

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH**  
**HỌC PHẦN: THỰC TẬP CƠ SỞ**  
**MÃ HỌC PHẦN: INT13147**

**Bài Thực Hành 1.5**

**SAO LƯU HỆ THỐNG**

Sinh viên thực hiện:  
B22DCAT206      PHẠM ĐỨC NAM

Giảng viên hướng dẫn: Đỗ Xuân Chợt

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# Mục lục

Mục lục .....	1
1. Mục đích.....	3
2. Nội dung thực hành .....	3
2.1. Cơ sở lý thuyết .....	3
2.1.1. SCP – Secure copy .....	3
2.1.2. FTP – Giao thức truyền tệp .....	3
2.1.3. Ổ đĩa mạng .....	4
2.1.4. Net use.....	5
2.1.5. Net view .....	5
2.2. Các bước thực hiện.....	6
2.2.1. Chuẩn bị môi trường .....	6
2.2.2. Sao lưu tới ổ đĩa mạng.....	7
2.2.3. Sao lưu tệp lên FTP Server.....	15
2.2.4. Sao lưu tệp sử dụng SCP .....	23
3. Kết luận .....	26
4. Tài liệu tham khảo .....	26

## Danh mục minh ảnh

Hình 1 Tạo thư mục chia sẻ file .....	8
Hình 2 Kết quả, trên Windows Server đã tồn tại ổ đĩa mạng chia sẻ .....	9
Hình 3 cài đặt window server backup.....	10
Hình 4 Cấu hình để thư mục backup lưu ở ổ đĩa mạng .....	12
Hình 5 Hoàn tất quá trình backup.....	13
Hình 6 Xuất hiện thư mục backup được lưu trên Windows Server tại ổ đĩa mạng .....	13
Hình 7 Trên Windows 10, xuất hiện thư mục backup của Windows Server tại thư mục được chia sẻ (C:\Share).....	14
Hình 8 Cài đặt FileZilla .....	15
Hình 9 Mở file /etc/netplan/01-network-manager-all.yaml và chỉnh sửa như hình sau đó netplan apply để cấu hình IP.....	16
Hình 10 Cấu hình IP thành công.....	16
Hình 11 Cài đặt ftp server.....	17
Hình 12 Sửa file /etc/vsftpd.conf như hình.....	18
Hình 13 Restart lại và bật dịch vụ ftp, kiểm tra xem đã hoạt động hay chưa .....	19
Hình 14 Kết nối đến ftp server.....	20
Hình 15 Kết quả sau khi kết nối.....	21
Hình 16 Sao lưu 1 file text trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client .....	21
Hình 17 Kiểm tra thư mục backup trong Ubuntu (Minh chứng) .....	22
Hình 18 cấu hình ip máy kali .....	23
Hình 19 Kiểm tra dịch vụ ssh đã bật hay chưa .....	24
Hình 20 Cấu hình ssh cho phép truy cập vào tài khoản root trên Kali .....	25
Hình 21 Tạo Secure Shell Keys trên máy Kali Linux .....	26
Hình 22 Kết quả, file và thư mục đã được sao lưu vào thư mục root trên máy Kali .....	26

## 1. Mục đích

Bài thực hành này giúp sinh viên tiếp thu các **công cụ** và **phương pháp phân tích log hệ thống**, tập trung vào các hình thức sao lưu dữ liệu cơ bản, bao gồm:

- Sao lưu tới ổ đĩa mạng
- Sao lưu tệp lên FTP Server
- Sao lưu tệp sử dụng SCP

## 2. Nội dung thực hành

### 2.1. Cơ sở lý thuyết

#### 2.1.1. SCP – Secure copy

**SCP (Secure Copy Protocol)** là một tiện ích được tích hợp sẵn trong các hệ thống Unix/Linux, dùng để sao chép và truyền tải các tệp tin và thư mục giữa các máy tính trong mạng. Đặc điểm nổi bật của SCP là việc sử dụng giao thức SSH (Secure Shell) để mã hóa dữ liệu trong suốt quá trình truyền tải, đảm bảo tính bảo mật và toàn vẹn của thông tin.

SCP cung cấp một cú pháp tương tự như lệnh cp (copy) trong Unix/Linux, nhưng cho phép bạn thực hiện sao chép giữa các máy tính từ xa thông qua kết nối SSH. Cú pháp cơ bản của SCP như sau:

**scp [options] source\_file destination\_file**

Trong đó:

- source\_file: là tệp tin hoặc thư mục cần sao chép.
- destination\_file: là vị trí mà bạn muốn lưu trữ tệp tin hoặc thư mục đã sao chép. Ví dụ:  
**scp /local/file.txt username@remotehost:/remote/directory/**

Lệnh này sẽ sao chép tệp tin **file.txt** từ máy local đến máy chủ **remotehost** và lưu vào thư mục **/remote/directory/**. Để đảm bảo tính bảo mật, SCP sử dụng SSH để thiết lập kết nối và mã hóa dữ liệu trong quá trình truyền tải.

#### 2.1.2. FTP – Giao thức truyền tệp

**FTP (File Transfer Protocol)** là một giao thức chuẩn dùng để **truyền tải dữ liệu** giữa máy tính và máy chủ trên mạng Internet. FTP thường được ứng dụng để **tải lên (upload)** hoặc **tải xuống (download)** các tệp tin, thư mục và dữ liệu từ hoặc đến một máy chủ.

FTP sử dụng cơ chế **xác thực người dùng** thông qua tên đăng nhập và mật khẩu. Tuy nhiên, do thông tin này không được mã hóa, FTP không được đánh giá cao về tính bảo mật khi truyền tải dữ liệu qua Internet. Để khắc phục hạn chế này, một phiên bản bảo mật hơn của FTP đã ra đời, được gọi là **FTPS (FTP Secure)** hoặc **FTP-SSL**, sử dụng SSL/TLS để mã hóa dữ liệu, tăng cường đáng kể tính bảo mật.

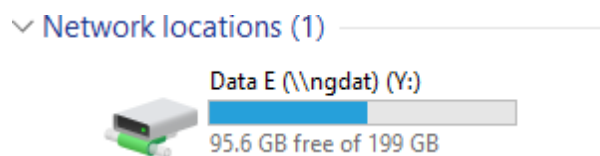
Một số đặc điểm chính của FTP bao gồm:

- **Truyền tải dữ liệu hai chiều:** FTP cho phép chuyển dữ liệu cả từ máy tính cá nhân lên máy chủ (upload) và từ máy chủ về máy tính (download).
- **Hỗ trợ đa người dùng:** Giao thức này có khả năng hỗ trợ đồng thời nhiều kết nối từ các người dùng khác nhau đến cùng một máy chủ FTP.
- **Quản lý thư mục:** Người dùng có thể thực hiện các thao tác quản lý thư mục như tạo, xóa, đổi tên và di chuyển thư mục cũng như tệp tin.
- **Thao tác tệp tin:** FTP cung cấp các lệnh để sao chép, di chuyển, đổi tên và xóa tệp tin.
- Để sử dụng FTP, người dùng cần một ứng dụng FTP client (ví dụ: FileZilla, WinSCP) để thiết lập kết nối tới máy chủ FTP và thực hiện truyền tải dữ liệu. Đồng thời, máy chủ cần được cài đặt phần mềm FTP server để cho phép người dùng kết nối và truy cập dữ liệu.

### 2.1.3. Ổ đĩa mạng

**Ổ đĩa mạng** là một thiết bị lưu trữ dữ liệu được **kết nối vào một mạng máy tính**, cho phép truy cập từ nhiều thiết bị khác nhau trong cùng mạng. Chúng thường được triển khai trong môi trường làm việc nhóm hoặc doanh nghiệp để **chia sẻ tệp và dữ liệu**. Các ổ đĩa mạng có thể được cấu hình để kiểm soát quyền truy cập, giúp người dùng dễ dàng truy cập, chỉnh sửa và chia sẻ dữ liệu một cách hiệu quả qua mạng.

**Map Network Drive (Ánh xạ ổ đĩa mạng)** là quá trình tạo một liên kết (shortcut) đến một thư mục (hoặc ổ đĩa) được chia sẻ trong mạng cục bộ. Sau khi một ổ đĩa hoặc thư mục được ánh xạ, bạn có thể truy cập các tài nguyên chia sẻ đó như thể chúng đang nằm trực tiếp trên máy tính của mình. Ổ đĩa mạng được ánh xạ có thể hiển thị như một ổ đĩa cục bộ (ví dụ: ổ C, D, E,...) trong File Explorer.



Điều này tương tự như việc tạo một shortcut cho một tệp tin ra màn hình Desktop, nhưng điểm khác biệt là nó tạo shortcut cho các tài nguyên trong mạng. Vì đây chỉ là các shortcut đến tệp tin được chia sẻ trong mạng, việc bạn ánh xạ ổ đĩa mạng không ảnh hưởng đến dung lượng ổ cứng trên máy tính hiện tại của bạn.

#### 2.1.4. Lệnh Net use

Net use là một lệnh trong hệ điều hành Windows được sử dụng để **kết nối hoặc ngắt kết nối với các tài nguyên mạng**, chẳng hạn như máy chủ, ổ đĩa mạng hoặc máy in trong cùng một mạng.

Cụ thể, lệnh này thường được dùng để **ánh xạ một đường dẫn mạng tới một ổ đĩa cục bộ**, cho phép người dùng truy cập các tài nguyên mạng như thể chúng là các ổ đĩa trên máy tính của mình.

Cú pháp cơ bản của lệnh net use như sau:

**net use [drive\_letter:] \\computer\_name\share\_name [/persistent:{yes | no}]**

Trong đó:

- **[drive\_letter:]** là chữ cái dùng để định danh cho ổ đĩa được ánh xạ tới tài nguyên mạng.
- **\\computer\_name\share\_name** là đường dẫn tới tài nguyên mạng muốn kết nối.
- **/persistent:{yes | no}** là tùy chọn để xác định liệu kết nối mạng này có được duy trì sau khi hệ thống khởi động lại hay không.

Ví dụ:

**net use Z: \\file\_server\shared\_folder /persistent:yes**

- Lệnh này sẽ ánh xạ tài nguyên mạng **\\file\_server\shared\_folder** tới ổ đĩa **Z:** trên máy tính của bạn và lưu kết nối này lại sau khi bạn khởi động lại hệ thống.

#### 2.1.5. Lệnh Net view

Net view là một lệnh khác trong hệ điều hành Windows, được sử dụng để hiển thị danh sách các tài nguyên chia sẻ trên mạng mà máy tính hiện tại có thể truy cập.

Cụ thể, lệnh này sẽ liệt kê các máy chủ, máy tính và các tài nguyên mạng khác đang có sẵn trên mạng cục bộ (local network).

Cú pháp cơ bản của lệnh `net view` là:

**net view [\\computer\_name]**

- Nếu không chỉ định **`computer\_name`**, lệnh sẽ hiển thị tất cả các tài nguyên mạng có sẵn trên mạng local.
- Nếu chỉ định **`computer\_name`**, lệnh sẽ hiển thị danh sách các tài nguyên chia sẻ trên máy tính có tên là **`computer\_name`**.

Ví dụ:

- net view: Lệnh này sẽ hiển thị danh sách các tài nguyên mạng có sẵn trên mạng cục bộ của máy tính hiện tại.
- net view \\file\_server: Lệnh này sẽ hiển thị danh sách các tài nguyên mạng chia sẻ trên máy

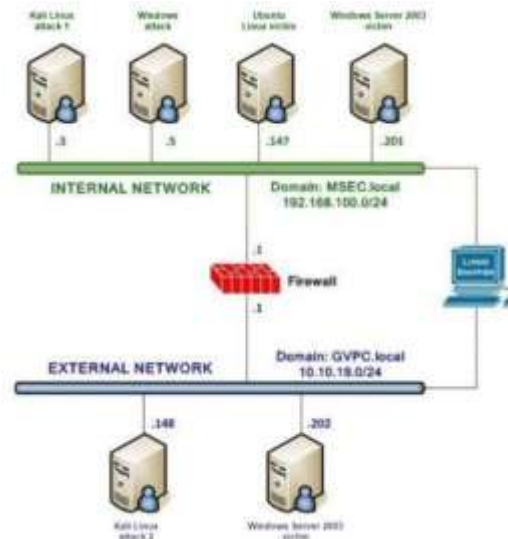
chủ có tên là **file\_server**.

## **2.2.** Các bước thực hiện

### **2.2.1.** Chuẩn bị môi trường

- Phần mềm VMWare Workstation( hoặc các phần mềm hỗ trợ ảo hóa khác).

- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
- Topo mạng như đã cấu hình trong bài 5.

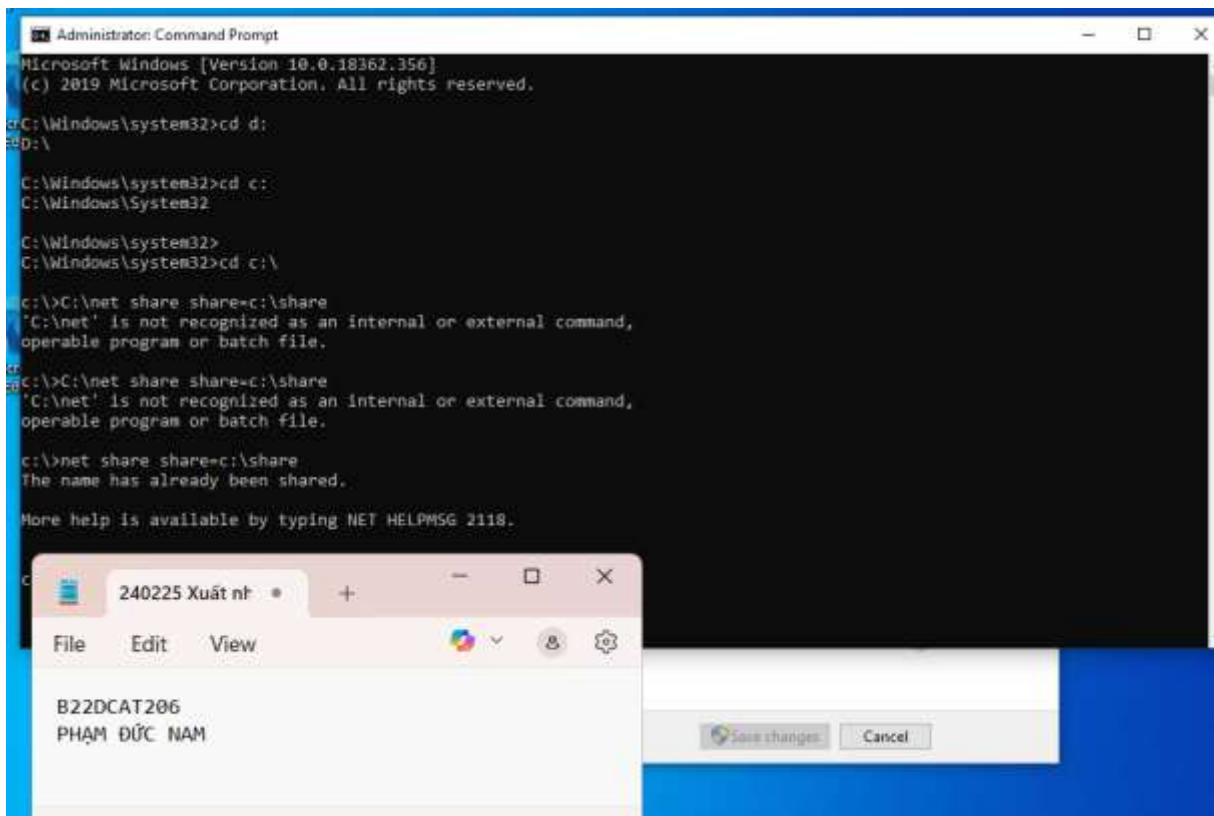


*Cấu hình topo mạng*

### 2.2.2. Sao lưu tới ổ đĩa mạng

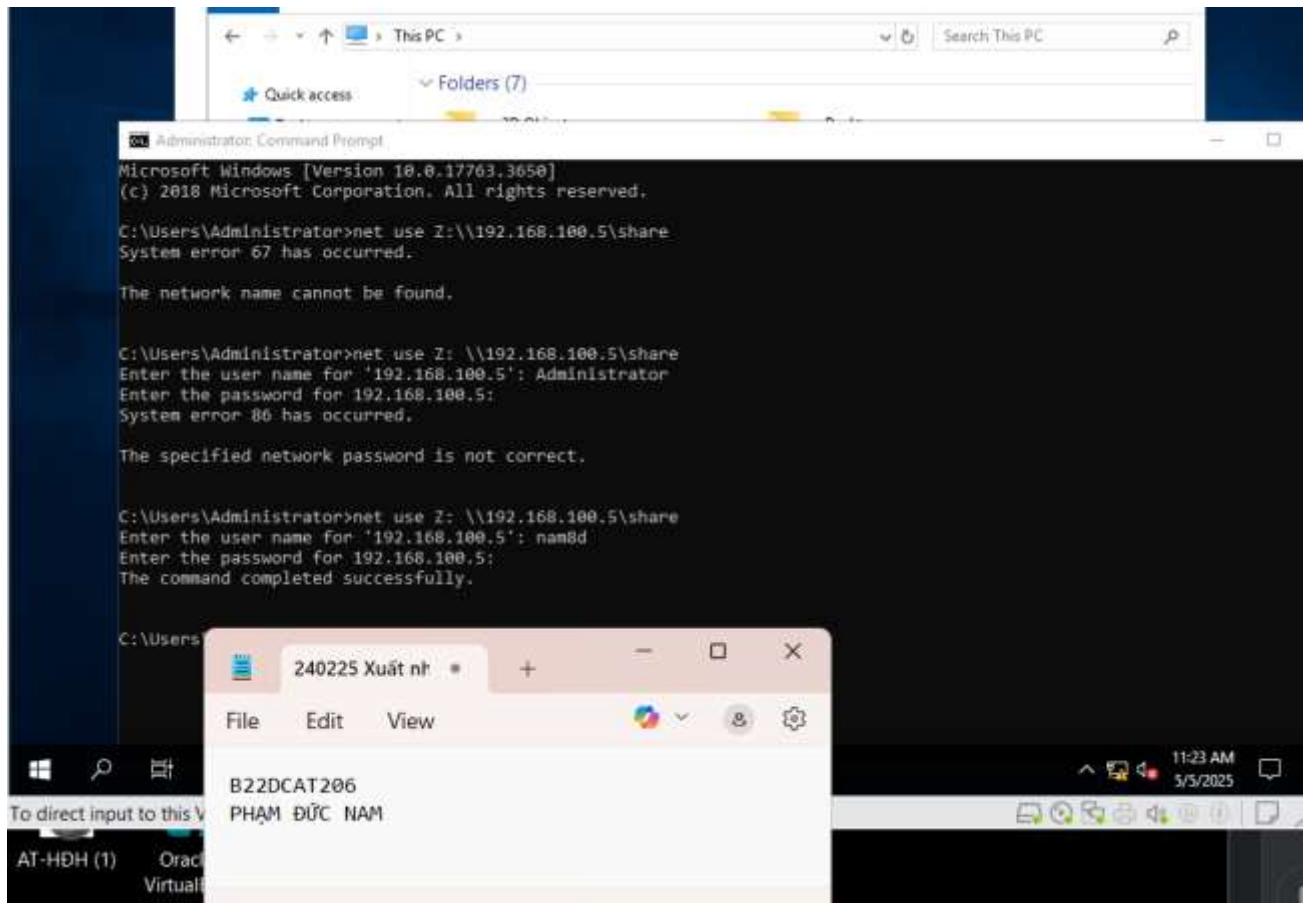
- Trên máy trạm Windows attack trong mạng Internal, tạo thư mục share rồi chia sẻ qua mạng (C:\net share share=c:\share)



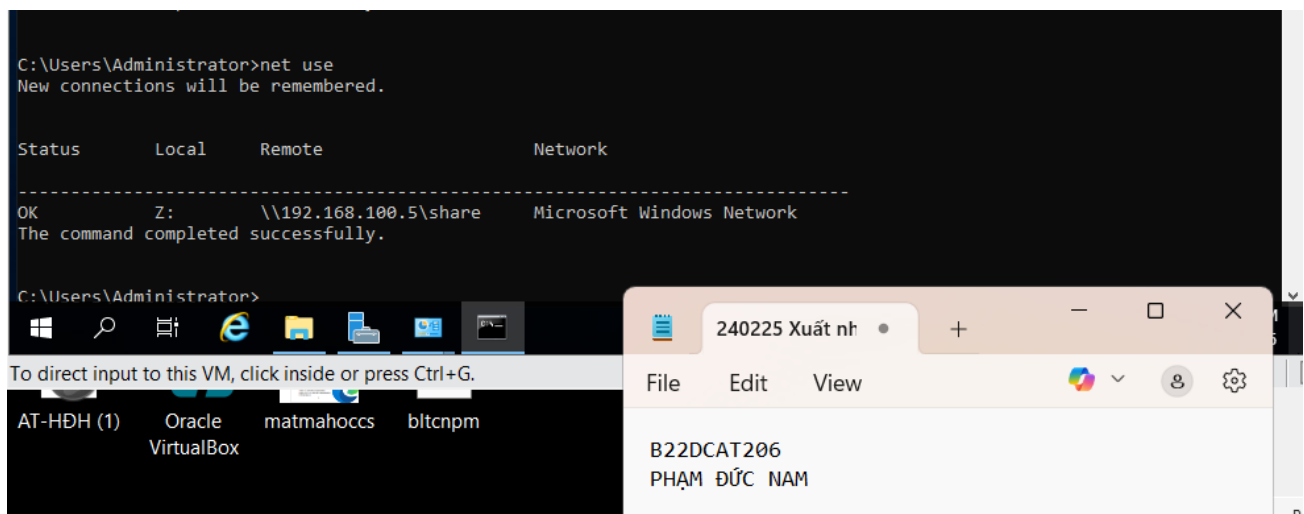


Hình 1 Tạo thư mục chia sẻ file

- Trên máy Windows server ở mạng Internal, cấu hình map ổ đĩa mạng trên máy:  
Vào File Explore -> This PC -> Computer -> Map Network Driver.

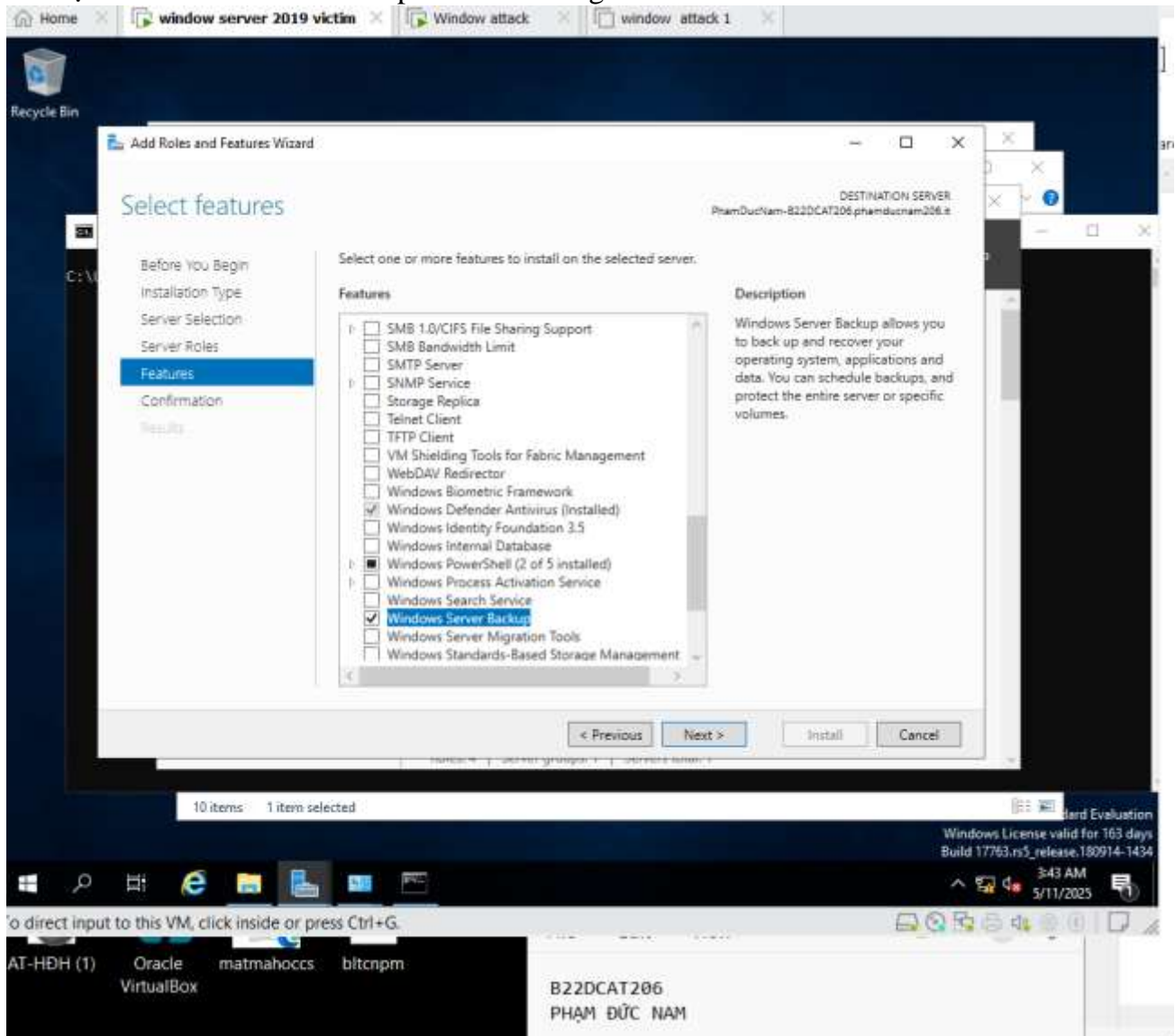


### *Cấu hình Map Network Driver*



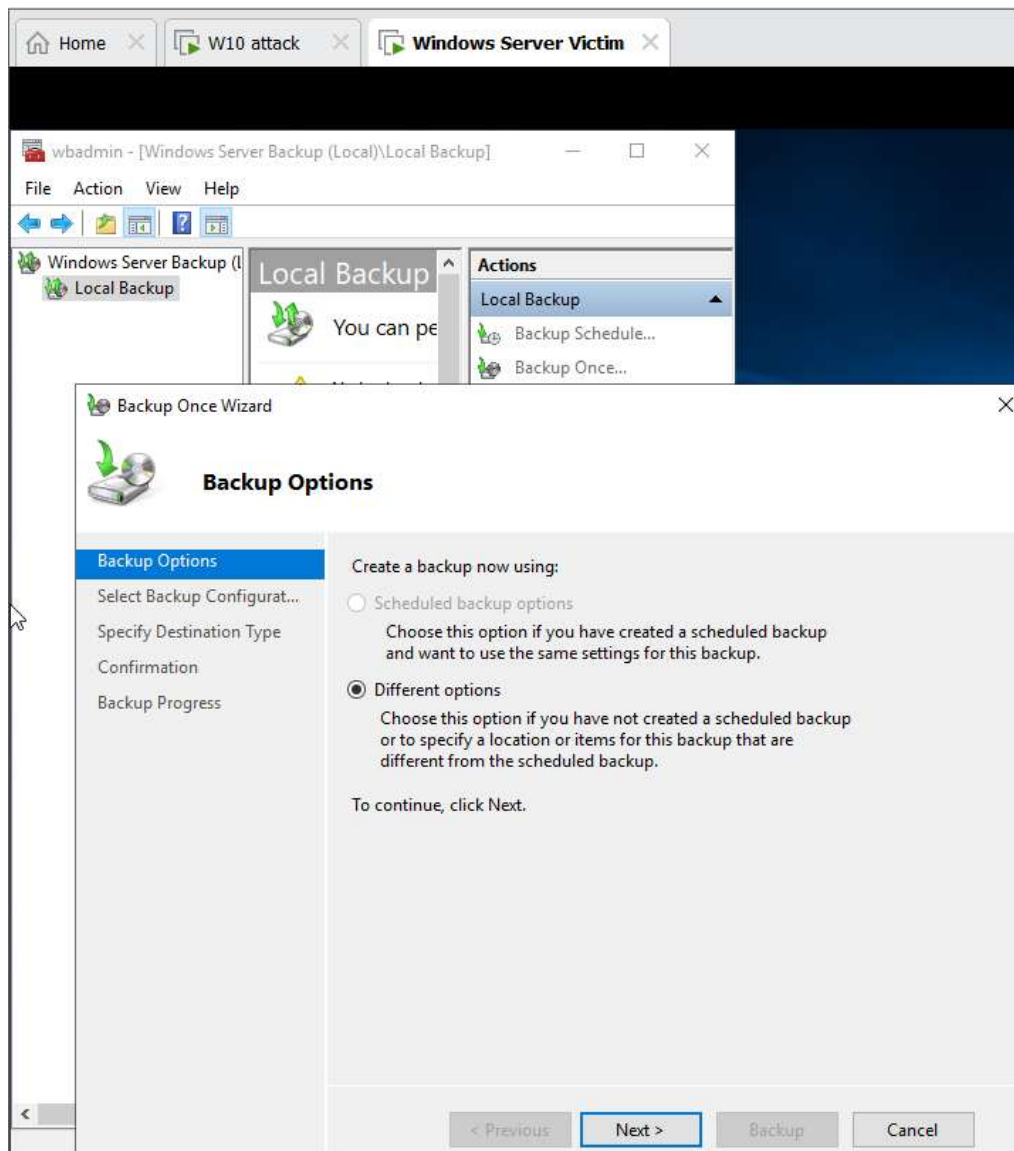
*Hình 2 Kết quả, trên Windows Server đã tồn tại ổ đĩa mạng chia sẻ*

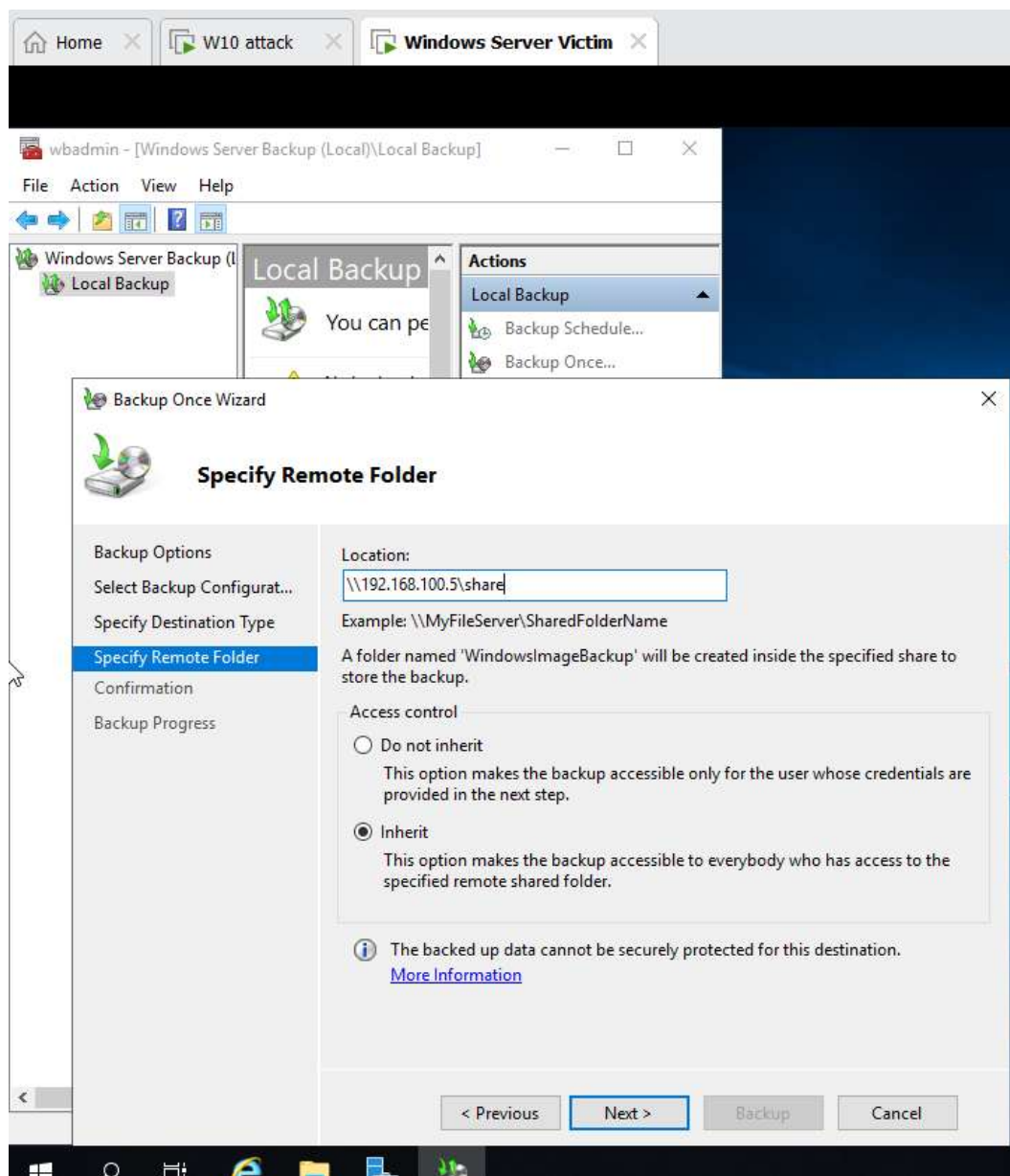
- Trên máy Windows attack trong mạng Internal, cấu hình thư mục ở đĩa mạng cho phép sao lưu tệp và thư mục từ máy khác nếu không tạo được thư mục trên máy Windows server
  - Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2003, 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.
- + Cài đặt Windows Server Backup: Server Manager → Add Roles and Features



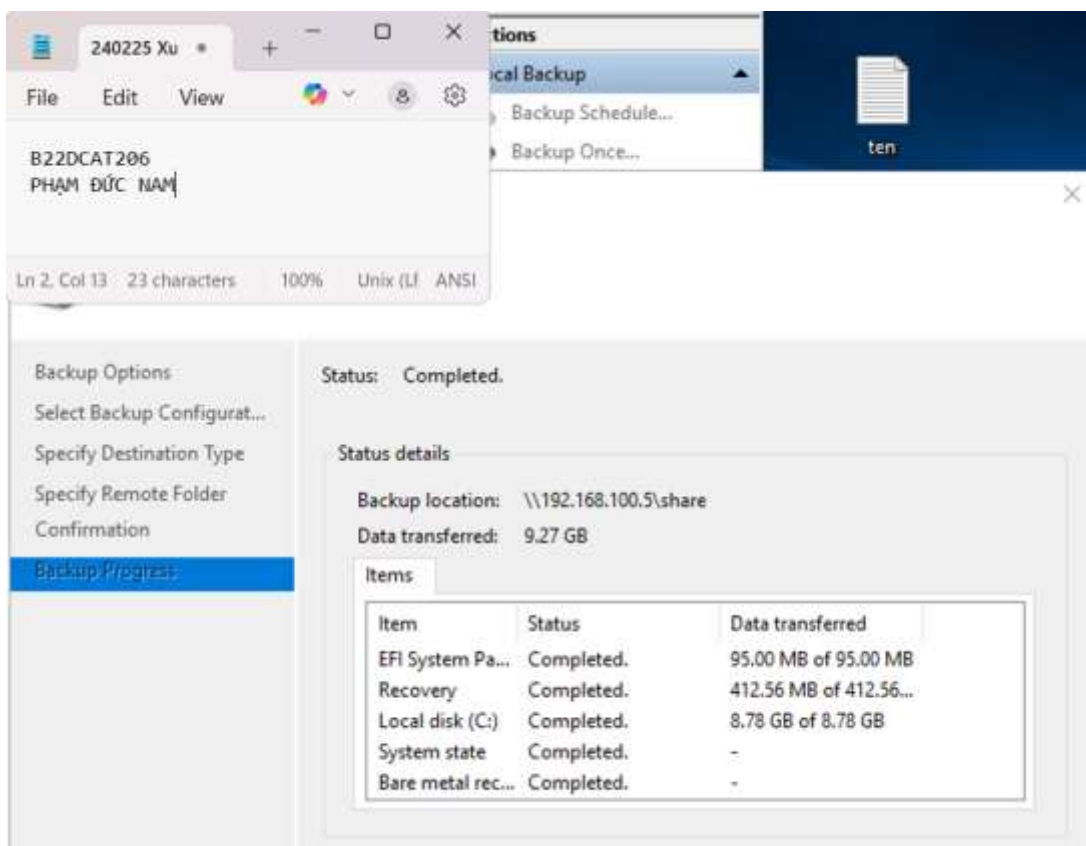
Hình 3 cài đặt window server backup

- + Sau khi đã cài xong, tiến hành backup: Server Manager → Tools → Windows Server Backup

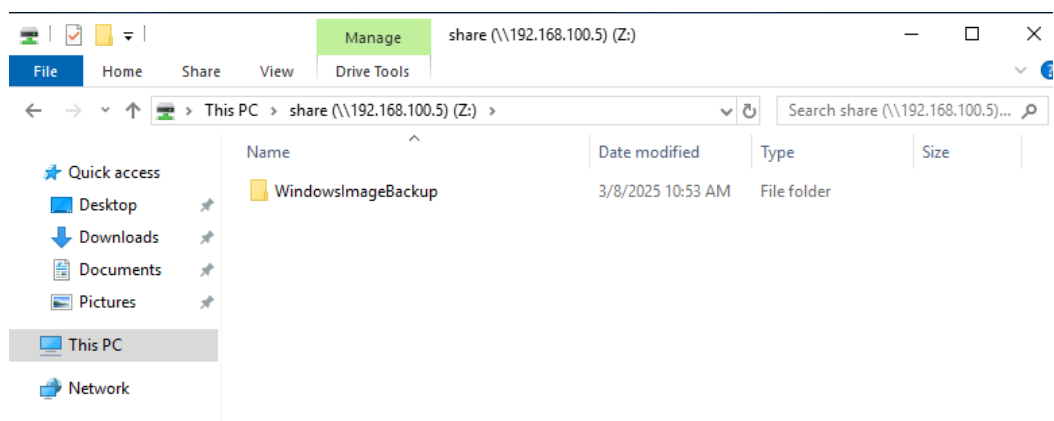




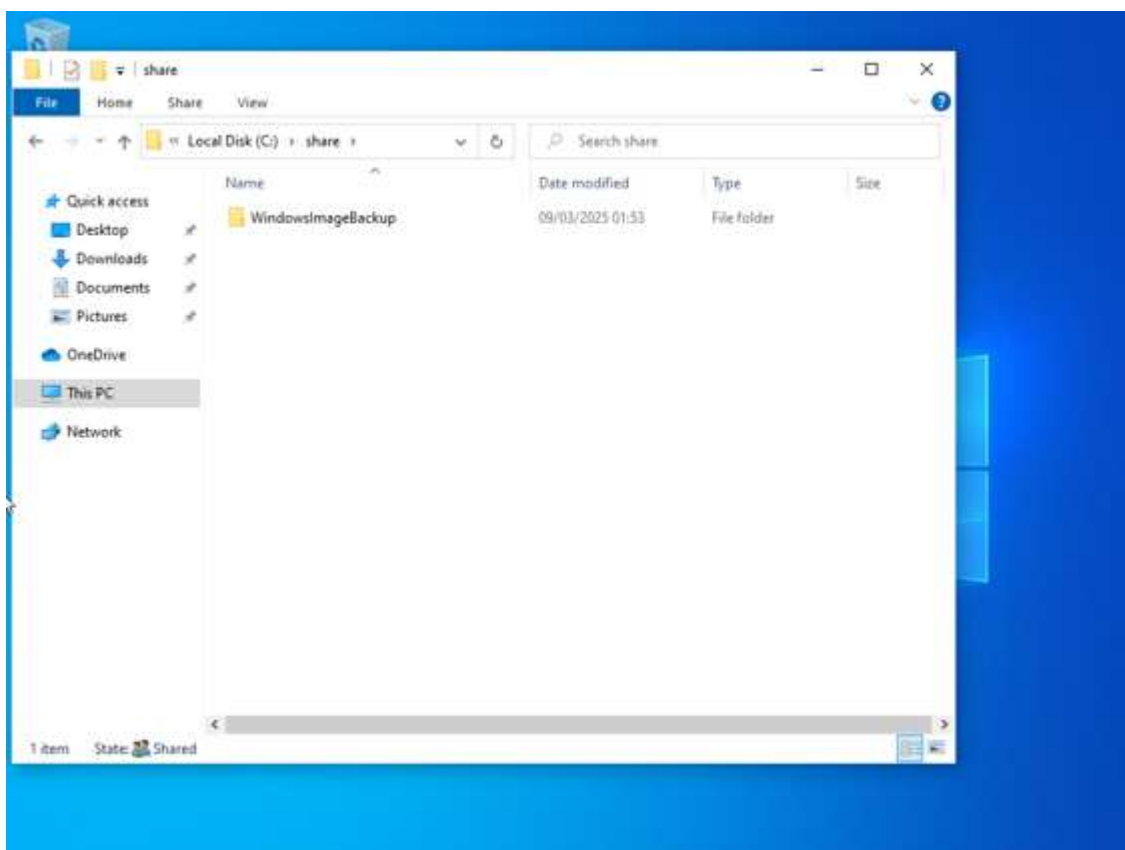
Hình 4 Cấu hình để thư mục backup lưu ở ổ đĩa mạng



Hình 5 Hoàn tất quá trình backup



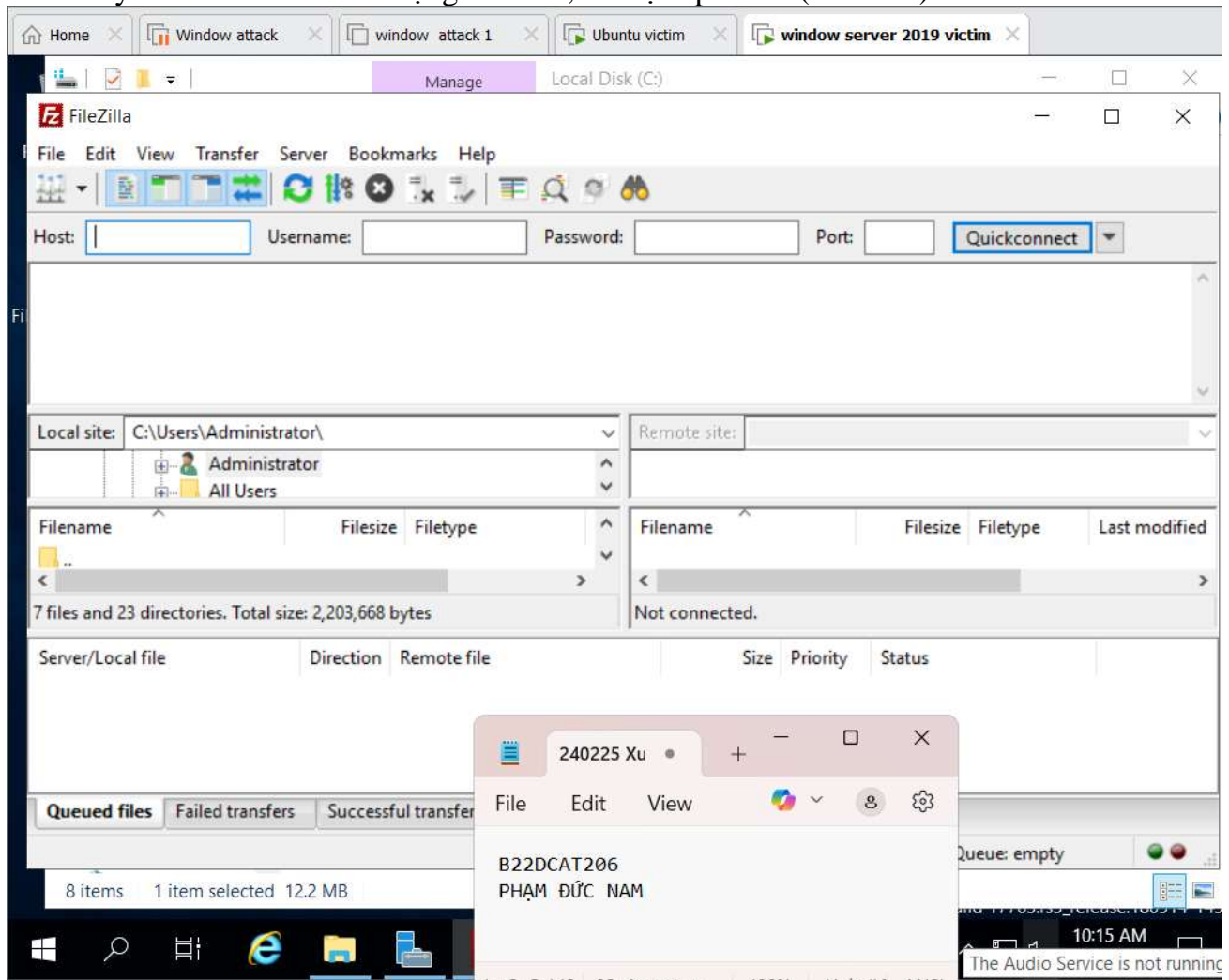
Hình 6 Xuất hiện thư mục backup được lưu trên Windows Server tại ổ đĩa mạng



Hình 7 Trên Windows 10, xuất hiện thư mục backup của Windows Server tại thư mục được chia sẻ (C:\Share)

### 2.2.3. Sao lưu tệp lên FTP Server

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



Hình 8 Cài đặt FileZilla

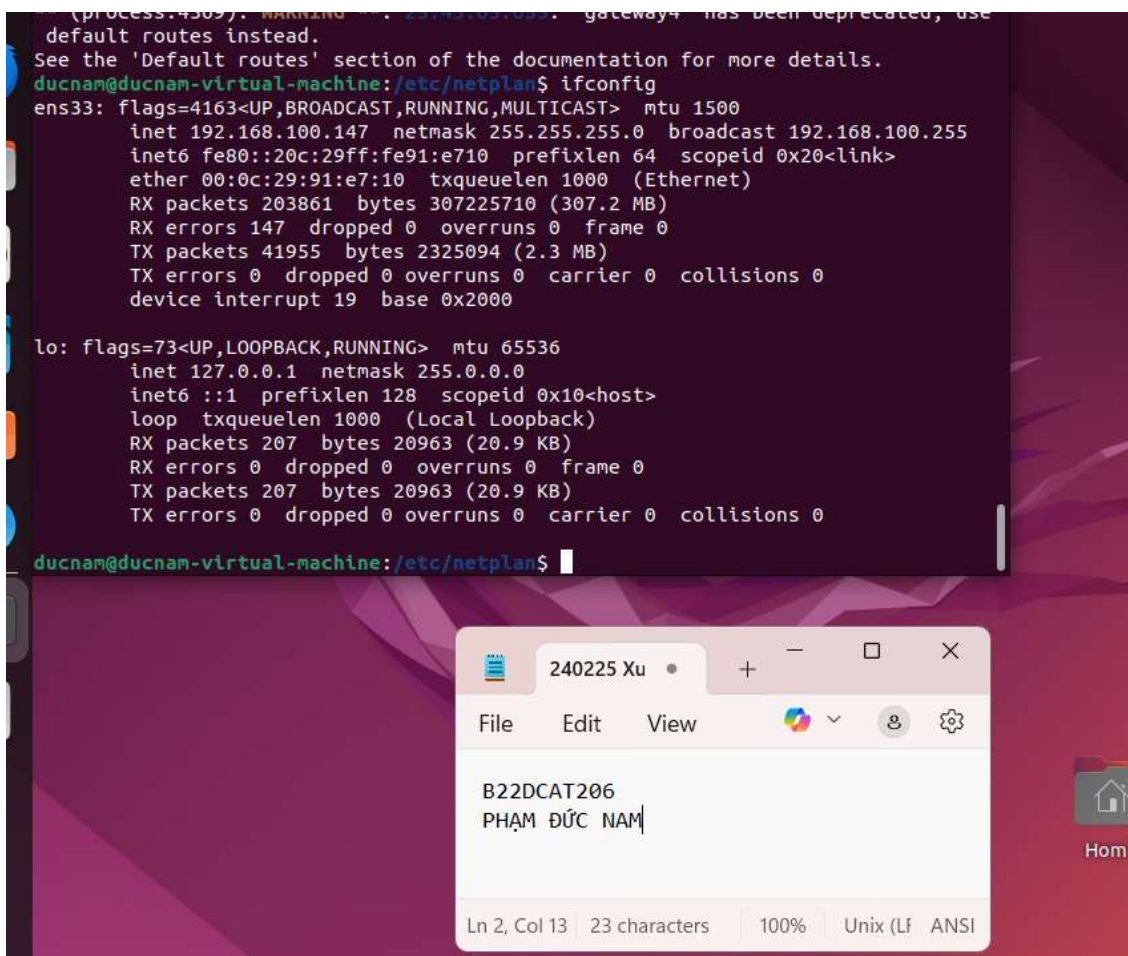
- Trên máy Linux trong mạng Internal, cài đặt ftp server



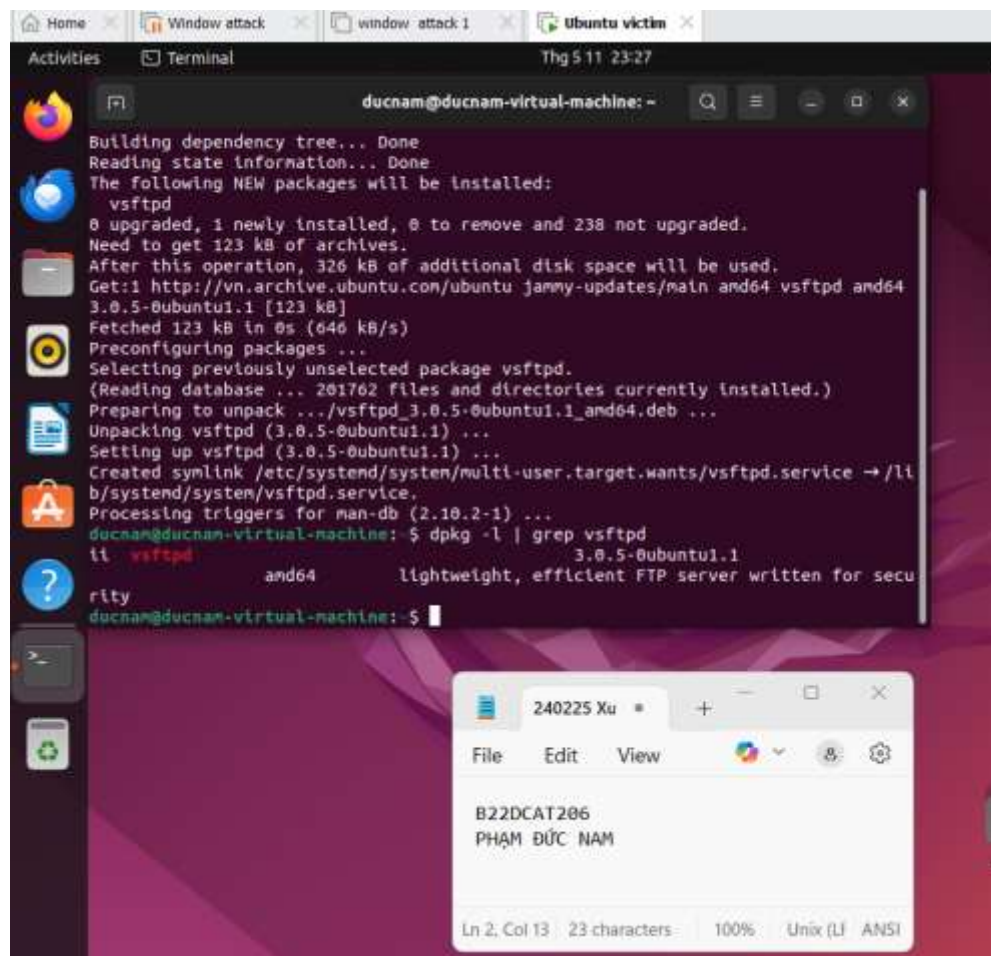
```
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml *
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.100.147/24
      gateway4: 192.168.100.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

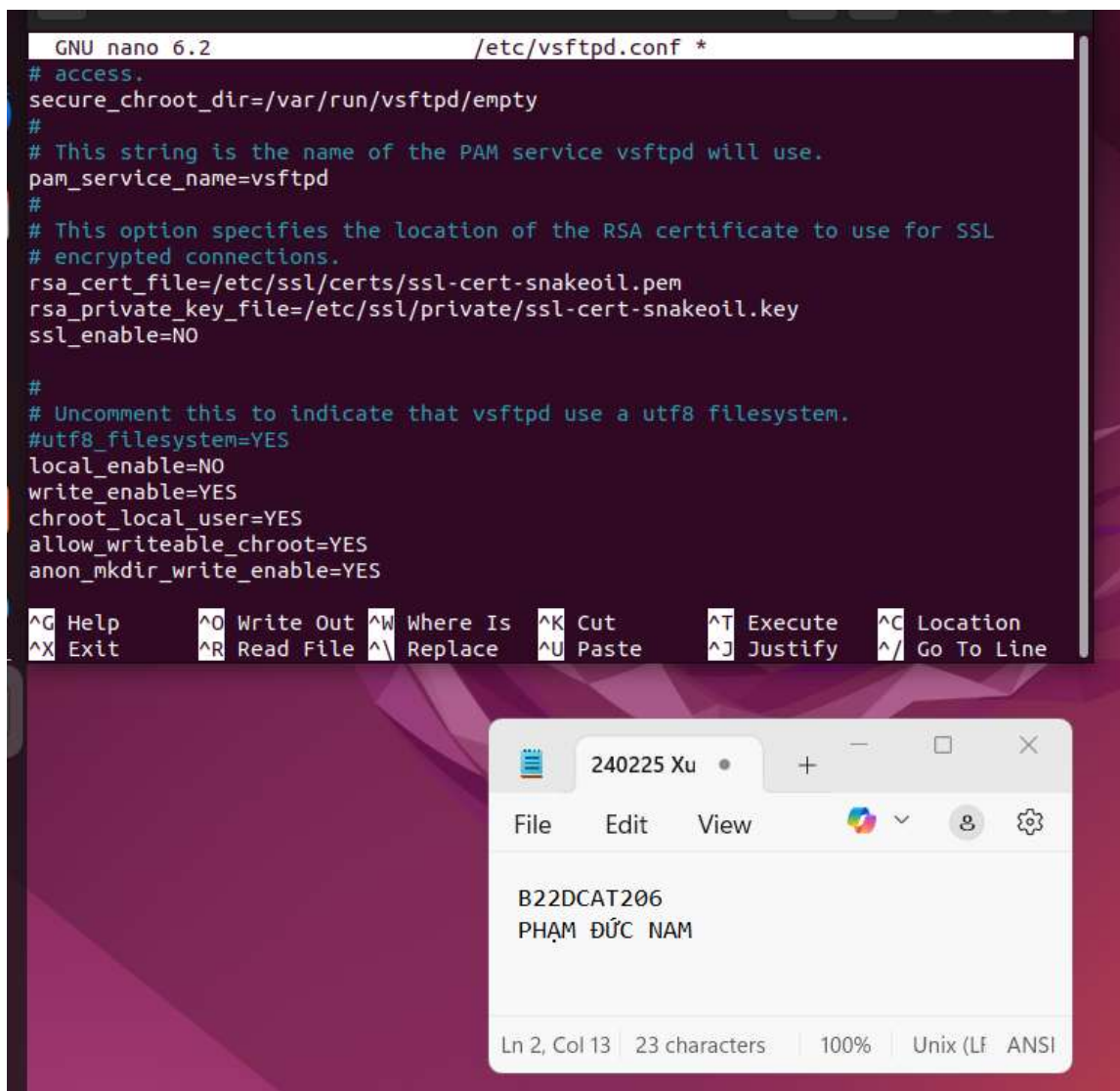
Hình 9 Mở file /etc/netplan/01-network-manager-all.yaml và chỉnh sửa như hình sau đó netplan apply để cấu hình IP



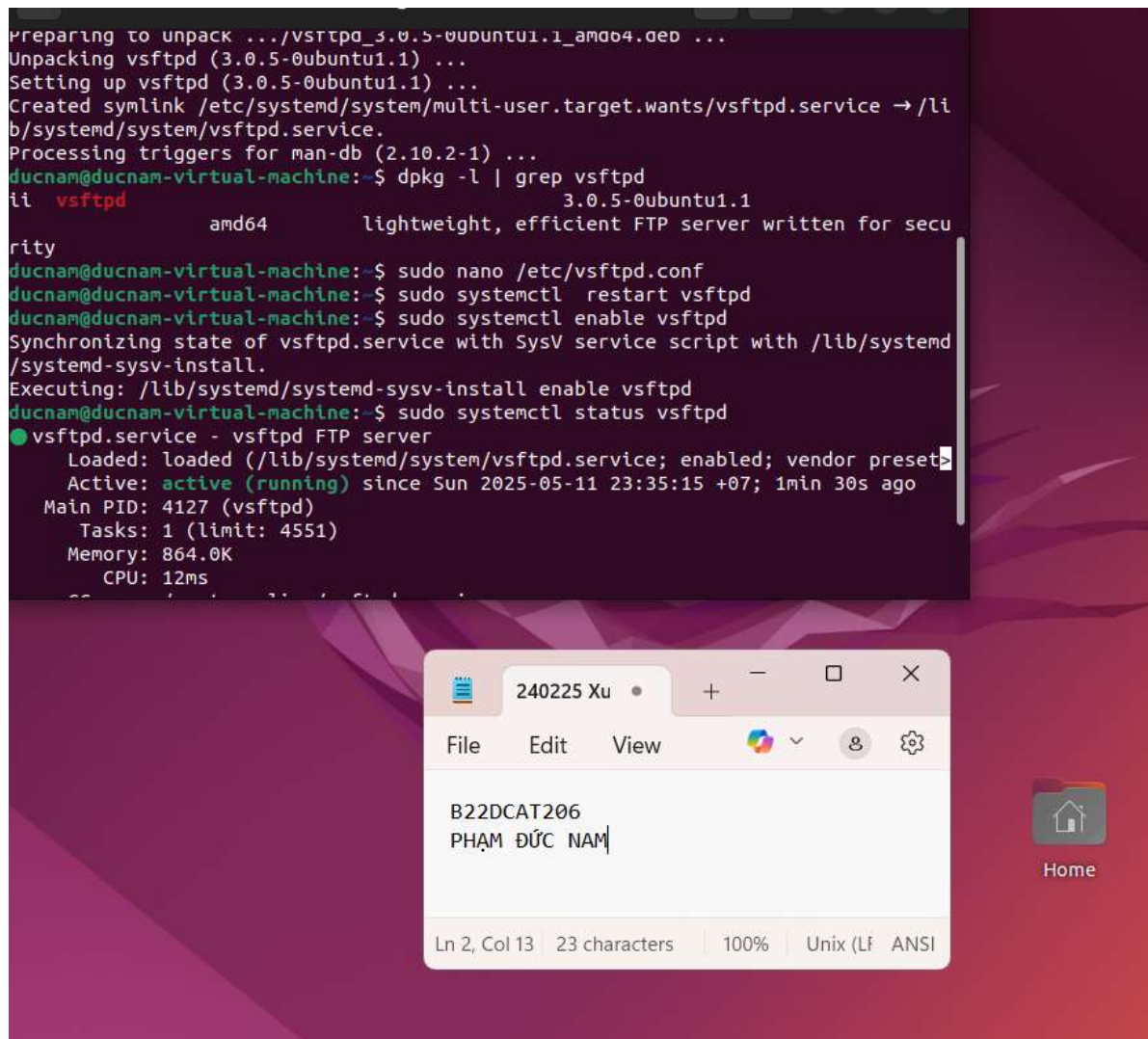
Hình 10 Cấu hình IP thành công



Hình 11 Cài đặt ftp server



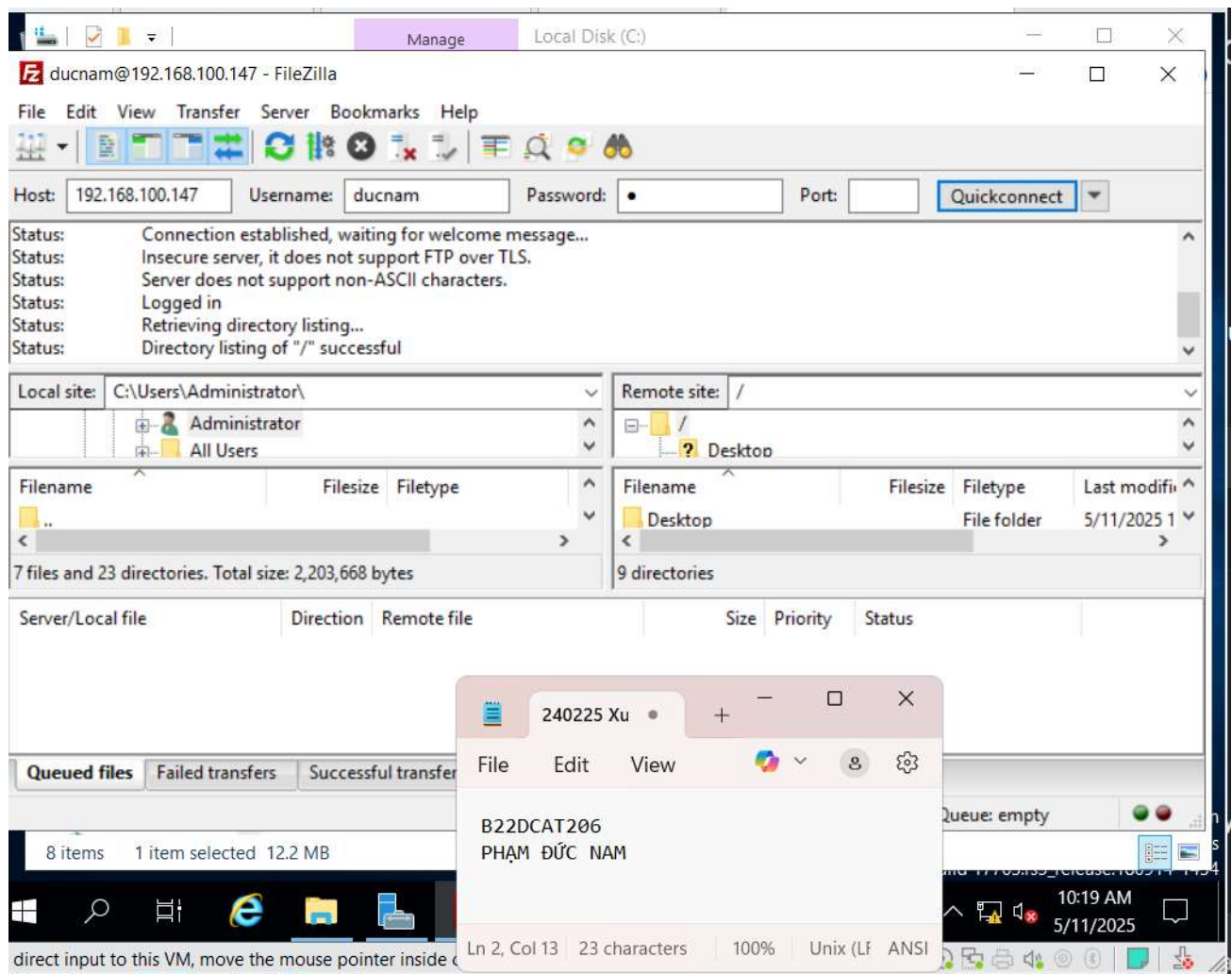
Hình 12 Sửa file /etc/vsftpd.conf như hình



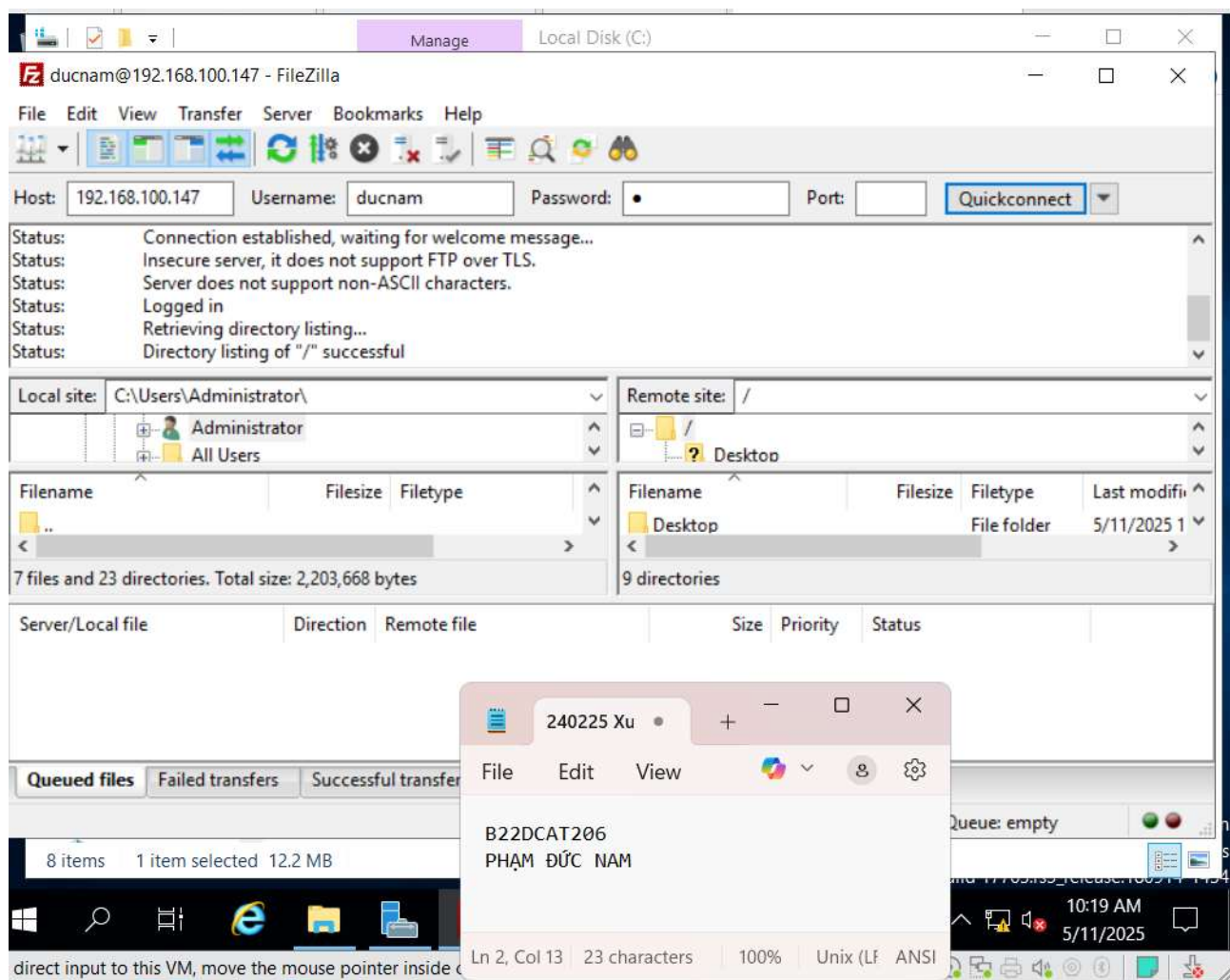
Hình 13 Restart lại và bật dịch vụ ftp, kiểm tra xem đã hoạt động hay chưa

- Sao lưu 1 thư mục trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client, sau khi kết nối tới ftp server
- + Tạo thư mục /home/truongtuan\_b22at270/backup trong ubuntu

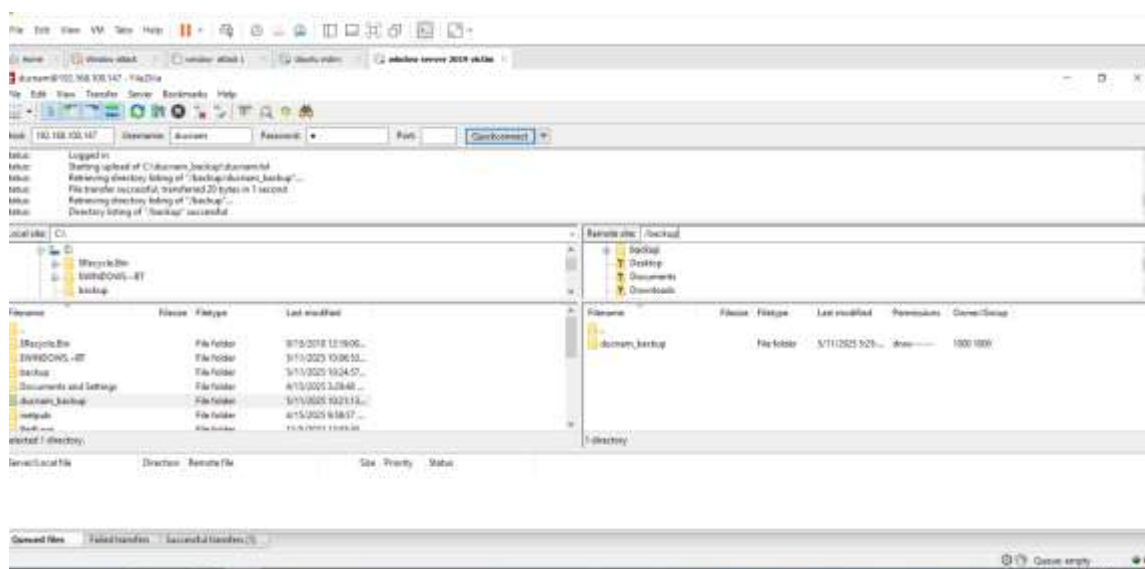




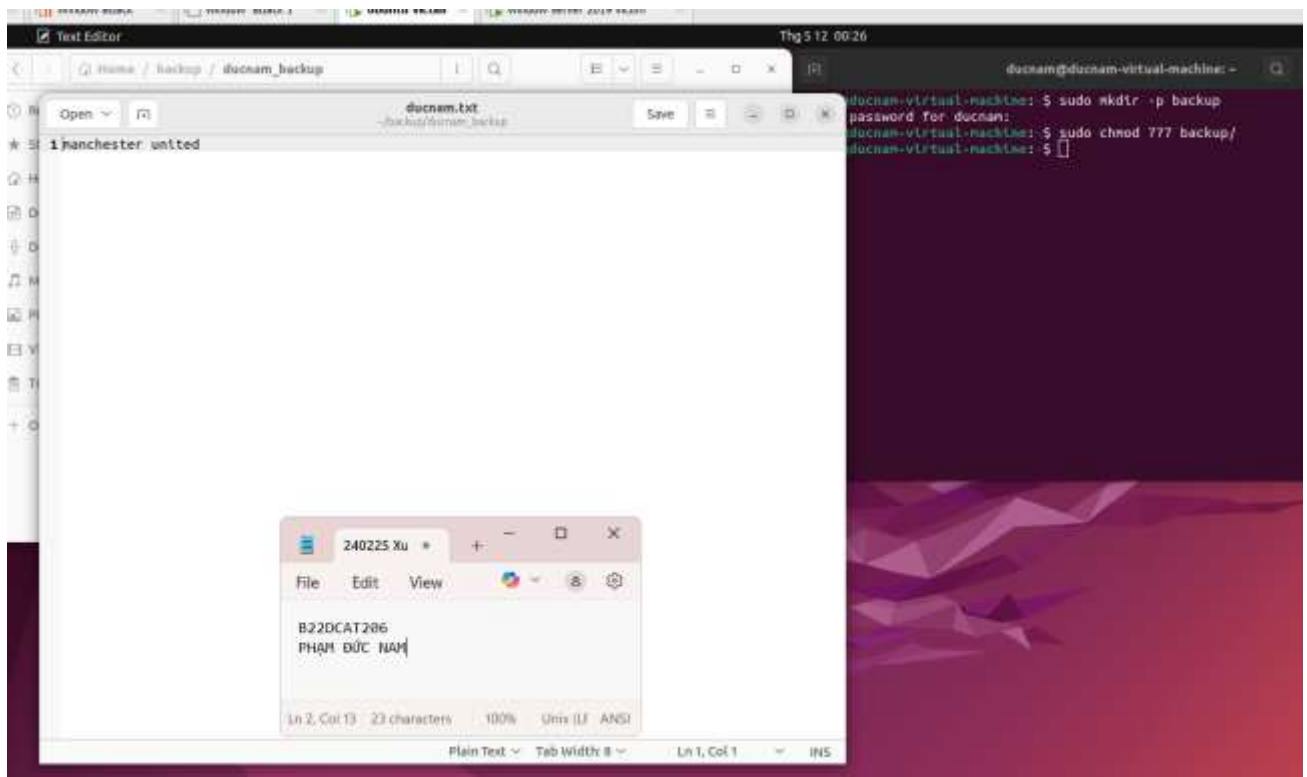
Hình 14 Kết nối đến ftp server



Hình 15 Kết quả sau khi kết nối



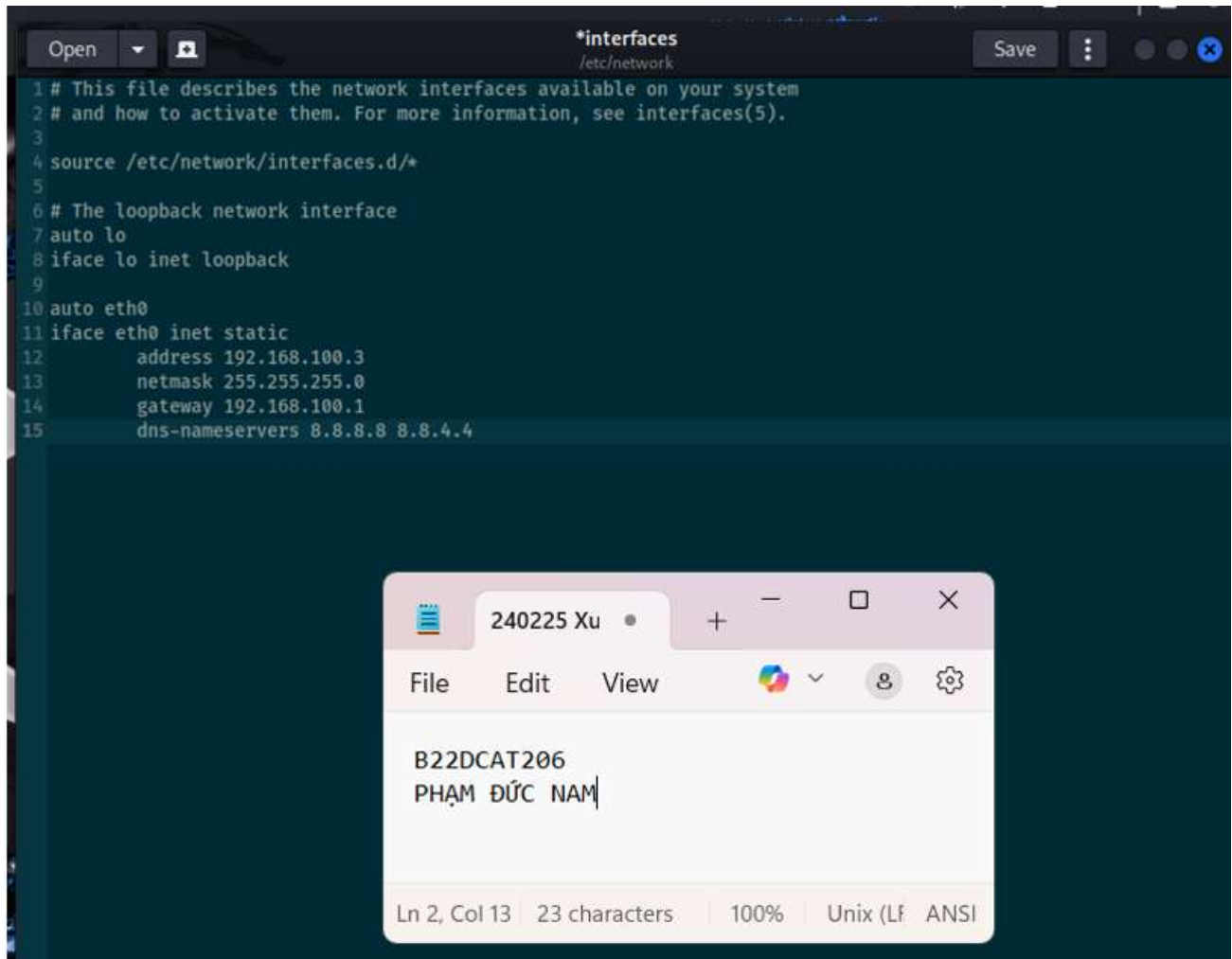
Hình 16 Sao lưu 1 file text trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client



Hình 17 Kiểm tra thư mục backup trong Ubuntu (Minh chứng)

#### 2.2.4. Sao lưu tệp sử dụng SCP

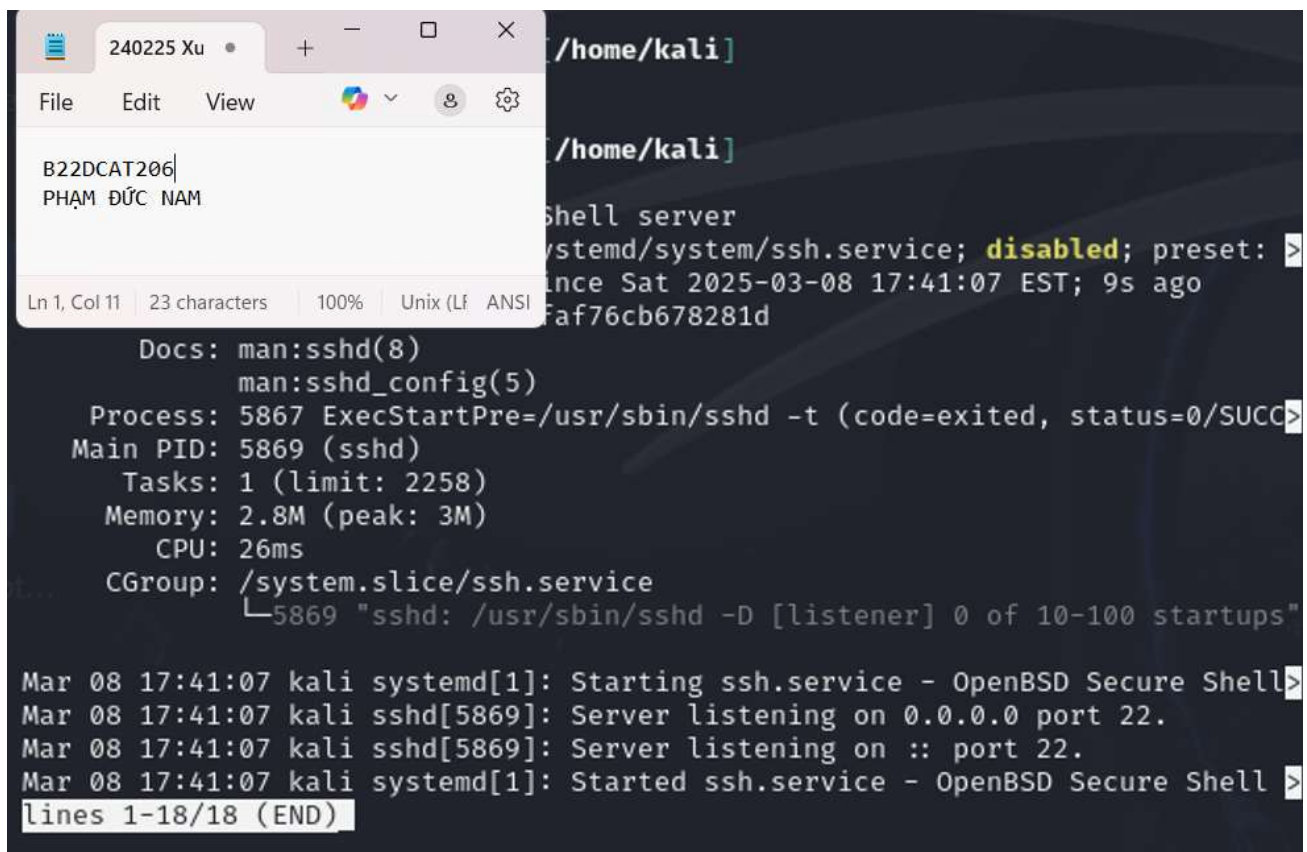
- Cấu hình IP cho máy Kali



Hình 18 cấu hình ip máy kali

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



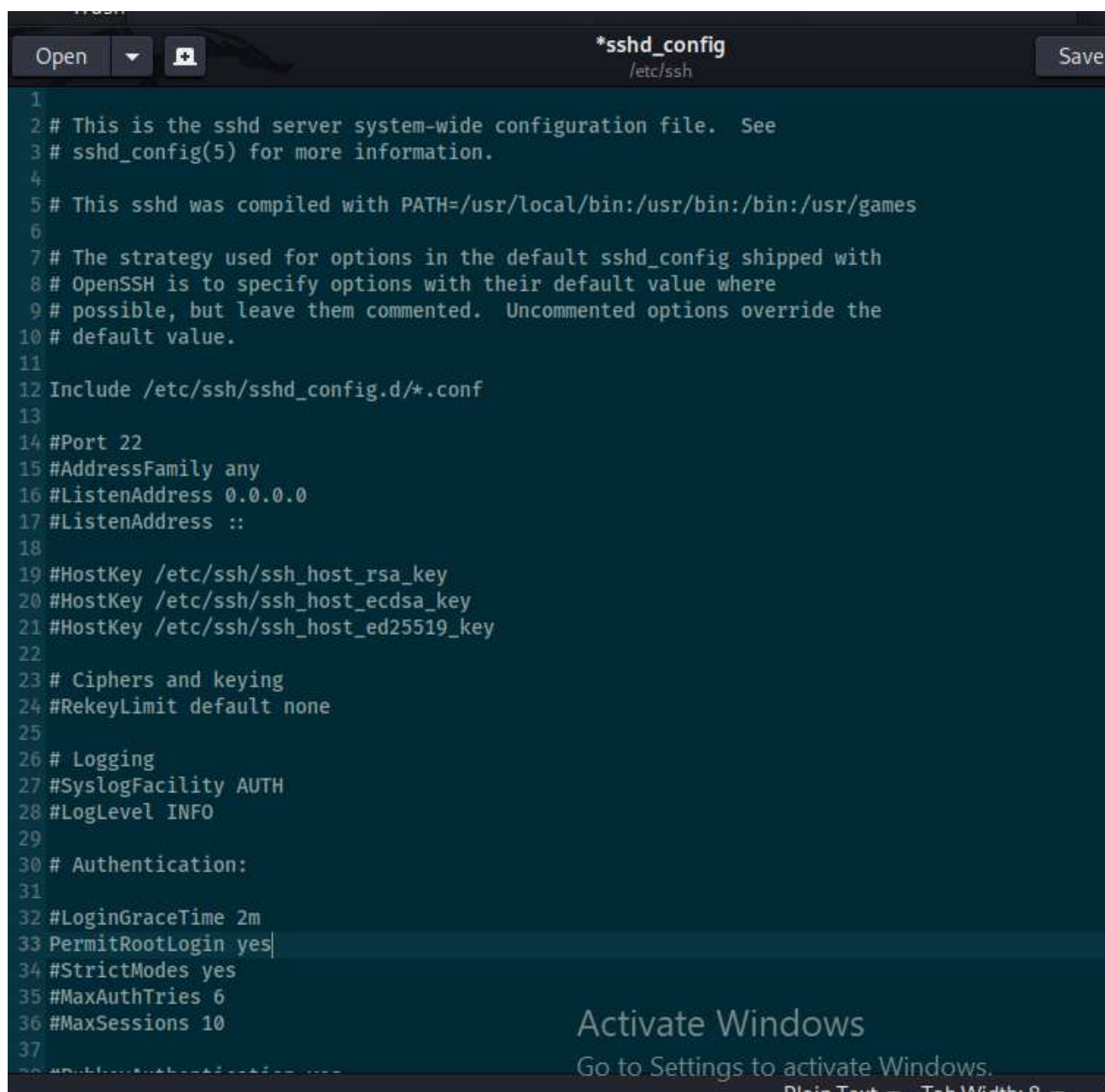


```
/home/kali]
/home/kali]
shell server
systemd/system/ssh.service; disabled; preset: >
since Sat 2025-03-08 17:41:07 EST; 9s ago
af76cb678281d

Docs: man:sshd(8)
      man:sshd_config(5)
Process: 5867 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 5869 (sshd)
Tasks: 1 (limit: 2258)
Memory: 2.8M (peak: 3M)
CPU: 26ms
CGroup: /system.slice/ssh.service
└─5869 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 08 17:41:07 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell>
Mar 08 17:41:07 kali sshd[5869]: Server listening on 0.0.0.0 port 22.
Mar 08 17:41:07 kali sshd[5869]: Server listening on :: port 22.
Mar 08 17:41:07 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell >
lines 1-18/18 (END)
```

Hình 19 Kiểm tra dịch vụ ssh đã bật hay chưa



```
1
2 # This is the sshd server system-wide configuration file. See
3 # sshd_config(5) for more information.
4
5 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games
6
7 # The strategy used for options in the default sshd_config shipped with
8 # OpenSSH is to specify options with their default value where
9 # possible, but leave them commented. Uncommented options override the
10 # default value.
11
12 Include /etc/ssh/sshd_config.d/*.conf
13
14 #Port 22
15 #AddressFamily any
16 #ListenAddress 0.0.0.0
17 #ListenAddress ::
18
19 #HostKey /etc/ssh/ssh_host_rsa_key
20 #HostKey /etc/ssh/ssh_host_ecdsa_key
21 #HostKey /etc/ssh/ssh_host_ed25519_key
22
23 # Ciphers and keying
24 #RekeyLimit default none
25
26 # Logging
27 #SyslogFacility AUTH
28 #LogLevel INFO
29
30 # Authentication:
31
32 #LoginGraceTime 2m
33 PermitRootLogin yes
34 #StrictModes yes
35 #MaxAuthTries 6
36 #MaxSessions 10
37
38 #PubkeyAuthentication yes
```

Hình 20 Cấu hình ssh cho phép truy cập vào tài khoản root trên Kali

- Tiếp tục, tạo Secure Shell Keys trên máy Kali Linux đó

```
root@kali:~# sudo ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:1rvqW3+YcrmJLylS7pzcG6mLrOHqsXzr+9am1FXctTQ root@kali
The key's randomart image is:
+--[RSA 4096]--+
|      . . . o o|
|      o . .    |
|      ..       |
|      S..      |
|      ..o .    |
|      ..+ oo. +|
|      ..o+.o.=++=..|
|      o==Bo=*O++*=o|
+--[SHA256]--+
```

Hình 21 Tạo Secure Shell Keys trên máy Kali Linux

- Trên máy Linux victim trong mạng Internal, thực hiện sao lưu sử dụng lệnh scp để copy file cần sao lưu tới thư mục root trên máy Kali Linux

```
root@kali:~# ls
B22DCAT206-phamducnam
```

Hình 22 Kết quả, file và thư mục đã được sao lưu vào thư mục root trên máy Kali

### 3. Kết luận

- Lý thuyết về SCP (Secure copy), FTP, ổ đĩa mạng.
- Cài đặt và sử dụng SCP, FTP để truyền/chia sẻ file và back up file trên Windows, Windows Server và Kali Linux.
- Sao lưu đến ổ đĩa mạng trên Windows.

### 4. Tài liệu tham khảo

- [1]. Lab 8 pfSense firewall của CSSIA CompTIA Security+®
- [2]. SCP: <https://viblo.asia/p/cach-su-dung-lenh-scp-de-truyen-tep-an-toan-Az45bLgVZxY>
- [3]. FTP: <https://tenten.vn/tin-tuc/ftp-la-gi/>
- [4]. Ổ đĩa mạng: <https://www.techtarget.com/whatis/definition/network-drive>