Nmap - Scan réseau

Le scan réseau permet d'identifier les machines sensibles (serveurs par ex) puis de lancer un scan de vulnérabilités sur celles-ci

- Scan **simple** (l'option **-T4** permet de paramétrer le timeout de chaque scan afin que nmap ne tourne pas éternellement) :

```
sudo nmap -T4 -sn 192.168.1.0/24
```

- Scan détaillé (**OS, ports, services**) :

```
sudo nmap -T4 -O -A 192.168.1.0/24
```

- Scan détaillé avec **rapport** :

```
sudo nmap -T4 -A 192.168.1.0/24 -oA inventaire_reseau
```

1. inventaire_reseau.**nmap** → lisible en texte brut
2. inventaire_reseau.**xml** → pour outils d'analyse ou XML viewer (le fichier XML peut être lu avec **Zenmap**)
3. inventaire_reseau.**gnmap** → format "grepable"

Analyse

- Dans **Zenmap** importer le fichier **xml**
- Puis dans **Topology** analyser les points **jaune** et **rouge** principalement
- Exporter la carte au format **SVG**