Práctica 7 – Servicio FTP

Se trata de que implementes un servicio FTP en Linux. Esta es la séptima práctica. Obligatoria.

Contenido práctica:

NOTA: El servidor de ficheros ProFTPD soporta diferentes tipos de usuarios a la hora de acceder al servidor. Los diferentes tipos de usuarios que soporta ProFTPD son los siguientes:

- Usuario de sistema: Son los usuarios propios del sistema operativo. Cuando se accede al servidor FTP con una cuenta de usuario, normalmente se accede a la carpeta $HOME del usuario.
- Usuario anónimo: El usuario anonymous, es un usuario que suele estar presente en muchos servidores FTP donde queremos tener un acceso público para las descargas de ficheros. Este usuario únicamente suele tener permiso de lectura y su password suele ser cualquier cadena de texto.
- Usuario virtual: Son usuarios independientes de los usuarios de sistema. Realmente no existen como usuarios normales del sistema operativo.

A) En el Servidor-1. Preliminares:
   a. Instala un servicio FTP mediante el paquete proftpd.
      i. Comprueba que no lo tienes instalado mediante sudo dpkg -L proftpd (si lo tienes instalado demuestra que lo tienes)
      ii. sudo apt-get install proftpd
      iii. Para, reinicia y verifica el status del servicio con systemctl stop/restart/status proftpd
      iv. Verifica que el puerto 21 está abierto con nmap

   b. Verifica que, tras instalar el paquete, se han generado dos nuevos usuarios: **proftpd** y **ftp**.
      i. El usuario **proftpd** es un usuario que utilizará el servicio ftp y el usuario **ftp** va permitir realizar conexiones anónimas por

protocolo ftp pero no son usuarios para ejecutar comandos por shell en el sistema. Demuestra esto último (indaga en /etc/passwd)

ii. Demuestra que el directorio asociado al usuario ftp es /srv/ftp
iii. Verifica que dentro de /srv/ftp está welcome.msg
iv. Verifica que el directorio /srv/ftp pertenece al usuario ftp y grupo nogroup (ls -al)
v. Crea fichero1.txt en /srv/ftp

B) Autenticación no anónima desde cliente ftp a protftpd:
   a. Desde el cliente Ubuntu conéctate por la terminal al servidor ftp del Ubuntu Server mediante la entrada DNS ftp.<nombreapellidos>.local
      i. Auténticate con un usuario y password (administrador, por ejemplo) del servidor.
      ii. Verifica con pwd que ves el directorio del lado servidor
      iii. Verifica con !pwd que ves el directorio local del cliente
   b. Instala Filezilla en el cliente Ubuntu desde la terminal:
      i. sudo apt install filezilla
      ii. Conéctate con Filezilla al servicio ftp con el mismo usuario y contraseña de B) a.i generando un Sitio nuevo.
      iii. Verifica que en el panel derecho, sitio remoto, puedes navegar sin control por directorios superiores, con lo que ello conlleva de fallo de seguridad, una vez te has conectado.
   c. Acude a /etc/proftpd en lado servidor:
      i. Edita proftpd.conf
         1. Deshabilita Ipv6
         2. Cambia el nombre del servidor por “Servidor FTP de <nombreapellidos>.local”
         3. Cambia el archivo de bienvenida por otro y dótale de contenido donde proceda. Visualízalo mediante conexión FTP por terminal (Filezilla no lo muestra).
         4. Guarda la configuración y reinicia el servicio con restart.
         5. Comprueba que las dos conexiones cliente ftp se han quedado desconectadas, bien por terminal, bien por filezilla.
         6. Verifica que 5 no sucede si utilizas reload en vez de restart

ii. El comando proftpd -t indica si la sintaxis del archivo de configuración es correcta

d. Verifica también desde el cliente ftp terminal que, al igual que en Filezilla, el usuario puede navegar por encima del directorio del usuario autenticado, con lo que ello supone de riesgo de seguridad.
   i. Modifica ese comportamiento desconmentando la línea adecuada en proftpd.conf (investiga cuál debe ser, basta que leas los comentarios, referido a “enjaulamiento” en inglés.)
   ii. Demuestra que las conexiones ftp ya quedan encapsuladas/enjauladas en el directorio del usuario autenticado y no pueden navegar por encima.

C) Autenticación anónima:

a. Para poder acceder de forma anónima, analiza qué directivas debes habilitar en proftp.conf. No elimines los comentarios ni habilites más de lo necesario.
   i. Observa que el usuario anónimo se referencia al usuario ftp del grupo nogroup.
   ii. El usuario ftp queda encapsulado en /srv/ftp. Verifícalo accediendo con los clientes de consola y filezilla y verificando que no pueden salir de dicho directorio. (usuario **anonymous ó ftp y password vacío).**
   iii. Agrega la directiva "AnonRequirePassword on" debajo de la directiva UserAlias y verifica que ahora al usuario anónimo se le solicita password. Ese password habría que aplicarlo en el archivo passwd para el usuario ftp (verifica en shadow que en efecto el usuario ftp no tiene password asociado). No le asignes password en la práctica, sólo juega con “AnonRequirePassword on” y con “AnonRequirePassword off”

b. Verifica con ftpwho en el servidor los clientes conectados que hay en cada momento y con qué usuario (con filezilla auténtica sin ser anónimo y con la consola anónimamente).

c. Para monitorizar el servicio ftp utiliza tail -f /var/log/proftpd/*
   i. Deja abierta la monitorización
   ii. Ejecuta acciones desde los clientes ftp y observa el registro de dichas acciones

d. En la directiva del usuario anónimo tenemos un DENYALL para escritura. Verifica que es así intentando subir un archivo al servidor desde el cliente ftp.
e. Si comentas toda la directiva que engloba a DENYALL verifica que ahora sí puedes subir archivos y descargarlos. Vuelve a dejarlo descomentado tras verificarlo.

D) En el archivo de configuración descomenta la parte “brava”. Hacerlo implica que, para el usuario anónimo, se puede permitir subir archivos (STORE) para el directorio incoming aunque no se va poder leer ni escribir pero sí almacenar archivos.
   a. En lado servidor crear en /srv/ftp el directorio incoming
   b. chown -R ftp:nogroup incoming/ -> haremos que pase a ser parte del usuario ftp
   c. Verifica que puedes usar el comando PUT con un archivo desde el cliente ftp y la operación termina con éxito. Para ello, desde lado cliente, debes estar posicionado dentro de incoming (con pwd aparecerá /incoming tras ejecutar cd incoming)
   d. Verifica que no puedes eliminar el archivo desde el cliente FTP. Después, modifica la directiva para que puedas eliminar un archivo.
   e. Si intentas subir un archivo encima del directorio incoming, en la raíz del usuario ftp ¿qué sucede?
E) Comprueba que mediante un sniffer podemos ver el usuario y contraseña del servicio ftp como datos planos:
   a. Ejecuta en lado servidor tcpdump -A port ftp
   b. Desde el cliente ftp autenticarse con usuario y contraseña y observar cómo en los paquetes se ve como texto plano el usuario y contraseña.

F) Hemos visto hasta ahora que hay usuarios del sistema y usuarios anónimos. Los primeros coinciden con un usuario del sistema operativo y los segundos con un usuario. Creemos usuarios virtuales.
   a. Asegúrate tener configurados estos parámetros

```
Include /etc/proftpd/modules.conf
DefaultRoot ~
RequireValidShell off
AuthUserFile /etc/proftpd/ftpd.passwd
```

b. Creamos el directorio personal para el usuario virtual:
    i. mkdir /srv/alumnoftp
c. Modificamos permisos:
    i. chown ftp.nogroup /srv/alumnoftp
    ii. chmod 777 /srv/alumnoftp
d. Creamos el fichero de usuarios vacío para almacenar ahí los usuarios virtuales:
    i. touch /etc/proftpd/ftpd.passwd
e. Ahora si, crearemos el usuario virtual. Deberemos seleccionar un uid y gid que no exista en el sistema. Se pueden ver los que ya están siendo usados se pueden ver en el fichero /etc/passwd. Se ha seleccionado un valor alto (3000) para evitar que coincidan con posibles usuarios del sistema. También hay que indicarle el $HOME del usuario y que la shell a utilizar sea /bin/false:
    i. ftpasswd --passwd --name=alumnoftp --uid=3000 --gid=3000 --home=/srv/alumnoftp --shell=/bin/false
f. Acude al terminal y con filezilla y verifica que puedes acceder con el usuario alumnoftp y contraseña la que hayas indicado.

G) NOTA: Vamos a instalar un sistema de cuotas para el servicio FTP. Esto es importante para controlar el espacio, además de verificar los permisos de lectura y escritura, para los usuarios que provengan del exterior. En caso contrario, podemos estar generando un riesgo de amenaza desde el exterior y convertirse en riesgo real, como entrar en un directorio que no sea el dedicado para FTP o como que se caiga el sistema por falta de espacio.

Existen dos tipos básicos de las cuotas de disco.

- La primera, conocida como cuota de uso o cuota de bloques, limita la cantidad de espacio en disco que puede ser utilizado.
- La segunda, conocida como cuota de archivo o de inodo, limita el número de archivos y directorios que se pueden crear.

Además, los administradores suelen definir un nivel de advertencia, o cuota blanda, en la que se informa al usuario que se están acercando a su límite, que es menor que el límite efectivo, o cuota dura. También puede haber un intervalo de gracia pequeño, lo que permite a los usuarios violar temporalmente sus cuotas en ciertas cantidades, si es necesario. Cuando una cuota blanda es sobrepasada, el sistema envía normalmente al usuario (y en ocasiones al administrador también) algún tipo de mensaje.

Para **activar e**l uso de las cuotas en ProFTPD, es necesario añadir las líneas siguientes, donde le indicamos que arranque el motor de cuotas y en qué ficheros estarán definidas las configuraciones de las cuotas. También es útil indicarle un fichero de log donde podemos ver si todo funciona correctamente ó si por el contrario, existe algún error.

a. Configura:

```
<IfModule mod_quotatab.c>
QuotaEngine on
QuotaLog /var/log/proftpd/quota.log
<IfModule mod_quotatab_file.c>
     QuotaLimitTable file:/etc/proftpd/ftpquota.limittab
     QuotaTallyTable file:/etc/proftpd/ftpquota.tallytab
</IfModule>
</IfModule>
```

El siguiente paso es crear las cuotas. Las cuotas de tipo **Limit** sirven para fijar unos máximos, bien de descarga de contenido, subida de contenido, ratios etc... y las cuotas de tipo **Tally** nos permiten llevar la cuenta de la cantidad de ficheros subidos o descargados hasta ese momento.

b. El primer paso es crear los ficheros (tablas) donde se guardarán las cuotas, tanto la **Limit** como la Tally. Para ello ejecutaremos los siguientes comandos:

ftpquota --create-table --type=limit --table-path=/etc/proftpd/ftpquota.limittab

ftpquota --create-table --type=tally --table-path=/etc/proftpd/ftpquota.tallytab

Cuotas para el usuario alumnoftp:

- Límite Subida: 200MB
- Límite Descarga: 400MB
- Límite Nº Total ficheros Subidos: 15
- Límite Nº Total ficheros Descargados: 50

c. Comando LIMIT:

ftpquota --add-record --type=limit --name=alumnoftp --quota-type=user --bytes-upload=200 --bytes-download=400 --units=Mb --files-upload=15 --files-download=50 --table-path=/etc/proftpd/ftpquota.limittab

d. Comando TALLY:

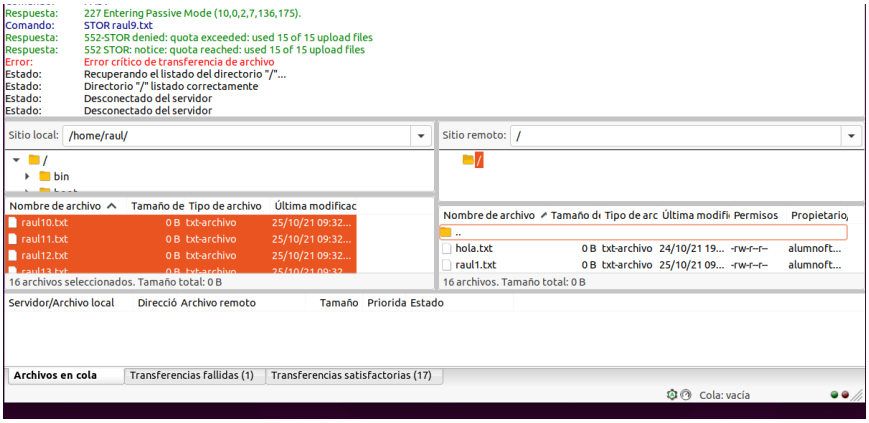
ftpquota --add-record --type=tally --name=alumnoftp --quota-type=user

e. Verificación de cuotas:

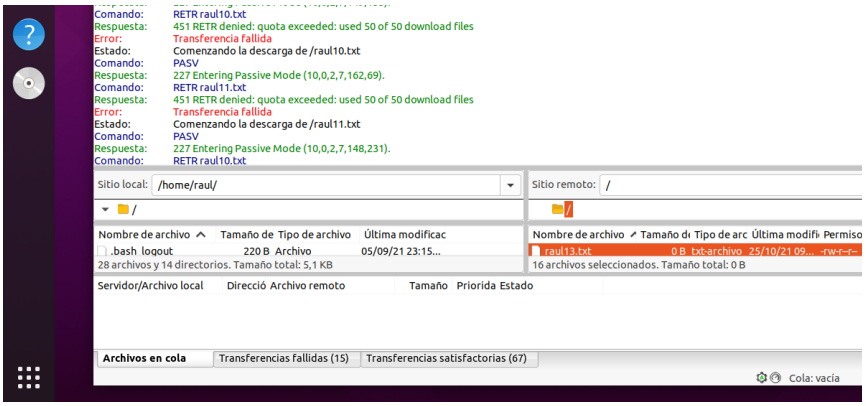
ftpquota --show-records --type=limit

ftpquota --show-records --type=tally

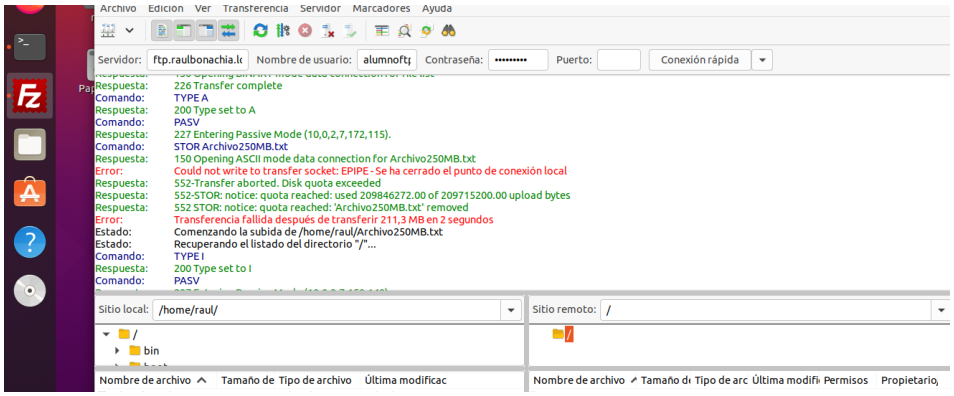
f. Verifica que los límites son correctos. Sube más de 15 archivos y descarga más de 50 archivos, y verifica que reciben mensajes similares a estos:



g.



h. Actualiza los límites para poder subir más archivos y poder comprobar que no puedes subir un archivo de más de 200 MB desde el cliente.



COMANDO ACTUALIZACIÓN:

ftpquota --update-record --type=tally --name=raul_quota --quota-type=user --files-uploads=100 --files-download=150 --table-path=/etc/proftpd/ftpquota.limittab

COMANDO PARA GENERAR UN ARCHIVO PESADO EN EL CLIENTE:

dd if=/dev/zero of=Archivo1MB.txt bs=1024 count=1024. → GENERA UN ARCHIVO DE 1MB. PARA GENERAR UN ARCHIVO DE 260 MB EN count asignar el resultado de 1024*260

i. Verifica también el límite de la descarga. Repite de forma análoga el proceso de h, pero desde lado servidor.

H) Nos marcamos como objetivo que un usuario dado de alta en el directorio LDAP pueda ser autenticado vía FTP mediante Proftpd. Para ello sigue los siguientes pasos:
   a. Instala en el servidor el paquete proftpd-mod-ldap
   b. En proftpd.conf:
      i. Descomenta si lo está la línea include /etc/proftpd/ldap.conf (se activa la conexión con LDAP).
      ii. Descomenta la directiva RequireValidShell off (permite entrar el usuario sin Shell válida).
   c. En el fichero modules.conf descomenta esta línea:
      i. LoadModule mod_lap.c (carga el módulo LDAP en el servicio FTP).
   d. En ldap.conf tendrás que activar una configuración similar a la siguiente:

```
#
LDAPLog /var/log/proftpd/ldap.log
LDAPAuthBinds on
LDAPServer ldap://10.0.2.7:389/??sub
LDAPBindDN "cn=admin,dc=raulbonachia,dc=local" "admin"
LDAPUsers "ou=usuarios,dc=raulbonachia,dc=local" "(&(uid=%v) (objectclass=*))"

LDAPGenerateHomedir on
LDAPGenerateHomedirPrefix /home
#
```

El significado de cada directiva viene reflejado en la siguiente tabla:

- *LDAPServer:* especifica el nombre o IP del servidor.
- *LDAPBindDN:* configura la entrada absoluta al servicio de directorio.
- *LDAPUsers:* detalla la unidad organizativa en la que se va a buscar el usuario dentro del directorio activo.

e. Ahora crearemos un usuario llamado **javier** de password **Javier** en el servicio de directorio LDAP, para la unidad organizativa usuarios, y le indicaremos estos parámetros:
   i. homeDirectory: /srv/ftp/Javier
   ii. userPassword: javier
   iii. loginShell: /bin/false

f. Verifica mediante slapcat que está bien dado de alta y configurado.

g. Crearemos el directorio del usuario ldap, teniendo en cuenta que debe pertenecer al usuario ftp y al grupo nogroup, con permisos 775
   i. mkdir –p /srv/ftp/javier
   ii. chgrp nogroup /srv/ftp/javier
   iii. chown ftp /srv/ftp/javier
   iv. chmod 775 /srv/ftp/Javier

h. Reinicia el servicio proftpd
i. Lanza el cliente ftp para el usuario **javier**, por terminal y por Filezilla y verifica:
   i. La conectividad se realiza en efecto en ambas opciones. Por ejemplo, en terminal: (hazlo ídem con Fileziila).

```
root@osboxes:/etc/proftpd# service proftpd restart
root@osboxes:/etc/proftpd# ftp 10.0.2.15
Connected to 10.0.2.15.
220 ProFTPD Server (Servidor FTP) [::ffff:10.0.2.15]
Name (10.0.2.15:root): javier
331 ContraseÃ±a necesaria para javier
Password:
230 Usuario javier conectado
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

   ii. Se genera la autenticación LDAP en el archivo log definido en ldap.conf

```
2020-03-31 14:52:22,278 mod_ldap/2.9.4[3148]: attempting connection to URL ldap://10.0.2.15:389/??sub
2020-03-31 14:52:22,278 mod_ldap/2.9.4[3148]: set LDAP protocol version to 3
2020-03-31 14:52:22,278 mod_ldap/2.9.4[3148]: connected to URL ldap://10.0.2.15:389/??sub
2020-03-31 14:52:22,278 mod_ldap/2.9.4[3148]: set dereferencing to 0
2020-03-31 14:52:22,278 mod_ldap/2.9.4[3148]: set query timeout to 5 secs
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: generated filter ou=usuarios,dc=cursolinux,dc=com from
template ou=usuarios,dc=cursolinux,dc=com and value javier
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: generated filter (&(uid=javier) (objectclass=*)) from
template (&(uid=%v) (objectclass=*)) and value javier
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: searched under base DN ou=usuarios,dc=cursolinux,dc=com
using filter (&(uid=javier) (objectclass=*))
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: fetching values for attribute uid
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: fetching values for attribute uidNumber
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: fetching values for attribute gidNumber
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: fetching values for attribute homeDirectory
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: fetching values for attribute loginShell
2020-03-31 14:52:22,279 mod_ldap/2.9.4[3148]: found user javier, UID 2020, GID 2020, homedir /srv/ftp/
javier, shell /bin/false
```