## Lab 17: Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

### Scenario

As a certified cybersecurity practitioner, it is essential to test the security of Wi-Fi networks to see if they are vulnerable to attacks. One of the ways to do this is by using tools like Wash and Wireshark.

### Solution

You are tasked with testing the security of a Wi-Fi network at a company’s office. You begin by using Wash to scan the area for Wi-Fi networks in range. Wash shows you a list of all the visible Wi-Fi networks, including the name of the network, the signal strength, and the encryption type.

Now, you use Wireshark. You run Wireshark to capture and analyze the Wi-Fi packets transmitted on the network.

**Note:** In this lab, we use a Linksys 802.11 g wireless network adapter. You can use any wireless adapter to perform this lab.

|  |
| --- |
| 1. You must plug in a wireless network (Linksys 802.11 g WLAN) adapter. A **New USB Device Detected** window appears; click **Connect to a virtual machine** and select your attacking machine. Click **OK**.    2. Open the terminal and enter the **sudo su** command to switch to root. Enter the **cd** command to go to the root directory.    3. Enter the **ifconfig** command to see the newly added wireless network interface name.    4. Enter the **airmon-ng start *wireless\_interface*** command to start the **Airmon-ng** software and bind the wireless adapter.    5. Enter the **airmon-ng check kill** command to stop the network managers and terminate the interfering processes.    6. Enter the **airmon-ng start wlx00e02d886189** command to put the wireless interface in monitor mode.    7. Enter the **wash -i wlx00e02d886189** command to detect the WPS-enabled devices. It shows the devices, signal strength, vendor names, and channel numbers.    8. Open Wireshark and double-click the wireless network adapter interface to capture the packets.    9. It starts capturing the packets. Wireless packets are labeled with **802.11** under the Protocol column.    **Note:** In a real-life attack, attackers use packet capture and filtering techniques to capture packets containing passwords (only for HTTP websites), perform attacks such as session hijacking, etc.  10. This concludes the demonstration of how to find Wi-Fi networks and sniff Wi-Fi packets using Wireshark. |