Fluxion

Information Security Inc.

Contents

- About Fluxion
- How it works
- Testing Environment
- Installing Fluxion
- Using Fluxion
- References

About Fluxion

- Fluxion => WPA/WPA2 Security Hacked Without Brute Force
- A remake of linset by vk496 (https://github.com/vk496/linset)

How it works

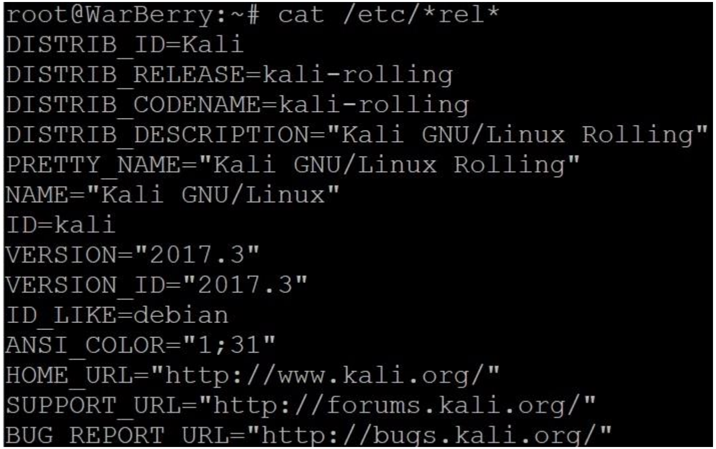
- Scan the networks.
- Capture a handshake (can't be used without a valid handshake, it's necessary to verify the password)
- Use WEB Interface *
- Launch a FakeAP instance to imitate the original access point
- Spawns a MDK3 process, which deauthenticates all users connected to the target network, so they can be lured to connect to the FakeAP and enter the WPA password.

How it works

- A fake DNS server is launched in order to capture all DNS requests and redirect them to the host running the script
- A captive portal is launched in order to serve a page, which prompts the user to enter their WPA password
- Each submitted password is verified by the handshake captured earlier
- The attack will automatically terminate, as soon as a correct password is submitted

Testing Environment

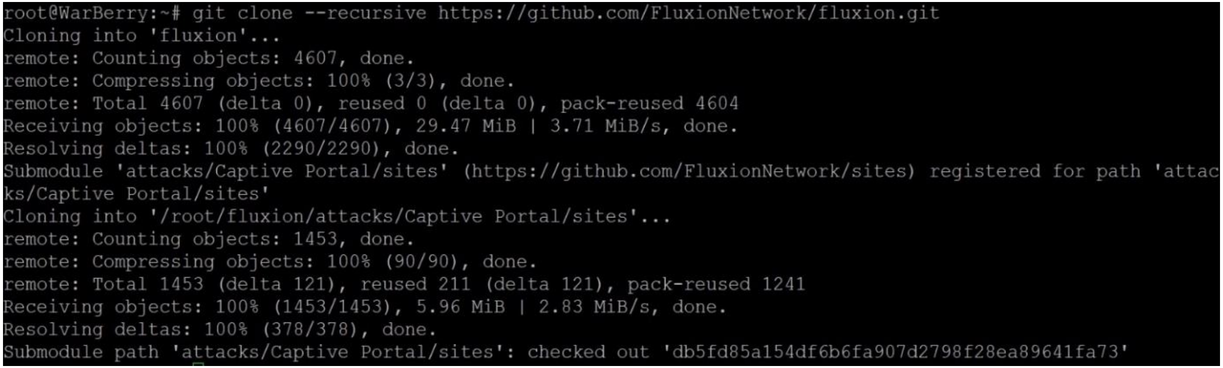
- Kali Linux 2017



```
root@WarBerry:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing Fluxion

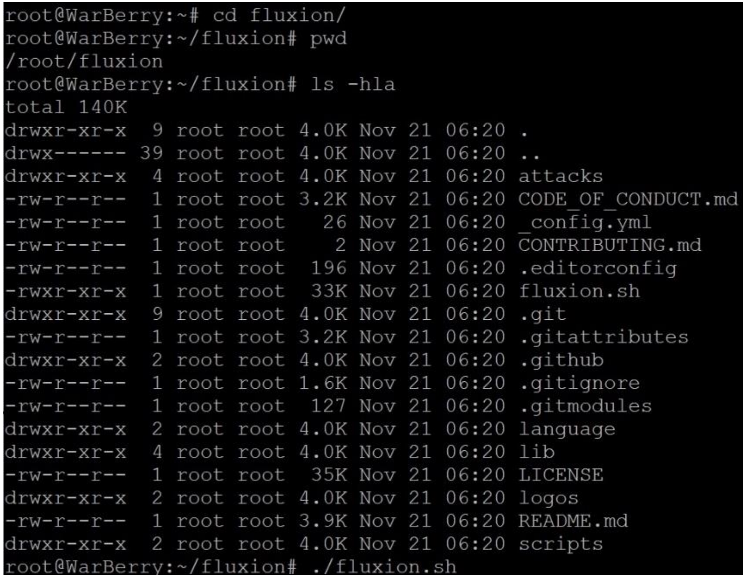
- Cloning GitHub repository



```
root@WarBerry:~# git clone --recursive https://github.com/FluxionNetwork/fluxion.git
Cloning into 'fluxion'...
remote: Counting objects: 4607, done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 4607 (delta 0), reused 0 (delta 0), pack-reused 4604
Receiving objects: 100% (4607/4607), 29.47 MiB | 3.71 MiB/s, done.
Resolving deltas: 100% (2290/2290), done.
Submodule 'attacks/Captive Portal/sites' (https://github.com/FluxionNetwork/sites) registered for path 'attac
ks/Captive Portal/sites'
Cloning into '/root/fluxion/attacks/Captive Portal/sites'...
remote: Counting objects: 1453, done.
remote: Compressing objects: 100% (90/90), done.
remote: Total 1453 (delta 121), reused 211 (delta 121), pack-reused 1241
Receiving objects: 100% (1453/1453), 5.96 MiB | 2.83 MiB/s, done.
Resolving deltas: 100% (378/378), done.
Submodule path 'attacks/Captive Portal/sites': checked out 'db5fd85a154df6b6fa907d2798f28ea89641fa73'
```

Installing Fluxion

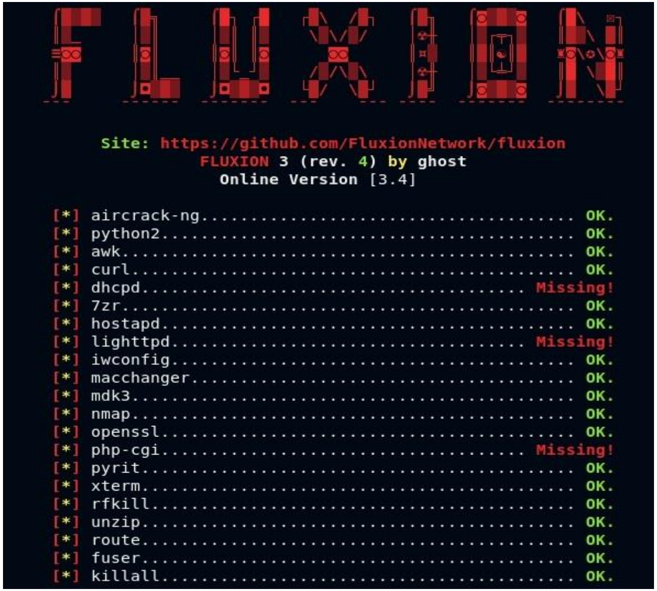
- Installing Fluxion



```
root@WarBerry:~# cd fluxion/
root@WarBerry:~/fluxion# pwd
/root/fluxion
root@WarBerry:~/fluxion# ls -hla
total 140K
drwxr-xr-x  9 root root 4.0K Nov 21 06:20 .
drwx------ 39 root root 4.0K Nov 21 06:20 ..
drwxr-xr-x  4 root root 4.0K Nov 21 06:20 attacks
-rw-r--r--  1 root root 3.2K Nov 21 06:20 CODE_OF_CONDUCT.md
-rw-r--r--  1 root root   26 Nov 21 06:20 _config.yml
-rw-r--r--  1 root root    2 Nov 21 06:20 CONTRIBUTING.md
-rw-r--r--  1 root root  196 Nov 21 06:20 .editorconfig
-rwxr-xr-x  1 root root  33K Nov 21 06:20 fluxion.sh
drwxr-xr-x  9 root root 4.0K Nov 21 06:20 .git
-rw-r--r--  1 root root 3.2K Nov 21 06:20 .gitattributes
drwxr-xr-x  2 root root 4.0K Nov 21 06:20 .github
-rw-r--r--  1 root root 1.6K Nov 21 06:20 .gitignore
-rw-r--r--  1 root root  127 Nov 21 06:20 .gitmodules
drwxr-xr-x  2 root root 4.0K Nov 21 06:20 language
drwxr-xr-x  4 root root 4.0K Nov 21 06:20 lib
-rw-r--r--  1 root root  35K Nov 21 06:20 LICENSE
drwxr-xr-x  2 root root 4.0K Nov 21 06:20 logos
-rw-r--r--  1 root root 3.9K Nov 21 06:20 README.md
drwxr-xr-x  2 root root 4.0K Nov 21 06:20 scripts
root@WarBerry:~/fluxion# ./fluxion.sh
```

Installing Fluxion

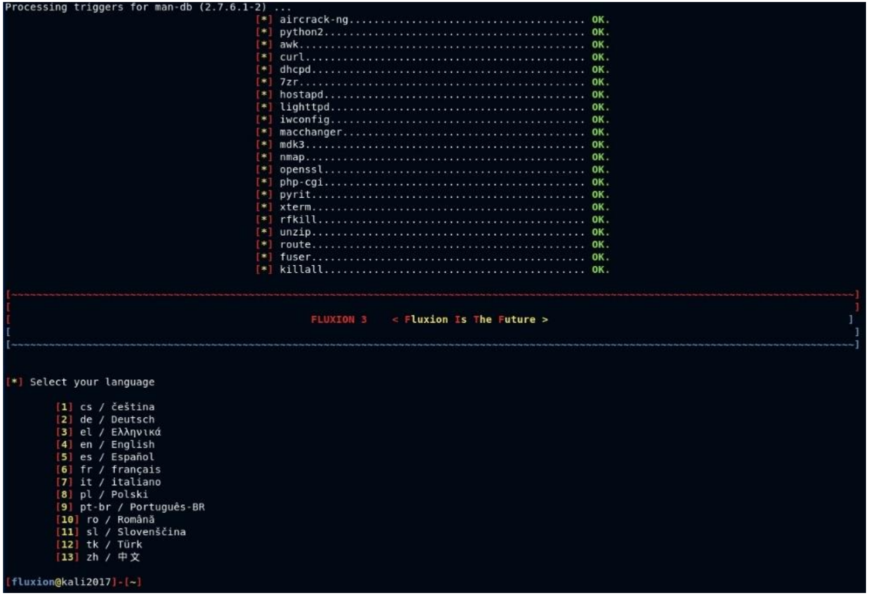
- Installing Fluxion



```
          Site: https://github.com/FluxionNetwork/fluxion
                   FLUXION 3 (rev. 4) by ghost
                     Online Version [3.4]

  [*] aircrack-ng..................................... OK.
  [*] python2......................................... OK.
  [*] awk............................................. OK.
  [*] curl............................................ OK.
  [*] dhcpd...................................... Missing!
  [*] 7zr............................................. OK.
  [*] hostapd......................................... OK.
  [*] lighttpd................................... Missing!
  [*] iwconfig........................................ OK.
  [*] macchanger...................................... OK.
  [*] mdk3............................................ OK.
  [*] nmap............................................ OK.
  [*] openssl......................................... OK.
  [*] php-cgi.................................... Missing!
  [*] pyrit........................................... OK.
  [*] xterm........................................... OK.
  [*] rfkill.......................................... OK.
  [*] unzip........................................... OK.
  [*] route........................................... OK.
  [*] fuser........................................... OK.
  [*] killall......................................... OK.
```

Using Fluxion

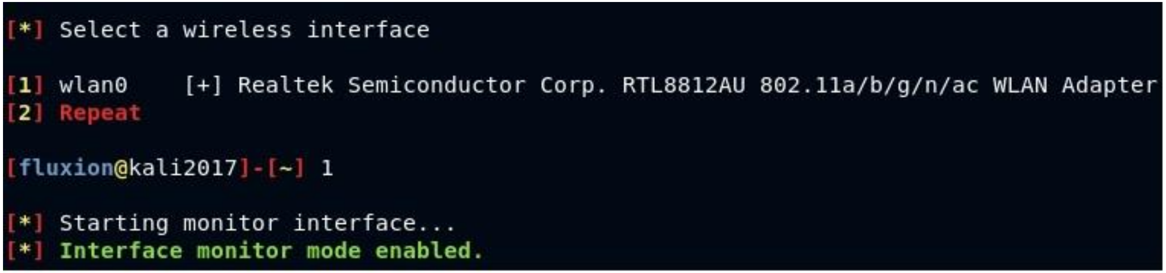
- Fluxion will start automatically after ./fluxion.sh script finishes



```
Processing triggers for man-db (2.7.6.1-2) ...
                                        [*] aircrack-ng...................................... OK.
                                        [*] python2.......................................... OK.
                                        [*] awk.............................................. OK.
                                        [*] curl............................................. OK.
                                        [*] dhcpd............................................ OK.
                                        [*] 7zr.............................................. OK.
                                        [*] hostapd.......................................... OK.
                                        [*] lighttpd......................................... OK.
                                        [*] iwconfig......................................... OK.
                                        [*] macchanger....................................... OK.
                                        [*] mdk3............................................. OK.
                                        [*] nmap............................................. OK.
                                        [*] openssl.......................................... OK.
                                        [*] php-cgi.......................................... OK.
                                        [*] pyrit............................................ OK.
                                        [*] xterm............................................ OK.
                                        [*] rfkill........................................... OK.
                                        [*] unzip............................................ OK.
                                        [*] route............................................ OK.
                                        [*] fuser............................................ OK.
                                        [*] killall.......................................... OK.

[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                                                                                      ]
[                                                FLUXION 3    < Fluxion Is The Future >                                               ]
[                                                                                                                                      ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


[*] Select your language

        [1] cs / čeština
        [2] de / Deutsch
        [3] el / Ελληνικά
        [4] en / English
        [5] es / Español
        [6] fr / français
        [7] it / italiano
        [8] pl / Polski
        [9] pt-br / Português-BR
        [10] ro / Română
        [11] sl / Slovenščina
        [12] tk / Türk
        [13] zh / 中文

[fluxion@kali2017]-[~]
```

Using Fluxion

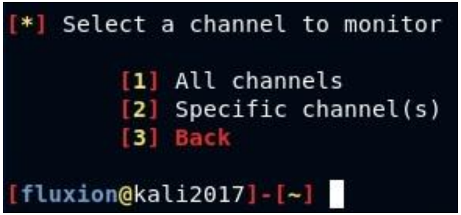
- Select a wireless interface



```
[*] Select a wireless interface

[1] wlan0    [+] Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac WLAN Adapter
[2] Repeat

[fluxion@kali2017]-[~] 1

[*] Starting monitor interface...
[*] Interface monitor mode enabled.
```

Using Fluxion

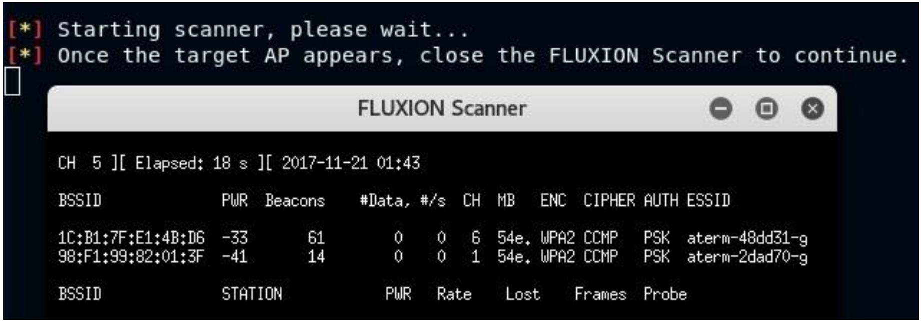
- Select a channel to monitor



```
[*] Select a channel to monitor

        [1] All channels
        [2] Specific channel(s)
        [3] Back

[fluxion@kali2017]-[~] 
```

Using Fluxion

- Starting the scanner

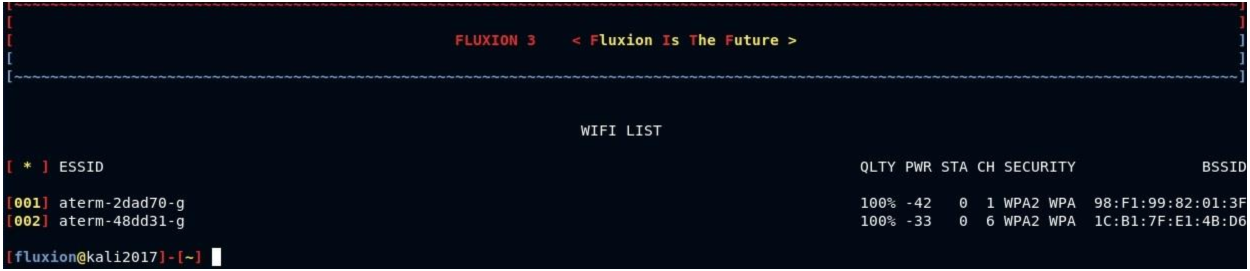


```
[*] Starting scanner, please wait...
[*] Once the target AP appears, close the FLUXION Scanner to continue.
```

```
 CH  5 ][ Elapsed: 18 s ][ 2017-11-21 01:43

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 1C:B1:7F:E1:4B:D6  -33       61        0    0   6  54e. WPA2 CCMP   PSK  aterm-48dd31-g
 98:F1:99:82:01:3F  -41       14        0    0   1  54e. WPA2 CCMP   PSK  aterm-2dad70-g

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Using Fluxion

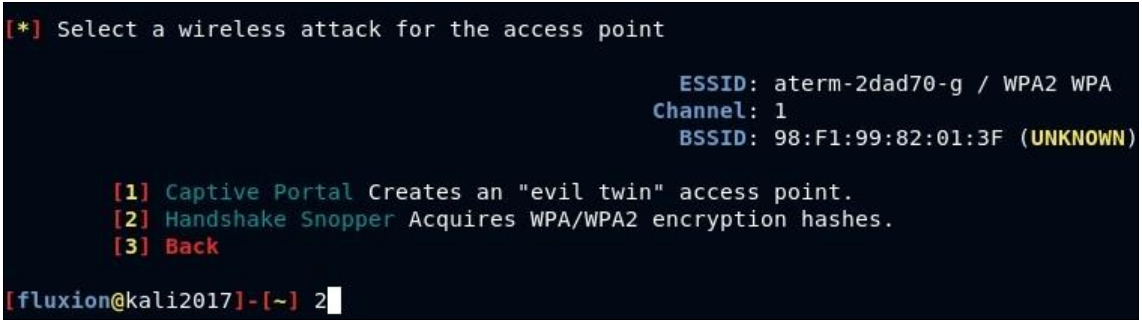
- Showing ESSID list



```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                                                                                  ]
[                                              FLUXION 3    < Fluxion Is The Future >                                              ]
[                                                                                                                                  ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


                                                            WIFI LIST

[ * ] ESSID                                                                                  QLTY PWR STA CH SECURITY             BSSID

[001] aterm-2dad70-g                                                                         100% -42   0  1 WPA2 WPA  98:F1:99:82:01:3F
[002] aterm-48dd31-g                                                                         100% -33   0  6 WPA2 WPA  1C:B1:7F:E1:4B:D6

[fluxion@kali2017]-[~] 
```

Using Fluxion

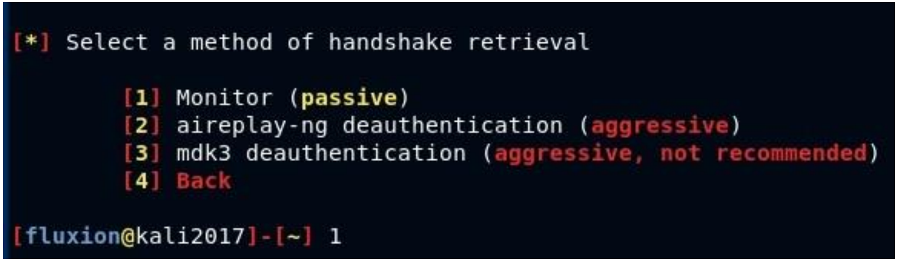
- Selecting a wireless attack for the AP



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

                                                         ESSID: aterm-2dad70-g / WPA2 WPA
                                                       Channel: 1
                                                         BSSID: 98:F1:99:82:01:3F (UNKNOWN)

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

[fluxion@kali2017]-[~] 2
```

Using Fluxion

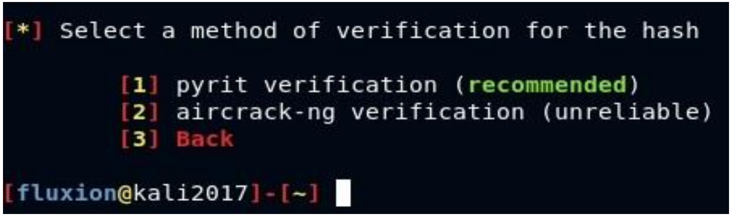
- Selecting handshake method



```
[*] Select a method of handshake retrieval

        [1] Monitor (passive)
        [2] aireplay-ng deauthentication (aggressive)
        [3] mdk3 deauthentication (aggressive, not recommended)
        [4] Back

[fluxion@kali2017]-[~] 1
```

Using Fluxion

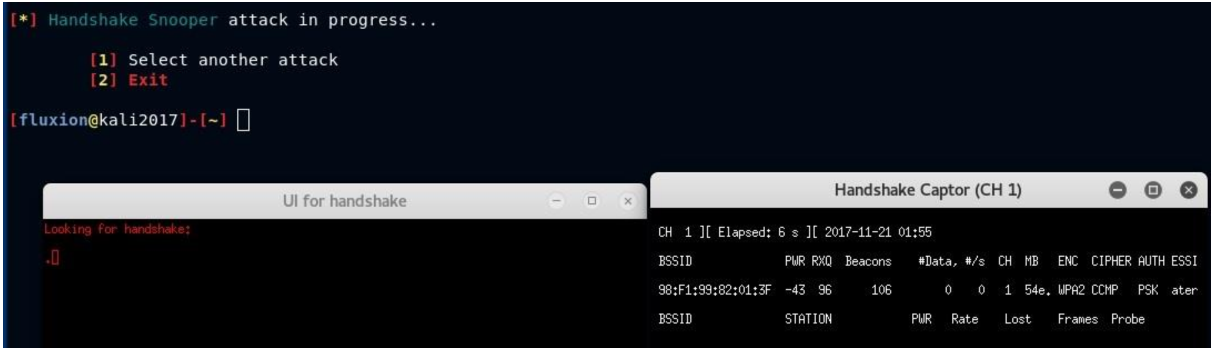
- Selecting the hash verification method



```
[*] Select a method of verification for the hash

        [1] pyrit verification (recommended)
        [2] aircrack-ng verification (unreliable)
        [3] Back

[fluxion@kali2017]-[~] 
```

Using Fluxion

- Attack in progress



```
[*] Handshake Snooper attack in progress...

        [1] Select another attack
        [2] Exit

[fluxion@kali2017]-[~]
```

```
Looking for handshake:

.
```

```
CH  1 ][ Elapsed: 6 s ][ 2017-11-21 01:55

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSI

98:F1:99:82:01:3F  -43  96      106        0    0   1  54e. WPA2 CCMP   PSK  ater

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

References

- Kitploit

http://www.kitploit.com/2016/10/fluxion-wpawpa2-security-hacked-without.html

- Kali Linux 2017

https://www.kali.org/downloads/

- vk496linset

https://github.com/vk496/linset