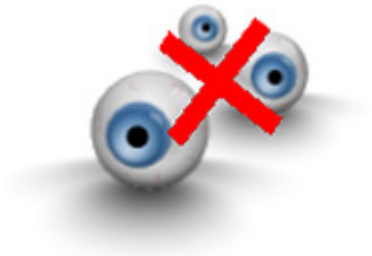
2.8.- Acceso seguro mediante TLS.



rfc (CC BY-NC-SA)

Para habilitar el acceso al servidor proftpd usando TLS (SSL) de debe proceder como sigue:

Primero habrá que instalar el módulo tls que nos va a proporcionar la capa de seguridad sobre la que van a enviarse las comunicaciones del protocolo FTP:

```
$ sudo apt install proftpd-mod-crypto
```

Después debemos habilitar el módulo tls, descomentando la siguiente línea del fichero **modules.conf** en el directorio **/etc/proftpd**:

```
LoadModule mod_tls.c
```

Edita el archivo **/etc/proftpd/proftpd.conf** y descomenta la línea:

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

Crea las claves, pública y privada, para la conexión cifrada:

- Método 1: Instalación del paquete OpenSSL y ejecución del comando openssl.

```
$ sudo apt-get install openssl
$ sudo openssl req -x509 -newkey rsa:1024 -keyout /etc/ssl/private/proftpd.key -o
 /etc/ssl/certs/proftpd.crt -nodes -days 3650
Generating a 1024 bit RSA private key
..++++++
.............................++++++
writing new private key to '/etc/ssl/private/proftpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []: Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DAWD
Organizational Unit Name (eg, section) []: DAW
Common Name (eg, YOUR name) []: ftp.dawdistancia.net
Email Address []: dawd@dawdistancia.net
```

- Método 2: Comando **proftpd-gencert**. Los dos comandos anteriores se resumen en uno, con la salvedad que el certificado será válido solamente durante 1 año y no 10:

```
$ proftpd-gencert
```

Modifica los permisos:

```
$ sudo chmod 0600 /etc/ssl/private/proftpd.key
$ sudo chmod 0644 /etc/ssl/certs/proftpd.crt
```

Modifica el fichero **/etc/proftpd/tls.conf** para que tenga el siguiente contenido:

```
##############################################Fichero /etc/proftpd/tls.conf###############
#
# Proftpd sample configuration for FTPS connections.
#
# Note that FTPS impose some limitations in NAT traversing.
# See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
# for more information.
#

<IfModule mod_tls.c>
TLSEngine                               on
TLSLog                                  /var/log/proftpd/tls.log
TLSProtocol                             SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
#          -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
#          -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
```

```
# chmod 0644 /etc/ssl/certs/proftpd.crt
#
TLSRSACertificateFile                   /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile                /etc/ssl/private/proftpd.key
#
# CA the server trusts
#TLSCACertificateFile            /etc/ssl/certs/CA.pem
# or avoid CA cert
TLSOptions                              NoCertRequest
#
# Authenticate clients that want to use FTP over TLS?
#
TLSVerifyClient                         off
#
# Are clients required to use FTP over TLS when talking to this server?
#
TLSRequired                             on
#
# Allow SSL/TLS renegotiations when the client requests them, but
# do not force the renegotations.  Some clients do not support
# SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
# clients will close the data connection, or there will be a timeout
# on an idle data connection.
#
TLSRenegotiate                          required off
</IfModule>

##############################################Fin /etc/proftpd/tls.conf###################
```

Recarga la configuración del servidor ProFTPD:

```
$ sudo  systemctl restart proftpd
```

1. Comprueba la configuración con un cliente FTPS, es decir, un cliente ftp que permita la conexión por TLS como FileZilla.

Puedes verificar en tiempo real las conexiones con el servidor ftp revisando los archivos de registro mediante los comandos:

```
$ tail -f /var/log/proftpd/proftpd.log
$ tail -f /var/log/proftpd/tls.log
```

7. Si deseas, puedes hacer valer la configuración para todos los usuarios, incluso aquellos pertenecientes a virtualhost, modificando el fichero **/etc/proftpd/tls.conf** como se indica en el fichero ejemplo tls2.conf (0.01 MB) .

Debes conocer

Te proponemos el siguiente enlace de un vídeo práctico sobre cómo configurar TLS en el servidor ProFTPD y cómo configurar una plantilla de FileZilla que soporta conexión TLS. La configuración se realiza sobre una distribución GNU/Linux basada en Debian.

https://www.youtube.com/embed/jvdR5nZ30gE

Resumen textual alternativo

« Anterior Siguiente »