Année Universitaire 2023-2024 session 1 d'automne

université de BORDEAUX

Parcours : TAH Licence pro ADSILLH **UE :** 4TAH506U
Épreuve : Examen réseaux
Date : 24 novembre **Heure :** 11h00 **Durée :** 1h30
Modalités : Épreuve sans document, calculatrice autorisée
Épreuve de : Mr Samuel Thibault 2 **pages**

Collège Sciences et technologie

Exercice 1. Questions / discussions de cours

Q1.1

confidentialité un attaquant ne peut pas lire le contenu du message

authentification un attaquant ne peut pas forger de message ayant l'apparence de venir d'un émetteur choisi

intégrité un attaquant ne peut pas modifier le contenu du message

Q1.2

```
client                  serveur
     ---------SYN--------->
     <------SYN+ACK--------
     ---------ACK--------->
```

Q1.3
Si un attaquant veut modifier un datagramme TCP, il peut très facilement recalculer le checksum TCP pour correspondre à la modification, ou bien produire une modification qui laisse le checksum inchangé. Il n'y a donc de protection que contre des modification non volontaires (fiabilité), pas contre les modifications volontaires (sécurité).

Q1.4 Cet en-tête permet au client de préciser le nom de domaine du site voulu, pour le cas où plusieurs sites web sont hébergés sur un même serveur. En effet, le serveur ne peut pas connaitre le nom de domaine puisqu'il reçoit simplement une connexion TCP sur son IP, il ne sait pas quel nom de domaine a été traduit en cette adresse IP.

Q1.5 La fonction accept prend en paramètre une socket d'écoute, et retourne une socket de client, c'est-à-dire une socket connectée au client qui vient de se connecter. On peut rappeler de nouveau accept sur la socket d'écoute, pendant que par exemple un autre thread s'occupe de discuter avec le client.

Exercice 2. Adresses

Q2.1 $2^{32-22} = 2^{10} = 1024$ adresses

Q2.2 de 185.233.0.1 à 185.233.3.254

Q2.3 Pour avoir 6 sous-réseaux distincts, il faut utiliser 3 bits pour les numéroter, donc des /25, par exemple :
- 185.233.0.0/25
- 185.233.0.128/25
- 185.233.1.0/25
- 185.233.1.128/25
- 185.233.2.0/25
- 185.233.2.128/25

(et il reste encore les .3.0 et .3.128 disponibles)

Q2.4 $2^{128-32} = 2^{96} = 64$ milliards de milliards de milliards d'adresses

Q2.5 Il faut de nouveau dépenser 3 bits. Pour simplifier, on aligne sur 4 bits :
- 2a0c :e300 :0000 : :/36
- 2a0c :e300 :1000 : :/36
- 2a0c :e300 :2000 : :/36
- 2a0c :e300 :3000 : :/36
- 2a0c :e300 :4000 : :/36
- 2a0c :e300 :5000 : :/36

et il reste encore beaucoup de sous-réseaux disponibles

Exercice 3. Calculs

Q3.1
$25Go/30 * 24 * 3600s \simeq 1G/100000s = 10Ko/s$

Q3.2
$3 * 4 * 3600s * 1Mbps \simeq 40000Mb = 5Go$

Q3.3
Un paquet fait typiquement 1500 octets, ou 12000 bits Il suffit donc de l'ordre de 80 paquets par seconde.

Q3.4 $10km/300000km/s \simeq 33s$, c'est plutôt négligeable !

Exercice 4. Analyse de paquet

Q4.1 10.0.0.129 et 10.0.0.254

Q4.2 0x404 = 1028, 0x16 = 22

Q4.3 C'est le récepteur qui a un numéro de port inférieur à 1024, donc c'est très probablement lui le serveur. On se souvient d'ailleurs qu'usuellement le port 22 est utilisé pour un serveur ssh.

Q4.4
C'est probablement plutôt le début : on voit du texte en clair, donc probablement on n'a pas encore échangé de clé de session, et l'on ne peut donc pas encore chiffrer.

Exercice 5. NFS (Network File System)

Q5.1 Si un utilisateur utilise sa clé ssh privée, elle passe en clair sur le réseau, et un attaquant peut alors la lire et l'utiliser pour se connecter à des serveurs (ou service gitlab).

Q5.2 Il peut demander l'ouverture d'un fichier quelconque (en forgeant l'identité de l'utilisateur ouvrant le fichier), et non seulement lire mais aussi écrire ce qu'il souhaite.

Q5.3 Le client NFS doit s'authentifier auprès du serveur, en utilisant par exemple une clé privée. Le serveur peut être ainsi sûr de l'identité du client qui fait des demandes d'ouverture/lecture/écriture/etc. On peut par ailleurs établir une clé de session qui permet de chiffrer toutes les données échangées.

Q5.4
On peut utiliser un VPN :
serveur NFS <-> serveur VPN <-> Internet <-> client VPN <-> ordinateur portable