Système et réseau : mise en oeuvre et exploitation

Mathieu Petit

Version. grincheux et dormeur

1 Introduction

1.1 Objectif

La finalité de ce TP est double. Il s'agit d'une part de vous familiariser avec l'environnement Unix et d'autre part, de vous faire analyser une communication entre ordinateurs.

Il s'agira d'effectuer la mise en réseau des 6 machines, de vérifier les protocoles de communication *telnet* et *Ssh*. Vous démontrerez, en analysant les trames TCP, que le protocole *Ssh* est plus sécurisé que le protocole *telnet*. Enfin, vous explorerez des mécanismes d'accès et d'exploitation de machine à distance.

A la fin du TP, vous me rendrez une copie contenant vos éléments de réflexion. Ceux-ci seront notés...J'attends donc de votre part un document rédigé et répondant aux questions ci après. Justifiez vos réponses, si vous manquez d'informations, internet est une bonne source, l'ordinateur "prof" est connecté sur l'extérieur.

1.2 Le matériel...

La démarche que nous vous proposons consiste à analyser les communications entre ordinateurs. Certains ont comme système d'exploitation Linux ("joyeux", "dormeur", "atchoum"), les autres utilisent Windows ("grincheux", "simplet", "timide"). Les machines seront montées en réseau Ethernet. Dans un premier temps, nous allons provoquer des communications entre les machines. Puis nous analyserons les communications entre celles-ci. Enfin nous exploiterons quelques possibilités plus subtiles d'Unix et Windows.

En utilisant la démarche présentée par la suite ainsi que les logiciels de la distribution Ubuntu et des logiciels Windows mis à votre disposition, vous réaliserez les taches suivantes.

2 Quelques vérifications

2.1 configuration physique du réseau (couche physique-liaison)

Cette opération est a effectuer en concertation avec les autres binommes présents. Les machines sont livrées en état "sortie d'usine" et aucune configu-

ration du réseau n'est effectuée. En premier lieu, et avant d'allumer les ordinateurs :

1. câblez l'ensemble du réseau. Utilisez les câbles droits et croisés fournis ainsi que les 2 hubs

   Question 1 *Présentez un schéma du câblage effectué*

   Question 2 *À quelle fin avez vous utilisé le câble croisé*

2. faites valider votre câblage par l'encadrant !

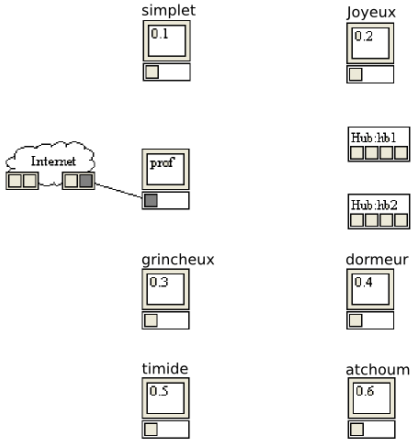

FIG. 1 – Plan du réseau

2.2 configuration des machines (couche transport-reseau)

Les comptes ouverts sur chaque machine sont du type "eleve" + "nom_de_machine" comme mot de passe ; vous êtes administrateur sur chaque machine. Nous allons configurer les cartes réseau pour pouvoir échanger des trames.

1. Démarrez les machines et logez vous.
2. Sous *Windows*, configurez le réseau à partir du panneau de configuration. L'IP est 10.5.0.3, le réseau 10.5.0.0/16.

   Question 3 *Précisez le masque de sous réseau*

3. faites de même sous *linux* à partir de *Système→administration→ réseau*. L'adresse IP est 10.5.0.4, le masque identique à celui de la machine *Windows*.
4. testez l'activation de la connexion depuis la console avec les commandes *ipconfig* et *ifconfig*, sous *windows* et *linux*, respectivement.[1]

   Question 4 *Quelles informations sont retournées par ces commandes ?*

[1] Rappel : sous *linux*, vous trouvez la console dans *applications→accessoires*, sous *windows*, c'est menu *démarrer→tout les programmes→accessoires*

2.3 La déclaration des machines (couche application)

Pour s'assurer du bon dialogue entre les machines, il faut les déclarer. Nous réaliserons cette étape sans utiliser de DNS (Domain Name Server). Pour cela, nous devons déclarer chacune des machines. Les machines sur lesquelles vous travaillez s'appellent respectivement "grincheux" (*Windows*) et "dormeur" (*linux*)

1. De **grincheux**, après avoir ouvert une boite de commande MS-DOS, essayez de "pinger" **dormeur**. avec la commande *ping dormeur*

   Question 5 *Que se passe t'il ?*

2. Éditez le fichier *c :\windows\system32\drivers\etc\hosts*. Ajoutez dans le fichier les lignes suivantes :

10.5.0.1	simplet
10.5.0.2	joyeux
...	
10.5.0.6	atchoum

3. Sous Linux, ouvrez une console et logez vous en tant qu'administrateur (tapez *sudo -s* et [enter] puis renseignez le mot de passe d'utilisateur pour vous connecter en super-utilisateur).
4. Dans le fichier */etc/hosts*, faites les mêmes modifications (*nano nom_fichier* pour éditer).
5. Essayez à nouveau de "pinger" **dormeur**.

   Question 6 *Que se passe t'il ? détaillez les champs des trames reçues*

6. Vérifiez que vous arrivez à joindre les stations des autres binomes

2.4 La connexion telnet

On considère maintenant qu'il n'y a plus de problèmes sur le réseau. Nous allons essayer de réaliser une connexion de type **telnet** entre **grincheux** et **dormeur**. Pour cela, nous allons ouvrir un serveur telnet sur la machine **Windows**,

1. Démarrez le service **telnet** sous Windows (voir dans le *panneau de configuration→ administration →services*)
2. Depuis la machine linux, connectez vous via un client telnet (commande *telnet nom_du_serveur*)

   Question 7 *Que vous affiche la console linux ouverte ? Expliquez*

3. A partir de Linux, créez un nouveau répertoire Lambda sur le disque c :\ (commandes MsDOS *cd* et *MkDir nom_du_répertoire*)
4. Vérifiez sur **grincheux** la présence du répertoire nouvellement crée

   Question 8 *En quelques mots, à quoi sert un serveur Telnet ?*

2.5 La connexion Ssh (couche session-application)

Pour réaliser une connexion Ssh, il est nécessaire qu'un serveur sécurisé soit installé. Le protocole Ssh permet une connexion sécurisée entre deux machines. À l'inverse du point précédent, nous installerons le serveur sur la machine **Linux**.

1. Vérifiez que le serveur est bien lancé (commande *ps -aux|grep sshd*)
2. Depuis la machine **Windows**, connectez vous à la station **dormeur** avec le logiciel **Putty**
3. une fois connecté, tapez sous linux la commande *who*

   Question 9 *Que constatez-vous ? À quoi sert cette commande*

3 La trame TCP/IP

On sait maintenant se connecter sur une machine distante. On sait aussi installer des logiciels. On va, maintenant, passer au reniflage de notre réseau.

3.1 Scan de port avec Nmap

Le produit que nous allons utiliser est **nmap**. il s'utilise en ligne de commande (*man nmap* vous donne sa syntaxe).

Question 10 *Quels ports sont ouverts sur* ***grincheux*** *? À quels services correspondent-ils ?*

3.2 Analyse de trames TCP/IP

Pour visualiser les trames qui transitent sur le réseau, je vous propose d'installer un autre produit : EtherReal. C'est un outil graphique qui permet de visualiser les trames TCP. Le même produit existe pour Windows.

1. Démarrez le logiciel depuis la console en mode super-utilisateur (*sudo ethereal &*)
2. Lancez un enregistrement de trames depuis ethereal et ouvrez une session **telnet** sur **grincheux** à partir de **dormeur**. effectuez quelques échanges et arrêtez l'acquisition

   Question 11 *Les trames reçues s'affichent dans la fenêtre principale de ethereal. D'où proviennent les paquets "sniffés" ?*

   Question 12 *Pourquoi l'utilisation de switchs à la place de hubs permettrait un niveau de sécurité plus élévé ?*

3. triez les trames par "destination" et analysez les paquets envoyés à **grincheux** (on connaît son adresse IP)

   Question 13 *Retrouvez vous le login et le mot de passe en clair ?*

   Question 14 *Pourquoi le mot de passe est-il découpé lettre par lettre (non, ce n'est pas une question de sécurité...)*

Nous allons reprendre la même manipulation, avec Ssh et dans le sens **Windows→Linux**.

1. Lancez une nouvelle collecte de trames
2. Avec putty, connectez vous à **dormeur**, lancez quelques commandes
3. Arrêtez l'enregistrement et passez à l'analyse des paquets reçus

   Question 15 *Concluez sur la sécurité de SSH par rapport à Telnet.*

4 plus loin avec Linux

À priori, des serveurs SSH doivent tourner sur les 3 machines **Linux**. Vous connaissez les noms et les mots de passe de ces stations, tout les ingrédients sont là pour permettre une connexion.

4.1 *"Follow the white rabbit"*

Vous avez sur **dormeur** une console en avant plan. À ce point nous pouvons assumer qu'il en est de même sur les stations Linux des autres binomes. Le but dans cette section va être d'afficher depuis **dormeur** des messages sur la console ouverte sous **atchoum**. Pour cela, prenons un moment pour introduire la gestion des périphériques sous Linux.

Vous utilisez en ce moment même des périphériques d'entrée-sortie... Clavier, souris, écran viennent à l'esprit, mais il faut aussi considérer les disques, cdroms, cartes son, imprimantes, etc. comme des périphériques. Sous Linux, un périphérique est toujours représenté par un fichier rangé dans le répertoire */dev/*. Ainsi, pour accéder au données de la souris, il vous suffit de lire le fichier correspondant dans */dev/*.

1. Dans une nouvelle console, lancez la commande sudo *cat /dev/psaux* et bougez la souris

Voila, nous accédons au périphérique. De la même manière, pour les périphériques en sortie, il suffit d'écrire dans le fichier correspondant. Par exemple, pour imprimer un fichier, on peut utiliser *sudo cat nom_du_fichier > /dev/lp0* ou */dev/lp0* désigne l'imprimante Linux n° 0 (Linux printer 0).

Question 16 *Décomposez la commande sudo cat reseau.pdf > /dev/lp0*

Pour des raisonS historique, les consoles sont des logiciels considérés comme des périphériques d'affichage physique. On retrouve donc des fichiers d'accès aux consoles dans l'arborescence */dev/*. Les consoles sont de 2 types : "les vrais" terminaux, représentés par les fichiers */dev/tty[1-63]* et les "pseudo" terminaux, représentés par */dev/pts/[0-N]*.

1. fermez les consoles ouvertes, sauf la console de traffic reseau que vous pouvez nettoyer (commande *clear*).
2. lancez la commande who

   Question 17 *quels sont les consoles ouvertes ? Par quels fichiers sont elles représentés dans /dev/ ?*
3. Ouvrez une console supplémentaire et dans la console fixe, relancez *who*

   Question 18 *Des changements ? Qu'est-ce qu'un "pseudo" terminal désigne ?*[2]
4. Écrivez un message depuis la console fixe vers la console nouvellement ouverte : *echo "message transmis">/dev/pts/2* . Celui-ci s'affiche dans l'autre console

[2]Vous devez constater la présence d'un vrais terminal dans la liste des connectés, il s'agit de la console qui a servi a lancer l'interface graphique de Linux et qui apparaît brièvement lors de la séquence de démarrage. On peut y accéder avec la combinaison de touches *[ctrl]+[alt]+[F1]* (*[ctrl]+[alt]+[F7]* pour revenir).

Avec ces bases techniques, vous pouvez maintenant effectuer la même manipulation sur un ordinateur distant, en l'occurrence **atchoum**.

1. connectez vous a joyeux par SSH depuis une nouvelle console linux (commande *Ssh nom_ordi*)
2. lancez la commande *who* et repérez le fichier lié à la console fixe affichée sur **atchoum**. Au passage, vous remarquez que votre propre connexion SSH est identifiée...
3. effacez le contenu de la console (commande clear > /dev/pts/[n° _de_console])
4. envoyez un message ("Wake up Neo" ou ce que vous voulez) et guettez la réaction ou allez constater de visu que le texte s'est bien affiché sur l'ordinateur distant.

4.2 affichage distant

Le serveur graphique de linux, Héritage de XWindow, permet une utilisation en réseau. Ces possibilités ne sont plus exploitées de nos jours mais étaient essentielles dans les années 80-90 où des ordinateurs centraux distribuaient leurs affichages graphique sur une multitude de terminaux. La couche réseau est toujours disponible, et c'est une source potentielle de nuisances... Nous allons effectuer un export d'affichage depuis **dormeur** vers **joyeux** pour faire "surgir" des fenêtres d'application sur l'écran de vos camarades.

La variable d'environnement *DISPLAY* définit les propriétés de l'affichage d'une application graphique. C'est une chaîne de caractères qui s'écrit de la façon suivante : <adresse_machine>:<n° serveur_graphique>.<n° écran> .

1. en local, affichez le contenu de *DISPLAY* (commande *echo $DISPLAY*)

   Question 19 *sur quel serveur et quel écran s'afficheront les application ?*

2. Vérifiez cela en lançant une application graphique depuis la console (commande *xeyes* & par exemple)

Nous allons maintenant déporter l'affichage vers **joyeux** en modifiant le contenu de DISPLAY

1. lancez *export DISPLAY="joyeux :0.0"* et vérifiez que la variable à bien été modifiée
2. lancez une application graphique depuis votre console[3] et guettez les réactions ...

Question 20 *Comment savez-vous que vos camarades ont fermé les applications que vous avez pu lancer depuis* ***dormeur*** *?*

4.3 Prise de main à distance

Dans cette dernière partie du TP, nous allons utiliser VNC pour prendre complètement la main sur la session Windows depuis Linux.

1. configurez le serveur sur **grincheux**. Après avoir défini le mot de passe de connexion, lancez le serveur VNC

[3] Vous pouvez d'ailleurs en ouvrir autant que vous voulez : *xeyes* & *firefox* & *xcalc* & etc.

2. Lancez ensuite le client **vncviewer** sur **dormeur**. Entrez le nom du serveur ou son IP et le mot de passe.

Question 21 *Comment prendre conscience de la prise en main à distance sur* **grincheux** *?*

Une fois la session VNC en cours. Lancez une session ethereal et collectez quelques trames.

Question 22 *Les trames sont elles exploitables ?*

Question 23 *Pouvez-vous expliquer pourquoi (réfléchissez au contenu transféré) ?*

Question 24 *À la vue des trames collectées, quels sont les inconvénients de la prise de contrôle par vnc ?*

5 Conclusion

Vous avez parcouru en trois heures quelques possibilités de l'utilisation d'ordinateurs en réseau. L'analyse des trames doit vous faire prendre conscience des dangers du manque de sécurité des transmissions qui est malheureusement généralisé aujourd'hui. En effet, toutes les transmissions Web reposent sur le protocole HTTP, qui tout comme telnet transmet ses information en clair ! Tout les formulaires d'abonnements, les pages de forums, vos éventuels mots de passe et logins transitent à la vue de qui veut bien prendre la peine d'y regarder (nous avons vu que c'est techniquement à la portée de tous). Prendre conscience des faiblesse des réseau, c'est déjà faire la moitié du chemin vers la sûreté informatique, l'autre moitié vous sera dispensée en cours de voie d'approfondissement.