -47        8        0    0   4  130   WPA2 CCMP   PSK  knetwork
BA:91:E3:7D:BE:B1  -47        8        0    0   4  130   WPA2 CCMP   PSK  <length: 30>
34:53:D2:DF:44:06  -14        6        0    0  11  260   WPA2 CCMP   PSK  Black Panther
14:59:C0:B9:6A:62  -45        6        0    0  10  130   WPA2 CCMP   PSK  NETGEAR49
74:93:DA:A4:65:D9  -58        1        0    0   1  720   WPA2 CCMP   PSK  SpectrumSetup-DB
20:B8:2B:6F:CD:E6  -44        5        0    0   1  720   WPA3 CCMP   SAE  TMOBILE-CDE1
74:93:DA:3F:E3:8D  -52        1        0    0   1  720   WPA2 CCMP   PSK  MorenoJ
A0:55:1F:57:D7:7C  -60        8        7    0   6  260   WPA2 CCMP   PSK  SpectrumSetup-D776

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

3C:84:6A:F1:B3:47  6C:56:97:68:A0:00  -76    0 -24e     0        8
14:AB:F0:BE:36:10  50:C2:E8:15:1C:3B  -69    0 - 1      0        1
A0:55:1F:57:D7:7C  FA:21:A1:83:B3:DB   -1    1e- 0      0        7
(not associated)   4E:0D:98:91:49:9C  -69    0 - 1      0        1
(not associated)   EE:12:2D:DD:A5:B3  -69    0 - 1      0        1
```

Encryption Type: Networks using WEP or WPA (without WPA2) are vulnerable to attacks, as these encryption methods have known weaknesses. For a secure network, WPA2 or WPA3 should be used.

Channel Overlap: If several networks operate on the same or overlapping channels (e.g., 1, 6, 11), this can lead to interference, degrading performance. Channel selection can be optimized to improve network efficiency.

Signal Strength: Monitoring signal strength helps in determining the range of an access point and identifying areas of weak coverage. Networks with very strong signals (close to -30 dBm) may be closely located, which could be important in a physical security assessment.