TCPdump

réseau, outils, tcpdump

Pour afficher les interfaces disponibles

```
sudo tcpdump -D
```

Pour écouter sur une interface en particulier

```
sudo tcpdump -i eth0
```

Pour afficher les paquets capturés en hexa et ascii

```
sudo tcpdump -XX -i eth0
```

Pour enregistrer les paquets capturés dans un fichier

```
sudo tcpdump -w capture.pcap -i eth0
```

Pour lire le fichier de traffic capturé

```
sudo tcpdump -r capture.pcap
```

Pour capturer les addresses IP

```
sudo tcpdump -n -i eth0
```

Capturer uniquement les paquets TCP

```
sudo tcpdump -i eth0 tcp
```

Écouter depuis un port particulier

```
sudo tcpdump -i eth0 port 443
```

Capturer le traffic depuis une IP source

```
sudo tcpdump -i eth0 src 192.168.1.1
```

Capturer le traffic depuis une IP de destination

```
tcpdump -i eth0 dst 192.168.1.5
```

Liens

- 11 exemples avec la commande Tcpdump pour débugger son réseau