HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Sécurité des réseaux sans fil

Laboratoire 802.11 MAC

A faire en équipes de deux personnes

Professeur
Abraham Rubinstein
abraham.rubinstein@heig-vd.ch

Assistant
Yohan Martini
yohan.martini@heig-vd.ch

Février 2018 – Juin 2018

Pour cette partie pratique, vous devez être capable de :

1. Détecter si un certain client WiFi se trouve à proximité
2. Obtenir une liste des SSIDs annoncés par les clients WiFi présents

Vous allez devoir faire des recherches sur internet pour apprendre à utiliser Scapy et la suite aircrack pour vos manipulations. Il est fortement conseillé d'employer une distribution Kali. Si vous utilisez une VM, il vous faudra une interface WiFi usb, disponible sur demande.

ATTENTION : Pour vos manipulations, il pourrait être important de bien fixer le canal lors de vos captures et vos injections. Si vous en avez besoin, la méthode la plus sure est d'utiliser l'option :

`--channel` de `airodump-ng`

et de garder la fenêtre d'airodump ouverte en permanence pendant que vos scripts tournent ou vos manipulations sont effectuées.

Pour les interfaces Alfa AWUS036ACH (interfaces noires), **il faut activer la compatibilité USB 3.0 sur votre VM**. Il faudra faire les manipulations suivantes pour les configurer en mode monitor (pour les autres interfaces, se renseigner sur Internet) :

Installer le driver (disponible sur Kali. Pour d'autres distributions, il faudra probablement le compiler à partir des sources) :

```
sudo apt-get install realtek-rtl88xxau-dkms
```

Ensuite, pour passer en mode monitor :

Mettre l'interface "down"

```
sudo ip link set wlan0 down
```

#Configurer le mode monitor

```
sudo iwconfig wlan0 mode monitor
```

A la fin de cette procédure, vous aurez une interface « wlan0 » en mode monitor (et non pas wlan0mon comme c'est souvent le cas avec d'autres interfaces).

Si vous devez compiler le driver :

```
git clone https://github.com/astsam/rtl8812au.git
cd rtl8812au
make
sudo make install
```

1 Détecter si un ou plusieurs clients 802.11 spécifiques sont à portée

Il peut être utile de détecter si certains utilisateurs se trouve dans les parages. Pensez, par exemple, au cas d'un incendie dans un bâtiment. On pourrait dresser une liste des dispositifs et la contraster avec les personnes qui ont déjà quitté le lieu.

La détection de client s'utilise également à des fins de recherche de marketing. Aux Etats Unis, par exemple, on sniffe dans les couloirs de centres commerciaux pour détecter, par exemple, quelles vitrines attirent plus de visiteurs, et quelle marque de téléphone ils utilisent. Ce service, interconnecté en réseau, peut aussi déterminer si un client visite plusieurs centres commerciaux un même jour ou sur un certain intervalle de temps.

ATTENTION : Le suivi de clients iPhone n'est plus possible depuis la version 8 d'iOS.

a) Développer un script en Python/Scapy capable de capturer les trames nécessaires pour la détection de clients 802.11. Le script se lance en ligne de commandes avec comme argument une adresse MAC d'un certain client. Le script surveille ensuite les messages capturés et imprime une confirmation quand l'adresse est détectée.

Question : quel type de trames sont nécessaires pour détecter les clients de manière passive ?

Question : pourquoi le suivi n'est-il plus possible sur iPhone depuis iOS 8 ?

2 Clients WiFi bavards

a) Utilisant le script que vous venez de développer comme base, faire les modifications nécessaires pour capturer les noms de réseau annoncés par les différents clients se trouvant à portée de votre scanner.

Vous pouvez afficher les noms des réseaux avec les adresses MAC correspondantes au fur et à mesure qu'ils sont capturés mais vous devez garder une trace de quels noms correspondent à quel client.

b) Utiliser une ressource online pour déterminer automatiquement la marque du constructeur de l'interface WiFi pour chaque message capturé. Afficher aussi cette information avec chaque ligne imprimée.

Ainsi, à chaque fois que votre client imprime des résultats, il affiche quelque chose comme ceci :

```
00:1B:63:21:10:33 (Apple Inc.) - HEIG-VD, GVA, Lausanne, MonWiFi
00:09:18:10:23:01 (Samsung) - HEIG-VD, Marathon, europa, eduroam
```

Quelques pistes importantes :

- Si vous devez capturer et injecter du trafic, il faudra configurer votre interface 802.11 en mode monitor.
- Python a un mode interactif très utile pour le développement. Il suffit de l'invoquer avec la commande « `python` ». Ensuite, vous pouvez importer Scapy, rc4 et autres et utiliser les commandes directement dans la console (voir script fourni pour plus d'information sur l'importation de modules). En fait, vous pouvez même exécuter tout le script fourni en mode interactif !
- Scapy fonctionne aussi en mode interactif en invoquant la commande « `scapy` ».
- Dans le mode interactif, « nom de variable + <enter> » vous retourne le contenu de la variable.
- Pour visualiser en détail une trame avec Scapy en mode interactif, on utilise la fonction « `show()` ». Par exemple, si vous chargez votre trame dans une variable nommée « `arp` », vous pouvez visualiser tous ces champs et ses valeurs avec la commande « `arp.show()` ». Utilisez cette commande pour connaître les champs disponibles et les formats de chaque champ.
- Pour obtenir les informations du constructeur de la MAC, vous pouvez vous servir du site `http://macvendors.co/api/xx:xx:xx:xx:xx:xx`

Livrables

Un fichier zip

- SWI18-Labo1-Dupont-Dubois.zip (**merci de respecter le nommage**)

contenant :

- Script de détection de clients 802.11 **abondamment commenté/documenté**
- Script de détection et affichage de SSID **abondamment commenté/documenté**
- Réponses aux éventuelles questions posées dans la donnée dans un README
- A envoyer par email au professeur et à l'assistant

Échéance

Le 16 mars 2018 à 18h00