**DAW Práctica 2.4: Certificados Apache**

**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:**

**Texto

Descripción generada automáticamente**

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

**Texto

Descripción generada automáticamente**

1. **Habilitar la configuración por defecto:**

**Texto

Descripción generada automáticamente**

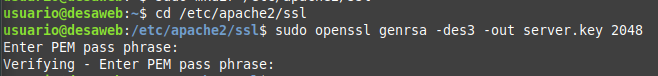
1. **Reiniciar el servicio.**

****

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.**

****

1. **Competa las funcionalidades del anterior comando**

* openssl genrsa: Genera una clave RSA.
* des3: Aplica el cifrado DES3 para proteger la clave privada.
* out server.key: Especifica que el archivo de salida será server.key.
* 2048: Define la longitud de la clave en bits.

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

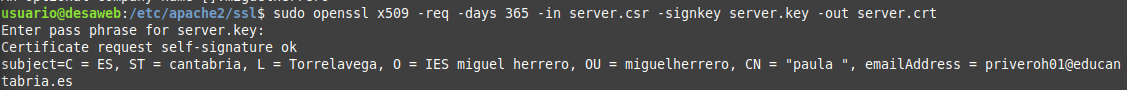
**Texto

Descripción generada automáticamente**

1. **Competa las funcionalidades del anterior comando**

* openssl req -new: Crea una nueva solicitud de firma de certificado (CSR).
* key server.key: Especifica la clave privada para generar la CSR.
* out server.csr: Especifica el archivo de salida de la solicitud de firma (server.csr).

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

****

1. **Competa las funcionalidades del anterior comando**

* openssl x509 -req: Crea un certificado a partir de una solicitud de firma.
* days 365: Especifica que el certificado será válido durante 365 días.
* in server.csr: Especifica el archivo CSR (server.csr) para la firma.
* signkey server.key: Utiliza la clave privada para firmar el certificado.
* out server.crt: Especifica el archivo de salida del certificado (server.crt).

1. **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**

1. **Reiniciar el servicio**

****

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

Cuando intentas acceder a tu servidor usando HTTPS (por ejemplo, https://mi-servidor.local), verás una advertencia en el navegador indicando que el certificado no es de confianza. Esto ocurre porque el certificado es auto-firmado y no está firmado por una autoridad certificadora (CA) reconocida. Los navegadores solo confían en certificados emitidos por CAs verificadas.

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**

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media**

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

* Crear un archivo de configuración para el host virtual
* Configurar el host virtual para usar SSL
* Habilitar el sitio SSL
* Habilitar el módulo SSL