

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] WiFi Cracking Tutorial - Part 1](#)

html - April 15, 2020, 9:40 am

Hi everyone.

Welcome to another Hacking Tutorial by HTML

My first tutorial explained on how to protect yourself from DoS/DDoS attacks. But of course, to actually attack a computer, you must have some form of connection to it. One of the obvious mediums of connectivity is a wireless network. By cracking into a network, you can then sniff the network, steal bandwidth, use their IP address to browse anonymously, and perform exploits against computers on that network with ease.

This tutorial will cover cracking the most basic common form of wireless encryption: WEP. WEP stands for Wired Equivalent Privacy, and this form of encryption is relatively weak, so can be cracked with some speed. It has been replaced by modern networks by WPA and WPA2 encryption, which I will cover in subsequent tutorials, but WEP is still surprisingly common, so it is a worthy subject for the beginning tutorial in my series.

Cracking a WEP encryption basically works on the principle of capturing packets of data sent on the network, and using them to decode the encryption key.

We will be using Aircrack-NG to crack the encryption in this tutorial, which is my favorite program for cracking wireless networks.

1) Find your wireless adapters name

This is simple, just open a terminal and use this command to find your wireless adapters identifier:

PHP Code

```
<?php  
airmon-ng
```

For example, the adapter name might be wlan0 or wlan1

2) Open Aircrack-Ng in Kali

This step is self explanatory. Then, Put the Wireless Adapter into Monitor Mode or Promiscuous Mode, by using this command:

PHP Code

```
<?php  
airmon-ng start wlan0
```

Of course, use the name of your wireless adapter in place of wlan0. airmon-ng will now name the monitor-mode wireless adapter mon0.

3) Start Capturing Traffic

We now need to start capturing "traffic" - wireless data being sent. We do this by using the airodump-ng command with the monitoring interface, mon0, to capture and show us data about networks the interface can detect:

PHP Code

```
<?php
```

airodump-ng mon0

You should see a list of Access Points appear after a small wait. Make sure the network you are targeting is using WEP encryption for this tutorial.

4) Capture traffic to/from the target AP

Use the following command to begin capturing data from the network you are targeting:

PHP Code

<?php

```
airodump-ng --bssid 00:11:22:33:44:55 -c 11 -w example mon0
```

Replace 00:11:22:33:44:55 with the bssid of the network you are targeting, and the 11 with the channel of the target network. "example" is the name of the file you want to store the captured packets in. They are stored in pcap format. The channel and bssid are obtained from the list of networks you got in step 3.

5) Capture enough packets to crack the encryption!

We could just wait until we capture enough data, but there is a faster way: we will need to inject packets into the AP. We can do this by imitating or "spoofing" a legitimate user connected to the network, using their MAC address. Just wait until someone connects.

6) Inject ARP Traffic

Next, we can use the aireplay-ng command to spoof their MAC address and inject packets. We just need the bssid of the AP and the MAC address of the client who connected to the AP. All we need to do is capture an "ARP" (Address Resolution Protocol) packet and then replay that ARP thousands of times in order to generate the "initialization vectors" that we need to crack WEP! Run this command in a new terminal window:

PHP Code

<?php

```
aireplay-ng -3 -b 00:11:22:33:44:55 -h 99:88:77:66:55:44 mon0
```

Where 00:11:22:33:44:55 is the bssid again, and 99:88:77:66:55:44 is the clients MAC address. After this command is run, the airodump-ng running in the other terminal will capture enough packets to crack the WEP.

7) Crack the Password

When we have captured several thousand packets, we can crack the password in the "example" file, by using the aircrack-ng command like this:

PHP Code

<?php

```
aircrack-ng example-01.cap
```

If we have enough IVs, aircrack-ng the key will be cracked and displayed on the screen, usually in hexadecimal format. You can now log in to the wireless using that key, and you are connected! Now you are at liberty to perform your every bidding on the network ?

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further wireless cracking tutorials and other common hacking topics!

I hope this helped some of you.

Regards

aneWra - April 15, 2020, 9:53 am

Thank you for posting this, man :)

I'm pretty new to this world but the tutorial it's very clean and easy to understand.
Off course should I use a VPN or Proxy while doing this?
Anyway,I'm waiting for the one about WPA/WPA2 and others.
Thank you again

SIM-5382664 - *July 2, 2023, 9:44 am*

thanks sir appreciate it

Roli0810 - *July 5, 2023, 12:49 pm*

Ty for sharing this with us