Assignment Name: Assessing Wi-Fi Security

Prepared By

Rimon Ahammed Bappy

Reg:11900151

To check the security of WPA/WPA2 Wi-Fi Routers we need to follow some certain steps. To hack Wi-Fi password, we need to break the DORA (Discover, Offer, Request, Acknowledgement) principle. This DORA helps to save the device details in the router logs file that is why we need to enter the password for first time only. Rest of the time our device gets connected automatically to the router until the password is changed. To hack the Wi-Fi, we need to break this DORA principle using the DOS attack. We will send n number of packets to break the DORA principle. After the DOS attack the DORA will be reestablished and we will be able to get the password.

At the time of hacking, we need to identify three things:

1. BSSID: Basic service set identifier (mac address of router device)
2. SSID : Service set identifier (wlan logical name)
3. ESSID: Extended service set identifier (AP mode) [only required for AP mode]

Process to hack wi-fi using Kali Linux and various tools:

- We need to check Wi-Fi port details using command ***airmon-ng***

- Then we need to change our Wi-Fi adapter form managed mode to monitor mode using command ***airmon-ng start wlan0***. We need to kill all the processes that could cause problem.

- Now we need to collect the SSID, BSSID and Channel ID of the router using command ***airodump-ng wlan0mon***.

- After that we need to download a word list of WPA/WPA2 password from google or we can use Kali Linux tool crunch to make a word list.

- To collect the client ID who is connected to that router we need to use command ***airodump-ng -c [channel] --bssid [bssid] -w [path of the word list] wlan0mon***

- Now we need to break the DORA between the router and the client. For this we need to go for the largest frames because they are connecting more packets. This terminal will work as a tunnel so take a new terminal and use command ***aireplay-ng --deauth [packets] -a [router bssid] -c [client bssid] wlan0mon***.

- After running the command, we see in the tunnel terminal a wpa handshake file has been saved in the word list location. It will be saved in a file of .cap extension. Here is our desired password but it is encrypted. So, we need to crack the password.

- To crack the password, we need to use command ***aircrack-ng -b [router bssid] -w [path to wordlist] [path to the encrypted file]***. Running this command, the password will be shown in the terminal.

This is how we can check our Wi-Fi security using kali Linux and its by default tools.

To secure our Wi-Fi we can take some steps:

1. We can use a long and hard combination of words for the password.
2. We can use WPA3 router because it is not possible to hack yet.