Configuración do servidor de transferencia de ficheiros

Índice

1. Modificación dos permisos de usuarios autenticados e anónimos en vsftpd

Configurar vsftpd para dotar de diferentes permisos de lectura/escritura aos usuarios autenticados e anónimos. Modificar a configuración do servidor vsftpd para dotar aos usuarios dos seguintes permisos:

- Só poden acceder os usuarios do sistema con permisos de lectura.
- Só poden acceder os usuarios do sistema con permisos de lectura e escritura.
- Poden acceder os usuarios do sistema con permisos de lectura e escritura e os usuarios anónimos (ao cartafol `/ftp-anon`) con permiso de só lectura.
- Poden acceder os usuarios do sistema e os usuarios anónimos (ao cartafol `/ftp-anon`) con permisos de lectura e escritura.

Pasos a seguir

Modificar a configuración do servidor vsftpd para dotar aos usuarios dos seguintes permisos:

Despois de cada cambio reiniciar o servidor: sudo service vsftpd restart

- Só poden acceder os usuarios do sistema con permisos de lectura.

  Esta é a configuración por defecto do servidor vsftpd, para o que teñen que estar no arquivo de configuración (`/etc/vsftpd.conf`) estas liñas:

```
anonymous_enable=NO
local_enable=YES
```

  E a directiva `write_enable` non debe aparecer, debe estar comentada ou co valor:

```
write_enable=NO
```

- Só poden acceder os usuarios do sistema con permisos de lectura e escritura.

  Debemos modificar a directiva `write_enable`:

```
write_enable=YES
```

- Poden acceder os usuarios do sistema con permisos de lectura e escritura e os usuarios anónimos (ao cartafol `/ftp-anon`) con permiso de só lectura.
  - Creamos o cartafol `/ftp-anon` con permisos de lectura para todos os usuarios:

```
sudo mkdir /ftp-anon
sudo chmod 755 /ftp-anon
```

  - Creamos nese directorio un arquivo para poder facer probas de descarga do mesmo.

- Modificamos o arquivo `/etc/vsftpd.conf` para que conteña estes valores das directivas:

```
anonymous_enable=YES
anon_root=/ftp-anon
local_enable=YES
write_enable=YES
#anon_upload_enable=YES
#anon_mkdir_write_enable=YES
```

As directivas `anon_upload_enable` e `anon_mkdir_write_enable` poden non aparecer, estar comentadas ou ter o valor:

```
anon_upload_enable=NO
anon_mkdir_write_enable=NO
```

- Poden acceder os usuarios do sistema e os usuarios anónimos (ao cartafol `/ftp-anon`) con permisos de lectura e escritura.
  - Cambiamos os permisos do cartafol `/ftp-anon para que todos os usuarios` teñan permiso de escritura.

```
sudo chmod 777 /ftp-anon
```

  - Modificamos o arquivo `/etc/vsftpd.conf` para que conteña estes valores das directivas:

```
anonymous_enable=YES
anon_root=/ftp-anon
local_enable=YES
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
```

A directiva `anon_mkdir_write_enable` só debe ter o valor `YES` se queremos que os usuarios anónimos poidan crear novos directorios.

2. Restrición de usuarios permitidos no FTP

Empregaremos as directivas `userlist_enable, userlist_deny` e `userlist_file` para restrinxir o acceso ao FTP a un conxunto de usuarios.

Crear dous novos usuarios locais na máquina onde está o servidor ftp: `usuario1` e `usuario2`. Modifica a configuración do servidor vsftpd para restrinxir o acceso do seguinte xeito.

- Prohíbese o acceso ao servidor a `usuario1`.
- Permítese o acceso ao servidor unicamente a `usuario1` e `alumno (ou outro usuario administrador que teñas no sistema)`.

Pasos a seguir

- Crear dous novos usuarios locais: `usuario1` e `usuario2`.

- Creamos os dous usuarios co comando `useradd` (empregamos `-m` para indicar que cree o directorio `HOME` e `-s` para indicar que intérprete de comandos empregará, xa que a configuración por defecto de vsftpd require que teñan un intérprete asignado) e despois creamos o contrasinal co comando `passwd`:

```
sudo useradd -d /home/usuario1 -m -s /bin/bash usuario1
sudo passwd usuario1
sudo useradd -d /home/usuario2 -m -s /bin/bash usuario2
sudo passwd usuario2
```

Nota: tanto a usuario1 como a usuario2, poner una password da que nos lembremos. Por exemplo abc123.

Comprobamos desde o cliente que podemos acceder ao servidor FTP con estes novos usuarios.

- Prohíbir o acceso ao servidor ftp a `usuario1`.
  - Creamos un ficheiro para indicar os usuarios permitidos, por exemplo `/etc/usuarios_ftp_prohibidos`

```
sudo gedit /etc/usuarios_ftp_prohibidos
```

Co contido:

```
usuario1
```

Engadimos as seguintes directivas no ficheiro `/etc/vsftpd.conf`:

```
userlist_enable=YES
userlist_deny=YES
userlist_file=/etc/usuarios_ftp_prohibidos
```

Reiniciamos o servidor:

```
sudo service vsftpd restart
```

E probamos desde o cliente que se nos permite o acceso a `usuario2` e `alumno` pero non a `usuario1`.

- Permítese o acceso ao servidor unicamente a `usuario1` e `alumno`.
  - Creamos un ficheiro para indicar os usuarios permitidos, por exemplo `/etc/usuarios_ftp_permitidos`

```
sudo gedit /etc/usuarios_ftp_permitidos
```

Co contido:

```
usuario1
alumno
```

Engadimos as seguintes directivas no ficheiro `/etc/vsftpd.conf`:

```
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/usuarios_ftp_permitidos
```

Reiniciamos o servidor:

```
sudo service vsftpd restart
```

E probamos desde o cliente que se nos permite o acceso a `usuario1` e `alumno` pero non a `usuario2`.

3. Engaiolamento de usuarios

Configurar o engaiolamento de usuarios para evitar o problema de seguridade que supón que os usuarios poidan ter acceso máis aló do seu propio cartafol persoal.

- Comprobar que un usuario do sistema (por exemplo, `alumno`) pode acceder a toda a árbore de directorios.
- Engaiolar aos usuarios no seu directorio `HOME`. Vamos a ter un erro que teremos que resolver.

Pasos a seguir

- Comprobar que un usuario do sistema (alumno) pode acceder a toda a árbore de directorios.

  Empregar Filezilla para conectarnos co usuario alumno e navegar cara a arriba na árbore de directorios e comprobar que podemos acceder.

- Engaiolar aos usuarios no seu directorio `HOME`.

  Para engaiolar aos usuarios, debe estar sen comentar a liña:

```
chroot_local_user=YES
```

  Pero cando tratamos de acceder desde o cliente, atopamos o seguinte erro:

```
500 OOPS: vsftpd: refusing to run with writable root inside chroot()
```

Que é debido á restrición que impón vsftpd de que o directorio de maior nivel ao que pode acceder un usuario non pode ter permisos de escritura. Ata o momento no que engaiolamos aos usuarios, o directorio de maior nivel era / e un usuario non ten permisos de escritura nel. Pero agora, o directorio de máis alto nivel sería /home/administrador (no caso do usuario administrador), no que si ten permisos de escritura.

- Resolve o problema.

  MALA SOLUCION: Eliminamos os permisos de escritura no directorio /home/administrador de xeito que neste non poida escribir, e teña que facelo nos outros directorios descendentes deste:

```
chmod 555 /home/administrador
```

  Pero moito mellor que a solución anterior e engadir a directiva

```
allow_writeable_chroot=YES
```

Comprobamos desde o cliente que podemos acceder e que o usuario xa non ten acceso a toda a árbore de directorios.