Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería Informática

Dept. Teoría de la Señal, Telemática y Comunicaciones

Práctica 1 – Configuración de servicios de red

(0.75 puntos)

Raúl Castro Moreno y Santiago Muñoz Castro
3ºA -- A2

Realización práctica

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?

```
root@pc1:/home/administrador# 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 5745  bytes 6791324 (6.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1220  bytes 103979 (103.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

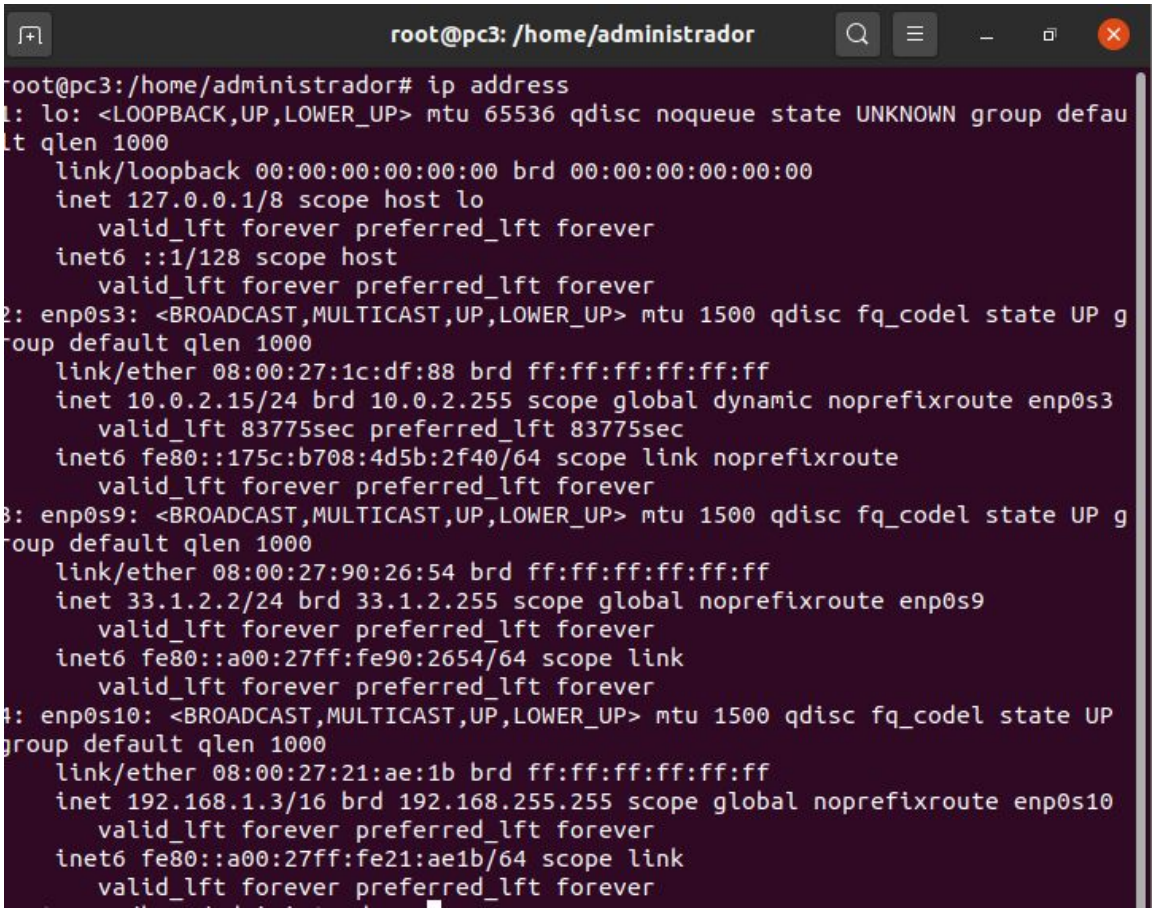
```
enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 33.1.1.2  netmask 255.255.255.0  broadcast 33.1.1.255
        inet6 fe80::a00:27ff:fee6:cd3c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e6:cd:3c  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 117  bytes 13049 (13.0 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:fee7:b1dc  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e7:b1:dc  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 566  bytes 40112 (40.1 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 1582  bytes 140510 (140.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1582  bytes 140510 (140.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Encontramos 4 interfaces de red diferentes, las cuales son:

-**enp0s3**, la cual su dirección de red definida es **“10.0.2.15”.**
-**enp0s9**, la cual su dirección de red definida es **“33.1.1.2”.**
-**enp0s10**, la cual su dirección de red definida es **“192.168.1.1”.**
-**lo**: Se refiere a loopback, que es una interfaz de red especial que el sistema utiliza para referirse a él mismo la cual su dirección de red definida es **“127.0.0.1”.**

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 la primera de las redes la llamaremos de *datos* mientras que la segunda será la de *gestión*.

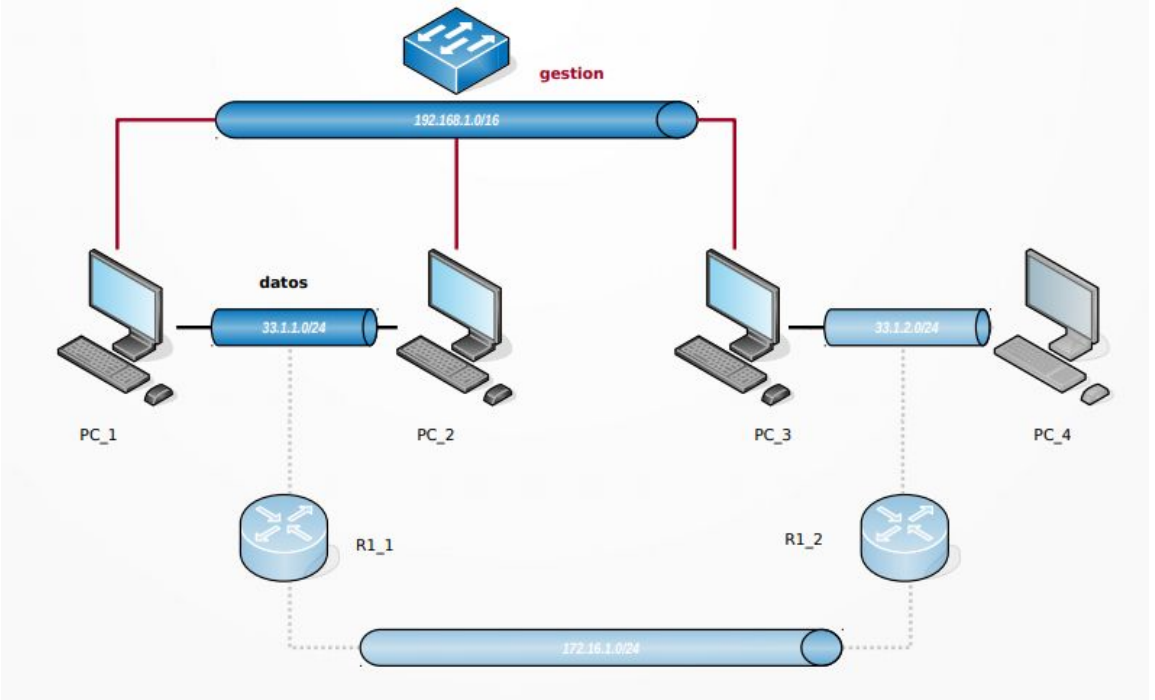
Para comprobar que se puede conectar a otro equipo del laboratorio, primero comprobamos las redes con el comando "ipaddress" en el PC_3.



Aquí encontramos la primera cosa que nos indica que no va a funcionar, y es que la red del PC_3 que empieza por 33, es 33.1.2.2 y no es 33.1.1.
Hacemos ping desde el PC_1 al PC_3 y efectivamente no conecta por la red 33.1.2
Luego haremos ping por la red 192.168.1.3 y esta red si hace ping correctamente luego están conectadas por esa red.

```
root@pc1: /var/www/restringido
root@pc1:/var/www/restringido# ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.
^Z
[6]+  Detenido                ping 33.1.2.2
root@pc1:/var/www/restringido# 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=0.399 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.453 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.463 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.499 ms
^Z
[7]+  Detenido                ping 192.168.1.3
root@pc1:/var/www/restringido#
```

A la hora de entender por que esto funciona así podemos usar una transparencia que se nos es proporcionada donde se habla de como funciona nuestro entorno virtualizado.



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

Primero creamos una cuenta de usuario para el equipo, utilizando el comando adduser "nombre" .

root@pc1:/home/administrador# adduser telnetsanti
Añadiendo el usuario `telnetsanti' ...
Añadiendo el nuevo grupo `telnetsanti' (1003) ...
Añadiendo el nuevo usuario `telnetsanti' (1003) con grupo `telnetsanti' ...
Creando el directorio personal `/home/telnetsanti' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para telnetsanti
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []: santiago muñoz castro
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
chfn: el nombre contiene caracteres ilegales (no ASCII): «santiago muñoz castro»
¿Es correcta la información? [S/n] S

Aquí ya tendríamos creado el nuevo usuario para el equipo. Ahora procedemos a habilitar el servicio de telnet, para ello debemos emplear el siguiente comando, el cual instala el servicio telnet, en nuestro caso ya lo teníamos instalado y entonces solo se actualiza.

root@pc1:/home/administrador# 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 182 no actualizados.

Finalmente terminamos de configurar el servicio de telnet, copiando el archivo que se nos ha proporcionado llamado "telnet" en /etc/xinetd.d/ , el cual es un fichero que contiene lo siguiente: (disable estaba en "yes", pero lo hemos modificado "no")

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

root@pc1:/home/administrador# cp telnet /etc/xinetd.d/

Una vez configurado el telnet, lanzamos el servicio usando el siguiente comando

root@pc1:/etc/xinetd.d# service xinetd start

En caso de querer hacerlo de forma segura, antes de hacer un start, hacemos un "service xinetd stop", por si estuviera activo de antes.
Ahora , para comprobar finalmente la accesibilidad, hacemos telnet a la ip del otro PC, en este caso el PC_3 con ip "192.168.1.3" ,y nos pedirá el usuario y contraseña del PC_3.

root@pc3:/etc/xinetd.d# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
pc1 login: telnetsanti
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-48-generic x86_64)

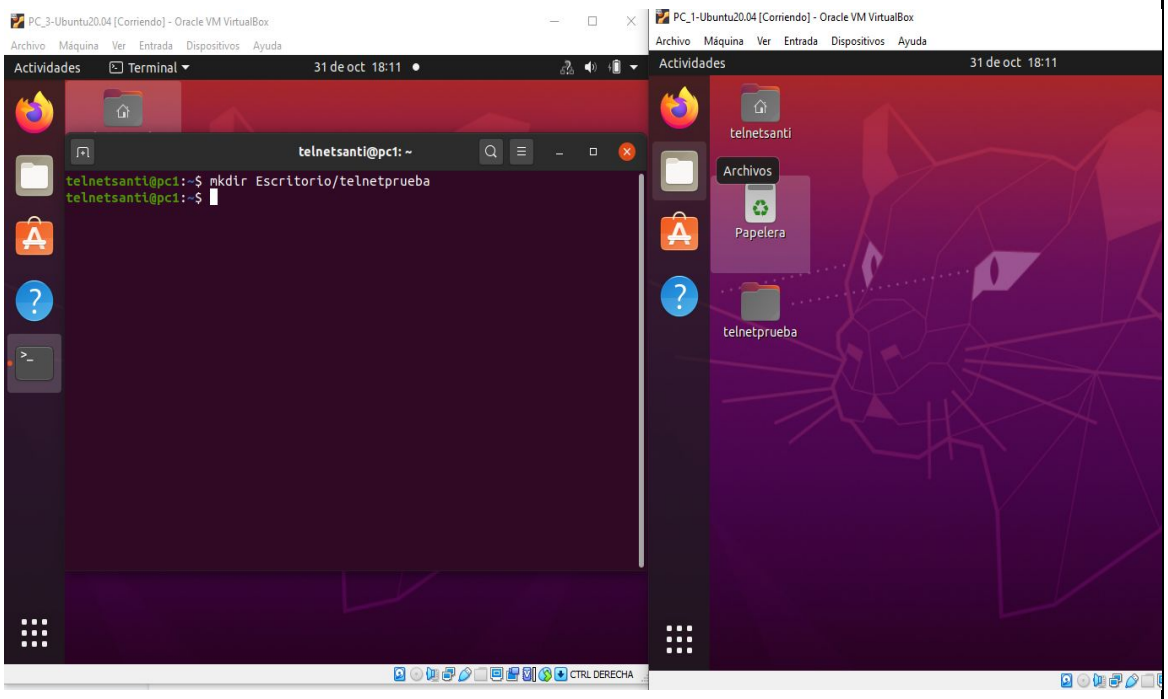
 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Oct 9 11:24:48 CEST 2020 on pts/1
telnetsanti@pc1:~$

Y ahora nos encontramos que funciona y estamos usando el terminal del PC_1, donde podemos crear carpetas, modificar archivos , etc

Como comprobación hemos creado desde PC_3 un directorio en PC_1



4. Configure el servicio telnet para que:

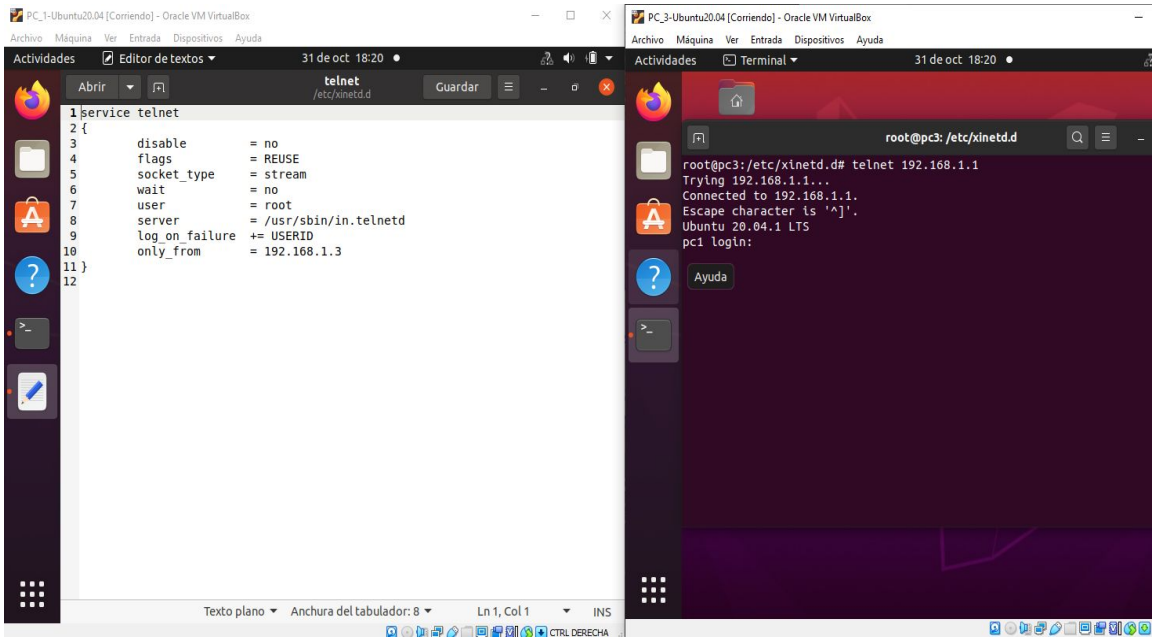
    1. Sólo sea accesible desde la dirección IP de su compañero.

*Solo tenemos que añadir en el archivo de configuración "telnet" , **only_from = (IP que permitamos que acceda al servicio)***

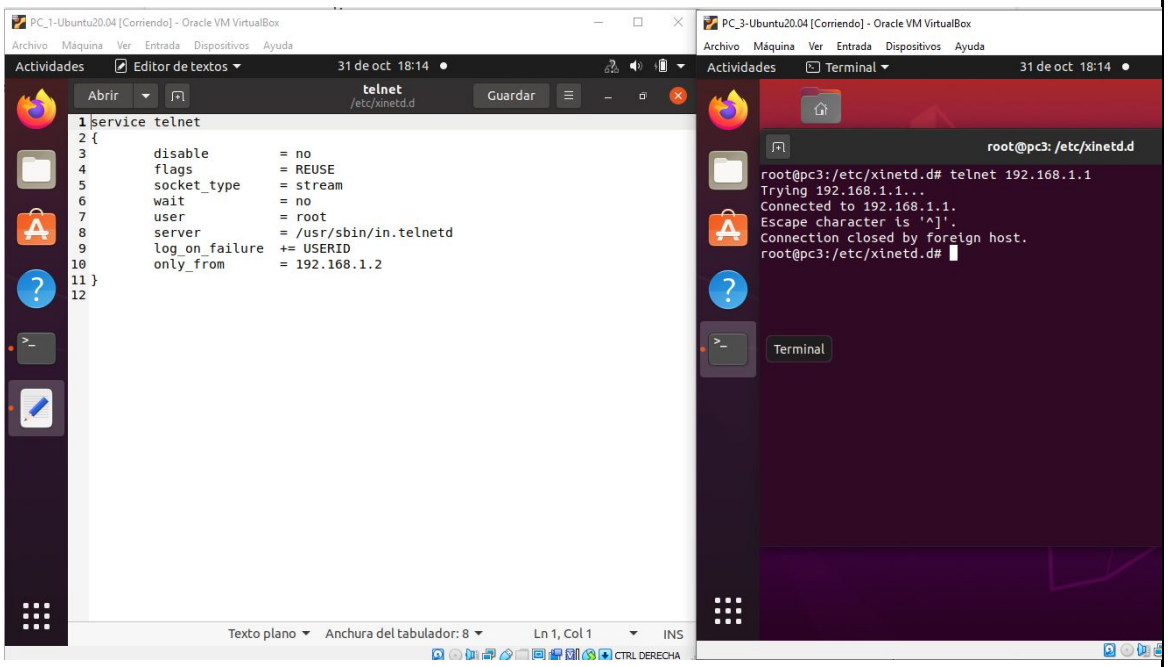
```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
```

```
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        only_from       = 192.168.1.3
}
```

Aquí podemos ver como nos permite conectarnos.



En este caso, hemos permitido el acceso a una IP diferente , para comprobar que no nos permite acceder al servicio de telnet.



1.
    2. 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 ello vamos a tener que volver a modificar el archivo de "telnet" añadiendo lo siguiente que está resaltado.

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        only_from       = 192.168.1.3
        log_on_failure  += HOST
        log_type        = FILE /var/log/telnet.log
        log_on_success  +=  HOST
}
```

*Con **log_on_failure**,configura xinetd para registrar si hay una falla de conexión o si la conexión no es permitida y con el valor **HOST**, determina la dirección desde la cual se ha intentado entrar.*

*Con **log_type**, configura xinetd para usar la facilidad de registro authpriv, el cual escribe las entradas de registro al archivo /var/log/secure. Al agregar una directiva tal como **FILE /var/log/telnet.log** aquí, creará un archivo de registro personalizado llamado **telnet.log** en el directorio /var/log/.*

*Con **log_on_success**, configura xinetd a registrar si la conexión es exitosa. Por defecto, la dirección IP del host remoto y el ID del proceso del servidor procesando la petición son grabados. Con el valor **HOST,** se determina la dirección desde la cual se ha entrado al servicio.*

Una vez realizado esto, debemos cambiar el archivo "/etc/xinetd.conf" , añadiendo lo siguiente que está resaltado.

```
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/
defaults
{
# Please note that you need a log_type line to be able to use log_on_success
# and log_on_failure. The default is the following :
# log_type = SYSLOG daemon info
     instances     = 50
     log_type      = FILE /var/log/xinetdlog
     log_on_failure       += USERID
}
includedir /etc/xinetd.d
```

Instances *sirve para configurar el máximo número de peticiones que xinetd puede manejar simultáneamente.*

Ahora realizamos la conexión desde la PC_2 y la PC_3 , y como se ve en el archivo "telnet" solo hemos permitido la conexión para PC_3. A continuación se ve el resultado de la conexión, pudiendo ver como queda guardado en el archivo telnet.log

```
root@pc1:/home/administrador/Escritorio# cat /var/log/telnet.log
20/10/31@19:10:45: START: telnet from=::ffff:192.168.1.2
20/10/31@19:10:45: FAIL: telnet address from=::ffff:192.168.1.2
20/10/31@19:11:10: START: telnet from=::ffff:192.168.1.3
```

5. Habilite el servicio *ftp* en su equipo (de la "*a"* a la "*c"*).

En primer lugar, instalamos vsftpd usando el comando que se ve a continuación, como ya lo teníamos instalado, nos muestra lo siguiente.

root@pc1:/home/administrador/Escritorio# 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 182 no actualizados.

*Después, en **/etc/xinetd.d** , añadimos el archivo proporcionado que se llama **"vsftp"** el cual su contenido es lo siguiente:(disable estaba en "yes", pero lo hemos modificado a "no".*

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

Ahora, para realizar los apartados a), b) y c), tendremos que modificar el archivo "/etc/vsftpd.conf" .

Para que ftp no funcione en modo standalone, buscamos "standalone" (usando Control + F) y en la primera linea que encontremos hay que poner lo siguiente.

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

Luego de esto, para impedir el acceso de la cuenta anonymous, *buscamos "anonymous" (usando Control + F) y en la primera linea que encontremos hay que poner lo siguiente.*

Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO

Finalmente, para permitir que cuentas locales accedan al servicio, buscamos "local_enable" (usando Control + F) y en la primera linea que encontremos hay que poner lo siguiente.

Uncomment this to allow local users to log in.
local_enable=YES

6. Pida a un compañero que pruebe el servicio ftp. ¿Qué comandos utilizó para ello?

Usamos el comando ftp desde PC_3 , con la ip del PC_1 (Antes de realizar esto sería conveniente asegurarse de que no hubiera procesos standalone activos)

root@pc3:/home/administrador# ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 3.0.3)
Name (192.168.1.1:administrador): telnetsanti
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

Ahora ya estamos con los archivos del PC_1 y vamos a descargar un archivo que hemos creado llamado "pruebaftp" al PC_3, el cual se guarda en la misma carpeta con la cual se usó el comando de "ftp (IP)".

ftp> cd Escritorio/
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1003 1003 0 Oct 31 20:35 pruebaftp
drwxrwxr-x 2 1003 1003 4096 Oct 31 18:10 telnetprueba
226 Directory send OK.
ftp> get pruebaftp
local: pruebaftp remote: pruebaftp
200 PORT command successful. Consider using PASV.

150 Opening BINARY mode data connection for pruebaftp (0 bytes).
226 Transfer complete.
ftp> exit
221 Goodbye.

Aquí comprobamos que ha realizado correctamente la transferencia

root@pc3:/home/administrador# ls
Descargas Escritorio Música pruebaftp rac
Documentos Imágenes Plantillas Público Vídeos

7. Configure el servicio ftp para que:

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

Para ello hay que modificar el archivo "/etc/vsftpd.conf", al cual le añadiremos lo siguiente al final:

userlist_deny=NO
userlist_enable=YES
userlist_file=/etc/xinetd.d/user_list

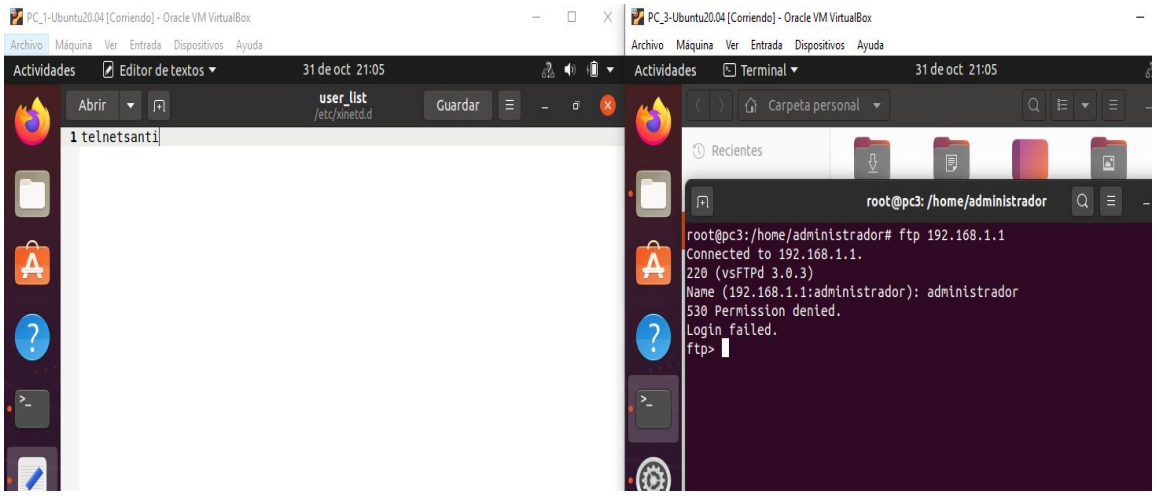
*Con **userlist_deny**, cuando se utiliza en combinación con la directriz **userlist_enable** y con el valor de **NO**, se les niega el acceso a todos los usuarios locales a menos que sus nombres están listados en el archivo especificado por la directriz **userlist_file.** Puesto que se niega el acceso antes de que se le pida la contraseña al cliente, al configurar esta directriz a **NO** previene a los usuarios locales a proporcionar contraseñas sin encriptar sobre la red.*

*Con **userlist_enable** , cuando está activada, se les niega el acceso a los usuarios listados en el archivo especificado por la directriz **userlist_file**. Puesto que se niega el acceso al cliente antes de solicitar la contraseña, se previene que los usuarios suministren contraseñas sin encriptar sobre la red.*

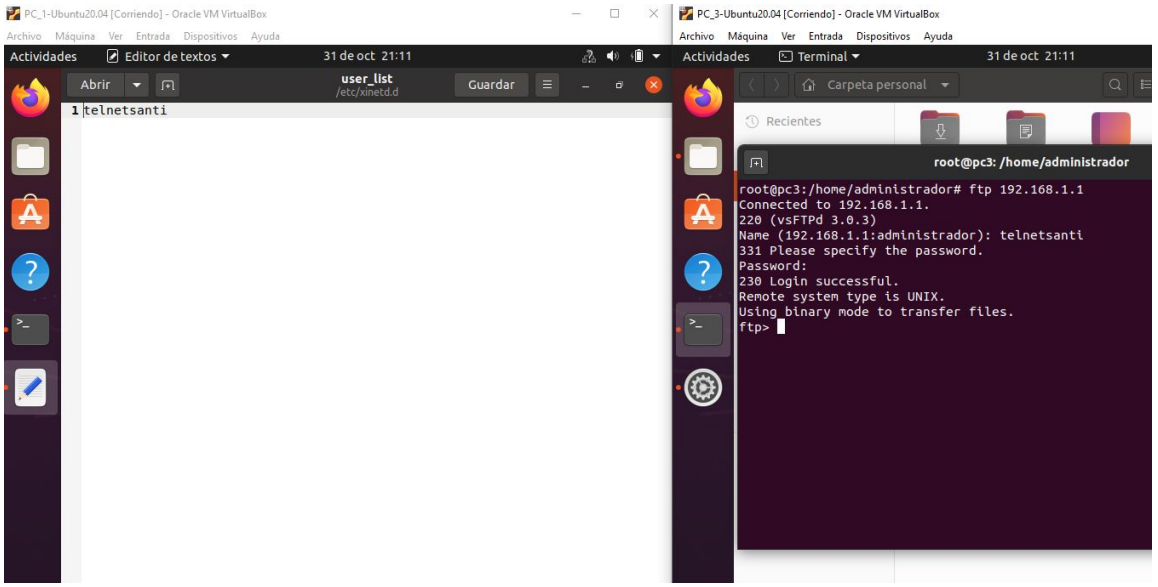
*Con **userlist_file** , especifica el archivo al que vsftpd hace referencia cuando la directriz **userlist_enable** está activada.*

*Una vez hecho esto, creamos en **"/etc/xinetd.d/"** el archivo **"user_list"**, el cual contendrá los nombres de los usuarios a los que se le permite el acceso.*

*En esta imagen podemos observar que si ponemos como usuario permitido a **"telnetsanti"** e introducimos al logear otro usuario(en este caso administrador) se nos deniega el permiso.*



*En esta imagen tenemos lo contrario, el usuario permitido es **"telnetsanti"** e introducimos dicho usuario al logear y esta vez si nos lo permite.*



7.

2.

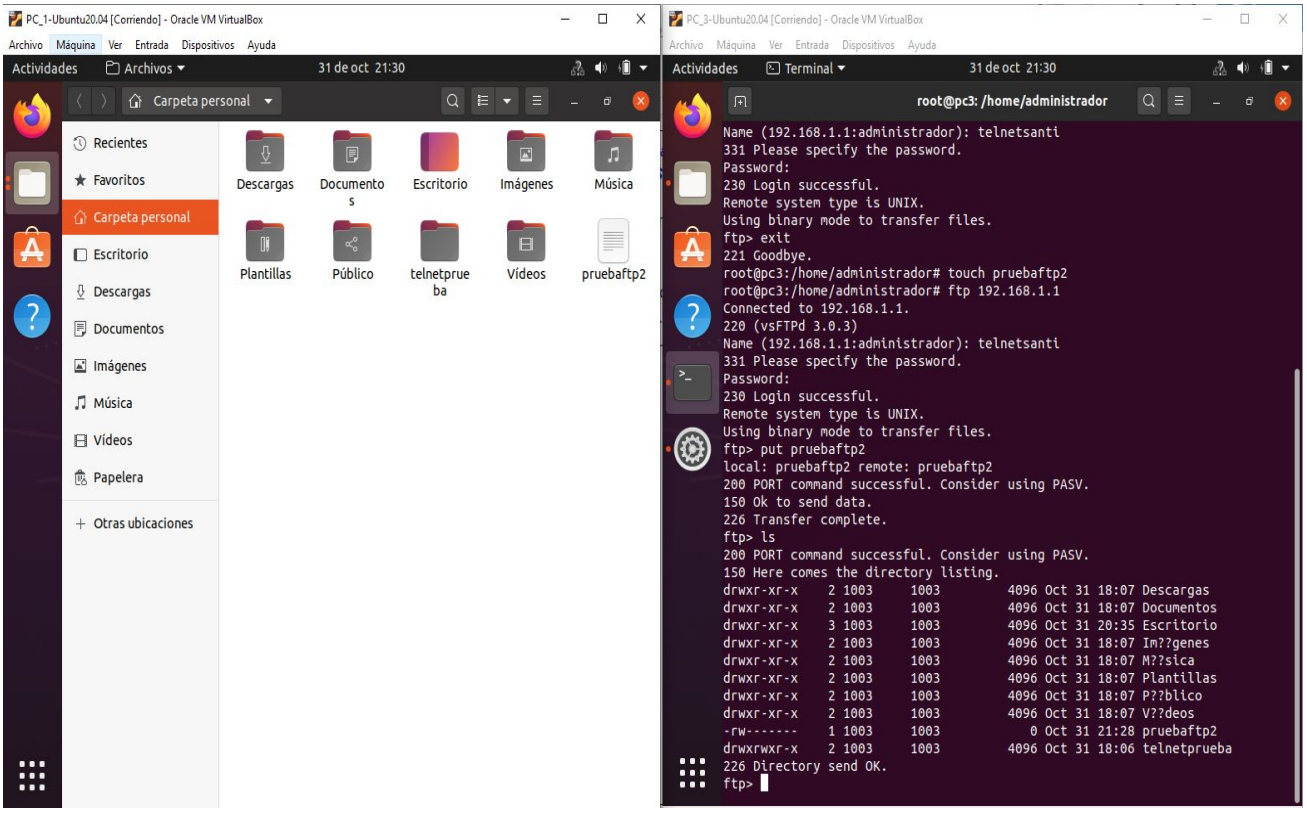
Acepte la subida de ficheros al servidor ftp.

*Solo hay que descomentar en **"/etc/vsftpd.conf"** , las variables que aparecen de **"anon_upload_enable=YES"** y la de **"write_enable=YES"***

Uncomment this to enable any form of FTP write command.
write_enable=YES

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

A continuación vemos un ejemplo de subir un archivo desde PC_3 a PC_1.



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 siguentes cambios:

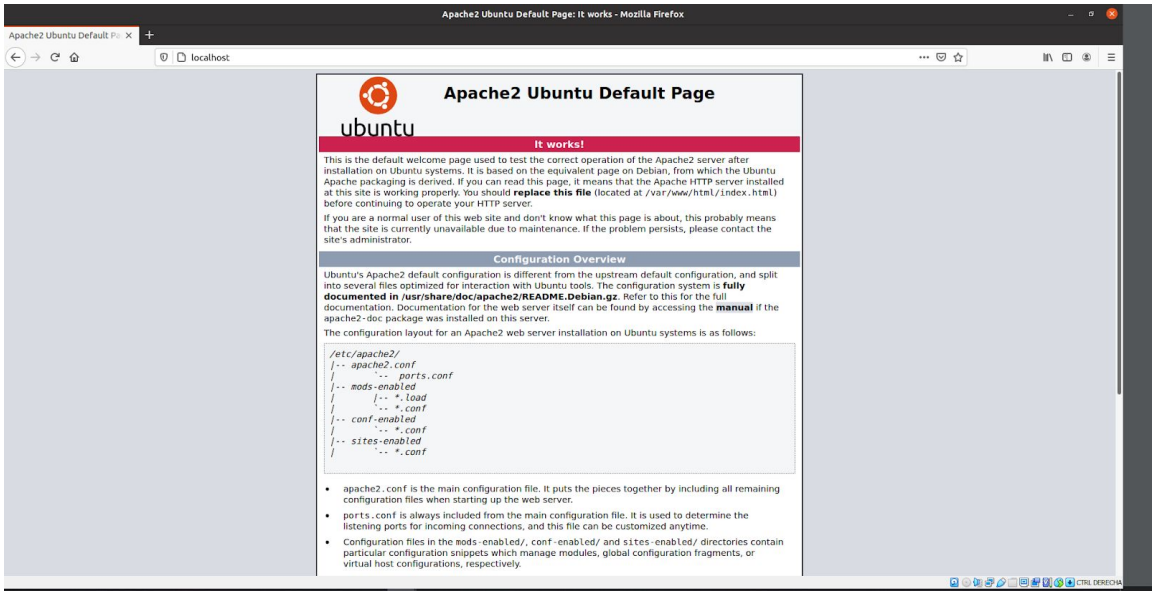
    1. Modifique el contenido de la página de inicio, y compruebe con la ayuda de su compañero que la dirección de su servidor es accesible.

Para habilitar el servicio de http, primero tendremos que instalar apache mediante el siguiente comando, como ya lo teníamos instalado solo se actualiza.

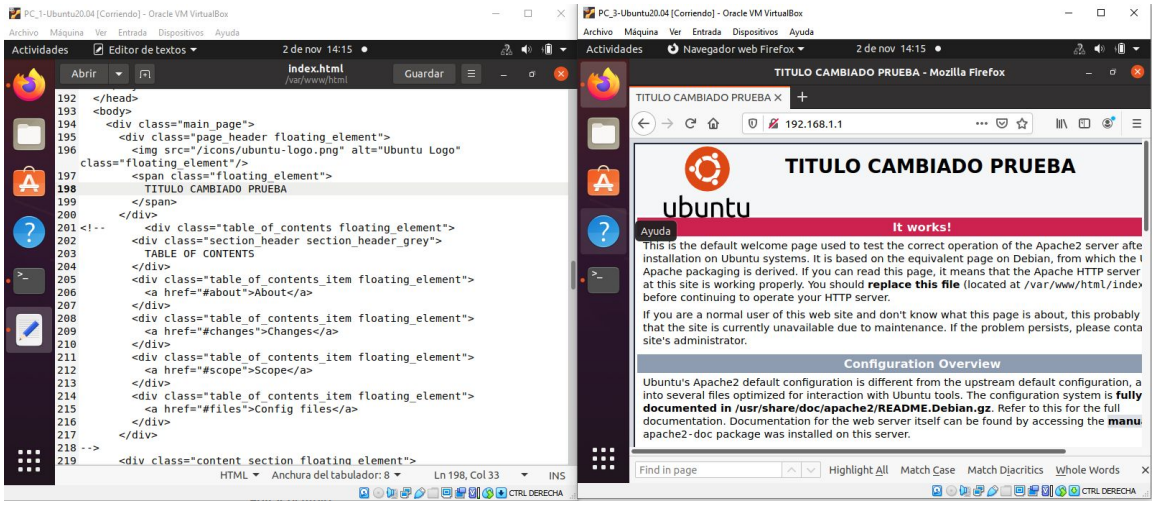
root@pc1:/home/administrador# apt-get install apache2 apache2-doc
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
apache2 ya está en su versión más reciente (2.4.41-4ubuntu3.1).
apache2-doc ya está en su versión más reciente (2.4.41-4ubuntu3.1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 182 no actualizados.

*Activamos el servicio y para comprobar que funciona, visitamos en el navegador **http://localhost** y nos muestra la página de inicio de apache2.*

root@pc1:/home/administrador# service apache2 start



*Para modificar el contenido de la página de inicio, deberemos modificar el archivo **"/var/www/html/index.html"** en el cual escribiremos un título. Desde PC_3 accedemos a **http://192.168.1.1** la cual es la IP de PC_1, y vemos el título que hemos escrito, comprobando así que la dirección de nuestro servidor es accesible.*



8.

2.

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 modificar el puerto de escucha del servidor , tendremos que actualizar 3 archivos para establecer el puerto 8080. El primer archivo es **"/etc/apache2/ports.conf"***

Abrir — ports.conf — /etc/apache2 — Guardar

```
1 # If you just change the port or add more ports here, you will likely also
2 # have to change the VirtualHost statement in
3 # /etc/apache2/sites-enabled/000-default.conf
4
5 NameVirtualHost *:8080
6 Listen 8080
7
8 <IfModule ssl_module>
9     Listen 443
10 </IfModule>
11
12 <IfModule mod_gnutls.c>
13     Listen 443
14 </IfModule>
15
16 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

*El segundo es "**/etc/apache2/sites-enabled/000-default.conf**"*

Abrir — *000-default.conf — /etc/apache2/sites-enabled — Guardar

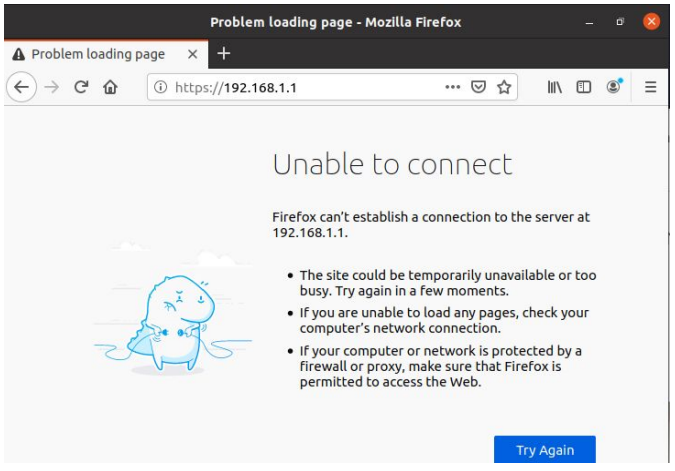
```
1 <VirtualHost *:8080>
2     # The ServerName directive sets the request scheme, hostname and port
  that
3     # the server uses to identify itself. This is used when creating
```

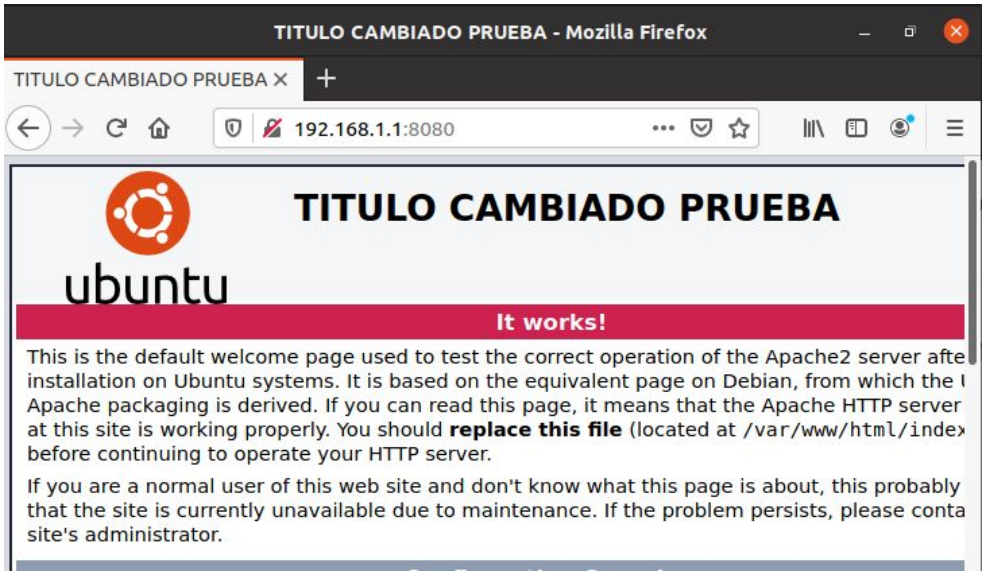
*Y por último el archivo **"/etc/apache2/sites-avaliable/default"***

Abrir — default — /etc/apache2/sites-available — Guardar

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

*Y para comprobarlo, reiniciamos el servicio y accedemos mediante "**http://192.168.1.1:8080**", ya que observamos que sin poner el puerto no nos deja entrar.*





8.
    3. Cree una página de acceso restringido (es decir, que requiera usuario y contraseña antes de mostrarla) en *http://localhost/restringida/*. Utilice como credenciales de acceso el usuario *admin* y la contraseña *1234*.

Lo primero que tenemos que hacer es crear una carpeta en **var/www/** con nombre restringida.

A continuación editamos el fichero **/etc/apache2/sites-enabled/000-default** y cambiamos la línea **AllowOverride None** por **AllowOverride all,** esto lo hacemos para que cuando estemos accediendo a los diferentes sitios, tenga que sobreescribir la configuración (la de acceso) y la coja independientemente de cada sitio(la página restringida).

Para que coja el archivo propio de la página que queremos restringir, vamos a crear un fichero **.htaccess** dentro de la carpeta restringida, a la cual le pondremos lo siguiente:

AuthType Basic
AuthName Acceso Restringido
AuthUserFile /etc/apache2/.htpasswd

La última línea indica el fichero que debe coger para identificar a los usuarios que tendrán acceso, en este caso lo hemos situado en **/etc/apache2/.htpasswd.**

Para crear este fichero utilizamos el comando **htpasswd -c /etc/apache2/.hpasswd admin,** admin es el usuario, con esto automáticamente lo ciframos y deja que solo apache tenga acceso para que no haya ningún tercero con acceso.

Este comando nos pedirá la contraseña dos veces, que será **1234.**
Con esto ya tendríamos la página restringida funcionando.