Examen de Sécurisation des réseaux non-filaires (partie WiFi/EAP – 30min)

Benoît Camredon, Anaïs Gantet

19 janvier 2020

Les documents et notes de cours sont autorisés pour cet examen.

Point de vocabulaire : dans le sujet, il vous sera demandé de réagir tour à tour en tant qu'un membre d'une des équipes suivantes :

- architecte : quelqu'un qui conçoit un réseau de manière sécurisée, connaissant l'ensemble des mesures de sécurisation existantes et leurs enjeux ;
- red team : quelqu'un qui teste la sécurité d'un réseau existant et met en œuvre des attaques lorsque cela est possible ;
- blue team : quelqu'un qui cherche à surveiller et détecter les attaques sur un réseau en place.

Le profil est indiqué au début de chaque question.

1 Questions génériques

1. Quelles sont les différentes sécurisations proposées par les normes 802.11 ? Pour chacune, en donner les principales caractéristiques cryptographiques, les propriétés de sécurité qu'elles assurent, le type de trafic concerné et la couche OSI impliquée.

2 Sécurité du Wi-Fi d'un hôtel

Un hôtel dispose de vieux points d'accès dont la mise à jour date de plus de 10 ans. Voulant s'enquérir de son niveau de sécurité en l'état avant de mettre à jour son parc, le service informatique de l'hôtel faire intervenir une équipe spécialisée pour tester la sécurité du réseau Wi-Fi existant. Les résultats obtenus sont les suivants : les points d'accès sont configurés en WEP, ne supportent que l'algorithme de chiffrement RC4 et sont vulnérables à une RCE (exécution de commandes à distance) connue depuis 8 ans.

1. (red team) Pour illustrer à quel point la confidentialité des échanges peut être compromise en WEP, la red team veut implémenter une preuve de concept permettant de retrouver la clé WEP utilisée par l'hôtel. Comment peut-elle s'y prendre ? Donner les différentes étapes ainsi que les faiblesses du WEP qui permettent de le faire.

2. (architecte) A l'issue de ces tests, quelle(s) recommandation(s) préconiser à l'équipe informatique de l'hôtel pour que la sécurité de son parc Wi-Fi devienne à l'état de l'art ? Plusieurs réponses sont envisageables.
3. (blue team) En attendant la mise en œuvre de ces recommandations, la blue team de l'hôtel souhaite surveiller le réseau Wi-Fi précédemment audité. Elle possède pour cela un ordinateur sous Linux, avec une carte Wi-Fi et un outil de détection maison. Dans quel mode doit-elle configurer sa carte réseau ? Décrire ce qu'est ce mode et ce qu'il permet de faire.

3 Sécurité du Wi-Fi d'une start up

1. (architecte) Une start up de 5 employés veut équiper ses nouveaux locaux de points d'accès Wi-Fi avec un niveau de sécurité maximum. Étant donné le faible nombre d'employés, la solution d'authentification choisie est le WPA-PSK. Quelle précaution doit prendre cette start up au sujet de la PSK qu'elle choisit ? Argumenter, notamment en expliquant le fonctionnement de l'attaque à laquelle elle s'expose si elle ne prend pas cette précaution.
2. (red team) L'attaque contre la PSK nécessite de capturer le 4-way handshake, échange qui se produit à l'établissement de la connexion entre une station et un point d'accès. Que peut faire un attaquant s'il arrive après que la connexion soit déjà établie ? Indiquer notamment quelle faiblesse du 802.11 rend cela possible.
3. (architecte) Quelles années plus tard, le nombre d'employés explose et l'authentification par WPA-PSK n'est plus gérable. L'architecte sécurité propose alors de passer le parc en WPA-EAP. Justifier ce choix, puis expliquer le principe de fonctionnement de l'entité "authenticator" en EAP. Proposer ensuite une méthode par login / mot de passe et une par certificats.