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 de red son eth2 que indican que son una red ethernet que en este caso es la segunda ya que tengo otro adaptador de red que corresponde a eth1.
   Las direcciones de red establecidas son la 192.168.1.x
2) **Compruebe que existe conectividad con otro equipo del laboratorio, mediante la utilidad ping.**
   Hacemos ping y efectivamente como pertenecen a la misma red, hacen ping entre ellas.
3) **Cree una cuenta de usuario en su equipo, habilite el servicio telnet y compruebe con algún compañero que dicho servicio es accesible.**
   - Crear un usuario → adduser usuario
   - Habilitar telnet → en el fichero /etc/xinetd.d/telnet debemos poner disable a no.
   - Para conectar → telnet <IP> o <nombre>
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.**

   a) Insertamos en el fichero /etc/xinetd.d/telnet → only_from = <IP>
   b) Insertamos en el fichero /etc/xinetd.d/telnet → log_on_failure +=HOST
   log_on_success += HOST
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

   a) Editamos el archivo /etc/vsftpd.conf → listen = NO
   b) Editamos el archivo /etc/vsftpd.conf → anonymous_enable = NO
   c) Editamos el archivo /etc/vsftpd.conf → 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.**
   Nos conectamos desde el cliente con – ftp <IP> -- , una vez conectados, con – get <fichero> -- descargamos el fichero que hemos seleccionado.
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.**

   a) Editamos el fichero /etc/ftpusers → Escribimos el nombre de los usuarios que NO queremos que se pueda acceder vía ftp
   Podemos en /etc/vsftpd.conf insertar las líneas userlist_enable=YES, userlist_deny=NO, userlist_file=…

b) Editamos el fichero /etc/vsftpd.conf → write_enable = YES

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.**
      i. **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).**
      ii. **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**

a) Editamos el fichero /var/www/index.html

b) Editamos el fichero /etc/apache2/ports.conf y /etc/apache2/sites-enabled/default

c) Hay que editar el fichero /etc/apache2/sites-enabled/default y añadir:

```
<Directory "/var/www/restringida">
    AllowOverride All
</Directory>
```

Editamos el fichero /var/www/restringida/.htaccess :

```
AuthType Basic
AuthName "Acceso restringido"
AuthUserFile /etc/apache2/passwd
Require valid-user
```