Commandes Nmap (une ligne)

1. **Scan SYN (TCP) rapide**

```
sudo nmap -sS -Pn -oN nmap_tcp_syn.txt 10.0.2.15
```

2. **Scan UDP (top 20 ports)**

```
sudo nmap -sU -Pn --top-ports 20 -oN nmap_udp_top20.txt 10.0.2.15
```

3. **Scan versions services & détection OS**

```
sudo nmap -sV -O -Pn -oN nmap_version_os.txt 10.0.2.15
```

4. **Scan de tous les ports TCP (1–65535)**

```
sudo nmap -p- -sS -Pn -oN nmap_tcp_all_ports.txt 10.0.2.15
```

5. **Scan avec scripts NSE par défaut + version**

```
sudo nmap -sC -sV -Pn -oN nmap_scripts.txt 10.0.2.15
```

Décomposition des arguments & justification

-sS

- `-s` : sélection du type de scan
- `S` : SYN scan (envoie un SYN sans compléter la connexion TCP)
- **Justification** : rapide, furtif, souvent non détecté par les systèmes de logs.

-sU

- `-s` : sélection du type de scan
- `U` : scan UDP
- **Justification** : détecte les services UDP (ex : DNS, SNMP), souvent ignorés.

-sV

- `-s` : sélection du type de scan
- `V` : détection des versions des services
- **Justification** : permet d'identifier précisément les versions pour cibler des vulnérabilités.

-sC

- `-s` : sélection du type de scan
- `C` : lance les scripts NSE de la catégorie « default »
- **Justification** : effectue des vérifications automatiques utiles pour la reconnaissance.

-O

- Active la détection du système d'exploitation (OS fingerprinting)
- **Justification** : connaître l'OS cible aide à orienter les attaques.

-p-

- Scanne tous les ports TCP (1 à 65535)
- **Justification** : ne pas manquer un service sur un port non standard.

-Pn

- Ne pas faire de ping préalable (pas de découverte d'hôte par ICMP ou ARP)
- **Justification** : utile si la cible bloque les pings, évite les faux négatifs.

--top-ports 20

- Scanne uniquement les 20 ports les plus courants (TCP ou UDP)
- **Justification** : accélère le scan UDP qui est naturellement lent.

-oN <fichier>

- Sortie normale (format texte lisible) dans un fichier
- **Justification** : garder un historique clair des résultats.

sudo

- Nécessaire pour certains types de scans (SYN, UDP, détection OS) qui demandent les droits root.

Autres options utiles

-T<0-5>

```
sudo nmap -sS -Pn -T4 10.0.2.15
```

- T0 = très lent et discret, T5 = très rapide mais bruyant + risque de perte de données

- Justification : T4 est un bon compromis vitesse/précision sur un réseau local

--reason

```
sudo nmap -sS -Pn --reason 10.0.2.15
```

- Explique la raison pour laquelle il pense qu'un port est dans un certain état (open, closed, filtered, etc.).
- Justification : utile pour comprendre la logique de Nmap

-v, -vv, -d, -dd

```
sudo nmap -sS -Pn -v -d 10.0.2.15
```

- -v, -vv : niveaux de verbosité
- -d, -dd : niveau de debug
- Justification : pour analyser les comportements anormaux ou les blocages

-A

```
sudo nmap -A -Pn 10.0.2.15
```

- Combine : -sC, -sV, -O, --traceroute
- Justification : reconnaissance complète rapide
- ⚠️ **Attention** : bruyant, à éviter sur des cibles sensibles

-oX, -oG, -oA

```
sudo nmap -sS -Pn -oA scan_result 10.0.2.15
```

- -oX : XML
- -oG : Grepable
- -oA : Tous les formats (.nmap, .xml, .gnmap)

-iL

```
sudo nmap -sS -Pn -iL targets.txt -oA multi_scan
```

- Permet de scanner plusieurs cibles définies dans un fichier

Bonnes pratiques après les scans

Nettoyage

```
rm -f *.xml *.nmap *.gnmap *.txt
```

- Évite l'encombrement avec des fichiers temporaires

Organisation

- Regrouper les scans par dossier : reconnaissance/, vulnérabilités/, etc.

Stratégie recommandée

> 1. Lancer un scan TCP SYN rapide (`-sS -Pn`).
> 2. Poursuivre par un scan UDP limité aux 20 ports principaux (`-sU --top-ports 20`).
> 3. Faire un scan avec détection des versions et OS (`-sV -O`).
> 4. Si besoin, scanner tous les ports TCP (`-p- -sS`).
> 5. Terminer par un scan avec scripts NSE par défaut (`-sC -sV`).