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**.

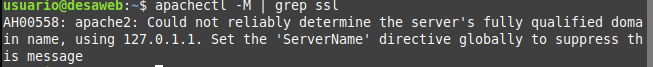
**Procedimiento:**

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.



1. En caso de que no esté activo deberemos habilitarlo:

sudo a2enmod ssl

Texto

Descripción generada automáticamente

1. Habilitar la configuración por defecto:

sudo a2ensite default-ssl.conf

Texto

Descripción generada automáticamente

1. Reiniciar el servicio.



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



1. 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 genrsa -des3 -out server.key 2048



1. Competa las funcionalidades del anterior comando

***Genrsa: El comando genrsa se usa para generar una clave privada en el algoritmo RSA.***

***-des3: Esta opción indica que la clave privada será encriptada con el algoritmo DES3 (Triple DES), lo que proporciona una capa adicional de seguridad.***

***-out: Este parámetro especifica el archivo de salida donde se guardará la clave privada generada.***

***Numbits (2048):*** ***Este valor especifica la longitud de la clave privada en bits.***

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

sudo openssl req -new -key server.key -out server.csr

Texto

Descripción generada automáticamente

1. Competa las funcionalidades del anterior comando

***Req: Este parámetro indica que OpenSSL debe trabajar con solicitudes de firma de certificado (CSR).***

***-new: Esta opción indica que estamos creando una nueva solicitud de firma de certificado (CSR).***

***-key: Este parámetro especifica el archivo de la clave privada que se utilizará para generar la CSR.***

***-out: Este parámetro especifica el archivo de salida donde se guardará el certificado recién creado.***

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

sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

Texto

Descripción generada automáticamente

1. Competa las funcionalidades del anterior comando

***x509: Se refiere a un tipo de certificado***

***-req: Este parámetro indica que el archivo de entrada es una solicitud de firma de certificado (CSR).***

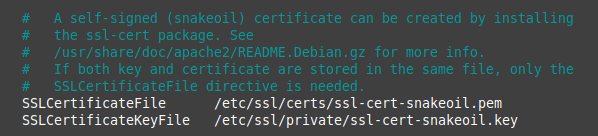
***-days:*** ***Este parámetro especifica la duración del certificado en días.***

***-in:*** ***Con esta opción se indica el archivo de entrada que contiene la solicitud de firma de certificado (CSR).***

***-signkey:*** ***Esta opción le indica a OpenSSL que firme el certificado con la clave privada***

***-out:*** ***Este parámetro especifica el archivo de salida donde se guardará el certificado recién creado.***

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



Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

1. Reiniciar el servicio.



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

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

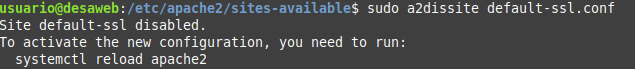
Porque intenta realizar una conexión segura y un certificado auto-firmado no lo es.

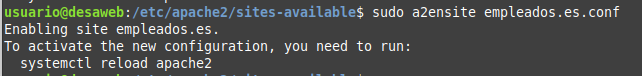
1. Los navegadores muestran información sobre los certificados que están utilizando, seleccionando el candado que aparece a la izquierda de la URL. Muestra la información de tu certificado.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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





Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente