

Rapport de scan Nmap – Metasploitable2 (Scan de versions et OS)

IP cible : 10.0.10.2

Date : 25 mai 2025

Commande : `nmap -sV -O -Pn -oN nmap_version_os.txt 10.0.10.2`

Durée du scan : 66.79 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
22/tcp	SSH	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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) DAV/2
111/tcp	RPCBind	RPC 2 (portmapper)
139/tcp	NetBIOS-SSN	Samba smbd 3.X - 4.X (WORKGROUP)
445/tcp	SMB	Samba smbd 3.X - 4.X (WORKGROUP)
512/tcp	RSH	netkit-rsh rexecd
513/tcp	Login	Inconnu (réponse partielle)
514/tcp	RSH	Netkit rshd
1099/tcp	Java RMI	GNU Classpath grmiregistry
1524/tcp	Backdoor	Metasploitable root shell
2049/tcp	NFS	Version 2 à 4
2121/tcp	FTP	ProFTPD 1.3.1
3306/tcp	MySQL	MySQL 5.0.51a-3ubuntu5
5432/tcp	PostgreSQL	PostgreSQL 8.3.0 à 8.3.7
5900/tcp	VNC	Protocole 3.3

Port	Service	Version / Info
6000/tcp	X11	Accès refusé
6667/tcp	IRC	UnrealIRCd
8009/tcp	AJP13	Apache JServ v1.3
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
- **Type de machine** : Usage général (générique)
- **Détails OS** : Linux kernel 2.6.9 à 2.6.33
- **Infos services** :
 - Hôtes : **metasploitable.localdomain, irc.Metasploitable.LAN**
 - OS : Unix, Linux

Vulnérabilités potentielles

- **vsftpd 2.3.4** → vulnérable à une backdoor connue (CVEs publiques).
- **FTP anonyme (à vérifier manuellement)**.
- **Telnet (port 23)** → Communication en clair.
- **RSH/Login (512, 513, 514)** → Protocole non chiffré.
- **Java RMI (1099)** → Problèmes de désérialisation fréquents.
- **Shell backdoor (1524)** → accès root non sécurisé.
- **Vieux services Samba (ports 139, 445)** → Exposition à EternalBlue / SambaCry.
- **X11 (6000)** → Accès réseau ouvert, même si "Access Denied".

Recommandations

- Désactiver tous les services inutilisés.
- Supprimer les protocoles en clair (Telnet, RSH).
- Restreindre les accès par un pare-feu.
- Mettre à jour tous les services exposés si hors environnement de test.
- Ne jamais exposer cette machine à Internet sans isolation.

 **Note** : Ce système est volontairement vulnérable (Metasploitable2) et destiné à des tests de sécurité. Ce rapport ne reflète pas des mauvaises configurations réelles mais des vulnérabilités intentionnelles.