

**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: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH ẢNH	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	5
I. Mục đích	5
II. Tìm hiểu lý thuyết.....	5
1. Hệ điều hành Windows Server.....	5
1.1 Lịch sử phát triển.....	5
1.2 Kiến trúc của Windows Server.....	5
2. So sánh giữa Windows Server và Windows Desktop	6
2.1 Giống nhau	6
2.2 Khác nhau.....	6
3. Một số dịch vụ	7
3.1 Web Server	7
3.2 FTP Server	7
3.3 Remote Desktop Users	8
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	9
I. Chuẩn bị môi trường	9
II. Các bước thực hiện	9
1. Cài đặt hệ điều hành Windows Server và máy trạm Windows trên VMWare	9
2. Nâng cấp Server thành Domain Controller	15
3. Cấu hình máy trạm Windows gia nhập vào domain vừa được tạo	25
4. Cài đặt Web Server và FTP Server	27
5. Cài đặt Remote Desktop Users	31
6. Cài đặt PStools	33
TÀI LIỆU THAM KHẢO	35

DANH MỤC CÁC HÌNH ẢNH

<i>Hình ảnh 1: Mô hình truyền dữ liệu của FTP: Client – Server</i>	6
<i>Hình ảnh 2 : Kết nối dữ liệu bằng phương thức Active hoặc Passive.</i>	6
<i>Hình ảnh 3: Hình ảnh ổ đĩa mạng NAS</i>	7
<i>Hình ảnh 4 : Tạo thư mục share qua C:\net share share=c:\share</i>	10
<i>Hình ảnh 5 : Cấu hình ổ đĩa mạng trên máy.</i>	11
<i>Hình ảnh 6 : Cấu hình ổ đĩa cho phép sao lưu tệp và thư mục từ máy khác.</i>	12
<i>Hình ảnh 7 : Sao lưu hệ thống bằng chương trình sao lưu.</i>	13
<i>Hình ảnh 8: Backup xong.</i>	14
<i>Hình ảnh 9: Kiểm tra lại trên máy Windows Attack.</i>	15
<i>Hình ảnh 10: Cấu hình FTP client.</i>	15
<i>Hình ảnh 11: Cài đặt FTP Server.</i>	16
<i>Hình ảnh 12: Tạo thêm thư mục ở Windows Attack.</i>	16
<i>Hình ảnh 13 :Cài đặt FTP Client và đăng nhập qua máy Linux.</i>	17
<i>Hình ảnh 14 : Sao lưu 1 thư mục trên máy Windows Attack.</i>	18
<i>Hình ảnh 15 : Kiểm tra folder B22DCAT176 trên máy Ubuntu.</i>	19
<i>Hình ảnh 16 : Cấu hình SSH server.</i>	19
<i>Hình ảnh 17 : Tạo Secure Shell Key trên máy Kali Linux.</i>	20
<i>Hình ảnh 18 : Tạo hai file txt</i>	20
<i>Hình ảnh 19 : Tiến hành gửi file.</i>	21
<i>Hình ảnh 20 : Tiến hành kiểm tra trên máy Kali Linux.</i>	21
TÀI LIỆU THAM KHẢO	22

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
AD	Active Directory	Thư mục động
DNS	Domain Name System	Giao thức tên miền
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ IP tự động
IIS	Internet Information Services	Dịch vụ Web Server chính của Microsoft
WAS	Windows Process Activation Service	Dịch vụ hỗ trợ cho IIS

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

I. Mục đích

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

- a. Sao lưu tới ổ đĩa mạng
- b. Sao lưu tệp lên FTP server
- c. Sao lưu tệp sử dụng SCP

II. Tìm hiểu lý thuyết

1. SCP – Secure copy

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 nên 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* và *Sao chép từ remote về local*.

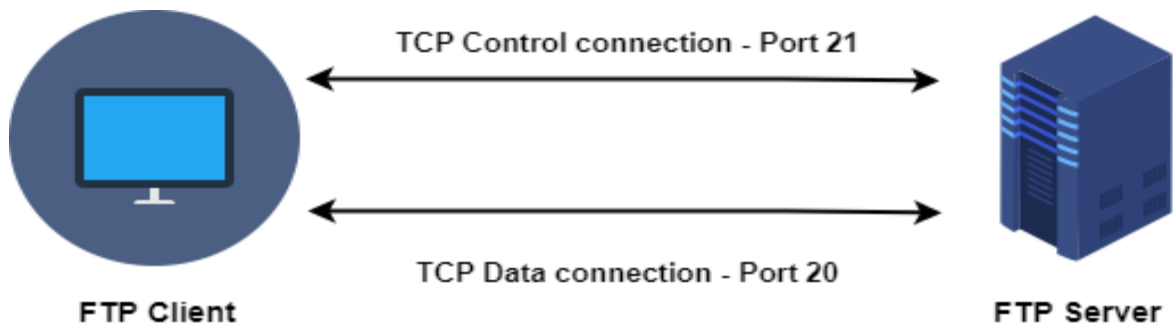
SCP là công cụ hữu ích cho các quản trị viên hệ thống hoặc những người làm việc với nhiều máy tính trong mạng khi giúp họ sao chép các tệp tin lớn, các script hoặc các tệp tin nhạy cảm một cách nhanh chóng và an toàn. Ngoài ra, SCP còn kết hợp với các lệnh dòng lệnh khác để tạo ra các tác vụ tự động 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.

Ngoài ra, SCP còn có hạn chế khi 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 một số công cụ 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.

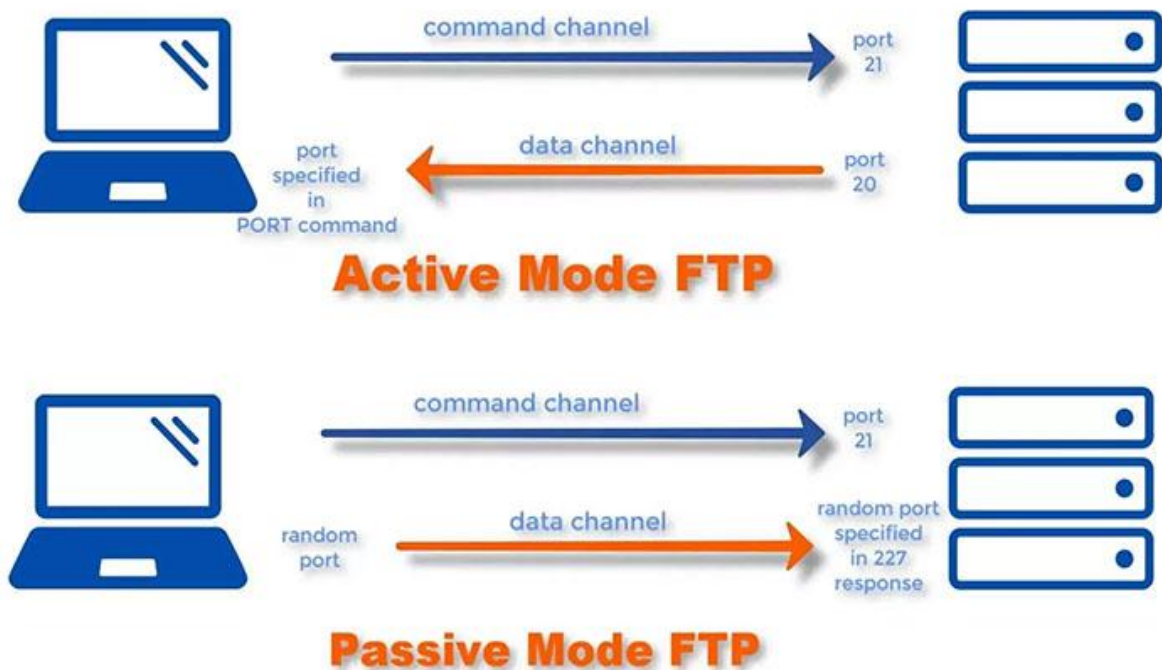
2. FTP – File Transfer Protocol

FTP (File Transfer Protocol) là giao thức truyền tệp dùng để truyền tệp tin giữa các máy tính trong mạng. Giao thức truyền 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.



Hình ảnh 1: Mô hình truyền dữ liệu của FTP: Client – Server

Trong giao thức FTP, khi một máy khách yêu cầu truyền một tệp tin từ máy chủ, nó kết nối với 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 để truyền tệp tin. Kết nối dữ liệu có thể được thiết lập bằng một trong hai phương thức: *Active* hoặc *Passive*.



Hình ảnh 2 : Kết nối dữ liệu bằng 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 *Phương thức Passive* yêu cầu máy chủ mở một cổng để chờ máy khách kết nối. Khi kết nối 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, hiển thị danh sách các tệp tin và thư mục trên máy chủ...

Việc sử dụng FTP còn có một số hạn chế: FTP không cung cấp tính năng mã hóa dữ liệu nên dữ liệu có thể bị đánh cắp hoặc bị thay đổi khi được truyền qua mạng. Hơn nữa, 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 cụ 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.

3.Ổ đĩa mạng – NAS

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 để lưu trữ và chia sẻ dữ liệu giữa các máy tính trong một doanh nghiệp hoặc gia đình.



Hình ảnh 3: Hình ảnh ổ đĩa mạng NAS

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... NAS cũng cung cấp các tính năng: 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 cứ đâu trên thế giới.

Tuy nhiên, để sử dụng được NAS, người dùng cần 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 nên khi lựa chọn NAS chúng ta cần phải cân nhắc đến nhu cầu sử dụng và khả năng tài chính của mỗi người dùng.

4. 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.. 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: SMB, NFS,... 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.

5. 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.

CHƯƠNG 2 : NỘI DUNG THỰC HÀNH

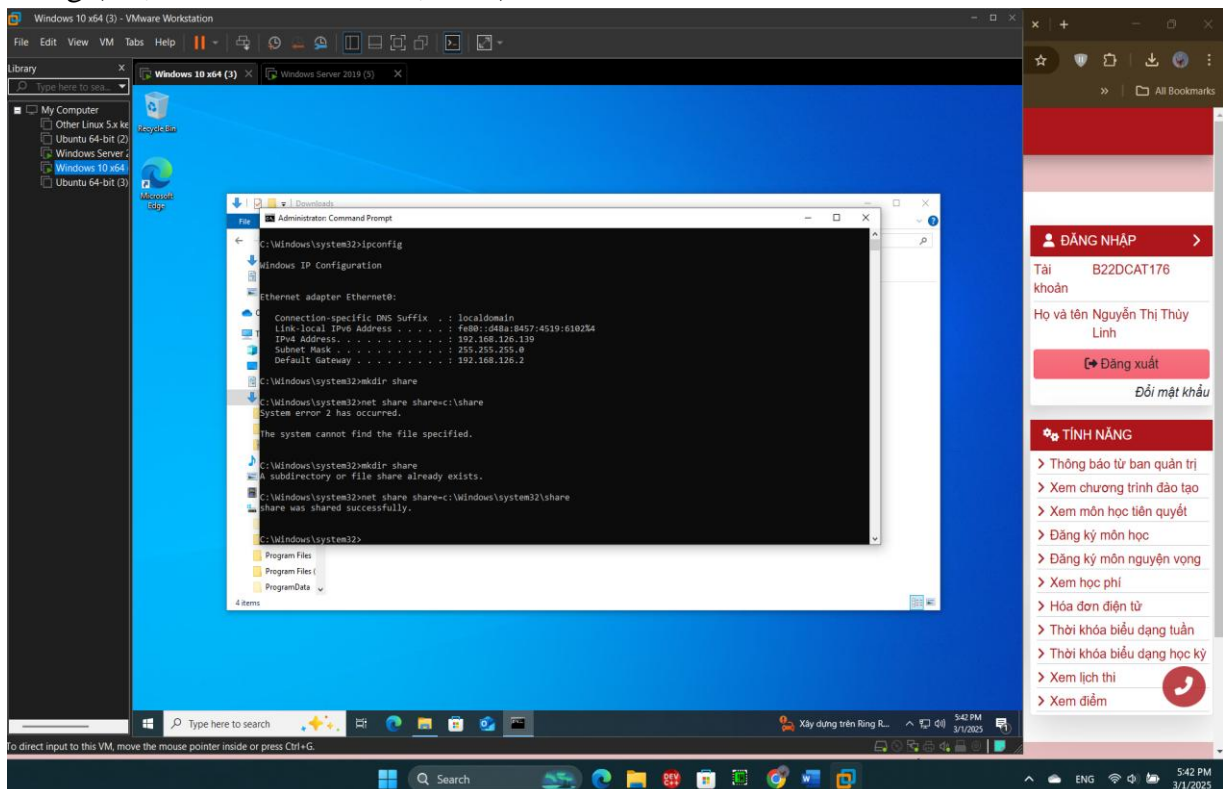
I. Chuẩn bị môi trường

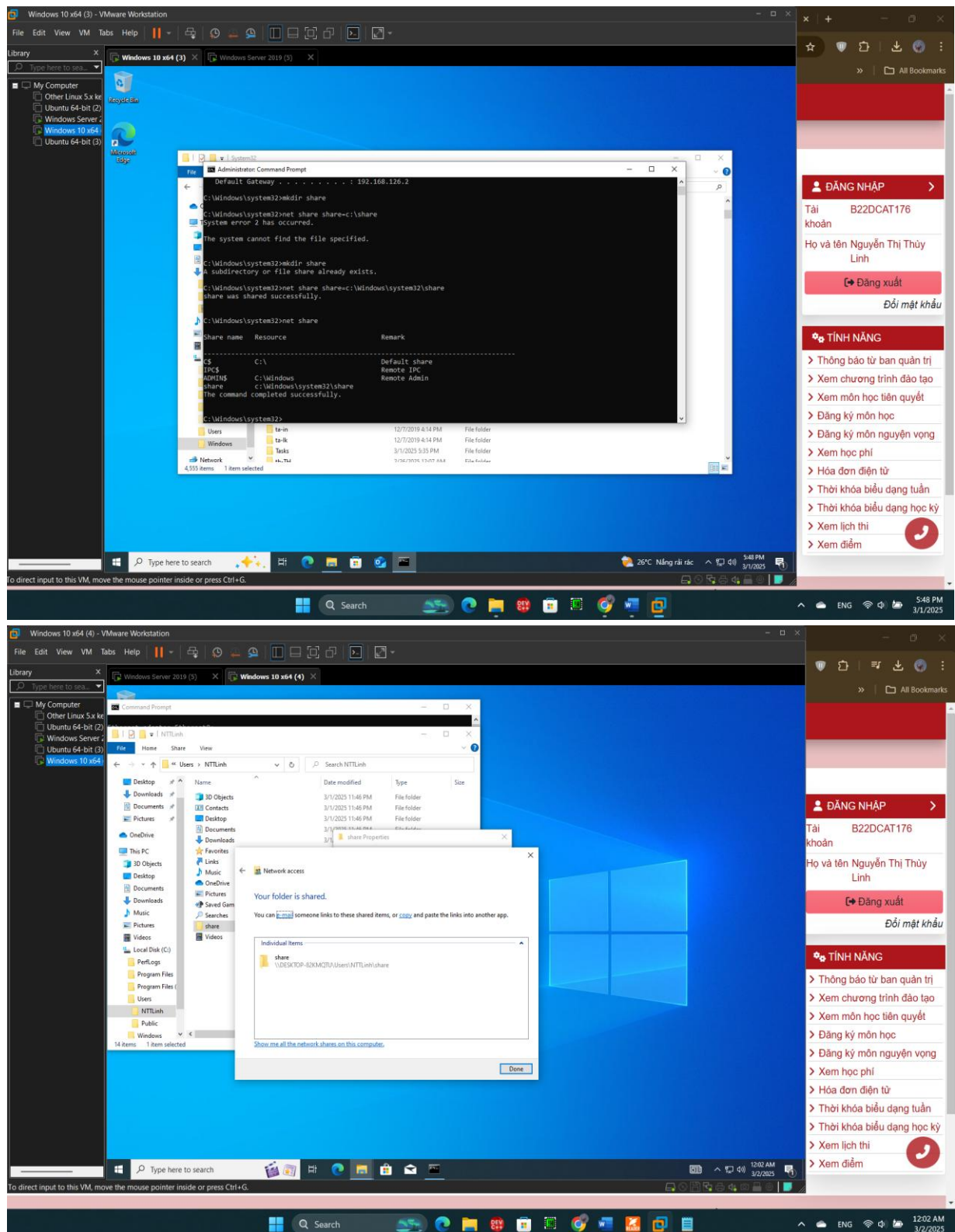
- Các file máy ảo VMWare và hệ thống mạng đã cài đặt trong bài lab trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux.
- Download máy trạm Windows 7 (hoặc Windows 10/11)
- Download phần mềm máy ảo : VMWare Workstation.

II. Các bước thực hiện

a. Sao lưu tới ổ đĩa mạng

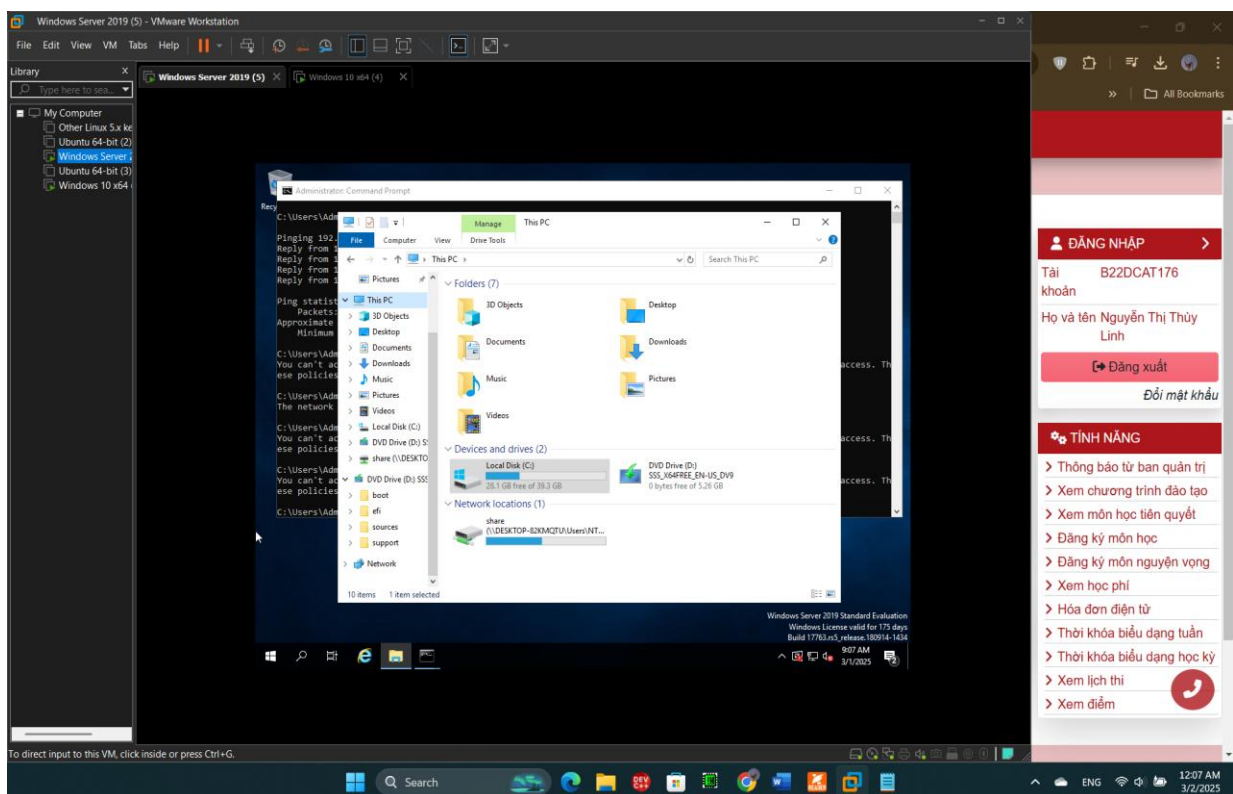
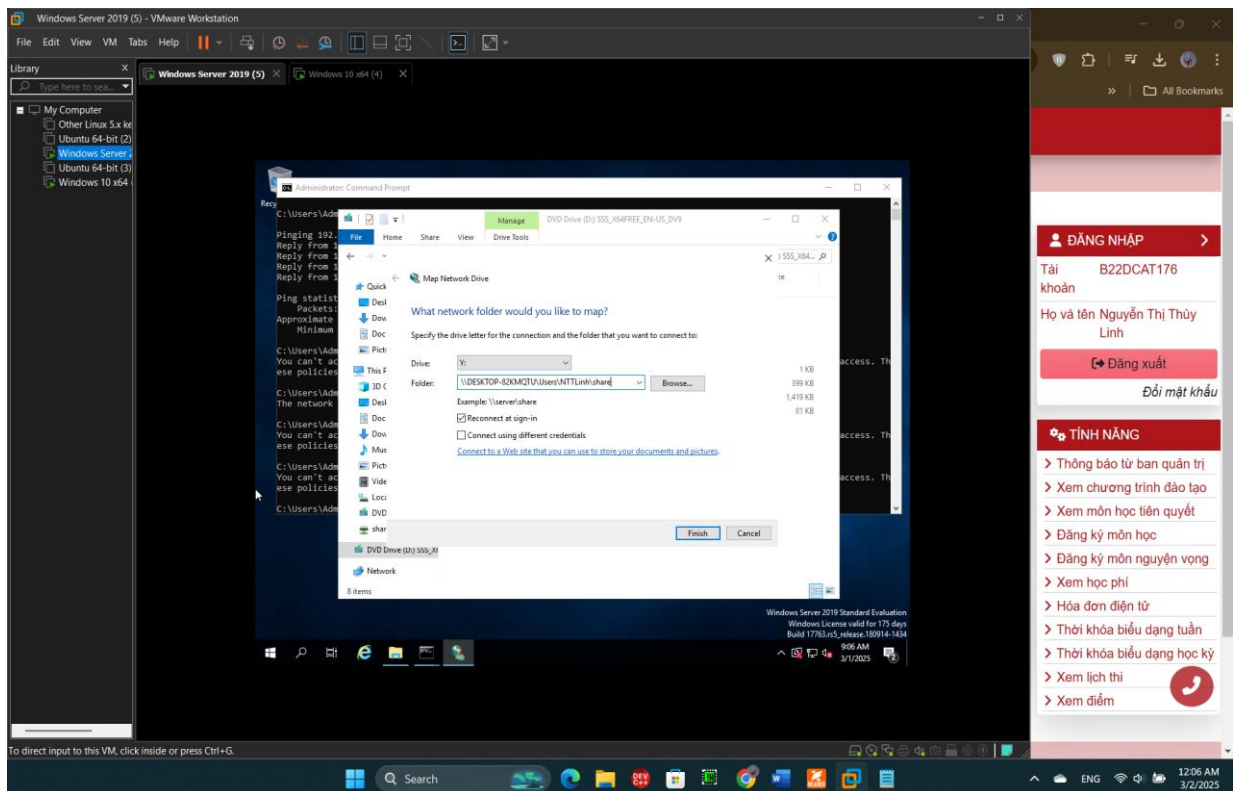
- Trên máy trạm Windows attack trong mạng Internal, tạo thư mục share rồi chia sẻ qua mạng (*C:\net share share=c:\share*)





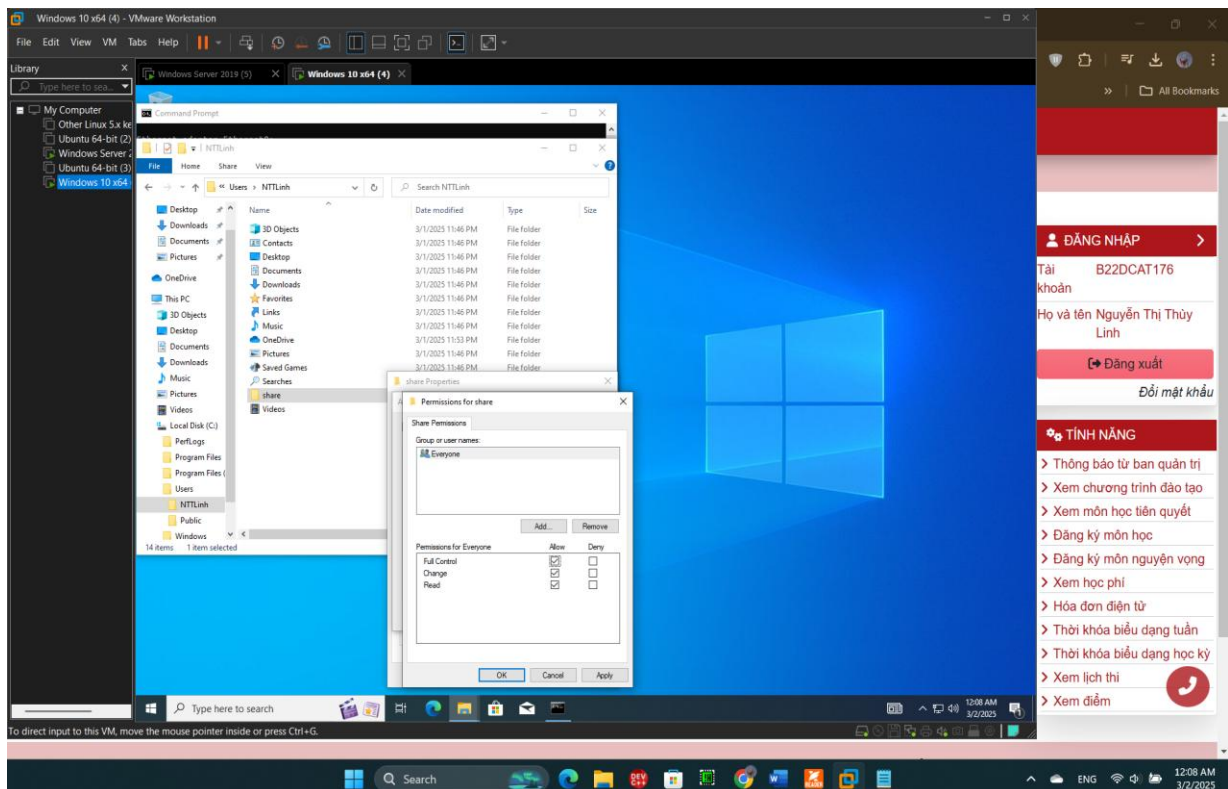
Hình ảnh 4 : Tạo thư mục share qua `C:\net share share=c:\share`

- Trên máy Windows Server ở mạng Internal, cấu hình map ổ đĩa mạng trên máy.



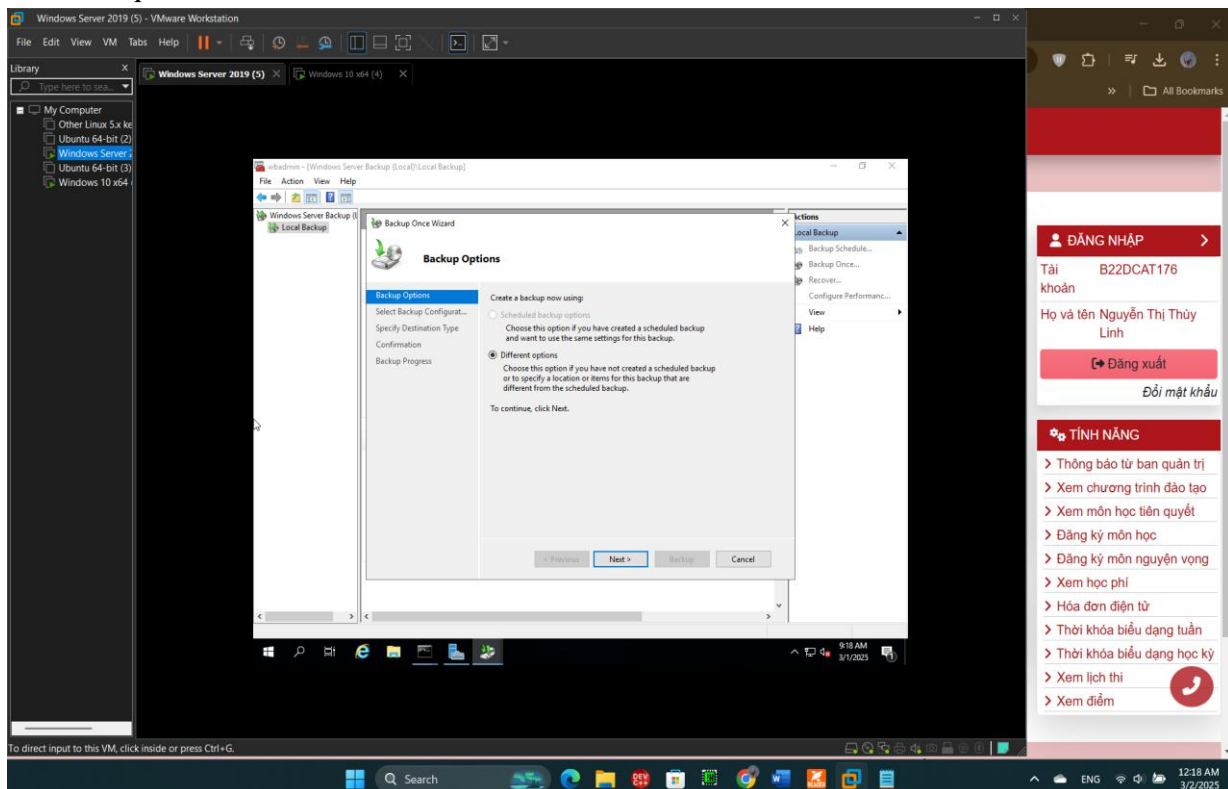
Hình ảnh 5 : Cấu hình ổ đĩa mạng trên máy.

- 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.



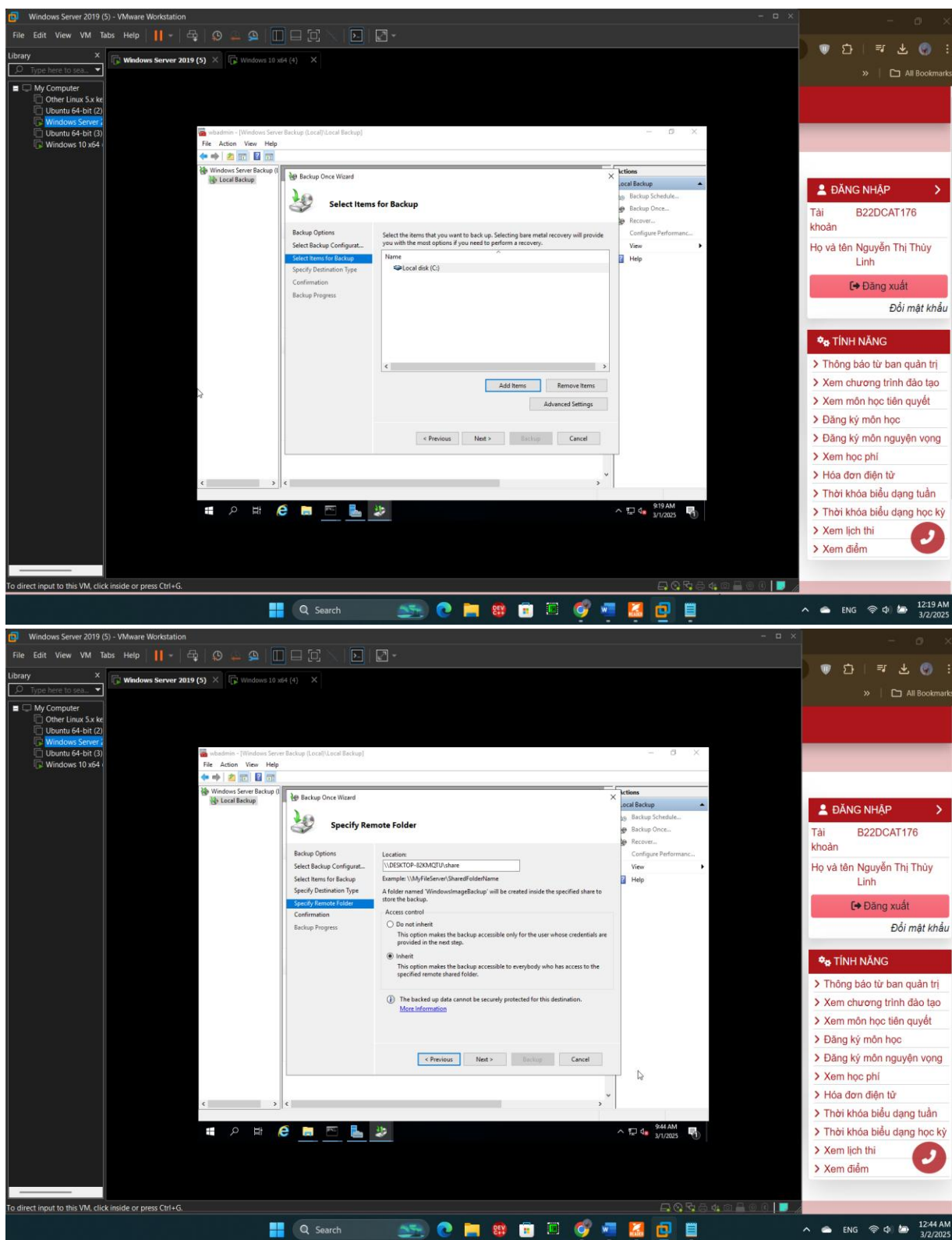
Hình ảnh 6 : Cấu hình ổ đĩa cho phép sao lưu tệp và thư mục từ máy khác.

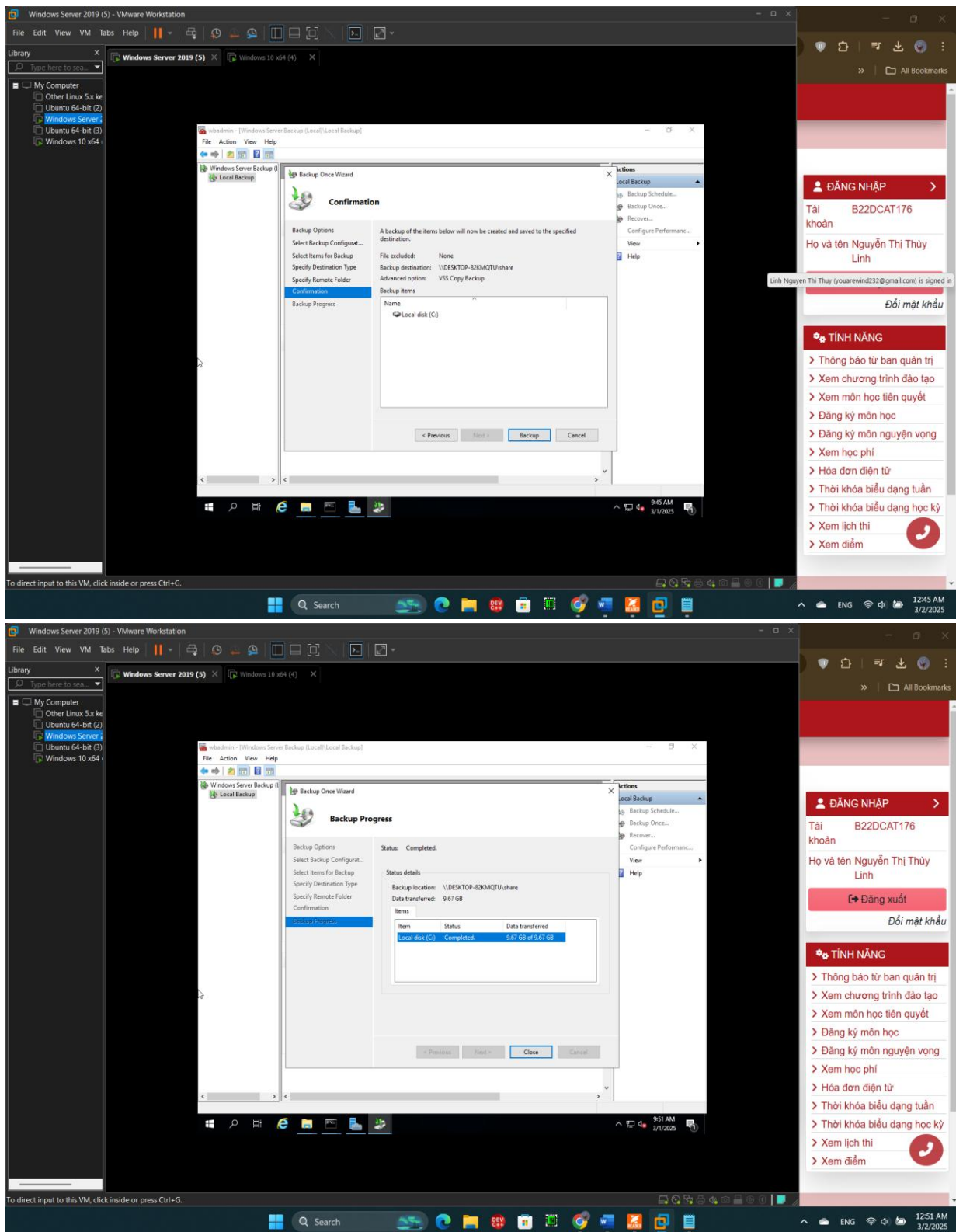
- Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2019, nếu sử dụng Windows khác thì có thể download ntback up để sử dụng), sau đó chọn 1 thư mục để sao lưu và đích là thư mục ổ mạng đã chia sẻ trên máy Windows attack trong mạng Internal:
- Vào *Server Manager* -> *Tools* -> *Windows Server Backup* -> Chuột phải *Local Backups* -> *Backup Once*.



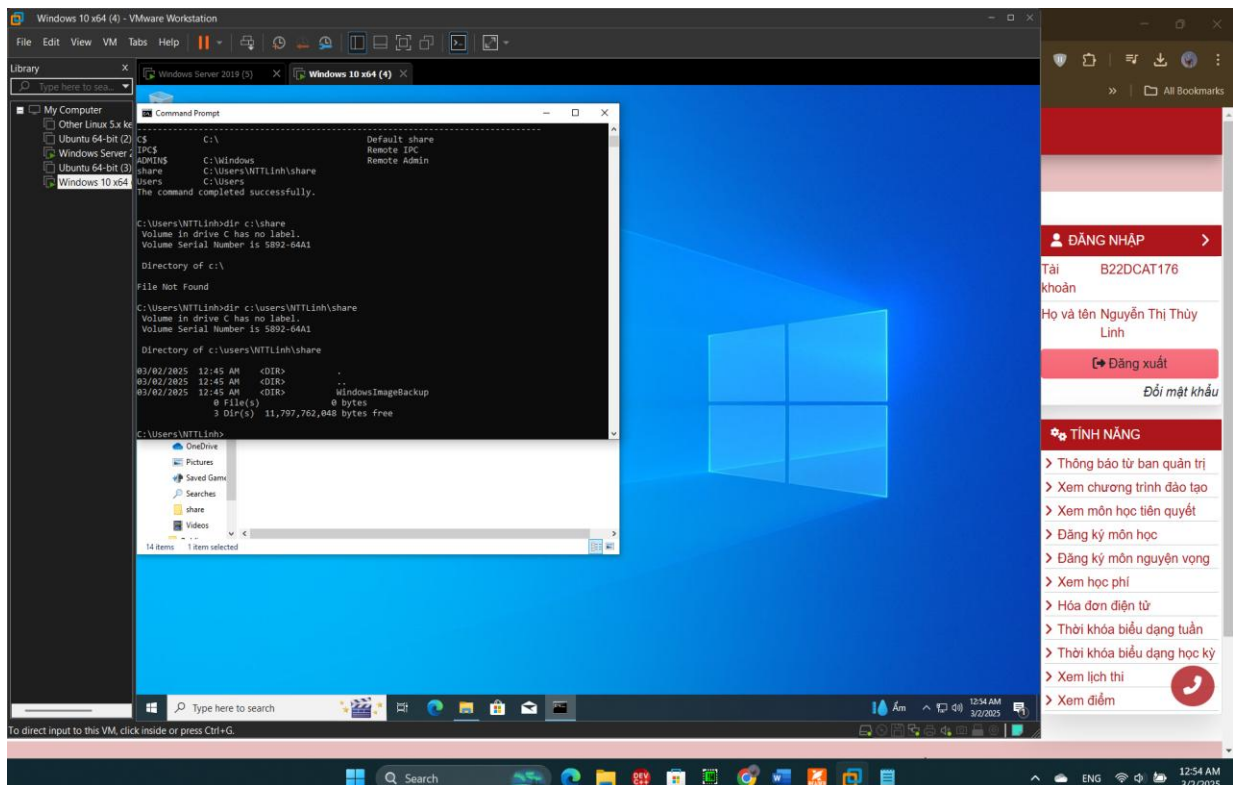
Hình ảnh 7 : Sao lưu hệ thống bằng chương trình sao lưu

-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.





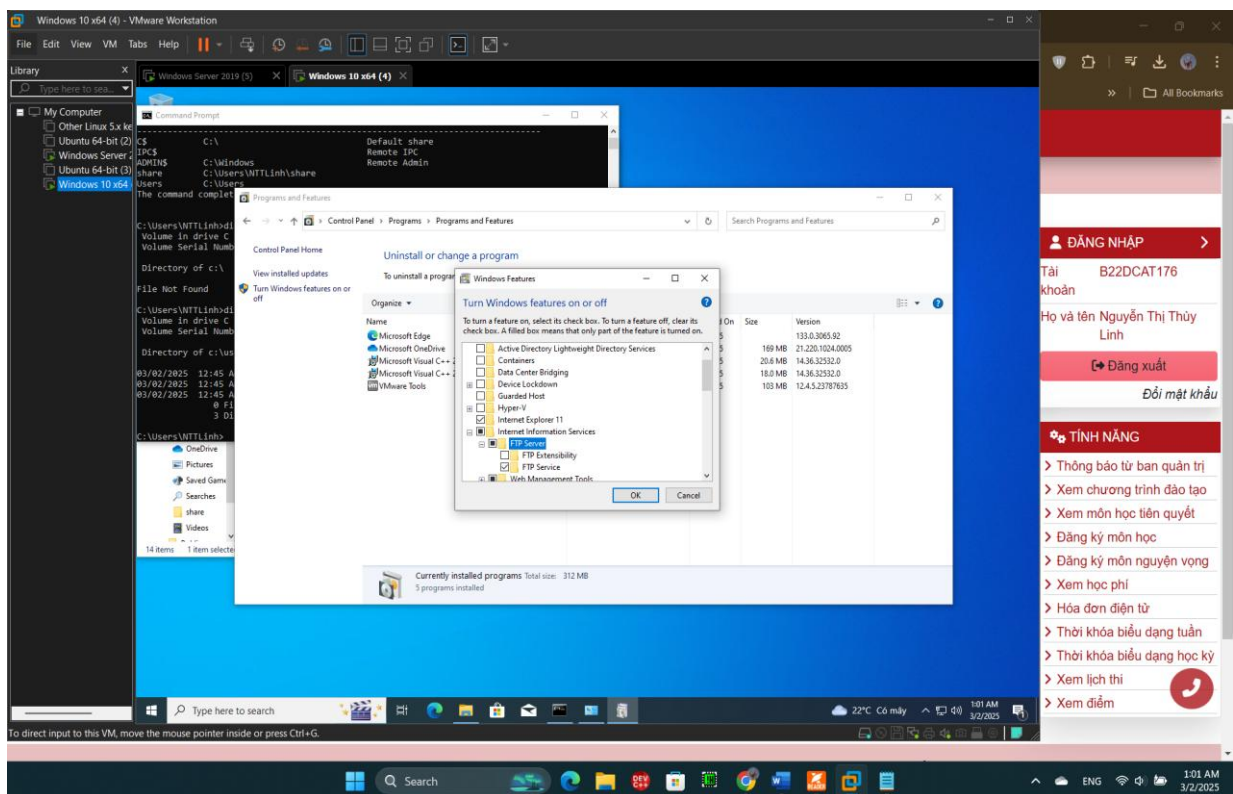
Hình ảnh 8: Backup xong.



Hình ảnh 9: Kiểm tra lại trên máy Windows Attack.

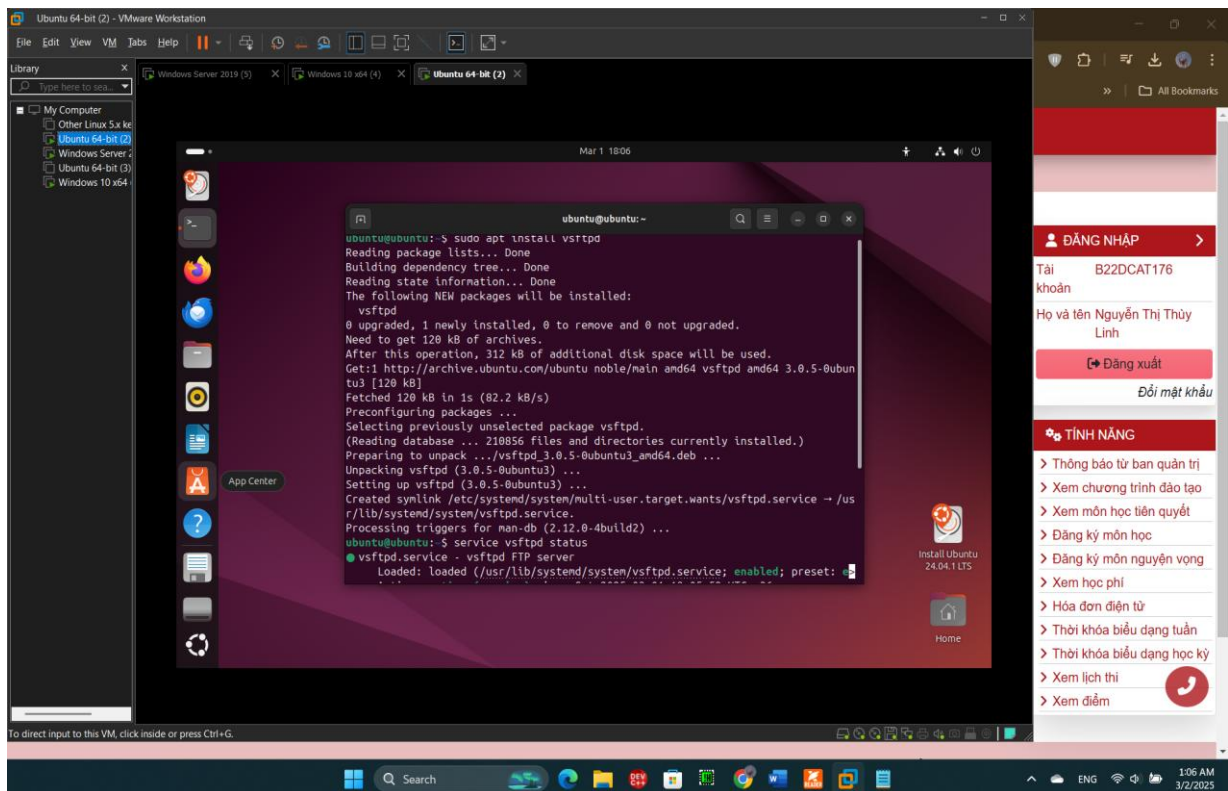
b. Sao lưu tệp FTP server

- Trên máy Windows Attack, cấu hình *FTP client*.



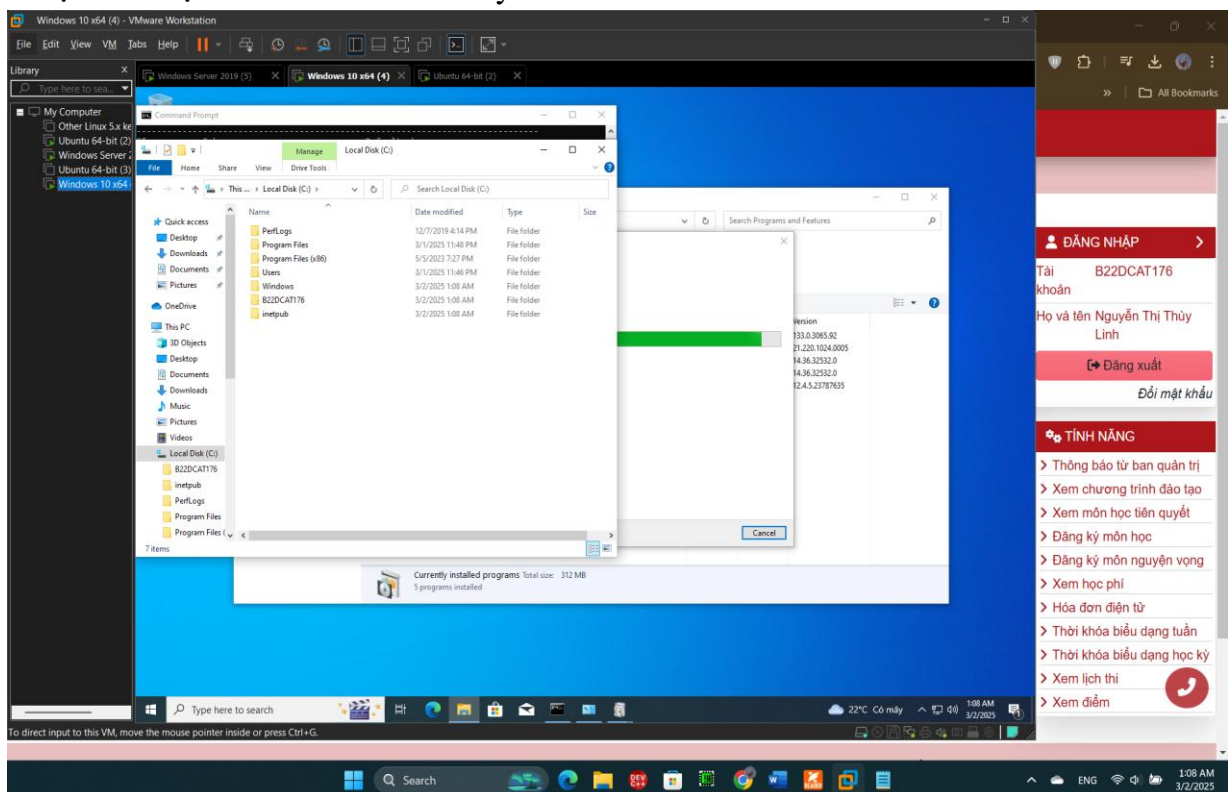
Hình ảnh 10: Cấu hình *FTP client*.

- Trên máy Ubuntu trong mạng Internal, cài đặt *FTP Server*.



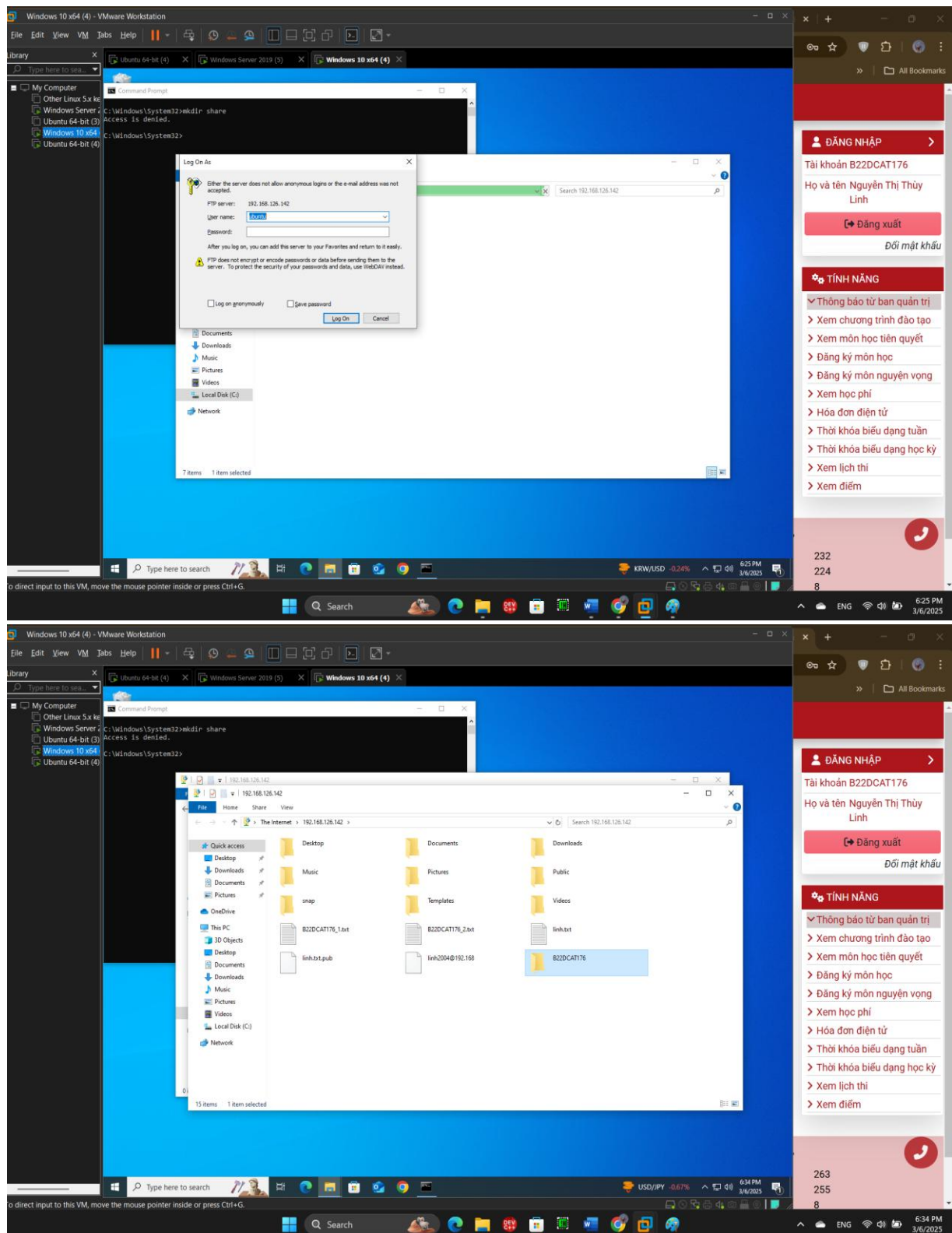
Hình ảnh 11: Cài đặt FTP Server.

- Tạo thư mục B22DCAT176 ở máy Windows Attack.



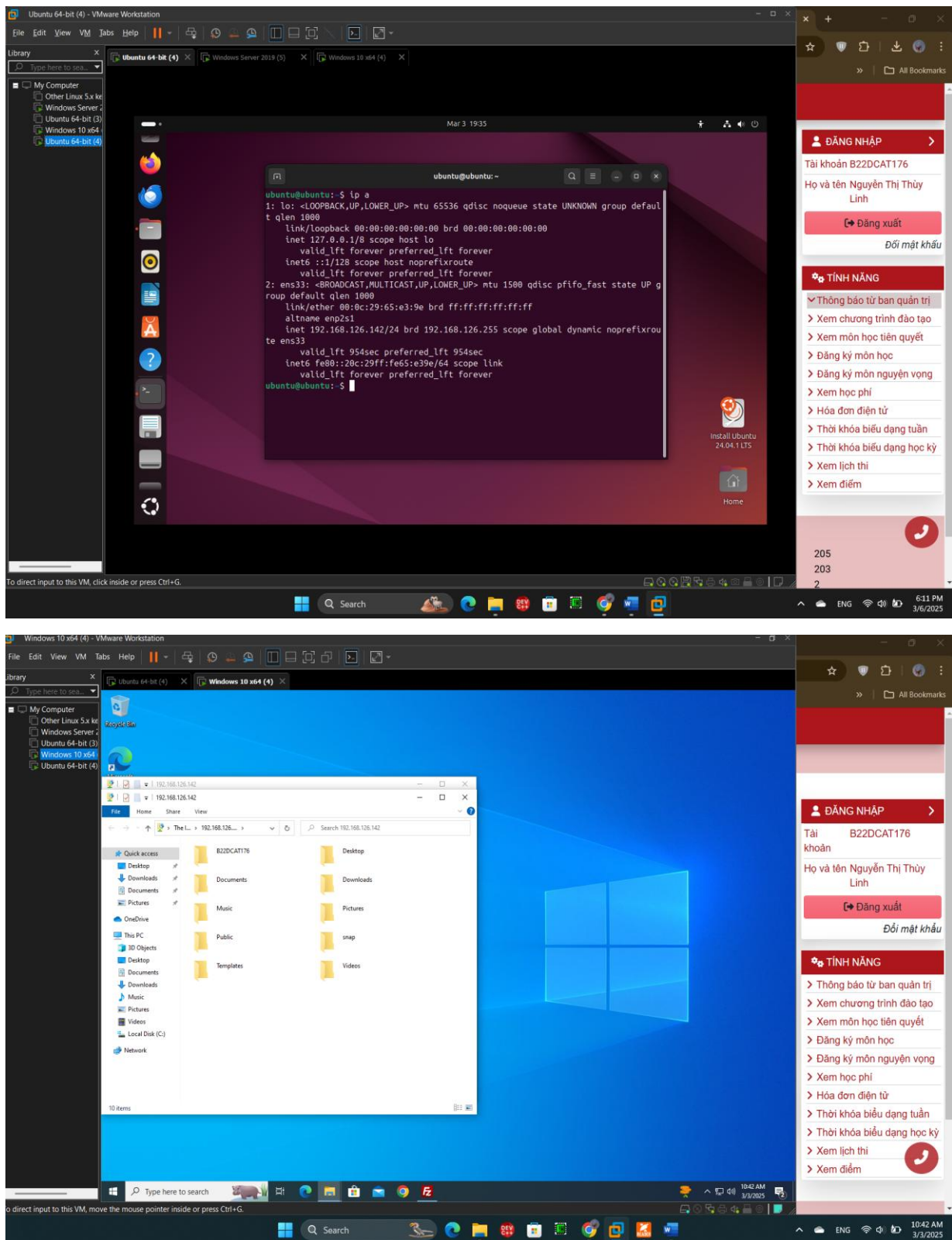
Hình ảnh 12: Tạo thêm thư mục ở Windows Attack.

- Trên máy Windows Attack ở mạng Internal, cài đặt ftp client và đăng nhập qua máy linux Internal 192.168.126.142



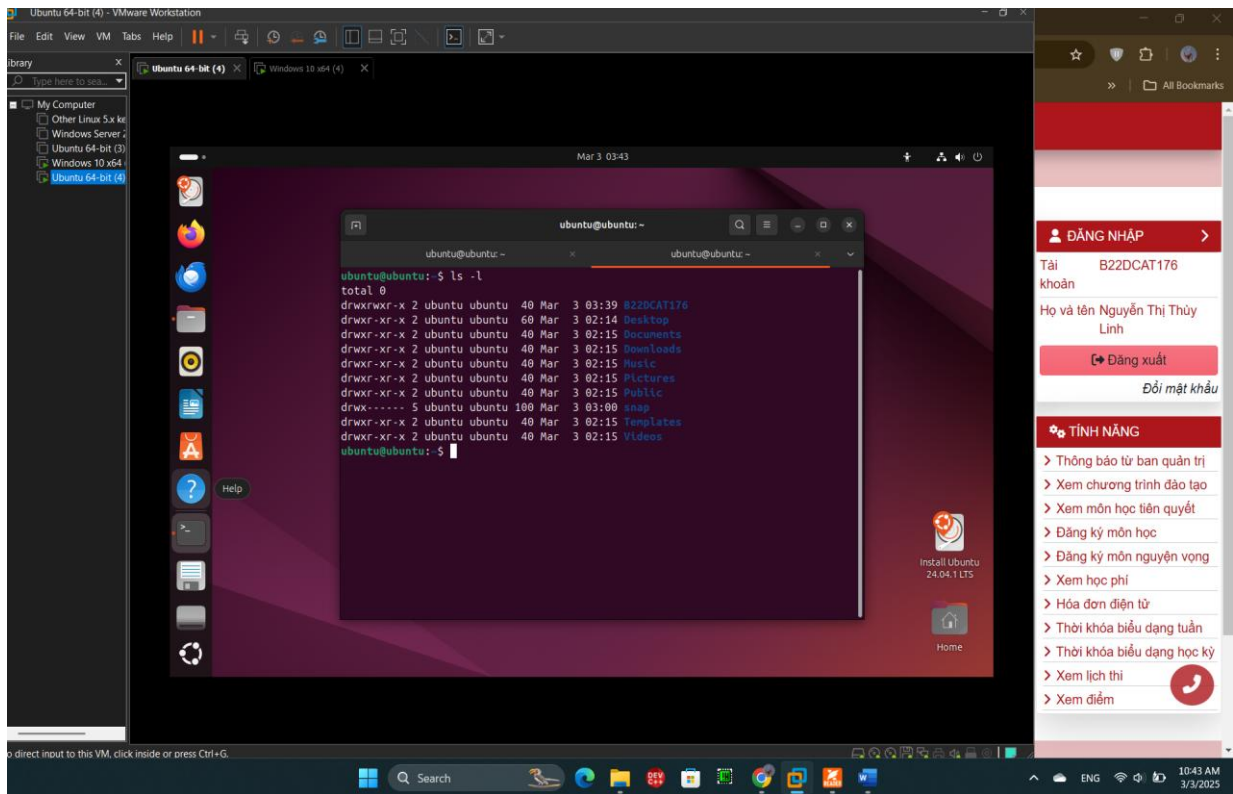
Hình ảnh 13 : Cài đặt FTP Client và đăng nhập qua máy Linux.

-Sao lưu 1 thư mục trên máy Windows Attack tới thư mục /backup trên máy Linux trong mạng Windows sử dụng *FTP client*, sau khi kết nối tới *FTP server*.



Hình ảnh 14 : Sao lưu 1 thư mục trên máy Windows Attack.

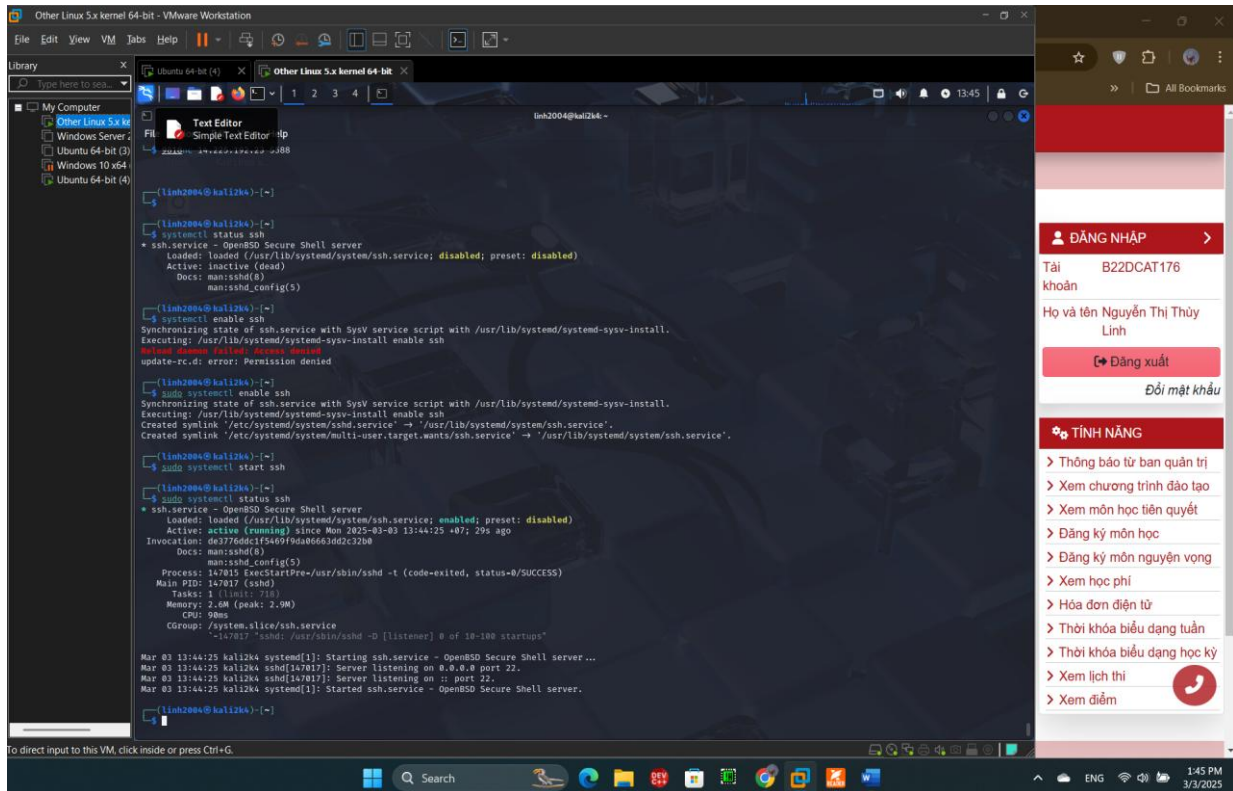
-Kiểm tra thấy folder *B22DCAT176* trên máy Ubuntu.



Hình ảnh 15 : Kiểm tra folder B22DCAT176 trên máy Ubuntu.

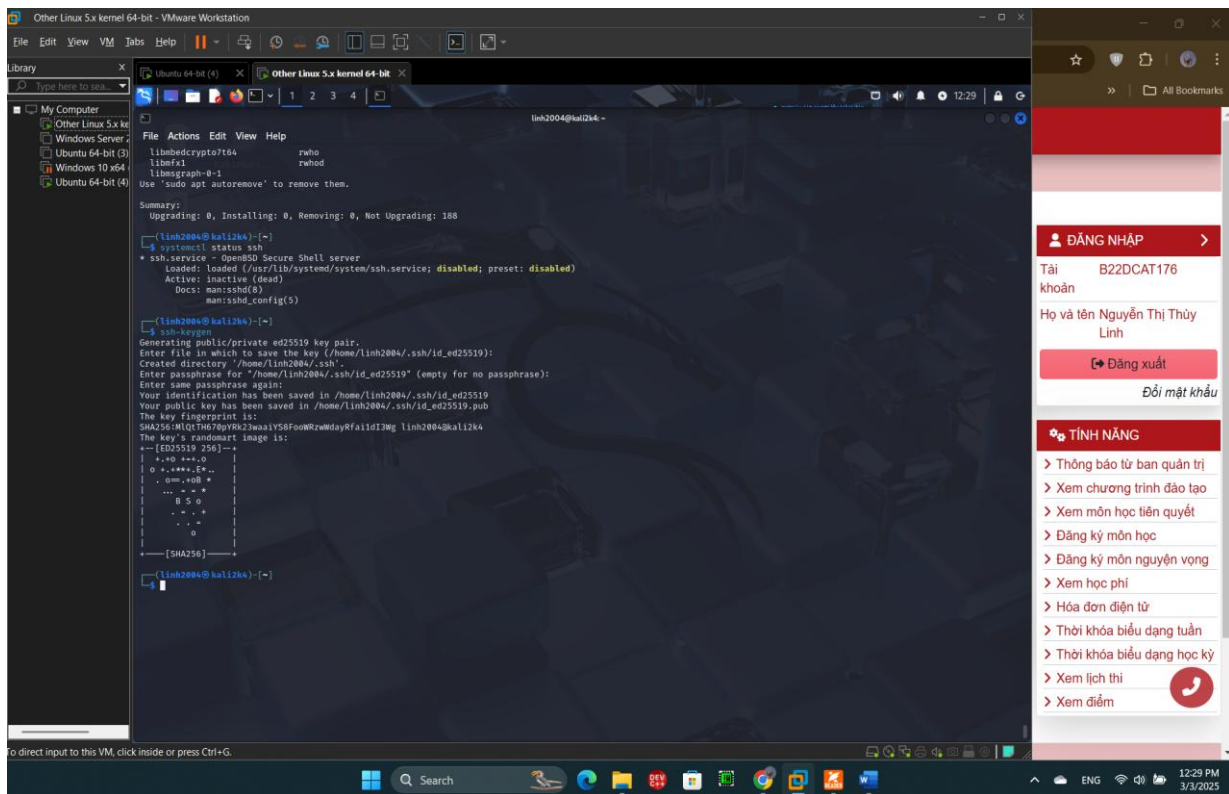
c. Sao lưu tệp sử dụng SCP

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



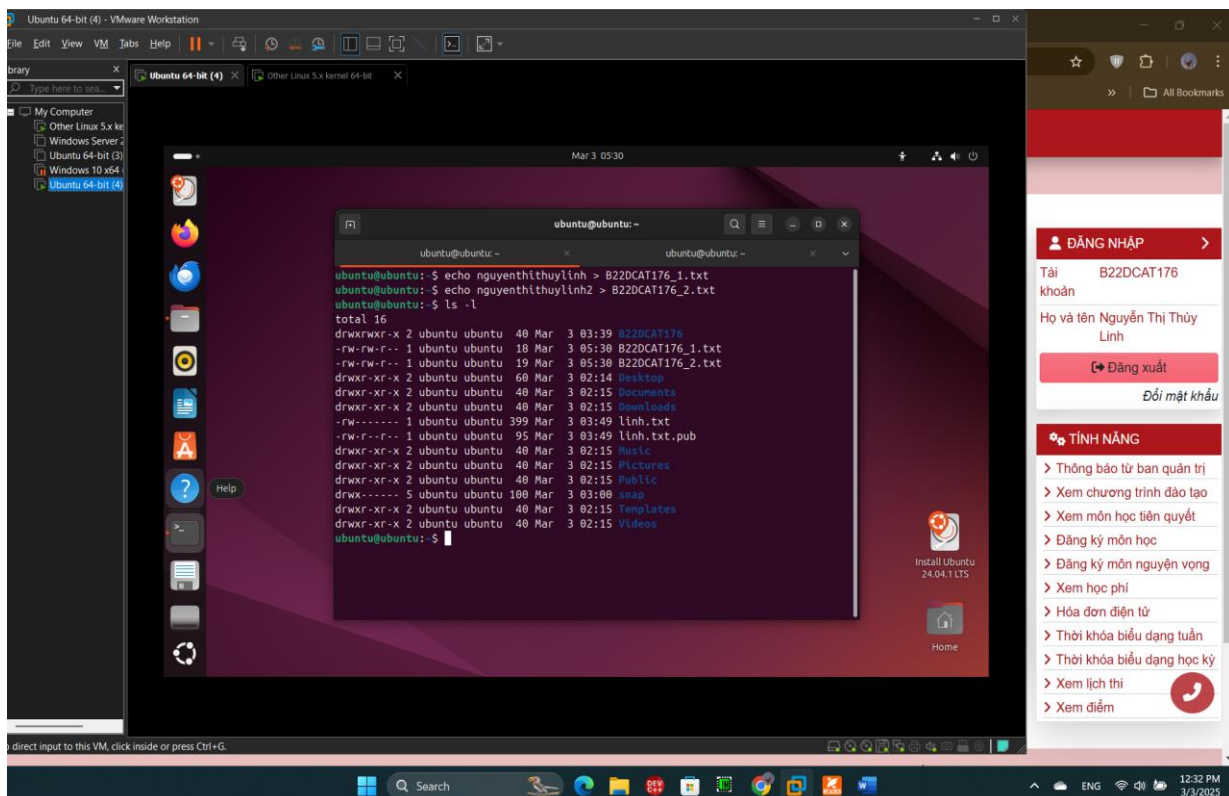
Hình ảnh 16 : Cấu hình SSH server.

-Tạo Secure Shell Key trên máy Kali Linux:



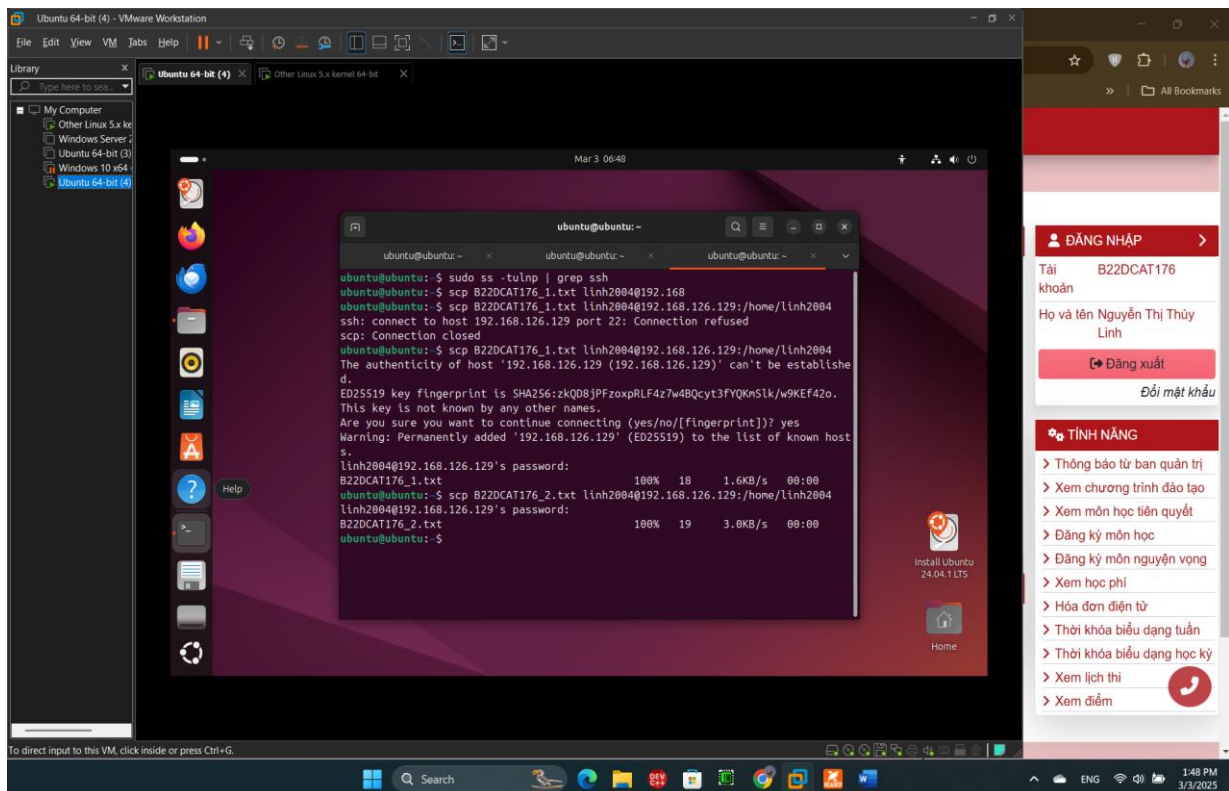
Hình ảnh 17 : Tạo Secure Shell Key trên máy Kali Linux.

-Trên máy Linux victim, tạo 2 file text lần lượt B22DCAT176_1.txt và B22DCAT176_2.txt



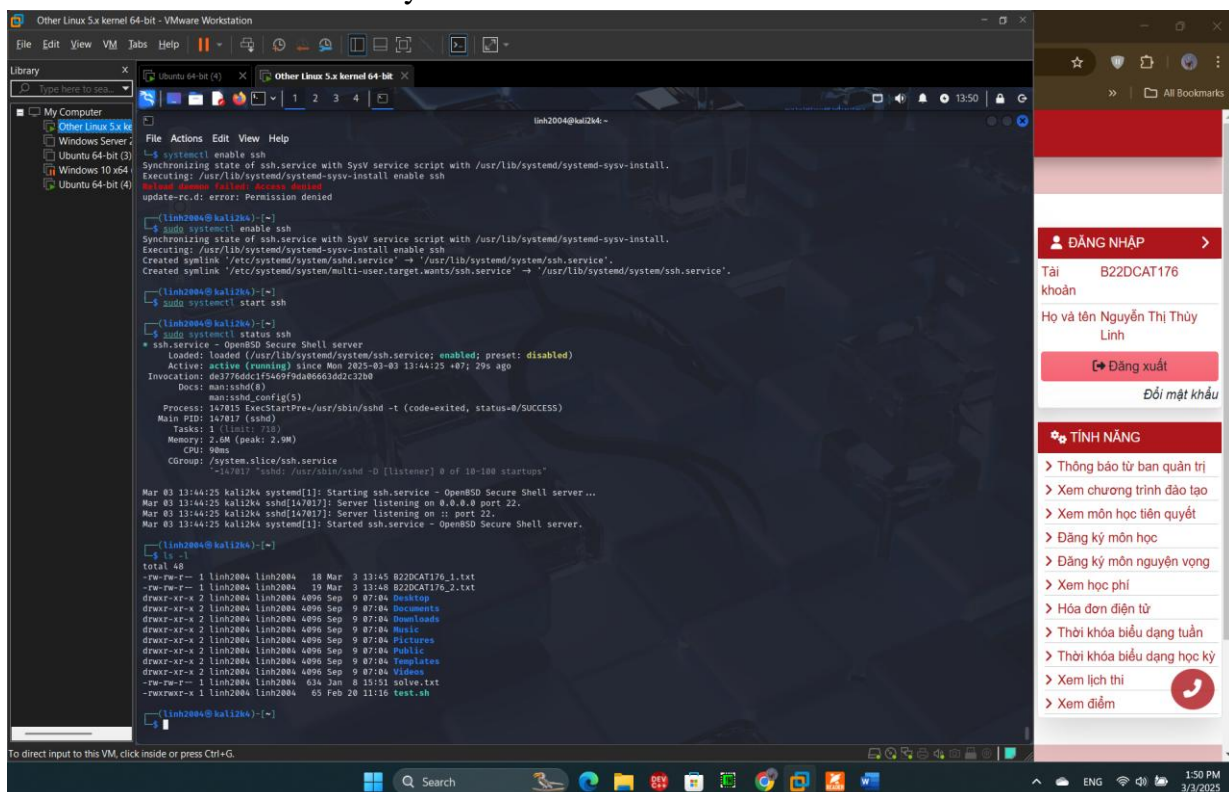
Hình ảnh 18 : Tạo hai file txt

- Trên máy Linux victim, tiến hành gửi file.



Hình ảnh 19 : Tiến hành gửi file.

- Tiến hành kiểm tra trên máy Kali Linux.



Hình ảnh 20 : Tiến hành kiểm tra trên máy Kali Linux.

III. Kết quả đạt được

- Học cách sao lưu tới ổ đĩa mạng.
- Sao lưu tệp qua FTP Server
- Chia sẻ file an toàn bằng SCP (Secure Copy)

TÀI LIỆU THAM KHẢO

- [1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.