

## Módulo 09 – Servidores – Atividade 04

### Exercícios:

1. Criar um usuário no sistema e definir a suas pastas/permissions para receber arquivos via FTP.
2. Demonstrar que ao conectar no servidor o serviço de FTP está 'chrooted', isto é, ao dar o comando 'pwd' não é possível a navegação em pastas superiores ao dos arquivos.
3. Demonstre onde mudou o arquivo de configurações do Apache 2 para o apontamento à pasta do usuário de FTP.
4. Faça upload de um arquivo utilizando o Filezilla.
5. Faça upload de arquivos utilizando o terminal.
6. Demonstre as páginas sendo acessadas via HTTPS do servidor Apache 2.

Q1) Segui o tutorial disponível nesse endereço:

<https://www.techrepublic.com/article/how-to-use-sftp-with-a-chroot-jail/>

Recomenda-se criar um grupo primeiro, através deste comando: “sudo groupadd sftponly”

A próxima etapa é adicionar um usuário. Para este tutorial o nome do nosso usuário será “enzo”

Portanto, aplica-se o seguinte comando para criar o usuário:

“sudo useradd -g sftponly -s /bin/false -m -d /home/enzo enzo”

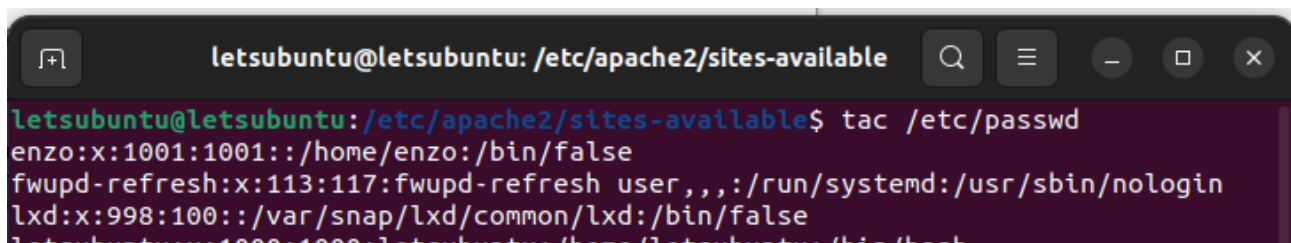
O comando acima garante que o usuário não consegue efetuar login via SSH, pois atribui /bin/false como o shell do usuário.

Falta adicionar uma senha para o novo usuário. Apliquei o comando:

“sudo passwd enzo”

Coloquei a senha “54321” para ser fácil de lembrar.

Através do comando “tac /etc/passwd”, posso observar se os comandos acima resultaram na criação do usuário. Tac imprime na ordem inversa, o que é interessante já que as informações aparecer na última linha, desse modo, ficam aparecendo na primeira linha:



```
letsubuntu@letsubuntu: /etc/apache2/sites-available
letsubuntu@letsubuntu: /etc/apache2/sites-available$ tac /etc/passwd
enzo:x:1001:1001::/home/enzo:/bin/false
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
letsubuntu:x:1000:1000:letsubuntu:/home/letsubuntu:/bin/bash
```

Além disso, nota-se que tem um “x” ao lado de enzo, indicando que o usuário possui uma senha criptografada.

Se você já possui usuários que deseja adicionar ao grupo, pode fazê-lo com o comando:

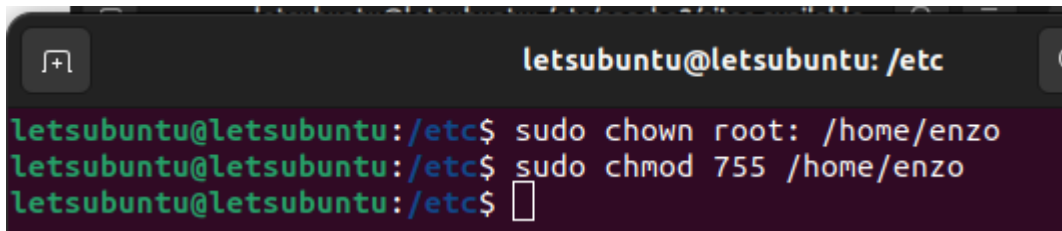
“sudo usermod -G sftponly -s /bin/false enzo”

Observe, no entanto, se o usuário exigir login SSH, ele não poderá fazer isso depois que você fizer essa alteração. Se for esse o caso, considere criar um novo usuário especificamente para suas necessidades de SFTP.

As permissões do diretório inicial do usuário (enzo) agora devem ser alteradas. Para fazer isso, emita os seguintes comandos:

“sudo chown root: /home/enzo”

“sudo chmod 755 /home/enzo”

A terminal window titled 'letsubuntu@letsubuntu: /etc' showing two commands being executed. The first command is 'sudo chown root: /home/enzo' and the second is 'sudo chmod 755 /home/enzo'. The prompt is 'letsubuntu@letsubuntu: /etc\$'.

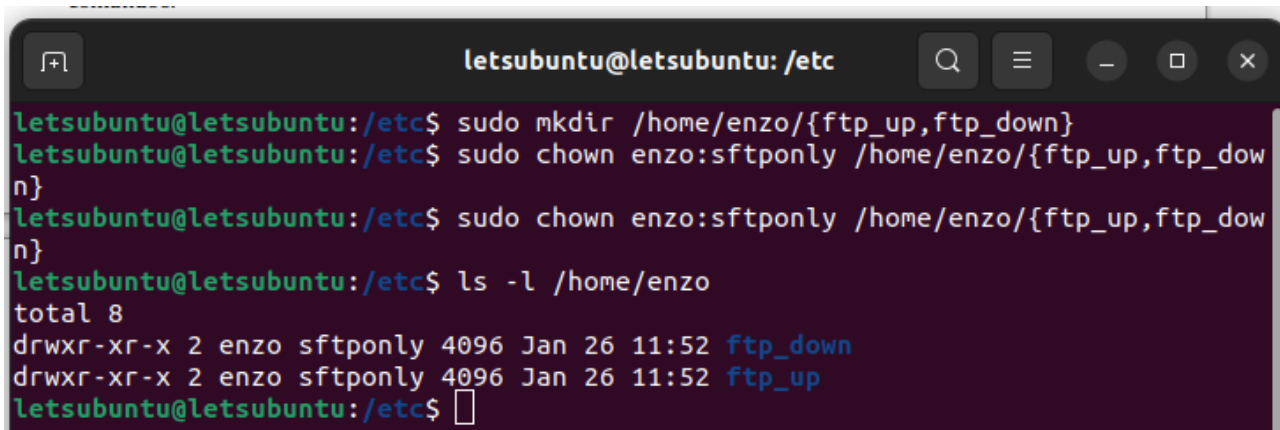
Com os diretórios do usuário agora pertencentes ao root, eles não poderão criar arquivos e/ou diretórios. Para contornar isso (para que eles possam fazer upload e download de arquivos), crie novos subdiretórios (dentro do diretório inicial) aos quais eles terão acesso com os seguintes comandos:

```
sudo mkdir /home/enzo/{ftp_up,ftp_down}
```

```
sudo chmod 755 /home/enzo/{ftp_up,ftp_down}
```

```
sudo chown enzo:sftponly /home/enzo/{ftp_up,ftp_down}
```

As chaves (“{“ e “}”), permitem criar dois diretórios na mesma linha de comando

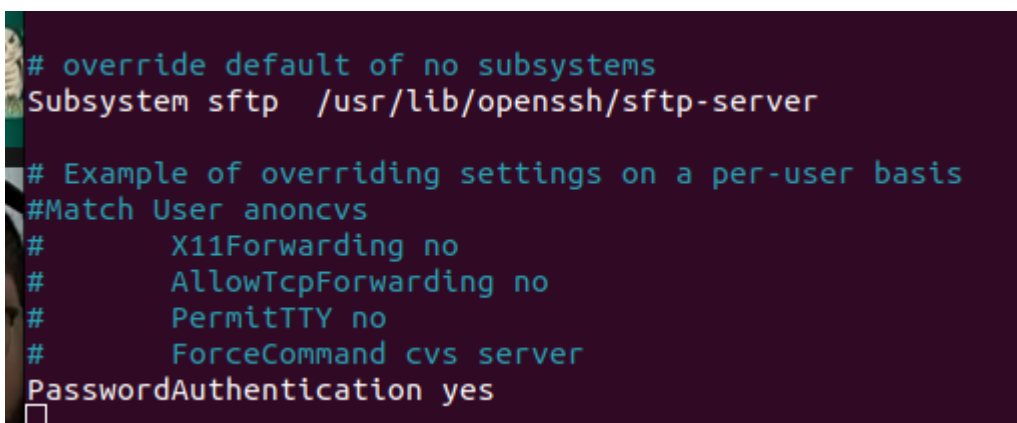
A terminal window titled 'letsubuntu@letsubuntu: /etc' showing three commands being executed. The first is 'sudo mkdir /home/enzo/{ftp\_up,ftp\_down}', the second is 'sudo chown enzo:sftponly /home/enzo/{ftp\_up,ftp\_down}', and the third is 'ls -l /home/enzo'. The output of the last command shows two directories, 'ftp\_down' and 'ftp\_up', with permissions 'drwxr-xr-x' and owner 'enzo'.

Ainda na imagem acima, empregou-se o comando “ls -l /home/enzo” para verificar as permissões e o dono das pastas. Está tudo conforme esperado.

A próxima etapa é configurar o SSH.

Comecei essa etapa aplicando o comando: “sudo nano /etc/ssh/sshd\_config”

Nesse arquivo, pede-se para procurármos pela linha {Subsystem sftp /usr/lib/openssh/sftp-server}. Esse trecho está próximo do final do arquivo.

A screenshot of the /etc/ssh/sshd\_config file. It shows the configuration for the sftp subsystem. The line 'Subsystem sftp /usr/lib/openssh/sftp-server' is highlighted. Below it, there is a section for overriding settings on a per-user basis, with 'Match User anoncvs' and several settings like 'X11Forwarding no', 'AllowTcpForwarding no', 'PermitTTY no', 'ForceCommand cvs server', and 'PasswordAuthentication yes'.

Pede-se para substituir a linha por essa: “Subsystem sftp internal-sftp”.

```
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp internal-sftp

# Example of overriding settings on a per-user basis
#Match User anoncvs
```

Em seguida, pede-se para irmos até o final do arquivo e adicionar algumas linhas:

```
Match Group sftponly
ChrootDirectory %h
ForceCommand internal-sftp
AllowTcpForwarding no
X11Forwarding no
```

```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
PasswordAuthentication yes

Match Group sftponly
ChrootDirectory %h
ForceCommand internal-sftp
AllowTcpForwarding no
X11Forwarding no

```

^G Get Help    ^O Write Out    ^W  
^X Exit        ^R Read File    ^\

Salve as alterações que ocorreram no arquivo, reiniciando o SSH com o comando: “sudo systemctl restart sshd”.

```
letsubuntu@letsubuntu:~$ sudo systemctl restart sshd
letsubuntu@letsubuntu:~$
```

Pronto, tudo que era necessário foi criado. Agora entramos na fase de testes.

Q2) Lembrando que o usuário criado foi “enzo” e que o IP da máquina remota é 192.168.0.114.

Fazemos o login com esse usuário, através do comando:

“sftp enzo@192.168.0.114”

A imagem a seguir ilustra exatamente isso. Onde abri o terminal na minha máquina local e apliquei o comando para logar na máquina virtual via sftp.

```
letonio@letonio-Inspiron-15-3567: ~  
letonio@letonio-Inspiron-15-3567:~$ sftp enzo@192.168.0.114  
The authenticity of host '192.168.0.114 (192.168.0.114)' can't be established.  
ED25519 key fingerprint is SHA256:rZ560fUKGQpl8k/2e29fcE28qrqgU+MSlWTWwWAnjBs.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [hashed name]  
  ~/.ssh/known_hosts:3: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.0.114' (ED25519) to the list of known hosts.  
enzo@192.168.0.114's password:  
Connected to 192.168.0.114.
```

Ao tentar usar o comando `pwd`, não temos acesso ao root, conforme ficou definido nos passos anteriores, o usuário “enzo” só tem acesso a sua pasta pessoal, que pra ele equivale ao root dele. Não é possível navegar para pastas superiores. Apenas para ficar registrado, o root tem acesso a tudo e o caminho até essa pasta seria `(/home/enzo/ftp_up)`. No entanto, o enzo tem acesso apenas a sua pasta local, portanto o caminho que ele pode acessar é `(/ftp_up)` Ele não consegue acessar pastas superiores a isso, é como se a raiz dele fosse a própria pasta pessoal.

```
enzo@192.168.0.114's password:  
Connected to 192.168.0.114.  
sftp> pwd  
Remote working directory: /  
sftp> █
```

Q3) A mudanças no arquivo já foram mostradas na Q1, durante o processo de criação de usuário.

Q4) Pronto, está tudo preparado para fazer trocas de arquivos. Sabendo disso, vamos fazer primeiro a transferência utilizando o Filezilla que já está instalado na máquina local. Durante a resolução desse exercício, tenho instalado a versão 3.58.0.

Abri outro terminal da minha máquina local, para criar um arquivo em `/home/letonio/arquivoFilezilla.txt`

```
letonio@letonio-Inspiron-15-3567: ~  
letonio@letonio-Inspiron-15-3567:~$ echo "Esse arquivo esta na maquina local  
era upload via filezilla" >> /home/letonio/arquivoFilezilla.txt  
letonio@letonio-Inspiron-15-3567:~$ ls /home/letonio/  
'Área de Trabalho'  group_ordenado.txt  pastaQ1-.tar.gz  
arquivoFilezilla.txt  Imagens  Público  
chave.txt  linux  snap
```

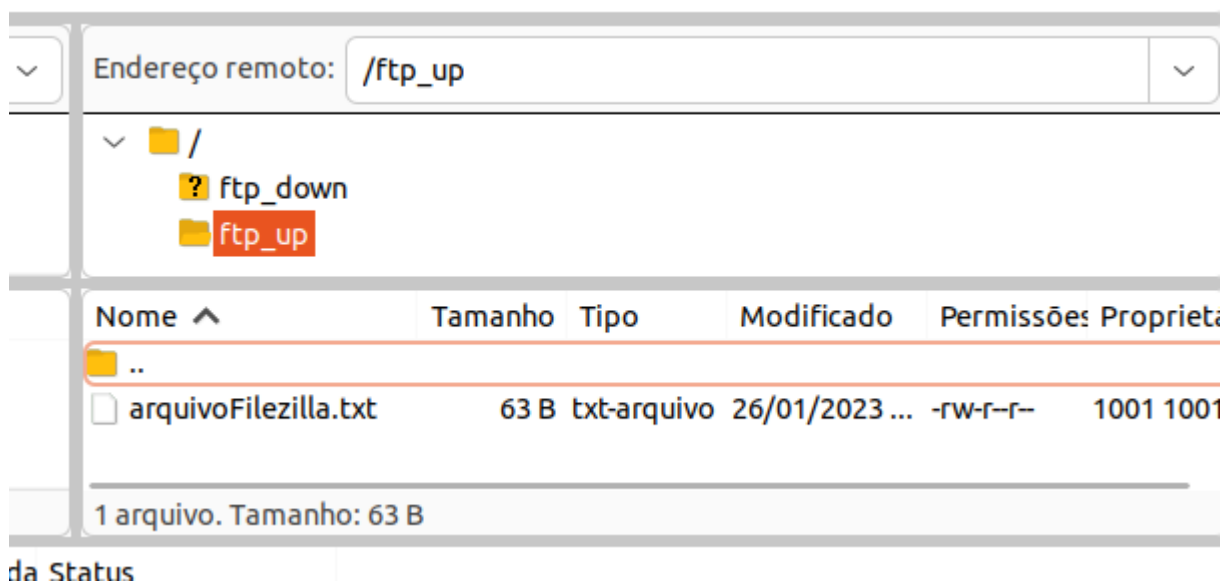
No filezilla coloquei as informações da máquina remota, usuário e senha e fiz a conexão:  
A conexão ocorreu:

Host:	192.168.0.114	Nome de usuário:	enzo	Senha:	.....
-------	---------------	------------------	------	--------	-------



O usuário (enzo) tem acesso apenas a pasta que ficou definida, sua própria pasta pessoal. Consequentemente, na sua própria raiz, nota-se apenas as duas pastas (upload e download).

Agora, dentro da pasta de upload, será feito o upload do arquivo “arquivoFilezilla.txt”: Arrastei o arquivo txt até a região e o upload aconteceu.



Se formos no terminal, onde estava o “sftp”, podemos entrar dentro da pasta ftp\_up e veremos que o arquivo está lá.

```
sftp> ls
ftp_down  ftp_up
sftp> ls /f
ftp_down/ ftp_up/
sftp> ls /ftp_up
/ftp_up/arquivoFilezilla.txt
sftp>
```

Q5) Agora, a próxima ideia é adicionar um arquivo via terminal.  
O arquivo está no seguinte caminho (path) na máquina local: /home/letonio/viaSFTP.txt

```
letonio@letonio-Inspiron-15-3567: ~  
letonio@letonio-Inspiron-15-3567:~$ echo "Esse arquivo esta na maquina local e s  
era upload via sftp comando put" >> /home/letonio/viaSFTP.txt  
letonio@letonio-Inspiron-15-3567:~$ ls ~  
'Área de Trabalho'      Imagens      snap  
arquivoFilezilla.txt    linux        user_ordenado.txt  
chave.txt               Modelos      viaSFTP.txt  
chave.txt.pub           Música       viaterminal.txt
```

Através do comando put podemos fazer a transferência/upload de um arquivo da máquina local, para a virtual. Uma observação importante é que o caminho completo para o usuário enzo, que somente tem acesso a sua pasta pessoal é /ftp\_up. Não confunda achando que começa de /home, pois o enzo, conta que estamos logados, não tem acesso ao root, tem acesso somente a própria pasta pessoal, ou seja, o caminho correto é /ftp\_up/arquivoFilezilla.txt, caso eu quisesse ver o arquivo que foi upado via filezilla.

Enfim, o comando empregado é  
“put /home/letonio/viaSFTP.txt /ftp\_up”

```
letonio@letonio-Inspiron-15-3567: ~  
letonio@letonio-Inspiron-15-3567:~$ sftp enzo@192.168.0.114  
The authenticity of host '192.168.0.114 (192.168.0.114)' can't be established.  
ED25519 key fingerprint is SHA256:rZ560fUKGQpl8k/2e29FcE28qrqgU+MSlWTWwAnjBs.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [hashed name]  
  ~/.ssh/known_hosts:3: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.0.114' (ED25519) to the list of known hosts.  
enzo@192.168.0.114's password:  
Connected to 192.168.0.114.  
sftp> put /home/letonio/via  
viaSFTP.txt          viaterminal.txt  
sftp> put /home/letonio/viaSFTP.txt /ftp_up  
Uploading /home/letonio/viaSFTP.txt to /ftp_up/viaSFTP.txt  
viaSFTP.txt          100% 70 46.3KB/s 00:00  
sftp> ls -l ftp_up  
-rw-r--r-- 1 1001 1001 63 Jan 26 14:02 arquivoFilezilla.txt  
-rw-r--r-- 1 1001 1001 70 Jan 26 14:13 viaSFTP.txt  
sftp> □
```

Além disso, utilizei o comando “ls -l” para verificar as permissões. Tenha em mente que 1001 corresponde ao ID do usuário enzo.

Lembrando que segui o tutorial disponível em:

<https://www.techrepublic.com/article/how-to-use-sftp-with-a-chroot-jail/>

Q6) Acho que essa questão faz parte do exercício anterior, na aula 03 pedia para fazermos o acesso a página via HTTPS. Não entendi esse pedido.