

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

Tout d'abord j'ai lancé la commande :

```
apt-get install net-tools
```

Permettant d'installer les commande arp pour pouvoir voir les caches arp l'address resolution protocol (L'address resolution protocol).

```
root@debian:~# arp -an
? (192.168.50.254) at 00:0c:29:40:a4:29 [ether] on ens33
```

2 - Depuis la machine Kali, réaliser une attaque de type empoisonnement de cache ARP ciblant le client légitime.

[illegible][illegible]

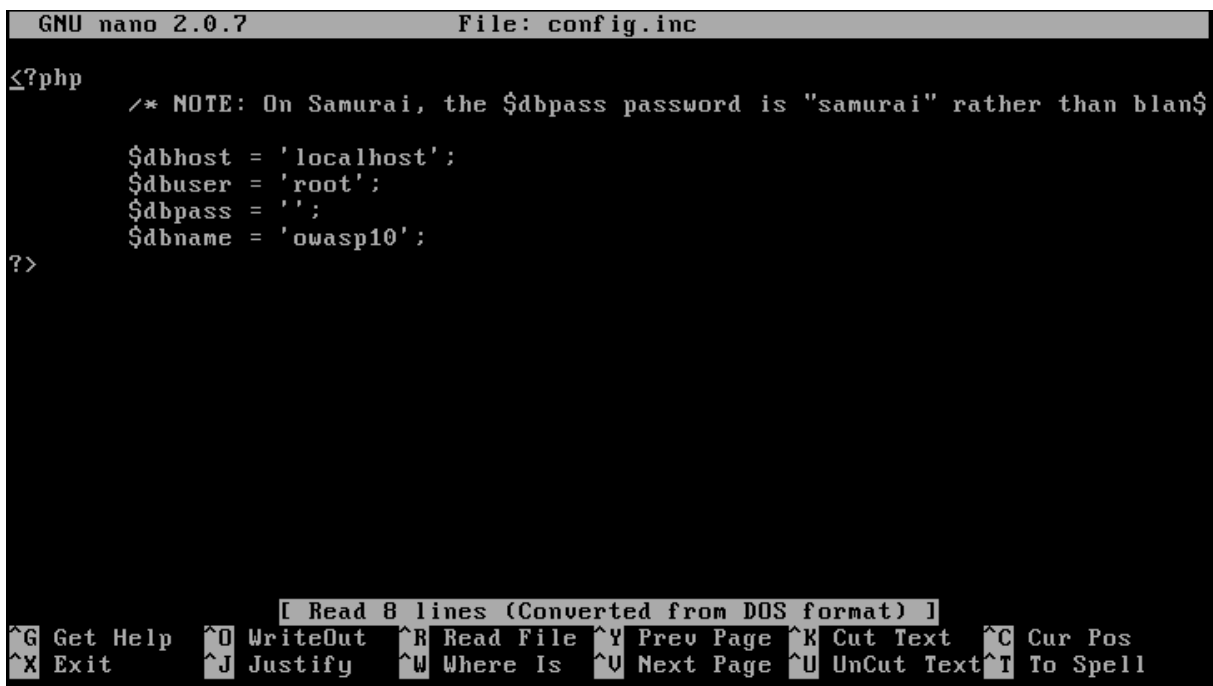
3 - Consulter à nouveau le cache ARP de la machine cliente victime. Que remarquez-vous ?

Je remarque que :

```
? (192.168.50.254) at 00:0c:29:40:a4:29 [ether] on ens33
? (192.168.50.20) at 00:0c:29:95:de:2a [ether] on ens33
```

J'ai une seconde adresse en .20 qui s'est ajouté. Ce qui veut dire que Parrot a réussi à infecter la debian.

4 - En configurant un site en HTTPS, l'empoisonnement de cache ARP est-il toujours possible ? Justifier en effectuant la configuration du site en HTTPS.



```
GNU nano 2.0.7 File: config.inc
<?php
/* NOTE: On Samurai, the $dbpass password is "samurai" rather than blank
$dbhost = 'localhost';
$dbuser = 'root';
$dbpass = '';
$dbname = 'owasp10';
?>
```

[Read 8 lines (Converted from DOS format)]

^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

J'ai ouvert le fichier htaccess situé à la racine de l'application de Mutillidae

J'ai utilisé la commande `#nano /var/www/mutillidae/.htaccess`

J'ai créé un fichier dans mon apache2 et j'ai redémarré le service apache

Le chiffrement des flux avec le protocole HTTPS n'empêche pas l'empoisonnement de cache ARP. Cela rend le flux reçu incompréhensible.

5 - Conclure sur l'expérience réalisée dans le contexte du client BOXTOBED

Beaucoup de solutions existent afin de contrer ce genre d'attaque. Les solutions les plus évidentes bien sûr, sont les gestionnaires de mots de passe avec des mots de passe incompréhensibles, forts voire cryptés.

Le fait déjà de voir qu'on est contaminé est de voir dans la table arp qui nous donnera donc une ligne qui montre la passerelle entre le Kali (ou Parrot) et la Debian.

La plupart des commutateurs Ethernet gérés sont dotés de fonctionnalités conçues pour atténuer les attaques ARP.

Les voyage ARP ne vont pas plus loin qu'en local donc limiter la taille du réseau et son accès est pertinent et permet d'éviter ce genre d'empoisonnement.