Mission 7 : Utilisation des protocoles SSL/TLS

EXPLICATION : QU'EST CE QUE C'EST EXACTEMENT

SSL (Secure Sockets Layer) et son successeur TLS (Transport Layer Security) sont des protocoles de chiffrement qui sécurisent les communications sur Internet. Ils assurent :
 Confidentialité (chiffrement des données)
 Intégrité (prévention des altérations)
 Authentification (vérification des identités via des certificats)

CERTIFICAT SSL/TLS ?

Un certificat SSL est un certificat numérique qui assure l'authenticité d'un site Web.

COMPOSITION D'UN CERTIFICAT SSL/TLS

Qu'est ce nous pouvons retrouver dans un certificat ? :

- Un FQDN (non de domaine)
- Une clé publique du serveur
- Une date d'expiration
- Le nom de l'AC(autorité de certification)
- La signature numérique de l'AC

PARTIE A : Analyse des trames

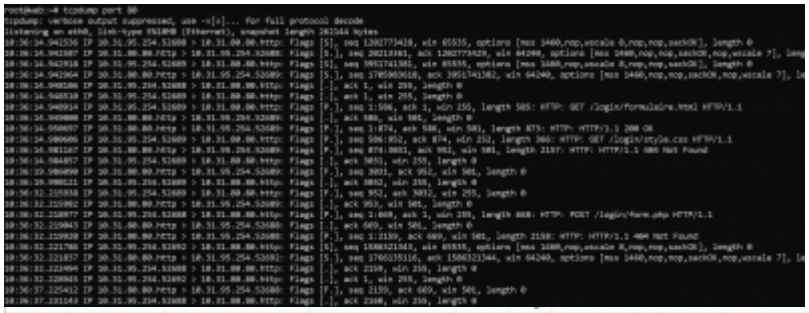
Après avoir télécharger le formulaire html sur le ENT pour le déposer dans le serveur , nous devons nous rendre dans le répertoire **/home/htdocs/m2l.org/www** et créer un dossier **Login** dans lequel nous allons mettre les fichiers de formulaire (html,php,css).

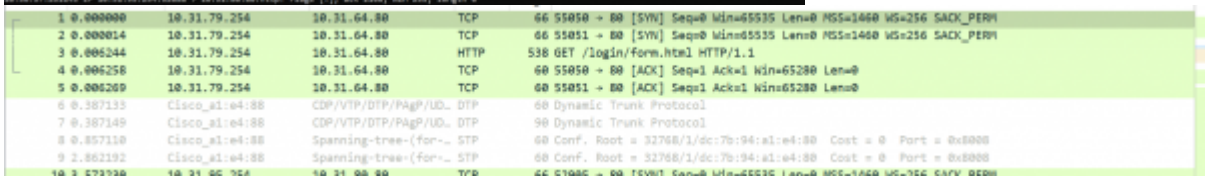
Capture de trames

Sur le serveur avec tcpdump ou sur votre machine avec wireshark, nous devons réaliser une capture de trame de l’échange HTTP entre notre machine et le serveur lorsque nous chargeons et soumettons le formulaire de login dans notre navigateur.
En ligne de commande avec **tcpdump** :

```
tcpdump -w capture.pcap
```

Le fichier **capture.cap** est enregistré dans le serveur et nous pouvons aussi voir le nombre de paquets capturés après avoir saisi la commande .





PARTIE B: HTTPS

I.Création et utilisation d'un certificat auto-signé

Dans cette partie , nous devons créer un certificat auto-signé en installant OpenSSL et créer un répertoire pour les certificats dans le serveur Web. Avec les commandes suivantes :

```
apt-get install openssl
mkdir /etc/ssl/localcerts # /etc et /ssl existent déjà
```

1. Création De La Clé

```
root@web:~# DIR=/etc/ssl/localcerts
root@web:~# openssl req -x509 -newkey rsa:4096 -nodes -keyout
$DIR/mydomainkey.key -out $DIR/mydomaincert.pem -days 365
```

- newkey rsa:4096 : Pour une clé RSA de 4096 bits
- keyout : La clef
- out : Le certificat
- nodes : Pas de passphrase lors de l'utilisation pour le déverrouiller
- days 365 : la durée de validité du certificat

Il faut créer la clé dans le répertoire /etc/ssl/localcerts

1.1 Illustration de la création d'un Certificat

1.2Activation du Vhost SSL par défaut

Nous devons activer le Vhost pour apache2 et le configurer, avec la commande suivante :

```
root@web:~# a2ensite default-ssl
```

1.3 Activation du module ssl pour Apache

```
root@web:~# a2enmod ssl
```

II.Modifications à Effectuer sur le Vhost

1.Modification sur le Vhost par défaut SSL

Le chemin du fichier :**/etc/apache2/sites-available/default-ssl.conf** . Nous devons entrer dans le fichier et rajouter les deux directives :

```
  SSLCertificateFile      /etc/ssl/localcerts/mydomaincert.pem
  SSLCertificateKeyFile   /etc/ssl/localcerts/mydomainkey.key
```

2.Vérification du Port

```
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      178/sshd: /usr/sbir
tcp6       0      0 ::1:25                  :::*                    LISTEN      89161/exim4
tcp6       0      0 :::10000                :::*                    LISTEN      283/perl
tcp6       0      0 :::443                  :::*                    LISTEN      406248/apache2
```

3.Test Avec Le Navigateur

Ici nous devons tester avec le **https** (www, intranet,extranet ect) de nos sites , et y accéder malgré l'interdiction

Cette erreur veut tout simplement dire que la page dans laquelle nous voulons nous rendre a un certificat.

III)Petit Changement dans le VirtualHost de chaque fichier intranet,extranet , www ...

Afin que nos sites soient en **https** nous devons copier le contenu de la configuration de chaque Vhost , puis coller tout en bas et modifier le port en mettant **443** à la place de **80** et rajouter les 2 deux directives des clés générés pendant la création du certificat.

1) Modification dans le VirtualHost www

```
<VirtualHost *:443>
        ServerAdmin ns1master@m2l.org
        ServerName m2l.org
        ServerAlias www.m2l.org

        DocumentRoot /home/htdocs/m2l.org/www/

        ErrorLog /var/log/apache2/www-error.log
        CustomLog /var/log/apache2/www-access.log combined

         SSLCertificateFile /etc/ssl/localcerts/mydomaincert.pem
         SSLCertificateKeyFile /etc/ssl/localcerts/mydomainkey.key

        <Directory /home/htdocs/m2l.org/www/>
                AllowOverride All
                Require all granted
        </Directory>
</VirtualHost>
```

2) Modification dans le VirtualHost intranet

```
<VirtualHost *:443>
     ServerAdmin vhanndanielle@gmail.com
     ServerName m2l.org
     ServerAlias intranet.m2l.org

     DocumentRoot /home/htdocs/m2l.org/intranet/
     ErrorLog /var/log/apache2/intranet-error.log

     CustomLog /var/log/apache2/intranet-access.log combined

    SSLCertificateFile /etc/ssl/localcerts/mydomaincert.pem
    SSLCertificateKeyFile /etc/ssl/localcerts/mydomainkey.key

   <Directory /home/htdocs/m2l.org/intranet/>
         Require all granted
         AllowOverride All
```

```
      </Directory>
</VirtualHost>
```

3) Modification dans le VirtualHost extranet

```
  <VirtualHost *:443>
     ServerAdmin vhanndanielle@gmail.com
     ServerName m2l.org
     ServerAlias extranet.m2l.org

     DocumentRoot /home/htdocs/m2l.org/extranet/
     ErrorLog /var/log/apache2/extranet-error.log

     CustomLog /var/log/apache2/extranet-access.log combined

    SSLCertificateFile /etc/ssl/localcerts/mydomaincert.pem
    SSLCertificateKeyFile /etc/ssl/localcerts/mydomainkey.key

   <Directory /home/htdocs/m2l.org/extranet/>
         Require all granted
          AllowOverride All
      </Directory>
</VirtualHost>
```

4) Modification dans le VirtualHost wiki

```
   <VirtualHost *:443>
     ServerAdmin vhanndanielle@gmail.com
     ServerName m2l.org
     ServerAlias wiki.m2l.org

     DocumentRoot /home/htdocs/m2l.org/wiki
     ErrorLog /var/log/apache2/wiki-error.log

     CustomLog /var/log/apache2/wiki-access.log combined

    SSLCertificateFile /etc/ssl/localcerts/mydomaincert.pem
    SSLCertificateKeyFile /etc/ssl/localcerts/mydomainkey.key

   <Directory /home/htdocs/m2l.org/wiki>
         AllowOverride All
         Require all granted
      </Directory>
</VirtualHost>
```

PARTIE C: FTPS

Dans cette partie nous allons chiffrer notre connexion FTP en FTPS grâce au protocole TLS(Transport Layer Security), afin que nos données ne circulent pas en clair.Nous avions déjà Installer **Open-SSl** avec la commande :
NB: Ceci se fait dans les serveur ftp1 et 2.

```
  apt-get install openssl
```

I)Créer un certificat pour proftpd

1) Création du répertoire pour stocker le certificat et la clé

```
root@ftp1:~# mkdir /etc/proftpd/ssl/
```

2) Génération du certificat SSL auto-signé et de la clé

```
root@ftp1:~# DIR=/etc/proftpd/ssl/ # dossier dans lequel se trouve le certificat et la clé
root@ftp1:~# openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/mydomainkey.key -out $DIR/mydomaincert.pem -days 365
```

3) Déclaration d'un Elément dans le fichier proftpd.conf

Nous devons éditer le fichier /etc/proftpd/proftpd.conf et activer TLS en décommentant une ligne :

```
Include /etc/proftpd/tls.conf
```

4) Configuration du fichier tls.conf

Notre but est d'éditer le fichier /etc/proftpd/tls.conf et paramétrer au minimum quelques directives :

```
   TLSEngine               on
   TLSLog                  /var/log/proftpd/tls.log

   TLSRSACertificateFile           /etc/proftpd/ssl/mydomaincert.pem
   TLSRSACertificateKeyFile        /etc/proftpd/ssl/mydomainkey.key

   TLSOptions      AllowClientRenegotiations NoSessionReuseRequired
```

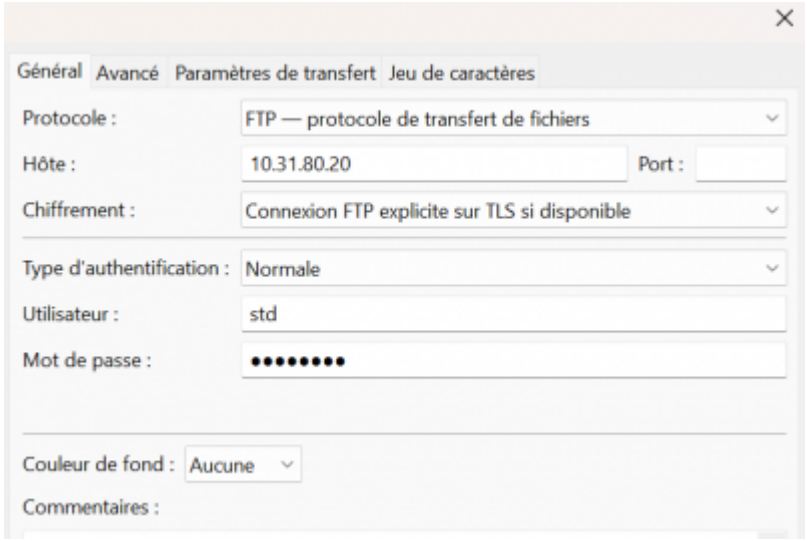
5)Modification dans le fichier modules.conf

Nous devons décommenter la ligne suivante et prêter attention au commentaire du dessus :

```
# Install proftpd-mod-crypto to use this module for TLS/SSL support.
LoadModule mod_tls.c
```

Par la suite nous devons Installer **proftpd-mod-crypto** avec la commande **apt-get install** .
Toujours redémarrer **proftpd** après modification ou configuration d'un fichier (systemctl restart proftpd).

II) Test Avec Un Client FileZilla



a) Illustration du Certificat