



# Rapport de scan Nmap – UDP (Top 20 ports)

**IP cible :** 10.0.10.2

**Date :** 25 mai 2025

**Commande :** `nmap -sU -Pn --top-ports 20 --reason -oN nmap_udp_top20.txt 10.0.10.2`

**Durée du scan :** 30 secondes

**Hôte actif :** Oui (ARP response)



## Ports UDP analysés

Port	État	Service	Raison
53/udp	open	domain	udp-response ttl 64
67/udp	closed	dhcps	port-unreach ttl 64
68/udp	closed	dhcpc	port-unreach ttl 64
69/udp	open	filtered	tftp
123/udp	closed	ntp	port-unreach ttl 64
135/udp	closed	msrpc	port-unreach ttl 64
137/udp	open	netbios-ns	udp-response ttl 64
138/udp	open	filtered	netbios-dgm
139/udp	closed	netbios-ssn	port-unreach ttl 64
161/udp	closed	snmp	port-unreach ttl 64
162/udp	closed	snmptrap	port-unreach ttl 64
445/udp	closed	microsoft-ds	port-unreach ttl 64
500/udp	closed	isakmp	port-unreach ttl 64
514/udp	closed	syslog	port-unreach ttl 64
520/udp	closed	route	port-unreach ttl 64
631/udp	closed	ipp	port-unreach ttl 64
1434/udp	closed	ms-sql-m	port-unreach ttl 64
1900/udp	closed	upnp	port-unreach ttl 64
4500/udp	closed	nat-t-ike	port-unreach ttl 64
49152/udp	closed	unknown	port-unreach ttl 64



## Informations systèmes


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

## Analyse

- **Port 53 (DNS) :** Répond sur UDP, peut indiquer un serveur DNS actif.
  - **Ports 69 (TFTP) et 138 (NetBIOS-DGM) :** état **open|filtered** → pas de réponse, peut être filtré par pare-feu.
  - **Port 137 (NetBIOS-NS) :** ouvert, typique d'un réseau Windows (résolution de nom NetBIOS).
- 

## Recommandations

- Filtrer ou bloquer les ports non utilisés au niveau du pare-feu.
  - Auditer les services DNS et NetBIOS si déployés volontairement.
  - Désactiver les services UDP inutiles sur les environnements en production.
- 

 **Note :** Ce scan UDP est limité aux 20 ports les plus courants. Un scan complet serait recommandé pour une évaluation approfondie.