# PROJET : SECURITE WIFI

## INTRODUCTION

L'objectif de ce TP est de comprendre le fonctionnement de WPA et d'analyser les différentes méthodes d'authentification `802.11i` à travers un serveur d'authentification RADIUS.

La maquette à monter nécessitent deux VM Linux. Les interfaces Wifi utilise l'émulateur Linux intégré **mac80211_hwsim** qui sera chargé comme un module dans le noyau Linux. Le point d'accès utilise le logiciel **hostapd** et les supplicants sont basé sur **wpa_supplicant**.

## A. CONFIGURATION ET ANALYSE DE WPA-PERSONNEL

1. Sur votre VM Linux, charger le module ***mac80211_hwsim*** en spécifiant quatre cartes réseaux sans fil :

```
/sbin/modprobe mac80211_hwsim radios=3
```

2. Consulter et expliquer quelques caractéristiques de la carte `wlan0` avec les commandes :

```
/sbin/iw wlan0 info
/sbin/iw phy0 info
```

3. Installer **hostapd** qui permet d'utiliser une carte sans fil en tant que point d'accès. Configurer-le pour créer un SSID avec WPA-Personnel sur wlan0.
4. Configurer ***wlan2*** afin de capturer tous les échanges sur votre réseau dans un fichier de capture. Vous devez tout d'abords configurer wlan2 en mode monitor en utilisant la commande **iw** ou bien en utilisant **airmon-ng** qui fait partie du logicien aircrack-ng. Après, utiliser airodump-ng pour lancer la capture.
5. Capturer les trames Beacons et expliquer leur contenu.
6. Configurer le **wpa_supplicant** sur ***wlan1*** pour se connecter à votre réseau.
7. Analyser la capture obtenue et expliquer le scénario complet de la connexion. Analyser le **4-way handshake**.
8. Expliquer les deux vulnérabilités conceptuelles sur le 4-way handshake :
   a. Attaque par dictionnaire offline
   b. KRACK

Pour la deuxième partie du TP, nous allons monter et configurer une architecture WPA-Entreprise.

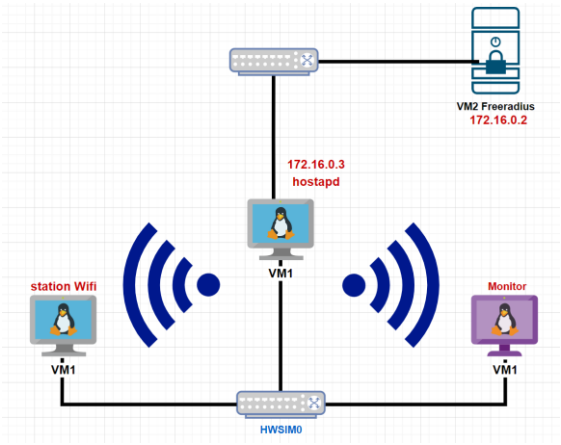


FIGURE 1: MAQUETTE DU TP - WPA ENTREPRISE –

## B. INSTALLATION ET CONFIGURATION DE FREERADIUS

1. Installer FreeRadius sur une VM Linux.
    - Quel est le répertoire d'installation de FreeRadius ?
    - Sur quels ports le serveur écoute les requêtes ?
    - Sous quel compte le serveur est lancé et pourquoi ?
    - Lancer Freeradius en mode debug et vérifier son bon fonctionnement.
2. Ouvrez le fichier de configuration ***clients.conf***.
    - Que déclare-t-on dans ce fichier ?
    - Assurez-vous que le client localhost est bien présent.
    - Le paramètre secret est `testing123` par défaut. A quoi sert ce paramètre ?
    - Comment s'authentifie le point d'accès auprès du serveur ?
3. Ouvrez le fichier ***users*** se trouvant dans le même répertoire et rajouter un nouvel utilisateur.
    - Quelle est la syntaxe de la déclaration de cet utilisateur ?
    - Peut-on utiliser le fichier **/etc/*passwd*** comme source des utilisateurs ?
4. Relancer votre serveur freeradius en mode debug.
    - Tester l'authentification avec la commande *radtest*.
    - Capturer les paquets et faites une analyse des AVP (Attribute-Value Pair) échangés.

## C. CONFIGURATION ET ANALYSE DE WPA-ENTREPRISE

1. Configuration du point d'accès AP :
    - Configurer hostapd pour annoncer WPA-Entreprise aux stations sans fil.
    - Configurer les paramètres freeradius dans le fichier de configuration de hostapd.
    - Déclarer l'adresse l'AP dans le fichier clients.conf de Freeradius (sinon, la connexion de l'AP vers le serveur sera ignorée).
2. Configuration du wpa_supplicant et capture Wireshark :
    - Configurer wpa_supplicant afin de se connecter à votre SSID en utilisant la méthode EAP/PEAP (lire le manuel).
    - Capturer toute la séquence d'authentification en utilisant wlan2.
    - En utilisant un diagramme d'échange, illustrer les messages eapol entre la station et l'AP, puis entre l'AP et Freeradius.
    - Tester et indiquer les différences entre les méthodes PEAP-MSCHAPv2, TTLS-PAP et TTLS-MSCHAPv2
    - Sauvegarder maintenant le mot de passe de l'utilisateur dans le fichier users sous format NT-Password puis sous format Crypt-Password et, à chaque fois, tester les méthodes de la question précédente. Quelle est votre conclusion concernant la compatibilité méthode/stockage ?
    - Que faut-il faire en plus pour utiliser EAP-TLS ?
3. Freeradius est un serveur AAA.
    - Que signifie ce terme ?
    - Interdire l'accès de votre utilisateur pour une plage horaire de votre choix.
4. Installer maintenant WPA3 sur hostapd et faire des tests de connexion.
5. Quels sont les changements majeurs de WPA3 par rapport à WPA2.