Récapitulatif tcpdump

Scanner le trafic réseau globale.

```
tcpdump -n
-n = ne pas resoudre les noms (surtout si acces DNS coupé)
```

→ vision du reseau cache 192.168.0.1

Scan et sauvegarde du scan dans un fichier.

```
tcpdump -n -w /root/infos.dump
-w = ecrire dans le fichier
Ctrl+C pour arrêter la capture.
```

Lire le fichier scanné (c'est là qu'il faut mettre l'option -n parce que c'est à ce moment qu'il va essayer de résoudre les noms).

```
tcpdump -n -r /root/infos.dump
-r = lire le fichier
```

ATTENTION le fichier est un binaire, il n'est donc pas lisible avec vi ou cat.

Recherche dans le fichier des requêtes ARP “who-has”

```
tcpdump -n -r /root/infos.dump arp[6:2]==1
```

Ensuite on fait des filtres dessus. ether[X]==1 arp[X]==1

[6:2] Ca veut dire on se positionne sur le 6ème octet et on lit les 2 octets qui suivent dans la trame ARP. Si cette valeur est 1 c'est qu'on est en présence d'un who-has.

Il faut trouver la liste des IP qui font du who-has.

```
tcpdump -n arp -w /root/arpinfo.dump
tcpdump -n -r /root/arpinfo.dump | cut -d ' ' -f 6
```

ou avec awk

```
tcpdump -n -r /root/arpinfo.dump | awk '{print$6}'
```

On récupère d'abord les trames avec -w dans un fichier et ur extraire des infos.

```
tcpdump -n arp[6:2]==1 -r /root/arpinfo.dump | cut -d ' ' -f 6 | sort | uniq
```

On récupère d'abord les trames avec -w dans un fichier et ensuite on fait des filtres dessus pour extraire des infos.

```
tcpdump -n arp[6:2]==1 -r /root/arpinfo.dump | cut -d ' ' -f 6 | sort | uniq
```

Installation de l'outil de recherche ARP.

```
apt-get install arpwatch
```

Recherche dans le fichier de scann de l'adresse MAC correspondante à l'adresse IP spécifiée.

```
arpwatch -d -f /root/arpinfo.dump -n 192.168.0.1
```

On obtient : 0:19:b9:5b:68:a8

http://www.frameip.com → Entrer dans le champ pour connaître le constructeur.

Nombre de requêtes ARP réalisées par les machines du réseau (les adresses IP du réseau).

```
tcpdump -l -n arp | grep 'arp who-has' | head -100 | awk '{print $NF }' |
sort | uniq -c | sort -n
```

Scan sur une seule interface.

```
tcpdump -n -i eth2
```

Filtrage sur le réseau.

```
tcpdump -i eth0 -vv src net <@IP> mask <mask>
```

Filtrage sur un hôte.

```
tcpdump -i eth0 -vv host <@IP>
```

Filtrage sur un hôte sans convertir les IP en noms.

```
tcpdump -nni eth0 -vv host <@IP>
```

Exclusion d'un port.

```
tcpdump -i eth0 not port 22
```

Filtrage sur l'host et exclusion du port.

```
tcpdump -nni eth0 -vv host <@IP> and not port 22
```

Filtrage sur port et host.

```
tcpdump -ni eth0 -vv port 20 and host <@IP>
```