B2 - Introduction to Cyber Security

B-SEC-200

Wifi Hacking

Comment pirater les codes d'accès d'un réseau Wi-Fi ?

Introduction

Bienvenue sur ce workshop où vous allez apprendre à vous connecter à un réseau wifi sans avoir le mot de passe et déconnecter tous les appareils d'un réseau. Plutôt sympa, non ?

Les méthodes et commandes que vous allez découvrir sont bien entendu à des fins éducatives et dans un esprit de bienveillance.

Présentation de AirCrack-ng

Pour ce workshop nous allons utiliser toute la suite Aircrack. Ce sont des outils qui seconcentrent sur différents domaines de la sécurité WiFi :

- **Surveillance** : capture de paquets et exportation de données vers des fichiers texte pour un traitement ultérieur par des outils tiers.

- **Attaque**: attaques par répétition, désauthentification, faux points d'accès et autres via l'injection de paquets.

- **Tests** : vérification des cartes WiFi et des capacités des pilotes (capture et injection).

- **Craquage** : WEP et WPA PSK (WPA 1 et 2).

Aujourd'hui nous allons nous concentrer sur l'attaque et le craquage.

Pour les curieux, voici le lien officiel de la documentation d'Aircrack

INSTALLATION

Pour cet atelier, comme dit précédemment, nous allons utiliser aircrack-ng, il vous faudra donc cloner le dépôt à l'adresse ci-dessous, ainsi qu'à exécuter le script bash qui installera toute la suite et les dépendances.

ETAPE N°1 : PRÉREQUIS

Description de l'étape : Dans cette étape, nous allons tout d'abord trouver le nom de votre carte wifi pour ensuite la préparer afin qu'elle puisse écouter tous les réseaux à proximité.

Activez le mode moniteur (airmon-ng)

```
Terminal
~/B-SEC-200> airmon-ng
```

Le mode moniteur (en anglais : Radio Frequency Monitoring) permet à un ordinateur équipé d'une carte réseau Wi-Fi, d'écouter tout le trafic d'un réseau sans fil.

Trouvez le nom du moniteur (sous «interface»)

Démarrez votre interface en mode moniteur

Cela vous permettra de scanner tous les réseaux aux alentours et donc de récupérer des informations qui pourraient être précieuses par la suite

```
Terminal
~/B-SEC-200> airmon-ng start [VOTRE MONITEUR]
```

Activez l'interface du mode moniteur

```
Terminal
~/B-SEC-200> iwconfig
```

Tuez tous les processus qui renvoient une erreur

Si nous ne tuons pas tous les processus autres que ceux dont nous avons besoins, cela pourrait interférer avec les écoutes, que nous allons faire dans les étapes suivantes.

Terminal

```
~/B-SEC-200> airmon-ng check kill
```

ETAPE N°2 : RECHERCHE DU RÉSEAU CIBLE

Description de l'étape : Dans cette étape nous allons rechercher le réseau que l'on souhaite pirater, pour ensuite récupérer le "Handshake". Le handshake, littéralement «poignée de main» en français, est un paquet qui peut être récupéré quand un utilisateur se connecte à un réseau. Une fois le mot de passe récupéré il faudra le décrypter dans l'étape suivante.

Lancez l'écoute des routeurs du secteur

Airodump permet d'écouter les réseaux aux alentours

Terminal

```
~/B-SEC-200> airodump-ng [VOTRE MONITEUR]
```

```
CH  1 ][ Elapsed: 10 mins ][ 2022-04-05 21:40

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

E4:9E:12:1F:07:FD   -1        0        0    0   6   -1                    <length:  0>
68:A3:78:5D:B3:E1   -1        0      488    0  13   -1   WPA              <length:  0>
10:0C:6B:A1:AD:24  -58      463   102933    0   1  130   WPA2 CCMP   PSK  ILOVEEPITECH
F4:06:8D:B7:2F:9D  -22      575       37    0   6  130   WPA2 CCMP   PSK   42<EPITECH
D4:6E:0E:FC:DC:0A  -25      156        1    0   1  270   WPA2 CCMP   PSK  <length:  0>
30:7E:CB:71:DA:84  -33       93        1    0  11  130   WPA  CCMP   PSK     APEWIFI
C2:7E:CB:71:DA:85  -32       63        0    0  11  130   OPN              SFR WiFi FON
72:35:C0:6F:AF:25  -34       36        0    0  11  130   WPA2 CCMP   MGT  SFR WiFi Mobile
C2:7E:CB:71:DA:87  -32       53        0    0  11  130   WPA2 CCMP   MGT  SFR WiFi Mobile
E4:9E:12:DC:C9:12  -32       42        0    0   7  195        CCMP   MGT  FreeWifi_secure
72:35:C0:6F:AF:27  -32       17        0    0  11  130   OPN              SFR WiFi FON
60:35:C0:6F:AF:26  -33        3        2    0  11  130   WPA  CCMP   PSK   DJIBRILWPA2
D0:AE:EC:40:8C:95  -33       26        0    0   6  130   WPA  CCMP   PSK     WTCWIFI
E4:9E:12:DC:C9:10  -31       34        5    0   7  195   WPA  CCMP   PSK IPHONEDERONDOUDOU
```

Oula ça fait beaucoup d'informations et en plus ça bouge vite ! Je vous ai concocté un petit guide rien que pour vous !

- BSSID : C'est tout simplement l'adresse MAC
- PWR : Il s'agit de la compatibilité avec l'optionwifi «low-power»
- Beacons : Les trames Beacon sont émises périodiquement, elles servent majoritairement à signaler la présence d'un LAN sans fil
- #Data : C'est le nombre de paquet échanger sur le réseau
- CH : Le canal
- ENC : C'est un protocole de chiffrement cela peut être WPA2, WPA ou WEP (la sécurité de nos grands parents).
- AUTH : En cryptographie, une clé pré-partagée (PSK = Pre-shared key) est un secret partagé qui était auparavant partagé entre les deux parties en utilisant un canal sécurisé avant de devoir être utilisé.
- ESSID : L'ESSID est un marqueur ou un identifiant électronique qui sert d'identification et d'adresse pour votre ordinateur ou périphérique réseau pour se connecter à un routeur ou un point d'accès sans fil, puis accéder à Internet.

Notez des différentes informations du réseau que vous voulez attaquer

Surveillez votre réseau à la recherche de l'établissement d'une liaison

Comme lors de la précédente étape, nous allons réutiliser la commande airodump mais cette fois-ci, au lieu d'écouter tous les réseaux, nous allons nous concentrer sur le réseau choisi précédemment jusqu'à l'obtention du "Handshake"

Terminal

```
~/B-SEC-200> airodump-ng -c [CH] --bssid [BSSID] -w (le dossier ou va être stocker votre résultat) [VOTRE MONITEUR]
```

Attendez l'établissement d'une liaison avec le réseau cible (Handshake)

Etape n°3 : Décryptage du code d'accès

Nous y sommes presque ! Grâce à l'étape précédente nous avons pu récupérer les codes d'accès (Handshake) ainsi que certains fichiers avec les codes d'accès. Alors c'est bon, non ? Malheureusement ce n'est pas si simple, le mot de passe que l'on possède est crypté. Nous allons devoir le décrypter pour avoir une version que l'on puisse utiliser.

Renommez le fichier contenant la clef cryptée

Le fichier .cap doit être renommé car si l'on répète le processus plusieurs fois on peut vite s'y perdre.

Lancement du déchiffrage de la clé grâce au dictionnaire

Pour déchiffrer le mot de passe nous allons utiliser un dictionnaire. Il en existe de différentes sortes (de quelques centaines de mots jusqu'à plusieurs centaines de millions). Pour ce workshop, nous allons utiliser Rockyou.txt une liste de 14 millions de mot de passe issue du piratage Rock You2009

Terminal

```
~/B-SEC-200> aircrack-ng -a2 -b [HANDSHAKE] -w [DICTIONNAIRE] [MDP.cap]
```

Attendre la découverte du mot de passe

Si le mot de passe est trouvé dans le dictionnaire, le programme marquera "KEY FOUND" suivi du mot de passe en clair. Suivant la taille du dictionnaire, le temps de découverte du mot de passe peut varier de quelques millisecondes jusqu'à des siècles.

Nombre de caractères	► Minuscules	► Minuscules + Majuscules	► Minuscules + Majuscules + Chiffres	► Minuscules + Majuscules + Chiffres + Caractères spéciaux
1 à 3	< 1 seconde	< 1 seconde	< 1 seconde	< 1 seconde
4	< 1 seconde	< 1 seconde	1 seconde	1 seconde
5	1 seconde	38 secondes	1 minute	3 minutes
6	30 secondes	32 minutes	1 heure	4 heures
7	13 minutes	1 jour	4 jours	15 jours
8	5 heures	61 jours	252 jours	3 ans
9	6 jours	8 ans	42 ans	237 ans
10	163 jours	458 ans	2 000 ans	17 000 ans
11	11 ans	23 000 ans	164 000 ans	1 million d'années
12	302 ans	1 million d'années	10 millions d'années	100 millions d'années
13	7 000 ans	64 millions d'années	633 millions d'années	7 milliards d'années

Etape n°4 : Attaque de désauthentification

Description de l'étape : L'attaque de désauthentification permet, comme le nom l'indique, de désauthentifier des clients connectés à un réseau grâce à l'envoi de paquets d'informations qui coupent la connexion Internet, obligeant ainsi l'utilisateur à se reconnecter, ce qui permet de générer un "Handshake", si utile par la suite.

Surveillez votre réseau à la recherche de l'établissement d'une liaison

```
Terminal
~/B-SEC-200> airodump-ng -c [CH] --bssid [MAC]
```

Envoie des paquets de désauthentification

```
Terminal
~/B-SEC-200> aireplay-ng -0 [NB PAQUETS] -a MAC1 -c MAC2 [VOTRE MONITEUR]
```

[NB PAQUETS] Vous pouvez augmenter cette valeur, mais cela entraînera des déconnections intempestives(ne faites pas crasher mon routeur svp ;() et cela augmente le risque de vous faire repérer dans votre tentative. Remplacez MAC1 par l'adresse MAC la plus à gauche des deux, au bas de la fenêtre d'arrière-plan de Terminal. Remplacez MAC2 par l'adresse MAC la plus à droite, au bas de la fenêtre d'arrière-plan de Terminal.

Etape n°5 : Bonus

Description de l'étape: On arrive à la fin de ce workshop, sniff :/. Si vous souhaitez continuer, vous pouvez combiner l'attaque de désauthentification pour ensuite pouvoir plus simplement si connecter :).