

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



BÀI BÁO CÁO THỰC HÀNH SỐ 10

MÔN THỰC TẬP CƠ SỞ

SAO LƯU HỆ THỐNG

Tên sinh viên: Ninh Chí Hường

Mã sinh viên: B20DCAT094

Số điện thoại: 0353770347

Giảng viên hướng dẫn : Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 5/2023

Contents

I. GIỚI THIỆU BÀI THỰC HÀNH.....	3
1. Mục đích:.....	3
2. Cơ sở lý thuyết:	3
II. TIẾN HÀNH THỰC HÀNH:.....	5
1. Sao lưu tới ổ đĩa mạng:	5
2. Sao lưu tệp lên FTP server:	8
3. Sao lưu tệp sử dụng SCP:.....	11
III. Tài liệu tham khảo	13

I. GIỚI THIỆU BÀI THỰC HÀNH

1. Mục đích:

Bài thực hành này giúp sinh viên nắm được công cụ và cách thức sao lưu hệ thống, bao gồm:

1. Sao lưu tới ổ đĩa mạng
2. Sao lưu tệp lên FTP server
3. Sao lưu tệp sử dụng SCP

2. Cơ sở lý thuyết:

a) SCP – Secure copy (SCP):

SCP (Secure Copy) là một công cụ dòng lệnh được sử dụng để sao chép và truyền tệp tin giữa các máy tính trong mạng với mức độ bảo mật cao. SCP sử dụng giao thức SSH (Secure Shell) để mã hóa dữ liệu trước khi truyền đi, giúp bảo vệ dữ liệu khỏi bị đánh cắp hoặc thay đổi trong quá trình truyền tải.

SCP hoạt động tương tự như công cụ sao chép (copy) dòng lệnh của hệ điều hành Unix/Linux, tuy nhiên nó cung cấp thêm tính năng bảo mật. Khi bạn sử dụng SCP để sao chép tệp tin, dữ liệu sẽ được mã hóa trước khi gửi đến máy chủ đích thông qua SSH. Do đó, dù có ai gián điệp trong mạng cũng không thể đọc được nội dung của tệp tin.

SCP có thể hoạt động ở hai chế độ: sao chép từ local lên remote hoặc ngược lại.

SCP là một công cụ rất hữu ích cho các quản trị viên hệ thống hoặc những người làm việc với nhiều máy tính trong mạng. Nó giúp họ có thể sao chép các tệp tin lớn, các script, hoặc các tệp tin nhạy cảm một cách nhanh chóng và an toàn.

Ngoài ra, SCP còn có thể kết hợp với các lệnh dòng lệnh khác để tạo ra các tác vụ tự động hoặc định kỳ. Ví dụ, bạn có thể sử dụng SCP kết hợp với Cron để sao chép các tệp tin định kỳ từ một máy tính đến một máy chủ khác.

Tuy nhiên, việc sử dụng SCP cũng có một số hạn chế. SCP chỉ có thể sao chép tệp tin một cách tuần tự, không thể sao chép nhiều tệp tin cùng lúc. Nếu bạn muốn sao chép nhiều tệp tin, bạn phải sử dụng một vòng lặp hoặc một lệnh tổng hợp khác để sao chép chúng.

Ngoài SCP, còn có một số công cụ khác để sao chép tệp tin qua SSH như rsync, lftp, ncftp,... Tuy nhiên, mỗi công cụ có những ưu điểm và hạn chế riêng, tùy thuộc vào mục đích sử dụng và tình huống cụ thể.

b) FTP - Giao thức truyền tệp:

FTP (File Transfer Protocol) là một giao thức truyền tệp dùng để truyền tệp tin giữa các máy tính trên mạng. Giao thức này được thiết kế để truyền tệp tin theo hai hướng: từ máy chủ về máy khách (download) và từ máy khách lên máy chủ (upload). FTP sử dụng mô hình kiến trúc máy chủ - máy khách để truyền dữ liệu.

Trong giao thức FTP, khi một máy khách yêu cầu truyền một tệp tin từ máy chủ, nó kết nối đến máy chủ thông qua cổng điều khiển (port 21) bằng cách sử dụng tài khoản và mật khẩu xác thực. Sau khi xác thực thành công, máy khách và máy chủ thiết lập kết nối dữ liệu trực tiếp để truyền tệp tin. Kết nối dữ liệu có thể được thiết lập bằng một trong hai phương thức: Active hoặc Passive.

Phương thức Active yêu cầu máy khách mở một cổng để chờ máy chủ kết nối trở lại, trong khi Passive yêu cầu máy chủ mở một cổng để chờ máy khách kết nối. Khi kết

nổi dữ liệu được thiết lập, máy khách và máy chủ có thể truyền dữ liệu theo hướng đơn chiều hoặc đồng thời.

FTP còn có một số chức năng khác như cho phép tạo thư mục mới, xóa thư mục, đổi tên thư mục, đổi tên tệp tin, xóa tệp tin, hiển thị danh sách các tệp tin và thư mục trên máy chủ, v.v.

Tuy nhiên, việc sử dụng FTP cũng có một số hạn chế. Ví dụ, FTP không cung cấp tính năng mã hóa dữ liệu, do đó dữ liệu có thể bị đánh cắp hoặc bị thay đổi khi được truyền qua mạng. Ngoài ra, FTP cũng không hỗ trợ các tính năng như đồng bộ hóa dữ liệu, sao lưu dữ liệu tự động, hoặc quản lý phiên làm việc. Do đó, các công nghệ mới như SFTP (Secure File Transfer Protocol) hay FTPS (FTP over SSL/TLS) được phát triển để thay thế cho FTP và cung cấp tính năng bảo mật và đầy đủ hơn cho việc truyền tệp tin trên mạng.

c) Ổ đĩa mạng:

Ổ đĩa mạng (Network Attached Storage hay NAS) là một thiết bị lưu trữ dữ liệu được kết nối vào mạng để các thiết bị khác trong mạng có thể truy cập và chia sẻ dữ liệu từ đó. NAS thường được dùng cho các mục đích lưu trữ và chia sẻ dữ liệu giữa các máy tính trong một doanh nghiệp hoặc gia đình.

NAS thường được thiết kế với một số khe cắm ổ đĩa cứng, nơi mà người dùng có thể cài đặt ổ đĩa cứng để lưu trữ dữ liệu. NAS thường được cài đặt và quản lý thông qua giao diện web hoặc phần mềm quản lý để người dùng có thể thực hiện các tác vụ quản lý như tạo thư mục, xóa thư mục, di chuyển tệp tin, cấu hình chia sẻ dữ liệu, v.v.

NAS cũng cung cấp một số tính năng đáng chú ý như sao lưu dữ liệu, phân quyền truy cập dữ liệu, mã hóa dữ liệu và chia sẻ tệp tin qua mạng. Ngoài ra, NAS còn có thể được cấu hình để truy cập từ xa qua Internet, cho phép người dùng truy cập dữ liệu từ bất kỳ đâu trên thế giới mà không cần phải có truy cập trực tiếp vào máy tính của mình.

Tuy nhiên, để sử dụng được NAS, người dùng cần phải có kiến thức cơ bản về mạng và quản lý hệ thống. Ngoài ra, NAS cũng có giá thành cao hơn so với một ổ đĩa di động thông thường, do đó, việc lựa chọn NAS cần phải cân nhắc đến nhu cầu sử dụng và khả năng tài chính của mỗi người dùng.

d) Net use:

"Net use" là một lệnh trong hệ điều hành Windows được sử dụng để kết nối và ngắt kết nối với các tài nguyên mạng như máy chủ, ổ đĩa mạng, máy in, v.v. thông qua đường mạng.

Khi sử dụng lệnh "Net use", người dùng có thể kết nối với các tài nguyên mạng thông qua các giao thức khác nhau như SMB, NFS, FTP, v.v. Bằng cách kết nối với các tài nguyên mạng này, người dùng có thể truy cập vào các tệp tin và thư mục được chia sẻ từ các máy tính khác trong mạng.

e) Net view:

"Net view" là một lệnh trong hệ điều hành Windows được sử dụng để hiển thị danh sách các máy tính và tài nguyên mạng có sẵn trên mạng. Lệnh này cho phép người dùng kiểm tra xem có bao nhiêu máy tính đang hoạt động trên mạng, tài nguyên được chia sẻ từ các máy tính đó, và tên của các nhóm làm việc trong mạng.

II. TIẾN HÀNH THỰC HÀNH:

1. Sao lưu tới ổ đĩa mạng:

- Trên máy trạm Windows attack trong mạng Internal, tạo thư mục share rồi chia sẻ qua mạng (C:\net share share=c:\share):

```
C:\>mkdir share
A subdirectory or file share already exists.

C:\>net share share=c:\share
share was shared successfully.

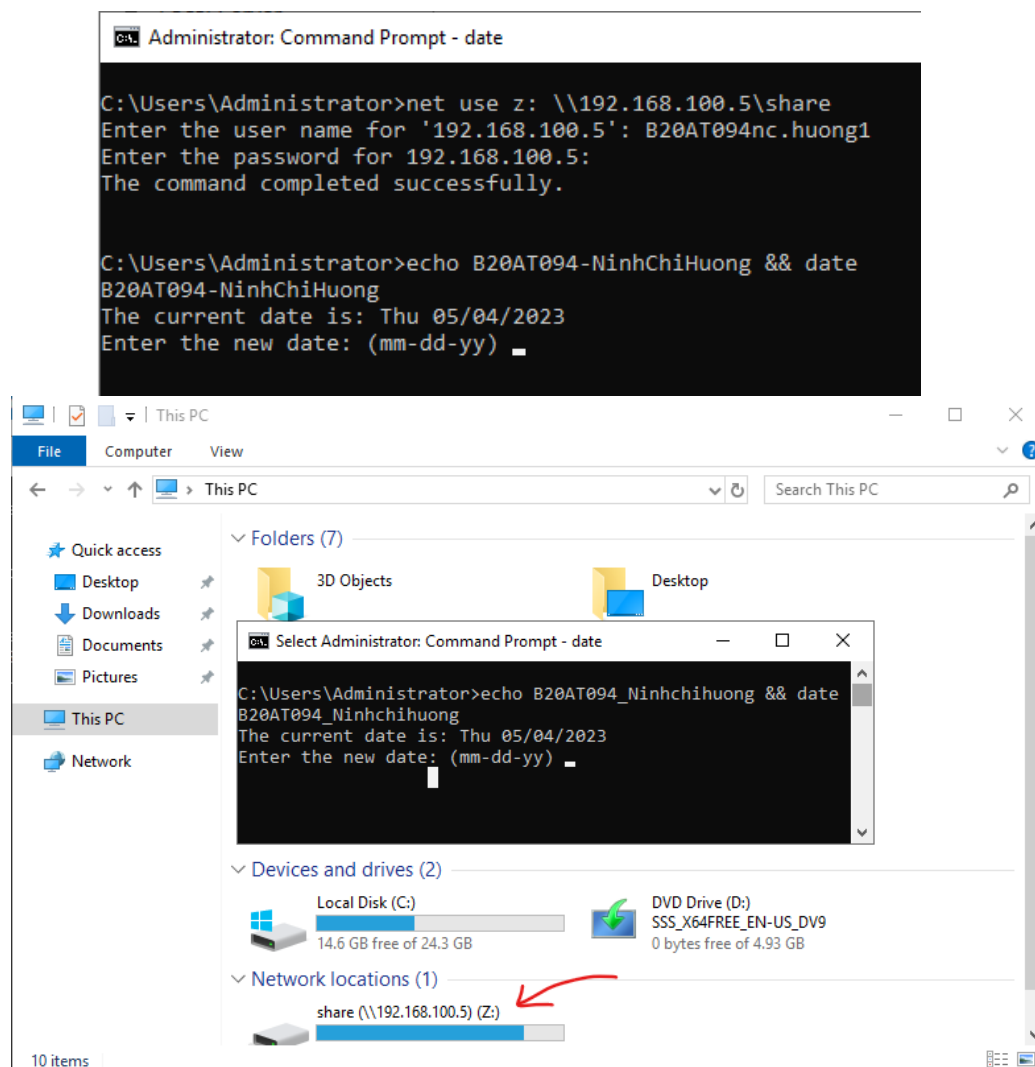
C:\>net share

Share name      Resource          Remark
-----
C$              C:\              Default share
IPC$            C:\Windows       Remote IPC
ADMIN$          C:\Windows       Remote Admin
share           c:\share
The command completed successfully.

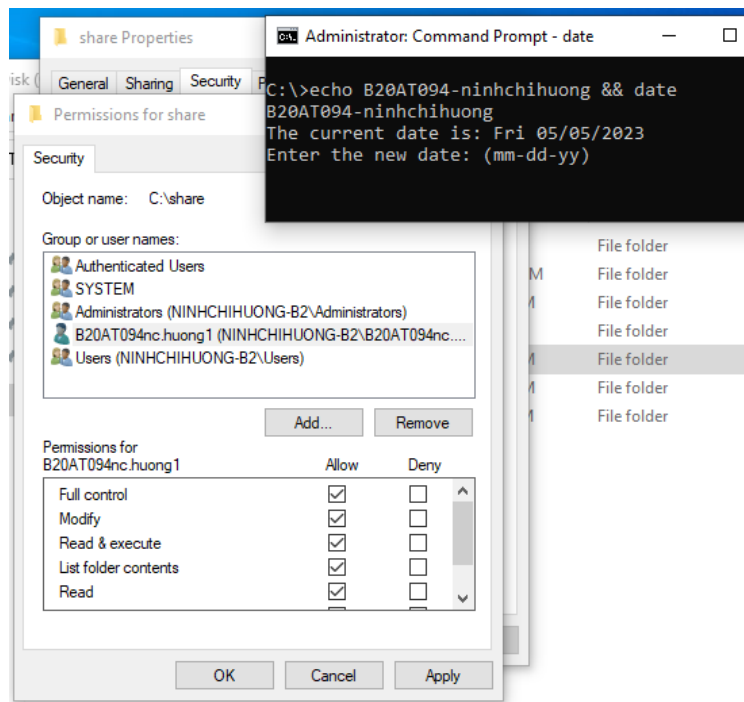
C:\>
```

```
Administrator: Command Prompt - date
C:\Windows\system32>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Thu 05/04/2023
Enter the new date: (mm-dd-yy)
```

- Trên máy Windows server ở mạng Internal, cấu hình map ổ đĩa mạng trên máy:

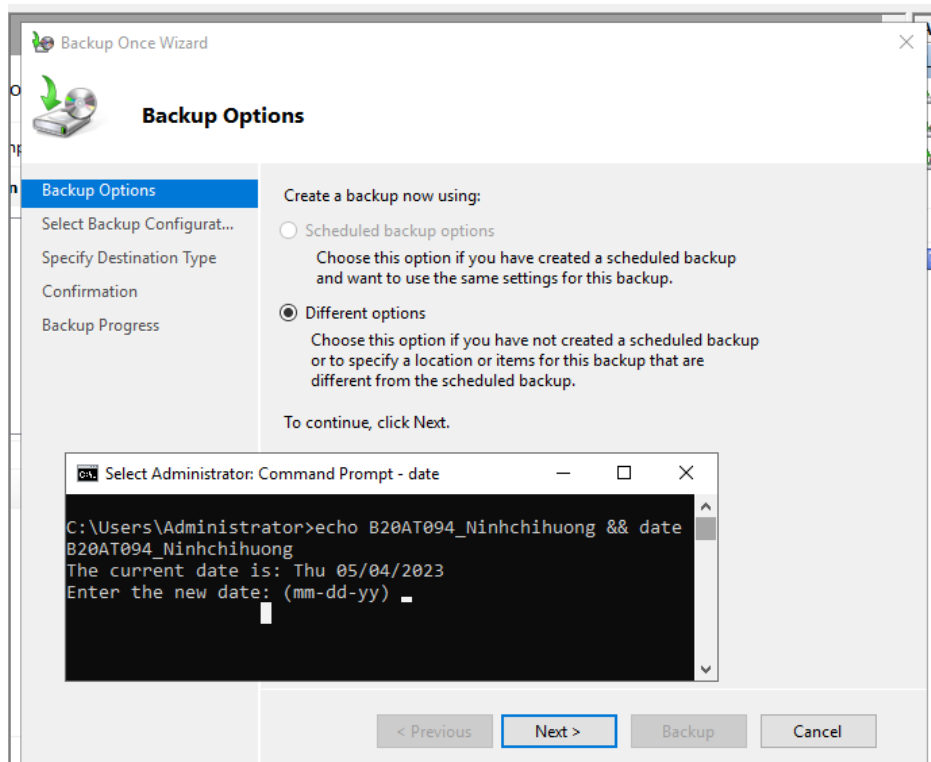


- Trên máy Windows attack trong mạng Internal, cấu hình thư mục ở đĩa mạng cho phép sao lưu tệp và thư mục từ máy khác nếu không tạo được thư mục trên máy Windows server:

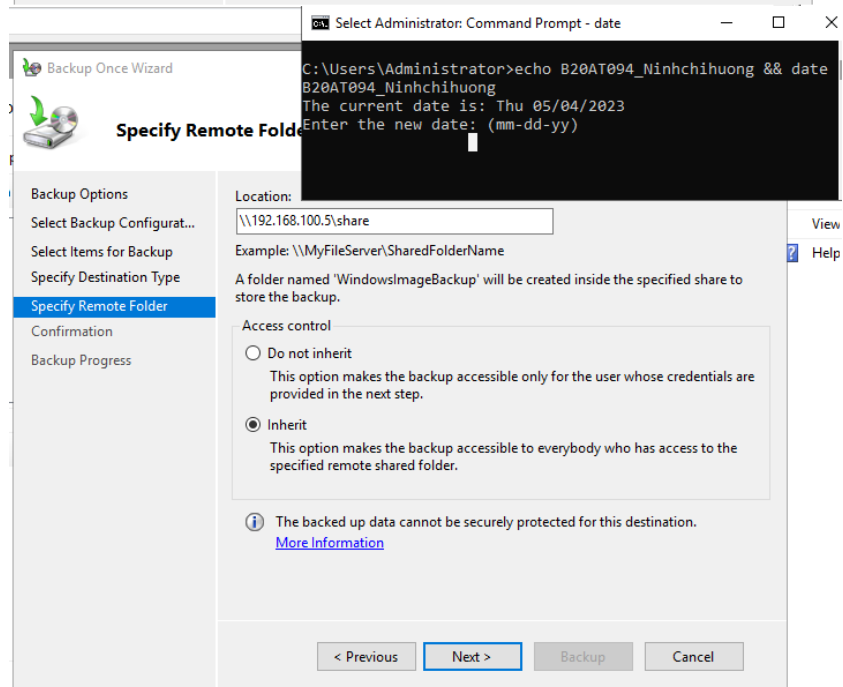
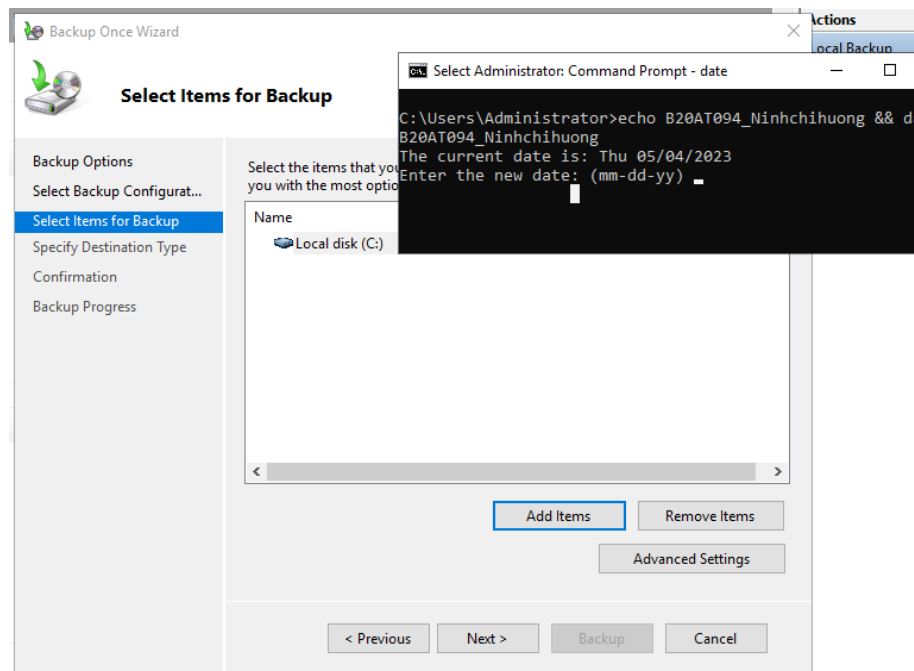


- Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2019, nếu sử dụng Win khác thì có thể download ntbackup để sử dụng), sau đó chọn 1 thư mục để sao lưu và đích là thư mục ổ mạng đã chia sẻ trên máy Windows attack trong mạng Internal:

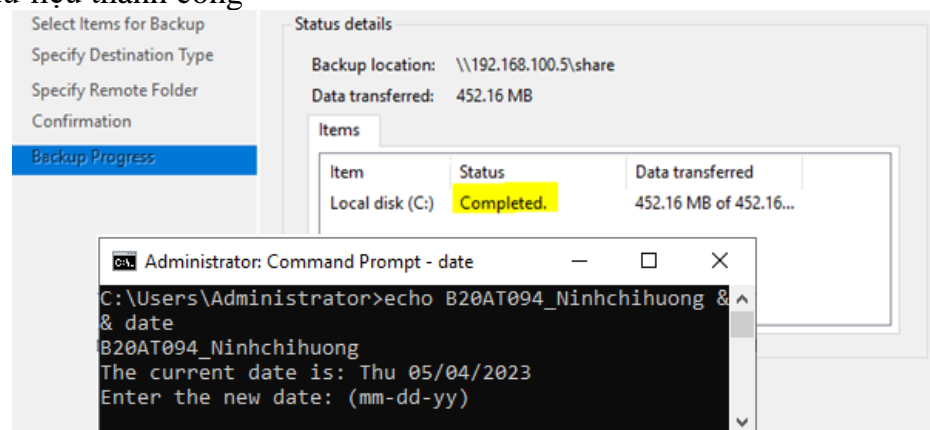
- Vào Server Manager -> Tools -> Windows Server Backup -> Chuột phải Local Backups -> Backup Once:



- Ở cửa sổ Backup Once Wizard: Different options -> Custom -> Chọn file muốn backups -> Chọn kiểu file muốn backups đến -> Chọn đường dẫn file để backups -> Backup:



Back up dữ liệu thành công



```

Administrator: Command Prompt - date

C:\>net share

Share name      Resource                Remark
-----
IPC$            C:\                    Remote IPC
C$              C:\                    Default share
ADMIN$          C:\Windows             Remote Admin
C               C:\
share           c:\share
The command completed successfully.

C:\>dir c:\share
Volume in drive C has no label.
Volume Serial Number is DE32-5BC2

Directory of c:\share

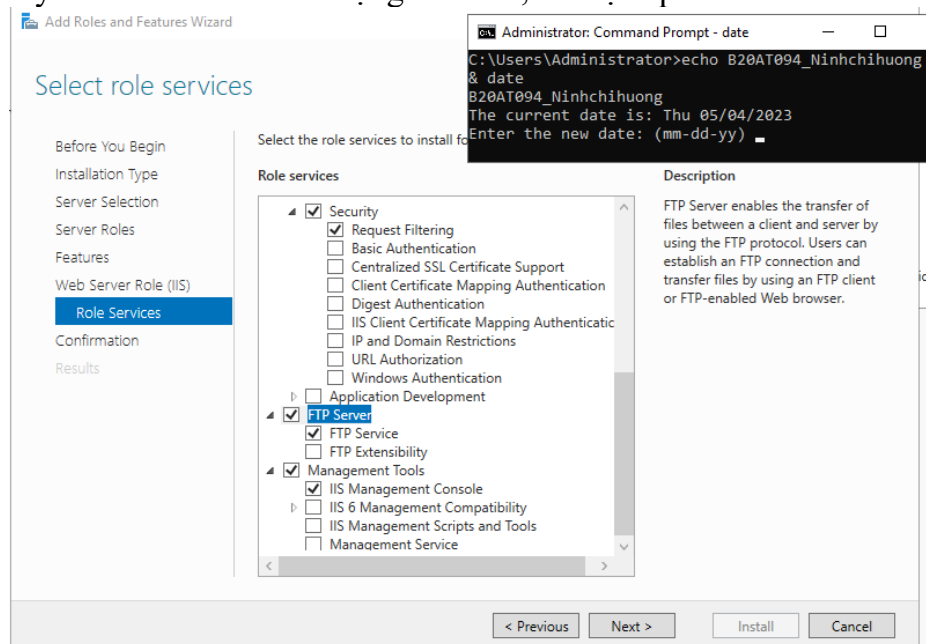
05/05/2023  04:00 PM  <DIR>          .
05/05/2023  04:00 PM  <DIR>          ..
05/05/2023  04:00 PM  <DIR>          WindowsImageBackup
                0 File(s)      0 bytes
                3 Dir(s)  5,008,310,272 bytes free

C:\>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Fri 05/05/2023
Enter the new date: (mm-dd-yy)

```

2. Sao lưu tệp lên FTP server:

- Trên máy Windows victim ở mạng Internal, cài đặt ftp client



- Trên máy Linux trong mạng Internal, cài đặt ftp server:

```

root@b20at094ninhchihuong-virtual-machine:~# apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 269 not upgraded.
Need to get 123 kB of archives.
After this operation, 326 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0ubuntu1 [123 kB]
Fetched 123 kB in 2s (52,0 kB/s)
Preconfiguring packages ...

```



```

root@b20at094ninhchihuong-virtual-machine:~# service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-05-06 09:52:27 +07; 58s ago
     Process: 224990 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
    Main PID: 224991 (vsftpd)
       Tasks: 1 (limit: 4573)
      Memory: 864.0K
         CPU: 16ms
        CGroup: /system.slice/vsftpd.service
                └─224991 /usr/sbin/vsftpd /etc/vsftpd.conf

Thg 5 06 09:52:27 b20at094ninhchihuong-virtual-machine systemd[1]: Starting vsftpd FTP server...
Thg 5 06 09:52:27 b20at094ninhchihuong-virtual-machine systemd[1]: Started vsftpd FTP server.
lines 1-13/13 (END)

```

Cấu hình tường lửa trên cả 2 máy, để cho phép dữ liệu được chuyển qua :

```

root@b20at094ninhchihuong-virtual-machine:~# ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
21/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
21/tcp (v6) ALLOW Anywhere (v6)

```

```

Administrator: Command Prompt - date
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netsh advfirewall firewall add rule name="FTP" dir=in action=allow program=%SystemRoot%\System32\ftp.exe enable=yes protocol=tcp
Ok.

C:\Users\Administrator>netsh advfirewall firewall add rule name="FTP" dir=in action=allow program=%SystemRoot%\System32\ftp.exe enable=yes protocol=udp
Ok.

C:\Users\Administrator>echo B20AT094-NinhChiHuong && date
B20AT094-NinhChiHuong
The current date is: Fri 05/05/2023
Enter the new date: (mm-dd-yy)

```

Tạo một tài khoản mới và cho phép quyền truy cập vào các tệp tin và thư mục trên hệ thống Linux được chia sẻ qua FTP:

```

b20at094-ninhchihuong@b20at094ninhchihuong-virtual-machine:~$ sudo adduser ftp_user
[sudo] password for b20at094-ninhchihuong:
Adding user `ftp_user' ...
Adding new group `ftp_user' (1004) ...
Adding new user `ftp_user' (1004) with group `ftp_user' ...
Creating home directory `/home/ftp_user' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
Changing the user information for ftp_user
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:

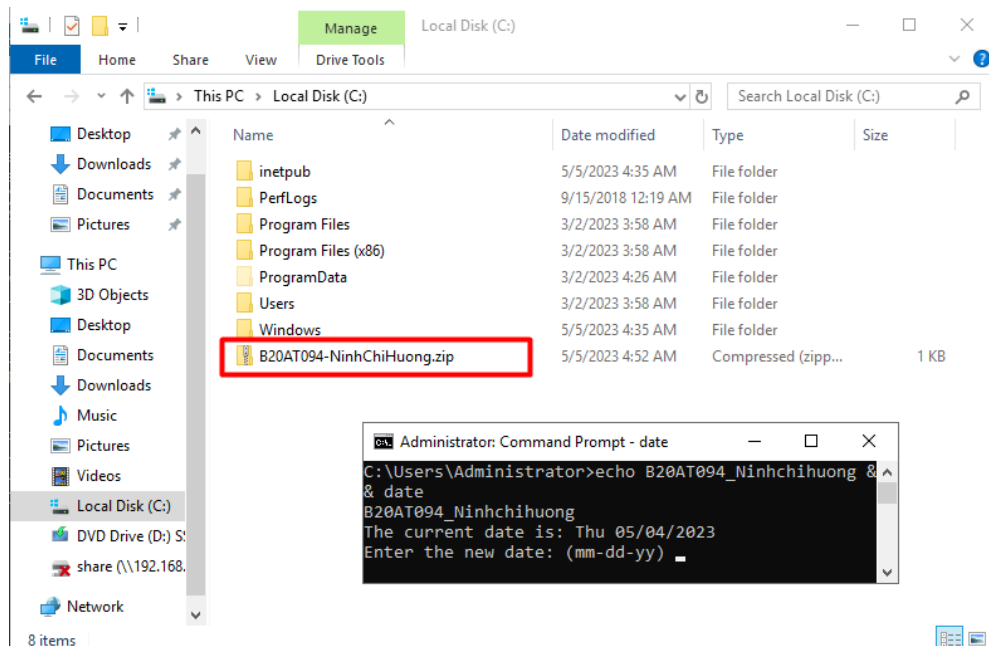
```

```

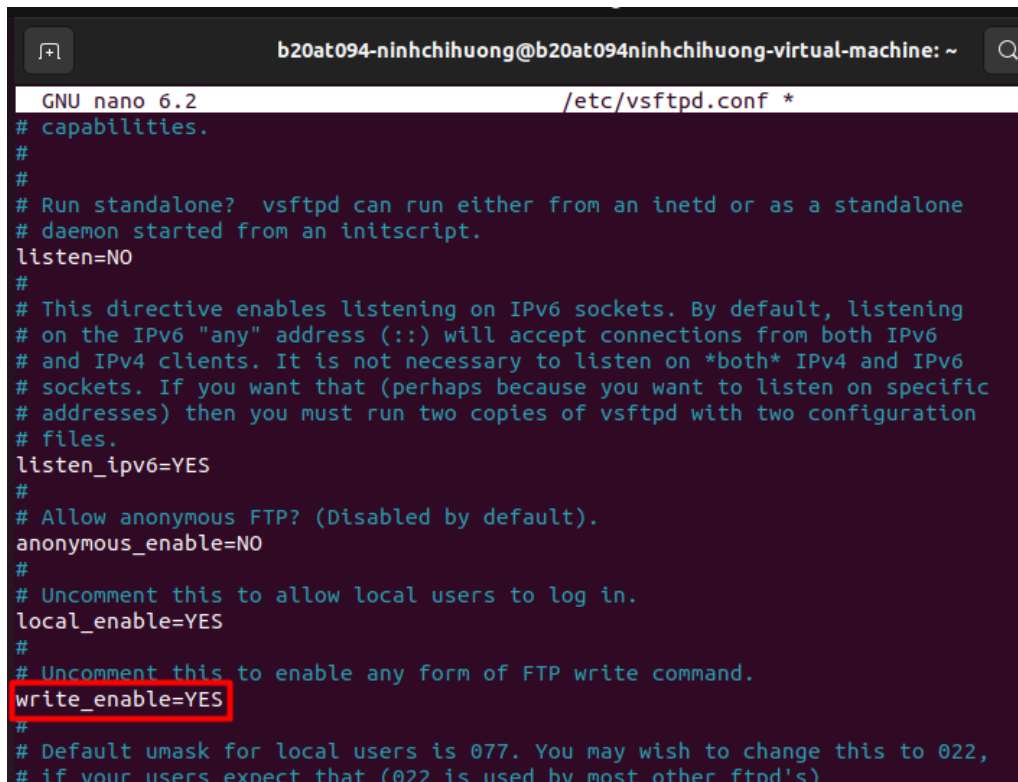
b20at094-ninhchihuong@b20at094ninhchihuong-virtual-machine:~$ sudo usermod -a -G ftp ftp_user
b20at094-ninhchihuong@b20at094ninhchihuong-virtual-machine:~$ sudo ufw allow ftp
Skipping adding existing rule
Skipping adding existing rule (v6)

```

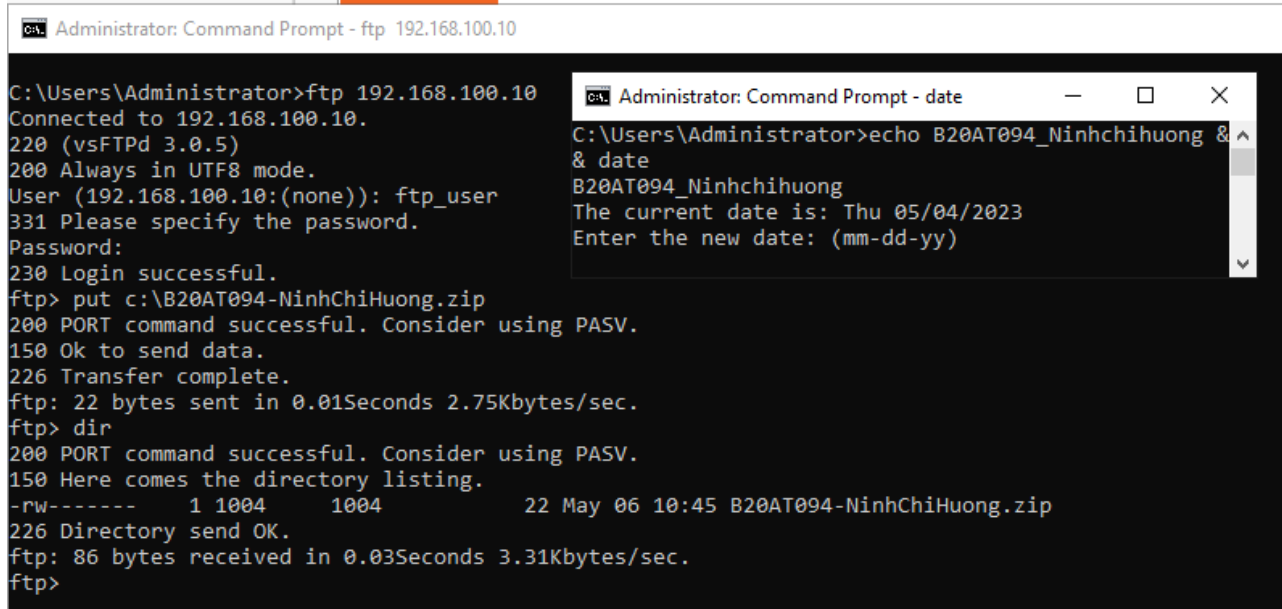
Trên máy windows, tạo một file có tên B20AT094-Ninhchihuong.zip để chia sẻ :



Trên máy Ubuntu, vào file /etc/vsftpd.conf để chỉnh sửa, nếu không khi sao lưu bên Win server sẽ gặp lỗi 550 permission denied:

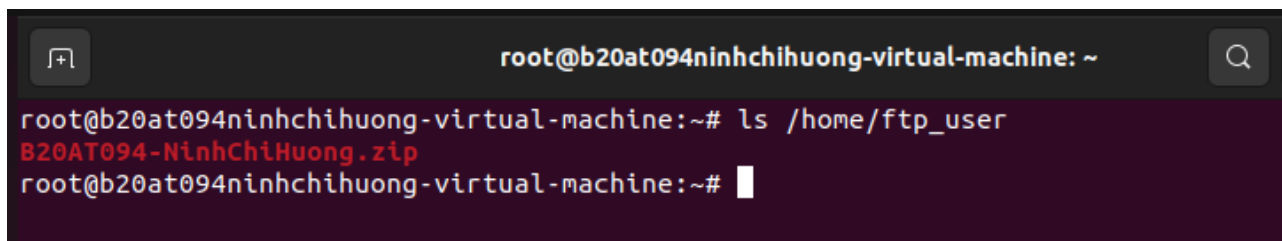


Trên máy windows, tiến hành chia sẻ file:



```
Administrator: Command Prompt - ftp 192.168.100.10
C:\Users\Administrator>ftp 192.168.100.10
Connected to 192.168.100.10.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
User (192.168.100.10:(none)): ftp_user
331 Please specify the password.
Password:
230 Login successful.
ftp> put c:\B20AT094-NinhChiHuong.zip
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 22 bytes sent in 0.01Seconds 2.75Kbytes/sec.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw----- 1 1004 1004 22 May 06 10:45 B20AT094-NinhChiHuong.zip
226 Directory send OK.
ftp: 86 bytes received in 0.03Seconds 3.31Kbytes/sec.
ftp>

Administrator: Command Prompt - date
C:\Users\Administrator>echo B20AT094_Ninhchihuong &
& date
B20AT094_Ninhchihuong
The current date is: Thu 05/04/2023
Enter the new date: (mm-dd-yy)
```

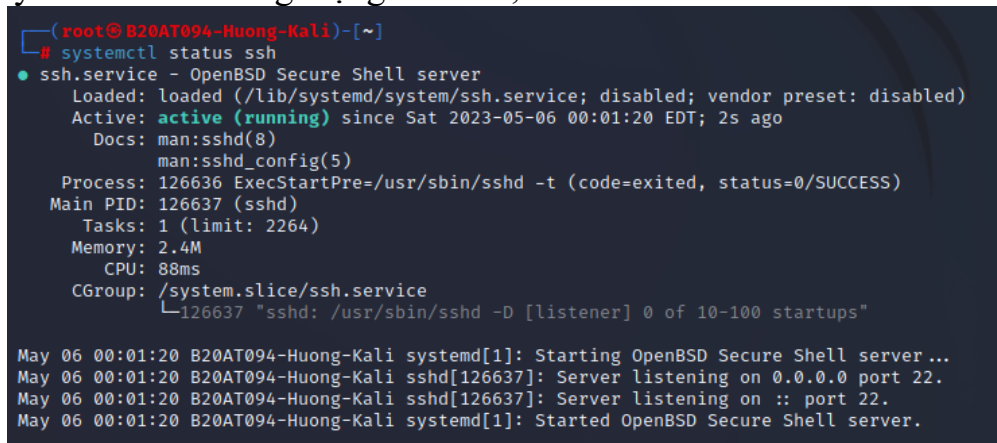


```
root@b20at094ninhchihuong-virtual-machine: ~
root@b20at094ninhchihuong-virtual-machine:~# ls /home/ftp_user
B20AT094-NinhChiHuong.zip
root@b20at094ninhchihuong-virtual-machine:~#
```

Trên máy linux, chạy lệnh ls và đã thấy file B20AT094-NinhChiHuong.zip

3. Sao lưu tệp sử dụng SCP:

- Trên máy Kali Linux trong mạng Internal, cấu hình SSH server:



```
(root@B20AT094-Huong-Kali)-[~]
# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2023-05-06 00:01:20 EDT; 2s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 126636 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 126637 (sshd)
       Tasks: 1 (limit: 2264)
      Memory: 2.4M
         CPU: 88ms
    CGroup: /system.slice/ssh.service
            └─126637 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 06 00:01:20 B20AT094-Huong-Kali systemd[1]: Starting OpenBSD Secure Shell server ...
May 06 00:01:20 B20AT094-Huong-Kali sshd[126637]: Server listening on 0.0.0.0 port 22.
May 06 00:01:20 B20AT094-Huong-Kali sshd[126637]: Server listening on :: port 22.
May 06 00:01:20 B20AT094-Huong-Kali systemd[1]: Started OpenBSD Secure Shell server.
```

Tạo Secure Shell Key trên máy Kali linux:

```
(root@B20AT094-Huong-Kali)-[~]
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): B20AT094-keygen
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in B20AT094-keygen
Your public key has been saved in B20AT094-keygen.pub
The key fingerprint is:
SHA256:ImfQbJq09Kv97AuuRp5aRc/6d1bIVKfcj3EuF+FNsMg root@B20AT094-Huong-Kali
The key's randomart image is:
+--[RSA 3072]-----+
|      ..          |
|      o +   oE+o.o|
|      . B    . o ooo|
|      . = * So .  *.|
|      ..= = . o . o +|
|      oo.=      . o  |
|      .+o = . o    |
|      .ooo+o*o o    |
+--[SHA256]-----+

(root@B20AT094-Huong-Kali)-[~]
# ls
B20AT094-keygen  B20AT094-keygen.pub  password

(root@B20AT094-Huong-Kali)-[~]
#
```

Trên máy ubuntu, tạo 2 file text lần lượt là B20AT094_Ninhchihuong1.txt và B20AT094_Ninhchihuong2.txt

```
root@b20at094ninhchihuong-virtual-machine: ~
root@b20at094ninhchihuong-virtual-machine:~# echo hello >B20AT094_Ninhchihuong1.txt
root@b20at094ninhchihuong-virtual-machine:~# echo hello >B20AT094_Ninhchihuong2.txt
root@b20at094ninhchihuong-virtual-machine:~# ls
B20AT094_Ninhchihuong1.txt  Docker_project  password.txt  rockyou.txt.1
B20AT094_Ninhchihuong2.txt  output.db      rockyou.txt   snap
root@b20at094ninhchihuong-virtual-machine:~#
```

Trên máy ubuntu, tiến hành gửi file :

```
root@b20at094ninhchihuong-virtual-machine:~# scp B20AT094_Ninhchihuong1.txt kali@192.168.100.147:/home/kali
kali@192.168.100.147's password:
B20AT094_Ninhchihuong1.txt                                100%  6    2.8KB/s   00:00
root@b20at094ninhchihuong-virtual-machine:~# scp B20AT094_Ninhchihuong2.txt kali@192.168.100.147:/home/kali
kali@192.168.100.147's password:
B20AT094_Ninhchihuong2.txt                                100%  6    2.4KB/s   00:00
root@b20at094ninhchihuong-virtual-machine:~# echo B20AT094-NINHCHIHUONG
B20AT094-NINHCHIHUONG
root@b20at094ninhchihuong-virtual-machine:~# date
Thứ bảy, 06 Tháng 5 năm 2023 11:29:49 +07
root@b20at094ninhchihuong-virtual-machine:~#
```

```
(kali@B20AT094-Huong-Kali)-[~]
$ ls
B20AT094-keygen  B20AT094_Ninhchihuong1.txt  backup  Documents  Music  Public  Videos
B20AT094-keygen.pub  B20AT094_Ninhchihuong2.txt  Desktop  Downloads  Pictures  Templates

(kali@B20AT094-Huong-Kali)-[~]
$ echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
Sat May  6 12:30:51 AM EDT 2023
```

Trên máy Kali, chạy lệnh ls và đã thấy 2 file text vừa nhận

III. Tài liệu tham khảo

https://winscp.net/eng/docs/ftp_modes#active

<https://www.hostinger.vn/huong-dan/lam-nao-de-dung-ftp-server-tren-ubuntu-vps>

<https://news.cloud365.vn/ftp-lab-phan-quyen-user-trong-ftp-server/>