项目 6 配置与管理 FTP 服务器-实训任务指导书（6-1）

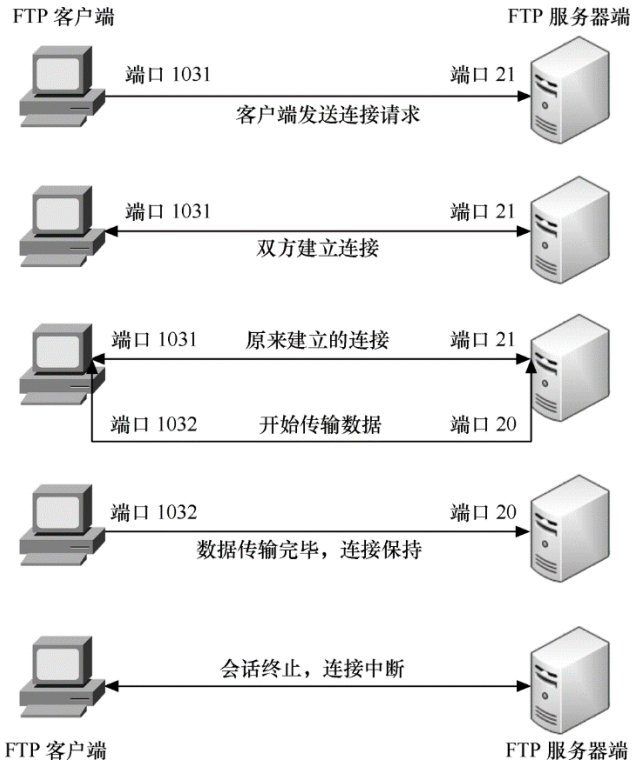
理论知识

1.FTP 服务简介

FTP 服务就是专门用于文件传输的服务，FTP 的全称是 File Transfer Protocol，顾名思义，就是文件传输协议，具备更强的文件传输可靠性和更高的效率。FTP 大大简化了文件传输的复杂性，它能够使文件通过网络从一台主机传送到另外一台计算机上却不受计算机和操作系统类型的限制。无论是 PC、服务器、大型机，还是 IOS、Linux、Windows 操作系统，只要双方都支持协议 FTP，就可以方便、可靠地进行文件的传送。

2. FTP 服务的具体工作原理过程

（1）客户端向服务器发出连接请求，同时客户端系统动态地打开一个大于 1024 的端口等候服务器连接（比如 1031 端口）。
（2）若 FTP 服务器在端口 21 侦听到该请求，则会在客户端 1031 端口和服务器的 21 端口之间建立起一个 FTP 会话连接。
（3）当需要传输数据时，FTP 客户端再动态地打开一个大于 1024 的端口（比如 1032 端口）连接到服务器的 20 端口，并在这两个端口之间进行数据的传输。当数据传输完毕后，这两个端口会自动关闭。
（4）当 FTP 客户端断开与 FTP 服务器的连接时，客户端上动态分配的端口将自动释放。



3. vsftpd 的认证模式

vsftpd 允许用户以三种认证模式登录到 FTP 服务器上。
①匿名开放模式：
通过使用一个共同的用户名 anonymous，密码不限的管理策略（一般使用用户的邮箱作为密

码即可）让任何用户都可以很方便地从这些服务器上下载软件
是一种最不安全的认证模式，任何人都可以无需密码验证而直接登录到 FTP 服务器。
②本地用户模式：是通过 Linux 系统本地的账户密码信息进行认证的模式，相较于匿名开放模式更安全，而且配置起来也很简单。但是如果被黑客破解了账户的信息，就可以畅通无阻地登录 FTP 服务器，从而完全控制整台服务器。
③虚拟用户模式：是这三种模式中最安全的一种认证模式，它需要为 FTP 服务单独建立用户数据库文件，虚拟映射用来进行口令验证的账户信息，而这些账户信息在服务器系统中实际上是不存在的，仅供 FTP 服务程序进行认证使用。这样，即使黑客破解了账户信息也无法登录服务器，从而有效降低了破坏范围和影响。

4 匿名用户登录的参数说明

参数	作用
listen=[YES|NO]	是否以独立运行的方式监听服务
listen_address=IP 地址	设置要监听的 IP 地址
listen_port=21	设置 FTP 服务的监听端口
download_enable＝[YES|NO]	是否允许下载文件
userlist_enable=[YES|NO] userlist_deny=[YES|NO]	设置用户列表为“允许”还是“禁止”操作
max_clients=0	最大客户端连接数，0 为不限制
max_per_ip=0	同一 IP 地址的最大连接数，0 为不限制
anonymous_enable=[YES|NO]	是否允许匿名用户访问
anon_upload_enable=[YES|NO]	是否允许匿名用户上传文件
anon_umask=022	匿名用户上传文件的 umask 值
anon_root=/var/ftp	匿名用户的 FTP 根目录
anon_mkdir_write_enable=[YES|NO]	是否允许匿名用户创建目录
anon_other_write_enable=[YES|NO]	是否开放匿名用户的其他写入权限（包括重命名、删除等操作权限）
anon_max_rate=0	匿名用户的最大传输速率（字节/秒），0 为不限制
local_enable=[YES|NO]	是否允许本地用户登录 FTP
local_umask=022	本地用户上传文件的 umask 值
local_root=/var/ftp	本地用户的 FTP 根目录
chroot_local_user=[YES|NO]	是否将用户权限禁锢在 FTP 目录，以确保安全
local_max_rate=0	本地用户最大传输速率（字节/秒），0 为不限制

任务 1 配置匿名用户 FTP 服务器实例

某企业想构建一台 FTP 服务器，允许匿名用户上传和下载文件，匿名用户的根目录设置为/var/ftp。为企业局域网中的计算机提供文件传送任务，为财务部门、销售部门和 OA 系统提供异地数据备份。

项目准备：

需要两台虚拟机，一台作为 FTP 服务器 主机名 server7-1，IP 地址为 192.168.10.2/24 ;FTP 客户端,主机名 client7-2,IP 地址为 192.168.1.3/24，DNS 为 192.168.1.2 ;Windows 客户端： Windows 7 IP 地址为 192.168.1.30

直接在网卡 VMnet 上设置 IP 地址为：192.168.1.30/24。

具体实训步骤

一、分别在 FTP 服务器 server7-1 上和 FTP 客户端 client7-2 上安装 FTP 软件包。

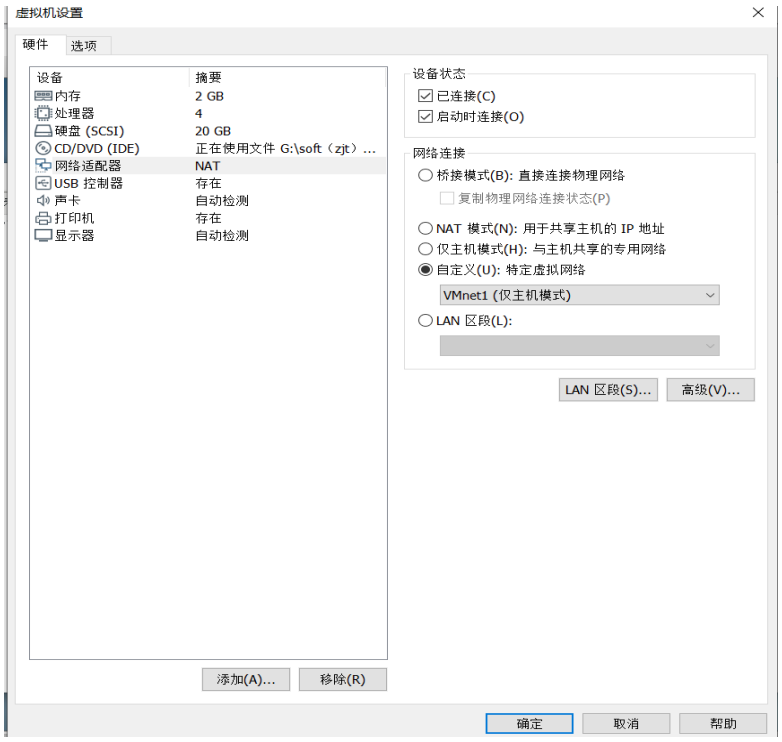
1. 打开 FTP 服务器主机修改为 server7-1，安装 vsftpd 服务。（网络 NAT 模式下，可选用 ens33 连接）

```
[root@server7-1]# yum clean all          //安装前先清除缓存
[root@server7-1]# yum install vsftpd -y
[root@server7-1]# rpm -qa|grep vsftpd  //检查安装组件是否成功
```

2. 打开 FTP 客户端主机主机名修改为 client7-2，安装 ftp 服务。（网络 NAT 模式下，可选用 ens33 连接）

```
[root@client7-2]# yum clean all       //安装前先清除缓存
[root@client7-2]# yum install ftp -y     //同时安装 ftp 软件包
```

3. 软件包安装完成后，分别进行网络配置，FTP 服务器 server7-1，IP 地址设为 192.168.1.2/24 ，默认网关 192.168.1.1；FTP 客户端 client7-2，IP 地址为 192.168.1.3/24，默认网关 192.168.1.1，DNS 为 192.168.1.2，两台主机网络设置模式均修改设置为自定义 VMnet1 仅主机模式，实现网络互联。



二、在 FTP 服务器主机 server7-1 上，启动 vsftpd 服务启动，并设置开机自动加载。

[root@ server7-1]# systemctl start vsftpd

[root@ server7-1]# systemctl enable vsftpd

```
[root@server7-1 ~]# systemctl start vsftpd
[root@server7-1 ~]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/v
sftpd.service to /usr/lib/systemd/system/vsftpd.service.
```

三、配置服务器的防火墙策略，添加允许 FTP 服务，并永久生效，并设置 selinux 为允许。

1.配置服务器的防火墙策略，添加允许 FTP 服务，并永久生效

[root@ server7-1]# firewall-cmd --permanent --add-service=ftp

[root@ server7-1]# firewall-cmd –reload

```
[root@server7-1 ~]# firewall-cmd --permanent --add-service=ftp
success
[root@server7-1 ~]# firewall-cmd --reload
success
[root@server7-1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ftp ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

2.查看防火墙配置,开启防火墙中的匿名上传服务

通过 getsebool -a | grep ftp 我们可以看到 selinux 是禁止了所有的 ftp 服务，需要开启防火墙中的匿名上传服务。

```
[root@server7-1 ~]# getsebool -a|grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@server7-1 ~]# setsebool  ftpd_anon_write  on
[root@server7-1 ~]# getsebool -a|grep ftp
ftpd_anon_write --> on
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@server7-1 ~]# getenforce
Enforcing
[root@server7-1 ~]# setenforce  0
[root@server7-1 ~]# getenforce
Permissive
[root@server7-1 ~]#
```

设置 FTP 服务完全访问为允许

[root@ server7-1]# setsebool -P ftpd_ full_access=on

3. 防火墙配置完成，需要重启 vsftpd 服务

[root@server7-1] systemctl restart vsftpd

四、分别在 FTP 客户端主机 client7-2 上和 windows 物理本机中，进行登录测试验证。

1. FTP 客户端主机 client7-2 使用 ftp 命令，进行登录验证。

①允许匿名用户登录：在 Linux 上测试，用户名输入：ftp，密码处直接回车即可

```
221 Goodbye.
[root@client7-2 ~]# ftp 192.168.1.2
Connected to 192.168.1.2 (192.168.1.2).
220 (vsFTPd 3.0.2)
Name (192.168.1.2:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
227 Entering Passive Mode (192,168,1,2,179,87).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0               6 Jun 09  2021 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (192,168,1,2,181,196).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
227 Entering Passive Mode (192,168,1,2,121,116).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0               6 Jun 09  2021 .
drwxr-xr-x    3 0        0              17 May 03 23:06 ..
226 Directory send OK.
ftp>
```

② 允许本机用户登录

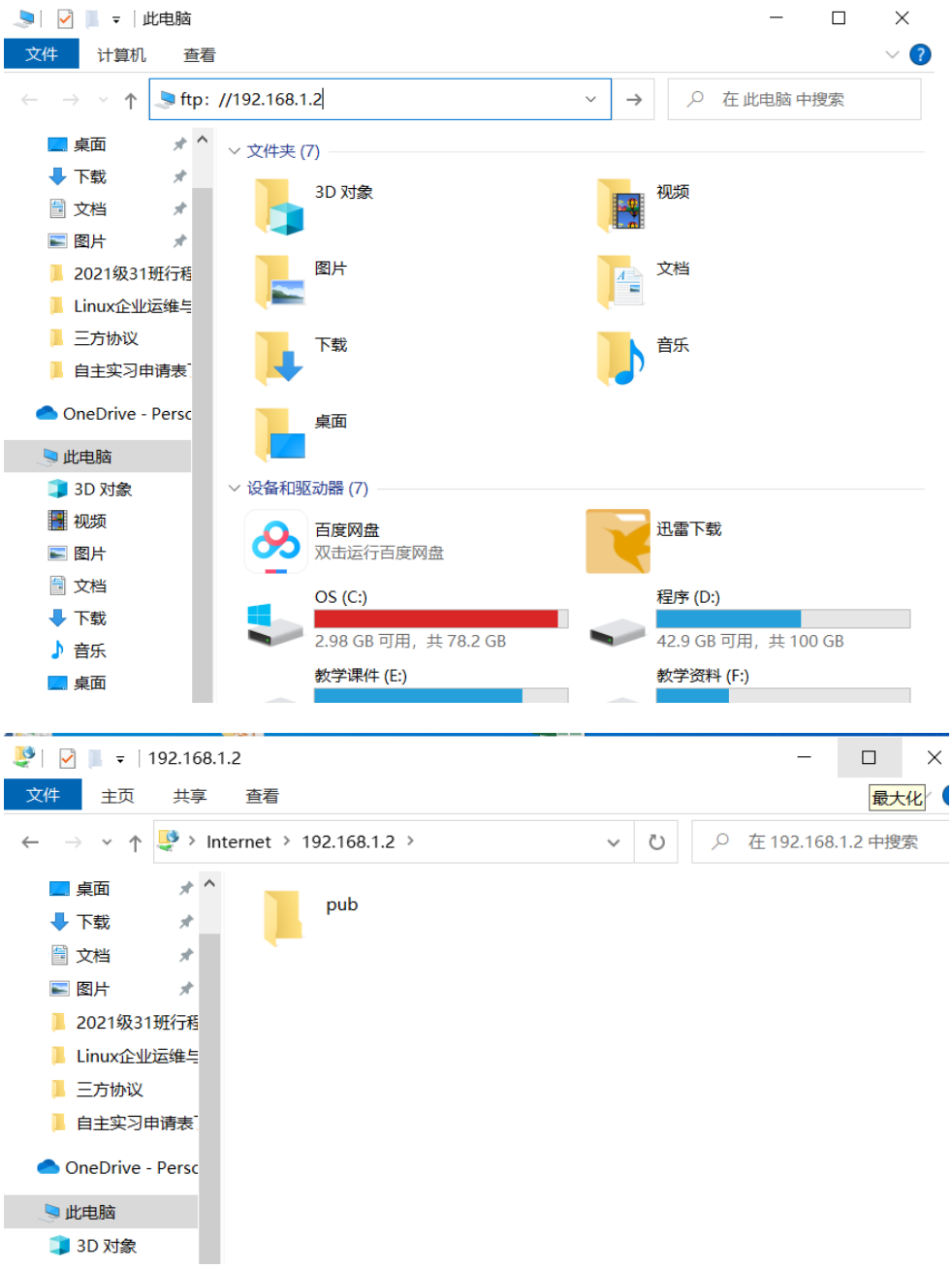
```
[root@client7-2 ~]# ftp 192.168.1.2
Connected to 192.168.1.2 (192.168.1.2).
220 (vsFTPd 3.0.2)
Name (192.168.1.2:root): dm
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
227 Entering Passive Mode (192,168,1,2,242,120).
150 Here comes the directory listing.
drwx------    3 1000     1000           78 Feb 23 08:52 .
drwxr-xr-x    3 0        0              16 Feb 23 09:00 ..
-rw-r--r--    1 1000     1000           18 Apr 01  2020 .bash_logout
-rw-r--r--    1 1000     1000          193 Apr 01  2020 .bash_profile
-rw-r--r--    1 1000     1000          231 Apr 01  2020 .bashrc
drwxr-xr-x    4 1000     1000           39 Feb 23 08:52 .mozilla
226 Directory send OK.
ftp>
```

2. FTP 客户端主机 client7-2 使用火狐浏览器：ftp：//192.168.1.2，进行登录验证。

3. Windows 中打开我的电脑，在地址栏输入 ftp：//192.168.1.2，进行登录验证。

设置物理本机的虚拟网卡 VMnet1，修改网络配置如下

然后在 Windows 中打开我的电脑，在地址栏输入 ftp：//192.168.1.2



但是不能实现文件的上传和下载。

五、修改 vsftpd 的主配置文件/etc/vsftpd/vsftpd.conf，实现 FTP 服务中数据的上传和下载

[root@ server7-1]# **vim /etc/vsftpd/vsftpd.conf**

#anon_upload_enable=YES　　29 行把前面的#去掉，允许匿名用户上传文件
#anon_mkdir_write_enable=YES　　33 行把前面的#去掉，允许匿名用户创建目录
然后重启 vsftpd 服务

[root@ server7-1]# systemctl　restart　vsftpd

六、在 vsftpd 的默认主目录中/var/ftp/pub 中，建立一个文本文件，文件名是 ftptest.txt

[root@ server7-1]#cd　/var/ftp/pub

[root@ server7-1]# vim ftptest.txt

输入 ftp service

按:wq 保存退出。

可以操作演示实现文件的下载，但不能实现文件的上传

七、修改 pub 目录的权限，使其他人具有写权限：

[root@ server7-1]# **chmod　777 /var/ftp/pub/**

[root@ server7-1]# ll　-d　/var/ftp/pub

[root@ server7-1]# **chown　ftp /var/ftp/pub/**　设置属主为 FTP

[root@ server7-1]# ll　-d　/var/ftp/pub

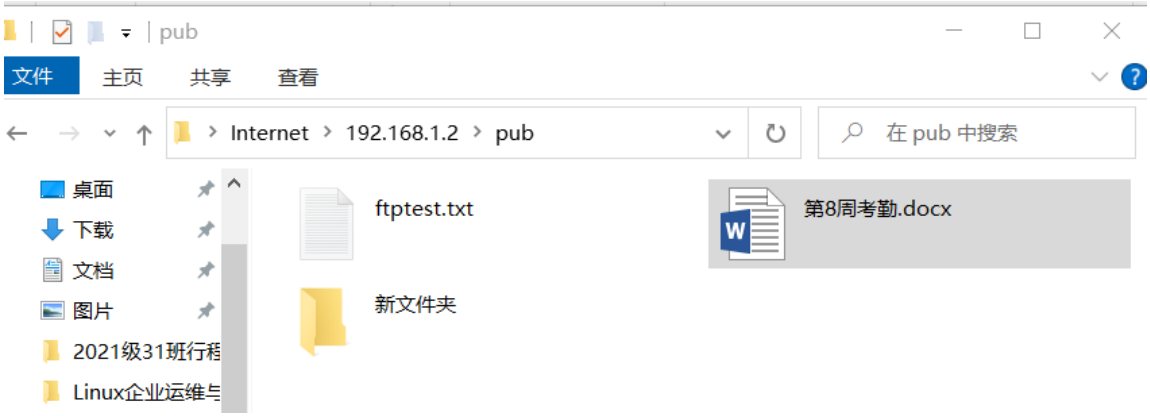
drwxrwxrwx. 2 ftp root 22 6 月　2 20:34 /var/ftp/pub

八、分别在 FTP 客户端主机 client7-2 上和 windows 物理本机中，进行测试验证，能够顺利进行文件的上传和下载，以及创建新的目录等操作。

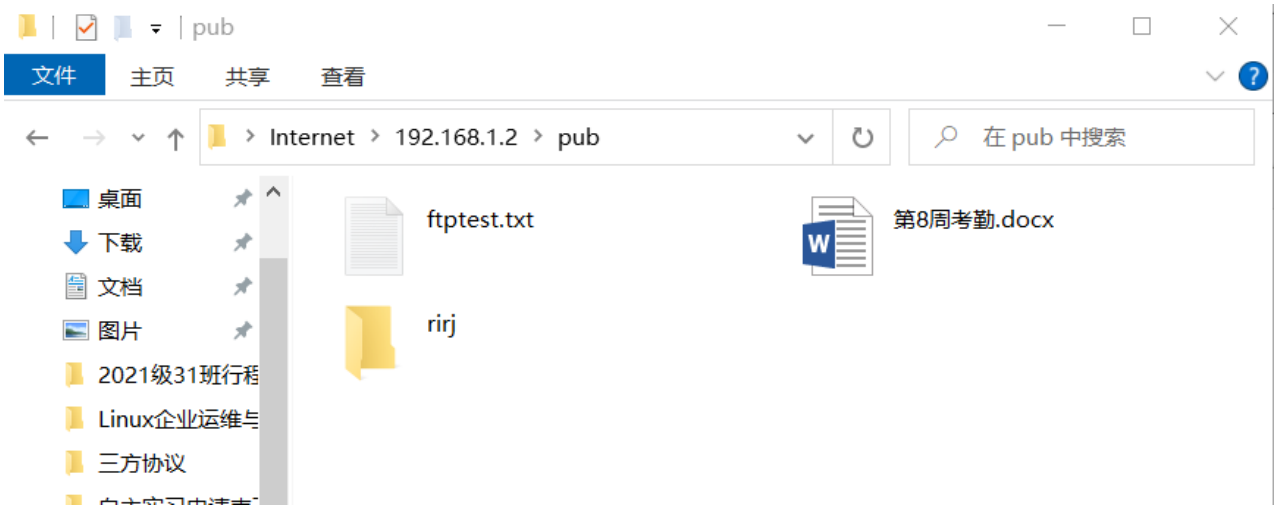
1. 在 FTP 客户端主机 client7-2 上进行创建新目录等测试

```
[root@client7-2 ~]# ftp 192.168.1.2
Connected to 192.168.1.2 (192.168.1.2).
220 (vsFTPd 3.0.2)
Name (192.168.1.2:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /var/ftp
550 Failed to change directory.
ftp> ll
?Invalid command
ftp> cd /var/ftp/pub
550 Failed to change directory.
ftp> ll
?Invalid command
ftp> mkdir rj
550 Create directory operation failed.
ftp> ls -l
227 Entering Passive Mode (192,168,1,2,196,4).
150 Here comes the directory listing.
drwxrwxrwx    3 14       0              70 May 04 07:47 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> mkdir rj rx
257 "/pub/rj" created
ftp>
```

2. 在 windows 物理本机中，进行文件的上传和下载，以及创建新的目录等测试验证操作。



拓展思考：如何实现目录重命名、删除等操作？



允许匿名用户删除文件，可修改配置文件/etc/vsftpd/vsftpd.conf

，添加语句 anon_other_write_enable=YES