Fiche pratique n’1 : Besoin de chiffrement des flux

* 1. Objectifs

Mettre en place une écoute clandestina via un positionnement (Man In The Middle) avec empoisonnement cache ARP

Utiliser le protocole HTTPS afin de chiffrer les flux vers un serveur web

Q1.

Remarque : La machine Kali du pirate doit jouer le role du routeur, il faut donc activer le routage sur cette machine donc il faut ouvrir le fichier /etc/sysctl.conf

Pour cela il faut enlever le commentaire devant le : net.ipv4.ip forward=1

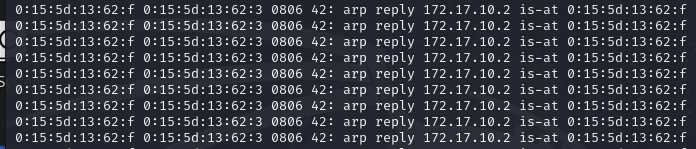
Q3. Relever le cache ARP de la machine cliente

00 :15 :5d :13 :62 :03 -> adresse ip : 172.17.10.10

Q5.

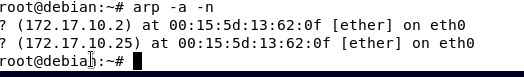
Arpspoof –t @ip-client-victime @ip passerelle (celle du RTR)

172.17.10.10 172.17.10.2

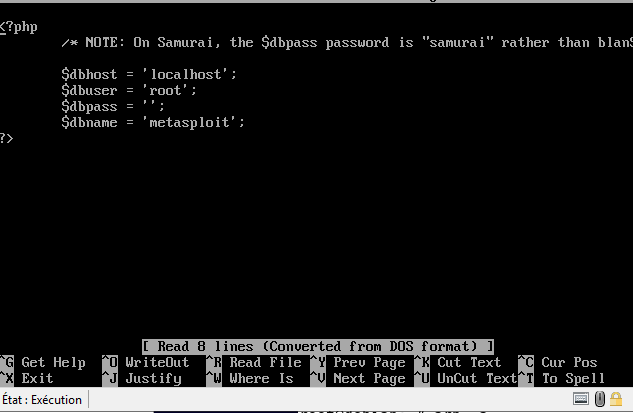


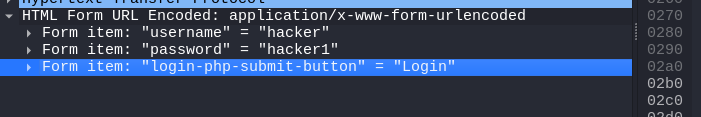
Arpspoof –t @ip-passerelle @ip-client-victime

Q6. Relever à nouveau le cache ARP de la victime



On remarque le serveur Kali a recuperer l’adresse MAC du client pour devenir sa passerelle à présent.



Depuis la machine cliente, on se connecte au navigateur via l’adresse IP du serveur Metasploitable (172.17.1.7) puis nous allons sur notre serveur Kali afin de capturer la trame Eth0 donc j’inscrit dans le moteur de recherche du Serveur Kali l’adresse IP du serveur Metasploitable, je m’identifie puis je reviens sur le serveur Kali et je regarde la section « 

q.4 : Ci-dessus on peut trouver le mot de passe du client piraté

Q.5 : Le mot de passe est visible

2.3 – Contre-mesures

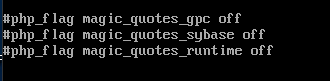
Configurer un virtualhost HTTPS sur l’application Mutilliedae en suivant les étapes suivantes :

Depuis la machine Metasploitable qui heberge l’application Mutillidae :

Ouvrir le fichier htaccess situé à la racine de l’application :

/var/www/mutillidae/.htaccess

**Mettre en commentaire les trois lignes commençant par php**



Se rendre dans le repertoire /etc/apache/sites-enabled/ puis créer le fichier default-ssl en y mettant le contenu suivant :



Si l’on installe le certificat, il faut activez d’abord HTTPS pour une connexion TLS :

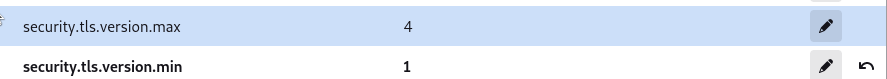
A2enmod ssl

Ensuite pour une connexion sécurisé, activez le virtualhost SSL par défaut

A2ensite default-ssl

**Regler le probleme de certificat :**

**Se rendre sur le navigateur FireFox puis tapez dans la barre de recherche : about :config**



Q2. Expliquer le code noté dans le fichier ssl

Q3.

L’empoisonnement ARP n’est plus possible lorsqu’on se connecte au login et au mot de passe, on capture la trame eth0

Les données sont passé donc chiffré



Q4. C’est une obligation légalecar elle contient des informations confidentiels et à partir du moment qu’on traite des données à caractère personnel nous devons chiffrer les comptes du site

Q5. Surveillance cache ARP

Un reseau doit être surveillé pour éviter toute sorte d’anomalie d’instrusion, il est important de metttre en place des mesures de prevention comme des outils qui permettent d’aider et à prévenir les attaques : ARPswatch