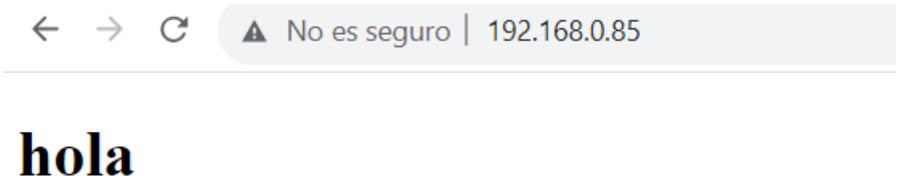
Tema 1: SERVIDORES WEB

PRACTICA: Protocolo HTTPS

Ahora vas a configurar el servidor Apache para que acepte el protocolo HTTPS y, de esta manera, garantizar la autenticación del servidor frente al cliente y la integridad de los datos. En este caso no se obtiene la confidencialidad, aunque los datos viajen cifrados porque el acceso a la información es libre.

Paso 1: Abre el navegador web y accede al servidor web.

Paso 2: Haz clic sobre el candado tachado que hay junto a su dirección IP y accede al enlace *Conexión no segura* para comprobar que no se está conectado de manera segura a este sitio.



Paso 3: Abre una consola y conéctate al servidor con el usuario *usuario* usando SSH.

```
$ ssh usuario@IP_Servidor
```

Paso 4: Ahora comprueba con el comando *a2query* los sitios y los módulos de Apache que tiene habilitado tu servidor. Solo deberías tener habilitado el sitio web por defecto y, respecto a los módulos, comprobarás que no tienes habilitado el módulo *ssl.*

```
admin01@srv:~$ a2query -s
000-default (enabled by site administrator)
admin01@srv:~$ a2query -m
```

```
status (enabled by maintainer script)
authz_host (enabled by maintainer script)
deflate (enabled by maintainer script)
authn_file (enabled by maintainer script)
authz_core (enabled by maintainer script)
alias (enabled by maintainer script)
mpm_prefork (enabled by maintainer script)
reqtimeout (enabled by maintainer script)
filter (enabled by maintainer script)
access_compat (enabled by maintainer script)
authn_core (enabled by maintainer script)
php8.1 (enabled by maintainer script)
.....
```

Paso 5: Comprueba que el módulo SSL para Apache está disponible y habilítalo con el comando *a2enmod.*

```
admin01@srv:~$ ll /etc/apache2/mods-available/ssl*
-rw-r--r-- 1 root root 3110 mar 23 02:00
/etc/apache2/mods-available/ssl.conf
-rw-r--r-- 1 root root  97 mar 23 02:00
/etc/apache2/mods-available/ssl.load
admin01@srv:~$ sudo a2enmod ssl
[sudo] password for admin01:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to
configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
```

```
admin01@srv:~$
```

Paso 6: Ahora comprueba si existe un sitio SSL predefinido entre los sitios disponibles en Apache y, en caso afirmativo, habilítalo con el comando *a2ensite.*

```
admin01@srv:~$ ll /etc/apache2/sites-available/
total 20
drwxr-xr-x 2 root root 4096 jun 13 06:24 ./
drwxr-xr-x 8 root root 4096 jun 13 06:24 ../
-rw-r--r-- 1 root root 1332 mar 23 02:00 000-
default.conf
-rw-r--r-- 1 root root 6338 mar 23 02:00 default-
ssl.conf
admin01@srv:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
 systemctl reload apache2
admin01@srv:~$
```

Paso 7: Como se indica en la salida de los comandos *a2enmod* y *a2ensite,* se debe reiniciar el servidor Apache para aplicar los cambios. En realidad, para activar el nuevo sitio solo es necesario recargar la configuración, pero vamos a reiniciarlo para activar el nuevo módulo.

```
admin01@srv:~$ sudo systemctl restart apache2.service
admin01@srv:~$
```

Paso 8: Una vez reiniciado, comprobamos de nuevo los sitios y módulos habilitados.

```
admin01@srv:~$ a2query -s
default-ssl (enabled by site administrator)
000-default (enabled by site administrator)
admin01@srv:~$ a2query -m | grep ssl
```

```
ssl (enabled by site administrator)
admin01@srv:~$
```

Paso 9: Configurar el Firewall. Para permitir las conexiones por https al servidor web hay que configurar el cortafuegos (firewall de Ubuntu)

```
sudo ufw app list
sudo ufw allow 'Apache Full'
sudo ufw reload
```

Paso 10: Por último, comprobamos el acceso desde el navegador web, pero esta vez indicando el esquema *https* en la URL. El navegador marca la conexión como insegura porque la página tiene un certificado autofirmado, pero, como es una página web tuya, puedes acceder con confianza. Pulsa el botón *Avanzado…* y luego el botón *Aceptar el riesgo y continuar.* Ahora ya te muestra el contenido, aunque te advierte de que sigue considerando la conexión como no segura.