



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





	Titre	Reference	Page	
	MITM	Assurmer	Page 2 sur 8	

Table des matières :

I.	Fonctionnement du MITM.....	2
1	Ce que nous cherchons	2
2	Scénario	2
3	Fonctionnement de l’empoisonnement du cache ARP via Ettercap.....	3
3.1	Test pirate pour capturer le mot de passe de la victime.....	3
3.2	Empoisonnement de cache ARP avec Ettercap.....	3
3.3	Capture de trame avec Wireshark.....	4
3.4	Machine cliente	5
3.5	Récupération du mot de passe de la victime	6
II.	Consignes.....	7



	Titre	Reference	Page	
	MITM	Assurmer	Page 3 sur 8	

I. Fonctionnement du MITM (Man In The Middle)

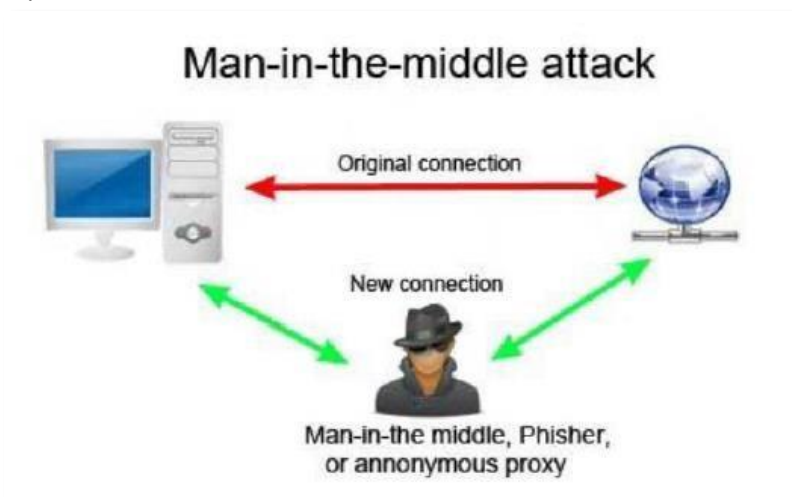
1 Ce que nous cherchons

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'outil Ettercap pour réaliser l'empoisonnement de cache ARP.



Nous utiliserons les logiciels :

- Ettercap via kali linux
- Wireshark via kali linux



	Titre	Reference	Page	
	MITM	Assurmer	Page 4 sur 8	

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.

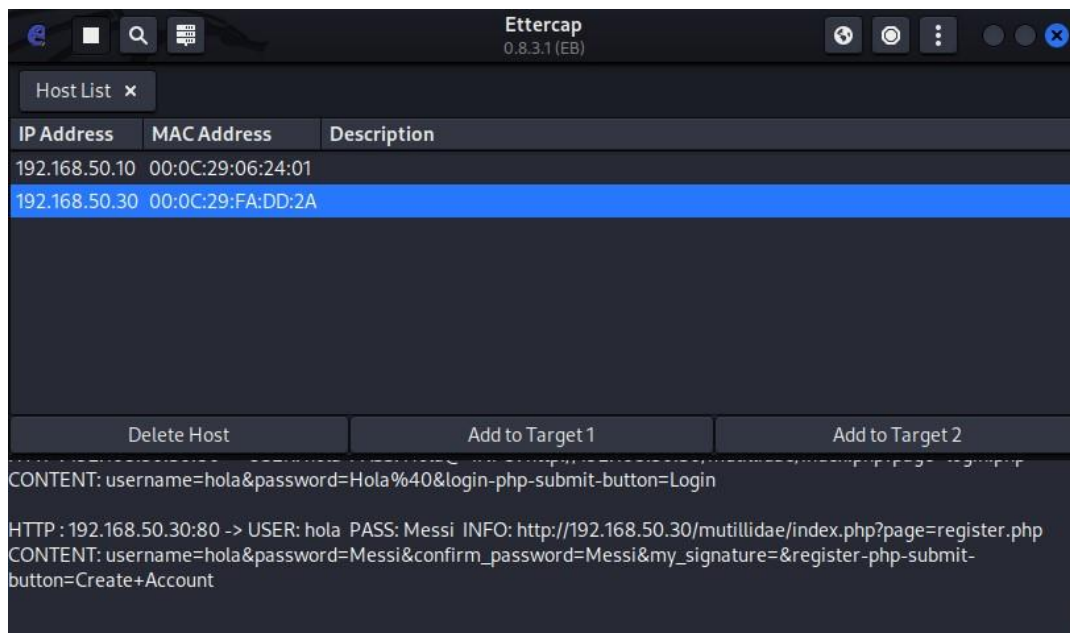
Ainsi, tout le flux passe par la machine du pirate qui peut se mettre en écoute avec un logiciel de capture de trames.

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'empoisonner le cache ARP, comme on peut le voir

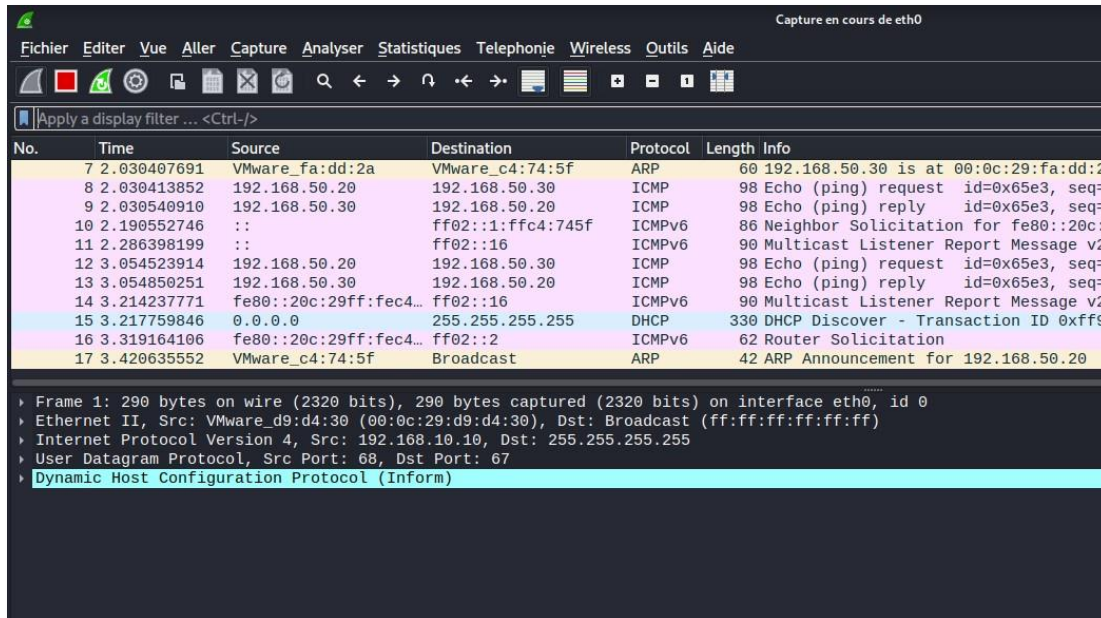


On trouve notre machine victime.





	Titre	Reference	Page	
	MITM	Assurmer	Page 5 sur 8	

3.3 Capture de trame avec Wireshark



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



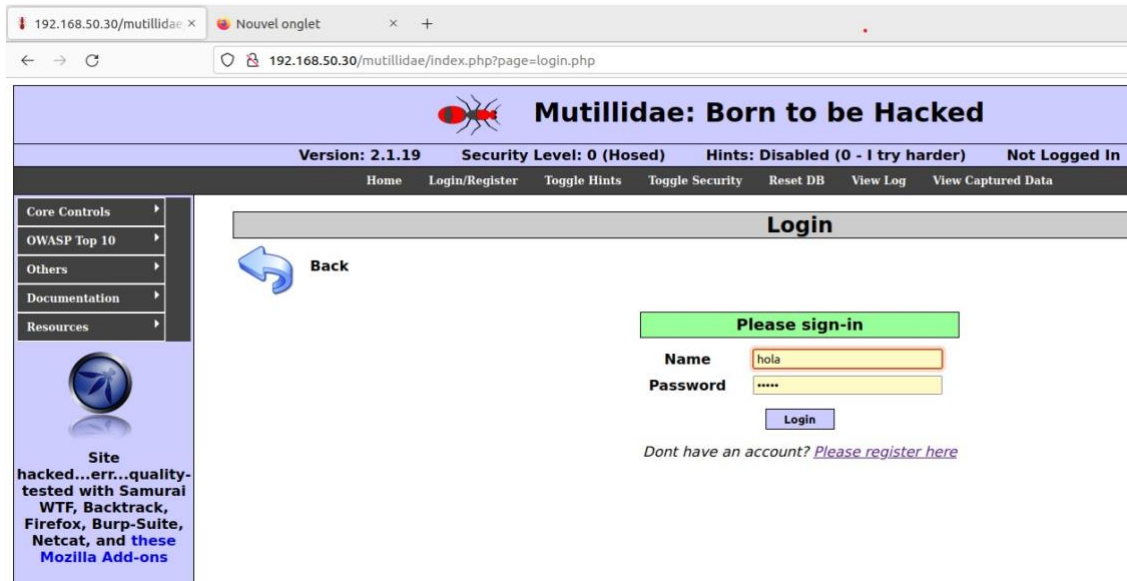
	Titre	Reference	Page	
	MITM	Assurmer	Page 6 sur 8	

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>



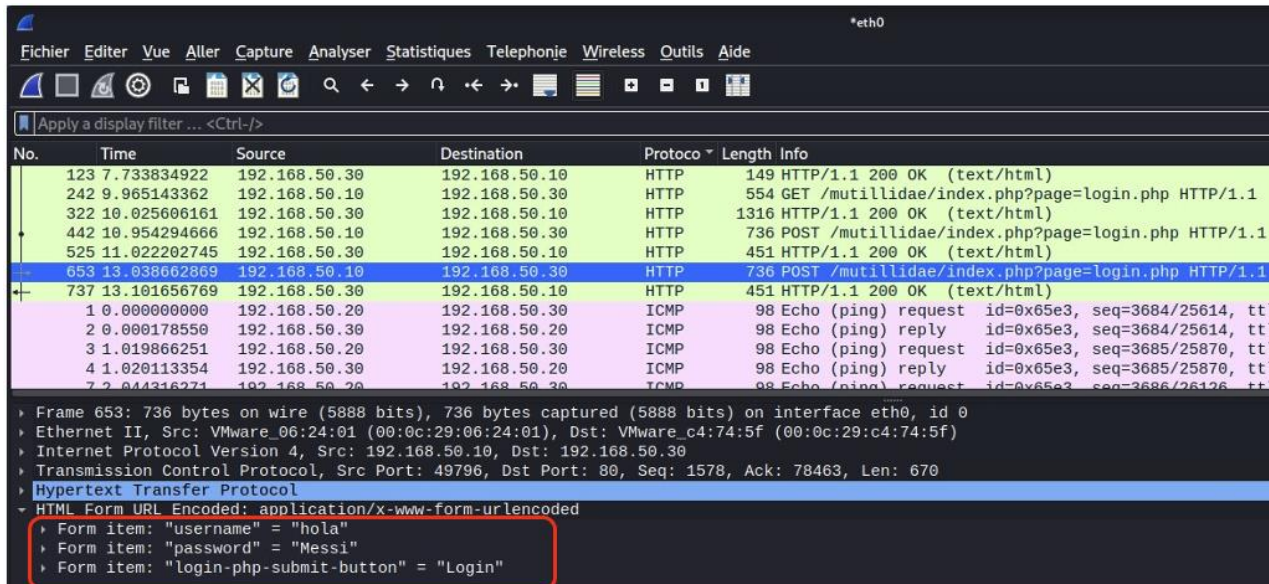
Une fois l'authentification réalisée, nous allons aller dans Kali.



	Titre	Reference	Page	
	MITM	Assurmer	Page 7 sur 8	

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>





The screenshot shows a Wireshark capture on interface eth0. The packet list pane highlights packet 653, which is an HTTP POST request to /mutillidae/index.php?page=login.php. The packet details pane is expanded to show the 'Hypertext Transfer Protocol' section, where the 'HTML Form URL Encoded' field is selected. A red box highlights the form items: 'username' = 'hola', 'password' = 'Messi', and 'login-php-submit-button' = 'Login'.

No.	Time	Source	Destination	Protocol	Length	Info
123	7.733834922	192.168.50.30	192.168.50.10	HTTP	149	HTTP/1.1 200 OK (text/html)
242	9.965143362	192.168.50.10	192.168.50.30	HTTP	554	GET /mutillidae/index.php?page=login.php HTTP/1.1
322	10.025606161	192.168.50.30	192.168.50.10	HTTP	1316	HTTP/1.1 200 OK (text/html)
442	10.954294666	192.168.50.10	192.168.50.30	HTTP	736	POST /mutillidae/index.php?page=login.php HTTP/1.1
525	11.022202745	192.168.50.30	192.168.50.10	HTTP	451	HTTP/1.1 200 OK (text/html)
653	13.038662869	192.168.50.10	192.168.50.30	HTTP	736	POST /mutillidae/index.php?page=login.php HTTP/1.1
737	13.101656769	192.168.50.30	192.168.50.10	HTTP	451	HTTP/1.1 200 OK (text/html)

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.



	Titre	Reference	Page	
	MITM	Assurmer	Page 8 sur 8	

II. Consignes :

Mettre en place quatre machines virtuelles. Un Kali, un Metasploitable 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.

