

TP Messagerie Electronique

Noms et Prénoms : **GUARDIA Quentin**

Date de remise du TP par courriel : dimanche 18h00

Courriel : master2srs.dir@gmail.com

Indiquer dans le sujet de votre email : « M1 TP Courriel »

Objectif du TP : installer, analyser et sécuriser un système de messagerie électronique d'entreprise.

Veuillez répondre aux questions suivantes en utilisant **une couleur de police de caractères BLEUE**, et si possible veuillez illustrer vos réponses avec des captures d'écrans (wireshark, tcpview, serveur, client, ...).

1. INSTALLATION D'UN SERVEUR DE MESSAGERIE ELECTRONIQUE

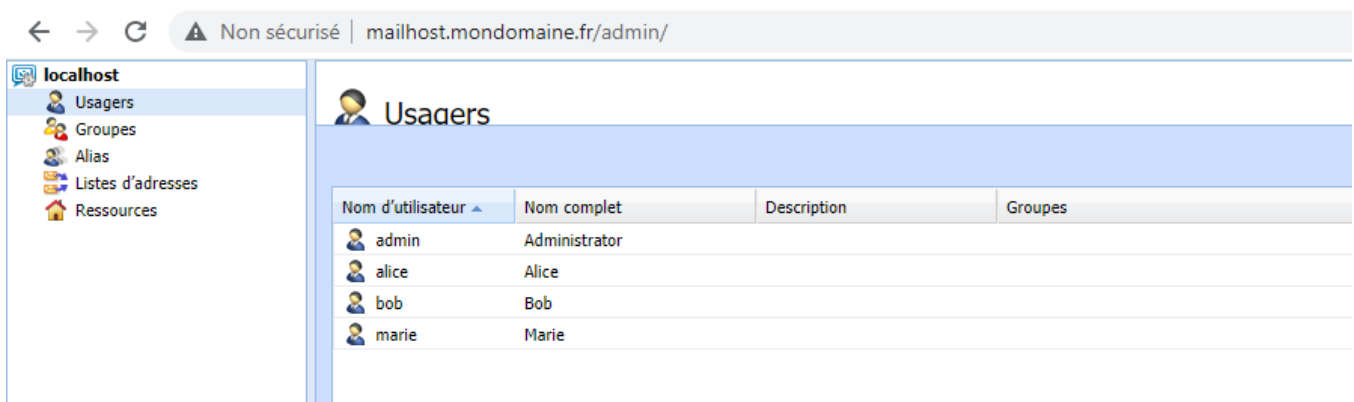
1.1 Sur le poste serveur, éditer le fichier système « hosts » ci-dessous pour associer le nom du serveur mail « mailhost.mondomaine.fr » avec l'adresse IP du serveur ou l'adresse « localhost ».

Windows\system32\drivers\etc\hosts

1.2 - installer ensuite et configurer sur ce poste, le serveur Mail (Kerio) fournit. Utiliser le nom de domaine « mondomaine.fr », et le nom de serveur : « mailhost.mondomaine.fr ». Aidez vous du guide d'administration du serveur si besoin.

1.3 - Sur ce serveur, créer 3 comptes utilisateurs au format suivant :

- login : **alice@mondomaine.fr** et mot de passe : **user1**
- login : **bob@mondomaine.fr** et mot de passe : **user2**
- login : **marie@mondomaine.fr** et mot de passe : **user3**



1.4 **Attention**, vous devez **désactiver l'antivirus intégré du serveur**, via la console d'administration du serveur et le menu à gauche « Filtre du contenu ». « Décocher l'option « *Utiliser l'outil antivirus intégré McAfee* » Sinon, les messages emails ne pourront pas être relayés par le serveur.

Attention : désactiver aussi les parefeux sur vos ordinateurs windows

2. MESSAGERIE AVEC UN CLIENT WEBMAIL

1 Sur les postes clients, éditer le fichier système « hosts » pour associer le nom du serveur mail « mailhost.mondomaine.fr » avec l'adresse IP du serveur mail.

Windows\system32\drivers\etc\hosts

2 - Sur deux postes clients utiliser vos navigateurs Web pour accéder au serveur email en utilisant les comptes clients emails « **alice** » et « **bob** » précédemment créés. Alice rédige et envoi un message à destination de « bob ».

3 - Quelle est l'URL que doit utiliser le client « alice » ?

Alice peut utiliser mailhost.mondomaine.fr

4 - Est-il possible de capturer votre login et votre mot de passe ? Passe-t-il en clair ?

Le login et le mot de passe passent en clair, comme on peut le voir sur Wireshark :

No.	Time	Source	Destination	Protocol	Length	Info
10	7.842524	127.0.0.1	127.0.0.1	TCP	56	80 → 51994 [SYN, ACK] Seq=0 Ack=
11	7.842631	127.0.0.1	127.0.0.1	TCP	44	51994 → 80 [ACK] Seq=1 Ack=1 Win
12	7.843066	127.0.0.1	127.0.0.1	TCP	56	51995 → 80 [SYN] Seq=0 Win=64240
13	7.843150	127.0.0.1	127.0.0.1	TCP	56	80 → 51995 [SYN, ACK] Seq=0 Ack=
14	7.843242	127.0.0.1	127.0.0.1	TCP	44	51995 → 80 [ACK] Seq=1 Ack=1 Win
15	7.845332	192.168.0.22	192.168.0.255	NBNS	82	Name query NB WPAD<00>
16	7.847024	fe80::e856:91d6:e43...	ff02::1:3	LLMNR	74	Standard query 0x2f3e A wpad
17	7.847649	192.168.0.22	224.0.0.252	LLMNR	54	Standard query 0x2f3e A wpad
18	7.853664	127.0.0.1	127.0.0.1	HTTP	969	POST /webmail/dologin.php HTTP/1
19	7.853734	127.0.0.1	127.0.0.1	TCP	44	80 → 51994 [ACK] Seq=1 Ack=926 W

Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
Referer: http://mailhost.mondomaine.fr/webmail/login.php?reason=logout\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
> Cookie: _ga=GA1.2.1888662351.1606394245; _gid=GA1.2.1718273218.1606394245; Session_webmail80=da613407ba9d
\r\n
[Full request URI: http://mailhost.mondomaine.fr/webmail/dologin.php]
[HTTP request 1/6]
[Response in frame: 22]
[Next request in frame: 24]
File Data: 72 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "x_2la" = "internal"
- > Form item: "kerio_username" = "alice" ←
- > Form item: "kerio_password" = "user1" ←
- > Form item: "kerio_mode" = "full"

0000 02 00 00 00 45 00 03 c5 5c 09 40 00 80 06 00 00E... \.0.....

5 - Est-il possible de lire le contenu du message ?

Oui, le titre de mon mail était « Salut ! » et le contenu « Salut Bob ! ». Voici une capture de Wireshark :

110	29.214041	127.0.0.1	127.0.0.1	TCP	44	52100 → 80	[ACK] Seq=682 Ack=249 Win=52
111	29.243941	127.0.0.1	127.0.0.1	TCP	56	52101 → 80	[SYN] Seq=0 Win=64240 Len=0
112	29.244030	127.0.0.1	127.0.0.1	TCP	56	80 → 52101	[SYN, ACK] Seq=0 Ack=1 Win=6
113	29.244101	127.0.0.1	127.0.0.1	TCP	44	52101 → 80	[ACK] Seq=1 Ack=1 Win=525568
114	29.267138	127.0.0.1	127.0.0.1	TCP	932	52100 → 80	[PSH, ACK] Seq=682 Ack=249 W
115	29.267201	127.0.0.1	127.0.0.1	TCP	44	80 → 52100	[ACK] Seq=249 Ack=1570 Win=5
116	29.267269	127.0.0.1	127.0.0.1	TCP	1504	52100 → 80	[ACK] Seq=1570 Ack=249 Win=5
117	29.267280	127.0.0.1	127.0.0.1	HTTP	736	POST /webmail/mailCompose.php?	HTTP/1.1

▼ [Timestamps]

[Time since first frame in this TCP stream: 0.311910000 seconds]

[Time since previous frame in this TCP stream: 0.000068000 seconds]

TCP payload (1460 bytes)

[Reassembled PDU in frame: 117]

TCP segment data (1460 bytes)

0220	72 6d 2d 64 61 74 61 3b	20 6e 61 6d 65 3d 22 6b	rm-data; name="k
0230	65 72 69 6f 5f 6d 61 69	6c 53 75 62 6a 65 63 74	erio_mailSubject
0240	22 0d 0a 0d 0a 53 61 6c	75 74 21 0d 0a 2d 2d 2d	"...Salut!..."
0250	2d 2d 2d 57 65 62 4b 69	74 46 6f 72 6d 42 6f 75	---WebKitFormBou
0260	6e 64 61 72 79 6b 6d 79	59 61 4f 6c 43 41 79 33	ndarykmy YaOlCAy3
0270	35 6b 41 36 77 0d 0a 43	6f 6e 74 65 6e 74 2d 44	5kA6w...Content-D
0280	69 73 70 6f 73 69 74 69	6f 6e 3a 20 66 6f 72 6d	isposition: form
0290	2d 64 61 74 61 3b 20 6e	61 6d 65 3d 22 6b 65 72	-data; name="ker
02a0	69 6f 5f 6d 61 69 6c 42	6f 64 79 22 0d 0a 0d 0a	io_mailBody"...
02b0	53 61 6c 75 74 20 42 6f	62 21 0d 0a 2d 2d 2d 2d	Salut Bob!..."
02c0	2d 2d 57 65 62 4b 69 74	46 6f 72 6d 42 6f 75 6e	---WebKitFormBoun

6 - Proposer et décrire une solution pour sécuriser votre accès au courriel par le web.

Kerio propose de chiffrer les données. Il suffit d'aller dans la console d'administration pour Kerio mailserver, puis dans « Configuration », avant de sélectionner l'onglet « options avancées » à gauche. Apparaît alors l'onglet « Politique de sécurité », c'est le deuxième onglet. Il faut alors aller dans « Police de sécurité » et choisir l'obligation d'authentification sécurisée, comme on peut le voir sur la capture infra :

On peut s'assurer que le certificat SSL du serveur soit connu du client. Pour cela, il faut le télécharger dans l'onglet « Certificats SSL » et l'installer sur la machine du client dans le magasin « autorités de certification racine de confiance ». Je suis allé vérifier sur Wireshark : impossible de retrouver des traces des identifiants ou du corps du mail. Comme c'est indiqué, tout est chiffré dès le handshake :

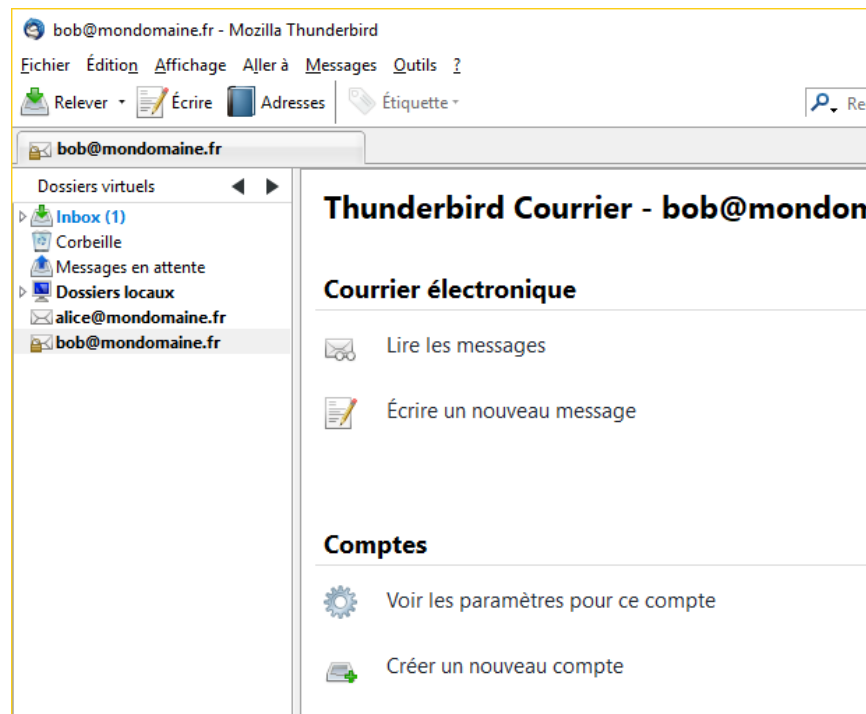
Time	Source	Destination	Protocol	Length	Info
1 0.000000	127.0.0.1	127.0.0.1	TCP	56	52272 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256 SACK_PER
2 0.000093	127.0.0.1	127.0.0.1	TCP	56	443 → 52272 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=2
3 0.000170	127.0.0.1	127.0.0.1	TCP	44	52272 → 443 [ACK] Seq=1 Ack=1 Win=525568 Len=0
4 0.000647	127.0.0.1	127.0.0.1	TCP	56	52273 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256 SACK_PER
5 0.000727	127.0.0.1	127.0.0.1	TCP	56	443 → 52273 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=2
6 0.000795	127.0.0.1	127.0.0.1	TCP	44	52273 → 443 [ACK] Seq=1 Ack=1 Win=525568 Len=0
7 0.001435	127.0.0.1	127.0.0.1	TLSv1	561	Client Hello
8 0.001499	127.0.0.1	127.0.0.1	TCP	44	443 → 52272 [ACK] Seq=1 Ack=518 Win=525568 Len=0
9 0.001701	127.0.0.1	127.0.0.1	TLSv1	182	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10 0.001740	127.0.0.1	127.0.0.1	TCP	44	52272 → 443 [ACK] Seq=518 Ack=139 Win=525568 Len=0
11 0.002155	127.0.0.1	127.0.0.1	TLSv1	561	Client Hello

7 - Quel est l'intérêt d'utiliser le WebMail en lieu et place d'un système classique de courriel (outlook, thunderbird) ?

Le mail ne passe pas par la machine par Webmail et il n'y est pas stocké dessus. Ainsi, c'est plus sécurisé.

3. MESSAGERIE VIA UN CLIENT MAIL THUNDERBIRD (PROTOCOLES SMTP, POP ET IMAP)

1. Installer et configurer sur les postes clients, le client email « Thunderbird » en utilisant les 2 comptes « **alice** » « **bob** » en utilisant les protocoles **IMAP** et **SMTP** en mode **non sécurisés**.



2. rédiger un email par le client **alice** et l'envoyer au client **bob** avec le contenu suivant « bonjour Bob, ceci est un test IMAP4 de Alice ». Avec Wireshark et TCPview analyser les échanges et répondre aux questions suivantes :

- Quel est le protocole applicatif utilisé par « **alice** » pour l'envoi du message ?

- Quel est le protocole de transport (UDP ou TCP) utilisé par « **alice** » pour l'envoi du message ?

- Quel est le port du client ?

- Quel est le port du serveur ?

- Est-il possible de capturer votre login et votre mot de passe ? Passe-t-il en clair ?

```

39 15.736146 127.0.0.1 127.0.0.1 TCP 44 25 → 53615 [ACK] Seq=55 Ack=19 Win=525568 Len=0
40 15.736317 127.0.0.1 127.0.0.1 SMTP 208 S: 250-mondomaine.fr | AUTH CRAM-MD5 PLAIN LOGIN DIGEST-MD5
41 15.736360 127.0.0.1 127.0.0.1 TCP 44 53615 → 25 [ACK] Seq=19 Ack=219 Win=261120 Len=0
42 15.736402 127.0.0.1 127.0.0.1 TCP 45 53064 → 53065 [PSH, ACK] Seq=14 Ack=1 Win=65335 Len=1
43 15.736444 127.0.0.1 127.0.0.1 TCP 44 53065 → 53064 [ACK] Seq=1 Ack=15 Win=65299 Len=0
44 15.736798 127.0.0.1 127.0.0.1 TCP 45 53064 → 53065 [PSH, ACK] Seq=15 Ack=1 Win=65335 Len=1
45 15.736847 127.0.0.1 127.0.0.1 TCP 44 53065 → 53064 [ACK] Seq=1 Ack=15 Win=65299 Len=0

Implement Mail Transfer Protocol
' Response: 250-mondomaine.fr\r\n
    Response code: Requested mail action okay, completed (250)
    Response parameter: mondomaine.fr
    Response parameter: AUTH CRAM-MD5 PLAIN LOGIN DIGEST-MD5 NTLM
    Response parameter: STARTTLS
    Response parameter: ENHANCEDSTATUSCODES
    Response parameter: 8BITIME
    Response parameter: PIPELINING
    Response parameter: ETRN
    Response parameter: DSN
    Response parameter: HELP

```

- Oui, voici la capture qui le met en évidence :

Offset	Hex	ASCII
74	15.785858	127.0.0.1
75	15.785865	127.0.0.1
76	15.788064	127.0.0.1
77	15.788127	127.0.0.1
78	15.788232	127.0.0.1
79	15.788247	127.0.0.1
80	15.788304	127.0.0.1

Offset	Hex	ASCII
45	53064 → 53065	[PSH, ACK] Seq=22 Ack=1 Win=65335 Len=1
44	53065 → 53064	[ACK] Seq=1 Ack=23 Win=65297 Len=0
45	53064 → 53065	[PSH, ACK] Seq=23 Ack=1 Win=65335 Len=1
44	53065 → 53064	[ACK] Seq=1 Ack=24 Win=65297 Len=0
1504	C: DATA fragment, 1460 bytes	
448	from: Alice <alice@localhost>, subject: Bonjour, (text/plain)	
44	25 → 53615 [ACK] Seq=270 Ack=1073 Win=53568 Len=0	


```

This is a multi-part message in MIME format.\r\n
-----030300030407020100030206\r\n
Content-Type: text/plain; charset=ISO-8859-1; format=flowed\r\n
Content-Transfer-Encoding: 7bit\r\n
\r\n
bonjour Bob, ceci est un test IMAP4 de Alice\r\n
\r\n
\r\n
-----030300030407020100030206\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
Content-Transfer-Encoding: 7bit\r\n
\r\n

```


Offset	Hex	ASCII
63	61 6c 68 6f 73 74 0d 0a 53 75 62 6a 65 63 74	calhost: Subject
64	3a 20 42 6f 6e 6a 6f 75 72 0d 0a 43 6f 6e 74 65	: Bonjour r...Conte
65	6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61	nt-Type: multipa
66	72 74 2f 61 6c 74 65 72 6e 61 74 69 76 65 3b 0d	rt/alter native;
67	0a 20 62 6f 75 6e 64 61 72 79 3d 22 2d 2d 2d 2d	boundary="----
68	2d 2d 2d 2d 2d 2d 2d 2d 30 33 30 33 30 30 33	----- 03030003
69	30 34 30 37 30 32 30 31 30 30 30 33 30 32 30 36	04070201 00030206
70	22 0d 0a 0d 0a 54 68 69 73 20 69 73 20 61 20 6d	"....This is a m
71	75 6c 74 69 2d 70 61 72 74 20 6d 65 73 73 61 67	ulti-par t messag
72	65 20 69 6e 20 4d 49 4d 45 20 66 6f 72 6d 61 74	e in MIM E format
73	2e 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d

Offset	Hex	ASCII
0	20	Text item (text), 18 byte(s)

Offset	Hex	ASCII
0	20	Request: 200 : Affichage

- Quel est le protocole de transport (UDP ou TCP) utilisé pour la réception du message ?

- Quel est le port du client ?

- Quel est le port du serveur ?

- Est-il possible de capturer votre login et votre mot de passe ? Passe-t-il en clair ?

127.0.0.1	TCP	44	143 → 50143 [ACK] Seq=53 Ack=15 Win=525568 Len=0
127.0.0.1	IMAP	283	Response: 1 OK CAPABILITY completed

OK ACL LITERAL+ UIDPLUS QUOTA ID SORT ANNOTATE ANNOTATEMORE STATUS-COUNTERS UNSELECT LISTEXT NAMESPACE XLIST STARTTLS AUTH=CRAM-MD5 AUTH=PLAIN AUTH=

- Oui, dans le segment IMAP(voir capture suivante)

3 expliquer dans un tableau comparatif, les principales différences fonctionnelles entre un client email utilisant le protocole **POP3** ou le protocole **IMAP4**.

	POP3	IMAP4
Conservation des mails	En local	Sur le serveur
Synchronisation sur autres machines	Non	Oui
Port du serveur	110	143
Possibilité de structurer mails dans dossiers	Non	Oui
Accessibilité	Une machine à la fois	Plusieurs machines simultanément
Possibilité de lire mail hors-ligne	Oui	Non

4 Au moyen de la commande système « nslookup », déterminer les adresses IP et les noms des serveurs SMTP de votre université ainsi que le nom symbolique du serveur DNS (Domain Name Service) utilisées par votre terminal pour naviguer sur l'Internet ? Reportez ces informations ci-dessous.

J'ai fait un nslookup sur mon localhost (qui a pour alias mailhost.mondomaine.fr). Voici le résultat :

Serveur : dns1.proxad.net
Address: 212.27.40.240

Nom : localhost
Addresses: ::1
127.0.0.1

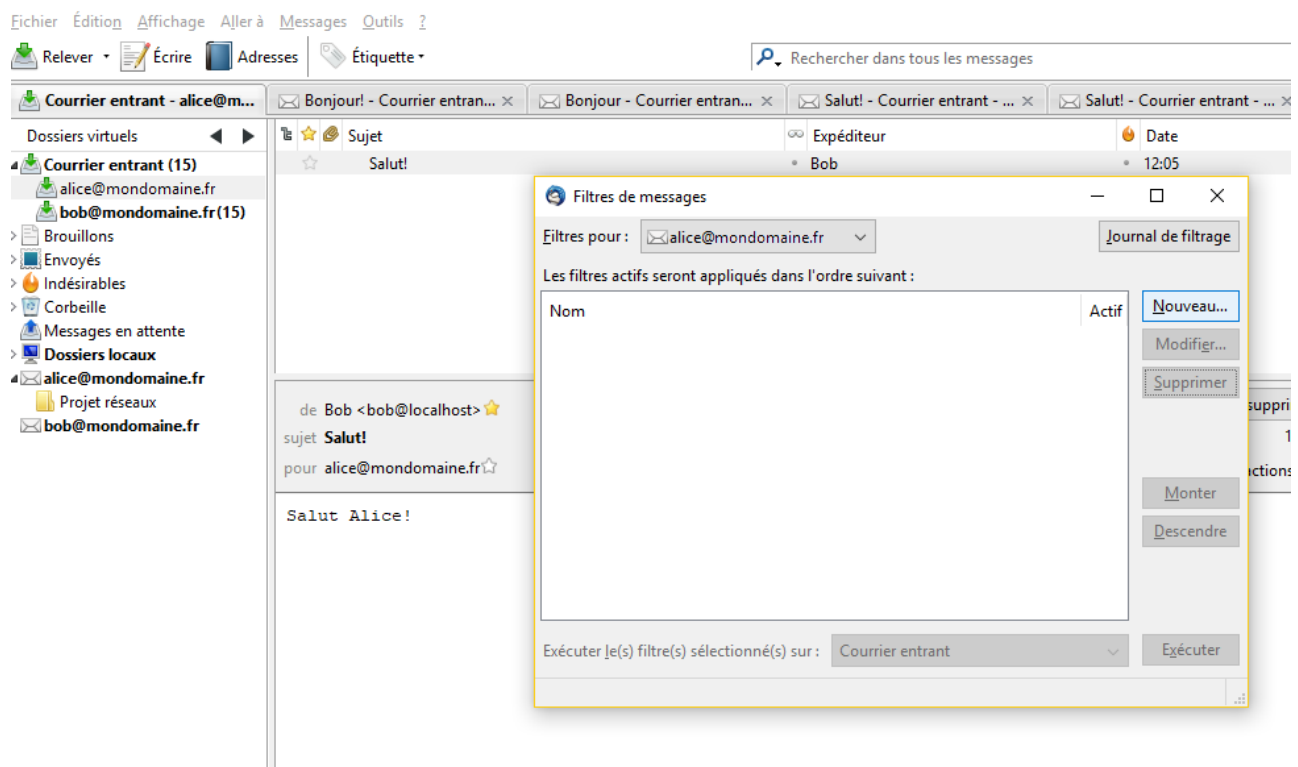
5. Créer un répertoire « Projet Réseaux » dans la boîte email de « Alice ». Puis configurer un « **Filtre** » des messages appelé « projet Réseaux » qui devra classer automatiquement les messages envoyés à Alice et respectant les règles suivantes :

- Si les mots « projet » OU « réseaux » font partis du sujet du message reçus ET si l'émetteur est « Bob ».

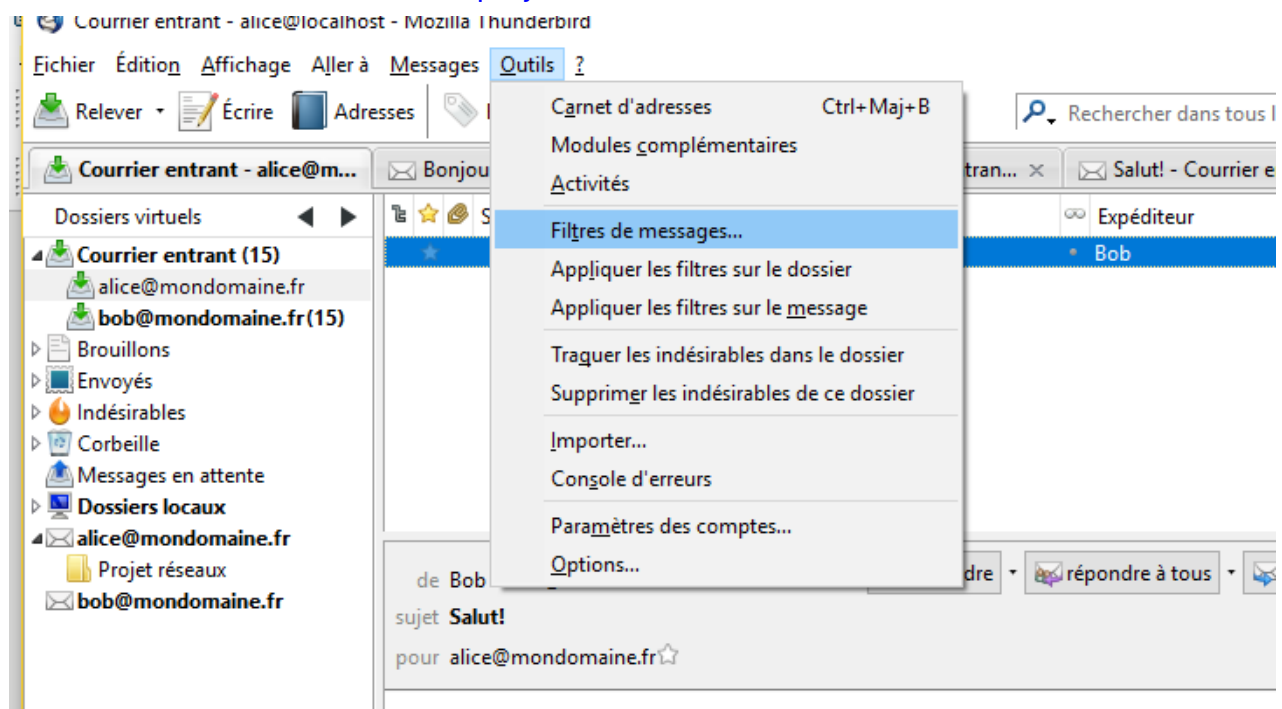
Faire un test d'envoi de messages de **Bob** vers Alice avec comme sujet « **projets** ». Puis un second message de **Bob** vers **Alice** avec comme sujet « **projet** ».

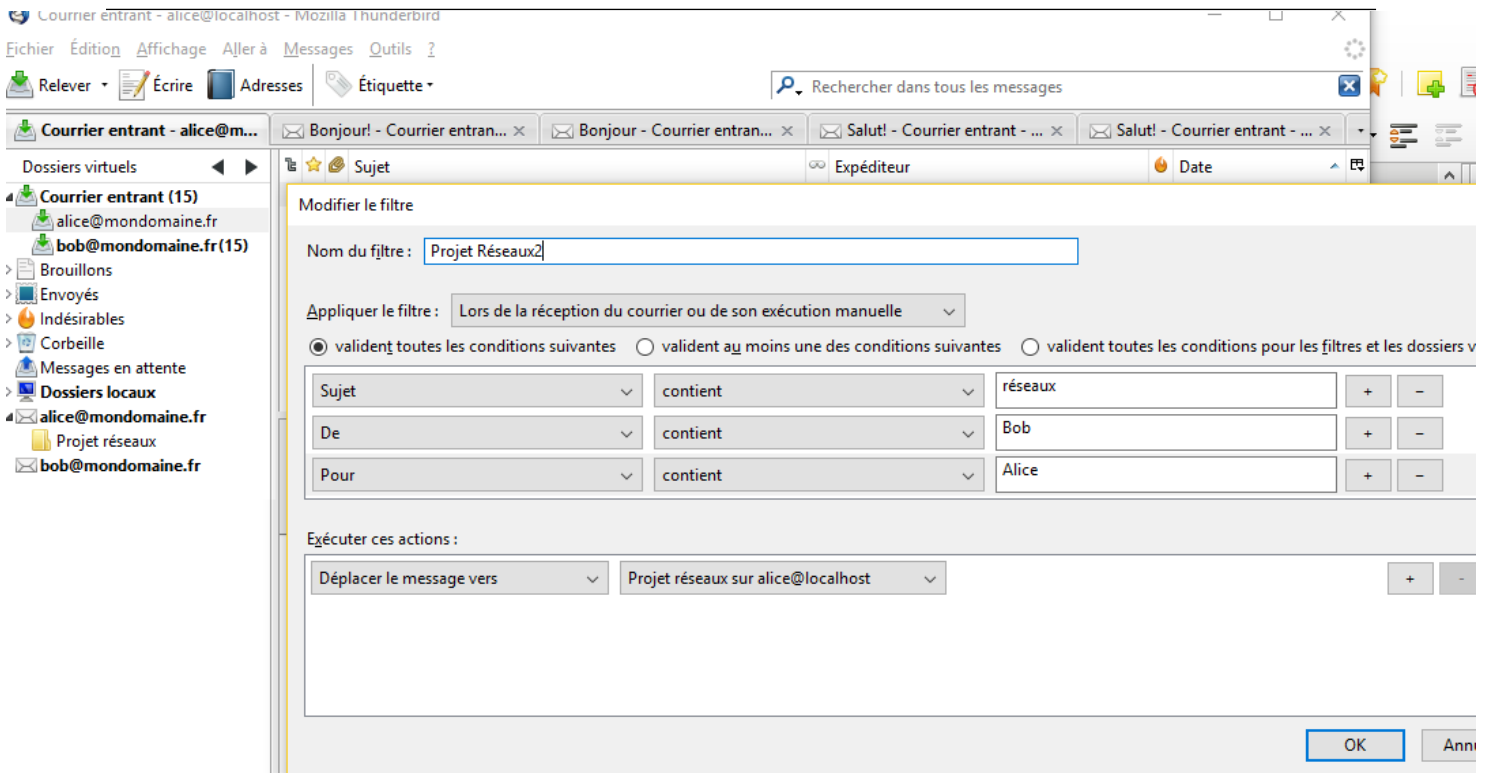
Les mails ayant « projets » et « projet » dans le titre sont automatiquement mis dans le dossier « Projet Réseaux ». Voici comment j'ai procédé :

1) Création du dossiers et accès au menu des filtres (capture à la page suivante)

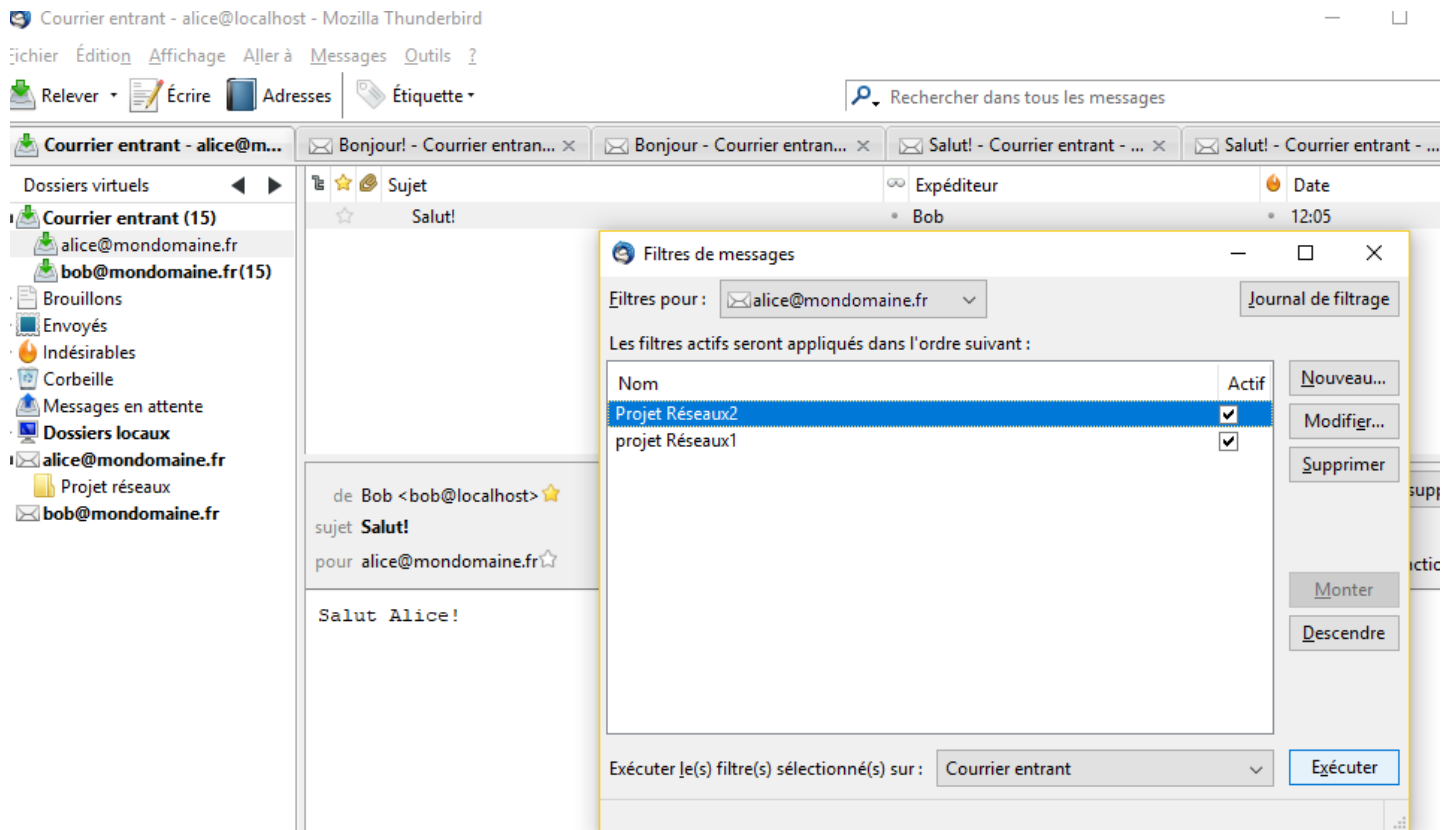


2) Ajout des filtres. Un qui vérifie que l'expéditeur soit Bob, le destinataire Alice et que le titre contienne « projet », l'autre identique sauf qu'il vérifie que le titre contienne « réseaux » et non « projet »



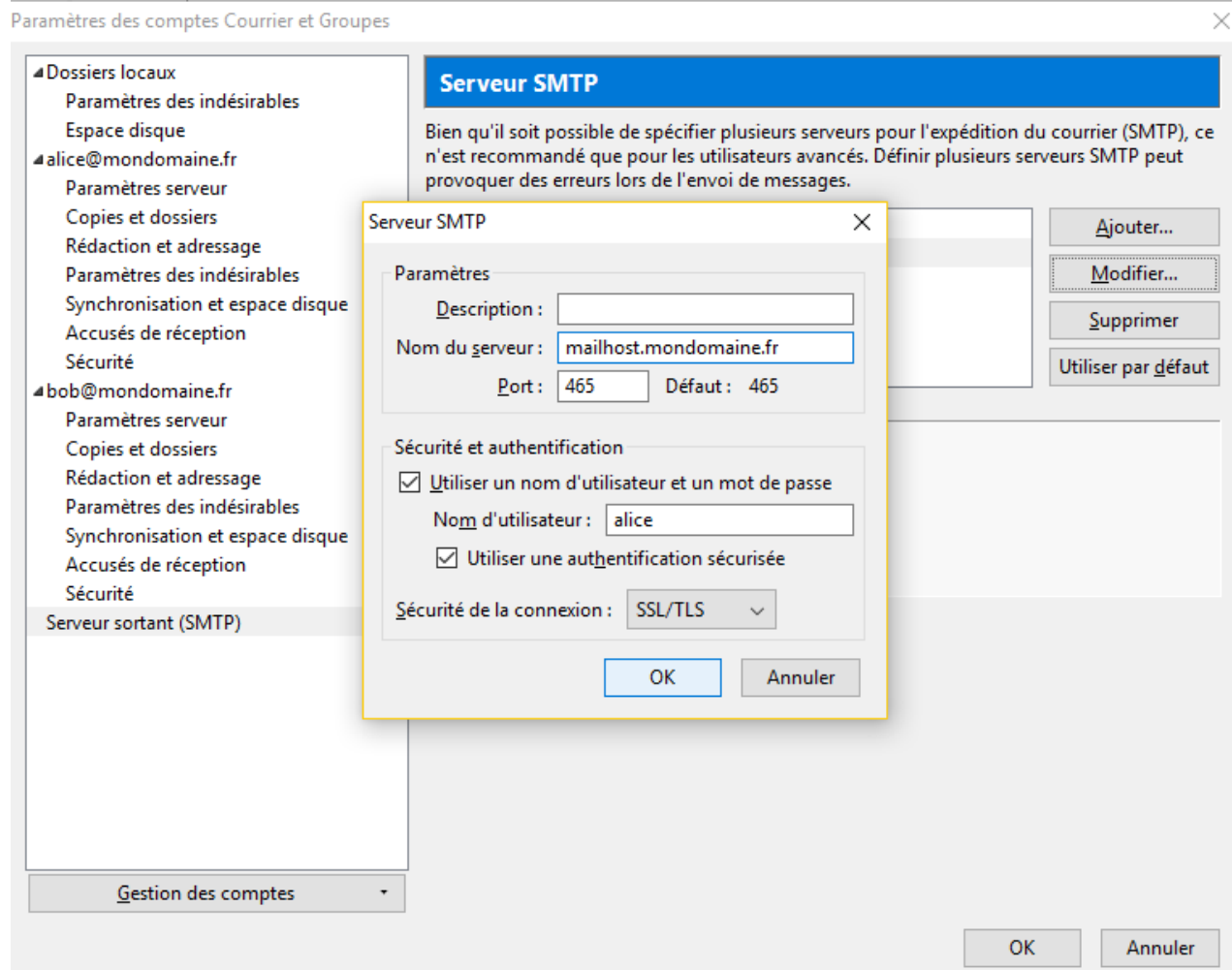


3) On exécute les filtres



4. SECURITÉ DU COURRIEL AVEC SSL (SMTPS ET IMAPS)

1 – configurer votre client pour que « **Alice** » puisse transmettre un email à « **Bob** » en utilisant le **protocole SMTP over SSL (SMTPS)**. Le sujet et le contenu du message seront « test d'envoi de message avec SMTPS »



2 – quel est le numéro de port du serveur **SMTPS** ?

Un serveur SMTPS a pour numéro de port le 465

3 – avec le sniffer de réseau, vérifier si :

- votre login et mot de passe sont transmis en clair ?

Les identifiants sont chiffrés.

- le contenu du message est en clair et peut donc être intercepté ?

Le contenu du message est chiffré.

4 – quel(s) type(s) de chiffrement et de clé(s) est (sont) utilisé(s) par SMTPS ?

Alice et Bob génèrent leurs paires de clés : chacun a une clé publique et une privée. Alice chiffre le message avec la clé publique de Bob et lui envoie le message chiffré. Bob reçoit le message et le déchiffre avec sa clé privée.

5 - Quels sont les services de sécurité fournis par une connexion SMTP over SSL (SMTPS) ?

SMTPS garantit l'authentification, l'intégrité des données et la confidentialité.

6 - configurer votre client pour que « **Alice** » puisse récupérer son email de « Bob » en utilisant le **protocole IMAP over SSL (IMAPS)**.

Paramètres des comptes Courrier et Groupes

×

7 - quel est le numéro de port du serveur **IMAPS** ?

IMAPS utilise le port 993

8 - avec le sniffer de réseau, vérifier si (faite une capture d'écran du logiciel wireshark):

Time	Source	Destination	Protocol	Length	Info
5.483121	127.0.0.1	127.0.0.1	TCP	45	50717 → 50718 [PSH, ACK] Seq=37 Ack=1 Win=261340 Len=1
5.483153	127.0.0.1	127.0.0.1	TCP	44	50718 → 50717 [ACK] Seq=1 Ack=38 Win=261300 Len=0
5.483399	127.0.0.1	127.0.0.1	TLSv1	204	Client Hello
5.483448	127.0.0.1	127.0.0.1	TCP	44	993 → 50731 [ACK] Seq=1 Ack=161 Win=525568 Len=0
5.483494	127.0.0.1	127.0.0.1	TCP	45	50723 → 50724 [PSH, ACK] Seq=4 Ack=1 Win=261340 Len=1
5.483527	127.0.0.1	127.0.0.1	TCP	44	50724 → 50723 [ACK] Seq=1 Ack=5 Win=261336 Len=0
5.483649	127.0.0.1	127.0.0.1	TCP	45	50717 → 50718 [PSH, ACK] Seq=38 Ack=1 Win=261340 Len=1
5.483711	127.0.0.1	127.0.0.1	TLSv1	618	Server Hello, Certificate, Server Hello Done
5.483725	127.0.0.1	127.0.0.1	TCP	44	50718 → 50717 [ACK] Seq=1 Ack=39 Win=261300 Len=0
5.483875	127.0.0.1	127.0.0.1	TCP	44	50731 → 993 [ACK] Seq=161 Ack=575 Win=260764 Len=0
5.483906	127.0.0.1	127.0.0.1	TCP	45	50717 → 50718 [PSH, ACK] Seq=39 Ack=1 Win=261340 Len=1
5.483951	127.0.0.1	127.0.0.1	TCP	44	50718 → 50717 [ACK] Seq=1 Ack=40 Win=261300 Len=0
5.489438	127.0.0.1	127.0.0.1	TLSv1	242	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5.489505	127.0.0.1	127.0.0.1	TCP	44	993 → 50731 [ACK] Seq=575 Ack=359 Win=525312 Len=0

800: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_{Loopback}, id 1

oopback

et Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

- votre login et mot de passe sont transmis en clair ?

Non, tout est chiffré depuis le handshake.

- le contenu du message est transmis en clair ?













Idem.

9 – Quel est le numéro port du serveur **POP3S** (POP3 over SSL) ?

Une serveur POP3S utilise le numéro port 995 par défaut, cf Kerio.



Services

Service	État	Type de démarrage	Adresses IP reconnues
 SMTP	Démarré	Automatique	Toutes les adresses:25
 SMTP sécurisé	Démarré	Automatique	Toutes les adresses:465
 POP3	Démarré	Automatique	Toutes les adresses:110
 POP3 sécurisé	Démarré	Automatique	Toutes les adresses:995
 IMAP	Démarré	Automatique	Toutes les adresses:143
 IMAP sécurisé	Démarré	Automatique	Toutes les adresses:993
 NNTP	Démarré	Automatique	Toutes les adresses:119
 NNTP sécurisé	Démarré	Automatique	Toutes les adresses:563
 LDAP	Démarré	Automatique	Toutes les adresses:389
 LDAP sécurisé	Démarré	Automatique	Toutes les adresses:636
 HTTP	Démarré	Automatique	Toutes les adresses:80
 HTTP sécurisé	Démarré	Automatique	Toutes les adresses:443