Ejercicio 1 - Proftpd en máquina virtual

Requisitos previos

En primer lugar vamos a configurar una máquina virtual con Ubuntu 16.04 y vamos a instalar las siguientes aplicaciones:

1. Servidor Web: Apache2
2. Servidor FTP: proftpd

En nuestro PC necesitamos instalar un cliente FTP:

1. Cliente gráfico Filezilla

Supongamos que tenemos una máquina virtual (con VirtualBox) con el sistema operativo Ubuntu 16.04, con las siguientes características:

- Usuario "**usuario**", passwd "**usuario1**"
- Configuramos la red dentro de Virtualbox como adaptador puente, de forma que la MV y nuestro PC se encuentren dentro de la misma red.

Procedemos a instalar los dos servidores en la MV.

- Actualizamos los repositorios
- **Instalamos apache2**: sudo apt-get install apache2
- comprobamos que funciona correctamente accediendo a través del navegador web. Verificamos la IP y accedemos a través de ella en nuestro navegador del PC
- Instalamos **proftpd:** sudo apt-get install proftpd
- Miramos los puertos abiertos (80, 21, en la MV).

Para el ejercicio realizaremos los siguientes apartados:

1. Acceso con usuario local de MV "usuario" desde nuestro PC
    a. Enjaular al usuario para que no pueda acceder a todo el equipo
2. Acceso anónimo al servidor FTP desde nuestro PC
    a. Cambiar alias para acceder como anónimo con otros nombres
3. Creación de tres usuarios virtuales, y configuración de acceso

1. Acceso al servidor FTP con un usuario del sistema

Abrir el cliente de FIlezilla en el PC y realiza los siguientes apartados:

- Acceder al servidor FTP de la MV con "usuario" y password "usuario1"
- Comprueba que el directorio remoto, es el directorio personal del usuario /home/usuario
- Crear alguna carpeta, archivos, borrar, descargarse al PC alguna carpeta o archivos.
- Trata de navegar a algún directorio del sistema.

A continuación vamos a cambiar algunas directivas del servidor FTP para evitar que los usuarios puedan navegar fuera de su directorio.

- Editamos **/etc/proftpd/proftpd.conf**
- Descomentamos **DefaultRoot ~** para poder enjaular a los usuarios.
- Reiniciamos el servidor FTP
- Comprobamos que "usuario" no puede navegar fuera de su directorio.

Personalización del mensaje de bienvenida y mensaje de directorios.

- Crear un archivo **welcome.msg** en el directorio raíz del usuario del sistema y comprueba que se muestra al conectarse con dicho usuario.
- Crea un archivo oculto **.message** en uno de los directorios del usuario, comprueba que se visualiza dicho mensaje cuando accedes a través de un terminal con dicho usuario y el directorio donde se encuentra el archivo .message

2. Acceso al servidor FTP con un usuario anónimo

En la instalación del servidor FTP, se crearon dos usuarios:.
Se añadió un usuario de sistema, sin contraseña, con nombre **proftpd**
— No se creó un directorio personal para el usuario proftpd, (apunta al directorio /svr/proftpd perteneciente a root)
— Se añadió un usuario de sistema, sin contraseña, con nombre **ftp**
— Se creó el directorio personal /srv/ftp para el usuario ftp con permisos drwxr-xr-x o lo que es lo mismo 755 el usuario ftp tendría permisos de lectura, escritura y ejecución, los miembros de su grupo sólo tendrían permisos de lectura y ejecución y el resto de los usuarios solo se les permitiría la ejecución.El segundo es usado para la autenticación anónima y el primero es el usuario que ejecuta el proceso del servidor.

Vamos a cambiar algunas directivas del servidor FTP para que puedan acceder usuarios anónimos:

- Editamos **/etc/proftpd/proftpd.conf**
- descomentamos todo lo que aparece entre **<Anonymous ~ftp>** y ….. **</Anonymous>**
- Reiniciamos el servidor
- Accedemos desde nuestro PC con el cliente FTP al servidor con el usuario ftp (sin password, o incluyendo uno genérico) o con el usuario anonymous.
- Puedes probar a cambiar la directiva correspondiente para poder acceder con otro nombre de usuario como anónimo.

3. Acceso al servidor FTP con un usuarios virtuales

Veamos ahora la forma de crear nuevos grupos y usuarios virtuales que utilizaremos más adelante para acceder al servidor ProftpD autentificándonos por medio del nombre de usuario y su contraseña.

Al instalar proftdp se incluye una herramienta llamada **ftpasswd** que, por medio de un script de Perl, permite crear e incluir datos en dos ficheros llamados **ftpd.group** y **ftpd.passwd** que contendrán la información relativa a los grupos y usuarios autentificados susceptibles de ser usados para la gestión del servidor FTP y que se incluirán en el directorio **/etc/proftpd/**.

Creación de grupos de usuarios virtuales

Empezaremos creando dos grupos de usuarios (podríamos crear cuantos quisiéramos). Para ello utilizaremos los comandos de consola siguientes:

- cd /etc/proftpd
- sudo **ftpasswd --group --name=webmaster --gid=1010** (ojo, debes verificar los id de los usuarios y grupos del sistema para no pisarlos (sudo cat /etc/shadow)
- sudo **ftpasswd --group --name=gestion --gid=1011**

Comprobaremos que se ha creado el archivo /etc/proftpd/ftpd.group

Creación de usuarios virtuales

Una vez creados los grupos vamos a crear tres usuarios:

- **webmaster** que tendrá como password *webmaster1* y pertenecerá al grupo webmaster cuyo gid

es 1010. A este usuario le asignaremos como directorio raiz /var/www y dado que va a requerir un número uid utilizaremos, por seguir un cierto orden, 1012 que es el correlativo al último utilizado

- **secre** que tendrá como password *secre1* y pertenecerá al grupo gestion cuyo gid es 1011. A este usuario le asignaremos como directorio raiz /home/servidorftp y dado que va a requerir un número uid utilizaremos, por seguir un cierto orden, 1013 que es el correlativo al último utilizado
- **super** que tendrá como password *super1* y pertenecerá también al grupo gestion cuyo gid es 1011. A este usuario le asignaremos el mismo directorio raiz que a secre /home/servidorftp y uid 1014.

Los comandos serán los siguientes:

- **sudo ftpasswd --passwd --name=webmaster --uid=1012 --gid=1010 --home=/var/www --shell=/bin/false**
- sudo ftpasswd --passwd --name=secre --uid=1013 --gid=1011 --home=/home/servidorftp --shell=/bin/false
- sudo ftpasswd --passwd --name=super --uid=1014 --gid=1011 --home=/home/servidorftp --shell=/bin/false

(ftpasswd --passwd --name=*user* --change-password para cambiar un password)

- Cambiamos los permisos al directorio /var/www con 777

El caso del directorio /home/servidorftp –asignado como raíz para los usuarios secre y super– no existe aún. Hemos de crearlo y aprovecharemos para hacerlo otorgándole los máximos permisos posibles (777). Podemos hacerlo por medio del siguiente comando de consola:

- sudo mkdir /home/servidorftp -m 777

Adelantándonos un poco a opciones que comentaremos más adelante, crearemos tres subdirectorios en /home/servidorftp y les asignaremos los nombres: Gestion, Alumnos y Documentacion. En lo que respecta a los permisos les atribuiremos también permisos 777. Podemos hacerlo con estos comandos:

- sudo mkdir /home/servidorftp/Gestion -m 777
- sudo mkdir /home/servidorftp/Alumnos -m 777
- sudo mkdir /home/servidorftp/Documentacion -m 777

Configuración del archivo proftpd.conf para permitir usuarios virtuales

Ahora vamos a configurar el servidor FTP para permitir los accesos a estos usuarios virtuales.
Editamos **/etc/proftpd/proftpd.conf**:
Añadimos:

- AuthUserFile "/etc/proftpd/ftpd.passwd"
- AuthGroupFile "/etc/proftpd/ftpd.group"
- AuthOrder mod_auth_unix.c mod_auth_file.c

Cambiamos:

- UseIPv6 off

Cambiaremos el nombre de nuestro servidor:

- ServerName

Para usar los usuarios virtuales descomentaremos para que no sea necesario un shell

- RequireValidShell off

Comprobación de acceso con usuarios virtuales

Probemos con los usuarios webmaster, secre o super y comprobemos que:

- No nos está permitido el acceso sin contraseña. Recuerda que la contraseña la hemos incluido al crear los usuarios

- No nos está permitido «Subir al directorio superior» con lo cual las posibilidades de que el usuario se mueva por todo el árbol de directorio plantea un problema de seguridad. Ya cambiamos la directiva anteriormente.

4. Configuración del servidor FTP, para restringir el acceso y permisos.

Estableciendo límites a usuarios y directorios

En el fichero de configuración de ProftpD (**/etc/prpftpd/proftpd.conf**) es posible establecer una muy amplia gama de limitaciones de acceso tanto para usuarios concretos como para directorios específicos. Se trata de las especificaciones contenidas entre las etiquetas <LIMIT> y </LIMIT> que han de incluir las instrucciones para permitir (ALLOW) o denegar (DENY) algo a alguien. En este aspecto es muy importante el orden en se apliquen esos filtros. Caben dos posibilidades de ordenación:

- Order Allow, Deny (valor por defecto)
    - Primero se evalúa lo que esté en Allow y se permite su acceso.
    - Si no cumple Allow se evalúa Deny y se deniega el acceso explicitamente
    - Los que no cumplan ninguna de los dos por defecto se permite el acceso.
- Order Deny, Allow
    - Primero se evalúa lo que está en Deny y se deniega su acceso
    - Si no lo cumple se evalúa Allow y explícitamente se permite su acceso
    - Si no cumple ambas se deniega el acceso.

Limitando los usuarios autorizados
Las condiciones restrictivas de usuarios deben incluirse entre las etiquetas <LIMIT LOGIN> y </LIMIT>
Dentro de ese bloque puede incluirse líneas de instrucciones con esta sintaxis:

- **Order Allow,Deny** o **Order Deny,Allow**
  Establece los criterios de evaluación según lo comentado en el epígrafe anterior. De no incluirse se comportará de acuerdo con sus condiciones por defecto: Order allow,deny
- **AllowUser** nombre_del_usuario o **AllowGroup** nombre_del_grupo o **AllowAll**
  Permite incluir nombres de usuarios autorizados, nombres de grupos de usuarios, o la forma más amplia de permisividad (AllowAll) que permitiría el acceso a todos los usuarios y grupos. Cuando se trate de más de un usuario o grupo en la documentación de ProftpD se recomienda utilizar siempre una línea para cada usuario.
- **DenyUser** nombre_del_usuario o **DenyGroup** nombre_del_grupo o **DenyAll**
  Se comporta de la misma forma que la directiva anterior con la lógica diferencia de que en este caso estaríamos refiriéndonos a usuarios o grupos cuyo acceso pretendemos impedir.

❏ Realizamos una primera prueba para permitir únicamente en el sistema el usuario webmaster. Editamos el fichero **proftpd.conf**:

```
<Limit LOGIN>
        Order Allow,Deny
        AllowUser webmaster
        DenyAll
</Limit>
```

❏ Editamos el fichero **proftpd.conf** para indicar que los únicos usuarios que tienen acceso al FTP son: ftp, los usuarios del grupo de gestión y webmaster. El resto no tienen acceso. Para ello incluimos en el fichero:

```
<Limit LOGIN>
        Order Allow,Deny
        AllowGroup gestion
        AllowUser webmaster
        AllowUser ftp
        DenyAll
</Limit>
```

- ❏ Cómo denegaríamos el permiso de LOGIN a todos los usuarios salvo al usuario anónimo (aunque se creen otros a posteriori)

```
<Limit LOGIN>
        AllowUser ftp
        DenyAll
</Limit>
<Limit LOGIN>
        Order Deny, Allow
        AllowUser ftp
</Limit>
```

- ❏ Cómo permitimos acceso a todos los usuarios salvo a secre

```
<Limit LOGIN>
        Order Deny, Allow
        DenyUser secre
        AllowAll
</Limit>
<Limit LOGIN>
        Order Allow, Deny
        DenyUser secre
</Limit>
```

- ❏ permitir acceder a todos los usuarios del grupo gestión salvo a secre

```
<Limit LOGIN>
        Order Deny, Allow
        AllowGroup gestion
        DenyUser secre
</Limit>
```

Permisos y restricciones en directorios no anónimos

La configuración de los servidores FTP suele permitir dos tipos de acceso: anónimos o no anónimos requiriéndose únicamente el nombre de usuario en el primer caso y siendo necesarios en el segundo supuesto el nombre de usuario y su contraseña. Vamos a empezar analizando el segundo tipo —no anónimos— y viendo la forma en la que pueden particularizarse las condiciones de acceso a directorios y subdirectorios estableciendo los usuarios a los que se permitirá el acceso y determinando también qué acciones están permitidas a cada uno de esos usuarios.
Empezaremos detallando las palabras reservadas asociadas a las diferentes acciones que serán utilizadas para establecer cuáles de ellas autorizaremos o denegaremos a cada usuario o grupo de usuarios.

Clave	Descripción de la acción asociada a la palabra clave
READ	Equivale a enumerar cada uno de los comandos FTP que se ocupan de la lectura de archivos (lista de directorios no incluidas)que son: **RETR**, **SITE**, **SIZE** y **STAT**
RETR	Transferir (descargar) un archivo desde el servidor al cliente.
SITE	Envía comandos específicos al servidor remoto
SIZE	Devuelve el tamaño de un archivo del servidor
STAT	Devuelve el estado (status) actual de servidor
WRITE	Equivale a enumerar todos los comandos FTP que se ocupan de la escritura y que son: **APPE**, **DELE**, **MKD**, **RMD**, **RNTO**, **STOR**, **XMKD**, **XRMD**
APPE	Añade o crea un fichero
DELE	Borra un fichero en el servidor
MKD XMKD	Crea un directorio en el servidor
RMD XRMD	Borrar un directorio en el servidor
STOR	Transferir (subir))un archivo desde el cliente al servidor
DIRS	Equivale a enumerar uno a uno los comandos FTP que se ocupan del listado de directorios y que son: **CDUP**, **XCDUP**, **CWD**, **XCWD**, **LIST**, **MDTM**, **NLST**, **PWD**, **XPWD**, **RNFR**
CDUP XCDUP	Cambiar el directorio de trabajo al directorio raíz
CWD XCWD	Cambiar el directorio de trabajo en el servidor
LIST	Si se especifica un directorio o archivo devuelve información sobre él. De lo contrario devuelve una lista del directorio de trabajo
MDTM	Devuelve la fecha de la última modificación de un fichero o directorio
NLST	Devuelve una lista de nombres de ficheros contenidos en un directorio específico
PWD XPWD	Muestra el directorio activo en el servidor.
RNFR	Enviado por el cliente formando un par junto RNTO permite renombrar un directorio o fichero en el servidor.

Veamos la forma de establecer las condiciones de acceso de usuarios no anónimos a un directorio concreto. Podría ser algo similar a esto:

<Limit LOGIN>
AllowUser usuarios_a los que se autorizan el acceso al directorio
DenyUser usuarios a quienes se deniegan el acceso al directorio
</Limit>
<Directory ruta_absoluta_del_directorio >
AllowOverwrite off
<Limit acciones_permitidas>
AllowUser usuarios_a los que se autorizan las acciones permitidos
DenyUser usuarios a quienes se deniegan la ejecución de las acciones permitidos
</Limit>
</Directory>

Por ejemplo: Veamos cómo establecer condiciones para la situación siguiente. Va a tratarse del directorio **/home/servidorftp** al que vamos a establecer las siguientes restricciones:

- Solo tendrán acceso los usuarios del grupo de **gestion** (secre y super)
- El usuario **super** tendrá libertad total de ejecución de comandos FTP tanto el directorio servidorftp como en todos sus subdirectorios
- El usuario **secre** solo podrá ver el contenido del directorio servidorftp. No podrá hacer nada en el directorio Alumnos, tendrá libertad total en el directorio Gestion y tendrá únicamente permisos de lectura (READ) dentro del subdirectorio Documentacion

```
#No se puede meter el login dentro de un directorio
<Limit LOGIN>
        AllowGroup gestion
        DenyAll
</Limit>
<Directory /home/servidorftp>
    <Limit DIRS READ>
        AllowGroup gestion
        DenyAll
    </Limit>
    <Limit ALL>
        AllowUser super
        DenyAll
    </Limit>
</Directory>
```

Ejercicio propuesto:
Poner el directorio por defecto para el usuario webmaster en /opt y para el grupo de gestion en /home/profesor
DefaultRoot /opt webmaster, ftp
DefaultRoot /home/profesor gestion