TP - Audit d'un réseau Wi-Fi

Objectif

La première partie de ce TP vise à familiariser les étudiants avec les commandes de base pour la configuration et la connexion à un réseau WiFi sous Linux.

La seconde partie vise à réaliser une capture et analyse de trafic sans fil avec Wireshark, et ceci afin de présenter le format de trames, notamment celles concernant la sécurité.

La troisième partie fournit quelques exemples d'attaques sur un réseau sans fil sécurisé avec le protocole WEP sous Kali-Linux.

Commandes de base Linux :

- Lister les cartes sans fil :

  #iwconfig

- Accéder à la configuration des cartes sans fil :

  #ifconfig ou **iwconfig**

- Changer l'adresse de l'interface eth0 en 192.168.0.252 :

  # ifconfig eth0 192.168.0.252 netmask 255.255.255.0

- Si vous disposez d'un serveur DHCP :

  # dhclient eth0

- 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**.
- Activer/ Désactiver une carte sans fil :

  #ifconfig wlan0 up (ou bien **down**)

- Pour activer le mode *managed* ou bien le mode *monitor :*

  #iwconfig wlan0 mode managed (ou bien **monitor**)

- Pour Se connecter à une interface sans fil en WEP, on utilise la commande :

#iwconfig wlan0 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.

Déverouillage de trames cryptées avec Wireshark (en connaiant la clé)

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) par exemple.

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 / Kali-Linux

Est une distribution spécialisée dans les tests d'intrusion. 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 / Kali-Linux :

1- Bootez sur le live-cd.

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**.

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 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 ?

Annexe 1

Format général

EN-TÊTE (7 champs sur 30 octets)

Contrôle de trame 2 octets	Durée/ID 2 octets	Adresse 1 6 octets	Adresse 2 6 octets	Adresse 3 6 octets	Contrôle de séquence 2 octets	Adresse 1 6 octets	Corps de la trame 0-2312 octets	CRC 4 octets

Contrôle de trame (11 sous champs sur 2 octets):

Version du protocole 2 bits	Type 2 bits	Sous-type 4 bits	TO-DS 1 bit	From DS 1 bit	More Frag 1 bit	Retry 1 bit	Pwe Mgmt 1 bit	More Data 1 bit	WEP 1 bit	Order 1 bit

- Version de protocole : toujours à 0
- Type et sous type : représente les 3 sortes de trames et leurs fonctions (2+4 bits)
- To DS et From DS : DS=Distribution Service (point d'accès).
  To DS : (bit à 1) la trame est adressée au point d'accès pour qu'il la fasse suivre.
  From DS (bit à 1) la trame vient du point d'accès.
- More Fragments : à 1 si les données sont fragmentées, à 0 si elles ne sont pas fragmentées ou s'il s'agit du dernier fragment.
- Retry : à 1 s'il s'agit d'une retransmission.
- Power Management : à 1 si la station est en mode d'économie d'énergie, à 0 si elle est active. Venant du point d'accès, les trames sont toujours en mode actif.
- More Data : ce bit est également utilisé pour la gestion de l'énergie. Il est utilisé par le Point d'Accès pour indiquer que d'autres trames sont stockées pour cette station. La station peut alors décider d'utiliser cette information pour demander les autres trames ou pour passer en mode actif (1 bit).
- WEP : ce bit indique que le corps de la trame est chiffré suivant l'algorithme WEP.
- Order : si à 1 cela indique que la trame est envoyée en utilisant une classe de service strictement ordonnée. Ne permet pas à la station d'envoyer des trames en multicast.

Durée/ID (2 octets) :

Ce champ a deux sens, dépendant du type de trame : pour les trames de polling en mode d'économie d'énergie, c'est l'ID de la station ou AID (Association IDentity). Dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV.

Trames de contrôle

- RTS (Request To Send) est utilisé pour réclamer le droit de transmettre une trame de données.

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	TA 6 octets	CRC 4 octets

  - RA est l'adresse du récepteur destinataire de la prochaine trame de données ou de gestion.
  - TA est l'adresse de la station qui transmet la trame RTS.

- CTS (Clear To Send) correspond à la réservation du canal pour émettre une trame de données

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	CRC 4 octets

  - RA correspond à l'adresse de la station source (champ TA) de la trame RTS.

- ACK permet l'acquittement des trames de données

Contrôl de trame 2 octets	Durée 2 octets	RA 6 octets	CRC 4 octets

  - RA correspond à l'adresse de la station source, qui provient du champ adresse 2 de la trame de données ou de gestion précédente.

Trames de gestion

Il existe quatre familles de trames de gestion :

- Trames liées aux fonctions d'association-désassociation
- Trames d'interrogation du voisinage radio
- Trames liées aux fonctions d'authentification
- Trames balises, utilisées par le point d'accès pour diffuser des informations dans le BSS.

Annexe 2

Les champs de trames peuvent être combinés dans un même filtre, vous pouvez utiliser les opérateurs suivants :

==	Egalité	!	Négation
< ou >	Inférieur ou supérieur à	!=	Inégalité
<	Inférieur à	>= ou <=	Supérieur ou égal inférieur ou égal
&&	contient	||	correspondance

Syntaxe des filtres d'affichage

Hots/Network	ip.addr, ip.src, ip.dst, eth.addr, eth.dst
ports	tcp.port, tcp.srcport, tcp.dstport, udp.port, udp.srcport, udp.dstport
protocoles	arp, bootp, dns, ftp, http, ip, ….
Exemples	ip.addr==10.0.0.1 !ip.addr==10.4.9.1 tcp.port==80 eth.dst==00 :04 :1F :2C :04 :10

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