WiFi Sécurité

Objectif : Apprendre le hacking WiFi pour mieux se défendre.

Aircrack-ng, *mdk3*, *hostapd*, ... sont des outils de sécurité Wi-Fi. Ils regroupent plusieurs formes d'attaques connues et moins connues pour l'intrusion sur un réseau WIFi. Ils peuvent être aussi utilisés pour l'audit et le monitoring de réseaux sans fil.

▸ Exercice 1 : Cracker le passphrase WPA/WPA2

1. créer une interface WiFi virtuelle en mode monitor en utilisant le script *airmon-ng* : **airmon-ng start wlan0**.
2. Faire tomber l'interface wlan0 avec la commande : **ifconfig wlan0 down**.
3. Dans un premier temps, il faut faire un état des lieux des réseaux alentours en utilisant le script *airmon-ng* : *airodump-ng mon0*
4. Dès que le réseau cible est identifié (*BadisNetwork*), relancer *airodump*, en lui précisant les filtres suivants :
   (a) $-c$ permet de cibler un canal, ex : $-c$ 1 ciblera le canal 1
   (b) $--$ *encrypt* permet de cibler selon l'encryptage des réseaux, ex : $--$ *encrypt wpa* ciblera uniquement les réseaux encryptés en WPA
   (c) $-w$ spécifie le nom du fichier de capture qui sera créé ex : $-w$ FileHandshake
   (d) $--$ *bssid* permet de cibler l'écoute sur un seul point d'accès ex : $--$ *bssid* 00 : AA : 11 : BB : 22 : CC : 33
5. Pour retrouver le *passphrase* utilisé par le réseau *BadisNetwork*, l'attaquant doit écouter les échanges entre le AP et un client valide lors de la phase d'authentification. Cet échange est appelé **4 way handshake**. L'attaque consiste donc à forcer la re-authentification des clients. Il va utiliser l'attaque de déauthentication.
6. Dans un nouveau shell, lancer une attaque de déauthentication en utlisant le script *aireplay-ng* : *aireplay-ng -0 5 -a bssid -c MAC_ client mon0*
7. Si l'attaque a réussi, sur le shell airodump-ng, il va apparaitre du WPA handshake en haut à droite de la fenêtre. Selon la qualité de la réception, la capture du handshake peut être immédiate, ou très fastidieuse. Renouveler l'attaque à de nombreuses reprises avant d'obtenir le tant attendu handshake.
8. Le handshake est maintenant dans le fichier de capture (*FileHandshake*), stopper airodump.
9. Pour trouver le *passphrase* à partir de fichier capture, il faut s'armer d'un dictionnaire de mots de passe existant ou forger de manière incrémentale des mots de passe. Nous allons tester la deuxième méthode.
10. Installer l'outil *crunch*, un générateur de mots de passe.
    (a) Exemple 1 : Tester et expliquer cette commande : *crunch 4 6 -f /usr/share/crunch/charset.lst mixalpha-numeric-symbol14-space -o wordlist.txt*
    (b) Exemple 2 : Tester et expliquer cette commande : *crunch 6 6 -t pass%%*
11. Afin de réduire le temps pour trouver le *passphrase*, nous supposons que ce dernier contient 7 caractères, il commence par le mot **bad** suivi par 3 caractères minuscules et enfin un chiffre. Lancer la commande : *crunch 8 8 -t badh@@%% | aircrack-ng -w - -e BadisNetwork FileHandshake-01.cap*

12. Si chaque mot de passe testé prend 0.5 seconde, quelle est le temps max pour trouver un mot de passe de taille 10 contenant des caractères de type mixalpha-numeric-symbol14-space.

▸ Exercice 2 : WPS-PBC

Le WPS, pour WiFi Protected Setup, est une technologie lancée par la WiFi Alliance pour simplifier la connexion d'un appareil à un réseau WiFi. Deux principales méthodes sont proposées par la norme.

La première méthode est le *PBC*, pour Push Button Connect. Comme son nom l'indique, il est nécessaire de presser un bouton sur le point d'accès pour lancer le jumelage. Le bouton est soit physique — le cas le plus courant — soit virtuel, dans l'interface de l'appareil. Ensuite, il faut presser un bouton — lui aussi physique ou virtuel — sur le périphérique à connecter pour que les deux appareils soient liés. L'attaque consiste à être plus rapide que le client pour répondre au AP des que le WPS est activé.

1. Activer en boucle un client WPA, puis lui donner l'ordre de répondre à toutes les APs dès que le WPS est activé : *while :; do sudo wpa_cli wps_pbc any; sleep 120; done &*
2. Comment le client détecte-il cette attaque ?

▸ Exercice 3 : WPS-PIN

Le WPS, pour WiFi Protected Setup, est une technologie lancée par la WiFi Alliance pour simplifier la connexion d'un appareil à un réseau WiFi. Deux principales méthodes sont proposées par la norme.

La Deuxième méthode consiste à doter le point d'accès d'un code PIN. Les appareils qui veulent se connecter au point d'accès doivent donc connaître le code PIN (8 chiffres) de ce dernier. L'attaque revient à bruteforcer le code PIN.

1. Installer l'outil **Reaver-wps**.
2. Scanner les APs qui proposent le WPS avec la commande *wash* sur une interface en mode monitor (mon0) : *wash -i mon0.*
3. Une fois le AP cible est trouvé, arrêter le scan, et lancer l'attaque : *reaver -i mon0 -b [BSSID de l'AP] -vv*

▸ Exercice 4 : Récupération des Clés WiFi par une clé USB Rubber Ducky

Le principe d'action de la clé USB Rubber Ducky, commercialisée par Hak5, est simple à comprendre. La clé USB se fait passer pour un clavier auprès du système et va, dès son lancement, exécuter des actions sur le système, à l'image d'un autorun.exe, sauf que cela va être la saisie des touches claviers.

lorsque la clé USB va être branchée, elle va contenir un ensemble de combinaisons et d'actions clavier qui vont lui faire saisir des touches au clavier. Ainsi, si on paramètre la clé USB Rubber Ducky pour faire un "CTRL+R" puis un saisir "CMD", "Entrée" puis saisir "ipconfig", dès que l'on va brancher notre clé USB Rubber Ducky, l'ensemble de ces actions vont s'exécuter, sans que nous n'ayons rien à faire. Cela est possible par la composition de la clé USB, qui renferme en fait une carte micro SD dans laquelle on injecte un .bin contenant les touches à saisir, celles-ci doivent donc être paramétrées au préalable

1. En se basant sur le site `https://ducktoolkit.com/` et `https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads`, tester des exemples sur le système Windows.
2. Pour exporter manuellement les profil WiFi :
   (a) ouvrir une invite de commande puis rendre dans le répertoire de votre choix avec la commande *cd*. Exemple : *cd c :\Users\Administrateur\Desktop*
   (b) saisir la commande suivante pour exporter l'ensemble de vos profils Wifi : *netsh wlan export profile key=clear*

(c) vérifier le contenu des fichiers XML exportés.

3. En utilisant la clé USB Rubber Ducky, écrire et tester le script qui permet d'exporter les profils wifi et de les envoyer par E-mail au compte de l'attaquant.