Ensimag 1ère année

TP n°3 — Messagerie : protocoles IMAP, SMTP, et authenticité

Il est recommandé de prendre des notes.
Une question sur l'effet ou l'utilisation d'une commande ?
man nom_de_la_commande !

Ce TP illustre quelques protocoles et applications relatifs à la messagerie présentés en cours.

On commence par étudier l'un des protocoles d'accès distant aux boites aux lettres : IMAP. On étudiera ensuite SMTP, le protocole de transfert de courrier électronique entre une station cliente et un serveur de messagerie, ou entre deux serveurs de messagerie. Enfin, le TP aborde quelques manières d'authentifier la provenance des emails.

Remarques :
— Lorsqu'un client établit une connexion avec un serveur, il peut le faire en clair. L'ensemble des communications seront visibles sur le réseau (par exemple avec `telnet`). Il peut également former un tunnel sécurisé où tous les messages sont chiffrés de point à point (par exemple avec `openssl`). De nos jours, certaines applications comme Zimbra n'hésitent pas à interdire les communications non sécurisées en bloquant les ports associés.
— Les différents protocoles étudiés ici (IMAP, SMTP...) ne dépendent pas de la couche de communication : peu importe si vous utilisez une connexion en clair ou sécurisée, vous continuerez à respecter les mêmes règles d'interaction. Nous utiliserons ici `openssl`.

Pour démarrer : L'ensemble des manipulations de cette partie est à réaliser depuis la session Linux Ubuntu des machines de TP. Si vous étiez connecté sur une session FreeBSD, redémarrez l'ordinateur et choisissez l'option Linux Ubuntu.

1 Accès distant aux boites aux lettres avec IMAP

Pour cette partie du TP, nous vous conseillons de créer un nouveau compte de messagerie sur `https://compte.laposte.net/inscription/index.do?srv_gestion=lapostefr` pour ne pas risquer des manipulations malencontreuses sur votre boite mail de l'école. **Indiquez un mot de passe unique que vous n'utilisez pas sur d'autres comptes, car vous serez amenés à le taper en clair dans le terminal !**

Les questions peuvent sinon se faire avec votre compte de messagerie `<prénom>.<nom>@grenoble-inp.org` si vous le souhaitez. Vérifiez que vous êtes en mesure d'y accéder depuis Zimbra : `https://webmail.grenoble-inp.org`.

Note : Si vous utilisez votre mail grenoble-inp, pour vous assurer de ne pas perdre de données, pensez à archiver vos courriels importants dans des dossiers et à conserver une boite de réception propre.

Avant de commencer, ajoutez des messages de test à votre boite de réception de la façon qui vous conviendra le mieux : envoyez-en vous-même depuis votre adresse, demandez à un camarade de le faire pour vous, ou utilisez une autre adresse que vous possédez.

À la différence du protocole POP, le protocole IMAP permet de manipuler les messages directement sur le serveur de messagerie. Il est par exemple possible de créer des dossiers sur le serveur IMAP (des boites aux lettres) et de déplacer des messages d'un dossier à un autre sans en télécharger le contenu.

Chaque commande est précédée d'un index unique sous forme d'une chaine de caractère. Ceci permet dans certaines conditions d'envoyer au serveur une nouvelle commande alors que l'on n'a pas encore reçu la réponse de la précédente. Vous pouvez utiliser toujours le même index.

On utilisera principalement les commandes `LOGIN`, `SELECT`, `FETCH`, `STATUS`, `CREATE`, `COPY` et `LOGOUT`. Vous trouverez leur mode d'emploi en consultant la RFC 3501 disponible à l'adresse suivante :
`https://tools.ietf.org/html/rfc3501`.

Cette documentation se présente de la manière suivante, pour les sections consacrées aux commandes.

> `Arguments:` Une liste des différents arguments à utiliser.
> `Responses:` Les réponses qui sont données à la requête, s'il y en a.
> `Result:` La signification qu'ont les codes d'erreur que l'on trouve en fin de réponse. Suit une description du fonctionnement de la commande.
> `Example:` Des exemples d'utilisation sur des cas courants avec le résultat obtenu.

Remarques :

— Dans toute la suite, faites bien attention à respecter la syntaxe du protocole IMAP : `INDEX COMMANDE PARAMETRES`. Il n'est pas nécessaire pour ce TP de choisir un index différent à chaque commande (vous serez le seul à accéder à votre compte de messagerie et n'exécutez qu'une commande à la fois). Nous vous conseillons pour ce TP de choisir comme `index` un simple caractère, comme un unique « `.` »
— Comme indiqué précédemment, votre mot de passe sera visible en clair dans votre terminal, nous vous conseillons d'utiliser rapidement la commande de « choix de boite de réception » qui est assez verbeuse : `. SELECT inbox` ou de changer de mot de passe pour la session.

Le serveur IMAP de laposte.net se trouve sur la machine `imap.laposte.net`. Le serveur IMAP de grenoble-inp.org se trouve sur la machine `webmail.grenoble-inp.org`. Par défaut, les serveurs IMAP écoutent en clair sur le port 143 et en chiffré sur le port 993.

Q 1 — *Initiez une connexion interactive sécurisée entre votre machine et le serveur via la commande `openssl s_client -quiet -connect imap.laposte.net:993` pour le serveur de laposte.net ou `openssl s_client -quiet -connect webmail.grenoble-inp.org:993` pour le serveur de l'école. Identifiez-vous sur le serveur au moyen de votre adresse électronique et de votre mot de passe. Vous devrez pour cela utiliser la commande `LOGIN`.*

Q 2 — *Ouvrez votre boîte aux lettres `inbox`, à l'aide de la commande `SELECT`. Combien cette boîte aux lettres contient-elle de messages ?*

Q 3 — *Lisez le contenu de quelques messages de votre `inbox` à l'aide de la commande `FETCH` et repérez l'identifiant d'un de vos courriels de tests.*

Q 4 — *Supprimez un courriel de test en lui ajoutant le flag `\Deleted` à l'aide de la commande `STORE`. Le message a-t-il été supprimé du serveur ? Si non, trouvez une commande permettant la suppression définitive de ce message.*

Q 5 — *Utilisez la commande `CREATE` pour créer dans votre boite de réception un sous-dossier `inbox/Archives`. Déplacez-y quelques messages depuis votre boite de réception. Marquez-les comme comme lus.*
Note : *sur les boites laposte.net, le dossier créé peut ne pas apparaitre dans l'interface du webmail. Pour vérifier si le dossier a bien été créé, vous pouvez utiliser la commande `. LIST "" *` pour lister tous les dossiers existants dans votre boite aux lettres.*

Q 6 — *Déconnectez-vous enfin du serveur IMAP.*

Informations :

— IMAP accède à la boite de réception (mailbox) mais également aux différents dossiers d'archives.
— L'intérêt principal de IMAP est de pouvoir accéder à ses courriels depuis différents clients de messagerie. Les données étant stockées sur le serveur, l'UA agit uniquement comme interface pour afficher les messages.
— Le principal inconvénient est que IMAP nécessite une connexion permanente si on veut que les données soient synchronisées sur le serveur distant (mais on peut faire une gestion en local tant qu'on ne le fait que d'une machine avant de se reconnecter).

2 Transfert de courrier électronique avec SMTP

Le protocole SMTP sert à transférer du courrier électronique entre une station cliente et un serveur de courriel ou entre deux serveurs de courriel. La RFC 5321 pour ce protocole est disponible à cette adresse : `https://tools.ietf.org/html/rfc5321`. Pour obtenir les informations sur l'utilisation des différentes commandes, vous pouvez vous référer à cette RFC ou bien aux transparents du cours.

Q 7 — *Qu'est ce qu'un enregistrement MX ?*

Q 8 — *En utilisant la commande `dig MX <nom de domaine>`, faites une requête DNS pour trouver les serveurs de messagerie associés au nom de domaine `grenoble-inp.org`.*

Q 9 — *Quel(s) port(s) (par défaut) utilise un serveur SMTP ?*

2.1 Envoi d'un mail « à la main »

Lancez une capture de paquets avec Wireshark. Créez une connexion interactive non sécurisée entre votre machine et un des serveurs de messagerie de `grenoble-inp.org`.

Q 10 — *Saluez le serveur, puis envoyez, en vous servant des commandes SMTP offertes par le serveur, un*

message à une autre personne de votre groupe, avec comme objet « J'aime les pommes ». Commencez par préciser l'expéditeur, c'est à dire vous (`MAIL FROM:<email>`), le destinataire (`RCPT TO:<email>`) et enfin le corps du courriel (`DATA`).

Vous pouvez trouver l'ensemble des commandes SMTP à partir des transparents du cours, sur Internet, ou grâce à la RFC 5321 mentionnée en introduction.

Arrêtez la capture de paquets, et analysez le résultat de cette capture, en utilisant par exemple le filtre « smtp ».

Q 11 — *Que pouvez-vous dire sur le niveau de sécurité de la communication ?*

2.2 Connexion sécurisée

Il est possible de demander à utiliser une session sécurisé avec le serveur SMTP, grâce à la commande `STARTTLS`. Pour cela, on peut de nouveau utiliser `openssl`, mais en précisant qu'on souhaite établir une session sécurisée avec `STARTTLS` :

```
openssl s_client -quiet -starttls smtp -connect <hôte>:<port>
```

Trouvez les serveurs de messagerie du domaine `univ-grenoble-alpes.fr`. Lancez une capture de paquets avec Wireshark, et connectez-vous en `STARTTLS` sur le port 25 à un de ces serveurs de messagerie. Analysez ensuite la capture.

Q 12 — *La communication avec le serveur est-elle entièrement chiffrée ? Comment fonctionne `STARTTLS` ?*

Q 13 — *Testez avec les serveurs de messagerie associés à `grenoble-inp.org`. Que se passe-t-il ?*

2.3 Transfert de pièce jointe

En utilisant un client de messagerie plus évolué, comme la messagerie Zimbra ou Thunderbird, envoyez-vous un courriel contenant une image GIF récupérée sur Internet. Utilisez pour cela la même adresse mail que celle utilisée pour la partie 1 du TP (laposte.net ou votre mail étudiant).

Consultez le message en vous connectant directement au serveur IMAP (cf. partie 1 du TP).

Q 14 — *Comment l'image est-elle véhiculée ?*

Vous pouvez aussi utiliser l'option « Code source du message » dans le menu de Thunderbird, ou sous Zimbra : « Actions » > « Montrer l'original » pour consulter la façon dont les messages que vous avez reçus ont été codés.

Choisissez un message contenant une petite pièce-jointe (par exemple un petit PDF ou une image JPG) et copiez le contenu codé en base 64 dans un fichier appelé `PJ.b64` sur votre ordinateur.

Q 15 — *Utilisez la commande `base64` dans un terminal pour reconstituer le fichier d'origine de la pièce-jointe à partir du fichier `PJ.b64`. Pensez à indiquer l'extension d'origine de la pièce-jointe pour pouvoir l'ouvrir ensuite.*

Informations :

— SMTP spécifie l'expéditeur ainsi que le destinataire d'un message, vérifie les noms de domaines puis envoie le message. La transmission du message depuis le serveur de messagerie expéditeur jusqu'au serveur de messagerie destinataire se fait grâce aux enregistrements MX des serveurs DNS.
— Le protocole peut être mis en place de manière peu sécurisée. Il faut être conscient que votre message peut circuler en clair sur le réseau.

3 Authenticité des courriers électroniques

Nous allons maintenant voir que les protocoles de messagerie n'incluent pas, de base, de mécanisme d'authentification de la provenance des courriers. **En clair, il est assez facile de se faire passer pour quelqu'un d'autre.**

Nous verrons ensuite quelques techniques qui essayent de pallier à cette déficience, pour se prémunir de certaines formes d'attaques (*phishing*) ou de spam.

Dans les questions suivantes, vous allez effectuer un envoi de courriel à vous-même sous une identité arbitraire, à l'aide du protocole SMTP.

Q 16 — *De façon générale, avez-vous le droit de réaliser une telle manipulation ?*

ATTENTION : Faites bien attention à envoyer ce message à vous-même. L'utilisation d'une autre adresse de destination constituerait un délit, et engagerait votre responsabilité (LOPPSI du 14 Mars 2011) :
« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. »
Par ailleurs : « Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne ».
En cas de doute, demandez à vos enseignants avant d'envoyer le message.

Ouvrez de nouveau une connexion avec telnet vers un des serveurs de messagerie de `grenoble-inp.org`, puis envoyez un message à vous-même paraissant venir de `James Bond <james.bond@gandi.net>` et dont l'objet serait « Compte rendu de mission ».

Pour cela, servez-vous des mêmes commandes SMTP que précédemment (`MAIL FROM`, `RCPT TO`, etc).

Q 17 — *Vérifiez que vous recevez le message dans votre boite mail `grenoble-inp.org`. Avez-vous un moyen de détecter la falsification ?*

Essayez d'envoyer un nouveau message, toujours en vous faisant passer pour `james.bond@gandi.net`, mais cette fois-ci à destination de `root@polyno.me`. Pensez bien à vous connecter à un des serveurs de messagerie responsable pour le domaine de destination !

Q 18 — *Que se passe-t-il ? Identifiez le mécanisme mis en place par le serveur SMTP de `polyno.me`*

pour détecter cette usurpation d'identité, et trouvez la RFC décrivant ce mécanisme.

Q 19 — *En vous aidant de la section 3 de la RFC, trouvez l'enregistrement dans le DNS permettant au serveur mail d'établir que vous n'êtes pas autorisé à envoyer un email d'une adresse* `@gandi.net`*. Vous devrez récursivement rechercher les adresses autorisées, comme décrit dans la section 5.2.*

Q 20 — *Le domaine* `grenoble-inp.org` *possède-t-il un tel enregistrement ? Réessayez d'envoyer avec telnet un message à* `root@polyno.me` *semblant provenir de* `james.bond@grenoble-inp.org`*. Que se passe-t-il cette fois-ci ?*