Wi-Fi Network Quality Assurance Engineer
Home assignment

Version 1

Demonstrate Linux Wi-Fi adapter operations in STA and Monitor modes

List of required equipment:

1. Test computer - PC/laptop with Wi-Fi adapter and Linux-based OS.
   If there is no Linux OS available, then a bootable USB stick can be used with Kali or Ubuntu OS.
2. Secured Wi-Fi Access Point (for Wi-Fi client's connectivity).
   Nice to have (not required):
   a. Dual/triple Band (2.4GHz/5GHz/6GHz) support.
   b. WPA3 support.
3. Wi-Fi client (example: another laptop or smartphone).

The test computer should be able to:

1. Establish Wi-Fi connectivity to a particular BSSID by using “wpa_supplicant”. Can browse the Internet.
2. Sniff Wi-Fi traffic by using “Wireshark”.

Deliverables

1. List of used tools and corresponding configuration changes for them if any.
2. Technical details about the WiFi adapter on the PC/laptop.
3. Two separate “wpa_supplicant.conf” files and connectivity logs:
   a. Connection to the particular SSID.
      Share Wi-Fi connection details by executing “status” in the “wpa_cli” tool.
      Share logs with the connectivity process details.
      Be ready to explain the output.
   b. Connects to the particular BSSID (connect to another AP Band if available).
      Share Wi-Fi connection details by executing “status” in the “wpa_cli” tool.
      Share logs with the connectivity process details.
      Be ready to explain the output.
4. Short how-to:
   a. switch the Wi-Fi interface to Monitor mode.
   b. start Wi-Fi sniffing on the particular Wi-Fi channel.
   c. decrypt Wi-Fi traffic in Wireshark.
   d. perform Wi-Fi scanning for available networks by using both “wpa_cli” and “iw” tools.

    e. (optional) measure channel utilization and interference using any other available tools and devices.
    f. check the Country's regulatory domain.
    g. change the Country's regulatory domain.
5. Wi-Fi captures with Beacon frames broadcasted by the secured Wi-Fi AP. Be ready to explain the fields of the particular Beacon frame (for example: how to recognize whether the WiFi5 standard is supported?)
6. Wi-Fi captures with the full connection flow between the Wi-Fi client and secured Wi-Fi AP. Be ready to explain Wi-Fi connection flow (including 4-way handshake) and different types of Wi-Fi frames (data, control, management frames).

There is no limitation on extra SW packages - install and use whatever is needed.

Test tasks

#1 - Linux WiFi adapter in STA mode

1. Prepare “wpa_supplicant.conf” file configuration:
    a. Set target SSID.
    b. Set target password.
    c. Set a country regulation domain (according to your actual location).
    d. (If WPA3 is supported by the Wi-Fi AP) Configure WPA3 security mode.
2. Run the “wpa_supplicant” service and ensure that the connection is established successfully. Verify “wpa_supplicant” logs to see the connectivity process details.
3. Analyze Wi-Fi connection details by executing the “status” command in the “wpa_cli” tool.
4. Ensure that your Wi-Fi network interface has received an IP. If there is no IP, then figure out how to get it.
5. Ensure that the Internet is accessible via the WiFi connection (can execute: “ping google.com”).
6. Perform Wi-Fi scanning for available networks by using the “wpa_cli” tool.
7. Perform Wi-Fi scanning for available networks by using the “iw” tool.
8. Compare “wpa_cli” and “iw” output results. Do you see the same list of available networks? If not, then explain why it differs?
9. Edit “wpa_supplicant.conf” file configuration:
    a. Replace the SSID name with the BSSID (select another Band if supported by the Wi-Fi AP)
10. Repeat steps 2-5.
11. Save the results for each point list to the log file and share it with the recruiter.

#2 - Linux WiFi adapter in Monitor mode

1. Switch the Wi-Fi adapter to Monitor mode.
2. Figure out which Wi-Fi channel is used by the Wi-Fi AP.
3. Configure the same channel on the Wi-Fi adapter.
4. Start Wi-Fi sniffing.
5. Wait for 20 seconds.

6. Stop Wi-Fi sniffing.
7. Open the Wi-Fi capture in Wireshark and filter Wi-Fi AP Beacons. Save the Wi-Fi capture.
8. Start Wi-Fi sniffing.
9. Connect the Wi-Fi client to the Wi-Fi AP.
10. Access the “http://info.cern.ch/” page on the Wi-Fi client.
11. Stop Wi-Fi sniffing.
12. Open the Wi-Fi capture in Wireshark and filter only data that belongs to this particular Wi-Fi client.
13. Decrypt the capture to see DNS (resolving of “info.cern.ch”) and HTTP data. Save the Wi-Fi capture.
14. Save the results for each point list to the log file and share it with the recruiter.