Année Universitaire 2022-2023 session 1 d'automne

université de BORDEAUX

Parcours : TAH Licence pro ADSILLH **UE :** 4TAH506U
Épreuve : Examen réseaux
Date : 18 novembre **Heure :** 14h00 **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 Quand une troisième machine voudra envoyer un paquet vers cette adresse IP, elle va envoyer une requête ARP mais recevoir deux réponses des deux machines configurées ainsi. Selon la réponse qui parvient le plus rapidement, notre troisième machine enverra ses trames à l'une ou l'autre seulement des deux machines. On aura donc l'impression que soit l'une, soit l'autre machine a un accès au réseau.

Q1.2 TCP vérifie l'intégrité à l'aide d'un checksum 16 bits. Avec 16 bits et des modifications purement aléatoires, il y a tout de même une chance sur $2^{16} = 65536$ pour que le checksum soit correct par erreur.

Q1.3 Si l'on les branche en boucle, un paquet envoyé par une machine à destination de l'adresse de broadcast sera relayé de switch en switch en boucle, sans fin. On peut utiliser STP pour que les switchs désactivent automatiquement l'un des lien pour casser la boucle.

Q1.4 socket listen accept read write close

accept prend en paramètre la socket d'écoute de départ, et retourne une nouvelle socket, correspondant à un client qui vient de se connecter.

Q1.5 C'est un problème d'encodage de caractères. Sur mon ordinateur l'encodage du système est apparemment latin1, alors que dans le fichier zip c'est de l'utf-8. Sur l'autre ordinateur, l'encodage du système est de l'utf-8, ce qui ne pose alors plus de problème. Il faudrait que le format zip spécifie l'encodage des noms de fichiers, pour que sur mon ordinateur la conversion d'encodage puisse être effectuée.

Exercice 2. Adresses

Q2.1 $2^{32-23} = 2^9 = 512$ adresses, de 10.0.0.1 à 10.0.1.254, c'est largement assez.

Q2.2 On peut utiliser 10.0.0.0/25, 10.0.0.128/25, 10.0.1.0/25, et 10.0.1.128/25.

Q2.3 On peut utiliser

```
2001:0db8:1234:1::/64
2001:0db8:1234:2::/64
2001:0db8:1234:3::/64
2001:0db8:1234:4::/64
```

Exercice 3. Calculs

Q3.1 $7\,Go = 56Gb \simeq 60Gb$. À 1Gbps il faut donc 60s, une minute.

Q3.2 C'est probablement le disque dur qui n'est pas capable de débiter à 125Mo/s, ou alors un chiffrement

Q3.3 Un paquet est typiquement de 1500o, cela fait donc environ 5 millions de paquets.

Q3.4 5 000 000 * 100µs = 500s, soit environ 8 minutes.

Exercice 4. Analyse de paquet

Q4.1 10.0.0.25

0x7b, c'est-à-dire 123
C'est le même port des deux côtés, d'habitude côté client c'est un port aléatoire.

Q4.2 0x38 = 56 octets

Exercice 5. Authentification SSH par certificats

Q5.1 TOFU (Trust On First Use) signifie qu'on fait a priori confiance, lorsque l'on se connecte pour la première fois à un service, que ce n'est pas un moment où le service est détourné par un attaquant. Si jamais plus tard un attaquant parvient à détourner le service, on pourra s'en rendre compte en constatant que la clé publique du service a changé.

Q5.2 Le principe est que le serveur fait certifier sa clé publique par une autorité de certification. Le client possède déjà la clé publique de l'autorité de certification (installée par firefox par exemple), et peut donc vérifier que la clé du serveur est valide, et donc peut lui faire confiance dès la première connexion au service.

Q5.3 Il y a de très nombreux sites web. Lorsque l'on navigue de site en site, le risque grandit que l'un d'entre eux soit détourné pendant la navigation, on ne préfère donc pas utiliser TOFU. Pour autant on ne veut pas avoir à récupérer à la main la clé publique de chaque site web visité. Avec un ensemble d'autorités de certifications bien connues installées par défaut dans les navigateurs web, les administrateurs système peuvent simplement faire présenter par leur site web un certificat signé par une autorité.

Q5.4 Si une entreprise fournit par exemple un service de ferme de calcul, chaque serveur de calcul ayant sa propre clé ssh, il est utile de les faire signer par une même autorité, dont on fournit la clé publique aux clients lors de la signature du contrat commercial, pour qu'ils puissent se connecter à n'importe quel serveur de calcul en toute sécurité.

Q5.5 À l'université par exemple de nombreux étudiants peuvent avoir besoin de se connecter par ssh à différents services. Il serait utile que le service de scolarité certifie la clé ssh d'un étudiant lorsqu'il s'inscrit, et l'université installe la clé publique de certification sur les différents serveurs ssh. Les étudiants peuvent alors se connecter immédiatement sur n'importe quel serveur ssh en utilisant leur clé certifiée.