<table>
<tr><td>  </td><td colspan="2">UNIVERSIDAD DON BOSCO
FACULTAD DE ESTUDIOS TECNOLÓGICOS
Escuela de computación</td></tr>
<tr><td rowspan="6">CICLO: 1/2015</td><td colspan="2">Guía de laboratorio # 6</td></tr>
<tr><td>Nombre de la practica:</td><td>FTP/TFTP server</td></tr>
<tr><td>Lugar de ejecución:</td><td>Laboratorio de redes</td></tr>
<tr><td>Tiempo estimado:</td><td>2 horas y 30 minutos</td></tr>
<tr><td>MATERIA:</td><td>Servicios de red</td></tr>
<tr><td>Facilitador:</td><td>Ing. Mauricio Figueroa</td></tr>
</table>

I. Objetivos.

Que el estudiante:

- Configure un servidor vsftp para acceso seguro y anónimo.
- Configure un servidor tftp y su respectiva seguridad.

II. Introducción teórica

Muchos usuarios están interesados en transferir archivos desde su PC local a una cuenta de web hosting en servidores remotos. Para este tipo de casos es el Protocolo de Transferencia de Archivos la herramienta ideal. FTP permite intercambiar datos entre un servidor y nuestra PC. La idea principal es manipular datos remotos sin mucha dificultad. La mayoría de los servicios de web hosting funcionan con FTP y es un estándar para transferencia de archivos, mirrors, etc.

Un derivado de FTP es el protocolo trivial de transferencia de archivos TFTP. Éste es generalmente utilizado en ambientes de LAN en el que tenemos máquinas que obtienen sus respectivas configuraciones desde este servidor. A diferencia de FTP, TFTP es un servidor no validado, es decir que cualquier máquina en la LAN puede acceder, es por eso que se combina con reglas de filtrado para evitar el acceso de máquinas no permitidas.

En los servidores derivados de Redhat, FTP se implementa utilizando VSFTP que es un

servidor FTP seguro. La implementación de TFTP está siempre asociada al demonio XINETD, que es un servidor que maneja diferentes pequeños servicios de red. En esta práctica se trabajará con la configuración de estos servidores.

III. Materiales y equipo

No.	Requerimiento.	Cantidad.
1.	Guía de laboratorio.	1
2.	PC con conexión a Internet como servidor.	1
3.	PC con acceso a la red LAN como cliente.	1

IV. Procedimientos

IMPORTANTE:

Recuerde que deberá de configurar el cliente de red un vez haya instalado todos los paquetes necesarios para la practica. En el momento de realizar las pruebas del servidor FTP, solicite a un compañero que haga las pruebas a su servidor FTP y TFTP.

Procedimiento 1: Configuración del servidor VSDTP anónimo.

1. Recuerde que en el momento oportuno, debe de estar **totalmente configurado el cliente de red**, para que no halla ningún problema con el servidor.
2. ***"Antes de modificar algún archivo por favor respaldar el archivo original."***
3. Verificar que el servidor VSFTPD esta instalado, para esto sera necesario utilizar el comando ***rpm***.

```
[manuel@PCmanuel ~]$ rpm -q vsftpd
```

4. Si el paquete esta instalado, salte hacía el paso 5, si no esta instalado lo haremos mediante el comando ***yum***.

```
[manuel@PCmanuel ~]$ sudo yum -y install vsftpd
```

5. Verifique en la maquina que sera cliente, que se encuentre instalado el paquete

ftp, para poder realizar la conexión con el servidor, mediante el comando ***rpm***, si no esta instalado, proceda a su instalación, con el comando ***yum***

6. Editar el archivo ***/etc/vsftpd/vsftpd.conf.*** Para mayor referencia sobre las opciones que se van a modificar, leer el manual ofical del servidor vsftpd: ***http://vsftpd.beasts.org/vsftpd_conf.html***
7. Identificar la linea que permite que el servicio este habilitado para las direcciones Ipv4 del sistema, descomentariarla: *listen=YES*
8. Identificar la línea anonymous_enable, asegurarse que tenga como valor YES. Tiene que quedar así: anonymous_enable=YES
9. Agregar el símbolo de comentario a la línea de usuarios local, quedando la línea de la siguiente manera: *#local_enable=NO*
10. Identificar la línea *write_enable=NO*. Si no está así, habilitarla.
11. Identificar la línea *anon_upload_enable=NO*. Si no está así, habilitarla.
12. Agregar la siguiente linea *no_anon_password=YES*
13. Identificar la línea *anon_mkdir_write_enable=NO*. Si no está así, habilitarla.
14. Agregar la línea *anon_root=/var/ftp/pub/*.
15. Agregar la línea *anon_other_write_enable=NO*
16. Agregar la línea *anon_world_readable_only=NO*
17. Agregar la línea *anon_max_rate=2048000*
18. Identificar la línea *xferlog_enable=YES*
19. Identificar la línea *xferlog_file=/var/log/xferlog*
20. Agregar la línea *listen_address=[ip del servidor]*
21. Agregar la línea listen_port=21
22. Identificar la linea *connect_from_port_20=YES*
23. Agregar la linea *pasv_enable=YES*

24. *Agregar la linea min_port=4000*

25. *Agregar la linea pasv_max_port=4020*

26. Ejemplo de como se vería el un archivo vsftpd para usuarios *anonymous* o *ftp*:

[root@ctserver vsftpd]#cat /etc/vsftpd/vsftpd.conf
listen=YES
local_enable=NO
anonymous_enable=YES
write_enable=NO
anon_root=/var/ftp/pub
no_anon_password=YES
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
anon_world_readable_only=NO
anon_max_rate=2048000
xferlog_enable=YES
xferlog_file=/var/log/xferlog
listen_address=10.0.2.1
listen_port=21
connect_from_port_20=YES
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=4020

27. Guardar el archivo vsftpd.conf.

28. Iniciar el servidor con el comando:

```
[manuel@PCmanuel vsftpd]$ sudo /etc/init.d/vsftpd start
```

29. Cree un archivo de texto plano, en el directorio ***/var/ftp/pub***, que servirá para probar la descarga con el cliente ftp.

30. Antes de iniciar las pruebas, es necesario que detenga el servicios de ***iptables***, de la siguiente manera:

```
[manuel@PCmanuel vsftpd]$ sudo /etc/init.d/iptables stop
```

31. Procederemos a realizar las pruebas con el cliente ftp. En la maquina cliente iniciaremos sesión de la siguiente manera:

```
[manuel@PCmanuel vsftpd]$ ftp XXX.XXX.XXX.XXX
```

Donde "XXX.XXX.XXX.XXX" es la IP del servidor.

32. Si realizo to correctamente, deberá mostrarse un aviso de autenticación como el siguiente:

```
[manuel@PCmanuel vsftpd]$ ftp 192.168.1.3
Connected to 192.168.1.3 (192.168.1.3).
220 Bienvenidos al servidor ftp de Guandique
Name (192.168.1.3:manuel): anonymous
```

En donde le pide el nombre, deberá escribir la palabra ***"anonymous"***, y dar enter

33. Una vez dentro del servidor, utilice los comandos vistos en la clase teórica, para listar los archivos disponibles y realizar una descarga. Llame a su instructor para que vea lo realizado hasta el momento.

PROCEDIMIENTO 2: CONFIGURACIÓN DEL SERVIDOR VSFTPD BASADO EN LA SEGURIDAD DEL SISTEMA.

```
[manuel@PCmanuel ~]$ ntpdate -s <ip_del_servidor>
```

1. Ir a la carpeta ***"/etc/vsftpd".***
2. Editar el archivo ***"vsftpd.conf"***, y editelo de la siguiente manera:

[root@ctserver vsftpd]#cat /etc/vsftpd/vsftpd.conf
listen=YES
local_enable=YES
anonymous_enable=NO
write_enable=YES
local_umask=077
dirmessage_enable=YES
connect_from_port_20=YES
ftpd_banner=Bienvenidos al servidor ftp de Guandique
pam_service_name=vsftpd
userlist_enable=YES
userlist_deny=YES
tcp_wrappers=YES
xferlog_enable=YES
xferlog_file=/var/log/xferlog
listen_address=192.168.1.3
listen_port=21
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=40020

3. Una vez, editado el archivo, guárdelo y procederemos a crear un usuario, en el servidor, el cual lo usaremos para conectarnos remotamente con el usuario. El usuario que se creara, sera solo para conectarse al FTP, pero lo restringiremos para que no pueda ingresar en el sistema anfitrión, que seria en el servidor FTP. Ejecute los siguientes comandos, exactamente como aparecen en las imagenes:

```
[manuel@PCmanuel vsftpd]$ sudo useradd -s /sbin/nologin -m -d /var/ftp/usuarioftp2  usuarioftp
```

```
[manuel@PCmanuel vsftpd]$ sudo passwd usuarioftp
```

4. Por ultimo, para poder subir archivos, habrá que pasar a modo pasivo el antivirus de linux, Selinux, con el siguiente comando:

```
[manuel@PCmanuel vsftpd]$ sudo setenforce 0
```

5. Proceda a realizar las pruebas necesarias con el cliente, utilizando los comandos para conectarse ya vistos en esta guía, y para descargar y subir los vistos en la clase teórica.

NOTA: Por defecto, todos los usuarios creados en el sistema, pueden acceder al servido, la seguridad radica en que los usuarios que se quieran denegar, deben de ser añadidos al archivo ***user_list*** o ***ftpusers,*** que se encuentra en la ruta ***/etc/vsftpd.*** Una vez haya probado la descarga y subida de archivos en el servidor, incluya el usuario credo en cualquiera de los archivos antes mencionados, luego trate de iniciar nuevamente sesión con el usuario. Llame a su instructor para que vea lo realizado hasta el momento.

PROCEDIMIENTO 3: CONFIGURACIÓN DEL SERVIDOR VSFTPD CON CHROOT

Uno de las desventajas del método anterior, es que el usuario, una vez iniciada la sesión en el servidor FTP, puede cambiar de carpetas de todo el sistema, en pocas palabras, no esta restringido a trabajar solo en su carpeta de usuario, tal como pasa cuando se utiliza el modo anónimo, en el cual no puede salirse de la carpeta que se le ha asignado como carpeta raíz.

estando conectado en el servidor escriba *cd /etc* y luego *ls*. Como se puede dar cuenta todos los usuarios pueden ver más de lo que les corresponde, y eso en algunos casos no es bueno.

Una solución fácil, a este problema de seguridad es activar el “enjaulamiento” de usuarios, mediante la activación del ***chroot,*** el cual se explica a continuación.

1. Ir a la carpeta ***/etc/vsftpd***

2. Editar el archivo ***vsftpd.conf*** y agregar las siguientes lineas:

chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list

3. Crear el archivo ***/etc/vsftpd/chroot_list***, dejarlo en blanco
4. Realizar la prueba del ftp desde el cliente, y tratar de listar el contenido del directorio ***/etc***.
5. Para evitar que un usuario sea enjaulado, colocar el nombre de usuario en el archivo ***chroot_list.***
6. Llame a su instructor para que observe lo realizado hasta el momento

PROCEDIMIENTO 4: CONFIGURAR EL SERVIDOR TFTP

1. Verificar que se encuentra instalado el paquete xinetd

```
[manuel@PCmanuel vsftpd]$ rpm -q xinetd
```

   De no encontrarse instalado el archivo, proceda a su instalación, mediante el comando ***yum.***

2. Realice lo mismo con el paquete ***tftp-server***, priemro verifique si se encuentra instalado, y de no ser así, proceda a su instalación.
3. Diríjase a la carpeta ***/etc/xinetd.d***, proceda ha abrir el archivo ***tftp*** para su modificación.
4. Identificar la línea ***disabled=no***, si no está así, modificarla.
5. Identificar la línea ***server_args = -c -s /tftpboot***, si no está así, modificarla.
6. El archivo ***tftp*** deberá quedar de la siguiente forma:

```
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -c -s /tftpboot
        disable                 = no
        per_source              = 11
        cps                     = 100  2
        flasgs                  = Ipv4
}
```

7. Cree la carpeta ***/tftpboot***
8. Cambie los permisos y el dueño a la carpeta creada, así:

```
[manuel@PCmanuel vsftpd]$ sudo chown nobody /tftpboot/
```

```
[manuel@PCmanuel vsftpd]$ sudo chmod 777 /tftpboot/
```

9. Guarde el archivo e inicie, reinicie el servidor.

```
[manuel@PCmanuel vsftpd]$ sudo /etc/init.d/xinetd start
```

10. Verifique si se encuentra instalado en el cliente, el paquete tftp, de no estar instalado proceda a su instalación.
11. Repita los pasos 7 y 8, pero ahora en el cliente.
12. En el cliente, cree un archivo llamado ***prueba.txt*** dentro de la carpeta /tftpboot:

```
[manuel@PCmanuel vsftpd]$ touch /tftpboot/prueba.txt
```

13. Ejecutar los siguientes comandos en el cliente, para probar el fucnionamiento del servidor ***tftp.***

```
[manuel@PCmanuel vsftpd]$ tftp 192.168.1.3
```

Donde "***192.168.1.3***" deberá reemplazarlo por la ip del servidor ***tftp.***

```
tftp> put prueba.txt
```

```
tftp> quit
```

14. Verificar que el archivo fue transferido a la carpeta /tftpboot del servidor. Llame a su instructor para que observe lo realizado hasta el momento,

PROCEDIMIENTO 5: DES-INSTALAR LOS SERVICIOS Y RESTAURAR LOS ARCHIVOS DE CONFIGURACIÓN

1. Removeremos el paquete vsftpd, tftp-server, tftp y xinetd por medio del comando ***yum.***

```
[manuel@PCmanuel vsftpd]$ sudo yum erase -y vsftpd tftp-server tftp xinetd
```

2. Llame a su instructor para que se cerciore que ha des-instalado los paquetes.

V. INVESTIGACIÓN COMPLEMENTARIA.

Redacte un documento explicando lo siguiente:

- Como configurar VSFTPD con una conexión segura por medio de SSH.
- Como realizar una conexión de tipo FTP por medio de una pagina web, dicho de otra forma, como integrar FTP con HTTP.

Para todos los puntos anteriores deberán ir reflejados con ejemplos, **echos por ud. en su maquina.**