RÉSEAUX – NETWORK II
EXERCICES

Exercice 0

1. Se connecter au serveur « ssh » « marion.szpieg.fr » avec votre compte.
2. Taper la commande « history -c », afin d'effacer votre historique du TP précédent.
3. Avec la commande « mkdir », créer un répertoire « tprx2 » dans votre home directory.
4. Vérifier avec la commande « ls » que le répertoire a bien été créé.
5. Avec la commande « cd », se placer dans le répertoire tprx2.

Exercice 1 : interroger un serveur ; notion de chemin emprunté par un paquet (ping)

Dans cet exercice, nous allons interroger un serveur de noms de Google qui se trouve aux Etats-Unis, et dont l'adresse IP est : 8.8.8.8.

1. Taper la commande « ping -c1 8.8.8.8 » puis valider.
   Vérifier que le ping est bien revenu, que le paquet n'a pas été perdu.

On aimerait connaître quel chemin a fait le paquet de notre machine à la machine interrogée. Pour cela, nous allons imposer un ttl (Time To Live) très petit et l'augmenter au fur et à mesure :

2. a) Taper la commande « ping -c1 -t2 8.8.8.8 » puis valider.
   b) Quelle est l'adresse IP du 1er routeur traversé après la box ?
3. a) Recommencer en augmentant le ttl de 1 à chaque fois jusqu'à ce que le paquet arrive.
   b) Par combien de routeurs le message est-il passé ? Noter les différentes adresses IP.

Exercice 2 : fragmentation de paquets (ping)

Pour obliger la machine à faire de la fragmentation de paquets lors de l'utilisation de la commande ping, il faut paramétrer la taille du paquet partant supérieure à 1500 octets (MTU!).

1. a) Taper la commande « ping -c1 -s2000 8.8.8.8 » puis valider.
   b) Expliquer le résultat.
2. Pour chercher une autre adresse de serveur sur internet, je vous propose de chercher l'adresse IP du serveur du site du lycée. Pour cela, on va se servir d'une nouvelle commande : « nslookup » à qui on va donner l'adresse du site du lycée, et qui va nous renvoyer son adresse IP.
   Taper la commande « nslookup lfcl-lisbonne.eu » puis valider. Quelle est l'adresse IP du site du lycée ?
3. a) Refaire un ping de 2000 octets sur cette machine et vérifier que cette fois on obtient une réponse.
   b) Voit-on que le paquet a été fragmenté ? Comment peut-on faire pour que cela soit le cas ?
4. a) Capturer les paquets avec tcpdump, et les enregistrer dans un fichier appelé bigping.cap.
   b) Combien de paquets ai-je capturé ? Est-ce normal ?
5. a) Ouvrir le fichier bigping.cap déposé sur classroom avec wireshark
   b) Expliquer les 4 lignes.
   c) Pourquoi le 1er paquet qui part fait 1514 octets et non 1500 octets ?
   d) Si elles ne sont pas visibles, faire apparaître les colonnes de n° de port source et destination : pourquoi ces colonnes sont-elles vides ?
   e) Quand on sélectionne le 1er paquet, on voit dans la ligne « Ethernet II » que l'adresse MAC destinataire est 44:a6:1e:8e:81:f6. A qui appartient cette adresse MAC ?
   f) Quand on sélectionne le 1er paquet, on voit dans la ligne «Internet Protocol Version 4 » que l'adresse IP destinataire est 83.166.138.20. A qui appartient cette adresse IP?
   g) Pourquoi est-ce que le protocole IPV4 met comme destinataire l'adresse du serveur du lycée, et le protocole Ethernet II met comme destinataire l'adresse de la box ?

Exercice 3 : étude d'un protocole de la couche 4 : DNS (nslookup)

1. On va capturer des paquets pour visualiser le protocole DNS. Taper les commandes suivantes :
   tcpdump port 53 -w dnspt.cap&
   valider deux fois
   nslookup lfcl-lisbonne.eu
   fg
   puis appuyer sur Ctrl+C
   Vous devez avoir un message vous indiquant que vous avez capturé un certain nombre de paquets.
2. Récupérer la fichier dnspt.cap dans le classroom puis l'ouvrir avec Wireshark
3. Commenter les lignes de la fenêtre du haut et celles de la fenêtre centrale.

Exercice 4 : étude du protocole TCP

1. Grâce à la commande « nslookup », retrouver l'adresse IP du site fredpeuriere.com.
2. On va capturer des paquets pour visualiser le protocole TCP. Taper les commandes suivantes :
   tcpdump host 213.186.33.3 -w peuriere.cap&
   valider deux fois
   wget fredpeuriere.com
   fg
   puis appuyer sur Ctrl+C
   Vous devez avoir un message vous indiquant que vous avez capturé un certain nombre de paquets.
3. Récupérer la fichier peuriere.cap dans le classroom puis l'ouvrir avec Wireshark
4. Commenter les lignes de la fenêtre du haut et celles de la fenêtre centrale.

Exercice 5 : sortir du serveur

Avant de vous déconnecter taper la commande suivante : « history>/home/lfclxx/tprx1/rx2hist.txt.

Pour quitter le serveur « marion.szpieg.fr » tapez « exit » (à faire pour éviter de faire tourner la session « pour rien » svp).