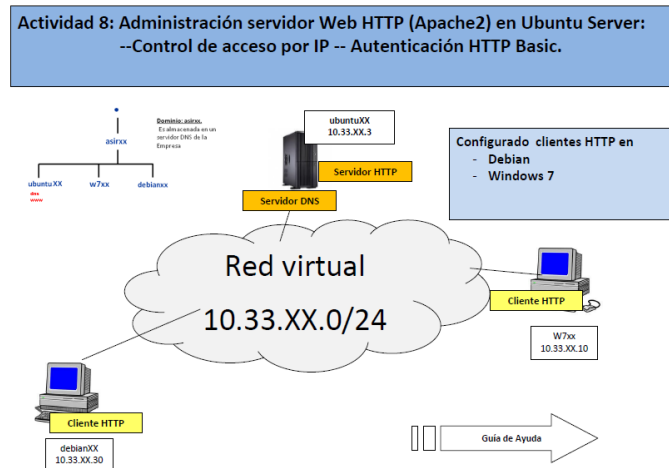


ACTIVIDAD 8 – CONTROL DE ACCESO POR IP- AUTENTICACION HTTP BASIC



Creamos un directorio que se llame privado dentro de /var/www

```
lales@ubuntu10:~$ sudo su
[sudo] password for lales:
root@ubuntu10:/home/lales# cd ..
root@ubuntu10:/home# cd ..
root@ubuntu10:/# cd /var
root@ubuntu10:/var# cd www
root@ubuntu10:/var/www# mkdir privado
root@ubuntu10:/var/www# _
```

Y dentro creamos un fichero html que incluya el siguiente texto

```
GNU nano 2.2.4 Archivo: privado1.html Modificado
<html>
<body>
<h1> PAGINA PRIVADA </h1>
</body>
</html>
```

Ahora vamos al fichero /etc/sites-available/default y vamos a poner una directiva para /var/www/privado, para denegar el acceso al directorio a todos los equipos excepto al local y a Debian en nuestro caso.

```
GNU nano 2.2.4 Archivo: default Modificado
allow from all
</Directory>

<Directory /var/www/datos>
  DirectoryIndex index.html
  Options FollowSymLinks MultiViews
  AllowOverride None
  Order allow,deny
  allow from all
</Directory>

<Directory /var/www/privado>
  Options Indexes FollowSymLinks MultiViews
  AllowOverride None
  Order allow,deny
  allow from 127.0.0.1 localhost
  allow from 10.33.10.30
</Directory>
-
```

Ahora nos vamos al navegador y ponemos 10.33.10.3/privado y nos aparecerá correctamente



PAGINA PRIVADA

Ahora vamos a comprobar que el módulo auth_basic está habilitado, para ello nos vamos al fichero /etc/apache2/mods-enabled y hacemos un ls

```
root@ubuntu10:/etc# cd apache2
root@ubuntu10:/etc/apache2# cd mods-enabled
root@ubuntu10:/etc/apache2/mods-enabled# ls
alias.conf          autoindex.conf     env.load           setenvif.load
alias.load          autoindex.load     mime.conf         status.conf
auth_basic.load     cgid.conf          mime.load         status.load
authn_file.load     cgid.load          negotiation.conf  userdir.conf
authz_default.load  deflate.conf       negotiation.load  userdir.load
authz_groupfile.load deflate.load        reqtimeout.conf
authz_host.load     dir.conf           reqtimeout.load
authz_user.load     dir.load           setenvif.conf
root@ubuntu10:/etc/apache2/mods-enabled#
```

Ahora vamos a crear un usuario dentro de apache2 que se llame mortadelo y otro filemon y la contraseña que le voy a poner va a ser invés para que puedan acceder ellos únicamente

```
root@ubuntu10:/etc/apache2/mods-enabled# cd ..
root@ubuntu10:/etc/apache2# sudo htpasswd -c /etc/apache2/passwd mortadelo
New password:
Re-type new password:
Adding password for user mortadelo
root@ubuntu10:/etc/apache2#
```

```
root@ubuntu10:/etc/apache2/mods-enabled# cd ..
root@ubuntu10:/etc/apache2# sudo htpasswd -c /etc/apache2/passwd mortadelo
New password:
Re-type new password:
Adding password for user mortadelo
root@ubuntu10:/etc/apache2# sudo htpasswd /etc/apache2/passwd filemon
New password:
Re-type new password:
Adding password for user filemon
root@ubuntu10:/etc/apache2#
```

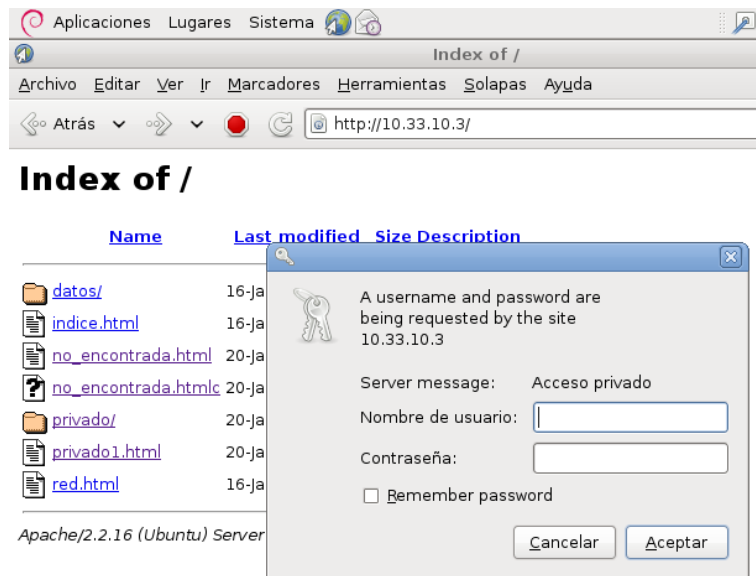
Ahora vamos a editar el fichero /etc/sites-available/default y vamos a permitir el acceso solo a los usuarios mortadelo y filemon

```
GNU nano 2.2.4          Archivo: default          Modificado

<Directory /var/www/privado>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from 127.0.0.1 localhost
    allow from 10.33.10.30
    AuthName "Acceso privado"
    AuthType Basic
    AuthUserFile /etc/apache2/passwd
    Require user mortadelo filemon
</Directory>

Alias /wiki /home/lales/wiki
<Directory /home/lales/wiki>
    DirectoryIndex index.html
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
^G Ver ayuda  ^O Guardar  ^R Leer Fich ^Y RePág.   ^K Cortar Tex ^C Pos actual
^X Salir     ^J Justificar ^W Buscar   ^V Pág. Sig. ^U PegarTxt  ^T Ortografía
```

Ahora vamos a acceder a 10.33.10.3/privado y vemos que nos pide un nombre de usuario y contraseña



Y ya nos deja pasar perfectamente

