**Ejercicio 2: protección de sitios web.** **Control de acceso a usuarios.**

Vamos a crear un sitio web protegido al que sólo puedan acceder, ciertos usuarios que se autentifiquen mediante nombre y password. Protegeremos un directorio llamado **prueba (755)**, creado dentro del DocumentRoot: **/var/www/html/**. Incluimos una página web dentro: **“prueba.html”.** Los pasos a seguir son:

* + Crear el archivo con los usuarios autorizados y sus contraseñas
  + Crear el archivo **.htaccess,** con las opciones de autenticación, dentro del directorio a proteger
  + Configura dentro del archivo de configuración de apache, la directiva contenedora: **<Directory ….>…</Directory>** para el directorio en cuestión con la opción: **AllowOverride**  **all**.

1. Creamos el fichero con las **contraseñas** de los usuarios a los que les permitiremos el acceso al sitio web, con el primer usuario: **#htpasswd –c /etc/httpd/.htusus\_seguros alumno** (la opción **–c**  crea el archivo, pide nombre y password del usuario).

El nombre que le hemos asignado al archivo empieza por **.ht** para queno sea accesible desde ningún equipo, (localizar la directiva **<Files ~”^\.ht”>**  y comprobueaba la cláusula:**deny from** all. Lo hemos guardado en el directorio raíz del servidor: **/etc/httpd/** (fuera del **DocumentoRoot**, por razones de seguridad para que no sea accesible vía web).

1. Para los siguientes usuarios, se repite el comando pero sin la opción **-c**: **#htpasswd /etc/httpd/.htusus\_seguros pepe**
2. Visualiza el archivo creado.
3. Visualiza los permisos de **.htusus\_seguros,** dejar los permisos con **640** propietario y grupo propietario:**apache** (**chown root.apache /etc/httpd/.htusus\_seguros).**
4. Creamos el fichero **.htaccess** dentro del directorio a proteger en nuestro caso, el directorio, **“/var/www/html/prueba”.** Este fichero tendrá el siguiente contenido (consultar apuntes) :

**AuthType Basic**

**AuthName “directorio protegido”**

**AuthUserFile .htusus\_seguros**

**require valid-user**

6. Configurar dentro de **httpd.conf** las opciones del directorio a proteger:

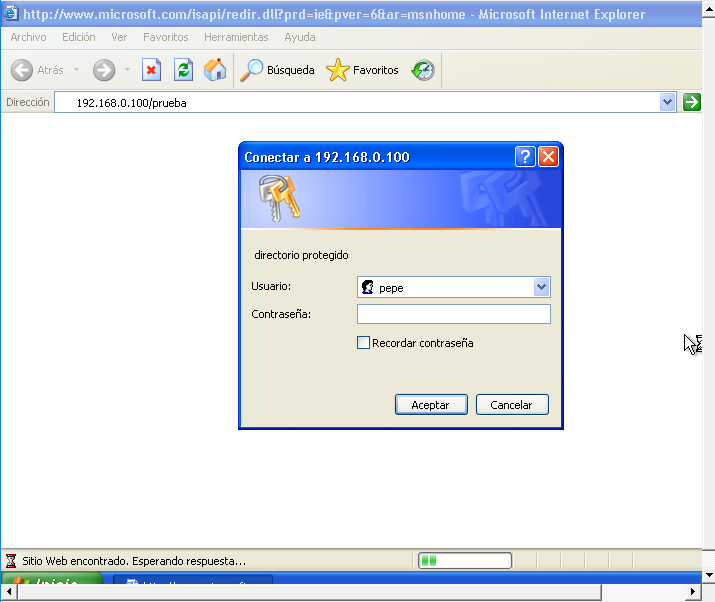
**<Directory /var/www/html/prueba>**

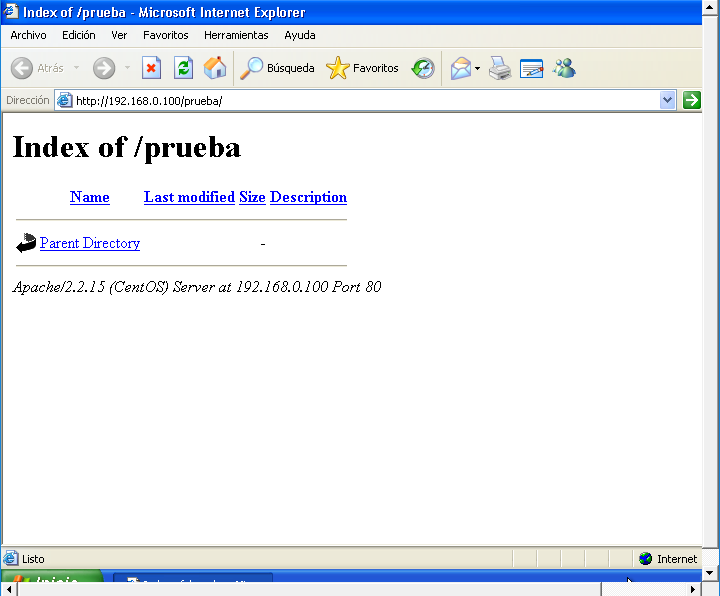
**AllowOverride All**

**Options Indexes FollowSymLinks ...**

**</Directory>**

1. Recarga el servicio. Accede al directorio **prueba** desde el navegador y comprueba que nos pide autentificación para acceder.
2. **Limitar el acceso a una lista de usuarios:** Cambia la línea **require valid-user**  por: **require user alumno** (en el archivo **.htaccess)** de forma que sólo este usuario de entre los incluidos en el archivo **AuthUserFile** podrá tener acceso al sitio (también se podría indicar una lista de usuarios separados por espacios en blanco). Pruébalo desde el clientexp. **Captura la pantalla.**

****

****

1. Vamos a proteger el directorio **/var/www/daw2/** para que sólo se autorice el acceso a los usuarios del grupo: **daw2** para ello, crea el archivo de contraseñas para estos usuarios: **/etc/httpd/.htusus\_daw2**   e incluye a los usuarios: alumno, profesor y pepe. Configura la directiva **<Directory /var/www/daw2>**  y modifica el valor de la opción **AllowOverride** a  **All**. Crea un nuevo archivo **.htaccess** dentro del directorio a proteger: **/var/ww/daw2** (o copia el que has hecho en el ejercicio anterior): el mensaje para la directiva **AuthName** será: “solo para usuarios de daw2**.** El archivo **.htaccess**  debe quedar así**:**

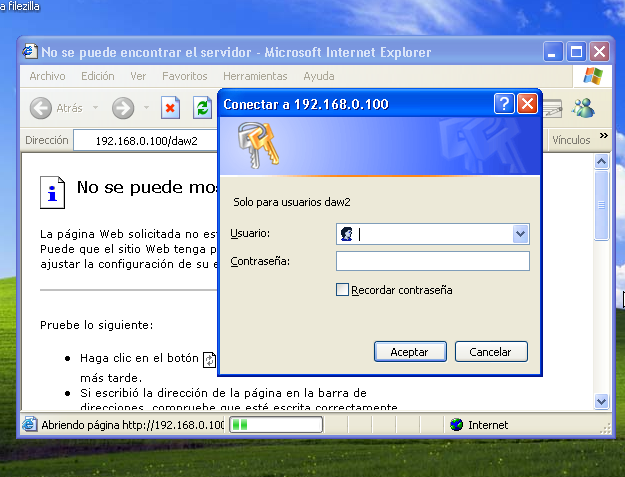
**AuthType Basic**

**AuthName “solo para usuarios de daw2”**

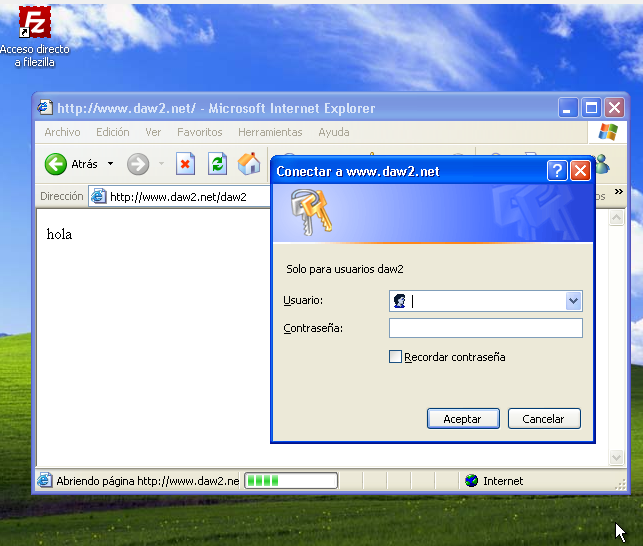
**AuthUserFile .htusus\_daw2**

**require valid-user**

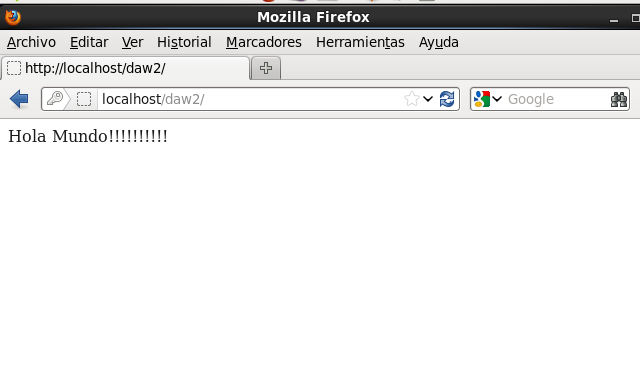
1. Prueba el acceso desde el navegador del clientexp. **Captura la pantalla.**



1. Comprueba si el servidor DNS del server 2008 tiene definido el alias: [www.daw2.net](http://www.daw2.net). Utiliza el alias para acceder a la página principal del servidor web: <http://www.daw2.net/daw2>).



1. Plataforma **LAMP** (**L**inux-**A**pache+**M**ySQL+**P**HP), para que nuestro servidor apache pueda ejecutar scripts en PHP con acceso a la base de datos MySQL, nos bastará con tener instalados los paquetes rpm de **PHP** y **MySQL**. Comprueba si están instalados.
2. Visualiza el directorio: **/etc/httpd/conf.d/**  y el archivo de configuración de **php.conf**. Comprueba que en este archivo se carga con la directiva **LoadModule** el módulo (librerías) de PHP y se añade a la lista **DirectoryIndex**, la página de inicio: **index.php**. Accede al archivo de configuración de apache y localiza y escribe la directiva **Include**  que sirve para que se puedan incluir todos los archivos de configuración **.conf** del directorio: **/etc/httpd/conf.d/**
3. Crea una página de php sencilla o copia al DocumentRoot, algún ejercicio de php que hayas realizado.
4. Visualiza la página de php desde el navegador. **Captura la pantalla.**



1. Visualiza también dentro del directorio: **/etc/httpd/conf.d/** el archivo de configuración de las páginas de manual: **manual.conf.** Accede a dichas páginas desde el navegador.
2. **Analizador de accesos.** Visualiza también dentro del directorio: **/etc/httpd/conf.d/** el archivo de configuración de la aplicación **webalizer**

es un analizador gráfico de los accesos que ha tenido el servidor web y se basa en el análisis del archivo: **/var/log/httpd/access\_log** (las páginas se encuentran en el directorio: **/var/www/usage/**  definido con la directiva **Alias**  dentro de **webalizer.conf**)**.** Autoriza el acceso sólo desde el equipo centos: añade el nombre del servidor (o la IP) a la línea **Allow from 127.0.0.1 192.168.0.100. Recarga apache**

1. Accede a la aplicación vía web: [**http://servidor/usage/**](http://servidor/usage/) **Captura la pantalla.**