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.

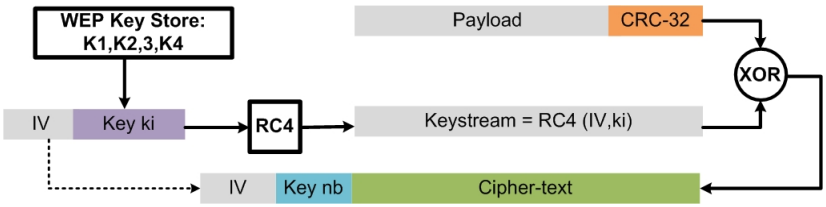

FIGURE 1 – Le protocole WEP.

   (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.

▸ 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 : Le mode *infrastructure*, vers une topologie réseau en étoile

Le mode *infrastructure*, nécessite la présence d'un point d'accès. L'outil *hostapd* permet à Linux de créer un point d'accès Wi-Fi virtuel.

1. Vérifier si votre carte WiFi supporte le mode Master ou AP avec la commande **iw list**
2. Installer l'outil *hostapd* avec la commande **apt-get update && apt-get -y install**
3. Configurer *hostapd* via le fichier de configuration **/etc/hostapd/hostapd.conf** avec les options suivantes :
   — Le nom de l'interface WiFi ;
   — Le driver WiFi **nl80211** qui fonctionne avec la majorité des drivers mac802.11 des cartes WiFi chipset Atheros ;
   — La norme à utiliser est la 802.11g ;
   — Un nom du réseau de votre choix ;
   — Un canal de votre choix ;
   — La diffusion du nom de votre réseau est activée ;
   — Le filtrage par adresses MAC est désactivé ;
   — L'algorithme d'authentification est le WEP ;
4. Lancer le deamon *hostapd* avec la commande **hostapd /etc/hostapd/hostapd.conf**
5. Vérifier la détection de votre point d'accès ainsi que le mode. Si vous utilisez un *network manager*, le logo de ce nouveau point d'accès doit correspondre à un hotspot avec un cadenas.
6. Pour qu'un client puisse se connecter, il lui faut une adresse IP attribuée pat le pont d'accès et une route par défaut pour sortir sur Internet. Installer un serveur DHCP sur le point d'accès par la commande **apt-get install isc-dhcp-server**
7. Configurer l'adresse IP de votre interface WiFi : **ifconfig ...**
8. Dans le fichier **/etc/default/isc-dhcp-server**, indiquer l'interface que *dhcpd* (le démon de isc-dhcp-server) devrait écouter.
9. Éditer le fichier de configuration de DHCP (/etc/dhcp/dhcpd.conf) et effacer toute la configuration. Ajouter les options suivantes en adaptant les adresses IP :

   option domain-name-servers 192.168.x.y ;
   default-lease-time 600 ;
   max-lease-time 7200 ;
   authoritative ;
   log-facility local7 ;
   subnet 192.168.x.0 netmask 255.255.255.0 {
   option routers 192.168.x.y ; option subnet-mask 255.255.255.0 ;
   option broadcast-address 192.168.x.0 ;
   option domain-name-servers 192.168.x.y ;
   range dynamic-bootp 192.168.x.100 192.168.x.200 ;
   }
10. Expliquer la configuration de notre serveur DHCP.
11. Lancer le serveur DHCP avec la commande **dhcpd -d -f -pf /var/run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf &**
12. Connecter un client à votre réseau WiFi et commenter son adresse IP et sa table de routage.
13. Pour communiquer avec la passerelle de la salle TP réseau (172.17.0.1) à partir d'une machine dans votre nouveau réseau, il faut activer le Forwardin et le NAT dans votre point d'accès WiFi.

14. Pour se connecter à Internet en utilisant les noms des domaines, il faut un serveur de cache DNS. Attention notre DNS ne fait que lire le fichier **/etc/resolv.conf** déjà alimenté de serveur par une autre interface ayant Internet. Installer un serveur DNS sur votre point d'accès par la commande **apt-get install dnsmasq**
15. Éditer Le fichier de configuration **/etc/dnsmasq.conf** :

    bogus-priv
    filterwin2k
    interface=wlan0
    no-dhcp-interface=wlan0
16. Expliquer le fichier de configuration.
17. Lancer le *dnmasq* par la commande **dnsmasq -x /var/run/dnsmasq.pid -C /etc/dnsmasq.conf**
18. Vérifier le fonctionnement de votre DNS via la commande **ping www.google.fr** sur un client.
19. Connecter un nouveau client au AP et tracer les trames WiFi échangées.
20. Activer le filtrage MAC et vérifier le fonctionnement.
21. Désactiver la diffusion du SSID et vérifier le résultat.

▸ Exercice 4 : 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 5 : 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), ...