Fiche Résumé

Informations Diverses

Nous avons pour but d'offrir une introduction au Pentest(Test d'intrusion) de façon éthique, ludique et accessible par toustes quelque soit l'expérience en informatique. Nous introduisons ici une initiation simplifiée de Aircrack-ng (disponible sur Windows, Linux, et macOS) pour comprendre les grand principe de réalisation comme : passer sa carte WIFI en mode moniteur, analyser le réseau, désauthentifier, capturer des paquets, ou encore déchiffrer une clé. C'est une démonstration générale qui se veut simplifier les concepts dans les grandes lignes,pour aller plus loin,il faut consulter la documentation web.
Ici nous travaillerons sur la syntaxe de Aircrack-ng sous Linux avec une tentative de reproduction d'invite de commande très basique.

Il est important de rappeler que ce projet a un but éducatif, axé sur la sécurité de nos réseaux Wi-Fi, et doit être réalisé dans un cadre éthique.

1. Privilège superutilisateur

Si tu viens de Windows, MacOs, Android ou encore IOS c'est que tu n'as probablement jamais eu la sensation d'être maître de ton appareil ! Interagir avec les composants de ton ordinateur nécessite que tu aies leur autorisation : et oui le consentement ! Ici Aircrack-NG a besoin de permissions pour fonctionner notamment pour manipuler la carte réseau. Donc, on commence par une commande qui lui donne ces droits, un peu comme un badge d'accès à un bâtiment ou des clés de voiture pour la démarrer. Passer en mode superutilisateur avec cette commande afin d'avoir la pleine utilisation de la machine :

```
sudo su
```

Puis,on regarde le nom de l'interface réseau que l'on a:

```
iwconfig
```

Ici on aura wlan0,cela dépend de la machine.

Fiche Résumé

2.Carte WIFI en mode moniteur

En temps normal ta carte wifi écoute grossièrement seulement les données qu'elle reçoit du réseau auquel est connecté ton appareil. Ce qu'on veut pour analyser le trafic réseau autour de toi c'est écouter tous les réseaux disponibles à proximité,donc on met la carte réseau en mode moniteur ! C'est comme papi à l'EHPAD qui respire h24 en bouteille d'oxygène et puis POUF il découvre l'air environnant ainsi que toutes les odeurs de ses compagnons de vie!

Alors il faut activer le mode moniteur sur la carte WIFI pour surveiller/écouter les réseaux:

```
airmon-ng start wlan0
```

Pour remettre en managed, on remplacera start par stop :

```
airmon-ng stop wlan0mon
```

On peut refaire un ifconfig ou iwconfig pour voir le mode actuel de la carte.

3. Scan de réseaux

Puis ensuite on veut connaître les réseaux wifi à proximité et leur caractéristiques. Grâce à un scan on obtient une liste de tous les réseaux dans la zone en temps réel,tu pourras connaître son nom ou encore si il est lent par exemple : pratique si tu veux mener une attaque/un pentest ! Notre carte en mode moniteur nous permet de scanner. On fait alors la commande suivante :

```
airodump-ng wlan0mon
```

On peut regarder les appareils connecté à un réseau cible :

```
airodump-ng wlan0mon --channel <numéro canal> --bssid <bssid cible>
```

Fiche Résumé

4. Désauthentification/Capture de paquet

Ce qu'on veut c'est récupérer des données pour analyser comment elles sont chiffrées ou bien trouver des vulnérabilités. Pour cela on peut désauthentifier un utilisateur du réseau cible pour que sa machine soit forcé de se reconnecter au réseau automatiquement et envoyer des paquets de données, ce que font les machine pour s'authentifier auprès d'un réseau (handshakes) !
Effectuez une attaque de désauthentification pour déconnecter un client spécifique :

```
aireplay-ng -0 <nb de désauth> -a <bssid cible> -c <machine connecté au bssid cible> wlan0mon
```

Pour capturer des paquets du réseau cible :

```
airodump-ng wlan0mon --channel <numéro canal> --bssid <bssid cible> -w <nom-fichier-capture.cap>
```

Aircrack-NG capture les paquets de données qui circulent. Les données peuvent être diverses, ce sont tout ce qui passe pour que les appareils puissent communiquer avec le réseau et donc échanger avec le routeur. Grâce à ces données, on aura une chance de découvrir la clé de sécurité du réseau ou un mot de passe directement.

5. Crack du mot de passe

Quand on a assez de paquets, Aircrack-NG peut tenter de trouver la clé de sécurité ou le mot de passe en clair du réseau. On utilise souvent un dictionnaire avec des millions de mots de passe pour qu'il teste rapidement par brute force. Si il trouve la clé alors on aura de quoi hacker le réseau,sinon il faudra recommencer ou bien utiliser d'autres nombreuses techniques de crack de clé. Les méthodes peuvent dépendre de comment est encrypté le réseau (WPE, WPA2, WPA3...).

```
aircrack-ng -w <dico-mdp.txt> -b <bssid cible> <fichier-capture.cap>
```

Quand on a assez de paquets, Aircrack-NG peut tenter de trouver la clé de sécurité ou le mot de passe en clair du réseau. On utilise souvent un dictionnaire avec des millions de mot de passe pour qu'il teste rapidement par brute force.Si il trouve la clé alors on aura de quoi hacker le réseau,sinon il faudra recommencer ou bien utiliser d'autres nombreuses techniques de crack de clé.