BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu
Sinh viên thực hiện : Nguyễn Nhật Minh
Mã sinh viên : B21DCAT132

Hà Nội, tháng 3 năm 2024

Môn học: Thực tập cơ sở
Bài 10: Sao lưu hệ thống

1. Mục đích

Bài thực hành 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. Tìm hiểu lí thuyết

2.1. SCP

SCP là viết tắt của "Secure Copy Protocol", là một giao thức dùng để truyền tệp tin một cách an toàn giữa hai máy tính qua mạng. SCP thường được sử dụng trong các môi trường Linux và Unix-like, nhưng cũng có thể hoạt động trên các hệ điều hành khác.

Dưới đây là một số điểm nổi bật về SCP:

- Bảo mật: SCP sử dụng SSH (Secure Shell) để mã hóa dữ liệu trước khi truyền qua mạng. Điều này đảm bảo rằng dữ liệu được truyền đi qua mạng một cách an toàn và bảo mật.
- Dễ sử dụng: SCP có cú pháp giống như lệnh "cp" (copy) trong Linux/Unix, điều này làm cho việc sử dụng SCP trở nên dễ dàng và quen thuộc đối với những người làm việc với các hệ thống này.
- Truyền tệp tin và thư mục: SCP cho phép truyền tệp tin cũng như thư mục từ một máy tính đến máy tính khác hoặc từ một máy tính đến một máy chủ từ xa.
- Hỗ trợ đa nền tảng: SCP có sẵn trên hầu hết các hệ điều hành Unix-like và Linux. Ngoài ra, có các phần mềm và công cụ thứ ba hỗ trợ SCP trên các hệ điều hành khác như Windows.
- Tích hợp với các công cụ khác: SCP có thể được tích hợp với các kịch bản tự động hoặc các công cụ quản lý hệ thống khác để tự động hóa việc sao chép và di chuyển tệp tin giữa các máy tính.

2.2. FTP

FTP là viết tắt của "File Transfer Protocol", là một giao thức mạng được sử dụng để truyền tệp tin giữa các máy tính trên mạng Internet. Dưới đây là một số điểm nổi bật về FTP:

- Cách thức hoạt động: FTP hoạt động dựa trên mô hình client-server, trong đó có một máy chủ FTP (FTP server) chứa các tệp tin và thư mục cần được truyền và các máy tính khác kết nối đến máy chủ để truy cập và tải xuống hoặc tải lên tệp tin.
- Phân quyền và bảo mật: FTP hỗ trợ phân quyền truy cập, cho phép người quản trị máy chủ quy định các quyền truy cập khác nhau cho người dùng hoặc nhóm người dùng. Tuy nhiên, trong phiên bản cơ bản, FTP không mã hóa dữ liệu truyền đi qua mạng, vì vậy thông tin có thể bị đánh cắp nếu không được bảo mật.
- Chế độ hoạt động: FTP hỗ trợ hai chế độ hoạt động chính: Active Mode và Passive Mode. Trong Active Mode, máy chủ kết nối đến máy khách để truyền dữ liệu, trong khi trong Passive Mode, máy khách kết nối đến máy chủ để truyền dữ liệu. Chế độ

Passive Mode thường được ưu tiên hơn trong các mạng có tường lửa hoặc NAT.

- Phổ biến và đa nền tảng: FTP là một giao thức truyền tệp tin phổ biến và được hỗ trợ trên nhiều hệ điều hành và nền tảng khác nhau, bao gồm Windows, Unix, Linux và các hệ điều hành khác.
- Ứng dụng: FTP thường được sử dụng để truyền tệp tin lớn, chẳng hạn như tải xuống hoặc tải lên các trang web, chia sẻ tệp tin giữa các máy tính trong mạng nội bộ, sao lưu dữ liệu và nhiều ứng dụng khác.

2.3. Ổ đĩa mạng

Ổ đĩa mạng là một phần của hệ thống tệp phân tán, cho phép người dùng truy cập và chia sẻ tệp tin qua mạng. Đây thường là một phần của môi trường làm việc nhóm hoặc doanh nghiệp, nơi nhiều người dùng có thể truy cập và làm việc với cùng một tập tin hoặc dữ liệu.

Một số điểm chính của ổ đĩa mạng:

- Truy cập từ xa: Người dùng có thể truy cập ổ đĩa mạng từ xa thông qua mạng nội bộ hoặc Internet. Điều này cho phép họ làm việc từ bất kỳ địa điểm nào có kết nối mạng, giúp tăng tính linh hoạt trong công việc.
- Chia sẻ tệp tin và dữ liệu: Ổ đĩa mạng cho phép nhiều người dùng truy cập và chia sẻ tệp tin và dữ liệu một cách dễ dàng. Điều này làm cho việc làm việc nhóm trở nên hiệu quả hơn, đặc biệt trong các môi trường làm việc cộng tác.
- Bảo mật và quản lý: Ổ đĩa mạng thường được quản lý và kiểm soát bởi quản trị viên hệ thống. Họ có thể thiết lập các quyền truy cập để đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào các tệp tin và thư mục cụ thể.
- Sự linh hoạt và mở rộng: Hầu hết các hệ thống ổ đĩa mạng cho phép mở rộng dung lượng lưu trữ một cách dễ dàng khi nhu cầu tăng lên. Điều này cung cấp sự linh hoạt cho tổ chức để mở rộng hệ thống lưu trữ theo thời gian.
- Sao lưu và phục hồi dữ liệu: Ổ đĩa mạng cũng thường được sử dụng để lưu trữ sao lưu dữ liệu, giúp bảo vệ thông tin quan trọng của tổ chức khỏi mất mát dữ liệu do sự cố hệ thống hoặc hỏng hóc.

2.4. Net use và Net view

Net use và net view là hai trong số các lệnh cơ bản được cung cấp trong hệ điều hành Windows để quản lý và truy cập vào tài nguyên mạng

Net use là một lệnh dùng để kết nối và quản lý các kết nối tài nguyên mạng trên Windows.

Công dụng:

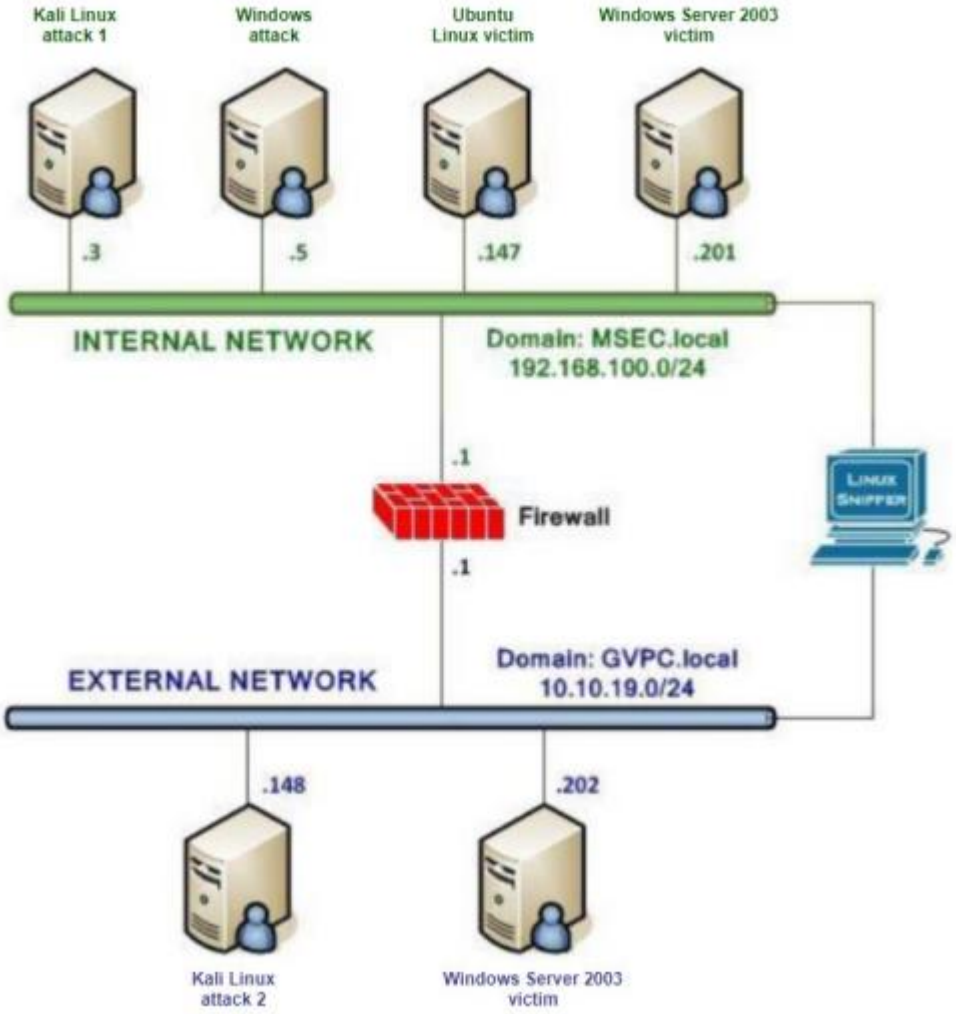
- Kết nối tới một ổ đĩa mạng, máy chủ hoặc tài nguyên mạng khác.
- Ngắt kết nối từ một ổ đĩa mạng, máy chủ hoặc tài nguyên mạng.
- Hiển thị danh sách các kết nối tài nguyên mạng đang được sử dụng.

Net view là một lệnh được sử dụng để hiển thị danh sách các máy tính và tài nguyên mạng có sẵn trên mạng.

Công dụng: Hiển thị danh sách các máy tính và tài nguyên mạng trên mạng LAN.

3. Chuẩn bị môi trường

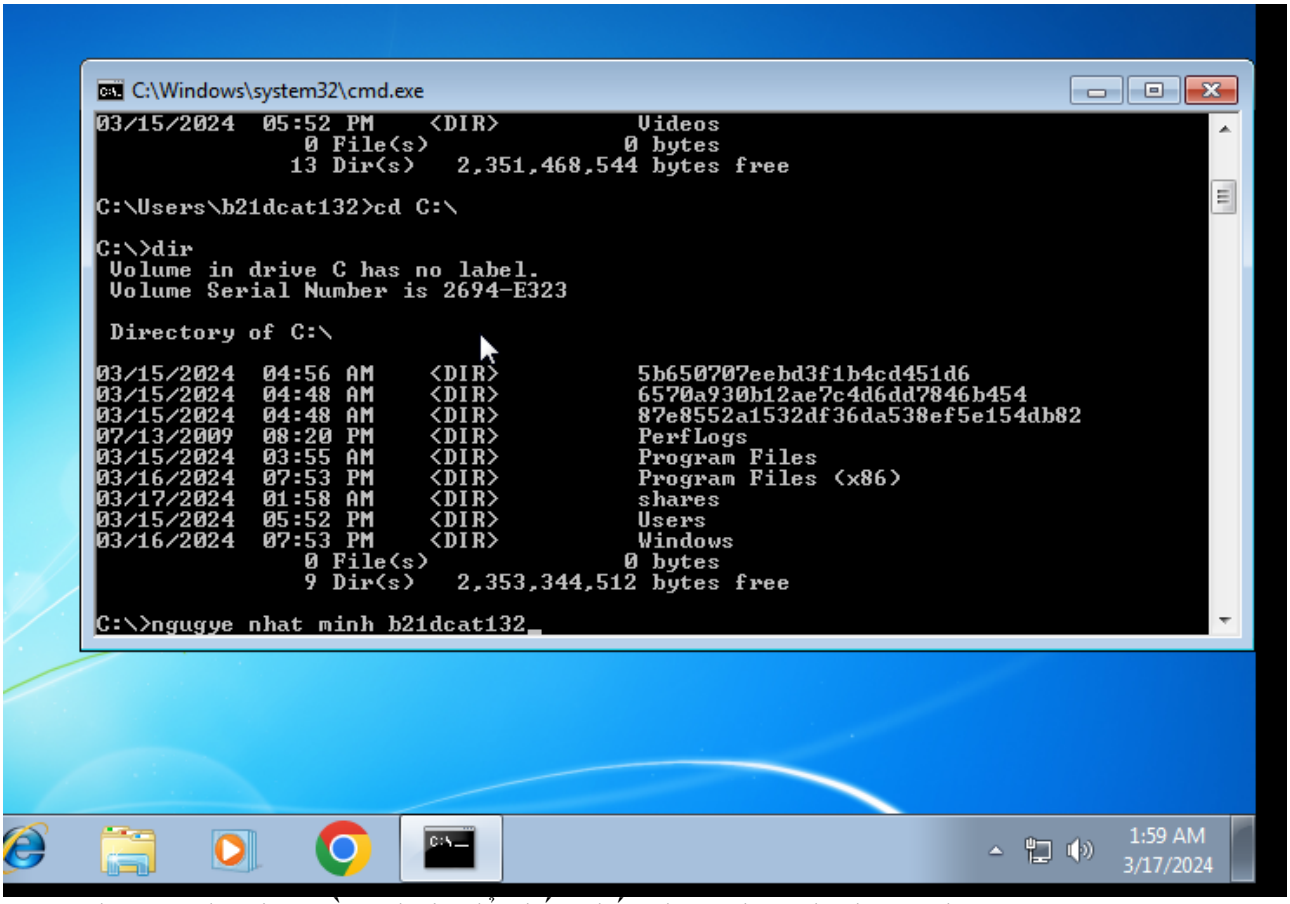
Mạng topo như trong bài thực hành 5 đã cài đặt



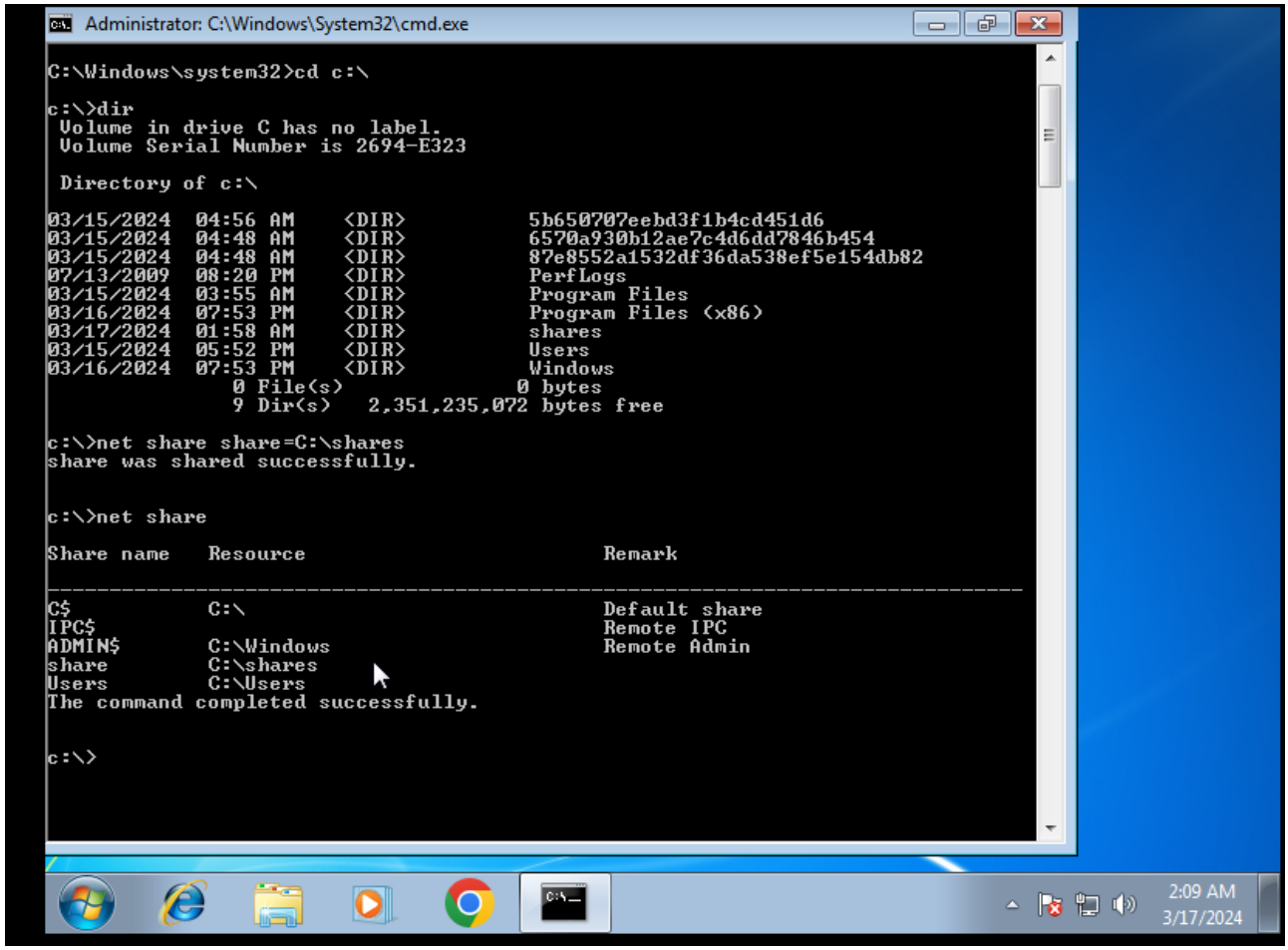
4. Thực hành

4.1. Sao lưu tới ổ đĩa mạng

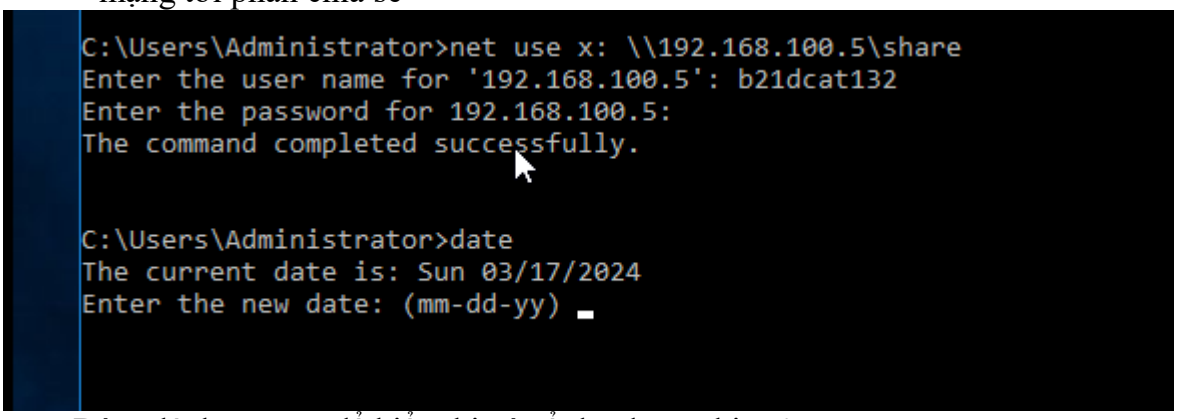
- Trên máy Windows 7 tạo thư mục shares trong ổ C



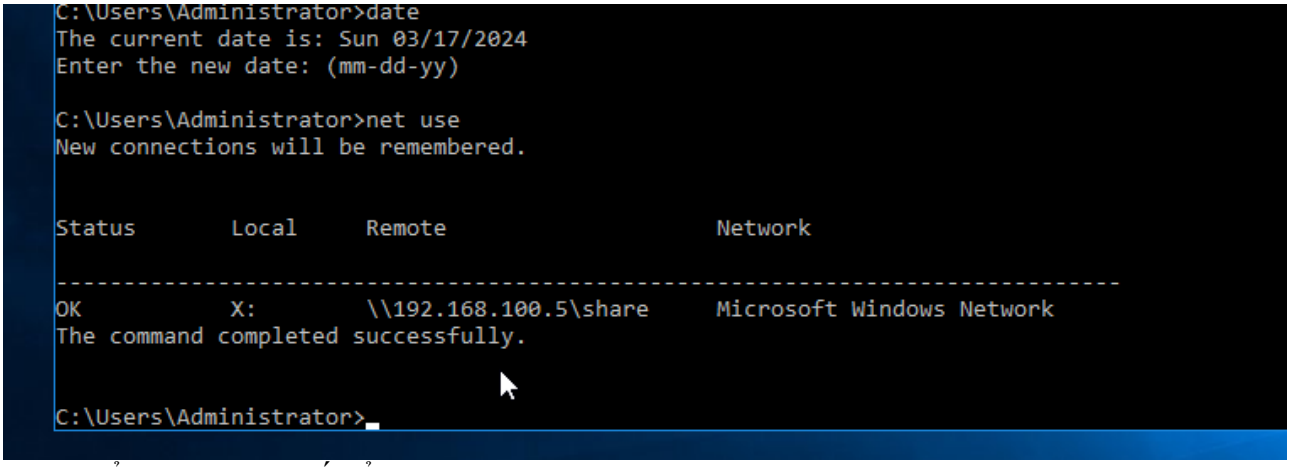
- Chạy cmd với quyền admin để chắc chắn dùng được lệnh net share
- Tạo thư mục tên shares ở ổ C
- Sử dụng lệnh net share share=C:\shares để chia sẻ thư mục



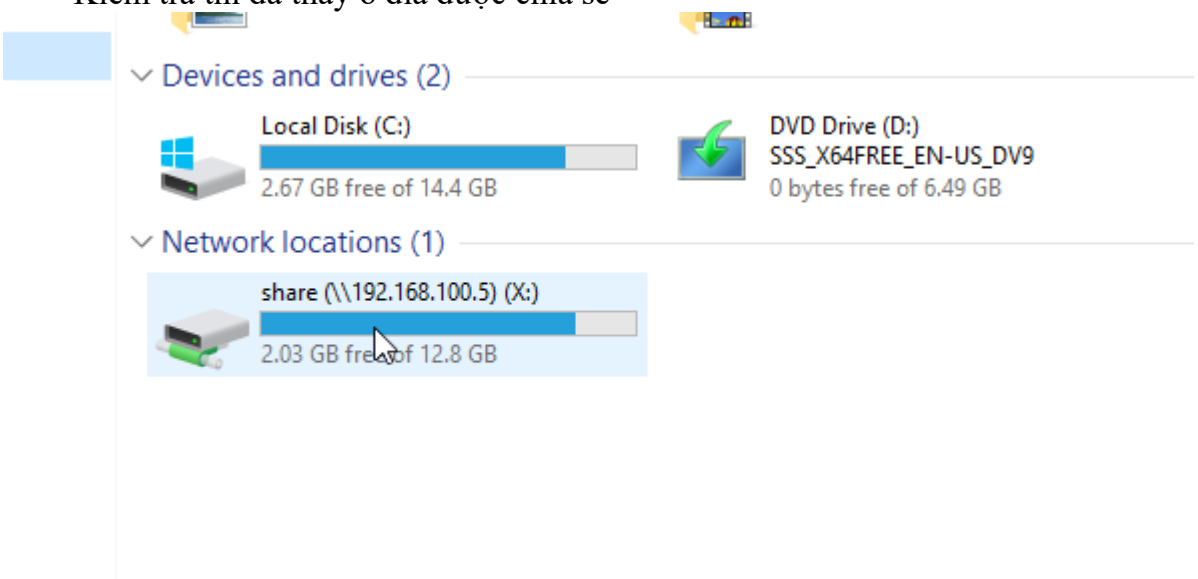
- Trên windows server 2016 dùng lệnh net use x: \\192.168.100.5\share để ánh xạ ổ đĩa mạng tới phần chia sẻ



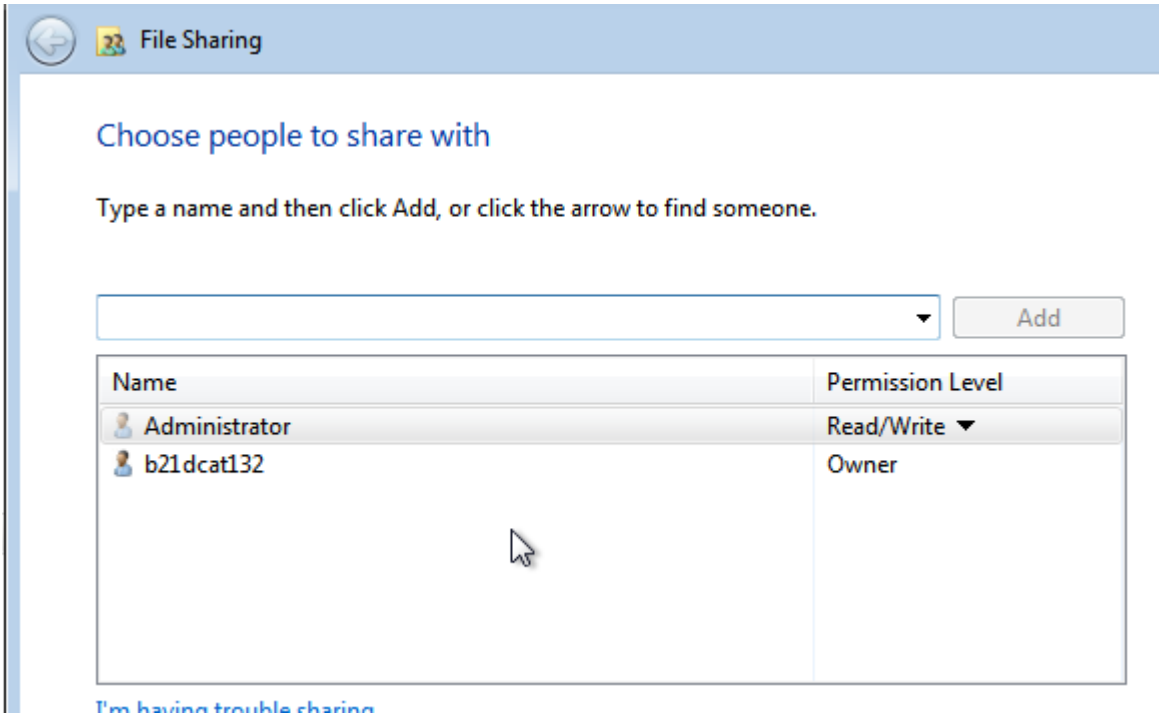
- Dùng lệnh net use để hiển thị các ổ đĩa được chia sẻ



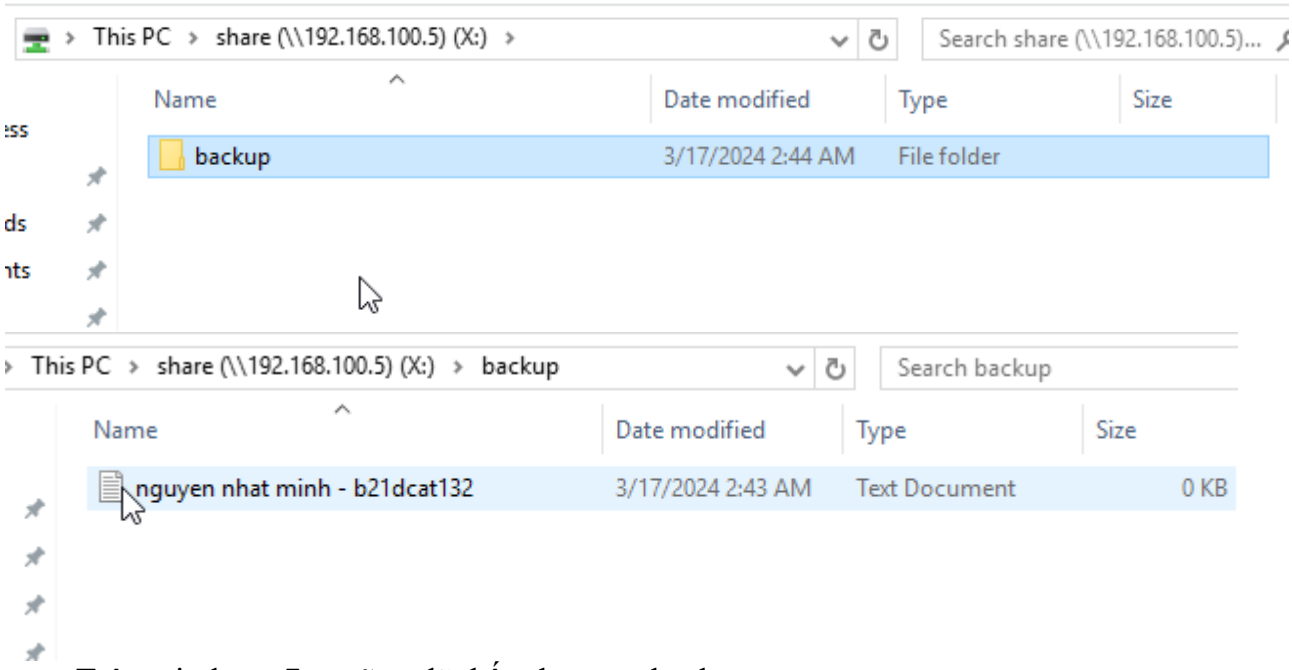
- Kiểm tra thì đã thấy ổ đĩa được chia sẻ



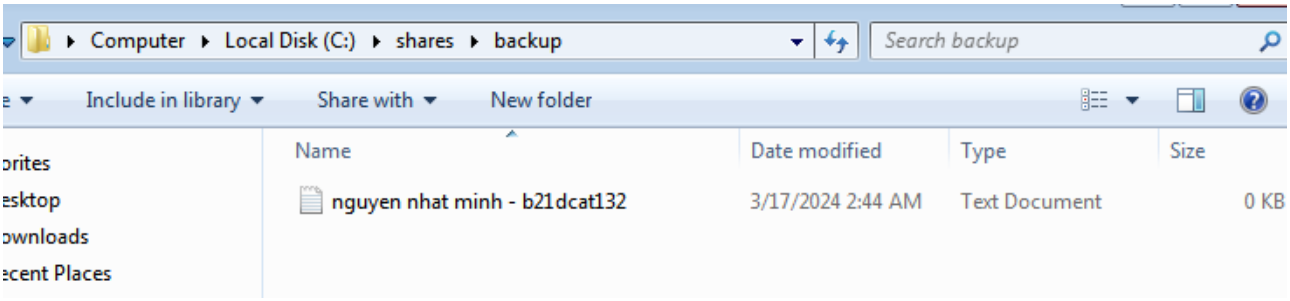
- Tại windows 7, chỉnh sửa quyền để windows server có thể tạo thư mục backup trong shares



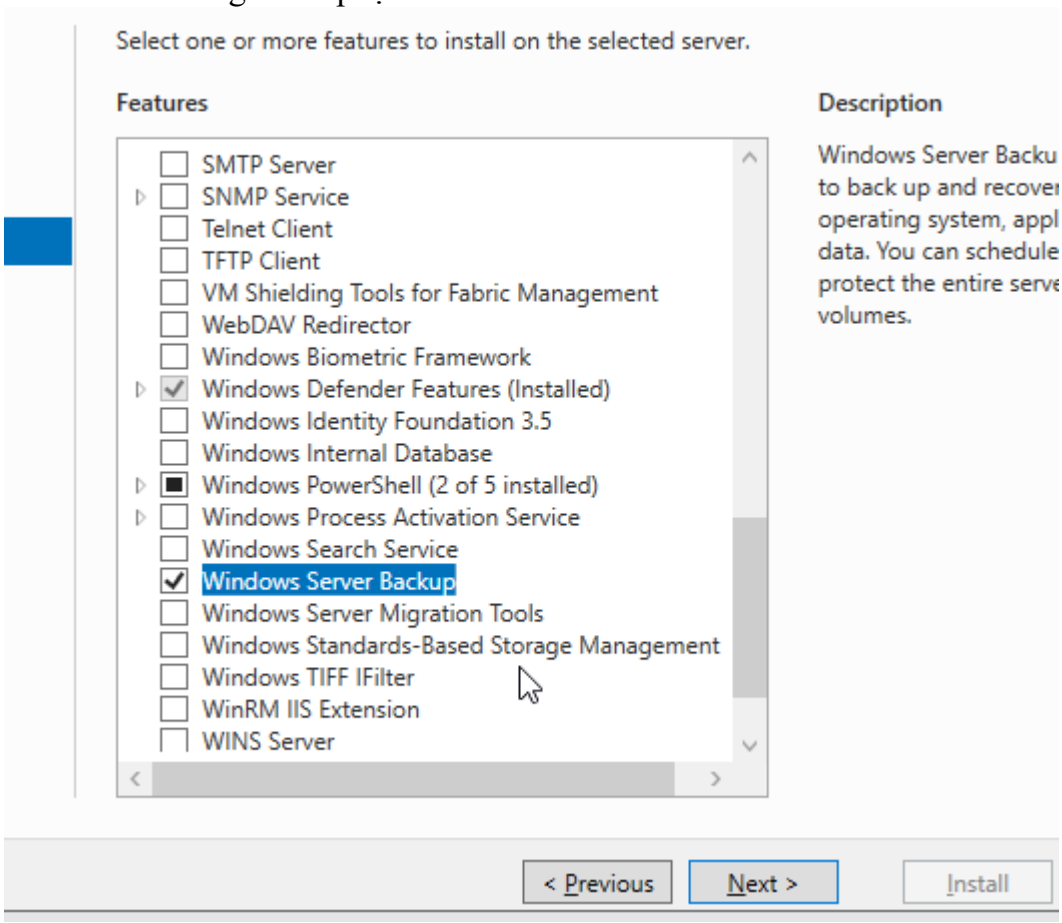
- Tại windows server, tạo thư mục backup trong ổ đĩa



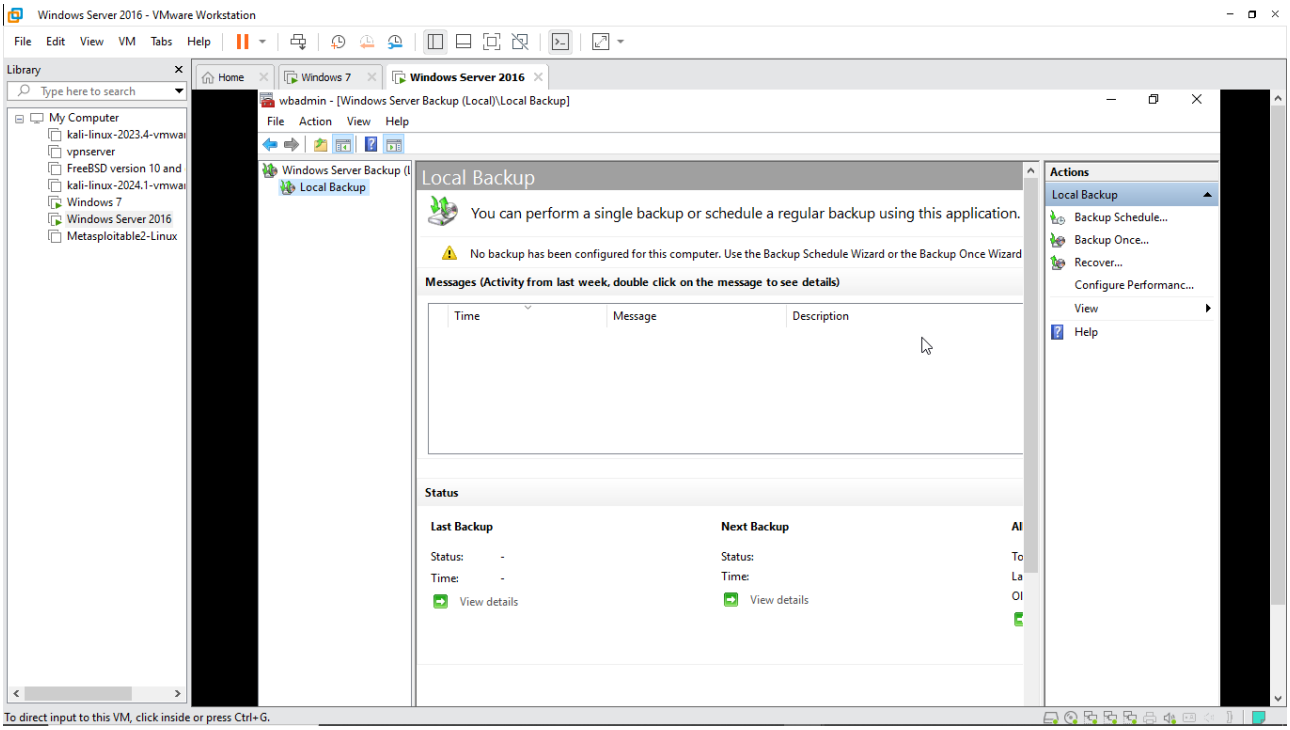
- Trên windows 7 ta cũng đã thấy thư mục backup



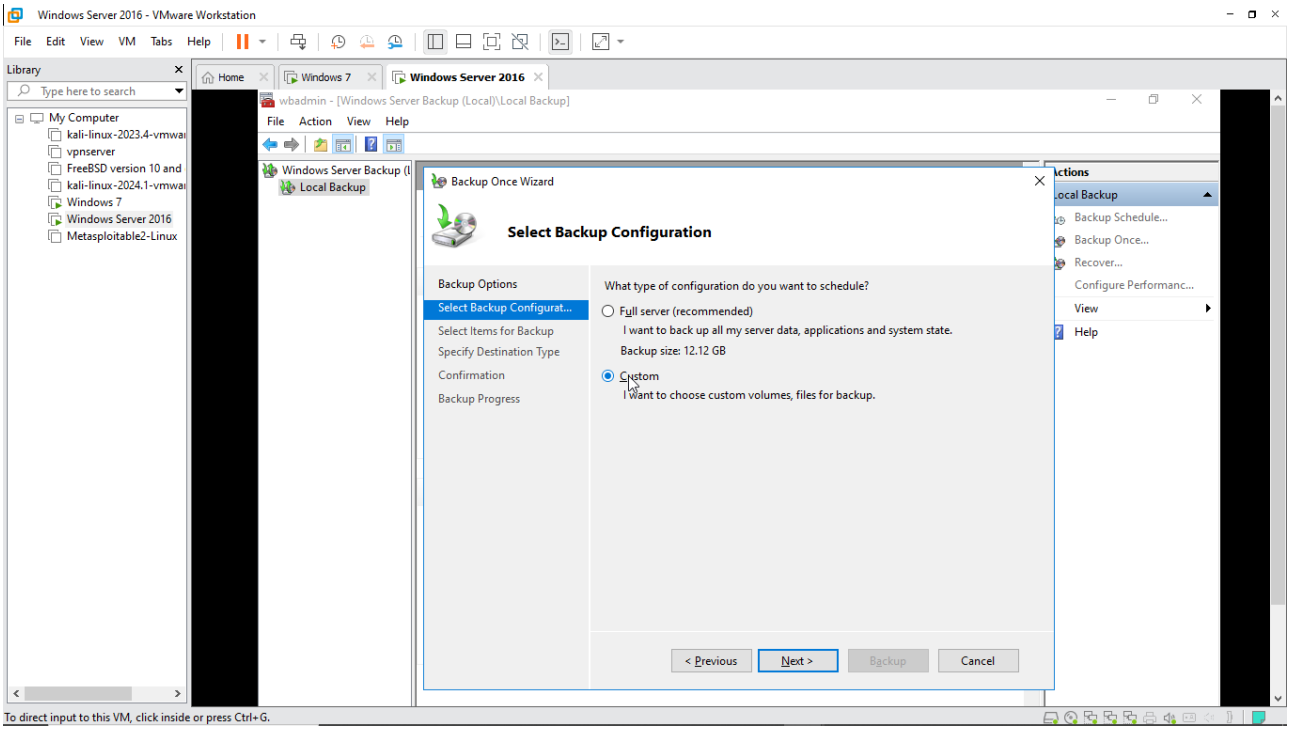
- Thêm tính năng backup tại windows server



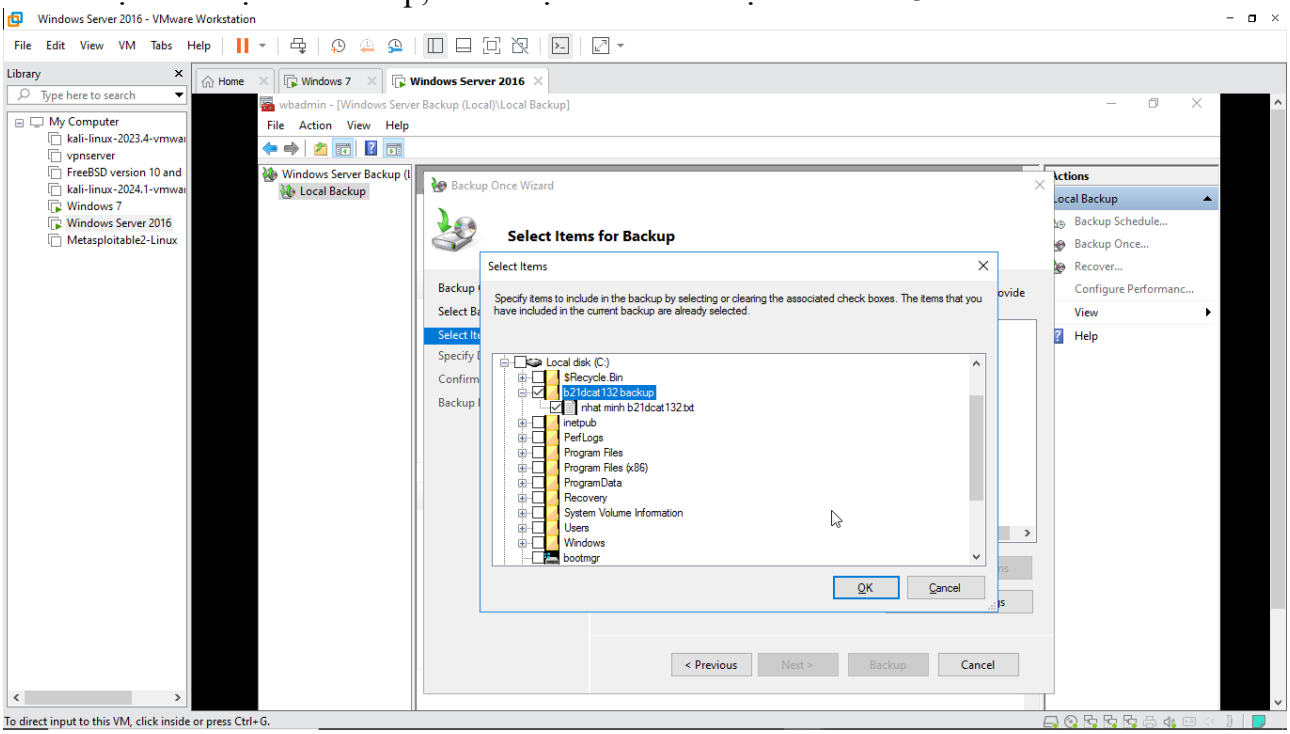
- Sau khi tải xong, vào server manager chọn tools, chọn windows server backup



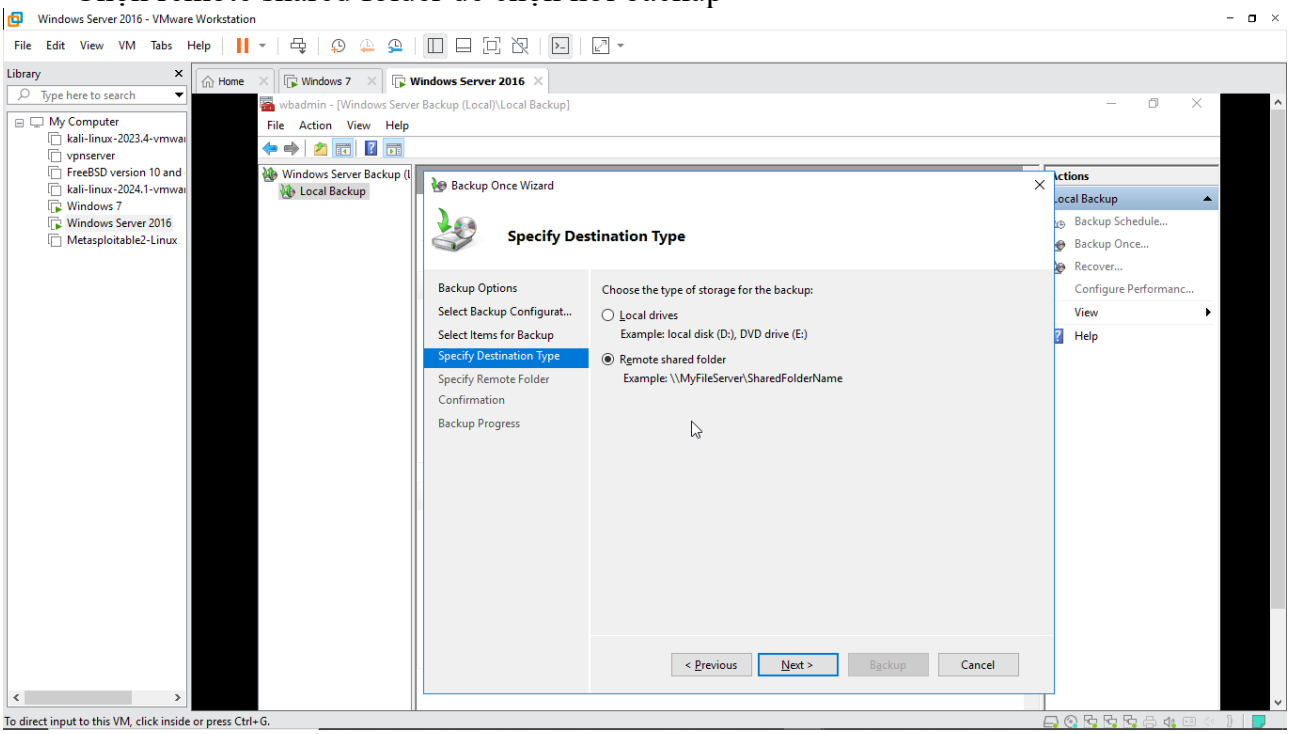
- Ở phần local backup chọn backup once ở góc trên bên phải màn hình, chọn custom



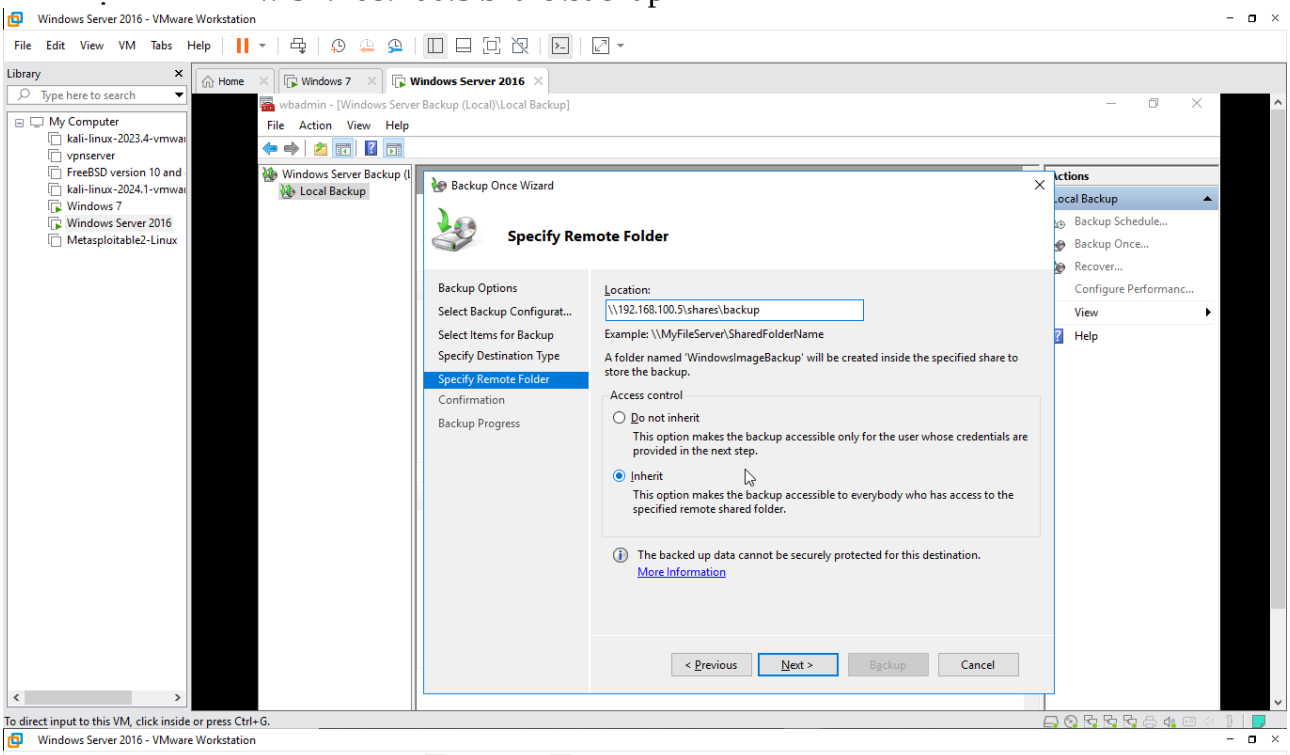
- Chọn thư mục để backup, em đã tạo sẵn 1 thư mục b21dcat132

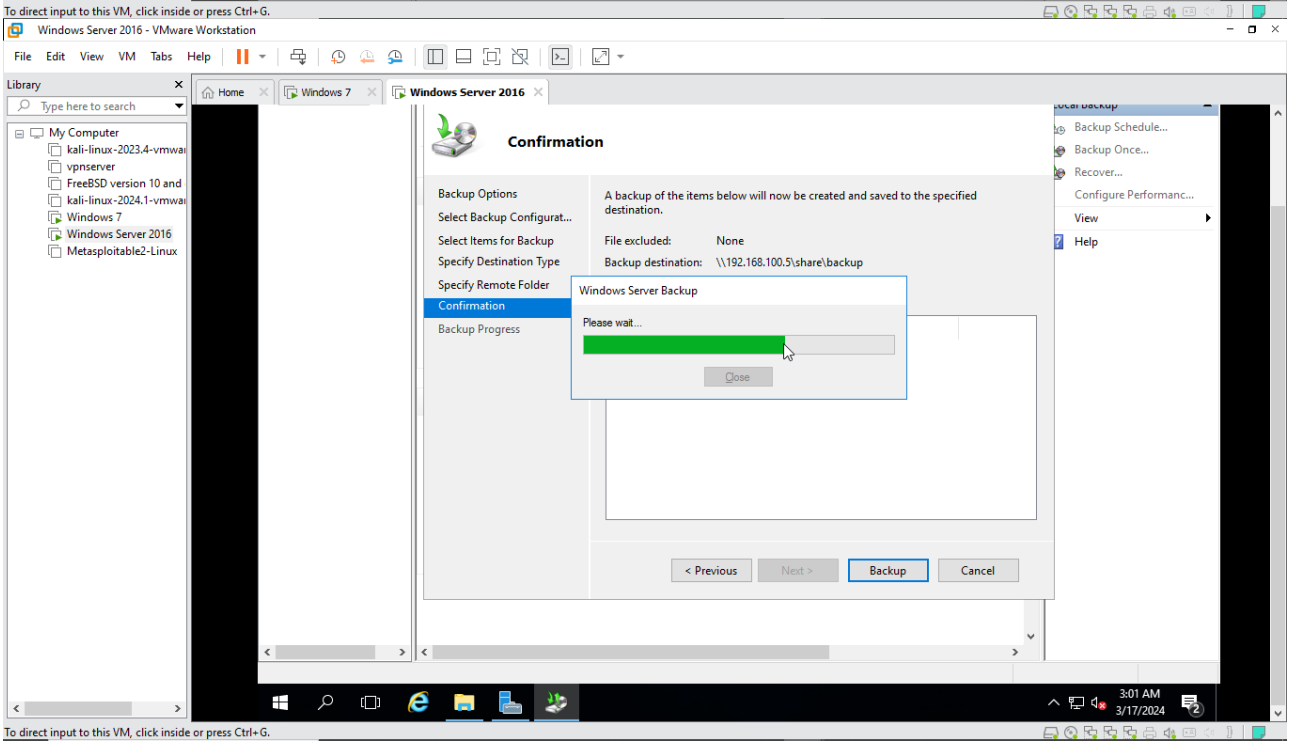


- Chọn remote shared folder để chọn nơi backup

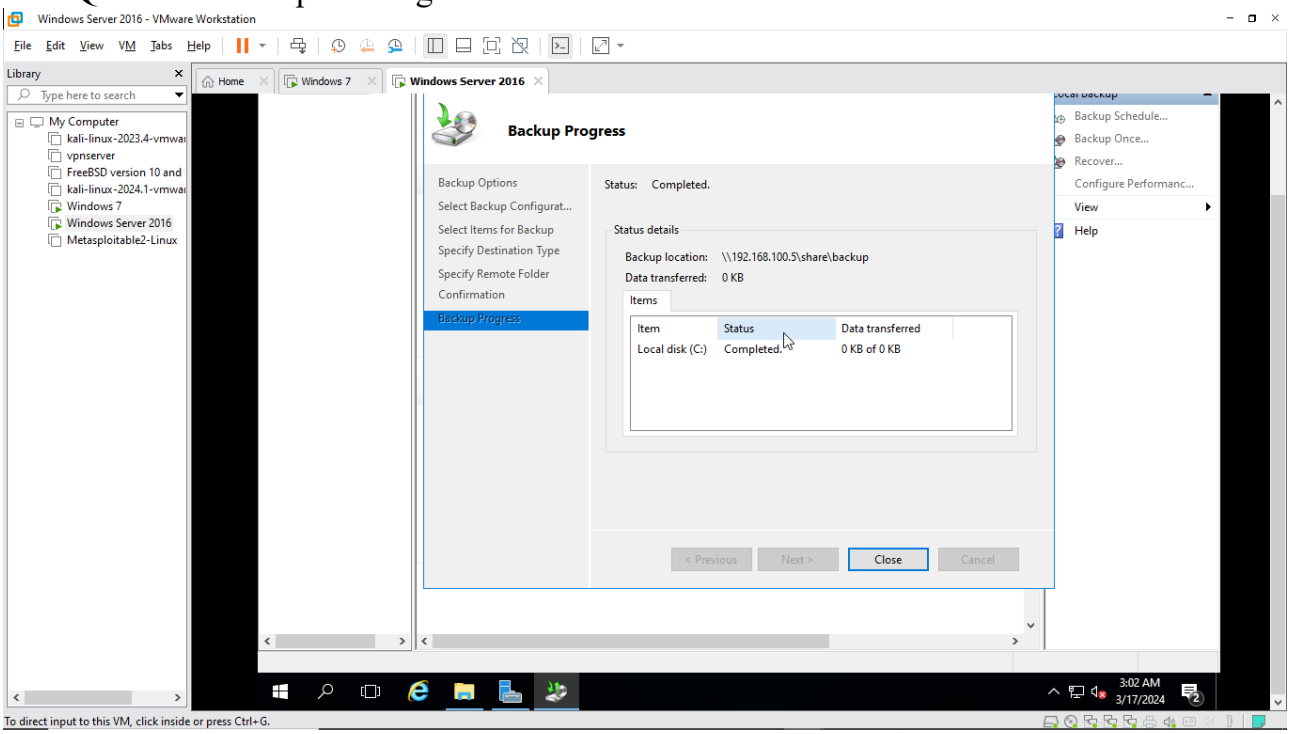


- Địa chỉ sẽ là \\192.168.100.5\share\backup

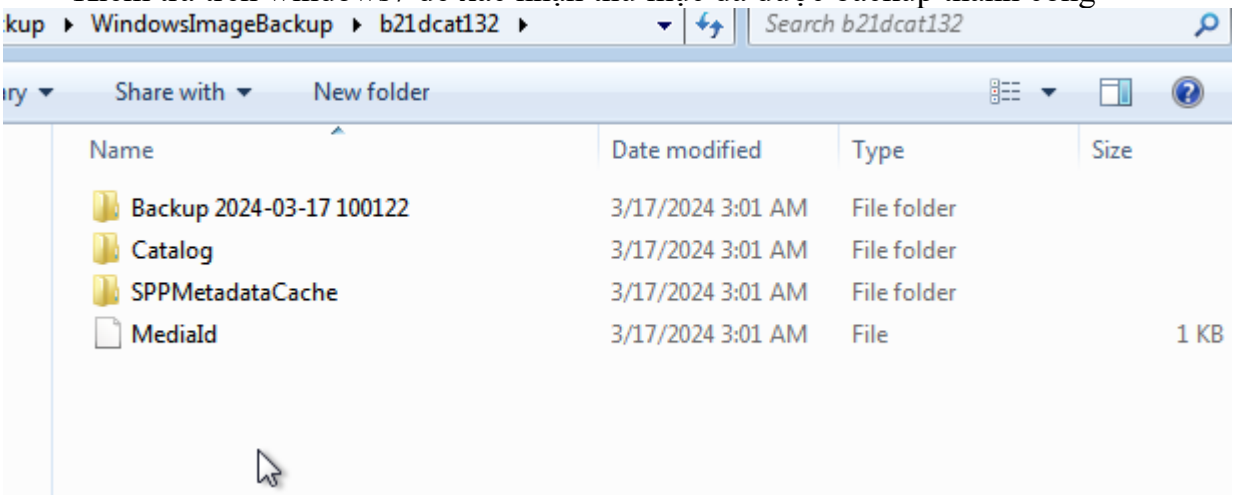




- Quá trình backup đã xong



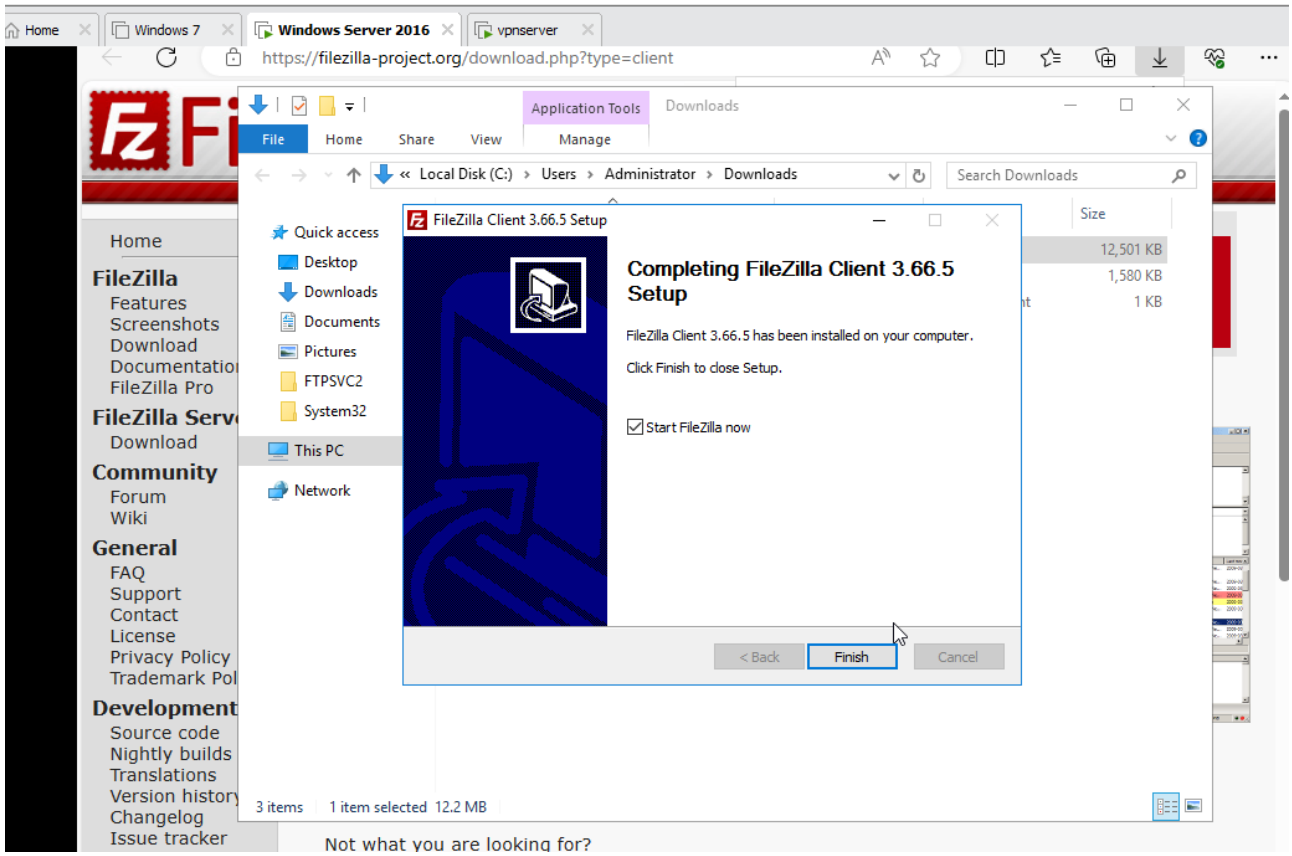
- Kiểm tra trên windows7 để xác nhận thư mục đã được backup thành công



4.2. Sao lưu tệp lên ftp server

Để cài đặt một FTP client trên Windows, ta có thể sử dụng nhiều cách khác nhau, nhưng một trong những cách phổ biến nhất là sử dụng ứng dụng FTP client của bên thứ ba. Ta sẽ dùng FileZilla

- Tải và cài đặt FileZilla trên windows victim



- Trên linux ubuntu cài đặt vsftpd qua lệnh sudo apt install vsftpd

```
vpnserver@minhnn132:~$ sudo apt install vsftpd
[sudo] password for vpnserver:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 277 not upgraded.
Need to get 115 kB of archives.
After this operation, 334 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu focal-updates/main amd64 vsftpd amd64 3.0.5-0ubuntu0.20.04.1 [11
Fetched 115 kB in 1s (134 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 188371 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0ubuntu0.20.04.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0ubuntu0.20.04.1) ...
Setting up vsftpd (3.0.5-0ubuntu0.20.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.s
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.20) ...
```

- Khởi động dịch vụ vsftpd trên máy Ubuntu victim bằng lệnh sudo systemctl start vsftpd và sudo systemctl enable vsftpd.
- Kiểm tra trạng thái vsftpd bằng câu lệnh sudo systemctl status vsftpd

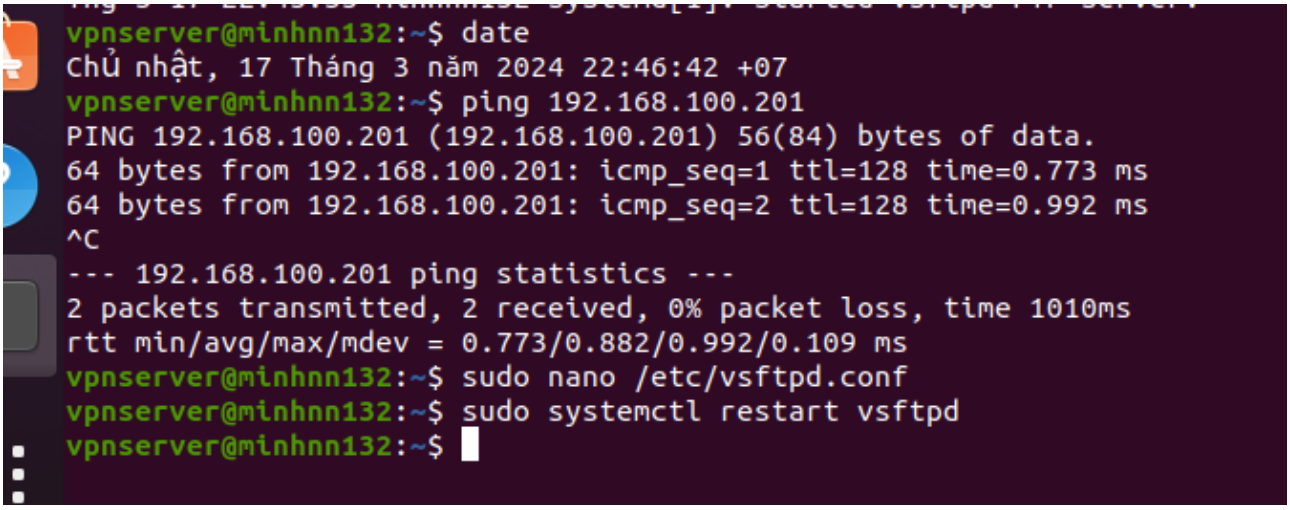
```
vpnserver@minhnn132:~$ sudo systemctl start vsftpd
[sudo] password for vpnserver:
vpnserver@minhnn132:~$ sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
vpnserver@minhnn132:~$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-03-17 22:43:35 +07; 3min 2s ago
   Main PID: 898 (vsftpd)
      Tasks: 1 (limit: 2141)
     Memory: 708.0K
     CGroup: /system.slice/vsftpd.service
             └─898 /usr/sbin/vsftpd /etc/vsftpd.conf

Thg 3 17 22:43:35 minhnn132 systemd[1]: Starting vsftpd FTP server...
Thg 3 17 22:43:35 minhnn132 systemd[1]: Started vsftpd FTP server.
vpnserver@minhnn132:~$ date
Chủ nhật, 17 Tháng 3 năm 2024 22:46:42 +07
vpnserver@minhnn132:~$
```

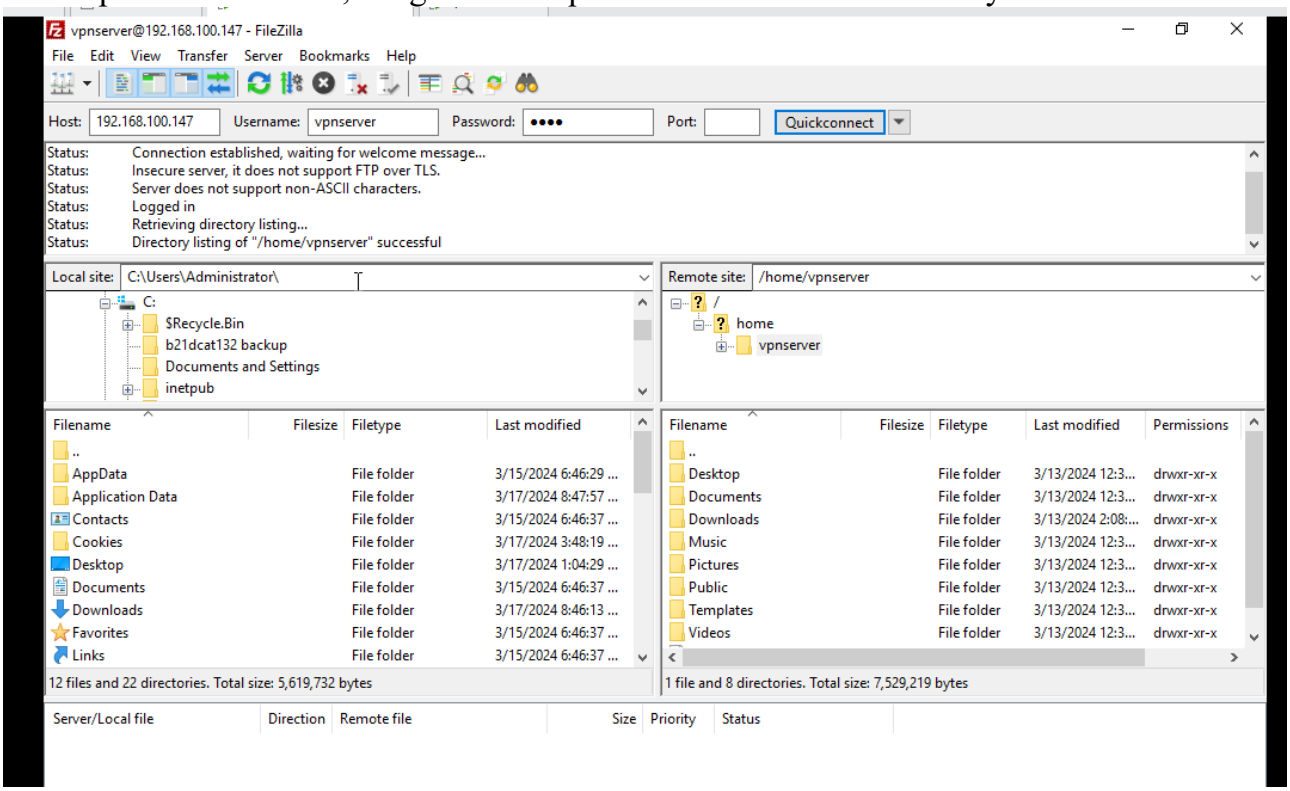
- Chỉnh sửa lại tệp vsftpd.conf , chuyển write_enable = YES và anon_mkdir_write_enable = YES để cho phép FTP client tải tệp mới.

```
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
```

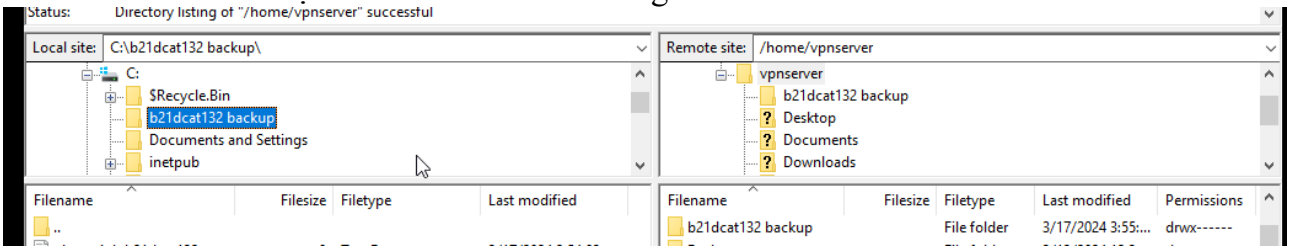
- Khởi động lại vsftps



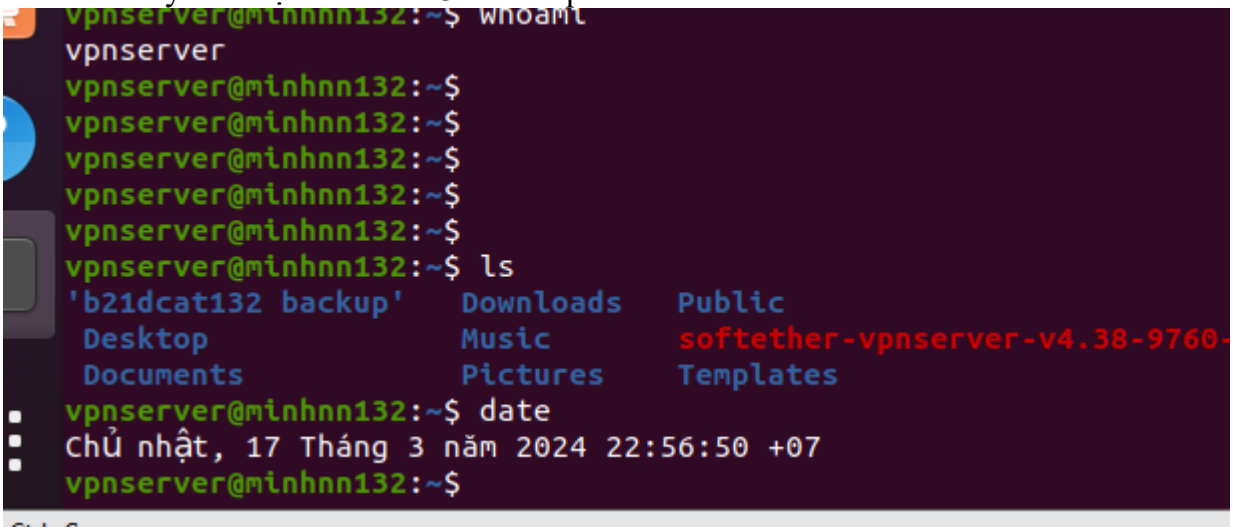
- Trên windows victim, vào filezilla chọn host là 192.168.100.147, user là vpnserver password là 3153, cổng số 21 và quickconnect để kết nối tới máy ubuntu



- Sao lưu 1 thư mục từ windows victim sang ubuntu

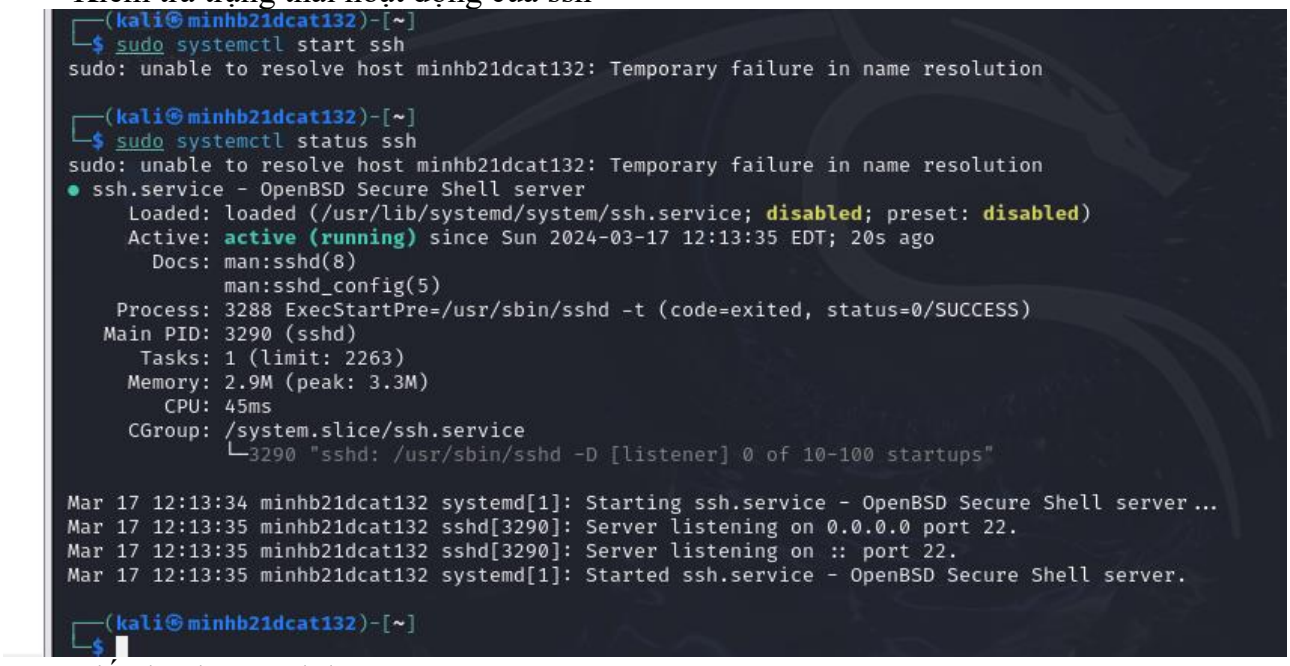


- Chuyển sang ubuntu để kiểm tra thư mục đã sao lưu thành công
- Đã thấy thư mục b21dcat132 backup

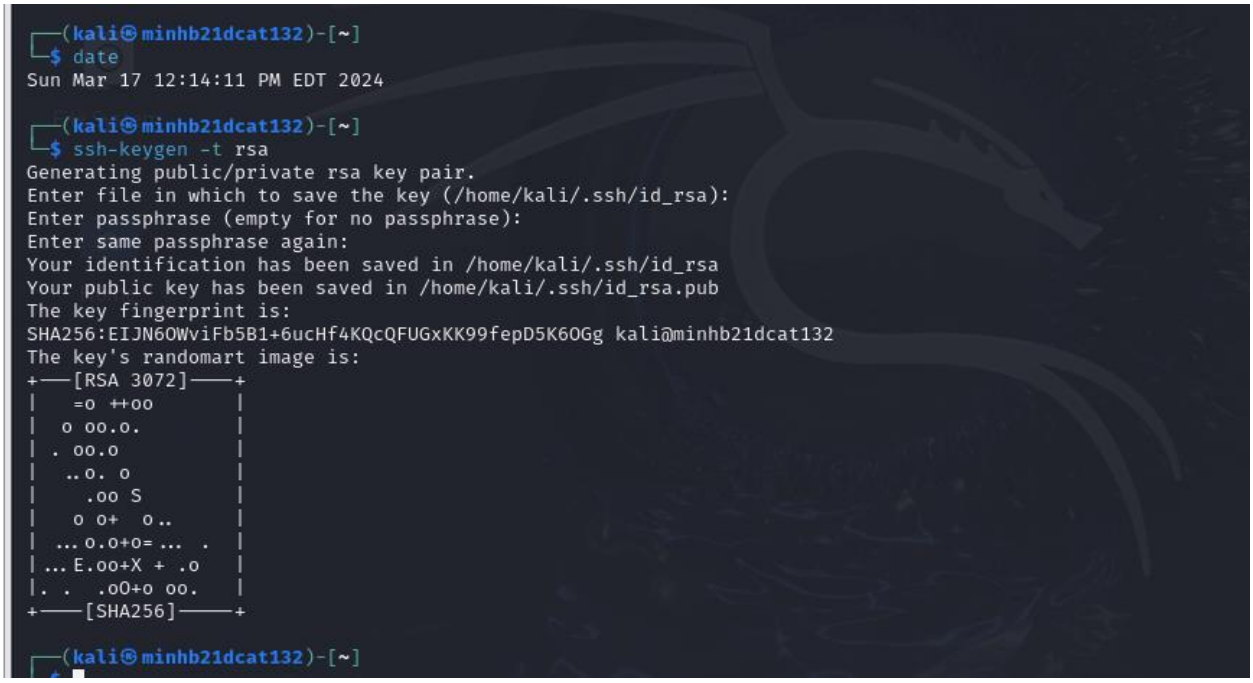


4.3. Sao lưu tệp sử dụng SCP

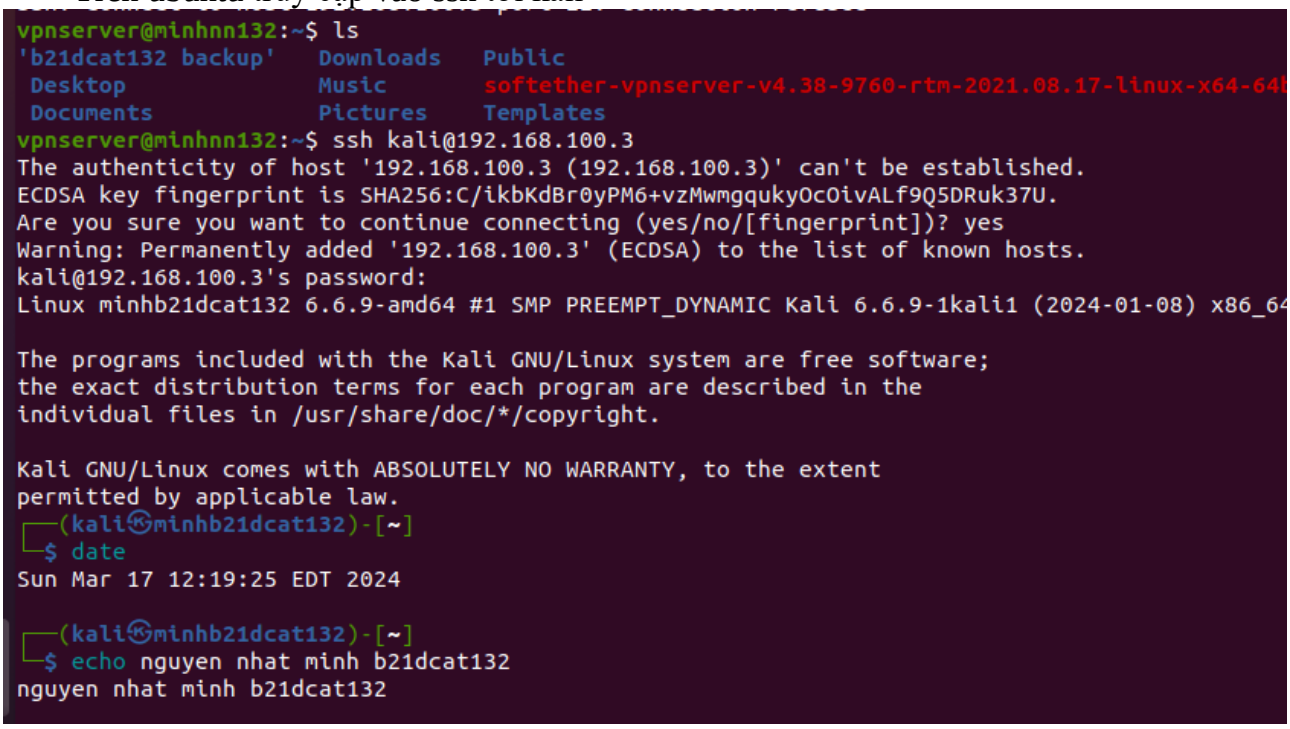
- Trên máy kali cài đặt ssh server qua lệnh sudo apt install openssh-server
- Kiểm tra trạng thái hoạt động của ssh



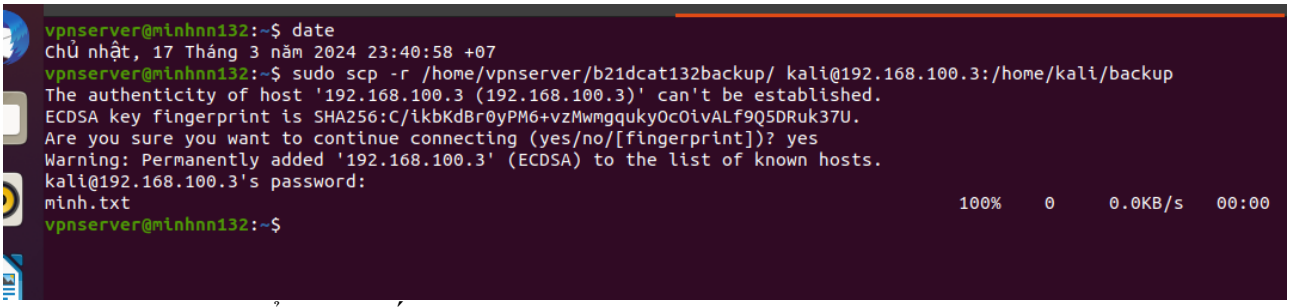
- Tiến hành tạo ssh key



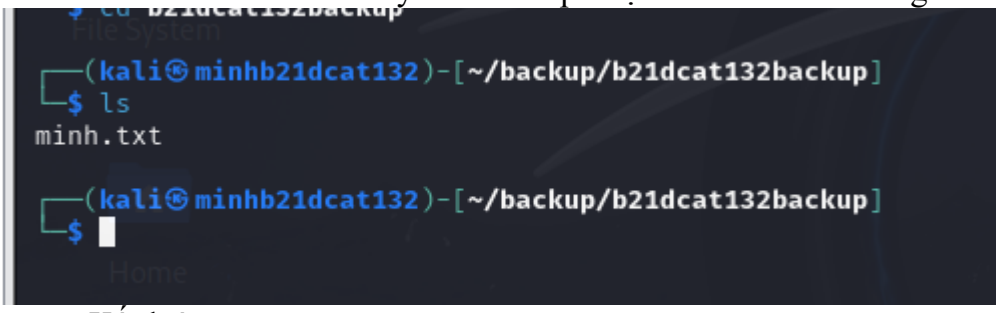
- Trên ubuntu truy cập vào ssh tới kali



- Copy file backup sang kali



- Trên kali ta kiểm tra thấy file backup được sao lưu thành công



5. Kết luận

- Bài thực hành hoàn thành vào ngày 17/03/2024