■ SDV Toolbox - Rapport de Sécurité

Outil:	Ettercap MITM
Date:	07/06/2025 à 16:23:34
Cible:	192.168.236.133 → 192.168.236.2 via eth0
Opérateur:	SDV Security Team

Rapport d'Attaque Man-in-the-Middle

ATTAQUE MITM REUSSIE - TRAFIC INTERCEPTE

Parametre	Valeur
Configuration	192.168.236.133 → 192.168.236.2 via eth0
Paquets interceptes	9
Paquets HTTP	0
Paquets HTTPS	1
Requetes DNS	1
Type attaque	ARP Spoofing
Date attaque	07/06/2025 à 16:23:34

Informations de la cible :

Propriete	Valeur
IP	192.168.236.133
MAC	Détecté via ARP réel
HOSTNAME	Victime MITM
OS	Détection via trafic

Detail des paquets interceptes :

Heure	Protocole	Source -> Destination	Information
16:23:16.106236	ARP	192.168.236.133 -> Network	ARP poisoning actif
16:23:26.116574	ARP	192.168.236.133 -> Network	ARP poisoning actif
192.168.236.133.68	OTHER	192.168.236.133 -> Network	Trafic OTHER intercepté
Client-IP	OTHER	192.168.236.133 -> Network	Trafic OTHER intercepté
16:16:45	ARP	192.168.236.133 -> 192.168.236.2	ARP poisoning successful - MITM established
16:16:46	ICMP	192.168.236.133 -> 8.8.8.8	Ping vers Google DNS intercepté
16:16:47	TCP	192.168.236.133 -> 142.250.185.174	Connexion TCP vers Google
16:16:48	DNS	192.168.236.133 -> 8.8.8.8	Résolution DNS google.com
16:16:49	HTTPS	192.168.236.133 -> 142.250.185.174	Trafic HTTPS vers Google (chiffré)

Extrait du log technique :

```
ATTAQUE MITM ETTERCAP - RAPPORT DTAILL
Configuration d'attaque:
- Interface rseau: eth0
Rsultats de l'attaque:
- Position MITM tablie avec succs
- ARP poisoning actif entre victime et passerelle
- Paquets ARP: 3
1. [16:23:16.106236] ARP: ARP poisoning actif
Source: 192.168.236.133 | Data: Paquet ARP rel captur via MITM Ettercap
2. [16:23:26.116574] ARP: ARP poisoning actif
Source: 192.168.236.133 | Data: Paquet ARP rel captur via MITM Ettercap
```

Recommandations de securite reseau :

• CRITIQUE : Attaque MITM reelle reussie sur votre reseau

• URGENT : Isolez immediatement le reseau compromis

• Verifiez tous les equipements reseau pour detecter d'autres attaques

• Requetes DNS interceptees - Utilisez DNS over HTTPS (DoH)

• Configurez des tables ARP statiques pour les serveurs critiques

• Implementez une surveillance reseau continue (IDS/IPS)

• Utilisez des certificats TLS pour authentifier les communications

• Configurez VLAN pour segmenter le reseau

• Formez les equipes a detecter les attaques MITM

• Effectuez des tests de penetration reguliers

• Installez des systemes de detection d'ARP spoofing

• Implementez une politique de securite reseau stricte