TP : Casse de mot de passe WPA2

Nom : El Atifi Djoumoi Krakria
Groupe : 2

Avertissement préalable

Dans ce TP, nous allons utiliser des outils à manipuler **uniquement dans un cadre autorisé**. Toute utilisation non autorisée sur un système tiers est interdite et punie par la loi (article 323-1 du Code pénal).
Ce TP a pour objectif un apprentissage légal et éthique.
Prérequis : Pour ce TP, une machine virtuelle est nécessaire. Vous pouvez utiliser celle mise à disposition sur `my.isima.fr`.

1 Exercice 1 : Analyse de la robustesse des mots de passe WPA2

Contexte

L'exercice consiste à casser une clé WPA2 (protocole de sécurité Wi-Fi utilisant AES pour chiffrer les communications) à l'aide d'un dictionnaire et de deux réseaux Wi-Fi.

Questions préliminaires

Q1. Expliquez ce qu'est un dictionnaire de mots de passe et à quoi il sert dans une attaque par dictionnaire.

Q2. Votre PC dispose-t-il d'une carte Wi-Fi active ? Quel est l'impact de sa présence ou de son absence sur sa capacité à analyser les réseaux environnants ?

Méthodologie

Comme vous l'aurez compris, dans ce TP, vous n'aurez pas à effectuer la capture du trafic réseau vous-même. Nous utiliserons des fichiers de capture contenant des **handshakes** déjà préparés.

Qu'est-ce qu'un handshake ? Un handshake correspond à l'échange entre un point d'accès et un client permettant de vérifier la validité du mot de passe et de générer les clés de chiffrement nécessaires à la connexion.

Fichiers fournis : Deux fichiers de handshake et un dictionnaire ont été préparés pour ce TP :

- `wpa2_handshake_weak_password` : handshake associé à un mot de passe faible.
- `wpa2_handshake_strong_password` : handshake associé à un mot de passe fort.
- Un dictionnaire des mots de passe les plus utilisés en France, présent sur le site : `https://github.com/tarraschk/richelieu`.

Utilisation d'aircrack-ng

Nous allons utiliser `aircrack-ng` pour tester hors-ligne les mots de passe.

Principe : `aircrack-ng` lit un fichier de capture contenant un handshake, teste chaque mot d'une wordlist (ici le dictionnaire) et compare le résultat au champ MIC (Message Integrity Code) du handshake. Le but est de trouver la clé correspondante.

1.1 Analyse avec mot de passe faible

Testez la première capture contenant le handshake avec un mot de passe faible.

Commande :

```
aircrack-ng -w [dictionnaire] [wpa2_handshake_weak_password]
```

Questions :

a) Combien de mots de passe ont été testés avant de trouver la bonne clé ?

b) Quel est le temps total nécessaire pour trouver le mot de passe ?

1.2 Analyse avec mot de passe fort

Testez maintenant la seconde capture contenant le handshake avec un mot de passe fort.

Commande :

```
aircrack-ng -w [dictionnaire] [wpa2_handshake_strong_password]
```

Questions :

a) Combien de mots de passe ont été testés cette fois-ci ?

b) Quel est le temps nécessaire pour cette tentative ?

c) Le mot de passe a-t-il été trouvé ? Si non, pourquoi, selon vous ?

1.3 Importance des mots de passe robustes

Question : Pourquoi est-il important d'avoir des mots de passe robustes plutôt que faibles ? Expliquez en quelques phrases les risques liés à l'utilisation de mots de passe faibles et comment un mot de passe fort renforce la sécurité d'un réseau Wi-Fi.