

## Práctica 1 –Configuración de servicios de red

- 1) Compruebe las direcciones IP que tienen asignadas las diferentes interfaces de red de su equipo mediante el comando `ifconfig`, ¿cómo se llaman dichas interfaces? ¿qué direcciones de red tienen definidas?

Las interfaces de nuestra MV son:

- `enp0s3`: con dirección de red 10.0.2.15
- `enp0s9` (datos): con dirección de red 33.1.1.2
- `enp0s10` (gestión): con dirección de red 192.168.1.1

```
administrador@pc1:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::3d00:5458:c3ab:e588 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:fd:98:cc txqueuelen 1000 (Ethernet)
    RX packets 13068 bytes 18345009 (18.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1134 bytes 107276 (107.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 33.1.1.2 netmask 255.255.255.0 broadcast 33.1.1.255
    inet6 fe80::a00:27ff:fe4f:4445 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:4f:44:45 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 87 bytes 9101 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 fe80::a00:27ff:fef9:fb7c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:f9:fb:7c txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 88 bytes 9189 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Bucle local)
    RX packets 404 bytes 37850 (37.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 404 bytes 37850 (37.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

La interfaz loop back no la tenemos en cuenta ya que esta crea una IP ficticia.

- 2) Compruebe que existe conectividad con otro equipo del laboratorio, mediante la utilidad ping. ¿Es posible hacer ping desde el PC\_1 al PC\_3 por la red 33.1.1.0/24? ¿Y por la red 192.168.1.0/16? Justifique su respuesta. A partir de ahora a la primera de las redes la llamaremos de datos, mientras que la segunda será la de gestión.

- Conectividad con otro equipo del laboratorio:

```
administrador@pc1:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.731 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=1.40 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.388 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.313 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3026ms
rtt min/avg/max/mdev = 0.313/0.707/1.399/0.429 ms
```

- Conectividad de PC\_1 a PC\_3 por la red de datos:

No se puede realizar la conexión porque no tiene ninguna interfaz de red con una dirección IP asignada dentro de esa red.

- Conectividad de PC\_1 a PC\_3 por la red de gestión:

```
administrador@pc1:~$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.564 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.402 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.384 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.351 ms
64 bytes from 192.168.1.3: icmp_seq=5 ttl=64 time=0.376 ms
^C
--- 192.168.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4103ms
rtt min/avg/max/mdev = 0.351/0.415/0.564/0.076 ms
```

- 3) Cree una cuenta de usuario en su equipo, habilite el servicio telnet y compruebe con algún compañero que dicho servicio es accesible.

Creamos una cuenta de usuario:

```
administrador@pc1:~$ sudo adduser pedroiniesta
Añadiendo el usuario 'pedroiniesta' ...
Añadiendo el nuevo grupo 'pedroiniesta' (1001) ...
Añadiendo el nuevo usuario 'pedroiniesta' (1001) con grupo 'pedroiniesta' ...
El directorio personal '/home/pedroiniesta' ya existe. No se copiará desde '/etc/skel'.
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para pedroiniesta
Introduzca el nuevo valor, o presione INTRO para el predeterminado
    Nombre completo []: Pedro Iniesta
    Número de habitación []:
    Teléfono del trabajo []:
    Teléfono de casa []:
    Otro []:
¿Es correcta la información? [S/n] S
```

Habilitamos el servicio telnet:

Para habilitarlo, primero debemos instalarlo:

```
administrador@pc1:~$ sudo apt-get install xinetd telnetd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
telnetd ya está en su versión más reciente (0.17-41.2build1).
xinetd ya está en su versión más reciente (1:2.3.15.3-1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 205 no actualizados.
```

Una vez instalado, configuramos el servicio de telnet. En /etc/xinetd.d/ creamos un archivo llamado telnet (si no se ha creado por defecto) y escribimos los siguiente:

```
administrador@pc1:~$ cd /etc/xinetd.d/
administrador@pc1:/etc/xinetd.d$ ls
chargen      daytime      discard      echo         servers      telnet       time-udp
chargen-udp  daytime-udp  discard-udp  echo-udp     services     time
administrador@pc1:/etc/xinetd.d$ nano telnet
```

service telnet

```
{
    disable = no
    flags = REUSE
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/in.telnetd
    log_on_failure += USERID
}
```



```
GNU nano 4.8                                telnet                                Modificado
service telnet
{
    disable = no
    flags = REUSE
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/in.telnetd
    log_on_failure += USERID
}
```

Nos aseguramos de que telnet funciona, para ello paramos el servicio xinetd y lo volvemos a arrancar.

```
administrador@pc1:/etc/xinetd.d$ service xinetd stop
administrador@pc1:/etc/xinetd.d$ service xinetd start
```

Vamos a comprobar que telnet funciona. Hacemos telnet a la IP que deseamos conectarnos. Ponemos el nombre del usuario y su contraseña.

```
administrador@pc1:/etc/xinetd.d$ telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
pc3 login: pedroiniesta
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

145 actualizaciones se pueden instalar inmediatamente.
41 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** Es necesario reiniciar el sistema ***
pedroiniesta@pc3:~$
```

Ya estamos conectados, ahora podemos crear, acceder, modificar y eliminar ficheros, directorios, ...

```
pedroiniesta@pc3:~$ ls
pedroiniesta@pc3:~$ mkdir Hola
lpedroiniesta@pc3:~$ ls
Hola
```

#### 4) Configure el servicio telnet para que:

##### a) Sólo sea accesible desde la dirección IP de su compañero.

Para que el servicio telnet sea sólo accesible por una dirección IP, debemos modificar el archivo de configuración de telnet (/etc/xinetd.d/telnet), añadiendo un nuevo campo al cual denominaremos "only\_from" y asignaremos la IP de nuestro compañero:

```
1 service telnet
2 {
3     disable          = yes
4     flags             = REUSE
5     socket_type       = stream
6     wait              = no
7     user              = root
8     server             = /usr/sbin/in.telnetd
9     log_on_failure    += USERID
10    only_from         = 192.168.1.3
11 }
```

Al no estar mi IP en el apartado de only\_from de mi compañero, me deniega el acceso. Cualquier persona que intente acceder a mi telnet tampoco podrá, a menos que la dirección IP sea 192.168.1.3.

```
administrador@pc1:~$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Connection closed by foreign host.
```

```
administrador@pc1:~$ telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
pc3 login: raul
Password:
```

##### b) Se registren en el fichero /var/log/telnet.log los intentos de acceso con y sin éxito al servicio telnet, indicando la dirección IP del equipo que intenta el acceso.

Para registrar los intentos de acceso, debemos añadir, en el archivo telnet del apartado anterior, tres atributos más: **log\_on\_failure** que determina la dirección desde la que se ha intentado entrar; **log\_type** que fija dónde va a escribirse la salida del registro de servicio y **log\_on\_success**, que determina la dirección desde la que se ha entrado al servicio:

```

1 service telnet
2 {
3     disable          = yes
4     flags             = REUSE
5     socket_type      = stream
6     wait             = no
7     user             = root
8     server           = /usr/sbin/in.telnetd
9     log_on_failure    += USERID
10    only_from         = 192.168.1.1|
11    log_on_failure     += HOST
12    log_type          = FILE /var/log/telnet.log
13    log_on_success     += HOST
14 }

```

Tras reiniciar el servicio, sólo podrá acceder el usuario que tenga la IP que está en `only_from`, el resto que trate de conectarse fallará y se quedará registrado en el archivo `/var/log/telnet.log`.

#### 5) Habilite el servicio ftp en su equipo. Para esto es necesario:

- a) Configurar ftp para que no funcione en modo standalone.
- b) Impedir el acceso de la cuenta anonymous.
- c) Permitir cuentas locales para acceder al servicio. Nota: Recuerde consultar el manual de configuración de este servicio `man vsftpd.conf`

Primero de todo, tenemos que tener instalado vsftpd. Para instalarlo hacemos:

```

administrador@pc1:/etc/xinetd.d$ sudo apt-get install vsftpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
vsftpd ya está en su versión más reciente (3.0.3-12).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 205 no actualizados.

```

```

administrador@pc1:/$ sudo nano /etc/xinetd.d/vsftp

```

```
GNU nano 4.8                                vsftp                                Modificado
service ftp
{
    disable = no
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/vsftpd
    #nice = 10
    log_on_failure += USERID
}
```

a) Configurar ftp para que no funcione en modo standalone:

La configuración de ftp suele estar en un fichero llamado vsftpd.conf en el directorio etc. Abrimos el fichero con:

```
administrador@pc1:/$ gedit /etc/vsftpd.conf
```

Buscamos la palabra standalone con Ctrl + F, y ponemos listen=NO para que no funcione en modo standalone.

```
12 # Run standalone? vsftpd can run either from an inetd or as a standalone
13 # daemon started from an initscript.
14 listen=NO
```

b) Impedir el acceso de la cuenta anonymous

Nos volvemos a meter en vsftpd.conf y buscamos con Ctrl + F anonymous. Viene deshabilitada por defecto así que no tenemos que hacer nada.

```
24 # Allow anonymous FTP? (Disabled by default).
25 anonymous_enable=NO
```

Hay más opciones marcadas para anonymous, pero son para crear directorios y demás. La que impide el acceso a la cuenta es la de la captura de pantalla.

c) Permitir cuentas locales para acceder a este servicio.

Nos volvemos a meter en vsftpd.conf y buscamos con Ctrl + F local\_enable.

```
27 # Uncomment this to allow local users to log in.
28 local_enable=YES
29 #
```

Una vez marcado a YES, guardamos y salimos.

**6) Pida a un compañero que pruebe el servicio ftp a través de la cuenta de usuario creada en el paso 3 descargando un fichero desde su equipo. I**

Antes de hacer nada, debemos comprobar que no hay procesos ftp ejecutándose en segundo plano, ya que pueden causar problemas. Por lo que observamos si tenemos algún proceso, y en dicho caso lo matamos:

```
administrador@pc3:~$ ps -x | grep ftp
3151 pts/0    T        0:00 ftp 192.168.1.1
3667 pts/0    S+       0:00 grep --color=auto ftp
administrador@pc3:~$ kill -9 3151
[1]+  Terminado (killed)      ftp 192.168.1.1
administrador@pc3:~$
```

Una vez que no tenemos procesos ftp ejecutándose, podemos proceder a conectarnos:

```
administrador@pc3:~$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 3.0.3)
Name (192.168.1.1:administrador): raulrguez
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1001    1001        4096 Nov 01 10:45 Descargas
drwxr-xr-x  2 1001    1001        4096 Nov 01 10:45 Documentos
drwxr-xr-x  3 1001    1001        4096 Nov 01 11:06 Escritorio
drwxr-xr-x  2 1001    1001        4096 Nov 01 10:45 Im??genes
drwxr-xr-x  2 1001    1001        4096 Nov 01 10:45 M??sica
drwxr-xr-x  2 1001    1001        4096 Nov 01 10:45 Plantillas
drwxr-xr-x  2 1001    1001        4096 Nov 01 10:45 P??blico
drwxr-xr-x  2 1001    1001        4096 Nov 01 10:45 V??deos
226 Directory send OK.
ftp> █
```

Una vez dentro podemos realizar varias acciones, como por ejemplo, ver los archivos que hay, descargar archivos con el comando 'get' (dichos archivos se descargan en la carpeta en la que me encontraba al iniciar ftp), etc.



```

ftp> cd Escritorio/
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0      0              0 Nov 01 11:06 ejemplo.txt
drwxr-xr-x    2 0      0          4096 Nov 01 11:04 prueba
226 Directory send OK.
ftp> get ejemplo.txt
local: ejemplo.txt remote: ejemplo.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ejemplo.txt (0 bytes).
226 Transfer complete.
ftp> █

```

## 7) Configure el servicio ftp para que:

a)Únicamente pueda ser utilizando a través de la cuenta de usuario que hemos creado en nuestro equipo.

Para hacer esto, tenemos que añadir las siguientes opciones al archivo /etc/vsft.conf:

```

---
156 userlist_deny=NO
157 underlist_enable=YES
158 underlist_file=/etc/xinetd.d/vsftpd.user_list

```

Ahora, creamos un archivo en /etc/xinetd.d llamado vsftpd.user\_list donde pondremos la lista de los usuarios permitidos, en este caso, solo nosotros.

```

administrador@pci:/etc/xinetd.d$ sudo nano vsftpd.user_list

```

```

GNU nano 4.8                                vsftpd.user_list                                Modificado
pedroiniesta

```

## b)Acepte la subida de ficheros al servidor ftp.

En el archivo /etc/vsft.conf buscamos con Ctrl+F upload\_enable y write\_enable y descomentamos ambas.

```

administrador@pci:/etc/xinetd.d$ sudo nano vsftpd.user_list

```

```

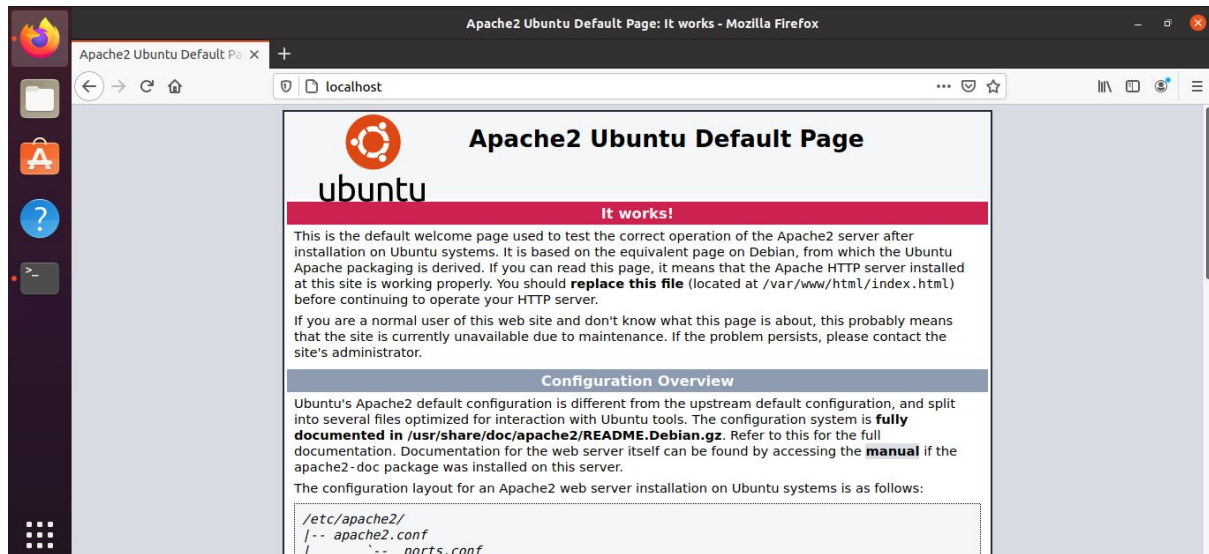
30 # Uncomment this to enable any form of FTP write command.
31 write_enable=YES
32 #

37 # Uncomment this to allow the anonymous FTP user to upload files. This only
38 # has an effect if the above global write enable is activated. Also, you will
39 # obviously need to create a directory writable by the FTP user.
40 anon_upload_enable=YES

```

Guardamos el archivo y lo cerramos.

- 8) Habilite el servicio http en su equipo. Abra un navegador web y pruebe a visitar la página de inicio desde su equipo (`http://localhost` o `http://127.0.0.1`). Además, realice los siguientes cambios:



- a) Modifique el contenido de la página de inicio, y compruebe con la ayuda de su compañero que la dirección de su servidor es accesible.

Al archivo `index.html`, que se encuentra en `/var/www/html/`, lo modificamos borrando su contenido, y añadiendo nuevas sentencias para escribir un nuevo título. Cualquiera que acceda a `http://192.164.1.3`, podrá ver el título.

```
administrador@pc1:/$ cd /var/www/  
administrador@pc1:/var/www$ ls  
html  
administrador@pc1:/var/www$ cd /var/www/html/  
administrador@pc1:/var/www/html$ ls  
index.html  
administrador@pc1:/var/www/html$ sudo gedit index.html
```

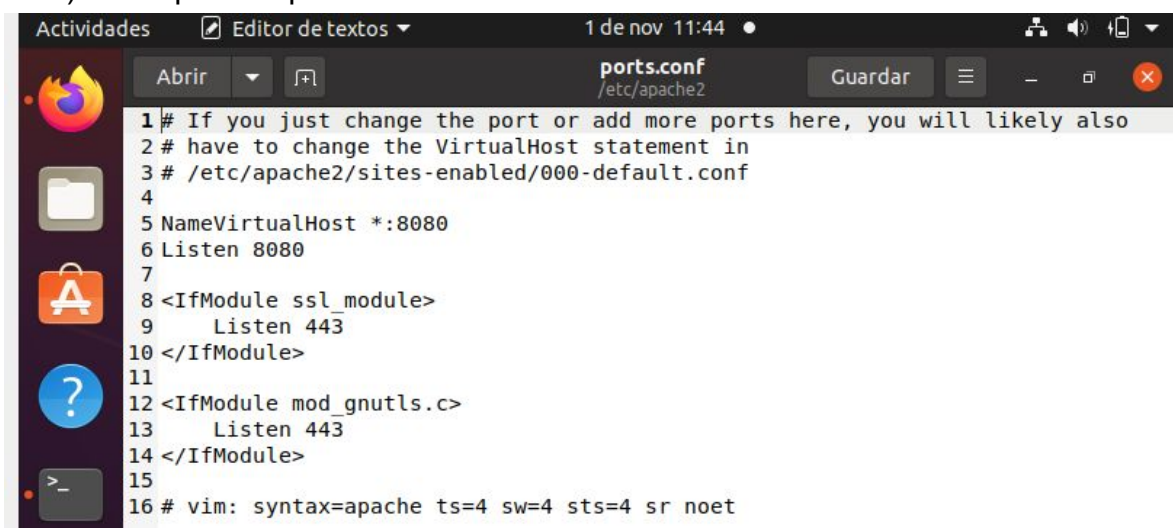
```
administrador@pc1:/var/www/html$ cat index.html  
<HTML>  
  <BODY>  
    <B><center><H1> Nuevo titulo para la prac1 </H1></center></B>  
  <BODY>  
</HTML>  
administrador@pc1:/var/www/html$
```



- b) Modifique el puerto de escucha del servidor de modo que el acceso a la página de inicio se haga mediante la dirección: <http://localhost:8080>.

Para conseguir modificar el puerto vamos a tener que modificar varios archivos de configuración:

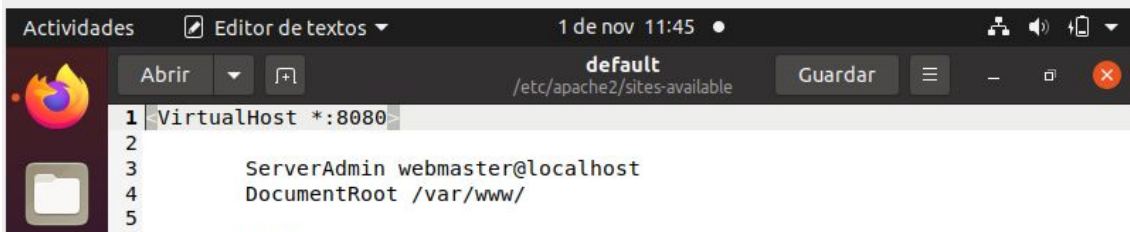
- a) `/etc/apache2/ports.conf`



- b) `/etc/apache2/sites-enabled/000-default`



- c) `/etc/apache2/sites-available/default`



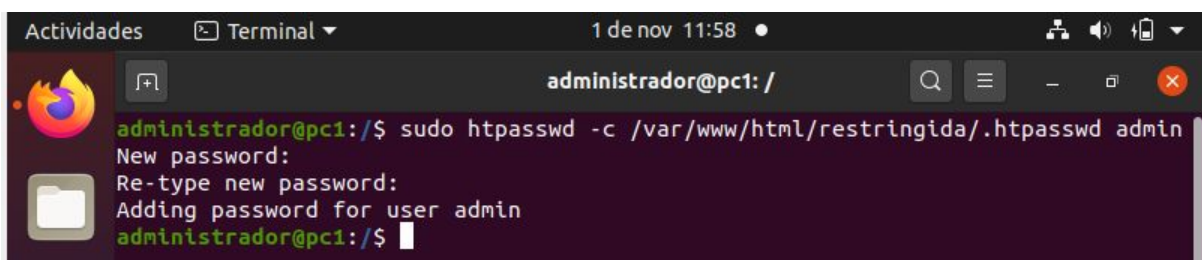
```
1 <VirtualHost *:8080>
2
3     ServerAdmin webmaster@localhost
4     DocumentRoot /var/www/
5
```

Tras la modificación, reiniciamos el servicio de apache, y accedemos a la página <http://192.168.1.1:8080>



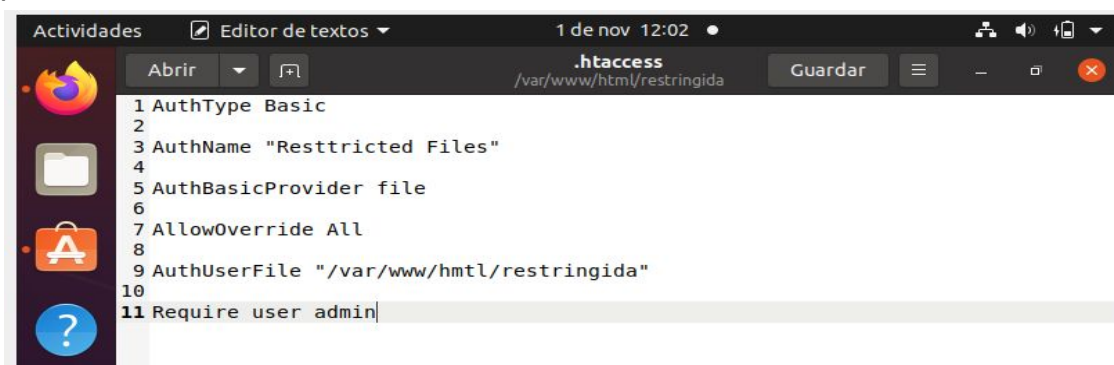
- c) Cree una página de acceso restringido (es decir, que requiera usuario y contraseña antes de mostrarla) en <http://localhost/restringida/>.

En primer lugar, ejecutamos el comando oportuno para dar acceso a la página con la contraseña 1234 y el usuario admin:



```
administrador@pc1: /
administrador@pc1:/$ sudo htpasswd -c /var/www/html/restringida/.htpasswd admin
New password:
Re-type new password:
Adding password for user admin
administrador@pc1:/$
```

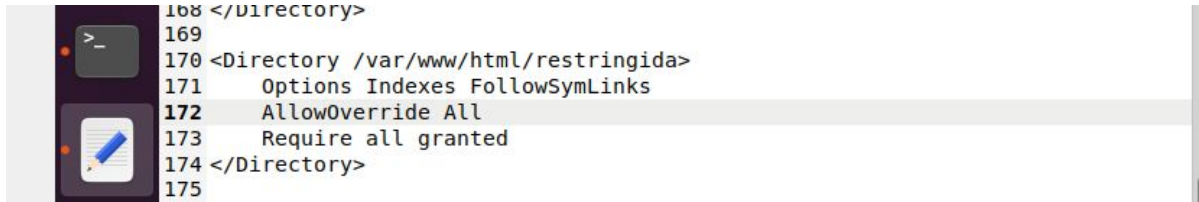
A continuación creamos el archivo .htaccess con el siguiente contenido para dar permiso de acceso solo a admin:



```
1 AuthType Basic
2
3 AuthName "Resttricted Files"
4
5 AuthBasicProvider file
6
7 AllowOverride All
8
9 AuthUserFile "/var/www/hmtl/restringida"
10
11 Require user admin
```



Tras esto, en el archivo de configuración de apache2 tenemos que cambiar la línea que se referencia al directorio que queremos cambiar poniendo 'AllowOverride' a 'all':



```
168 </Directory>
169
170 <Directory /var/www/html/restringida>
171     Options Indexes FollowSymLinks
172     AllowOverride All
173     Require all granted
174 </Directory>
175
```

Finalmente, ya podemos comprobar que cuando hacemos localhost/restringida nos pide un usuario y una contraseña para acceder.