# TP : Casse de mot de passe WPA2

Nom : El Atifi Djoumoi Kraria
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

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.** Qu'est-ce qu'un dictionnaire de mots de passe ? Expliquez son utilité dans le cadre d'une attaque par dictionnaire.

**Q2.** Est-ce que votre PC possède une carte Wi-Fi active ? Si oui (ou non), comment cela influence-t-il sa capacité à capturer et analyser le trafic des réseaux Wi-Fi aux alentours ?

**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 jugé faible.
- `wpa2_handshake_strong_password` : handshake associé à un mot de passe jugé 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 :** Pour la suite, il est nécessaire d'installer aircrack-ng afin de pouvoir effectuer les tests de mots de passe en mode hors ligne.

**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] [handshake]
```

**Questions :**

a) Quel est le mot de passe correct, et combien de tentatives ont été nécessaires avant de le trouver ?

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] [handshake]
```

**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 ? Pourquoi ?

### 1.3 Importance des mots de passe robustes

**Question :**
Pourquoi est-il important de choisir un mot de passe long incluant des majuscules, des minuscules, des chiffres et des caractères spéciaux, et comment cela renforce-t-il la sécurité d'un compte ou d'un réseau en général ?