

■ SDV Toolbox - Rapport de Sécurité

Outil:	Wireshark
Date:	07/06/2025 à 14:13:34
Cible:	eth0 (10 paquets)
Opérateur:	SDV Security Team

■ Analyse de Capture Réseau Wireshark

Paramètre	Valeur
■ Interface	eth0
■ Paquets capturés	10
■ Filtre appliqué	Aucun
■ Date de capture	07/06/2025 à 14:13:34
■ Protocole principal	ICMP
■ Activité détectée	FAIBLE

■ Échantillon des paquets capturés :

#	Temps	Source → Destination	Protocole
1	0.000000s	192.168.236.137 → 8.8.8.8	ICMP
2	0.007585s	8.8.8.8 → 192.168.236.137	ICMP
3	0.232523s	→	ARP
4	0.232647s	→	ARP
5	1.001533s	192.168.236.137 → 8.8.8.8	ICMP
6	1.007916s	8.8.8.8 → 192.168.236.137	ICMP
7	2.002684s	192.168.236.137 → 8.8.8.8	ICMP
8	2.008476s	8.8.8.8 → 192.168.236.137	ICMP
9	3.004804s	192.168.236.137 → 8.8.8.8	ICMP
10	3.008560s	8.8.8.8 → 192.168.236.137	ICMP

■ Recommandations d'analyse réseau :

- ■ Analysez régulièrement le trafic réseau pour détecter les anomalies
- ■ Surveillez les connexions vers des IPs externes inconnues
- ■■ Implémentez une surveillance réseau continue (SIEM)
- ■ Documentez les patterns de trafic normal pour détecter les déviations
- ■ Configurez des alertes pour les protocoles inhabituels
- ■ Effectuez des analyses de trafic périodiques avec Wireshark