tcpdump

tcpdump est un analyseur de paquets en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau. L'outil sous GNU/Linux, *BSD et Mac OS X dépend de la bibliothèque logicielle **libpcap**.

www.tcpdump.org

La bibliothèque logicielle **libpcap** est à l'origine développée pour l'outil tcpdump mais peut être utilisée par tous les analyseurs de paquets. Elle fournit en effet une interface de programmation pour de tels programmes leur permettant de capturer et d'analyser n'importe quel paquet à partir d'un périphérique réseau. Le portage sous Windows est connu sous les appellations **WinPCAP/WinDUMP**.

---

https://www.tcpdump.org/manpages/tcpdump.1.html

Lister les interfaces disponibles :

```
$ tcpdump -D
1.enp4s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up,
Running]
3.lo [Up, Running, Loopback]
 ...
```

Les options principales :

-i nom_interface : permet de choisir l'interface d'écoute
-v : permet d'afficher encore plus d'informations sur les paquets. Il y a trois niveaux de verbosité : **-v, -vv, -vvv**
-e : affiche l'en-tête de niveau Liaison (par exemple Ethernet_II et IEEE 802.11)
-n : ne pas convertir les adresses (hôte, les numéros de port, etc.) en noms
-t : n'affiche pas l'horodatage sur chaque ligne
-XX : affiche en hexadécimal et ASCII

Ce qui donne les commandes de base suivantes :

```
$ sudo tcpdump -tne -XX -i interface
```

```
$ sudo tcpdump -tne -XX -vvv -i interface
```

https://www.tcpdump.org/manpages/pcap-filter.7.html

tcpdump dispose d'un **filtre** puissant des paquets nommés BPF (***BSD packet filter***). Il est possible de combiner les règles avec : and (**&**) et/ou or (**|**) et not (**!**).

On utilisera principalement **hote**, **port**, les **protocoles** (ip, icmp, arp, tcp etc.) et les **adresses src/dst**.

```
$ sudo tcpdump src 192.168.1.100 and dst 192.168.1.2 and port ftp
```