MISE EN PLACE D'UN POSITIONNEMENT MITM (MAN IN THE MIDDLE)

Document qui explique la mise en place d'un positionnement MITM.

ASSURMER

Services informatiques

Version : 1.0

Service IT

08/03/2023

Yohan HALIMI

Kevin ORTIZ

Table des matières :

I. Fonctionnement du MITM (Man In The Middle)

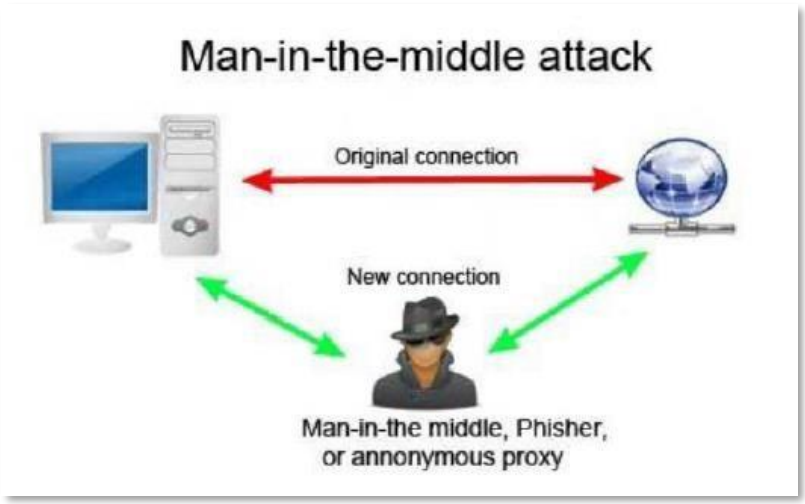
1 Ce que nous cherchons

Écoute clandestine via un positionnement MITM (Man In The Middle) avec empoisonnement de cache ARP. Utilisation du protocole HTTPS afin de chiffrer les flux vers un serveur web.

2 Scénario

L'attaquant empoisonne le cache ARP de la victime et récupère le mot de passe de la victime saisi dans un formulaire via une connexion non sécurisée http. La contre-mesure passe par le chiffrement des conversations et l'activation de l'IPS sur le firewall.

Il s'agit d'un classique du genre très facile à réaliser. Sur kali, il est possible d'utiliser l'outils Ettercap pour réaliser l'empoisonnement de cache ARP.



Nous utiliserons les logiciels :

- Ettercap via kali linux
- Wireshark via kali linux

3 Fonctionnement de l'empoisonnement du cache ARP via Ettercap

L'empoisonnement du cache ARP permet de falsifier le cache ARP de la victime en associant, par exemple, l'adresse IP de la passerelle à l'adresse MAC du pirate.

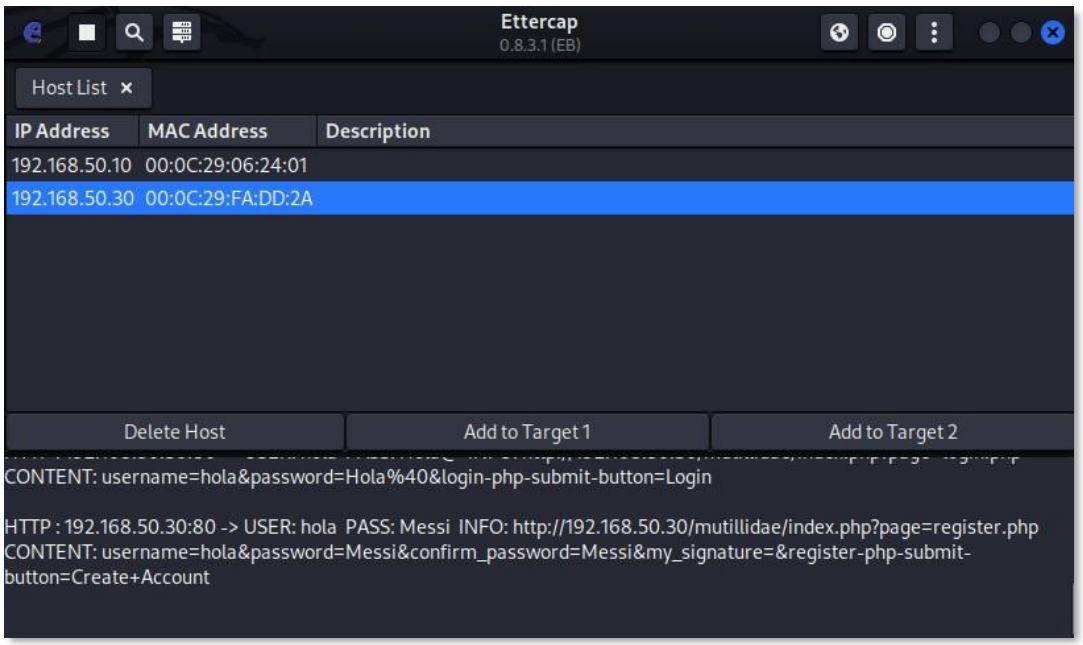
Ainsi, tout le flux passe par la machine du pirate qui peut se mettre en écoute avec un logiciel de capture de trames.

3.1 Test pirate pour capturer le mot de passe de la victime

Une fois que toutes les machines ont été configurées, il faut vérifier qu'elles arrivent à communiquer entre elles.

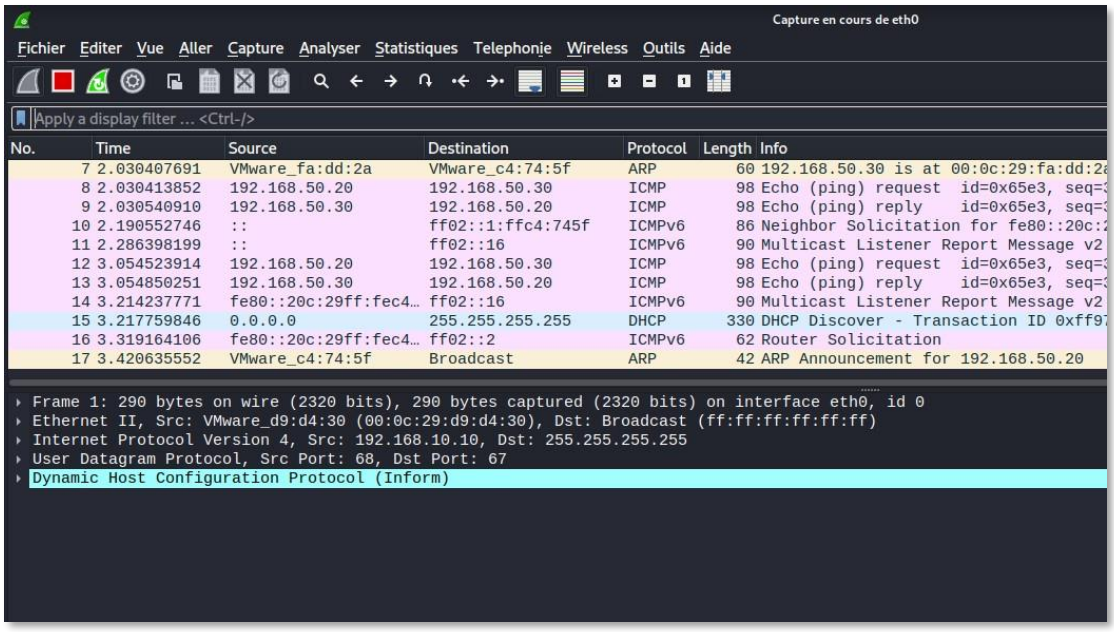
3.2 Empoisonnement de cache ARP avec Ettercap

Dans Kali, nous allons ouvrir l'outil Ettercap afin d'empoissonner le cache ARP, comme on peut le voir



On trouve notre machine victime.

3.3 Capture de trame avec Wireshark



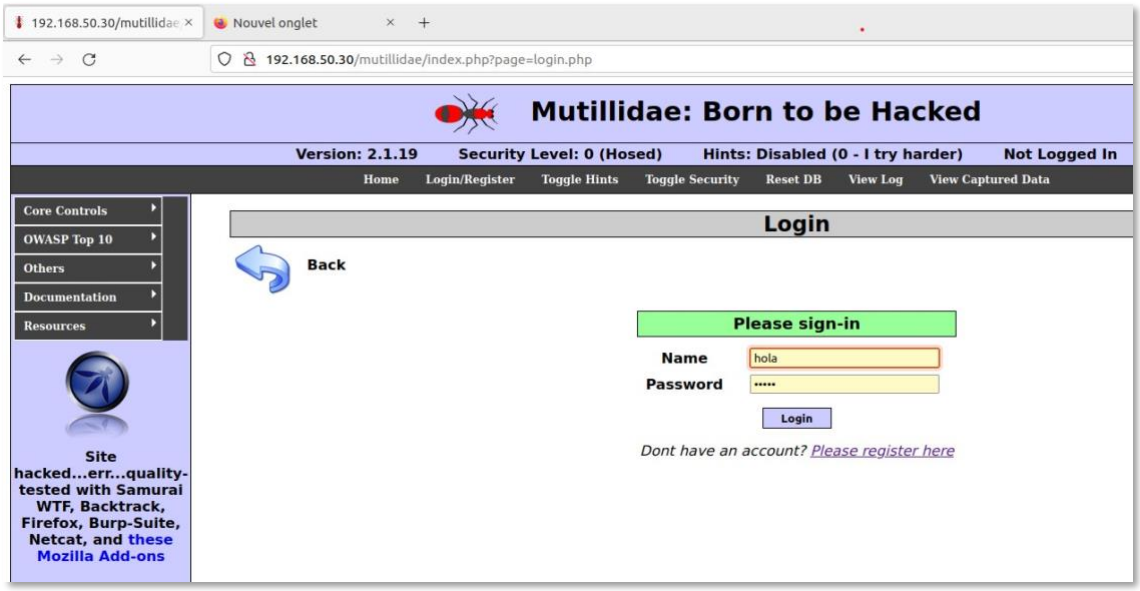
Puis, nous allons lancer Wireshark qui va nous permettre de voir le trafic réseau en temps réel.

3.4 Machine cliente

Une fois que les deux outils seront lancés nous allons aller dans notre machine cliente et nous allons ouvrir le navigateur :

Depuis le navigateur nous allons créer un compte puis nous **identifier** sur le site **Mutillidae** :

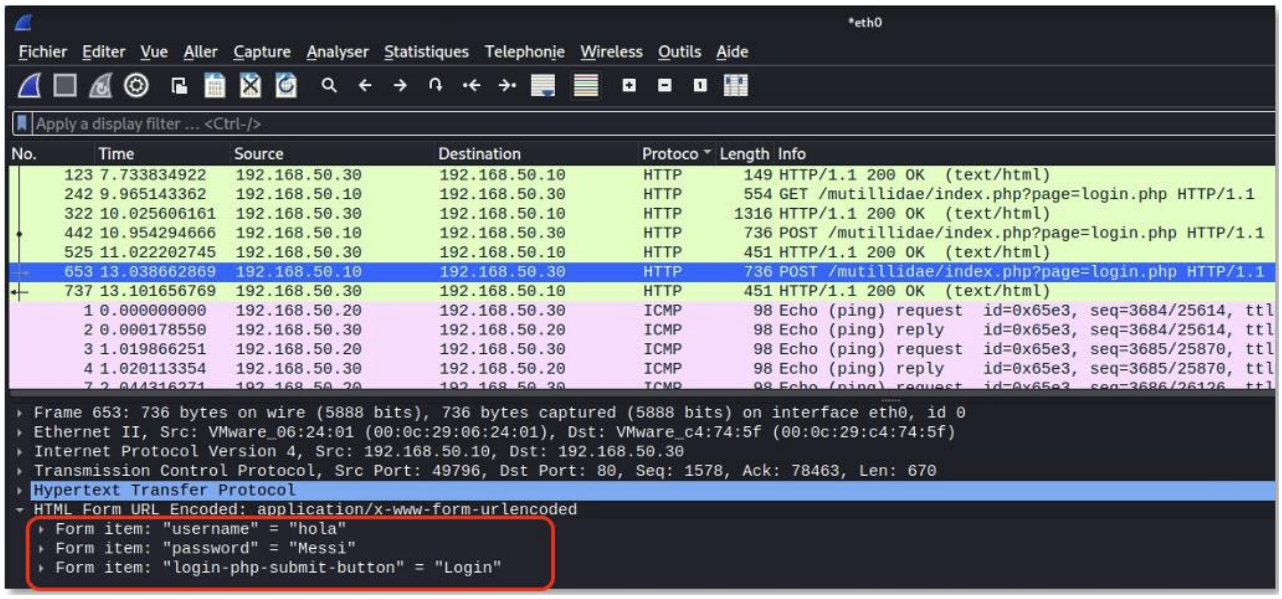
- https://172.16.10.5/mutillidae



Une fois l'authentification réalisée, nous allons aller dans Kali.

3.5 Récupération du mot de passe de la victime

Après avoir ouvert Wireshark dans Kali, nous allons chercher dans le trafic réseau le protocole http qui a été utilisé par le site : https://172.16.10.5/mutillidae



Puis dans l'onglet « Hypertext Tranfert Protocol », nous allons trouver l'identifiant et le mot de passe que la victime a utilisé pour se connecter.

II. Consignes :

Mettre en place quatre machines virtuelles. Un Kali, un Metasploitbale Le Windows 10 sera le poste client, et un Windows Serveur qui sera notre serveur routeur.

Dans le Srv-ROU, nous allons mettre en place les services de routeur afin de faire connecter toutes les machines entre elles.

Le metasploitable est une machine linux qui peut dispenser des informations en matière de sécurité, elle va nous aider pour tester des techniques de pénétration dans le système.

Le Kali va nous fournir des outils pour réaliser des tests de sécurité du système d'information, notamment le test d'intrusion.

Le poste client sera la cible, on va récupérer, analyser tout ce qu'il fait.