



PRÁCTICA 6.

Configuración Servidor Web de una empresa para entrega.

Francmirror

2º SMR

Fecha de realización: 19 - 01 - 23



INDICE

1. TOPOLOGÍA
2. ACCESO HTTP
3. ACCESO HTTPS
4. CONFIGURACIÓN .HTACCESS Y .HTPASSWD
5. PRUEBAS
6. FINALIZADO



2. ACCESO HTTP

Voy a utilizar un servidor (Ubuntu 22 LTS SERVER) y un cliente (Ubuntu 22 LTS SERVER).

Comenzaré creando el host virtual para el sitio web de `www.construccionesmoreno.com`.

```
root@ubu22:/home/ubu22# cd /var/www/  
root@ubu22:/var/www# mkdir construccionemoreno.com  
root@ubu22:/var/www# _
```

Ahora crearé un directorio dentro del anterior creado, dónde guardaremos los archivos que será públicos:

```
root@ubu22:/var/www# cd construccionemoreno.com/  
root@ubu22:/var/www/construccionemoreno.com# mkdir public_html  
root@ubu22:/var/www/construccionemoreno.com# _
```

Dentro del nuevo directorio creado, he realizado un archivo `index.html` sencillo que dirá lo siguiente:

```
<html>  
  <head>  
    <title>Construcciones moreno S.L.</title>  
  </head>  
  <body>  
    <h1>Construcciones Moreno S.L.</h1>  
    <h3>Tus construcciones al mejor precio</h3>  
  </body>  
</html>
```

Por ahora llevamos lo siguiente:

```
root@ubu22:/var/www/construccionemoreno.com# ls -R  
.:  
public_html  
./public_html:  
index.html  
root@ubu22:/var/www/construccionemoreno.com#
```



Ahora habilito el sitio `construccionesmoreno.com` y reinicio el servicio `apache2` para aplicar cambios:

```
root@ubu22:/etc/apache2/sites-available# sudo a2ensite construccionsmoreno.com
Enabling site construccionsmoreno.com.
To activate the new configuration, you need to run:
systemctl reload apache2
```

```
root@ubu22:/etc/apache2/sites-available# systemctl reload apache2
```

Procedo a editar el archivo `/etc/hosts` configurando la resolución DNS.

```
127.0.0.1 localhost
127.0.1.1 ubu22

127.0.0.1 construccionsmoreno.com

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

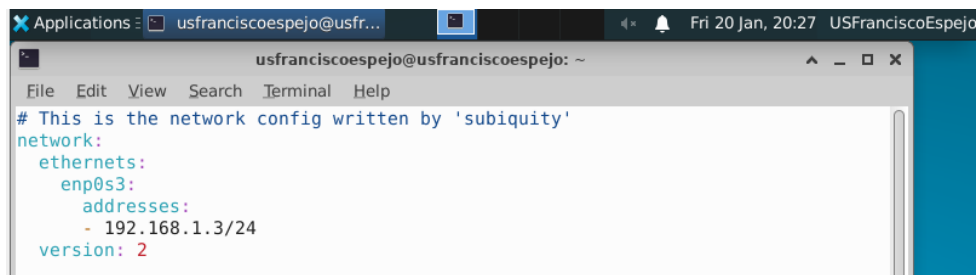
Voy a realizar una comprobación con mi cliente ubuntu server 22 para comprobar que funciona la página <http://construccionesmoreno.com>. Lo primero, he configurado el archivo de los dos ordenadores con `netplan` (`/etc/netplan/00-installer-config.yaml`). He escrito un artículo de `netplan` en mi blog, para su mayor comprensión.

<https://blog.francmirror.es/uso-de-la-utilidad-netplan/>

- Servidor:

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses:
        - 192.168.1.1/24
  version: 2
```

- Cliente:





Ahora que tenemos las redes configuradas, el archivo `/etc/hosts` de nuestro cliente lo modificaremos e incluimos lo siguiente:

```
Applications      usfranciscoespejo@usfranciscoespejo: ~
File Edit View Search Terminal Help
127.0.0.1 localhost
127.0.1.1 usfranciscoespejo

192.168.1.1 construccionemoreno.com
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
~
~
```

Y mediante algún navegador, buscaremos `http://construccionemoreno.com`



Cómo hemos podido comprobar en la anterior imagen ya tenemos acceso mediante `http` a nuestro sitio web



Copiaré el archivo `default-ssl.conf` para tener los datos predeterminados, de la siguiente manera:

```
root@ubu22:/etc/apache2/sites-available# cp default-ssl.conf construccionesmoreno.com.conf
```

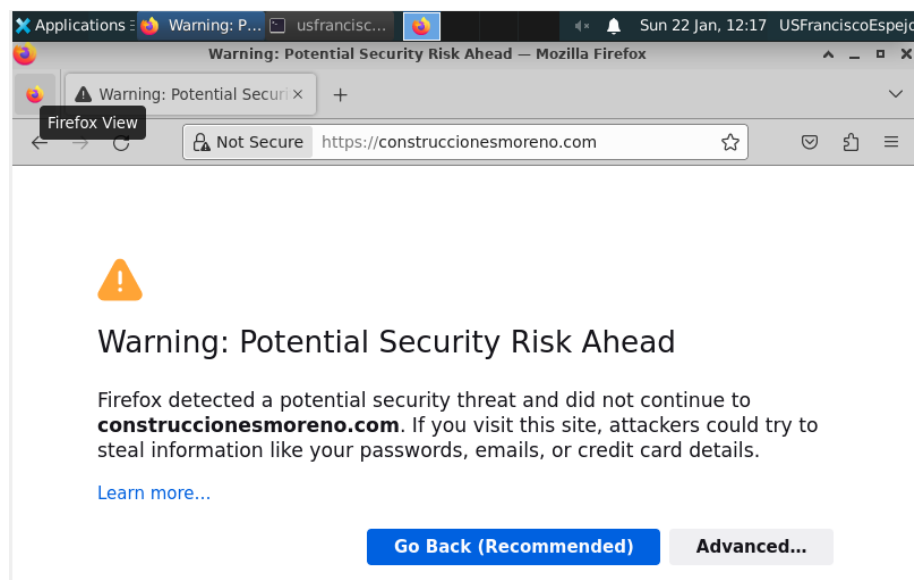
Ahora en el archivo `construcciones.com.conf` tendremos que tener los siguientes datos:

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerAdmin admin@construccionesmoreno.com
    ServerName construccionesmoreno.com
    ServerAlias www.construccionesmoreno.com
    DocumentRoot /var/www/construccionesmoreno.com/public_html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key
```

Seguiré ejecutando los siguientes comandos de la siguiente manera:

```
root@ubu22:/etc/apache2/sites-available# a2ensite construccionesmoreno.com.conf
Site construccionesmoreno.com already enabled
root@ubu22:/etc/apache2/sites-available# service apache2 restart
```

Ahora desde mi cliente comprobaré si tenemos conexión segura con https





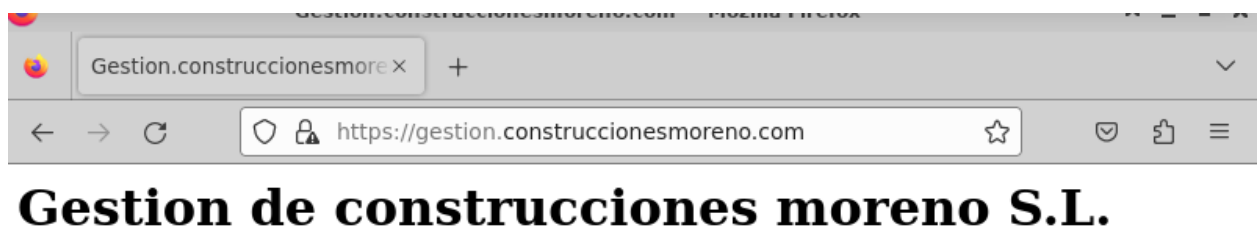
Como podemos comprobar en la siguiente captura, todo ha funcionado a la perfección



Yo he configurado otro host virtual con https que se llama `gestion.construccionesmoreno.com`. Muestro el archivo de configuración del host virtual nuevo es así:

```
<IfModule mod_ssl.c>
    <VirtualHost *:443>
        ServerAdmin admin@gestion.construccionesmoreno.com
        ServerName gestion.construccionesmoreno.com
        ServerAlias www.gestion.construccionesmoreno.com
        DocumentRoot /var/www/gestion.construccionesmoreno.com/public_html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/apache.crt
        SSLCertificateKeyFile /etc/apache2/ssl/apache.key
```

A continuación muestro cómo este nuevo host virtual que actúa como subdominio funciona a la perfección:



Tus gestiones al alcance de tu ordenador



4. CONFIGURACIÓN .HTACCESS Y .HTPASSWD

Ya tenemos nuestro sitio web configurado como https, es decir, conexión segura. Ahora solo nos queda el último paso, proteger los archivos presupuestos.php, el subdominio gestion.construccionesmoreno y el archivo de texto confidencial.txt.

Lo primero que tenemos que hacer es escribir lo siguiente en el archivo `/etc/apache2/sites-available/construccionesmoreno.com.conf` y haremos lo mismo en `/etc/apache2/sites-available/gestion.construccionesmoreno.com.conf`

```
<VirtualHost *:443>
    ServerAdmin admin@construccionesmoreno.com
    ServerName construccionesmoreno.com
    ServerAlias www.construccionesmoreno.com
    DocumentRoot /var/www/construccionesmoreno.com/public_html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key

    <Directory /var/www/construccionesmoreno.com/public_html>
        AllowOverride all
    </Directory>
```

De esta forma apache buscará el contenido .htaccess cuando se acceda al sitio web y controlará las restricciones de acceso que definamos en él. Una vez modificado recargamos la configuración con `service apache2 reload`

Ahora voy a mostrar los archivos que vamos a mostrar. Mi archivo presupuestos.php será así

```
root@ubu22:/var/www/construccionesmoreno.com/public_html# cat presupuestos.php
<html>
    <head>
        <title>Presupuestos</title>
    </head>

    <body>
        <?php echo '<h2> Le quedan 100.000 euros y una deuda de 32.000 euros</h2>'
    </body>
</html>
```



El archivo `confidencial.txt` quedará así:

```
Usted tiene acceso al archivo con información confidencial y crítica de la empresa Construcciones Moreno S.L.
```

El subdominio `gestión` lo protegeremos para que solo puedan entrar desde la red `192.168.13.x`

Ahora vamos a proteger esos archivos. Para empezar, mi archivo `.htaccess` del dominio `construccionesmoreno.com` quedará así:

```
AuthUserFile "/var/www/construccionesmoreno.com/claveclientes"
AuthName "Confidencial, introduzca su usuario y su contraseña"

<Files presupuestos.php>
AuthType Basic
require user promocionesluis construccionessatlantic reformascontratas
</Files>
```

Primero creo todos los usuarios, y mi archivo `claveclientes` quedará de la siguiente manera:

```
root@ubu22:/var/www/construccionesmoreno.com# htpasswd -cb claveclientes promocionesluis gerencia123
Adding password for user promocionesluis
root@ubu22:/var/www/construccionesmoreno.com# htpasswd -b claveclientes construccionessatlantic gerencia123
Adding password for user construccionessatlantic
root@ubu22:/var/www/construccionesmoreno.com# htpasswd -b claveclientes reformascontratas gerencia123
Adding password for user reformascontratas
root@ubu22:/var/www/construccionesmoreno.com# cat claveclientes
promocionesluis:$apr1$IK8S$ki0$ngf.e6o30y6PjBC1Q59a30
construccionessatlantic:$apr1$0zaDJ6QV$mzuuBs86y21qUkBTiZs99/
reformascontratas:$apr1$Ri0goHOM$raWLOQkAP7DRbys7bdbAc/
root@ubu22:/var/www/construccionesmoreno.com# _
```



El archivo `clavesconfidencial` para el subdominio quedará así:

```
root@ubu22:/home/ubu22# cd /var/www/gestion.construccionesmoreno.com/
root@ubu22:/var/www/gestion.construccionesmoreno.com# ls
clavesconfidencial public_html
root@ubu22:/var/www/gestion.construccionesmoreno.com# cat clavesconfidencial
peperoig:$apr1$NqcsKxNz$BL7LbeQMP3PTsPH91/g6h0
florentinoperez:$apr1$zo0KW.B8$I/JeF1Ukh.xp7RSru60AX.
root@ubu22:/var/www/gestion.construccionesmoreno.com#
```

El archivo `.htaccess` del subdominio quedará de la siguiente manera:

```
AuthUserFile "/var/www/gestion.construccionesmoreno.com/clavesconfidencial"
AuthName "Confidencial, introduzca su usuario y contraseña"

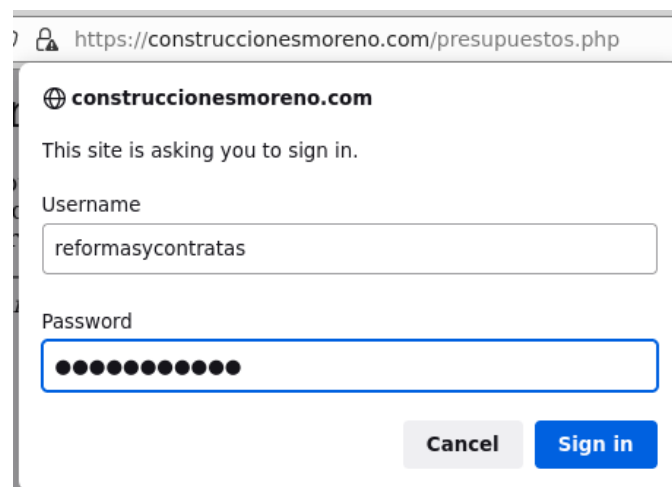
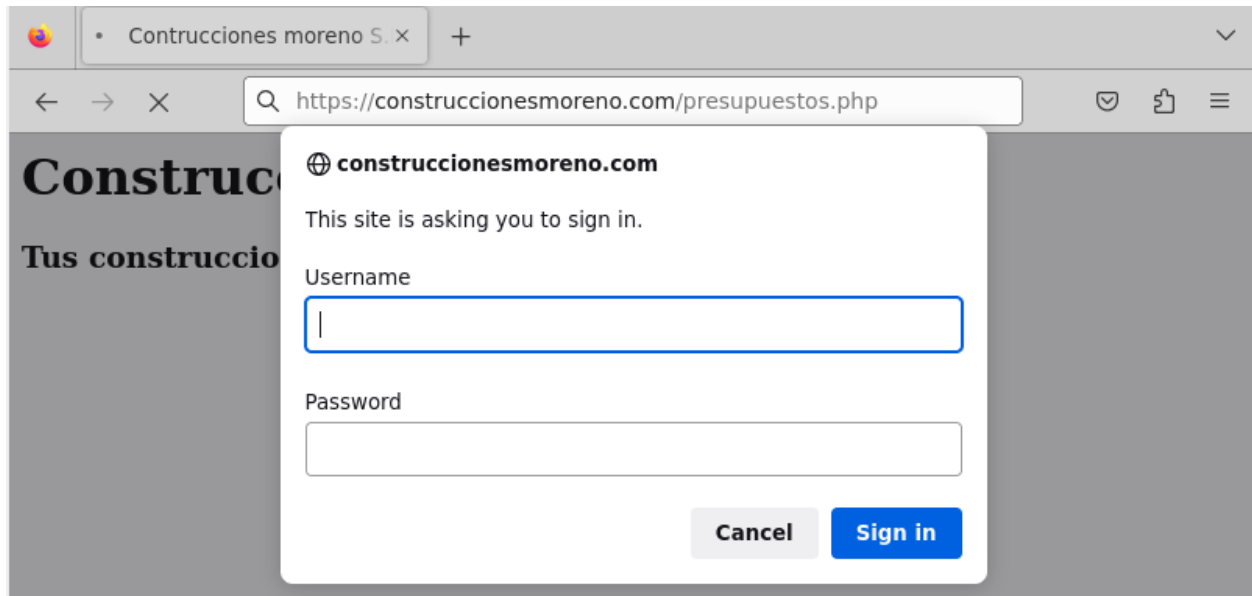
<Files public_html>
Order deny, allow
Deny from all
Allow from 192.168.13
</Files>

<Files confidencial.txt>
AuthUserFile "/var/www/gestion.construccionesmoreno.com/clavesconfidencial"
AuthType Basic
require user peperoig florentinoperez
</Files>
~
```



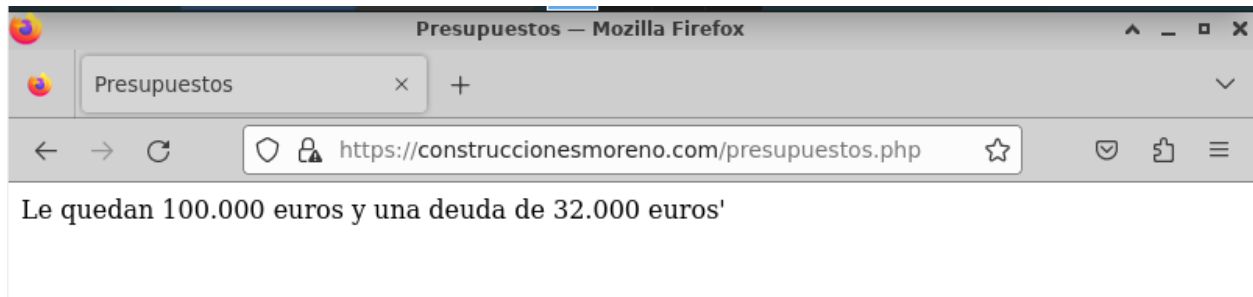
5. PRUEBAS

Ahora si buscamos `presupuestos.php`, nos pedirá usuario y contraseña, y si entramos con un usuario y contraseña correcto, como por ejemplo en este caso, el usuario "reformasycontratas", pasará lo siguiente:

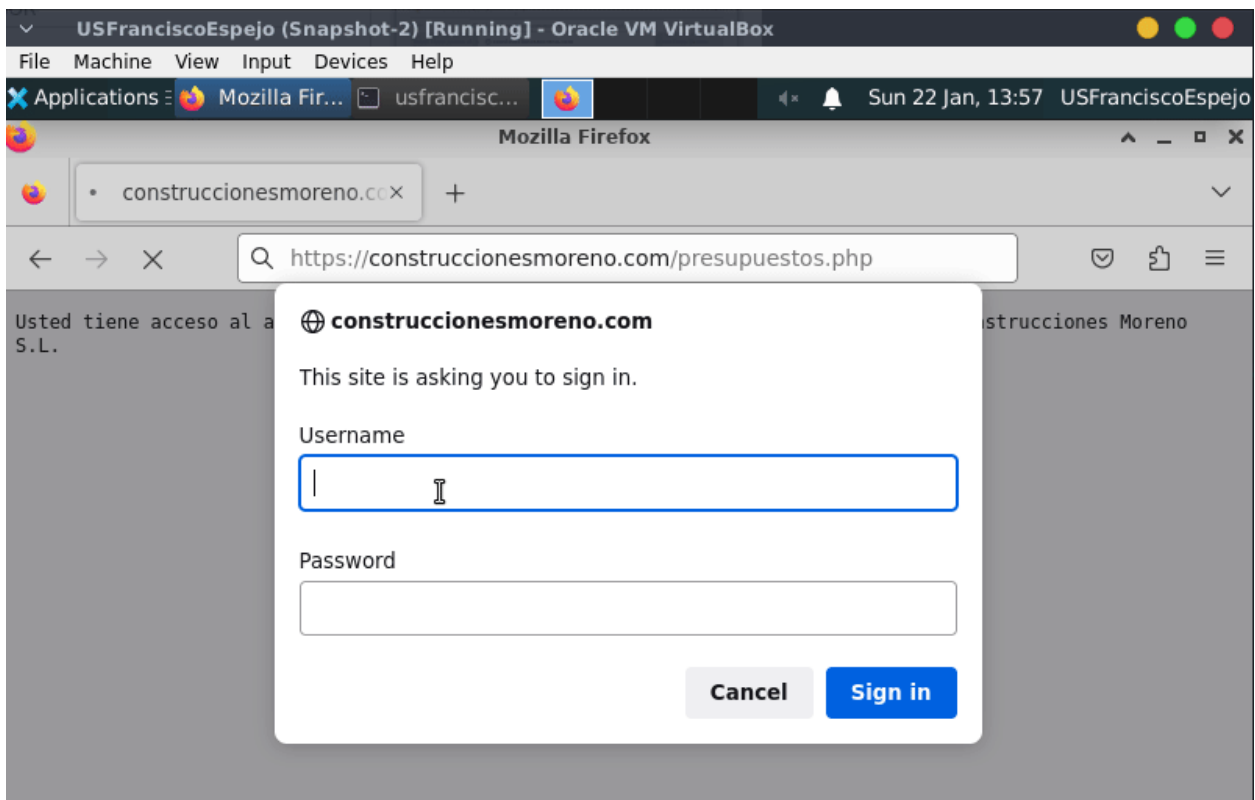




Cómo podemos comprobar, tenemos acceso correctamente.



Ahora probaré a entrar con una cuenta no permitida, por ejemplo con florentinoperez pero no me deja y me da error. Usaré un software llamado "peek" para hacer un gift para mostrar cómo no me deja acceder con ese usuario y contraseña:



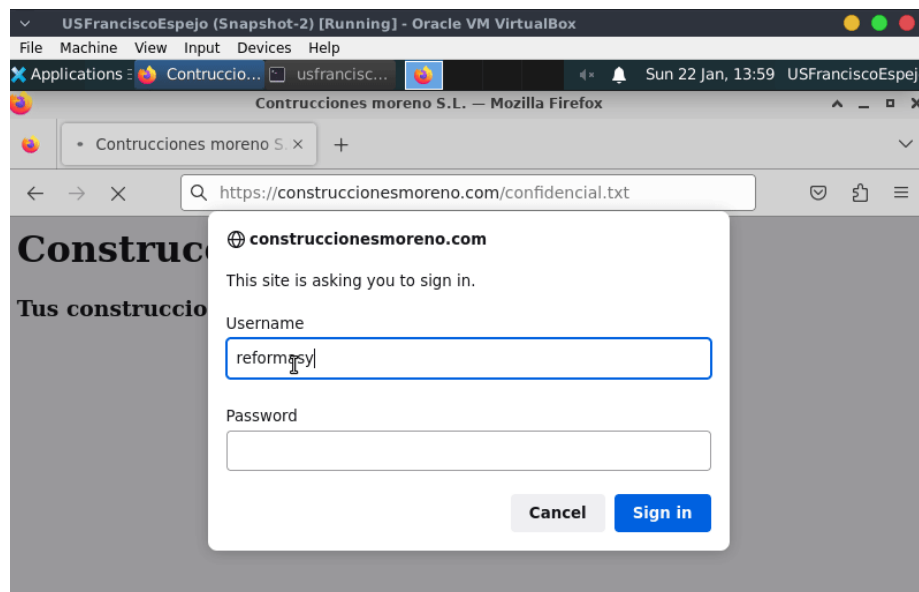
Cómo se puede comprobar en el video, intento iniciar sesión y no me deja, pero cuando lo hago con el usuario permitido me da acceso al archivo correctamente.



A continuación, voy a entrar en el archivo `confidencial.txt`, con el usuario "florentinoperez":



Ahora, voy a comprobar si con un usuario distinto me da acceso, lo haré con "reformasycontratas". Volverá a usar peek para demostrar el correcto funcionamiento:



6. FINALIZADO

Con esto, ya habríamos finalizado la práctica correctamente, dejando el acceso a los archivos a los usuarios indicados y permitidos y con acceso https al dominio y al subdominio. Gracias por su tiempo