**Compte Rendu d’Activité**

**1. Installation et Configuration d’Apache**

**Téléchargement et Installation d’Apache** :

sudo apt update

sudo apt install apache2

**Création des Sites Physiques** :

* **SITE1** :
* mkdir -p /var/www/html/SITE1
* nano /var/www/html/SITE1/index.html

Contenu de index.html :

<html>

<body>

<h1> BIENVENUE SUR LA SOCIETE 1 </h1>

</body>

</html>

* **SITE2** :
* mkdir -p /var/www/html/SITE2
* nano /var/www/html/SITE2/index.html

Contenu de index.html :

<html>

<body>

<h1> BIENVENUE SUR LA SOCIETE 2 </h1>

</body>

</html>

**Configuration des Sites dans Apache** :

* Copie du contenu du fichier /etc/apache2/sites-available/000-default.conf pour créer deux nouveaux fichiers de configuration :
* sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/societe1.conf
* sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/societe2.conf
* Modification des fichiers de configuration :
  + **societe1.conf** :
  + DocumentRoot /var/www/html/SITE1
  + **societe2.conf** :
  + DocumentRoot /var/www/html/SITE2
* Activation des sites :
* sudo a2ensite societe1.conf
* sudo a2ensite societe2.conf
* sudo systemctl reload apache2

**2. Activation du SSL**

**Installation d’OpenSSL** :

sudo apt-get update

sudo apt-get install openssl

**Génération des Certificats SSL** :

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key

**Configuration du SSL dans Apache** :

* Création et modification du fichier /etc/apache2/sites-available/default-ssl.conf :
* <IfModule mod\_ssl.c>
* <VirtualHost \_default\_:443>
* ServerAdmin webmaster@localhost
* DocumentRoot /var/www/html
* SSLEngine on
* SSLCertificateFile /etc/apache2/server.crt
* SSLCertificateKeyFile /etc/apache2/server.key
* ErrorLog ${APACHE\_LOG\_DIR}/error.log
* CustomLog ${APACHE\_LOG\_DIR}/access.log combined
* </VirtualHost>
* </IfModule>
* Activation du module SSL et du site SSL :
* sudo a2enmod ssl
* sudo a2ensite default-ssl
* sudo systemctl reload apache2

**3. Configuration de ProFTPD pour FTPS**

**Installation de ProFTPD** :

sudo apt install proftpd

**Configuration de ProFTPD pour FTPS** :

* Modification du fichier de configuration principal :
* sudo nano /etc/proftpd/proftpd.conf

Ajout des lignes suivantes :

<IfModule mod\_tls.c>

TLSEngine on

TLSLog /var/log/proftpd/tls.log

TLSProtocol SSLv23

TLSRSACertificateFile /etc/ssl/certs/proftpd.crt

TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key

TLSOptions NoCertRequest

TLSVerifyClient off

TLSRequired on

</IfModule>

**Génération des Certificats SSL pour ProFTPD** :

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt

**Redémarrage de ProFTPD** :

sudo systemctl restart proftpd

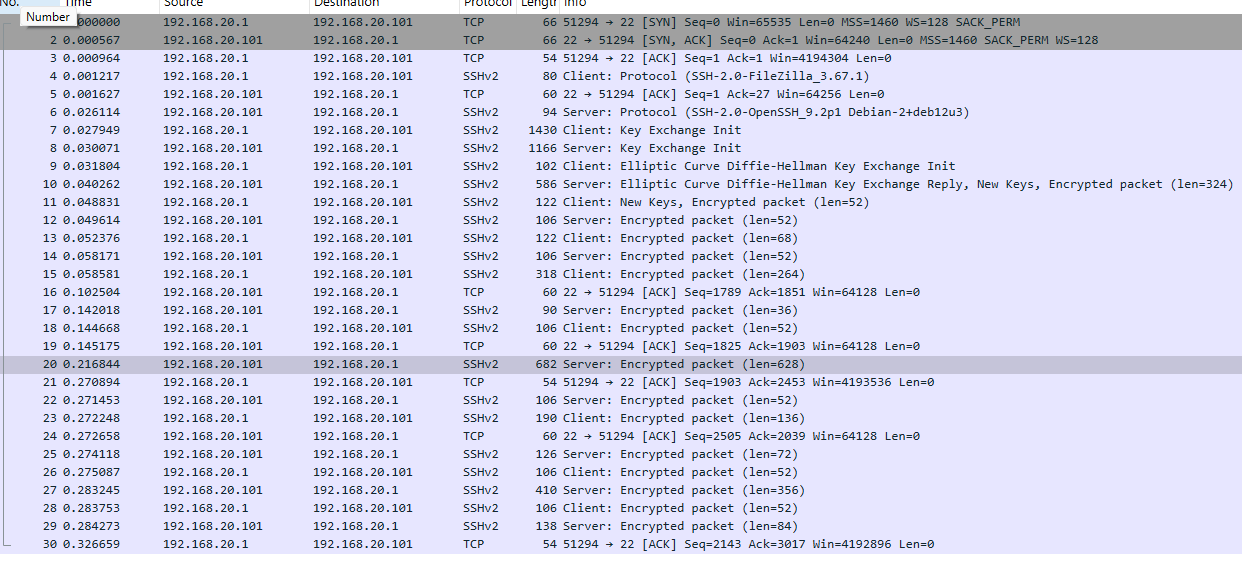
**Test de la Connexion FTPS** :

* Utilisation d’un client FTP comme FileZilla pour tester la connexion FTPS :
  + Configuration d’une nouvelle connexion avec l’adresse du serveur, le nom d’utilisateur et le mot de passe FTP.
  + Sélection de FTPS comme protocole.
  + Connexion et acceptation du certificat SSL si demandé.

**4. Vérification de la Sécurité avec Wireshark**

* Capture du trafic réseau avec Wireshark pour vérifier que les mots de passe sont cryptés lors de la connexion FTPS.

Voici un exemple de ma trame crypter en ftps



Voici un exemple de ma trame non crypter en ftp

