

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
MÔN THỰC TẬP CƠ SỞ



BÀI THỰC HÀNH 1.5
SAO LƯU HỆ THỐNG

Tên sinh viên: Nguyễn Văn Hùng

Mã sinh viên: B22DCAT136

Nhóm: 09

HÀ NỘI, THÁNG 03/2025

MỤC LỤC

MỤC LỤC	1
DANH MỤC CÁC HÌNH VẼ	2
I. GIỚI THIỆU CHUNG	4
1. Mục đích	4
2. Lý thuyết	4
2.1. Secure Copy Protocol (SCP)	4
2.2. File Transfer Protocol (FTP)	5
2.3. Network Drive (Ổ đĩa mạng)	9
2.4. Lệnh net use	10
2.5. Lệnh net view	11
II. NỘI DUNG THỰC HÀNH	12
1. Chuẩn bị môi trường	12
2. Thực hành	13
2.1. Sao lưu tới ổ đĩa mạng	13
2.2. Sao lưu tệp lên FTP Server	18
2.3. Sao lưu tệp sử dụng SCP	22
TÀI LIỆU THAM KHẢO	27

DANH MỤC CÁC HÌNH VẼ

<i>Hình 1. Kết nối TCP trong FTP</i>	5
<i>Hình 2. Mô hình FTP</i>	7
<i>Hình 3. Internal Network</i>	12
<i>Hình 4. Máy Kali Linux attack 1</i>	12
<i>Hình 5. Máy Windows attack</i>	12
<i>Hình 6. Ubuntu Linux victim</i>	13
<i>Hình 7. Windows Server victim</i>	13
<i>Hình 8. Tạo thư mục sao lưu</i>	13
<i>Hình 9. Chia sẻ và kiểm tra chia sẻ thư mục</i>	14
<i>Hình 10. Cấu hình chia sẻ thư mục</i>	14
<i>Hình 11. Ảnh xạ thư mục chia sẻ thành ổ đĩa mạng</i>	15
<i>Hình 12. Kiểm tra ổ đĩa mạng</i>	15
<i>Hình 13. Cài đặt WSB</i>	16
<i>Hình 14. Sao lưu thư mục</i>	16
<i>Hình 15. Sao lưu thành công</i>	17
<i>Hình 16. Kiểm tra thông tin sao lưu</i>	17
<i>Hình 17. Kiểm tra trên Windows attack</i>	17
<i>Hình 18. Kết quả thực hành sao lưu tới ổ đĩa mạng</i>	18
<i>Hình 19. Cài đặt FTP Server</i>	18
<i>Hình 20. Trạng thái FTP Server</i>	19
<i>Hình 21. Chỉnh sửa file cấu hình FTP Server</i>	19
<i>Hình 22. Khởi động dịch vụ FTP</i>	20
<i>Hình 23. Tạo thư mục lưu trữ file sao lưu</i>	20
<i>Hình 24. Kiểm tra quyền người dùng</i>	20
<i>Hình 25. Sao lưu tệp lên FTP Server</i>	21
<i>Hình 26. Kiểm tra sao lưu trên máy Kali</i>	22
<i>Hình 27. Cài đặt SSH trên Kali Linux</i>	22
<i>Hình 28. Cài đặt SSH trên Ubuntu</i>	23

<i>Hình 29. Kiểm tra trạng thái tường lửa</i>	23
<i>Hình 30. Tạo SSH Key</i>	24
<i>Hình 31. Sao chép khóa công khai</i>	24
<i>Hình 32. Kiểm tra kết nối SSH</i>	25
<i>Hình 33. Tạo tệp để sao lưu</i>	25
<i>Hình 34. Sao lưu tệp từ Ubuntu sang Kali Linux</i>	26
<i>Hình 35. Kiểm tra kết quả sao lưu trên Kali Linux</i>	26

I. GIỚI THIỆU CHUNG

1. Mục đích

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

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

2. Lý thuyết

2.1. Secure Copy Protocol (SCP)

a. Khái niệm

Secure Copy Protocol (SCP) là một phương tiện truyền tệp một cách an toàn giữa một máy chủ cục bộ và một máy chủ từ xa hoặc giữa hai máy chủ từ xa, dựa trên giao thức Secure Shell (SSH). Các tệp có thể được tải lên bằng giao thức SSH với SCP. Các tệp sẽ được mã hóa khi gửi qua mạng. Cổng TCP được sử dụng để truyền SCP là cổng chuẩn SSH 22.

Secure Copy là đa nền tảng. Có các phiên bản và chương trình cho các hệ điều hành Windows, macOS, Linux, Android và iOS.

b. Cách thức hoạt động

- Xác thực: SCP yêu cầu xác thực từ cả hai máy chủ tham gia. Trước khi thực hiện truyền tải bằng giao thức này, bạn phải thiết lập kết nối SSH giữa máy chủ cục bộ và máy chủ từ xa mục tiêu. Điều này đòi hỏi thông tin đăng nhập SSH hoặc một khóa được ủy quyền cho xác thực khóa công khai.
- Truyền tải dữ liệu: Sau khi kết nối SSH được thiết lập, SCP sử dụng kết nối này để sao chép và truyền tải dữ liệu một cách an toàn. Dữ liệu được mã hóa trong quá trình truyền, ngăn chặn việc truy cập trái phép và đảm bảo tính toàn vẹn của dữ liệu. Có 2 quá trình sao chép an toàn có sẵn:
 - Chế độ nguồn (Source mode): Một yêu cầu SCP ở chế độ nguồn sẽ đọc các tệp từ máy chủ từ xa được nhắm đến và gửi chúng về máy khách.
 - Chế độ đích (Sink mode): Nếu chế độ đích được sử dụng cho các yêu cầu thông qua giao thức SCP ở phía máy khách, điều này sẽ báo hiệu cho máy chủ từ xa rằng có dữ liệu đang được gửi đến và cần ghi vào máy chủ từ xa.

Các máy khách SCP thường sử dụng cờ -f (from) để kích hoạt chế độ nguồn. Để kích hoạt chế độ đích và truyền dữ liệu đến máy chủ từ xa được nhắm đến, cờ -t (to) được sử dụng thay thế.

c. Cách sử dụng cơ bản

- Sao chép tệp từ máy cục bộ đến máy từ xa:
`scp [tùy chọn] nguồn người_dùng@máy_chủ_từ_xa:đích`
- Sao chép tệp từ máy từ xa đến máy cục bộ:
`scp [tùy chọn] người_dùng@máy_chủ_từ_xa:nguồn đích`

d. Ưu nhược điểm của SCP

Ưu điểm:

- Bảo mật: Sử dụng SSH, SCP đảm bảo dữ liệu được mã hóa trong suốt quá trình truyền tải, bảo vệ dữ liệu an toàn
- Đơn giản và hiệu quả: SCP cho phép truyền tải tệp nhanh chóng và dễ dàng thông qua dòng lệnh mà không cần cài đặt thêm phần mềm phức tạp.

Nhược điểm:

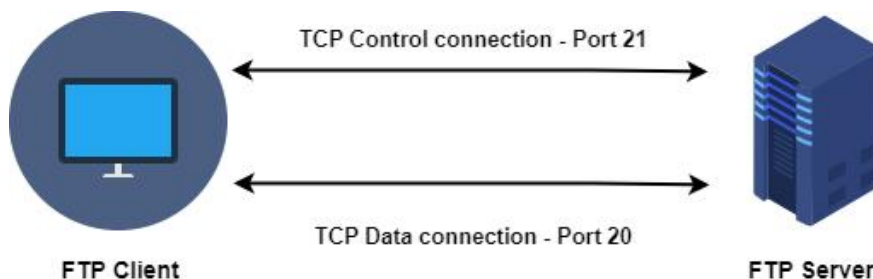
- Ít chức năng: SCP chủ yếu chức năng là truyền tải tệp và không hỗ trợ các chức năng quản lý tệp nâng cao.
- Dễ gián đoạn: SCP không hỗ trợ tiếp tục từ điểm dừng mà phải bắt đầu lại từ đầu nếu truyền tải bị gián đoạn.

2.2. File Transfer Protocol (FTP)

a. Khái niệm

Giao thức truyền tệp hay FTP cho phép người dùng truyền tệp từ máy này sang máy khác từ xa thông qua mạng TCP/IP. Hạn chế của việc sử dụng FTP là dữ liệu được gửi dưới dạng văn bản không được mã hóa.

b. Kết nối TCP trong FTP



Hình 1. Kết nối TCP trong FTP

Giống như hầu hết các giao thức TCP/IP, FTP dựa trên mô hình Client - Server. Tuy nhiên, FTP cần tới 2 kết nối TCP:

- Control connection (sử dụng port 21 – trên server): Đây là kết nối TCP logic chính được tạo ra khi phiên làm việc được thiết lập. Nó được thực hiện giữa

các quá trình điều khiển. Nó được duy trì trong suốt phiên làm việc và chỉ cho các thông tin điều khiển đi qua như lệnh hay response(phản hồi)

- Data connection (sử dụng port 20 – trên server): Kết nối này sử dụng các quy tắc rất phức tạp vì các loại dữ liệu có thể khác nhau. Nó được thực hiện giữa các quá trình truyền dữ liệu. Kết nối này mở khi có lệnh chuyển tệp và đóng khi tệp truyền xong.

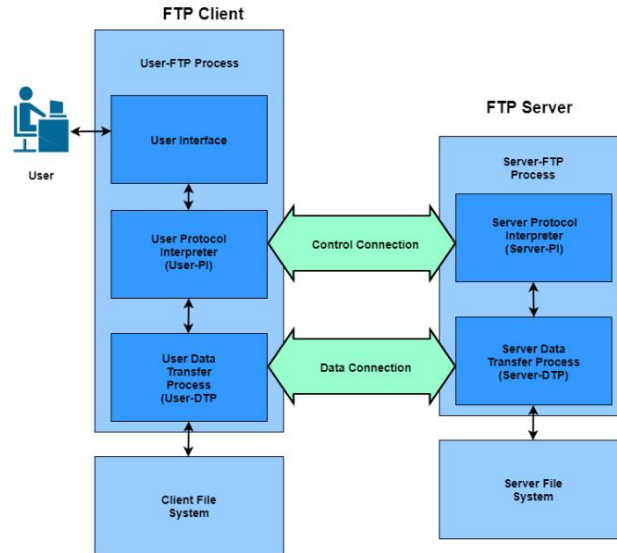
Có 2 chế độ kết nối chính:

- Active Mode (Chế độ chủ động): Trong chế độ Active Mode, máy khách mở một cổng ngẫu nhiên (>1024) trên máy của mình và thông báo cổng này cho máy chủ qua cổng điều khiển của FTP. Máy chủ thực hiện kết nối đến cổng đã được chỉ định trên máy khách để truyền dữ liệu. Đây là phương pháp truyền dữ liệu truyền thống của FTP, nhưng có thể bị chặn bởi tường lửa do server cần kết nối ngược lại với máy khách.
- Passive Mode (Chế độ bị động): Trong chế độ Passive Mode, máy khách mở một kết nối điều khiển đến máy chủ và yêu cầu một cổng để truyền dữ liệu. Máy chủ thông báo cho máy khách về cổng dữ liệu và máy khách thực hiện kết nối dữ liệu trực tiếp tới cổng này trên máy chủ. Phương pháp này ít gặp vấn đề với tường lửa và thương an toàn hơn trong môi trường mạng phức tạp và lưu lượng truy cập lớn.

c. Phương thức truyền dữ liệu trong FTP

- Stream Mode (Mặc định): Truyền dữ liệu liên tiếp dưới dạng byte không cấu trúc. Thiết bị gửi chỉ đơn thuần đẩy luồng dữ liệu qua kết nối TCP tới phía nhận. Kết thúc bằng EOF hoặc đóng kết nối.
- Block Mode: Phương thức truyền dữ liệu mang tính quy chuẩn hơn. Chia dữ liệu thành các khối nhỏ và đóng gói thành các FTP block. Mỗi block có 1 trường Header 3 byte (báo hiệu độ dài và chứa thông tin về các khối dữ liệu đang được gửi. Phù hợp truyền file lớn và kháng lỗi tốt hơn do sử dụng một thuật toán đặc biệt được sử dụng để kiểm tra các dữ liệu đã truyền đi.
- Compressed Mode: Nén dữ liệu trước khi truyền bằng Run-Length Encoding, giúp tiết kiệm băng thông. Trong thực tế, việc nén dữ liệu thường được thực hiện ở chỗ khác, làm phương thức này trở nên không cần thiết.
- Extended Block Mode: Một biến thể nâng cao của Block Mode, cho phép truyền dữ liệu nhanh hơn bằng cách sử dụng cơ chế kiểm soát lỗi và phân đoạn tối ưu hơn.

d. Mô hình FTP



Hình 2. Mô hình FTP

Mô hình FTP chia mỗi thiết bị thành 2 phần giao thức logic chịu trách nhiệm cho mỗi kết nối ở trên:

- Protocol interpreter (PI): Là thành phần quản lý kênh điều khiển, phát và nhận lệnh và trả lời.
- Data transfer process (DTP): chịu trách nhiệm gửi và nhận dữ liệu giữa client và server.

Chức năng từng phần trong mô hình FTP:

Phía Server:

- Server Protocol Interpreter (Server-PI) : Chịu trách nhiệm quản lý Control Connection trên Server. Nó lắng nghe yêu cầu kết nối hướng từ User trên cổng 21. Khi kết nối được thiết lập, nó nhận lệnh từ User-PI, gửi phản hồi và quản lý tiến trình truyền dữ liệu trên Server.
- Server Data Transfer Process (Server-DTP) : chịu trách nhiệm nhận và gửi file từ User-DTP. Server-DTP vừa làm nhiệm vụ thiết lập Data Connection và lắng nghe Data Connection của User thông qua cổng 20. Nó tương tác với Server File System trên hệ thống cục bộ để đọc và chép file.

Phía Client:

- User Interface: Đây là chương trình được chạy trên máy tính cung cấp giao diện xử lý cho người dùng, chỉ có trên phía Client.
- User Protocol Interpreter (User-PI): Chịu trách nhiệm quản lý Control Connection phía Client. Nó khởi tạo phiên kết nối FTP bằng việc phát hiện ra Request tới Server-PI. Sau khi kết nối được thiết lập, nó xử lý các lệnh nhận

được trên User Interface, gửi chúng tới Server-PI rồi đợi nhận Response trở lại. Nó cũng quản lý các tiến trình trên Client.

- User Data Transfer Process (User-DTP): Có nhiệm vụ gửi hoặc nhận dữ liệu từ Server-DTP. User-DTP có thể thiết lập hoặc lắng nghe DataConnection từ Server thông qua cổng 20. Nó tương tác với Client File System trên Client để lưu trữ file.

e. Các phương thức kết nối FTP

FTP có hai phương thức truy cập phổ biến:

- Anonymous FTP (FTP ẩn danh): không cần tài khoản, ai cũng có thể kết nối và tải dữ liệu công khai. Thường sử dụng trong việc phân phối phần mềm hoặc tài liệu công khai.
- Authenticated FTP (FTP có xác thực): Yêu cầu đăng nhập, được sử dụng để quản lý tệp riêng tư trên server.

f. Một số lệnh FTP cơ bản

Lệnh	Chức năng
ftp [server]	Kết nối đến máy chủ FTP
quit hoặc bye	Thoát khỏi phiên làm việc FTP
get [tên tập tin]	Tải tập tin từ server về máy
put [tên tập tin]	Tải tập tin từ máy lên server
delete [tên tập tin]	Xóa tập tin trên server

g. Ưu nhược điểm của FTP

Ưu điểm:

- Hỗ trợ truyền tải tệp lớn hơn so với các giao thức như HTTP
- Truyền dữ liệu hiệu quả, hỗ trợ nhiều phương thức truyền dữ liệu
- Hỗ trợ nhiều chế độ kết nối và phương thức bảo mật
- Hỗ trợ quyền truy cập và quản lý file từ xa

Nhược điểm:

- Dữ liệu truyền qua FTP không được mã hóa nếu không dùng FTPS hoặc SFTP
- FTP truyền dữ liệu khá chậm so với các giao thức hiện đại như HTTP hoặc SCP
- Không có chức năng theo dõi thay đổi như các hệ thống quản lý tệp hiện đại

- Dễ bị tường lửa chặn trong Active Mode

2.3. Network Drive (Ổ đĩa mạng)

a. Khái niệm

Ổ đĩa mạng là thiết bị lưu trữ được chia sẻ trên mạng cục bộ (LAN), cho phép người dùng truy cập và lưu trữ dữ liệu từ nhiều thiết bị khác nhau. Nó có thể là thiết bị vật lý như máy chủ, hệ thống lưu trữ gắn mạng (NAS), mạng lưu trữ (SAN) hoặc là dịch vụ lưu trữ đám mây như Google Drive, OneDrive, Dropbox.

b. Các giao thức truy cập ổ đĩa mạng

- SMB (Server Message Block): Chủ yếu được sử dụng trong hệ điều hành Windows, hỗ trợ chia sẻ tệp tin, máy in và truyền dữ liệu.
- NFS (Network File System): Giao thức phổ biến trong môi trường Linux và Unix, cho phép máy khách truy cập tệp từ xa giống như ổ đĩa cục bộ.
- FTP (File Transfer Protocol): Một cách đơn giản để truyền tệp qua mạng nhưng không hỗ trợ tính năng ổ đĩa như SMB hoặc NFS.
- iSCSI (Internet Small Computer Systems Interface): Một giao thức giúp kết nối máy chủ với lưu trữ từ xa như một ổ đĩa vật lý thực sự.

c. Các loại ổ đĩa

- Ổ đĩa cục bộ (Local Drive): Kết nối trực tiếp với máy tính, ví dụ ổ cứng HDD, SSD.
- Ổ đĩa mạng (Network Drive): Lưu trữ trên một máy chủ hoặc thiết bị NAS, truy cập qua mạng.
- Ổ đĩa được ánh xạ (Mapped Drive): Gán một ký tự ổ đĩa (ví dụ Z:) cho ổ đĩa mạng, giúp truy cập dễ dàng như ổ đĩa cục bộ.

d. Ưu nhược điểm của ổ đĩa mạng

Ưu điểm	Nhược điểm
<ul style="list-style-type: none"> • Dễ dàng chia sẻ dữ liệu mà không tốn tài nguyên máy tính cá nhân. • Có thể truy cập từ bất kỳ thiết bị nào trong mạng hoặc qua internet. • Sao lưu an toàn, hạn chế rủi ro mất dữ liệu. • Nhiều người dùng có thể chỉnh sửa, chia sẻ tệp dễ dàng. 	<ul style="list-style-type: none"> • Phụ thuộc vào mạng, không có kết nối mạng thì không thể truy cập. • Hiệu suất thấp hơn ổ cứng cục bộ do phụ thuộc tốc độ mạng. • Dữ liệu dễ bị tấn công nếu không có cơ chế bảo vệ tốt.

e. Quyền truy cập vào ổ đĩa mạng

- Chỉ đọc (Read-Only): Người dùng chỉ có thể xem hoặc sao chép tệp nhưng không thể sửa đổi hoặc lưu dữ liệu mới vào đó.
- Đọc/ghi (Read/Write): Người dùng có thể xem, chỉnh sửa, xóa hoặc tải tệp lên ổ đĩa.

f. Bảo mật ổ đĩa mạng

- Phân quyền người dùng
- Mã hóa dữ liệu, đặc biệt với các dữ liệu nhạy cảm
- VPN (Virtual Private Network): Kết nối an toàn từ xa đến ổ đĩa mạng qua Internet
- Một số NAS cao cấp có tính năng phát hiện mã độc và hỗ trợ snapshot để khôi phục dữ liệu

2.4. Lệnh net use

Lệnh net use được sử dụng để kết nối, ngắt kết nối hoặc hiển thị thông tin về ổ đĩa mạng (Network Drive) trong hệ điều hành Windows. Nó giúp ánh xạ một thư mục hoặc tài nguyên chia sẻ từ xa vào hệ thống của bạn dưới dạng một ổ đĩa ảo.

Cú pháp cơ bản:

```
net use [DriveLetter:] \\ServerName\ShareName [Password] [/user:UserName] [/persistent:{yes | no}]
```

Các tùy chọn quan trọng của net use:

- Hiển thị danh sách các ổ đĩa mạng đã kết nối:

```
net use
```

→ Liệt kê tất cả các kết nối mạng hiện tại trên máy.

- Ánh xạ ổ đĩa mạng:

```
net use Z: \\192.168.1.100\SharedFolder /user:Admin password
```

→ Lệnh này ánh xạ thư mục SharedFolder trên máy chủ 192.168.1.100 thành ổ đĩa Z: và đăng nhập bằng tài khoản Admin.

- Ngắt kết nối ổ đĩa mạng:

```
net use Z: /delete
```

→ Ngắt kết nối ổ Z: khỏi hệ thống.

- Ngắt kết nối tất cả các ổ đĩa mạng:

```
net use * /delete
```

→ Xóa tất cả các ổ đĩa mạng đã kết nối.

- Kết nối mạng vĩnh viễn (tự động khởi động lại khi máy tính khởi động lại):

`net use Z: \\192.168.1.100\SharedFolder /persistent:yes`

→ Kết nối sẽ vẫn tồn tại ngay cả sau khi khởi động lại máy tính.

2.5. Lệnh net view

Lệnh net view được sử dụng để hiển thị danh sách các tài nguyên chia sẻ trên một máy tính trong mạng nội bộ.

Cú pháp cơ bản:

`net view [\\ComputerName] [/all]`

Các tùy chọn quan trọng của net view:

- Hiển thị tất cả các máy tính chia sẻ trong mạng LAN:

`net view`

→ Liệt kê tất cả các máy tính có tài nguyên chia sẻ trên mạng nội bộ.

- Hiển thị danh sách thư mục chia sẻ trên một máy tính cụ thể:

`net view \\192.168.1.100`

→ Lệnh này liệt kê tất cả thư mục và tài nguyên chia sẻ trên máy tính có địa chỉ IP 192.168.1.100.

- Hiển thị tất cả các thông tin chi tiết về chia sẻ mạng:

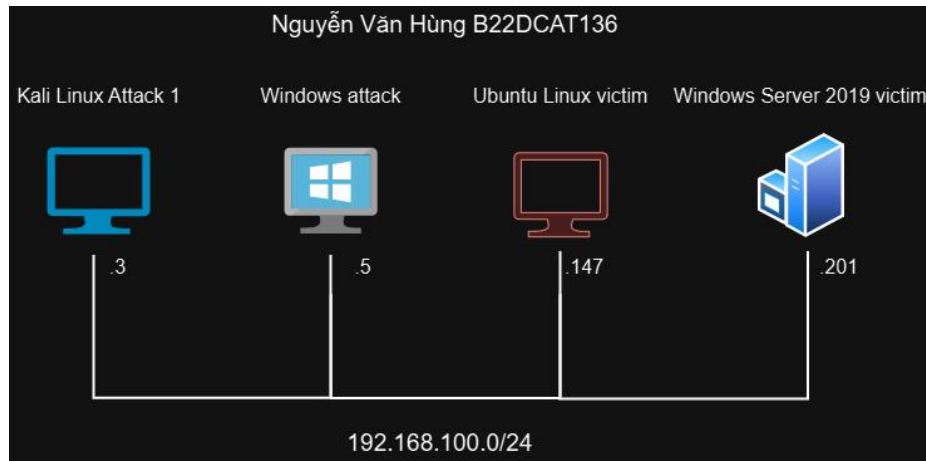
`net view /all`

→ Hiển thị danh sách đầy đủ các chia sẻ mạng, kể cả những chia sẻ ẩn.

I. NỘI DUNG THỰC HÀNH

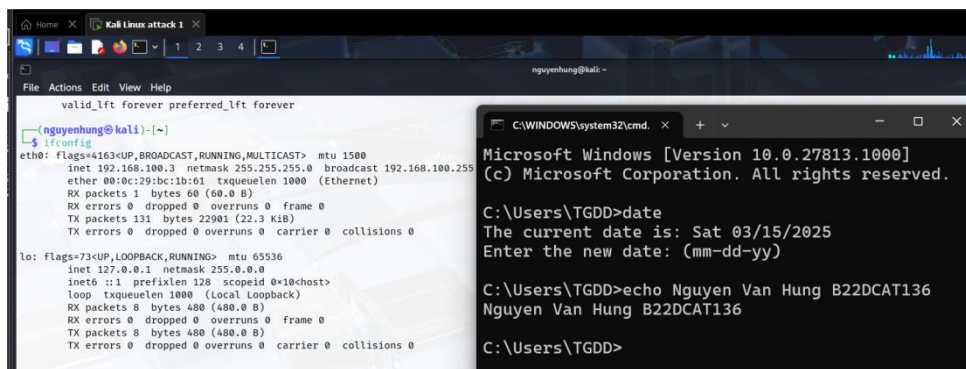
1. Chuẩn bị môi trường

- Phần mềm VMWare Workstation
- Các file máy ảo VMWare và hệ thống mạng đã cài đặt: máy Windows, máy Kali Linux, Windows Server 2019 và Ubutu.



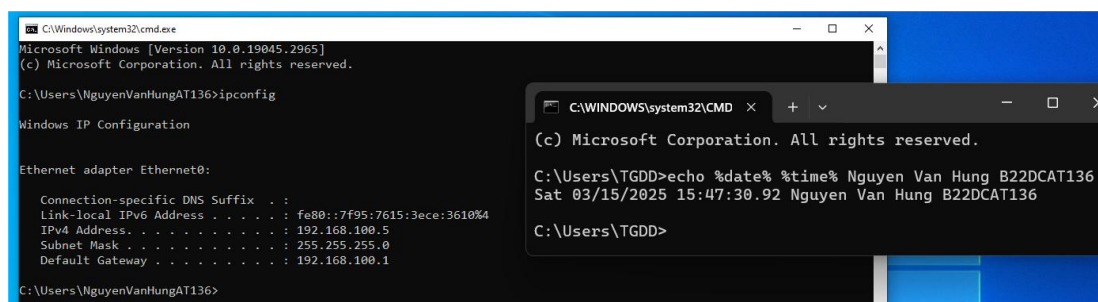
Hình 3. Internal Network

- Cấu hình các máy:
 - Máy Kali Linux Attack 1:



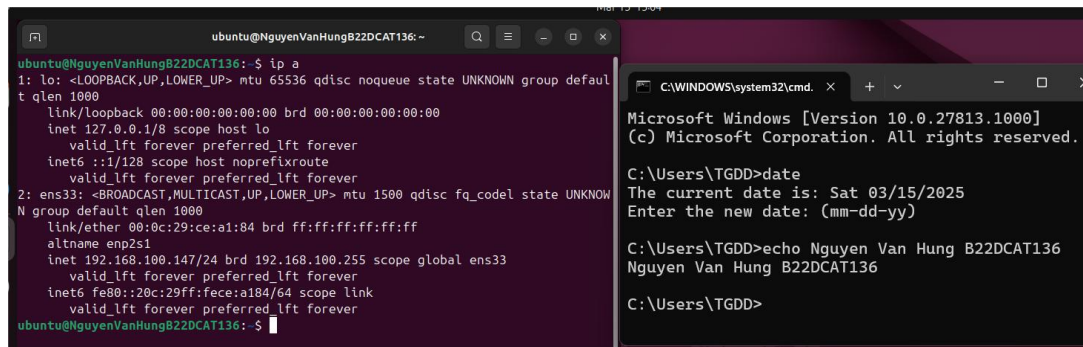
Hình 4. Máy Kali Linux attack 1

- Máy Windows attack:



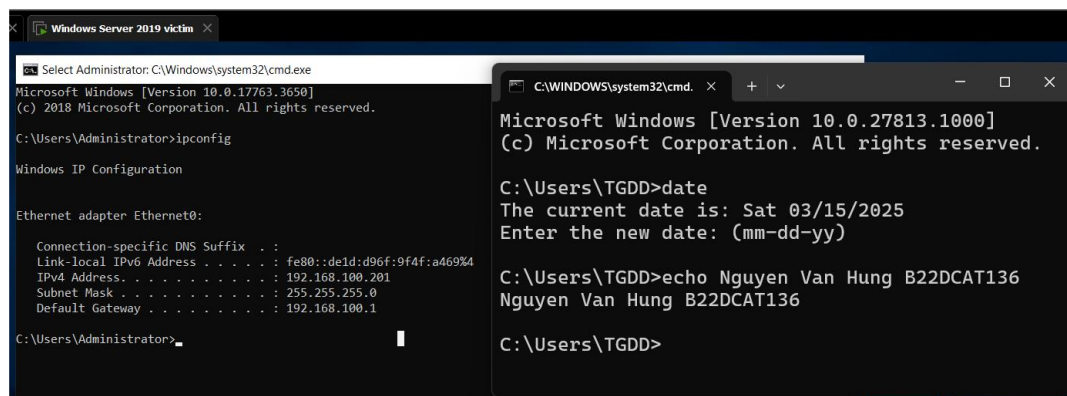
Hình 5. Máy Windows attack

- Ubuntu Linux victim



Hình 6. Ubuntu Linux victim

- Windows Server 2019 victim



Hình 7. Windows Server victim

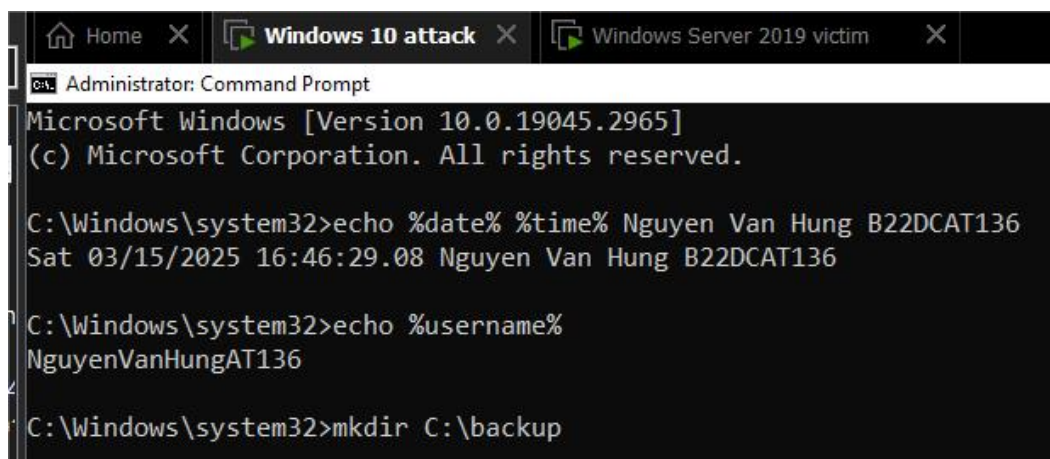
2. Thực hành

2.1. Sao lưu tối ồ đĩa mạng

a. Tạo thư mục chia sẻ trên Windows Attack

Tạo một thư mục sao lưu bằng lệnh :

`mkdir C:\backup`



Hình 8. Tạo thư mục sao lưu

Chia sẻ thư mục vừa tạo: *net share backup=C:\backup /grant:Everyone,full*

Lệnh này chia sẻ thư mục cho tất cả người dùng trong mạng với quyền đầy đủ.

```
C:\Windows\system32>net share backup=C:\backup /grant:Everyone,full
backup was shared successfully.

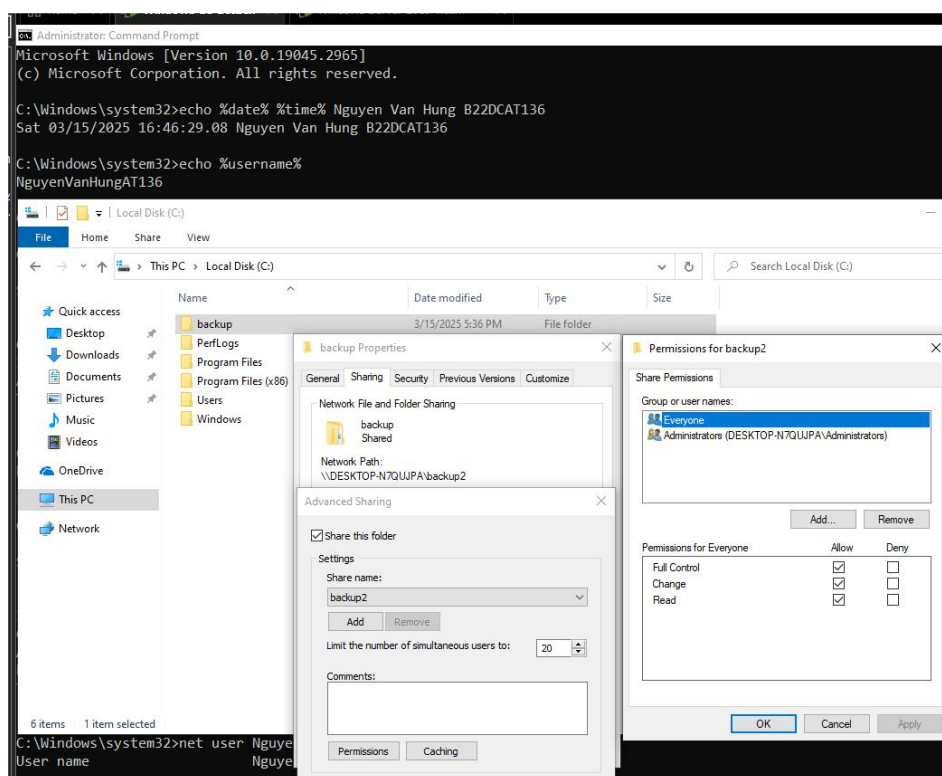
C:\Windows\system32>net share

Share name    Resource
-----
IPC$          Remote IPC
C$            C:\
ADMIN$        C:\Windows
backup        C:\backup
The command completed successfully.
```

Hình 9. Chia sẻ và kiểm tra chia sẻ thư mục

Kiểm tra thư mục đã được chia sẻ thành công: *net share*

Vào ổ C, nhấn chuột phải vào thư mục chia sẻ, chọn Properties → Sharing → Advanced Sharing → chọn Share this folder, đặt tên Share name, chọn Permissions, chọn Full Control, Apply, Ok.



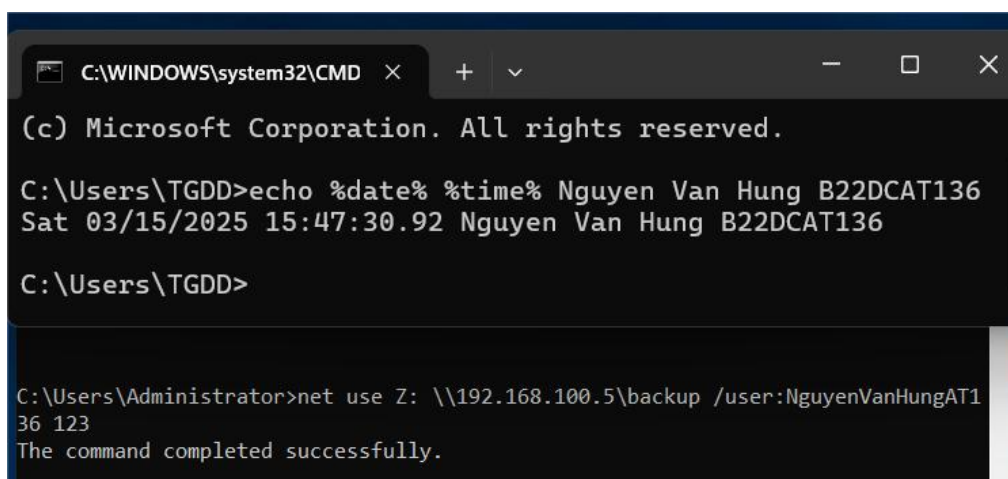
Hình 10. Cấu hình chia sẻ thư mục

b. Kết nối ổ đĩa mạng trên Windows Server 2019

Trên Windows Server 2019, ánh xạ thư mục chia sẻ thành ổ đĩa mạng bằng lệnh:

net use Z: \\192.168.100.5\backup /user:TênUser MậtKhẩu

user: TênUser MậtKhẩu là tài khoản của Windows attack



```
C:\WINDOWS\system32\CMD
(c) Microsoft Corporation. All rights reserved.

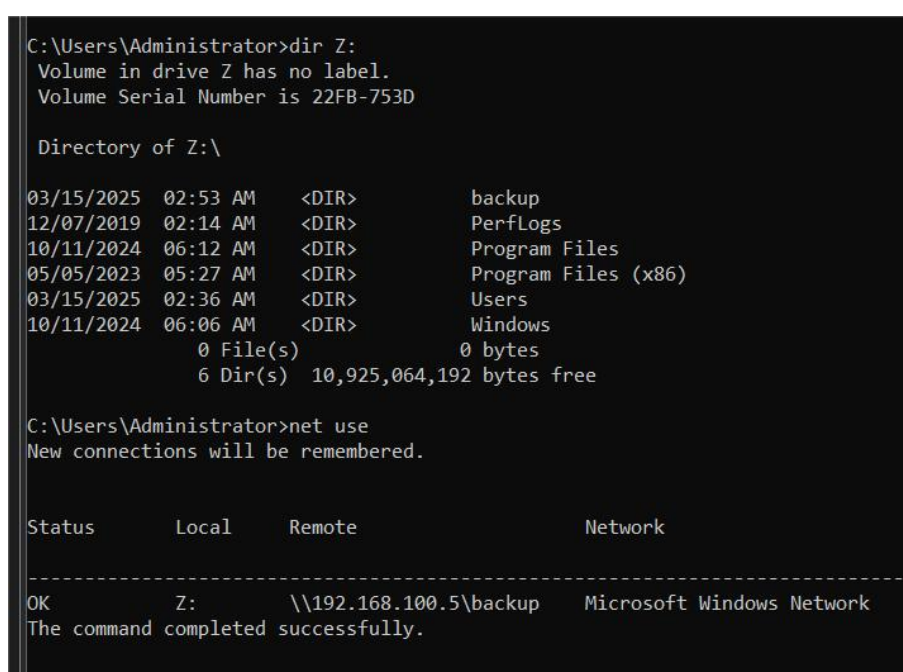
C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 15:47:30.92 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

C:\Users\Administrator>net use Z: \\192.168.100.5\backup /user:NguyenVanHungAT136 123
The command completed successfully.
```

Hình 11. Ánh xạ thư mục chia sẻ thành ổ đĩa mạng

Kiểm tra ổ đĩa mạng đã kết nối thành công:



```
C:\Users\Administrator>dir Z:
Volume in drive Z has no label.
Volume Serial Number is 22FB-753D

Directory of Z:\

03/15/2025  02:53 AM  <DIR>          backup
12/07/2019  02:14 AM  <DIR>          PerfLogs
10/11/2024  06:12 AM  <DIR>          Program Files
05/05/2023  05:27 AM  <DIR>          Program Files (x86)
03/15/2025  02:36 AM  <DIR>          Users
10/11/2024  06:06 AM  <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s) 10,925,064,192 bytes free

C:\Users\Administrator>net use
New connections will be remembered.

Status      Local      Remote              Network
-----
OK          Z:         \\192.168.100.5\backup  Microsoft Windows Network
The command completed successfully.
```

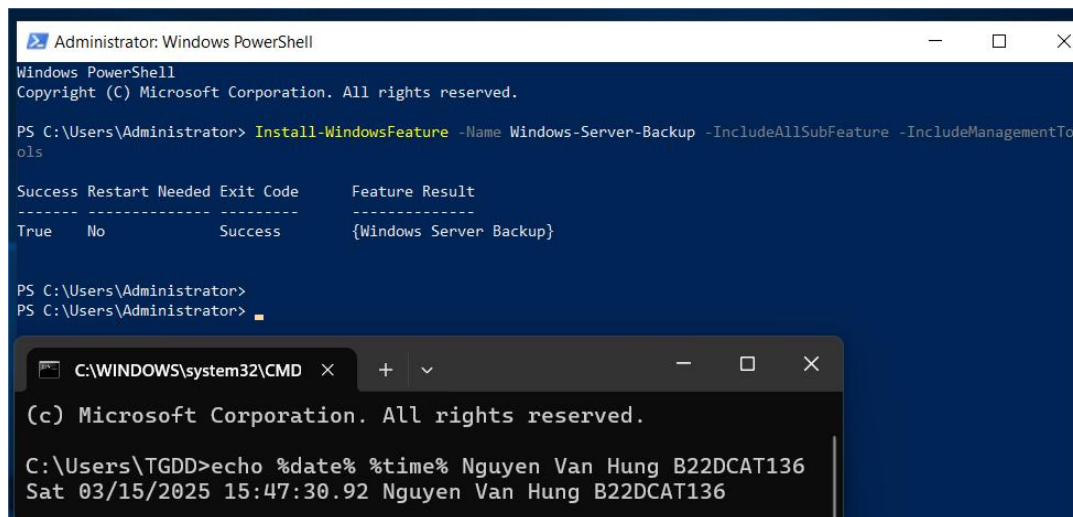
Hình 12. Kiểm tra ổ đĩa mạng

c. Sao lưu dữ liệu từ Windows Server

Trên Windows Server, sử dụng Windows Server Backup để sao lưu dữ liệu.

- Mở PowerShell với quyền Admin (Run as administrator).
- Chạy lệnh sau để cài đặt Windows Server Backup:

Install-WindowsFeature -Name Windows-Server-Backup -IncludeAllSubFeature -IncludeManagementTools



Hình 13. Cài đặt WSB

Dùng lệnh sau để sao lưu thư mục C:\Users lên thư mục chia sẻ của Windows Attack (IP Windows Attack là 192.168.100.5):

wbadmin start backup -backupTarget:\\192.168.100.5\backup -include:C:\Users -quiet

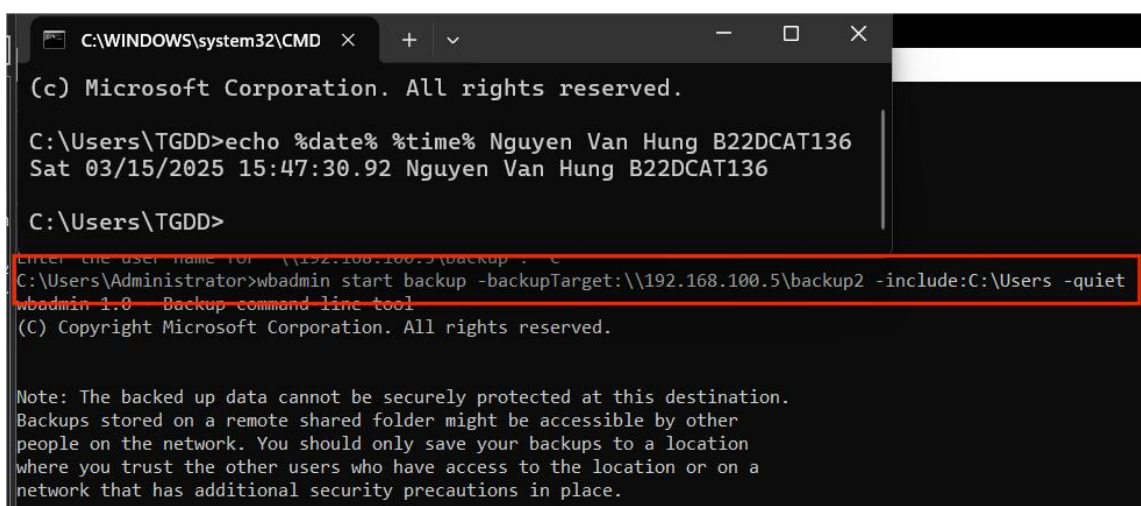
Giải thích lệnh:

wbadmin start backup: Bắt đầu sao lưu.

-backupTarget:\\192.168.100.5\backup2: Chỉ định thư mục mạng để lưu bản sao lưu.

-include:C:\Users: Chọn thư mục cần sao lưu (C:\Users).

-quiet: Chạy không cần xác nhận.



Hình 14. Sao lưu thư mục

```

File identification is complete.
The backup of volume (C:) to \\192.168.100.5\backup2 is starting...
The backup of volume (C:) completed successfully.
Summary of the backup operation:
-----

The backup operation successfully completed.
The backup of volume (C:) completed successfully.
Log of files successfully backed up:
C:\Windows\Logs\WindowsServerBackup\Backup-15-03-2025_10-36-41.log

C:\WINDOWS\system32\CMD
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 15:47:30.92 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

```

Hình 15. Sao lưu thành công

Kiểm tra thông tin sao lưu trên Windows Server:

```

C:\WINDOWS\system32\CMD
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 15:47:30.92 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

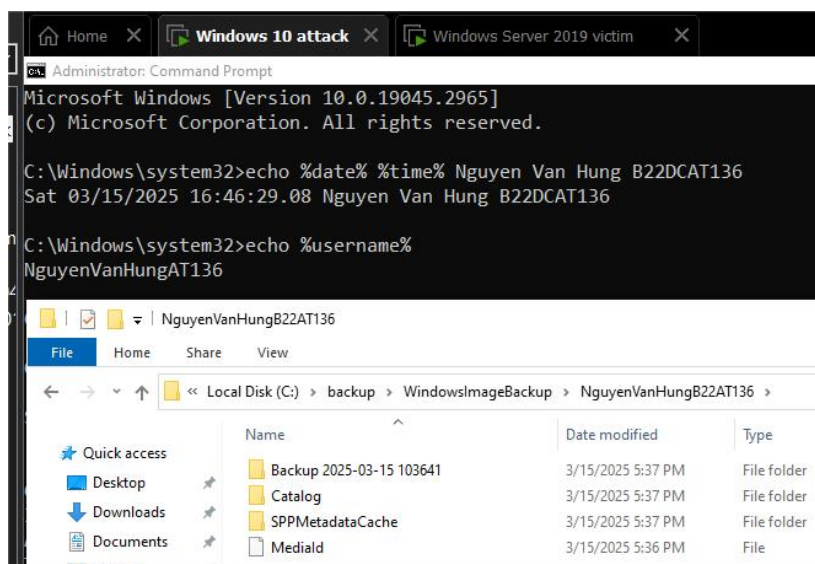
C:\Users\Administrator>wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright Microsoft Corporation. All rights reserved.

Backup time: 3/15/2025 3:36 AM
Backup location: Network Share labeled \\192.168.100.5\backup2
Version identifier: 03/15/2025-10:36
Can recover: Volume(s), File(s)

```

Hình 16. Kiểm tra thông tin sao lưu

Mở máy Windows attack kiểm tra:



Hình 17. Kiểm tra trên Windows attack

```

C:\Users\NguyenVanHungAT136>echo %username%
NguyenVanHungAT136

C:\Users\NguyenVanHungAT136>date
The current date is: Sat 03/15/2025
Enter the new date: (mm-dd-yy)

C:\Users\NguyenVanHungAT136>net share

Share name      Resource                Remark
-----
C$              C:\                    Default share
IPC$            C:\                    Remote IPC
ADMIN$          C:\Windows             Remote Admin
backup          C:\
backup2         C:\backup
The command completed successfully.

C:\Users\NguyenVanHungAT136>dir C:\backup
Volume in drive C has no label.
Volume Serial Number is 22FB-753D

Directory of C:\backup

03/15/2025  05:36 PM    <DIR>          .
03/15/2025  05:36 PM    <DIR>          ..
03/15/2025  05:36 PM    <DIR>          WindowsImageBackup
               0 File(s)              0 bytes
               3 Dir(s)          9,570,336,768 bytes free

```

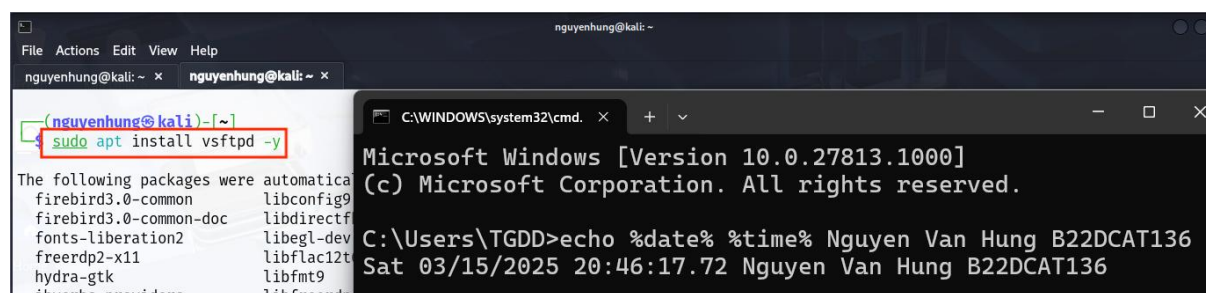
Hình 18. Kết quả thực hành sao lưu tới ổ đĩa mạng

2.2. Sao lưu tệp lên FTP Server

a. Cài đặt và cấu hình FTP Server trên máy Kali Linux

Mở máy Kali Linux, chạy lệnh `sudo apt update` để cập nhật hệ thống

Cài đặt FTP Server: `sudo apt install vsftpd -y`



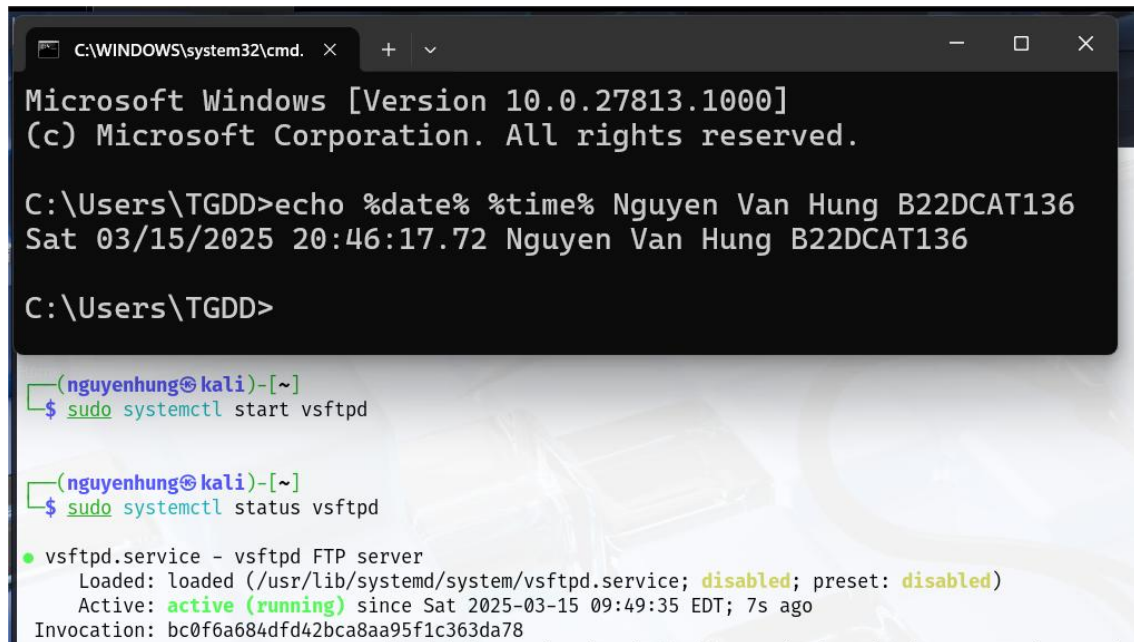
Hình 19. Cài đặt FTP Server

Kiểm tra trạng thái dịch vụ: `sudo systemctl status vsftpd`

Nếu chưa chạy, bật dịch vụ bằng các lệnh:

```
sudo systemctl start vsftpd
```

```
sudo systemctl enable vsftpd
```



```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [Version 10.0.27813.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

(nguyenhung@kali)-[~]
$ sudo systemctl start vsftpd

(nguyenhung@kali)-[~]
$ sudo systemctl status vsftpd

● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-03-15 09:49:35 EDT; 7s ago
   Invocation: bc0f6a684dfd42bca8aa95f1c363da78
```

Hình 20. Trạng thái FTP Server

Mở và chỉnh sửa file cấu hình FTP Server:

```
sudo nano /etc/vsftpd.conf
```

Tìm và đảm bảo các dòng sau được bật YES:

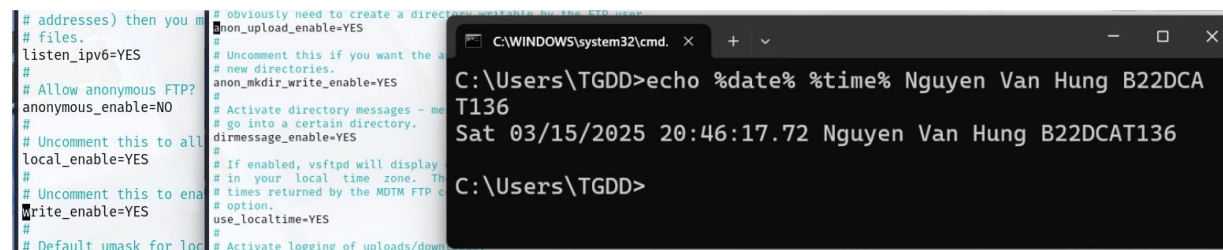
```
write_enable=YES
```

```
local_enable=YES
```

```
anon_upload_enable=YES
```

```
anon_mkdir_write_enable=YES
```

Lưu file (Ctrl + X → Y → Enter)

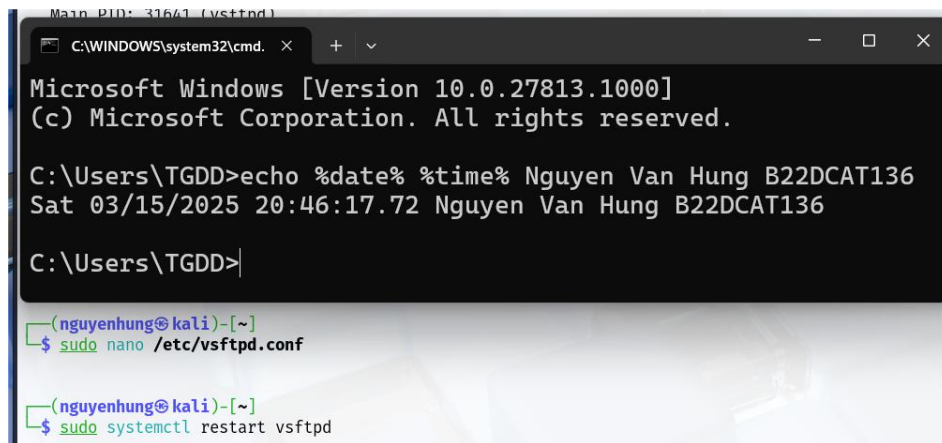


```
# addresses) then you m # obviously need to create a directory writable by the FTP user
# files. # anon_upload_enable=YES
listen_ipv6=YES # Uncomment this if you want the s
# new directories. # anon_mkdir_write_enable=YES
# Allow anonymous FTP? # Activate directory messages - m
anonymous_enable=NO # go into a certain directory. Th
# Uncomment this to all # dirmmessage_enable=YES
local_enable=YES # If enabled, vsftpd will display
# Uncomment this to ena # in your local time zone. Th
write_enable=YES # times returned by the MDTM FTP C
# option.
# use_localtime=YES
# Default umask for loc # Activate logging of uploads/down
```

Hình 21. Chỉnh sửa file cấu hình FTP Server

Sau đó khởi động lại dịch vụ FTP:

```
sudo systemctl restart vsftpd
```



```
Microsoft Windows [Version 10.0.27813.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136

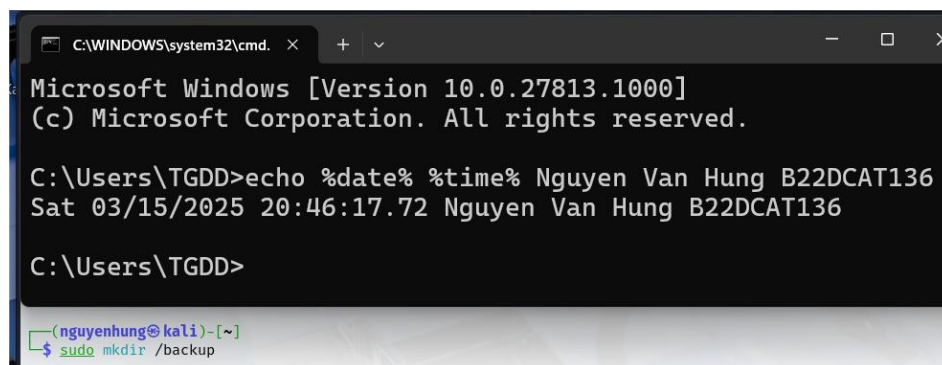
C:\Users\TGDD>

(nguyenhung@kali)-[~]
$ sudo nano /etc/vsftpd.conf

(nguyenhung@kali)-[~]
$ sudo systemctl restart vsftpd
```

Hình 22. Khởi động dịch vụ FTP

Tạo thư mục để lưu trữ file sao lưu: `sudo mkdir /backup`



```
Microsoft Windows [Version 10.0.27813.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

(nguyenhung@kali)-[~]
$ sudo mkdir /backup
```

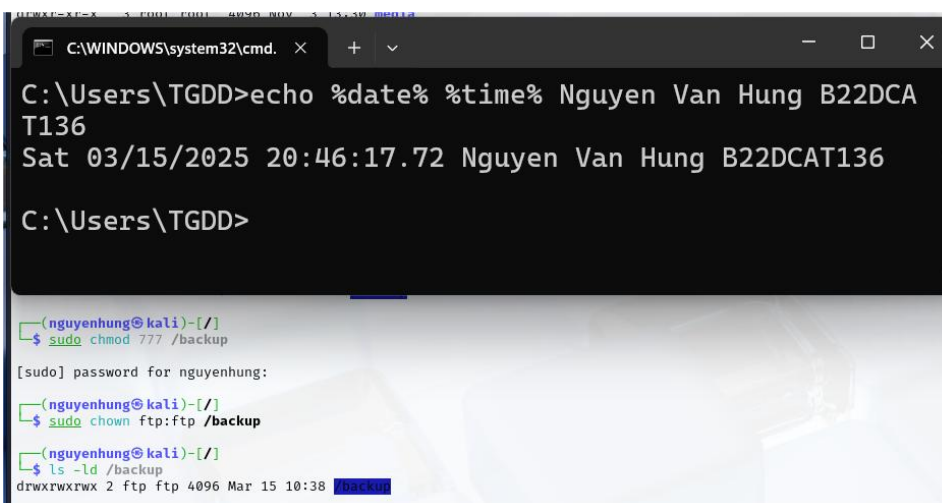
Hình 23. Tạo thư mục lưu trữ file sao lưu

Cấp quyền cho thư mục:

`sudo chmod 777 /backup`

`sudo chown ftp:ftp /backup`

Kiểm tra quyền: `ls -ld /backup`



```
Microsoft Windows [Version 10.0.27813.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCA
T136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

(nguyenhung@kali)-[/]
$ sudo chmod 777 /backup

[sudo] password for nguyenhung:

(nguyenhung@kali)-[/]
$ sudo chown ftp:ftp /backup

(nguyenhung@kali)-[/]
$ ls -ld /backup
drwxrwxrwx 2 ftp ftp 4096 Mar 15 10:38 /backup
```

Hình 24. Kiểm tra quyền người dùng

b. Cài đặt và sử dụng FTP Client trên Windows victim

Mở cmd trên Windows victim, gõ lệnh *ftp*, nếu xuất hiện *ftp>* thì FTP Client đã có sẵn. Nếu báo lỗi, cần bật tính năng này:

- Control Panel → Programs and Features → Turn Windows features on or off
- Bật FTP Client và nhấn OK.

Tiến hành sao lưu thư mục trên máy Windows victim (file *Tmp.zip* được tạo ra để sao lưu):

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\NguyenVanHungAT136>echo %username% %date%
NguyenVanHungAT136 Sat 03/15/2025

C:\Users\NguyenVanHungAT136>dir /b C:\Windows\System32\ | findstr /i "ftp"
ftp.exe
msieftp.dll
softpub.dll

C:\Users\NguyenVanHungAT136>ftp 192.168.100.3
Connected to 192.168.100.3.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
User (192.168.100.3:(none)): nguyenhung
331 Please specify the password.
Password:
230 Login successful.
ftp> binary
200 Switching to Binary mode.
ftp> lcd C:\
Local directory now C:\.
ftp> cd \backup
550 Failed to change directory.
ftp> cd /backup
250 Directory successfully changed.
ftp> put Tmp.zip
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 212645 bytes sent in 0.00Seconds 212645000.00Kbytes/sec.
ftp> bye
221 Goodbye.
```

Hình 25. Sao lưu tệp lên FTP Server

ftp 192.168.100.3

Đăng nhập tài khoản máy kết nối

Bật chế độ truyền binary để không lỗi file: *binary*

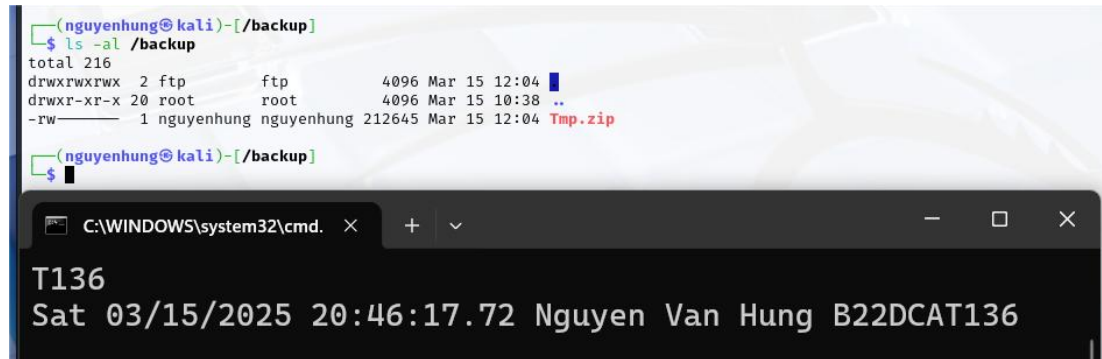
Chuyển đến thư mục cần sao lưu: *lcd C:*

Chuyển đến thư mục đích trên máy Kali Linux: *cd /backup*

Tải tệp lên thư mục đích: *put Tmp.zip*

Thoát FTP: *bye*

Kiểm tra bên Kali Linux:



Hình 26. Kiểm tra sao lưu trên máy Kali

2.3. Sao lưu tệp sử dụng SCP

a. Cài đặt và cấu hình SSH

Trên máy Kali Linux, cài đặt SSH:

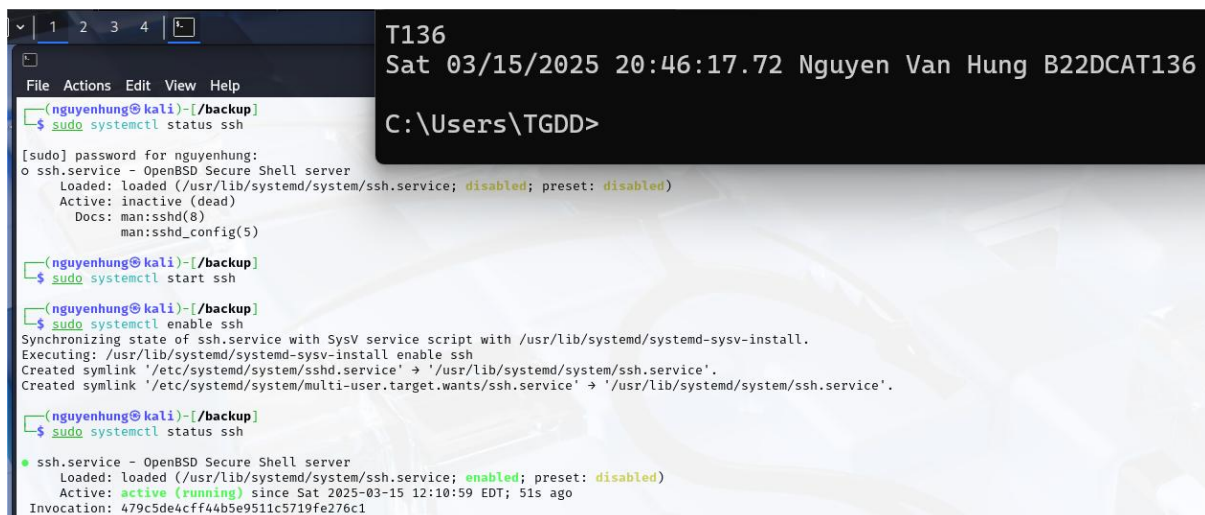
sudo apt update

sudo apt install -y openssh-server

Nếu SSH chưa chạy, khởi động dịch vụ:

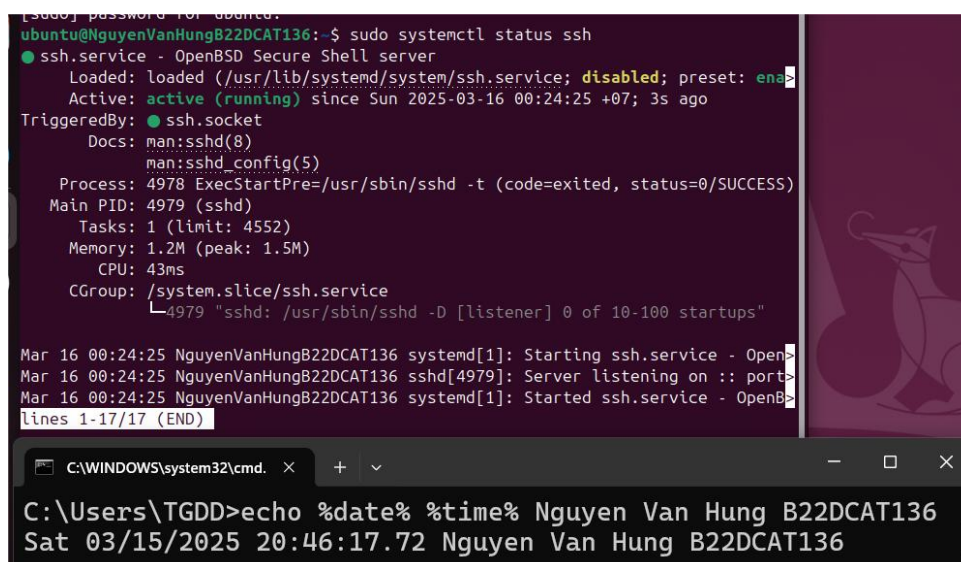
sudo systemctl start ssh

sudo systemctl enable ssh



Hình 27. Cài đặt SSH trên Kali Linux

Tương tự, cài đặt trên máy Ubuntu:



```
[sudo] password for ubuntu:
ubuntu@NguyenVanHungB22DCAT136:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: ena>
   Active: active (running) since Sun 2025-03-16 00:24:25 +07; 3s ago
   TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 4978 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 4979 (sshd)
     Tasks: 1 (limit: 4552)
    Memory: 1.2M (peak: 1.5M)
       CPU: 43ms
    CGroup: /system.slice/ssh.service
           └─4979 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 16 00:24:25 NguyenVanHungB22DCAT136 systemd[1]: Starting ssh.service - Open>
Mar 16 00:24:25 NguyenVanHungB22DCAT136 sshd[4979]: Server listening on :: ports>
Mar 16 00:24:25 NguyenVanHungB22DCAT136 systemd[1]: Started ssh.service - OpenB>
lines 1-17/17 (END)

C:\WINDOWS\system32\cmd. x + v
C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136
```

Hình 28. Cài đặt SSH trên Ubuntu

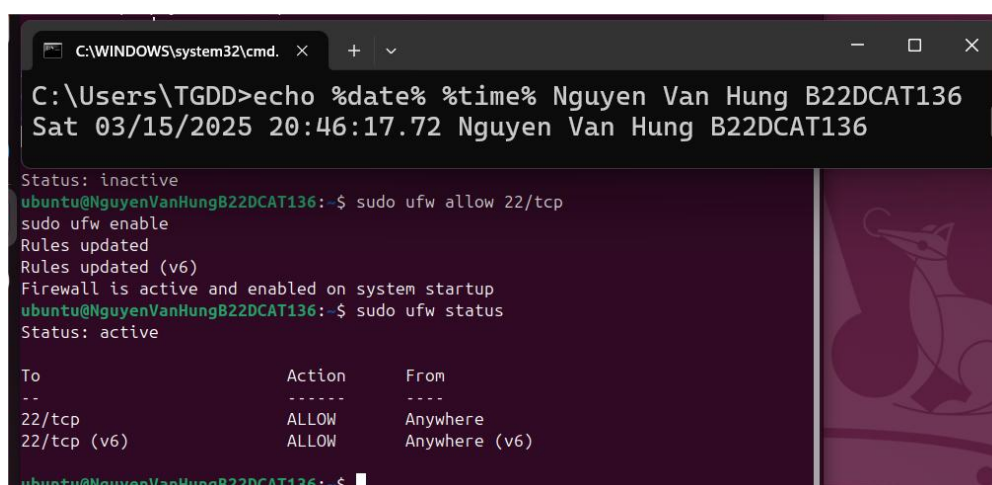
Kiểm tra tường lửa trên máy victim, chạy lệnh sau để mở cổng SSH:

```
sudo ufw allow 22/tcp
```

```
sudo ufw enable
```

Kiểm tra lại trạng thái tường lửa: `sudo ufw status`

Nếu thấy dòng 22/tcp ALLOW, nghĩa là cổng SSH đã được mở



```
C:\WINDOWS\system32\cmd. x + v
C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136

ubuntu@NguyenVanHungB22DCAT136:~$ sudo ufw allow 22/tcp
sudo ufw enable
Rules updated
Rules updated (v6)
Firewall is active and enabled on system startup
ubuntu@NguyenVanHungB22DCAT136:~$ sudo ufw status
Status: active

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

ubuntu@NguyenVanHungB22DCAT136:~$
```

Hình 29. Kiểm tra trạng thái tường lửa

b. Tạo Secure Shell Keys trên Kali Linux

Tạo Secure Shell Keys:

```
ssh-keygen -t rsa -b 4096 -C "Nguyen Van Hung B22DCAT136"
```

Giải thích:

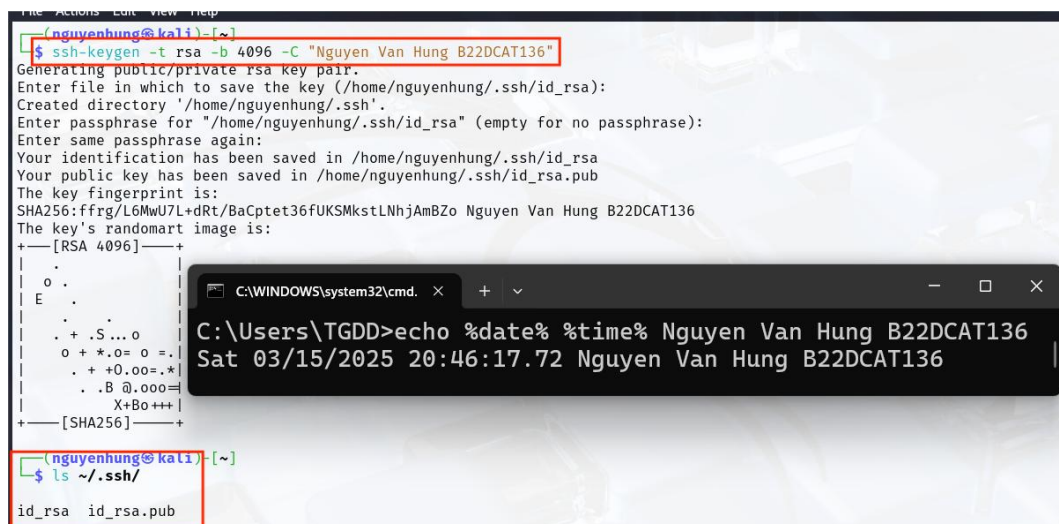
- ssh-keygen: Lệnh tạo cặp khóa SSH.

- -t rsa: Chọn thuật toán mã hóa RSA (một trong những thuật toán phổ biến nhất cho SSH).
- -b 4096: Tạo khóa có độ dài 4096 bit (càng dài, càng bảo mật hơn).
- -C "Nguyen Van Hung B22DCAT136": Thêm phần mô tả cho key (comment) – thường là tên và mã sinh viên của bạn để dễ nhận diện.

Sau khi chạy lệnh, hệ thống sẽ hỏi nơi lưu trữ khóa, nếu bạn nhấn enter, nó sẽ lưu tại mặc định:

- ~/.ssh/id_rsa # Khóa riêng tư
- ~/.ssh/id_rsa.pub # Khóa công khai

Kiểm tra key đã tạo ra: `ls ~/.ssh/`

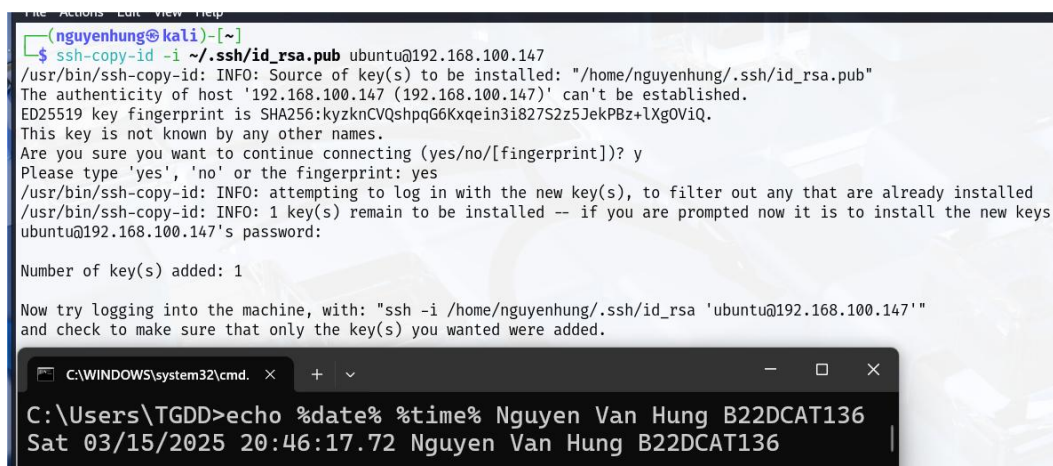


```
(nguyenhung@kali)~$ ssh-keygen -t rsa -b 4096 -C "Nguyen Van Hung B22DCAT136"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/nguyenhung/.ssh/id_rsa):
Created directory '/home/nguyenhung/.ssh'.
Enter passphrase for "/home/nguyenhung/.ssh/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nguyenhung/.ssh/id_rsa
Your public key has been saved in /home/nguyenhung/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:ffrg/L6MwU7L+dRt/BaCptet36fUKSMkstLNhJAmBZo Nguyen Van Hung B22DCAT136
The key's randomart image is:
+--[RSA 4096]--+
|  .
| o .
| E
|
| . + .S...o
| o + *.o = o =.
| . + +.o.o =.+.
| .B @.ooo=
| X+B@+++
+--[SHA256]--+
(nguyenhung@kali)~$ ls ~/.ssh/
id_rsa  id_rsa.pub
```

Hình 30. Tạo SSH Key

Sao chép khóa công khai sang máy Ubuntu:

`ssh-copy-id -i ~/.ssh/id_rsa.pub ubuntu@192.168.100.147`



```
(nguyenhung@kali)~$ ssh-copy-id -i ~/.ssh/id_rsa.pub ubuntu@192.168.100.147
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/nguyenhung/.ssh/id_rsa.pub"
The authenticity of host '192.168.100.147 (192.168.100.147)' can't be established.
ED25519 key fingerprint is SHA256:kyzknCVqshpqG6Kxqein3i827S2z5JekPBz+LXgOviQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
ubuntu@192.168.100.147's password:

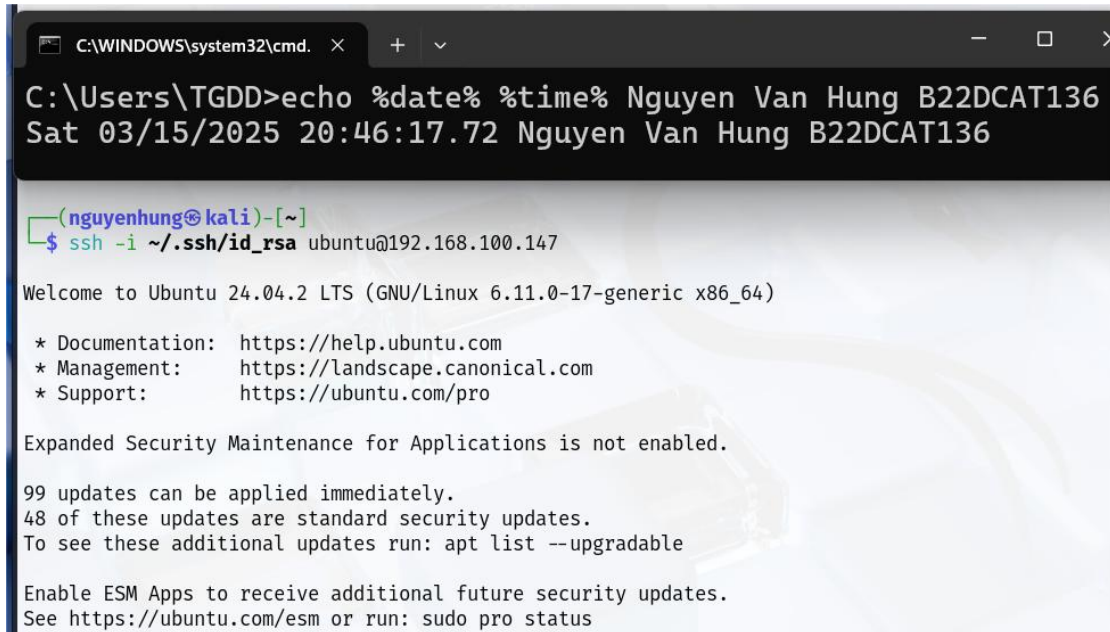
Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i /home/nguyenhung/.ssh/id_rsa 'ubuntu@192.168.100.147'"
and check to make sure that only the key(s) you wanted were added.
```

Hình 31. Sao chép khóa công khai

Kiểm tra kết nối SSH không cần mật khẩu từ Kali Linux vào Ubuntu victim:

```
ssh -i ~/.ssh/id_rsa ubuntu@192.168.100.147
```

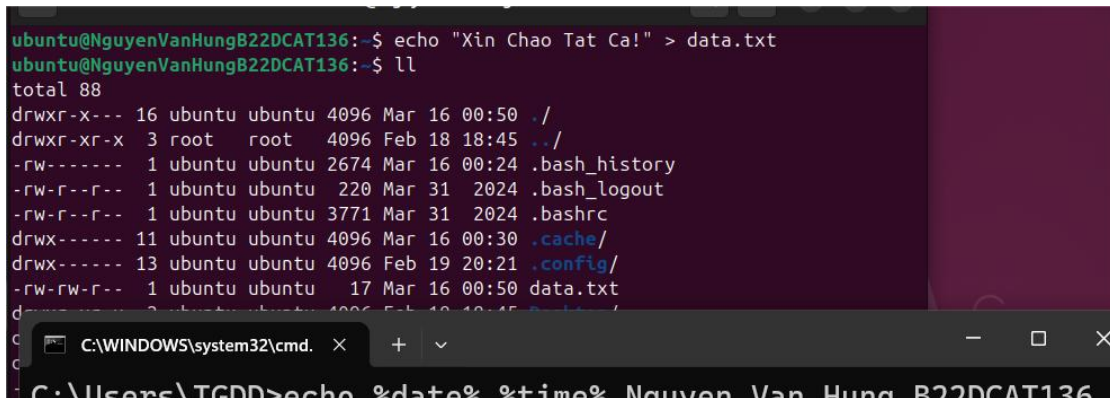


Hình 32. Kiểm tra kết nối SSH

Nếu kết nối thành công mà không yêu cầu mật khẩu, nghĩa là thiết lập SSH Key đúng cách.

c. Sao lưu tệp từ máy victim sử dụng SCP

Mở Ubuntu victim, tạo một tệp để sao lưu:



Hình 33. Tạo tệp để sao lưu

Thực hiện sao lưu bằng SCP:

```
scp /home/ubuntu/data.txt nguyenhung@192.168.100.3:/backup
```

Giải thích:

- /home/ubuntu/data.txt → Đường dẫn tệp trên victim.
- nguyenhung@192.168.100.3:/backup → Đích đến trên Kali Linux

```
ubuntu@NguyenVanHungB22DCAT136:~$ scp /home/ubuntu/data.txt nguyenhung@192.168.100.3:/backup
The authenticity of host '192.168.100.3 (192.168.100.3)' can't be established.
ED25519 key fingerprint is SHA256:qZDyoVRBQIr3jscDtCin/V8pXPamViJ6hh7/OHTymdA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.3' (ED25519) to the list of known hosts.
nguyenhung@192.168.100.3's password:
data.txt                               100% 17   13.4KB/s   00:00
ubuntu@NguyenVanHungB22DCAT136:~$
```

```
C:\WINDOWS\system32\cmd.  x  +  v
C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136
```

Hình 34. Sao lưu tệp từ Ubuntu sang Kali Linux

Mở máy Kali Linux, kiểm tra kết quả:

```
(nguyenhung@kali)-[/]
$ cd /backup
(nguyenhung@kali)-[/backup]
$ ls
Tmp.zip  data.txt
```

```
C:\WINDOWS\system32\cmd.  x  +  v
C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 20:46:17.72 Nguyen Van Hung B22DCAT136
```

Hình 35. Kiểm tra kết quả sao lưu trên Kali Linux

TÀI LIỆU THAM KHẢO

- [1] Lab 8 pfsense firewall của CSSIA CompTIA Security+®
- [2] <https://www.ionos.com/digitalguide/server/know-how/scp-secure-copy/>
- [3] <https://www.ssh.com/academy/ssh/scp>
- [4] <https://news.cloud365.vn/ftp-tim-hieu-ve-giao-thuc-ftp/>
- [5] <https://fptshop.com.vn/tin-tuc/danh-gia/ftp-la-gi-167440>
- [6] <https://www.techtarget.com/whatis/definition/network-drive>