

**Índice**

[**A) Módulos de Linux 2**](#_f5x6ye5007tp)

[A.1) Módulos 2](#_1e9fe9nipa8)

[A.2 Módulo userdir 4](#_w142mjazj8u7)

[A.3 Módulo userdir en el servidor de clase 6](#_syuifmlqkenh)

[**B) Control de acceso por IP y nombre de dominio 11**](#_9jry8xpwv1mn)

[**C) AUTENTICACIÓN Y AUTORIZACIÓN BASIC Y DIGEST 16**](#_om98si3v0xg7)

[C.1 Autenticación Basic 16](#_7ete2hgra95o)

[C.2. Autenticación Digest 19](#_yxwo3m28jhcn)

[**D) FICHEROS .htaccess 24**](#_nh5h87ndk7qe)

[**E) FICHEROS DE REGISTROS (LOGS) 27**](#_jtds62ty934a)

[**F) MÓDULOS STATUS E INFO 29**](#_ppe2qjdksroe)

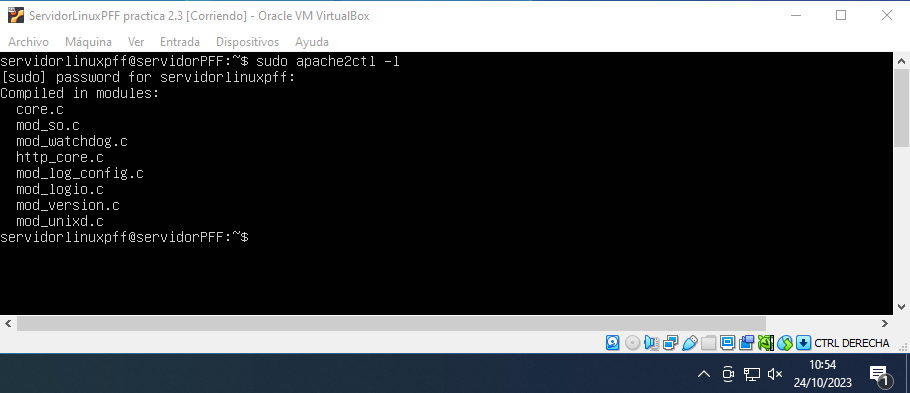
[**G) WEBALIZER 33**](#_ojj4ywojr6cs)

[**H) GITHUB 36**](#_wpfx6mfrnke)

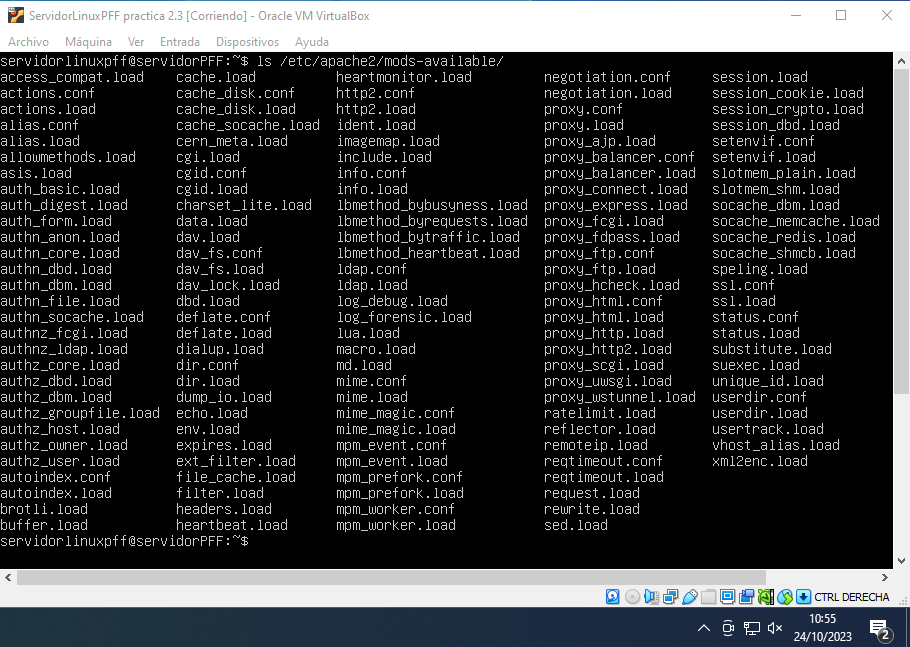
# **Módulos de Linux**

## **A.1) Módulos**

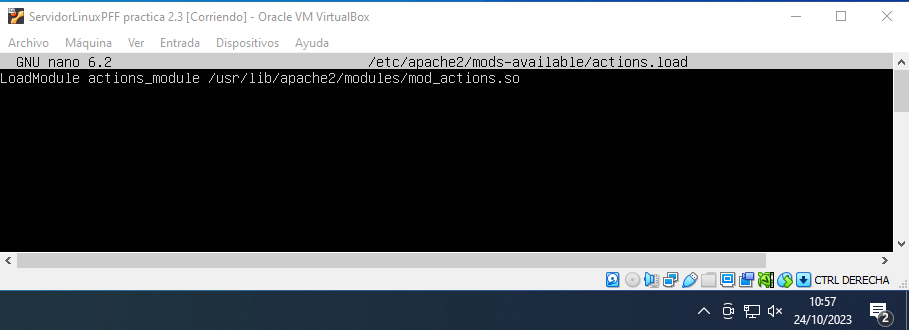
**PASO 1)** Comprueba los módulos estáticos que se han cargado al compilar el servidor ejecutando el comando correspondiente.



**PASO 2)** Comprueba los módulos que se han cargado dinámicamente al arrancar el servidor.



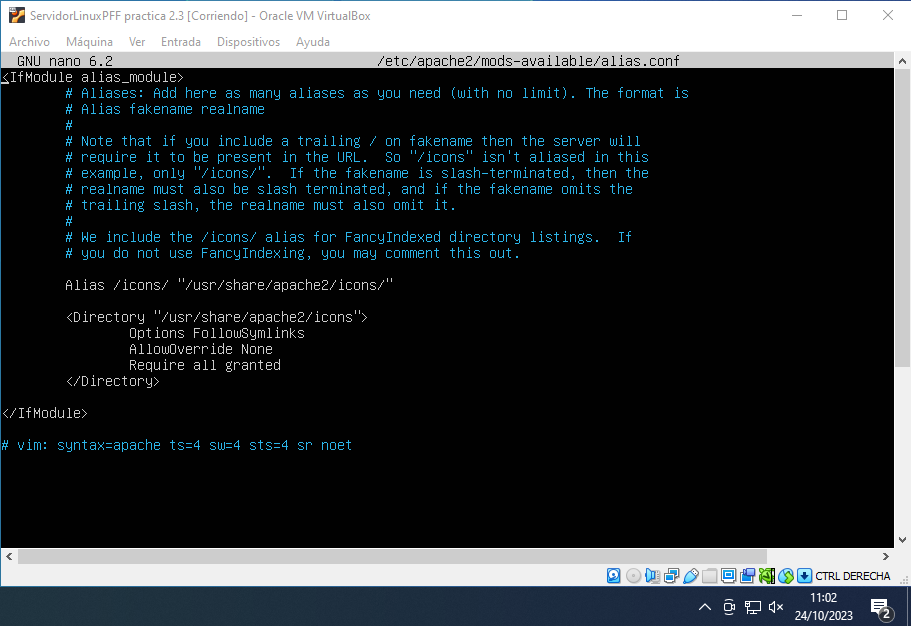
**PASO 3)** Edita uno de los archivos .load y observa cómo se usa la directiva LoadModule. ¿Qué extensión tienen los archivos donde está el código del módulo?



Tienen la extensión “.so”.

**PASO 4)** Edita uno de los archivos .conf y observa cómo se añaden directivas dentro del módulo.

¿Qué etiquetas se utilizan en estos archivos?



Se usan las etiquetas <IfModule alias\_module> y <Directory>. En la primera de ella se incluye la definición del alias junto a la etiqueta <Directory>, que establece las diferentes opciones de configuración que se van a aplicar a los ficheros del directorio que se indique, en este caso “/usr/share/apache2/icons”.

**PASO 5)** Consulta el directorio /usr/lib/apache2/modules/ ¿qué archivos contiene?

Los archivos que contienen el código de los diferentes módulos.

## **A.2 Módulo userdir**

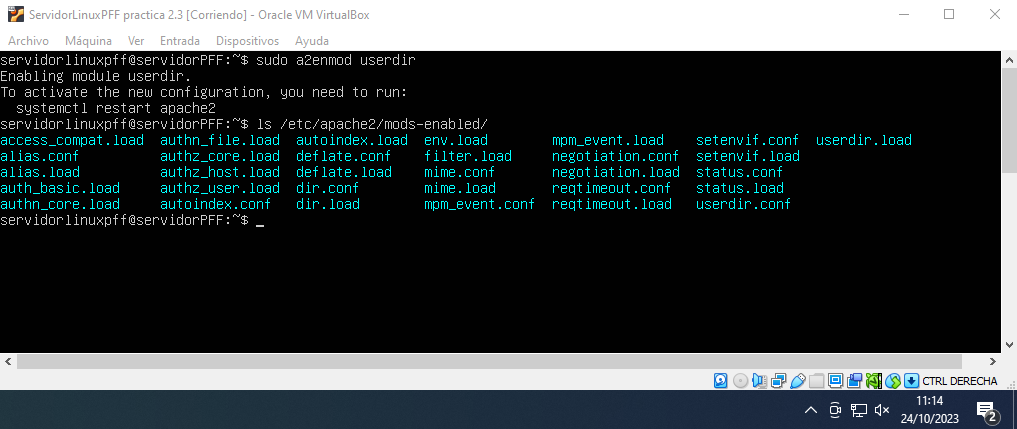
**PASO 1)** Comprueba si el módulo userdir está habilitado. ¿Lo está?

No se encuentra habilitado.

**PASO 2)** Si no lo está, habilita el módulo userdir.

Habilitado con el comando a2enmod userdir.

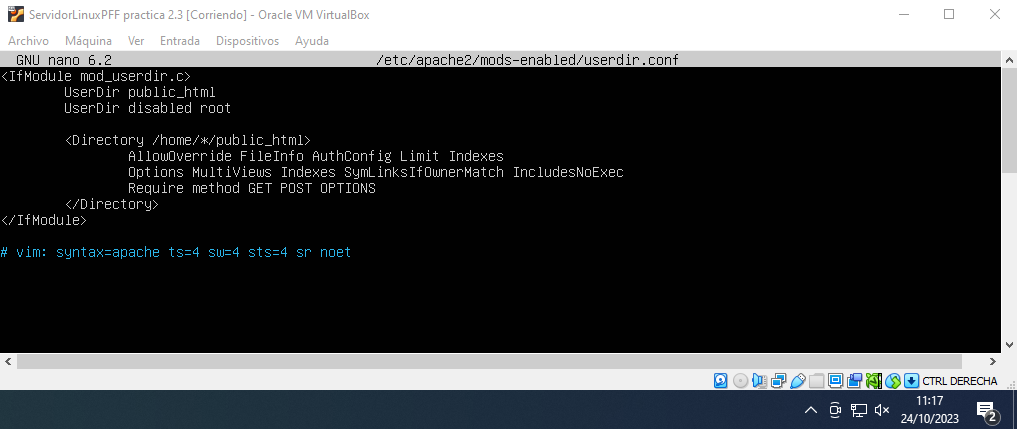
**PASO 3)** Verifica ahora si el módulo está habilitado.



Ahora sí se encuentra habilitado.

**PASO 4)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 5)** Consulta el archivo **/etc/apache2/mods-enabled/userdir.conf**. ¿Cuál es el único usuario para el que está deshabilitado el uso de directorios personales? ¿Cuál es el subdirectorio que deben crear los usuarios en su carpeta home para poner sus páginas personales?

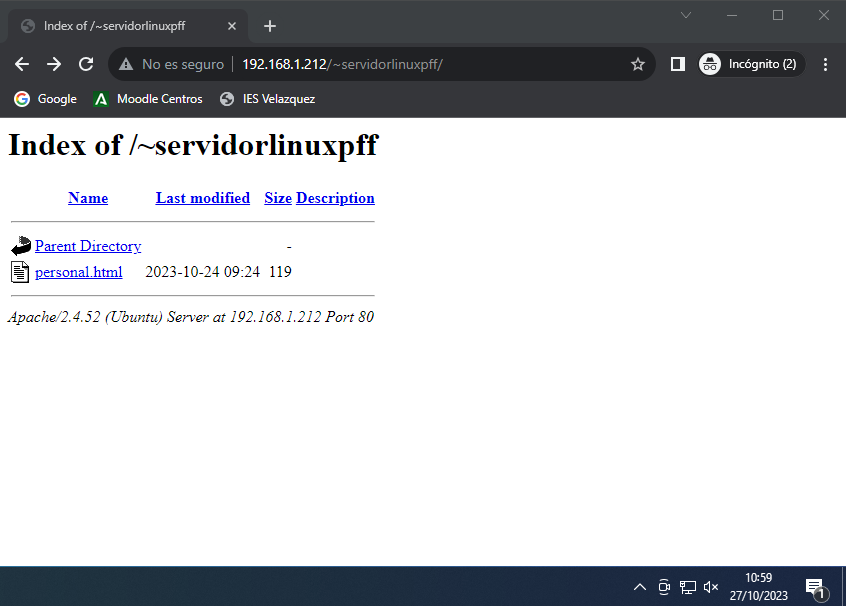


Está deshabilitado únicamente para el root.

El subdirectorio que debe crear el usuario en su carpeta home es “public\_html”.

**PASO 6)** Crea el directorio necesario dentro de tu usuario y añade un fichero denominado **personal.html** con el contenido Tu nombre e indicando que es personal.

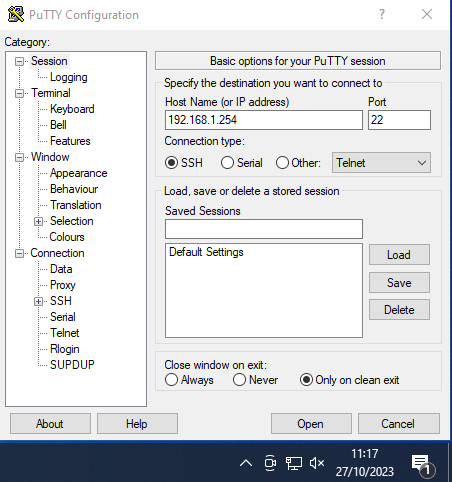
**PASO 7)** Desde la máquina física, abre un navegador y accede al directorio raíz de tu usuario Linux.

****

**PASO 8)** Descarga el módulo y reinicia el servidor para que los cambios tengan efecto.

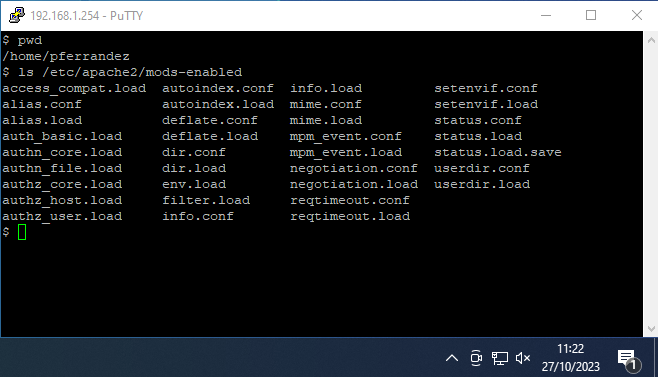
## **A.3 Módulo userdir en el servidor de clase**

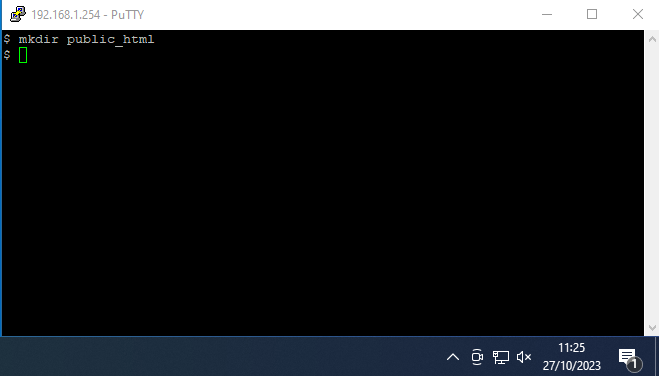
**PASO 1)** Accede al servidor a través de Putty. IP: 192.168.1.254

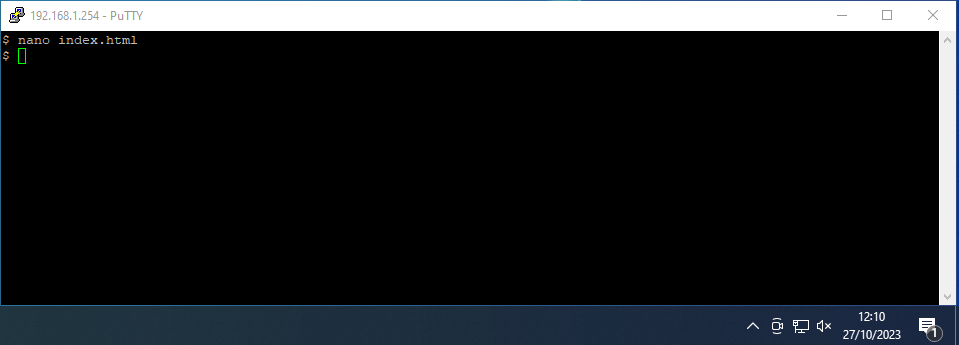


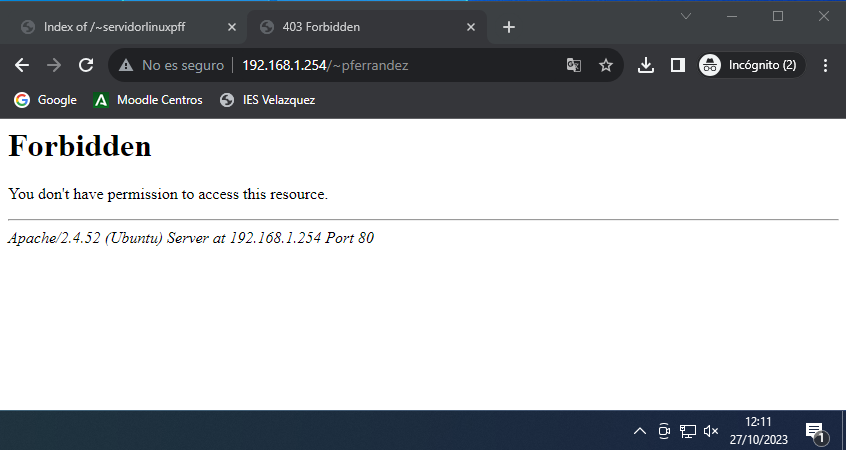
**PASO 2)** Da ***los pasos necesarios*** para qué al acceder a http://192.168.1.254/~agutierrez se vea tu página web en el servidor.

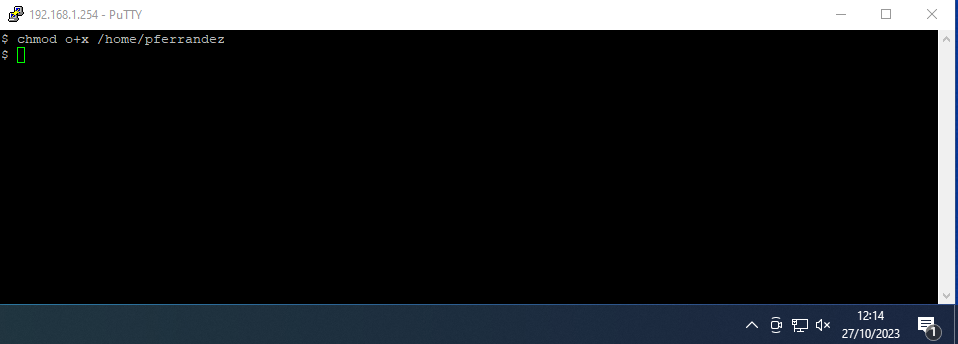
La página debe contener la IP de servidor y tu nombre completo

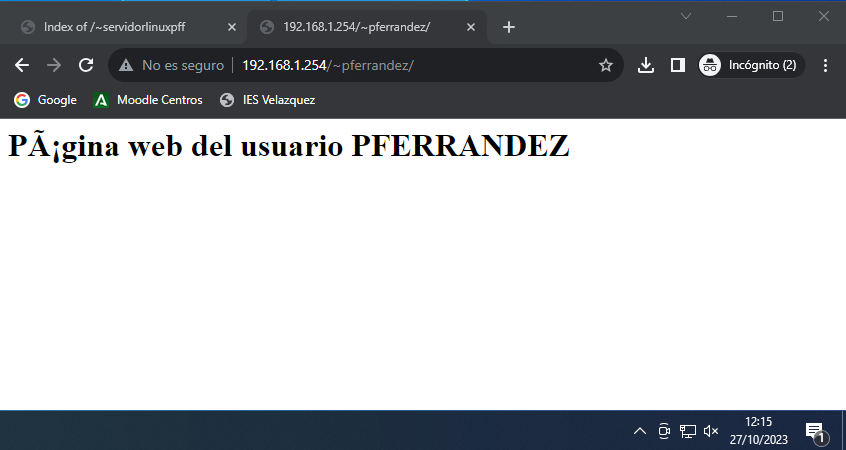












# 

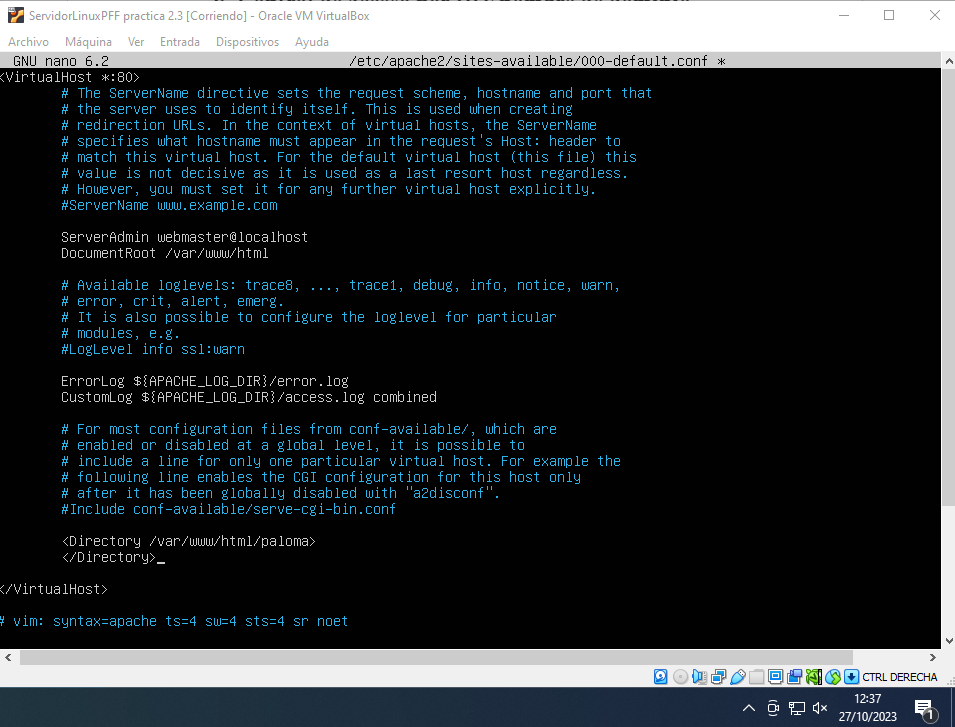
# **Control de acceso por IP y nombre de dominio**

**PASO 1)** Comprueba si está habilitado el módulo **authz\_host**. ¿Lo está?

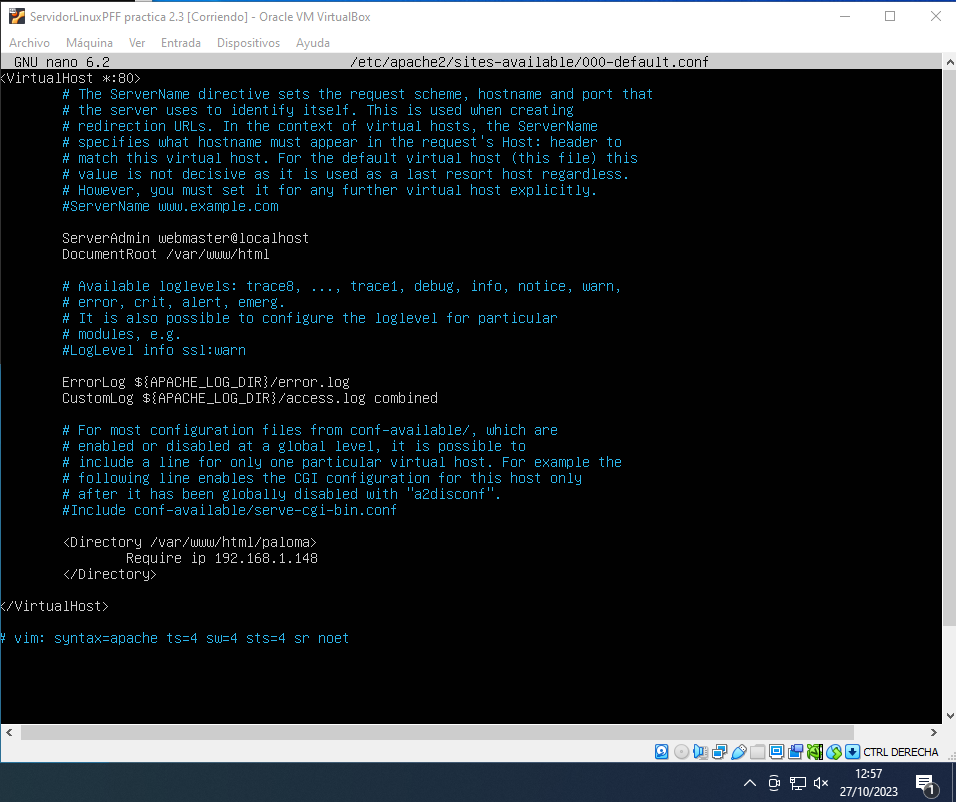
Sí, está habilitado.

**PASO 2)** Crea un directorio ***/var/www/html/tuNombre/***. Dentro del directorio crea un archivo y llámalo **tuNombre.html** y añade el contenido que quieras.

**PASO2)** Edita el fichero de configuración **/etc/apache2/sites-available/000-default.conf** y añade la directiva Directory para el recurso creado anteriormente.

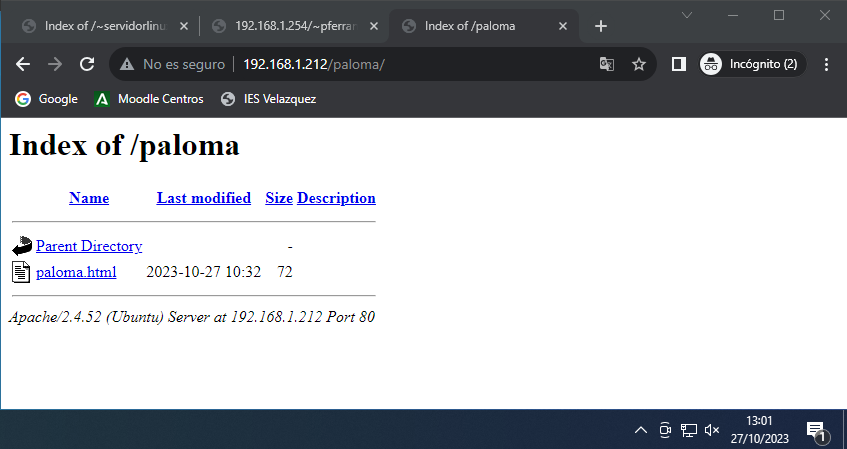


**PASO 3)** Añade dentro de la directiva anterior las directivas de acceso necesarias para que la máquina física, a partir de su dirección IP, pueda acceder a este recurso pero no la máquina del compañero (échale un vistazo al enlace informativo del módulo authz\_host que hay más arriba).

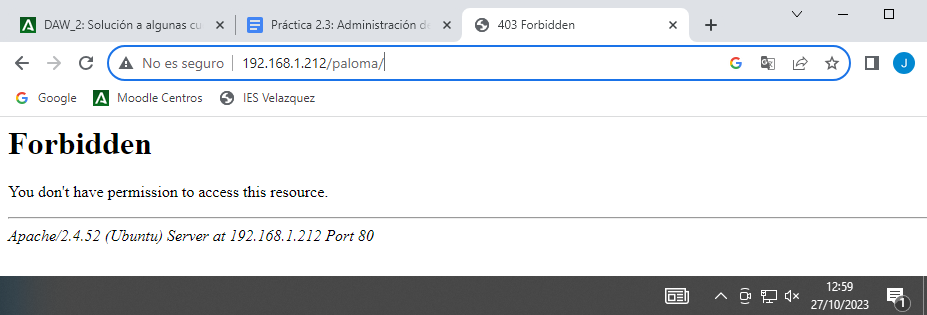


**PASO 4)** Reinicia el servidor para que los cambios tengan efecto.

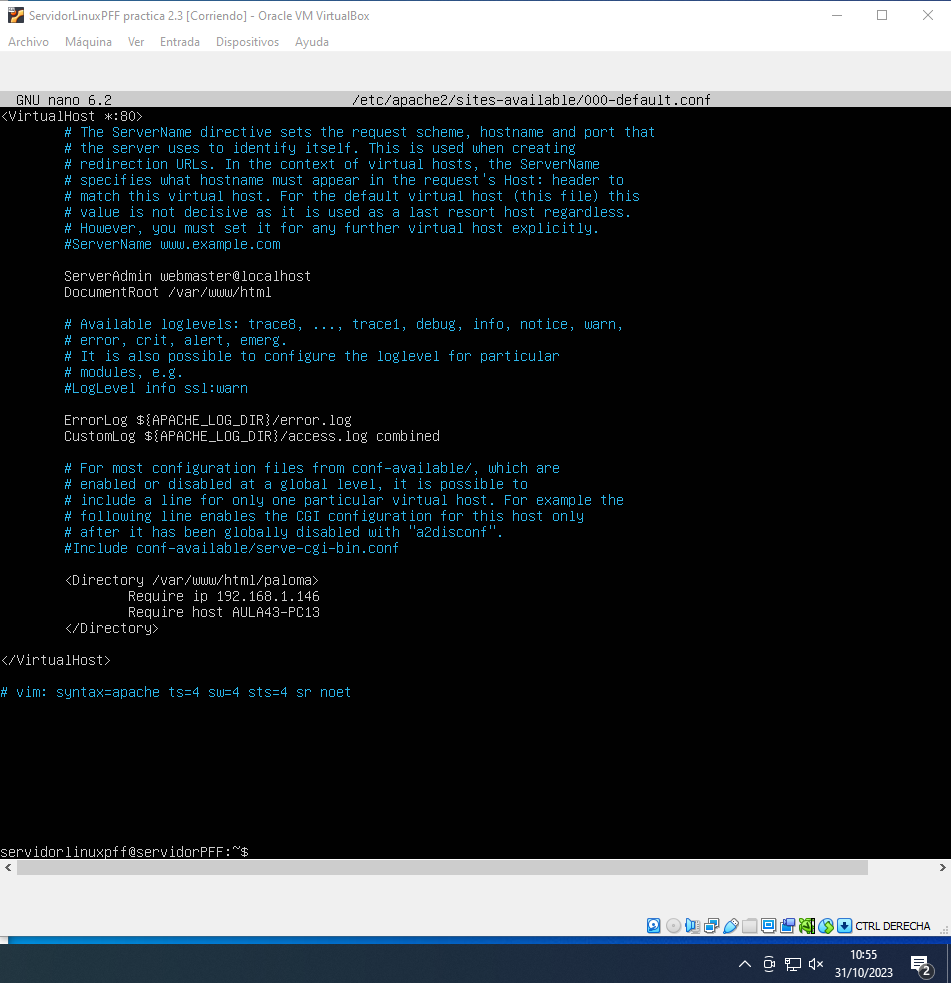
**PASO 5)** Abre un navegador desde tu máquina física e intenta acceder al recurso **/tuNombre/** y comprueba que se puede.



**PASO 6)** Abre un navegador desde la máquina del compañero e intenta acceder al recurso **/tuNombre/** y comprueba que no se puede.

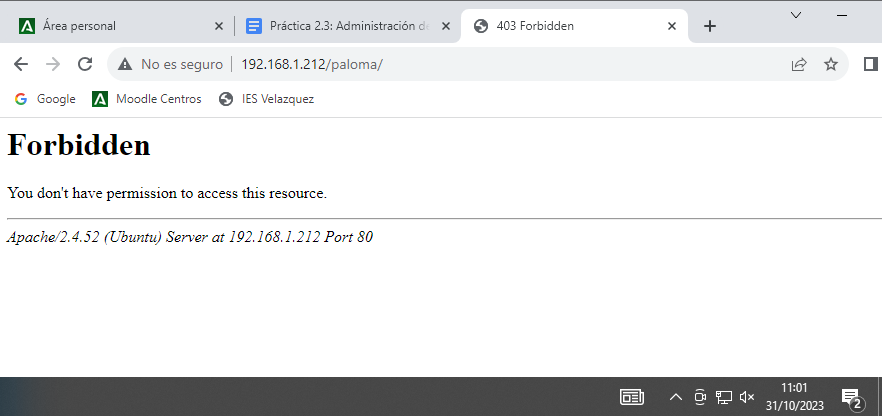
****

**PASO 7)** Añade el acceso al recurso de tu carpeta para la máquina del compañero pero **usando su nombre de host en vez de su IP**.



**PASO 8)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 9)** Abre un navegador desde la máquina del compañero e intenta acceder al recurso **/tuNombre/** y comprueba que ahora sí se puede.

****

# 

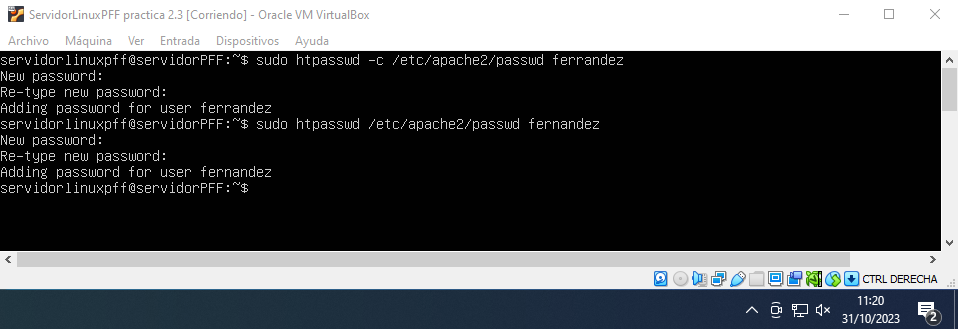
# **AUTENTICACIÓN Y AUTORIZACIÓN BASIC Y DIGEST**

## **C.1 Autenticación Basic**

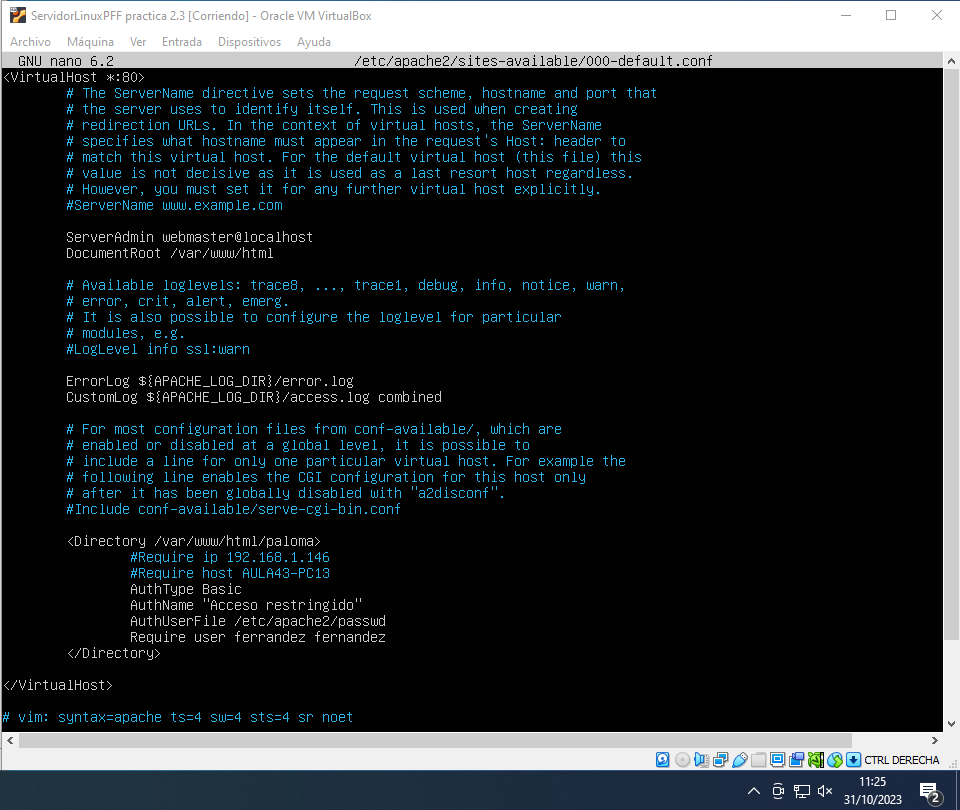
**PASO 1)** Comprueba si el módulo **auth\_basic** está habilitado, si no lo está, habilítalo.

**PASO 2)** Vamos a crear el directorio **/nombreAlumno/** dentro de nuestro directorio raíz **/var/www/html/.** Dentro añadiremos un archivo **nombreAlumno.html** donde incluiremos el contenido que queramos.

**PASO 3)** Para usar la autenticación Basic hay que crear un fichero accesible (el fichero que se creará será **/etc/apache2/passwd**) en el que se guardarán los usuarios y contraseñas. Para crear ese fichero se utilizará el comando httpaswd (ver cuadro arriba). Añade los usuarios **apellido1** y **apellido2**.

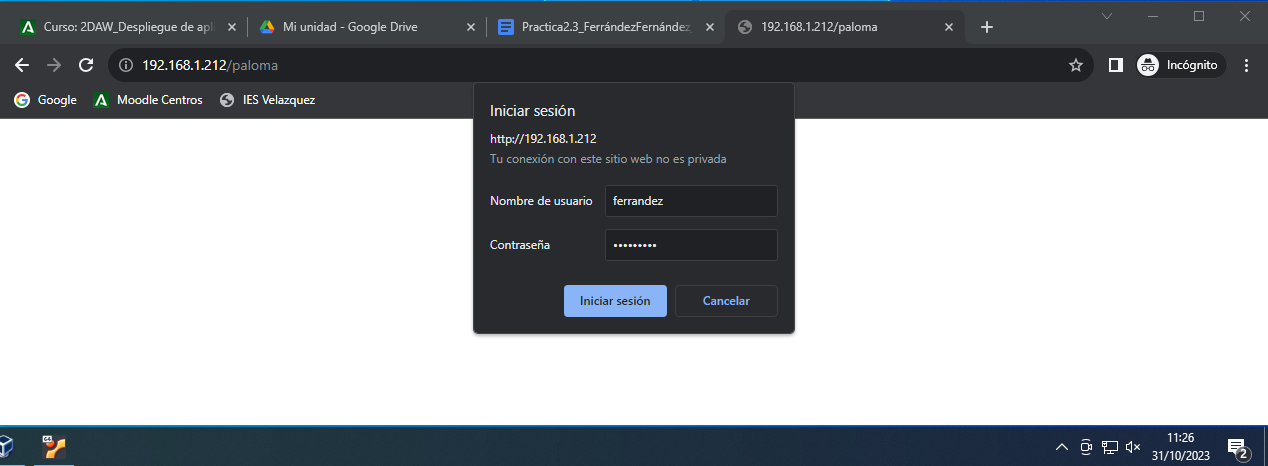


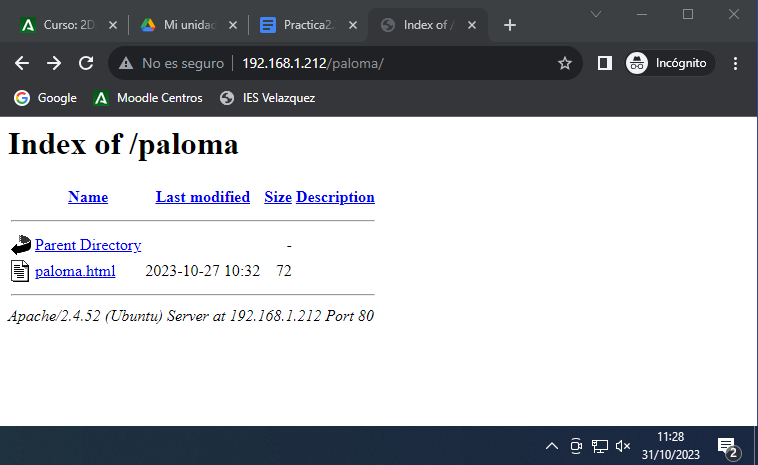
**PASO 4)** Edita el fichero de configuración **/etc/apache2/sites-available/000-default.conf** y permite el acceso al directorio **/var/www/html/nombreAlumno** a los usuarios **apellido1** y **apellido2** (ver cuadro ejemplo arriba).



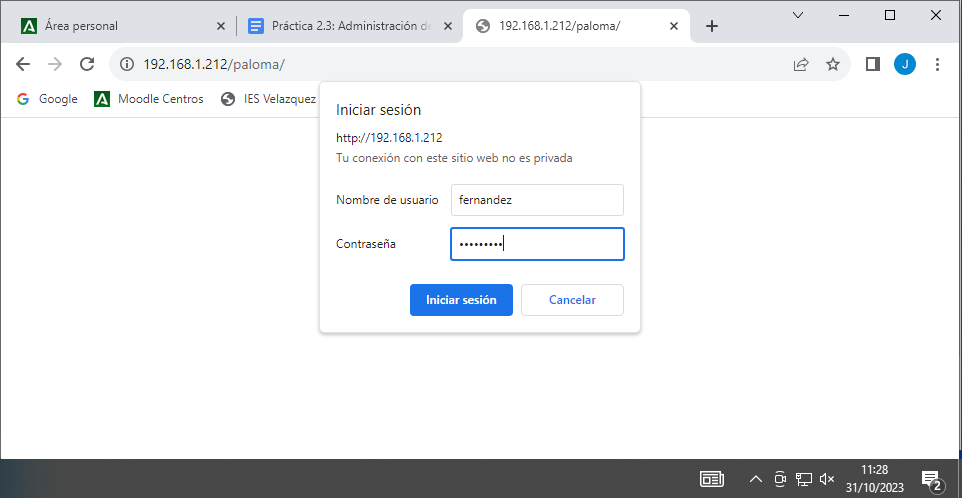
**PASO 5)** Reinicia el servidor para que los cambios tengan efecto.

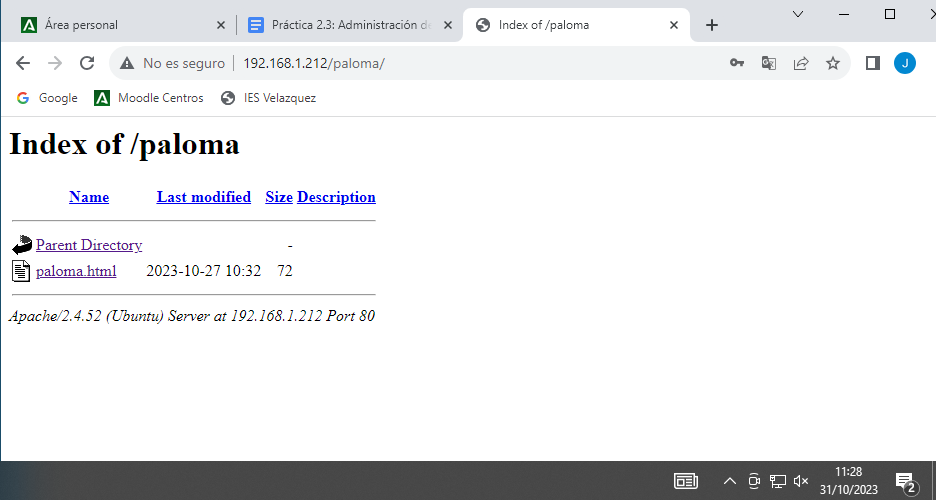
**PASO 6)** Abre un navegador desde tu máquina física y accede al recurso **/nombreAlumno** como usuario **apellido1**.





**PASO 7)** Abre un navegador desde la máquina de un compañero y accede al recurso **/nombreAlumno** como usuario **apellido2**.

****

****

## **C.2. Autenticación Digest**

**PASO 1)** Comprueba si el módulo **auth\_digest** está habilitado, si no lo está, habilítalo.

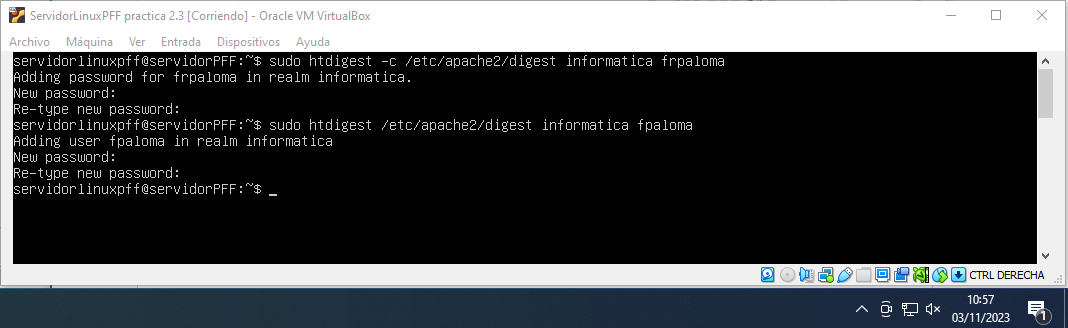
**PASO 2)** Vamos a crear el directorio **/tareac2/** dentro de nuestro directorio raíz **/var/www/html/.** Dentro añadiremos un archivo **tareac2.html** donde incluiremos el contenido que queramos.

**PASO 3)** Para usar la autenticación Digest también hay que crear un fichero accesible (el fichero que se creará será también **/etc/apache2/passwd** pero para digest) en el que se guardarán los usuarios y contraseñas, pero esta vez asociados a un dominio (en el cuadro ejemplo de arriba el dominio o “realm” es informática). Para crear ese fichero se utilizará el comando httdigest (ver cuadro arriba). Añade los usuarios **inicialPrimerApellidoNombre** y **inicialSegundoApellidoNombre**.

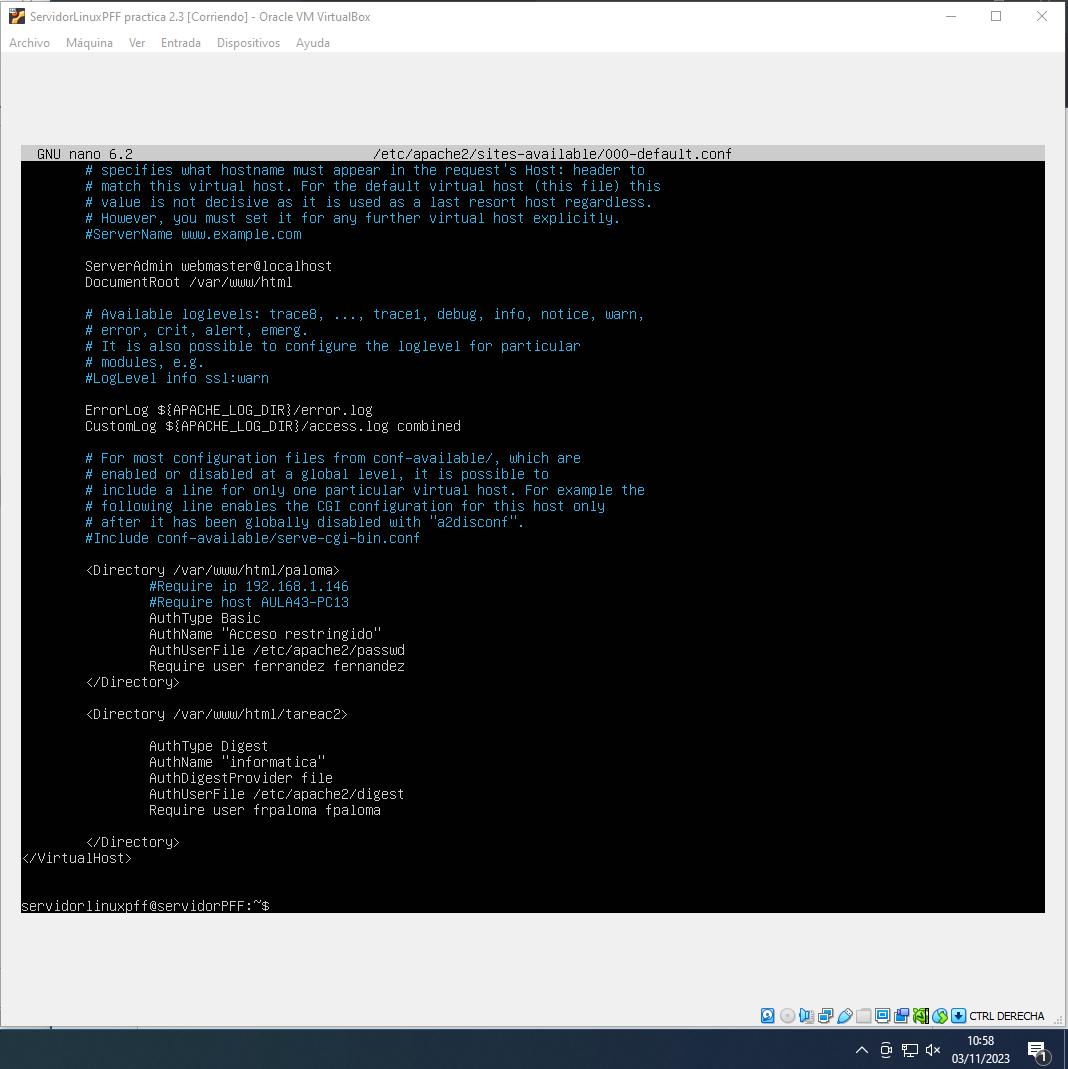
Ejemplo: Amapola Gutierrez de la Vega:

gamapola

vamapola

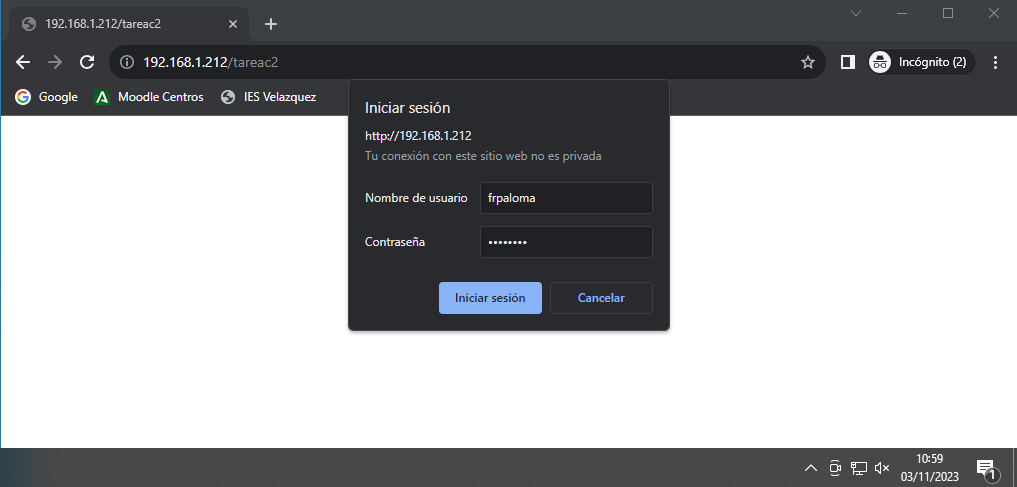


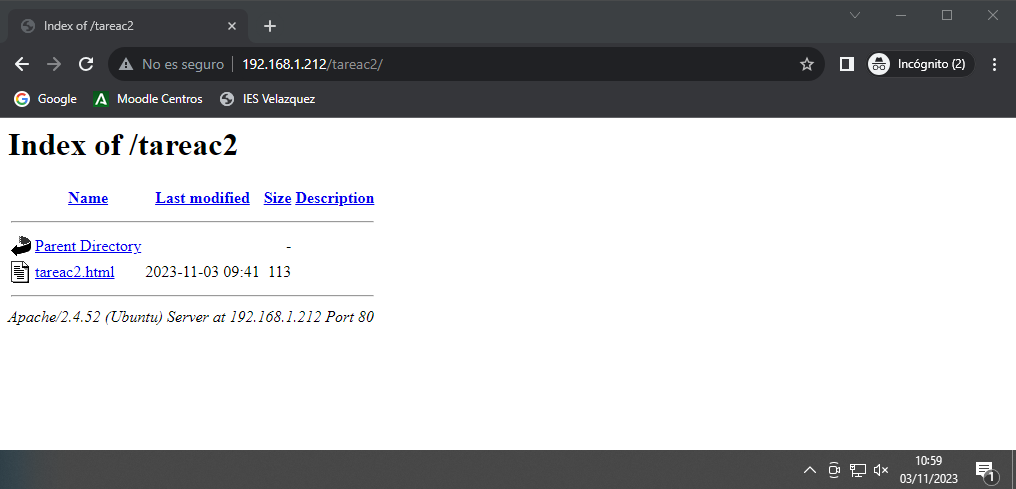
**PASO 4)** Edita el fichero de configuración **/etc/apache2/sites-available/000-default.conf** y permite el acceso al directorio **/var/www/html/tareac2** a los usuarios **inicialPrimerApellidoNombre** y **inicialSegundoApellidoNombre** (ver cuadro ejemplo arriba). Ten en cuenta que en la directiva AuthName tienes que poner lo mismo que pusiste en el dominio o “realm”.



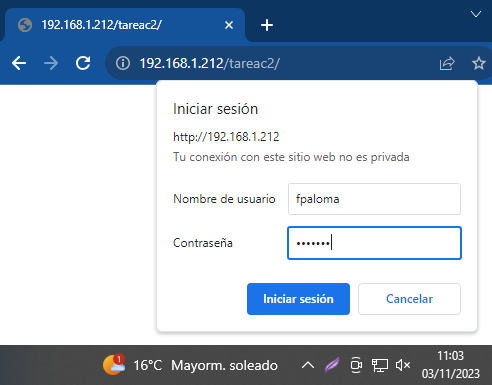
**PASO 5)** Reinicia el servidor para que los cambios tengan efecto.

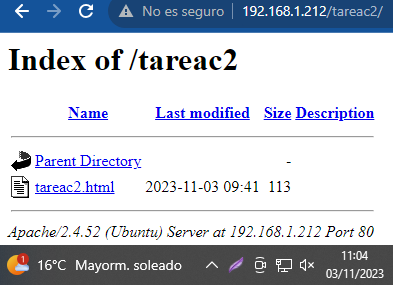
**PASO 6)** Abre un navegador desde tu máquina física y accede al recurso **/tareac2** como usuario **inicialPrimerApellidoNombre**.





**PASO 7)** Abre un navegador desde la máquina de un compañero y accede al recurso **/tareac2** como usuario **inicialSegundoApellidoNombre**.



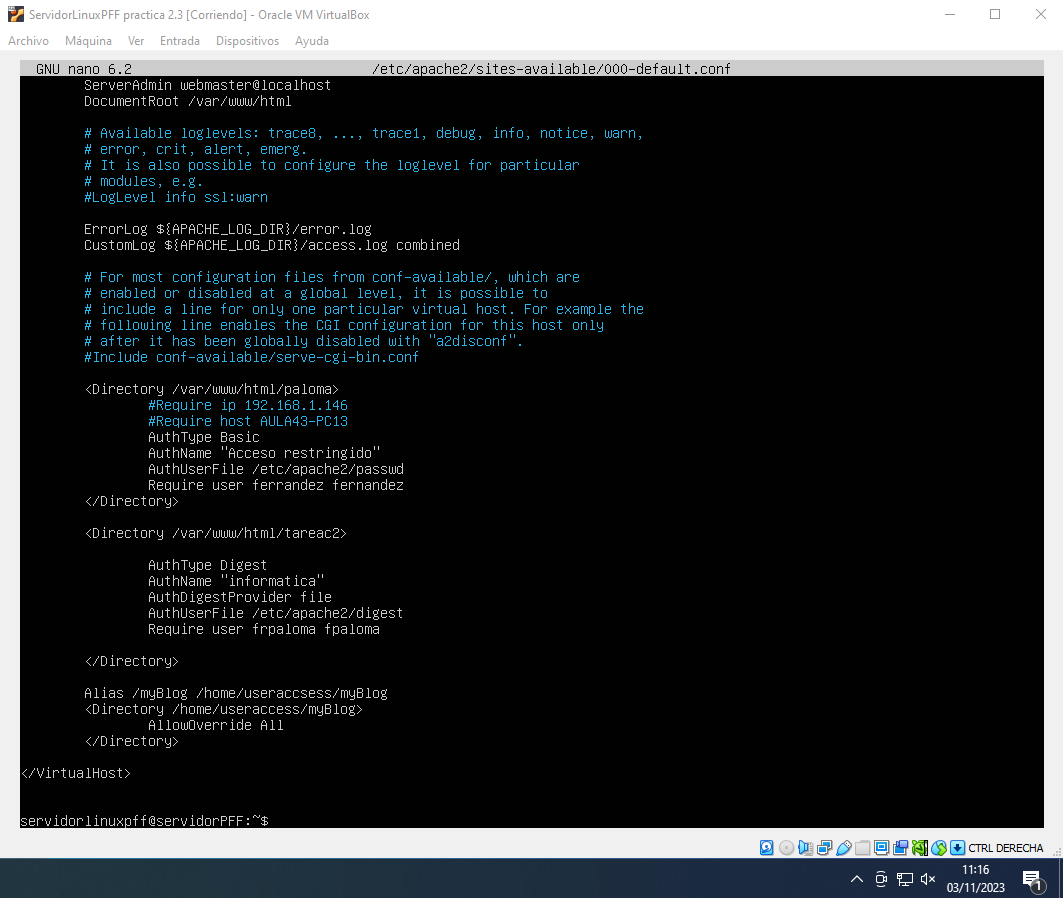


# 

# **FICHEROS .htaccess**

**PASO 1)** Crea el usuario **useraccess**.

**PASO 2)** Abre el fichero de configuración **000-default** y crea el **alias myBlog** dentro de la carpeta personal del nuevo usuario **useraccess**. Deja como única directiva **AllowOverride All**.

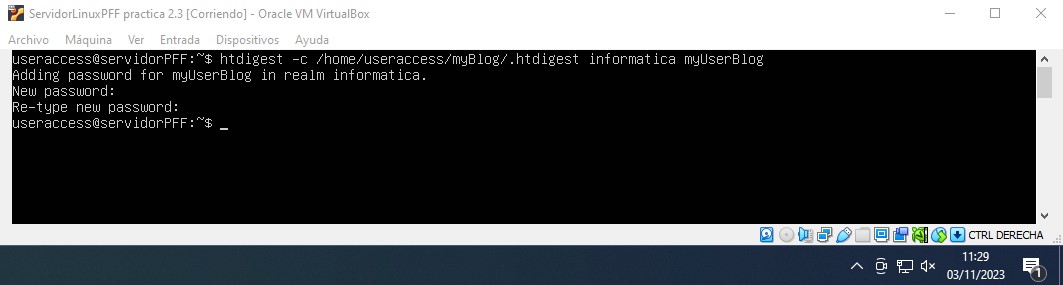
****

**PASO 3)** Reinicia el servidor para que los cambios tengan efecto.

**PASO 4)** Inicia sesión con el nuevo usuario **useraccess**.

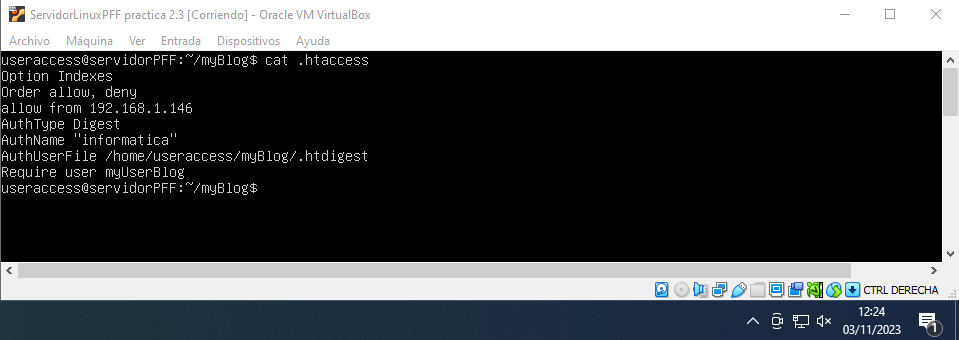
**PASO 5)** Crea dentro del directorio home de este usuario **el directorio myBlog**. Crea dentro el archivo **myBlog.html** con el contenido que quieras.

**PASO 6)** Para el acceso a los recursos de myBlog vamos a usar un tipo de autenticación Digest, por lo que dentro de este directorio vamos a crear el fichero **.htdigest** para el servidor informática y para el usuario myUserBlog (ver punto anterior acceso mediante Digest).

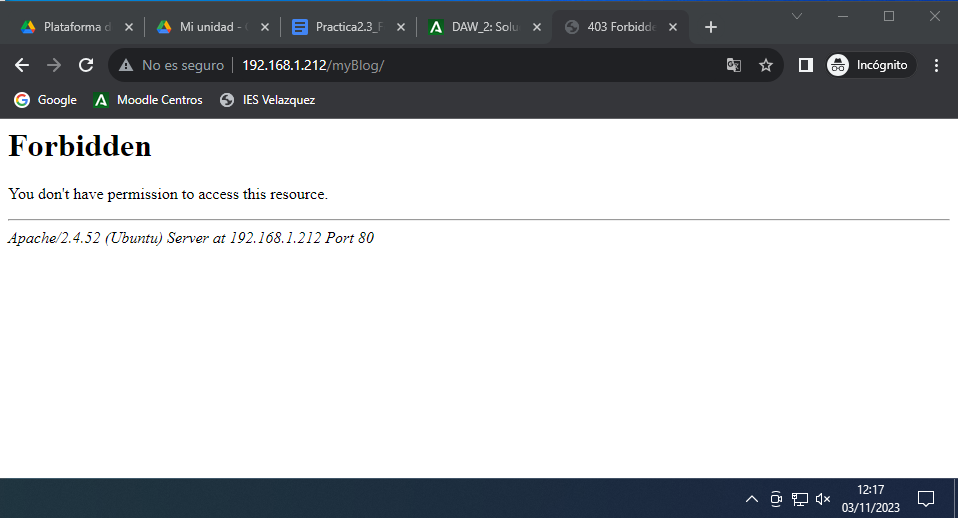


**PASO 7)** Ahora tendremos que crear el fichero **.htaccess** (también dentro de myBlog).

Dentro añadiremos las directivas necesarias para que se acceda solo desde nuestra máquina física (no es necesario poner las directivas Directory pues ya las incluimos en nuestro Alias para este directorio dentro de 000-default).



**PASO 8)** Vamos a acceder desde nuestra máquina física al recurso **myBlog** para ver que nos pide la autenticación y que podemos acceder al recurso.



# 

# **FICHEROS DE REGISTROS (LOGS)**

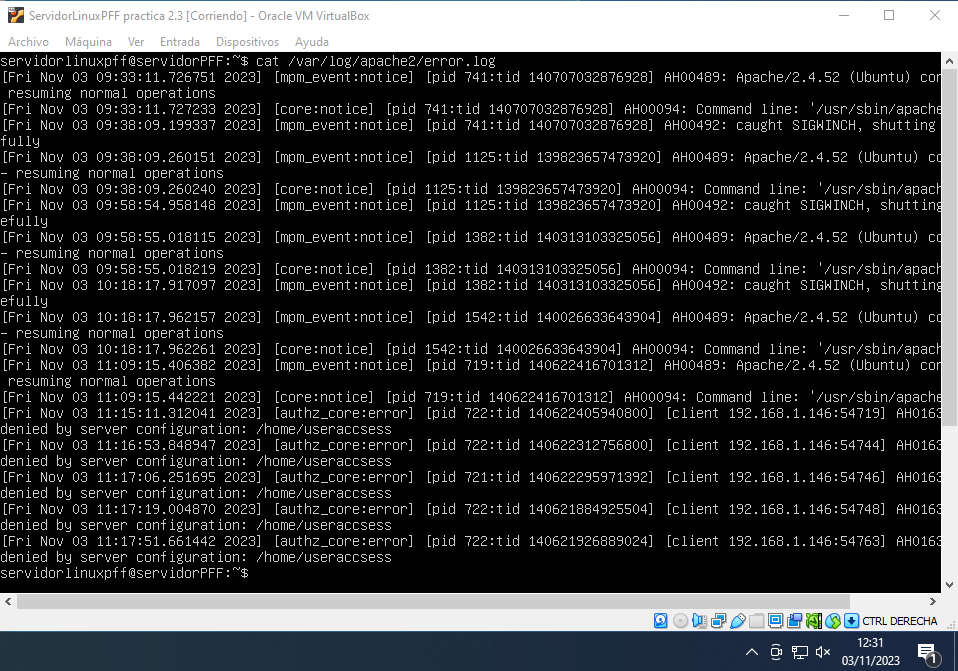
**PASO 1)** En tu servidor Linux, consulta el fichero 000-default y responde a las siguientes preguntas: **¿Qué directiva marca la ruta del archivo de los errores? ¿Cuál es el fichero de logs de errores? ¿Qué nivel de prioridad tiene?**

Lo marca la directiva ErrorLog, y el fichero correspondiente es error.log. El nivel de prioridad no está especificado.

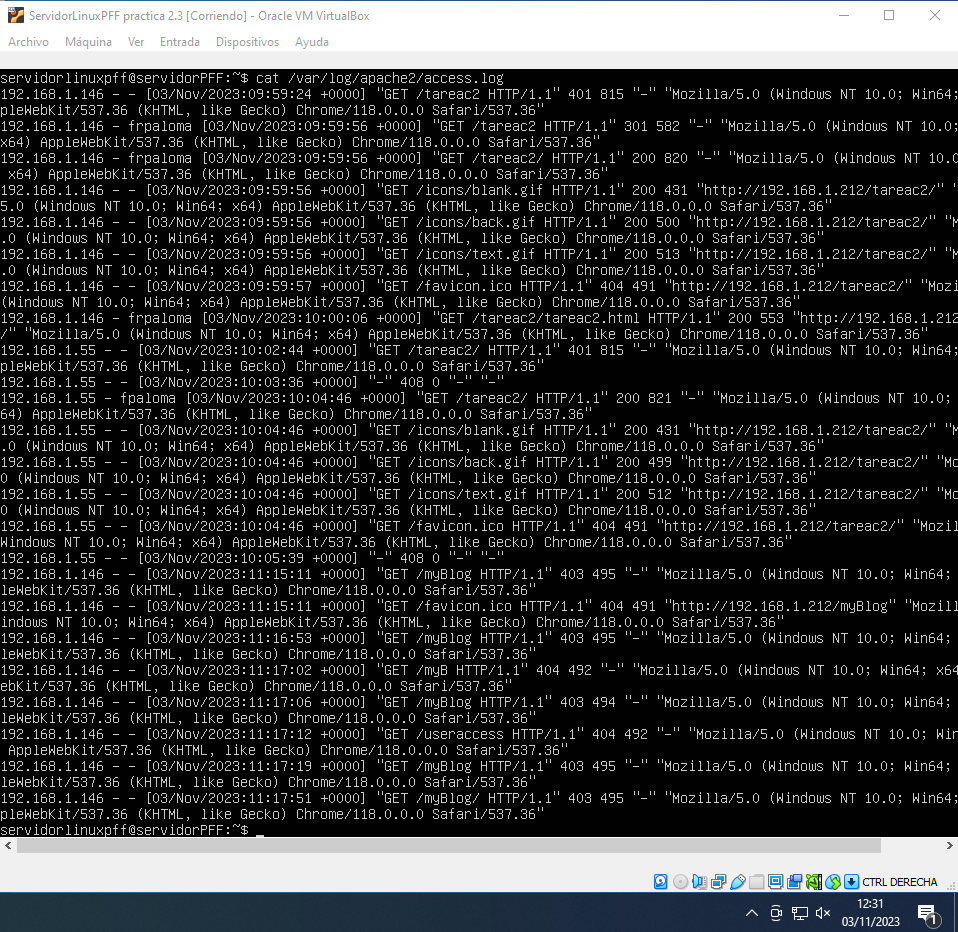
**¿Qué directiva marca la ruta del archivo de los accesos? ¿Cuál es el fichero de logs de accesos?**

Lo marca la directiva CustomLog, y el fichero de accesos es access.log

**PASO 2)** Consulta el log de errores



**PASO 3)** Consulta el log de accesos

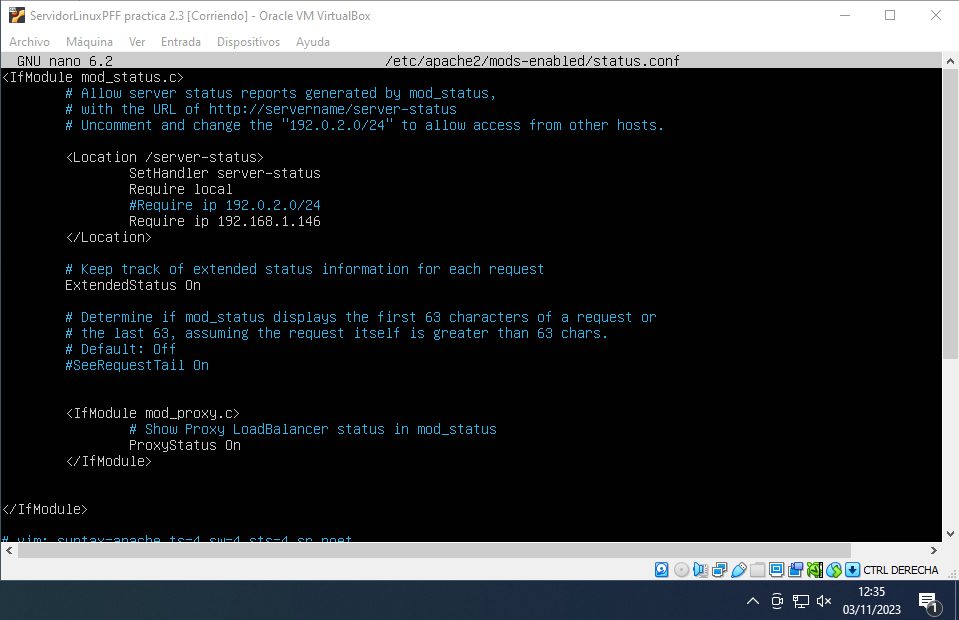


# 

# **MÓDULOS STATUS E INFO**

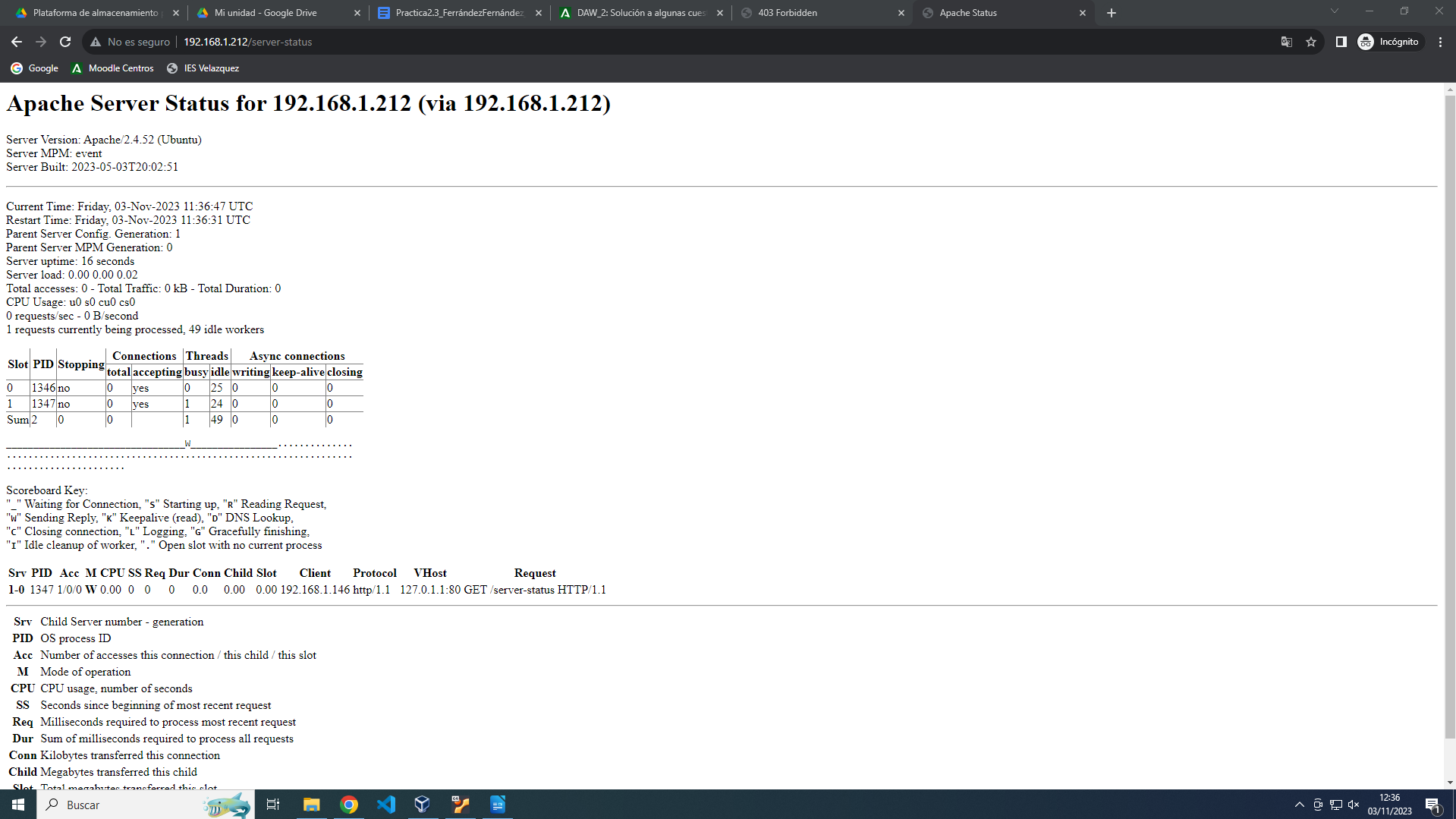
**PASO 1)** En tu servidor Linux, habilita el módulo **status**.

**PASO 2)** El fichero de configuración del módulo es **status.conf**, edita el fichero y habilita el acceso desde tu máquina física.

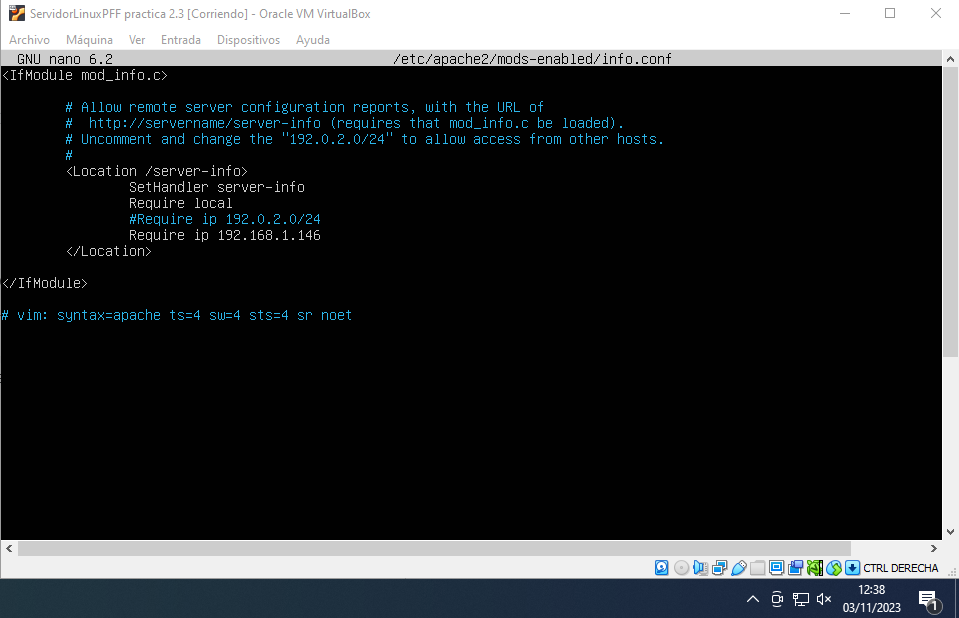


**PASO 3)** Reinicia el servidor para aplicar los cambios.

**PASO 4)** Desde tu máquina física conéctate al recurso server-status

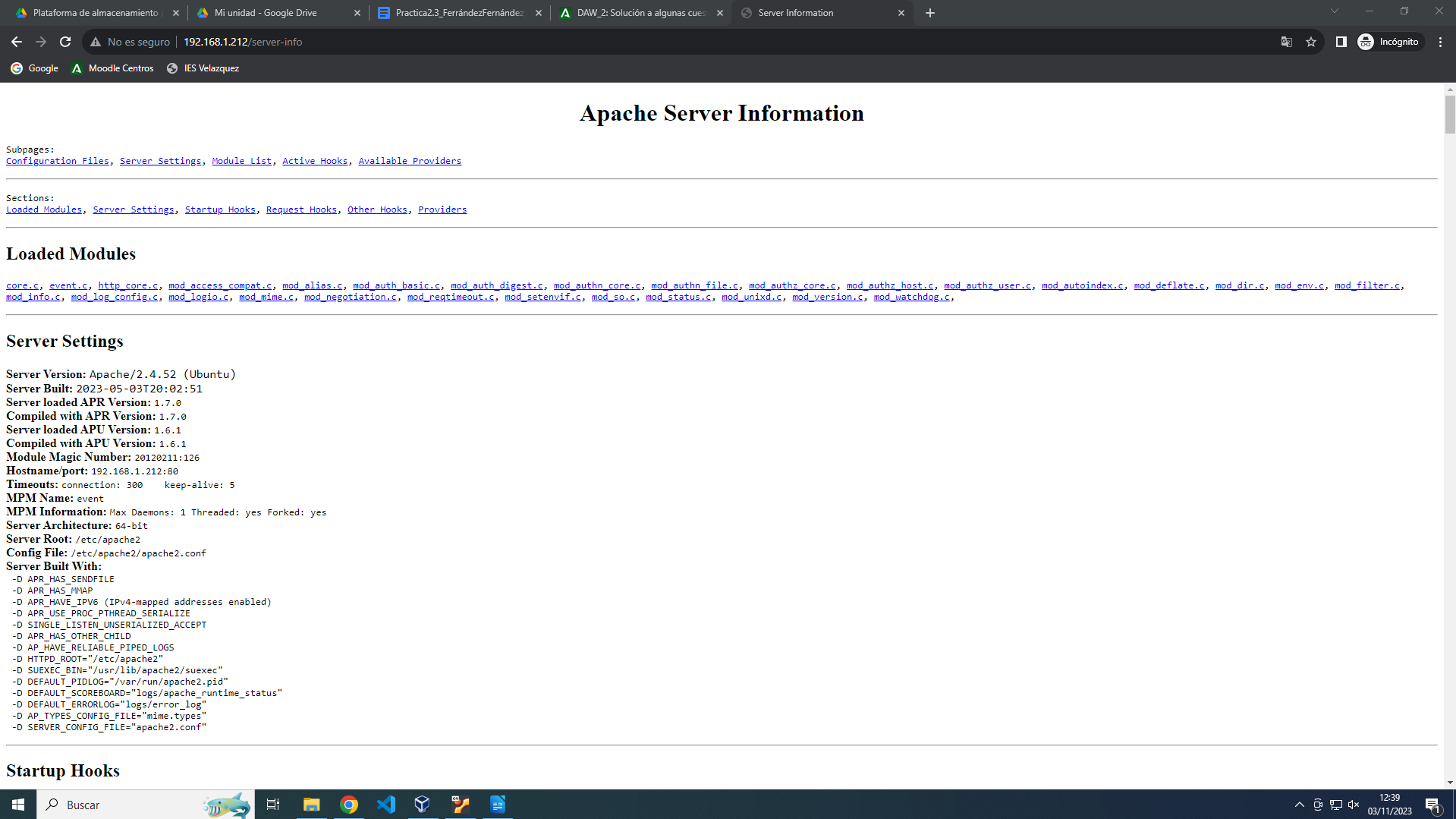
**  
PASO 5)** En tu servidor Linux, habilita el módulo **info**.

**PASO 6)** El fichero de configuración del módulo es **info.conf**, edita el fichero y habilita el acceso desde tu máquina física.



**PASO 7)** Reinicia el servidor para aplicar los cambios.

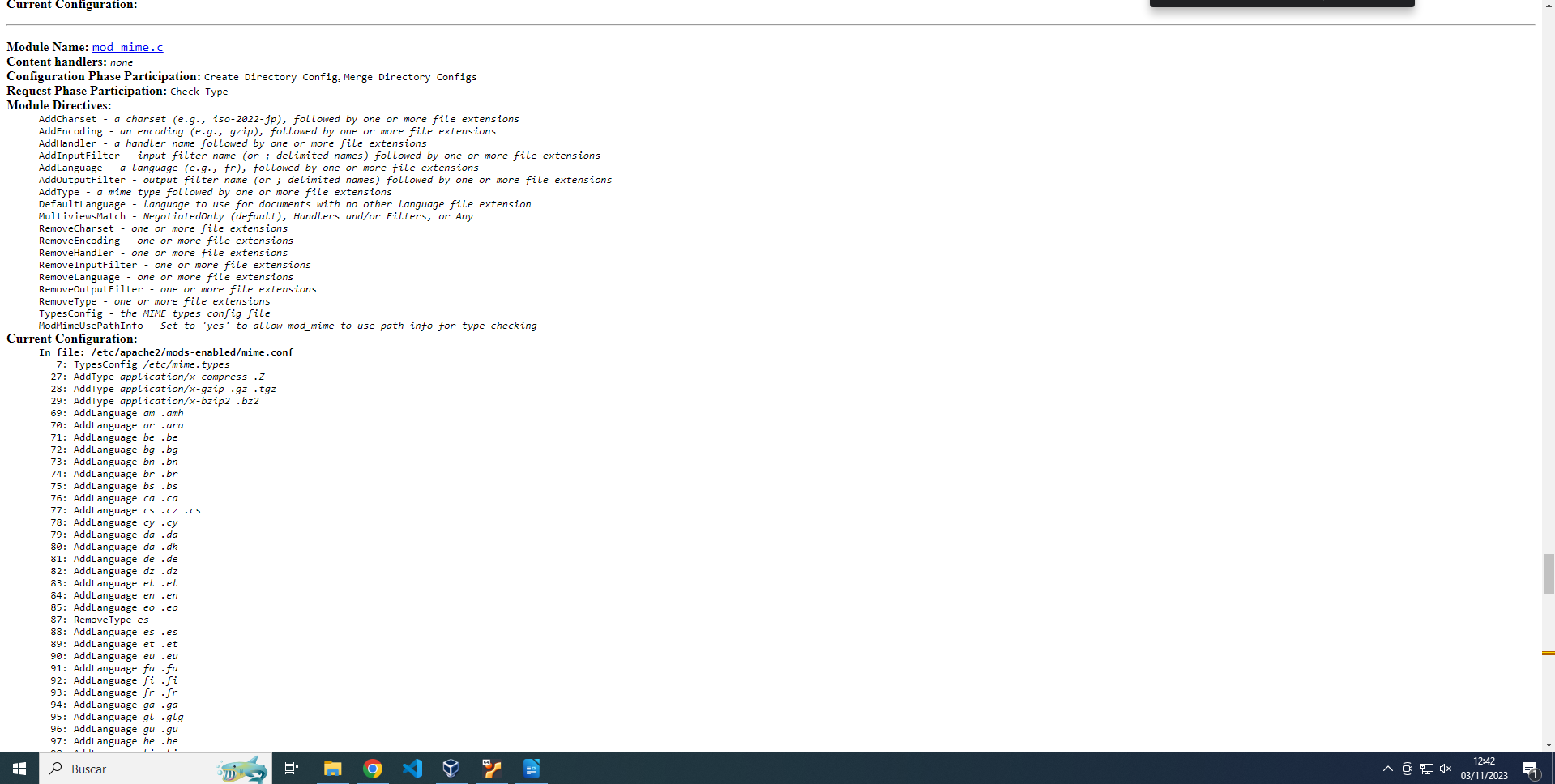
**PASO 8)** Desde tu máquina física conéctate al recurso server-info

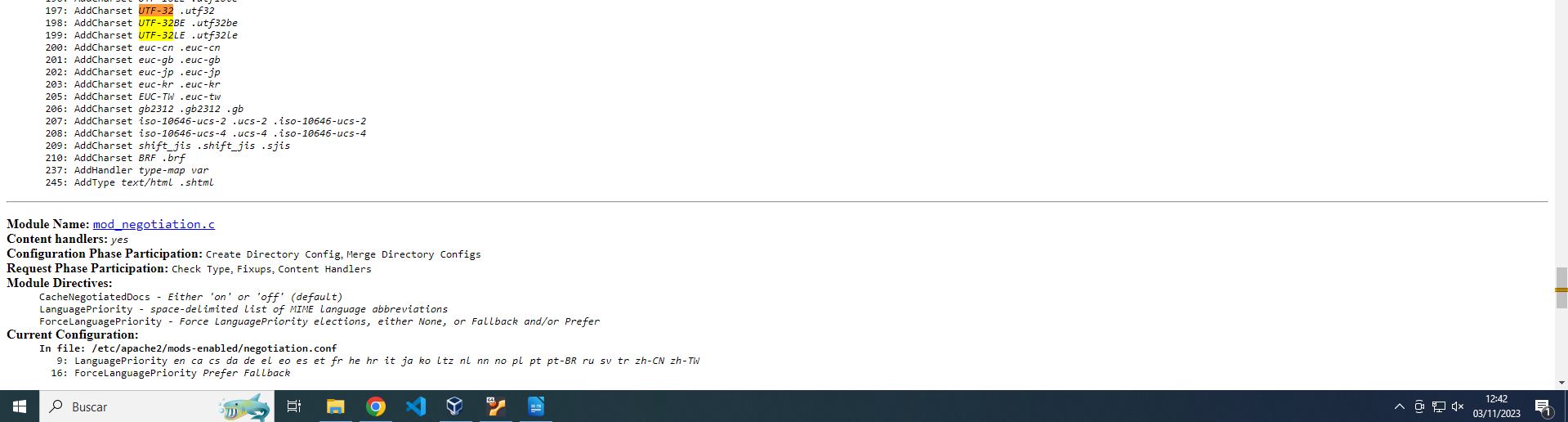


Consulta el fichero server-info, ¿tienes cargado el módulo mod\_mime? ¿en caso que lo tuvieras, tiene el módulo cargada la configuración de caracteres UTF-32?

Sí, está cargado.

Sí, tiene cargada la configuración de caracteres UTF-32.





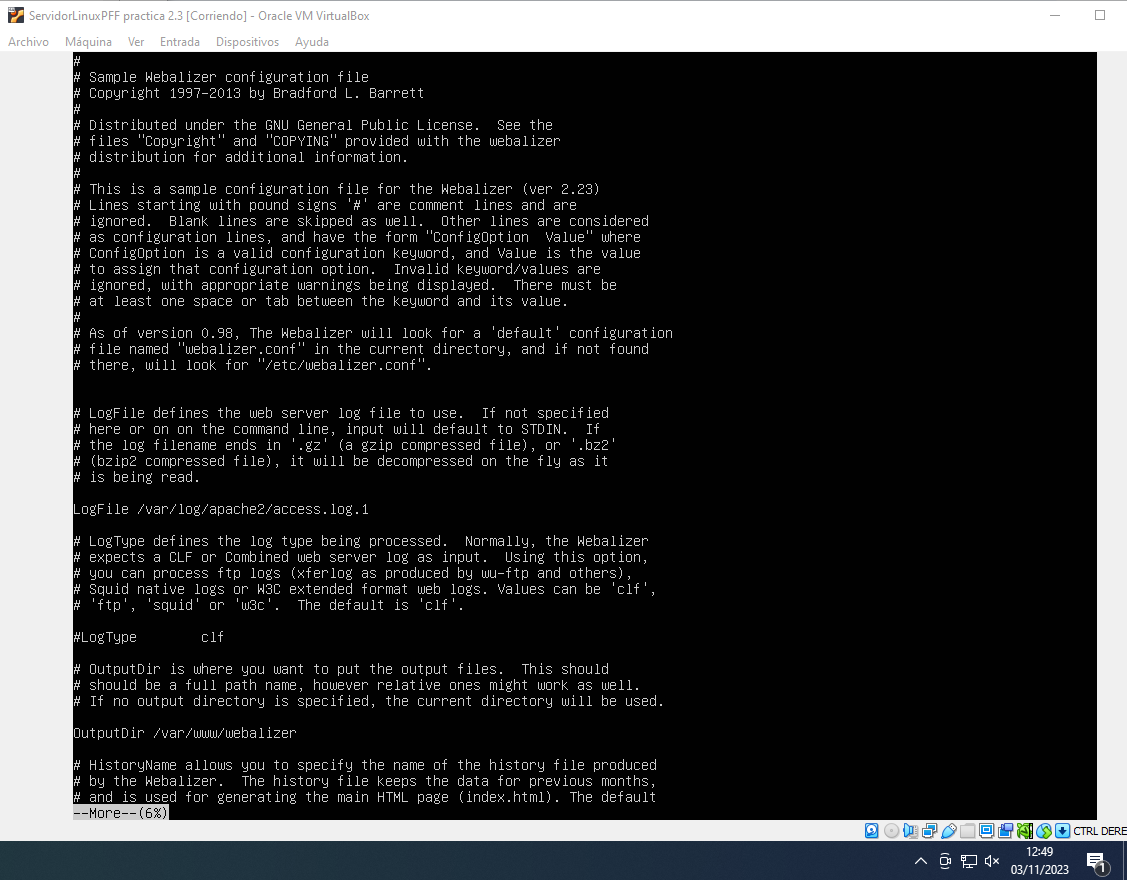
# 

# **WEBALIZER**

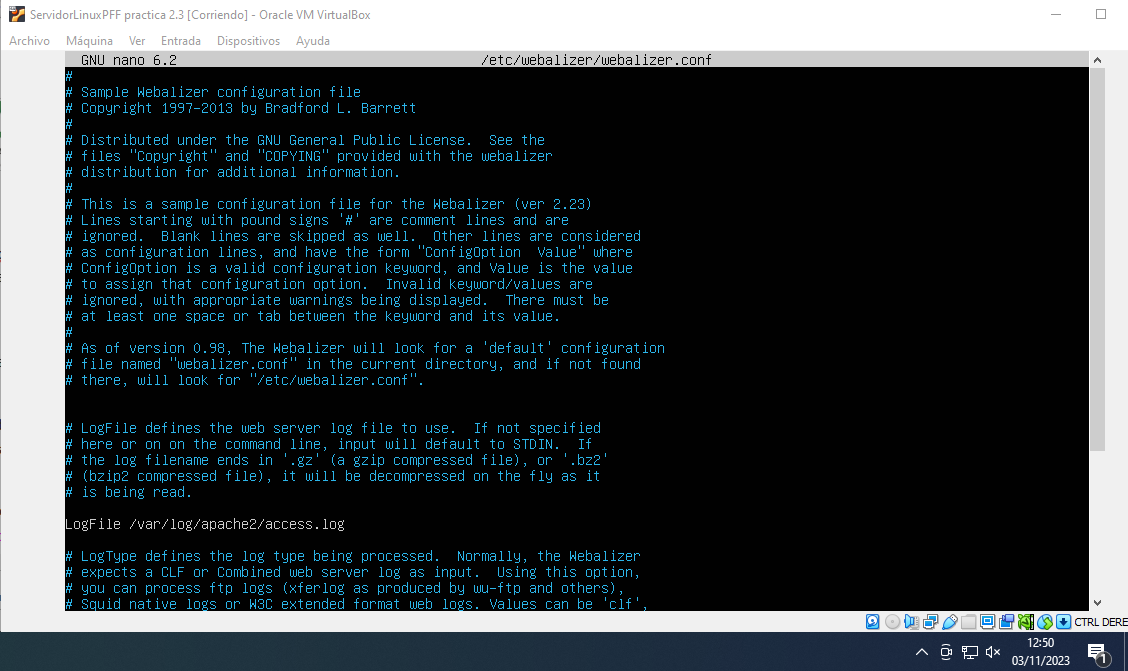
**PASO 1)** En tu servidor Linux, instala la aplicación Webalizer (usa apt-get install, pero antes actualiza el servidor Linux).

**PASO 2)** Una vez instalado se habrá creado un directorio para la aplicación en el **directorio /etc/.** Abre el fichero de configuración de webalizer, ¿de qué fichero log coge los datos para hacer las estadísticas? ¿es correcta la ruta y el nombre del fichero? Si no es así, modifícala.

Del fichero de log de accesos de apache2. La ruta del archivo actual es correcta, pero no el nombre del fichero (access.log.1 en lugar de access.log).



Con el nombre modificado:



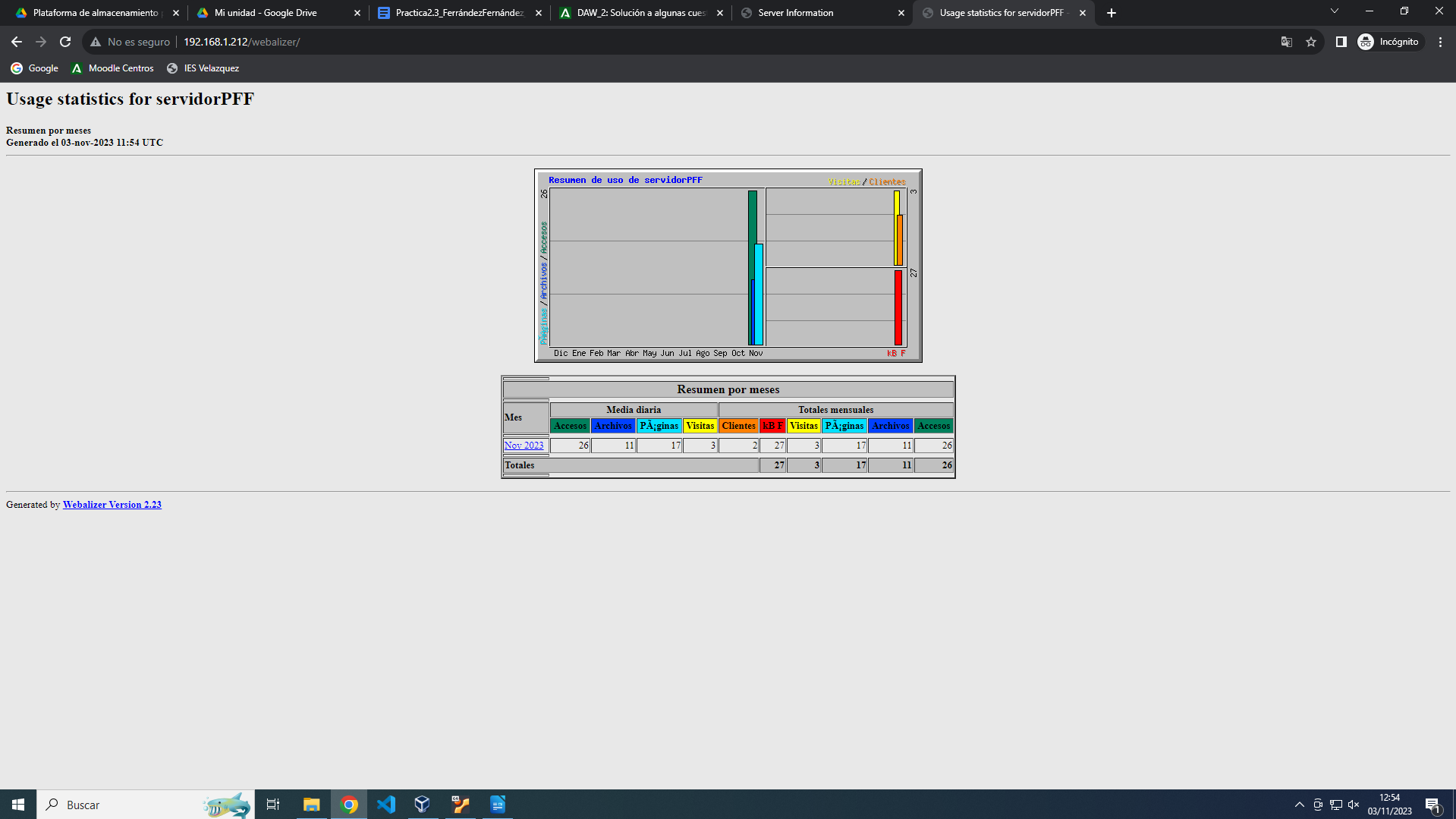
**PASO 3)** La instalación también implica la creación del recurso que se servirá desde el navegador, ¿Dónde está este fichero? ¿Es correcta la ubicación para servirlo? Si no es así, muévelo a la ubicación correcta.

Está en la carpeta /var/www, pero debería estar en la ruta /var/www/html.

**PASO 4)** Lanza el programa (con permisos de administrador) para que lea el fichero de log correspondiente y genere el documento html con las estadísticas.

**sudo webalizer**

**PASO 5)** Accede al recurso /webalizer/ desde tu máquina física.



# 

# 

# **GITHUB**