■ SDV Toolbox - Rapport de Sécurité

Outil:	Nmap
Date:	07/06/2025 à 14:22:13
Cible:	10.8.0.1
Opérateur:	SDV Security Team

■ Rapport de Scan Réseau Nmap

■ PORTS CRITIQUES OUVERTS DÉTECTÉS

Métrique	Valeur
■ Cible scannée	10.8.0.1
■ Type de scan	rapide
■ Ports ouverts	2
■■ Ports critiques	1
■ Ports fermés	1
■■ Services détectés	2
■ Date du scan	07/06/2025 à 14:22:13

■ Ports ouverts détectés :

Port	Protocole	Service	Version	Risque
443	tcp	ssl/http	Apache httpd 2.4.63 ((Debian))	ÉLEVÉ
5000	tcp	http	Werkzeug httpd 3.1.3 (Python 3...	FAIBLE

■■ Services identifiés :

Service	Occurrences	Ports associés
ssl/http	1	443
http	1	5000

■ Informations système :

Propriété	Valeur
Latence	0.0000080s

■ Extrait du scan technique :

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 14:21 EDT
Nmap scan report for 10.8.0.1
Host is up (0.0000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
443/tcp open ssl/http Apache httpd 2.4.63 ((Debian))
5000/tcp open http Werkzeug httpd 3.1.3 (Python 3.13.3)
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.87 seconds
```

■■ Recommandations de sécurité réseau :

- ■ CRITIQUE : Des ports à haut risque sont ouverts
- Fermez les ports non nécessaires (Telnet, FTP, NetBIOS, SMB)
- Renforcez l'authentification sur les services exposés
- ■ HTTP détecté - Migrez vers HTTPS avec certificats valides
- ■■ Configurez un pare-feu pour filtrer le trafic entrant
- ■ Surveillez régulièrement les ports ouverts avec Nmap
- ■ Effectuez des scans périodiques pour détecter les changements
- ■ Formez les équipes aux bonnes pratiques de sécurité réseau
- ■ Documentez et justifiez chaque port ouvert
- ■ Implémentez une surveillance réseau continue (SIEM)
- ■ Mettez à jour régulièrement les services exposés