

Wireless Section (10pts)

A tar file is included with this exercise. It includes two folders: crack_wpa and crack_wep. You will be using aircrack-ng to crack WPA and WEP. This tool can be installed on any Linux box (using apt-get on Ubuntu for instance) or you can download Kali Linux.

1: WEP

In the directory, there are several captures (*.cap files) from a WLAN network configured for WEP. To crack the password using the run.sh script. All it does is run: aircrack-ng *.cap. The tool will consume all the files and attempt to crack the WEP password.

Q1: What is the WEP password? It should take you about a second to crack but this is because you have all the data already. Show screenshot of the cracked password

2: WPA

In this directory, there are several captures (*.cap files) from a WLAN network configured for WPA. To crack the password using the run.sh script. It runs a dictionary attack using the dictionary file provided.

What is the WPA password? Show screenshot of the cracked password