

Bloc 3 cybersécurité

Je copie les ISO vers mon hdd et je crée les différentes vm (pfsense ,metasploitable,client légitime,kali)

J'ai créer 2 nouvelles cartes réseaux qui seront 2 interfaces internes

- LAN-IN pour la zone client
- SRV-IN zone serveurs

Une fois toutes mes vm créer je crée une vm debian 11 qui sera un client

Configuration de pfSense :

Appuyer sur boot multi user



Une fois que j'arrive sur cet interface j'appuie sur 1

```

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces         10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system            14) Disable Secure Shell (sshd)
6) Halt system              15) Restore recent configuration
7) Ping host                16) Restart PHP-FPM
8) Shell

```

Ensuite on me demande si je veux utiliser les vlan je dis non

Ensuite on me montre hn0,hn1,hn2 et leur adresse mac

```

Valid interfaces are:

hn0      00:15:5d:13:1a:05   (up) Hyper-V Network Interface
hn1      00:15:5d:13:1a:06   (up) Hyper-V Network Interface
hn2      00:15:5d:13:1a:07   (up) Hyper-V Network Interface

```

Et je dois dire si hn0 est ma patte wan ou lan

Pour vérifier quelles adresse mac correspond a quel adresse mac de mon hyper-V pour mieux définir quel est la patte wan lan etc

PfSenseCybersecu			
Carte	Connexion	Adresses IP	État
Carte réseau (MAC dynamique: 00:15:5D:13:1A:06)	Lan_In	172.16.10.2...	OK
Carte réseau (MAC dynamique: 00:15:5D:13:1A:07)	SRV_IN	0.0.0.0, fe8...	OK
Carte réseau (MAC dynamique: 00:15:5D:13:1A:05)	Intel(R) Ether...	192.168.50....	OK

Résumé	Mémoire	Gestion de réseau	Réplication
--------	---------	-------------------	-------------

Une fois choisis je valide

```
If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.
```

```
Enter the WAN interface name or 'a' for auto-detection  
(hm0 hm1 hm2 or a): hm0
```

```
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(hm1 hm2 a or nothing if finished): hm1
```

```
Optional interface 1 description found: SRU_IN  
Enter the Optional 1 interface name or 'a' for auto-detection  
(hm2 a or nothing if finished): hm2
```

```
The interfaces will be assigned as follows:
```

```
WAN -> hm0  
LAN -> hm1  
OPT1 -> hm2
```

```
Do you want to proceed [y/n]? █
```

Configuration Kali

J'allume la VM kali

Je modifie l'ip de ma kali linux pour qu'elle soit conforme au tp

```
auto eth0  
address 192.168.50.20/24  
gateway 192.168.50.254█
```

Je lui configure sa gateway

Comme sur la capture plus haut

Ne pas oublier de rajouter iface eth0 inet static

Redémarrer l'interface réseaux

Par défaut pfSense n'accepte pas les ping

Configuration metasploitable

J'allume la vm le mdp et login par default est

msfadmin / msfadmin

Je passe le clavier en azerty comme ceci loadkeys fr

Je lui configure son ip : 172.16.10.5

Fiche pratique numero 1 :

Vérifier la somme de contrôle du logiciel notepad

-Installer une des versions du logiciel notepad dans cette installation la somme de contrôle du logiciel est intégrer dans un fichier texte dans le téléchargement

-Ensuite je recalcule la somme du logiciel que je viens d'installer et je verifie qu'elle est exactement identique à celle dans le fichier .txt

Je vais installer notepad sur linux avec ce lien

<https://notepad-plus-plus.org/downloads/v7.5.4/>

En fin de compte je vais utiliser ma Windows car il n'y a pas de nat sur la patte WAN du pare-feu

-J'installe la version du fichier demander

J'ai installer la dernière version du fichier et j'ai trouver le fichier avec les différentes empreintes

Download checksum

- SHA-256/SHA-1/MD5 digests for binary packages

J'appuie dessus

SHA-1 Digest

9633920a02980be62273093c4364bd07b8bb64a2	npp.7.5.4.bin.7z
f6f63a8c489410f465ddbbd2d90f6ba97f590b48	npp.7.5.4.Installer.x64.exe
c5b0205a3aa9ed2c15ad9788281a27c083b044b8	npp.7.5.4.Installer.exe
2bded4510cbc4ecc93c3fcb42a686597ff5bfc36	npp.7.5.4.bin.zip
4034e9f182e52c0d92d9bcf3ff6996d665a0a34c	npp.7.5.4.bin.x64.zip
c61121bb1e04caaf8455528a6855cd0751043611	npp.7.5.4.bin.x64.7z
8bf3a4366060efc8d1fbb04e61e902c8ced9fa01	npp.7.5.4.bin.minimalist.x64.7z
f1ebc737c06c4577d60a56c255b71ff4b2355f26	npp.7.5.4.bin.minimalist.7z

MD5 Digest

68742899078f903de720357bb3bf5b60	npp.7.5.4.bin.7z
2f2db9d802edca5f95badf80c2039811	npp.7.5.4.bin.minimalist.7z
f3006787fce99aae840e3dfaaa4baee8	npp.7.5.4.bin.minimalist.x64.7z
f04a5ed8c5e79fde1241240eaa3b661c	npp.7.5.4.bin.x64.7z
db6a81ed64ec7ab024f62c70be87c01e	npp.7.5.4.bin.x64.zip
d4d9503aef011b434deeb6bc6a16c93b	npp.7.5.4.bin.zip
0079e0ad38bf97d019776bb6a6409359	npp.7.5.4.Installer.exe
1bb3a3b41ac1108dc010258d95285078	npp.7.5.4.Installer.x64.exe

Je copie la somme de fichier de l'installer que j'ai stabilotter en haut je la met dans un fichier

Q3 = Une somme de contrôle est le résultat du hashage des données dans un fichier généralement

Q4=

ALGORITHMES

MD5

SHA256

EXPLICATION

MD5 produit une sortie 128 bits

SHA-256 produit une sortie 256 bits

Q5=

Une somme de contrôle ne permet pas de garantir la confidentialité des échanges mais permet de garantir l'intégrité des documents

TP 2 :

Q1 = Je vais vérifier la somme de contrôle de l'installer de notepad que j'ai installé tout à l'heure à l'aide de la commande Get-FileHash

Voilà le résultat

```
PS C:\Users\Administrateur\Downloads> Get-FileHash .\npp.7.5.4.Installer.exe -Algorithm SHA1

Algorithm      Hash
-----
SHA1           C5B0205A3AA9ED2C15AD9788281A27C083B044B8
Path           C:\Users\Administrateur\Downl...

PS C:\Users\Administrateur\Downloads>
```

Get-FileHash <nomFichier> -Algorithm SHA1

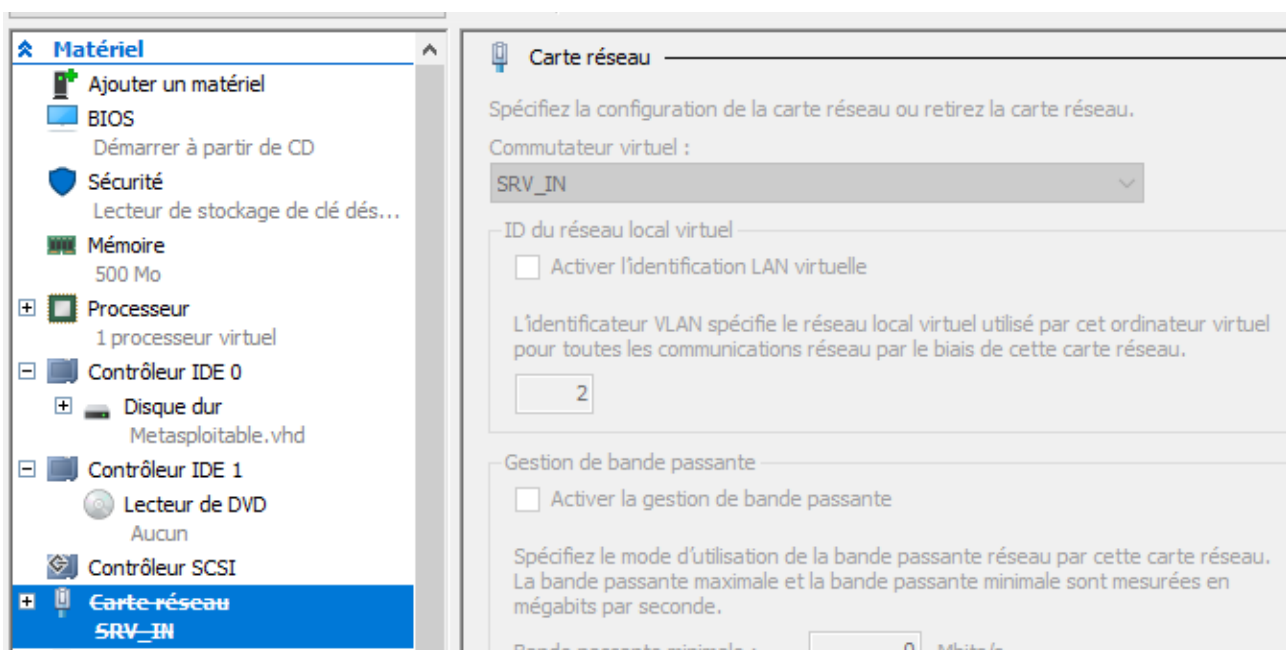
Je compare :

Les 2 sommes de contrôles (hashage) sont identiques l'intégrité de l'installateur est donc garantie

Mise en place MAN IN THE MIDDLE

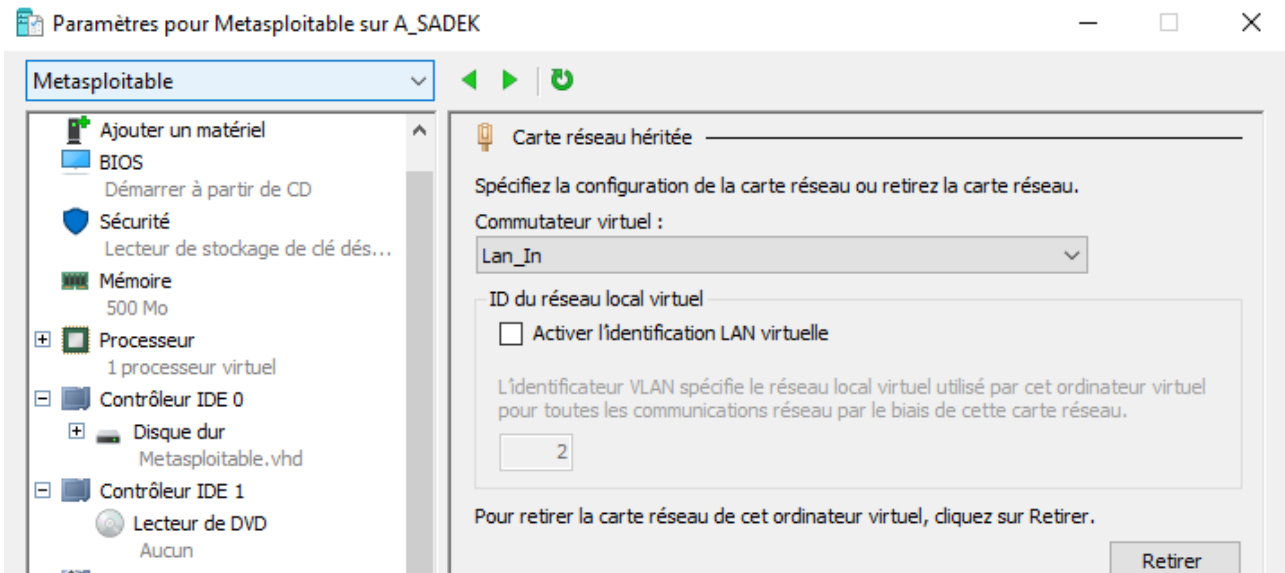
Soluce pour l'interface metasploitable qui bug

Il faut supprimer la carte réseau



Ensuite ajouter du materiel

Carte réseau hérité et mettre notre commutateur



Erreur je modifie Lan_In par SRV_IN

Ma kali linux ping le serveur metasploitable

Je démarre mon client debian

Son ip sera dans le réseau LAN_In = 192.168.50.10

Je vérifie si mon client debian peut aller sur le serveur web de metasploitable



Avant de lancer empoisonnement de cache je regarde

Avant je modifie L'IP de metasploitable parce que je l'ai remis dans l'interface LAN

Je lui met comme ip 192.168.50.15

Ici il y'a L'IP de mon serveur metasploitable plus son adresse mac

```
root@debianAdel:~# arp -a
? (192.168.50.20) at 00:15:5d:13:1a:08 [ether] on eth0
? (192.168.50.254) at <incomplete> on eth0
? (192.168.50.15) at 00:15:5d:13:1a:18 [ether] on eth0
```

J'ai réaliser cette commande depuis mon client légitime

Je vais sur ma machine kali linux

J'active le mode routage IPV4

Je lance la commande

arp spoof -t 192.168.50.10(ip client légitime) 192.168.50.15(ip srv vulnérable)

Cette commande permet d'envoyer au client légitime des trame ARP lui disant l'ip du serveur vulnérable son adresse mac c'est la mienne (celle du hacker kali linux)

Vu que les trames communiquent avec les adr MAC toutes les trames du client légitime vers le srv vulnérable passeront par ma machine kali linux avant et comme j'ai activé le routage je pourrai renvoyer ensuite les trames au serveur metasploitable

J'exécute la commande voici le résultat les trames sont envoyées

```
(root@kali)~# arpspoof -t 192.168.50.10 192.168.50.15
0:15:5d:13:1a:8 0:15:5d:13:1a:d 0806 42: arp reply 192.168.50.15 is-at 0:15:5d:13:1a:8
0:15:5d:13:1a:8 0:15:5d:13:1a:d 0806 42: arp reply 192.168.50.15 is-at 0:15:5d:13:1a:8
0:15:5d:13:1a:8 0:15:5d:13:1a:d 0806 42: arp reply 192.168.50.15 is-at 0:15:5d:13:1a:8
```

J'ouvre un deuxième terminal et j'exécute cette commande

arpspoof -t 192.168.50.15 192.168.50.10

Sa c'est pour le trafic retour je dis au serveur metasploitable que L'IP du client légitime est associée à mon adresse mac ce qui me permet de capter tout le trafic retour

J'exécute la commande

```
(root@kali)~# arpspoof -t 192.168.50.15 192.168.50.10
0:15:5d:13:1a:8 0:15:5d:13:1a:18 0806 42: arp reply 192.168.50.10 is-at 0:15:5d:13:1a:8
0:15:5d:13:1a:8 0:15:5d:13:1a:18 0806 42: arp reply 192.168.50.10 is-at 0:15:5d:13:1a:8
```

Je consulte maintenant ma table ARP sur mon client légitime

Comme on le voit l'adresse mac du serveur metasploitable pour mon client légitime à changer par rapport à tout à l'heure

```
root@debianAdel:~# arp -a
? (192.168.50.20) at 00:15:5d:13:1a:08 [ether] on eth0
? (192.168.50.254) at <incomplete> on eth0
? (192.168.50.15) at 00:15:5d:13:1a:08 [ether] on eth0
root@debianAdel:~#
```

Pour être remplacé par celle de ma VM kali linux

Je lance la commande ip a sur ma VM hacker pour montrer que cette adresse mac appartient bien à la vm hacker kali

```
(root@kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:13:1a:08 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.20/24 brd 192.168.50.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe13:1a08/64 scope link
        valid_lft forever preferred_lft forever

(root@kali)-[~]
└─#
```

Je lance wireshark sur kali linux

Et depuis le client légitime j'essaye de m'identifier sur le serveur metasploit

Je vais ici

Login

 **Back**

Please sign-in

Name	<input style="width: 150px; height: 20px;" type="text"/>
Password	<input style="width: 150px; height: 20px;" type="password"/>
<input style="background-color: #ccccff; border: 1px solid black; padding: 5px 15px;" type="button" value="Login"/>	

Dont have an account? [Please register here](#)

J'enregistre un compte

J'ai renseigné un user et mdp avant de valider je lance wireshark

Username

adel

Password

●●●●●●●●●●

Confirm Password

●●●●●●●●●●

Signature

lmdp |

Create Account

J'ai appuyer sur create account en même temps j'ai lancer la capture des trames via wireshark j'ai mis un filtre pour n'avoir que le trafic http

J'ai capturer la trame avec l'entête post php et dedans il y'a le mdp user etc

Comme ici sur la capture que j'ai fais

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
11 2.554658900 192.168.50.10 192.168.50.15 HTTP 776 POST /mutillidae/index.php?page=re

\r\n
[Full request URI: http://192.168.50.15/mutillidae/index.php?page=register.php]
[HTTP request 1/1]
File Data: 125 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "adel"
  Form item: "password" = "monsupermdp"
  Form item: "confirm_password" = "monsupermdp"
  Form item: "my_signature" = "lemdp "
  Form item: "register-php-submit-button" = "Create Account"

0270 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ
0280 65 73 74 73 3a 20 31 0d 0a 0d 0a 75 73 65 72 6e ests: 1- ... usern
0290 61 6d 65 3d 61 64 65 6c 26 70 61 73 73 77 6f 72 ame=adel &passwor
02a0 64 3d 6d 6f 6e 73 75 70 65 72 6d 64 70 26 63 6f d=monsup ermdp&co
02b0 6e 66 69 72 6d 5f 70 61 73 73 77 6f 72 64 3d 6d nfirm_pa ssword=m
02c0 6f 6e 73 75 70 65 72 6d 64 70 26 6d 79 5f 73 69 onsuperm dp&my_si
02d0 67 6e 61 74 75 72 65 3d 6c 65 6d 64 70 2b 26 72 gnature= lemdp+&r
02e0 65 67 69 73 74 65 72 2d 70 68 70 2d 73 75 62 6d egister- php-subm
02f0 69 74 2d 62 75 74 74 6f 6e 3d 43 72 65 61 74 65 it-butto n=Create
0300 2b 41 63 63 6f 75 6e 74 +Account

```

a

Q3 = Oui on peut capturer le mdp

Q4 = Comme le flux n'est pas crypter oui

2.3 Contre-mesures :

Q1=

Je vais dans le fichier htaccess dans `var/www/mutillidae/.htaccess`

Je met un commentaire sur les trois ligne commençant par `php_flag`

Ensuite je vais dans `etc/apache2/sites-enabled` et je crée le fichier `default-ssl` et je met le contenu demandé dans le fichier

```
<IfModule_mod_ssl.c>
<Virtualhost *:443>
  ServerName 192.168.50.15
  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
    Allow from all
  </Directory>
</VirtualHost>
</IfModule>
```

Je redémarre le serveur apache

Le https est correctement configuré

il fallait installer le module ssl avec la commande

`a2enmod ssl`

Je relance la capture de trame au moment où je saisi mon login mdp

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls
OWASP Top 10
Others
Documentation
Resources

Site hacked...err...quality-tested with Samurai

Back

Please sign-in

Name adel

Password ●●●●●●●●

Login

Dont have an account? [Please register here](#)

Q2 = Oui empoisonnement est toujours possible mais je ne peux pas capturer le mdp en clair

Le protocole ce n'est plus http mais TLS

Les données dans la trame sont cryptée

The screenshot shows a Wireshark interface with a packet list table and a packet details pane. The packet list table shows several TLSv1 packets. The selected packet (No. 81) is expanded in the details pane, showing the TLSv1 Record Layer and the Encrypted Application Data field. The Encrypted Application Data field contains a long hexadecimal string: 12fc59418c3f1c5a6d40ac4e7661afc91282aebd7773e3abbe149603484cb9fa42359fa8...

No.	Time	Source	Destination	Protocol	Length	Info
62	18.783503200	192.168.50.10	192.168.50.15	TLSv1	807	Application Data
67	18.820342400	192.168.50.15	192.168.50.10	TLSv1	1174	Application Data, Application
73	18.823178900	192.168.50.15	192.168.50.10	TLSv1	2962	Application Data
81	18.826158200	192.168.50.15	192.168.50.10	TLSv1	2962	Application Data [TCP segment]
91	18.831605000	192.168.50.15	192.168.50.10	TLSv1	249	Application Data
101	18.834059000	192.168.50.15	192.168.50.10	TLSv1	260	Application Data, Application
107	18.834881000	192.168.50.15	192.168.50.10	TLSv1	1514	Application Data
115	18.836128900	192.168.50.15	192.168.50.10	TLSv1	710	Application Data, Application

```
Internet Protocol Version 4, Src: 192.168.50.15, Dst: 192.168.50.10
Transmission Control Protocol, Src Port: 443, Dst Port: 48858, Seq: 9381, Ack: 1515, Len: 2896
[4 Reassembled TCP Segments (8037 bytes): #73(2859), #75(1448), #79(2896), #81(834)]
Transport Layer Security
  TLSv1 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.0 (0x0301)
    Length: 8032
    Encrypted Application Data: 12fc59418c3f1c5a6d40ac4e7661afc91282aebd7773e3abbe149603484cb9fa42359fa8...
    [Application Data Protocol: http-over-tls]
```

Donc je ne peux plus voir le mdp saisis en clair

Q3 =

L'intérêt du chiffrement dans le contexte est que les données à caractère personnel des utilisateurs ne passeront pas en clair dans le réseaux leur codes de cartes bancaires pour des réservations ici donc si un pirate tente grâce à l'arp spoofing et la capture de trames de récolter ces données à caractère personnel il ne pourra pas car ils sont cryptée avec TLS comme dans la capture en haut ce que j'ai surligner ce sont les données crypter envoyer

Pour arpwatch j'utiliserai ce tuto

<http://arobaseinformatique.eklablog.com/surveiller-votre-reseau-avec-arpwatch-a106417302>

Installation d'un outil de surveillance de cache

Sa permet de surveiller le cache arp d'une machine pour ce prévenir des attaques arpspoof

Je vais installer le paquet arpwatch

-le paquet arpalert ne fonctionne pas j'installe le paquet arpalert

Le fichier de configuration est *etc /arpalert/*

```
GNU nano 5.4 /etc/arpalert/arpalert.conf
# Copyright (c) 2005-2010 Thierry FOURNIER
# $Id: arpalert.conf.in 690 2008-03-31 18:36:43Z $
#
# Default config file
#
# white list
maclist file = "/etc/arpalert/maclist.allow"
# black list
maclist alert file = "/etc/arpalert/maclist.deny"
# dump file
maclist leases file = "/var/lib/arpalert/arpalert.leases"
# list of authorized request
#auth request file = /etc/arpalert/authrq.conf
# log file
log file = "/var/log/arpalert.log"
# pid file
lock file = "/var/run/arpalert.pid"
# log level
use syslog = true
```

On peut préciser le fichier de log le niveau de log etc le fichier est assez simple

Ensuite pour lancer arpalert sur son interface eth0

Il faut taper ceci

```
arpalert -i eth0
```

Ensuite regarder dans le fichier */var/lib/arpalert/arpalert.leases*

On peut voir ceci

```
root@debianAdel:~# tail -30 /var/lib/arpalert/arpalert.leases
00:1a:6d:f5:0c:90 172.17.1.1 eth0 1632898582 458508
00:15:5d:13:1a:0d 172.17.1.12 eth0 1632898582 458430
root@debianAdel:~#
```

On peut voir les adresses mac recenser

Ensuite pour voir toute nouvelle connexion directement il faut aller

/var /log /syslog

On pourra voir ceci

```
Sep 29 08:56:14 debianAdel arpalert[1560]: Starting Ethernet station monitor daemon: (chown arpalert /var/lib/arpalert/arpalert.leases)
Sep 29 08:56:14 debianAdel arpalert[1566]: Sep 29 08:56:14 arpalert: Auto selected device: eth0
Sep 29 08:56:14 debianAdel arpalert[1560]: arpalert.
Sep 29 08:56:14 debianAdel systemd[1]: Started LSB: start and stop the arpalert daemon.
Sep 29 08:56:14 debianAdel arpalert[1567]: Sep 29 08:56:14 arpalert: Auto selected device: eth0
Sep 29 08:56:22 debianAdel arpalert: Selected device: eth0
Sep 29 08:56:22 debianAdel arpalert: daemon instance already running (file: /var/run/arpalert.pid locked)
Sep 29 08:56:22 debianAdel arpalert: seq=1, mac=00:15:5d:13:1a:0d, ip=172.17.1.12, type=new, dev=eth0, vendor="Microsoft Corporation"
Sep 29 08:56:22 debianAdel arpalert: seq=2, mac=00:1a:6d:f5:0c:90, ip=172.17.1.1, type=new, dev=eth0, vendor="Cisco Systems, Inc"
```

Q4) Il est important de surveiller le cache pour éviter une attaque arspooft parce que on verra que deux IP ont la même adresse mac