🔎 Rapport de scan Nmap – Metasploitable2 (Scan SYN TCP)

IP cible : 10.0.10.2
Date : 25 mai 2025
Commande : `nmap -sS -Pn --reason -oN nmap_tcp_syn.txt 10.0.10.2`
Durée du scan : 13.19 secondes
Hôte actif : Oui (réponse ARP)

🔐 Ports ouverts détectés

Port	Service	Raison
21/tcp	FTP	syn-ack ttl 64
22/tcp	SSH	syn-ack ttl 64
23/tcp	Telnet	syn-ack ttl 64
25/tcp	SMTP	syn-ack ttl 64
53/tcp	DNS	syn-ack ttl 64
80/tcp	HTTP	syn-ack ttl 64
111/tcp	RPCBind	syn-ack ttl 64
139/tcp	NetBIOS-SSN	syn-ack ttl 64
445/tcp	SMB	syn-ack ttl 64
512/tcp	Rexec	syn-ack ttl 64
513/tcp	Login	syn-ack ttl 64
514/tcp	Shell	syn-ack ttl 64
1099/tcp	Java RMI	syn-ack ttl 64
1524/tcp	Ingreslock	syn-ack ttl 64
2049/tcp	NFS	syn-ack ttl 64
2121/tcp	FTP (alt)	syn-ack ttl 64
3306/tcp	MySQL	syn-ack ttl 64
5432/tcp	PostgreSQL	syn-ack ttl 64
5900/tcp	VNC	syn-ack ttl 64
6000/tcp	X11	syn-ack ttl 64
6667/tcp	IRC	syn-ack ttl 64

Port	Service	Raison
8009/tcp	AJP13	syn-ack ttl 64
8180/tcp	HTTP Alt	syn-ack ttl 64

🧠 Informations systèmes

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

✅ Remarques

- Ce scan SYN (stealth scan) permet une détection discrète des ports ouverts sans établir de connexion complète.
- La machine cible présente une surface d'attaque très large, typique de Metasploitable2.
- Pour une évaluation de la sécurité, combiner ce scan avec un scan de version (`-sV`) et de scripts (`-sC`).

> ⚠️ **Note** : Cette machine est volontairement vulnérable pour des tests en environnement contrôlé.