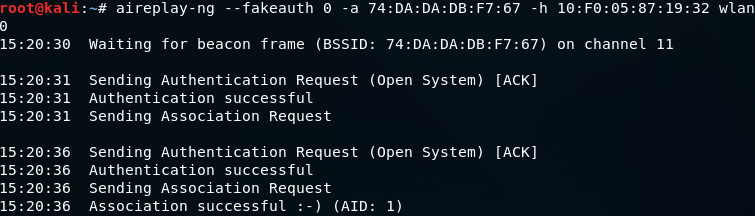
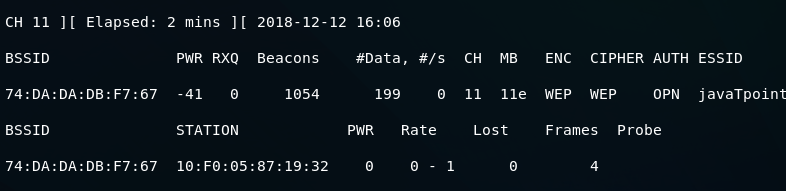
Fake authentication attack [3]

In this attack we inject packets into the traffic and force the AP to create a new packet with the new IVs in them, and then capture these IVs. But we have to authenticate our device with the target AP before we can inject packets. APs have lists of all of the devices that are connected to them. They can ignore any packets that come from a device that is not connected. If a device that doesn't have the key tries to send a packet to the router, the router will just ignore the packet, and it wouldn't even try to see what's inside it. Before we can inject packets into a router, we have to authenticate ourselves with the router. To do this, we're going to use a method called fake authentication. -a, to include the target network and -h, to include our MAC address. [3]

  
In the above image, we can see that -a sent an authentication request, and it was successful. The network becomes an open network, and our client showed up as if it was a client connected to the network. We're not actually connected, but we are authenticated with the network and have an association with it so that we can inject packets into the AP and It will now receive any request that we send to it. Following is the output:



ARP request replay attack[3]

The AP now accepts packets that we send to it because we've successfully associated ourselves with it by using a fake authentication attack. We are now ready to inject packets into the AP and make the data increase very quickly, in order to decrypt the WEP key.[3]

ARP request replay is the first method of packet injection. In this method, we're going to wait for an AP packet, capture the packet, and inject it into the traffic , then the AP will be forced to create a new packet with a new IVs. We will capture the new packets, inject it back into the traffic again, and force the AP to create another packet with another IV. We will be repeating this process until the amount of data is high enough to crack the WEP key. Using the following command we can launch airodump-ng:

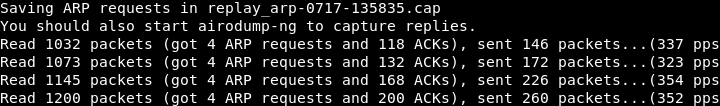
ARP request replay attack

We're going to add a --write command to store all of the packets that we capture into a file which is arp-request-reply-test. When it runs, we will see that the target network has 0 data, it has no clients associated with it, and there is no traffic going through, which means that it's not useful, we can't crack its key. To solve this problem, we are going to perform a fake authentication attack as shown in the Fake authentication section, so that we can start injecting packets into the network, and it will accept them.

That leads us to our next step, which is the ARP request reply step. In this step, we will inject packets into the target network, forcing it to create new packets with new IVs. Following command is used to do this:

ARP request replay attack

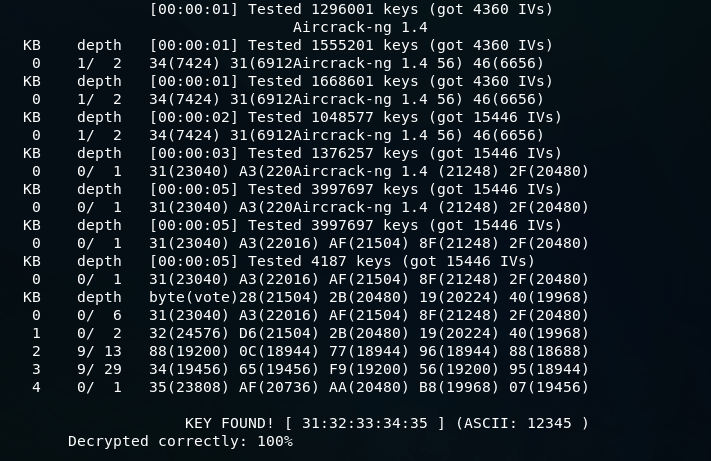
This command is very similar to the previous command, but in this command, we're going to use --arpreplay instead of ?fakeauth. We will also include -b, for BSSID. With this command, we are going to wait for an ARP packet, capture it, and then reinject it out into the air. We can then see that we have captured an ARP packet, inject it, captured another, inject it into the traffic, and so on. The AP then creates new packets with new IVs, we receive them, we inject them again, and this happens over and over. After executing the above command, the following output will be shown:



At this time, the wireless adapter wlan0 is waiting for an ARP packet. Once there is an ARP packet transmitted in the network, it's going to capture that packets and then retransmitted it. Once it has done, the access point will be forced to generate a new packet with a new IV, and we will keep doing this since the access point will continuously generate the new packet with new IV. When the amount of Data reaches 9000 or above, we can launch aircrack-ng to crack it. Use the following command to do this:

ARP request replay attack

After running the above command, the following output will be shown. We can see the WEP Key, and we are able to crack it.



**References**

[3] <https://www.kb.cert.org/vuls/id/228519>