**Lab 10-01: Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark**

**Scenario**

As a penetration tester, 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. |

**Lab 10-02: Crack a WPA2 Network using Aircrack-ng**

**Scenario**

As a penetration tester, one of your tasks involves testing the security of wireless networks. One way to test a wireless network’s security is to crack its password. WPA2 is one of the most commonly used wireless security protocols, and cracking its password can give the tester access to the network and the information transmitted over it.

**Solution**

A pentester may use a tool like Aircrack-ng to crack a WPA2 network. The tool allows the tester to capture packets transmitted over the network and use them to determine its encryption key. It can be done by capturing a sufficient number of packets and then performing a dictionary attack or a brute-force attack on the captured packets.

**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. Plug the wireless network adapter (Linksys 802.11 g WLAN) and select the **Connect to a virtual machine** option. Select your attacking virtual machine and click **OK**.    2. Enter the **sudo su** command to switch to root. Enter the **cd** command to move 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. **wlx00e02d886189** is now running in monitor mode.    7. To list the detected Access Points and the connected clients (or stations), enter the **airodump-ng wlx00e02d886189** command. You can see the Access Point used in this example.    9. Enter the **airodump-ng --bssid *target\_AP* -c *channel\_number* -w *file\_name* wlx00e02d886189** command to capture the packets from the Access Point and leave it running.   * **--bssid flag** specifies the target Access Point * **-c flag** specifies the channel number on which the target AP is configured to run * **-w flag** writes the captured data in the file     10. Open a new terminal, and enter the **aireplay-ng -0 11 -a *AP\_MAC\_address* -c *destination\_MAC\_address* wlx00e02d886189** command to send deauthentication packets.   * **-0 flag** activates the deauthentication mode * **11** specifies the number of deauthentication packets to be sent * **-a flag** specifies the MAC address of the Access Point * **-c flag** specifies the destination MAC address   **Note:** Run the above command multiple times if you get an error.    Return to the terminal where **airodump-ng** is running and keep it running until you receive the **WPA handshake: 22:7F:AC:6D:E6:8B** packet, which tells you that a WPA/WPA2 handshake has successfully been captured for the target BSSID.  11. Open a new terminal window and enter the **aircrack-ng -a2 *AP\_MAC\_address* -w *path\_to\_password.txt path\_to\_captured\_file*** command.   * **-a flag** specifies the attack mode * **-w flag** specifies the path to the wordlist   It displays the captured WPA handshake packet. It also displays the Wi-Fi password in clear text next to the **KEY FOUND!** message.    12. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng. |