Servidor virtual HTTPS en Linux

Vamos a realizar la siguiente configuración en el servidor Apache instalado en ServidorLinuxXX.

- Deshabilitar el servidor virtual ssl por defecto (default-ssl).
- Crear un certificado digital auto firmado con openssl para el dominio seguro.dawXX.net.
- Crear y habilitar un servidor virtual https para el dominio seguro.dawXX.net
    - Se servirá el fichero index.html si no se indica ningún fichero en la URL.
    - Se mostrará un listado del directorio raíz si no se solicita ningún fichero.
    - Podrán acceder todos los usuarios.
- El log de errores será **/var/log/apache2/seguro.error.log**.
- El log de accesos será **/var/log/apache2/seguro.access.log**, con formato combined.

Sigamos los siguientes pasos para la configuración

1. Crea el directorio **/var/www/html/seguro**. **(Imagen)**

2. Crea el fichero de texto **/var/www/html/seguro/index.html** con el contenido que quieras. **(Imagen)**

3. Crea un certificado digital autofirmado usando openssl.

    3.1. Sitúate en el directorio home del usuario con el que has iniciado sesión.

    3.2. Crea una clave privada RSA de 2048 bit, Figura 5.119.

```
openssl genrsa -out seguro.key 2048
```

    (Imagen)

    3.3. Genera una solicitud de certificado (CSR, Certificate Signing Request).

```
openss1 req -new -key seguro.key -out seguro.csr
```

    Introduce los datos del certificado. Lo que veas oportuno, los utilizaremos más tarde.

Esta solicitud de certificado se la podrías enviar a una autoridad de certificación para que generase el certificado (CRT). En este caso lo vamos a firmar nosotros, vamos a crear un certificado auto firmado.

(Imagen)

3.4. Crea el certificado digital autofirmado usando la clave privada.

```
openssl x509 -req -days 365 -in seguro.csr -signkey seguro.key
-out seguro.crt
```

(Imagen)

4. Copia la clave y el certificado en los directorios que utiliza por defecto Apache y configura los permisos adecuados.

```
sudo mv seguro.key /etc/ssl/private/
sudo mv seguro.crt /etc/ssl/certs/
sudo chown root:ssl-cert /etc/ssl/private/seguro.key
sudo chmod 640 /etc/ssl/private/seguro.key
sudo chown root:root /etc/ssl/certs/seguro.crt
```

5. Crea el fichero **/etc/apache2/sites-available/seguro.conf** con las siguientes directivas

```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerName seguro.net
        DocumentRoot /var/www/html/seguro
        ErrorLog ${APACHE_LOG_DIR}/seguro.error.log
        CustomLog ${APACHE_LOG_DIR}/seguro.access.log
        combined
        <Directory /var/www/html/seguro>
            Options Indexes FollowSymLinks
            AllowOverride None
            Require all granted
```

```
            </Directory>
            SSLEngine on
            SSLCertificateFile    /etc/ssl/certs/seguro.crt
            SSLCertificateKeyFile /etc/ssl/private/seguro.key
      </VirtualHost>
</IfModule>
```

(Imagen)

6. Deshabilita el servidor ssl por defecto.

```
sudo a2dissite default-ssl
```

7. Habilita el servidor virtual seguro.

```
sudo a2ensite seguro
```

8. Verifica que dentro del directorio **/etc/apache2/sites-enabled** se ha creado el enlace **seguro.conf**.

(Imagen)

9. Reinicia el servidor para que los cambios tengan efecto.

10. Abre el navegador y establece una conexión a **https://localhos/seguro**

¿Qué ocurre? En avanzado ver el certificado y capturad una imagen, observando cómo es y qué datos tiene. Compáralos con los que has puesto.