■ SDV Toolbox - Rapport de Sécurité

Outil:	Ettercap
Date:	07/06/2025 à 16:29:41
Cible:	192.168.236.133 → 192.168.236.2 via eth0
Opérateur:	SDV Security Team

■ Résultats de Ettercap

```
ATTAQUE MITM ETTERCAP - RAPPORT DE SÉCURITÉ
==========================================

CONFIGURATION D'ATTAQUE:
- Interface réseau: eth0
- IP victime: 192.168.236.133
- IP passerelle: 192.168.236.2
- Mode: RÉEL
- Date: 07/06/2025 à 16:29:41

RÉSULTATS DE L'ATTAQUE:
- Position MITM établie avec succès
- ARP poisoning actif entre victime et passerelle
- Interception du trafic réseau effective
- Vulnérabilité ARP spoofing confirmée

STATISTIQUES DES PAQUETS INTERCEPTÉS:
- Total paquets interceptés: 6
- Paquets ICMP (ping): 1
- Paquets TCP: 1
- Paquets DNS: 1
- Paquets HTTP: 1
- Paquets HTTPS: 1
- Paquets ARP: 1

DÉTAIL DES PAQUETS INTERCEPTÉS:
1. [16:30:45] ARP: ARP poisoning successful - MITM established
2. [16:30:46] ICMP: Echo Request vers Google DNS
3. [16:30:47] DNS: Query: google.com A
4. [16:30:48] TCP: Connexion TCP vers serveurs Google
5. [16:30:49] HTTPS: Trafic HTTPS vers Google (chiffré)
6. [16:30:50] HTTP: GET /index.html HTTP/1.1

ANALYSE DE SÉCURITÉ:
- Le réseau est vulnérable aux attaques MITM
- L'ARP spoofing fonctionne sans protection
- Le trafic non chiffré est interceptable
- Position d'écoute établie avec succès

RECOMMANDATIONS DE SÉCURITÉ PRIORITAIRES:
```

- Configurer des tables ARP statiques pour les équipements critiques
- Implémenter la sécurité des ports sur les commutateurs réseau
- Surveiller le trafic ARP pour détecter les anomalies
- Utiliser exclusivement des protocoles chiffrés (HTTPS, SSH, VPN)
- Mettre en place une segmentation réseau avec VLANs
- Installer des systèmes de détection d'intrusion (IDS/IPS)
- Former les utilisateurs aux risques des réseaux non sécurisés

CONCLUSION:
L'attaque MITM Ettercap a démontré la vulnérabilité du réseau face aux attaques ARP spoofing.
Des mesures de sécurité doivent être mises en place immédiatement.