Commandes NMAP

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
```

- **À quoi ça sert ?** Cette option règle la vitesse du scan.

    - `T0` = très lent, très discret (pratique si tu veux rester invisible, mais ça prend beaucoup de temps)
    - `T5` = très rapide, mais ça fait du bruit sur le réseau (tu risques d'être détecté et même de perdre des paquets)
- **Pourquoi utiliser `-T4` ?** C'est un bon compromis : rapide sans trop faire de bruit, surtout sur un réseau local.

`--reason`

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

- **À quoi ça sert ?** Cette option indique pourquoi Nmap a classé un port comme ouvert, fermé ou filtré.
    - Exemple : "Port 80 ouvert parce que Nmap a reçu un paquet SYN/ACK"
- **Pourquoi c'est utile ?** Ça t'aide à comprendre la logique derrière le résultat, surtout si tu veux analyser ou vérifier le scan.

`-v, -vv, -d, -dd`

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

- **À quoi ça sert ?** Ce sont des niveaux d'information que Nmap affiche pendant le scan :
    - `-v` ou `-vv` = verbosité : plus il y a de v, plus Nmap détaille ce qu'il fait
    - `-d` ou `-dd` = debug : montre encore plus de détails techniques (utile si ça bloque ou plante)
- **Pourquoi c'est utile ?** Pour surveiller ce qui se passe en temps réel, comprendre des erreurs, ou analyser un comportement étrange.

`-A`

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

- **À quoi ça sert ?** C'est un scan complet qui combine plusieurs options :
    - `-sC` : lance des scripts de reconnaissance simples
    - `-sV` : détecte les versions des services
    - `-O` : détecte le système d'exploitation
    - `--traceroute` : trace le chemin réseau vers la cible

- **Pourquoi c'est utile ?** Pour faire une reconnaissance approfondie rapide, et avoir un maximum d'informations sur la cible.
- **Attention !** Ce scan est bruyant, donc il peut être détecté facilement. À éviter sur des systèmes sensibles ou en production.

`-oX, -oG, -oA`

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

- **À quoi ça sert ?** Ces options permettent d'enregistrer les résultats du scan dans des fichiers, pour les analyser plus tard :
  - `-oX` : format XML (utile pour des outils qui lisent ce format)
  - `-oG` : format "grepable" (texte simple, facile à filtrer avec grep)
  - `-oA` : enregistre dans tous les formats d'un coup (.nmap, .xml, .gnmap)
- **Pourquoi c'est utile ?** Pour garder une trace des scans, faire des rapports, ou automatiser des analyses.

`-iL`

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

- **À quoi ça sert ?** Permet de scanner plusieurs adresses IP ou hôtes listés dans un fichier texte (targets.txt).
- **Pourquoi c'est utile ?** Quand tu dois scanner beaucoup de cibles, tu évites de taper chaque IP manuellement.

Bonnes pratiques après les scans

Nettoyage

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

- **Pourquoi ?** Après un ou plusieurs scans, Nmap peut créer beaucoup de fichiers (résultats en XML, en texte, etc.). Ces fichiers peuvent vite s'accumuler et encombrer ton dossier de travail.
- **Ce que fait cette commande** Elle supprime tous les fichiers qui ont ces extensions (fichiers de résultats Nmap et fichiers texte), pour garder ton espace propre.

- **Important** Fais attention à ne pas supprimer des fichiers importants par erreur. Si tu veux garder certains résultats, déplace-les avant de lancer cette commande.

Organisation

- **Pourquoi organiser ?** Quand tu fais beaucoup de scans différents (reconnaissance, détection de vulnérabilités, audits, etc.), ça devient difficile de retrouver les résultats.
- **Conseil** Crée des dossiers avec des noms clairs pour chaque type de scan :
    - reconnaissance/ pour les scans de découverte réseau
    - vulnerabilites/ pour les scans de failles de sécurité
    - etc.
- **Avantage** Ça facilite la gestion, la consultation, et le partage des résultats.

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`).