PRACTICA 6.5

TLS/SSL. PROTOCOLOS SEGUROS

Amenaza o vulnerabilidades

El software Caín & Abel para sistemas Windows permite en caso de realizar un ataque MitM, poder analizar el tráfico de una red local, identificar los mensajes y extraer credenciales de los protocolos que envían sus mensajes en texto plano, por ejemplo entre los más conocidos y empleados: FTP, POP3, SMTP, Telnet y HTTP.

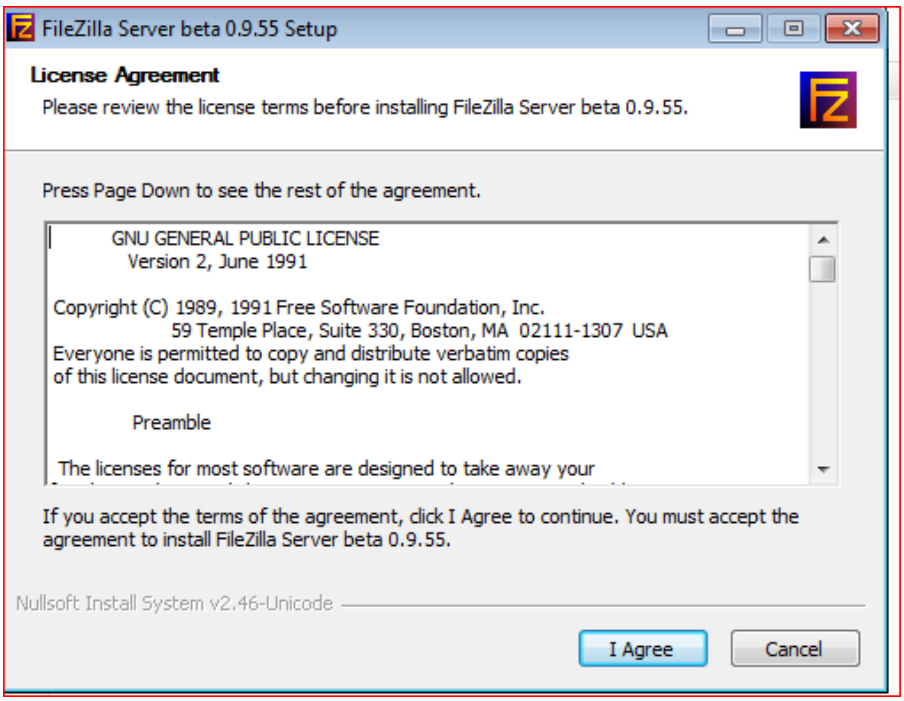
Recomendaciones

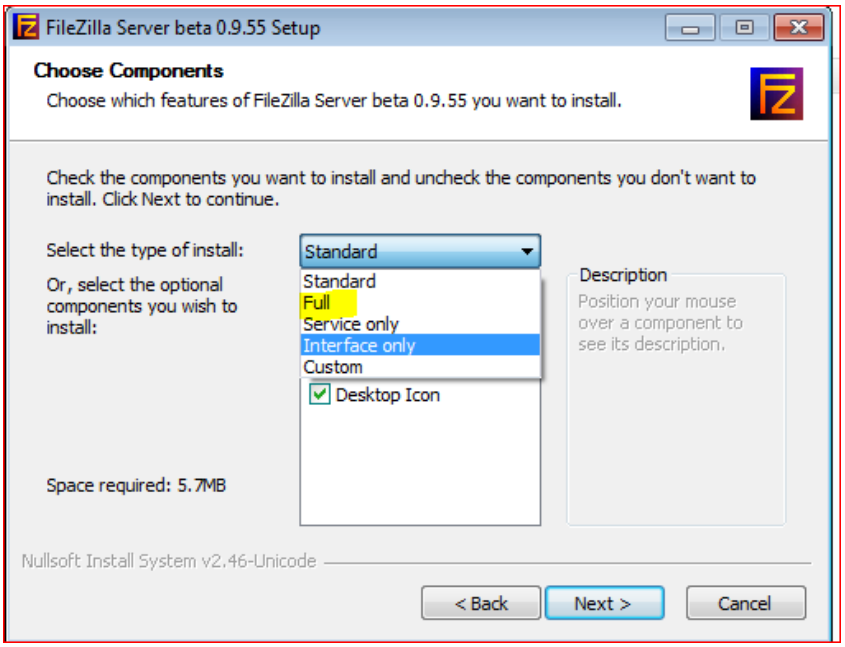
En esta práctica veremos distintos ejemplos de aplicación de protocolos seguros:

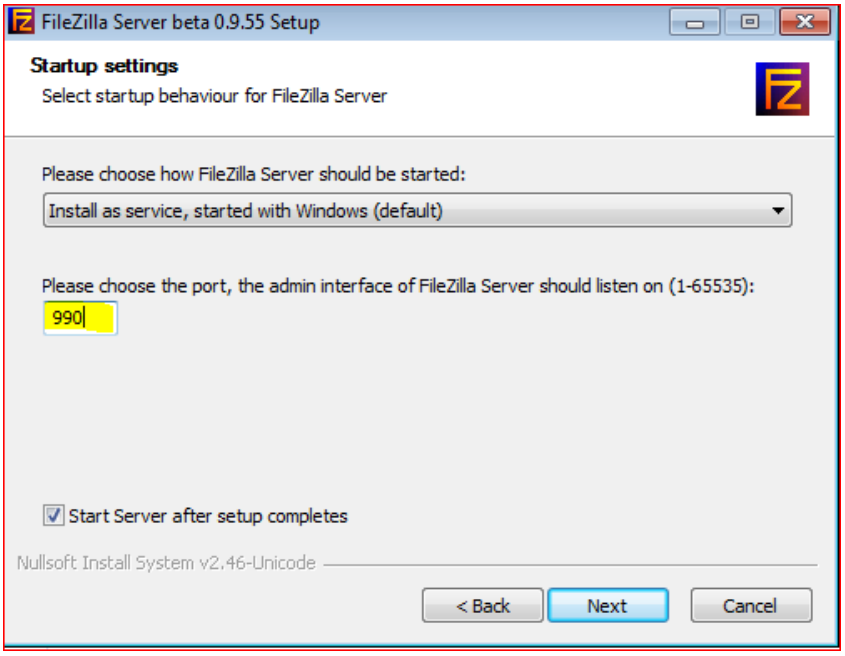
- ✓ **HTTPS**: siempre que visitemos una web en la que enviemos credenciales, verificar que se emplea el protocolo https. Para verificar la autenticidad y confiar en la web, los navegadores web obtienen un certificado SSL del sitio web. En caso de querer administrar una web segura deberemos obtener un certificado SSL para nuestra web, suministrado por una autoridad certificadora externa de confianza como lo son Verisign, Thawte, beTRUSTed o ValilCert.

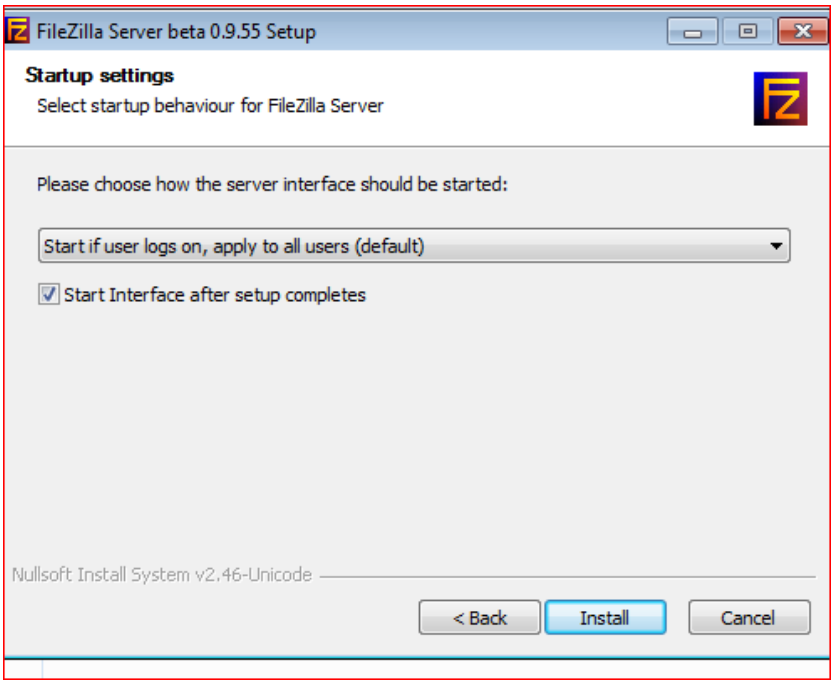
En ocasiones los navegadores web dudan de la veracidad de los certificados SSL, en ese caso debemos añadir una excepción de seguridad en caso de confiar en el sitio web. De ese modo el navegador web añadirá dicha excepción y confiará en el sitio para próximas visitas.

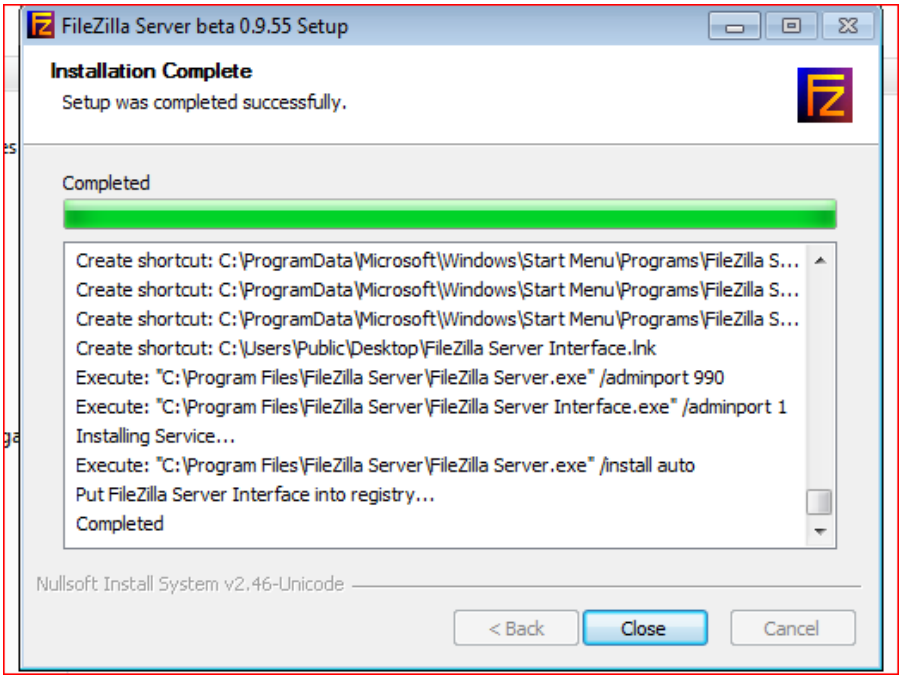
- ✓ **FTP seguro**: la mayoría de los servidores y clientes FTP, soportan conexiones seguras, cifradas sobre SSH y TLS/SSL. Veamos cómo podemos configurar en un servidor FTP administrado las opciones de seguridad SSL. La configuración se realizará sobre el servidor FTP gratuito **Filezilla Server**.




FileZilla Server beta 0.9.55 Setup
Choose Components
Choose which features of FileZilla Server beta 0.9.55 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Standard
Or, select the optional components you wish to install:
Standard
Full
Service only
Interface only
Custom
Desktop Icon
Description
Position your mouse over a component to see its description.
Space required: 5.7MB
Nullsoft Install System v2.46-Unicode
< Back
Next >
Cancel

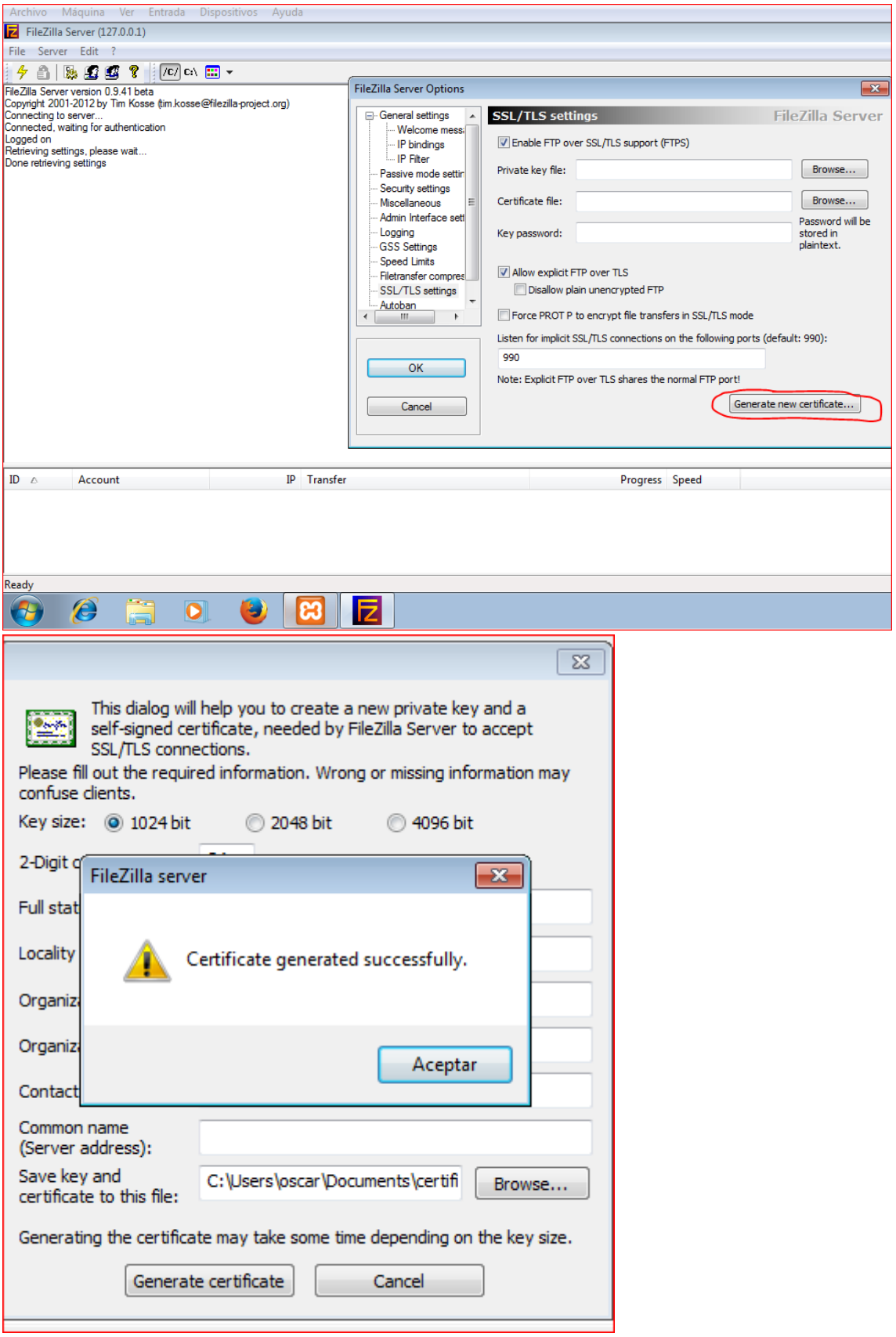

FileZilla Server beta 0.9.55 Setup
Startup settings
Select startup behaviour for FileZilla Server
Please choose how FileZilla Server should be started:
Install as service, started with Windows (default)
Please choose the port, the admin interface of FileZilla Server should listen on (1-65535):
990
Start Server after setup completes
Nullsoft Install System v2.46-Unicode
< Back
Next
Cancel





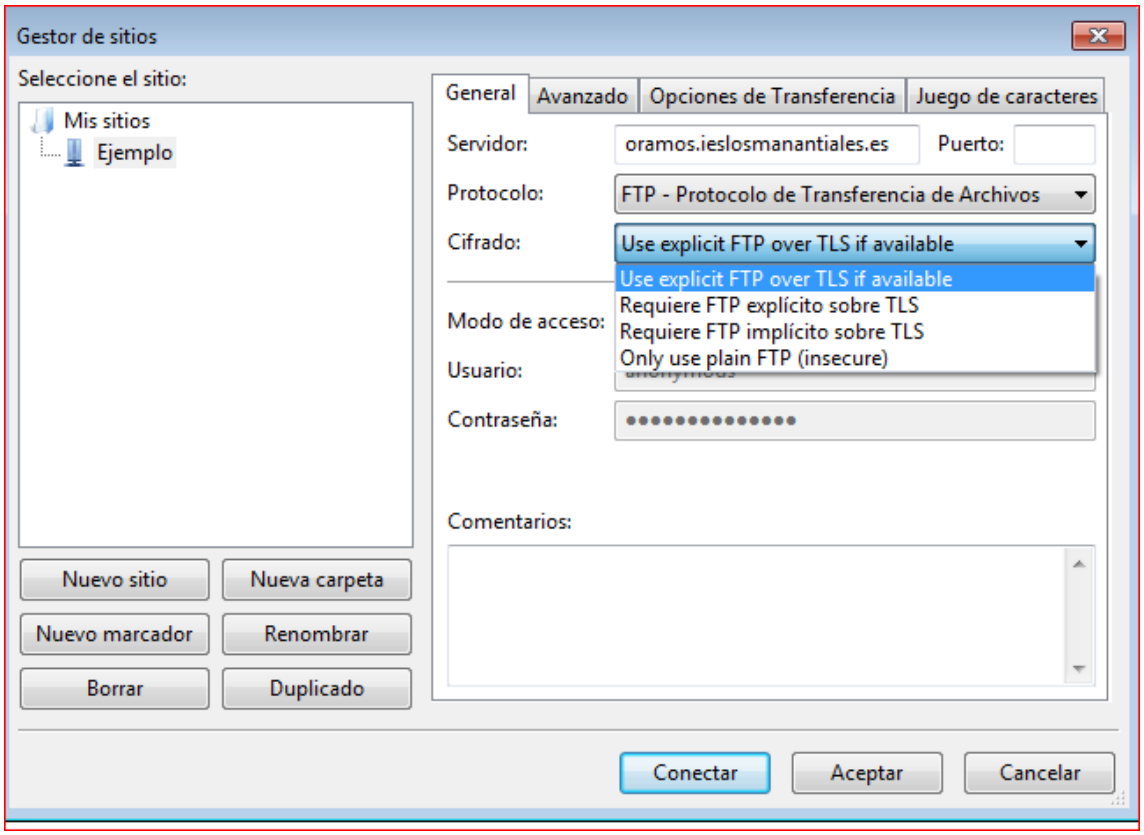
1. En primer lugar configuraremos SSL en Options – SSL/TLS settings. Marcaremos todas las opciones y generar certificado con Generate new certificate. Seleccionamos la opción de longitud de clave, y rellenamos los campos para la creación del certificado y se especificará la ruta al certificado. Una vez generado asignaremos puerto de escucha alternativo para las conexiones seguras en Listen for SSL/TLS – only connections…(por ejemplo el 990).

   A continuación para los usuarios que se deseen conectar mediante soporte SSL/TLS, debemos de marcar la casilla Force SSL for user login en sus opciones de contraseña.



2. En la mayoría de **clientes FTP**, las opciones de configuración de cuentas de usuario FTP, permiten conexiones seguras mediante SSH y SSL/TLS.

Al intentar conectarnos mediante TLS/SSL nos mostrará una pantalla para aceptar el certificado del servidor, si confiamos lo aceptaremos, haciendo que dicha conexión vía FTP sea cifrada y no viajarán datos en texto plano.



3. En caso de no poder configurar las opciones en el servidor TLS/SSL por disponer de un alojamiento con opciones reducidas, es posible al menos emplear en la mayoría de los casos, como opción segura SFTP a través de SSH. En la mayoría de los casos usuario y contraseña se corresponden con los de FTP.
    - Correo electrónico: en las cuentas de correo es recomendable revisar la configuración y sus opciones para que siempre empleen https.
      Para la configuración de cuentas de mail a través de clientes de escritorio algunos servidores como Gmail comienzan a requerir el uso de puertos y protocolos de transferencia seguros mediante SSL:
    - Cuenta de Correo: usuario@gmail.com.
    - Datos POP: Servidor: pop.gmail.com. Usar SSL: Sí. Puerto: 995.
    - Datos SMTP: Servidor: smtp.gmail.com. Usar TLS/SSL: Sí. Puerto: 465 o 587.

Recomendación

Siempre que tengamos que configurar servicios tanto clientes como servidores, que requieran el uso y envío de contraseñas, es recomendable el uso de configuraciones y puertos que transmitan sus mensajes cifrados.