Kali : le besoin de chiffrement des flux

Présentation

Objectifs

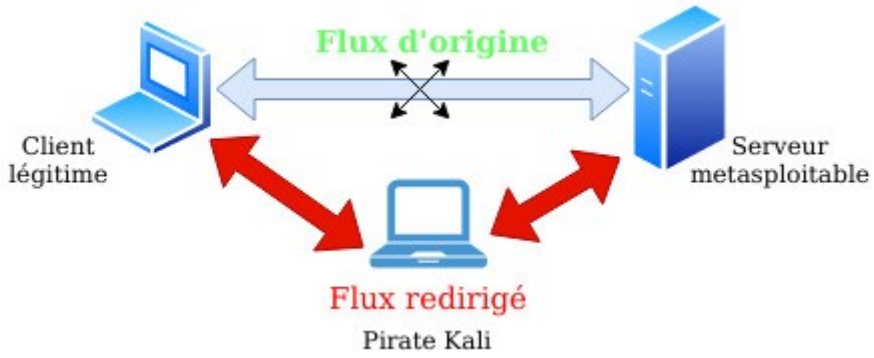
- Mettre en place une écoute clandestine via un positionnement MITM (Man In The Middle) avec empoisonnement de cache ARP.
- Utiliser le protocole HTTPS afin de chiffrer les flux vers un serveur web en tant que contre-mesure.

Scénario

Un étudiant hacker empoisonne le cache ARP d'un autre étudiant (client légitime) et récupère le mot de passe de son compte Mutillidae via une connexion non sécurisée http.

La contre-mesure passe par le chiffrement des conversations.

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 du cache ARP.



Logiciels utilisés

- Arpspoof ou Ettercap (ou bettercap) via Kali Linux. Si la commande arpspoof n'est pas installée, il faut installer le paquet dsniff.
- Wireshark via Kali Linux.

Manipulations

Empoisonnement du cache ARP via arpspoof

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.

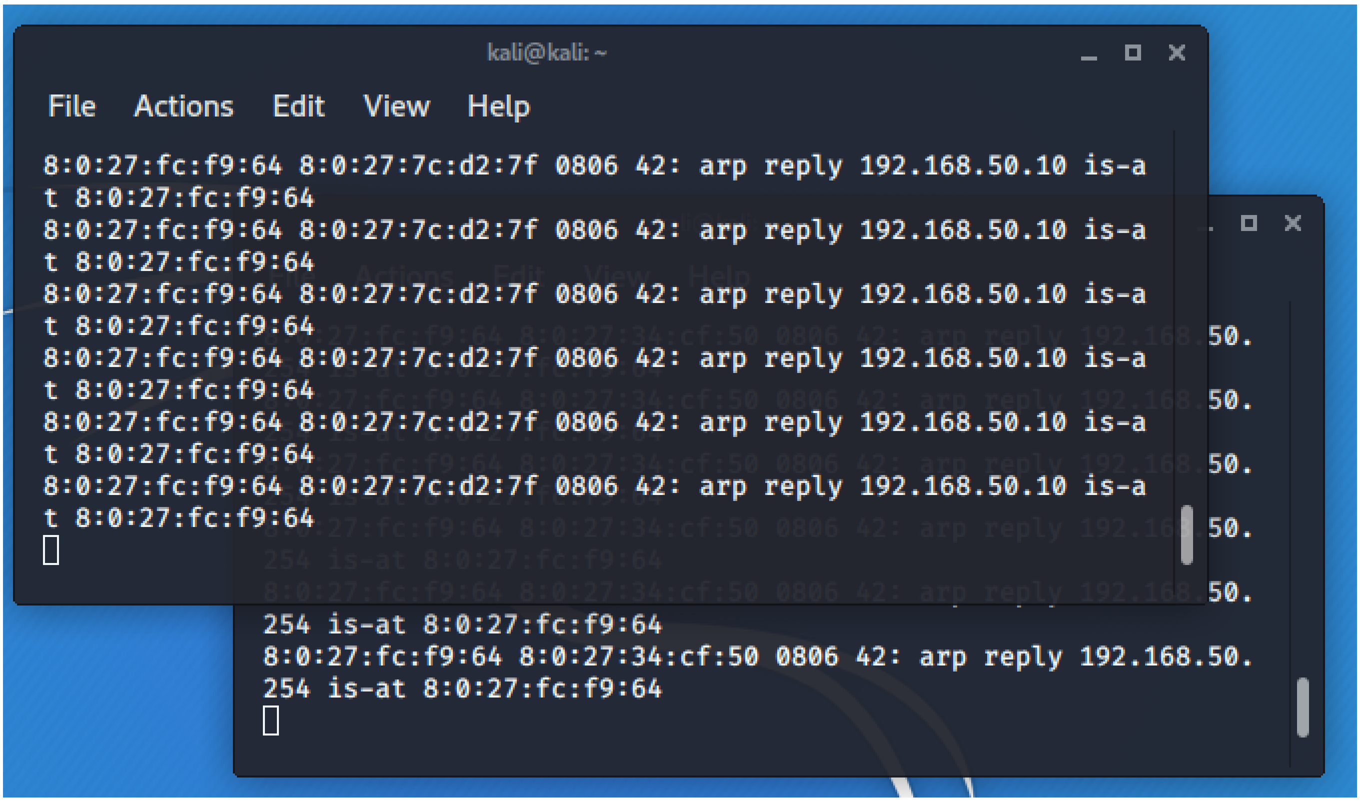
Consultation des caches ARP avant l'empoisonnement :

Par exemple, dans la capture d'écran ci-dessous, le cache ARP de la machine cliente légitime (prof@prof) est relevé avant la réalisation de l'attaque. La correspondance adresse ip/adresse MAC indiquée est donc non falsifiée.

Empoisonnement des caches ARP de la victime et de la passerelle :

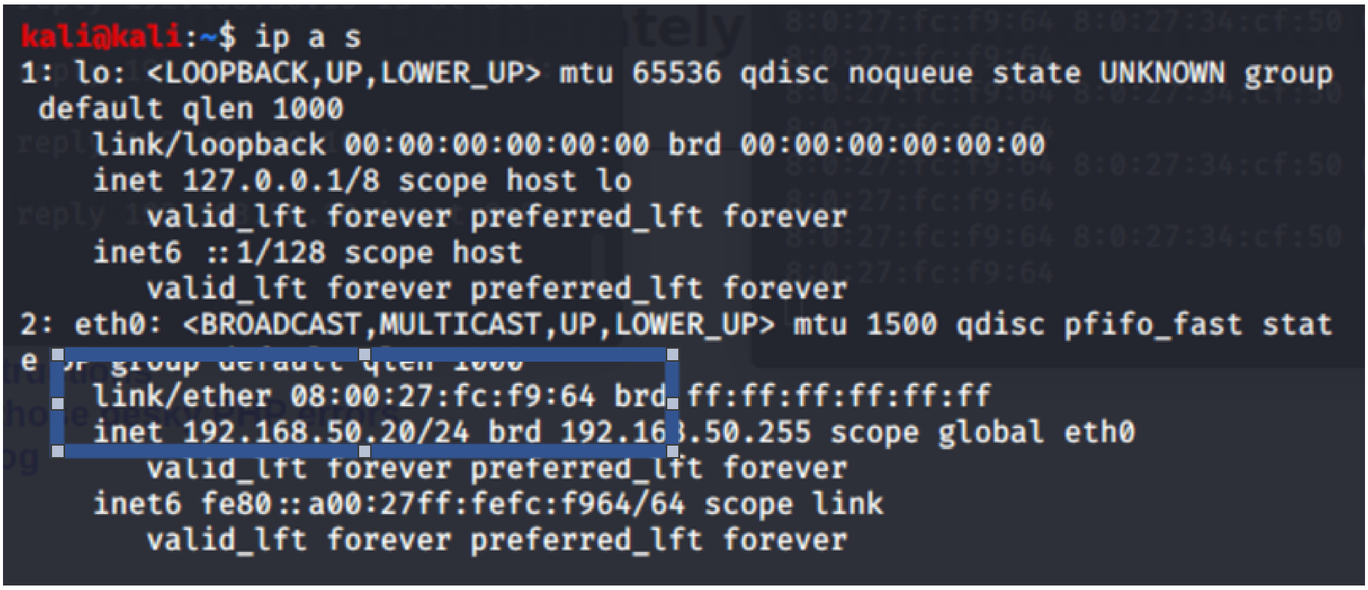
L'étape suivante consiste à réaliser l'empoisonnement ARP. Depuis la machine pirate kali en ouvrant deux fenêtres de type terminal.

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



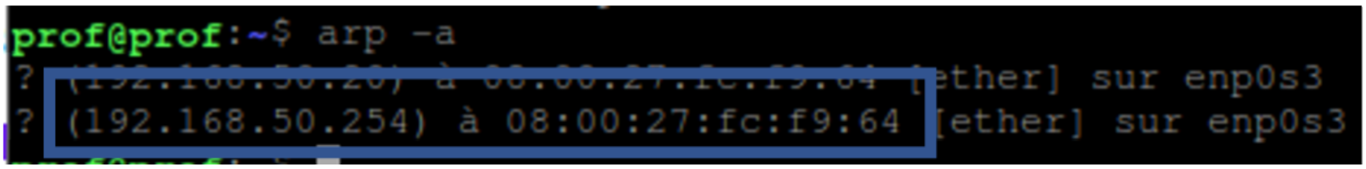
Configuration IP de la machine kali :

La configuration IP de la machine kali est donnée à titre d'illustration afin de pouvoir relever l'adresse IP et l'adresse MAC du pirate.



Consultation du cache ARP après l'empoisonnement :

- Depuis la machine cliente légitime victime.



Dans cette capture d'écran, l'attaque est un succès car l'adresse IP de la passerelle est associée à l'adresse MAC du pirate kali.

Travail à faire

- Q1. Démarrer les 4 machines de la maquette de test :

- 1. Kali ;
- 2. Metasploitable ;
- 3. Le client légitime sous forme de machine virtuelle Linux (plus léger) ;
- 4. Le firewall (stormshield, pfsense ou autre).

Remarque :

- la machine Kali du pirate doit jouer le rôle de routeur. Il faut donc activer le routage sur cette machine. Pour cela, ouvrir le fichier /etc/sysctl.conf, enlever le commentaire devant la ligne suivante et sauvegarder le fichier :

```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
```

- Il faut ensuite exécuter la commande suivante pour recharger les paramètres système :

```
sysctl -p
```

- Q2. Consulter le cache ARP de la machine cliente légitime avant de réaliser l'attaque.

ADRESSE MAC	ADRESSE IP
.	.

* Q3. Depuis la machine Kali, réaliser une attaque de type empoisonnement de cache ARP ciblant le client légitime. Pour cela, suivre les étapes suivantes depuis la machine Kali :

- 1 – Ouvrir un premier terminal en root puis saisir la commande suivante :

```
#arpspoof -t @ip-client-victime @ip-passerelle
```

En remplaçant @ip-client-victime par l'adresse IP du client victime et @ip-passerelle par l'adresse IP de la passerelle sur le routeur.

```
* 2 – Ouvrir un second terminal en root puis saisir la commande suivante :
```

```
#arpspoof -t @ip-passerelle @ip-client-victime
```

En remplaçant @ip-client-victime par l'adresse IP du client victime et @ip-passerelle par l'adresse IP de la passerelle sur le routeur.

- Q5. Consulter à nouveau le cache ARP de la machine cliente victime.

Que remarquez-vous ?

ADRESSE MAC	ADRESSE IP
.	.

Dans la suite du labo, un étudiant utilise la machine du pirate pour réaliser une capture de trames sur le protocole HTTP depuis la machine kali. Lorsqu'un autre étudiant (client légitime) s'authentifie sur l'application Mutillidae de la machine Metasploitable en HTTP, le pirate peut capturer le mot de passe saisi.

Travail à faire 4

Travail préalable :

Vous devez auparavant configurer l'application Multilidae pour utiliser la base de données **owaps10** à la place de la base de données **mutillidae** en modifiant le fichier **/var/www/mutillidae/config.inc** :

Lien : https://ch-info.org/configurer-le-fichier-config-inc-de-mutillidae-dans-metasploitable/

```
$ sudo mano /var/www/mutillidae
```

mskljqlmkjqmfkl

```
* Q1.   Depuis la machine kali, ouvrir le logiciel Wireshark puis configurer une écoute sur le protocole
```

```
HTTP.
```

Q2. Depuis la machine cliente victime, se connecter au site Mutillidae. Créer un nouveau compte si cela est nécessaire.

- Q3. À l'aide d'un analyseur de paquets depuis la machine kali du pirate, peut-on capturer le mot de passe saisi par le client légitime ?
- Q4. Le flux n'étant pas chiffré, le pirate peut-il lire le mot de passe de la victime ? Réaliser la capture écran de cette interception.

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. On peut citer l'exemple de l'outil arpwatch.

Travail à faire 5

- Q1. Configurer un virtualhost HTTPS sur l'application Mutillidae en suivant les étapes suivantes :
  - Depuis la machine Metasploitable qui héberge l'application Mutillidae:
  - 1 – Ouvrir le fichier htaccess situé à la racine de l'application de Mutillidae :

```
#nano /var/www/mutillidae/.htacess
```

Mettre en commentaire les trois lignes commençant par php*flag en ajoutant le caractère # devant :*

```
## The following section disables PHP magic quoting feature.
## Turning these on will cause issues with Mutillidae.
## Note: Turning these on should NEVER be relied on as a method for securing ag$
## As of PHP 6 these options will be removed for exactley that reason.

## Donated by Kenny Kurtz
#php_flag magic_quotes_gpc off
#php_flag magic_quotes_sybase off
#php_flag magic_quotes_runtime off
```

* 2 – Se rendre dans le répertoire /etc/apache2/sites-enable puis créer le fichier default-ssl en y mettant le contenu suivant :

```
 GNU nano 2.0.7              File: default-ssl

<IfModule mod_ssl.c>
        <VirtualHost 172.16.10.5:443>
                ServerName 172.16.10.5:443
                DocumentRoot /var/www

                SSLEngine On
                SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
                SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

                ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
                <Directory "/usr/lib/cgi-bin">
                        AllowOverride None
                        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                        Order allow,deny
                        Allow from all
                </Directory>
        </VirtualHost>
</IfModule>
```

* 3 – Redémarrer le service apache en saisissant la commande suivante : <code shell> #/etc/init.d/apache2 restart </code> * 4 – Depuis la machine client légitime, se connecter à l'application Mutillidae en saisissant l'url suivante : https://172.16.10.5/mutillidae puis accepter le certificat auto signé présenté par défaut via une exception de sécurité. * Q2. En configurant un site en HTTPS, l'empoisonnement de cache ARP est-il toujours possible ? Peut-on encore capturer le mot de passe en clair ? * Q3. Conclure sur l'intérêt du chiffrement dans le contexte du client BOXTOBED.

Remarque :

Vous pouvez configurer une surveillance du cache ARP et répondre à la question suivante :

- Q4. Expliquer pourquoi il peut être important de surveiller les caches ARP de son routeur.