



# Rapport de scan Nmap – Metasploitable2

**IP cible :** 10.0.10.2

**Date :** 25 mai 2025

**Commande :** `nmap -A --reason -oN nmap_all.txt 10.0.10.2`

**Durée du scan :** 142 secondes

**Hôte actif :** Oui (ARP response)

**OS détecté :** Linux 2.6.9 – 2.6.33

**Nom d'hôte :** metasploitable.localdomain



## Ports ouverts détectés

Port	Service	Version / Info
21/tcp	FTP	vsftpd 2.3.4 (Anonyme autorisé)
22/tcp	SSH	OpenSSH 4.7p1 Debian
23/tcp	Telnet	Linux telnetd
25/tcp	SMTP	Postfix smtpd
53/tcp	DNS	ISC BIND 9.4.2
80/tcp	HTTP	Apache 2.2.8 (Ubuntu)
111/tcp	RPCBind	RPC services NFS, mountd, etc.
139/tcp	NetBIOS-SSN	Samba smbd (WORKGROUP)
445/tcp	SMB	Samba smbd 3.0.20
512–514	RSH/Login	Netkit
1099/tcp	Java RMI	GNU Classpath
1524/tcp	Backdoor	Metasploitable root shell
2049/tcp	NFS	NFS over TCP
2121/tcp	FTP	ProFTPD 1.3.1
3306/tcp	MySQL	MySQL 5.0.51a
5432/tcp	PostgreSQL	PostgreSQL 8.3.X
5900/tcp	VNC	Protocol 3.3
6000/tcp	X11	Access denied
6667/tcp	IRC	UnrealIRCd
8009/tcp	AJP13	Apache JServ

Port	Service	Version / Info
8180/tcp	HTTP	Apache Tomcat/Coyote JSP engine 1.1

## Informations systèmes


- **MAC address :** 08:00:27:32:E4:1F (VirtualBox NIC)
- **Distance réseau :** 1 saut
- **Certificat SSL (port 5432) :**
  - Valide de : 2010-03-17 à 2010-04-16
- **Heure système :** 2025-05-25T11:15:03-04:00

## Vulnérabilités potentielles

- **FTP anonyme activé** sur port 21 → Possibilité d'accès libre.
- **Telnet (port 23)** en clair → Risque d'interception.
- **SMB v1 (port 445)** activé → Risque EternalBlue.
- **RSH & Login (ports 512–514)** non sécurisés.
- **Java RMI (1099)** → Souvent vulnérable à la désérialisation.
- **Shell bind (1524)** → backdoor volontaire pour test.
- **Tomcat (8180)** avec gestion JSP accessible → Vulnérable sans authentification forte.

## Recommandations

- Fermer les ports inutilisés.
- Remplacer ou désactiver les services en clair (telnet, rsh).
- Restreindre l'accès aux services critiques via pare-feu.
- Mettre à jour les versions logicielles si environnement réel.
- Ne jamais exposer ce type de machine en production.

 **Note :** Metasploitable est une machine volontairement vulnérable. Ce rapport ne reflète pas des erreurs de configuration mais un environnement de test.