**Práctica 6. HTTPS**

Lee detenidamente cada uno de los puntos antes de realizar las tareas solicitadas.

1. Abre wireshark y empieza a capturar tráfico. Abre un navegador y accede a www.sitio1.com/ficheros e introduce las credenciales de un usuario con acceso. Dírigite al Wireshark y detén la captura de tráfico. Filtra por HTTP. Busca una trama con la siguiente información: (Captura de página personal creada previamente, “sitio1”, con solicitud de login del navegador. Captura del contenido del archivo “ficheros” creado previamente y captura de imagen del trafico capturado)



2. Inspecciona la trama en los apquetes capturados de HTTP y obtén las credenciales de acceso. (Captura de los datos de Hypertext Transfer Protocol del paquete localizado previamente, mostrando información sobre autenticación de usuario).

3. Dirígete al directorio /etc/apache2/sites-available y genera mediante openssl el certificado autofirmado para sitio1. Comprueba que se han creado los certificados en el directorio. (Captura de comando para crear .key y .crt, y su resultado. Captura del contenido de certificado creado [verificación mediante openssl]. Captura del contenido de la carpeta sites-available tras creación)

Detalles de la clave y certificados auto-firmados a generar:

* Formato del certificado a generar: X.509
* Duración del certificado: 365 días
* Clave privada **sin** encriptación DES
* Para la clave; utilizar el algoritmo RSA con un tamaño de clave de 2048 bits
* .La clave y el certificado deben tener un nombre específicos; ej. sitio1.key y sitio1.crt (o equivalentes a los sitios web creados)

(Opcional) Certificado y clave, con estos detalles, se pueden crear en una única instrucción.

Ver apartado **Recursos** para más información.

4. Activa el módulo HTTPS y haz un restart. (Captura de sudo a2enmod para activar el modulo de ssl y su resultado, y posterior reinicio de apache)

5. Copia el fichero de plantilla de SSL “default-ssl.conf” en sitio1.conf. **¡OJO!** RECUERDA COPIAR ANTES EL “DIRECTORY” CON LOS PERMISOS A SITIO1/FICHEROS CONFIGURADOS EN LA PRACTICA 4. Modifica el fichero sitio1.conf para que sitio1 se conecte por HTTPS con la clave y el certificado que antes hemos creado. Añade el directory con la configuración de usuarios y grupos. Luego guarda los cambios. (Captura de sitio1.conf donde se vea un nuevo Directory con la configuración de conexión vía SSL según el fichero copiado, junto con la configuración de prácticas anteriores)

6. Comprueba la sintaxis y realiza un reload. (Captura del comando apache2ctl –t y un reload)

7. Abre un nuevo navegador y dirígete a http://www.sitio1.com y comprueba si ahora te dirige a la página por defecto. (Captura del navegador)

8. Dirígete ahora a **https://www.sitio1.com**. y comprueba que vuelve a salir la página que creamos en su momento. Comprueba que accedes mediante https. (Captura del navegador accediendo a la web creada vía https, Si el navegador te solicita “aceptar riesgos adicionales” para entrar a la página, incluye las capturas de estos pasos)

9. Cierra el navegador y abre Wireshark e inicia la captura de tráfico. Abre el navegador y dirígete a https:///www.sitio1.com**/ficheros**. Introduce las credenciales de un usuario válido. Comprueba que accedes mediante https. Detén la captura de tráfico. (Imagen del navegador con URL a carpeta ficheros, empezando por https solicitando credenciales y tras acceder correctamente)

10. Detén la captura. Filtra por http y observa que no se ha capturado nada porque hemos accedido por https, por tanto las credenciales han sido encriptadas. Filtra por ssl y comprueba que el tráfico está encriptado. (Captura de trafico http y captura de trafico empleando TLS/SSL. Esta segunda captura debería mostrar transferencias de paquetes entre maquina host [cliente] y maquina guest [servidor]).

**Recursos:**

<https://techexpert.tips/es/apache-es/habilitar-https-en-apache/>

**PASO 3**: <https://medium.com/@yakuphanbilgic3/create-self-signed-certificates-and-keys-with-openssl-4064f9165ea3>

Tutorial creando un certificado propio tipo CA (como si fuera de entidad certificadora):

<https://luisgomezcaballero.com/es/apache-http-server-configurar-https-2/>

**Condiciones de entrega:**

* La práctica se **debe** entregar de forma **individual**, cada uno debe presentar sus propias respuestas. Sin embargo, se puede trabajar en equipo.
* Se debe entregar un documento de texto (.pdf, .docx, .odt, etc.)
* En la portada del documento debe aparecer el nombre completo del alumno.
* La nota comprenderá un valor numérico entre 0 y 10.
* **La fecha límite de entrega es el 28 de noviembre de 2024 a las 23:59:59.**
* **Se podrá entregar hasta 72 horas más tarde de la fecha límite pero con una penalización sobre su puntuación (no será posible aspirar al 10).**