Aircrack-ng

flowchart

Simple Wep Cracking with a flowchart

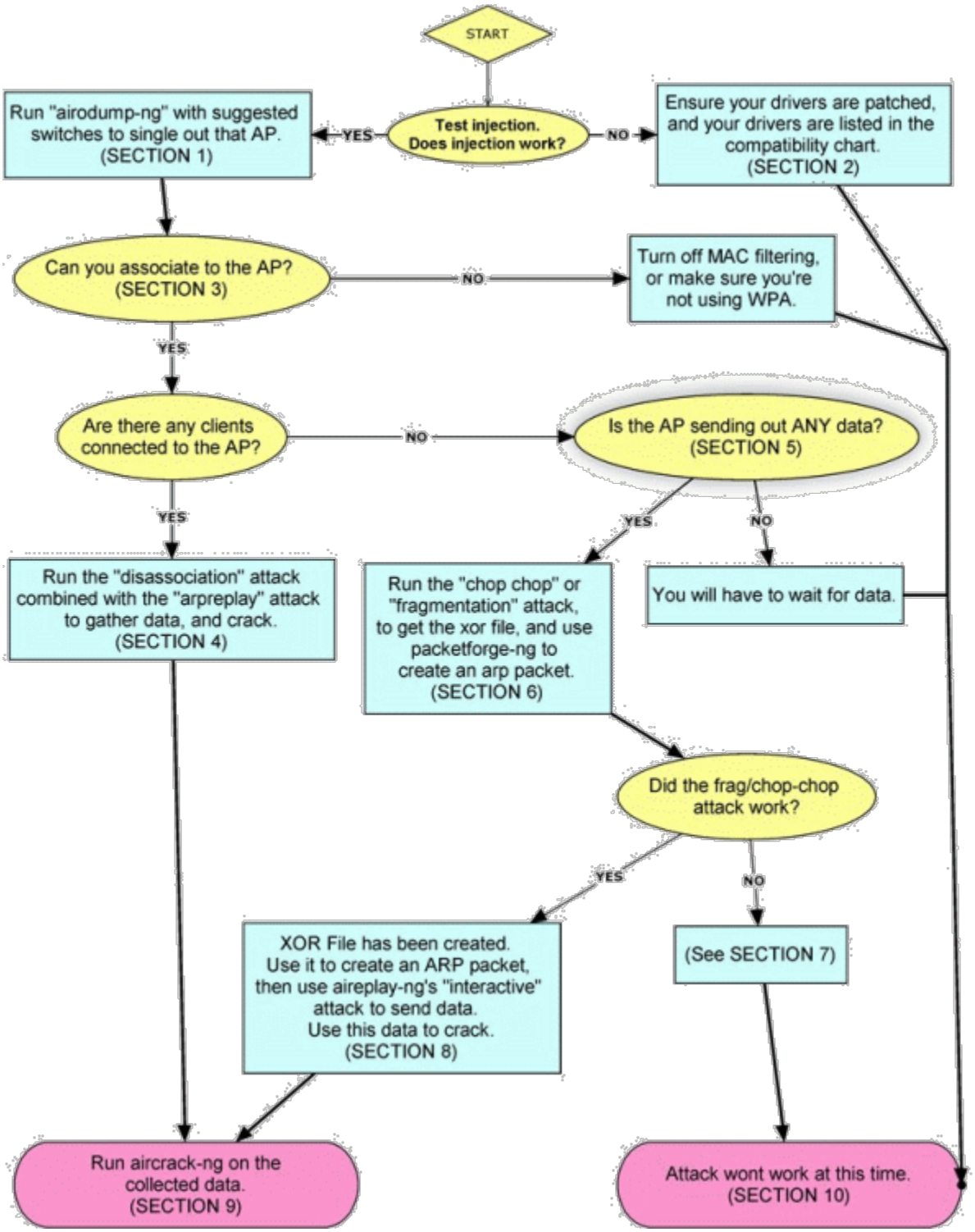
Last update: May 9, 2008
Author: matts

Foreword

Aircrack is very simple to use once you know the concept. This flowchart will hopefully teach you the concept behind simple wifi cracking. You will want to keep airodump-ng running to collect data, and then run your attacks. Each attack will use aireplay-ng, and the ultimate goal is to generate data on the network... most commonly ARP data. In this tutorial I assume you have read the wiki and are familiar with the different tools and attacks. This is not a hand-holding tutorial, this is a theory tutorial. It tells you WHEN to use an attack, not the command lines and switches. Remember, this is for simple wep cracking, where the goal is to recover the wep-key for your network. It tells you when to use the tools, not how. See the tool's wiki entry for details on the tool, links are under the flowchart.

Basically: Read the flowchart, read the wiki entries for the different tools I've listed, and follow the flowchart to go step-by-step until you reach an end.

Flow Chart



Links to the different tools needed for simple cracking

- aircrack-ng

- aireplay-ng
- airodump-ng
- packetforge-ng

The following sections correspond to the flow chart's blocks.

Read the flowchart to understand where the section is in the flowchart so you get a better understanding on the flow. The section numbers do not correlate to the procedure for cracking.

Section 1: Singling out the AP you are cracking.

Running airodump-ng with no parameters will show you every AP in your area. You will want to use a few parameters to single out the AP you are trying to crack, so you only collect the information you need.

```
airodump-ng -c 6 --bssid 11:22:33:44:55:66 -w output
```

-c 6	Sets channel to 6, change the number to whatever channel your AP is on. Very important, so you are not chan hopping.
--bssid 11:22:33:44:55:66	Sets the BSSID to single out. This is set to your AP's MAC Address (seen in airodump-ng)
-w output	Sets the output file, this will start outputting data to output-##.cap

Section 2: Ensure your drivers are patched and compatible

See the following URL's for compatibility information:

Cards	compatible_cards
Drivers	compatibility_drivers
Patching	install_drivers

Section 3: Associating to the AP

If you can not associate to your AP, you need to turn off WPA/WPA2 encryption, or make sure you have turned off MAC filtering. If you have MAC filtering on, make sure your MAC address is not spoofed and is in the list of allowed clients.

Section 4: Clients are connected, run deauth and arpinteractive attacks

Since clients are connected, you will first want to run the arp interactive (-3) attack, and leave it running so it can listen for the ARP packet which will be generated when you deauth the client who is connected. By deauthing, you will generate an arp which can be re-injected, thus generating data on the network.

Section 5: Is the AP sending out ANY data?

In order to crack anything, the AP has to send out at least 1 packet. This packet will be used on the chopchop (-4) or fragmentation (-5) attack, or hopefully the arpinteractive (-3) attack. If the AP is not sending out any data, it likely means no one is connected to the AP via wired or wireless. You will just have to wait, keep airodump-ng running with the -w switch (to output data) overnight, and you may get lucky.

Section 6: Generate an XOR file (chopcop or fragmentation attack)

The point of cracking is to generate data. You can generate data in Section 4, but sometimes there are no clients connected to wifi, but the AP is still sending out data. In this case, you will want to capture the data that the AP is sending out, and use it to determine a valid XOR keystream (basically a file which allows you to create a packet with out knowing the key). The two attacks for this are “fragmentation” and “chop-chop”. Fragmentation is quickest, but you have to have a good connection to the AP (be close to the AP), and it doesn't work with all cards. Chop-chop usually works with all cards, but it doesn't always work on every AP.

Section 7: Frag / Chop-chop failed

For fragmentation: try a few more packets sent out by the AP. Try spoofing your mac address to the source address in the packet. If this still doesn't work, the AP may not be vulnerable to the fragmentation attack.

For the Chop-Chop attack, you really need to have a good connection to the AP, you have to be close. You should choose a packet that is very small, you only need about a 70 byte packet… this reduces the number of packets required to generate the xor keystream (choosing a larger file takes longer and therefore is more likely to fail).

- You have to be associated to the AP.

- Some AP's will start to ignore you if you flood it too fast, so use the -x switch to throttle the speed of your packet sending.
- Most AP's are ok with 30-50 packets per second (-x 30 or -x 50), if they are the type that ignore you for sending packets too fast.
- The AP may ignore you if your MAC address is not the same as the packet's MAC address, so you can spoof your mac address to suit the packet.
- Some APs don't discard corrupted packets correctly. Such APs are not vulnerable to chopchop.

Section 8: Success! XOR Keystream file generated.

We have an XOR keystream meaning we can make any packet we want, as long as we have enough bytes in the keystream. For an ARP packet (packetforge -0), 70 is enough bytes which is the shortest packet you'll generally see from the AP. Generate an ARP packet using packetforge, you may use arp amplification if you like. For the -l and -k switches I generally use 255.255.255.255 and it works just fine.

Section 9: Running aircrack-ng on the collected data

If you have done things right, you should start to see the #/s and “Data” fields in airodump-ng climb to high numbers. While this is going on, you will want to run aircrack-ng on the .cap files you are creating with airodump-ng. You may also use wildcards if you have run multiple airodump sessions. For example:

```
aircrack-ng output-*.cap
```

This will open up any file starting with “output-” and ending with ”.cap”.

Section 10: Attack wont work at this time

There are many reason that you wont be able to.

- Your drivers aren't patched: See Installing Drivers and the patch directory [http://patches.aircrack-ng.org/].
- Turn off MAC filtering and WPA/WPA2.
- The AP isn't sending out any data, you will have to wait, or manually generate some data on your network.
- Frag/ChopChop aren't working… chopchop may or may not work, and fragmentation is very sensitive to distance from AP.

EOF

I hope you have found this tutorial helpful.

flowchart.txt · Last modified: 2012/04/02 14:33 by wims