Manuel Complet d'Aircrack-ng

Introduction à Aircrack-ng

Aircrack-ng est une suite logicielle complète d'outils d'évaluation de la sécurité des réseaux WiFi. Elle est largement utilisée par les professionnels de la cybersécurité, les auditeurs de sécurité et les passionnés pour tester la robustesse des réseaux sans fil. La suite Aircrack-ng se concentre sur plusieurs domaines clés 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 de relecture, désauthentification, création de faux points d'accès et autres via l'injection de paquets.
- **Test** : Vérification des capacités des cartes WiFi et des pilotes (capture et injection).
- **Craquage** : Craquage des clés WEP et WPA/WPA2-PSK.

Tous les outils sont en ligne de commande, ce qui permet une automatisation poussée. Bien qu'il existe des interfaces graphiques (GUI) qui ont tiré parti de cette fonctionnalité, Aircrack-ng fonctionne principalement sur Linux, mais aussi sur Windows, macOS, FreeBSD, OpenBSD, NetBSD, Solaris et même eComStation 2.

Installation d'Aircrack-ng

Aircrack-ng est disponible sur la plupart des distributions Linux orientées sécurité, comme Kali Linux. Pour les autres systèmes, voici les méthodes d'installation :

Installation sur Linux (Debian/Ubuntu)

Sur les systèmes basés sur Debian ou Ubuntu, vous pouvez installer Aircrack-ng via le gestionnaire de paquets `apt` :

```
 sudo apt update
sudo apt install aircrack-ng
```

Installation sur Arch Linux

Sur Arch Linux, vous pouvez l'installer depuis les dépôts officiels :

```
sudo pacman -S aircrack-ng
```

Installation depuis les sources

Si vous souhaitez compiler Aircrack-ng depuis les sources (par exemple, pour obtenir la dernière version ou pour une distribution non prise en charge), vous pouvez suivre ces étapes :

1. **Cloner le dépôt GitHub** : `bash git clone https://github.com/aircrack-ng/aircrack-ng.git cd aircrack-ng`
2. **Installer les dépendances** (les noms des paquets peuvent varier selon la distribution) : `bash sudo apt install build-essential autoconf automake libtool pkg-config libnl-3-dev libnl-genl-3-dev libssl-dev ethtool`
3. **Compiler et installer** : `bash autoreconf -i ./configure --with-nl-prefix=/usr/local make sudo make install`

Installation sur Windows

Pour Windows, Aircrack-ng est généralement fourni sous forme de binaires précompilés. Vous pouvez les télécharger depuis le site officiel d'Aircrack-ng. Le paquet inclut les exécutables et les pilotes nécessaires.

1. Rendez-vous sur le site officiel d'Aircrack-ng : https://www.aircrack-ng.org/downloads.html
2. Téléchargez la dernière version du paquet Windows (généralement un fichier `.zip`).
3. Extrayez le contenu du fichier `.zip` dans un dossier de votre choix.
4. Vous devrez peut-être installer des pilotes spécifiques (comme WinPcap ou Npcap) pour que la capture de paquets fonctionne correctement. Ces pilotes sont souvent inclus ou recommandés lors du téléchargement.

Installation sur macOS

Pour macOS, vous pouvez utiliser Homebrew pour installer Aircrack-ng :

```
brew install aircrack-ng
```

Vérification de l'installation

Après l'installation, vous pouvez vérifier que Aircrack-ng fonctionne correctement en exécutant la commande suivante dans votre terminal :

```
aircrack-ng --version
```

Ceci devrait afficher la version d'Aircrack-ng installée, confirmant que l'installation a réussi.

Composants Principaux d'Aircrack-ng et Leurs Fonctions

La suite Aircrack-ng est composée de plusieurs outils, chacun ayant une fonction spécifique dans le processus d'audit de sécurité WiFi. Comprendre le rôle de chaque composant est essentiel pour utiliser efficacement la suite.

1. `airmon-ng` : Activation du Mode Moniteur

`airmon-ng` est l'outil utilisé pour activer le mode moniteur sur votre carte réseau sans fil. Le mode moniteur permet à la carte de capturer tous les paquets WiFi qui transitent à portée, sans être associée à un point d'accès spécifique. C'est la première étape cruciale pour toute opération d'audit.

Commandes clés :

- `airmon-ng check kill` : Tue les processus qui pourraient interférer avec le mode moniteur (par exemple, NetworkManager).
- `airmon-ng start <interface>` : Active le mode moniteur sur l'interface spécifiée (par exemple, `wlan0`). Cela créera généralement une nouvelle interface en mode moniteur (par exemple, `wlan0mon`).
- `airmon-ng stop <interface_moniteur>` : Désactive le mode moniteur sur l'interface spécifiée (par exemple, `wlan0mon`) et restaure l'interface d'origine.

Exemple :

```
sudo airmon-ng check kill
sudo airmon-ng start wlan0
```

2. `airodump-ng` : Capture de Paquets et Surveillance

`airodump-ng` est l'outil de capture de paquets. Il est utilisé pour collecter des informations sur les réseaux WiFi à proximité, y compris les BSSID (adresses MAC des points d'accès), les ESSID (noms des réseaux), les canaux, le type de chiffrement (WEP, WPA, WPA2), et les clients connectés. Il peut également enregistrer les paquets capturés dans un fichier pour une analyse ultérieure.

Commandes clés :

- `airodump-ng <interface_moniteur>` : Démarre la capture de paquets sur l'interface en mode moniteur.
- `airodump-ng --bssid <BSSID> --channel <canal> --write <fichier_capture> <interface_moniteur>` : Capture les paquets d'un point d'accès spécifique sur un canal donné et les enregistre dans un fichier.

Exemple :

```
 sudo airodump-ng wlan0mon
# Pour cibler un réseau spécifique et enregistrer les paquets
sudo airodump-ng --bssid 00:11:22:33:44:55 --channel 6 --write
mon_reseau wlan0mon
```

3. `aireplay-ng` : Attaques d'Injection et de Relecture

`aireplay-ng` est un outil d'injection de paquets et de relecture. Il est utilisé pour générer du trafic réseau afin d'accélérer la collecte de données nécessaires au craquage des clés WEP, ou pour effectuer des attaques de désauthentification pour capturer le handshake WPA/WPA2.

Commandes clés :

- `aireplay-ng --deauth <nombre_paquets> -a <BSSID_AP> -c <BSSID_CLIENT> <interface_moniteur>` : Effectue une attaque de désauthentification contre un client spécifique ou tous les clients connectés à un point d'accès.
- `aireplay-ng --fakeauth 0 -e <ESSID> -a <BSSID_AP> <interface_moniteur>` : Effectue une fausse authentification pour s'associer à un point d'accès WEP.
- `aireplay-ng --arpreplay -b <BSSID_AP> -h <MAC_CLIENT> <interface_moniteur>` : Effectue une attaque de relecture ARP pour générer des IVs (vecteurs d'initialisation) pour le craquage WEP.

Exemple :

```
sudo aireplay-ng --deauth 0 -a 00:11:22:33:44:55 wlan0mon
```

4. `aircrack-ng` : Craquage de Clés WEP et WPA/WPA2-PSK

`aircrack-ng` est l'outil principal de la suite, utilisé pour craquer les clés WEP et WPA/WPA2-PSK à partir des fichiers de capture (`.cap`) générés par `airodump-ng` .

Craquage WEP :

Le craquage WEP nécessite un nombre suffisant de IVs (vecteurs d'initialisation) collectés. Plus il y a de IVs, plus les chances de succès sont élevées.

Commande :

- `aircrack-ng <fichier_capture>.cap` : Tente de craquer la clé WEP à partir du fichier de capture.

Exemple :

```
aircrack-ng mon_reseau-01.cap
```

Craquage WPA/WPA2-PSK :

Le craquage WPA/WPA2-PSK est basé sur une attaque par dictionnaire. Il nécessite la capture d'un handshake à quatre voies (four-way handshake) entre un client et le point d'accès, ainsi qu'une liste de mots de passe (dictionnaire).

Commande :

- `aircrack-ng -w <fichier_dictionnaire> <fichier_capture>.cap` : Tente de craquer la clé WPA/WPA2-PSK en utilisant un dictionnaire.

Exemple :

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt
mon_reseau-01.cap
```

5. `aircrack-ng-oui` : Mise à jour de la Base de Données OUI

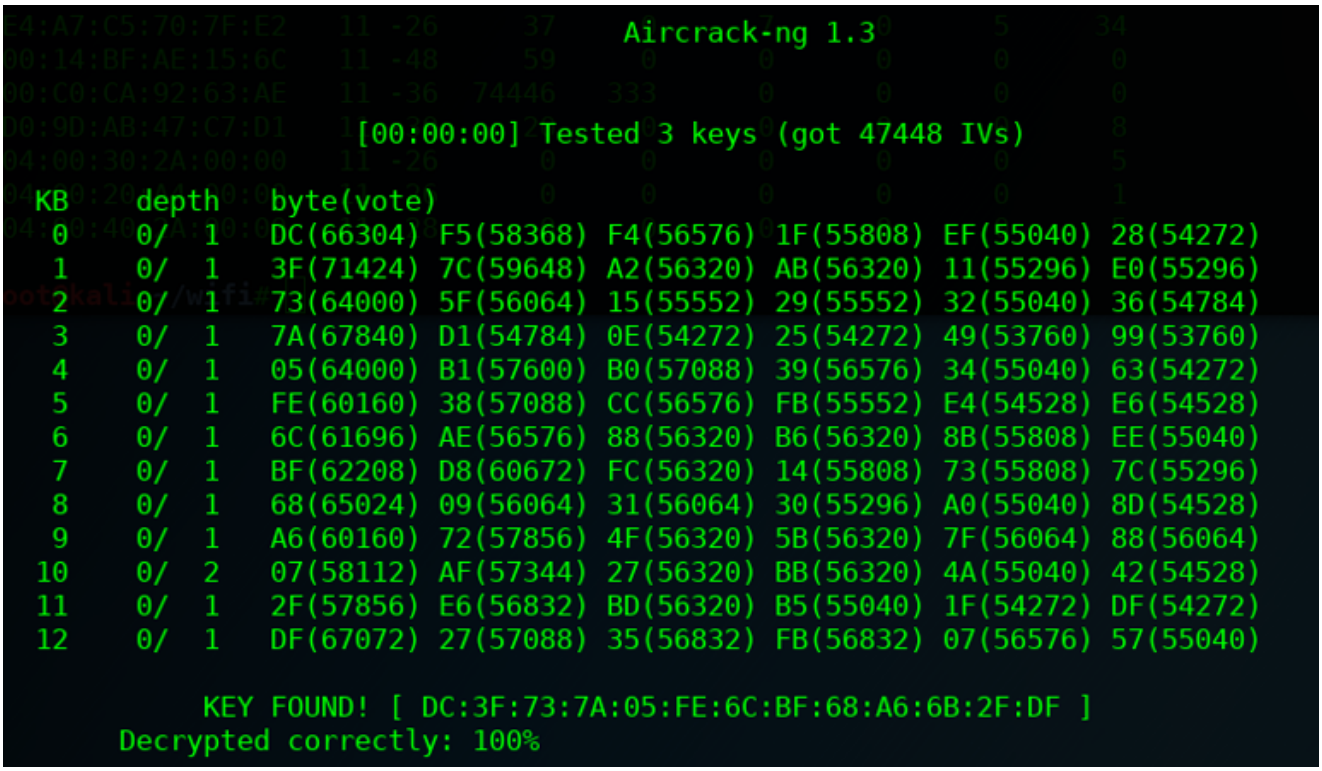
`aircrack-ng-oui` est un script qui met à jour la base de données OUI (Organizationally Unique Identifier) utilisée par Aircrack-ng pour identifier les fabricants des cartes réseau à partir de leurs adresses MAC.

Commande :

```
aircrack-ng-oui update
```

Exemples Visuels et Captures d'Écran

Pour mieux comprendre le fonctionnement d'Aircrack-ng et de ses outils, voici quelques captures d'écran illustrant les différentes étapes d'un audit de sécurité WiFi.



Cette image montre une vue d'ensemble de l'utilisation des outils Aircrack-ng dans un terminal Linux, illustrant potentiellement les sorties de `airmon-ng`, `airodump-ng` et `aircrack-ng` lors d'un processus de craquage de clé. Elle met en évidence l'environnement en ligne de commande typique dans lequel ces outils sont utilisés.