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

I. Fonctionnement du MITM (Man In The Middle)

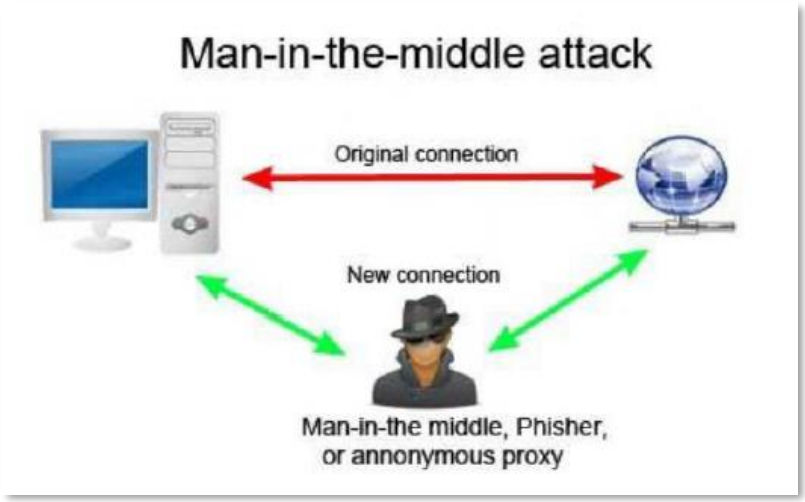
Ce que nous cherchons

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

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

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.

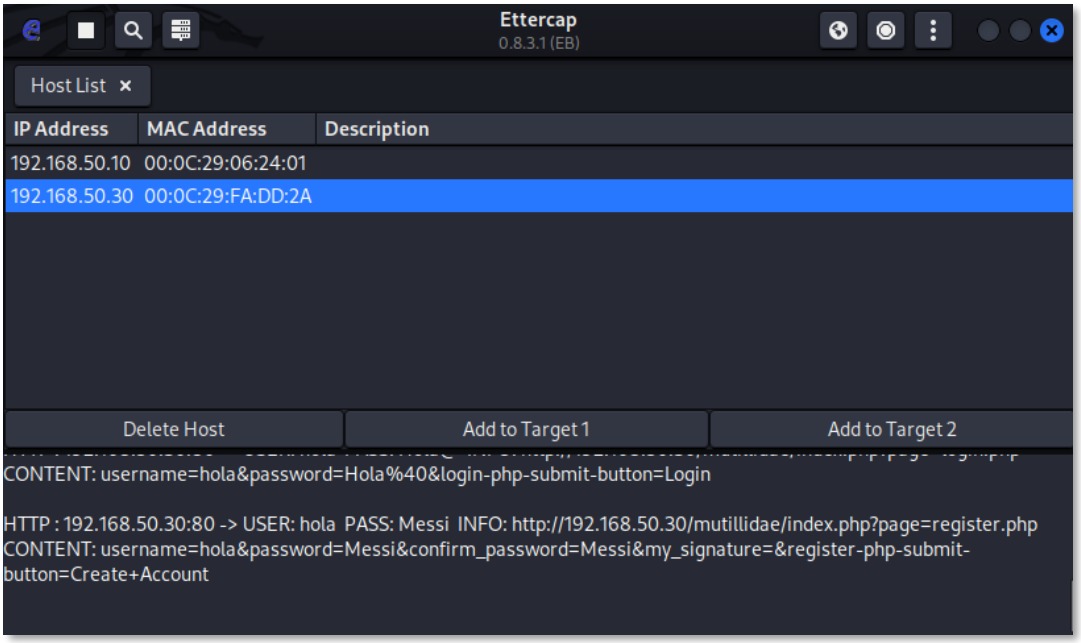
Ainsi, tout le flux passe par la machine du pirate qui peut se mettre en écoute avec un logiciel de capture de trames.

Test pirate pour capturer le mot de passe de la victime

Une fois que toutes les machines ont été configurée, il faut vérifier que toutes les machines arrivent à ping entre elles.

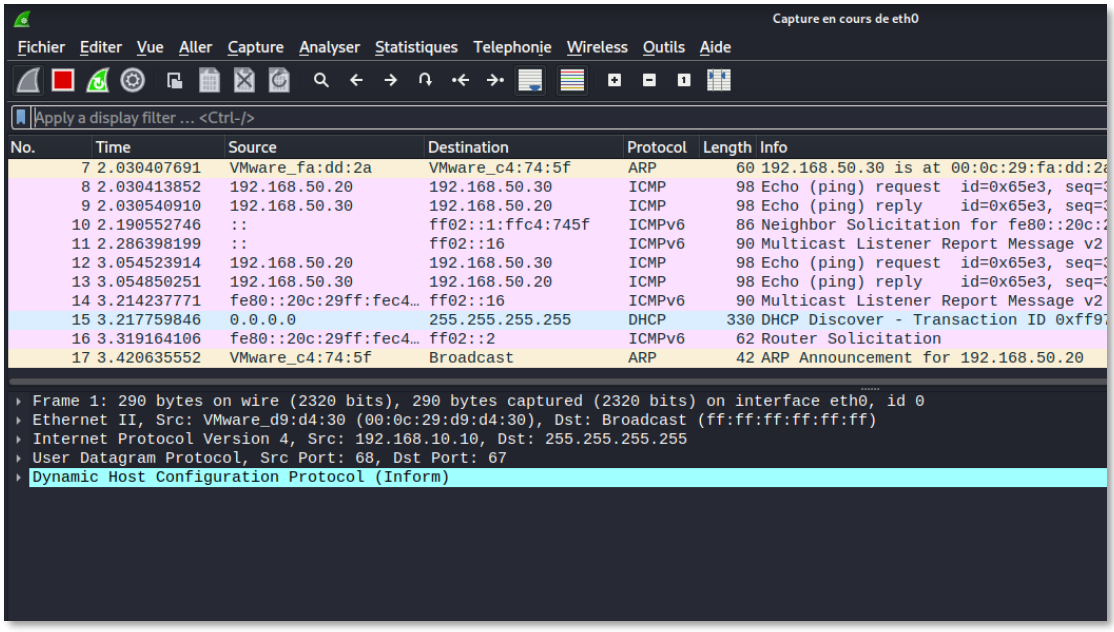
Empoisonnement de cache ARP avec Ettercap

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



on trouve notre machine victime.

capture de trame avec Wireshark



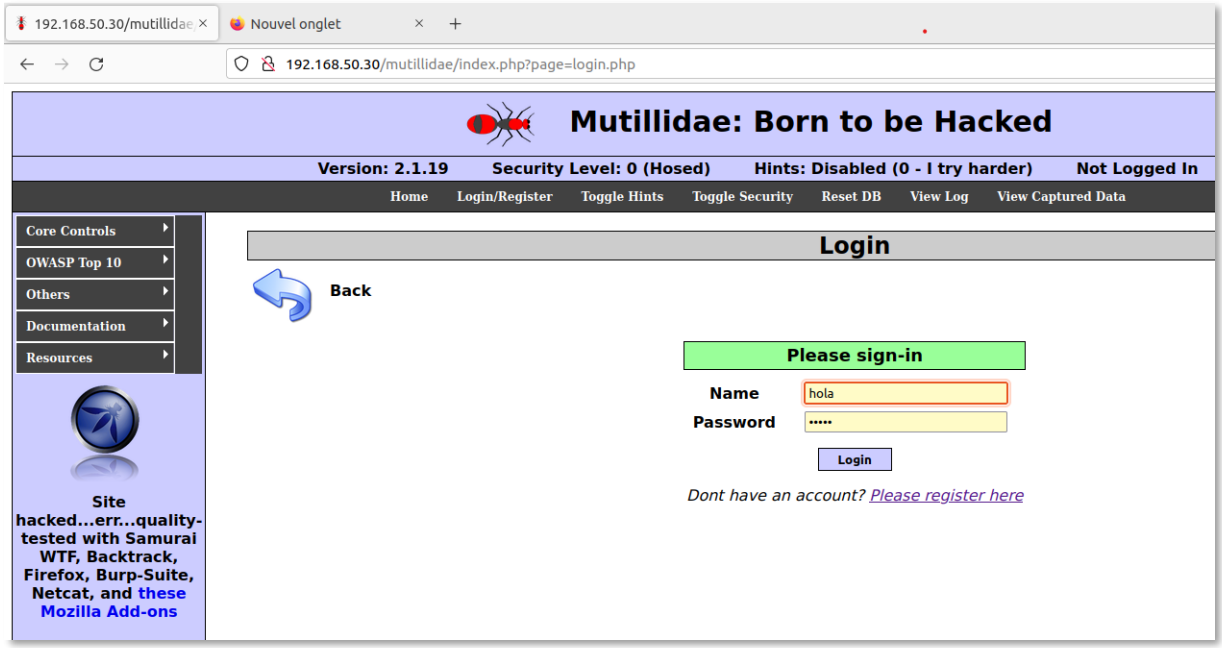
Puis nous allons lancer Wireshark qui va nous permettre de voir le **trafic réseau** en temps réel.

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 puis nous **identifier** sur le site **Mutillidae** :

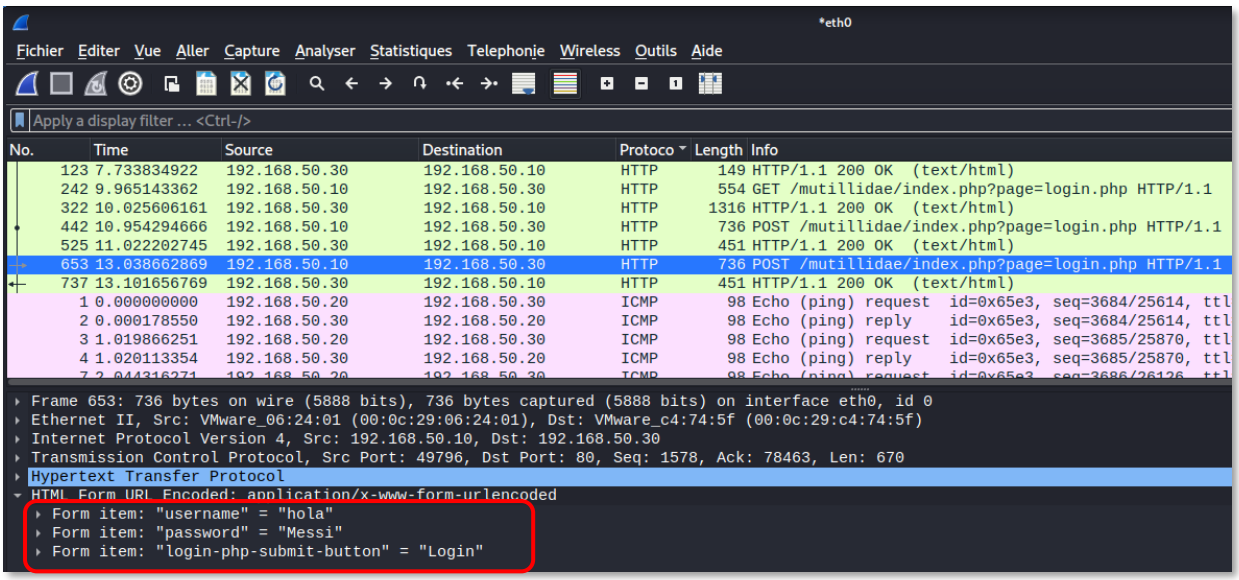
- https://172.16.10.5/mutillidae



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

Récupération du mot de passe de la victime

Une fois dans kali, nous allons ouvrir Wireshark, nous allons chercher entre dans trafic réseau le protocole http qui a été utilisé par le site : https://172.16.10.5/mutillidae



Puis dans l'onglet ''**Hypertext Transfer Protocol**''

Nous allons trouver l'identifiant et le mot de passe que la victime à utiliser pour se connecter.