SÉCURITÉ DES SI-PROTOCOLE ARP

RAPPORT DE TRAVAUX PRATIQUES

OLIER CLÉMENT

2017-2018

MICKAEL RIGONNAUX

Présentation de la plateforme

Introduction

Ce TP a été réalisé dans le cadre du cours de sécurité des SI.

Afin de réaliser ce TP il nous a été nécessaire de disposer de trois machines, une machine servant de victime, une autre employée comme la machine attaquante (installée avec le système d'exploitation Kali Linux) et une dernière utilisée comme serveur FTP. Nous avons aussi décidé d'utiliser un réseau privé établi grâce à un partage de connexion depuis un Smartphone.

Durant ce TP nous allons effectuer trois types d'attaque :
- Attaque ARP DOS (Denial Of Service)
- Attaque ARP MINT Serveur (Man in the Middle)
- Attaque ARP MINT Internet (Man in the Middle)

Le protocole ARP est un protocole qui, de par sa conception, expose les réseaux informatiques et leurs composants à des vulnérabilités et des dangers qui sont faciles à exploiter lorsque l'on connaît bien son fonctionnement. En clair ce protocole permet la résolution d'une adresse MAC à partir d'une adresse IP. Nous allons ici étudier le fonctionnement des attaques utilisant le protocole ARP puis essayer de donner des pistes pour s'en protéger.

Nom	Adresse IP	Adresse Mac
Attaquant	172.20.10.2 /28	b0:10:41:16:aa:8f
Victime	172.20.10.8 /28	ac:bc:32:89:61:b5
Passerelle	172.20.10.1 /28	6a:4b:aa:e3:9:64
Serveur FTP	172.20.10.4 /28	12:ba:71:ff:d5:6e

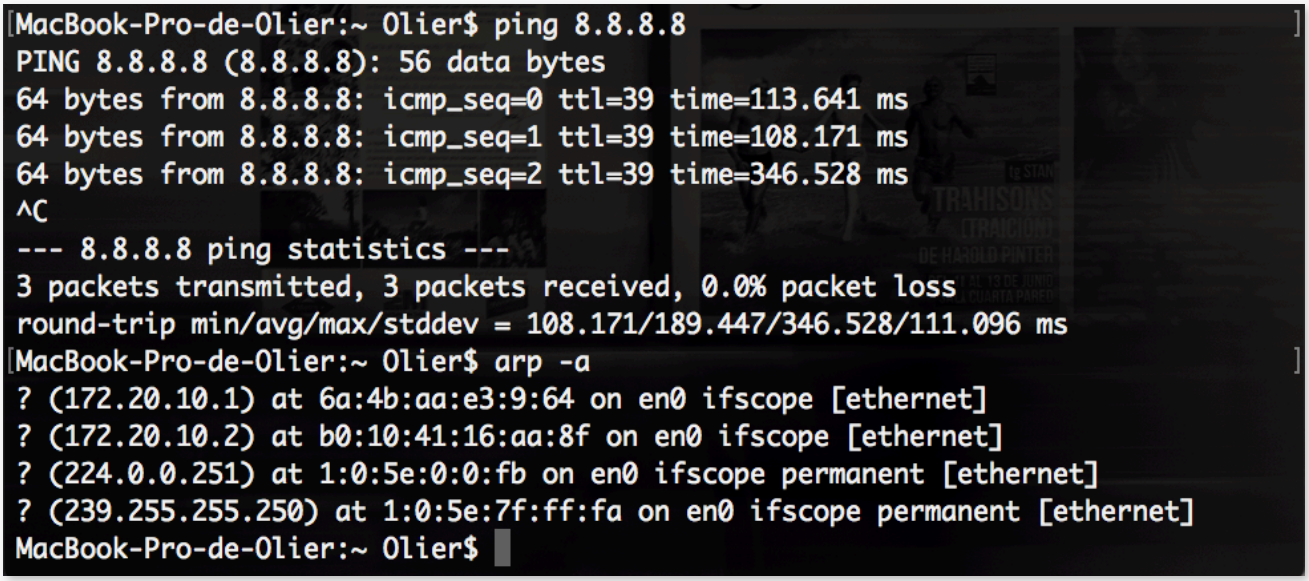
Attaque ARP DOS

L'attaque DOS a pour objectif d'empêcher un système victime de communiquer sur le réseau.

Dans cet exemple le but sera de bloquer l'accès internet de l'hôte, il faut alors empoisonner le cache ARP de la machine victime de façon permanente grâce à l'utilisation de l'outil « arpspoof » pré-installé sous l'OS Kali Linux.

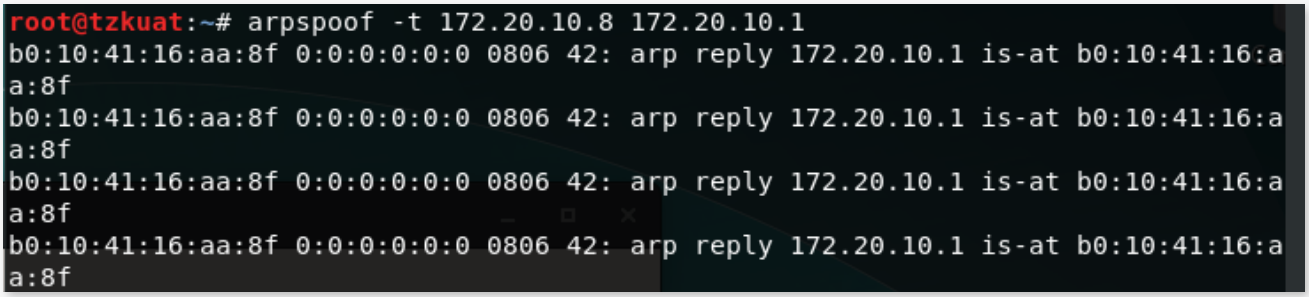
Le principe de l'ARP spoofing (spoofing voulant dire « *parodier », « usurper »)* est d'envoyer des informations à un système afin de lui faire enregistrer des informations qui ne sont pas les bonnes et qui usurpent l'identité (la relation IP-MAC) d'un autre système.

Cache ARP de la victime avant l'attaque



On peut donc remarquer grâce à la capture d'écran ci-dessus que la machine victime parvient bien à établir une connexion à internet, ainsi que les différentes associations IP-MAC.
Maintenant si l'attaquant exécute la commande **« arpspoof -t 172.20.10.8 172.20.10.1 »** alors les paquets ne seront pas retransmis à leur cible originelle et tomberont donc dans le vide, rendant ainsi la connectivité de la cible impossible car aucun paquet n'arrivera à destination.

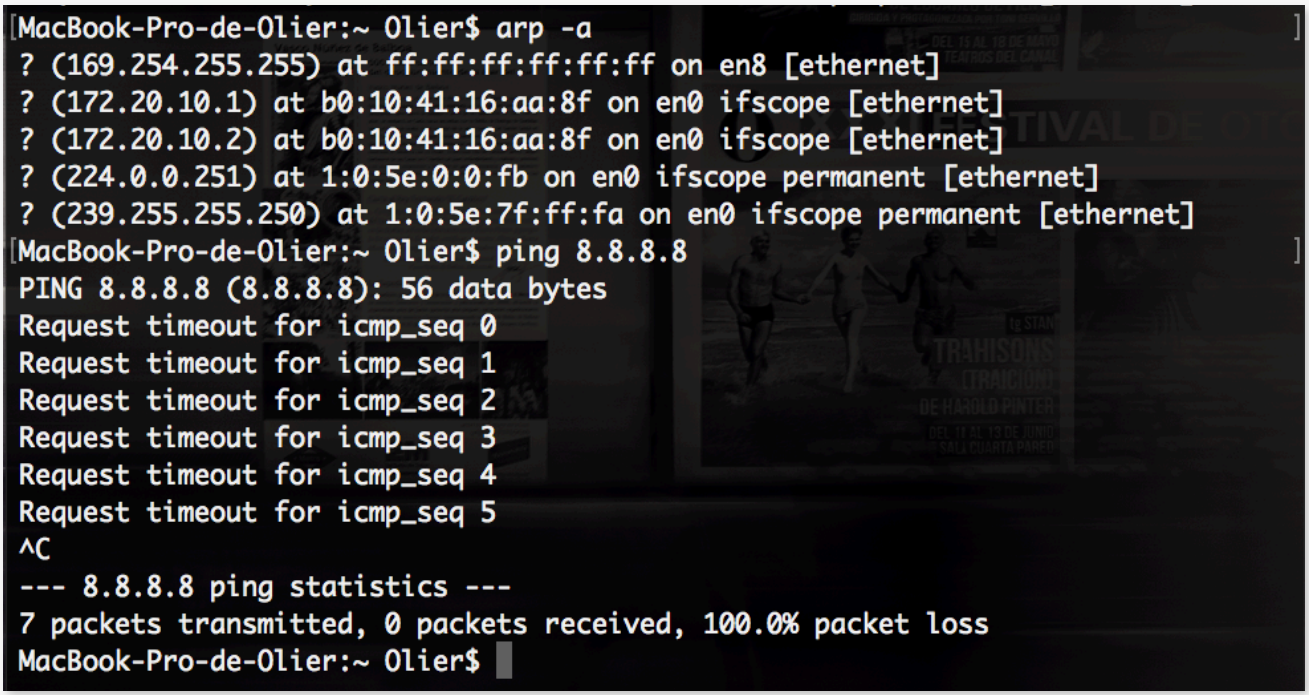
Commande « arpspoof » exécuté sur l'attaquant



On peut traduire cette ligne de commande par "fait moi passer pour 172.20.10.1 auprès de 172.20.10.8". Cette commande permettra la mise a jour continuelle de la table ARP en envoyant des paquets de façon constante à la cible afin qu'elle reste falsifiée.

On remarque dans cet exemple l'envoie de paquets « arp reply » indiquant que l'IP de la passerelle (172.20.10.1) a maintenant l'adresse MAC de la machine attaquante (b0:10:41:16:aa:8f).

Cache ARP de la victime après l'attaque



L'exécution de la commande **« arp -a » et de « ping 8.8.8.8 »** sur la victime montre que :

- l'IP de la passerelle (172.20.10.1) a maintenant l'adresse MAC de la machine attaquante (b0:10:41:16:aa:8f).
- La connexion à internet n'est plus effective

Attaque ARP MITM Serveur

L'attaque MITM Serveur a pour objectif de voler les identifiants d'accès d'un utilisateur sur un serveur.

Dans cet exemple le but sera de récupérer les login / mot de passe de la victime avec l'utilisation de l'outil « Wireshak » . Une attaque Man in the Middle permet à l'attaquant de se positionner au milieu d'une conversation ou d'un échange réseau pour intercepter, lire, supprimer ou modifier tout ou partie de cette communication.

Nous allons ici capturer une session FTP via ARP spoofing afin d'intercepter les communications de la machine victime, initialement destinées au serveur FTP, tout en veillant bien à faire suivre les paquets afin que la victime ne se doute de rien et accède bien au serveur. Il s'agira donc de rediriger les paquets détournés afin que les utilisateurs naviguent et utilisent le réseau sans perturbation ou coupure, et avec le moins de ralentissement réseau possible.

Activation du « forwarding de paquet » exécuté sur l'attaquant

```
root@tzkuat:~# echo 1 > /proc/sys/net/ipv4/ip_forward
ip_forward           ip_forward_use_pmtu
root@tzkuat:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@tzkuat:~#
root@tzkuat:~#
root@tzkuat:~#
root@tzkuat:~# cat /proc/sys/net/ipv4/ip_forward
1
root@tzkuat:~#
```

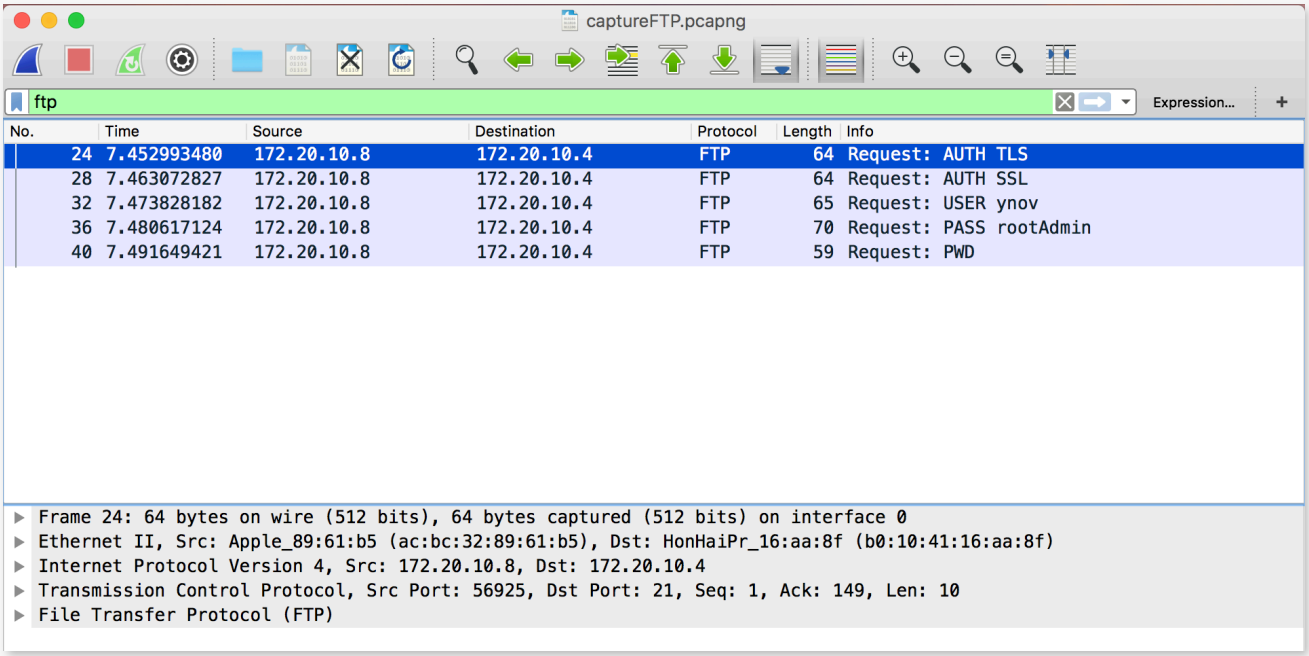
C'est grâce à cette commande **« echo 1 > /proc/sys/net/ipv4/ip_forward »** que les paquets pourront transiter à travers le système de l'attaquant et aussi atteindre leur cible originelle.
Comme précédemment il faudra utiliser la commande « arpspoof » pour envoyer continuellement des paquets ARP qui vont falsifier la table ARP de la victime et indiquer que l'IP du serveur FTP a notre adresse MAC :

« arpspoof -t 172.20.10.8 172.20.10.4 »

Exploitation de l'attaque

Une fois fait il s'agira d'exploiter l'attaque en utilisant l'outil « Wireshark ». Une capture du trafic réseau devra être effectuée sur l'attaquant et lorsque la victime se connecte et s'authentifie sur le serveur FTP les identifiants de connexion sont alors récupéré.

Capture « Wireshark »



On remarque alors que les identifiants FTP passent par la machine attaquante bien qu'ils ne doivent normalement pas y transiter. La destination des paquets FTP est bien l'IP du serveur FTP mais que l'adresse MAC est celle de l'attaquant.

Comme cela est expliqué juste en dessous il est également possible d'effectuer une attaque « arpspoof » pour le chemin retour, usurpant ainsi l'identité (l'adresse MAC) de la victime auprès du serveur FTP. On pourrait alors récupérer par exemple les fichiers téléchargés par la victime sur le serveur FTP et les reconstituer directement dans Wireshark.

Attaque ARP MITM Internet

L'attaque MITM Internet est réalisé de la même manière que l'attaque précédente et a pour objectif d'espionner la navigation Internet d'un utilisateur.

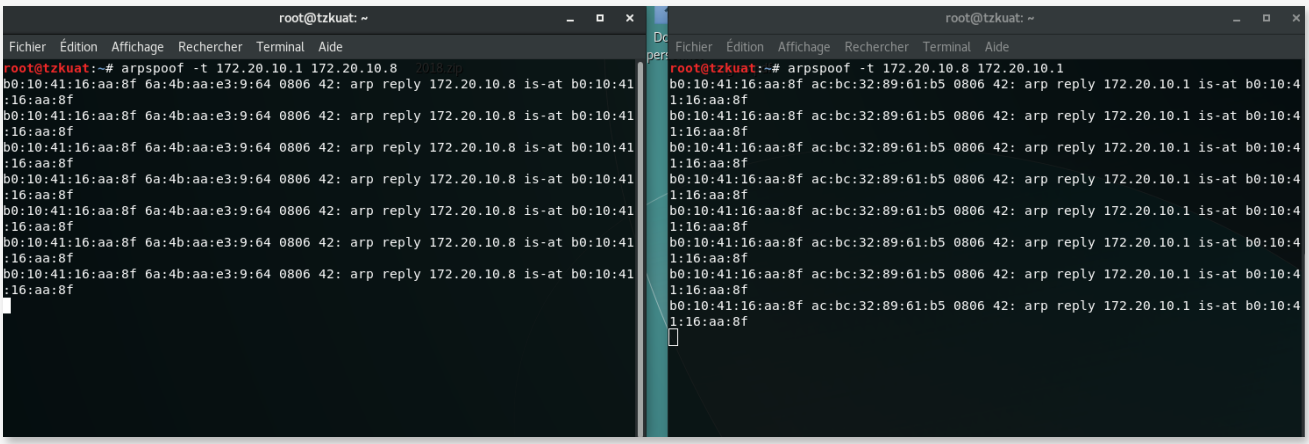
En effet dans cet exemple le but sera de récolter les URLs visités par la victime avec l'utilisation de l'outil « Wireshak » .

Le principe reste sensiblement identique à la dernière attaque la seule différence réside dans l'exécution d'une autre attaque « arpspoof » pour le chemin retour.

Ce qui donne étape par étape :

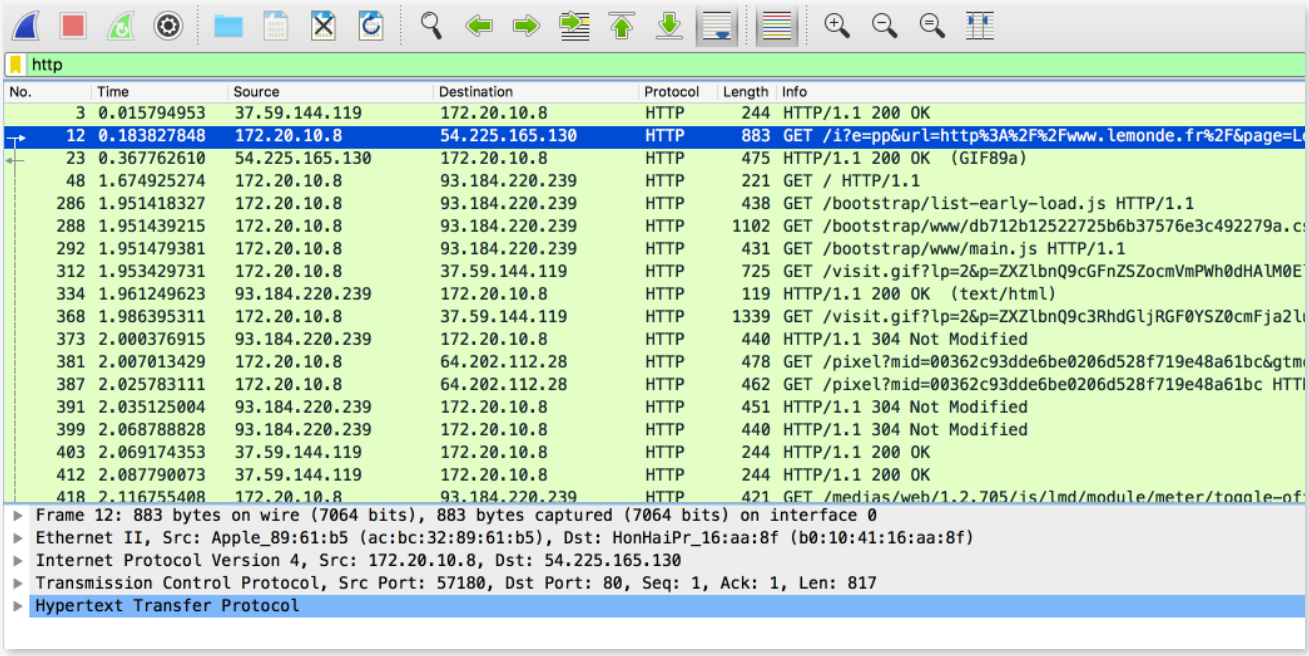
- Activation du « forwarding de paquet » sur l'attaquant. **« echo 1 > /proc/sys/net/ipv4/ip_forward »**
- Usurpation de l'adresse MAC de la passerelle auprès de la victime. La table ARP de la victime étant falsifiée, les paquets qu'il enverra seront dans un premier temps envoyés à l'attaquant. **« arpspoof -t 172.20.10.1 172.20.10.8 »**
- Usurpation de l'adresse MAC de la victime auprès de la passerelle. La table ARP de la passerelle étant falsifiée, les paquets qu' enverra seront dans un premier temps envoyés à notre pirate. **« arpspoof -t 172.20.10.8 172.20.10.1 »**
- Exploitation de l'attaque avec une capture « Wireshark »

Commandes « arpspoof » exécutées sur l'attaquant



L'attaquant intercepte les paquets envoyés par la victime puis les rejoue auprès de la passerelle, et inversement, nous sommes donc dans un contexte d'attaque par "L'homme du milieu" (Man in the middle).

Exploitation de l'attaque, Capture « Wireshark »



On peut donc remarquer ici que la victime s'est rendu sur le site www.lemonde.fr et que l'adresse IP source est celle de la victime.

Attaque à une plus grande échelle (Gratuitous ARP)

Dans cet exemple un seul hôte fut ciblé, cependant, il est également possible de diffuser des messages ARP falsifiant les tables ARP des cibles en broadcast, ce qui aura pour effet d'affecter toutes les machines se situant sur la même plage IP que celle de l'attaquant.

Par exemple : « arpspoof -t 172.20.10.15 172.20.10.1 »

Cette commande va faire passer l'attaquant pour la passerelle sur tout le réseau et va donc rediriger l'intégralité du trafic du réseau vers lui. Ce qui laisse alors au choix, en activant l'IP forwarding, de capturer le trafic et le faire suivre pour que les postes ne se doutent de rien ou alors désactiver l'IP forwarding pour causer une attaque par déni de service.

Solutions

Dans cette partie il sera présenté présenté plusieurs outils permettant de se protéger contre l'ARP spoofing.

Donc pour résumer les attaques ARP spoofing permettent aux pirates de se positionner entre les flux de communication transitant entre leur victime et une passerelle. Cette technique leur permettent notamment d'intercepter ou de modifier des trafics, et même d'empêcher tout trafic.

L'enregistrement ARP statique

La technique la plus simple de protection contre l'ARP spoofing est l'enregistrement statique des tables ARP. Cette technique permet de rendre les tables ARP du système infalsifiable par des requêtes ARP malicieuses.

Bien que cette protection soit très sécurisante elle peut s'avérer extrêmement lourde d'utilisation dans un contexte d'entreprise. En effet dans le cadre d'une maintenance quotidienne d'un parc informatique, si le système enregistré de façon statique est modifié (un serveur ou la passerelle par exemple), il faut aller changer l'enregistrement statique sur tous les hôtes clients du parc.

Il est également possible de s'aider d'un script de démarrage ou par déploiement de GPO.

« arp -s adresseIP adresse MAC »

Détection via IDS

Une autre des techniques pouvant servir à la détection des attaques ARP spoofing est la détection via un système de détection d'intrusion. Simple et peut être mis en place avec des logiciels libres, cette détection s'effectue lors de l'analyse par des IDS d'un grand nombre de paquets ARP-reply envoyés qui enverrons alors une alerte aux équipes de sécurité.
Son principal inconvénient réside donc dans le fait que ce système requiert une intervention humaine. Certains IDS propose la réalisation la mise en place de réponse active pour combler ce manque. **« OSSEC, ALIEN VAULT »**

Les solutions propriétaires

Un autre moyen de se prémunir face aux attaques ARP est l'utilisation de solutions propriétaires du type **« Symentec ou SonicWall »** appelées **« Anti-MAC spoofing ou MAC-IP anti Spoof».** Le principe de ces solutions est de bloquer le "*gratuitous ARP*" qui est le fait d'envoyer des réponses ARP à des machines n'ayant rien demandé dans le but de fausser leur table ARP, ce qui est la base de l'ARP spoofing.

Dynamic ARP Protection

Le **DAI** est une solution intégrer aux éléments actifs **Cisco et HP**. Le principe de cette technologie est que pour chaque réponse ARP envoyée depuis un port qui n'est pas de confiance, elle va comparer les données qu'elle contient à une base de données de confiance pré-enregistrée dans le réseau et dropper les paquets ARP-reply contenant de fausses informations. Cela évite alors en principe la falsification d'une correspondance MAC – IP au sein d'un réseau et ainsi les attaques MITM via ARP spoofing.

Elle peut être mise en association avec une table ARP statique centralisée servant alors de référence.

L'outil shARP

shARP est un script shell qui peut détecter les attaques ARP spoofing. Il comprend de mode de d'opérations :

- **Defensive mode :** Dans ce mode d'opération, dès la détection d'une attaque ARP spoofing, shARP désactive automatiquement la carte réseau de machine.
- **Offensive mode :** Avec ce mode d'opération, en plus de la désactivation de la carte réseau, l'outil shARP fait appel à Airmon-ng et Aircrack-ng, puis tente de virer l'attaquant du réseau grâce à des paquets de désauthentification.

Après les détections, shARP sauvegarde les informations de l'attaquant dans un fichier /usr/shARP/log.txt créé par l'outil lui-même.

Capture d'écran du script « shARP »

RAPPORT DE TP