TP 3 – Mails

Après avoir configuré Postfix, on peut envoyer un email en telnet sur le port 25 ou avec la commande mail, et on s'aperçoit que le mail a été traité dans /var/log/mail.log. Alice peut lire son mail dans /var/mail/alice :

```
thomas@lxle-vmware:~$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 lxle.cs.sr ESMTP Postfix (Ubuntu)
HELO client
250 lxle.cs.sr
MAIL FROM: Bob<bob@client.fr>
250 2.1.0 Ok
RCPT TO: Alice<alice@lxle.cs.sr>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subjet: test

Helo Alice
.
250 2.0.0 Ok: queued as B575265B5E
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
thomas@lxle-vmware:~$
```

```
thomas@lxle-vmware:~$ mail -s Coucou alice@lxle.cs.sr
Cc:
Helo, Alice (bis)
```

```
thomas@lxle-vmware:~$ sudo cat /var/mail/alice
From bob@client.fr  Wed Jan  4 08:42:43 2023
Return-Path: <bob@client.fr>
X-Original-To: alice@lxle.cs.sr
Delivered-To: alice@lxle.cs.sr
Received: from client (localhost [127.0.0.1])
        by lxle.cs.sr (Postfix) with SMTP id B575265B5E
        for <alice@lxle.cs.sr>; Wed,  4 Jan 2023 08:41:33 +0100 (CET)
Subjet: test
Message-Id: <20230104074153.B575265B5E@lxle.cs.sr>
Date: Wed,  4 Jan 2023 08:41:33 +0100 (CET)
From: bob@client.fr

Helo Alice

thomas@lxle-vmware:~$
```

Je change ensuite les interfaces d'écoute :

```
mydestination = $myhostname, $mydomain, localhost.$mydomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 192.168.126.0/24
```

Adresse inconnue :

```
VRFY pouet@lxle.cs.sr
550 5.1.1 <pouet@lxle.cs.sr>: Recipient address rejected: User unknown in local recipient table
```

Pour se connecter depuis kali, il ne faut pas oublier d'ouvrir le port 25 sur le parefeu :

sudo ufw allow 25

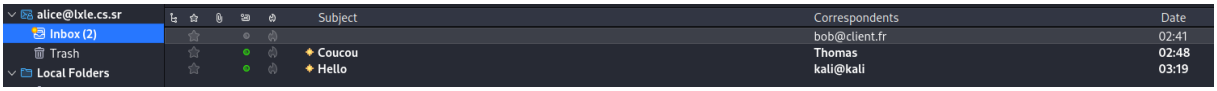
L'envoi de mail fonctionne correctement

Si on change la configuration de ssmtp, on peut utiliser sendmail :

```
┌──(kali㉿kali)-[~]
└─$ sendmail alice@lxle.cs.sr
Subject: Hello

Hello from kali

┌──(kali㉿kali)-[~]
```

```
Received: from kali (unknown [192.168.126.21])
        by lxle.cs.sr (Postfix) with SMTP id C28F065B5E
        for <alice@lxle.cs.sr>; Wed,  4 Jan 2023 09:19:52 +0100 (CET)
Received: by kali (sSMTP sendmail emulation); Wed, 04 Jan 2023 03:19:13 -0500
From: kali@kali
Date: Wed, 04 Jan 2023 03:19:13 -0500
Subject: Hello

Hello from kali
```

Après avoir configué Thunderbird pour utiliser STARTTLS sur le port 443, avec le nom d'utilisateur alice :



Si le serveur SMTP n'est pas correctement configuré, cela semble très imprudent de le laisser ouvert à l'extérieur.

Il doit être possible de retrouver son mot de passe si elle se connecte par IMAP dans le cas où le mot de passe n'est pas hashé, ou bien d'intercepter la connexion pour la forcer à envoyer ses mots de passe en clair.

Tunnel SSH :

On ouvre le port sur LXLE : *sudo ufw allow 22*

Sur KALI, on créé le tunnel : ssh -L 2023:localhost:143 thomas@192.168.126.11

Il ne reste plus qu'à utiliser le port 2023 et l'hôte localhost sur Thunderbird sur KALI

On observe sur Wireshark que tout le trafic transite via SSH.