Laborator 2 - WiFi Password Cracking

***Aircrack-ng***

In today's lab we look into WiFi security and break the WPA/WPA2 password.

You can easily run this lab in Kali Linux or install the necessary tools available at:

<https://www.aircrack-ng.org/doku.php?id=Main>

Aircrack-ng Tutorial: How to crack WPA/WPA2 - <https://www.aircrack-ng.org/doku.php?id=cracking_wpa>

IMPORTANT! To proceed with this lab you need to set up your own WPA/WPA2 network with NO connection to the internet.

IMPORTANT! Take care! Do not use this directly on your usual internet network or any other network, you can flood the network and/or ending up doing illegal actions. You are fully responsible for your action!

***Setting up the network***

1. Use your mobile phone.

2. Turn OFF your data connection.

3. Turn OFF your WiFi Connection.

4. Set up a hotspot, setting up WPA/WPA2-Personal with a weak password.

You can check if the password is in the dictionary of password (password.lst, e.g., located in /usr/share/john/)

5. Try to connect to the hotspot using your computer. You will NOT have access to the internet, but this is not a problem.

Take care! Check that the data connection and the WiFi are turned off on your phone.

Note: If you use a weak password you will need to collect less packets to crack it.

***Change the WiFi interface to monitor mode***

Check the exact steps in the tutorial and if needed, use other resources too:

<https://www.aircrack-ng.org/doku.php?id=cracking_wpa>

<https://linuxhint.com/monitor_mode_kali_linux_2020/>

Take care! You might need to run the commands as root.

1. Use the following command to check the available interfaces:

airmon-ng

2. It is not recommended to have more interfaces in monitor mode, so destroy all the interfaces, if any:

airmon-ng stop mon0

airmon-ng stop mon1

airmon-ng stop mon2

...

3. Change your wireless interface to monitor mode, using the following command:

airmon-ng start <interface>

(Check the exact steps in the tutorial: <https://www.aircrack-ng.org/doku.php?id=cracking_wpa#step_1_-_start_the_wireless_interface_in_monitor_mode> )

4. Check that your wireless interface is in monitor mode using the following commands:

ifconfig

iwconfig

***Identify the target network***

Tutorial: <https://www.aircrack-ng.org/doku.php?id=cracking_wpa>

Use Airodump-ng to identify the networks and then sniff the target traffic.

IMPORTANT! Take care! You need to correctly identify the network setup by yourself before (the hotspot). Do NOT consider other networks and do NOT mount attacks against other networks. This might have legal consequences you are fully responsible for!

1. The general format for airpdump-ng commands is:

airodump-ng <options> <interface>

2. Use the tool to find all the parameters of your network:

airodump-ng <interface>

3. Use the ESSID to identify the target BSSID, channel (CH) and other parameters. Copy them, you will use these in the next step.

4. Stop the network discovery once you see your network in the list:

CTRL+C

***Collect authentication handshakes***

Tutorial: <https://www.aircrack-ng.org/doku.php?id=cracking_wpa>

1. Use airodump-ng to capture the 4-way authentication handshakes for your target network (remember to put the channel, BSSID and interface of interest; also, name the capture file and establish the path for where to store the capture):

airodump-ng -c <CH> --bssid <BSSID> -w <path/capture\_destination\_file> <interface>

2. Use another device (another phone, tablet, etc.) to connect to the target network.

3. Notice the “WPA handshake: 00:14:6C:7E:40:80” in the top right-hand corner.

4. Manually disconnect and connect the device to the network several times, to generate 4whs.

Optional, use aireplay-ng to disconnect the client. For this, check the tutorial: <https://www.aircrack-ng.org/doku.php?id=cracking_wpa#step_3_-_use_aireplay-ng_to_deauthenticate_the_wireleaiss_client>

***Crack the password***

Tutorial: <https://www.aircrack-ng.org/doku.php?id=cracking_wpa>

1. Use aircrack-ng to crack the password:

aircrack-ng -w <path/password\_file> -b <BSSID> <path/capture\_destination\_file>

2. If your password is not in the password file, take care to add it, otherwise the attack will not succeed.

Alternatively, you can use a richer password file, or use a tool to generate it.

3. Remember to close the monitor mode:

airmon-ng stop <interface>

4. Remember to take a screen shot!

***Capture inspection***

You can inspect the capture file in Wireshark to see again, the 4-way handshake. Remember the lab WPA, 802.1X, Wireshark.