SWI - Laboratoire 2

Julien Huguet & Antoine Hunkeler

16 mars 2020

Task 1

Comment ça se fait que ces trames puissent être lues par tout le monde ? Ne serait-il pas plus judicieux de les chiffrer ?

Le nom du SSID et l'adresse MAC contenus dans la trame du Probe Request ne sont pas chiffrés, car ces informations doivent être visibles par tous les points d'accès autour de la station.

Il serait à notre avis trop long de négocier une technique de chiffrement entre la station émettrice et tous les points d'accès aux alentours lors de l'envoi de la Probe Request en broadcast.

Oui, il est plus judicieux de les chiffrer afin de ne pas attaquer une station avec un sniffer, mais ces informations doivent être lisibles par tous les points d'accès comme cité plus haut.

Il est aussi possible de tracer les stations avec les probes requests.

Pourquoi les dispositifs iOS et Android récents ne peuvent-ils plus être tracés avec cette méthode ?

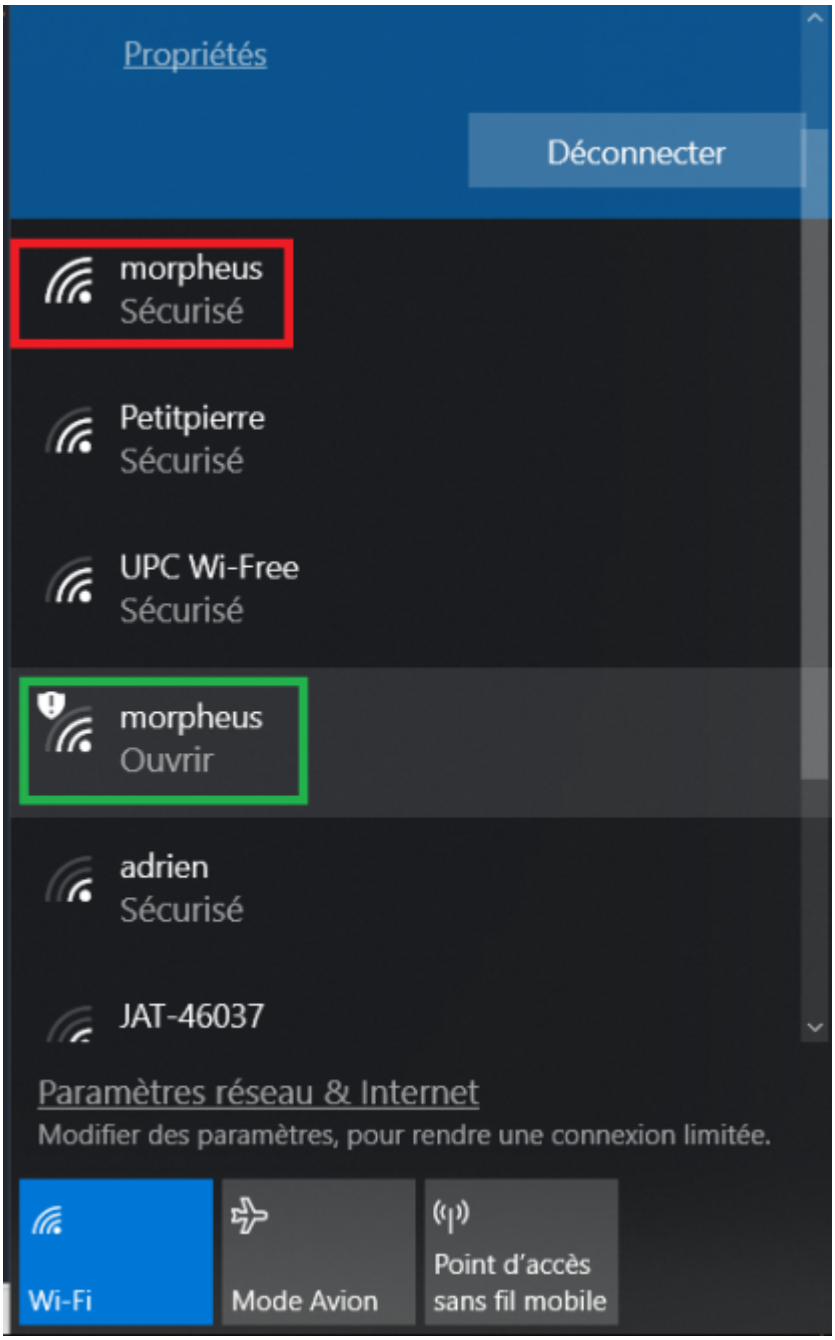
Les versions récentes de Android et iOS utilisent la technique d'envoyer dans les probes requests des adresses MAC aléatoires, ce qui permet d'éviter à ces dispositifs mobiles d'être tracés.

Fonctionnement du script

La capture ci-dessous montre le scan des SSIDs alentours et les affiche sous forme de liste. L'utilisateur après avoir stoppé le scan entre le numéro du SSID trouvé.

```
kali@kali:~/Desktop/SWI/Laboratoires/Lab02$ sudo ./task1_swi.py
| Num Target : 1 | SSID : morpheus | Channel : 4 | Intensity : -37 |
^CPlease select the num target : 1
```

Ensuite, le script envoie des trames beacon afin d'avoir un nouveau point d'accès dans la liste sous un canal différent.



Task 2

Fonctionnement du script

Un premier script (`task2_ap_swi.py`) qui reprend le script du laboratoire 1 qui génère un SSID à partir d'une liste dans un fichier ou encore que l'utilisateur spécifie le nombre de SSIDs à génerer pour que le script génère des noms aléatoires.

Ensuite, le deuxième script (`task2_sta_swi.py`) sniffe les trames Probe Response pour détecter les stations associés aux faux SSIDs et dresse une liste avec les adresses MAC des stations avec les adresses MAC des points d'accès dont elles sont associées.

Par manque de temps et de connaissances, nous n'avons pas pu implémenter la phase d'authentification et d'association avec une station et un faux SSID, mais nous avons déjà implémenter les scripts pour le fonctionnement de base.

Task 3

Expliquer en quelques mots la solution que vous avez trouvée pour ce problème ?

Un réseau caché envoie dans ces trames beacon un SSID vide, ce qui correspond à un "hidden network".

le script sniffe simplement toutes les trames beacon reçues et filtre ceux dont le champ SSID est vide et affiche un message d'avertissement et stocker l'adresse du point d'accès dans une liste.

Pour afficher un SSID, la fonction teste que si le paquet est une Probe Response et l'adresse du point d'accès venant de ce Hidden SSID est présent dans la liste, il affiche le SSID et l'adresse du point d'accès.

Pour des raisons techniques, nous n'avons pas pu tester le script.