TP4 : Protocoles mail

**2. Contenu d’un mail**

*1. Quels champs permettent de connaître l’expéditeur/le destinataire ?*

Le champ “From” permet de connaître l’adresse mail de l’expéditeur.

Le champ “To” permet de connaître la liste des eMails de l’ensemble des destinataires.

*2. À quoi sert le champ Return-Path ?*

Le champ Return-Path permet de déterminer comment seront traitées les erreurs liées à l’envoi d’un message.  Cet en-tête, également appelé "adresse de rebond" ou "chemin inverse", est une adresse SMTP distincte de l'adresse d'envoi initiale, utilisée spécifiquement pour collecter et traiter les messages non remis(ex:  lorsqu’une adresse email d’un contact incorrect).

*3. Expliquer le contenu des champs Received.*

Ce champ indique les différents serveurs de messagerie par lesquels le mail à transité. Chaque point de passage donne les informations suivantes :  date, l’heure, de qui ils l’ont reçu (ip ou nom de serveur) et à qui ils l’ont renvoyé.

*4. Comment peut-on retrouver le temps d’acheminement du mail ?*

Si l’on lit les détails du mail, nous pouvons retrouver l’heure à laquelle le message est envoyé via le MUA et l’heure à laquelle il arrive à l'expéditeur. Ainsi il suffit de comparer l’heure à laquelle les serveurs ont traité les mails afin de connaître le temps d’acheminement du mail.

Par exemple, lorsque je lis un mail reçu par Ebay en texte brut, je retrouve dans les premières lignes le serveur sur lequel je reçois le mail (localhost), le return-path et l’heure exacte à laquelle j’ai reçu le mail.

Tue, 28 Feb 2023 09:39:01

La dernière date que l’on peut trouver est :

Date: Tue, 28 Feb 2023 02:38:59 -0700

From: eBay <[ebay@ebay.fr](mailto:ebay@ebay.fr)>

Donc le temps d’acheminement est de 7h dans ce cas-là. Il est généralement de quelques secondes voire moins lorsque l’on partage un message simple avec un contact.

*5. Comment peut-on (espérer) détecter une telle usurpation ?*

Ici aussi, en s’intéressant aux sources du mail (en regardant le code brut), on peut retrouver des informations de la réelle adresse de l’expéditeur et vérifier qu’elle correspond à celle d'une source légitime. Nous pouvons également vérifier l'en-tête du message pour voir si les informations d'adresse sont cohérentes avec celles de l'expéditeur présumé. Il existe également des nouvelles technologies de vérification d’authenticité des e-mails ainsi que des logiciels anti-spam détectant des éléments suspects automatiquement et ainsi contrer automatiquement une telle usurpation.

**3. Acheminement**

**3.2 Votre premier mail (au terminal)**

• Sur la même machine :

On envoie :

Une image contenant texte

Description générée automatiquement

Le mail reçu est :

Une image contenant texte

Description générée automatiquement

• Sur l’adresse mail étudiante

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

• En changeant l’IP: Une image contenant texte

Description générée automatiquement

On ne peut continuer l’envoie du mail, une authentification est demandée.

**3.4 Failles**

*Expliquer comment une personne mal intentionnée (ayant accès au réseau) pourrait :*

*-Lire les mails reçus par un utilisateur donné*

On pourrait utiliser un logiciel afin d’intercepter les données de l'utilisateur. Cela est d'autant plus facile que les données POP ne sont pas cryptées.

*-Envoyer des mails en se faisant passer pour un autre utilisateur*

En usurpant l’identité d’une personne, on peut créer un domaine sur hmail ayant un nom similaire à un célèbre domaine par exemple etu-univ.fr. On peut ensuite y associer des adresses mails. Dans le cas des adresses universitaires, il suffit de créer une adresse mail avec le nom et le prénom d’un étudiant pour se faire passer pour lui. On pourra ensuite piéger les autres utilisateurs.

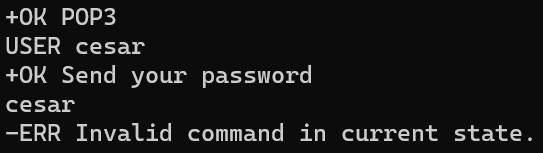
**4. Post Office Protocol**

**4.1 Fonctionnement**

*1. Quels sont les deux types de réponses du serveur ? Quelle est leur syntaxe ?*

Le serveur renvoie deux types de réponse :

* Les réponses positives lorsque la commande est exécutée avec succès. Elles sont écrites de la façon suivante :
  + +OK
* Les réponses négatives lorsque la commande ne peut pas être exécutée avec succès. Elles sont écrite de la façon suivante :
  + -Err <raison>



*2. Expliquer ce que renvoient les commandes STAT, LIST, et LIST <entier>*

La commande STAT renvoie un descriptif de l'état de la boîte aux lettres, c’est-à-dire le nombre total de messages dans la boîte aux lettres et la taille totale en octets de ces messages. Le serveur POP envoie une réponse au client dans le format suivant : +OK <num\_messages> <taille\_boîte\_en\_octets>.

Une image contenant texte

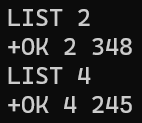
Description générée automatiquement

La commande LIST permet d'afficher la liste des messages présents dans la boîte aux lettres, avec leur numéro d'ordre et leur taille en octets. Le serveur POP envoie une réponse au client dans le format suivant :  
+OK <num\_messages> messages : <num\_message\_1> <taille\_message\_1> <num\_message\_2> <taille\_message\_2> ... <num\_message\_n> <taille\_message\_n>

Une image contenant texte

Description générée automatiquement

La commande LIST <entier> permet d'afficher les informations sur un message particulier, identifié par son numéro d'ordre dans la boîte aux lettres. Le serveur POP envoie une réponse au client dans le format suivant : +OK <num\_message> <taille\_message>.



*3. La commande RETR prend un entier comme argument, tandis que TOP en prend deux. Tester et expliquer leur fonctionnement. Quelle utilité a la commande TOP 0 ?*

La commande RETR permet de récupérer tous les détails d’un courriel y compris son corps. L’entier entré correspond à l’id du message à traiter.

Une image contenant texte

Description générée automatiquement

La commande TOP permet de récupérer l'en-tête et un nombre n de ligne provenant du corps du message i. La variable i correspond à l’id du message tandis que n correspond aux nombres de lignes du corps du message à récupérer.

Une image contenant texte

Description générée automatiquement

Si on écrit Top id 0, avec id un id de mail. On récupère l'entête du mail seulement.

*4. Les commandes DELE et RSET gèrent la suppression de messages. Authentifiez-vous, puis lancez (dans l’ordre) les commandes DELE 1, LIST, RSET, LIST. En déduire à quel moment le serveur supprime effectivement le message*

Une image contenant texte

Description générée automatiquement

Comme on peut le voir, c’est la commande DELE 1 qui a supprimé le premier message, la commande LIST comme on l’a vu précédemment affiche <num\_message\_i> <taille\_message\_i> et RSET réinitialise l'état de la session de la communication avec le serveur et permet donc de récupérer l’email supprimé avec DELE. Ainsi, on peut en déduire que le message est réellement supprimé à la fermeture de la connexion avec le serveur (commande “QUIT”).

**4.2 Scriptage**

**Une image contenant texte

Description générée automatiquement**

*5. La commande NOOP ne fait rien. À quoi peut-elle donc servir ?*  
 La commande NOOP est utilisée pour maintenir une connexion active entre le client de messagerie et le serveur POP, sans effectuer d'opération spécifique de récupération ou de suppression de messages. Elle est généralement utilisée pour empêcher le serveur POP de fermer la connexion après une période d'inactivité, ce qui peut se produire si aucun message n'est récupéré ou supprimé pendant une période prolongée.

*6. Le protocole POP est-il sécurisé ?*

POP est considéré comme un protocole non sécurisé car les données transitent en clair sur le réseau, ce qui signifie que les informations telles que les noms d'utilisateur, les mots de passe et les messages eux-mêmes peuvent être facilement interceptées par des tiers malveillants. Il existe cependant une version plus récente de POP, POP3S, qui utilise une connexion sécurisée SSL/TLS pour chiffrer les données transitant sur le réseau.

*7. Est-il possible d’utiliser le protocole POP pour récupérer ses mails sur plusieurs machines (ordinateur + smartphone, par exemple) ? Si oui, est-ce une bonne idée ?*

Il est possible d'utiliser le protocole POP pour récupérer ses e-mails sur plusieurs machines. Mais cela peut poser des problèmes de synchronisation et de gestion des messages car en utilisant POP pour récupérer les e-mails, les messages sont téléchargés sur l'appareil qui effectue la connexion. De plus, en utilisant POP sur plusieurs appareils, il est possible que certains messages soient manqués ou perdus. Si un appareil se connecte et télécharge tous les messages du serveur, les autres appareils ne pourront pas accéder à ces messages à moins qu'ils ne soient téléchargés à nouveau.

**5. Internet Mail Access Protocol**

**5.2 Manipulations**

*8. Que renvoie la commande SELECT INBOX*

La commande nous renvoie des informations sur la boîte de réception tel que :

* Le nombre total de messages dans la boîte de réception
* Le nombre total d'octets utilisés pour stocker les messages dans la boîte de réception
* Le numéro de séquence du premier message dans la boîte de réception
* Le numéro de séquence du dernier message dans la boîte de réception

Une image contenant texte

Description générée automatiquement

*9. Déconnectez et reconnectez-vous, puis réutilisez SELECT INBOX. Le résultat a-t-il changé ? Pourquoi ?*

Le nombre de mails RECENT change pour passer de 10 à 0 car lors de la première connexion, les messages récents ont étés vues, donc ils ne sont plus relevés ici.

Une image contenant texte

Description générée automatiquement

*10. IMAP manipule des drapeaux (par exemple : Seen, Answered, Deleted, Recent). On peut visualiser les drapeaux des mails du dossier courant avec FETCH 1:\* (FLAGS). Expliquez le fonctionnement des drapeaux Seen et Recent.*

Le drapeau "Seen" est utilisé pour indiquer qu'un message a été vu ou lu par le client IMAP. Si on a "Seen", cela signifie que le client a ouvert et visualisé le contenu du message.

Le drapeau "Recent" est utilisé pour indiquer qu'un message est nouveau et qu'il n'a pas encore été vu par le client IMAP. Lorsqu'un message est reçu, iil est automatiquement marqué comme "Recent". Si le client ouvre le message, le drapeau "Recent" est supprimé et remplacé par le drapeau "Seen".

*11. À quoi sert le 1:\* dans la commande précédente ? Comment récupérer le contenu d’un mail donné (au lieu de juste ses drapeaux) ?*

L'argument "1:" dans la commande précédente signifie que l’on va récupérer les informations de tous les e-mails dans la boîte aux lettres, à partir du premier (1) jusqu'au dernier (indiqué par \*).

Pour récupérer le contenu d'un mail spécifique, on utilise la commande FETCH en spécifiant le numéro de séquence unique du courriel en question.

*12. Pour supprimer un mail, il faut lui donner le drapeau Deleted (STORE), puis se déconnecter (LOGOUT) ou fermer le dossier (CLOSE). Quelle suite de commandes permet de supprimer le premier mail d’Astérix ?*

Il existe deux suites de commande permettant d’effacer premier mail d'Astérix :

* Premièrement, il faut attribuer le flag DELETED au mail que l’on souhaite supprimer. Pour cela, on utilise la fonction STORE pour enregistrer la modification. On finit par se déconnecter avec CLOSE afin que les changements soient effectifs.
* La deuxième méthode consiste à utiliser la fonction EXPUNGE, même façon de fonctionner mais la déconnexion n’est pas nécessaire ici.

Une image contenant texte

Description générée automatiquement Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement Une image contenant texte

Description générée automatiquement