SÉCURITÉ DES SYSTÈMES DE MESSAGERIE

Jonathan CERTES

1 Environnement de travail

1.1 Travail dans une machine virtuelle

Télécharger Oracle VirtualBox :
`https://www.virtualbox.org/wiki/Downloads`
Installer VirtualBox sur sa machine personnelle :
`https://www.virtualbox.org/manual/UserManual.html#installation`
Télécharger la machine virtuelle fournie par l'enseignant.
Importer la machine virtuelle dans VirtualBox :
`https://www.virtualbox.org/manual/UserManual.html#ovf-import-appliance`
Démarrer la machine virtuelle :
`https://www.virtualbox.org/manual/UserManual.html#intro-starting`
Tout le TP sera réalisé dans la machine virtuelle.

1.2 Environnement

La machine virtuelle contient un conteneur `lxc` par machine du réseau virtuel pour ce TP (hôte ou routeur). Ces conteneurs ne possèdent pas d'interface graphique. Il s'agit de lancer un terminal dans la machine virtuelle et de s'y attacher autant de fois que nécessaire, pour tous les conteneurs.

Le lancement des conteneurs est automatisé par un script présent dans la machine virtuelle. Pour procéder à leur lancement, ouvrir un terminal et exécuter les commandes suivantes :

```
debian@myhostname:~$ cd tp-mail/
debian@myhostname:~/tp-mail$ ./start.sh
```

Le mot de passe pour le compte utilisateur est : `debian`.

1.3 S'associer aux conteneurs

Dans 4 terminaux, répéter ces actions pour les 4 conteneurs `alice`, `bob`, `gafam` et `eve` :

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$
```

1.4 Ouvrir Wireshark sur la machine virtuelle

La dernière étape de préparation de ce TP est le lancement de Wireshark sur les bridges (switchs virtuel) de notre réseau. Il n'est nécessaire d'observer le traffic que sur le bridge `br-gafam` mais vous pouvez également regarder ailleurs.

Dans un terminal :

```
debian@myhostname:~$ sudo wireshark
```

Réduire le terminal **sans le fermer**. Sélectionner la capture sur le bridge `br-gafam`. Une fois la capture lancée, appliquer le filtre `imap||smtp`.

2 Objectifs

L'objectif de ces séances est de se familiariser avec la configuration serveurs mails et les principes de confidentialité et d'authentification des systèmes de messagerie.

C'est parti !

3 Introduction

Postfix est un serveur de messagerie électronique et un logiciel libre développé par Wietse Venema et plusieurs contributeurs. Il se charge de la livraison de courriers électroniques (courriels) et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail.

Il est le serveur de courriel par défaut dans plusieurs systèmes de type UNIX, comme Mac OS X, NetBSD, diverses distributions GNU/Linux, etc.

Postfix est publié sous licence IBM Public License 1.0. C'est une licence libre, mais incompatible avec la GPL.

Source : `https://fr.wikipedia.org/wiki/Postfix`

Dovecot est un serveur IMAP et POP3 pour les systèmes d'exploitation Unix et dérivés, conçu avec comme premier but la sécurité. Dovecot est distribué en double licence MIT et LGPL-2.1-only.

Source : `https://fr.wikipedia.org/wiki/Dovecot`

OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques, libcrypto et libssl, fournissant respectivement une implémentation des algorithmes cryptographiques et du protocole de communication SSL/TLS, ainsi qu'une interface en ligne de commande, `openssl`.

Développée en C, OpenSSL est disponible sur les principaux systèmes d'exploitation et dispose de nombreux wrappers, ce qui la rend utilisable dans une grande variété de langages informatiques. En 2014, deux tiers des sites Web l'utilisaient.

Source : `https://fr.wikipedia.org/wiki/OpenSSL`

Pretty Good Privacy (qu'on pourrait traduire en français "assez bon niveau de confidentialité"), plus connu sous le sigle PGP, est un logiciel de chiffrement cryptographique, développé et diffusé aux États-Unis par Philip Zimmermann en 1991.

PGP se propose de garantir la confidentialité et l'authentification pour la communication des données. Il est souvent utilisé pour la signature de données, le chiffrement et le déchiffrement des textes, des courriels, fichiers, répertoires et partitions de disque entier. Utilisant la cryptographie asymétrique mais également la cryptographie symétrique, il fait partie des logiciels de cryptographie hybride.

PGP et les produits similaires suivent le standard OpenPGP (RFC 4880) pour le chiffrement et le déchiffrement de données.

Source : `https://fr.wikipedia.org/wiki/Pretty_Good_Privacy`

Mozilla Thunderbird est un client de messagerie, libre, distribué gratuitement par la fondation Mozilla et issu du projet Mozilla. Consacré à l'origine au courrier électronique, aux groupes de discussion et aux flux RSS et Atom, il s'est au fil du temps équipé de fonctionnalités supplémentaires tels qu'agenda, de gestionnaire de tâches et de messagerie instantanée, lui conférant désormais le titre de collecticiel.

Il est également "extensible", c'est-à-dire qu'il peut facilement recevoir de nouvelles fonctionnalités par l'ajout d'extensions.

Thunderbird est distribué selon les termes de la licence publique Mozilla (MPL) et diverses autres licences libres, ce qui lui permet d'être porté sur la plupart des systèmes d'exploitation.

Le logiciel est intégré à la liste des logiciels libres préconisés par l'État français dans le cadre de la modernisation globale de ses systèmes d'informations (SI).

Le logiciel est disponible dans 65 langues.

Source : `https://fr.wikipedia.org/wiki/Mozilla_Thunderbird`

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Wireshark utilise la bibliothèque logicielle Qt pour l'implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows. Il existe aussi entre autres une version en ligne de commande nommé TShark. Ces programmes sont distribués gratuitement sous la licence GNU General Public License.

Wireshark reconnaît 1 515 protocoles.

Source : `https://fr.wikipedia.org/wiki/Wireshark`

4 Configuration réseau

Procéder au lancement des conteneurs comme décrit dans la section 1.2. L'architecture du réseau virtuel créée est représentée sur la figure 1. Chaque machine possède, sur ce réseau, une adresse IPv6 et un nom.

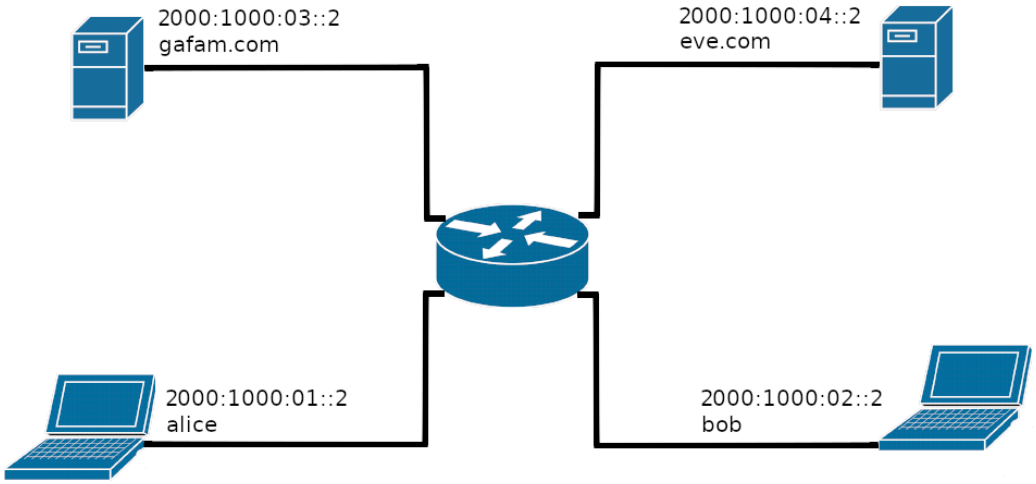

FIGURE 1 – Architecture du réseau

Dans ce TP, nous incarnons de manière très originale Alice et Bob, qui travaillent tous deux pour l'entreprise GAFAM. Alice est administratrice système, Bob est gestionnaire. Alice et Bob sont en télétravail et peuvent se connecter à la machine qui héberge le site `gafam.com`.

Également, dans ce TP, nous incarnons Eve, notre utilisateur malveillant, qui possède son propre serveur hébergeant le site `eve.com`.

Chacune des machines est connectée au réseau publique "internet", simulé ici par un simple routeur. Il est également possible de prendre le contrôle de ce routeur avec la commande suivante :

```
debian@myhostname:~$ sudo lxc-attach router
root@router:/$
```

5 Mise en place du serveur mail

Nous utilisons les fonctionnalités de Postfix pour le serveur SMTP et celles de Dovecot pour le serveur IMAP.

Question 1 Installer Postfix sur la machine qui héberge le site `gafam.com`.

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ sudo apt install postfix
# chose "Internet Site" and select "gafam.com" as domain.
```

Vérifier qu'un processus écoute bien sur le port 25 :

```
root@gafam:/$ sudo ss -lnpt
```

Créer deux utilisateurs sur le serveur, `alice` et `bob`, qui seront respectivement les comptes de Alice et de Bob.

```
root@gafam:/$ sudo adduser alice
# chose a password and fill the informations (or leave them empty)
root@gafam:/$ sudo adduser bob
```

Envoyer un message de test à `alice` et vérifier sa réception.

```
root@gafam:/$ echo "My test message." | /usr/sbin/sendmail alice@localhost
root@gafam:/$ cat /var/mail/alice
```

Dans un premier temps, nous allons communiquer sur le réseau public sans chiffrement. Désactiver le chiffrement dans la configuration de Postfix et relancer le processus pour appliquer les changements.

```
root@gafam:/$ sudo nano /etc/postfix/main.cf
# replace the line "smtpd_tls_security_level=..." with "smtpd_tls_security_level=none"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart postfix
```

Question 2 Installer Dovecot sur la machine qui héberge le site `gafam.com`. Ajouter `dovecot` au groupe `mail` pour que celui-ci puisse accéder aux messages.

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ sudo apt install dovecot-core dovecot-imapd
root@gafam:/$ sudo adduser dovecot mail
```

Activer le protocole IMAP dans la configuration de Dovecot.

```
root@gafam:/$ sudo nano /etc/dovecot/dovecot.conf
# after the line "# Enable installed protocols", add "protocols = imap"
# save with Ctrl+O and quit with Ctrl+X
```

Dans un premier temps, nous allons communiquer sur le réseau public sans chiffrement. Autoriser l'authentification par mot de passe en clair, désactiver le chiffrement dans la configuration de Dovecot et relancer le processus pour appliquer les changements.

```
root@gafam:/$ sudo nano /etc/dovecot/conf.d/10-auth.conf
# replace the line "disable_plaintext_auth = ..." with "disable_plaintext_auth = no"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo nano /etc/dovecot/conf.d/10-ssl.conf
# replace the line "ssl = ..." with "ssl = no"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart dovecot
```

Vérifier qu'un processus écoute bien sur le port 143 :

```
root@gafam:/$ sudo ss -lnpt
```

6 Communication (avec le serveur) sans chiffrement

Nous utilisons Mozilla Thunderbird comme client de messagerie, qui permet une communication facile avec le serveur `gafam.com` pour Alice et pour Bob. Nous utilisons Wireshark pour analyser le trafic sur notre réseau virtuel, en particulier sur le bridge `br-gafam` qui est là où transitent tous les paquets en provenance de et à destination du serveur `gafam.com`.

Question 3 Utiliser Wireshark pour observer le trafic sur le réseau virtuel.

```
debian@myhostname:~$ sudo wireshark
```

Lancer une capture sur le bridge `br-gafam`. Appliquer le filtre `imap||smtp` pour ne voir affichés que les paquets des protocoles IMAP et SMTP.

Question 4 Sur la machine d'Alice, restaurer la configuration de Mozilla Thunderbird par défaut et utiliser Mozilla Thunderbird pour se connecter au serveur mail installé sur `gafam.com`.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ rm -rf /root/.thunderbird/ /root/.mozilla/
root@alice:/$ thunderbird
```

Lorsque Mozilla Thunderbird se lance, renseigner le nom, l'adresse mail et le mot de passe d'Alice (précédemment choisis sur le serveur) et configurer le client mail comme suit :

```
Your name:      Alice
Email address:  alice@gafam.com
Password:       <previously_chosen_password>

  INCOMMING
Protocol:       IMAP
Server:         gafam.com
Port:           143
SSL:            None
Authentication: Normal password
Username:       alice

  OUTGOING
Protocol:       SMTP
Server:         gafam.com
Port:           25
SSL:            None
Authentication: Normal password
Username:       alice
```

Valider avec le bouton "Done", cocher la case "I understand the risks." et valider de nouveau avec le bouton "Done".

Question 5 Depuis le compte d'Alice, désactiver la copie des message dans le dossier "Sent" et envoyer un message électronique à Bob.

- Dans le menu de Mozilla Thunderbird, choisir "Edit", puis "Account Settings" et enfin "Copies & Folders". Décocher la case "Place a copy in :" puis fermer l'onglet.
- Rédiger un nouveau message et l'envoyer à `bob@gafam.com`. Une fois le message envoyé, fermer Mozilla Thunderbird (important).

Question 6 Dans Wireskark, appliquer le filtre `smtp` et faire une recherche de la chaîne de caractères "from :".

Vous devriez être en mesure de lire le message transmis par Alice. Après cette lecture, relancer une nouvelle capture sur le bridge `br-gafam`.

Question 7 Sur la machine de Bob, restaurer la configuration de Mozilla Thunderbird par défaut et utiliser Mozilla Thunderbird pour se connecter au serveur mail installé sur `gafam.com`.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ rm -rf /root/.thunderbird/ /root/.mozilla/
root@bob:/$ thunderbird
```

Lorsque Mozilla Thunderbird se lance, renseigner le nom, l'adresse mail et le mot de passe de Bob (précédemment choisis sur le serveur) et configurer le client mail comme suit :

```
Your name:       Bob
Email address:   bob@gafam.com
Password:        <previously_chosen_password>

  INCOMMING
Protocol:        IMAP
Server:          gafam.com
Port:            143
SSL:             None
Authentication:  Normal password
Username:        bob

  OUTGOING
Protocol:        SMTP
Server:          gafam.com
Port:            25
SSL:             None
Authentication:  Normal password
Username:        bob
```

Valider avec le bouton "Done", cocher la case "I understand the risks." et valider de nouveau avec le bouton "Done". Depuis le compte de Bob, recevoir les messages en provenance du serveur `gafam.com`. Une fois les messages reçus, répondre à Alice et fermer Mozilla Thunderbird (important).

Question 8 Dans Wireskark, appliquer le filtre `imap` et faire une recherche de la chaîne de caractères "from :".

Vous devriez être en mesure de lire le message reçu par Bob. Après cette lecture, relancer une nouvelle capture sur le bridge `br-gafam`.

Que pouvons-nous conclure de ces communications sans chiffrement avec le serveur ?

7 Configuration du chiffrement pour le serveur mail

Nous utilisons OpenSSL pour le chiffrement de la communication avec le serveur. OpenSSL est installé en même temps que Postfix ou Dovecot, il est donc déjà présent sur le serveur `gafam.com`.
Notons que pour ce TP, nous faisons abstraction de l'autorité de certificat et nous utilisons un certificat auto-signé.

Question 9 Modifier la configuration de Postfix pour rendre possible le chiffrement avec le serveur SMTP et relancer le processus pour appliquer les changements.

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ sudo nano /etc/postfix/main.cf
# replace the line "smtpd_tls_security_level=..." with "smtpd_tls_security_level=may"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart postfix
```

Vérifier qu'un processus écoute bien sur le port 25 :

```
root@gafam:/$ sudo ss -lnpt
```

Question 10 Modifier la configuration de Dovecot pour rendre possible le chiffrement avec le serveur IMAP et relancer le processus pour appliquer les changements.

```
root@gafam:/$ sudo nano /etc/dovecot/conf.d/10-ssl.conf
# replace the line "ssl = ..." with "ssl = yes"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart dovecot
```

Vérifier qu'un processus écoute bien sur le port 143 et le port 993 :

```
root@gafam:/$ sudo ss -lnpt
```

Notons que nous n'utilisons pas le port 993 mais que c'est un témoin que Dovecot peut recevoir une communication utilisant SSL.

8 Communication (avec le serveur) avec chiffrement

De nouveau, nous utilisons Mozilla Thunderbird comme client de messagerie et Wireshark pour analyser le trafic sur notre réseau virtuel.

Question 11 Utiliser Wireshark pour observer le trafic sur le réseau virtuel.

```
debian@myhostname:~$ sudo wireshark
```

Lancer une capture sur le bridge `br-gafam`. Appliquer le filtre `imap||smtp` pour ne voir affichés que les paquets des protocoles IMAP et SMTP.

Question 12 Sur la machine d'Alice, restaurer la configuration de Mozilla Thunderbird par défaut et utiliser Mozilla Thunderbird pour se connecter au serveur mail installé sur `gafam.com`.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ rm -rf /root/.thunderbird/ /root/.mozilla/
root@alice:/$ thunderbird
```

Lorsque Mozilla Thunderbird se lance, renseigner le nom, l'adresse mail et le mot de passe d'Alice (précédemment choisis sur le serveur) et configurer le client mail comme suit :

```
Your name:      Alice
Email address:  alice@gafam.com
Password:       <previously_chosen_password>

  INCOMMING
Protocol:       IMAP
Server:         gafam.com
Port:           143
SSL:            STARTTLS
Authentication: Normal password
Username:       alice

  OUTGOING
Protocol:       SMTP
Server:         gafam.com
Port:           25
SSL:            STARTTLS
Authentication: Normal password
Username:       alice
```

Valider avec le bouton "Done". Mozilla Thunderbird nous indique que le certificat est auto-signé, ce qu'il ne considère pas comme valide. Nous choisissons de faire confiance à ce certificat car nous l'avons nous-même généré. Valider de nouveau avec le bouton "Confirm Security Exception".

Question 13 Depuis le compte d'Alice, désactiver la copie des message dans le dossier "Sent" et envoyer un message électronique à Bob.

- Dans le menu de Mozilla Thunderbird, choisir "Edit", puis "Account Settings" et enfin "Copies & Folders". Décocher la case "Place a copy in :" puis fermer l'onglet.
- Rédiger un nouveau message et l'envoyer à `bob@gafam.com`. Une fois le message envoyé, fermer Mozilla Thunderbird (important).

Question 14 Dans Wireskark, appliquer le filtre `imap||smtp` et faire une recherche de la chaîne de caractères "from :".

Vous ne devriez plus être en mesure de lire le message transmis par Alice. De plus, que remarquez-vous sur le protocole d'envoi de mails avec chiffrement ?

Après cette tentative, relancer une nouvelle capture sur le bridge `br-gafam`.

Question 15 Sur la machine de Bob, restaurer la configuration de Mozilla Thunderbird par défaut et utiliser Mozilla Thunderbird pour se connecter au serveur mail installé sur `gafam.com`.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ rm -rf /root/.thunderbird/ /root/.mozilla/
root@bob:/$ thunderbird
```

Lorsque Mozilla Thunderbird se lance, renseigner le nom, l'adresse mail et le mot de passe de Bob (précédemment choisis sur le serveur) et configurer le client mail comme suit :

```
Your name:      Bob
Email address:  bob@gafam.com
Password:       <previously_chosen_password>

  INCOMMING
Protocol:       IMAP
Server:         gafam.com
Port:           143
SSL:            STARTTLS
Authentication: Normal password
Username:       bob

  OUTGOING
Protocol:       SMTP
Server:         gafam.com
Port:           25
SSL:            STARTTLS
Authentication: Normal password
Username:       bob
```

Valider avec le bouton "Done". Mozilla Thunderbird nous indique que le certificat est auto-signé, valider de nouveau avec le bouton "Confirm Security Exception".
Depuis le compte de Bob, recevoir les messages en provenance du serveur `gafam.com`. Une fois les messages reçus répondre à Alice, fermer Mozilla Thunderbird (important).

Question 16 Dans Wireskark, appliquer le filtre `imap` et faire une recherche de la chaîne de caractères "from :".

Vous ne devriez plus être en mesure de lire le message reçu par Bob. Après cette tentative, fermer Wireshark.

9 Confidentialité des communications sur le réseau

Partons du principe qu'Alice configure son client mail pour utiliser le chiffrement mais que Bob ne le fait pas. L'objectif de cette section est de vérifier la confidentialité des communications d'Alice.

De nouveau, nous utilisons Mozilla Thunderbird comme client de messagerie et Wireshark pour analyser le trafic sur notre réseau virtuel.

Question 17 Utiliser Wireshark pour observer le trafic sur le réseau virtuel.

```
debian@myhostname:~$ sudo wireshark
```

Lancer une capture sur le bridge `br-gafam`. Appliquer le filtre `imap||smtp` pour ne voir affichés que les paquets des protocoles IMAP et SMTP.

Question 18 Sur la machine d'Alice, restaurer la configuration de Mozilla Thunderbird par défaut et utiliser Mozilla Thunderbird pour se connecter au serveur mail installé sur `gafam.com`.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ rm -rf /root/.thunderbird/ /root/.mozilla/
root@alice:/$ thunderbird
```

Lorsque Mozilla Thunderbird se lance, renseigner le nom, l'adresse mail et le mot de passe d'Alice (précédemment choisis sur le serveur) et configurer le client mail comme suit :

```
Your name:       Alice
Email address:   alice@gafam.com
Password:        <previously_chosen_password>

  INCOMMING
Protocol:        IMAP
Server:          gafam.com
Port:            143
SSL:             STARTTLS
Authentication:  Normal password
Username:        alice

  OUTGOING
Protocol:        SMTP
Server:          gafam.com
Port:            25
SSL:             STARTTLS
Authentication:  Normal password
Username:        alice
```

Valider avec le bouton "Done". Mozilla Thunderbird nous indique que le certificat est auto-signé, ce qu'il ne considère pas comme valide. Nous choisissons de faire confiance à ce certificat car nous l'avons nous-même généré. Valider de nouveau avec le bouton "Confirm Security Exception".

Question 19 Depuis le compte d'Alice, désactiver la copie des message dans le dossier "Sent" et envoyer un message électronique à Bob.

- Dans le menu de Mozilla Thunderbird, choisir "Edit", puis "Account Settings" et enfin "Copies & Folders". Décocher la case "Place a copy in :" puis fermer l'onglet.
- Rédiger un nouveau message et l'envoyer à `bob@gafam.com`. Une fois le message envoyé, fermer Mozilla Thunderbird (important).

Question 20 Dans Wireskark, appliquer le filtre `imap||smtp` et faire une recherche de la chaîne de caractères "from :".
Vous ne devriez pas être en mesure de lire le message transmis par Alice. Peut-on conclure sur la confidentialité des communication d'Alice ?

Après cette tentative, relancer une nouvelle capture sur le bridge `br-gafam`.

Question 21 Sur la machine de Bob, restaurer la configuration de Mozilla Thunderbird par défaut et utiliser Mozilla Thunderbird pour se connecter au serveur mail installé sur `gafam.com`.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ rm -rf /root/.thunderbird/ /root/.mozilla/
root@bob:/$ thunderbird
```

Important : lorsque Mozilla Thunderbird se lance, renseigner le nom, l'adresse mail et le mot de passe de Bob (précédemment choisis sur le serveur) et configurer **manuellement** le client mail comme suit :

```
Your name:      Bob
Email address:  bob@gafam.com
Password:       <previously_chosen_password>

  INCOMMING
Protocol:       IMAP
Server:         gafam.com
Port:           143
SSL:            None            (<- important ici)
Authentication: Normal password
Username:       bob

  OUTGOING
Protocol:       SMTP
Server:         gafam.com
Port:           25
SSL:            None            (<- important ici)
Authentication: Normal password
Username:       bob
```

Valider avec le bouton "Done", cocher la case "I understand the risks." et valider de nouveau avec le bouton "Done". Depuis le compte de Bob, recevoir les messages en provenance du serveur `gafam.com`. Une fois les messages reçus, répondre à Alice et fermer Mozilla Thunderbird (important).

Question 22 Dans Wireskark, appliquer le filtre `imap||smtp` et faire une recherche du contenu des messages. Vous devriez être en mesure de lire les messages reçus et envoyés par Bob. Après cette lecture, relancer une nouvelle capture sur le bridge `br-gafam`.

Que pouvons-nous conclure de la confidentialité des communications d'Alice alors que celle-ci a activé le chiffrement sur son client ?

Comment Alice peut-elle s'assurer que les communications des clients avec le serveur ne soient pas en clair : si elle est simple utilisatrice ? si elle est administratrice système ?

10 Forcer le chiffrement pour la communication au serveur mail

Question 23 Modifier la configuration de Postfix pour rendre le chiffrement obligatoire avec le serveur SMTP et relancer le processus pour appliquer les changements.

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ sudo nano /etc/postfix/main.cf
# replace the line "smtpd_tls_security_level=..." with "smtpd_tls_security_level=encrypt"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart postfix
```

Vérifier qu'un processus écoute bien sur le port 25 :

```
root@gafam:/$ sudo ss -lnpt
```

Question 24 Modifier la configuration de Dovecot pour rendre le chiffrement obligatoire avec le serveur IMAP et relancer le processus pour appliquer les changements.

```
root@gafam:/$ sudo nano /etc/dovecot/conf.d/10-ssl.conf
# replace the line "ssl = ..." with "ssl = required"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart dovecot
```

Vérifier qu'un processus écoute bien sur le port 143 et le port 993 :

```
root@gafam:/$ sudo ss -lnpt
```

Question 25 Rejouer la procédure décrite dans la section 9. Que se passe-t-il lorsque Bob tente de configurer son client mail pour se connecter au serveur sans chiffrement ?

11 Sécurité vis-à-vis de l'hébergeur

L'entreprise GAFAM fournit désormais un service de messagerie à Alice et à Bob. La communication avec le serveur est obligatoirement chiffrée : nous avons donc obligé les utilisateurs à sécuriser leurs communications sur le réseau public. Ici, nous nous intéressons à la sécurité des communications entre Alice et Bob alors que leurs messages transitent par le serveur de l'entreprise GAFAM.

Nous partons du principe que l'hébergeur du service de messagerie n'est plus de confiance. Cela fait évoluer notre modèle d'attaquant. Notre nouvel attaquant est un membre de l'entreprise GAFAM qui a des accès légitimes au serveur.

Question 26 Prendre le contrôle du serveur mail et tenter de lire le contenu des messages de Bob.

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ cat /var/mail/bob
```

Vous devriez voir que les mails sont stockés en clair sur le serveur.

Que pouvons-nous conclure, vis-à-vis de la **confidentialité** des messages, de la sécurité que nous avons réalisée dans les sections précédentes ?

Question 27 Prendre le contrôle du serveur mail et tenter de modifier le contenu du dernier message de Bob.

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ nano /var/mail/bob
```

Sur la machine de Bob, restaurer la configuration de Mozilla Thunderbird par défaut et utiliser Mozilla Thunderbird pour lire le dernier message.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ rm -rf /root/.thunderbird/ /root/.mozilla/
root@bob:/$ thunderbird
```

Vous devriez voir que le message a bien été modifié.

Que pouvons-nous conclure, vis-à-vis de l'**intégrité** des messages, de la sécurité que nous avons réalisée dans les sections précédentes ?

Question 28 Prendre le contrôle du serveur mail et tenter d'ajouter un nouveau message à Bob. Copier-coller le dernier message et modifier :

- le titre
- le contenu
- l'adresse de l'expéditeur
- les différentes dates et heures (émission, transfert, réception)

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ nano /var/mail/bob
```

Sur la machine de Bob, lire le dernier message.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ thunderbird
```

Vous devriez voir que le message a bien été créé.

Que pouvons-nous conclure, vis-à-vis de l'**authenticité** des messages, de la sécurité que nous avons réalisée dans les sections précédentes ?

12 Envoi de messages frauduleux

Dans cette section, nous incarnons Eve, notre utilisateur malveillant qui utilise les protocoles de messagerie pour usurper l'identité d'un utilisateur légitime. Eve possède son propre serveur qui héberge le site `eve.com`.

Question 29 Installer Postfix sur la machine qui héberge le site `eve.com`.

```
debian@myhostname:~$ sudo lxc-attach eve
root@eve:/$ sudo apt install postfix
# chose "Internet Site" and select "eve.com" as domain.
```

Question 30 Par défaut, Postfix utilise la résolution DNS pour trouver l'adresse IP du destinataire. Dans notre environnement virtuel, nous n'avons pas de résolveur DNS, les noms de domaines sont définis dans les fichiers `/etc/hosts` de chaque conteneur.

Désactiver la résolution DNS dans la configuration de Postfix et relancer le processus pour appliquer les changements.

```
root@eve:/$ sudo nano /etc/postfix/main.cf
# add the line "disable_dns_lookups = yes"
# save with Ctrl+O and quit with Ctrl+X
root@eve:/$ sudo systemctl restart postfix
```

Vérifier qu'un processus écoute bien sur le port 25 :

```
root@eve:/$ sudo ss -lnpt
```

Question 31 Nous pouvons utiliser `telnet` pour communiquer avec Postfix sur le port 25 et lui transmettre les commandes permettant l'envoi de notre message. Commencer par rédiger un script qui contient le message frauduleux avec un éditeur de texte.

```
root@eve:/$ nano /tmp/mail
# write the script. Once done, it must look like this:
root@eve:/$ cat /tmp/mail
MAIL FROM: bob@eve.com
RCPT TO: alice@gafam.com
DATA
Subject: An important message from Bob
Hi Alice. This is me, Bob!
Can you send me money to this account, please?
0123.4567.8910
.

QUIT
root@eve:/$
```

Une fois le script terminé, le transmettre à telnet pour une communication sur le port 25.

```
root@eve:/$ cat /tmp/mail | telnet localhost 25
```

Question 32 Ouvrir Mozilla Thunderbird sur la machine d'Alice et vérifier que celle-ci a bien reçu le message frauduleux. Comment Alice peut-elle s'assurer que ce n'est pas son collègue Bob qui a envoyé ce message ?

Question 33 Se baser sur le nom de l'expéditeur n'est pas suffisant pour s'assurer de l'authenticité du message. Eve peut très bien le modifier lors de son envoi. Modifier le script qui contient le message frauduleux avec un éditeur de texte et remplacer le nom de l'expéditeur.

```
root@eve:/$ nano /tmp/mail
# modify the script. Once done, it must look like this:
root@eve:/$ cat /tmp/mail
MAIL FROM: bob@gafam.com
RCPT TO: alice@gafam.com
DATA
Subject: An important message from Bob
Hi Alice. This is me, Bob!
Can you send me money to this account, please?
0123.4567.8910
.

QUIT
root@eve:/$
```

Une fois le script terminé, le transmettre à telnet pour une communication sur le port 25.

```
root@eve:/$ cat /tmp/mail | telnet localhost 25
```

Question 34 Ouvrir Mozilla Thunderbird sur la machine d'Alice et vérifier que celle-ci a bien reçu le nouveau message frauduleux. Comment Alice peut-elle s'assurer que ce n'est pas son collègue Bob qui a envoyé ce message ?
Indice : Mozilla Thunderbird permet d'afficher le code source des messages.

13 Usurpation d'adresse IP et de nom d'hôte

L'usurpation d'adresse IP (en anglais : IP spoofing ou IP address spoofing) est une technique de piratage informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.

Source : `https://fr.wikipedia.org/wiki/Usurpation_d%27adresse_IP`

Eve a un complice qui a accès à l'infrastructure du réseau et peut modifier les adresses IP des paquets qui transitent dessus. Eve peut aussi modifier la configuration de son serveur Postfix pour usurper le nom d'une autre machine que celui du serveur qui procède à l'envoi.

Si Bob possède son propre serveur mail `bob.com`, Eve peut se faire passer pour un utilisateur légitime en usurpant l'adresse IP et le nom de domaine de Bob.

Question 35 Sur le serveur d'Eve, modifier la configuration de Postfix pour remplacer le nom de machine de l'émetteur par celui de la machine de Bob.

```
debian@myhostname:~$ sudo lxc-attach eve
root@eve:/$ sudo nano /etc/postfix/main.cf
# replace the line "myhostname = ..." with "myhostname = bob"
# save with Ctrl+O and quit with Ctrl+X
root@eve:/$ sudo systemctl restart postfix
```

Vérifier qu'un processus écoute bien sur le port 25 :

```
root@eve:/$ sudo ss -lnpt
```

Question 36 Sur le routeur, appliquer un traitement sur les paquets IP (durant l'attaque d'Eve) pour modifier les adresses IP suivantes :

- source, en provenance du serveur d'Eve lorsqu'elles sont à destination de `gafam.com`, pour les remplacer par celle de Bob ;
- à destination du serveur de Bob lorsqu'elles sont en provenance de `gafam.com`, pour les remplacer par celle d'Eve.

```
debian@myhostname:~$ sudo lxc-attach router
root@router:/$ sudo ip6tables -t nat -A POSTROUTING \
                --source 2000:1000:4::2/112 --destination 2000:1000:3::2/128 \
                -j SNAT --to-source 2000:1000:2::2
root@router:/$ sudo ip6tables -t nat -A PREROUTING \
                --source 2000:1000:3::2/112 --destination 2000:1000:2::2/128 \
                -j DNAT --to-destination 2000:1000:4::2
```

Question 37 Sur le serveur d'Eve, modifier le script qui contient le message frauduleux avec un éditeur de texte et remplacer le nom de l'expéditeur.

```
debian@myhostname:~$ sudo lxc-attach eve
root@eve:/$ nano /tmp/mail
# modify the script. Once done, it must look like this:
root@eve:/$ cat /tmp/mail
MAIL FROM: bob@bob.com
RCPT TO: alice@gafam.com
DATA
Subject: An important message from Bob
Hi Alice. This is me, Bob!
I installed my own SMTP server.
Can you send me money to this account, please?
0123.4567.8910
.

QUIT
root@eve:/$
```

Une fois le script terminé, le transmettre à telnet pour une communication sur le port 25.

```
root@eve:/$ cat /tmp/mail | telnet localhost 25
```

Question 38 Une fois l'attaque terminée, sur le routeur, supprimer le traitement sur les paquets IP pour passer inaperçu.

```
debian@myhostname:~$ sudo lxc-attach router
root@router:/$ sudo ip6tables -t nat -D POSTROUTING \
                --source 2000:1000:4::2/112 --destination 2000:1000:3::2/128 \
                -j SNAT --to-source 2000:1000:2::2
root@router:/$ sudo ip6tables -t nat -D PREROUTING \
                --source 2000:1000:3::2/112 --destination 2000:1000:2::2/128 \
                -j DNAT --to-destination 2000:1000:4::2
```

Question 39 Ouvrir Mozilla Thunderbird sur la machine d'Alice et vérifier que celle-ci a bien reçu le message frauduleux. Comment Alice peut-elle s'assurer que ce n'est pas son collègue Bob qui a envoyé ce message ?

14 Signature numérique

La signature numérique est un mécanisme permettant de garantir la non-répudiation d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.

Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères. Elle ne doit pas être confondue avec la signature électronique manuscrite.

Source : `https://fr.wikipedia.org/wiki/Signature_num%C3%A9rique`

L'objectif de cette section n'est pas de détailler le fonctionnement des primitives cryptographiques de signature mais de les utiliser à des fin d'authentification.

14.1 Fonctionnement de PGP

Avec PGP, il est possible de vérifier si un message provient bien de l'origine (via les signatures cryptographiques), ainsi que de chiffrer des messages afin qu'un seul destinataire puisse les lire. En bref, chaque utilisateur crée une paire de clés de chiffrement asymétriques (une publique, l'autre privée), et distribue la clé publique. **Les signatures effectuées avec la clé privée peuvent être vérifiées en utilisant la clé publique correspondante** et **les messages chiffrés utilisant la clé publique sont déchiffrables en utilisant la clé privée correspondante**. Ce fonctionnement a été initialement décrit dans le document RFC 1991.

Authentification : l'expéditeur crée un condensat de son message (avec par exemple SHA-1), chiffre ce condensat avec sa clé privée et l'ajoute en début de message. Le destinataire déchiffre l'ajout en début de message avec la clé publique de l'émetteur et en extrait le condensat. Il calcule ensuite lui-même un condensat du message en utilisant la même fonction de condensat et le compare à celui qu'il a déchiffré ; même résultat → expéditeur authentifié et message intègre.

Source : `https://fr.wikipedia.org/wiki/Pretty_Good_Privacy`

14.2 OpenPGP dans Mozilla Thunderbird

OpenPGP est activé par défaut dans Mozilla Thunderbird depuis la version 78.2.1.
Source : `https://support.mozilla.org/fr/kb/openpgp-thunderbird-guide-faq`

Question 40 Ouvrir Mozilla Thunderbird sur la machine d'Alice et générer une paire de clés.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ thunderbird
```

— Dans le menu de Mozilla Thunderbird, choisir "Edit", puis "Account Settings" et enfin "End-to-End Encryption".
— Dans la section *OpenPGP*, cliquer sur le bouton "Add Key...".
  — Si vous disposez déjà d'une paire de clés personnelles OpenPGP d'un autre logiciel, choisissez "Import an existing PGP key" ;
  — Si vous n'avez pas encore de clé, choisissez "Create a New OpenPGP key".
— Après son importation ou sa création, tout en restant dans les paramètres des comptes, sélectionnez la clé que vous voulez utiliser activement avec votre compte de messagerie.

Question 41 Depuis Mozilla Thunderbird sur la machine d'Alice, envoyer un courrier électronique à Bob en signant le message et en transmettant la clé publique d'Alice.
— Lors de la rédaction du message dans Mozilla Thunderbird, dans le menu, choisir "Options", puis cocher les cases "Digitally Sign This Message" et "Attach My Public Key".
— Rédiger un nouveau message et l'envoyer à `bob@gafam.com`. Une fois le message envoyé, fermer Mozilla Thunderbird (important).

Question 42 Sur la machine de Bob, utiliser Mozilla Thunderbird pour importer la clé publique d'Alice.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ thunderbird
```

Réceptionner le message signé d'Alice et importer sa clé publique :
— Lors de la lecture du message dans Mozilla Thunderbird, cliquer sur le bouton "OpenPGP" puis sur le bouton "Import".

Mozilla Thunderbird demande si cette clé publique doit être acceptée : en effet, Bob n'a aucun moyen de vérifier que le message provient bien d'Alice. Nous admettons que Alice et Bob sont physiquement côte à côte lors de l'envoi de la clé publique et nous acceptons la clé : cocher le bouton "Accepted (unverified)" et cliquer sur OK.

Question 43 Sur la machine de Bob, utiliser Mozilla Thunderbird pour vérifier la signature d'Alice.
Fermer et ré-ouvrir le message si besoin, puis :
— Lors de la lecture du message dans Mozilla Thunderbird, cliquer sur le bouton "OpenPGP" puis vérifier que Mozilla Thunderbird affiche bien "Good Digital Signature".

Question 44 Mozilla Thunderbird nous informe également que nous avons bien accepté la clé publique mais que rien n'indique qu'elle appartient bien à son propriétaire. Afin de terminer la procédure, nous pouvons dire à Mozilla Thunderbird que la clé importée est de confiance. Pour cela, Bob doit vérifier sur la machine d'Alice que l'empreinte de la clé est la même que celle qu'il a reçue. Si elle est identique, Bob peut alors valider :
— Lors de la lecture du message dans Mozilla Thunderbird, cliquer sur le bouton "OpenPGP" puis sur le bouton "View signer key".
— Choisir l'option "Yes, I've verified in person this key has the correct fingerprint".

Question 45 Répéter la procédure complète dans l'autre sens pour que Bob aussi puisse signer ses messages et qu'Alice puisse les vérifier :

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ thunderbird
```

— Générer une paire de clés pour Bob.
— Envoyer la clé publique de Bob à Alice en signant le message.

Puis, sur la machine d'Alice :

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ thunderbird
```

— Importer la clé publique de Bob.
— Vérifier la signature du message.
— Informer Mozilla Thunderbird que la clé est de confiance.

14.3 Tentative de forge de signature

Alice et Bob peuvent désormais authentifier leurs messages grâce à la signature numérique. Si un attaquant voulait usurper leur identité, il devrait forger une signature correcte ou obtenir leur clé privée.

Ici, nous illustrons simplement le fait que la signature est bien le résultat d'un chiffrement sur le condensat du message et que nous ne pouvons pas ré-utiliser une signature pour un message différent. Nous admettons qu'Eve ait pu obtenir un message signé de Bob.

Question 46 Sur le serveur d'Eve, modifier le script qui contient le message frauduleux avec un éditeur de texte pour former un message signé. La signature est à copier/coller depuis un message authentique, signé, de Bob.

```
debian@myhostname:~$ sudo lxc-attach eve
root@eve:/$ nano /tmp/mail
# modify the script. Once done, it must look like this:
root@eve:/$ cat /tmp/mail
MAIL FROM: bob@bob.com
RCPT TO: alice@gafam.com
DATA
Subject: An important message from Bob
Content-Type: multipart/signed; micalg=pgp-sha256;
 protocol="application/pgp-signature";
 boundary="BOUNDARY"

--BOUNDARY

Hi Alice. This is me, Bob!
I installed my own SMTP server.
Can you send me money to this account, please?
0123.4567.8910

--BOUNDARY
Content-Type: application/pgp-signature; name="OpenPGP_signature.asc"
Content-Description: OpenPGP digital signature
Content-Disposition: attachment; filename="OpenPGP_signature"

-----BEGIN PGP SIGNATURE-----

wsD5BAABCAAjFiEEVZvPQE505cvOn93EV/gK58ipPMUFAmGJL8wFAwAAAAAACgkQV/gK58ipPMWL
ogwAu7WuKfnOrgRtiDNPezCBqhfvlEyjlZviTGaNQwEkbGevugHtBZBxBXYpr6B3lBmF2H5DyoQk
F28sqeEgo0eanTMgEHJ0plL/fDqlZe7F7JE8zXQ1e/Z68L8/rIxWUdUQlvkbjBbB+GNwM1oI3Cvg
arby9WJOwXrjxNR2M/yzhMmESQkLHx14nLO6/xlUPXBjPYLP2W7IZGEgabUGo3/I7o7ZBHfR5W8W
GFJeG3LlBgclLhn4QAPTUlcm0NZ12NMTKk/Wva739oUSsZoQ1IsYvo7NXtPayJ5Yj0RHCC1+++pR
cyQ5JqqBWksnWe4654vgfceAGLREpLtKij2jo7KT6l+019NOLn9UJ2nHG9KPyHV0FDUKv5Gx7YU/
TY8UYSMx3cpVCEnOOcbaOErAEQLr0SOETIkpLtorpPb9NufBG7CdRSmvKa3LibVl0bpyC1N3J90Y
MksaIJS8e3CO00lanGKlm/ZQmoOaLsygLCHH4OiMDiJPwwkyQ6Yto7EB3D4j
=kL6E
-----END PGP SIGNATURE-----

--BOUNDARY--
.

QUIT
root@eve:/$
```

Une fois le script terminé, le transmettre à telnet pour une communication sur le port 25.

```
root@eve:/$ cat /tmp/mail | telnet localhost 25
```

Question 47 Sur la machine d'Alice, utiliser Mozilla Thunderbird pour vérifier la signature de Bob :
— Lors de la lecture du message dans Mozilla Thunderbird, cliquer sur le bouton "OpenPGP" puis vérifier.
Que nous dit OpenPGP ?

15 Chiffrement de bout en bout

Le chiffrement de bout en bout (en anglais, End-to-end encryption ou E2EE) est un système de communication où seules les personnes qui communiquent peuvent lire les messages échangés. En principe, il empêche l'écoute électronique, y compris par les fournisseurs de télécommunications, par les fournisseurs d'accès Internet et même par le fournisseur du service de communication.

Source : `https://fr.wikipedia.org/wiki/Chiffrement_de_bout_en_bout`

L'objectif de cette section n'est pas de détailler le fonctionnement des primitives cryptographiques de chiffrement mais de les utiliser à des fin de confidentialité.

15.1 Fonctionnement de PGP

Confidentialité : la première étape est la génération d'une clé secrète, nommée clé de session, valable pour un seul fichier ou un seul message. **Le message ou le fichier est chiffré au moyen de cette clé de session avec un algorithme de cryptographie symétrique**. Puis **cette clé secrète est chiffrée au moyen de la clé publique du destinataire et ajoutée au début du message ou du fichier**. **Le destinataire du message déchiffre l'en-tête du message avec sa clé privée et en extrait la clé secrète qui lui permet de déchiffrer le message**. Pour que la sécurité de l'échange soit plus sûre il ne faudrait pas utiliser le chiffrement sans authentification. PGP générant des clés très souvent (à chaque fichier ou message), le générateur aléatoire associé à PGP doit être particulièrement efficace afin de ne pas générer des séquences de clés prévisibles.

Source : `https://fr.wikipedia.org/wiki/Pretty_Good_Privacy`

15.2 OpenPGP dans Mozilla Thunderbird

Nous avons généré une paire de clés publique/privée pour Alice et pour Bob dans la section 14. Nous avons également vu dans la section 11 que les communications d'Alice et de Bob sont stockées en clair sur le serveur de l'entreprise GAFAM.

Ici, nous utilisons les primitives cryptographiques de chiffrement pour garantir la confidentialité des communications de bout en bout, également vis-à-vis de l'entreprise GAFAM.

Question 48 Pour vérifier que les messages que nous transmettons sont chiffrés, commencer par supprimer tous les messages reçus sur le compte de Bob. Attention à ne pas supprimer les dossiers suivants :
— `/root/.thunderbird/`
— `/root/.mozilla/`
sinon on supprime également les clés PGP générées et échangées.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ thunderbird
```

Supprimer tous les messages reçus dans Mozilla Thunderbird. Une fois les messages supprimés, fermer Mozilla Thunderbird (important).

Question 49 Vérifier que tous les messages ont bien été supprimés sur le serveur :

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ cat /var/mail/bob
```

Vous ne devriez voir qu'un seul message envoyé par `MAILER_DAEMON`. Ce message est un fichier de configuration créé automatiquement par Dovecot. Le corps du message détaille son utilité.

Question 50 Ouvrir Mozilla Thunderbird sur la machine d'Alice et envoyer un message chiffré à Bob.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ thunderbird
```

— Lors de la rédaction du message dans Mozilla Thunderbird, dans le menu, choisir "Options", puis cocher l'option "Require Encryption".
— Rédiger un nouveau message et l'envoyer à `bob@gafam.com`. Une fois le message envoyé, fermer Mozilla Thunderbird (important).

Question 51 Sur la machine de Bob, utiliser Mozilla Thunderbird pour déchiffrer le message transmis par Alice.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach bob
root@bob:/$ thunderbird
```

Réceptionner le message chiffré d'Alice et vérifier qu'il peut être lu.

Question 52 Vérifier que le message est bien stocké chiffré sur le serveur :

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ cat /var/mail/bob
```

Vous devriez voir deux messages :
— un envoyé par `MAILER_DAEMON`
— un envoyé par `alice@gafam.com`, dont le corps est chiffré

15.3 Confidentialité sur le réseau

Le chiffrement de bout en bout garantit la confidentialité des communications entre pairs : cela inclut les messages stockés sur le serveur du fournisseur de service mais également sur le réseau public. Pour s'en convaincre, nous pouvons temporairement désactiver le chiffrement pour la communication avec le serveur mail et tenter un envoi de message chiffré avec le protocole OpenPGP seul.

Note : deux couches de chiffrement valent mieux qu'une. Il est conseillé de toujours activer le chiffrement de la communication avec le serveur, même en cas de chiffrement de bout en bout.

Question 53 Sur la machine qui héberge le site `gafam.com`, désactiver le chiffrement dans la configuration de Postfix et relancer le processus pour appliquer les changements.

```
debian@myhostname:~$ sudo lxc-attach gafam
root@gafam:/$ sudo nano /etc/postfix/main.cf
# replace the line "smtpd_tls_security_level=..." with "smtpd_tls_security_level=none"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart postfix
```

Vérifier qu'un processus écoute bien sur le port 25 :

```
root@gafam:/$ sudo ss -lnpt
```

Question 54 Toujours sur la machine qui héberge le site `gafam.com`, désactiver le chiffrement dans la configuration de Dovecot et relancer le processus pour appliquer les changements.

```
root@gafam:/$ sudo nano /etc/dovecot/conf.d/10-ssl.conf
# replace the line "ssl = ..." with "ssl = no"
# save with Ctrl+O and quit with Ctrl+X
root@gafam:/$ sudo systemctl restart dovecot
```

Vérifier qu'un processus écoute bien sur le port 143 mais pas sur le port 993 :

```
root@gafam:/$ sudo ss -lnpt
```

Question 55 Utiliser Wireshark pour observer le trafic sur le réseau virtuel.

```
debian@myhostname:~$ sudo wireshark
```

Lancer une capture sur le bridge `br-gafam`. Appliquer le filtre `imap||smtp` pour ne voir affichés que les paquets des protocoles IMAP et SMTP.

Question 56 Ouvrir Mozilla Thunderbird sur la machine d'Alice et désactiver le chiffrement de la communication avec le serveur.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ thunderbird
```

— Dans le menu de Mozilla Thunderbird, choisir "Edit", puis "Account Settings" et enfin "Server Settings". Dans la section "Security Settings", choisir "None" pour "Connection security".
— Choisir ensuite "Outgoing Server (SMTP)" et cliquer sur le bouton "Edit...". Dans la section "Security and Authentication", choisir "None" pour "Connection security" puis cliquer sur "OK".
— Fermer l'onglet.

Question 57 Ouvrir Mozilla Thunderbird sur la machine d'Alice et envoyer un message chiffré à Bob.

```
debian@myhostname:~$ sudo xhost +
debian@myhostname:~$ sudo lxc-attach alice
root@alice:/$ thunderbird
```

— Lors de la rédaction du message dans Mozilla Thunderbird, dans le menu, choisir "Options", puis cocher l'option "Require Encryption".
— Rédiger un nouveau message et l'envoyer à `bob@gafam.com`. Une fois le message envoyé, fermer Mozilla Thunderbird (important).

Question 58 Dans Wireskark, appliquer le filtre `smtp` et faire une recherche de la chaîne de caractères "from :".

Vous devriez être en mesure de voir le message transmis par Alice, mais le corps du message est chiffré, de la même manière que sur le serveur du fournisseur de service.
Qu'en est-il des métadonnées (expéditeur, destinataire, sujet, date...) ?

Question 59 Conclure sur les limitations du chiffrement de bout en bout.