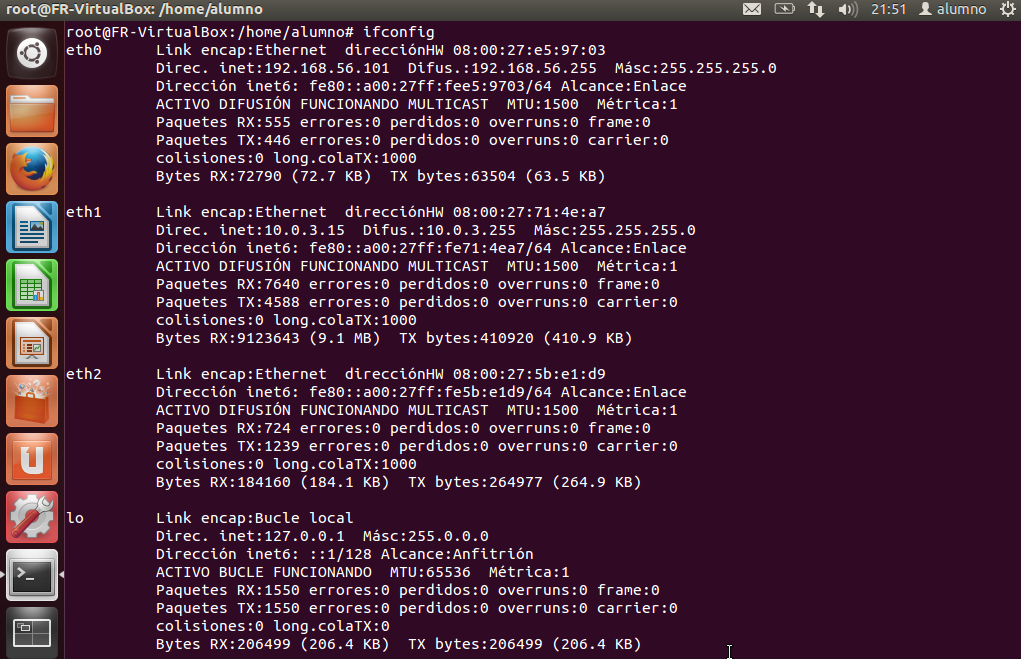
1. Compruebe las direcciones IP que tienen asignadas las diferentes interfaces de red de su equipo mediante el comando *ifconfig*, ¿cómo se llaman dichas interfaces? ¿qué direcciones de red tienen definidas?

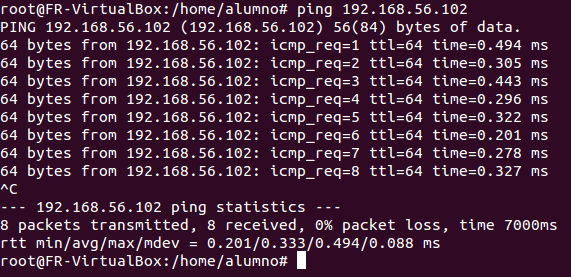


Como vemos, tenemos eth0, eth1 y eth2, las tres son Ethernet. Las direcciones IP de eth0 y eth1 son 192.168.56.101 y 10.0.3.15. Eth0 y eth1 son de tipo Solo-Anfitrión y NAT, respectivamente. Eth2 no tiene dirección IP pues es una red interna.

Además, tenemos un loopback o bucle local, que se suele utilizar cuando la transmisión de datos tiene como destino el propio host. Su IP es 127.0.0.1.

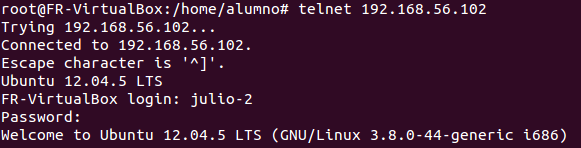
2) Compruebe que existe conectividad con otro equipo del laboratorio, mediante la utilidad *ping*.

En este caso voy a usar dos máquinas virtuales. Vamos a ver si, desde la primera ( IP 192.168.56.101 ) podemos comprobar que hay conectividad con la segunda ( IP 192.168.56.102 ):

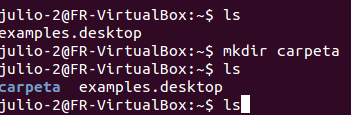
Como vemos, se han enviado 8 paquetes exitosamente entre la primera máquina virtual y la segunda, por lo que podemos comprobar que existe conectividad entre ambas máquinas.

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

Una vez instalado telnet, podemos conectarnos desde una máquina con la otra usando el comando telnet <ID>.



Una vez conectados (usando el usuario de la otra máquina), podemos manejar la segunda máquina desde la primera.



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:

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

Para realizar a), b) y c) vamos a tener que modificar el fichero /etc/vsftpd.conf

En A), debemos añadir la línea:

listen=NO

Aunque así es como está por defecto.

En B), debemos añadir la línea:

anonymous\_enable=NO

En C), debemos añadir la línea:

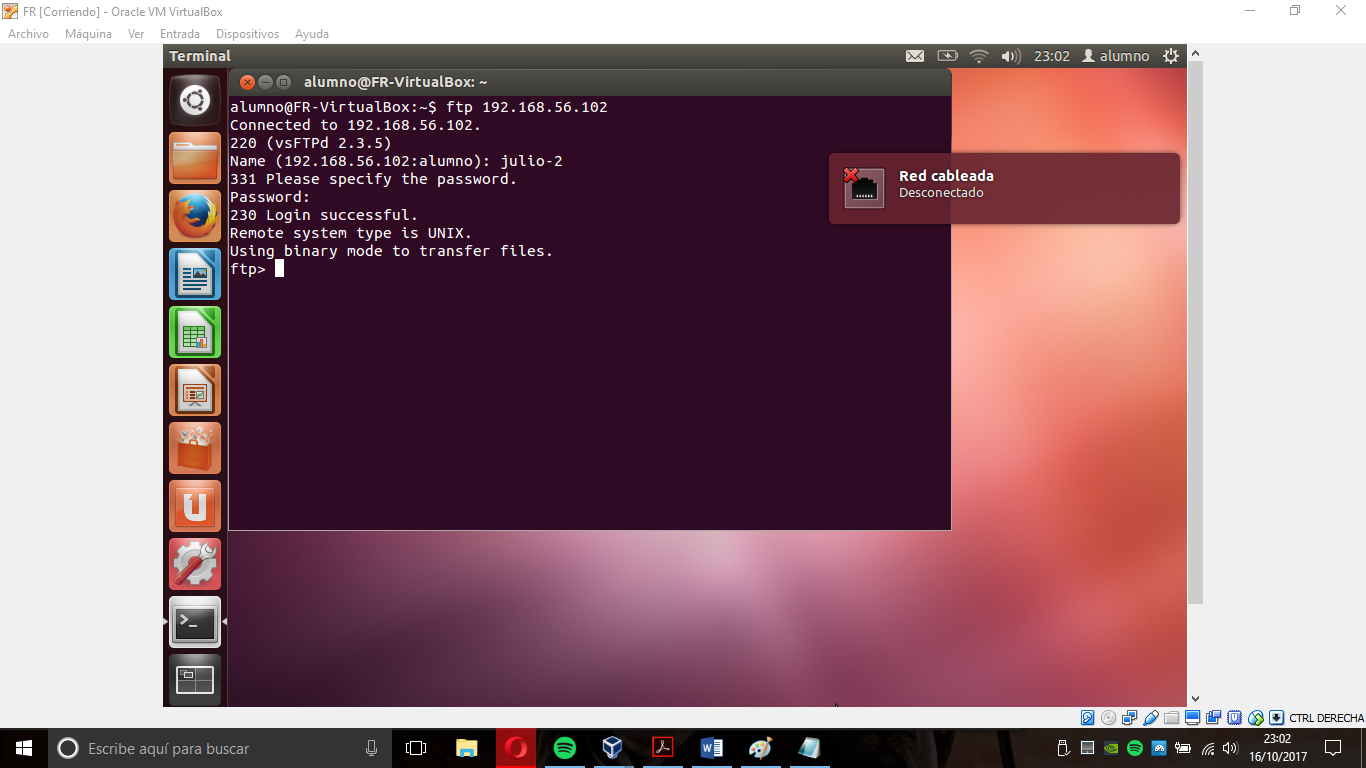
local\_enable=YES

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.

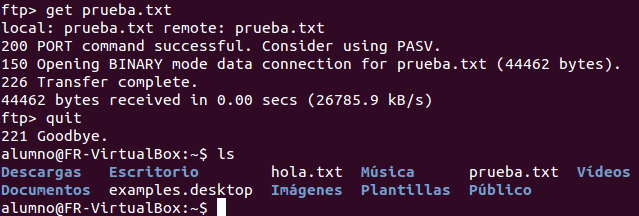
Vamos a usar las máquinas virtuales. Vamos a probar a descargarnos el siguiente fichero desde la otra máquina:



En la primera máquina, nos conectamos al ftp:



Ahora podemos descargarnos el archivo prueba.txt:



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.

b) Acepte la subida de ficheros al servidor ftp.

Para configurar, debemos añadir estas líneas al archivo /etc/vsftpd.conf:

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.

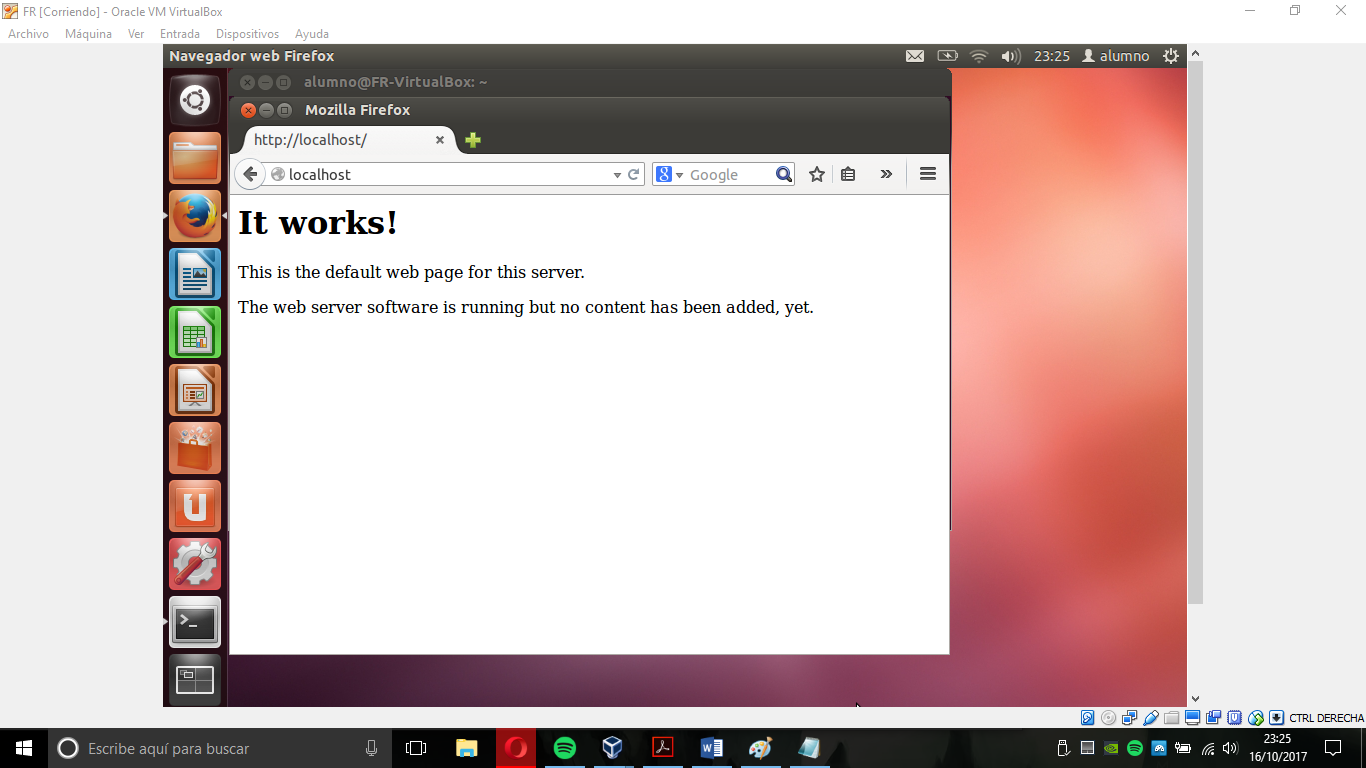
b) Modifique el puerto de escucha del servidor de modo que el acceso a la página de inicio se haga mediante la dirección: *http://localhost:8080*.

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

Vemos que funciona:



A)