# Práctica 3 – Servicios avanzados de red: HTTPS (2ª sesión)

## 1.1 Objetivo

El objetivo de esta práctica es conocer y familiarizarse con las tareas habituales en la administración y configuración, en un S.O. LINUX, del protocolo HTTPS (*HyperText Transfer Protocol Secure*) conde Apache2. Para ello se proponen los siguientes ejercicios:

- Generación de un certificado SSL autofirmado con la utilidad openssl para autenticar un sitio web.
- Configuración de un sitio web con Apache para su acceso mediante HTTPS.
- Captura y análisis del tráfico TLS (*Transport Layer Security*) generado cuando se accede a un sitio web mediante HTTPS.

## 1.2 Información básica para la realización de la práctica

En esta sección se ofrece la información básica y las referencias necesarias para llevar a cabo las tareas que se proponen en la práctica.

### 1.2.1 Acceso al sistema y elección de sistema operativo

Para la realización de esta práctica, es necesario arrancar el equipo con la opción "Redes"→"Ubuntu 20.04". La práctica se realizará en parejas en donde uno de los equipos actuará como cliente y otro como servidor web. Será en este último en donde se configure adecuadamente Apache2.

### 1.2.2 Gestión de servicios básicos

Hay dos formas de gestionar servicios. Por un lado, los servicios básicos de red se pueden ejecutar y configurar desde un único superservidor denominado `xinetd`. En este caso, con un único proceso se monitorizan tantos puertos como sean necesarios y a petición de los clientes, el superservidor ejecutará el proceso correspondiente al servicio demandado. `xinetd` facilita una gestión unificada de todos los servicios, con mecanismos de seguridad de control de accesos, incluyendo restricciones horarias o accesos dependiendo de la IP de origen, además de otras muchas condiciones, con ayudas para la contabilidad y con posibilidad de registro de todos los eventos (en ficheros de `log`). La configuración de `xinetd` se realiza mediante el fichero `/etc/xinetd.conf`.

Para obtener más ayuda sobre la configuración de este servidor, consulte la sintaxis del fichero de configuración en el manual del sistema:

```
# man xinetd.conf
```

Alternativamente o complementariamente, todo servidor se puede ejecutar en modo *standalone*. Esto consiste básicamente en, tras editar los preceptivos ficheros de configuración del propio servicio, lanzar un ejecutable (`daemon`) en *background*, controlándolo posteriormente si fuese necesario con el comando `systemctl`.

### 1.2.3 Gestión y configuración básica de Apache2 (HTTP)

El protocolo HTTP facilita el acceso desde un cliente (que ofrece una interfaz universal o *navegador*) a objetos web (texto, imágenes, vídeo, etc) situados en un servidor identificado por su dirección IP o su nombre de dominio. El servidor Apache2, una de las implementaciones de HTTP de mayor difusión, ya está instalado en las máquinas Ubuntu 20.04 y se ejecutará en modo *standalone*. Con el siguiente comando podemos gestionar y comprobar el estado del servicio (iniciar, parar, reiniciar, re-ejecutar sin perder conexiones, deshabilitar o habilitar el inicio automático):

```
# sudo systemctl [start|stop|restart|reload|disable|enable] apache2
```

En un despliegue real en explotación lo habitual sería tener cualquier tipo de *firewall* instalado. En ese caso, habría que incluir una regla que habilite el acceso a los puertos correspondientes (dependiendo si queremos facilitar el tráfico sin cifrar directamente sobre TCP en el puerto 80, o tráfico cifrado en el puerto 443 usando el protocolo seguro TLS, o ambos).

Para comprobar la correcta instalación y funcionamiento del servidor, después de iniciar este, acceder a la URL `http://localhost` o `http://direccion_ip` desde cualquier navegador usando cualquiera de las direcciones IP locales disponibles. La página web que aparecerá será la que se define por defecto durante la instalación de Apache2.

La configuración de Apache2 se lleva a cabo principalmente mediante la edición de una serie de ficheros de texto. Los más relevantes son:

- `/var/www/html`: Aquí se almacena el contenido del sitio web. Se puede modificar en los ficheros de configuración.
- `/etc/apache2/apache2.conf`: Configuración principal de Apache2. Las diferentes características y parámetros se definen mediante directivas.
- `/etc/apache2/ports.conf` : Puertos en los que Apache2 atenderá solicitudes.
- `/etc/apache2/sites-available/`: Directorio donde almacenan los *hosts* virtuales. Ver Sección 1.2.4 para más detalles.
- `/etc/apache2/sites-enabled/`: Directorio donde se almacenan los *hosts* virtuales.
- `/etc/apache2/mods-available/` y `/etc/apache2/mods-enabled/`: Contienen los módulos disponibles y habilitados, respectivamente. Por ejemplo, para dar soporte a transacciones MySQL o PHP.
- `/var/log/apache2/access.log`: Fichero de trazas donde se almacenan todas las transacciones.
- `/var/log/apache2/error.log`: Fichero donde se registran los errores.

Para obtener más ayuda sobre la configuración de Apache2 y las directivas disponibles, abra el navegador web y visite la dirección:

```
http://httpd.apache.org/docs/2.4/
```

### 1.2.4 Creación de un certificado SSL

Un certificado digitaltípicamente se expide por una Autoridad de Certificación (entidad de confianza) que vincula de forma fehaciente a una entidad con su clave pública. Se trata de una especie de tarjeta de visita en donde la Autoridad de Certificación garantiza que esa vinculación es cierta e irrevocable. El certificado está firmado con la clave privada de la Autoridad de Certificación, de tal manera que vincula datos asociados al sitio web (su identidad) y la clave pública del mismo. De este modo, es posible autenticar a un sitio web en Internet, ya que si suponemos la hipótesis de que la autoridad certificadora es de confianza, si enviamos los mensajes cifrados con la clave pública del sitio web (garantizada por la autoridad) obtenida del certificado, nadie excepto el que posea la clave privada podrá descifrar los mensajes cifrados, por lo que con este cifrado estaremos autenticando al servidor.

En esta práctica se usará la utilidad de línea de comandos `openssl` para crear el certificado SSL autofirmado (no estará expedido por una Autoridad de Certificación). En concreto usaremos el siguiente comando para crear el certificado:

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

Consulte la página de manual y compruebe las diferentes opciones y argumentos del comando anterior.

A continuación, le pedirá la siguiente información para incluirla en el certificado:

```
Country Name (2 letter code) [XX]: SP
State or Province Name (full name) []: Granada
Locality Name (eg, city) [Default City]: Granada
Organization Name (eg, company) [Default Company Ltd]: UGR
Organizational Unit Name (eg, section) []: DTSTC
Common Name (eg, your name or your server's hostname) []: frdominioseguro.com
Email Address []: webmaster@frdominioseguro.com
```

Las principales opciones empleadas para generar el certificado SSL se explican a continuación:

- `req -x509`: Selección de solicitud de firma de certificados X.509 (formato del certificado).
- `-nodes`: Indicamos que no queremos proteger el certificado con contraseña dado que Apache necesitará leerlo sin intervención del usuario.
- `-days 365`: Periodo de validez del certificado de un año.
- `-newkey rsa:2048`: Indicamos que queremos generar una clave privada para el certificado (porque no la hemos creado anteriormente). En concreto se creará una clave RSA de 2048 bits de longitud.
- `-keyout`: Para indicar el directorio en el cual queremos almacenar la clave privada creada.
- `-out`: Para indicar el directorio en el que almacenaremos el certificado a crear.

### 1.2.5 Configuración de Apache para habilitar el acceso a un sitio por HTTPS

Una vez disponemos de un certificado válido, es necesario configurar Apache para usar SSL. En primer lugar, es necesario habilitar el módulo Apache `mod_ssl`. Para ello se puede usar el *script* `a2enmod` incluido en la distribución de Apache2 como sigue:

```
# sudo a2enmod ssl
```

A continuación, Apache se debe reiniciar para activar el módulo habilitado:

```
# sudo systemctl restart apache2
```

Ahora vamos a crear un *virtual host* para que funcione con HTTPS haciendo uso del certificado SSL. En primer lugar, en el directorio `/etc/apache2/sites-available` crearemos el fichero de configuración del *virtual host* con la siguiente configuración mínima:

```
<VirtualHost *:443>
ServerName frdominioseguro.com
DocumentRoot /var/www/frdominioseguro.com

SSLEngine on
SSLProtocol -all +TLSv1.2
SSLCertificateFile          /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile     /etc/ssl/private/apache-selfsigned.key
</VirtualHost>
```

Hay que tener en cuenta que el valor `Common Name` que configuró para el certificado ha de coincidir con el valor de la directiva `ServerName` en la configuración de arriba.

En el directorio especificado con la directiva `DocumentRoot` crearemos un archivo HTML muy simple para testeo. Primero, comenzamos creando dicho directorio raíz para el sitio:

```
# sudo mkdir -p /var/www/frdominioseguro.com
```

Ahora creamos dentro de /var/www/frdominioseguro.com el archivo HTML index.html con un editor de texto con el siguiente contenido:

```
<h1> FR DOMINIO SEGURO <\h1>
```

Es necesario cambiar el propietario de los directorios raíz y de sus ficheros al usuario de apache2 `www-data`, por ejemplo:

```
# chown -R www-data: /var/www/frdominioseguro.com
```

Una vez creados los ficheros de configuración, hay que crear enlaces simbólicos desde el directorio `sites-available` al directorio `sites-enabled`. Esto se puede hacer directamente con el comando `ln`, o bien usando un *script* especialmente preparado en la distribución de apache2:

```
# sudo a2ensite frdominioseguro.com.conf
```

Comprobamos si la configuración tiene algún error:

```
# sudo apachectl configtest
```

Puede que le aparezca un mensaje de advertencia indicando que la directiva `ServerName` no está configurada a nivel global. Opcionalmente, para eliminar este mensaje, puede configurar `ServerName` en el nombre de dominio o la dirección IP de su servidor en `/etc/apache2/apache2.conf`. Sin embargo, este mensaje es sólo un aviso y no causará problemas si el resultado contiene `Syntax OK` (no hay errores de sintaxis en su archivo de configuración).

La creación de *hosts* virtuales no implica que se creen automáticamente las entradas para que DNS sepa resolver adecuadamente los nombres de los dominios creados. Para ello, habría que configurar adecuadamente DNS para los nombres de dominios virtuales. No obstante, para hacer pruebas, esto se puede hacer localmente editando el fichero `/etc/hosts`, añadiendo los nombres de dominios virtuales creados a una de las IP locales, por ejemplo, la IP de la interfaz de datos. Una vez hecho esto, reiniciamos el servicio:

```
# sudo systemctl reload apache2
```

Y finalmente, desde un navegador comprobamos que el dominio creado es accesible usando `https://` al principio (`https://frdominioseguro.com`). El navegador mostrará una advertencia de seguridad porque estamos usando un certificado autofirmado y, por tanto, no está firmado por ninguna autoridad de certificación confiable. Permite el acceso al sitio

haciendo click en `avanzado` y luego eligiendo la opción `aceptar riesgo y continuar`.

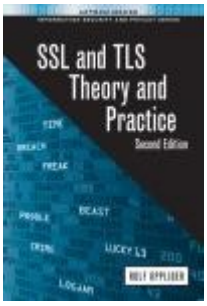
## 1.3 Realización práctica

1) Cree un certificado SSL con la utilidad `openssl` para asociarlo al sitio `frpracticahttps.com`. Nombre el fichero del certificado como `frpracticahttps.crt` y el nombre del fichero de la clave privada como `frpracticahttps.key`.
2) Inspeccione los ficheros `frpracticahttps.crt` y `frpracticahttps.key`.
3) Cree un host virtual con una página de inicio que muestre el mensaje "FR HTTPS" y configúrelo para que funcione con `HTTPS` haciendo uso del certificado creado anteriormente. Compruebe su correcto funcionamiento usando un navegador.
4) Abra Wireshark en su equipo y capture los mensajes que se generan cuando accede al sitio creado anteriormente. ¿Qué mensajes `TLS` se intercambian la aplicación cliente (navegador web) y el servidor (Apache) durante el inicio de la conexión? ¿Qué información relevante se intercambia en esos mensajes? ¿Es posible ver los mensajes del protocolo `HTTP`?

**BIBLIOGRAFÍA**

[1] Library: OpenSSL Cookbook, 3ed By Ivan Ristić
https://www.feistyduck.com/library/openssl-cookbook/

[2] SSL and TLS: Theory and Practice, Second Edition por Rolf Oppliger. Accesible on line desde la biblioteca de UGR.




[3] https://httpd.apache.org/docs/2.4/es/ssl/

[4] Opcionalmente para instalar LAMP (Linux + Apache + MySQL + PHP) consultar https://ubunlog.com/lamp-instala-apache-mariadb-php-ubuntu-20-04/