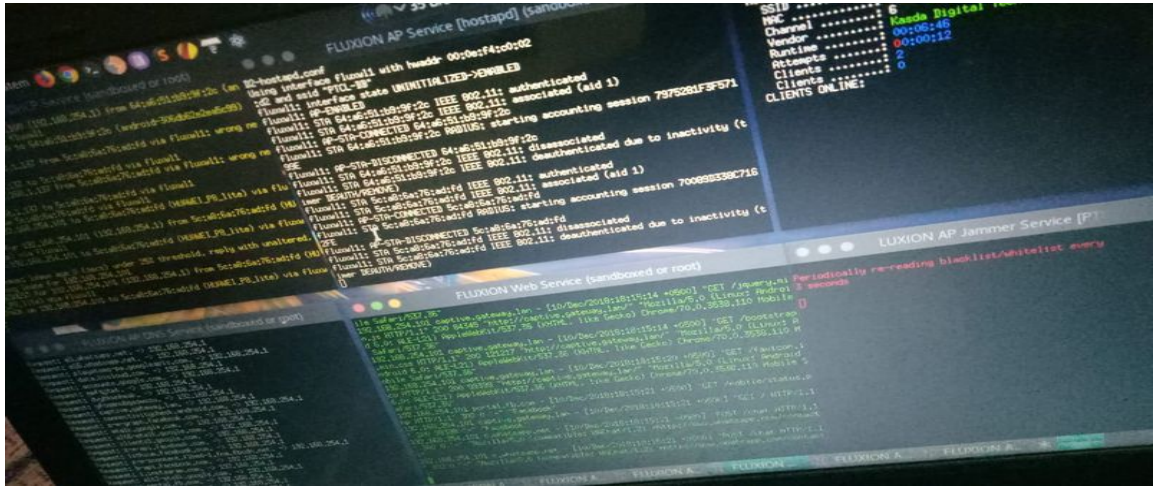
WiFi Phishing: Acquire WPA/WPA2 Key Using (Rogue AP) Fluxion

by **hash3liZer** . 10 December 2018



Fluxion was first introduced as the remake of linset. It's a social engineering auditing tool to acquire WPA/WPA2 passphrase by means of Wireless Phishing i.e hosting a Fake Access Point along with a forged document. Well, in some earlier tutorials we manually did this same task by configuring files and tools like hostapd and dnsmasq. However, with this in hand, the attack can't be much of a sophisticated task.

Fluxion has almost pre-configured interface to interact and all you have to do is select. Fluxion starts by scanning the area in range of adapter, make sure you have an external one. Then it tries to capture the **handshake** of your target AP

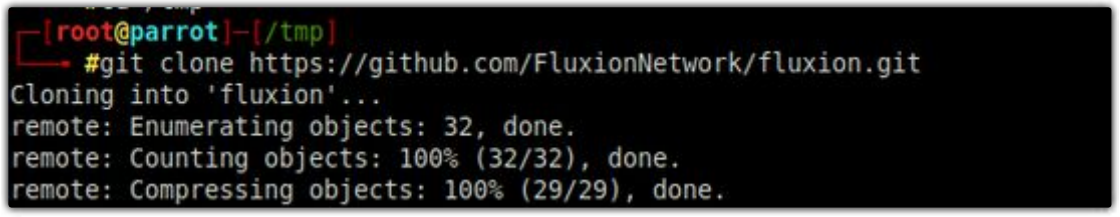
(Access Point). After this, rogue ap and captive portal comes into the scene and fluxion will host a forged document for you where the user will enter wireless passphrase to be matched by the **MIC code**.

MIC code as we know is derived from the calculation of various hashes from the handshake. Upon successful verification of passphrase key, the key will be logged and fluxion will shutdown. So, there's not much of our time taken nor do we have to manually place files for **dnsmasq, hostapd and airplay-ng** etc.

STEP 1 Installation

Clone the fluxion repository from github:

```
$ git clone https://github.com/FluxionNetwork/fluxion.git
```



Move into the fluxion directory and execute the bash installation file:

```
$ cd fluxion/
$ chmod a+x ./fluxion.sh
$ ./fluxion.sh -i
```

STEP 2 Wireless Adapters

Now, to perform a successful Rogue AP attack, atleast **two** wireless cards are required both supporting ***promiscious*** mode and packet injection. A variety of Wireless adapters is availble but not all support what we want. For instance, **deauthentication** can be performed with **WN727N** (TP-Link) but hostapd doesn't support it.

I'll be using Alpha **AWUS036NH** for hosting an Access Point and TP-Link WN722N for deauthentication purpose.

STEP 3 Monitor Mode

Put your both wireless cards in monitor mode. Remember, altough scripts like wifiphisher and fluxion place the card in monitor mode by using some deprecated techniques but it's better to do it manually.

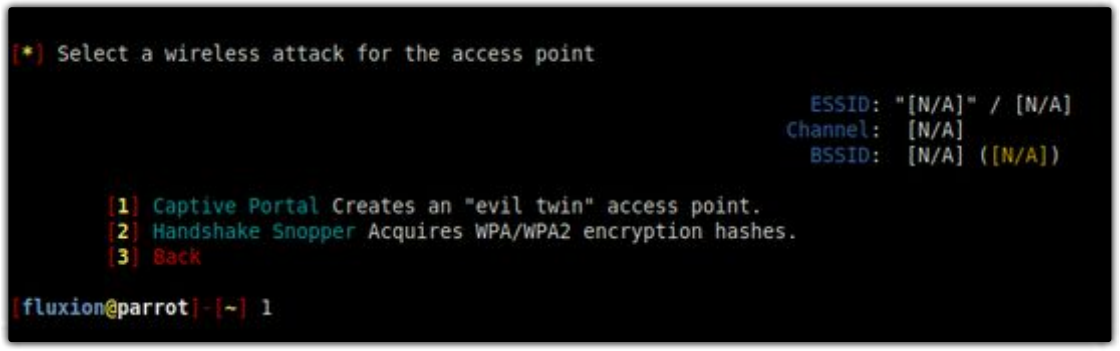
```
$ airmon-ng start wlan1 // WN722N v1
$ airmon-ng start wlan2 //ALFA 036NH
```

STEP 4 Scanning The Area!

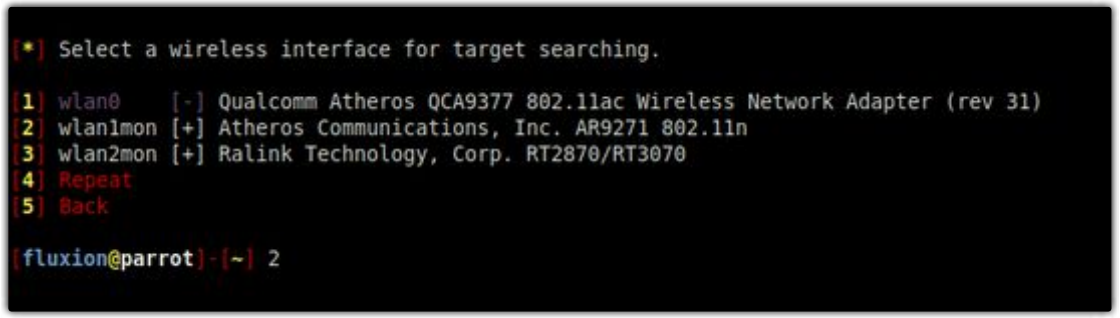
Fire up the script:

```
$ ./fluxion.sh
```

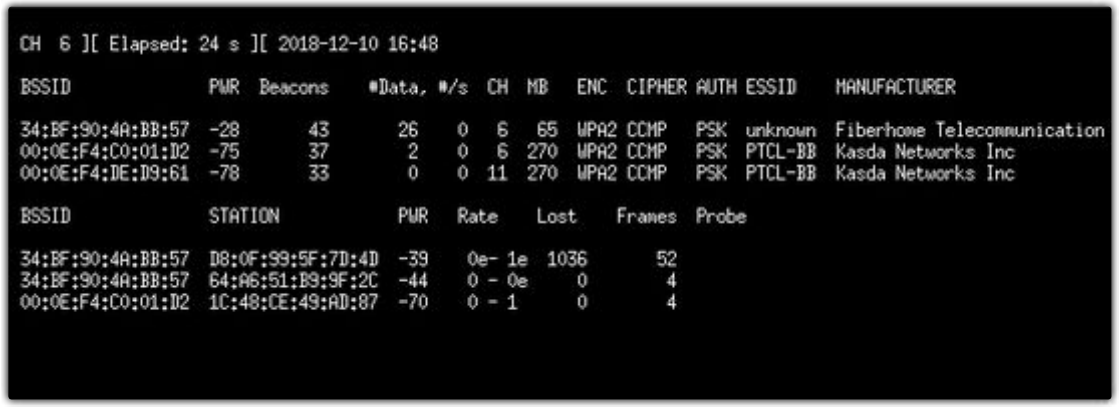
You will asked whether you want to capture a handshake first or perform Rogue AP attack. If you already captured a handshake, you can skip the second part. As the scope of this tutorial is limited to **captive portal** AP, i suppose you already know how to capture a **WPA/WPA2** handshake. So, select *captive portal* from the list:



Here in the below screenshot, i got three wireless adapters. Note that the **wlan0** interface is indicating internal wireless adapter and doesn't support packet injection. Now, choose one of the monitor interfaces to scan the area and then choose the channels to look for:

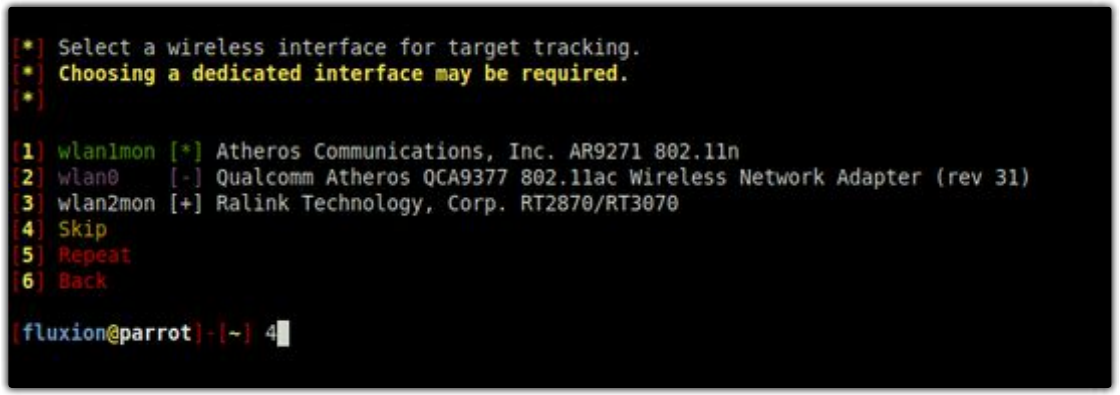


When you have your target on screen, close the scanning window and you will be prompted to choose a target. Select your target and press Enter.

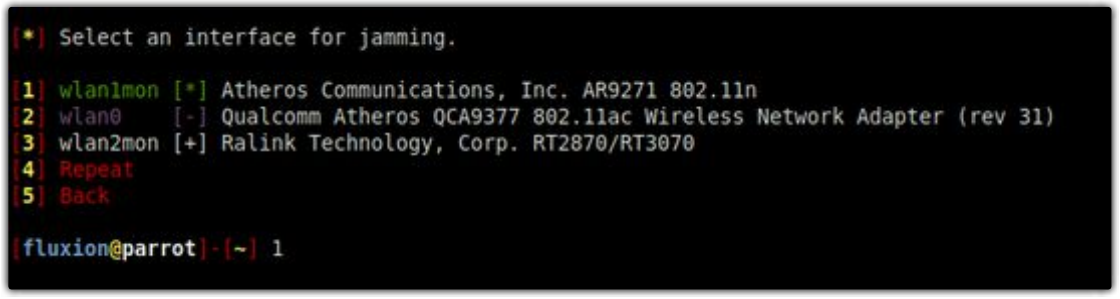


STEP 5 Choosing Interfaces

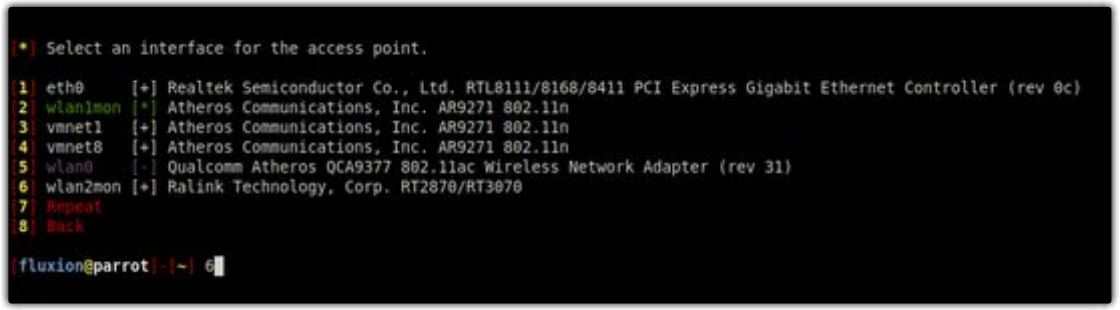
Now, we have to allocate some tasks to the wireless adapters. First, you will be asked for an interface to keep track of your target **Access Point**. It might mess up things a bit, so it's better to skip this interface. However, in case you have one more wireless adapter it's even more good. Choose skip from the list:



Next, we need an interface to send deauthentication frames. The interface you choose here must support packet injection and I got **TP-Link WN722N v1** for this:



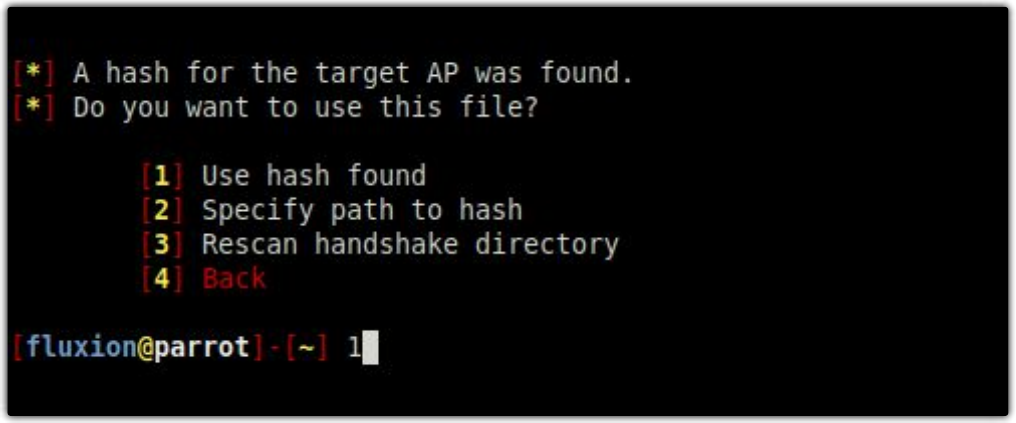
The next interface you will be asked for is to launch the Rogue Access Point. Make sure the adapter you use is powerful enough to throw signals on long range. I am using **Alpha AWUS036NG** with hostapd for this.



STEP 6 Select AP Service And Handshake.

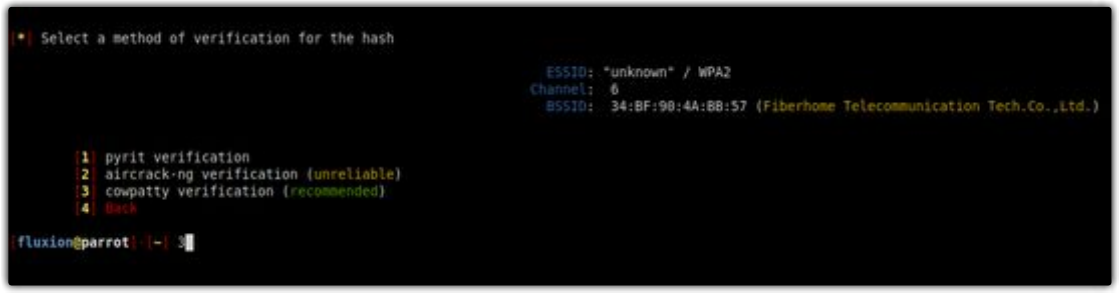
Depending on your wireless adapter **chipset**, you can select b/w hostapd and airbase-ng. Airbase-ng is slower than hostapd but supports a wider range of chipsets. Since, hostapd supports my adapter, I'll go with hostapd:

Next, you will be asked for the handshake. I've captured a handshake of target AP with fluxion earlier. So, i go with the option: found hash:



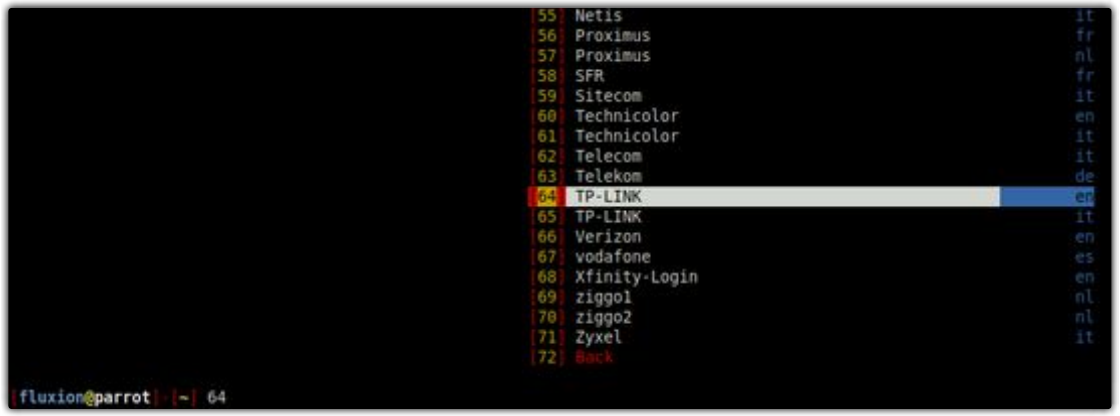
STEP 7 Cracking

Cracking the right password is an important factor in all of this attack. We need to find the right key, *right*? For this, when anything will be entered to the fake page it will be manipulated and matched against the right hash derived from handshake. Upon successful cracking, the key will be printed on screen and fluxion will be stopped. So, choose one of the cracking softwares accordingly:



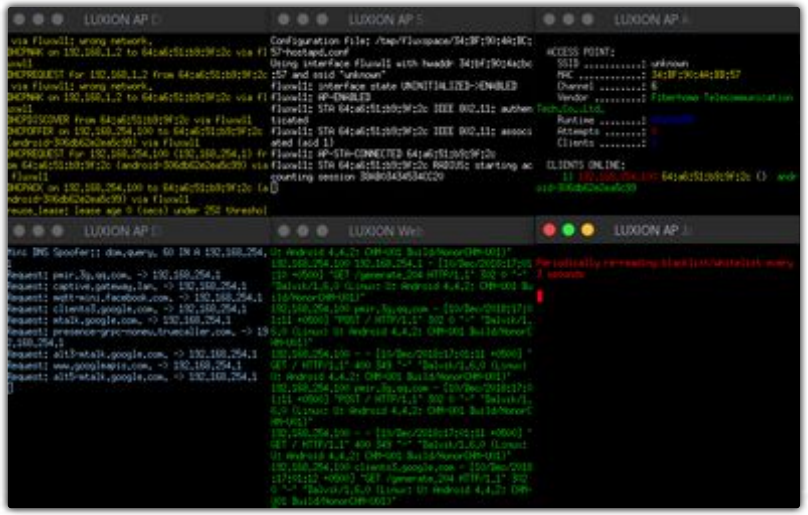
STEP 8 Forged Document

Next, choose disconnected from the internet conenctivity list. Cause we don't want to provide the users with internet facility. And lastly, choose the forged document from the available list:

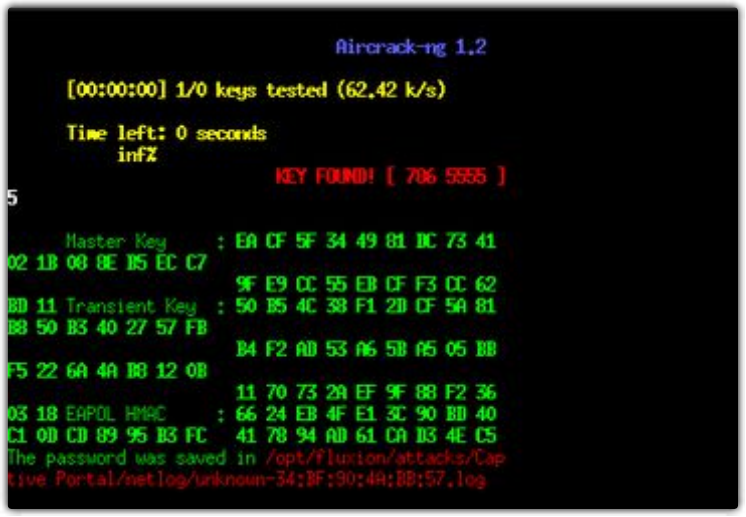


STEP 9 WPA/WPA2 Key

Now, let the fluxion do it's work:



Let's play the victim role. If a user connects to our Rogue Access Point, captive portal will come into scene and the user will be prompted to the forged document and if the user enters the right WPA/WPA2 password in the fields. Rogue AP will shutdown and the key will be printed on screen:



So, we cracked WPA/WPA2 key with Rogue AP.

Conclusion

Fluxion is an extensive rogue AP tool for acquiring WPA/WPA2 passphrase by inducing the users for giving secret credentials through a forged document. Moreover, fluxion also verifies the key before terminating the actual attack. So, only validated keys are accepted and only the attack terminates when the correct hash has been cracked.

0 Comments Shellvoide 1 Login

Recommend Tweet Share Sort by Best

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus to your site Disqus' Privacy Policy DISQUS

';

Social

Shellvoide

Like Page 816 likes

Shellvoide
about 3 weeks ago

#Hashcat #Guide: Cracking WPA/WPA2.

https://www.shellvoide.com/…/hashcat-guide-how-to-brute-fo…/

4 Comment 2

Shellvoide

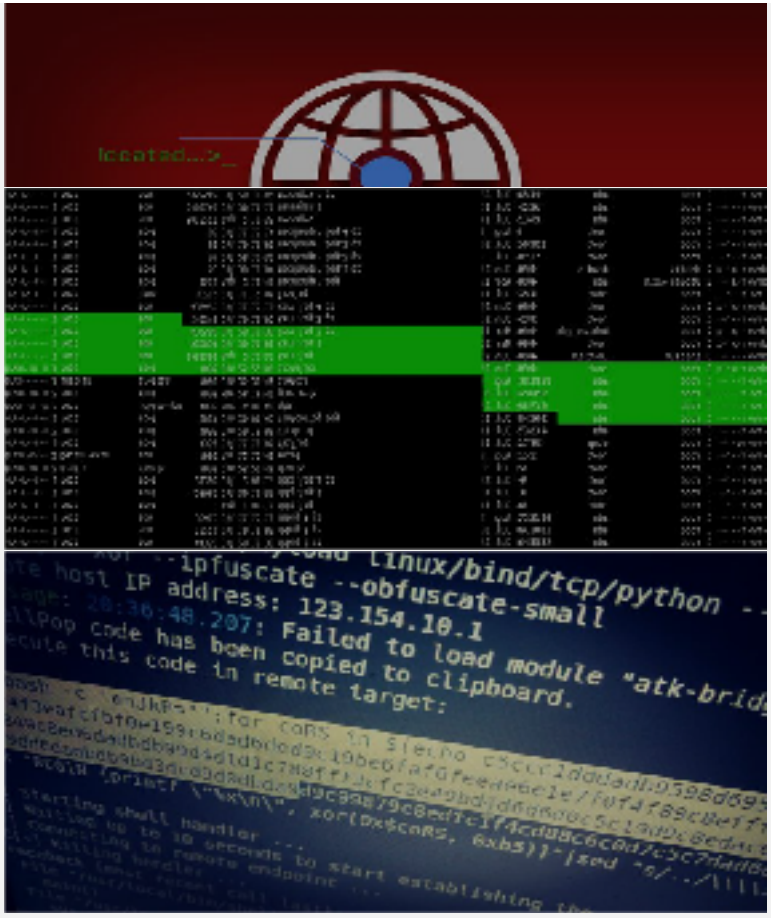
Subscribe

Subscribe to our Newsletter.

email...

Subscribe

Also Read



Subscribe To Newsletter

email...

Subscribe

Contact Me: admin@shellvoide.com