🔎 Rapport de scan Nmap – Metasploitable2

IP cible : 10.0.10.2
Date : 25 mai 2025
Commande : `nmap -sC -sV -Pn -oN nmap_scripts.txt 10.0.10.2`
Durée du scan : 140 secondes
Hôte actif : Oui (latence : 0.000043s)
OS détecté : Linux (probablement 2.6.x)
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, nlockmgr, etc.)
139/tcp	NetBIOS-SSN	Samba smbd (3.X – 4.X, WORKGROUP)
445/tcp	SMB	Samba smbd 3.0.20-Debian
512–514	RSH/Login	Netkit (rsh, login, rexecd)
1099/tcp	Java RMI	GNU Classpath
1524/tcp	Backdoor	Metasploitable root shell (bindshell)
2049/tcp	NFS	NFS v2–v4
2121/tcp	FTP	ProFTPD 1.3.1
3306/tcp	MySQL	MySQL 5.0.51a
5432/tcp	PostgreSQL	PostgreSQL 8.3.X
5900/tcp	VNC	VNC Protocol 3.3
6000/tcp	X11	Access denied
6667/tcp	IRC	UnrealIRCd
8009/tcp	AJP13	Apache JServ Protocol v1.3

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 – PCS Systemtechnik)
- **Distance réseau :** 1 saut
- **Certificat SSL (PostgreSQL, port 5432)** :
  - **Sujet :** ubuntu804-base.localdomain
  - **Organisation :** OCOSA
  - **Valide de :** 17/03/2010 au 16/04/2010
- **Nom NetBIOS :** METASPLOITABLE
- **Nom de domaine :** localdomain
- **FQDN :** metasploitable.localdomain
- **Heure système :** 2025-05-25T11:04:52-04:00

🛡️ Vulnérabilités potentielles

- **FTP anonyme (port 21)** : accès sans authentification → fuite de données possible.
- **Telnet (port 23)** : communication en clair → interception simple.
- **RSH & rexec (ports 512–514)** : protocoles obsolètes, pas de chiffrement.
- **SMB v1 (port 445)** : vulnérable à EternalBlue et autres exploits.
- **Port 1524 (bindshell)** : backdoor délibérément ouverte pour tests.
- **Java RMI (port 1099)** : vulnérable aux attaques par désérialisation.
- **Tomcat (8180)** : JSP ouvert, souvent utilisé pour déploiements non sécurisés.
- **VNC (port 5900)** : ancien protocole sans authentification forte → peut être contourné.

✅ Recommandations

- **Fermer ou filtrer les ports inutilisés** via un pare-feu.
- **Désactiver les services obsolètes** (telnet, rsh, rexec).
- **Appliquer des contrôles d'accès réseau** (ACLs ou pare-feu local).
- **Changer les services non chiffrés par des alternatives sécurisées** (SSH au lieu de Telnet/RSH).
- **Éviter d'utiliser cette machine sur un réseau ouvert** : environnement volontairement vulnérable.

> ⚠️ **Remarque** : Cette machine est conçue pour l'entraînement à la cybersécurité. Les vulnérabilités listées sont intentionnelles.