Laboratoire OSER

Sécurité Wi-Fi

4 décembre 2019

Objectifs

A la fin de ce laboratoire, vous devriez être capables de :

- Découvrir une adresse MAC en analysant des Probe Request
- Déchiffrer une capture protégée avec une clé WEP
- Déchiffrer une capture protégée avec une passphrase WPA

Matériel/Logiciels

- Machine virtuelle Kali Linux
-

Travail demandé

Première partie - Identification d'un dispositif

Pour la première partie de ce laboratoire, nous allons utiliser une capture Wireshark pour essayer de déterminer si une cible se trouvait présente à l'HEIG-VD, lieu où une capture devant être analysée, a été faite.

Nous savons que la cible s'est hébergée à l'hôtel « Black Rain » et qu'elle a aussi visité un Starbucks où elle s'est peut-être servie du Wi-Fi gratuit.

1. Copiez le fichier « coursWLAN-IdentifyTarget.pcap » sur votre machine virtuelle.
2. Analysez la capture avec Wireshark pour déterminer l'adresse MAC du dispositif de la cible (**Indice :** trouvez un filtre qui permet de n'afficher que les Probe Request).

   Dans le rapport, mettez une capture d'écran qui montre le filtre utilisé et les informations que vous avez trouvées qui permettent de déterminer l'adresse MAC. Expliquez en une ou deux phrases ce que sont les Probe Request et à quoi elles servent. Expliquez la capture en quelques phrases et donnez clairement l'adresse MAC trouvée.
3. **Bonus :** Quels autres endroits la cible a-t-elle probablement visité ?

   Listez les endroits et mettez une capture d'écran montrant les informations qui vous ont permis de déterminer que la cible a visité ces endroits. Commentez en quelques mots les informations présentes sur la capture d'écran.

Deuxième partie – Déchiffrer une capture WEP

Nous allons nous servir de l'outil aircrack-ng pour retrouver la clé de chiffrement WEP utilisée pour protéger un réseau dont nous avons une capture avec assez de trafic pour cracker la clé. Une fois la clé récupérée, nous l'utiliserons Wireshark pour rendre la capture lisible.

1. Copiez la capture chiffrée avec WEP « coursWLAN-WEP.cap » sur votre machine virtuelle.

2. Ouvrez la capture avec Wireshark et essayez de lire son contenu. Utilisez des filtres d'affichage de protocoles connus (http, icmp). Quelles trames arrivez-vous à trouver ? A votre avis, pourquoi obtenez-vous ce résultat ?

   Notez la réponse à la première question dans le rapport et illustrez-la avec une capture d'écran. Donner ensuite une réponse en une ou deux phrases à la deuxième question.

3. Utilisez aircrack-ng pour récupérer la clé de chiffrement du réseau WEP. Dans une console, dans le répertoire où vous avez copié aircrack et la capture, utilisez la commande suivante :

   aircrack-ng <nom-du-fichier-capture>

   Mettez une capture d'écran montrant le résultat de cette commande dans le rapport et commentez-la en quelques mots.

4. Maintenant que vous avez la clé WEP, configurez la dans Wireshark afin de déchiffrer le trafic (**Indice :** recherchez l'option protocole dans les préférences de Wireshark).

   Montrez avec le nombre de captures d'écran nécessaires les étapes qui vous ont permis de configurer la clé WEP. Commentez en quelques mots chacune des captures d'écran.

5. Essayez à nouveau de lire le contenu de la capture. Utilisez encore une fois des filtres de protocoles connus (http, icmp). Quelles trames arrivez-vous à trouver ?

   Notez la réponse à cette question dans le rapport et illustrez-la avec une capture d'écran.

6. **Bonus :** Quelles sont les informations d'identification (credentials) de l'authentification basique http contenue dans la capture ?

   Notez la réponse dans le rapport et illustrez-la avec une capture d'écran. Expliquez en quelques mots comment vous avez trouvé ces informations.

Troisième partie – Déchiffrer une capture WPA

Nous allons nous servir de l'outil aircrack-ng et d'un dictionnaire pour retrouver la passphrase utilisée pour protéger un réseau dont nous avons une capture. Une fois la passphrase récupérée, nous l'utiliserons dans Wireshark pour rendre la capture lisible.

1. Copiez le dictionnaire « french_dico.txt » et la capture chiffrée avec WPA « coursWLAN-WPA.cap » sur votre machine virtuelle.
2. Utilisez aircrack-ng en ligne de commande pour cracker la passphrase du réseau WPA. Dans une console, dans le répertoire où vous avez copié la capture WPA et le dictionnaire, utilisez la commande suivante :

   aircrack-ng <nom-du-fichier-capture> -w <nom-du-dictionnaire>

   Mettez une capture d'écran montrant le résultat de cette commande dans le rapport et commentez-la en quelques mots.
3. Ouvrez la capture dans Wireshark et configurez la passphrase WPA afin de déchiffrer le trafic.

   Mettez une ou plusieurs captures d'écran dans le rapport pour la/les étape(s) qui diffèrent de la configuration de clé WEP effectuée dans la partie précédente. Commentez en quelques mots la/les capture(s) d'écran.
4. **Bonus :** Lors de la capture, la cible a fait un « ping » sur un serveur. Arrivez-vous à dire de quel serveur il s'agit (adresse IP et nom de domaine) ?

   Donnez la réponse dans le rapport et illustrez-la avec une ou plusieurs capture(s) d'écran. Expliquez en quelques phrases comment vous avez récupéré ces informations.

Rapport

Un rapport sera écrit par groupe de 4 étudiantes (à définir au début du laboratoire). L'écriture du rapport consiste à remplir les différentes sections du template fourni avec la donnée en tenant compte des différentes indications qui se trouvent dans la donnée. Les explications doivent être faites de la manière la plus claire possible et les exemples doivent être illustrés par des schémas ou des captures d'écran.

Rendu

Le rapport devra être envoyé par mail à lucie.steiner@heig-vd.ch avant le dimanche 22 décembre 2019 à 23h59. Le sujet du mail devra contenir le nom du cours, le numéro du laboratoire et le numéro de groupe.