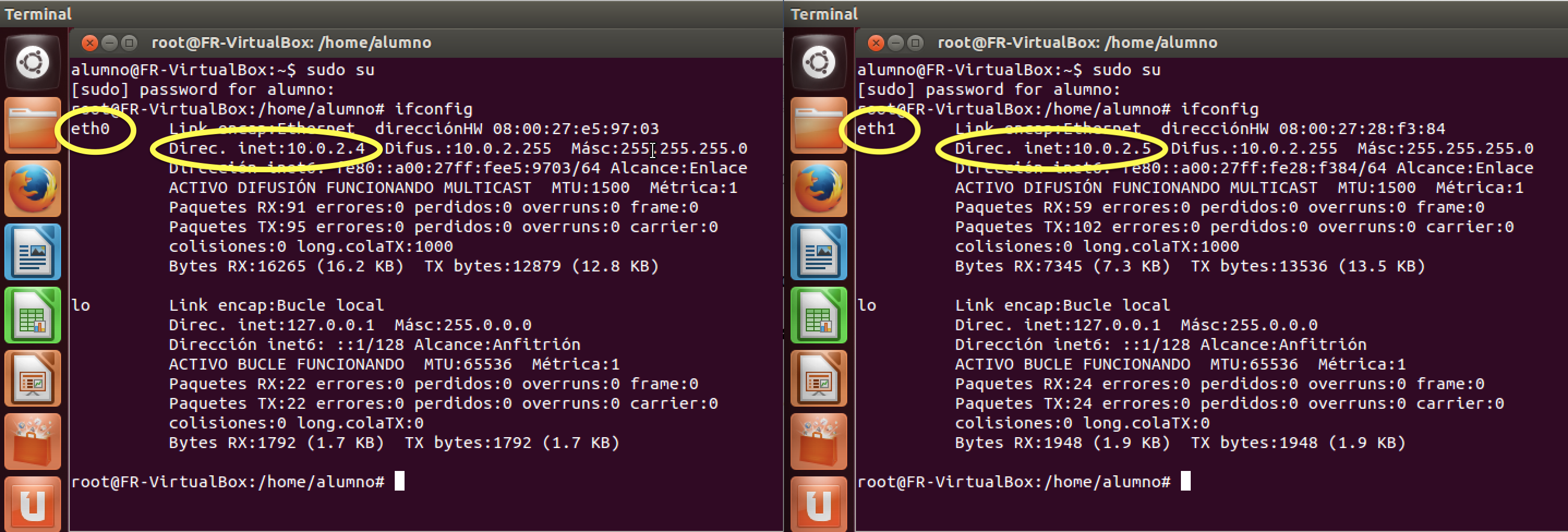
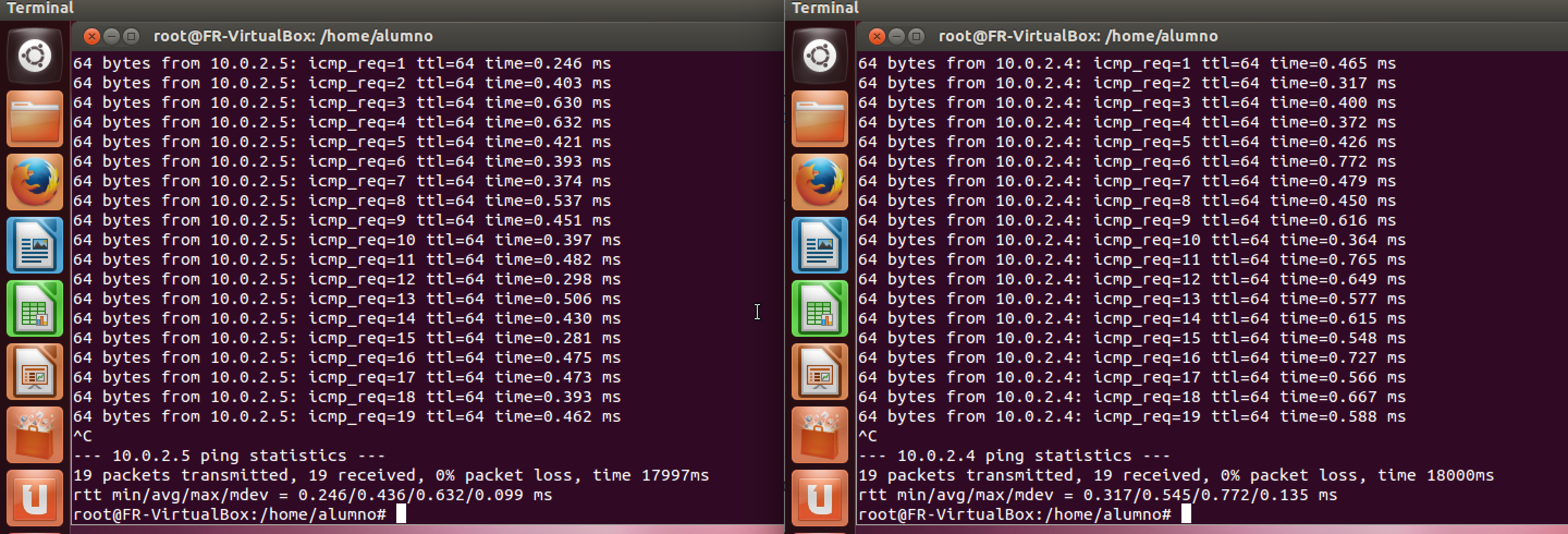
**Realización PRACTICA 1**

* **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?**

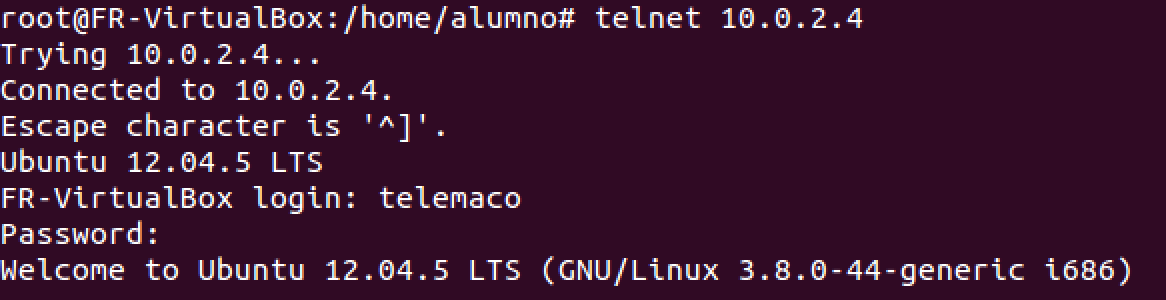
-Las interfaces son eth0 y eth1. Direcciones de red: 10.0.2.4 y 10.0.2.5 respectivamente.



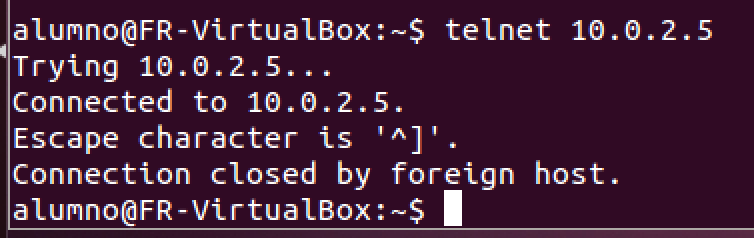
* **2)  Compruebe que existe conectividad con otro equipo del laboratorio, mediante la utilidad *ping*.**

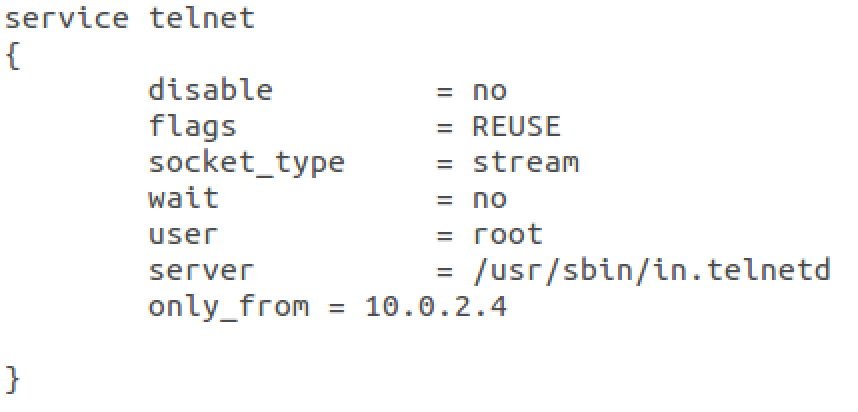


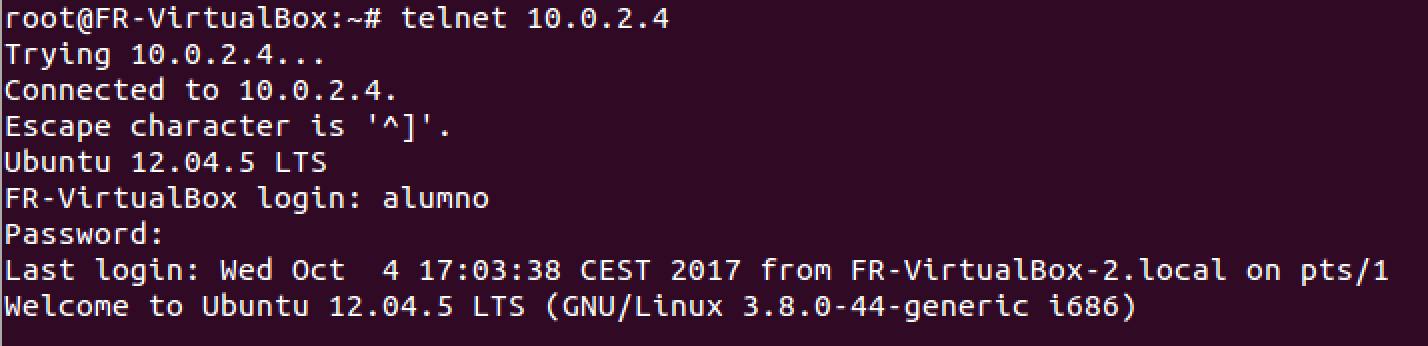
* **3)  Cree una cuenta de usuario en su equipo, habilite el servicio *telnet* y compruebe con algún compañero que dicho servicio es accesible.**



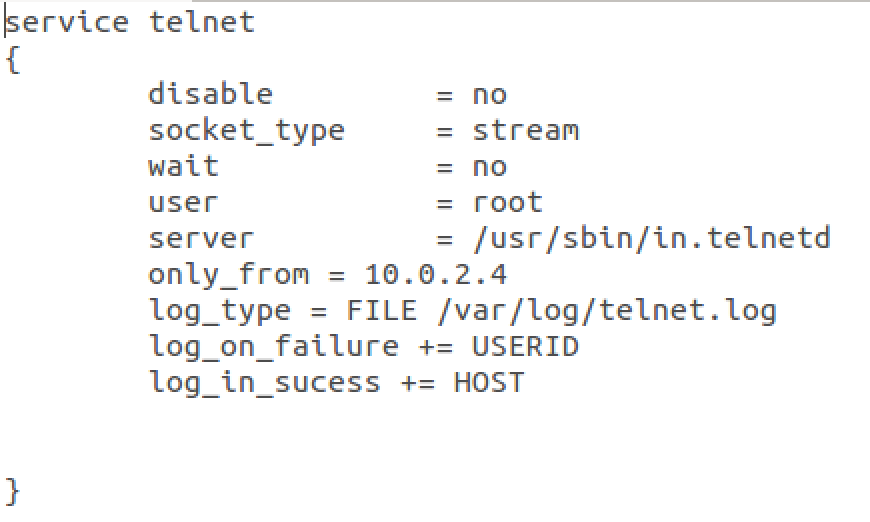
* **4)  Configure el servicio telnet para que:** 
  + **a)  Sólo sea accesible desde la dirección IP de su compañero.**





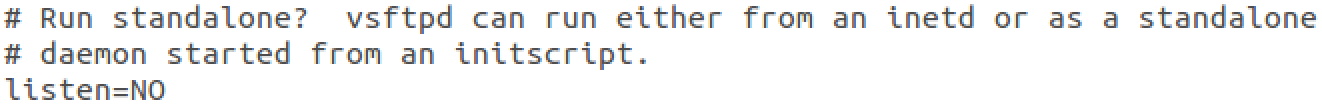


**b)  Se registren en el fichero /var/log/telnet.log los intentos de acceso con y sin  éxito al servicio telnet, indicando la dirección IP del equipo que intenta el acceso.**



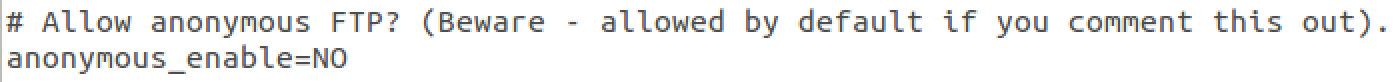
* **5)  Habilite el servicio *ftp* en su equipo. Para esto es necesario:**

1. **Configurar ftp para que no funcione en modo *standalone*.**



1. **Impedir el acceso de la cuenta *anonymous*.**

Dentro del archivo /etc/vsftp.conf se cambia la variable anonymous\_enable por defecto YES, a NO.

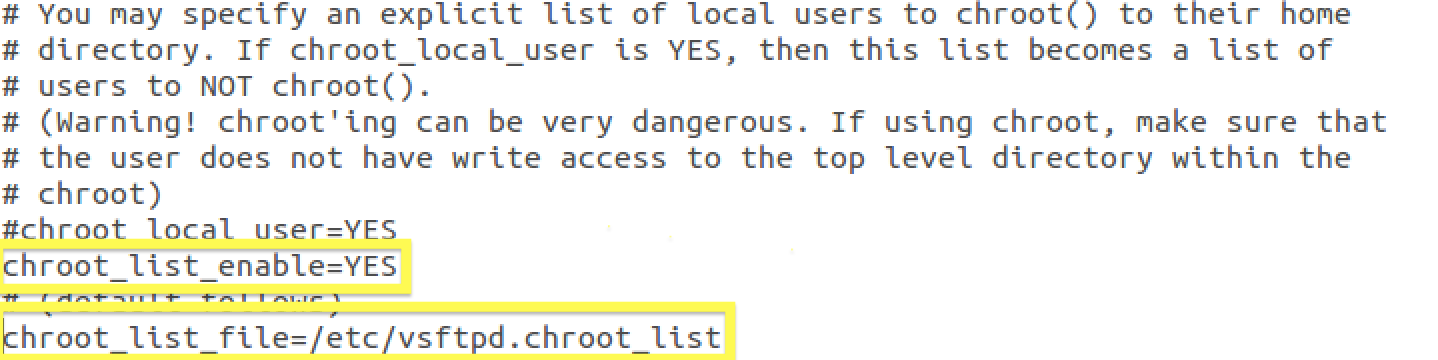


1. **Permitir cuentas locales para acceder al servicio.**

Se descomenta la sentencia -> local\_enable=YES

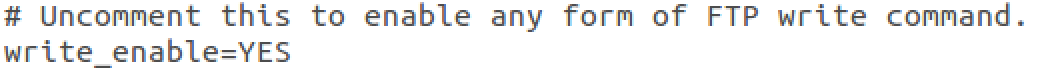


* **6)  Pida a un compañero que pruebe el servicio ftp a través de la cuenta de usuario creada en el paso 3 descargando un fichero desde su equipo.**
* **7)  Configure el servicio ftp para que:** 
  + **a)  Únicamente pueda ser utilizando a través de la cuenta de usuario que hemos creado  en nuestro equipo.**



Después de esto, hago service xinetd restart y luego creo el archivo /etc/vsftpd.chroot\_list con el nombre de usuario creado (telemaco).

* + **b)  Acepte la subida de ficheros al servidor ftp.**



* **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.**

* + **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*.**
  + **c)  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*. Para crear un archivo de credenciales utilice el comando htpasswd -c  /ruta/passwords <usuario>, donde ruta será un directorio fuera de los  directorios servidor por Apache (por motivos de seguridad).**

Para realizar este apartado existen dos posibilidades: usar directamente el fichero

de configuración general *apache2.conf* o un archivo de configuración *.htaccess* dentro del directorio restringido. Utilice éste última forma de proceder (*.htaccess*). Recuerde usar la directiva AllowOverride que, bien configurada, hace que prevalezcan las directivas incluidas en el fichero .htaccess sobre las generales que podemos encontrar dentro del fichero apache2.conf