



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

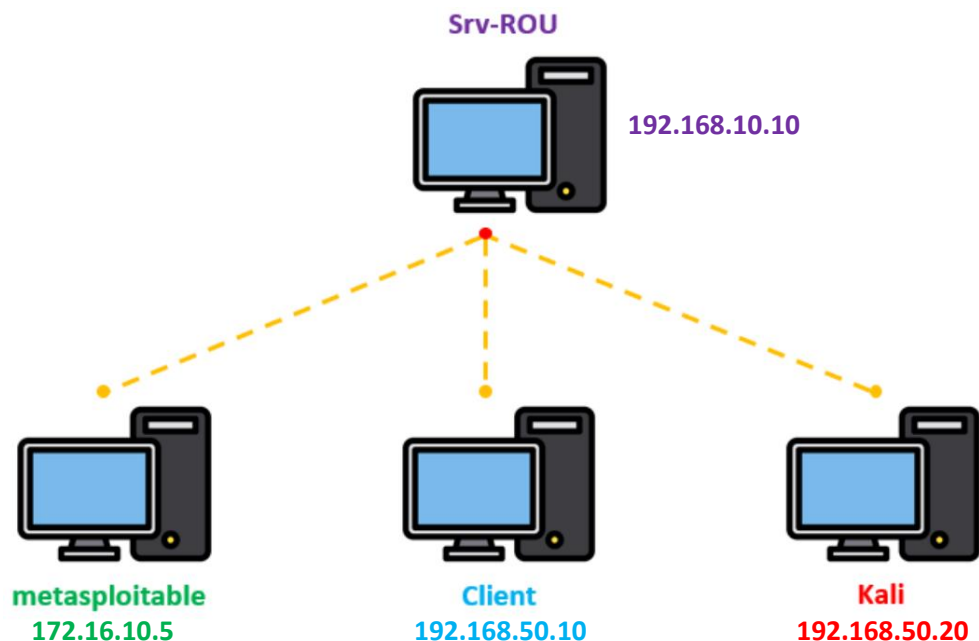
 ASSURMER Services informatiques	Titre	Reference	Page	
	MITM	Assurmer	Page 1 sur 7	

Table des matières

I.	Installation du MITM (Man In The Middle)	2
II.	Fonctionnement du MITM (Man In The Middle)	5

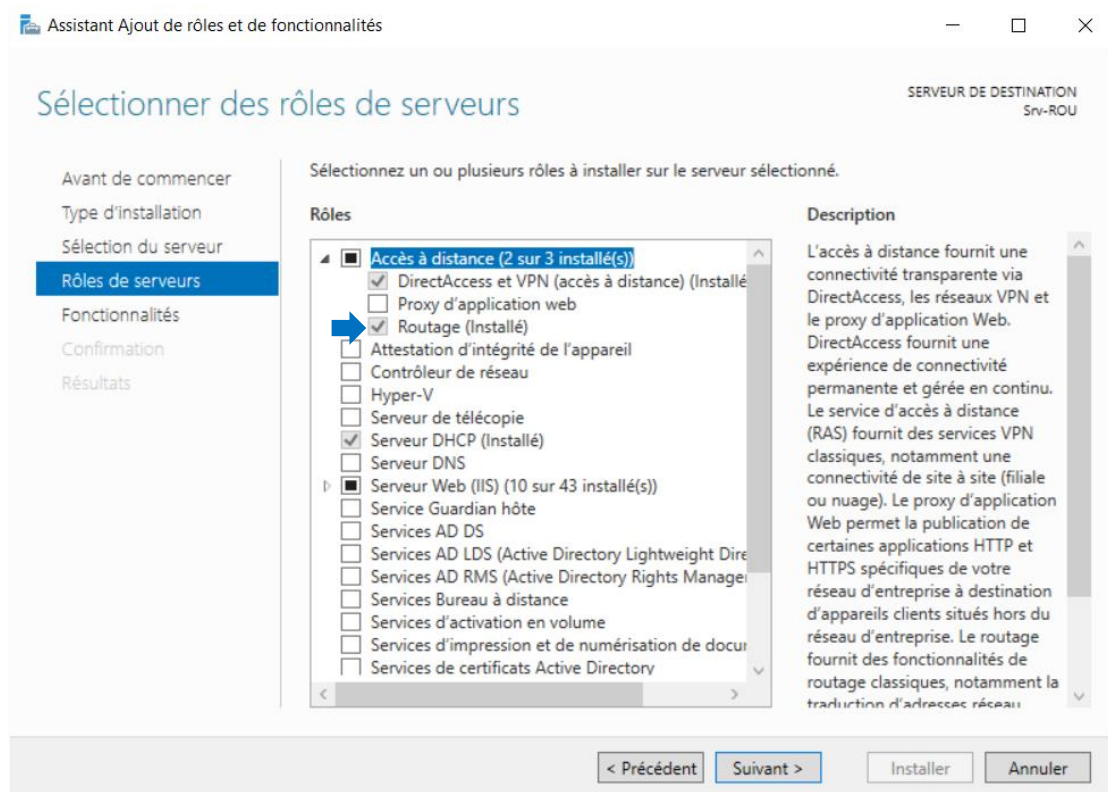


I. Installation du MITM (Man In The Middle)



Le Srv-ROU va nous aider à faire communiquer **metasploitable** avec la machine **cliente** et le **Kali** car ils n'appartiennent pas au même réseau.

Configuration du Srv-ROU



Dans rôles et serveurs, nous allons **installer** :

- **Routage**



Une fois le rôle
Routeur installé,
nous allons le
configurer de
façon qu'il fasse
communiquer nos
deux réseau
distincts.

Configuration de matasploitable

Dans metasploitable nous allons modifier l'adresse IP dynamique afin de mettre en place une adresse IP statique qui est : **172.16.10.5**.

Pour cela nous allons utiliser la commande :

- **Sudo nano /etc/network/interfaces**

```

GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 172.16.10.5
netmask 255.255.0.0
network 172.16.0.0
broadcast 172.16.255.255
gateway 172.16.10.254
dns-nameservers 172.16.10.254 172.16.10.254

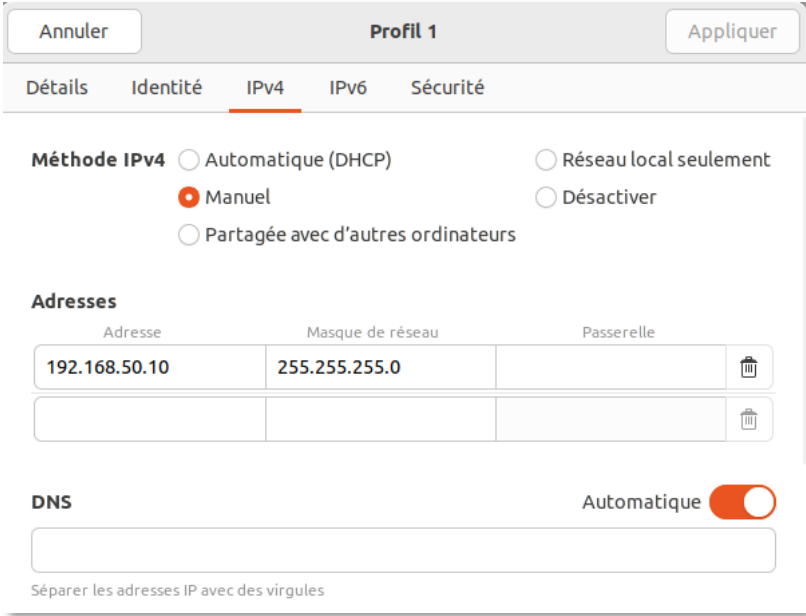
[ Read 16 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell

```

Configuration de la machine cliente

Dans notre machine cliente linux, nous allons mettre en place une adresse IP statique qui est :

192.168.50.10.



Annuler Profil 1 Appliquer

Détails Identité **IPv4** IPv6 Sécurité

Méthode IPv4 ☐ Automatique (DHCP) ☐ Réseau local seulement
☒ Manuel ☐ Désactiver
☐ Partagée avec d'autres ordinateurs

Adresses

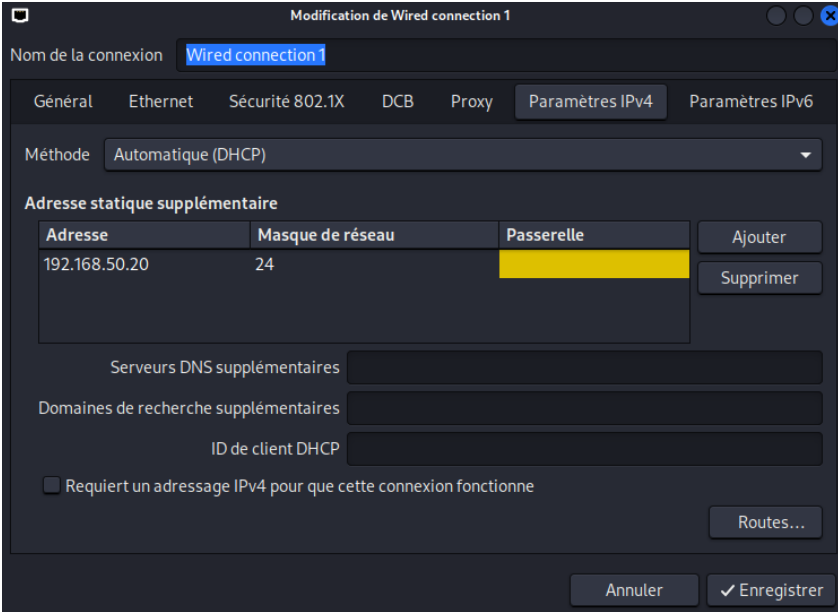
Adresse	Masque de réseau	Passerelle
192.168.50.10	255.255.255.0	

DNS Automatique ☒

Séparer les adresses IP avec des virgules

Configuration de Kali

Dans Kali, nous allons mettre en place une adresse IP statique qui est : **192.168.50.20.**



Modification de Wired connection 1

Nom de la connexion **Wired connection 1**

Général Ethernet Sécurité 802.1X DCB Proxy **Paramètres IPv4** Paramètres IPv6

Méthode Automatique (DHCP)

Adresse statique supplémentaire

Adresse	Masque de réseau	Passerelle
192.168.50.20	24	

Serveurs DNS supplémentaires

Domaines de recherche supplémentaires

ID de client DHCP

☐ Requiert un adressage IPv4 pour que cette connexion fonctionne

Routes...

Annuler Enregistrer



II. Fonctionnement du MITM (Man In The Middle)

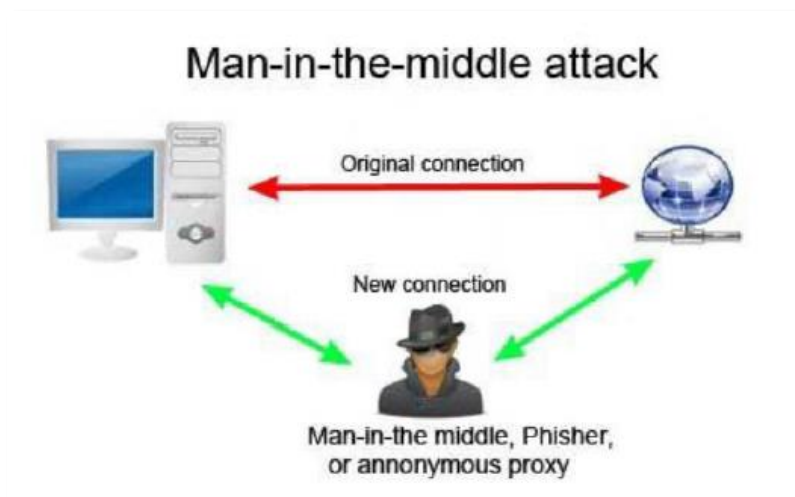
Ce que nous cherchons

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'outil 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.

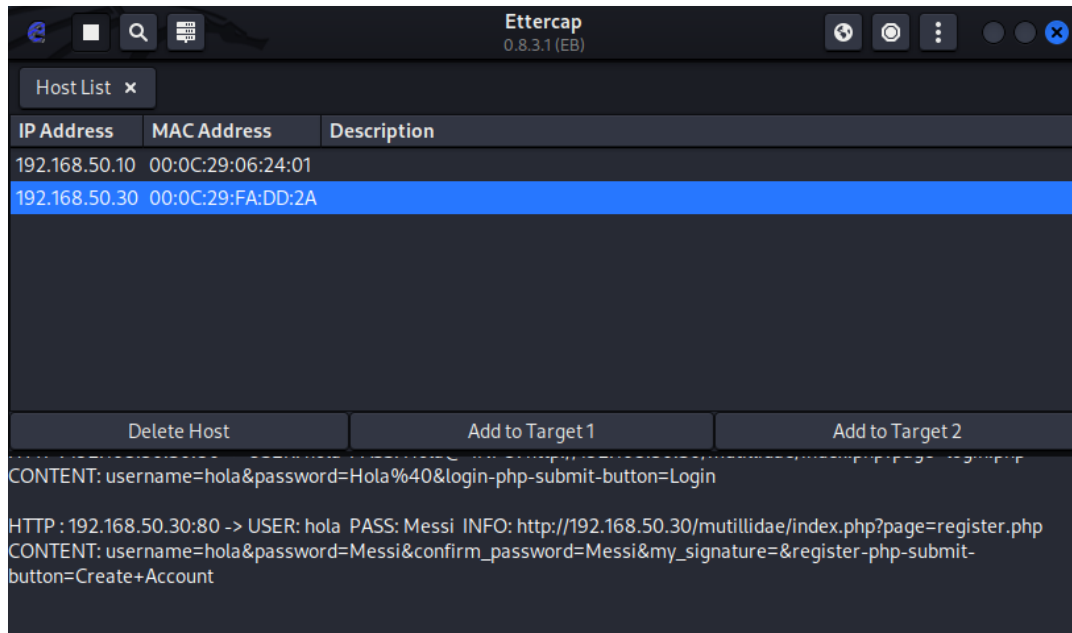
Ainsi, tout le flux passe par la machine du pirate qui peut se mettre en écoute avec un logiciel de capture de trames.

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.

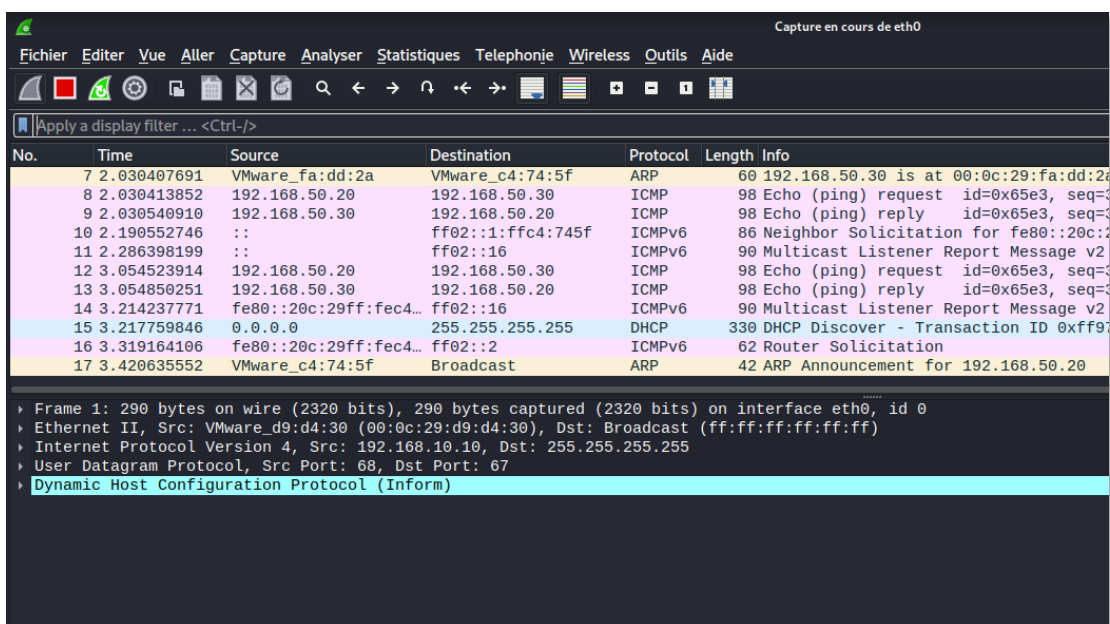
Empoisonnement de cache ARP avec Ettercap

Dans kali, nous allons ouvrir l'outil Ettercap afin empoisonner 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.

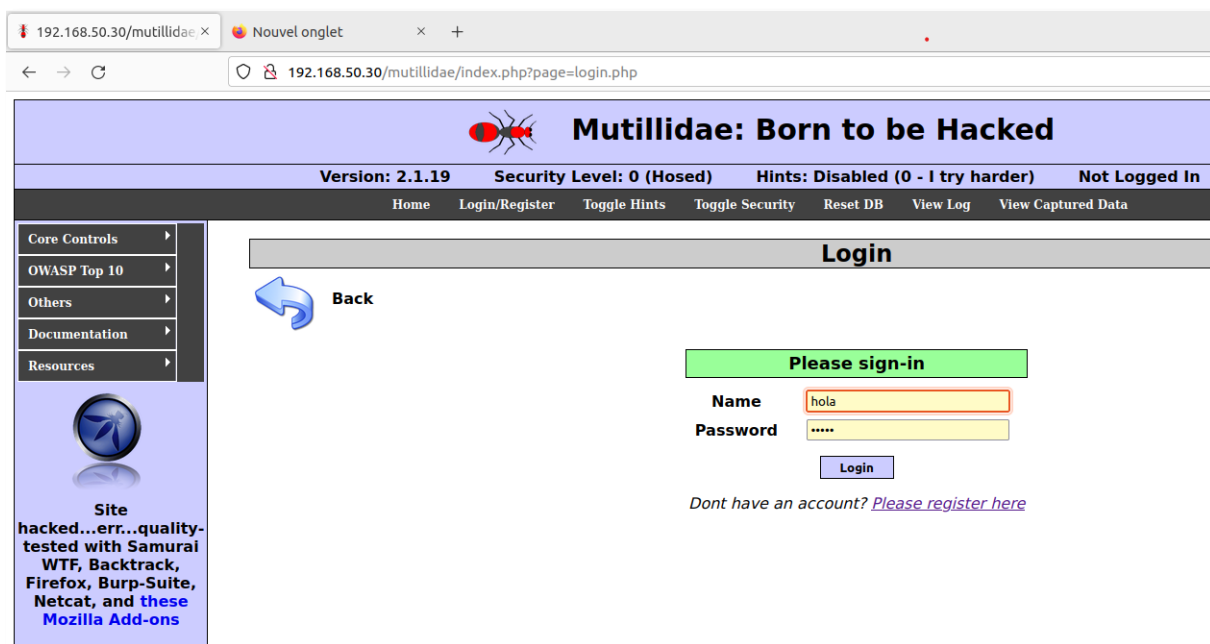


Machine cliente

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** :

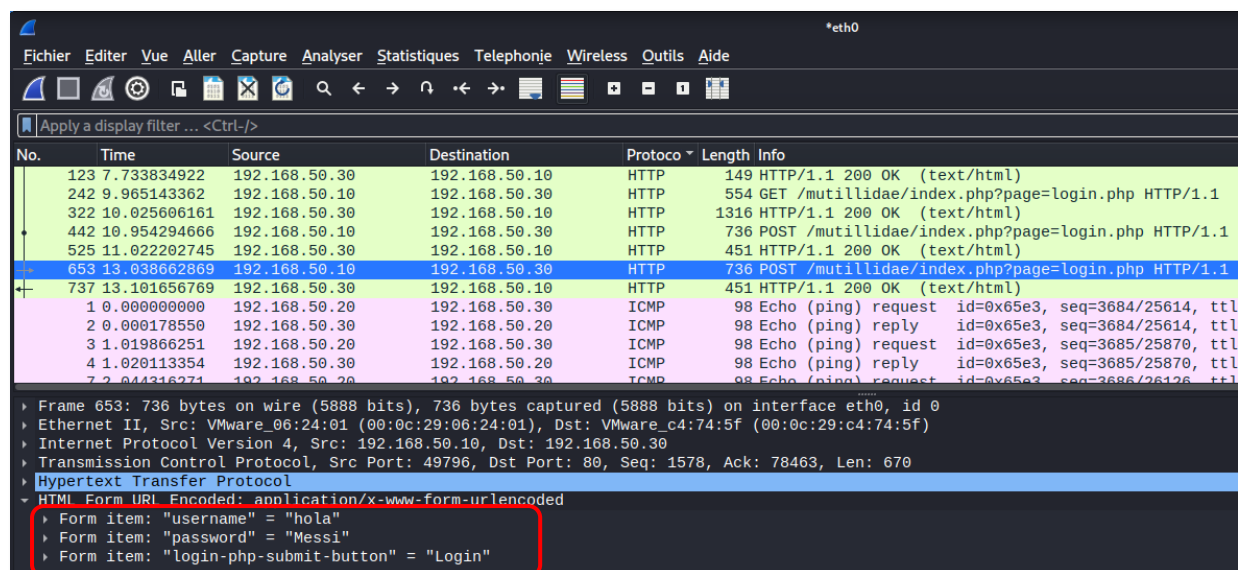
- <https://172.16.10.5/mutillidae>



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.

