B2-LAB2
RÉSEAU & SÉCURITÉ 2
Reconnaissance active et passive

Commencer par vérifier que votre machine DEBIAN_TRAINING_DMZ a accès à internet. Pour cela, faire un 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=3.44 ms
64 bytes from 151.101.122.137 (151.101.122.137): icmp_seq=2 ttl=59 time=3.72 ms
64 bytes from 151.101.122.137 (151.101.122.137): icmp_seq=3 ttl=59 time=3.56 ms
64 bytes from 151.101.122.137 (151.101.122.137): icmp_seq=4 ttl=59 time=4.07 ms
^C
--- lemonde.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.435/3.694/4.068/0.237 ms
root@www:~#
```

Depuis la machine DEBIAN_TRAINING_DMZ :
Whois
Installer le paquet whois puis lancer la commande suivante : whois rene-descartes.fr et répondre aux
questions suivantes :
• Quand a été enregistré le nom de domaine rene-descartes.fr ?
2016-09-30T17:56:58Z
• Quelle est la date d'expiration de ce nom de domaine ?
2025-09-30T17:56:58Z
• Quel est l'organisme qui fait office de registrar ?
GANDI
• Quelles sont les adresses des serveurs de noms publics qui gèrent ce domaine ?

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

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

```
address:                    63-65 boulevard Massena
address:                    75013 PARIS
country:                    FR
phone:                      +33.170377661
```

Dig
Vous connaissez déjà nslookup et host comme outils clients d'interrogation d'un serveur de nom. Dig est un
autre outil de ce type.
Tester les quatre commandes suivantes en expliquant leurs différences :
• 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
```

Cette commande demande spécifiquement l'enregistrement de type A (adresse IPv4) pour `rene-descartes.fr` en utilisant le serveur DNS 1.1.1.1 comme résolveur.

• 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
```

Similaire à la première, mais cette fois, elle utilise le serveur DNS configuré par défaut sur 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
```

Ici, la commande cherche une résolution DNS pour `imap`, qui n'est pas un nom de domaine complet.

• nslookup 192.168.100.10

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

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

Cette commande tente une résolution inverse (Reverse DNS Lookup), c'est-à-dire qu'elle cherche le nom de domaine associé à l'adresse IP `192.168.100.10`.

les différences
Les commandes 1 et 2 effectuent une résolution directe (nom → IP).

La commande 1 interroge un serveur DNS spécifique (Cloudflare), tandis que la 2 utilise le DNS par défaut du système.

La commande 3 peut échouer si `imap` n'est pas un domaine complet ou connu du serveur DNS.
La commande 4 effectue une résolution inverse (IP → nom de domaine), contrairement aux autres qui effectuent des résolutions directes.

A l'aide de vos recherches sur internet, compléter le tableau suivant qui explique le rôle de chaque type d'enregistrement DNS.

TYPE D'ENREGISTREMENT	EXPLICATION
A	C'est l'enregistrement DNS le plus courant. Il permet d'associer un nom de domaine à une adresse IPv4
PTR	Utilisé pour la résolution inverse du DNS (Reverse DNS Lookup). Il permet de mapper une adresse IP à un nom de domaine. C'est l'inverse d'un enregistrement A ou AAAA. Il est souvent utilisé pour la validation des serveurs de messagerie.
AAAA	Similaire à l'enregistrement A, mais pour IPv6. Il associe un nom de domaine à une adresse IP en version 6
TXT	Stocke des informations sous forme de texte. Il est souvent utilisé pour des vérifications de domaine (SPF, DKIM, etc.) et pour des configurations spécifiques (par exemple, Google Search Console).
SOA	Fournit des informations sur la zone DNS, comme l'administrateur responsable, la fréquence de mise à jour, le numéro de série de la zone, etc. Il est essentiel pour la gestion des zones DNS.
MX	Spécifie les serveurs de messagerie responsables de la réception des e-mails pour un domaine. Il définit aussi la priorité entre plusieurs serveurs de messagerie.
CNAME	Permet de faire un alias d'un nom de

	domaine vers un autre

Tester les commandes suivantes puis expliquer leur rôle :
• dig rene-descartes.fr MX

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

;; AUTHORITY SECTION:
.                       85862   IN      NS      k.root-servers.net.
.                       85862   IN      NS      h.root-servers.net.
.                       85862   IN      NS      j.root-servers.net.
.                       85862   IN      NS      l.root-servers.net.
.                       85862   IN      NS      i.root-servers.net.
.                       85862   IN      NS      f.root-servers.net.
.                       85862   IN      NS      b.root-servers.net.
.                       85862   IN      NS      m.root-servers.net.
.                       85862   IN      NS      g.root-servers.net.
.                       85862   IN      NS      c.root-servers.net.
.                       85862   IN      NS      a.root-servers.net.
.                       85862   IN      NS      d.root-servers.net.
.                       85862   IN      NS      e.root-servers.net.

;; Query time: 27 msec
;; SERVER: 192.168.100.10#53(192.168.100.10)
;; WHEN: Wed Mar 05 08:59:19 CET 2025
;; MSG SIZE  rcvd: 309
```

Cette commande interroge le serveur DNS par défaut configuré sur votre système pour obtenir les enregistrements MX (Mail Exchange) du domaine `rene-descartes.fr`. Les enregistrements MX spécifient les serveurs de messagerie responsables de la réception des e-mails pour un domaine donné.

• dig @8.8.8.8 rene-descartes.fr MX

```
root@www:~# dig @8.8.8.8 rene-descartes.fr 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: 226
;; 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: 31 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Mar 05 09:00:33 CET 2025
;; MSG SIZE  rcvd: 101
```

Cette commande est similaire à la précédente, mais elle spécifie explicitement le serveur DNS à interroger en utilisant `@8.8.8.8`, qui est l'adresse du serveur DNS public de Google. Cela peut être utile si vous souhaitez contourner les paramètres DNS locaux ou tester la réponse d'un serveur de noms externe.

• dig -t MX rene-descartes.fr

```
;; MSG SIZE  rcvd: 101

root@www:~# dig -t MX rene-desartes

; <<>> DiG 9.16.48-Debian <<>> -t MX rene-desartes
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 5461
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 202503
00 1800 900 604800 86400

;; Query time: 11 msec
;; SERVER: 192.168.100.10#53(192.168.100.10)
;; WHEN: Wed Mar 05 09:01:52 CET 2025
;; MSG SIZE  rcvd: 117
```

Cette commande utilise l'option `-t` pour spécifier explicitement le type d'enregistrement à rechercher, en l'occurrence les enregistrements MX pour le domaine `rene-descartes.fr`. La fonction est identique à celle de la première commande, mais elle montre une autre manière de formuler la requête.

DNSDumpster

Il s’agit d’un outil sur internet qui permet d’inspecter des noms de domaines afin de recueillir des
informations.

Se rendre sur le site suivante : https://dnsdumpster.com

Puis saisir rene-descartes.fr et répondre aux questions suivantes :

• Quelle est la valeur de l’enregistrement TXT ?

"MS=ms94839092"

• Quelles sont les deux valeurs des enregistrements A ?

Host	IP	ASN	ASN Name	Open Services (from DB)	Rev IP
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

• 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 ?

ent

shodan.io

Se rendre sur shodan.io puis saisir https://cloud.rene-descartes.fr. Dans quel pays est hébergé cette application web ?

En france

6°) Outils pour reconnaissance active

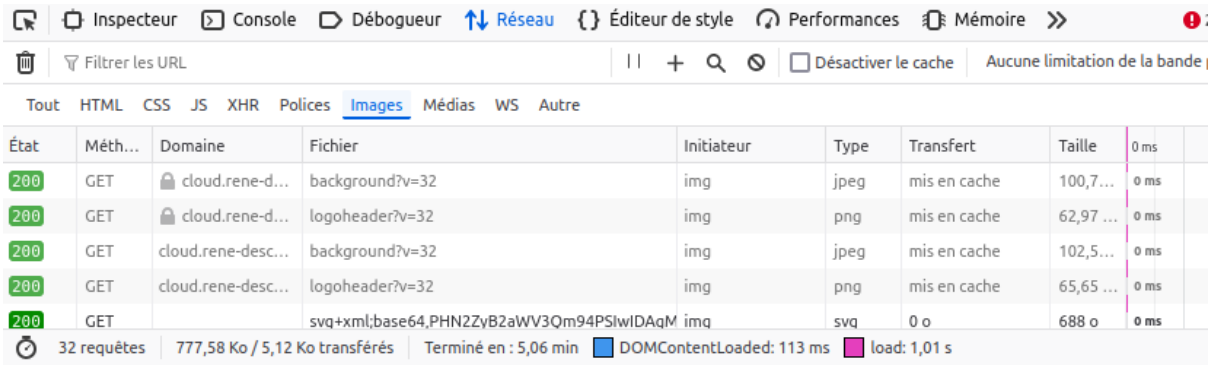
6.1°) Outil Web Developer de Firefox

Se rendre sur l'application cloud.rene-descartes.fr, s'authentifier puis ouvrir la console des outils de développement web de Firefox (CTRL+SHIFT+I). Rafraîchir la page avec la touche F5.

Répondre aux questions suivantes :

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

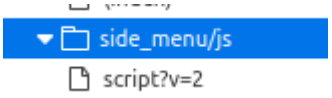
il ny en a 0



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

Nom	Valeur	Domain	Path	Expiration / Durée ma	Taille	HttpOnly	Secure	SameSite	Dernier accès
__Host-n...	true	cloud.rene-...	/	Sat, 20 Dec 2025 1...	31	true	true	Lax	Wed, 05 Mar 2
__Host-n...	true	cloud.rene-...	/	Sat, 20 Dec 2025 1...	34	true	true	Strict	Wed, 05 Mar 2
nc_sessi...	ih0emp0tkc4n...	cloud.rene-...	/	Thu, 20 Mar 2025 0...	39	true	true	Lax	Wed, 05 Mar 2
nc_token	iYwaRXuLPutD...	cloud.rene-...	/	Thu, 20 Mar 2025 0...	40	true	true	Lax	Wed, 05 Mar 2
nc_usern...	7F7D9363-0DE...	cloud.rene-...	/	Thu, 20 Mar 2025 0...	47	true	true	Lax	Wed, 05 Mar 2
oc1qa1s...	ih0emp0tkc4n...	cloud.rene-...	/	Session	38	true	true	Lax	Wed, 05 Mar 2
oc_sessi...	6Ee%2B4HCYC...	cloud.rene-...	/	Session	164	true	true	Lax	Wed, 05 Mar 2

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



6.2°) Ping

Depuis la machine DEBIAN_TRAINING_DMZ :

Effectuer la commande ping suivante puis répondre aux questions suivantes :

ping -c 5 messagelab

• Que signifie l'option c ?

L'option `-c` (pour "count") spécifie le nombre de requêtes ICMP à envoyer. Dans ce cas, `-c 5` indique que cinq requêtes seront envoyées, après quoi la commande `ping` s'arrêtera automatiquement.

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

Lorsqu'une machine ne répond pas à une requête ping, cela ne signifie pas nécessairement qu'elle est éteinte. Plusieurs facteurs peuvent en être la cause, notamment des

configurations de pare-feu qui bloquent les requêtes ICMP, des problèmes de connectivité réseau, des paramètres de sécurité ou des configurations système spécifiques.

6.3°) Traceroute
Depuis la machine DEBIAN_TRAINING_DMZ :
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 ?
En exécutant `traceroute messagelab`, vous obtenez la liste des routeurs que les paquets traversent pour atteindre `messagelab`, ainsi que le temps nécessaire pour chaque saut. Cette information est utile pour diagnostiquer des problèmes de réseau, tels que des latences élevées ou des points de défaillance. il y a 2 lignes afficher.

•Quel est l'équivalent de cette commande sous Windows?
C'est Tracert.

6.4°) Telnet
Telnet est un outil qui permet de se connecter à un service réseau via une conversation non chiffrée.

Depuis la machine DEBIAN_TRAINING_SERVEUR:
Effectuer la commande suivante :
telnet messagelab 80
Ensuite saisir la chaîne de caractères suivante :
GET / HTTP/1.1

Reproduire sur votre documentation le résultat obtenu puis répondre aux questions suivantes :

```
root@messagelab:~# telnet messagelab 80
Trying 127.0.1.1...
Connected to messagelab.
Escape character is '^]'.
GET/HTTP/1.1
HTTP/1.1 400 Bad Request
Date: Wed, 05 Mar 2025 08:52:36 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</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

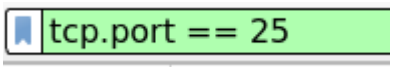
Démarrer le service de serveur mail avec la commande suivante :
service postfix start
Puis effectuer la commande telnet suivante :
telnet localhost 25
Envoyer le mail suivant en ligne de commande :

```
root@messagelab:~# service postfix start
root@messagelab:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 messagelab.mlif.local ESMTP Postfix (Debian/GNU)
mail from: user2@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 D0E9E40A7E
quit
221 2.0.0 Bye
Connection closed by foreign host.
root@messagelab:~# /etc/postfix/
-bash: /etc/postfix/ : est un dossier
root@messagelab:~#
```

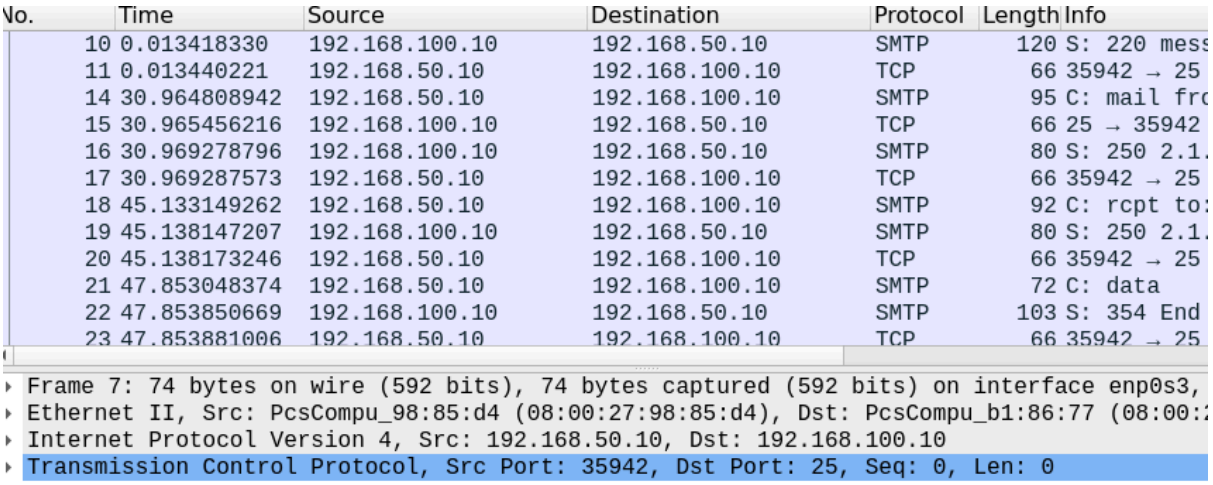
Vérifier la bonne réception du mail en consultant les logs systèmes via la commande suivante :
tail /var/log/syslog

```
root@messagelab:~# tail /var/log/syslog
Mar  5 09:55:07 messagelab systemd[1]: Started Postfix Mail Transport Agent (instance -).
Mar  5 09:55:07 messagelab systemd[1]: Starting Postfix Mail Transport Agent...
Mar  5 09:55:07 messagelab systemd[1]: Started Postfix Mail Transport Agent.
Mar  5 09:55:20 messagelab postfix/smtpd[1114]: connect from localhost[::1]
Mar  5 09:56:33 messagelab postfix/smtpd[1114]: D0E9E40A7E: client=localhost[::1]
Mar  5 09:56:48 messagelab postfix/cleanup[1119]: D0E9E40A7E: message-id=<20250305085633.D0E9E40A7E@
messagelab.mlif.local>
Mar  5 09:56:48 messagelab postfix/qmgr[1102]: D0E9E40A7E: from=<user2@mlif.local>, size=321, nrcpt=
1 (queue active)
Mar  5 09:56:48 messagelab postfix/local[1120]: D0E9E40A7E: to=<user2@mlif.local>, relay=local, dela
y=33, delays=33/0.01/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
Mar  5 09:56:48 messagelab postfix/qmgr[1102]: D0E9E40A7E: removed
Mar  5 09:56:53 messagelab postfix/smtpd[1114]: disconnect from localhost[::1] mail=1 rcpt=1 data=1
quit=1 commands=4
```

Depuis la machine LUBUNTU_TRAINING_CLIENT:
Ouvrir un terminal, se connecter en root puis lancer wireshark avec la commande suivante :
wireshark &
Après avoir sélectionné votre carte réseau, positionner le filtre suivant



Ouvrir ensuite un second terminal puis reproduire la conversation telnet précédente de user1 vers user2.
telnet messagelab 25
Capturer le flux SMTP (capture d'écran attendue) puis répondre aux questions suivantes:

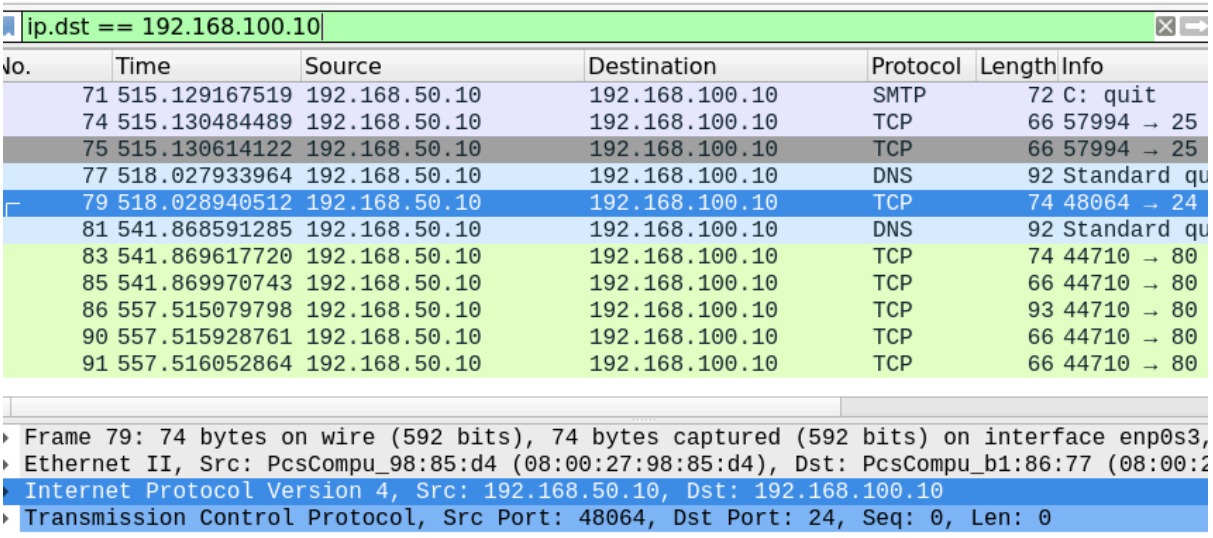


No.	Time	Source	Destination	Protocol	Length	Info
10	0.013418330	192.168.100.10	192.168.50.10	SMTP	120	S: 220 mess
11	0.013440221	192.168.50.10	192.168.100.10	TCP	66	35942 → 25
14	30.964808942	192.168.50.10	192.168.100.10	SMTP	95	C: mail fr
15	30.965456216	192.168.100.10	192.168.50.10	TCP	66	25 → 35942
16	30.969278796	192.168.100.10	192.168.50.10	SMTP	80	S: 250 2.1.
17	30.969287573	192.168.50.10	192.168.100.10	TCP	66	35942 → 25
18	45.133149262	192.168.50.10	192.168.100.10	SMTP	92	C: rcpt to:
19	45.138147207	192.168.100.10	192.168.50.10	SMTP	80	S: 250 2.1.
20	45.138173246	192.168.50.10	192.168.100.10	TCP	66	35942 → 25
21	47.853048374	192.168.50.10	192.168.100.10	SMTP	72	C: data
22	47.853850669	192.168.100.10	192.168.50.10	SMTP	103	S: 354 End
23	47.853881006	192.168.50.10	192.168.100.10	TCP	66	35942 → 25

```
▸ Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3,
▸ Ethernet II, Src: PcsCompu_98:85:d4 (08:00:27:98:85:d4), Dst: PcsCompu_b1:86:77 (08:00:
▸ Internet Protocol Version 4, Src: 192.168.50.10, Dst: 192.168.100.10
▸ Transmission Control Protocol, Src Port: 35942, Dst Port: 25, Seq: 0, Len: 0
```

• Quel est le port d'écoute du service SMTP ? Le flux est-il chiffré ?
25 non
• Quel est le protocole de couche 4 associé à SMTP ?
le protocol TCP
• Que signifie SMTP ?
SMTP, ou Simple Mail Transfer Protocol, est un protocole de communication standard utilisé pour l'envoi de courriers électroniques sur Internet. Il définit les règles permettant aux clients de messagerie et aux serveurs de messagerie de transmettre des messages électroniques entre eux.

Modifier le filtre précédent afin de créer les filtres wireshark suivants puis les tester :
• Adresse IP de destination = 192.168.100.10 ;

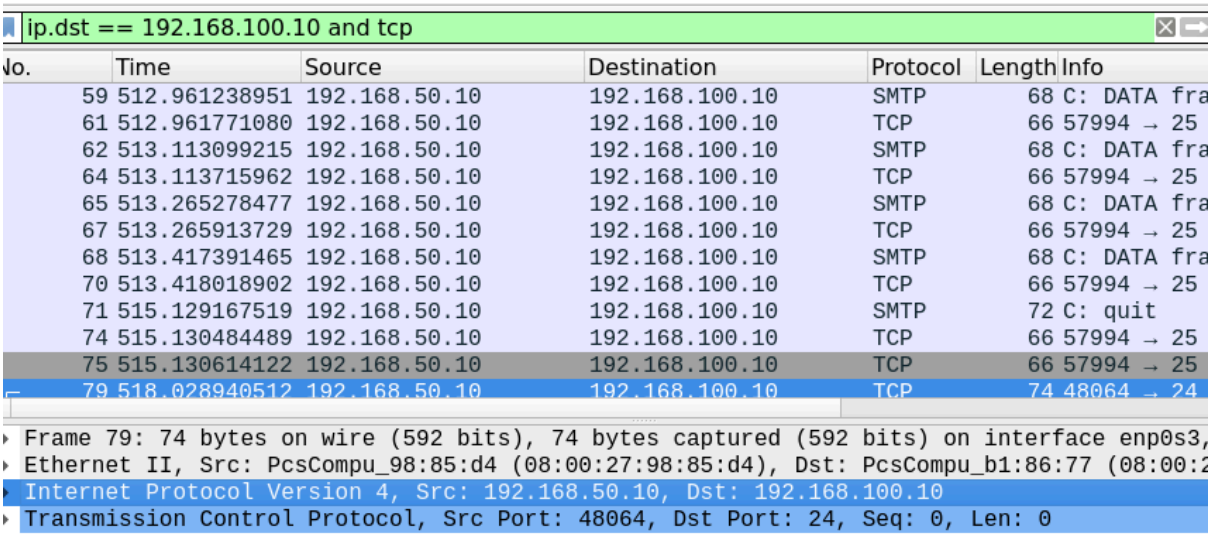


ip.dst == 192.168.100.10

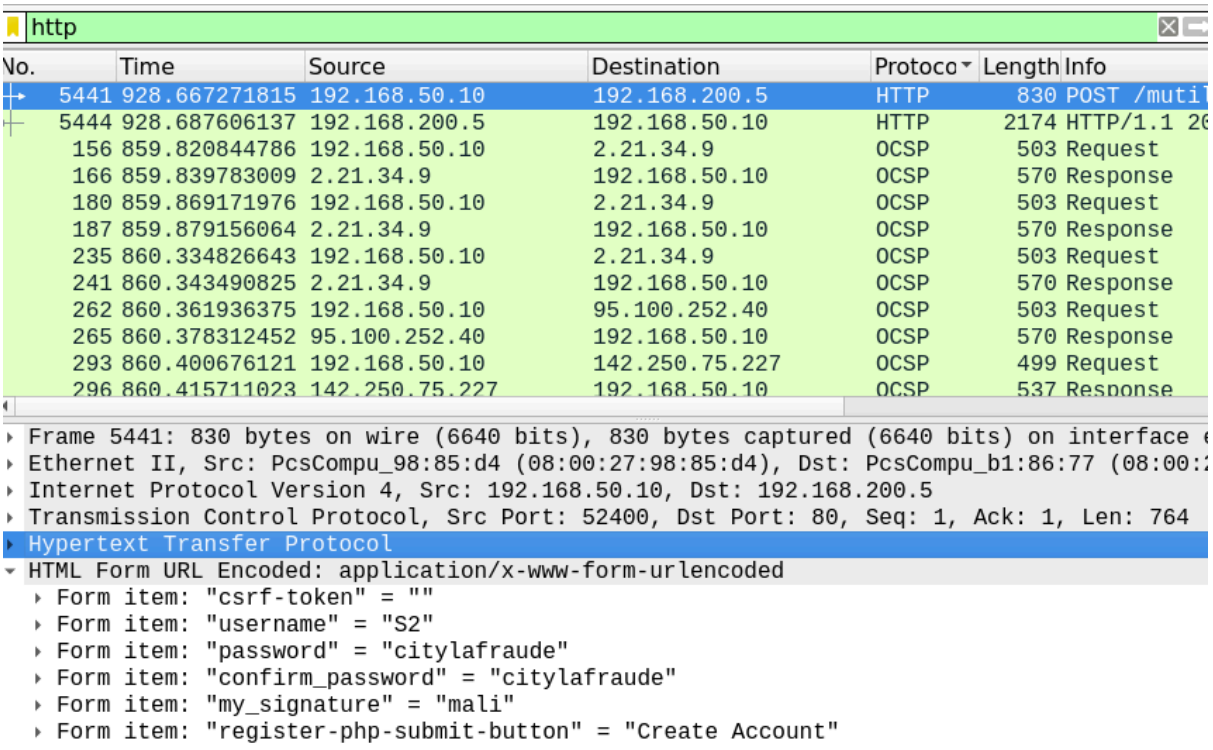
No.	Time	Source	Destination	Protocol	Length	Info
71	515.129167519	192.168.50.10	192.168.100.10	SMTP	72	C: quit
74	515.130484489	192.168.50.10	192.168.100.10	TCP	66	57994 → 25
75	515.130614122	192.168.50.10	192.168.100.10	TCP	66	57994 → 25
77	518.027933964	192.168.50.10	192.168.100.10	DNS	92	Standard qu
79	518.028940512	192.168.50.10	192.168.100.10	TCP	74	48064 → 24
81	541.868591285	192.168.50.10	192.168.100.10	DNS	92	Standard qu
83	541.869617720	192.168.50.10	192.168.100.10	TCP	74	44710 → 80
85	541.869970743	192.168.50.10	192.168.100.10	TCP	66	44710 → 80
86	557.515079798	192.168.50.10	192.168.100.10	TCP	93	44710 → 80
90	557.515928761	192.168.50.10	192.168.100.10	TCP	66	44710 → 80
91	557.516052864	192.168.50.10	192.168.100.10	TCP	66	44710 → 80

```
▸ Frame 79: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3,
▸ Ethernet II, Src: PcsCompu_98:85:d4 (08:00:27:98:85:d4), Dst: PcsCompu_b1:86:77 (08:00:2
▸ Internet Protocol Version 4, Src: 192.168.50.10, Dst: 192.168.100.10
▸ Transmission Control Protocol, Src Port: 48064, Dst Port: 24, Seq: 0, Len: 0
```

• 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.
Ensuite, avec le navigateur, se rendre sur l'application Mutillidae via http://www.mlif.local/mutillidae.
Créer un compte sur cette application puis s'authentifier et capturer le mot de passe saisi avec wireshark.
• La conversation est-elle chiffrée ?
Non elle n'est pas chiffrer
• Quel protocole faudrait-il utiliser pour rendre le flux confidentiel ?
Le protocole sécurisé HTTPS.



• Quel est le code de retour HTTP en cas de tentative d'accès à un site inexistant ?
le code 404 Not Found

• Dans le cas du site www.mlif.local, quel est le code de retour HTTP
le code HTTP 200 OK

7°) Détail de l'outil NMAP pour reconnaissance active
Considérer le schéma suivant pour avoir une vue d'ensemble des modèles OSI et TCP/IP.

Depuis la machine LUBUNTU_TRAINING_CLIENT:
Fermer puis relancer wireshark sans aucun filtre. Lancer une nouvelle capture.
Ouvrir un terminal en root puis saisir la commande suivante :
nmap -A imap

```
root@client-mlif:/home/test# nmap -A imap
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 14:06 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 3.35 seconds
root@client-mlif:/home/test# ^C
root@client-mlif:/home/test# nmap -A imap
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 14:06 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 3.37 seconds
```

o.	Time	Source	Destination	Protocol	Length	Info
→	1 0.000000000	192.168.50.10	192.168.100.10	DNS	86	Standard query 0
←	2 0.000669673	192.168.100.10	192.168.50.10	DNS	138	Standard query r
	3 0.002089240	192.168.50.10	192.168.100.20	ICMP	42	Echo (ping) requ
	4 0.002106992	192.168.50.10	192.168.100.20	TCP	58	61186 → 443 [SYN
	5 0.002112716	192.168.50.10	192.168.100.20	TCP	54	61186 → 80 [ACK]

```
Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_98:85:d4 (08:00:27:98:85:d4), Dst: PcsCompu_b1:86:77 (08:00:27:b1:
Internet Protocol Version 4, Src: 192.168.50.10, Dst: 192.168.100.10
User Datagram Protocol, Src Port: 58481, Dst Port: 53
```

Observer la capture puis répondre aux questions suivantes :

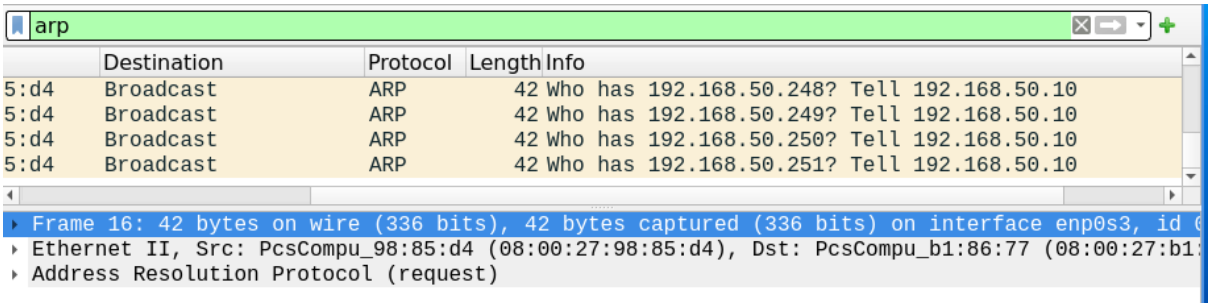
• Pourquoi y a t-il une résolution DNS au début de votre capture ?
La résolution DNS en début de capture se produit car nmap essaie d'obtenir l'adresse IP associée au nom "imap" avant de poursuivre son scan.

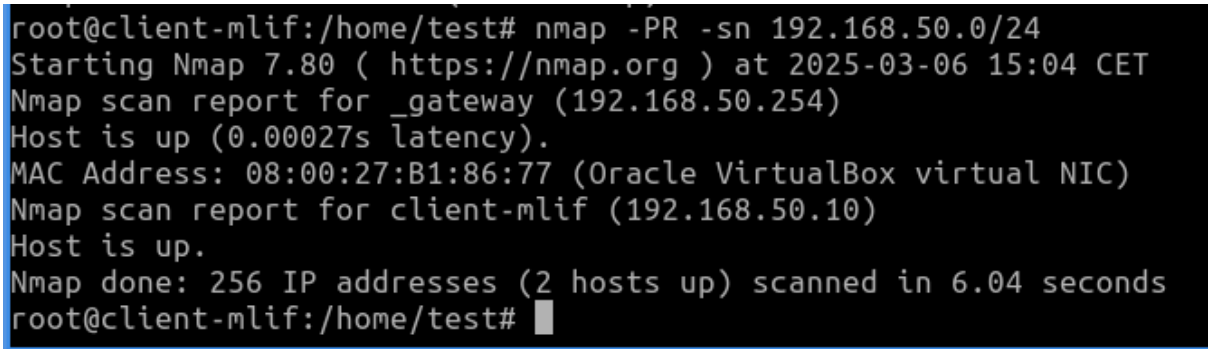
• La machine de nom imap est l'alias (CNAME) de quel autre nom ?

```
DNS       162 Standard query response 0x3b43 A imap.mlif.local CNAME mail.mlif.local A 192.168.100.20 NS messagelab.mlif.local
DNS       157 Standard query response 0x2187 AAAA imap.mlif.local CNAME mail.mlif.local SOA messagelab.mlif.local OPT
```

L'alias de imap est 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 résolution ARP concerne 192.168.50.254 et non 192.168.100.10 parce que la machine source doit passer par la passerelle pour atteindre un hôte situé dans un sous-réseau différent.
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 ?

PR

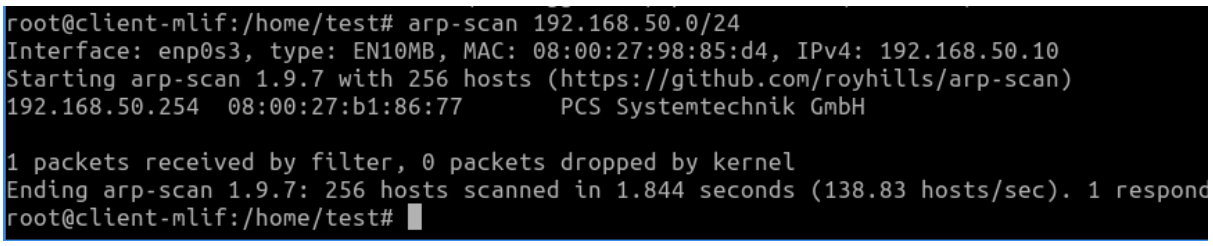
L'option PR dans un scan réseau est utilisée pour tenter de passer par un proxy intermédiaire afin d'atteindre la cible. Cependant, en fonction de l'outil utilisé cette option peut ne pas exister sous cette forme exacte.

SN

L'option sn désactive le scan des ports et ne fait que identifier les hôtes actifs sur le réseau.

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 ?

Un scan arp-scan 192.168.50.0/24 permet d'identifier tous les appareils connectés au réseau en récupérant leurs adresses IP et MAC, même s'ils bloquent les pings. Il est utile en administration réseau pour détecter les équipements inconnus, vérifier les conflits d'IP,

surveiller l'état du réseau et renforcer la sécurité en repérant d'éventuelles connexions non autorisées.

• Quel peut-être l'intérêt d'un tel scan en matière de hacking ?
En matière de hacking, un scan arp-scan 192.168.50.0/24 permet de cartographier rapidement un réseau en détectant tous les appareils connectés, même ceux qui ne répondent pas aux pings. Cela peut être utile pour identifier des cibles potentielles, comme des serveurs, des routeurs ou des dispositifs vulnérables.

Tester les scans suivants puis expliquer leurs différences :
• 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 15:26 CET
Nmap scan report for messagelab.mlif.local (192.168.100.10)
Host is up (0.00071s latency).
Nmap scan report for 192.168.100.254
Host is up (0.00032s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.93 seconds
root@client-mlif:/home/test#
```

• 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 15:27 CET
Nmap scan report for messagelab.mlif.local (192.168.100.10)
Host is up (0.00071s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 1.93 seconds
root@client-mlif:/home/test#
```

Différences

-PE utilise des ICMP Echo Request (ping classique), qui sont très souvent filtrés par les pare-feu.
-PU utilise des ICMP Timestamp Request, moins courants et souvent moins filtrés que les Echo Request.

installer le paquet masscan.

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

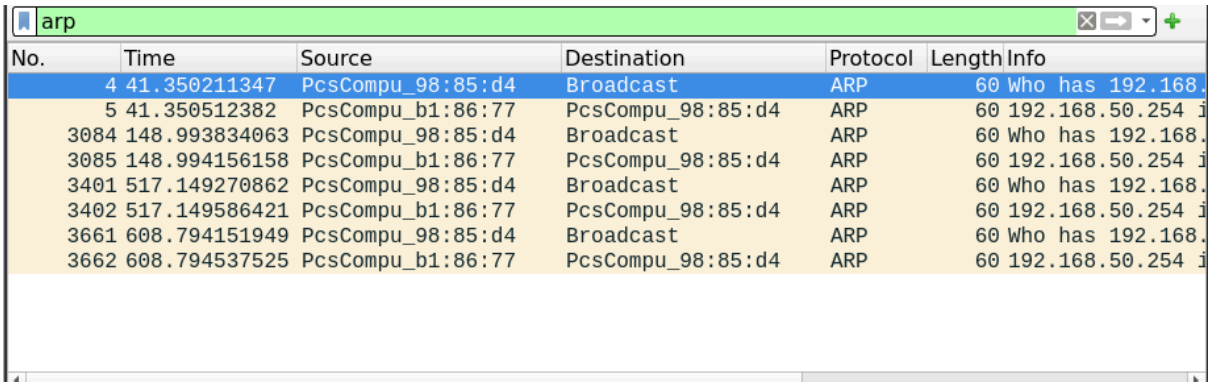
Ensuite, tester le scan suivant :
masscan 192.168.200.5 -p80,443,22
Expliquer ce que fait ce scan et quel est peut-être son intérêt en administration réseaux et en hacking.

Masscan
Masscan est un outil de scan de ports extrêmement rapide, conçu pour analyser de grands réseaux en très peu de temps.

En administration réseau, ce scan aide à surveiller et sécuriser les services ouverts, garantissant qu'aucun port non nécessaire n'est exposé.
En hacking, c'est un outil de reconnaissance rapide permettant de cibler des ports ouverts pour exploiter des failles.

Tester les scans suivants puis expliquer leurs objectifs :
masscan 192.168.200.5 -p1-1024

```
root@client-mlif:/home/test# masscan 192.168.200.5 -p1-1024
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-03-07 13:50:01 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1024 ports/host]
Discovered open port 22/tcp on 192.168.200.5
Discovered open port 80/tcp on 192.168.200.5
Discovered open port 443/tcp on 192.168.200.5
rate:  0.00-kpps, 100.00% done, waiting -11-secs, found=3
```



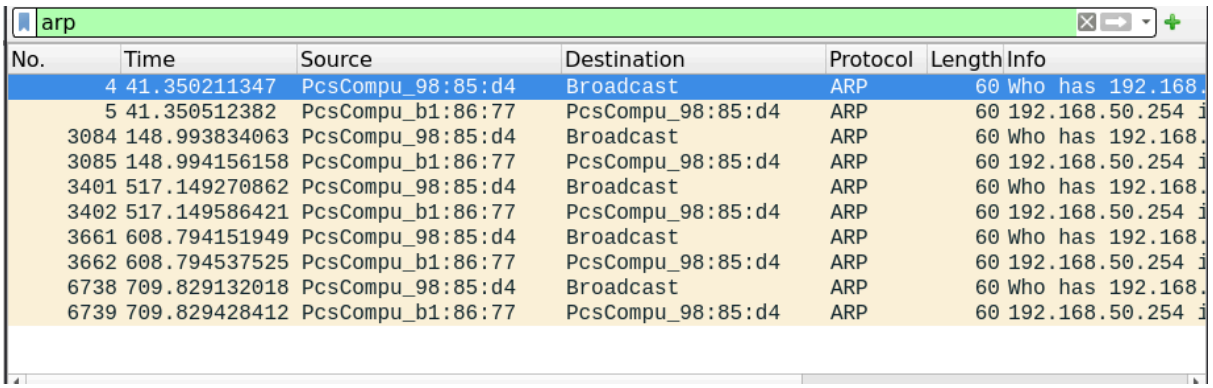
arp

No.	Time	Source	Destination	Protocol	Length	Info
4	41.350211347	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
5	41.350512382	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i
3084	148.993834063	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
3085	148.994156158	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i
3401	517.149270862	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
3402	517.149586421	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i
3661	608.794151949	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
3662	608.794537525	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i

Objectifs: Détecter quels ports sont ouverts sur l'hôte 192.168.200.5 parmi les ports privilégiés (souvent utilisés par les services courants comme SSH, HTTP, FTP…)

masscan -p22 192.168.200.1-192.168.200.254

```
root@client-mlif:/home/test# masscan -p22 192.168.200.1-192.168.200.254
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-03-07 13:51:48 GMT
Initiating SYN Stealth Scan
Scanning 254 hosts [1 port/host]
Discovered open port 22/tcp on 192.168.200.5
rate:  0.00-kpps, 100.00% done, waiting 2-secs, found=1
```



arp

No.	Time	Source	Destination	Protocol	Length	Info
4	41.350211347	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
5	41.350512382	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i
3084	148.993834063	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
3085	148.994156158	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i
3401	517.149270862	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
3402	517.149586421	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i
3661	608.794151949	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
3662	608.794537525	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i
6738	709.829132018	PcsCompu_98:85:d4	Broadcast	ARP	60	Who has 192.168.
6739	709.829428412	PcsCompu_b1:86:77	PcsCompu_98:85:d4	ARP	60	192.168.50.254 i

Objectifs: Identifier les machines du réseau 192.168.200.0/24 qui ont le service SSH actif.

Attention, ce type de scan n'est pas furtif et laisse beaucoup de traces largement détectables par un IDS/IPS.

Relancer le scan en ouvrant une capture wireshark sans filtres.

No.	Time	Source	Destination	Protocol	Length	Info
207	42.710413913	192.168.50.10	192.168.200.5	TCP	54	55401 → 717
208	42.710773126	192.168.200.5	192.168.50.10	TCP	60	717 → 55401
209	42.720425469	192.168.50.10	192.168.200.5	TCP	60	55401 → 717
210	42.730910903	192.168.50.10	192.168.200.5	TCP	54	55401 → 700
211	42.731268934	192.168.200.5	192.168.50.10	TCP	60	700 → 55401
212	42.741378974	192.168.50.10	192.168.200.5	TCP	60	55401 → 700
213	42.752172911	192.168.50.10	192.168.200.5	TCP	54	55401 → 684
214	42.752185110	192.168.50.10	192.168.200.5	TCP	54	55401 → 962
215	42.752618669	192.168.200.5	192.168.50.10	TCP	60	684 → 55401
216	42.752700694	192.168.200.5	192.168.50.10	TCP	60	962 → 55401
217	42.755112051	192.168.50.10	192.168.200.5	TCP	60	55401 → 684
218	42.794714118	192.168.50.10	192.168.200.5	TCP	60	55401 → 962

8°) Hydra

Rappelez vous la force brute de mot de passe avec le script python. Hydra est un bruteforceur de connexion très rapide qui peut travailler sur de nombreux protocoles.

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

D'abord faire un apt-get update de la machine

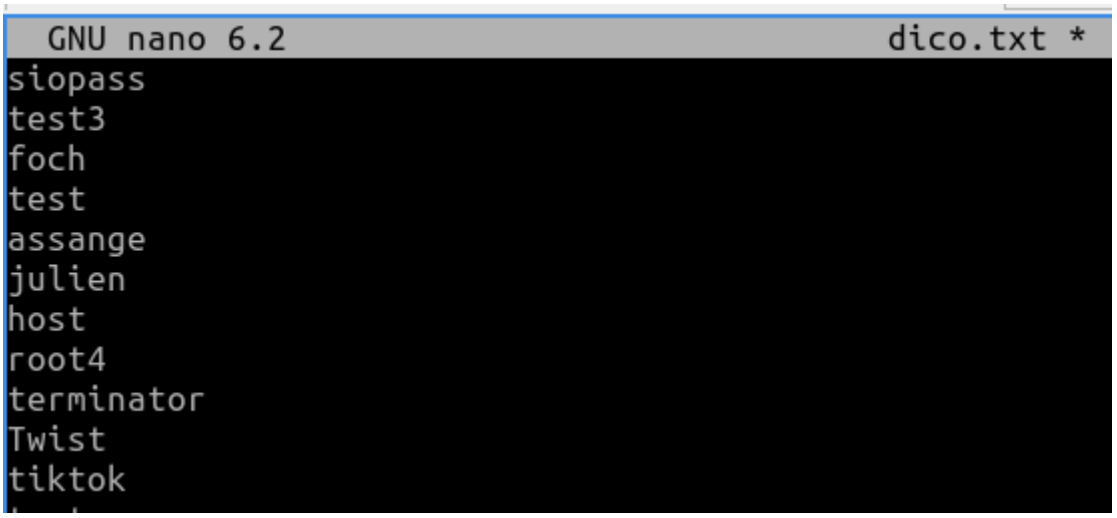
```
root@client-mlif:/home/test# apt-get update
```

Puis ensuite faire un apt install hydra

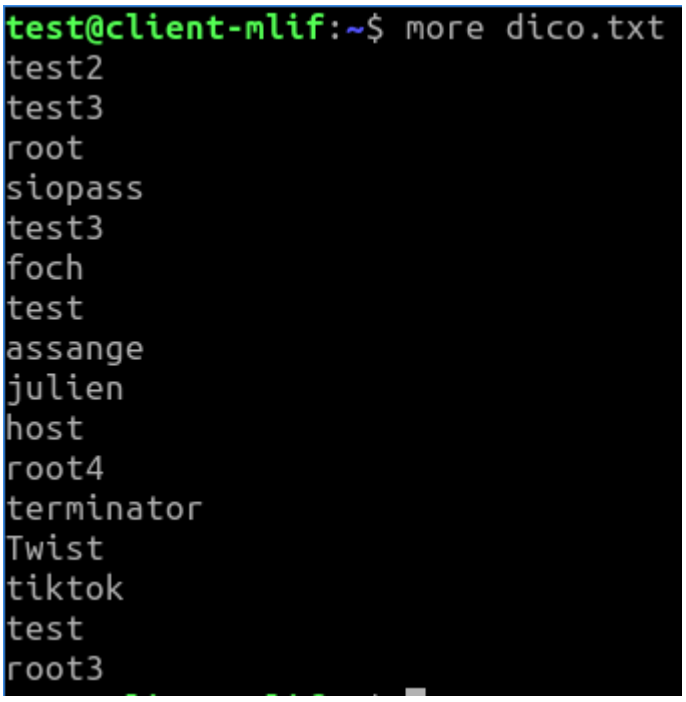
```
root@client-mlif:/home/test# apt install hydra
```

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

Il faut d'abord faire un nano dico.txt puis remplir le dictionnaire



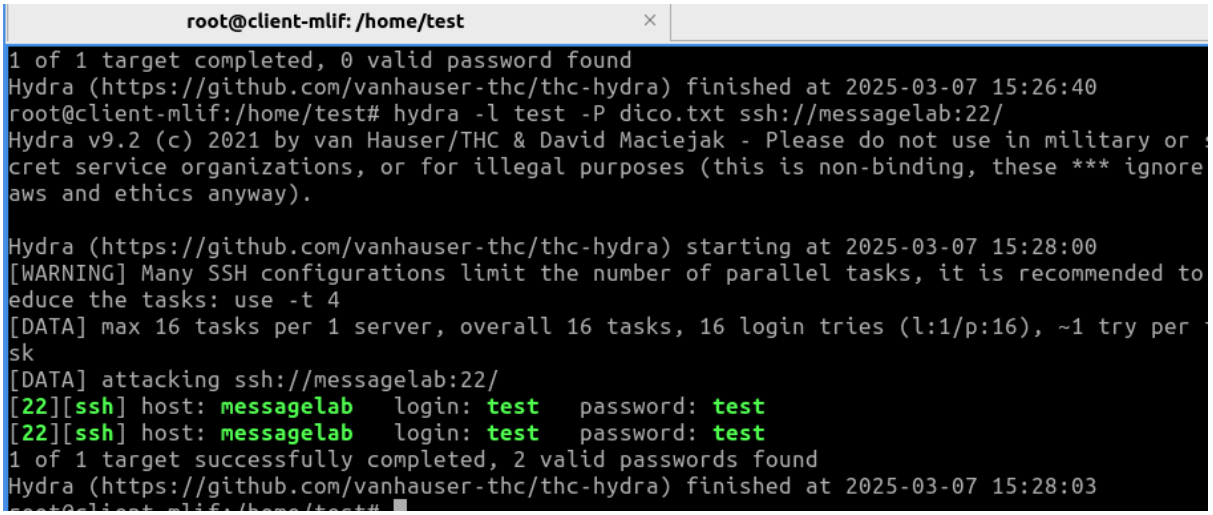
Puis faire un more dico.txt pour afficher le contenu



Lancer une attaque afin de trouver le mot de passe ssh de l'utilisateur test avec hydra. Pour vous aider, voici les options à utiliser :

Option	description
-l	Login de la victime
-P	Le dictionnaire à utiliser

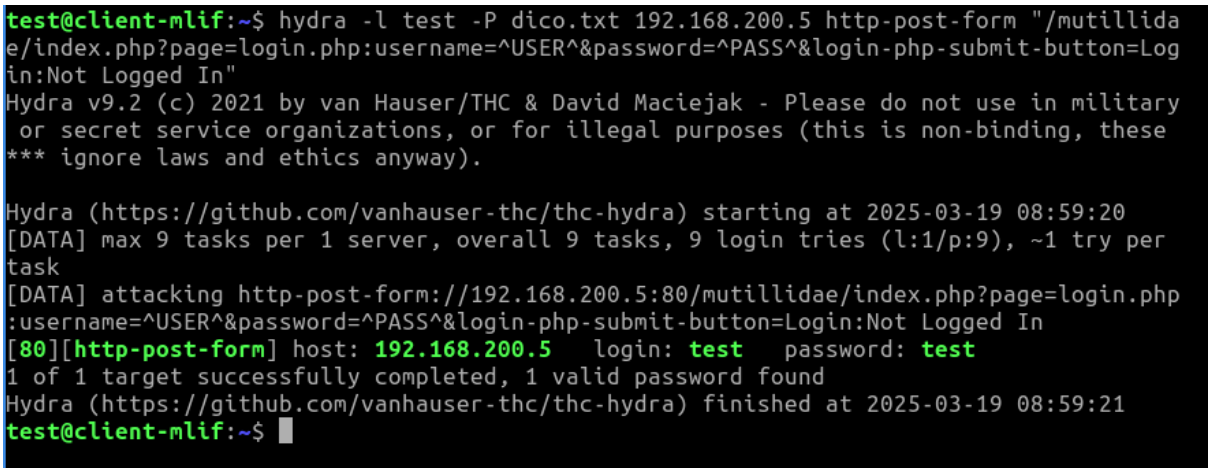
Le service à attaquer est à indiquer à la fin. Si vous ne trouvez pas comment faire, il n'est pas interdit d'utiliser internet. Si cela fonctionne, vous devriez trouver ceci :



STOP 2 : Appelez moi pour que je puisse vérifier cette partie du travail.

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. Vous pouvez utiliser le compte créé précédemment.

En parallèle de votre attaque, lancer une capture wireshark avec le filtre http



A vous de jouer ! Répondre ensuite aux questions suivantes :

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).

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


 class="label">Password</td>
>
 <input type="password" name="password" size="20"
                    />
```

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.

```
 <a class="attribute-value">username</a>
 <a class="attribute-value">password</a>
```

9°) Épuisement des ressources

Expliquer ce qu'est un DOS, un DDOS

Les attaques DoS (*Denial of Service*) et DDoS (*Distributed Denial of Service*) visent à rendre un service en ligne indisponible en le submergeant de trafic inutile. La différence principale réside dans la source de l'attaque :

DOS : l'attaque provient d'une seule machine.

DDOS : l'attaque est lancée depuis plusieurs machines simultanément, souvent via un réseau d'ordinateurs compromis appelé botnet.

CODE HTTP	SIGNIFICATION
200	La requête a été traitée avec succès et le serveur a renvoyé le contenu demandé.
301	La ressource demandée a été déplacée de façon permanente à une nouvelle URL. Les clients doivent utiliser cette nouvelle URL pour les futures requêtes.

401	L'accès à la ressource requiert une authentification. Le client doit fournir des identifiants valides pour obtenir une réponse.
404	La ressource demandée est introuvable sur le serveur. Cela peut être dû à une URL incorrecte ou à une ressource supprimée.
500	Le serveur a rencontré une condition inattendue qui l'a empêché de traiter la requête.
504	Le serveur, agissant comme passerelle ou proxy, n'a pas reçu de réponse à temps d'un serveur en amont pour compléter la requête.

Toujours depuis votre machine LUBUNTU :
Installer le paquet hping3

```
sudo apt install hping3
```

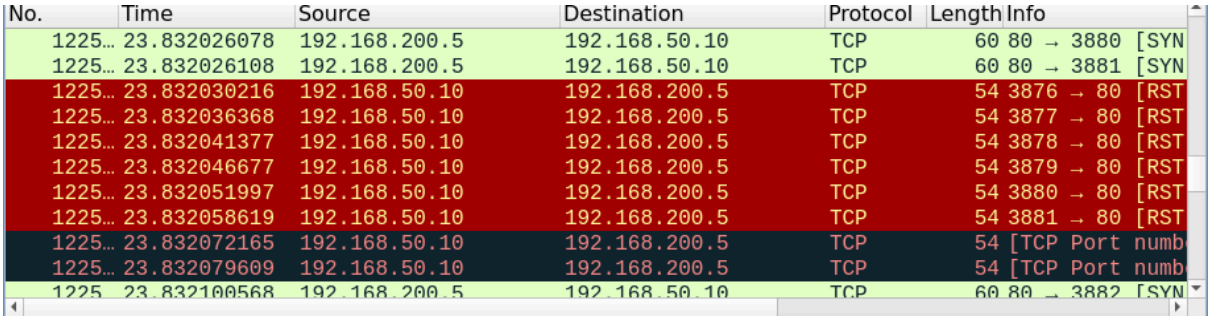
Lancer une capture de trame sans filtre wireshark puis lancer une attaque contre le serveur web www.mlif.local par épuisement de ressources.

Remarque :
Ce type d'attaque laisse des traces dans les journaux du serveur cible. Ne jamais essayer en dehors de la maquette pédagogique de la MLIF.

la commande:

```
root@client-mlif:/home/test# hping3 -S --flood -V -p 80 192.168.200.5
using enp0s3, addr: 192.168.50.10, 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
```

la capture de trame sur wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
1225…	23.832026078	192.168.200.5	192.168.50.10	TCP	60	80 → 3880 [SYN
1225…	23.832026108	192.168.200.5	192.168.50.10	TCP	60	80 → 3881 [SYN
1225…	23.832030216	192.168.50.10	192.168.200.5	TCP	54	3876 → 80 [RST
1225…	23.832036368	192.168.50.10	192.168.200.5	TCP	54	3877 → 80 [RST
1225…	23.832041377	192.168.50.10	192.168.200.5	TCP	54	3878 → 80 [RST
1225…	23.832046677	192.168.50.10	192.168.200.5	TCP	54	3879 → 80 [RST
1225…	23.832051997	192.168.50.10	192.168.200.5	TCP	54	3880 → 80 [RST
1225…	23.832058619	192.168.50.10	192.168.200.5	TCP	54	3881 → 80 [RST
1225…	23.832072165	192.168.50.10	192.168.200.5	TCP	54	[TCP Port numb
1225…	23.832079609	192.168.50.10	192.168.200.5	TCP	54	[TCP Port numb
1225	23.832100568	192.168.200.5	192.168.50.10	TCP	60	80 → 3882 [SYN

Pour que l'épuisement de ressources soit plus probant il faudrait s'y mettre à plusieurs (DDOS). Reproduire la capture d'écran des flux wireshark capturés

Expliquer le principe d'une attaque de type DDOS:
Une attaque DDoS (Distributed Denial of Service, ou déni de service distribué) vise à rendre un service en ligne, comme un site web, indisponible en le submergeant de trafic excessif**.**

Utiliser à nouveau hping3 pour réaliser les actions suivantes :

• scan de ports de la machine 192.168.200.5 ;

```
test@client-mlif:~$ sudo hping3 -S 192.168.200.5 -p 80 -c 1
HPING 192.168.200.5 (enp0s3 192.168.200.5): S set, 40 headers + 0 data bytes
len=46 ip=192.168.200.5 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=

--- 192.168.200.5 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.4/7.4/7.4 ms
```

• découverte des services de la machine 192.168.100.10 ;

```
test@client-mlif:~$ sudo hping3 -S 192.168.100.10 -p 80,443,22,21,25,110
HPING 192.168.100.10 (enp0s3 192.168.100.10): S set, 40 headers + 0 data byte
s
len=46 ip=192.168.100.10 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt
=5.4 ms
len=46 ip=192.168.100.10 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt
=5.3 ms
len=46 ip=192.168.100.10 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=29200 rtt
=5.2 ms
len=46 ip=192.168.100.10 ttl=63 DF id=0 sport=80 flags=SA seq=3 win=29200 rtt
=5.2 ms
len=46 ip=192.168.100.10 ttl=63 DF id=0 sport=80 flags=SA seq=4 win=29200 rtt
=5.1 ms
^C
--- 192.168.100.10 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.1/5.2/5.4 ms
```

Vérifie si les ports communs (HTTP, HTTPS, SSH, FTP, SMTP, POP3) sont ouverts.
En fonction des réponses (RST/ACK, SYN-ACK), on peut déterminer quels services tournent.

• **sniffing du réseau**

```
test@client-mlif:~$ sudo hping3 -S 192.168.200.5 -p 80 --count 1
HPING 192.168.200.5 (enp0s3 192.168.200.5): S set, 40 headers + 0 data bytes
len=46 ip=192.168.200.5 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=
7.7 ms
```

Cela envoie un paquet SYN à l'IP `192.168.200.5` sur le port 80 et écoute la réponse.

STOP 3 : Appelez moi pour que je puisse vérifier cette partie du travail.