Travail personnel - Familiarisation avec les outils de communication

Remarques préliminaires

Les problèmes/oublis constatés dans ce support sont à signaler à l'adresse `clot@univ-lyon1.fr`.

Ci-après, nous vous proposons quelques exercices visant à vous faire découvrir l'environnement auquel est connecté votre machine ainsi que des outils classiques pour le travail sur des ressources distantes. Nous présenterons différents outils permettant de travailler tantôt dans l'environnement WinXX (questions précédées de ), tantôt dans un environnement LinuX (resp.), tantôt dans les deux sans distinction notable.

Signalons dès à présent que les machines sur lesquelles vous allez effectuer des connexions sont des machines de travail. Elles servent à différentes personnes dans des tâches d'enseignement et de recherche. Il vous est demandé de respecter ces environnements de travail et de les utiliser uniquement dans le cadre de ce TP. Les services de connexion qui sont proposés ci-après seront disponibles jusqu'au 19/12/2014. Au-delà, ils seront fermés.

Identification de l'hôte

Dans le menu démarrer, sélectionnez "Executer" puis saisissez la commande "cmd". Une fenêtre de commande s'ouvre. La commande `ipconfig` vous permet de connaitre les paramètres d'identification de votre poste pour le système d'exploitation en cours. Exécutez `ipconfig` et repérez l'adresse IP de la machine, le masque sous-réseau et l'adresse IP de la passerelle. Que pouvez-vous en déduire sur l'organisation du réseau auquel vous êtes connecté ? Exécutez à nouveau la commande `ipconfig` mais avec l'option `/all` à présent. Quel est le nom de votre poste ? Quel est le domaine auquel il appartient ?...

Pour obtenir le nom d'hôte de la machine, utilisez la routine `hostname`. En fait, la commande `hostname` renvoie par défaut le nom de l'hôte mais son output peut être beaucoup plus riche. Les nombreuses options de `hostname` permettent d'obtenir tous les renseignements nécessaires à l'identification de l'hôte. Nous reviendrons sur ce sujet dans la section portant sur telnet.

FTP

Ouvrez un navigateur web et pointez vers l'url `ftp://130.59.10.36`. Vous êtes connecté au serveur ftp mirror.switch.ch (s'il cela vous est demandé, réalisez une connexion comme invité). Tentez à présent une connexion en suivant l'url `ftp://195.220.111.226`. Contrairement au premier serveur, la connexion sur minisfa nécessite une identification/authentification. Vous pouvez utiliser le login `invite` avec le mot de passe `3|\|te!2` (ce qui diffère de `3|\|te!2`). Reformez l'url en y intégrant le login, mais pas le mot de passe (laisser des mots de passe dans l'historique n'est pas une bonne idée si vous n'êtes pas l'unique utilisateur du poste !). Placez-vous dans le répertoire `XXX` et récupérez l'image `angular_momentum.jpg`.

Vous allez refaire votre connexion sans utiliser de navigateur graphique, mais utiliser la commande `ftp` en mode texte.

Connexion

Dans le menu démarrer de windows, sélectionnez "Executer" puis saisissez la commande "cmd". Sous Linux, loguez vous sur une console ou démarrez un terminal. Dans la fenêtre de commande, saisissez la commande `ftp`. Au nouveau prompt, vous allez tenter une connexion avec la commande `open` en précisant le nom du serveur visé. Saisissez les login et mot de passe lorsqu'ils vous sont réclamés. Une fois logué, tapez la commande `binary`.

Découverte de l'environnement

La commande `pwd` (acronyme de *present working directory*, i.e. répertoire de travail courant) vous renseigne sur votre position actuelle dans l'arborescence de fichiers sur le serveur. Pour connaître votre position dans le système de fichier local, utilisez la commande `lpwd` (pour *local pwd*, i.e. pwd local). Pour lister le contenu sur repertoire courant distant vous pouvez faire appel aux commandes `ls` ou dir. Il est possible d'employer des «patrons» de noms de fichers en utilisant les caractères `*` et `?` pour limiter la liste à certains fichiers. Par exemple, `ls␣*.png` liste tous les fichiers d'extension png, `ls␣d*g` liste tous les noms de fichiers commençant par d et finissant par g. Le caractère `*` symbolise toute chaîne de caractères et le caractère `?` représente un unique caractère. Ainsi `ls␣???` liste les fichiers dont le nom est formé de trois caractères et le contenu des répertoires dont le nom est formé de trois caractères. Listez le contenu du répertoire et repérer les noms des répertoires.

Se déplacer

Pour vous déplacer dans l'arborescence distante, utilisez la commande `cd` (*change directory*) avec le nom du répertoire visé en argument. Il est aussi possible de se déplacer localement avec la commande `lcd` (*local change directory*). Placez-vous dans `X␣X`. Listez le contenu du répertoire. Positionnez-vous dans le répertoire `XXX` et listez son contenu (Pour remonter au niveau supérieur, vous pouvez utiliser la commande `cd␣..` (deux fois le caractère point)).

Récupérer des fichiers

Deux commandes permettent de récuperer des fichiers présents sur le serveur : `get` et `mget`. La commande `get` prend un argument obligatoire (le nom du fichier distant) et un argument optionnel permettant de renommer le fichier localement. Récupérez le fichier `im_an_idiot.jpg` en le plaçant dans un fichier nommé `Image01_VotreNom_VotrePrenom.jpg`. La commande `mget` (pour multiple get) permet d'obtenir plusieurs fichiers, ces fichiers étant listés ou fournis en utilisant des patrons de nom de fichier. Par exemple, `mget sandwich.png self_description.png` et `mget s*.png` permettent de récuperer les mêmes fichiers. Utilisez `mget` pour récuperer les fichiers commençant par `s`. Déplacez vous à présent dans le répertoire distant `X␣X`.

Envoyer des fichiers

Deux commandes permettent de placer sur le serveur des fichiers dans le répertoire courant : `put` et `mput` (pour multiple put). Placez le fichier `Image01_VotreNom_VotrePrenom.jpg` sur le serveur avec la commande `put` et assurez-vous que le fichier a bien été reçu en listant le répertoire distant.

Déconnexion

Pour mettre fin à la connexion, il y a diverses commandes : `exit` ou `bye` pour fermer la connexion et finir la session ftp, `close` ou `disconnect` pour fermer la connexion sans sortir de la session ftp. Déconnectez-vous de minisfa.

Telnet

La commande `telnet` est la commande «client» qui permet de se connecter au service `telnet` sur une machine pour laquelle ce service est ouvert et d'interagir avec le shell de connexion. La connexion nécessite un login et un mot de passe. De facon plus claire, l'utilisateur logué peut travailler à distance avec l'interface textuelle de telnet. Il faut donc connaitre les commandes en ligne...et faire le deuil de sa souris le temps de la connexion :o).

Connexion

Dans le menu démarrer de windows, sélectionnez "Executer" puis saisissez la commande "cmd". Sous Linux, loguez vous sur une console ou démarrez un terminal. Dans la fenêtre de commande, saisissez la commande `telnet`. Vous ouvrez ainsi une session telnet. La demande de connexion au système distant se fait comme dans une session ftp, par la commande `open`. Saisissez le login et le mot de passe lorsqu'ils sont demandés.
Lors de l'établissement de la connexion, le message d'accueil est affiché, puis le prompt du shell de connexion apparait, vous laissant saisir vos commandes.

```
telnet> open 195.220.111.226
```

```
Trying 195.220.111.226...
Connected to minisfa.
Escape character is '^]'.

minisfa login: invite
Password:
Last login: Thu Nov 18 17:57:51 from massdcpo.univ-lyon1.fr
Have a lot of fun...
invite@minisfa:~>
```

Interagir

Et maintenant, que faire sur la machine distante ? De l'édition de fichier, de la compilation...de la messagerie...de la consultation de documentation !

Revenons sur la commande `hostname` invoquée plus haut, dans la section Identification de l'hôte. Exécutez la commande `hostname` pour obtenir le nom d'hôte de la machine. Pour obtenir d'avantage de précision, il est nécessaire d'avoir recours aux options de cette commande. La commande `man` permet d'accéder à la documentation des commandes du système. Exécutez `man hostname` afin de prendre connaissance des différentes options. Pour vous déplacer dans les écrans d'aide (les pages du manuel), vous pouvez utiliser les flèches du curseur et la touche q pour sortir de l'aide. Déterminez les options adéquates pour afficher le domaine de l'hôte, son adresse IP et le nom complétement qualifié. Sachant que les options sont cummulables, exécutez `hostname` avec les bonnes options pour afficher les informations mentionnées ci-dessus.

Pour puiser dans les ressources communes, poursuivons en faisant une mini-séance de R. Invoquez pour cela R à l'aide de la commande `R`. Vous pouvez observer les messages habituels :

```
invite@minisfa:~> R
Copyright (C) 2010 The R Foundation for Statistical Computing
ISBN 3-900051-07-0
Platform: x86_64-apple-darwin9.8.0/x86_64 (64-bit)

R est un logiciel libre livré sans AUCUNE GARANTIE.
Vous pouvez le redistribuer sous certaines conditions.
Tapez 'license()' ou 'licence()' pour plus de d'etails.

R est un projet collaboratif avec de nombreux contributeurs.
Tapez 'contributors()' pour plus d'information et
'citation()' pour la facon de le citer dans les publications.

Tapez 'demo()' pour des d'emonstrations, 'help()' pour l'aide
en ligne ou 'help.start()' pour obtenir l'aide au format HTML.
Tapez 'q()' pour quitter R.

>
```

Dans cet environnement, vous pouvez travailler avec la seule limitation suivante : si votre système ne permet pas la gestion des applications graphiques à distance, vous ne pouvez créer de fenêtre graphique. Mais si votre système le permet, vous pouvez travailler sans restriction (dans la mesure où vous avez indiqué à `ssh` de permettre le transfert des fenêtre X11...option `-X`) !
Générez une matrice aléatoire de taille 10×20 que vous placerez dans une variable X. Centrez et réduisez les colonnes de X, puis déterminez les valeurs et vecteurs propres de la matrice $\frac{1}{20} X'X$..
Pour mettre fin à cette courte session R, utilisez la commande `q()`.

Pour finir, vous allez utiliser une commande vous permettant de voir les ports utilisés sur la machine distante pour les connexions extérieures. La commande à utiliser pour cela est `netstat` avec notamment l'option `-p tcp`. Consultez la page man de cette commande pour saisir son but et surtout l'option nécessaire à l'affichage sous forme numérique des adresses et numéros de ports

utilisés pour chaque connexion. Quel est le numéro de port sur le serveur associé à la connexion telnet ?

Déconnexion

Pour mettre fin à la connexion telnet, vous pouvez utiliser au choix les commandes `logout`, `exit` ou utiliser l'une des séquences de caractères `^]` (i.e., probablement pour votre clavier, la séquence de touches `<ctrl>+<AltGr>+<]>`) ou `<Ctrl>+D`.

ssh et sftp

Un des gros problèmes de telnet est de faire passer l'information sur le réseau en clair (sans cryptage). Ainsi, il est possible de repérer, avec des outils aisément accessibles, le mot de passe associé à un certain login utilisé dans une connexion en cours.


Dans la console, exécutez la commande ssh pour établir une connexion vers minisfa. Une fois connecté, vous pouvez travailler comme cela a été illustré avec `telnet`.


Afin d'établir une connexion par le protocole ssh, il est nécessaire d'avoir un client ssh. Aucun client ssh n'est présent par défaut sous windows. Il est donc nécessaire d'en télécharger un si aucun client n'est déjà installé sur le système. Vous pouvez utiliser google pour rechercher l'utilitaire Putty. Une fois le client pris en main, saisissez les paramètres pour une connexion vers minisfa (assurez-vous bien que ssh est utilisé et non telnet, comme certains clients le permettent) et connectez-vous.


Pour laisser une trace de votre passage, vous allez envoyer un mail à l'utilisateur de login denis. Pour cela, saisissez au prompt la commande `mail denis`. Le mail aura pour sujet :

`Reponses de prenom nom`
où prenom et nom sont à remplacer par vos nom et prénom. Dans le corps du mail, vous préciserez vos réponses concernant l'identification de votre poste de travail. Tapez votre réponse dans le terminal puis pour mettre fin au corps du mail, allez à la ligne et taper la séquence de caractères `<ctrl>+D`. Votre mail est envoyé sitôt que vous voyez apparaitre la ligne
`EOT`
à l'écran.

Pour finir, utilisez la commande `netstat` comme précédement pour identifier le port du serveur utilisé pour la connexion puis déconnectez-vous.


Comme `telnet`, `ftp` organise les échanges d'information en clair sur le réseau. Le protocole sftp est la version cryptée du protocole ftp. Une fois la main mise sur un client `sftp`, connectez-vous sur minisfa par sftp. Quelques différences au niveau des commandes existent par rapport à celles de `ftp` : `mput` et `mget` ne sont généralement pas implantées. Ouvrez une seconde connexion avec telnet sur minisfa pour observer le numéro de port utilisé par le serveur pour établir la connexion `sftp`.

Mail

Nous avons utilisé jusqu'à présent `telnet` pour effectuer des connexions selon le mode le plus standard : `telnet` <Nom d'hôte>. Il est possible de préciser à `telnet`, en plus du nom d'hôte, le numéro de port à utiliser pour la connexion. Ceci permet d'utiliser telnet comme application «client» pour le service associé au port, pour peu que l'on sache converser avec le serveur «en attente derrière le port». C'est ce que vous allez faire ci-dessous, en instaurant un dialogue avec un serveur de mail.

Différents protocoles permettent d'organiser l'échange de mails. POP3 fait parti des plus courants pour la consultation (pas pour l'envoi !), mais ces dernières années, l'accent ayant été mis sur la confidentialité, il est souvent encapsulé dans un tunnel SSL (comprenez par là qu'une couche de chiffrement a été ajoutée juste sous la couche où les échanges au niveau POP3 ont lieu. Ainsi les données transitent en plus, pour une meilleure confidentialité, par un service de chiffrement SSL...) Nous allons ci-dessous utiliser un compte sur gmail (l'adresse est `aimedeuhihair@gmail.com` et le mot de passe est le mot de passe correspondant aux supports sur la page `IRM2.html`, substitué ci-dessous par `toctoc`) pour consulter l'état de la boîte aux lettres et interagir avec via le protocole POP.

Précisons que les choses se passent de manière analogue avec le serveur de mail de l'université et sur lequel vous disposez de votre compte étudiant [1].

Afin de ne vous permettre d'utiliser le protocole POP3 de manière transparente à travers la couche SSL, il faut créer un tunnel SSL entre votre hôte et le serveur de mail. Un programme permet de faire cela simplement sur `minisfa` :


Ouvrez une session ssh vers `minisfa` et exécutez la commande `MonTunnelVersGmail`. Un message vous indique la commande `telnet` à axécuter pour utiliser le tunnel vers le serveur `gmail`. Ouvrez ensuite une seconde session ssh vers `minisfa` pour exécuter la commande `telnet` indiquée.

Pour éviter les complications d'accès concurrents, un serveur basé sur POP3 n'autorise pas plusieurs connexions simultanées d'un même utilisateur. `gmail` semble faire exception...

Nous passons à présent aux détails des échanges.

Identification/authentification


Dans la session `telnet` démarrée ci-dessus, saisissez la commande `USER aimedeuhihair` pour permettre au serveur de vous identifier. Le serveur envoie une réponse à votre demande d'identification et en cas de succes, la prochaine information attendue est votre mot de passe. La commande `PASS toctoc` transmet votre mot de passe au serveur et celui-ci, en cas de succès de l'authentification, renvoie une réponse du type :

```
+OK welcome
```

A tout moment, l'utilisateur peut mettre fin à la connexion en utilisant la commande `QUIT`.

Interaction

Différentes commandes permettent d'obtenir des informations sur les messages contenus dans la boite :

- La commande `STAT` permet de connaitre le nombre de message contenus dans la boite et la taille totale de ces messages. La réponse envoyée est normalement constituée d'une seule ligne. Les messages marqués pour l'opération d'effacement (cf plus bas) ne sont pas pris en compte dans l'information renvoyée.
- La commande `LIST` permet d'obtenir une liste des messages non marqués pour l'opération d'effacement.


Testez ces deux commandes. Quelle différence caractérise ces deux commandes.

Notez que la commande `LIST` accepte comme argument optionnel le numéro d'un mail.

Lecture

Différentes commandes permettent de lire une partie ou l'intégralité d'un message

- La commande `RETR` prend comme argument le numéro du mail qui sera envoyé par le serveur vers le client. Le numéro ne peut être celui d'un mail programmé pour l'opération d'effacement.
- La commande `TOP` est une commande optionnellement implantée dans le protocole POP3. Cette dernière prend deux arguments : un numéro de mail et un entier positif. La commande `TOP 2 30` permet d'envoyer vers le client les trentes premières lignes du second mail.


Essayez d'obtenir les premières lignes d'un de vos mails. Ces premières lignes constituent l'entête du mail. Obtenez la totalité de votre mail avec la commande RETR.

Effacement et annulation d'effacement

L'opération d'effacement se programme lors d'une session et est réellement effectuée après que l'utilisateur se soit déconnecté.

La commande `DELE` prend comme argument le numéro du mail qui sera programmé pour l'effacement. La commande `RSET` permet d'annuler l'ensemble des effacements programmés.

1. Tout étudiant de l'UCLB dispose d'un compte sur accesbv. Vous pouvez acceder à votre boite à partir de la rubrique mail du site http://edu.univ-lyon1.fr et trouver là des précisions sur le nom du serveur de mail.

 Effectuez une demande `DELE` sur un numéro de mail excédant le nombre de mail présent dans la boite. Quelle réaction a le serveur ? Assurez-vous qu'aucun effacement n'est réalisé.

Les détails du protocole POP3 sont donnés par le document nommé RFC 1939 (Request For Comment numéro 1939 publié par le Network Working Group). Les protocoles de communication tels que FTP, HTTP font l'objet d'autres RFCs.

Terminal Server

L'université met également à disposition un service de terminal Microsoft. Cet accès est réalisable hors du campus, sans l'utilisation du vpn. Pour cela, il est possible d'utiliser :
— l'outil Connexion Bureau à distance à partir des systèmes Microsoft (et mac) ;
— la commande `rdesktop` sur les systèmes linux/bsd (i.e. les mac en particuliers).

 A partir de l'un des outils indiqués, ouvrez une connexion vers `tseetu.univ-lyon1.fr`.

 Sur cet écran de connexion, sélectionnez Autre utilisateur et dans le champ de saisie de l'utilisateur entrez votre login étudiant précédé de `univ-lyon1\` et le mot de passe associé dans le champ correspondant. En cas de difficulté avec...le clavier, il est possible d'avoir recours à un clavier visuel.

 Une fois connecté, vous pouvez utiliser les applications de cet hôte distant. Il est également possible de monter un nouveau lecteur réseau sur votre répertoire de fichiers personnels afin de conserver votre travail.

Virtual Private Network

Après cette présentation des outils les plus classiques, les plus légers également, nous revenons sur le problème de la protection des données. Les services abordés, pour un certain nombre, n'ont pas été conçus dans la préoccupation de protéger les données échangées. Ssh est un protocole qui apporte une réponse assez générale, étant donnée la possibilité d'encapsuler dans ce protocole beaucoup d'échanges (comme illustré ci-dessus...). Les réseaux virtuels privés constituent également une solution intéressante : un réseau n'est plus limité aux hôtes pouvant y être reliés physiquement, mais peut être étendu à des hôtes distants qui recevront une adresse IP du réseau en question. Il est possible d'imaginer des services peu sécurisés mais peu exposés dans la mesure où ils sont uniquement visibles de l'intérieur d'un réseau privé. Le VPN permet de donner à des hôtes distants accès à ces services en préservant leur protection.

Cette partie présente un intérêt particulier si vous la réalisez hors du campus, i.e. dans un environnement où vous n'avez normalement pas accès à certains services (comme `ftp` ou `telnet` sur minisfa) !

 Ouvrez un navigateur web et pointez vers l'url `http://vpn.univ-lyon1.fr`. L'université met à la disposition des personnels (et occasionnellement des étudiants) un service de VPN permettant d'accéder à l'ensemble de son infrastructure réseau, alors qu'une grande partie n'est pas accessible de l'extérieur de son réseau, pour des raisons évidentes de sécurité. Identifiez-vous avec vos paramètres d'étudiant.

 Sélectionnez dans le menu à gauche AnyConnect puis cliquez sur Start AnyConnect afin de lancer le client VPN qui devrait permettre à votre poste d'intégrer le VPN, i.e. d'obtenir une adresse IP du campus. Une fois la connexion réalisée, observez l'adresse IP de votre hôte. Observez également les connexions afin d'observer le pont existant entre votre ancienne adresse et l'adresse du campus qui vous est attribuée.

 Dans la console de commande ou un terminal, tentez une connexion vers `ftp://195.220.111.226`. Ceci fonctionne à présent puisque votre hôte a une vue sur l'ensemble du réseau du campus.

 Il en va de même du service `telnet` normalement innaccessible depuis l'extérieur du campus.

Il existe d'autres services intéressants et utilisables sur le campus...Notamment l'accès aux ressources bilbiographiques de l'université. Poursuivez à votre guise et selon vos intérêts.