

# ■ SDV Toolbox - Rapport de Sécurité

Outil:	Wireshark
Date:	07/06/2025 à 16:44:18
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 16:44:18
■ Protocole principal	ICMP
■ Activité détectée	FAIBLE

### ■ Échantillon des paquets capturés :

#	Temps	Source → Destination	Protocole
1	0.000000s	192.168.236.133 → 8.8.8.8	ICMP
2	0.005615s	8.8.8.8 → 192.168.236.133	ICMP
3	0.112263s	→	UDP/XML
4	0.285870s	192.168.236.1 → 239.255.255.250	UDP/XML
5	0.949165s	→	ARP
6	0.949276s	→	ARP
7	1.001987s	192.168.236.133 → 8.8.8.8	ICMP
8	1.007631s	8.8.8.8 → 192.168.236.133	ICMP
9	2.002750s	192.168.236.133 → 8.8.8.8	ICMP
10	2.008222s	8.8.8.8 → 192.168.236.133	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