

Découvrir des services avec **NMap**





Qu'est-ce que **Nmap** ?

- ◉ Scanner réseau le plus **populaire**
- ◉ Découvrir des hôtes ou des **services**
- ◉ Interface graphique : *Zenmap*
- ◉ Documentation importante



Commandes basiques de **NMap**

- `nmap -sP <IP>` (ping)
- `nmap -sS <IP>` (TCP SYN)
- `nmap -sV <IP>` (ports ouverts et versions des services)
- `nmap -sL <IP>` (liste les cibles)
- `nmap -p 80 <IP>` (spécifie un port)
- `nmap IP > scan.txt`



États de ports reconnus par **NMap**

- **ouvert** (service actif)
- **fermé** (pas de service)
- **filtré** (bloqué)
- **non-filtré** (?)



Autres options de **NMap**

- `nmap -v <IP>`
- `nmap -A <IP>`
- `nmap -6 <IPv6>`
- `nmap -sC <IP> (NSE)`



Alternatives ou compléments

- SuperScan (enumeration)
- AutoScan



Différents types de scans

- ◉ **Ping Sweep** : identifier les machines qui répondent sur le réseau
- ◉ **Scan de port** : quels services ?
- ◉ **Network mapping** : carte du réseau
- ◉ **OS Fingerprinting** : quels systèmes d'exploitation sont utilisés ?



Aspects juridiques

- ◉ Scan non autorisé par défaut
- ◉ Peut faire réagir des **systèmes de détection d'intrusion**



Se protéger du Scanning Réseau

- Utiliser un pare-feu (ufw)
- Désactiver ou bloquer des ports
- Utiliser des IDS