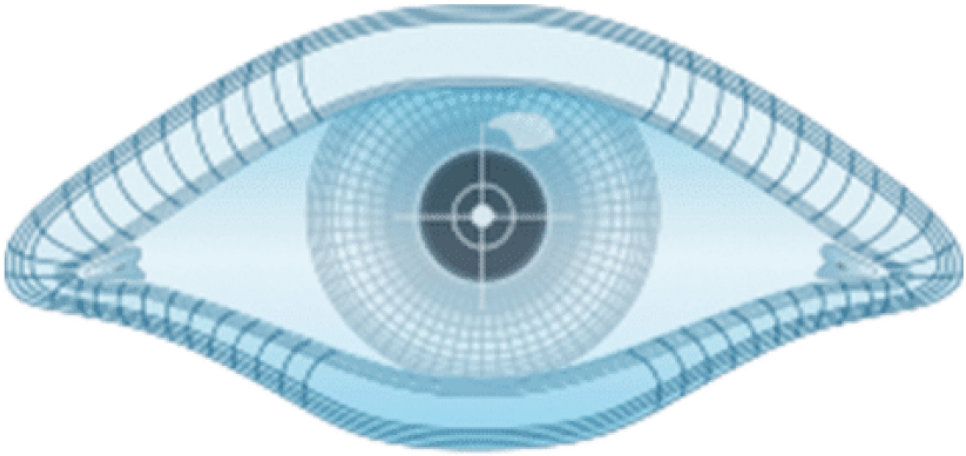
# [Énumération/Réseau] Nmap

# 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 ..
```

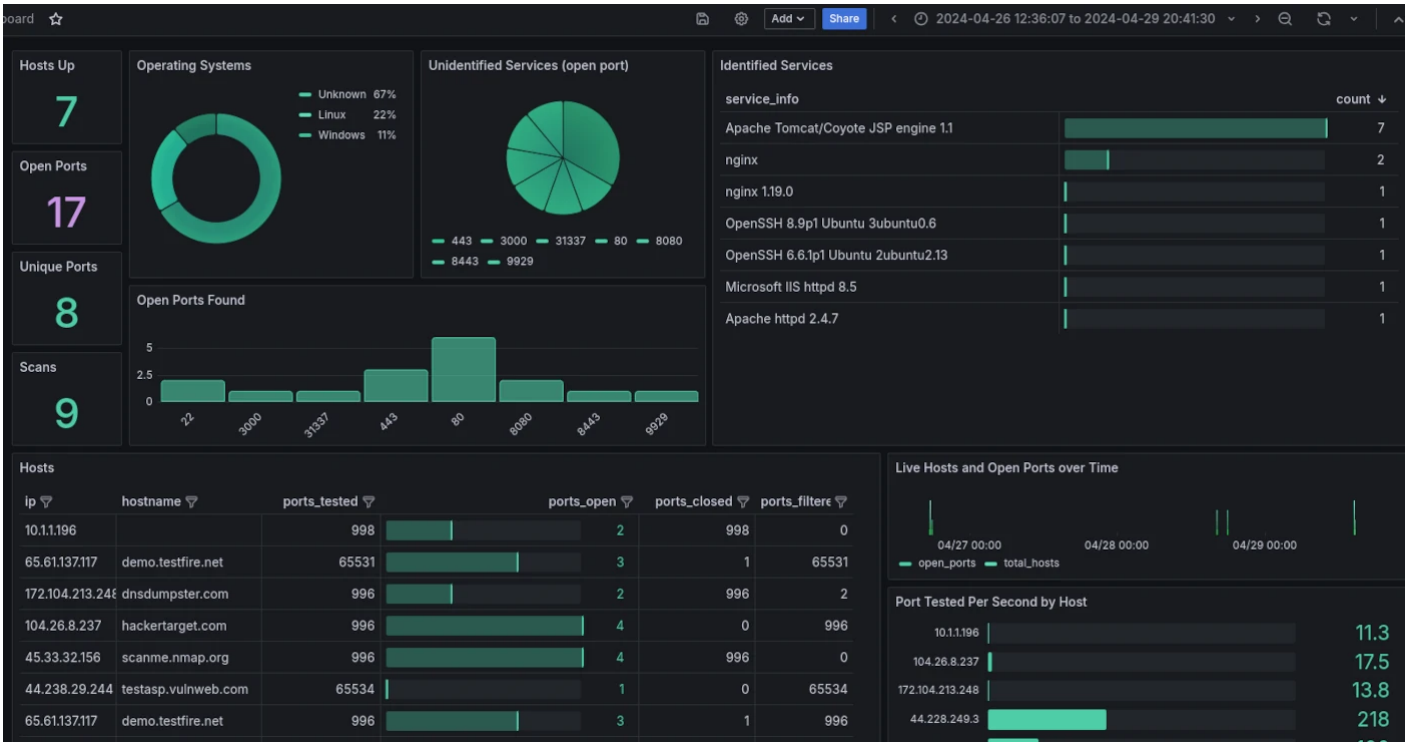
Lancez la stack docker :

```
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 :




---

Revision #14
Created 2023-10-12 19:15:26 UTC by Elieroc
Updated 2024-10-03 06:33:41 UTC by Elieroc