

## 5.9. Control de acceso por IP y nombre de dominio

En la máquina **ServidorLinuxXX** crea el directorio `/var/www/html/profesor` y configura *Apache* para que solo se pueda acceder desde el equipo local y desde **DesarrolloW7XX** (192.168.1.X6).

1. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administrador.
2. Crea en directorio `/var/www/html/profesor`. Dentro del directorio crea un fichero denominado `profesor.html` con el contenido que quieras.
3. Edita el fichero de configuración `/etc/apache2/sites-available/000-default.conf` y utiliza la directiva `<Directory>` junto con la directivas `Require` para denegar el acceso al directorio a todos los equipos excepto al local y a **DesarrolloW7XX**, Figura 5.65.

```
<Directory /var/www/html/profesor>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require ip 127.0.0.1
    Require ip 192.168.1.16
</Directory>
```

Figura 5.65: Control de acceso por IP y nombre de dominio

4. Reinicia el servidor para que los cambios tengan efecto.
5. Comprueba que se puede acceder a `http://192.168.1.X7/profesor/` desde **DesarrolloW7XX** pero no desde la máquina real, Figuras 5.66 y 5.67.

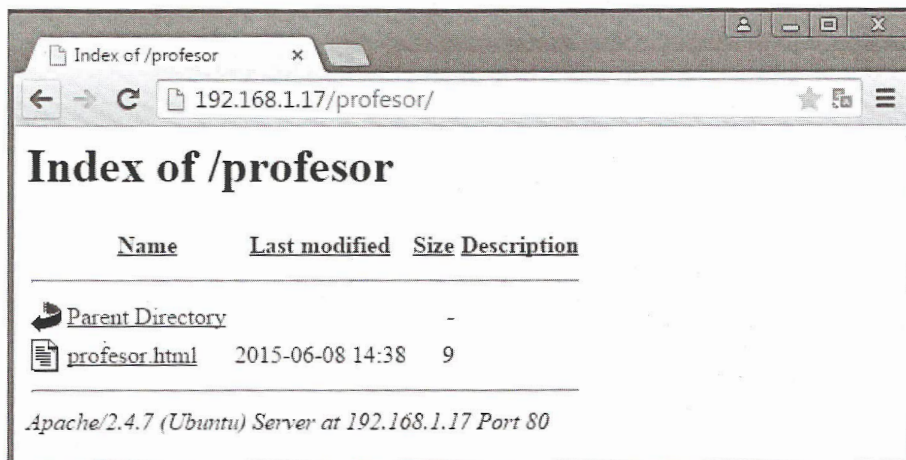


Figura 5.66: Conexión desde **DesarrolloW7XX**

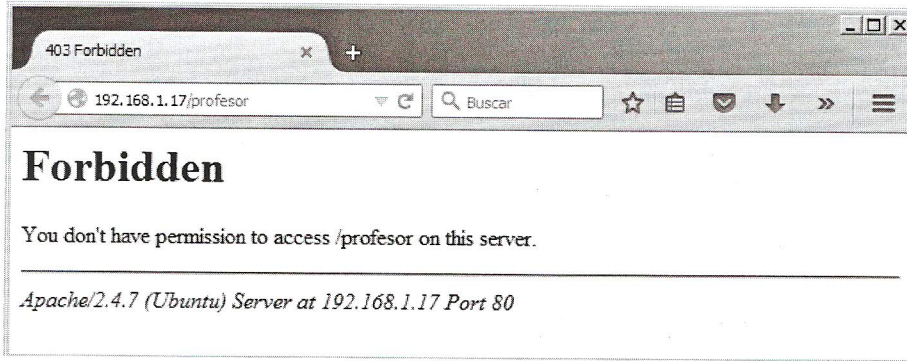


Figura 5.67: Conexión desde la máquina real

6. Prueba a permitir/denegar el acceso desde las máquinas de tus compañeros.

## 5.10. Autenticación y autorización *Basic* y *Digest*

En la máquina **ServidorLinuxXX** configura la autenticación HTTP *Basic* sobre el directorio `/var/www/html/profesor` para que solo puedan acceder los usuarios **profesor1** y **profesor2**. Configura la autenticación HTTP *Digest* sobre el directorio `/var/www/html/departamento` para que solo puedan acceder los usuarios **admin1** y **admin2**.

### 1. Autenticación HTTP *Basic*

- 1.1. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administrador.
- 1.2. Comprueba, consultando el directorio `/etc/apache2/mods-enabled`, que el módulo ***auth\_basic*** está habilitado.
- 1.3. Para usar la autenticación *basic* hay que crear un fichero accesible por *Apache* en el que se guardarán los usuarios y sus contraseñas. Para crear este fichero se utilizará el comando **htpasswd** (<http://httpd.apache.org/docs/2.4/programs/htpasswd.html>).
  - a Instala el paquete **apache2-utils** que contiene **htpasswd**.

```
sudo apt-get install apache2-utils
```

- b Crea el fichero y añade el usuario **profesor1** (la opción `-c` es para crear el fichero).

```
sudo htpasswd -c /etc/apache2/passwd profesor1
```

- c Añade el usuario **profesor2** (no se usa la opción `-c` porque el fichero ya existe).

```
sudo htpasswd /etc/apache2/passwd profesor2
```

- 1.4. Edita el fichero de configuración `/etc/apache2/sites-available/000-default.conf` y permite el acceso a directorio `/var/www/html/profesor` a los usuarios **profesor1** y **profesor1**, es necesario utilizar las directivas `<RequireAll>` y `<RequireAny>` para controlar cuáles de las directivas *Require* queremos que se cumplan. Figura 5.68.



- 1.5. Reinicia el servidor para que los cambios tengan efecto.
- 1.6. Desde **DesarrolloW7XX** accede a `http://192.168.1.X7/profesor/` con el usuario **profesor1**, Figura 5.69. Intenta el acceso con otro usuario ¿Es posible?

```
<Directory /var/www/html/profesor>
  Options Indexes FollowSymLinks
  AllowOverride None
  AuthType Basic
  AuthName "Acceso restringido"
  AuthUserFile /etc/apache2/passwd
  <RequireALL>
    Require user profesor1 profesor2
  <RequireAny>
    Require ip 127.0.0.1
    Require ip 192.168.1.16
  </RequireAny>
</RequireALL>
</Directory>
```

Figura 5.68: Autenticación *Basic*

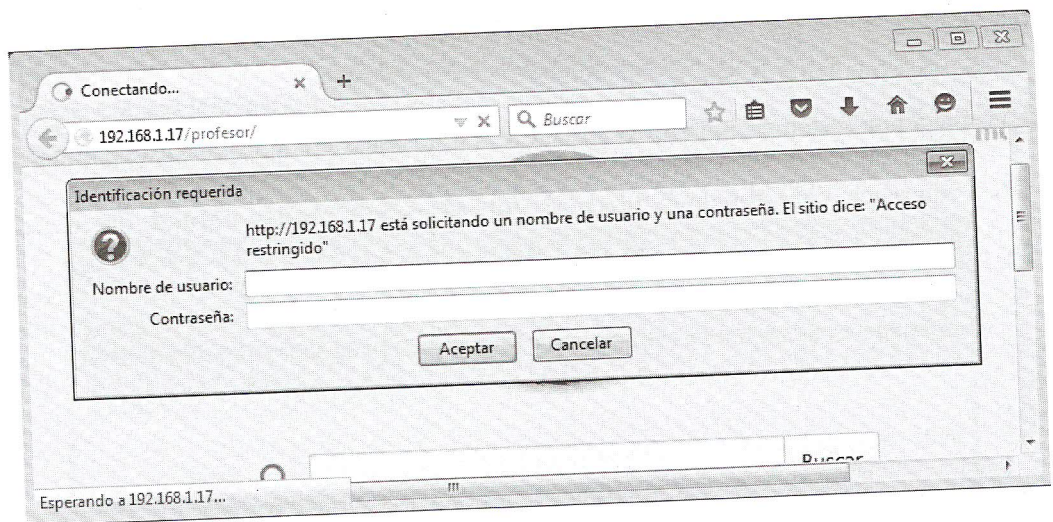


Figura 5.69: Conexión desde **DesarrolloW7XX**

## 2. Autenticación HTTP *Digest*

- 2.1. Crea en directorio `/var/www/html/departamento`. Dentro del directorio crea un fichero denominado **departamento.html** con el contenido que quieras.
- 2.2. Habilita el módulo *auth\_digest*.

```
sudo a2enmod auth_digest
```

- 2.3. Reinicia el servidor para que los cambios tengan efecto.

2.4. Para usar la autenticación *digest* hay que crear un fichero accesible por *Apache* en el que se guardarán los usuarios y sus contraseñas asociados a un dominio (*realm*). Para crear este fichero se utilizará el comando `htdigest` (<http://httpd.apache.org/docs/2.4/es/programs/htdigest.html>).

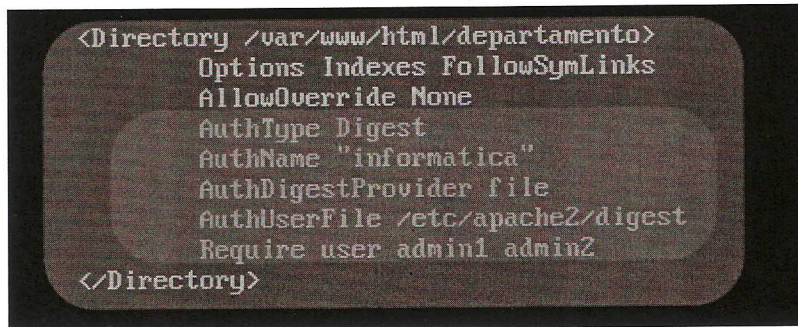
a Crea el fichero y añade el usuario **admin1** al dominio **informatica** (la opción `-c` es para crear el fichero).

```
sudo htdigest -c /etc/apache2/digest informatica admin1
```

b Añade el usuario **admin2** (no se usa la opción `-c` porque el fichero ya existe).

```
sudo htdigest /etc/apache2/digest informatica admin2
```

2.5. Edita el fichero de configuración `/etc/apache2/sites-available/000-default.conf` y permite el acceso a directorio `/var/www/html/departamento` a los usuarios **admin1** y **admin2**, Figura 5.70.



```
<Directory /var/www/html/departamento>
    Options Indexes FollowSymLinks
    AllowOverride None
    AuthType Digest
    AuthName "informatica"
    AuthDigestProvider file
    AuthUserFile /etc/apache2/digest
    Require user admin1 admin2
</Directory>
```

Figura 5.70: Autenticación *Digest*

2.6. Desde **DesarrolloW7XX** accede a `http://192.168.1.X7/departamento/` con el usuario **admin1**, Figura 5.71. Intenta el acceso con otro usuario ¿Es posible?