DAW Práctica 2.4: Certificados Apache Elabora un documento donde figuren todos los pasos realizados con las pantallas significativas, explicando cada uno de los pasos. Procedimiento: Apache

1. En apache utilizaremos el módulo SSL con su configuración por defecto (default-ssl). Para ver que módulos tenemos activos en apache utilizamos el siguiente comando: apachectl -M Si queremos filtrar los resultados obtenidos ya sabéis que podemos añadir | grep ssl.

Texto

Descripción generada automáticamente

2. En caso de que no esté activo deberemos habilitarlo: sudo a2enmod ssl

Imagen de la pantalla de un celular de un mensaje en letras blancas

Descripción generada automáticamente con confianza baja

3. Habilitar la configuración por defecto: sudo a2ensite default-ssl.conf



4. Reiniciar el servicio.



5. Creamos un directorio llamado ssl en /etc/apache2



6. Dentro del directorio recientemente creado generamos la clave privada con el cifrado des3 y la longitud 2048 bits. Pedirá introducir el nombre que vamos a generar como clave. sudo openssl

Forma, Rectángulo, Cuadrado

Descripción generada automáticamente

genrsa -des3 -out server.key 2048

 genrsa: Genera una clave RSA.

 -des3: Utiliza el cifrado DES3 para proteger la clave privada.

 -out server.key: Especifica el nombre del archivo de salida.

 2048: Define la longitud de la clave en bits.

7. Competa las funcionalidades del anterior comando

8. Crear la solicitud de certificado con la llave con el siguiente comando (contestar a las preguntas que nos hagan):

Texto

Descripción generada automáticamente

9. Competa las funcionalidades del anterior comando

Forma, Rectángulo, Cuadrado

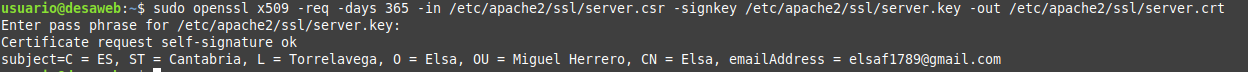
Descripción generada automáticamente

* req: Solicita la creación de una CSR.
* -new: Crea una nueva solicitud.
* -key server.key: Usa la clave privada generada previamente.
* -out server.csr: El archivo de salida para la solicitud.

Durante la ejecución del comando, se te pedirá que ingrese

9.Completar funcionalidades del comando anterior:

10. Crear el certificado digital auto-firmado usando la clave privada:



11.Competa las funcionalidades del anterior comando

Imagen que contiene Texto

Descripción generada automáticamente

 x509: Indica que estamos creando un certificado X.509.

 -req: Usa una solicitud de certificado (CSR).

 -days 365: Establece la validez del certificado a 365 días.

 -in server.csr: La solicitud de certificado que generamos previamente.

 -signkey server.key: Firma el certificado con la clave privada.

 -out server.crt: El archivo de salida para el certificado

12. Incluir el certificado en Apache modificando el fichero /etc/apache2/sitesavailable/default-ssl.conf, reemplazando la dirección del certificado y la clave que se ha creado previamente.



Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

13. Reiniciar el servicio.

Contraseña:usuario



14. ¿Qué aparece al intentar acceder con https? ¿Por qué sucede?

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

15. Los navegadores muestran información sobre los certificados que están utilizando, seleccionando el candado que aparece a la izquierda de la URL. Muestra la información de tu certificado.

16. ¿Se podría implementar para un host virtual? ¿Qué deberías hacer?

crear un archivo de configuración para un host virtual SSL en Apache



agregar la configuración SSL para tu sitio.

Texto

Descripción generada automáticamente

Habilitar el sitio SSL usando a2ensite: