Institut Universitaire de Technologie
Aix*Marseille Université

Réseaux & Télécoms

TP Analyse de protocole

ETUDE DU PROTOCOLE TCP

1. Liminaire

Chaque question en gras correspond à une question sur le relevé numérique de TP intitulé `Questionnaire Analyse Protocole TCP` et disponible sur AMETICE

Ouvrez une fenetre DOS et récupérer les informations suivantes :

l'adresse ip de votre machine ?

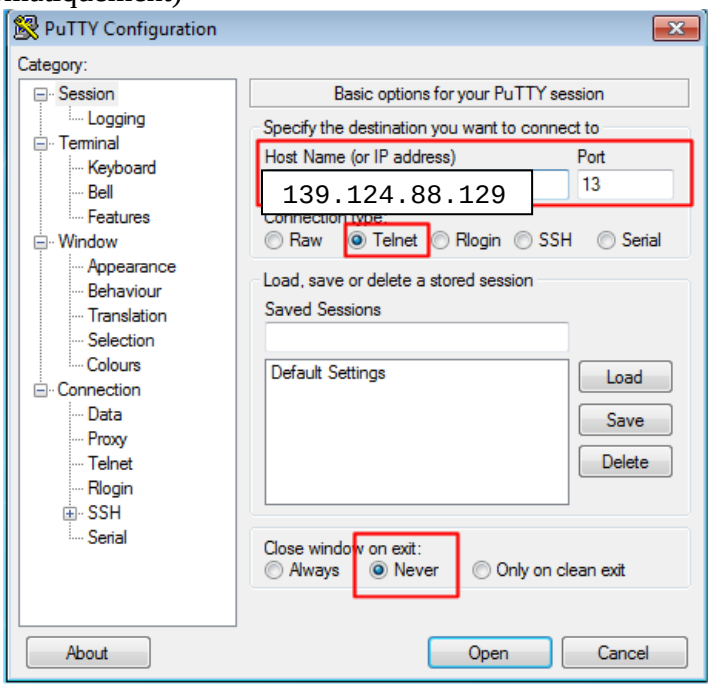
le masque de réseau ?

l'adresse ip de votre passerelle ?

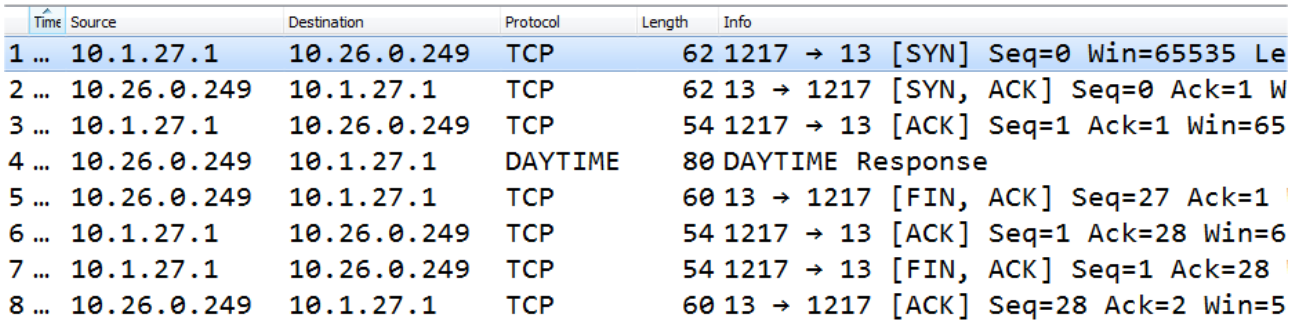
A partir du menu `Démarrer`, lancer le logiciel `wireshark.`

2. Analyse d'un trafic TCP simple : `daytime`

Lancez une capture de trames. Puis dans le menu menu `Démarrer-> Tous les programmes -> WinSCP-Putty`, sélectionner `Putty.`La fenetre suivante va s'ouvrir remplissez les champs comme indiqué (sélection du protocole `telnet`, du port `13` et la fenêtre ne doit pas se fermer automatiquement)



Dès que vous obtenez la réponse du serveur de temps, arrêter la capture et sélectionner le protocole `tcp` dans le champ `filter`. Aux valeurs près, vous devriez obtenir ceci :



Time	Source	Destination	Protocol	Length	Info
1 …	10.1.27.1	10.26.0.249	TCP	62	1217 → 13 [SYN] Seq=0 Win=65535 Le
2 …	10.26.0.249	10.1.27.1	TCP	62	13 → 1217 [SYN, ACK] Seq=0 Ack=1 W
3 …	10.1.27.1	10.26.0.249	TCP	54	1217 → 13 [ACK] Seq=1 Ack=1 Win=65
4 …	10.26.0.249	10.1.27.1	DAYTIME	80	DAYTIME Response
5 …	10.26.0.249	10.1.27.1	TCP	60	13 → 1217 [FIN, ACK] Seq=27 Ack=1
6 …	10.1.27.1	10.26.0.249	TCP	54	1217 → 13 [ACK] Seq=1 Ack=28 Win=6
7 …	10.1.27.1	10.26.0.249	TCP	54	1217 → 13 [FIN, ACK] Seq=1 Ack=28
8 …	10.26.0.249	10.1.27.1	TCP	60	13 → 1217 [ACK] Seq=28 Ack=2 Win=5

2.1 Analyse de la phase d'ouverture

Indiquez le ou les numéros des trames correspondant à l'ouverture de la connexion TCP

Comment appelle-t-on familièrement cette phase ?

Quel est le numéro du port sur lequel vous interrogez le serveur ?

Quel est le numéro du port sur lequel le serveur va vous répondre ?
Pourquoi ce numéro du port sur lequel le serveur va répondre au client est supérieur à 1023 ?

Tracer le chronogramme de la phase d'ouverture en indiquant clairement les numéros de séquences et les numéros d'acquittement

En regardant le premier segment portant un drapeau `SYN`, déterminer la taille de la fenêtre de réception de votre machine ?

En regardant le deuxième segment portant un drapeau `SYN`, déterminer la taille de la fenêtre de réception du serveur ?

2.2 Analyse de la phase d'échange des données

Indiquez le ou les numéros des trames correspondant à l'échange des données
Comment se nomme le protocole utilisé ?

En examinant en détail le segment, retrouvez la longueur des données envoyées ?

En utilisant la commande `Follow TCP Stream` du menu `Analyze`, retrouvez les informations envoyées par le serveur de temps.

2.3 Analyse de la phase de fermeture

Indiquez le ou les numéros des trames correspondant à la fermeture de la connexion TCP

Combien de demie-fermetures comporte t-elle ?
Pourquoi ?

Quel est le numéro de séquence porté par le premier segment FIN ?
Pourquoi cette valeur ?

3. Analyse d'un trafic `telnet`

Lancez une capture de trames[1]. Toujours avec Putty connectez-vous en Telnet sur le port 23 (le port par défaut du protocole `telnet`) sur `139.124.88.129` (le login est `tpreseau1a` et le password est `tpreseau1a`). Une fois connecté, tapez la commande `ls`, puis la commande `exit`. Arrêtez alors la capture.

Sur quel protocole de la couche transport le protocole `telnet` s'appuie t-il ?

Repérez les trois phases de l'échange ?

Sur quel port le serveur est-il à l'écoute des connexions `telnet` ?

Combien de segments ont été nécessaires pour envoyer le password ?

4. Analyse d'un trafic `ssh`

Toujours avec Putty connectez-vous en SSH sur le port 22 (le port par défaut du protocole `SSH`) sur `139.124.88.129`. Cliquez sur `Open`

Répondez `yes` à la question posée, puis une fois la connexion établie ((le login est `tpreseau1a` et le password est `tpreseau1a`), tapez la commande `ls` suivi d'un `exit`. Arrêtez la capture.

[1] N'oubliez pas de supprimer le filtre d'affichage. Pour cela cliquez sur le bouton `Clear`.

Sur quel protocole de la couche transport le protocole `ssh` s'appuie t-il ?

Sur quel port le serveur attend-il les connexions par `ssh` ?

En utilisant la commande `Follow TCP Stream` du menu `Analyze`, essayez de retrouver votre mot de passe.

Si vous aviez à vous connecter de manière sécurisée sur une machine distante, quel protocole utiliseriez vous :

- **telnet**
- **dns**
- **ssh**
- **http**

5. Trafic FTP

Lancez une capture de trames. Puis, dans une fenêtre DOS, lancez la commande `ftp 139.124.88.129 .` Pour l'authentification, utilisez le login `tpreseau1a` et comme password `tpreseau1a`. Si tout se passe bien, vous devriez voir apparaître en autres choses :

```
230 Login successful.
```

Puis l'invite du client FTP `ftp>`

Le client attend donc une commande à envoyer au serveur FTP. Pour afficher la liste des commandes disponibles pour le client FTP, tapez `help` <ENTRÉE> :

```
ftp> help ↵
```

5.1 Transfert de fichier

Parmi toutes les commandes disponibles, nous allons utiliser la commande `get` pour transférer le fichier `blague.txt` sur votre machine depuis le serveur. Tapez pour cela :

```
ftp>get blague.txt ↵
```

Une fois le fichier transféré, quittez le client ftp au moyen de la commande `quit` et arrêtez a capture.

Quel est le numéro du port sur lequel le serveur accepte les connexions ftp ?

Combien y a t-il de phases d'ouverture dans la capture ?

Combien de trames a t-il fallu pour envoyer le password au serveur FTP ?

Quel est le port utilisé par le serveur pour l'échange de données FTP-DATA ?

Quel est le port utilisé par le client pour l'échange de données FTP-DATA ?

Qui du serveur ou du client a établit la connexion pour le transfert des données ?

En utilisant la commande `Follow TCP Stream` du menu `Analyze`, retrouvez le contenu du fichier transféré entre le client et le serveur.

5.2 Actif ou passif

Le protocole ftp fonctionne selon deux modes différents qui sont très importants du point de vue de la sécurité des informations.
En mode de transfert actif, un client démarre une session FTP avec le serveur sur le port 21. Pour le transfert des données, le serveur lance une connexion à partir du port 20 vers un port élevé d'un client (supérieur à 1023).

Que se passerait-il pour le transfert des données si le pare-feu du client FTP était configuré pour ne pas autoriser les connexions de l'extérieur ?

En mode de transfert passif, un client démarre également une session FTP avec le serveur sur le port 21. Par contre, pour le transfert des données, deux modifications majeures interviennent :

1. c'est le client qui établit la connexion des données avec le serveur ;
2. des numéros de ports élevés sont utilisés aux deux extrémités de la connexion.

Dans la capture précédente, étiez vous en mode actif ou passif ?

Relancer une capture et le transfert du fichier mais en utilisant le client Filezilla.

Quel est le port utilisé par le serveur pour l'échange de données FTP-DATA ?

Quel est le port utilisé par le client pour l'échange de données FTP-DATA ?

Qui du serveur ou du client a établit la connexion pour le transfert des données ?

Les résultats obtenus sont-ils conformes à la description du protocole ftp en mode passif ?