**Labo Wifi 2 : Analyse de trames avec Wireshark**

# Partie 1 : Questions théoriques

3. Qu’est-ce que les cartes Alfa ?

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

4. Qu’est-ce que aircrack-ng ?

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

5. Que font les commandes de ligne suivantes ?

1. airmon-ng

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

1. airodump-ng

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

# Partie 2 : Wireshark

**Attention**: les réseaux que vous allez créer dans ce labo doivent avoir comme SSID votre nom ou, sil s’agit d’une équipe, du nom d’un ou une des membres. Le nom doit apparaître dans les captures des Beacons.

Chaque équipe doit faire ses propres captures.

Dans ce laboratoire, nous utiliserons Wireshark pour analyser les trames. Il est possible d'utiliser Wireshark sur la machine native mais nous utiliserons Wireshark sur une machine virtuelle Kali Linux qui a les bons pilotes pour les cartes Alfa.

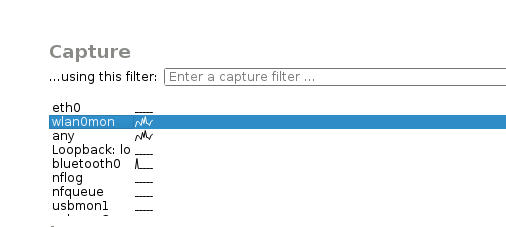
* Mettez en place un réseau wi-fi à l'aide d'un point d'accès fourni par le personnel enseignant.
* Installez une machine virtuelle Kali Linux. Pour ce faire, vous pouvez utiliser un ISO et l'installer par vous-même ou directement télécharger la machine virtuelle déjà préconfigurée. <https://www.kali.org/downloads/>
* Connectez une carte wi-fi externe ALFA, cette dernière permettra la capture des trames sur la machine virtuelle car il est impossible de capturer via l'interface native quand on utilise une vm.
* Assurez-vous que la carte wi-fi est connectée à la machine virtuelle.
* Utilisez la commande airmon-ng pour afficher les interfaces wifi. Vous devriez obtenir un résultat de ce type :



* Ensuite, activez le mode moniteur sur cette interface : airmon-ng start wlan0. Le nom de l'interface peut varier selon les cas. Si vous effectuez à nouveau la commande airmon-ng, vous verrez le nouveau nom de l'interface, par exemple: wlan0mon.
* Puis affichez la liste des ssid : airodump-ng wlan0mon
* Pour finir, focalisez-vous sur les trames relatives au canal qui vous intéresse:

airodump-ng wlan0mon --ch 11

Lancez wireshark tout en laissant la commande airodump-ng executée afin de rester fixer sur le canal 11. Vous devriez voir apparaitre votre interface en mode moniteur (wlan0mon par exemple) :



Sélectionnez-la pour démarrer une capture. Etant donné que votre machine Kali est en mode moniteur, elle n'est pas associée à l'AP. Il vous faudra donc générer du trafic depuis une autre machine physique ou virtuelle.

# Partie 3 : Analyse des protocoles CSMA/CA et RTS/CTS

Vous avez analysé des captures existantes au labo précédent. Dans ce labo, vous allez les produire et les capturer.

Lancez une capture, puis générez du trafic sur le réseau à l'aide de la commande ping. Identifiez des échanges de trames qui correspondent à CSMA/CA unicast.

Abaissez le seuil RTS dans les paramètres de votre AP. Envoyez maintenant un ping avec une payload suffisante (voir option –s du ping) pour tester si le mode RTS/CTS est effectivement activé. Effectuez une capture pour capturer RTS + CTS + Trame de données + ACK et joignez une capture d'écran de cette séquence de 4 trames.

# Partie 4 : Fragmentation

De la même manière que pour le seuil RTS, abaissez le seuil de fragmentation, puis envoyez un ping avec une payload suffisamment grande pour provoquer la fragmentation. Effectuez une capture de trame fragmentée avec CSMA/CA et un échange fragmenté avec RTS/CTS.

# Partie 5 : Exemple d’une Attaque contre le chiffrement WPA ou WEP par le réseau câblé

Cette partie peut se faire à plusiuers personnes.

Connectez deux machines physiques sur un hub, puis connectez ce HUB sur un AP. La première machine sera l'attaquant (Hacker), la seconde sera la victime (Alice).

Après avoir activé WPA ou WEP sur l’AP, associez-y vous avec une troisième machine, Bob. Vous pouvez utiliser un Laptop ou un smartphone.



Faites un ping entre Bob et Alice. Capturez les trames depuis la station du hacker.

Joignez une capture d'écran. Pouvez-vous voir ces trames en clair ? Commentez.

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

Est-ce qu'il y aurait eu le même résultat en utilisant un switch au lieu d’un HUB ? Justifiez.

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………

…………………………………………………………………………………………………………