Cybersécurité des services informatiques Bloc 3

Table des matières

Présentation du support de formation

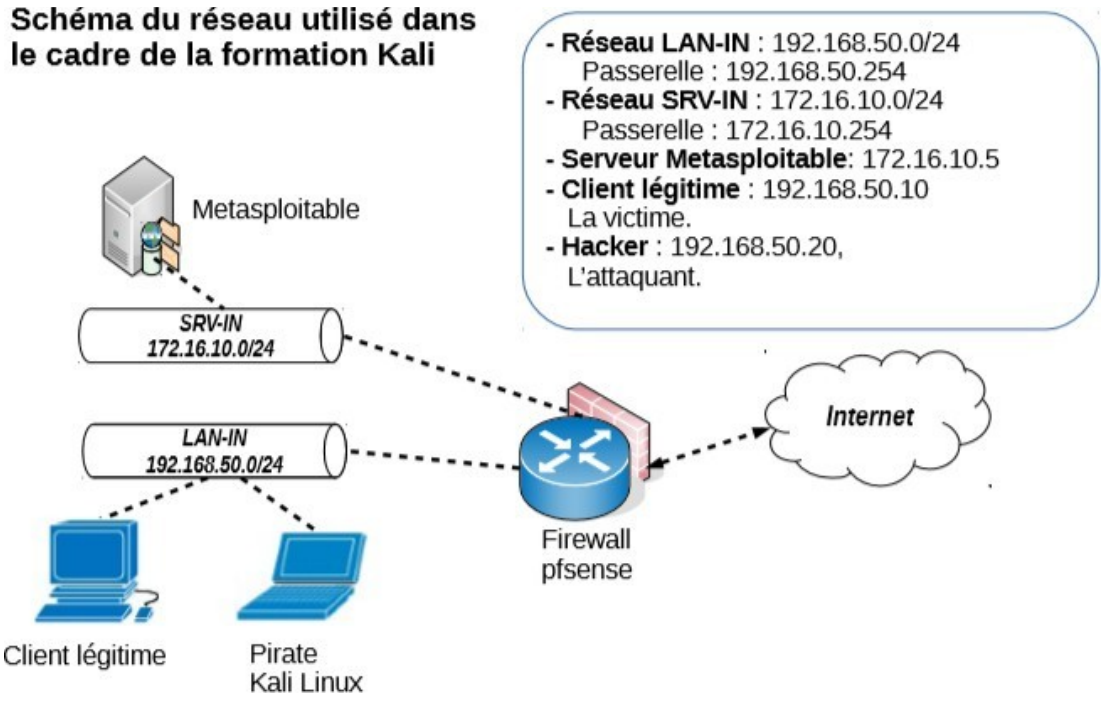
I- Objectifs de la formation

Travaux en laboratoire permettant d'exploiter la distribution kali linux afin d'aborder certaines compétences du bloc 3 sur la cybersécurité. La même distribution sera aussi utilisée dans le cadre des TP de Mme Hadi.

II- Utilisation du support de formation

Chaque travail en laboratoire est destiné à aborder certaines compétences du bloc 3. Les compétences mettent en œuvre les techniques utilisées par les attaquants ainsi que les contre-mesures.

Schéma de la maquette utilisée



III- Présentation des distributions utilisées

Kali Linux

L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion. L'intérêt de Kali linux est de comporter près de 300 outils déjà installés pour travailler dans le domaine de la cybersécurité. Ainsi, une fois la distribution prête, il y a peu d'outils supplémentaires à installer.

Metasploitable

Metasploitable est une distribution linux intentionnellement vulnérable. Son objectif est d'apprendre à tester les principales vulnérabilités en liaison avec la distribution kali linux (https://sourceforge.net/projects/metasploitable). Première connexion : **msfadmin / msfadmin**. Pour avoir un clavier en français, il faut saisir la commande **loadkeys fr** puis valider.

IV- Avertissement

Il convient de compléter chaque démonstration par la présentation des contre-mesures correspondantes (bonnes pratiques de codage, contre-mesure de chiffrement…).

V- Quelques outils utilisés et intégrés dans la distribution kali.

Outils	Utilisation
Arpspoof	Empoisonnement de cache ARP
BurpSuite	Proxy d'attaque
Ettercap	Empoisonnement de cache ARP
Kali	Distribution ethical hacking
Metasploit	Framework d'exploitation de vulnérabilités
Metasploitable	Distribution vulnérable
Mutillidae	Application web vulnérable
Nmap	Scan de ports et de logiciels
Onlinemd5.com	Calcul de somme de contrôles
Pfsense	Pare-feu
Python	Script d'attaques
Stormshield	Pare-feu
VsFTPd	Serveur FTP
Wapiti	Scanner de vulnérabilités
Wireshark	Capture de trames

VI- Travail à rendre

Une documentation par étudiant ou groupe de travail selon les instructions données par le professeur. Chaque documentation comporte des captures d'écrans ainsi que des descriptions sur mes tâches réalisées pour parvenir aux résultats demandés dans le LABO.

LABO n°1 : Vérification de l'intégrité d'une ressource informatique

Présentation

I- Objectifs

Bonnes pratiques en matière de téléchargement d'une ressource informatique. Utilisation des sommes de contrôles afin de garantir l'intégrité d'une ressource.

II- Public

SLAM et SISR.

III- Compétences du référentiel

- Prévenir les attaques ;
- Garantie des critères de disponibilité, d'intégrité et de confidentialité face aux cyberattaques ;
- Assurer la cybersécurité d'une solution applicative et de son développement ;
- Assurer la cybersécurité d'un infrastructure réseau, d'un système, d'un service.

IV- Scénario

Lors du téléchargement de la distribution Kali linux, il convient de mettre en place les deux bonnes pratiques suivantes :

1- Télécharger l'image ISO depuis le site officiel de Kali ;
2- Vérifier la somme de contrôle de l'image téléchargée.

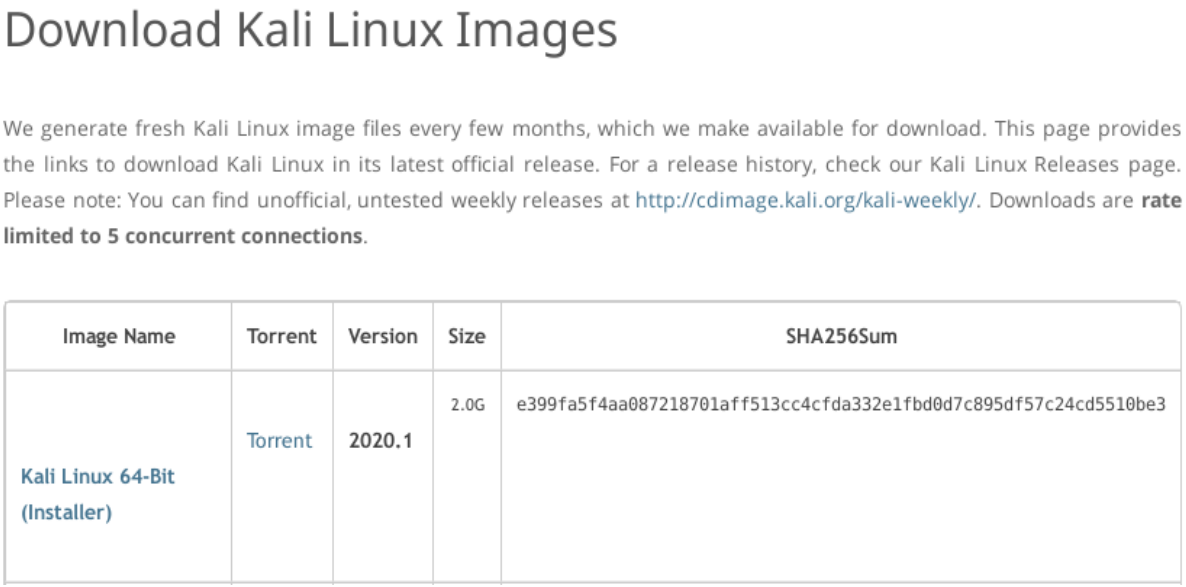
Ces bonnes pratiques peuvent s'appliquer à toute ressource téléchargée dans le cadre de travaux en laboratoires en option SLAM ou SISR. L'objectif est d'éviter le téléchargement d'une ressource non légitime et contenant du code malveillant. Ce code peut permettre à un attaquant d'ouvrir une porte dérobée sur le serveur de la victime.

Exemple : une personne malveillante peut mettre sur internet une distribution kali contenant du code malveillant et la proposer en téléchargement.

Travail à faire

I- Téléchargement de kali depuis le site officiel

Il faut se rendre sur le site officiel de kali : kali.org puis se rendre dans la rubrique de téléchargement.
Sur la page de téléchargement, la somme de contrôle est affichée avec indication de l'algorithme de hash utilisé.



Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/. Downloads are **rate limited to 5 concurrent connections**.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.1	2.0G	e399fa5f4aa087218701aff513cc4cfda332e1fbd0d7c895df57c24cd5510be3

1- Commencer par se rendre sur le site officiel de Kali puis télécharger l'image ISO afin de procéder à l'installation via la création d'une nouvelle machine virtuelle. Si cette installation est déjà réalisée, vous pouvez passer à la question suivante.

https://www.kali.org/downloads/

2- Relever la somme de contrôle associée au fichier ISO de kali. La conserver sur un fichier à part.

3- A l'aide de vos recherches sur internet, expliquer ce qu'est une somme de contrôle.

4- Quelles sont les principales différences entre les algorithmes MD5 et SHA256 ?

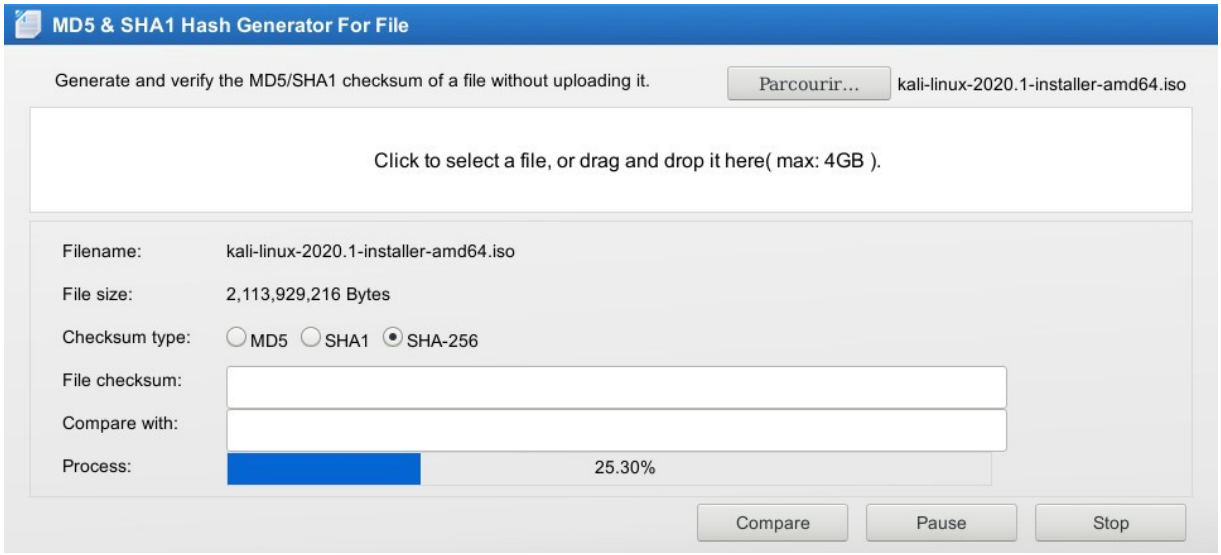
ALGORITHMES	EXPLICATIONS
MD5	
SHA256	

5- Que permet de garantir le calcul des sommes de contrôle ?

6- Rédiger un court paragraphe qui explique les conséquences possibles du téléchargement d'une version non officielle d'un logiciel sans vérification des sommes de contrôle.

II- Vérification de la somme de contrôle

Le site **onlinemd5.com** permet d'illustrer un test de vérification de somme de contrôle. Il convient de sélectionner l'algorithme de hash correspondant à celui indiqué sur la page de téléchargement de kali (sha256).



La somme de contrôle calculée doit être identique à celle indiquée sur le site officiel.

7- Se rendre sur le site onlinemd5.com. Si le site n'est pas accessible, chercher une alternative.

8- Calculer la somme de contrôle du fichier ISO de la distribution kali téléchargée précédemment.

9- Comparer le résultat obtenu avec la somme de contrôle indiquée sur le site officiel de kali. Conclure.

10- Expliquer ce qu'est une porte dérobée.

11- Comment peut-on détecter une porte dérobée ?

III- Procédure sécurisée de téléchargement

Le site officiel de Kali propose une procédure sécurisée pour le téléchargement des images en ligne de commande.

Download Kali Linux Images Securely

When you download an image, be sure to download the **SHA256SUMS** and **SHA256SUMS.gpg** files that are next to the downloaded image (i.e. in the same directory on the Kali Linux Download Server). Before verifying the checksums of the image, you must ensure that the SHA256SUMS file is the one generated by Kali. That's why the file is signed by Kali's official key with a detached signature in SHA256SUMS.gpg. Kali's official key can be downloaded like so:

Kali propose une autre méthode permettant un téléchargement sécurisé. Voir la capture d'écran ci- dessus.

12- Se rendre à nouveau sur la page de téléchargement de kali dans la rubrique associée à la capture d'écran ci-dessus.

https://www.kali.org/downloads/

13- Suivre la procédure de téléchargement indiquée en utilisant le terminal de votre machine physique.

14- Expliquer le rôle des commandes suivantes en consultant le manuel en ligne de commande.

Le manuel d'une commande peut se lancer à l'aide de la commande **man** suivi du nom de la commande.

COMMANDES	EXPLICATIONS
wget	
gpg	

15- A quoi correspond le terme **fingerprint** présent dans les options de la commande **gpg** ?

IV- Machines virtuelles kali

Kali propose de télécharger directement des machines virtuelles prêtes à l'emploi. Ces machines sont disponibles sous VMWare et sous VirtualBox.

Avec une machine VirtualBox importée (fichier OVA), la connexion se fait avec le **login kali** et **le mot de passe kali**. Pour passer en root, il faut saisir la commande **sudo su** puis valider. Pour avoir un clavier en français, il faut saisir la commande **setkxbmap fr** puis valider.

16- Tester le téléchargement d'une machine virtuelle kali prête à l'emploi au format VirtualBox.

17- Démarrer la machine virtuelle téléchargée et essayer de vous connecter.

LABO n°2 : Besoin de chiffrement des connexions

Présentation

I- Objectifs

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.

II- Public

SISR.

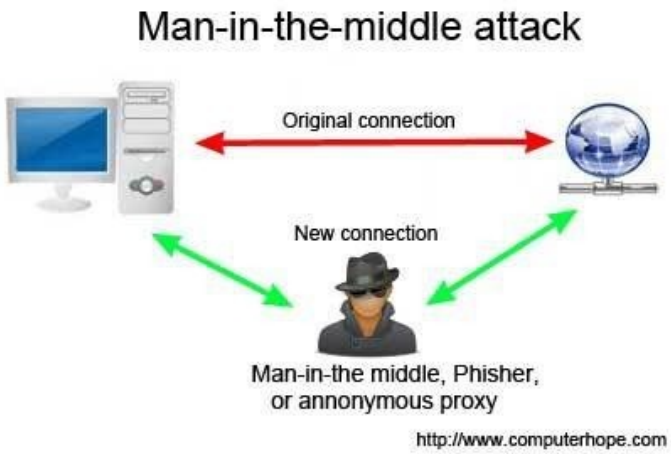
III- Compétences du référentiel

- Prévenir les attaques ;
- Analyser les connexions ;
- Garantie des critères de disponibilité, d'intégrité et de confidentialité face aux cyberattaques ;
- Assurer la cybersécurité d'une solution applicative et de son développement ;
- Assurer la cybersécurité d'un infrastructure réseau, d'un système, d'un service.
- Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures.

IV- 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 les outils **Ettercap** ou **arpspoof** pour réaliser l'empoisonnement de cache ARP.



V- Logiciels utilisés

- Arpspoof ou Ettercap via kali linux ;

- Wireshark via kali linux

Travail à faire

I- Empoisonnement du cache ARP via Arpspoof

Eléments d'explications :

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.

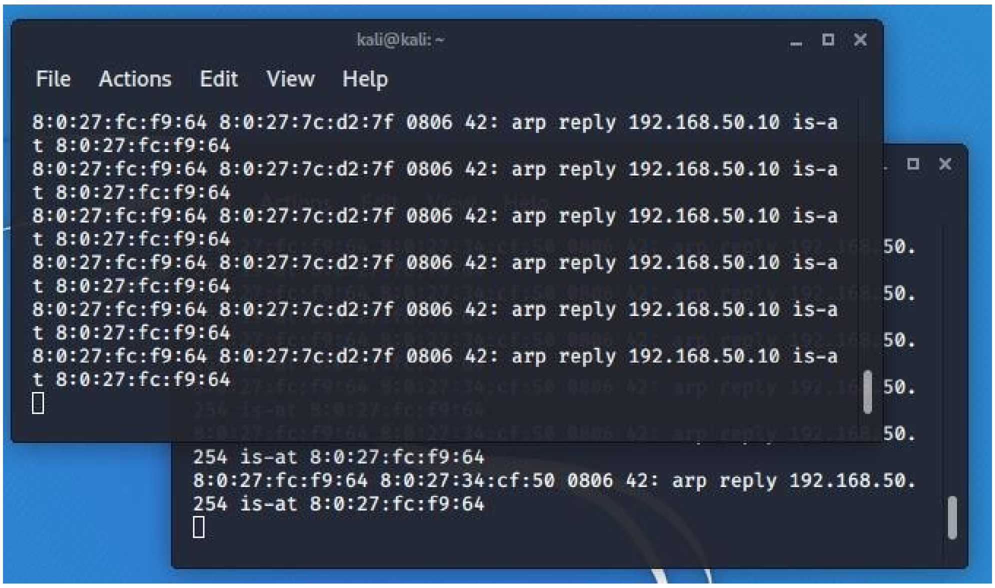
<u>Consultation des caches ARP avant l'empoisonnement :</u>

Depuis la machine cliente légitime.

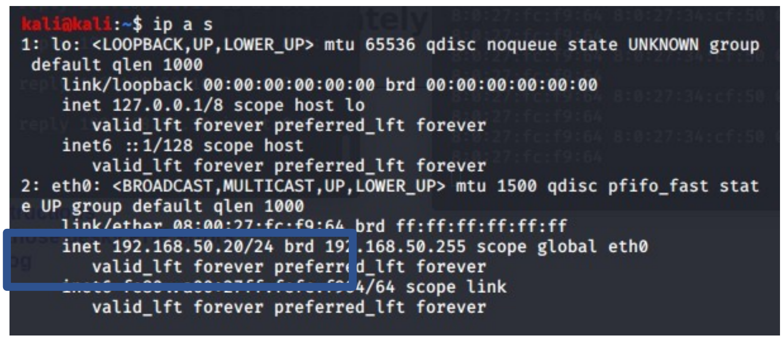
<u>Empoisonnement des caches ARP de la victime et de la passerelle :</u>

Depuis la machine pirate kali en ouvrant deux fenêtres de type terminal.

#arpspoof -t 192.168.50.10 192.168.50.254
#arpspoof -t 192.168.50.254 192.168.50.10

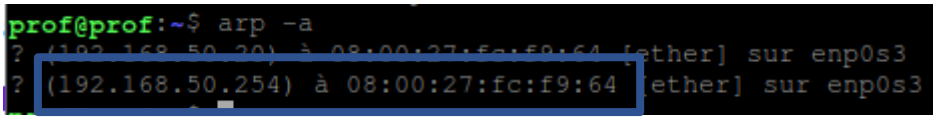


Configuration IP de la machine kali.



Consultation du cache ARP après l'empoisonnement :

Depuis la machine cliente légitime victime.



Travail à faire :

L'objectif est d'empoisonner le cache ARP de la machine cliente légitime afin de pouvoir mettre en place une écoute clandestine (eavesdropping). Tous les flux de la victime passeront par la machine pirate kali.

1- Commencer par démarrer les 4 machines du contexte :

- Kali ;
- Metasploitable ;
- Le client légitime ;
- Le firewall Pfsense.

Ensuite, vérifier la connectivité de l'ensemble à l'aide de commandes ping.

2- Consulter le cache ARP de la machine cliente légitime avant de réaliser l'attaque.

ADRESSE MAC	ADRESSE IP

3- Rappeler la différence entre une adresse IP et une adresse MAC.

4- Depuis la machine kali, réaliser une attaque de type empoisonnent de cache ARP.

5- Consulter à nouveau le cache ARP de la machine cliente victime.

ADRESSE MAC	ADRESSE IP

Que remarquez-vous ?

II- Capture de trame avec Wireshark

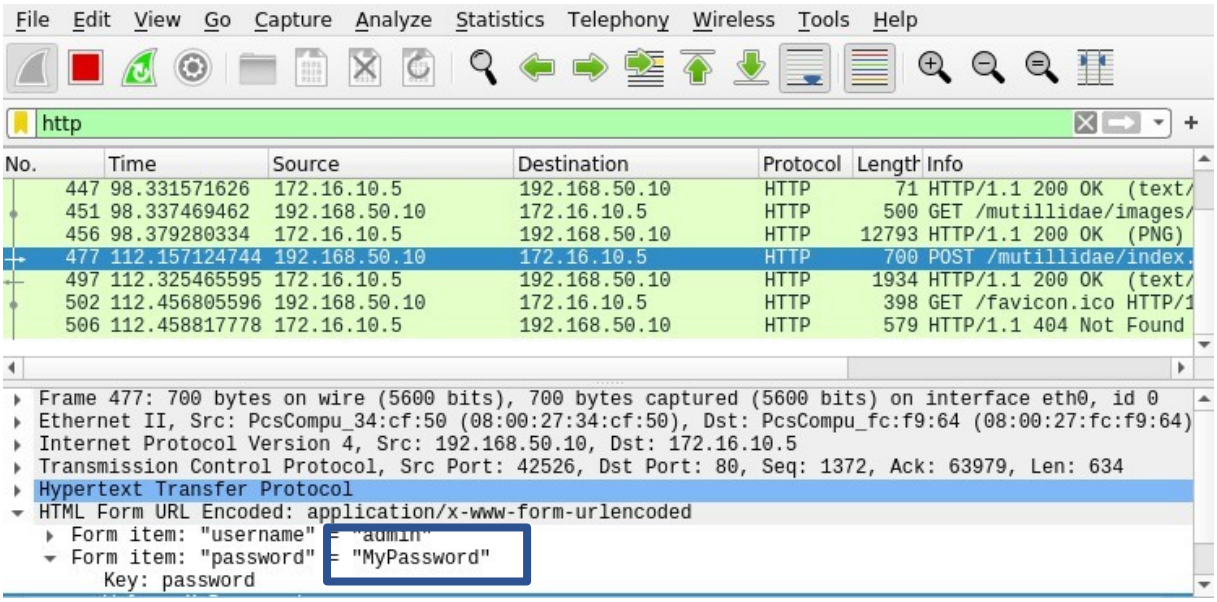
L'étudiant utilise la machine du pirate pour réaliser une capture de trame sur le protocole HTTP depuis la machine kali. Lorsque la victime s'authentifie sur le site Mutillidae en HTTP, le pirate peut capturer le mot de passe saisi.

6- Depuis la machine cliente légitime, ouvrir un navigateur puis s'authentifier sur le site Mutillidae : https://172.16.10.5/mutillidae

7- Créer un compte sur l'application Mutillidae.

III- Récupération du mot de passe de la victime

Le flux n'étant pas chiffré, le pirate peut capturer le mot de passe de la victime.



8- Depuis la machine kali, ouvrir le logiciel Wireshark puis configurer une écoute sur le protocole HTTP.

9- Depuis la machine cliente victime, se connecter au site Mutillidae à l'aide du compte crée précédemment.

10- Depuis la machine kali, retrouver le mot de passe saisi par la victime.

IV- Contre-mesures

1ère contre-mesure : chiffrement HTTPS :

Le chiffrement des flux avec le protocole HTTPS n'empêche pas l'empoisonnement de cache ARP mais rend le flux capturé incompréhensible par l'attaquant.

2ème contre-mesure : inspection du cache ARP :

Des outils permettent de contrôler les modifications du cache ARP afin de vérifier les modifications suspectes : arpwatch.

11- Configurer un virtualhost HTTPS en utilisant le certificat par défaut d'Apache sur le site Mutillidae et tester à nouveau l'attaque.

12- L'attaque est-elle possible ? La capture du mot de passe est-elle possible ?