Cracking WEP

Cassandra McCandless

Aircrack-ng is a set of tools that assess Wifi network security. It is an 802.11 WEP and WPA PSK keys cracking program that can recover keys once data packets have been captured. It will implement the FMS attack with some optimization like KoreK attacks and PTW attacks. This makes attacks faster than other WEP attacking tools. It is a complete suite, and it focuses on different areas of wireless security. These areas include; monitoring, attacking, testing, and cracking. For monitoring there is a packet capture and then data is exported to text files so that further processing can be done by third party tools. For attacking, attacks are replayed, there is deauthentication, fake access points, and other attacks done by packet injection. For testing there is checking WiFi cards and driver capabilities. Finally, for cracking WEP and WPA PSK are used. The good thing about aircrack-ng is that all tools are commandline. This makes heavy scripting possible, and GUIs can take advantage of this feature. It works primarily with Linux, but there are other operating systems that use it, too, including; Windows, OS X, and more. Airodump-np is a scan visualizer that allows you to filter, sort, and visualize Airodump-ng scan data. This tool uses the CSV file that is generated Airodump-ng with the -w option. This can work locally or on a hosted device.

To crack WEP keys, you need to gain access to IVs. Normal network traffic does not give access to IVs very quickly. One way to spread this process up is to use an injection. Injection involves having the access point resend selected packets over and over again very quickly. This enables you to get a lot IVs way faster than just waiting for the network traffic to come through and saving them. To do this method, you start the wireless interface in monitor mode on a specific AP channel. Then, you test the injection capability of the wireless device to the AP. This is where aireplay-ng comes in and a fake authentication is used with the access point. Then, you start the airodump-ng on the AP channel with a bssid filter. This will collect the new unique IVs. Then, start aireplay-ng in ARP request replay mode to inject the packets. Finally, you can run aircrack-ng to crack the keys using the IVs that you have collected.

You can also use something called BackTrack to utilize these tools. In order to do this, you want to start BackTrack and make sure that your wireless adapter is recognized and operational. To do this you would type iwconfig. Once you have done that you will see something like wlan0, wlan1, or wlan2. Then, you will put the wireless adapter in monitor mode. You do this by typing airmon-ng start wlan0. The interface's name will probably be changed to something like mon0. This is where you start capturing traffic. By typing in airodump-ng mon0 you will be able to see all the APs and clients that are within range. You then will start a specific capture of an AP. Some of the APs will have WEP encryption. You can type in irodump-ng --bssid 00:09:5B:6F:64:1E -c 11 -w WEPcrack mon0. This will start capturing packets from the SSID. These will be written to a file WEPcrack in the pcap format. This does not allow us to capture packets very quickly in order to crack the WEP key. Speeding this up is possible, though. To do this we will need to inject ARP traffic by spoofing the MAC. To do this we will use the aireplay-ng command. The BSSID of the AP and the MAC address of the client who are connected will be needed. This is where ARPs are injected into APs to capture the IVs that are generated into the WEPcrack airodump file. Once there are several thousand IVs, running that file against aircrack-ng by using something like aircrack-ng WEPcrack-01.cap will display the keys on the screen in hexadecimal format. By taking the hex key and applying it when logging into the remote AP, you can access free WiFi.

Works Cited

“Aircrack-Ng.” *Penetration Testing Tools*, tools.kali.org/wireless-attacks/aircrack-ng.

“Aircrack-Ng.” *simple_wep_crack [Aircrack-Ng]*, www.aircrack-ng.org/doku.php?id=simple_wep_crack.

Blaise, et al. “How to Hack Wi-Fi: Cracking WEP Passwords with Aircrack-Ng.” *WonderHowTo*, WonderHowTo, 3 Apr. 2018, null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/.

“Documentation.” *Aircrack*, www.aircrack-ng.org/.