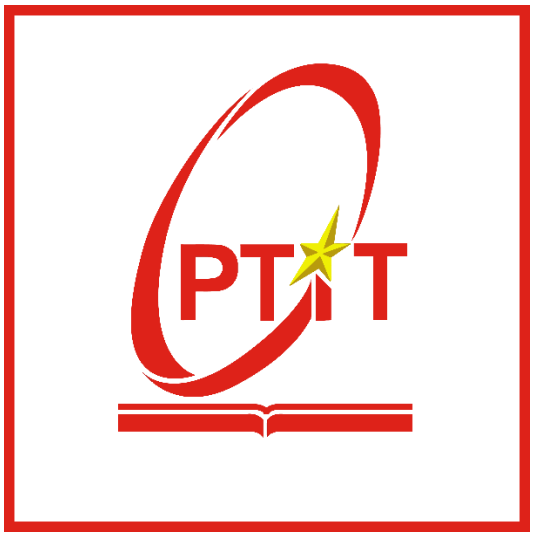
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



Môn học: **THỰC TẬP CƠ SỞ**

BÁO CÁO BÀI THỰC HÀNH SỐ 10

SAO LƯU HỆ THỐNG

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 4/2024 ~

Mục Lục

Bài 10: Sao lưu hệ thống

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

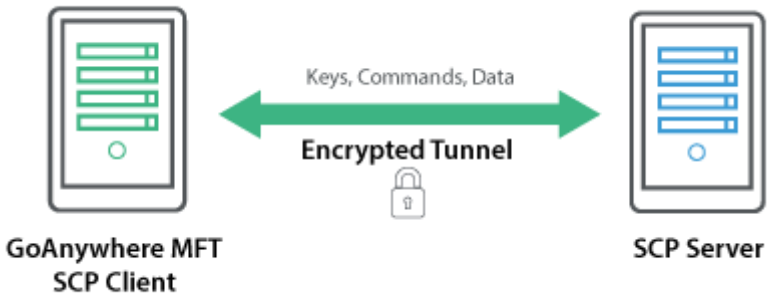
- Sao lưu tệp lên FTP server

- Sao lưu tệp sử dụng SCP

2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết

2.1.1 SCP



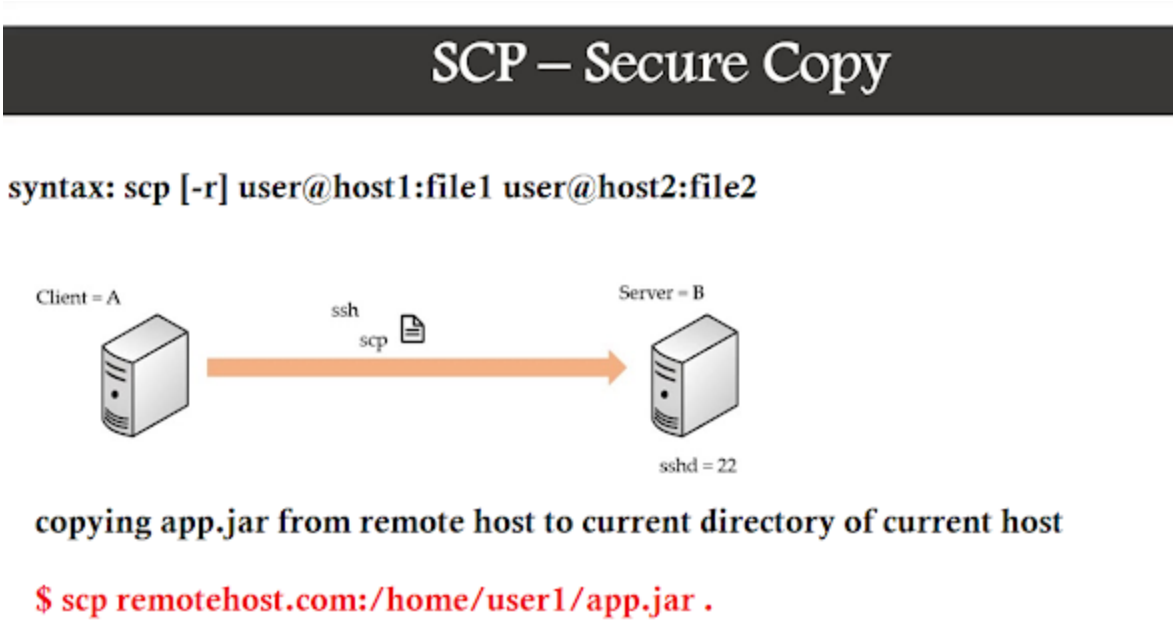
Hình 1: Mô hình SCP

SCP – Secure copy (Bản sao an toàn) 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.

Máy client cung cấp cho máy server tất cả các tệp sẽ được tải lên. Yêu cầu tải xuống các tập tin và thư mục được gửi bởi client. Máy server cung cấp cho client tất cả các thư mục con và tệp có sẵn để tải xuống. Vì việc tải xuống được kiểm soát bởi máy server, có rất nhiều rủi ro bảo mật khi được kết nối với một máy server độc hại.

SCP thường được sử dụng trong các kịch bản sao lưu dữ liệu, đồng bộ hóa thư mục, và chuyển đổi tệp tin giữa các máy chủ. Người dùng có thể sử dụng SCP thông qua dòng lệnh trên terminal, chỉ đơn giản là nhập lệnh với các tham số như nguồn tệp tin, đích đến, và thông tin xác thực. Giao thức này không chỉ đảm bảo tính toàn vẹn của dữ liệu mà còn cung cấp khả năng truyền tải dữ liệu an toàn qua mạng, đặc biệt là khi sử dụng qua kết nối

SSH. Điều này làm cho SCP trở thành một công cụ quan trọng trong quản lý và duy trì hệ thống mạng, đặc biệt là trong môi trường có yêu cầu về an ninh cao.
Mặt khác, chương trình SCP thực hiện giao thức SCP dưới dạng máy client hoặc trình nền dịch vụ. Chương trình Máy server SCP và Máy client SCP là một và giống nhau. Một ví dụ điển hình của chương trình SCP là chương trình SCP dòng lệnh có sẵn với hầu hết các triển khai SSH.



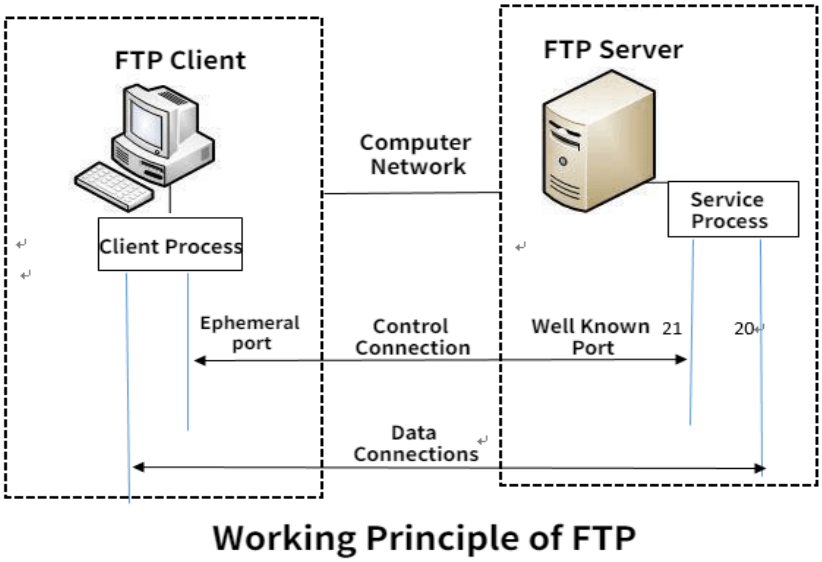
Hình 2: Cách hoạt động SCP

2.1.2 FTP

FTP - File Transfer Protocol (Giao thức truyền tệp) cho phép người dùng truyền tệp từ máy này sang máy khác từ xa, thông qua giao thức TCP/IP thường hoạt động với 2 cổng 20 và 21.

Hình 3: Mô hình FTP

FTP thường chạy trên hai cổng, 20 và 21, và chỉ chạy riêng trên nền của TCP. Trình chủ FTP lắng nghe các yêu cầu dịch vụ từ những kết nối vào máy của các trình khách FTP, trên cổng 21. Đường kết nối trên cổng 21 này tạo nên một dòng truyền điều khiển, cho phép các dòng lệnh được chuyển qua trình chủ FTP. Để truyền tải tập tin qua lại giữa hai máy, chúng ta cần phải có một kết nối khác. Tùy thuộc vào chế độ truyền tải được sử dụng, trình khách (ở chế độ chủ động - active mode) hoặc trình chủ (ở chế độ bị động - passive mode) đều có thể lắng nghe yêu cầu kết nối đến từ đầu kia của mình. Trong trường hợp kết nối ở chế độ chủ động, (trình chủ kết nối với trình khách để truyền tải dữ liệu), trình chủ phải trước tiên đóng kết nối vào cổng 20, trước khi liên lạc và kết nối với trình khách. Trong chế độ bị động, hạn chế này được khắc phục, và việc đóng kết nối trước là một việc không cần phải làm



Hình 4: Cách thức hoạt động FTP

Hạn chế của việc sử dụng FTP là dữ liệu được gửi dưới dạng văn bản không được mã hóa.

2.1.3 Ổ đĩa mạng

Ổ đĩa mạng là bộ nhớ trên máy tính khác được gán ký tự ổ đĩa.

Hình 5: Ổ đĩa mạng

Trong một số trường hợp, người dùng sẽ chỉ có quyền truy cập đọc vào ổ đĩa mạng, vì vậy họ sẽ không thể lưu trữ bất kỳ tệp nào. Nếu quyền ghi tồn tại, người dùng có thể lưu trữ tệp.

2.1.4 Net use & net view

Các lệnh Net này thực chất là dùng chương trình net.exe đặt trong thư mục system32 trong thư mục cài đặt WINDOWS, dùng để quản lý tài nguyên chia sẻ, và giao tiếp với các máy tính khác trong LAN.

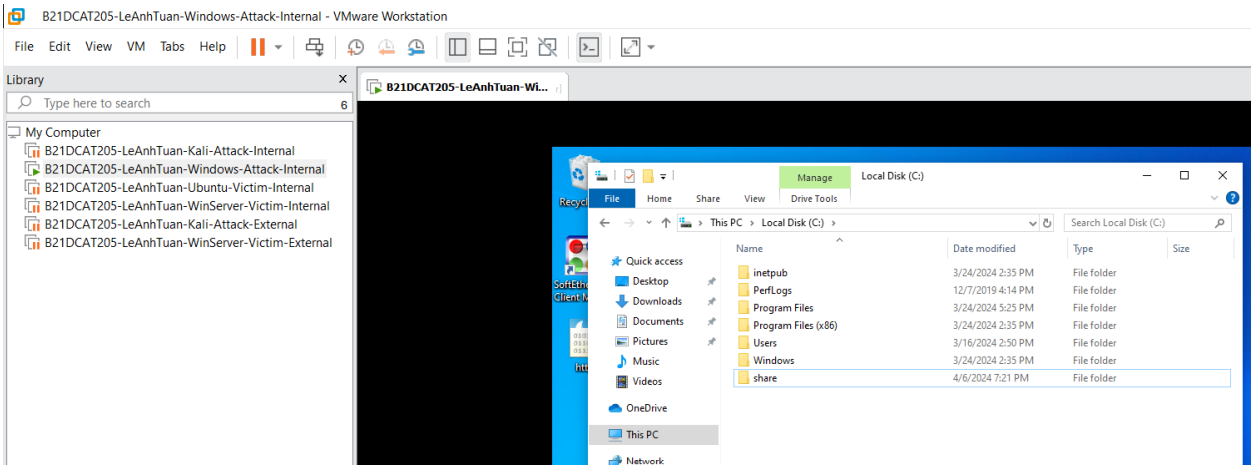
Net use có thể được sử dụng để ánh xạ các ổ đĩa của hệ thống từ xa, ngoài ra còn được dùng để liệt kê tất cả các nguồn được chia sẻ, hoặc bỏ ánh xạ một ổ.

Net view sẽ hiển thị danh sách các mạng chia sẻ của hệ thống.

2.2 Các bước thực hiện

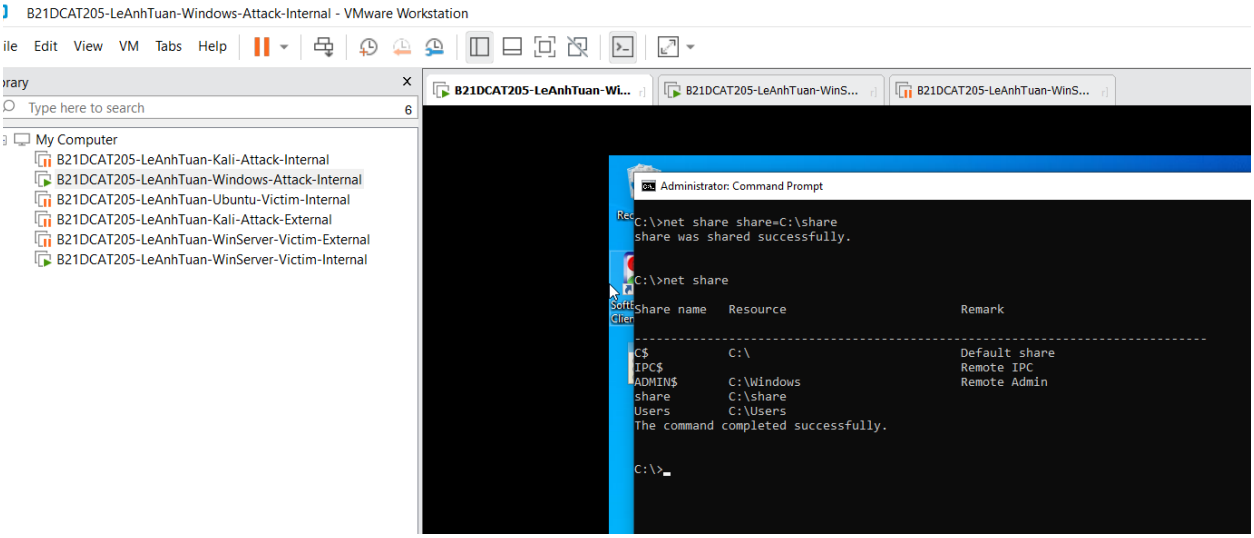
2.2.1 Sao lưu tới ổ đĩa mạng

Trên máy trạm Windows attack trong mạng Internal, tạo thư mục **share**



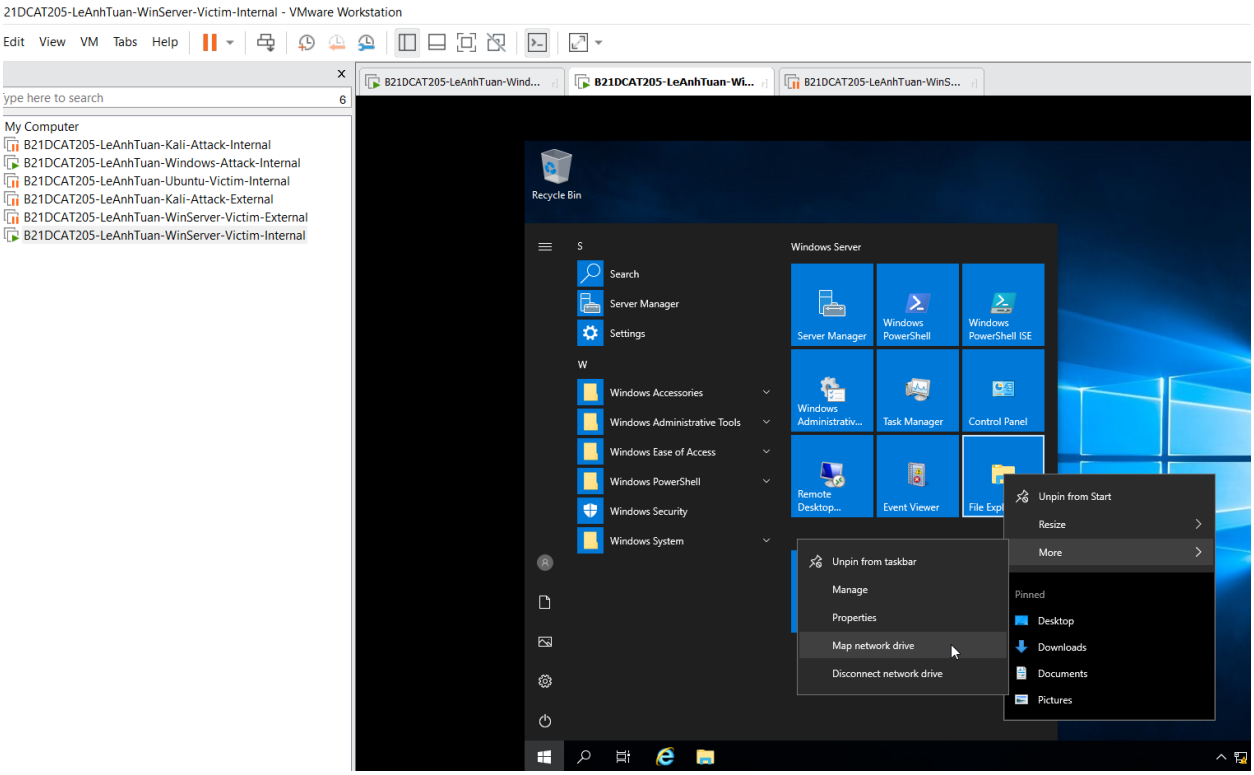
Hình 6: Tạo thư mục share tại Windows-Attack-Internal

Chia sẻ qua mạng **(C:\net share share=c:\share)**

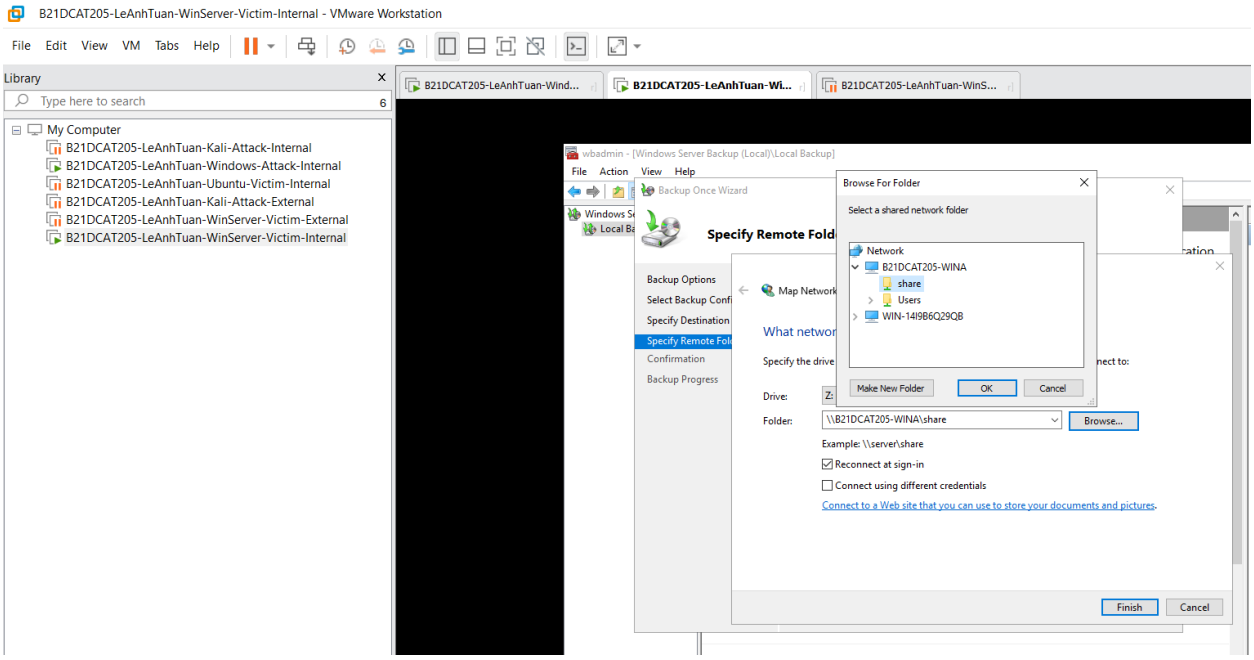


Hình 7: Dùng net share để kiểm tra lại

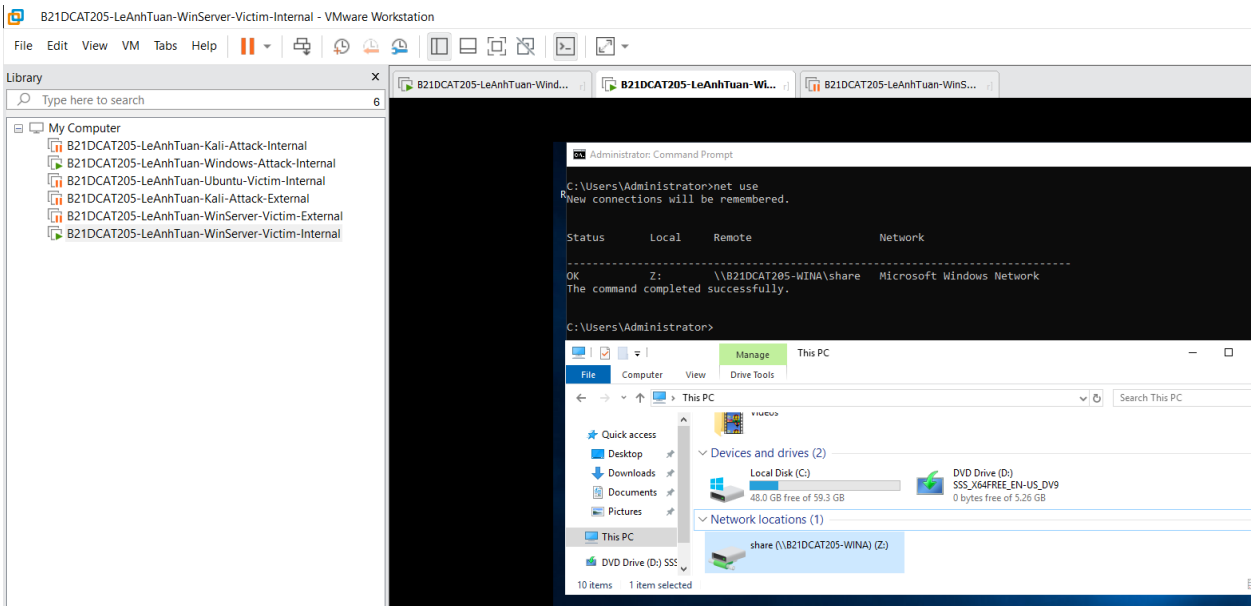
Trên máy **Windows server** ở mạng **Internal**, cấu hình map ổ đĩa mạng trên máy



Hình 8: Chọn Map network drive

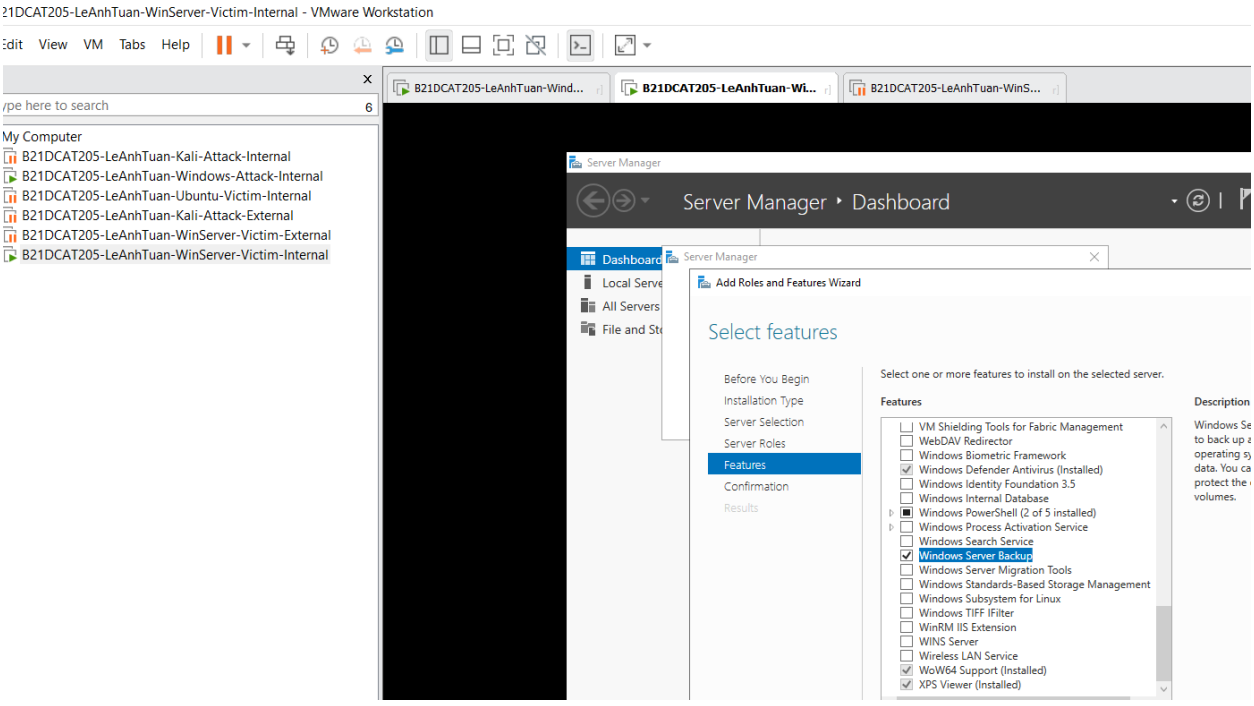


Hình 9: Cấu hình map ổ đĩa mạng trên máy WinServer-Victim-Internal, chọn file share đã tạo

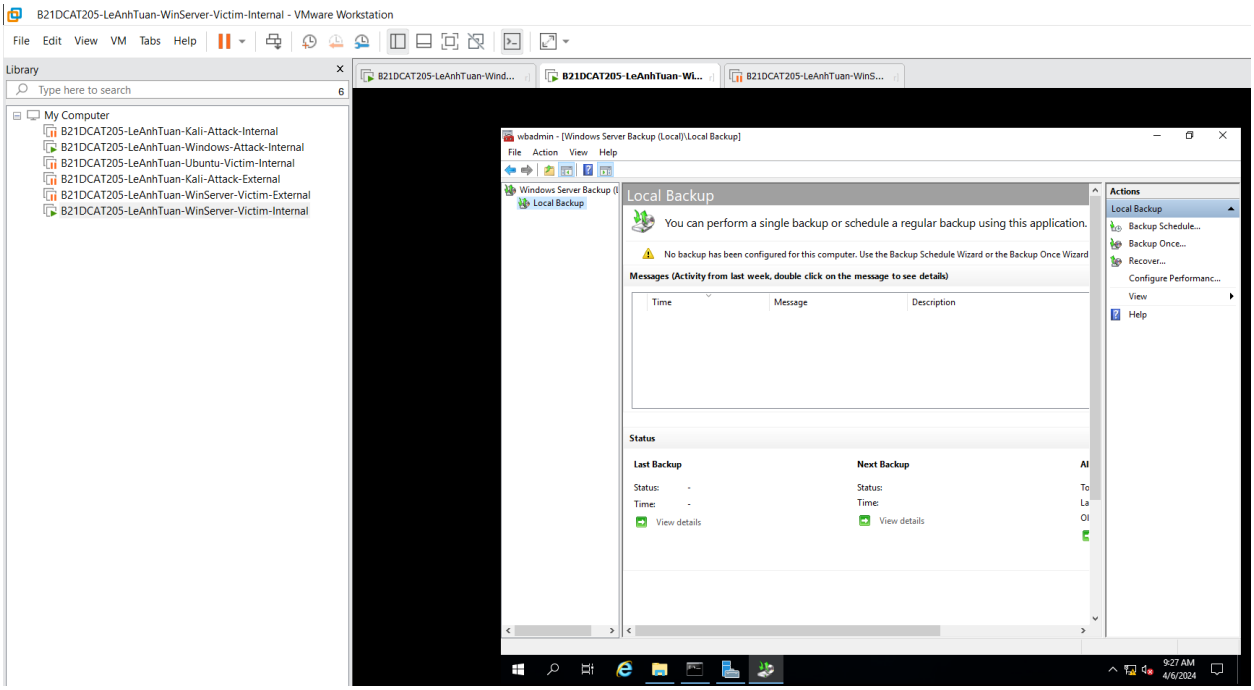


Hình 10: Kết quả sau khi cấu hình.

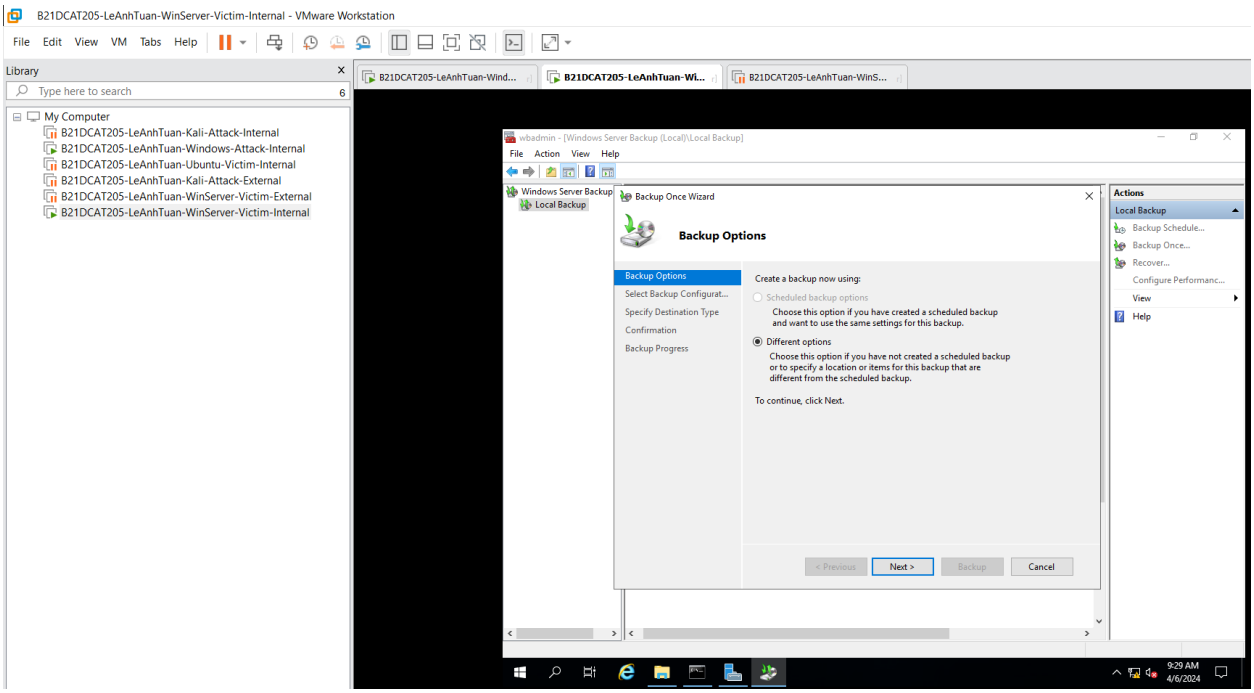
Trên máy **Windows server** ở mạng **Internal**, sao lưu hệ thống bằng chương trình sao lưu của Windows server **(Windows Server Backup)**.



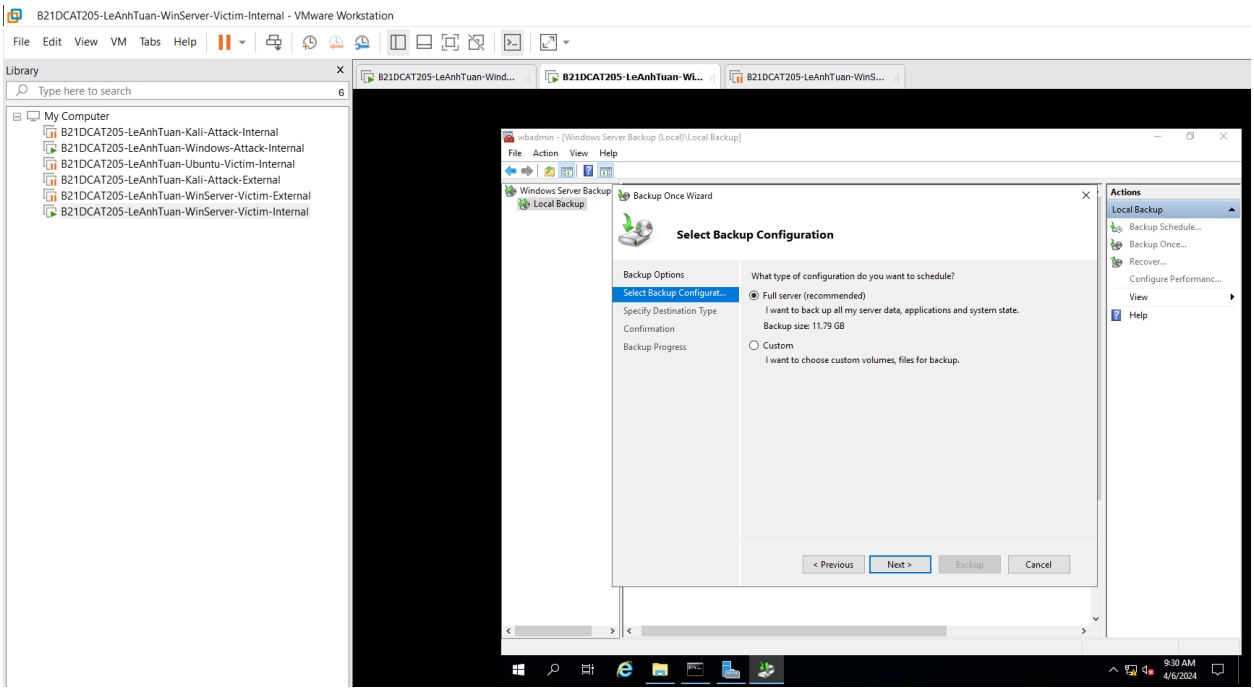
Hình 11: Cài đặt Windows Server Backup



Hình 12: Giao diện sau khi cài xong Windows Server Backup

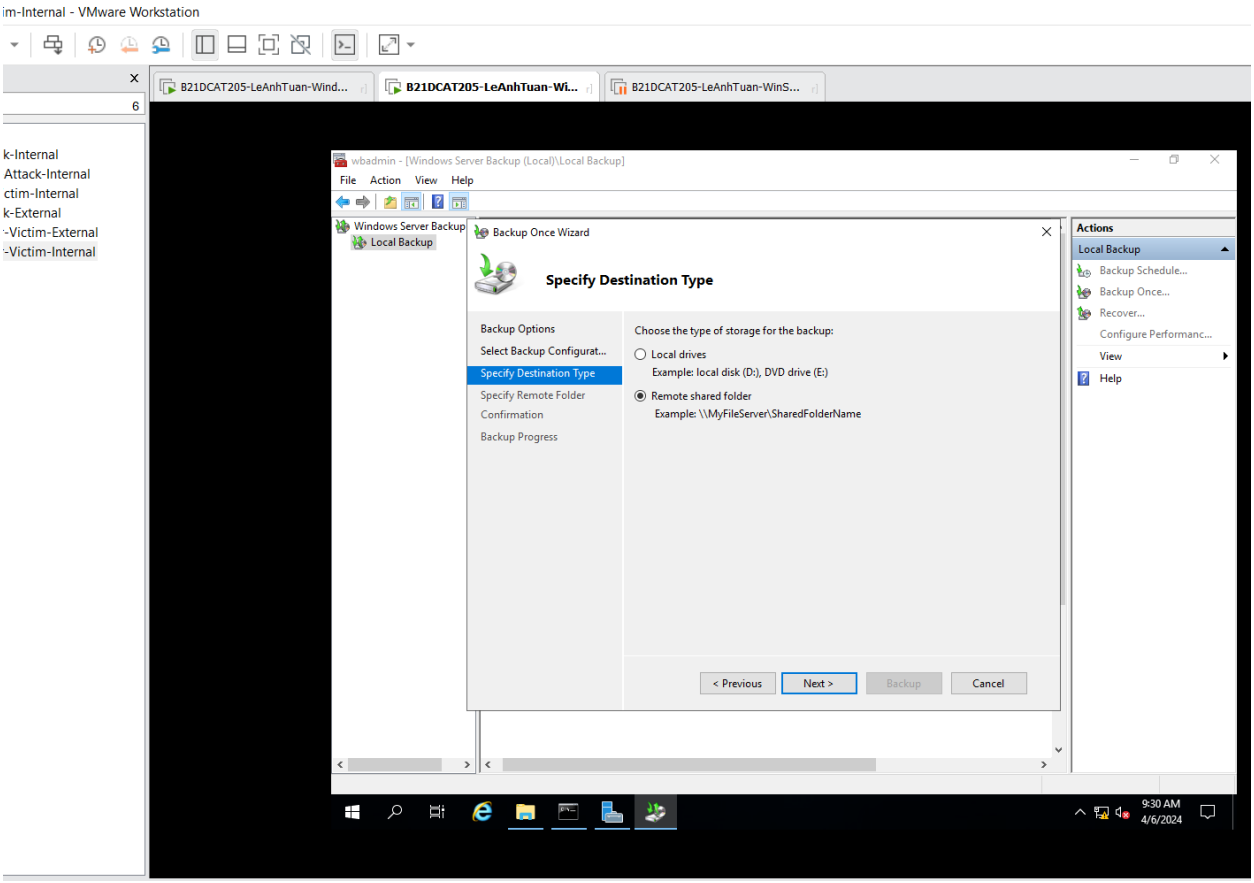


Hình 13: Tại mục Backup Options chọn Different options



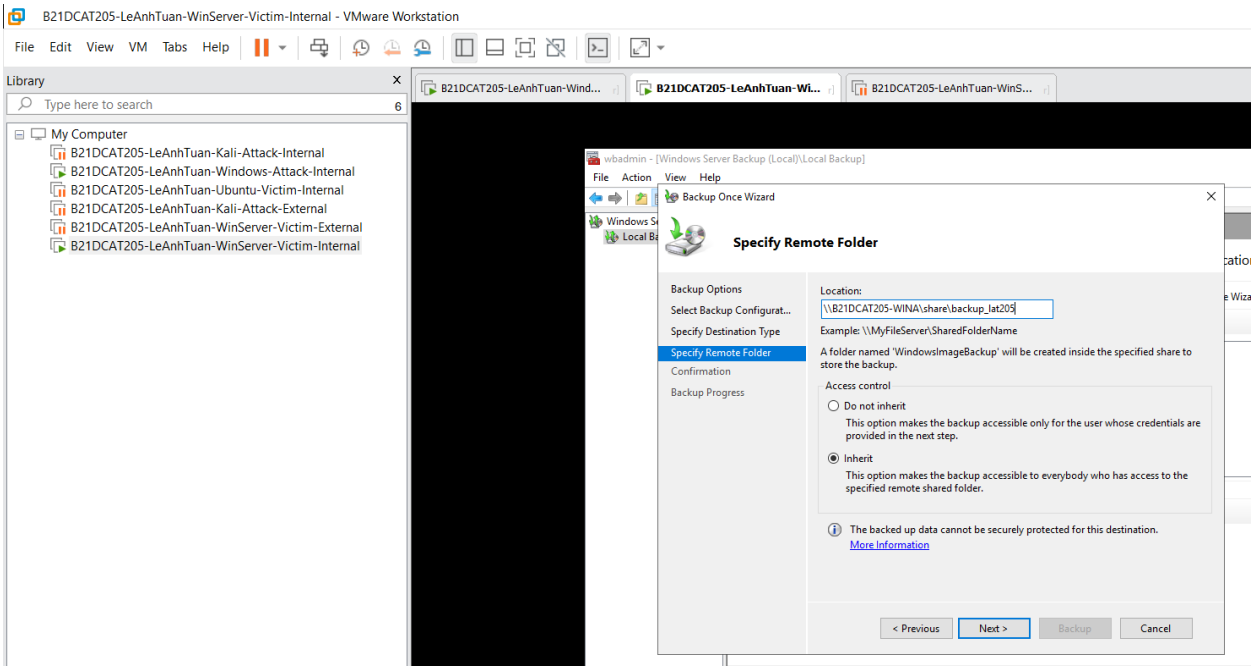
Hình 14: Tại mục Select Backup Configuration chọn Full server

Chọn chia sẻ folder trên 1 hệ thống mạng.

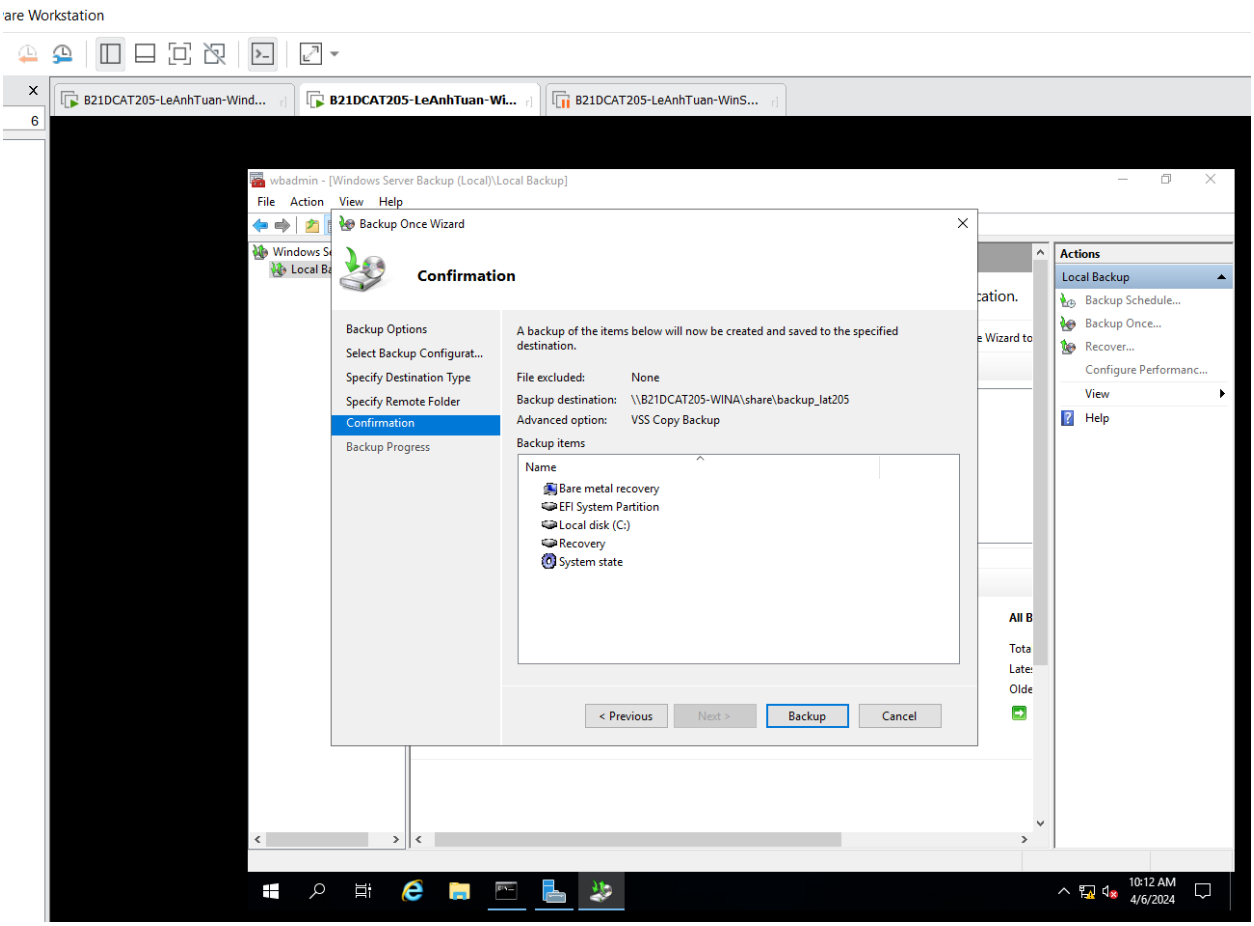


Hình 15: Tại mục Specify Destination Type chọn Remote shared folder

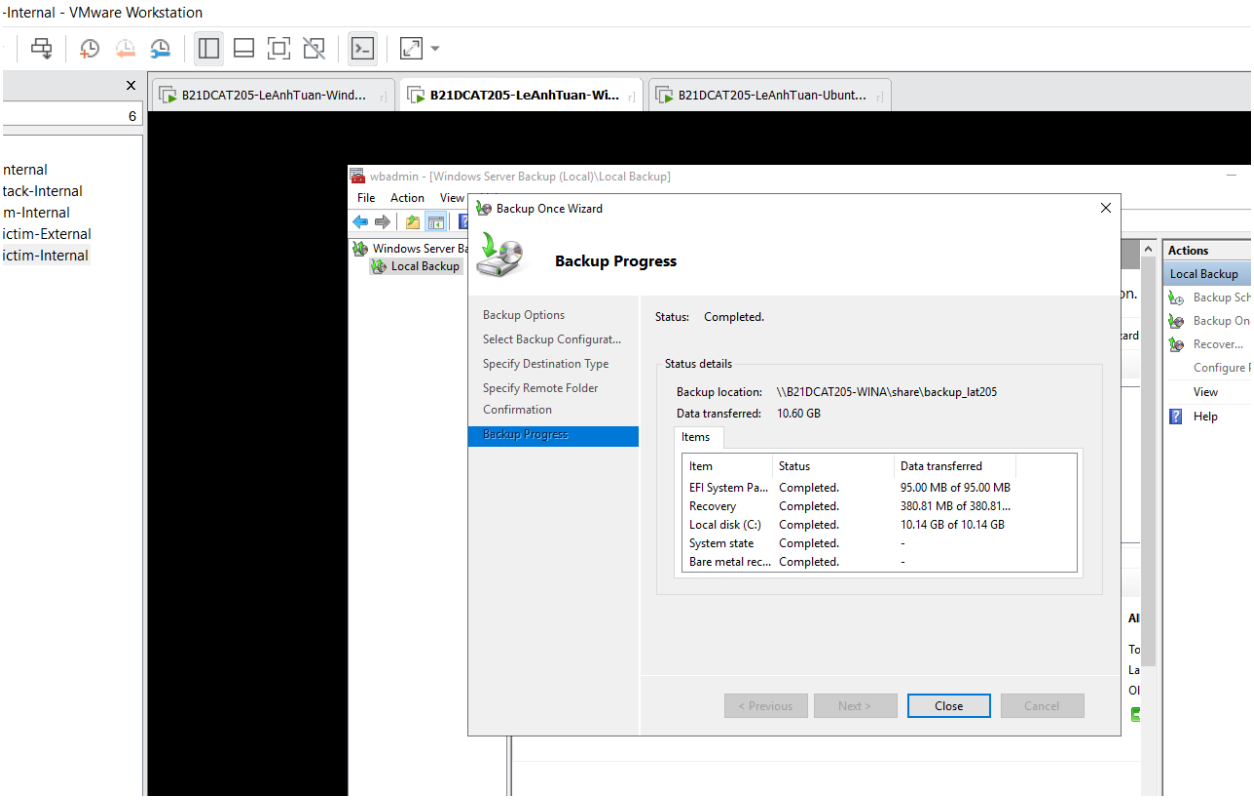
Tạo folder **backup_lat205** trong folder **Share**. Copy đường dẫn đó vào ô **Location** như bên dưới:



Hình 16:Tại mục Specify Remote Folder thêm Location

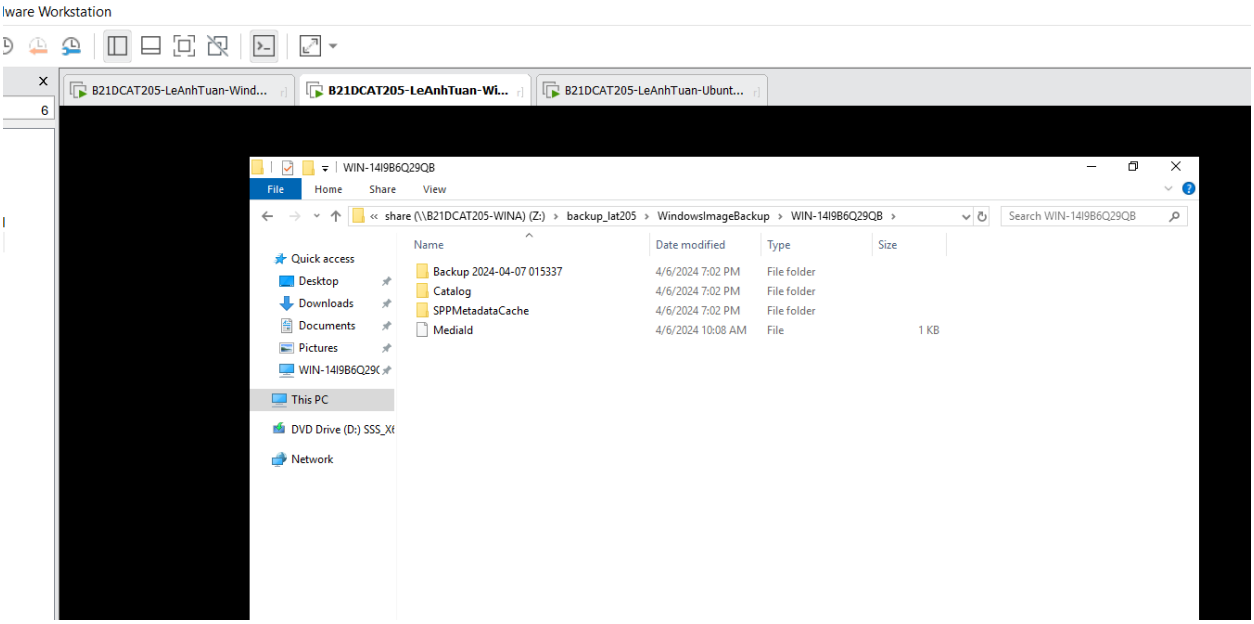


Hình 17: Ấn chọn Backup



Hình 18: Sau lưu thành công

Sau khi sao lưu thành công, ta thấy thư mục backup xuất hiện ở máy **Windows attack internal.**

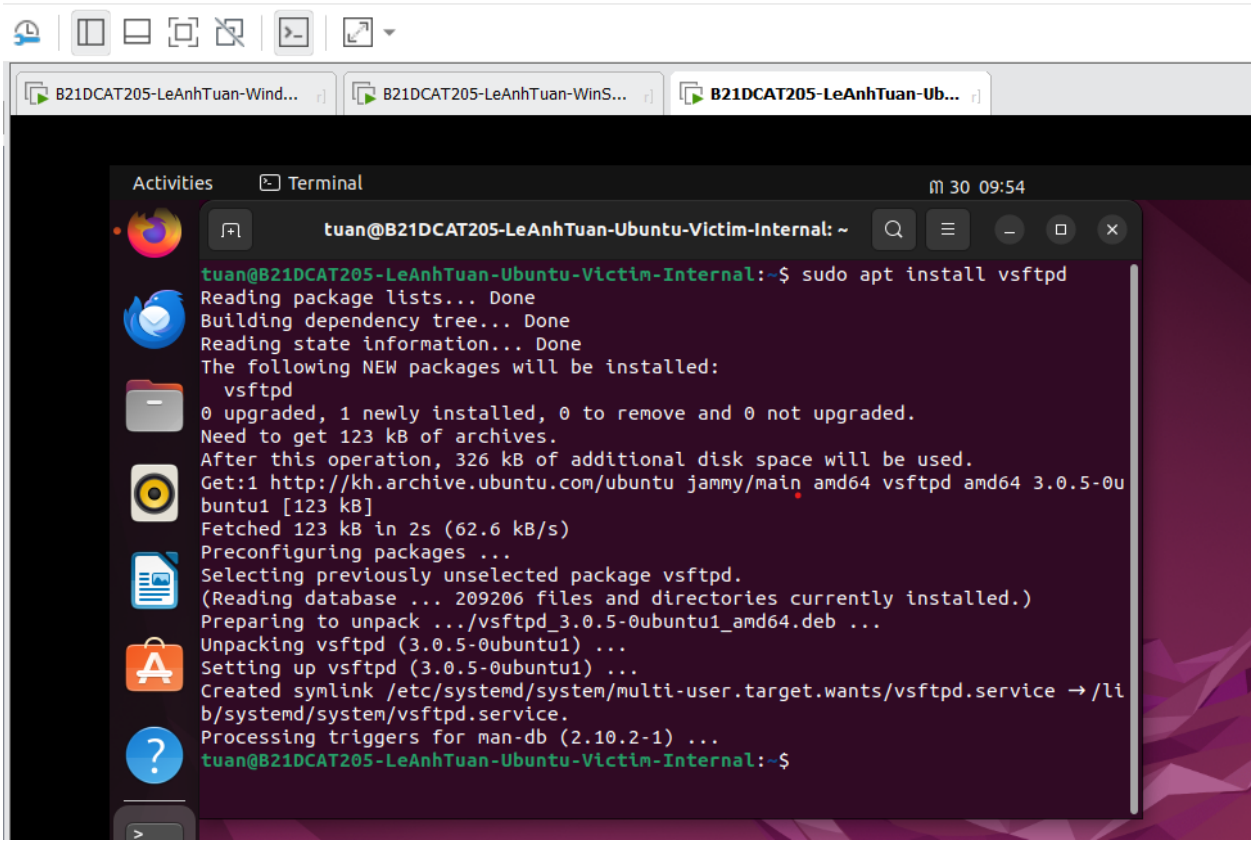


Hình 19: Các mục chứa thông tin sao lưu

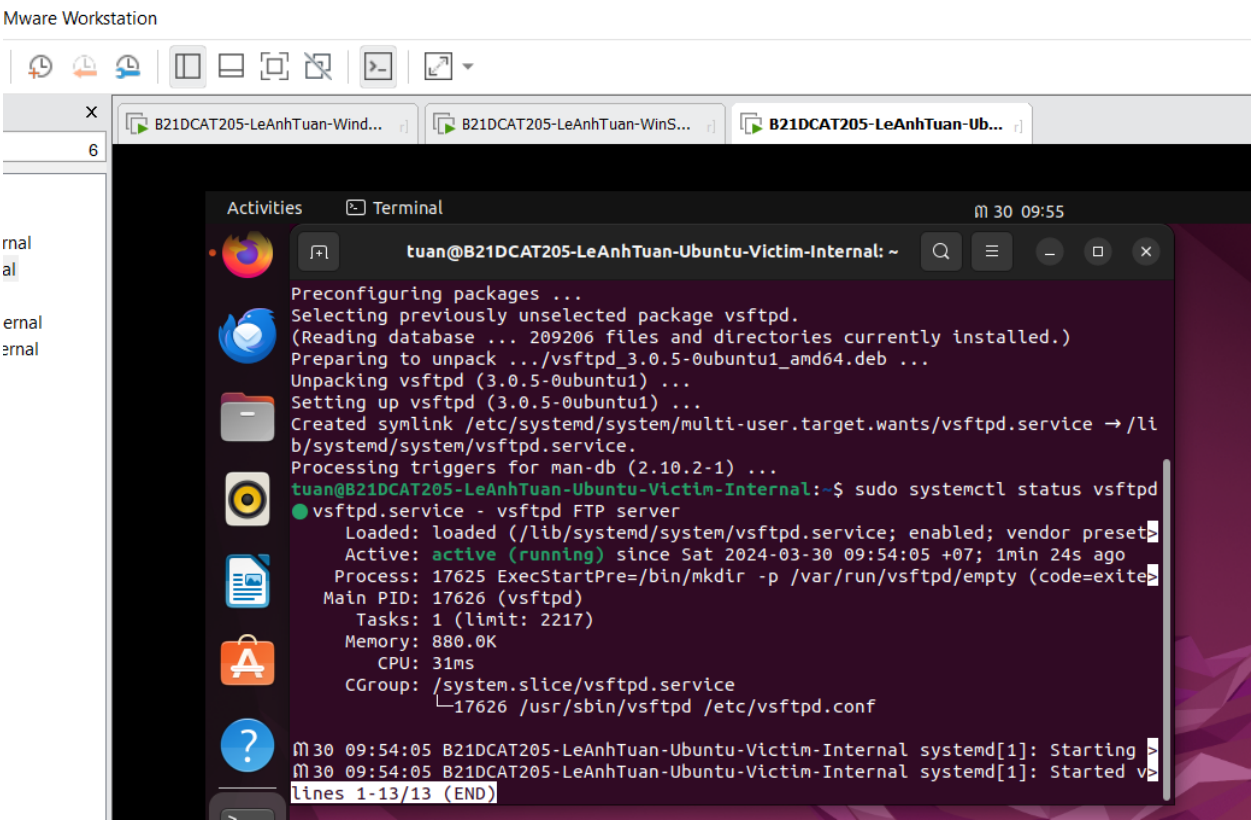
2.2.2 Sao lưu tệp lên FTP server

Trên máy **Linux** trong mạng **Internal**, cài đặt **ftp server**, kiểm tra dịch vụ **ftp**

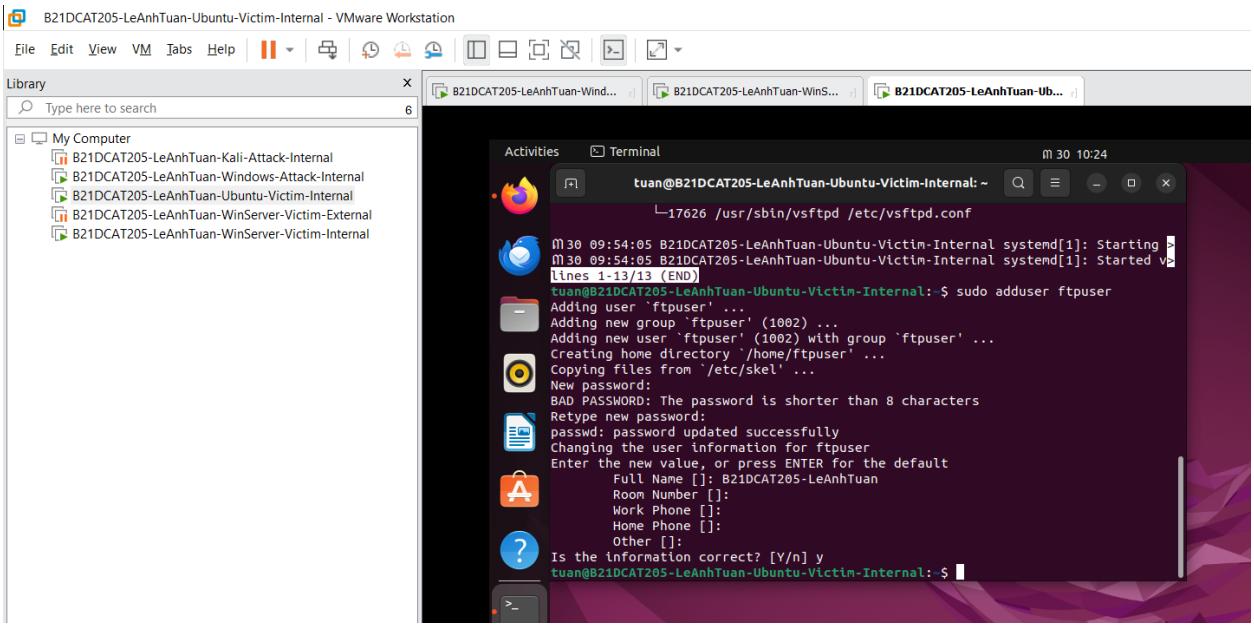
station



Hình 20: Cài đặt ftp

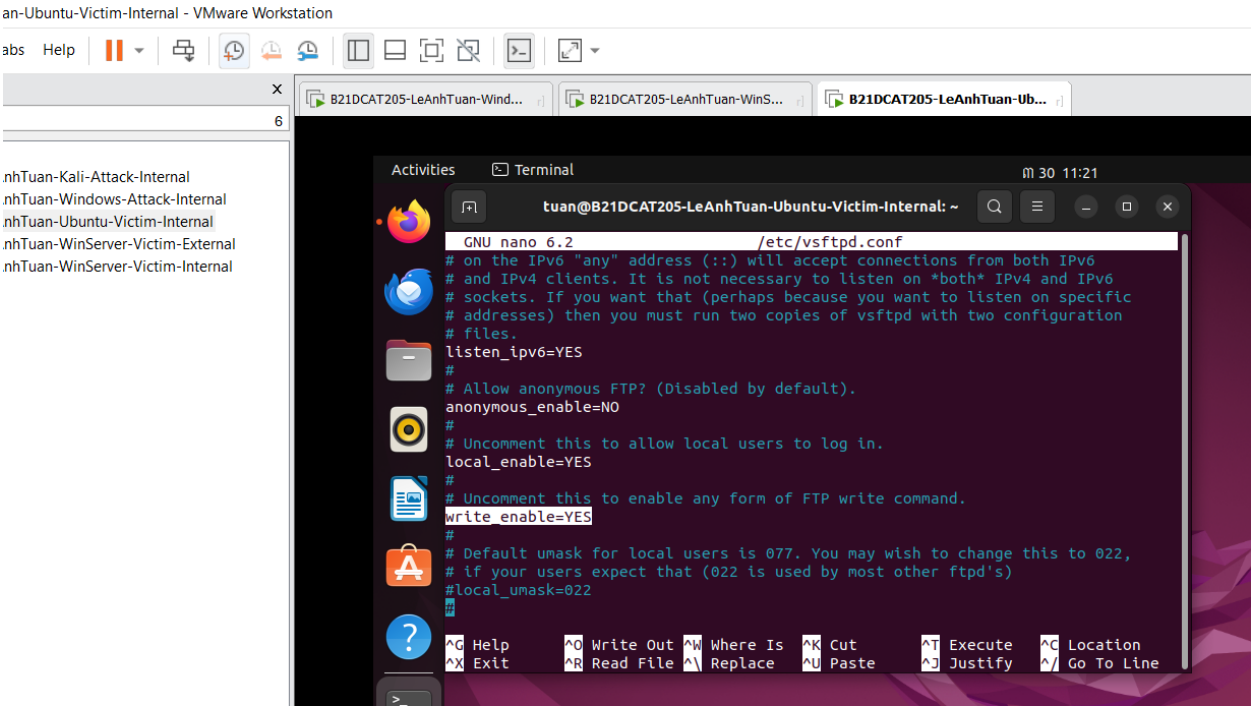


Hình 21: Kiểm tra trạng thái hoạt động ftp

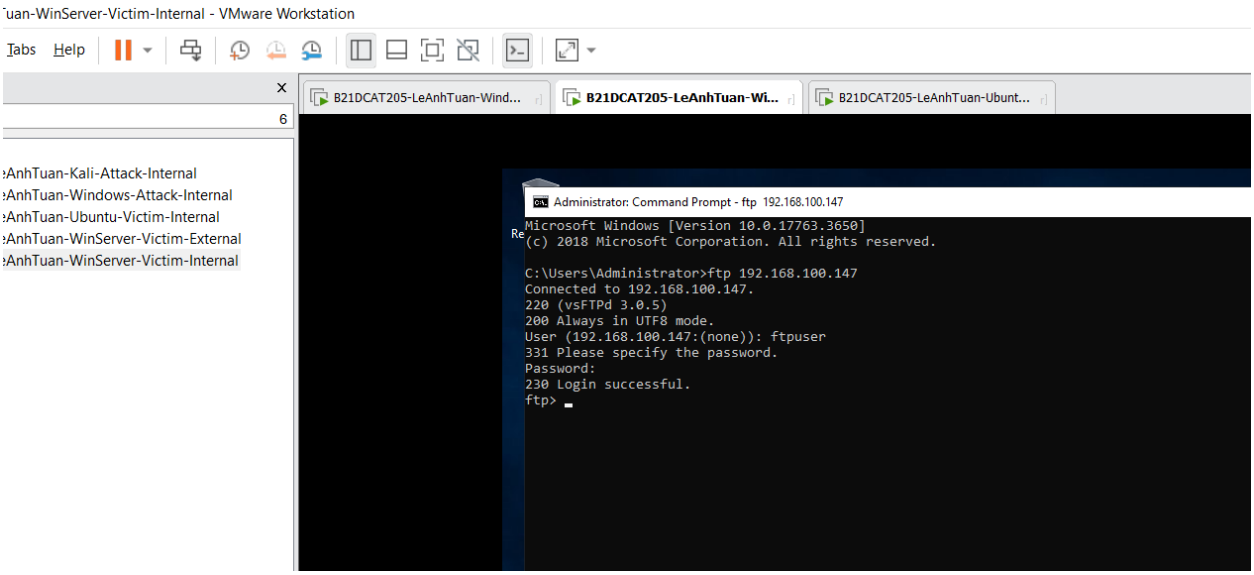


Hình 22: Thêm mới 1 user tên ftpuser

Mở tệp cấu hình **vsftpd (sudo nano /etc/vsftpd.conf)** và bỏ comment dòng **write_enable=YES**, sau đó lưu và sử dụng **sudo service vsftpd restart** để restart lại dịch vụ.

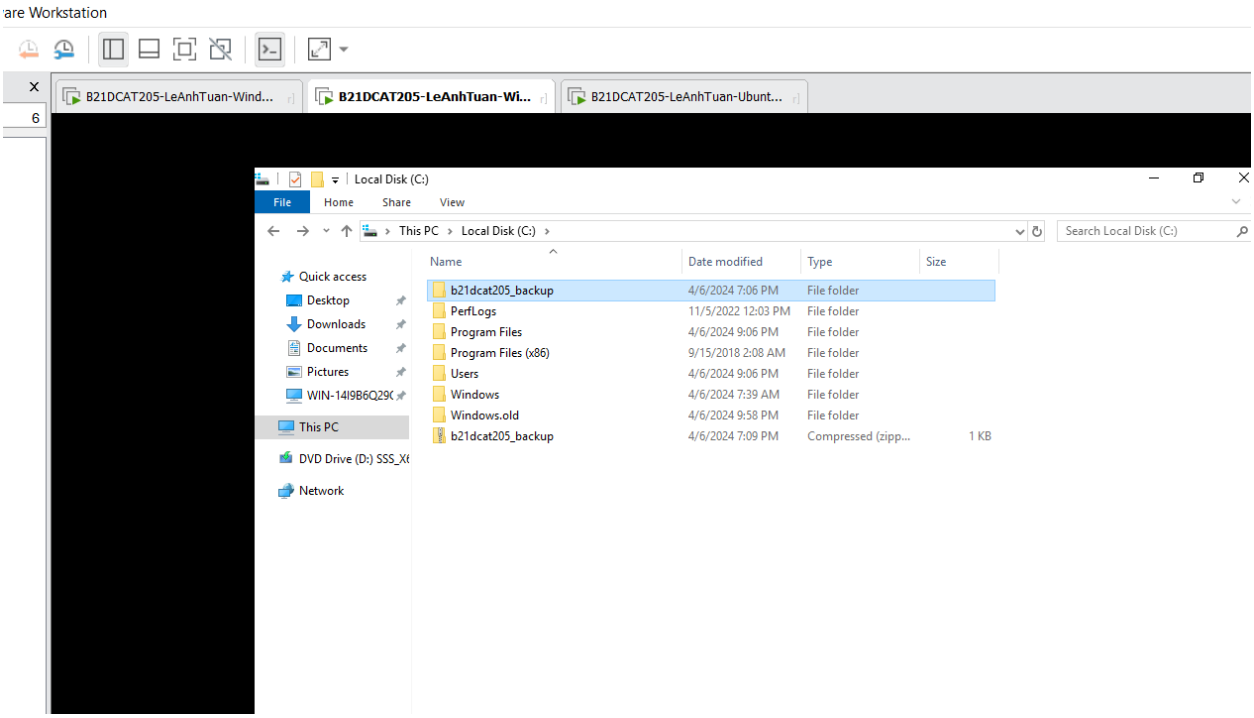


Hình 23: Tùy chỉnh cấu hình ftp

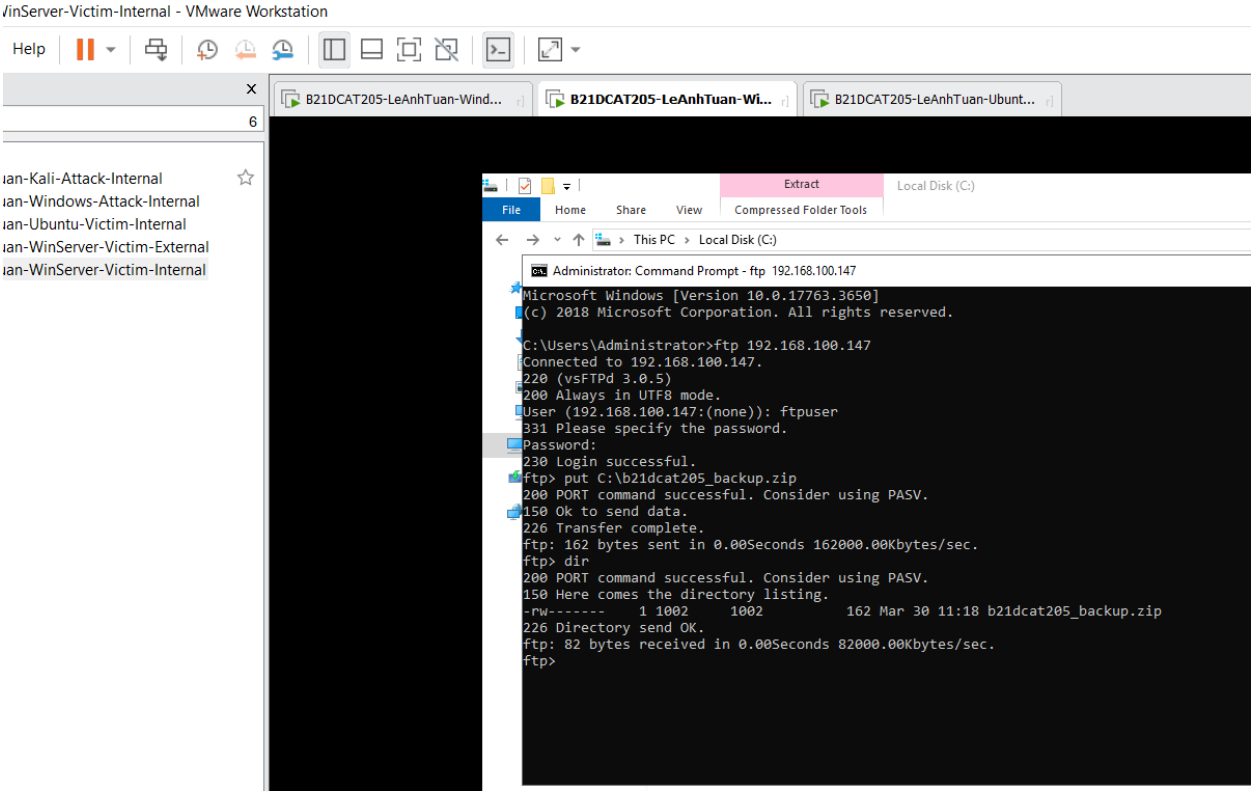


Hình 24:ftp thành công từ máy WinServer-Victim-Internal với Ubuntu-Attack-Internal

Trên máy **Windows server internal** ta tạo mới 1 thư mục **b21dcat205_backup**. Sau đó tạo 1 file bất kì trong thư mục đó và nén lại thành **file zip.**

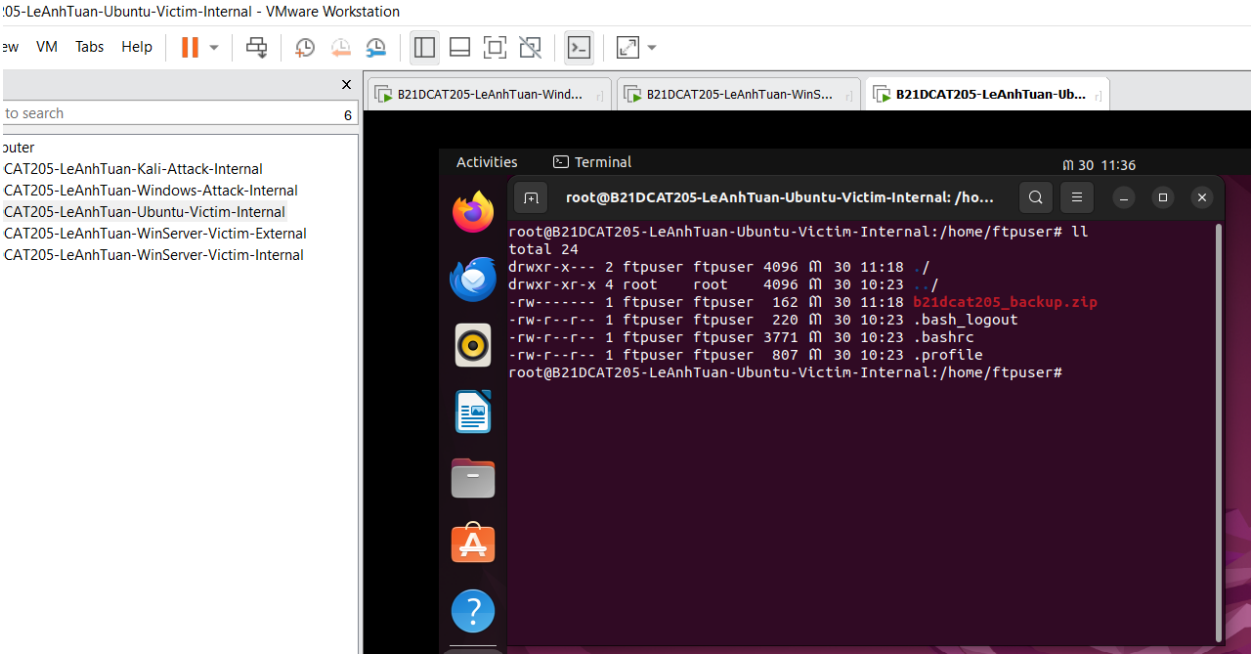


Hình 25: Nén thành file b21dcat205_backup.zip



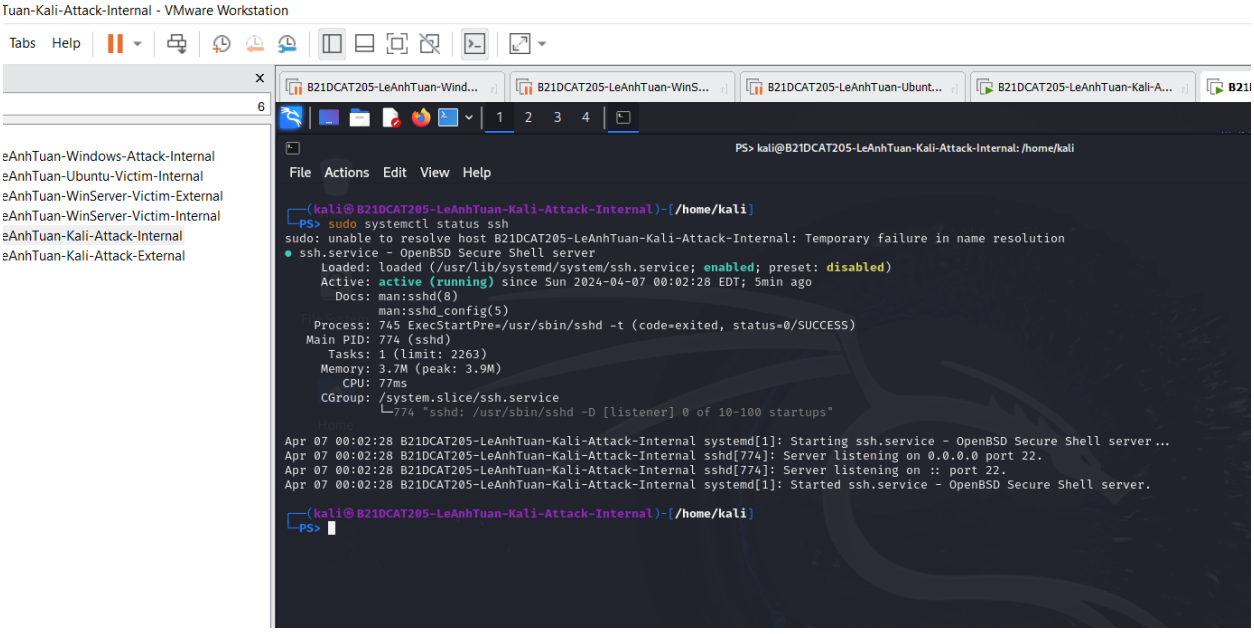
Hình 26: Truyền dữ liệu file sang servver

Trên máy **ftp server** ta thấy được thư mục vừa sao lưu

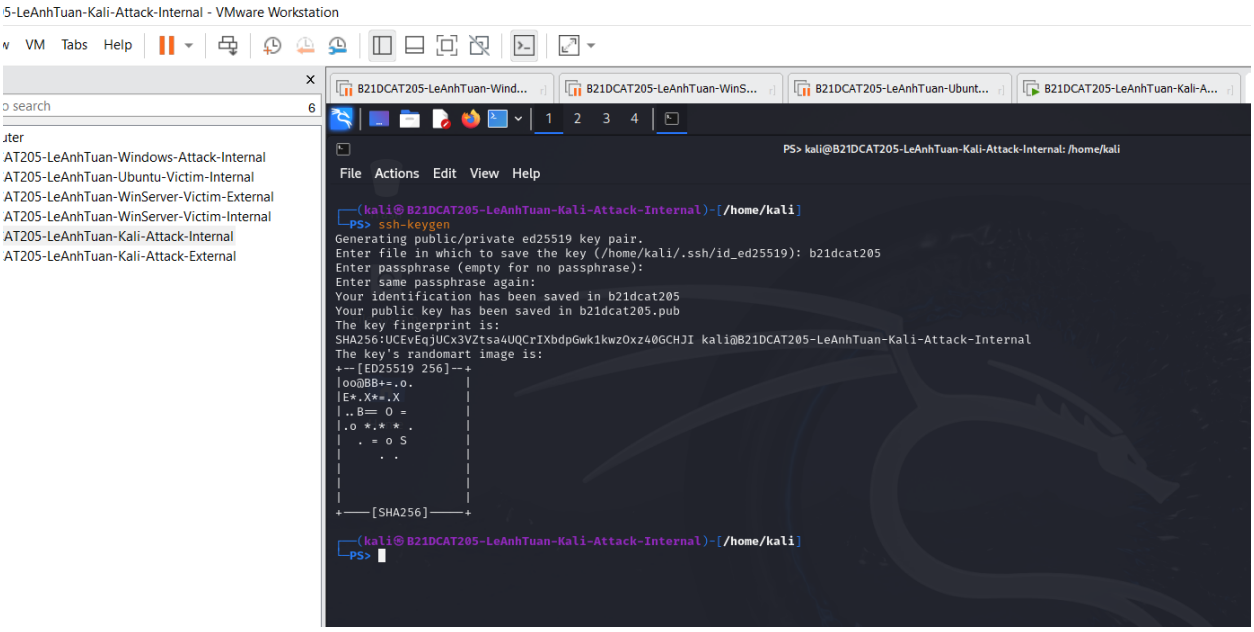


Hình 27: Sao lưu b21dcat205_backup.zip thành công

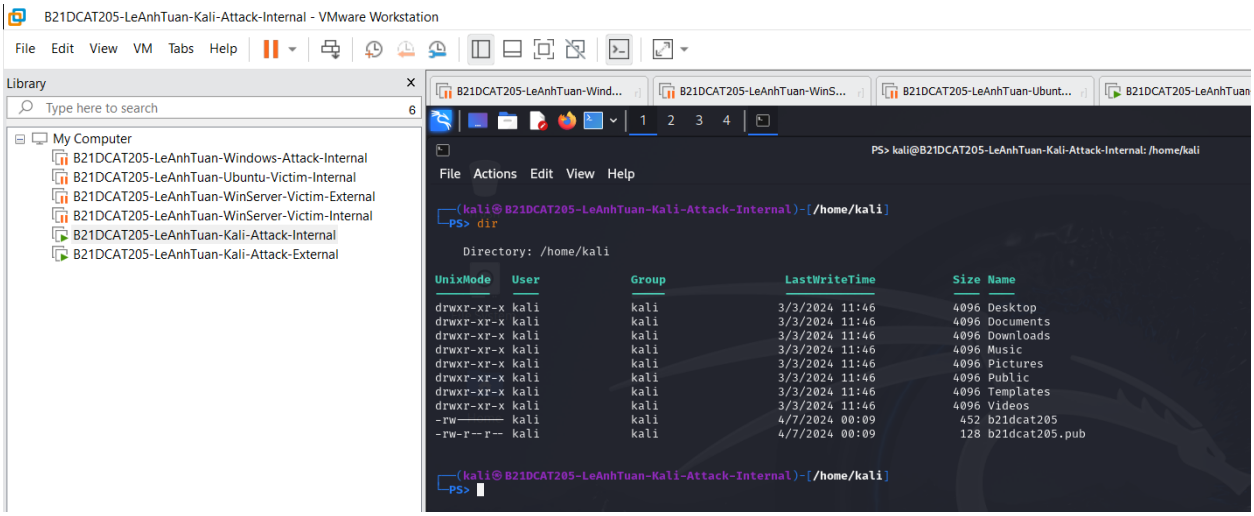
2.2.3 Sao lưu tệp sử dụng SCP



Hình 28: Kiểm tra trạng thái hoạt động ssh

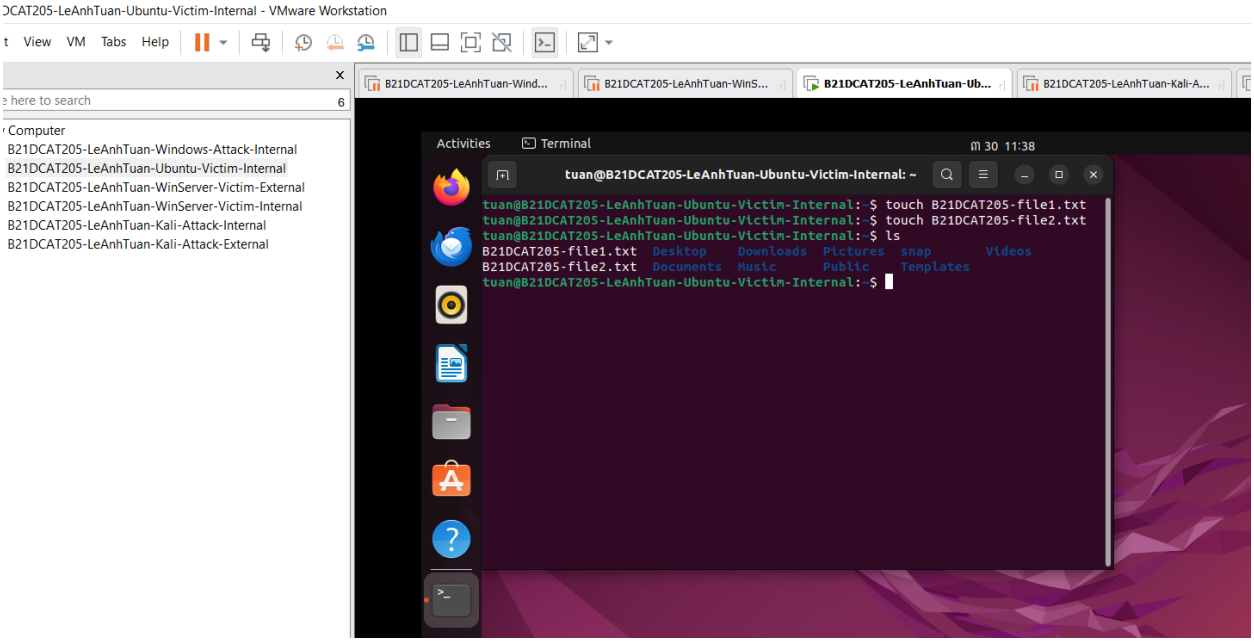


Hình 29: Tiến hành tạo một khóa ssh



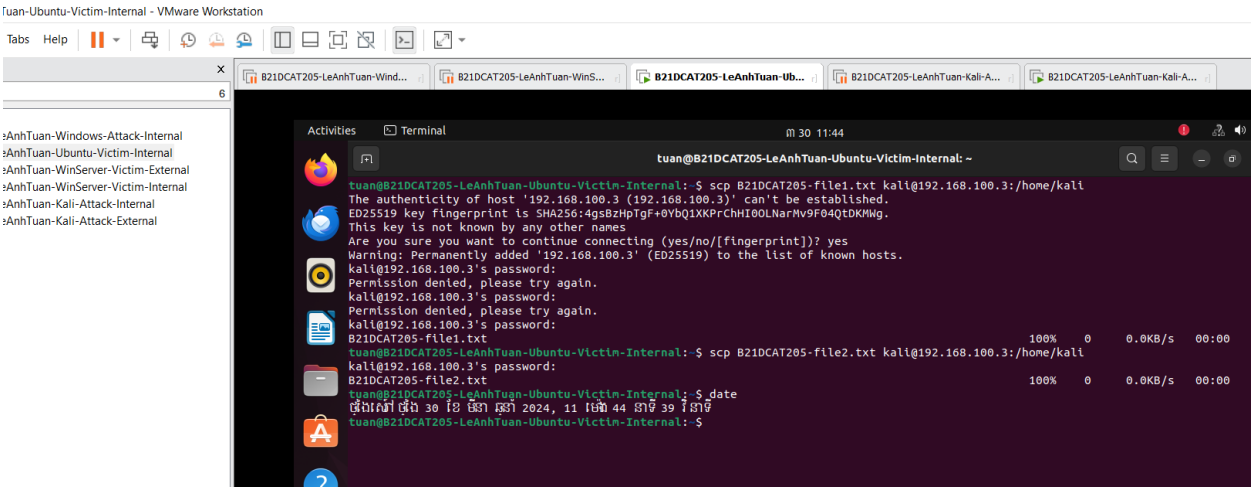
Hình 30: Kiểm tra khóa đã được tạo lưu vào b21dcat205.pub

Trên máy **Linux victim** trong mạng **Internal** tạo 2 file **B21DCAT205-file1.txt** và **B21DCAT205-file2.txt**



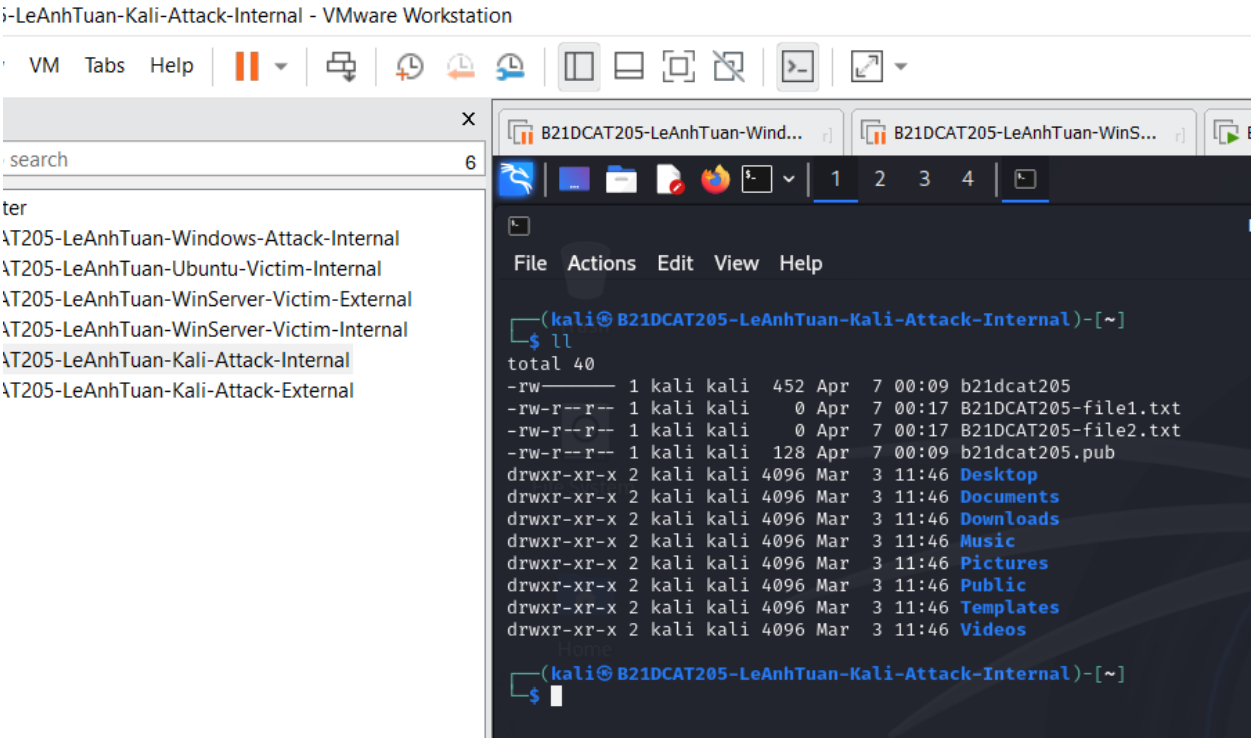
Hình 31:Tạo 2 file như hình

Dùng lệnh **scp** để sao lưu file vừa tạo



Hình 32: Sao lưu sử dụng scp

Trên máy **Kali Attack** trong mạng **Internal** kiểm tra bằng lệnh **ll**



Hình 33: Sao lưu thành công với scp

3 Kết luận

- Nắm vững 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.
- Sao lưu tới ổ đĩa mạng thành công
- Sao lưu tệp lên FTP server thành công
- Sao lưu tệp sử dụng SCP thành công

4 Tài liệu tham khảo

- Lab 8 pfsense firewall của CSSIA CompTIA Security+®