Université d'Angers	Département Informatique
Faculté des Sciences	L3 Pro Informatique 2012/13
Module : *Utilisation des systèmes et réseaux : TCP/IP*	David Lesaint

TP n° 1
Modèle en couches

L'objectif du TP est de vous faire découvrir le modèle en couches et vous donner des outils pour travailler en réseau, notamment sur les serveurs de l'Université.

Exercice 1 - SSH/SCP : Secure Shell/Secure CoPy

La commande *ssh* permet de lancer un terminal (shell) sécurisé (par cryptage des échanges) sur une machine distante. Le protocole SSH (couche application) définit les règles de communication. Pour en savoir plus sur la commande *ssh*, lisez la page correspondante du manuel. Pour en savoir plus sur le protocole SSH, consultez les RFC 4251, 4252, 4253 et 4254 ou l'article Wikipedia http://fr.wikipedia.org/wiki/Ssh.

1. Connectez-vous à *forge* en *ssh*, essayez de lancer *konqueror*, puis déconnectez-vous.
2. Connectez-vous à *forge* en *ssh* en activant le X11 forwarding. Cela signifie que l'application sera exécutée sur *forge* mais se connectera au serveur X de votre machine pour l'affichage. Lancez *konqueror*, naviguez dans vos dossiers personnels et déconnectez-vous.
3. Lancez la commande *ls* via *ssh*.
4. Lancez uniquement *konqueror* via *ssh*.

   La commande *scp* permet de copier des fichiers de façon sécurisée en s'appuyant sur SSH.
5. Copiez un fichier sur *forge* depuis votre poste.
6. Copiez un fichier depuis *forge* dans votre home directory.

   Le protocole SSH est sensible aux attaques de type "Man in the Middle". L'attaque consiste à se placer entre le client et le serveur et à se faire passer pour le serveur auprès du client et vice versa. Il est alors possible d'es-pionner la communication et donc de récupérer par exemple les mots de passe. Pour parer à ce genre de désagréments, le protocole SSH propose une authentification par clé public/privé (cryptage asymétrique).
7. Commencez par générer une paire de clés à l'aide de la commande *ssh-keyge*n. Attention ! Il faut mettre un mot de passe à vos clés. Sinon il sera possible de se connecter au serveur en possédant juste votre clé privé ! Pour le TP, choisissez un mot de passe différent de votre compte sur *forge* afin de pouvoir vérifier le bon fonctionnement de l'authentification par clé.

   Les clés publiques autorisées à se connecter sont mises dans le fichier *~/.ssh/authorized_keys* (le signe ~sert à désigner votre home). Il sera possible de se connecter à l'aide du mot de passe qui chiffre votre clé privée.
8. Gérer vos connexions à *forge* de cette façon. Il faut passer votre clé privé en paramètre à *ssh*.

Exercice 2 - ARP, DNS, DHCP, . . .

Le protocole ARP se situe entre la couche 2 et 3 du modèle OSI. Il définit comment relier une adresse IP (adresse du protocole Internet, couche 3 OSI : réseau) à une adresse MAC (Media Access Control, adresse matérielle, couche 2 OSI : lien). Le protocole ARP est décrit dans la RFC 826.

1. Cherchez et parcourez la RFC 826.
2. Quelles sont les adresses IP, réseau et MAC de la carte réseau de votre machine qui vous connecte au réseau du département ?

3. Comparez ces informations à celles d'un de vos voisins : adresse IP et adresse MAC.
4. Affichez la table ARP de votre machine. Comparez cette table avec celle de votre voisin.

La commande *ping* permet de tester l'accessibilité d'une machine sur un réseau IP par l'émission d'une requête *ICMP echo*. La machine peut répondre par une requête *ICMP echo reply* pour signifier sa présence. Cette commande est donc rattachée à la couche 3 du modèle OSI.

5. Faites un *ping* sur la machine de votre voisin.
6. Affichez les tables ARP de vos machines, comparer aux résultats de la question 4 et expliquez.
7. Connectez-vous à *forge* et consultez sa table ARP.

Il est plus pratique de retenir le nom de domaine d'une machine connectée à Internet que son adresse IP. Le protocole pour interroger un DNS (couche7 OSI : applications) permet de relier un nom de domaine comme *google.fr* à une adresse IP (couche 3 OSI : réseau). L'interrogation d'un serveur DNS passe donc par la couche de transport (couche 4 OSI) et utilise le protocole de transport UDP. Les couches 5 et 6 du modèle OSI n'ont pas des sens ici, nous en reparlerons avec le modèle en couche TCP/IP.

8. Quelle est l'IP du DNS de votre poste de travail ?
9. Quelle est l'IP du DNS sur *forge* ? Que contient le fichier */etc/resolv.conf* ?
10. Déterminez le chemin emprunté pour atteindre *google.fr*. Utilisez les commandes *dig*, *nslookup* et *host* sur *google.fr*. Utilisez le manuel pour déterminer à quoi correspondent les informations retournées.

Pour en savoir plus sur les DNS, leur hiérarchie et bien plus encore : `http://en.wikipedia.org/wiki/Domain_Name_System` ainsi que les articles associés.

11. Quelle est la passerelle de votre réseau : son adresse privée sur votre réseau local, son adresse publique, son nom et son adresse MAC ?
12. Quelles sont les adresses IP actives sur votre réseau ?
13. Quels sont les serveurs actifs sur votre poste ?
14. Quels sont les ports ouverts sur la passerelle de votre réseau ?
15. Quel est le serveur de courrier électronique du journal L'Equipe ?
16. Déterminez l'adresse du serveur DHCP de votre réseau ainsi que tous les paramètres qu'il fixe lors du renouvellement du bail de votre poste.

Exercice 3 - Le Web

Utiliser *Firefox* pour réaliser les opérations suivantes :

1. Allez à la page du département informatique en tapant l'adresse dans la barre d'adresse, puis faites de cette page la page d'accueil de *Firefox*.
2. Dans un nouvel onglet, ouvrez la page du Wiki du département informatique `http://forge.in-fo.univ-angers.fr/wiki`. Ajoutez cette page en favori.
3. Dans un nouvel onglet, allez à la page d'adresse IP 74.125.230.84.
4. Ajoutez le moteur de recherche *Wikipedia* à la liste des moteurs disponibles dans la barre de recherche de *Firefox*, puis cherchez "Web" dans *Wikipedia* à partir de cette barre de recherche. Ajoutez cette page en favoris dans un dossier nommé "réseaux".

Exercice 4 - VPN

Afin d'accéder aux ressources informatiques du département à partir de chez soi (afin par exemple de continuer des TP de programmation à distance sans avoir à installer les compilateurs chez soi), plusieurs outils existent. Nous allons en explorer trois : le VPN du département, Putty et WinSCP.

Ouvrir une connexion VPN par `https://vpn.info.univ-angers.fr/`. Une fois la connexion ouverte :

1. Envoyez un fichier sur son compte.

2. Téléchargez un fichier de son compte.
3. Ouvrez une session sur *forge* par *ssh*.
4. Essayer de refaire ces manipulations en dehors de l'Université, c'est tout l'intérêt du VPN.

Exercice 5 - PuTTY sous Windows

PuTTY est un client libre SSH/Telnet pour Windows et Unix.

1. Ouvrez une session sur *forge* par SSH.
2. Ouvrez une session sur *forge* par SSH avec l'authentification par clés.
3. Essayez d'ouvrir une application graphique (activez le X11 forwarding). Expliquez.

Exercice 6 - WinSCP sous windows

WinSCP est un client libre SFTP/SCP pour Windows utilisant SSH (il partage une partie de son code avec PuTTY). Il permet le transfert sécurisé de fichiers entre un client et un serveur SSH.

1. Ouvrez une session sur votre compte *forge* par SSH.
2. Envoyez / téléchargez des fichiers sur votre compte.
3. Testez l'identification par clés.