1. **Creamos un directorio llamado ssl en /etc/nginx**



1. **Dentro del directorio recientemente creado generamos la clave privada con el cifrado RSA y la longitud 2048 bits. Pedirá introducir el nombre que vamos a generar como clave.**

**Imagen en blanco y negro

Descripción generada automáticamente con confianza baja**

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

* Genpkey: Utiliza OpenSSL para generar una clave privada.
* Algorithm (RSA): Especifica el algoritmo RSA.
* Pkeyopt: Define un tamaño de 2048 bits para la clave.
* Numbits (2048): **)** hace referencia al número de bits que componen la longitud de la clave generada

1. **Generamos el certificado autofirmado:**

Texto

Descripción generada automáticamente

1. **¿Esta configuración cuenta con passphrase? ¿En la anterior práctica estaba implementada? ¿Qué diferencia hay entre tener o no tener passphrase?**

No, esta configuración no cuenta con passphrase, ya que se utilizó el parámetro -nodes al generar la clave privada con el comando

El argumento -nodes ("no DES encryption") instruye a OpenSSL a no cifrar la clave privada con una passphrase.

1. **Completa las funcionalidades del anterior comando**
   1. **req:** Es el subcomando de OpenSSL que permite trabajar con solicitudes de firma de certificado (Certificate Signing Requests, CSR) y certificados autofirmados.
   2. **nodes:** Indica que la clave privada no debe ser cifrada.
   3. **days:** Especifica la cantidad de días de validez del certificado.
   4. **key:** Indica el archivo que contiene la clave privada que se utilizará para firmar el certificado.
   5. **out:** Define el nombre del archivo de salida para el certificado o la CSR generada.
2. **Incluir el certificado en Nginx modificando el fichero de configuración de nuestro host vitual. En el fichero de configuración se deberá añadir una nueva configuración de servidor con, al menos, las siguientes características:**
   1. **SSL escuche por el puerto 443 (listen 443 ssl).**
   2. **El nombre del servidor.**
   3. **Raíz desde donde buscará los archivos.**
   4. **La referencia a la clave y a los certificados.**
   5. **Location / para que busque las url o muestre el error 404 al no encontrarlas.**

****

**Texto

Descripción generada automáticamente**

1. **Confirmar la correcta sintaxis de los ficheros de configuración.**

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, Correo electrónico

Descripción generada automáticamente**

1. **Ahora que se ha implementado https puede ser interesante que se redirija el posible tráfico de http. Para ello, en la parte del puerto 80 del fichero de configuración, si estamos trabajando con Nginx añadimos la siguiente instrucción.**

**Texto

Descripción generada automáticamente**

1. **Reiniciamos el servicio**

****

1. **Probamos la nueva implementación.**

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**