**Miembros:**

Jaime Millán Gálvez

José Santos Salvador

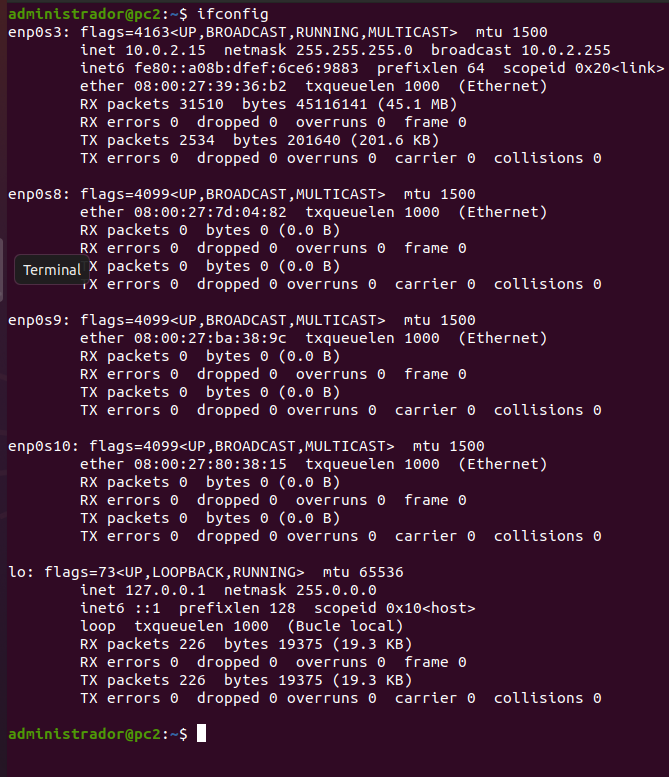
Práctica 1 – Configuración de servicios de red

(0.75 puntos)

## Realización práctica

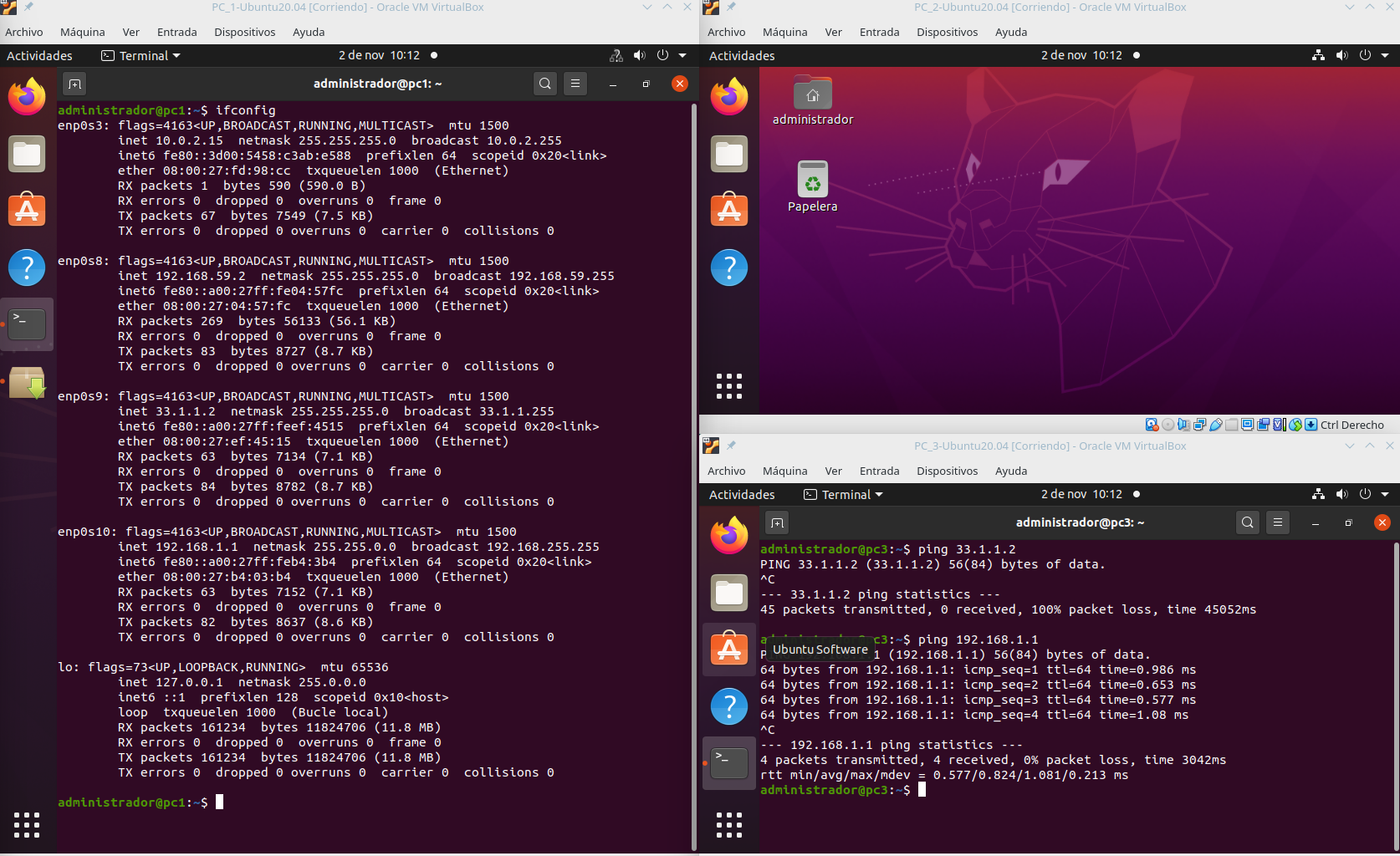
1. Compruebe las direcciones IP que tienen asignadas las diferentes interfaces de red de su equipo mediante el comando *ifconfig*, ¿cómo se llaman dichas interfaces? ¿qué direcciones de red tienen definidas?

|  |
| --- |
| Hay cuatro interfaces de red, enp0s3, enp0s8, enp0s9, enp0s10 y lo. Las direcciones son:  enp0s3 – 10.0.2.15  enp0s8 – 192.168.59.3 //terminan en 3 para pc2, termina en 2 para pc1, termina en 4 para pc3  enp0s9 – 33.1.1.3  enp0s10 – 192.168.1.2 //en el pc1 termina en 1, pc2 termina en dos, pc3 termina en 3  lo – 127.0.0.1  24 es la mascara de red, y 32- 24 = 8 bits para identificar a los distintos equipos.  La interfaz enp0s9 (datos) tiene una mascara de red de 24 bits, por lo tantos 32-24 = 8 bits para identificar los hosts, de ahí que cada máquina tenga una terminación distinta para las mismas interfaces de red.  Con la interfaz enp0s10 (gestión) pasa igual pero con una mascara de red de 16 bits. |



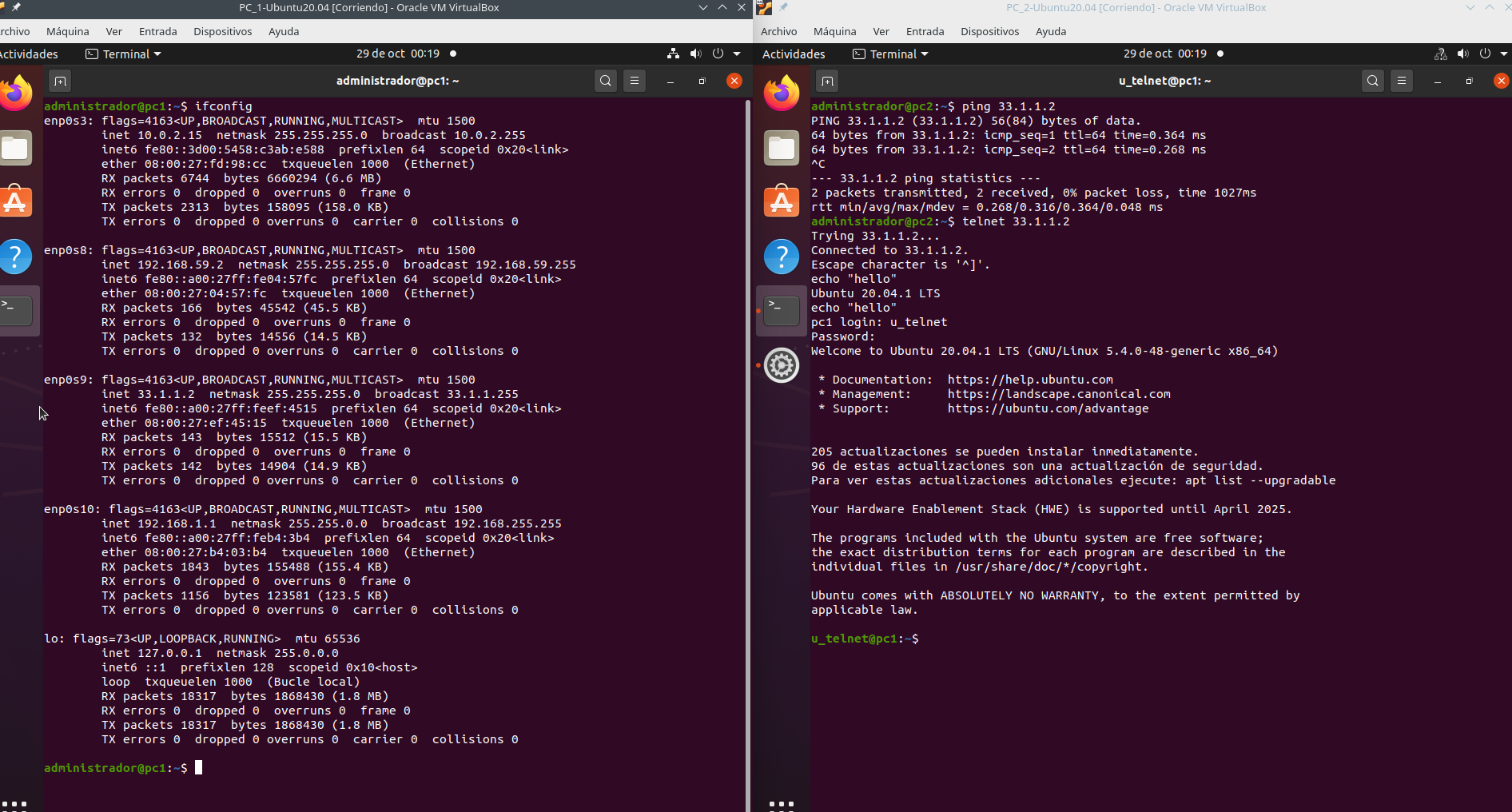
1. Compruebe que existe conectividad con otro equipo del laboratorio, mediante la utilidad *ping*. ¿Es posible hacer ping desde el PC\_1 al PC\_3 por la red 33.1.1.0/24? ¿Y por la red 192.168.1.0/16? Justifique su respuesta. A partir de ahora la primera de las redes la llamaremos de *datos* mientras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

|  |
| --- |
| No es posible hacer ping de PC1 a PC3 por la red 33.1.1.0/24. Por la red 192.168.1.0/16 si se puede hacer. Esto es debido a que la conexión a través de la red 33.1.1.0/24, solo es posible entre PC1 y PC2. Para conectarte con la 3 es necesario que los 8 penúltimos tienen que ser iguales para que se conecten entre maquinas.  Ya que la interfaz de red enp0s9 proporciona la ip  33.1.1.2 //PC1  33.1.1.3 //PC2  33.1.2.2 //PC3  //estás cambiando los 16 últimos y no puedes, dirección 24 bits y 8 bits para host.  Red = IP + HOST // Son 32 bits |



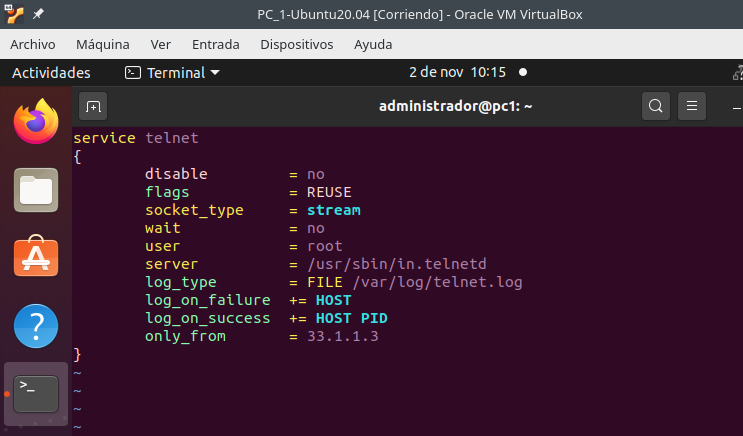
1. Cree una cuenta de usuario en su equipo, habilite el servicio *telnet* y compruebe con algún compañero que dicho servicio es accesible.

|  |
| --- |
| //PC1  add user u\_telnet  cp telnet /etc*/*xinetd.d  sudo service xinetd restart //si no está iniciado hay que usar start  //PC2  telnet 33.1.1.2  escribes user y contraseña |



1. Configure el servicio telnet para que:
   1. Sólo sea accesible desde la dirección IP de su compañero.

|  |
| --- |
| Se hace con only\_from en el archivo de xinetd de telnet  only\_from = 33.1.1.3 |



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

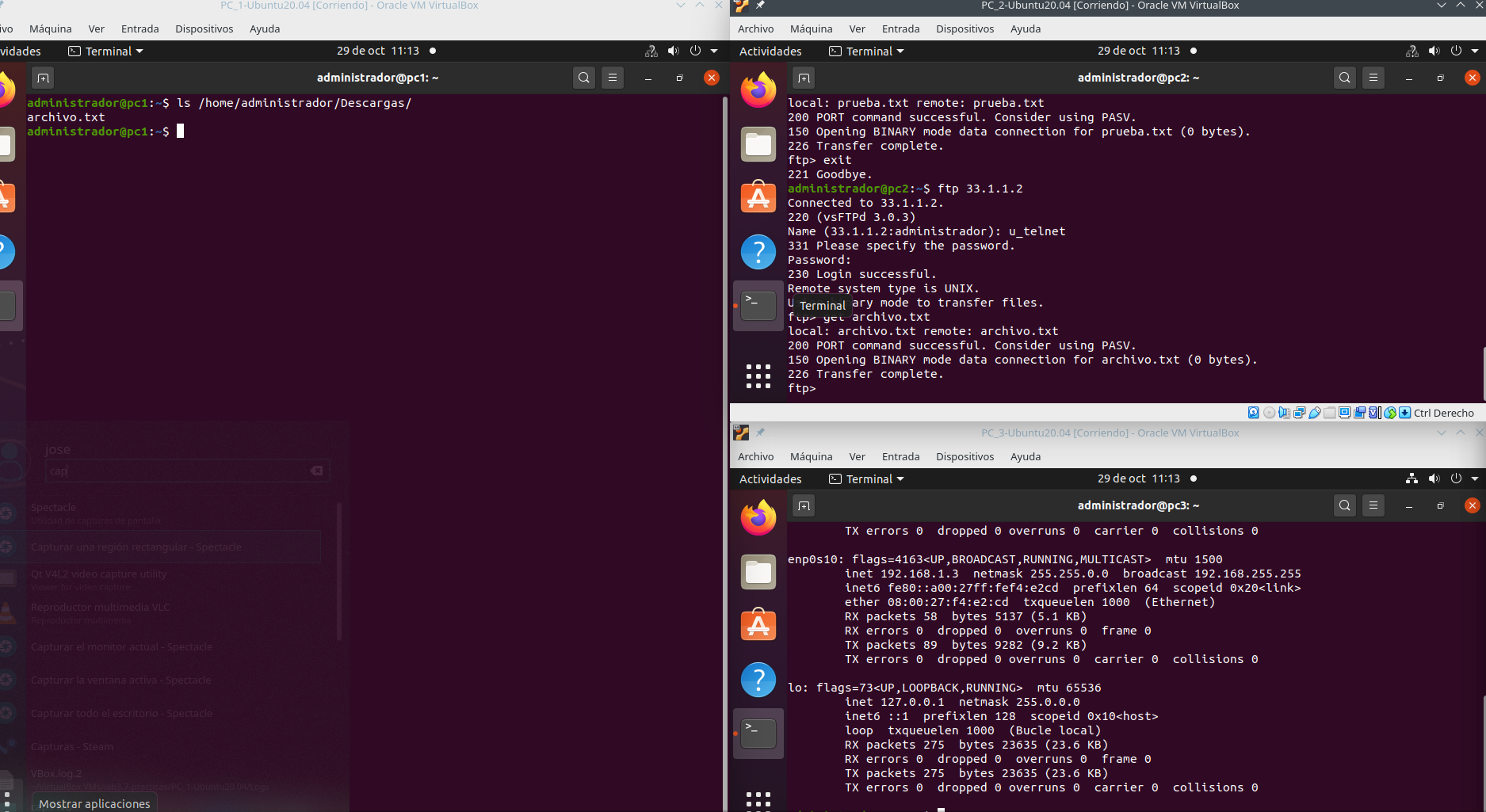
|  |
| --- |
| Cambias ruta donde va el log con log\_type y para decir IP pues HOST y += porque por defecto  “Configures xinetd to log if the connection is successful. By default, the remote host's IP address and the process ID of server processing the request are recorded”  “log\_on\_failure — Configures xinetd to log if there is a connection failure or if the connection is not allowed”[1][2]  service telnet  {  disable = no  flags = REUSE  socket\_type = stream  wait = no  user = root  server = /usr/sbin/in.telnetd  log\_type = FILE /var/log/telnet.log  log\_on\_failure += HOST USERID  log\_on\_success += HOST USERID  only\_from = 33.1.1.3  } |

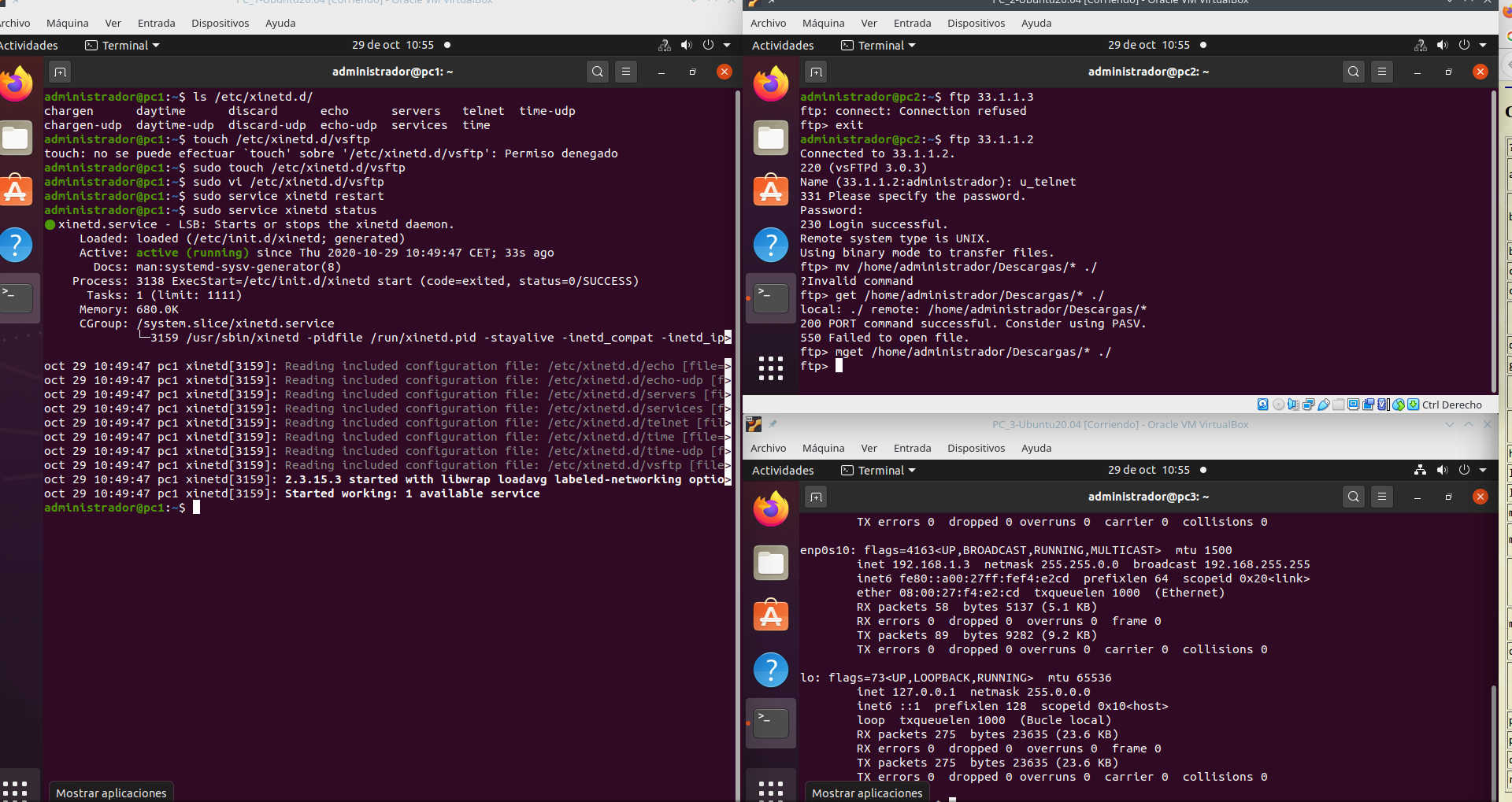
1. Habilite el servicio *ftp* en su equipo (de la “*a”* a la “*c”*).

|  |
| --- |
| Lo primero que tenemos que hacer es instalar el servicio como se indica en el guión, con apt-get install vsftpd. Luego copiamos el archivo que nos dan en la carpeta /etc/xinetd.d/. El archivo que debemos modificar es el que se encuentra en /etc/vsftdp.conf:  a) Para desactivar el modo stanalone debemos escribir la orden **listen = NO**  b) Si no queremos que que la cuenta anonymous acceda escribimos **anonymous\_enable = NO**  c)Si queremos permitir cuentas locales escribimos **local\_enable = YES** |

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

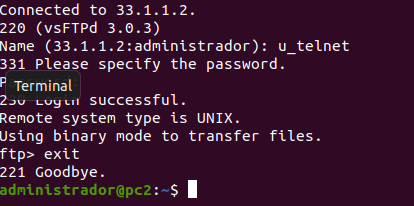
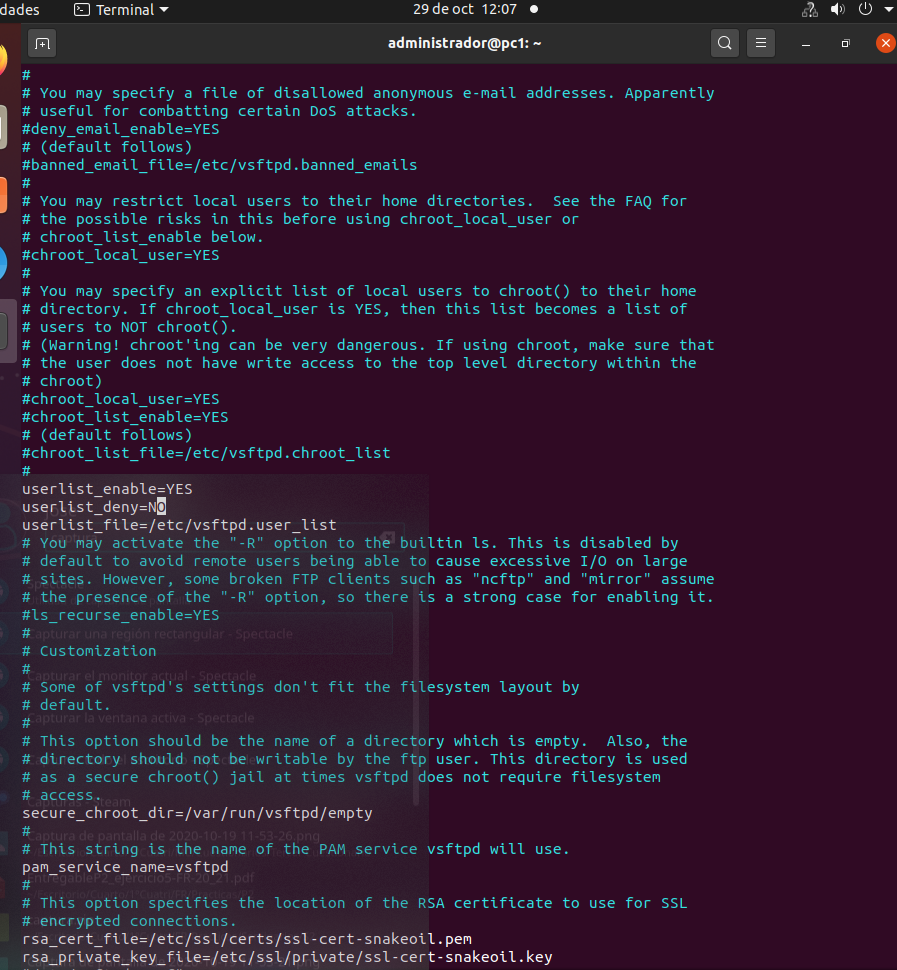
|  |
| --- |
| mget para descargar varios archivos  get para descargar un unico archivo  para hacer put (subir archivo) tuvimos que cambiar etc/vsftpd.conf y habiliar write\_enable YES  para cambiar el directorio al que llegan los archivos lcd. Por defecto llegan a /home*/*administrador |





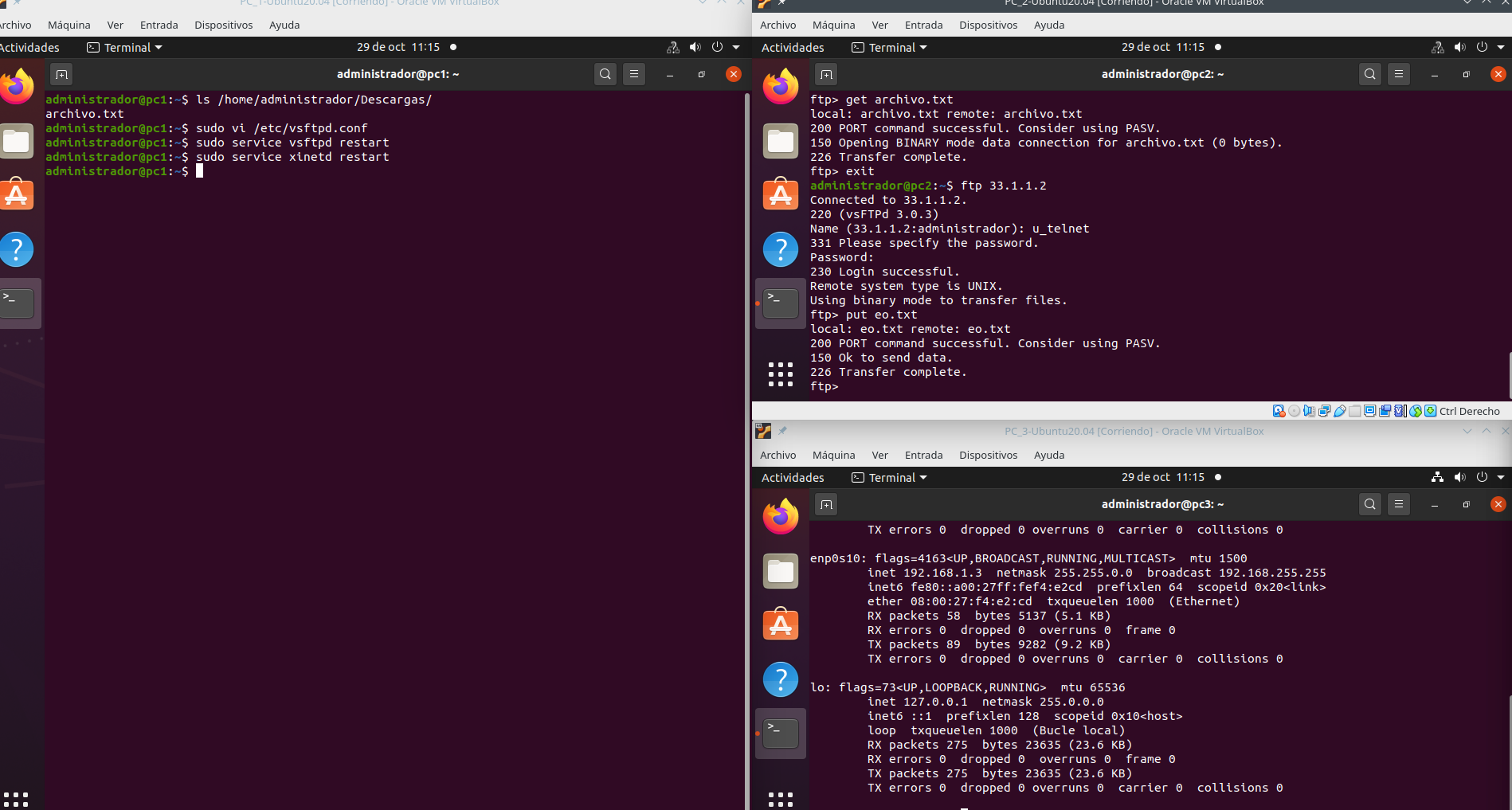
1. Configure el servicio ftp para que:
   1. Únicamente pueda ser utilizando a través de la cuenta de usuario que hemos creado en nuestro equipo.

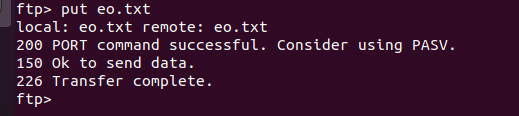
|  |
| --- |
| En /etc/vsftpd.conf editas  userlist\_enable=YES  userlist\_deny=NO  userlist\_file=/etc/vsftpd.user\_list  he creado el archivo etc/vsftpd.user\_list  y le he puesto u\_telnet dentro |



* 1. Acepte la subida de ficheros al servidor ftp.

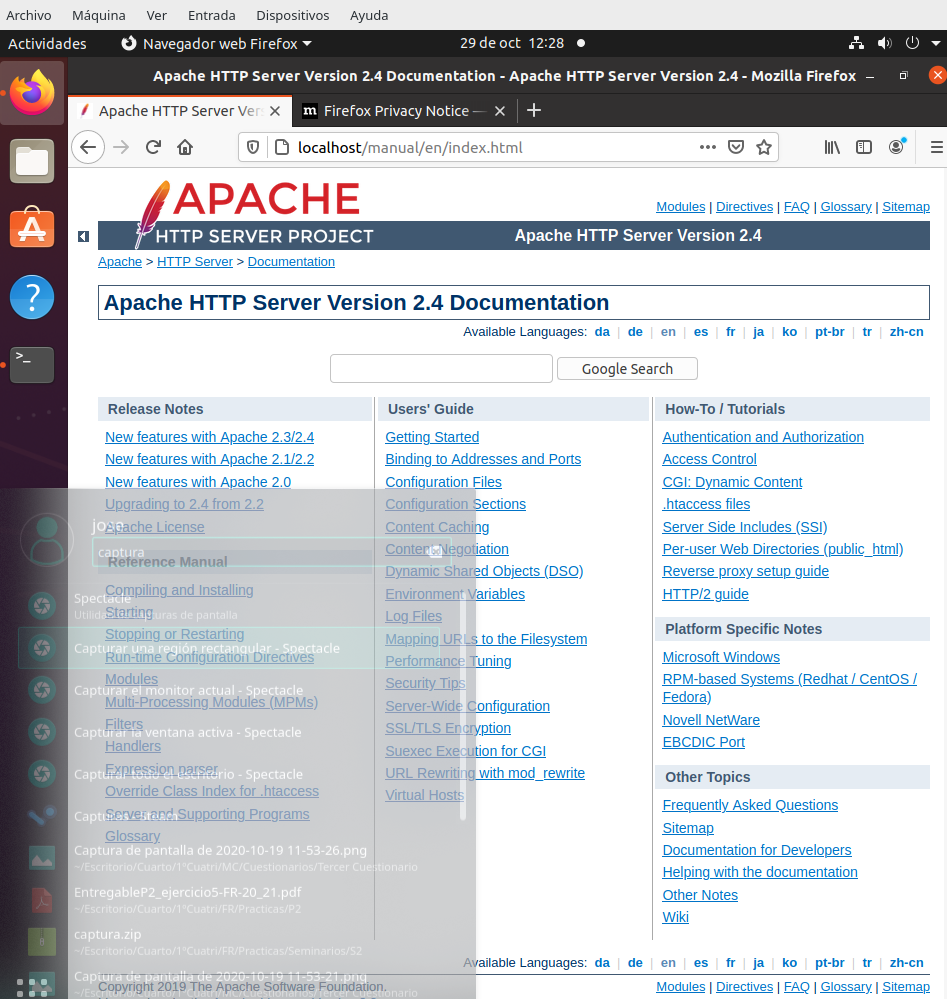
|  |
| --- |
| Editamos el archivo /etc/vsftpd.conf  write\_enable =YES |

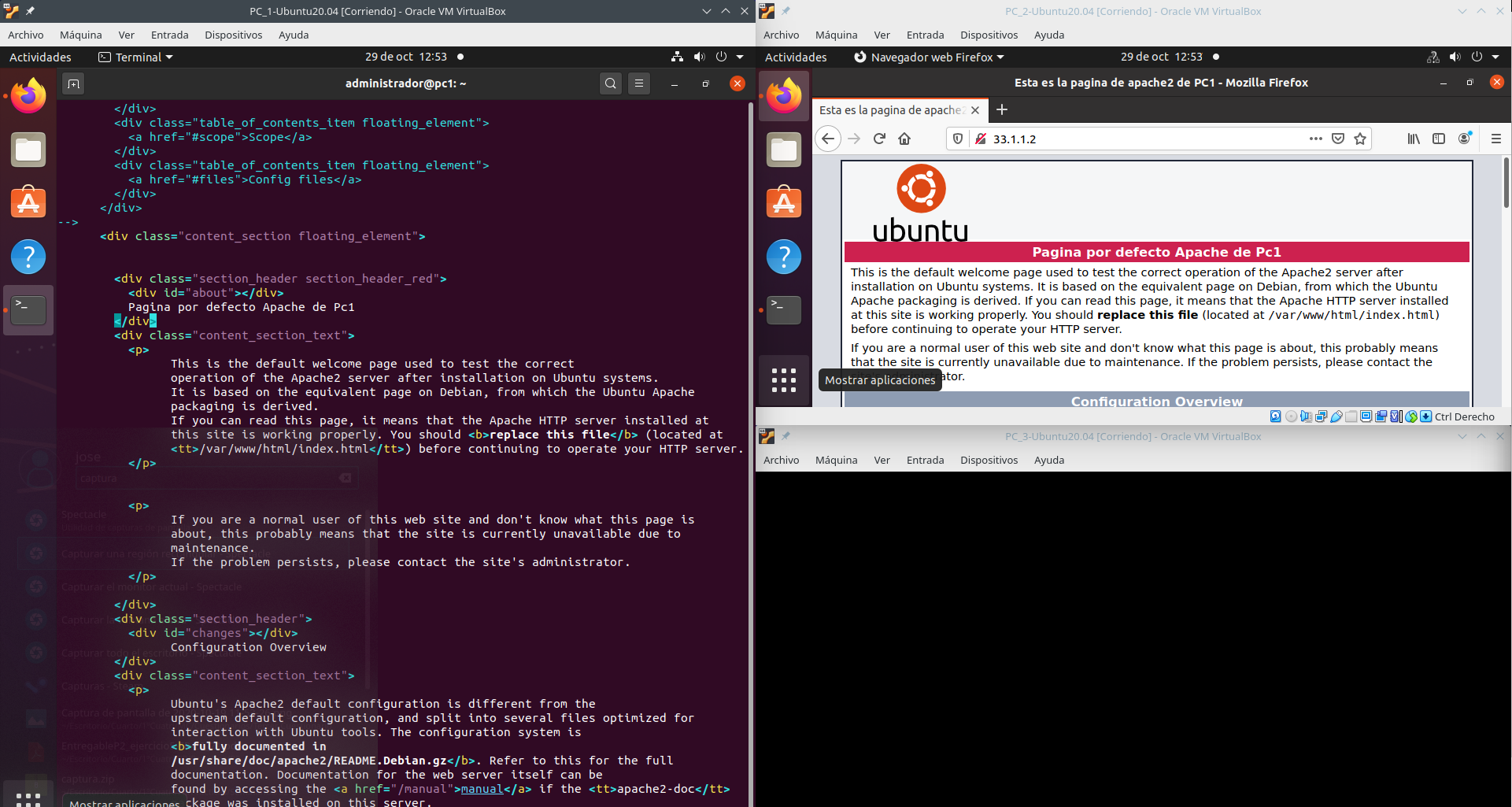




1. Habilite el servicio *http* en su equipo. Abra un navegador web y pruebe a visitar la página de inicio desde su equipo (http://localhost o http://127.0.0.1). Además, realice los siguentes cambios:
   1. Modifique el contenido de la página de inicio, y compruebe con la ayuda de su compañero que la dirección de su servidor es accesible.

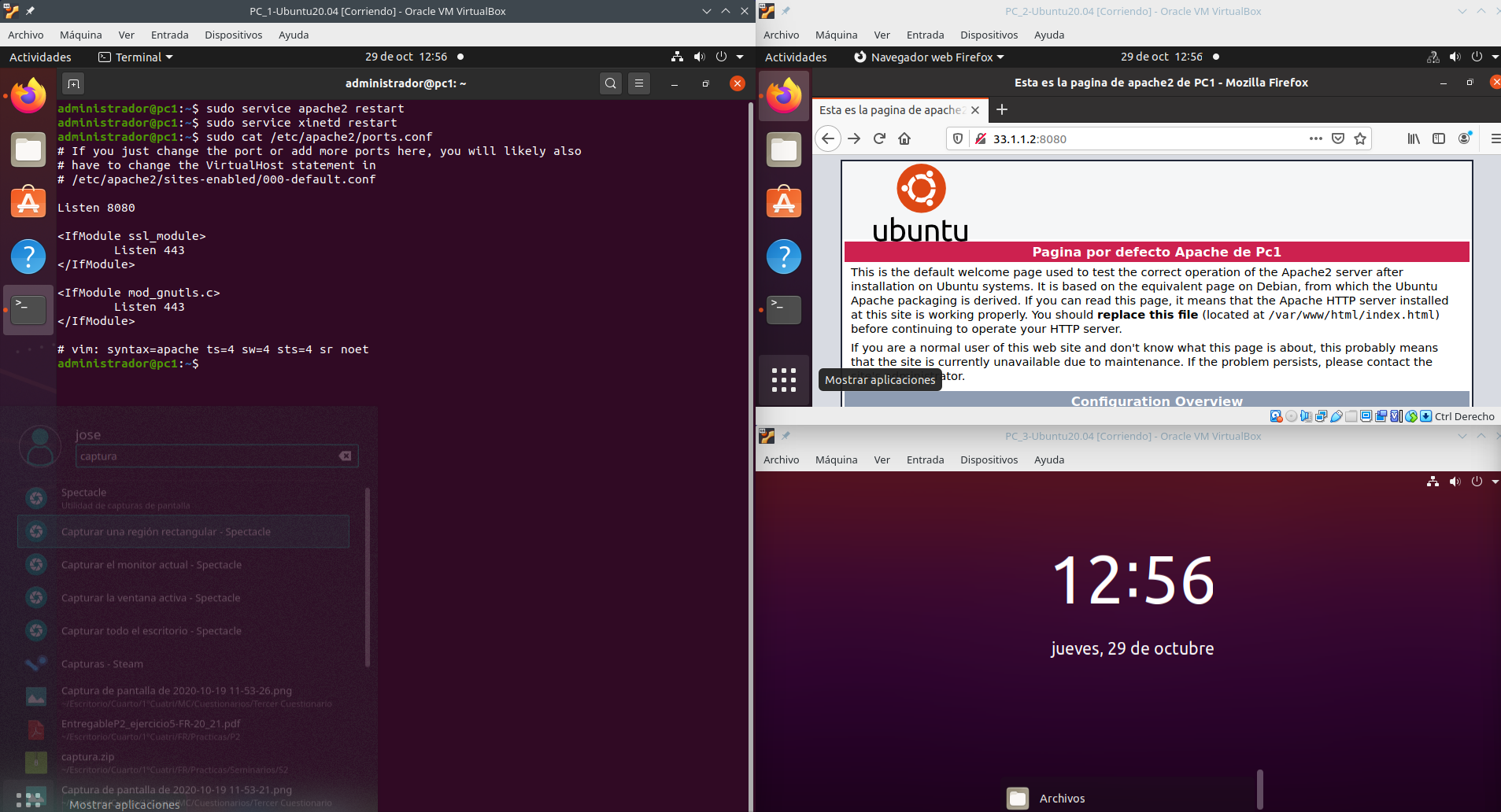
|  |
| --- |
| modificar index.html en la carpeta var/www/html  luego llamas con el otro desde diraccion ip, que es 33.1.1.2 y no pones puerto porque escoge por defecto el 80 de apache2 |





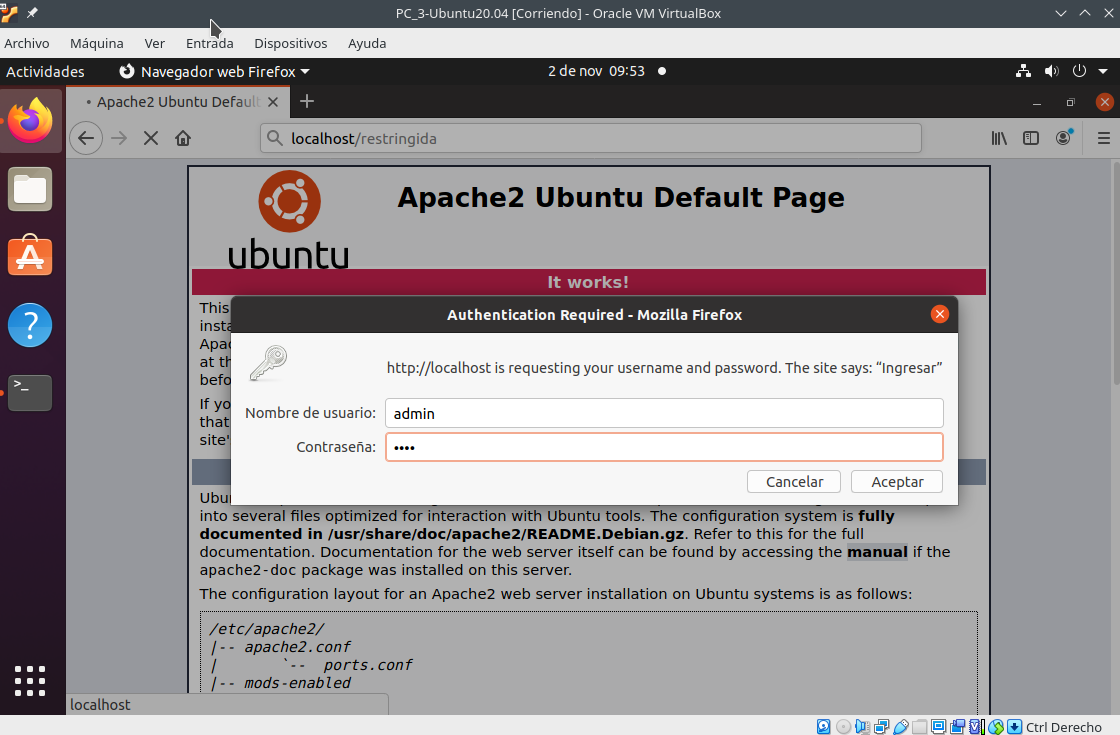
* 1. Modifique el puerto de escucha del servidor de modo que el acceso a la página de inicio se haga mediante la dirección: *http://localhost:8080*.

|  |
| --- |
| cambias sudo vi /etc/apache2/ports.conf  Listen 8080  luego haces sudo service apache2 restart  http://localhost:8080 |



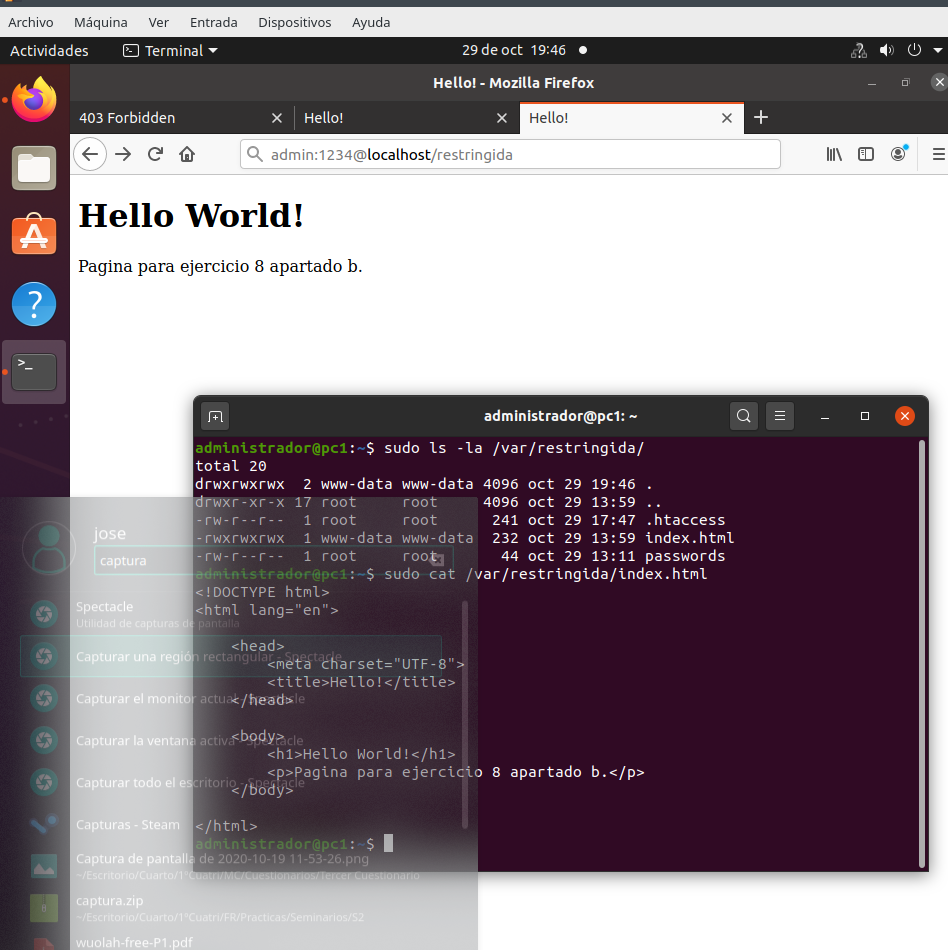
* 1. Cree una página de acceso restringido (es decir, que requiera usuario y contraseña antes de mostrarla) en [*http://localhost/restringida/*](http://localhost/restringida/). Utilice como credenciales de acceso el usuario *admin* y la contraseña *1234*.

|  |
| --- |
| mkdir /var/www/html/restringida  touch /var/www/html/restringida/index.html  vi /var/www/html/restringida/index.html  cat /var/www/html/restringida/index.html  <!DOCTYPE html>  <html lang="en">  <head>  <meta charset="UTF-8">  <title>Hola!</title>  </head>  <body>  <h1>Hola Practica!</h1>  <p>Pagina para ejercicio 8 apartado c.</p>  </body>  </html>  sudo vi /etc/apache2/apache2.conf  <Directory /var/www/>  Options Indexes FollowSymLinks  AllowOverride AuthConfig  Require all granted  </Directory>  Se tiene que modificar apache2.conf para que prevalezcan los cambios de .htaccess con AuthConfig en AllowOverride.  htpasswd -c /home/passwords admin  quedando el archivo .htaccess de la siguiente forma:  AuthName "Pagina restringida, entrar:"  AuthType Basic  AuthUserFile /home/passwords  Require user admin  despues es necesario recargar apache2  sudo service apache2 reload |



**Método de trabajo:**

Cada uno la realizó por su cuenta y después quedamos para ponerlo en común y discutir las ideas que había desarrollado cada uno. Una vez puesto en común, completamos el entregable con las ideas que más nos convencieron.



Referencias:

[1]: https://linux.die.net/man/5/xinetd.conf

[2]https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/4/html/reference\_guide/s1-tcpwrappers-xinetd-config