Aller au contenu

SSL / TLS

♦ Premièrement, installation d'openssl :

```
1 apt-get install openssl
```

♦ Ensuite on créer le répertoire

```
1 mkdir /etc/ssl/localcerts
```

♦ Pour continuer on a créer un certificat :

```
1 root@http-pub:~# openssl req -new -x509 -sha256 -days 365 -nodes -out /etc/ssl/localcerts/gsb.crt -keyo
```

♦ Explications :

```
- REQ permet de créer et traiter les demandes de certificats.
- NEW permet de générer la demande de certificat.
- NODES désactive le chiffrement de la clé privé.
- KEYOUT donne le nom ou le fichier ou la clé privée sera crée.
- OUT nom du fichier de sortie (cela correspond au certificat).
- DAYS nombre de jour ou le certificat est valide.
```

- On obtient ça :

```
-----BEGIN CERTIFICATE-----
MIIDrTCCApWgAwIBAgIUcxA7R0jZ8tLarCVxfuvrnhNM1mswDQYJKoZIhvcNAQEL
BQAwZjELMAkGA1UEBhMCRlIxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEfMB0GCSqGSIb3DQEJARYQYWRtaW5n
QGdtYWlsLmNvbTAeFw0yMTExMDkxMDE5NDRaFw0yMjExMDkxMDE5NDRaMGYxCzAJ
BgNVBAYTAkZSMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5l
dCBXaWRnaXRzIFB0eSBMdGQxHzAdBgkqhkiG9w0BCQEWEGFkbWluZ0BnbWFpbC5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDPrHI7zDe0IPKktWd+
l4xUkzEbVQkk/L76nZsh3XGrtNePZqyrS/SHtt5eNDS97ZzhNWUO5lfgj9Nn+/M0
uo1e8qsg6vpVRUWs/bInydGJhvKdY7zgrONFLvpRbCH66B2pq4F8cDsoKX4jjx6h
SCMRXUWMuhd9V5mKesY9RusYNX4LMX2dBvEKsg5Cm08Ykc8sAd4NHs1Kfdx2hoBR
AsZHmKYLi+/d9fi4NzSNsxEZmsp1gckCNAQZ11cTMdkYTIqLvHLMmW9zKydWHUbW
3OUJa1Fh6kgXPjDEmfPWnsByGxorsrHYVK/Pyn8+v7784b6uv4u3I/E1GoUmgzrc
Pu9bAgMBAAGjUzBRMB0GA1UdDgQWBBQklIgFgSkE+pehluAcDNjY86wxXjAfBgNV
HSMEGDAWgBQklIgFgSkE+pehluAcDNjY86wxXjAPBgNVHRMBAf8EBTADAQH/MA0G
CSqGSIb3DQEBCwUAA4IBAQB3PGlYP0kvFu4oOcVuxbeulabm6UJxmJ6TDyQFR+Ev
Inujzg0KoiIsEZobSe/fwAMSsNWCtcCoz6ZML3DV1vS0o5ilr7Y4Dao+yXI5je4W
nr4MDQiIPxgrmSMwz0M3GubKRaXDI40XZ4TfRHHbOCXD7OAwklXXpbtibZyDXhe4
BAhRc7GNJqQCCFYc/h6ZqPB8xiyW3wBrtnub/WAqbLLu5SxOMeKKA092RKyV7g2n
irqT8objco/yMHLsh+akAv0QE8Xx/hkf5hdm2Tc9B91dciFinAaw7usH/IeVpH3c
MWMb6SgxcIN7QF7JYSSi/nPXxxf1xiLzKi3MFTTZDvNn
-----END CERTIFICATE-----
```

- Cette clé va être stocké dans /etc/ssl/localcerts/

- Vérification :

```
root@http-pub:/etc/ssl/localcerts# ls
gsb.crt  gsb.key.org
```

Adaptation des Vhosts et de la configuration d'Apache

- Pour chaque VirtualHost il a fallut les modifier de la sorte :

```
<VirtualHost *:443>
        DocumentRoot /home/htdocs/afrique.gsb.org/www/wiki
        ServerName doc.afrique.gsb.org
        ServerAlias wiki.afrique.gsb.org

# Autres directives ici
        <Directory /home/htdocs/afrique.gsb.org/www/wiki>
                Require all granted
        </Directory>
# Fichier de log
        ErrorLog /var/log/apache2/www-error.log
        CustomLog /var/log/apache2/www-access.log combined


        ServerAdmin webmaster@gsb.org

SSLCertificateFile /etc/ssl/localcerts/gsb.crt
SSLCertificateKeyFile /etc/ssl/localcerts/gsb.key.org


```

```
21 </VirtualHost>
```

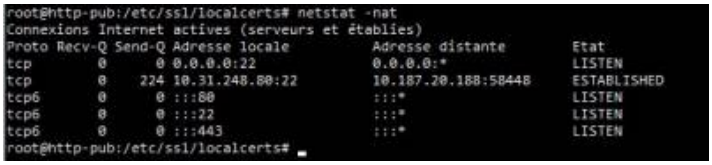
Il faut penser à laisser l'ancien virtualHost c'est-à-dire qu'il faut rajouter ce bloc en ★**dessous**★.

♦ Quand c'est fait on fait **a2enmod ssl**.

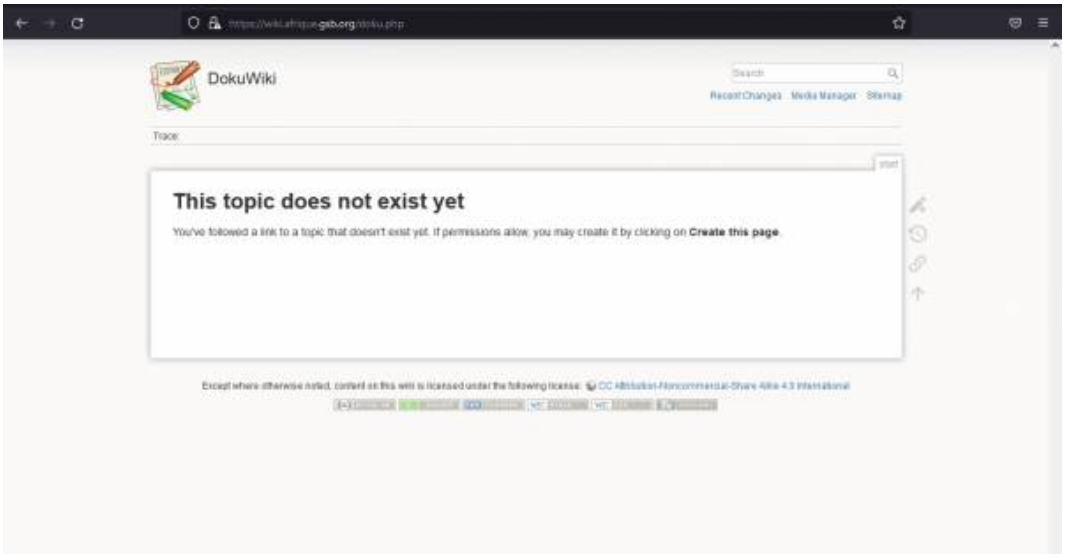
> La commande a2enmod permet d' **activer** un module.

♦ On redémarre avec **systemctl restart apache2**.

♦ On test avec **netstat -nat**.



Test



TLS over FTP avec ProFTPD

- Il faut aller dans le dossier /etc/proftpd/

```
1 cd /etc/proftpd
```

- Création du dossier SSL

```
1 mkdir ssl
```

- Se déplacer dans le dossier

```
1 cd ssl
```

♦ Génération du certificat ssl auto-signé et la clé :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -out proftpd-rsa.pem -keyout proftpd-key.pem
```

♦ Puis protéger la clé

```
chmod 440 proftpd-key.pem
```

Chmod 440 correspond à :

	Owner Rights (u)	Group Rights (g)	Others Rights (o)
Read (4)	☑	☑	☐
Write (2)	☐	☐	☐
Execute (1)	☐	☐	☐

♦ Éditer le fichier /etc/proftpd/proftpd.conf et activer TLS en décommentant la ligne :

```
# This is used for FTPS connections
Include /etc/proftpd/tls.conf
```

♦ Éditer le fichier /etc/proftpd/tls.conf

```
<IfModule mod_tls.c>
#
TLSEngine on
TLSLog /var/log/proftpd/tls.log
```

```
TLSProtocol SSLv23
#
TLSRSACertificateFile /etc/proftpd/ssl/proftpd-rsa.pem
TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd-key.pem
#
TLSRequired on
TLSRenegotiate required off
</IfModule>
```

♦ Se déplacer dans /etc/proftpd/modules.conf :

→ Et décommenter la deuxième ligne ci-dessous

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

♦ Installer proftpd-mod-crypto :

```
apt-get install proftpd-mod-crypto
```

♦ Il faut redémarrer proftpd :

```
/etc/init.d/proftpd restart
```

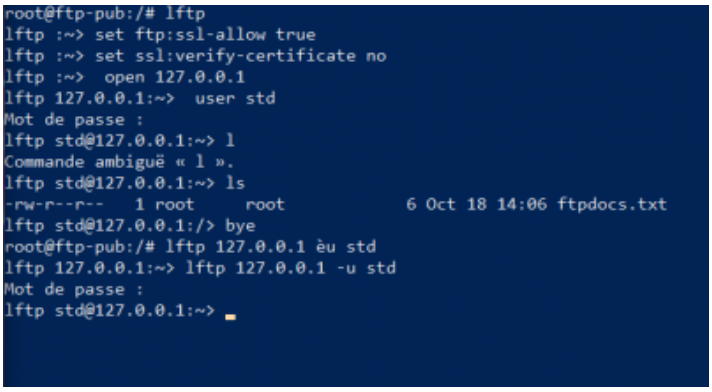
```
root@ftp-pub:/# systemctl restart proftpd
root@ftp-pub:/#
```

Tester le serveur avec un client en mode commande :

♦ Installation de LFTP :

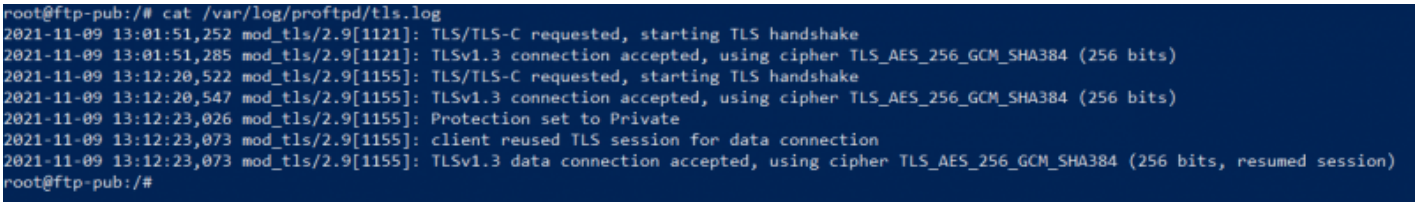
```
apt install lftp
```

Test en mode interactif :



Avec filezilla :

♦ Voici les logs afficher dans /var/log/proftpd/tls.log après s'être connecté sur le serveur avec filezilla :



♦ Voici le certificat après s'être connecté sur le serveur avec filezilla :

Capture de trames

Pour commencer on install tcpdump :

```
apt-get install tcpdump
```

Commande pour lancer une capture de trame :

```
sudo tcpdump -n -i enp1s0 -s0 port 21 -w (nom).pcap
```

Il faut se connecter au serveur sur filezilla et actualiser pour avoir la trame.

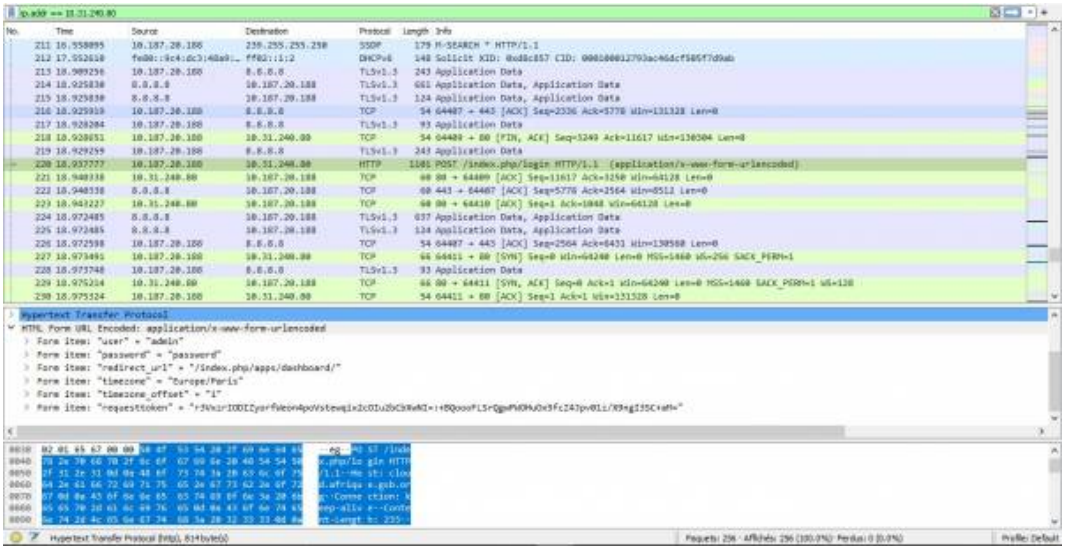
Réponse du serveur après avoir lancé une analyse TLS :

```
root@ftp-pub:~# tcpdump -n -i enp1s0 -X -s0 port 21 -w tcp.pcap
tcpdump: listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C38 packets captured
38 packets received by filter
0 packets dropped by kernel
```

Réponse du serveur après avoir lancé une analyse sans TLS (ne pas oublier se connecter sur filezilla sans utiliser TLS):

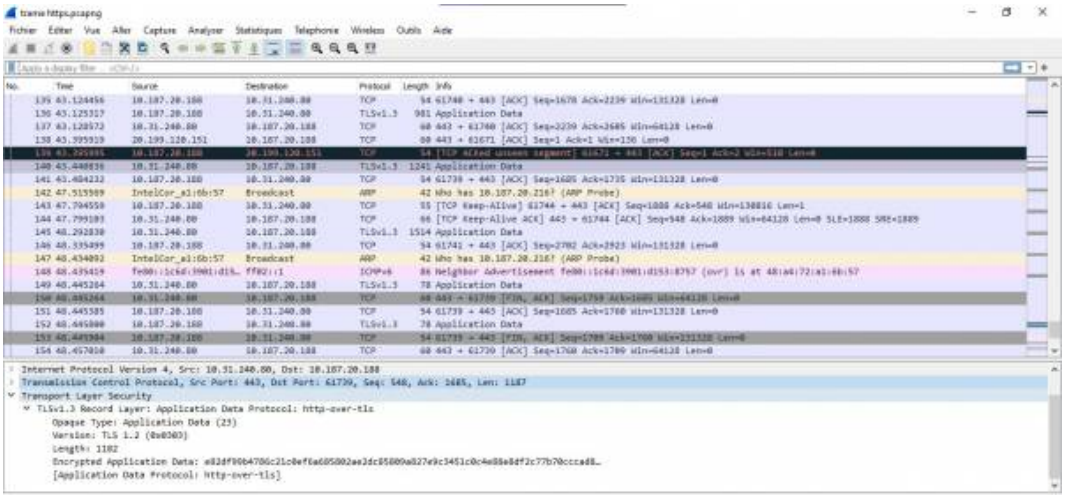
```
root@ftp-pub:/home/ftpdocs# tcpdump -n -i enp1s0 -X -s0 port 21 -w tcp2.pcap
tcpdump: listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C119 packets captured
119 packets received by filter
0 packets dropped by kernel
```

Voici, sur Wireshark l'analyse d'une trame HTTP :



On peut voir ici que l'identifiant et le mot de passe sont en clair.

Voici, sur Wireshark l'analyse d'une trame HTTPS :



On voit ici la ligne Encrypted Application qui nous indique que tout à été chiffré.

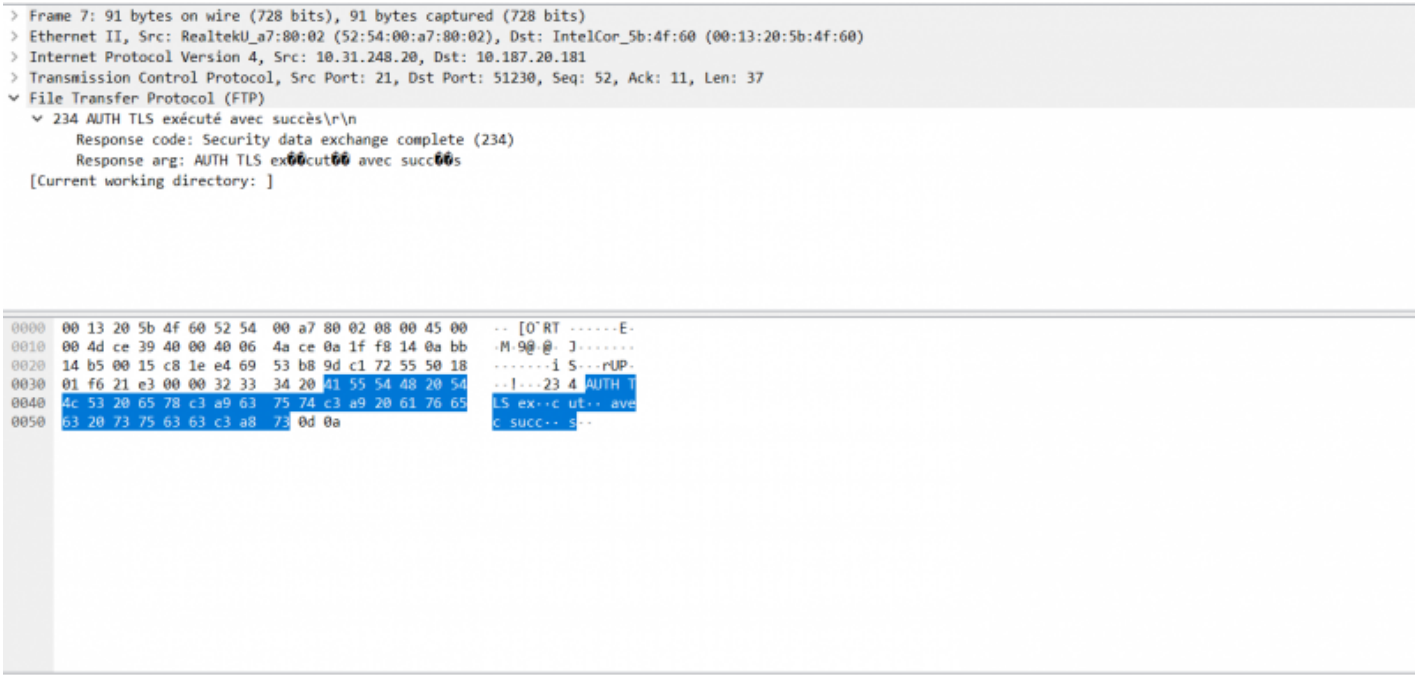
Commande pour lancer une capture de trame :

```
sudo tcpdump -n -i lo -X -s0 port 21 -w (nom).pcap
```

Il faut se connecter au serveur sur filezilla et actualiser pour avoir la trame.

Il faut vérifier que la connexion sur filezilla utilise TLS

Réponse du serveur après avoir lancé une analyse TLS :



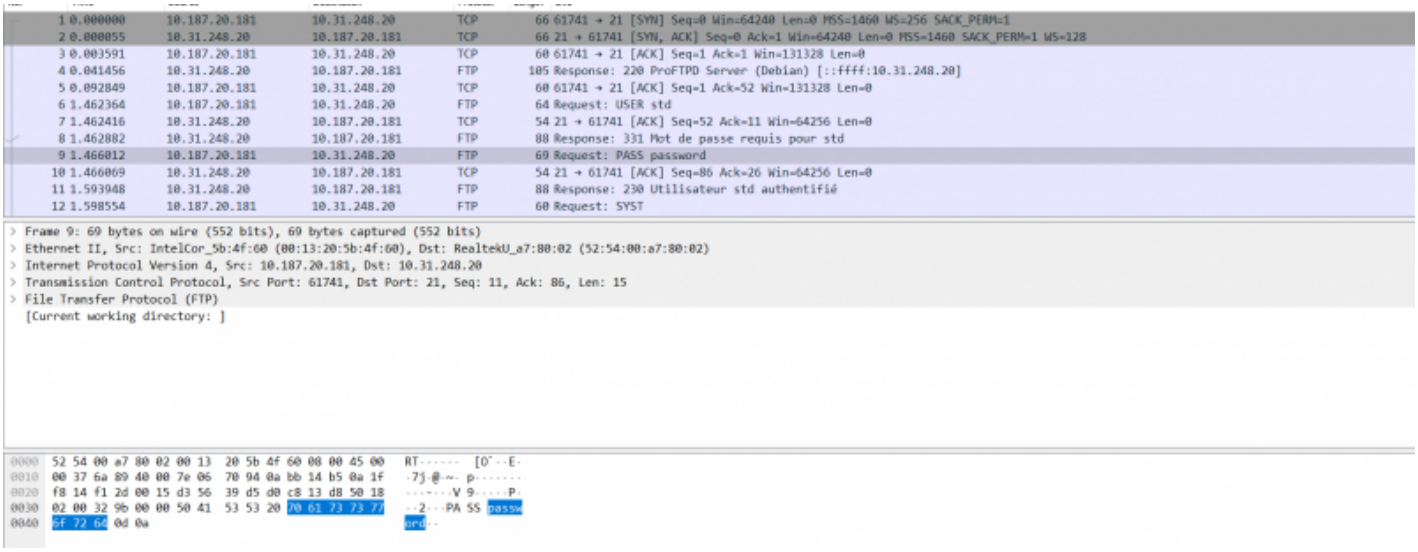
Commande pour lancer une capture de trame :

```
sudo tcpdump -n -i lo -s0 port 21 -w (nom).pcap
```

Il faut se connecter au serveur sur filezilla et actualiser pour avoir la trame.

> Il faut vérifier que la connexion sur filezilla n'utilise pas TLS

Réponse du serveur après avoir lancé une analyse TLS :



On peut voir ici que l'identifiant et le mot de passe sont en clair.