🔎 Rapport de scan Nmap – Ports TCP complets

IP cible : 10.0.10.2
Date : 25 mai 2025
Commande : `nmap -p- -sS -Pn -oN nmap_tcp_all_ports.txt 10.0.10.2`
Durée du scan : 13.76 secondes
Hôte actif : Oui (latence 0.000049s)

🔐 Ports TCP ouverts détectés

Port	Service
21/tcp	ftp
22/tcp	ssh
23/tcp	telnet
25/tcp	smtp
53/tcp	domain
80/tcp	http
111/tcp	rpcbind
139/tcp	netbios-ssn
445/tcp	microsoft-ds
512/tcp	exec
513/tcp	login
514/tcp	shell
1099/tcp	rmiregistry
1524/tcp	ingreslock
2049/tcp	nfs
2121/tcp	ccproxy-ftp
3306/tcp	mysql
3632/tcp	distccd
5432/tcp	postgresql
5900/tcp	vnc
6000/tcp	X11
6667/tcp	irc

Port	Service
6697/tcp	ircs-u
8009/tcp	ajp13
8180/tcp	unknown
8787/tcp	msgsrvr
50385/tcp	unknown
51924/tcp	unknown
52639/tcp	unknown
52677/tcp	unknown

🧠 Informations supplémentaires

- **MAC address :** `08:00:27:32:E4:1F` (VirtualBox NIC)

✅ Recommandations

- Corréler ces résultats avec un scan `-sV` pour identifier les versions.
- Fermer les ports inutilisés si ce n'est pas un environnement de test.
- Surveiller les services inconnus ou inhabituels (`unknown`).
- Ne jamais exposer ce type de machine directement sur Internet.

> ⚠️ **Note** : Ce scan montre tous les ports TCP ouverts, sans détection de version. Un scan complémentaire est nécessaire pour approfondir les risques potentiels.