ACTIVIDAD: APACHE (2.4)

Configurar un sitio virtual

Instalar apache

```
$ sudo apt-get update
$ sudo apt-get install apache2
```

Configurar un *virtual host* asociado al nombre *www.srdsi.lab* :

1. Crear los directorios y ficheros del sitio web:

   Directorio principal del sitio *www.srdsi.lab*

   `$ sudo mkdir -p /var/www/srdsi-lab`

   Directorio para los archivos accesibles por el usuario

   `$ sudo mkdir /var/www/srdsi-lab/docs`

   Cambiar permisos

   Para contenido éstatico: `root:root y 755`

   Para contenido dinámico: `www-data:www-data`

2. Crear el fichero de prueba */var/www/srdsi-lab/docs/index.html* con el siguiente contenido:

   ```
   <html><title>Test</title>
   <body><h1> Laboratorio SRDSI
   </h1></body></html>
   ```

3. En ports.conf (contenido por defecto)

   `Listen 80`

4. Crear el fichero de configuración del sitio, con el nombre:

   `/etc/apache2/sites-available/srdsi-lab.conf`

   y el siguiente contenido mínimo:

   ```
   <VirtualHost *:80>
       ServerName www.srdsi.lab
       DocumentRoot /var/www/srdsi-lab/docs
   </VirtualHost>
   ```

5. Activar el sitio web configurado en el paso anterior.

   `$ sudo a2ensite srdsi-lab`

   `$ sudo apache2ctl graceful`

   Si se produce algún error a la hora de lanzar el servidor, es recomendable revisar el contenido del fichero log:

   `$ sudo tail /var/log/apache2/error.log`

6. Comprobar que el sitio web está activo en el servidor:

   ```
   $ sudo apache2ctl -S
   ```

7. Comprobar desde un cliente que el sitio `http://www.srdsi.lab` está activo.

Configurar acceso restringido a una zona privada

Autenticación básica del usuario mediante usuario/contraseña

1. Crear el directorio para los documentos de la zona privada:

   ```
   $ sudo mkdir -p /var/www/srdsi-lab/docs/zona-privada
   ```

2. Dentro del directorio crear el fichero de prueba *index.html* con el siguiente contenido:

   ```
   <html><title>Test</title>
   <body><h1> Laboratorio SRDSI ACCESO RESTRINGIDO </h1>
   </body></html>
   ```

3. Añadir la configuración del directorio a proteger en el fichero del sitio web

   ```
   /etc/apache2/sites-available/srdsi-lab
   <Directory /var/www/srdsi-lab/docs/zona-privada>
       AuthType Basic
       AuthName "Zona acceso restringido a personal autorizado"
       AuthUserFile /etc/apache2/usersweb
       Require valid-user
   </Directory>
   ```

   Requiere el módulo `mod_auth_basic ($ sudo a2enmod auth_basic)`

4. Crear fichero de usuarios autorizados

   ```
   $ sudo htpasswd -c /etc/apache2/usersweb admin1
   ```

   Añadir nuevos usuarios:

   ```
   $ sudo htpasswd /etc/apache2/usersweb admin2
   ```

5. Actualizar configuración del servidor apache.

   ```
   $ sudo apache2ctl graceful
   ```

6. Comprobar desde un cliente que el sitio `http://www.srdsi.lab/zona-privada` solo es accesible por un usuario autorizado [1]

7. Realizar una captura con Wireshark[2] del acceso anterior y comprobar que puede conocerse el usuario y password que se han utilizado

[1] acceder con *Nueva ventana privada*

[2] También puede observase intercambio en `Firefox --> Herramientas --> H. Desarrollador --> Red`

Autenticación del usuario con Digest

1. Activar el módulo `mod_auth_digest`

   ```
   # sudo a2enmod auth_digest
   ```

2. Modificar sitio virtual incluyendo las directivas del esquema `digest`:

   ```
   <Directory /var/www/srdsi-lab/docs/zona-privada>
       AuthType Digest
       AuthName "Area privada"
       AuthDigestAlgorithm MD5
       AuthDigestDomain http://www.srdsi.lab/zona-privada/
       AuthDigestProvider file
       AuthUserFile /etc/apache2/digest_users
       Require valid-user
   </Directory>
   ```

3. Crear fichero con contraseñas de tipo "`digest`"

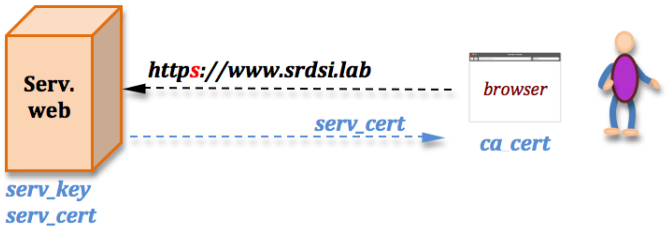
   ```
   # sudo htdigest [ -c ] /etc/apache2/digest_users "Area privada"
   username
   ```

   username y *password* es sólo válido para un `realm` (`AuthName` *string*) dado, así en el fichero de credenciales por cada `usuario/realm` aparecerá una entrada:

   ```
   admin1:Area privada:f64f2af9501033efe7c402417681e05b
   ```

4. Comprobar con Wireshark qué información viaja cifrada

Configurar un sitio virtual con soporte para SSL con autenticación del servidor:



Necesitaremos disponer de un certificado para el sitio virtual (CN=*www.srdsi.lab*) en el servidor, además del certificado de la Autoridad de Certificación para poder verificarlo en el navegador del usuario.

1. Habilitar el módulo `ssl ( mod_ssl )`

   ```
   $ sudo a2enmod ssl
   ```

2. Crear los directorios y ficheros del sitio web (con permisos para el usuario `www-data`):

   ```
   $ sudo mkdir -p /var/www/srdsi-ssl/docs
   ```

3. Crear el fichero de prueba */var/www/srdsi-ssl/docs/index.html* con el siguiente contenido:

   ```
   <html><title>Test</title>
   <body><h1> www.srdsi.lab CONEXI&Oacute;N SEGURA </h1></body></html>
   ```

4. Comprobar puertos habilitados en `/etc/apache2/ports.conf`

   ```
   Listen 443
   ```

5. Crear el fichero de configuración del sitio web seguro `/etc/apache2/sites-available/`*srdsi-ssl.conf*

   ```
   <IfModule mod_ssl.c>
   <VirtualHost *:443>
       ServerName www.srdsi.lab
       DocumentRoot /var/www/srdsi-ssl/docs

       SSLEngine on
       SSLProtocol -all +TLSv1.2
       SSLCertificateFile pathfile-certificado-sitiovirtual
       SSLCertificateKeyFile pathfile-clave-privada-sitiovirtual
   </VirtualHost>
   </IfModule>
   ```

6. Activar sitio virtual

   ```
   $ sudo a2ensite srdsi-ssl
   ```

7. Comprobar configuración

   ```
   $ sudo apache2ctl configtest
   ```

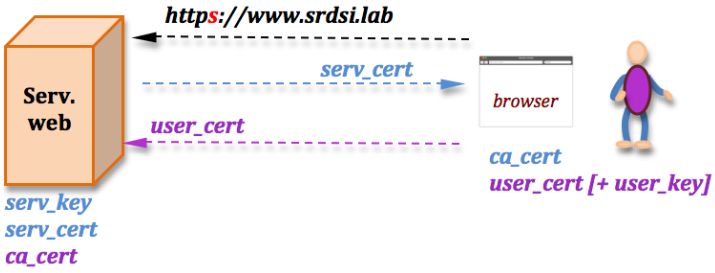
8. Reiniciar servidor apache

   ```
   $ sudo apache2ctl graceful     [sudo service apache2 restart]
   ```

9. Comprobar que el servidor web seguro está en marcha accediendo desde el navegador a `https://www.srdsi.lab`, **antes** y **después** de importar el certificado de la CA[3]

[3] `Preferencias -> Privacidad&seguridad -> Certificados -> Ver certificados -> Autoridades -> Importar`

Configurar un sitio virtual con soporte para SSL con autenticación del usuario:



Cada usuario que desee conectarse al sitio web deberá presentar su certificado (previamente importado en su navegador). Además el servidor para verificarlo deberá disponer del certificado de la CA que lo ha firmado.

- Añadir en el fichero `/etc/apache2/sites-available/`*`srdsi-ssl.conf`*

  ```
  SSLVerifyClient require
  SSLVerifyDepth 2
  [SSLProtocol all -TLSv1.3]

  SSLCACertificateFile pathfile-certificados-CA
  [SSLCACertificatePath pathfile-certificados]
  ```

Comprobar que el acceso desde el navegador a `https://`*`www.srdsi.lab`*, **antes** y **después** de importar el certificado del usuario

Configurar acceso a una zona privada con autenticación del usuario mediante certificado

- En `/etc/apache2/sites-available/`*`srdsi-ssl.conf`* añadir el contenedor para el directorio de la zona privada:

  ```
  <Directory /var/www/srdsi-ssl/docs/zona-privada>
      SSLVerifyClient require
      SSLVerifyDepth 5
      SSLRequireSSL                # Require ssl
      [SSL]Require (%{SSL_CLIENT_S_DN_O} eq "SRDSI" \
          and %{SSL_CLIENT_S_DN_OU} in {"LABS", "ALUM", "PROF"} )

  </Directory>
  ```

- En el navegador del usuario deberá estar disponible el certificado del usuario, que deberá tener el valor "SRDSI" en el DN_O, y en DN_OU alguno de los valores indicados.

Referencias

1. http://httpd.apache.org/docs/2.4/vhosts/examples.html
2. http://httpd.apache.org/docs/2.4/mod/mod_auth_digest.html
3. http://httpd.apache.org/docs/2.4/mod/mod_ssl.html
4. HTTP Digest Authentication (RFC2617)