Fiche technologique TCPDump : capturer et analyser le trafic réseau sur Linux

Ressources

Lien : https://www.malekal.com/tcpdump-capturer-des-paquets-reseaux-sur-linux/

Prrésentation

Tcpdump est un utilitaire de ligne de commande qui vous permet de capturer et d'analyser le trafic réseau passant par une interface réseau.

Installer TCPDump

```
$ sudo apt-get install tcpdump
```

Options

Flag	Description
-i <interface>	Ecouter une interface réseau spécifique, .e.g. "-i igb0"
-n	N'effectuez pas de résolution DNS inversée sur les adresses IP
-w <filename>	Enregistrez la capture au format pcap dans <nom de fichier>, par exemple "-W /tmp/wan.pcap"
-s	Durée de capture: quantité de données à capturer à partir de chaque image
-c <packets>	Quitter après avoir reçu un nombre spécifique de paquets
-p	Ne mettez pas l'interface en mode promiscuité
-v	Mode Verbose (bavard)
-e	Imprimer l'en-tête de la couche de liaison sur chaque ligne

exemple de commandes

- Lister les interfaces réseaux : <code shell> sudo tcmpdump -D </code>