■ SDV Toolbox - Rapport de Sécurité

Outil:	Nmap
Date:	07/06/2025 à 16:40:52
Cible:	192.168.236.133
Opérateur:	SDV Security Team

■ Rapport de Scan Réseau Nmap

■ PORTS CRITIQUES OUVERTS DÉTECTÉS

Métrique	Valeur
■ Cible scannée	192.168.236.133
■ Type de scan	complet
■ Ports ouverts	2
■■ Ports critiques	2
■ Ports fermés	1
■■ Services détectés	2
■ Date du scan	07/06/2025 à 16:40:52

■ Ports ouverts détectés :

Port	Protocole	Service	Version	Risque
21	tcp	ftp	vsftpd 3.0.5	CRITIQUE
22	tcp	ssh	OpenSSH 9.9p1 Debian 3 (protoc	ÉLEVÉ

■■ Services identifiés :

Service	Occurrences	Ports associés
ftp	1	21
ssh	1	22

■ Informations système :

Propriété	Valeur
Latence	0.00038s
Adresse MAC	00:0C:29:AF:91:A8
Type appareil	general purpose
OS	Linux 4.X|5.X
Distance réseau	1 hop

■ Extrait du scan technique :

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-07 16:40 CEST
Nmap scan report for 192.168.236.133
Host is up (0.00038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.5
22/tcp open ssh OpenSSH 9.9p1 Debian 3 (protocol 2.0)
| ssh-hostkey:
| 256 60:5d:cd:12:5e:04:41:61:e3:b5:14:a4:1a:7c:12:26 (ECDSA)
|_ 256 41:fd:4c:33:fe:52:18:8e:01:6b:4a:35:8a:59:b5:ea (ED25519)
MAC Address: 00:0C:29:AF:91:A8 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.38 ms 192.168.236.133

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.90 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

• ■ SSH détecté - Utilisez l'authentification par clés et désactivez root

• ■ FTP détecté - Remplacez par SFTP ou FTPS

• ■■ 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