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.

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

```
sudo a2enmod ssl
```

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  genrsa -des3 -out server.key 2048
```

7. Completa las funcionalidades del anterior comando

genrsa
-des3
-out
Numbits (2048)

8. 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
```

9. Completa las funcionalidades del anterior comando

req

-new

-key

-out

10. 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
```

11. Completa las funcionalidades del anterior comando

x509

-req

-days

-in

-signkey

-out

12. 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.

```
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile   /etc/ssl/private/ssl-cert-snakeoil.key
```

13. Reiniciar el servicio.

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

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?