TP Services Internet et Sécurité

(Veuillez reporter vos réponses directement sur ce document)

Nom et Prénom : GUARDIA Quentin
Toutes les images sont personnelles
Délai de remise : Dimanche 18h00 par émail : master2srs.dir@gmail.com

1. COMMANDES SYSTÈMES & RÉSEAUX

1.1 – Quelle commande permet de visualiser l'adresse MAC (Physique) et l'adresse IP (logique) de votre station ?

Je peux trouver l'adresse MAC et l'adresse IP de ma station grâce à la commande ifconfig -a. Mon adresse MAC est b0:10:41:bb:b2:f7 et mon adresse IP 192.168.86.81

```
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.86.81  netmask 255.255.255.0  broadcast 192.168.86.255
        inet6 fe80::727b:f49a:e09c:d628  prefixlen 64  scopeid 0x20<link>
        ether b0:10:41:bb:b2:f7  txqueuelen 1000  (Ethernet)
        RX packets 1616171  bytes 1456157986 (1.4 GB)
```

1.2 – A partir de votre terminal, exécuter la commande « **ping** » avec une station voisine. Quelle commande système permet de visualiser les adresses MAC et IP des hôtes avec lesquelles vous avez échangés des trames ?

```
arp -a
```

1.3 – Sur votre terminal exécuter la commande proposée dans la question précédente 1.2. et reportez le résultat dans la table ci-dessous :

```
_gateway (192.168.86.1) à 70:3a:cb:8b:8c:02 [ether] sur wlp2s0
```

1.4 éditer les fichiers systèmes suivants et expliquer leur fonction :

- Windows\system32\drivers32\etc\hosts
- Windows\system32\drivers32\etc\services
- Windows\system32\drivers32\etc\protocol

- /etc/host/ associe noms d'hôte et adresses IP (comme localhost pour 127.0.0.1)
- /etc/services contient les correspondance entres les applications et les numéros de port qui leurs sont associés, ainsi que la connexion (tcp ou udp) utilisée.

- /etc/protocols donne pour chaque protocole internet DARPA, le numéro officiel de protocole, l'éventuel alias et la description en commentaire.

2. DNS ET TRACEROUTE

2.1 – lancer un navigateur web sur votre terminal et connecter vous sur le site de l'université de Paris. Puis celui de l'université de Berkeley. Quelle est l'adresse IP interne (privée) et externe (publique) de la passerelle locale (gateway) vous permettant d'accéder à ces sites ?

IP privée : 192.168.86.1
IP publique : 90.113.79.110

2.2 – Au moyen de la commande système « nslookup », déterminer l'adresse IP ainsi que le nom symbolique du serveur DNS (Domain Name Service) utilisées par votre terminal pour naviguer sur l'Internet ? Reportez ces informations ci-dessous.

110.79.113.90.in-addr.arpa name = lfbn-mon-1-1386-110.w90-113.abo.wanadoo.fr.

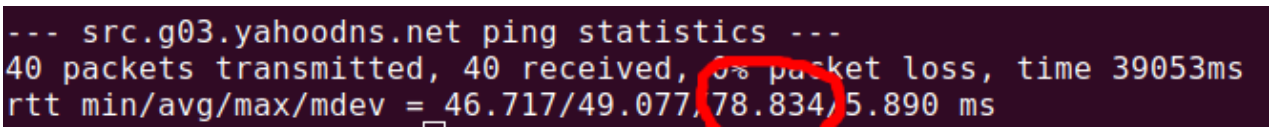
2.3 – A partir de votre terminal, exécuter la commande « traceroute » (linux) ou « tracert (windows) vers la machine www.yahoo.fr

Combien y a-t-il de passerelles sur le chemin entre votre terminal et ce serveur ?

15 passerelles d'après traceroute

Quel est le délai de transmission aller-retour maximum vous séparant de ce serveur ?

78.834ms d'après ping



Au moyen du logiciel Wireshark, déterminer quel protocole et quelle procédure permettent d'obtenir ces informations.

Ping envoie une requête echo par ICMP et chronomètre le temps de réponse

3. TELNET ET SSH (SECURE SHELL)

3.1 – quel est le rôle d'un serveur TELNET ? Est-il opérationnel sur votre PC windows ?

Un serveur Telnet permet qu'un client puisse envoyer des commandes vers la machine grâce à une connexion TCP. Telnet a été delaissé pour SSH car les informations sont transmises en clair. J'utilise Linux, Telnet y est déjà installé et est opérationnel.

3.2 - Quel est le numéro du port du serveur TELNET ?

23

3.3 - Proposer une solution pour vous connecter au serveur telnet au moyen d'un alias de machine « telnetsrv and non plus avec l'adresse IP du serveur.

On rajoute danc /etc/hosts une ligne contenant l'adresse IP concernée et l'alias « telnetsrv »

3.4 – installer et configurer le serveur SSH avec le compte « guest ». Associer ce compte avec le home directory « C:\Documents and Settings\GUEST\Mes documents ».

Dans une invite de commandes, connectez vous au serveur SSH de votre voisin avec le compte « guest » a moyen de la commande « ssh guest@ip_serveur_ssh ». Après connexion, lancer la commande « dir ».

3.7 - Quel est le numéro du port du serveur SSH ?

22

3.8 – Pouvez vous retrouvez votre login et mot de passe, ainsi que le résultat de votre commande « dir »?

Non, d'après Wireshark, les paquets sont chiffrés (encrypted)

3.9 – Expliquer le rôle de ce protocole SSH ?

SSH permet un échange sécurisé (chiffré) entre un client et un serveur en utilisant TCP/IP. Contrairement à Telnet, des clés de chiffrement sont échangées en début de connexion.

4. FTP : File Transfer Protocol, et FTPS (FTP Securise)

4.1 – Installer et configurer sur votre terminal le serveur FTP sans créer de compte utilisateur particulier (utiliser le nom de domaine « ftp.monsite.com ».

4.2 – Est il possible de ce connecter au serveur FTP à partir du compte « anonymous » (login : anonymous ; et mot de passe : email@email.fr). et de télécharger le fichier RFC959.txt ? Capturez les trames échangées avec le logiciel Wireshark.

C'est possible, sous VsFTPd il suffit de configurer correctement /etc/vsftpd.conf en ajoutant des autorisations, telles que :

anonymous_enable=YES

anon_upload_enable=YES

anon_mkdir_write_enable=YES

Et en octroyant les droits nécessaires au dossier racine du serveur

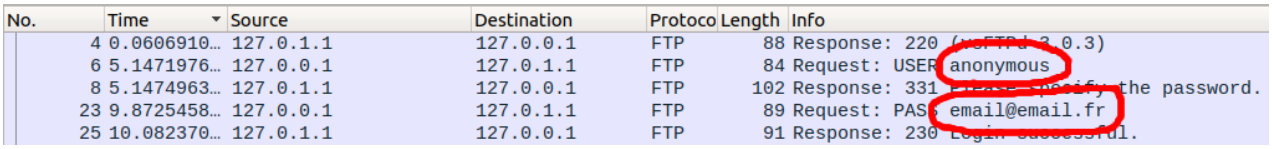
4.3 – Quel est le numéro du port du serveur FTP qui permet l'envoi des commandes FTP ?

21

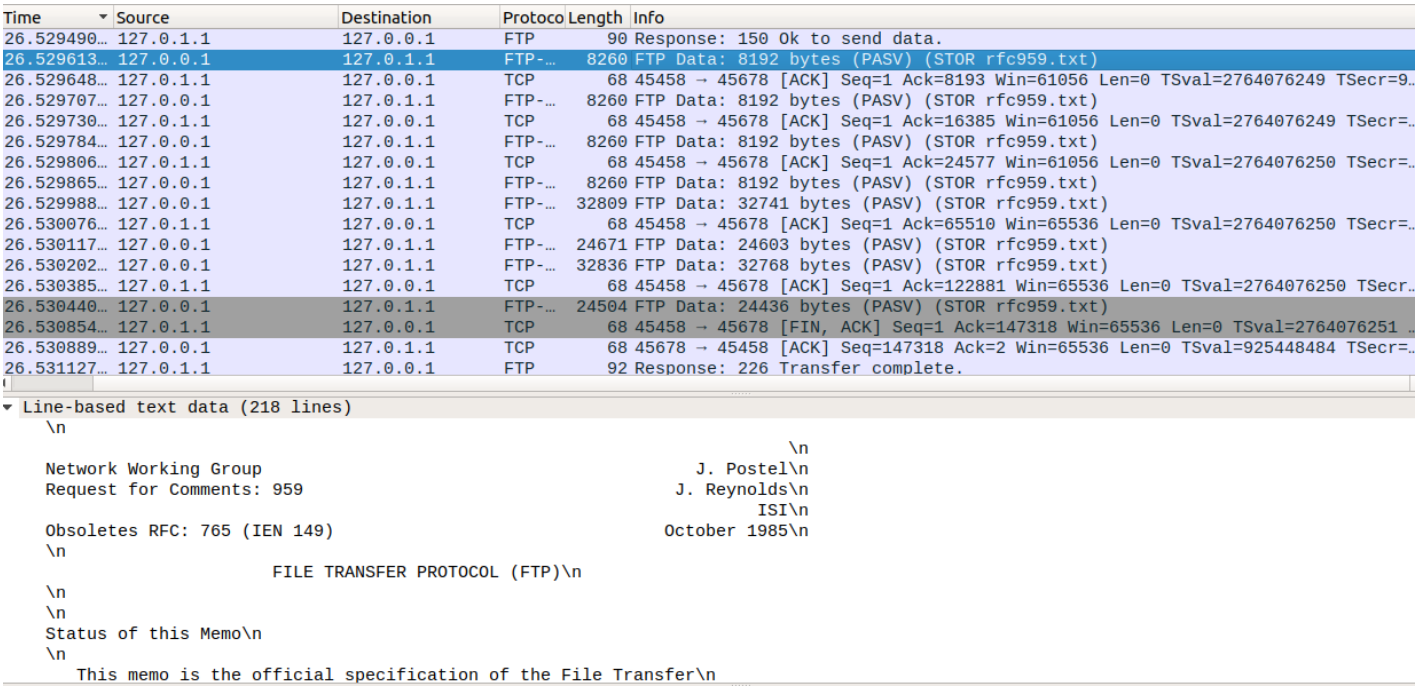
4.4 – Quel est le numéro du port du serveur FTP qui permet l'envoi des données (fichiers) FTP ?

20

4.5 – est il possible de récupérer votre login et password ? Si oui faites une capture d'écran de wireshark et insérer là ci-dessous.



4.6 – est il possible de récupérer le contenu du fichier RFC959.txt ? Si oui faites une capture d'écran de wireshark et insérer là ci-dessous.



4.7 – Pour sécuriser le serveur FTP ainsi que les transferts de fichiers, on vous propose d'appliquer les règles de configurations suivantes :

- Désactiver le compte utilisateur « anonymous »
- Créer un compte guest avec login : guest et mot de passe : guest.

- Limiter l'accès au serveur FTP avec ce compte à partir de votre poste terminal en spécifiant son adresse IP.
- Limiter le nombre de connexions simultanées à partir de ce compte à 2.
- Forcer la connexion au serveur en mode sécurisé avec le protocole SSL (Secure Socket Layer) FTPS (FTP over SSL) en utilisant comme nom de serveur « ftps://adresse_ip_serveur »
- Associer à cet utilisateur un home directory en lecture seule, et y copier le fichier RFC959.txt
- Limiter le débit binaire de téléchargement à 300 Ko/s

4.8 – Quel est le numéro du port du serveur FTPS qui permet l'envoi des commandes ?

990

4.9 – Quel est le numéro du port du serveur FTPS qui permet l'envoi des données (fichiers)?

989

4.10 –Avez-vous la possibilité de capturer le login et mot de passe de « guest » lors de ce transfert de fichier en mode FTPS (FTP over SSL) ?

Non, les commandes, et donc login et mot de passe sont chiffrés. Cependant, comme tout est fait en local, j'ai accès à la clé privée RSA et au certificat, qui sont définis dans /etc/vsftpd.conf :

- rsa_cert_file=/etc/ssl/private/vsftpd.pem
- rsa_private_key_file=/etc/ssl/private/vsftpd.pem

Je peux accéder au fichier susmentionné en root, afin de récupérer la clé définie dans la première partie du fichier. J'ai suivi une procédure proposée sur le site de Wireshark mais j'aboutis à cette erreur dans les logs :

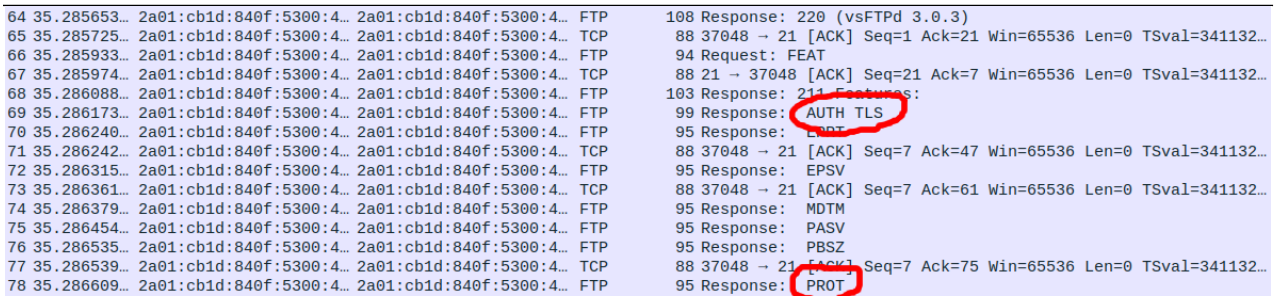
- tls13_load_secret Cannot find CLIENT_HANDSHAKE_TRAFFIC_SECRET, decryption impossible
- tls13_load_secret Cannot find SERVER_HANDSHAKE_TRAFFIC_SECRET, decryption impossible

Erreur que je n'arrive à résoudre par manque de connaissance. Donc je dois avoir la possibilité de voir les identifiants, mais ils sont chiffrés par défaut.

4.11 –Avez-vous la possibilité de capturer et de visualiser le contenu du fichier RFC791.txt en mode FTPS (FTP over SSL) ?

Les données sont chiffrés, je ne peux pas visualiser le contenu du fichier RFC791.txt

Afin de corroborer mes propos, voici une capture de Wireshark qui montre que l'AUTH TSL qui indique le début de chiffrement des commandes arrive avant l'échange d'identifiants et que PROT qui initie le chiffrement des données arrive avant l'envoie du fichier RFC791.txt.



5. SFTP vs FTPS

5.1 – installez le client Filezilla et effectuer les tests de connexion sur les serveurs SSH, FTP et FTPS.

5.2 – Expliquer les différences entre les protocoles SFTP et FTPS :

D'après le RFC4217, FTPS est le protocole FTP sécurisé par SSL, c'est-à-dire qu'en se connectant, le client peut faire confiance au serveur grâce au certificat d'authentification de ce dernier. De plus les échanges de commandes et/ou de données sont chiffrées. Ainsi deux canaux peuvent s'avérer nécessaires : un pour les commandes et un pour les données.

SFTP est une extension de SSH permettant au client de manipuler les fichiers du serveur avec la sécurité apportée par SSH. Ainsi c'est le port TCP 22 qui est utilisé, et non 21 comme FTPS et FTP.