

RAPPORT

Attaque Man-in-the-Middle par Empoisonnement ARP Analyse et Contre-Mesures



Réalisé par :
Manar Ouberri

Table des matières

1	Introduction	2
2	Environnement de Test	2
2.1	Configuration du Laboratoire	2
2.2	Outils Utilisés	2
3	Préparation de l'Environnement	2
3.1	Activation du Forwarding IP	2
4	Exécution de l'Attaque ARP Poisoning	3
4.1	Lancement d'Ettercap	3
4.2	Procédure Détailée	3
4.3	Alternative en Ligne de Commande	3
5	Analyse et Surveillance	3
5.1	Capture avec Wireshark	3
5.2	Vidage du Cache ARP	3
5.3	Génération de Trafic de Test	3
6	Résultats et Observations	4
6.1	Sur la Machine Attaquante	4
6.2	Sur la Machine Victime (Wireshark)	4
7	Mécanisme Technique	4
7.1	Processus d'Empoisonnement ARP	4
8	Contre-Mesures et Protection	5
8.1	Détection de l'Attaque	5
8.2	Prévention	5
8.3	Commandes de Sécurité	5
9	Conclusion	6
9.1	Bilan de l'Exercice	6
9.2	Recommandations	6
9.3	Perspectives	6
10	Références Techniques	6

1 Introduction

Information

Ce document présente une analyse complète d'une attaque **Man-in-the-Middle (MITM)** utilisant la technique d'empoisonnement du cache **ARP (Address Resolution Protocol)**. L'objectif est de démontrer comment un attaquant peut intercepter et manipuler le trafic réseau entre une victime et sa passerelle par défaut dans un environnement contrôlé.

2 Environnement de Test

2.1 Configuration du Laboratoire

Configuration des Machines

- | | | |
|--------------------------|---------------------|--|
| • PC Victime | • Routeur | • IP : 192.168.1.20 |
| • IP : 192.168.1.10 | • IP : 192.168.1.1 | • Système : Ubuntu avec outils de sécurité |
| • Système : Ubuntu 22.04 | • Rôle : Passerelle | |
| | • Attaquant | |

2.2 Outils Utilisés

- **Ettercap** : Outil principal pour l'attaque MITM
- **Wireshark** : Analyseur de paquets pour surveillance
- **Terminal Linux** : Commandes système et réseau
- **Outils de sécurité** : Installés sur Ubuntu

3 Préparation de l'Environnement

3.1 Activation du Forwarding IP

Information

Pour que l'attaquant puisse relayer le trafic entre la victime et le routeur, le forwarding IP doit être activé.

```
1 # Sur la machine attaquante
2 echo 1 > /proc/sys/net/ipv4/ip_forward
3
4 # Vérification
5 cat /proc/sys/net/ipv4/ip_forward
```

Listing 1 – Activation du forwarding IP

4 Exécution de l'Attaque ARP Poisoning

4.1 Lancement d'Ettercap

```
1 ettercap -G
```

Listing 2 – Lancement d'Ettercap en mode graphique

4.2 Procédure Détailée

1. Sélectionnez l'interface réseau (ex : eth0)
2. Scannez les hôtes du réseau : **Hosts** → **Scan for hosts**
3. Visualisez la liste : **Hosts** → **Host list**
4. Ajoutez le routeur (**192.168.1.1**) à **Target 1**
5. Ajoutez la victime (**192.168.1.10**) à **Target 2**
6. Lancez l'attaque : **Mitm** → **ARP poisoning** → **Sniff remote connections**

4.3 Alternative en Ligne de Commande

```
Attaque ARP Poisoning en une commande sudo ettercap -T -q -M  
arp:remote /192.168.1.10/ /192.168.1.1/
```

5 Analyse et Surveillance

5.1 Capture avec Wireshark

```
1 # Sur la machine victime  
2 wireshark &
```

Listing 3 – Lancement de Wireshark

5.2 Vidage du Cache ARP

```
1 arp -d *
```

Listing 4 – Vidage du cache ARP sur la victime

5.3 Génération de Trafic de Test

```

1 # Ping vers une adresse externe
2 ping 8.8.8.8
3
4 # Navigation vers site non-HTTPS
5 curl http://example.com

```

Listing 5 – Trafic depuis la victime

6 Résultats et Observations

6.1 Sur la Machine Attaquante

Succès

- **Traffic intercepté** : Affichage en temps réel dans Ettercap
- **Données lisibles** : Paquets HTTP non chiffrés visibles
- **Sessions capturées** : Connexions web et identifiants
- **Redirection réussie** : Tout le trafic passe par l'attaquant

6.2 Sur la Machine Victime (Wireshark)

Observations dans Wireshark

Observation	Signification
Requêtes ARP répétées	Victime cherche l'adresse MAC du routeur
Réponses ARP non sollicitées	Provenant de l'attaquant, prétendant être le routeur
Adresse MAC du routeur modifiée	Pointe maintenant vers l'attaquant
Traffic redirigé	Tous les paquets passent par l'attaquant
Latence augmentée	Légère augmentation due au relais

7 Mécanisme Technique

7.1 Processus d'Empoisonnement ARP

1. L'attaquant envoie une réponse ARP forgée à la victime : "*Je suis 192.168.1.1, mon MAC est XX :XX :XX :XX :XX :XX*"
2. L'attaquant envoie une réponse ARP forgée au routeur : "*Je suis 192.168.1.10, mon MAC est XX :XX :XX :XX :XX :XX*"
3. La victime met à jour son cache ARP avec la fausse information
4. Le routeur met à jour son cache ARP avec la fausse information

5. Tout le trafic passe maintenant par l'attaquant

⚠️ Attention

Vulnérabilité critique : Le protocole ARP ne possède aucun mécanisme d'authentification, ce qui permet à n'importe quel hôte du réseau de répondre aux requêtes ARP, même s'il n'est pas la cible légitime.

8 Contre-Mesures et Protection

8.1 Détection de l'Attaque

- **Surveillance ARP** : Détecter les réponses non sollicitées
- **Analyse des tables ARP** : Vérifier les changements inhabituels
- **Outils spécialisés** : ARPwatch, XArp, Snort
- **Surveillance réseau** : Analyser les patterns de trafic

8.2 Prévention

🛡️ Méthodes de Prévention

Méthode	Description
ARP Statique	Configuration manuelle des associations IP-MAC sur les équipements critiques
Port Security	Sur les switches, limiter le nombre d'adresses MAC par port
DHCP Snooping	Valider les baux DHCP pour prévenir les attaques
Dynamic ARP Inspection	Inspecter les paquets ARP sur les switches managés
VLANs	Segmenter le réseau pour limiter la portée des attaques
Chiffrement	Utiliser HTTPS, VPN, SSH pour protéger les données

8.3 Commandes de Sécurité

```

1 # V rifier le cache ARP (Linux)
2 arp -a
3
4 # Configurer une entr e ARP statique
5 arp -s 192.168.1.1 00:11:22:33:44:55
6
7 # Installer un outil de surveillance ARP

```

```
8 sudo apt install arpwatch
9
10 # Démarrer la surveillance
11 sudo arpwatch -i eth0
```

Listing 6 – Commandes de protection réseau

9 Conclusion

9.1 Bilan de l'Exercice

Information

Cette démonstration a permis de :

- Comprendre le fonctionnement du protocole ARP et ses vulnérabilités
- Mettre en œuvre une attaque MITM complète dans un environnement contrôlé
- Analyser les impacts et les risques associés à cette vulnérabilité
- Identifier les mécanismes de détection et de prévention appropriés

9.2 Recommandations

1. Toujours utiliser **HTTPS** pour les sites web, surtout pour les connexions sensibles
2. Implémenter des **VLANs** pour segmenter le réseau selon les besoins de sécurité
3. Utiliser des **VPN** pour les communications importantes sur des réseaux non fiables
4. Sensibiliser les utilisateurs aux risques des réseaux publics et non sécurisés
5. Mettre en place une surveillance proactive du réseau avec des outils adaptés
6. Maintenir les systèmes à jour avec les derniers correctifs de sécurité

9.3 Perspectives

- **Développement** : Outils de détection plus avancés
- **Formation** : Sensibilisation continue des administrateurs
- **Recherche** : Protocoles ARP sécurisés (S-ARP, TARP)
- **Automatisation** : Tests de sécurité réguliers

10 Références Techniques

- RFC 826 - Address Resolution Protocol
- Documentation officielle d'Ettercap
- Guide d'utilisation de Wireshark
- Documentation Ubuntu
- OWASP - ARP Poisoning Attack