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

Sécurité des réseaux sans fil

Laboratoire WPA2 Entreprise

hostapd-wpe

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

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

Février 2018 – Juin 2018

Objectif :

1. Analyser les étapes d'une connexion WPA Entreprise avec une capture Wireshark
2. Implémenter une attaque WPE (Wireless Pwnage Edition) contre un réseau WPA Entreprise

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 : Il est **particulièrement important pour ce laboratoire** 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.

1 Capture et analyse d'une authentification WPA Entreprise

Dans cette première partie, vous allez capturer une connexion WPA Entreprise au réseau de l'école avec Wireshark et fournir des captures d'écran indiquant dans chaque capture les données demandées.

a) Identifier le canal utilisé par l'AP dont la puissance est la plus élevée. Vous pouvez faire ceci avec airodump-ng, par exemple
b) Lancer une capture avec Wireshark
c) Etablir une connexion depuis un poste de travail (PC), un smartphone ou une tablette. Attention, il est important que la connexion se fasse à 2.4 GHz pour pouvoir sniffer avec les interfaces Alfa. Vous pouvez utiliser une même interface Alfa pour vous connecter au réseau et sniffer en même temps
d) Comparer votre capture au processus d'authentification expliqué en classe (n'oubliez pas les captures !). En particulier, identifier les étapes suivantes :
    a. Requête et réponse d'authentification système ouvert
    b. Requête et réponse d'association
    c. Sélection de la méthode d'authentification
    d. Phase d'initiation. Arrivez-vous à voir l'identité du client ?
    e. Phase hello :
        i. Version TLS
        ii. Suites cryptographiques et méthodes de compression proposées par le client et acceptées par l'AP
        iii. Nonces

iv. Session ID

f. Phase de transmission de certificats
   i. Certificat serveur
   ii. Change cipher spec

g. Authentification interne et transmission de la clé WPA (échange chiffré, vu comme « Application data »)

h. 4 way hadshake

i. Répondez aux questions suivantes :

1. **Quelle ou quelles méthode(s) d'authentification est/sont proposé(s) au client ?**

2. **Quelle méthode d'authentification est utilisée ?**

3. **Lors de l'échange de certificats entre le serveur d'authentification et le client :**

   a. **Le serveur envoie un certificat au client ?**
   b. **Le client envoie un certificat au serveur ?**
   c. **Les deux s'échangent des certificats ?**

2 Attaque WPA Entreprise

Les réseaux utilisant une authentification WPA Entreprise sont considérés aujourd'hui comme étant très surs. En effet, puisque la Master Key utilisée pour la dérivation des clés WPA est générée de manière aléatoire dans le processus d'authentification, les attaques par dictionnaire ou brute-force utilisés sur WPA Personnel ne sont plus applicables.

Il existe pourtant d'autres moyens pour attaquer les réseaux Entreprise, se basant sur une mauvaise configuration d'un client WiFi. En effet, on peut proposer un « evil twin » à la victime pour l'attirer à se connecter à un faux réseau qui nous permette de capturer le processus d'authentification interne. Une attaque par brute-force peut être faite sur cette capture, beaucoup plus vulnérable d'être craquée qu'une clé WPA à 256 bits, car elle est effectuée sur le compte d'un utilisateur.

Pour faire fonctionner cette attaque, il est impératif que la victime soit configurée pour ignorer les problèmes de certificats ou que l'utilisateur accepte un nouveau certificat lors d'une connexion.

Pour implémenter l'attaque :

a) Télécharger et installer `hostapd-wpe`. Lire la documentation du site de l'outil ou d'autres ressource sur Internet pour comprendre son utilisation
b) Modifier la configuration de `hostapd-wpe` pour proposer un réseau semblable au réseau de l'école. Si vous avez des problèmes pour vous connecter, vous pouvez proposer votre propre réseau (par exemple HEIG-VD-Faux)
c) Lancer une capture Wireshark

d) Tenter une connexion au réseau (ne pas utiliser vos identifiants réels)
e) Utiliser un outil de brute-force (`john`, par exemple) pour attaquer le hash capturé (utiliser un mot de passe assez petit pour minimiser le temps)
f) Répondez aux questions suivantes :

4. **Quelles modifications sont nécessaires dans la configuration de hostapd-wpe pour cette attaque ?**

5. **Quel type de hash doit-on indiquer à john pour craquer le handshake ?**

6. **Quelles méthodes d'authentification sont supportées par hostapd-wpe ?**

Quelques détails importants :

- Solution à l'erreur éventuelle « `Could not configure driver mode` » :

```
nmcli nm wifi off (nmcli radio wifi off pour kali 2)
rfkill unblock wlan
```

- Pour pouvoir capturer une authentification complète, il faut se déconnecter d'un réseau et attendre 1 minute (timeout pour que l'AP « oublie » le client)
- Les échanges d'authentification entreprise peuvent être trouvés facilement utilisant le filtre d'affichage « `eap` » dans Wireshark

Livrables

Un fichier zip contenant :

- Captures d'écran + commentaires
- Réponses aux questions

Echéance

Le 22 mai 2018 à 18h00