Helec Bastien

TP1 : La couche IP :

exercice 1 : Mise en place d'un serveur echo L'outil netcat est un peu le couteau suisse de l'administrateur réseau. Il permet de mettre en place très simplement un petit serveur en une simple commande :

nc -l -p 7 -c "/bin/cat"

Expliquez ce que fait la commande ci-dessus. Démarrez un serveur echo en UDP sur le port XX de la vm mise à votre disposition, et montrez comment vous y connecter depuis votre machine à l'aide de la commande telnet. Pour rappel, un serveur echo ouvre un port, et répète en retour tout message que vous lui enverrez.

nc -l -u -p 7 -c "/bin/cat" : permet de lancer un serveur echo en UDP sur le port 7 connexion avec la machine physique :

```
netcat -u 10.213.0.169 7
```

exercice 2 : Encapsulation/ Désencapsulation

Capturez une trame émise par votre machine vers le serveur echo. Vous devrez capturer la même trame simultanément sur la machine émettrice et sur la machine réceptrice. Comparez le contenu des entêtes Ethernet, IP et UDP des deux paquets. Qu'est-ce qui a changé ? Expliquez.

Le contenu des entêtes Ethernet, IP et UDP des deux paquets sont identiques sauf pour l'adresse MAC de la machine émettrice qui a changé.

exercice 3: forgeage de trame avec hping

L'utilitaire hping, sous linux, permet de "fabriquer" une trame telle que vous la voulez. Montrer comment l'utiliser. Forgez une trame obéissant aux contraintes suivantes : . Couche IP ; . Adresse IP source : La votre. . Adresse IP destination : celle de votre VM . TTL : 200 . Couche TCP : . Port source : 666 . Port destination : 22 . FLAGS : SYN . Numéro de séquence : 2355 Capturez la trame que vous avez émise et vérifiez qu'elle obéit bien aux contraintes demandées.

```
hping3 -p 22 -s 666 -t 200 -a 10.213.8.1 -S 10.213.0.169
```

La trame emise correspond bien au contraintes emises

Exercie 4 : Le role du champs ttl : A l'aide de hping, émettez des trames vers votre VM avec une valeur croissante de TTL. (Démarrez à 1 et augmentez à chaque étape). Capturez les échanges émis et reçus. Que constatez vous ? Qui vous répond ? Expliquez.

```
```
hping3 -p 22 -s 666 -t 1++ -a 10.213.8.1 -S 10.213.0.169
```
```

La trame emise envoie chaque trame avec un ttl superieur a chauqe fois , la machine virtuelle repond avec un ttl par defaut 64. ce qui veut dire que la machine virtuelle ne repond pas a la trame car le ttl est trop petit.

exercice 5 : Traceroute L'outil traceroute permet de déterminer par quels routeurs une connexion sera ache- minée. Que donne la commande suivante ?

```
traceroute -T -p 80 208.97.177.124
```

Le resultat de cette commande donne les differents routeurs des differents reseau permettant d'acceder a l'adresse 208.97.177.124

A l'aide d'un sniffer, expliquez comment fait traceroute pour obtenir ce résultat. Il est possible, mais rare, que la commande ne donne pas toujours le même résultat deux fois d'affilée. Pourquoi, selon vous ? Le traceroute prend la route la plus courte pour atteindre l'adresse Parce que le protocole qui calcul la route la plus courte peut changer indiquant alors d'autre routeur de passage

Exercice 6 : Le MTU

Qu'est-ce que le MTU ? Quelle est sa valeur actuelle sur votre machine ?

Le MTU est la taille maximale d'un paquet de données qui peut être transmis sur un réseau. La valeur actuelle sur ma machine est 1500

Comment peut-on le changer sous Linux ? Fixez le à 500. A l'aide de hping, Emettez un paquet UDP de 400 Octets vers votre VM. Capturez la trame émise. Recommencez avec une trame de 2000 Octets. Que se passe-t-il ? Analysez les trames capturées et montrez comment la couche IP a géré le problème.

```
ip link set dev eno1 mtu [valeur]
hping3 -p 22 -s 666 -t 1++ -a
```

mtu = 500 : L'emission d'un paquet de 400 octets fonctionne mais pas un paquet de 2000 octets car le mtu est trop petit pour 2000 octets

exercice 7 : Mettre en place un réseau ip Vous configurerez les adresses, masques, MTU et route par défaut de chaque machine. Pour activer le routage, utilisez la commande : echo 1 1> /proc/sys/net/ipv4/ip_forward Montrez, captures de trames à l'appui, comment une trame IP est fragmentée/réassemblée sur votre réseau.