# Réseau

- [Énumération/Réseau] Nmap
- [Énumération/Réseau] SNMP
- [Énumération/Réseau] DNS
- [Énumération/Réseau] Zmap

# [Énumération/Réseau] Nmap

# Introduction

**Nmap** est certainement le plus grand outil d'énumération réseau au monde.

Il permet de découvrir un réseau ou de scanner des ports et même de chercher des vulnérabilités.

Il est incontournable pour les professionnels de la cybersécurité.




# Manuel

## Syntaxe globale

```
nmap [OPTIONS] <IP>
```

## Découverte du réseau

```
nmap -sn <IP>/<MASK>
```

## Scan d'un port

```
nmap -p <PORT> <IP>
```

## Scan d'une plage de ports

```
nmap -p <FIRST_PORT>-<LAST_PORT> <IP>
```

## Scan des 1000 ports les plus populaires

```
nmap -F <IP>
```

## Scan avancé

```
nmap -A <IP>
```

> L'option -A regroupe les options -O, -sV et exécute certains scripts NSE pour chercher des services et des vulnérabilités.

## Scan UDP

```
nmap -sU <IP>
```

> Vous pouvez aussi utiliser l'option -p pour ne scanner qu'un ou une plage de ports.

## Scan rapide

```
nmap -T4 <IP>
```

## Scan discret

```
nmap -T1 <IP>
```

> Le scan sera beaucoup plus lent qu'un scan habituel.

## Autres options

| Options | Fonctions |
| --- | --- |

| | |
|---|---|
| -v | Mode verbeux |
| -n | Désactive la résolution DNS |
| -g <SRC_PORT> | Permet de spécifier un port source de la connexion |
| -oN <OUTPUT_FILE> | Sauvegarde la sortie dans un fichier |
| -oX <OUTPUT_FILE> | Sauvegarde la sortie dans un fichier au format XML |
| --exclude <FILE> | Exclue les IP contenues dans le fichier lors du scan |
| --stats-every <TIME> | Affiche les statistiques du scan en temps réel |
| --script <DEFAULT\|SCRIPT> | Exécute le script spécifié ou tous les scripts si default est indiqué |

# Scripts

L'ensemble des scripts fournis par nmap sont disponibles dans le dossier **/usr/share/nmap/scripts** .

# Projet dashboard grafana

Voici un projet que je trouve intéressant pour intégrer des graphiques de vos scans nmap dans vos rapports de pentest :

- https://github.com/hackertarget/nmap-did-what

Tout d'abord clonez le dépôt :

```
git clone https://github.com/hackertarget/nmap-did-what
```

Ensuite lancez votre scan nmap avec un fichier d'export au format XML avec l'option **-oX** :

```
nmap -sC -sV -Pn -n <IP> -oX scan.xml
```

Injectez les données récupérées dans la base de données du projet :

```
cd nmap-did-what && cp scan.xml /data/ && python3 nmap-to-sqlite.py scan.xml && cd ..
```

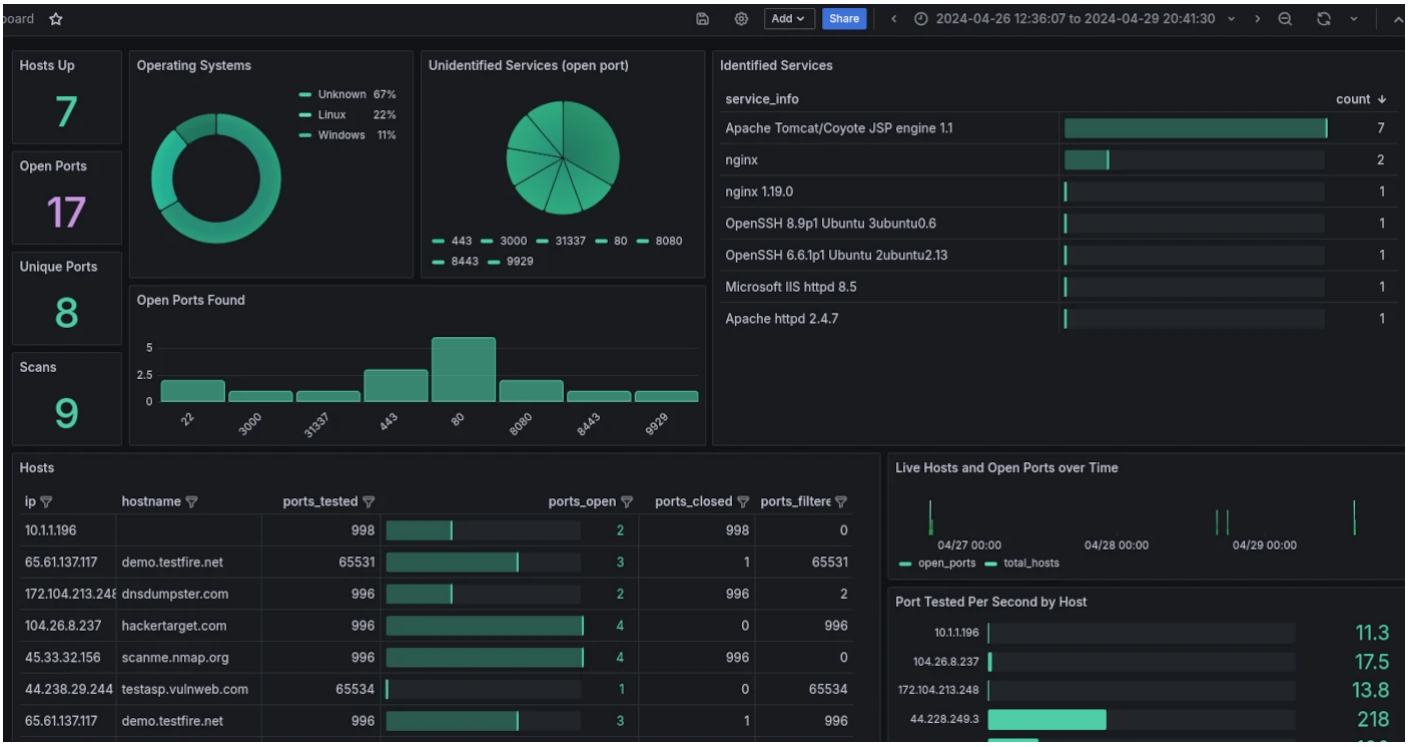
Lancez la stack docker :

```
cd grafana-docker/ && docker compose up -d && cd ..
```

Rendez-vous sur l'interface Grafana :

- https://localhost:3000

Depuis le menu **Dashboard**, retrouvez ces graphiques préconfigurés :



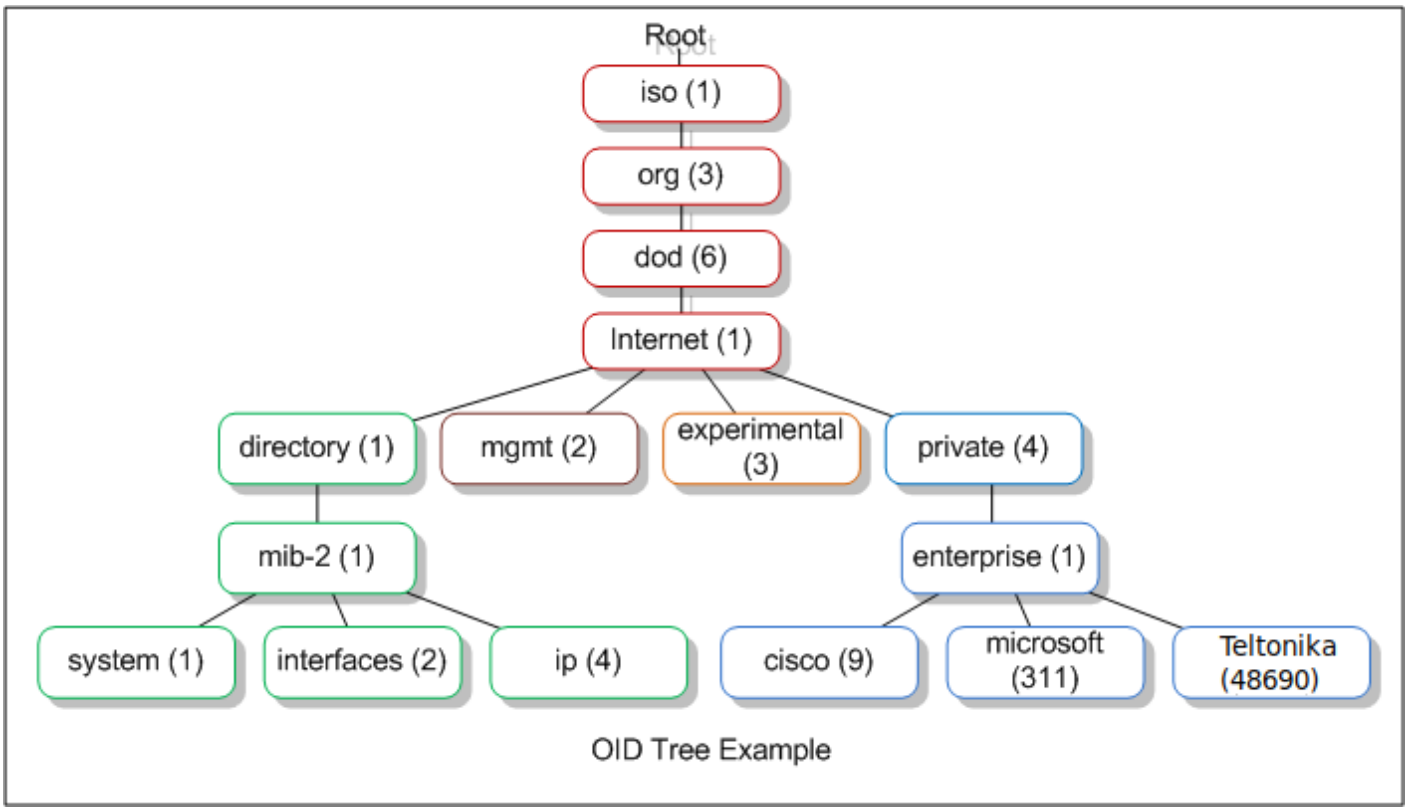
# [Énumération/Réseau] SNMP

## Introduction

Le protocole **SNMP** pour *Simple Network Management Protocol* permet de gérer les ressources sur un réseau.

Il existe des agents SNMP (installés sur les hôtes réseaux) et des managers SNMP qui sont capables de récupérer des informations identifiées par un OID, sur les agents.

Par défaut, il utilise le port **161**.




## Composition de l'OID

Pour identifier les objets, on utilise ce qu'on appelle un **OID** qui est formé selon l'arbre ci-dessus.

Par exemple, pour obtenir l'OID de l'ip, on parcours l'arbre du haut vers le bas en mettant un point entre chaque numéro, ce qui donnerait : **1.3.6.1.1.1.4** .

# Les versions de SNMP

## Communautés SNMP

Le terme de "communauté" fait référence à la méthode d'authentification utilisé dans les SNMPv1 et SNMPv2c.

Il existe deux types de communauté :

- **Communauté "publique" (public) :** Offre un accès en lecture seule aux informations de l'agent.
- **Communauté "privée" (private) :** Permet un accès en lecture et en écriture, permettant de modifier la configuration de l'agent.

## SNMPv3

Contrairement aux anciennes versions du protocole, SNMPv3 introduit un modèle de sécurité plus avancé, offrant des fonctionnalités telles que l'authentification, la confidentialité et le contrôle d'accès de manière plus robuste. Il n'utilise pas de communautés, mais des mécanismes d'authentification et de chiffrement plus sophistiqués pour assurer la sécurité des données échangées entre le gestionnaire et les agents.

# SNMPget

## Syntaxe globale

```
snmpget [OPTIONS] <TARGET_IP> <OID>
```

## Exemples d'utilisation

- Interroger un agent pour obtenir une information spécifique :

```
snmpget -v2c -c community 192.168.1.1 1.3.6.1.2.1.1.1.0
```

- Utiliser SNMP v3 avec des informations d'identification :

```
snmpget -v3 -u username -l authPriv -a MD5 -A authpass -x DES -X privpass 192.168.1.1
1.3.6.1.2.1.1.1.0
```

- Récupérer des informations à partir d'une cible nommée plutôt que son IP :

```
snmpget -v2c -c public -n mytarget 1.3.6.1.2.1.1.1.0
```

# Options courantes

| Options | Descriptions |
| --- | --- |
| -v[X] | Spécifie la version SNMP (X peut être 1, 2c ou 3). |
| -c | Spécifie la communauté SNMP (uniquement pour SNMP v1 et v2c). |
| -u | Spécifie l'identifiant d'utilisateur (uniquement pour SNMP v3). |
| -l | Spécifie le niveau de sécurité (SNMP v3). |
| -a | Spécifie l'algorithme d'authentification (SNMP v3) |
| -x | Spécifie l'algorithme de chiffrement (SNMP v3). |
| -A | Spécifie le mot de passe d'authentification (SNMP v3). |
| -X | Spécifie le mot de passe de chiffrement (SNMP v3). |
| -n | Nomme la cible en utilisant un nom au lieu d'une adresse IP. |

# [Énumération/Réseau] DNS

# Introduction

Il existe plusieurs outils qui permettent d'énumérer un serveur DNS car ce dernier est souvent le point d'entrée des attaquants et regorge d'informations utiles sur les sous-domaines, les serveurs de messageries ou les adresses IP utilisés par la cible.




# Dig

Certainement l'outil le plus connu pour énumérer les serveurs DNS, il est très puissant et possède de nombreuses options.

## Utilisation standard

```
dig <FQDN>
```

## Énumération des serveurs de messagerie

```
dig <FQDN> -t mx +short
```

# Host

Cette commande va énumérer tous les serveurs se trouvant derrière le nom de domaine indiqué :

```
host <FQDN>
```

# DNSenum

## Installation

```
sudo apt install -y dnsenum
```

## Manuel

```
dnsenum <FQDN>
```

> Vous pouvez utiliser l'option **--noreverse** pour ne pas lancer la procédure de reverse lookup sur les IP trouvées.

# [Énumération/Réseau] Zmap

## Introduction

**Zmap** est un outil qui permet de scanner très rapidement toute ou une partie de plage IPv4 d'Internet pour savoir lesquelles ont un ou plusieurs ports ouverts.



## Installation

```
sudo apt update && sudo apt install -y zmap
```

## Manuel

### Syntaxe globale

```
sudo zmap -p <PORT> -o <FILE> <TARGET_IP>
```

### Exemples d'utilisation

- Scanner tout internet sur le port 80 :

```
sudo zmap -p 80 -o scan_port_80_results.txt 0.0.0.0/0
```

- Balayer une plage d'IP sur plusieurs ports :

```
sudo zmap -p 22,80,443 -o scan_result.json 192.168.1.0/24
```

- Limiter l'utilisation de la bande passante :

```
sudo zmap -p 3389 -o rdp_results.csv -B 5M 10.0.0.0/16
```

# Options courantes

| Options | Descriptions |
|---|---|
| -p <PORT> | Spécifie le numéro de port à balayer. |
| -o <FILE> | Spécifie le fichier de sortie pour enregistrer les résultats. |
| -B <BYTES> | Limite la bande passante utilisée (par exemple, "-B 10M" pour limiter à 10 Mbps). |
| -f <FORMAT> | Spécifie le format de sortie (par exemple, **json** ou **csv**). |
| -q | Mode silencieux (supprime les avertissements) |
| -N | Définit le nombre de threads à utiliser pour le balayage. |