TP - Audit d'un réseau Wi-Fi

Commandes de base Linux :

- On veut changer l'adresse de l'interface eth0 en 192.168.0.252 :

ifconfig 192.168.0.252 (ou # ifconfig eth0 192.168.0.252)

- La commande **iwconfig -a** permet de lister toutes les interfaces sans fils existantes
- La commande **iwconfig wlan0** permet de voir l'état d'une interface (wlan0 par exemple).
- Pour voir l'entourage sans fils actif, on utilise la commande **iwlist scan**.
- Pour Se connecter à une interface sans fil en WEP, on utilise la commande :

iwconfig interface essid SSID key clé_wep

- Pour se connecter à une interface sans fil en WPA, on utilise la commande wpa_supplicant couplée à son fichier de configuration (généralement /etc/wpa_supplicant.conf)

wpa_supplicant –c fichier_de_configuration -Ddriver -iinterface

Analyse du réseau avec Wireshark

Lancez Wireshark dans l'invite commande.

Vérifiez que le menu « Wireless Toolbar » est activé.

Le numéro de canal peut être changé durant la capture. Wireshark peut visualiser les trames sans décryptage si aucune clé n'est précisée, ou avec décryptage en précisant la clé de décryptage dans le menu « Wireless Settings » (la clé doit être entrée en hexa).

Créez un filtre pour afficher toutes les trames sauf les trames Beacon.

Créez un filtre pour n'afficher que les trames de données.

Créez un filtre pour capturer le trafic vers un hôte destination.

Quelles sont les informations portées dans une trame Beacon ?

Identifiez les trames de découverte (Probe Request / Probe Reply).

Identifiez les requêtes d'association et de désassociation (Request/ Response).

Identifiez les trames CTS/RTS.

Aircrack-ng :

La suite aircrack-ng comprend plusieurs programmes dont les 3 principaux sont :

- airodump-ng, le logiciel de capture de paquets, c'est lui qui scan les réseaux et conserve les paquets qui serviront à décrypter la clef.
- aireplay-ng, un logiciel dont la principale fonction est l'envoi de paquets dans le but de stimuler le reseau et capturer plus de paquets.
- aircrack-ng, le logiciel de crack de clef, c'est un logiciel qui à partir des informations capturées à l'aide d'airodump va nous donner la clef.

Backtrack :

Est une distribution spécialisée dans les tests d'intrusion. Il existe bien sur d'autres distributions comme whax ou encore *troppix* (toutes ces distributions sont particulièrement adaptées au cracking wep).

Dans ces distributions, tout est déjà préinstallé : les drivers des cartes wifi et tous les logiciels nécessaires (aireplay, airodump, aircrack, wireshark, kismet ..).

Démarrer avec Backtrack :

1- Bootez sur le live-cd de Backtrack.

2- Le login est root, le mot de passe est toor et pour lancer le mode graphique tapez startx.

3- Puis tapez **"airmon-ng"** pour détecter les interfaces wifi puis sélectionnez celle que vous voulez démarrer avec la commande

airmon-ng start « l'interface wifi »

Le mode monitor permet de capter tous les paquets qui transitent même ceux qui ne vous sont pas adressés. (aussi appelé mode promiscuous). Il est activé automatiquement. Pensez à activer votre carte réseau sans fil si elle ne l'est pas avec la commande :

ifconfig « carte » up

Airodump

Airodump permet de scanner les réseaux wifi :

airodump-ng --write "NomFichierSortie" --channel "NumeroChannel" "Interface"

Pour choisir de scanner tous les canaux ne précisez pas "--channel XX".

La colonne BSSID correspond à l'adresse mac des points d'accès (AP).
La colonne ESSID correspond au nom du réseau.

Pous pouvez limiter le scan à un seul AP en précisant en mettant un filtre :

airodump-ng --write capture_fichier -channel X --bssid adresse-mac-AP Interface

Vous pouvez arrêter la capture avec **Ctrl-C.**

En présence de trafic, les #data augmentent et airodump nous indique dans la colonne **ENC** le cryptage utilisé.

Il faut savoir que pour cracker la clef wep d'un réseau wifi, un minimum de trafic est nécessaire. Nous allons donc usurper l'adresse MAC de la station connectée au point d'accès et ayant généré le trafic afin de pouvoir injecter des trames valides.

Aireplay est un injecteur de paquets qui permet d'accélérer le trafic et surtout de stimuler les **IVs**.

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 metre 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 ?

Connexion au PA

La commande iwconfig Interface permet de visualiser les paramètres de configuration sans fil.

1. La configuration de la carte nécessite le passage en mode *managed* :

iwconfig Interface mode managed

2. La configuration de la clef wep est réalisée par la commande :

iwconfig Interface key xx :xx :xx :xx :xx :xx

3. Si le PA 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 :

ifconfig Interface down

Puis pour changer l'adresse mac :

« ifconfig ath0 hw ether xx :xx :xx :xx :xx :xx

Vous pouvez vous connecter au réseau en activant le DHCP avec la commande :

dhcp interface

Ou changer votre adresse IP selon la plage d'adressage du réseau à l'aide de l'outil de sniffing Wireshark.

Allez dans : Edit/préférences/protocols/IEEE 802.11 (pour ouvrir protocols cliquez sur le petit triangle. Et configurez la clef wep.
Cochez « Assume packets have FCS ».

Allez dans « capture/options », choisissez l'interface, cochez la case (capture paquets in promiscuous mode, cochez la case enable network name resolution.

Pour n'afficher que ceux qui vous intéressent appliquez un filtre dans la case filter un filtre de type « (wlan.bssid == bssid de l'ap) && (TCP).

Annexes

Fields can be combined using operators. Wireshark supports a standard set of comparison operators:

==	for equality	!=	for inequality
>	for greater than	>=	for greater than or equal to
<	for less than	<=	for less than or equal to
&&	Contains	||	Matches
!	Not		

Display Filter Syntax

Hosts/Network	ip.addr, ip.scr, ip.dst, eth.addr, eth.src, eth.dst
Ports	tcp.port, tcp.srcport, tcp.dstport, udp.port, udp.srcport, udp.dstport
Various Protocols	arp, bootp, dcerpc, dns, eth, ftp, http, icmp, ip, ncp, netbios, ntp, ospf, sip, smtp, snmp, tcp, udp
Examples	ip.addr==10.4.2.19
	!ip.addr==10.4.15.27
	!arp && !bootp
	tcp.port==80
	eth.dst==00:04:5a:df:80:37
	tcp.flags.reset==1

802.11 Header Field

Either Source or Destination Address	wlan.addr
Transmitter Address	wlan.ta
Source Address	wlan.sa
Receiver Address	wlan.ra
Destination Address	wlan.da
BSSID	wlan.bssid
Duration	Wlan.duration

Frame Control Subfields

Frame Type	wlan.fc.type
Frame Subtype	wlan.fc.subtype
ToDS Flag	wlan.fc.tods
FromDS Flag	wlan.fc.fromds
Retry Flag	wlan.fc.retry
Protected Frame (WEP) Flag	wlan.fc.wep

Frame Type/Subtype	Filter
Management Frames	wlan.fc.type==0
Association Request	wlan.fc.type_subtype==0
Association Response	wlan.fc.type_subtype==1
Ressociation Request	wlan.fc.type_subtype==2
Ressociation Response	wlan.fc.type_subtype==3
Probe Request	wlan.fc.type_subtype==4
Probe Response	wlan.fc.type_subtype==5
Beacon	wlan.fc.type_subtype==8
ATIM	wlan.fc.type_subtype==9
Disassociate	wlan.fc.type_subtype==10
Authentication	wlan.fc.type_subtype==11
Deauthentication	wlan.fc.type_subtype==12
Association Request	wlan.fc.type_subtype==0
Association Request	wlan.fc.type_subtype==0
Control Frames	wlan.fc.type==1
Power-Save Poll	wlan.fc.type_subtype==26
Request To Send - RTS	wlan.fc.type_subtype==27
Clear To Send - CTS	wlan.fc.type_subtype==28
Acknowledgement - ACK	wlan.fc.type_subtype==29
Data Frmaes	wlan.fc.type==2
NULL Data	wlan.fc.type_subtype==36