Les ports

Définition

Un **port** est un point de communication logique que les ordinateurs utilisent pour distinguer différents services réseau. Quand une machine envoie ou reçoit des données sur un réseau, elle combine son **adresse IP** (qui identifie l'appareil) et un numéro de **port** (qui identifie le service ou l'application).

Exemple :

- Adresse IP : **192.168.1.10**
- Port : **80**

Ce qui signifie que la communication est établie avec l'application qui écoute sur le port **80** de la machine ayant l'adresse **192.168.1.10**

Types de Ports : TCP et UDP

TCP (TRANSMISSION CONTROL PROTOCOL)

- **Fiable** : Assure que les données arrivent intactes et dans le bon ordre.
- **Connexion** : Nécessite un processus d'établissement de connexion (3-way handshake).
- **Utilisations courantes** : HTTP (80), HTTPS (443), FTP (21), SSH (22).

UDP (USER DATAGRAM PROTOCOL)

- **Non fiable** : Pas de garantie de livraison des paquets.
- **Sans connexion** : Moins de surcharge, donc plus rapide pour les transmissions en temps réel.
- **Utilisations courantes** : DNS (53), DHCP (67/68), VoIP, streaming.

Les Plages de Ports

Il existe **65 536 ports** possibles (numérotés de 0 à 65535), répartis en **trois catégories** :

PLAGE DE PORTS	NUMÉROS	DESCRIPTION
PORTS BIEN CONNUS (WELL-KNOWN)	0 À 1023	RÉSERVÉS POUR LES SERVICES STANDARDS (HTTP, FTP, SSH).
PORTS ENREGISTRÉS	1024 À 49151	ASSIGNÉS À DES APPLICATIONS UTILISATEUR SPÉCIFIQUES.
PORTS DYNAMIQUES OU PRIVÉS	49152 À 65535	UTILISÉS TEMPORAIREMENT POUR DES CONNEXIONS CLIENT.

Ports Courants et Leurs Utilisations

Voici une liste des **ports** les plus utilisés et leurs services associés :

PORT	PROTOCOLE	SERVICE
22	TCP	SSH (SECURE SHELL)
25	TCP	SMTP (SIMPLE MAIL TRANSFER PROTOCOL)
53	UDP/TCP	DNS (DOMAIN NAME SYSTEM)
80	TCP	HTTP (WEB)
443	TCP	HTTPS (WEB SÉCURISÉ)

Comment Fonctionnent les Ports ?

PROCESSUS DE COMMUNICATION

Lorsqu'un ordinateur souhaite communiquer avec un autre appareil sur le réseau :

1. **Ouverture d'un port** : L'application (ex. navigateur web) ouvre un port source sur le client.
2. **Connexion au serveur** : Le client envoie une requête à l'adresse IP du serveur via un port de destination (ex. 80 pour HTTP).
3. **Réponse** : Le serveur répond via le même port de destination, et la communication est établie.

EXEMPLE DE CONNEXION TCP : 3-WAY HANDSHAKE

- **SYN** : Le client envoie une requête de synchronisation (SYN) au serveur.
- **SYN-ACK** : Le serveur répond avec une synchronisation + accusé de réception (SYN-ACK).
- **ACK** : Le client envoie un accusé de réception (ACK), et la connexion est établie.

Comment Voir les Ports Utilisés ?

SUR WINDOWS

`netstat -an`

- `-a` : Affiche toutes **les connexions** et **ports d'écoute**.
- `-n` Affiche les **adresses IP** et **ports** sous forme numérique.

SUR LINUX

`sudo netstat -tuln`

- `-t` : Affiche les connexions **TCP**.
- `-u` : Affiche les connexions **UDP**.
- `-l` : Affiche uniquement les **ports en écoute**.
- `-n` : Affiche les **adresses numériques**.

Qu'est-ce qu'un Scan de Ports ?

Un **scan de ports** est une technique pour identifier les ports ouverts sur une machine afin de déterminer quels services sont actifs sur un réseau.

SCAN ACTIF

Envoie des requêtes directes à une machine pour **identifier** les ports ouverts, ce qui peut être détecté par les systèmes de sécurité.

Outil : `nmap`

Commande : `nmap -p -65535 -A <adresse IP>`

- `-p` : Spécifie la plage de **ports**.
- `-A` : Active la **détection avancée** (services, versions, OS).

SCAN PASSIF

Analyse le trafic réseau existant **sans envoyer de requêtes**, permettant une collecte discrète d'informations sur les ports ouverts.

Outil : `Wireshark` `Zeek`

Le **scan actif** est **illégal** si vous scannez des systèmes sans autorisation tandis que le **scan passif** est **illégal** que si vous interceptez et analysez le trafic réseau d'autrui sans leur permission.