

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



Môn học: Thực Tập Cơ Sở
Báo Cáo Bài Thực Hành 11
Sao lưu hệ thống

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 04

Giảng viên: Đinh Trường Duy

Hà Nội, 3/2024

Mục lục

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	4
2.1.5. Net view	5
2.2. Các bước thực hiện	5
2.2.1. Chuẩn bị môi trường.....	5
2.2.2. Sao lưu tới ổ đĩa mạng.....	6
2.2.3. Sao lưu tệp lên FTP Server	12
2.2.4. Sao lưu tệp sử dụng SCP	15
3. Kết luận	18
4. Tài liệu tham khảo.....	18

Danh mục hình ảnh

Cấu hình topo mạng.....	6
Tạo thư mục chia sẻ file	6
Cấu hình Map Network Driver.....	7
Kết quả, trên Windows Server đã tồn tại ổ đĩa mạng chia sẻ.....	7
Cấu hình để thư mục backup lưu ở ổ đĩa mạng.....	9
Hoàn tất quá trình backup.....	10
Xuất hiện thư mục backup được lưu trên Windows Server	10
Trên Windows 10, xuất hiện thư mục backup của Windows Server	11
Minh chứng.....	11
Cài đặt FileZilla.....	12
Cài đặt.....	12
Bật dịch vụ ftp	13
Kết nối đến ftp server	13
Kết quả sau khi kết nối	14
Sao lưu 1 thư mục trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client.....	14
Kiểm tra thư mục backup trong Ubuntu (Minh chứng)	15
Kiểm tra dịch vụ ssh đã bật hay chưa.....	15
Bật dịch vụ ssh.....	15
Cấu hình ssh cho phép truy cập vào tài khoản root trên Kali.....	16
Khởi động lại dịch vụ ssh	16
Tạo Secure Shell Keys trên máy Kali Linux	16
Sao lưu file vào thư mục root	17
Sao lưu thư mục backup vào thư mục root trên máy Kali.....	17
Kết quả, file và thư mục đã được sao lưu vào thư mục root trên máy Kali	17

1. Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log 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. Cơ sở lý thuyết

2.1.1. SCP – Secure copy

SCP (Secure Copy Protocol) là một công cụ trong hệ thống Unix/Linux được sử dụng để sao chép và truyền tải các tệp tin và thư mục giữa các máy tính qua mạng. SCP sử dụng giao thức SSH (Secure Shell) để mã hóa dữ liệu trong quá trình truyền tải, giúp đảm bảo tính bảo mật 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 bạn muốn sao chép.
- destination_file: là nơi bạn muốn lưu trữ tệp tin hoặc thư mục sao chép đến.

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 truyền tệp dùng để truyền tải dữ liệu giữa máy tính và máy chủ trên mạng Internet. FTP thường được sử dụng để tải lên (upload) hoặc tải xuống (download) tệp tin, thư mục và dữ liệu từ hoặc tới một máy chủ.

FTP sử dụng cơ chế xác thực người dùng thông qua tên đăng nhập và mật khẩu, nhưng thông tin này không được mã hóa, nên FTP không được coi là an toàn khi truyền tải dữ liệu qua Internet. Tuy nhiên, có một phiên bản bảo mật của FTP được gọi là FTPS (FTP Secure) hoặc FTP-SSL, sử dụng SSL/TLS để mã hóa dữ liệu và cung cấp tính bảo mật hơn.

Một số đặc điểm chính của FTP bao gồm:

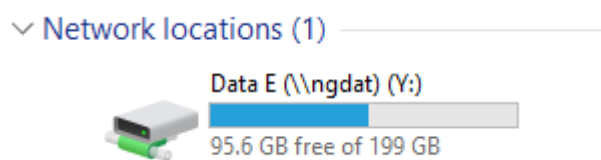
- **Truyền tải dữ liệu hai chiều:** FTP cho phép truyền tải dữ liệu cả từ máy tính tới máy chủ (upload) và từ máy chủ tới máy tính (download).
- **Hỗ trợ đa người dùng:** FTP hỗ trợ đồng thời nhiều kết nối từ nhiều người dùng khác nhau tới cùng một máy chủ FTP.
- **Quản lý thư mục:** FTP cho phép người dùng thực hiện các thao tác quản lý thư mục như tạo, xóa, đổi tên và di chuyển thư mục và tệp tin.
- **Thao tác tệp tin:** FTP cung cấp các thao tác để thực hiện các thao tác với tệp tin như sao chép, di chuyển, đổi tên và xóa tệp tin.
- Để sử dụng FTP, bạn cần một ứng dụng FTP client (như **FileZilla**, **WinSCP**) để kết nối tới máy chủ FTP và truyền tải dữ liệu. Máy chủ cũng cần được cài đặt một 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 với mạng máy tính và có thể truy cập từ nhiều thiết bị khác nhau trong mạng đó. Thường được sử dụng 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 cung cấp quyền truy cập và kiểm soát dữ liệu, cho phép người dùng truy cập, chỉnh sửa và chia sẻ dữ liệu một cách dễ dàng và hiệu quả qua mạng.

Map Network Drive (map ổ đĩa mạng) hay còn gọi là ánh xạ ổ đĩa mạng, là việc tạo liên kết (shortcut) tới thư mục (ổ đĩa) được chia sẻ trong mạng cục bộ.

Sau khi một ổ đĩa hoặc thư mục chia sẻ được ánh xạ, bạn có thể truy cập những tài nguyên được chia sẻ đó như thể nó đang nằm trên máy tính của mình. Network Drive có thể trông như một ổ đĩa cục bộ (ví dụ ổ đĩa C,D,E,...) trong File Explorer.



Việc này cũng tương tự như khi bạn tạo một shortcut cho tệp tin ra Desktop, khác ở chỗ nó tạo shortcut cho các tài nguyên trong mạng. Vì nó chỉ là những shortcut đến tệp tin được chia sẻ trong mạng nên việc bạn Map ổ đĩa mạng không ảnh hưởng đến dung lượng ổ cứng trên máy tính hiện tại.

2.1.4. Net use

Net use là một lệnh trong hệ điều hành Windows dùng để kết nối hoặc ngắt kết nối với một tài nguyên mạng, chẳng hạn như máy chủ, ổ đĩa mạng, hoặc máy in trên mạng. Cụ thể, lệnh này thường được sử dụng để ánh xạ một đường dẫn mạng tới một ổ đĩa

địa phương, cho phép người dùng truy cập các tài nguyên mạng như thể chúng là các ổ đĩa cục bộ.

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 định danh của ổ đĩa được ánh xạ tới tài nguyên mạng.
- \\computer_name\share_name là đường dẫn tới tài nguyên mạng mà bạn muốn kết nối.
- /persistent:{yes | no} là tùy chọn để xác định liệu kết nối mạng này sẽ được lưu lại sau khi bạn khởi động lại hệ thống 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. Net view

Net view là một trong những lệnh 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 liệt kê các máy chủ, máy tính và các tài nguyên mạng khác có sẵn trên mạng local.

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 bạn 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 local 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**.

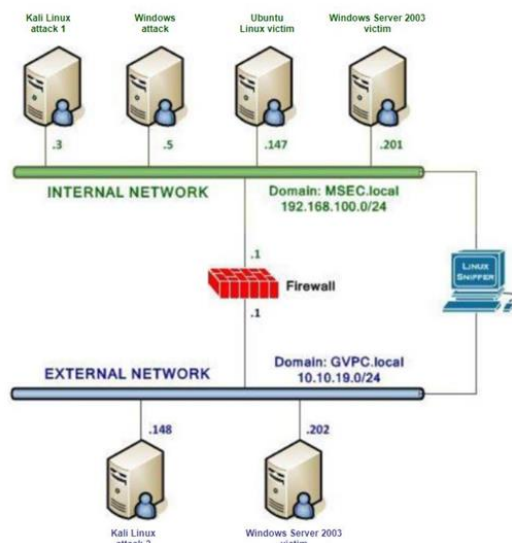
2.2. Các bước thực hiện

2.2.1. Chuẩn bị môi trường

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

Bài 11: Sao lưu hệ thống

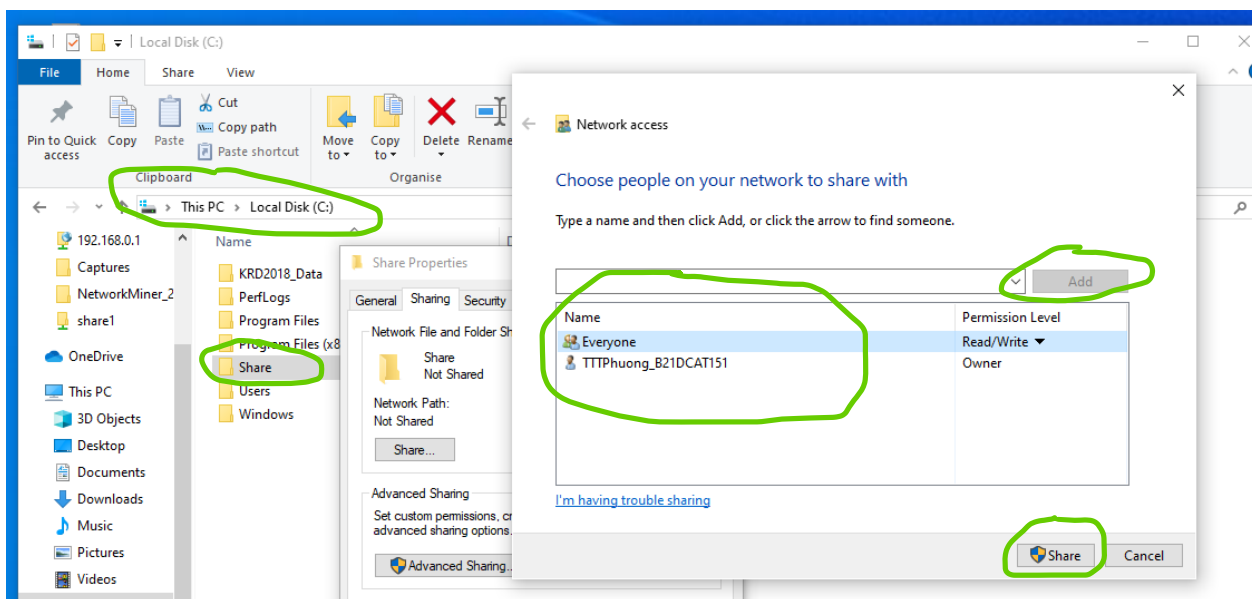
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
- Topo mạng như đã cấu hình trong bài 5.



Cấu hình topo mạng

2.2.2. Sao lưu tới ổ đĩa mạng

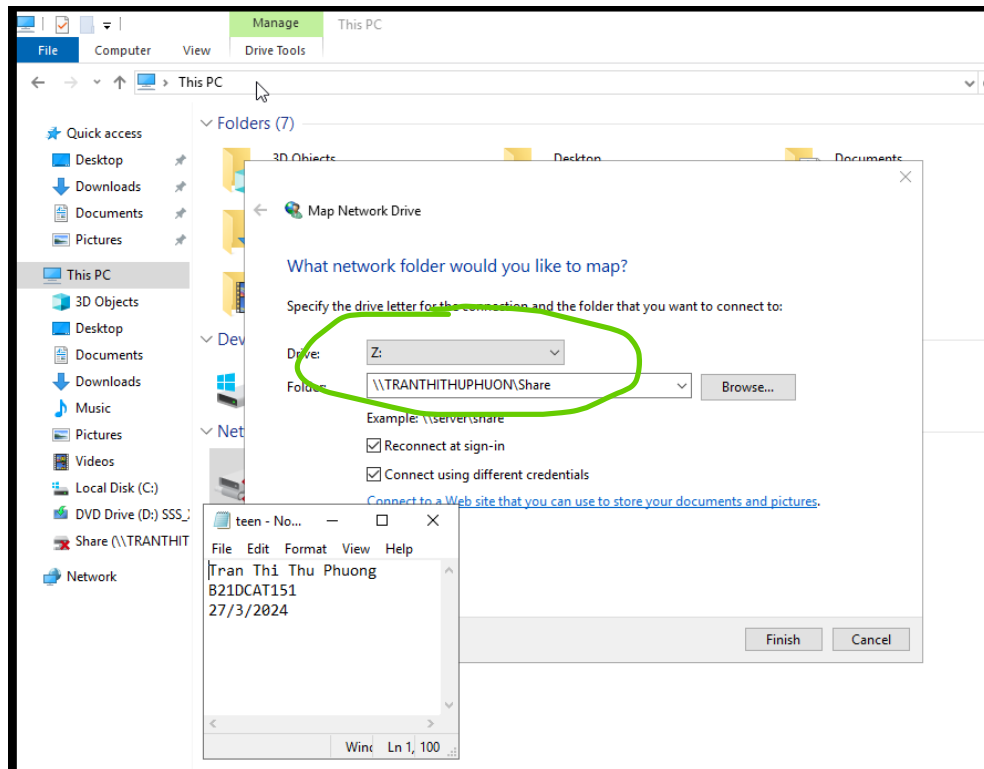
- Trên máy trạm Windows attack trong mạng Internal, tạo thư mục share rồi chia sẻ qua mạng (C:\net share share=c:\share)



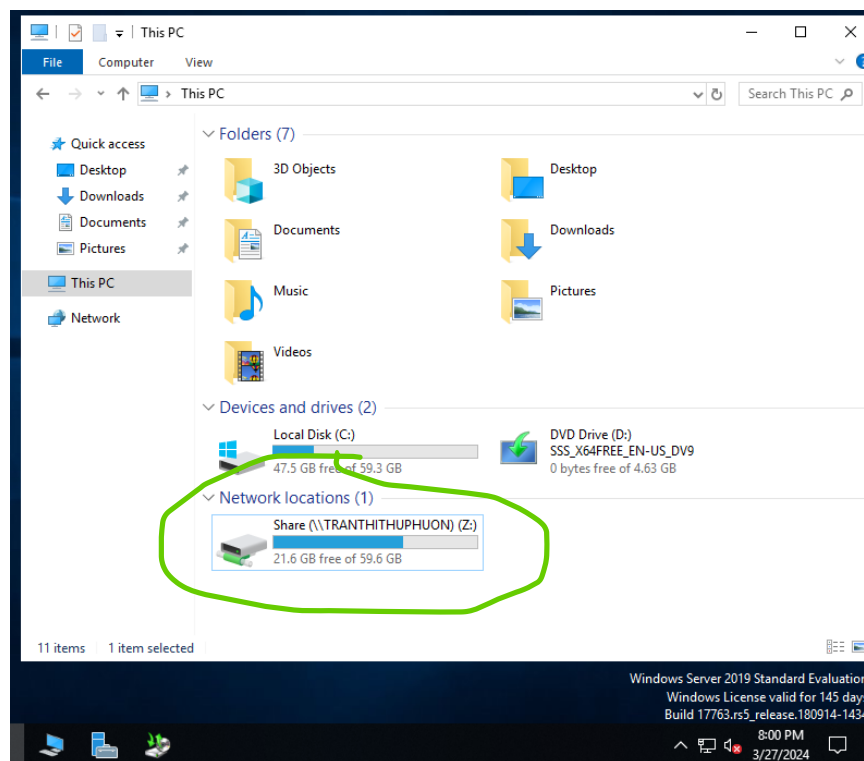
Tạo thư mục chia sẻ file

Bài 11: Sao lưu hệ thống

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



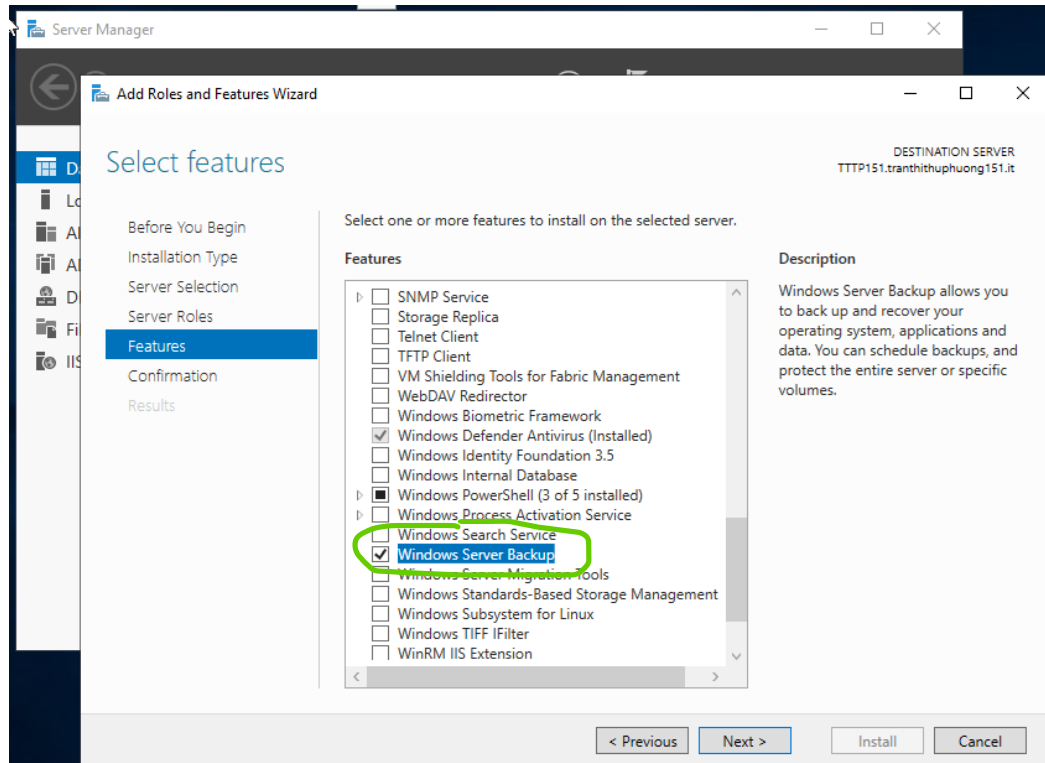
Cấu hình Map Network Driver



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

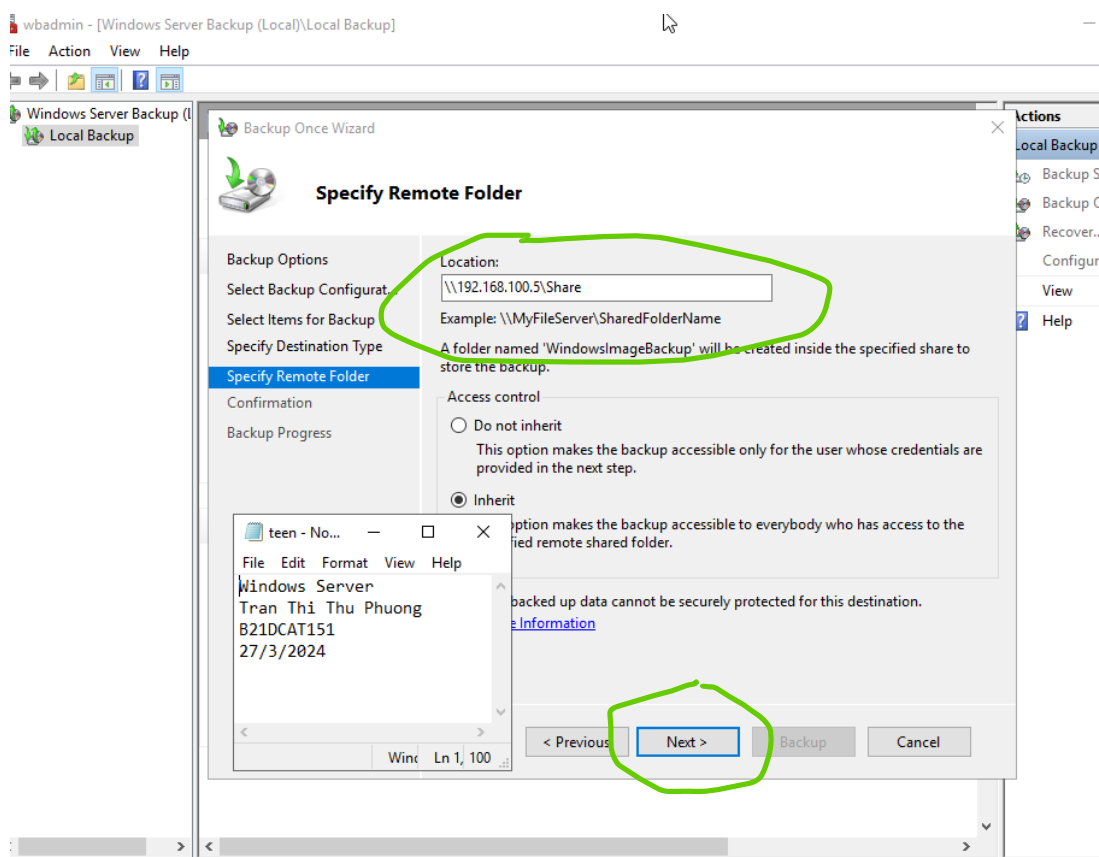
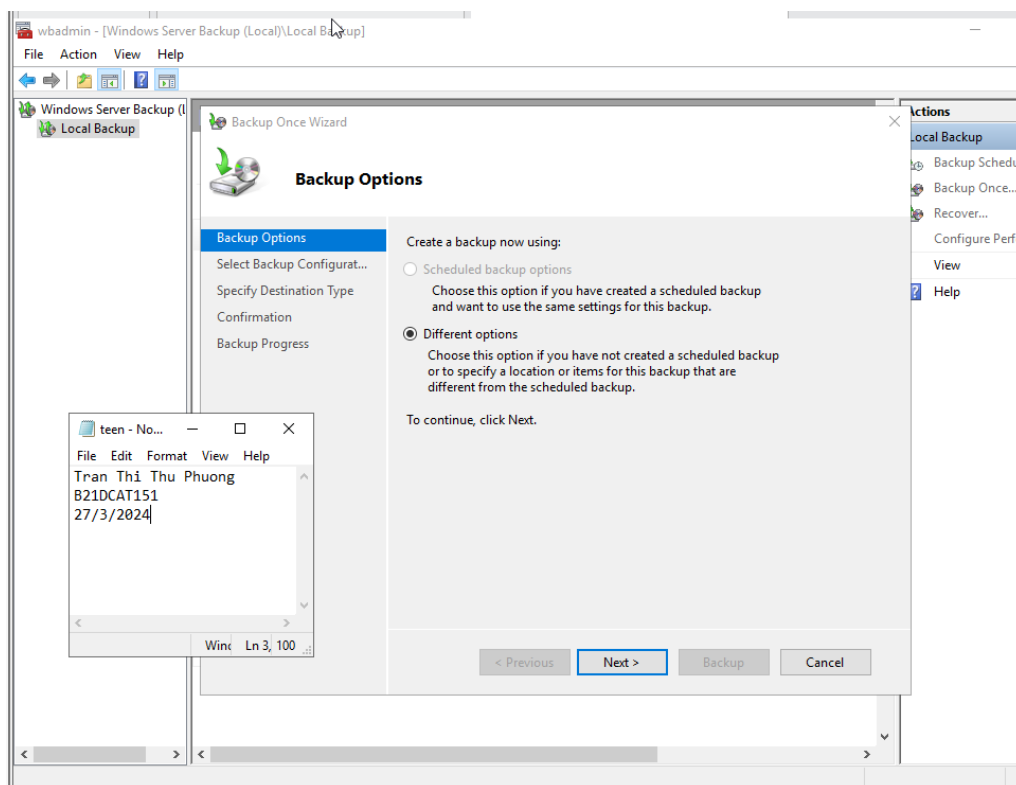
Bài 11: Sao lưu hệ thống

- 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 ở mạng đã chia sẻ trên máy Windows attack trong mạng Internal.
- + Cài đặt Windows Server Backup: Server Manager → Add Roles and Features



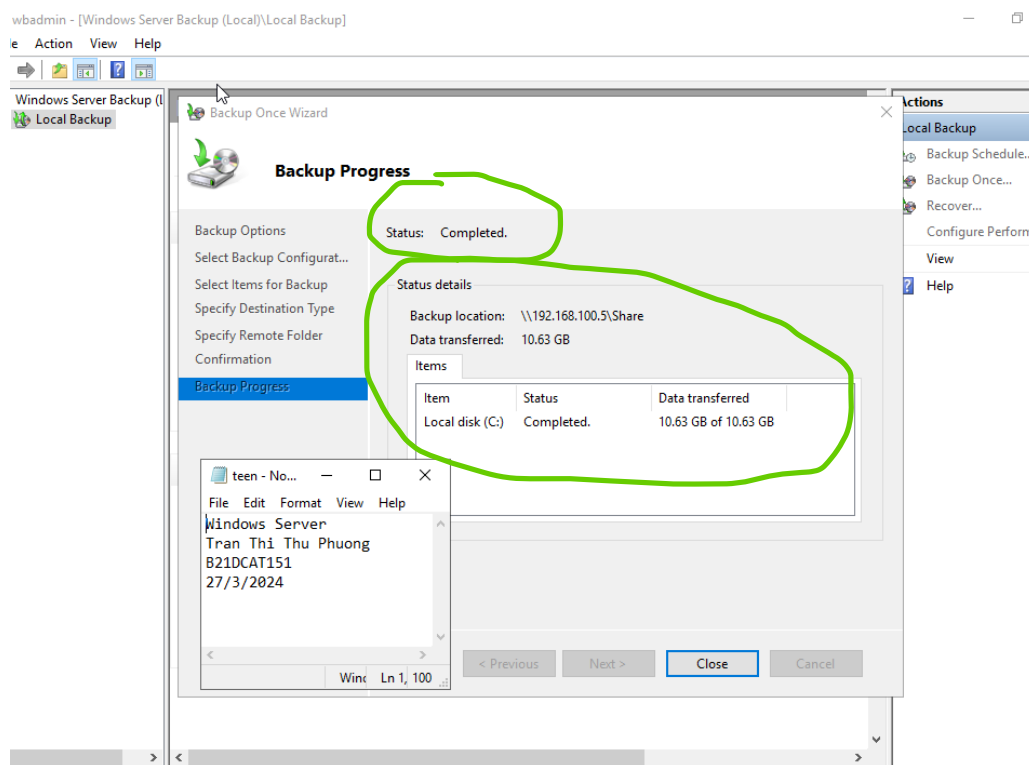
- + Sau khi đã cài xong, tiến hành backup: Server Manager → Tools → Windows Server Backup

Bài 11: Sao lưu hệ thống

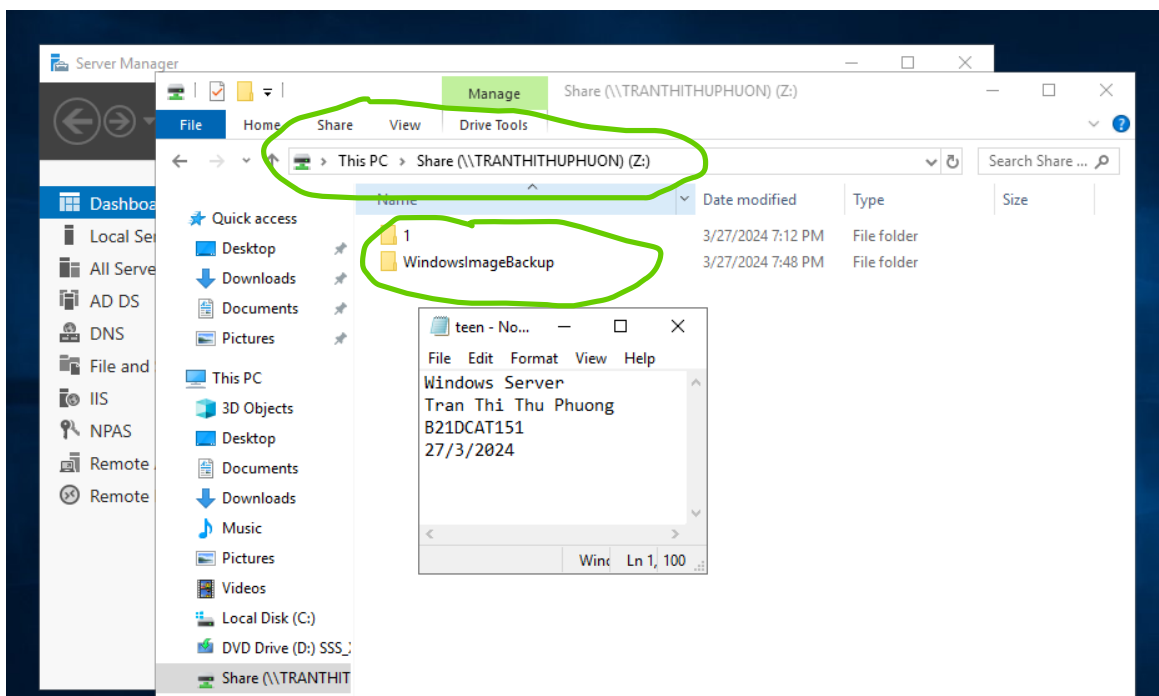


Cấu hình để thư mục backup lưu ở ổ đĩa mạng

Bài 11: Sao lưu hệ thống

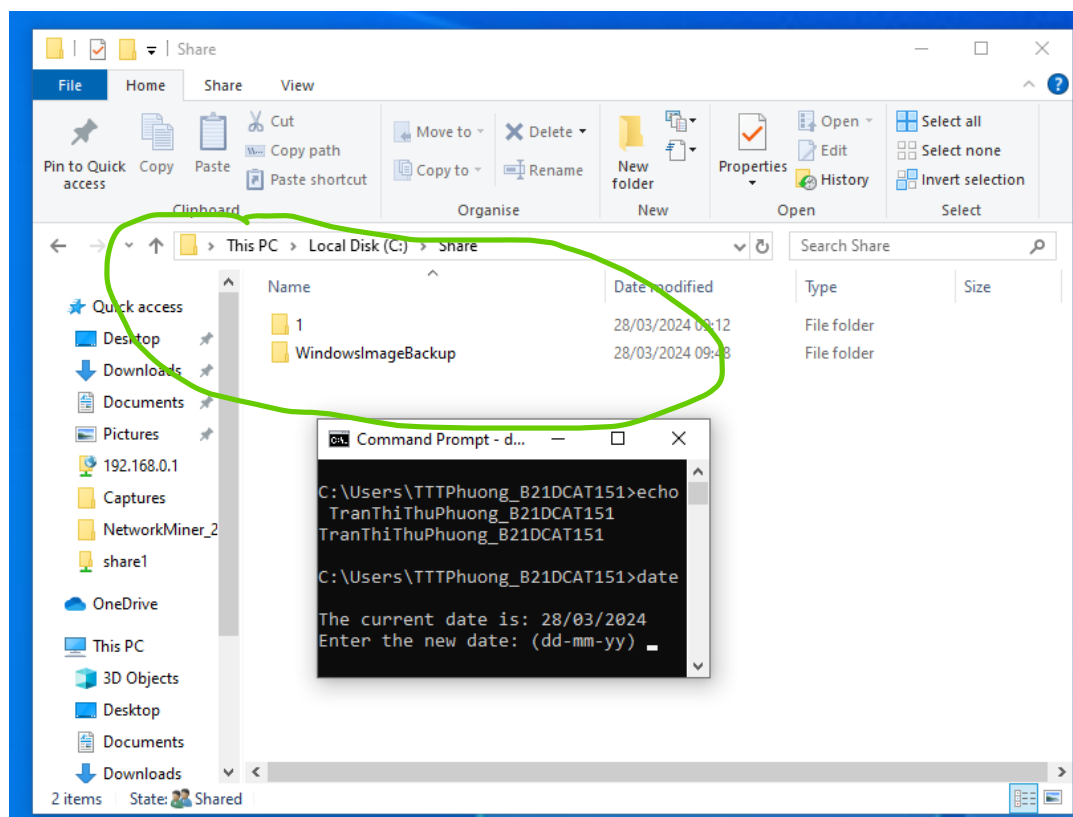


Hoàn tất quá trình backup

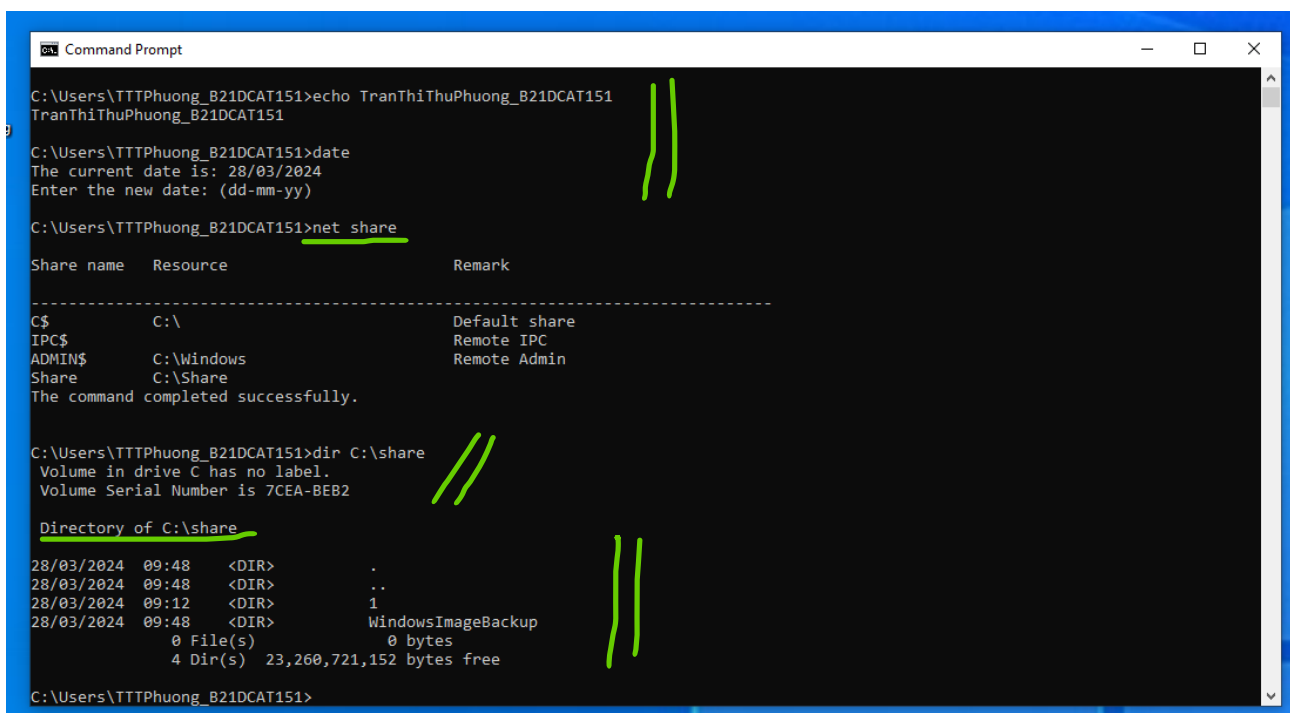


Xuất hiện thư mục backup được lưu trên Windows Server tại ổ đĩa mạng

Bài 11: Sao lưu hệ thống



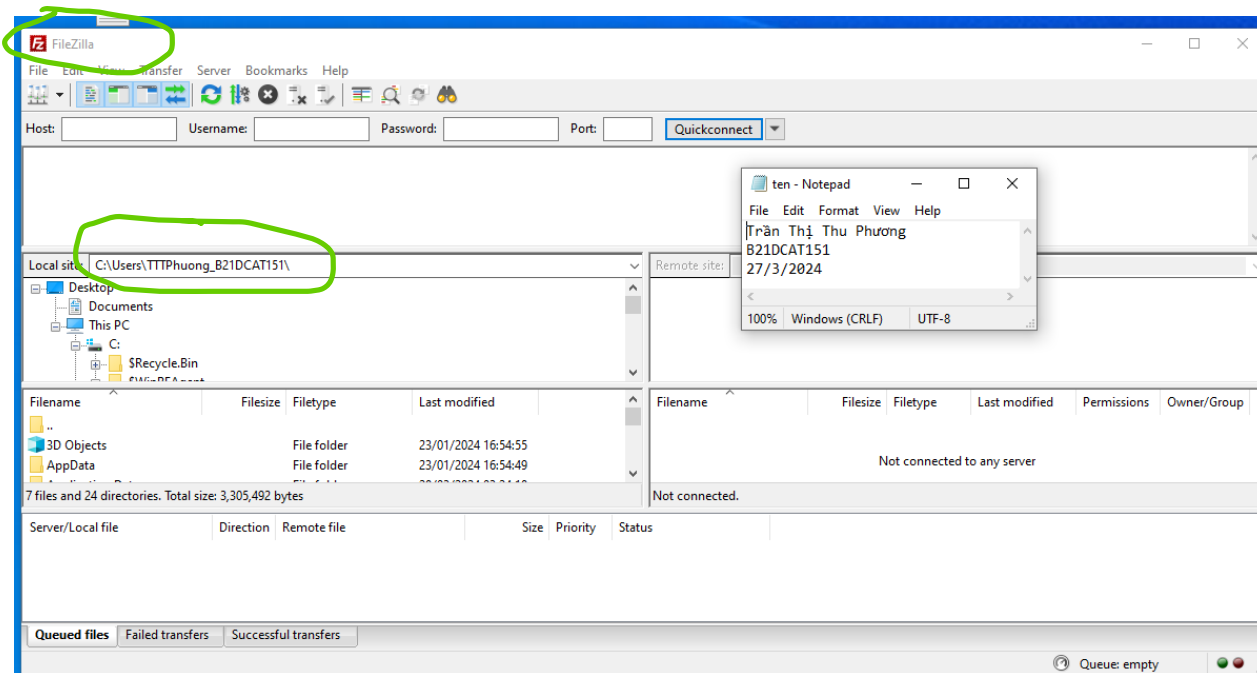
Trên Windows 10, xuất hiện thư mục backup của Windows Server tại thư mục được chia sẻ (C:\Share)



Minh chứng

2.2.3. Sao lưu tệp lên FTP Server

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



Cài đặt FileZilla

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

```
SIOCSIFADDR: operation not permitted
tranthithuphuongb21dcat151@slave-1:~$ sudo -s
[sudo] password for tranthithuphuongb21dcat151:
root@slave-1:~# ifconfig end33 192.168.100.147
SIOCSIFADDR: No such device
end33: ERROR while getting interface flags: No such device
root@slave-1:~# ifconfig ens33 192.168.100.147
root@slave-1:~# apt install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-liberation2 fonts-opensymbol gir1.2-goa-1.0
  gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0
  gir1.2-snapd-1 gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3
  libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1
```

Cài đặt

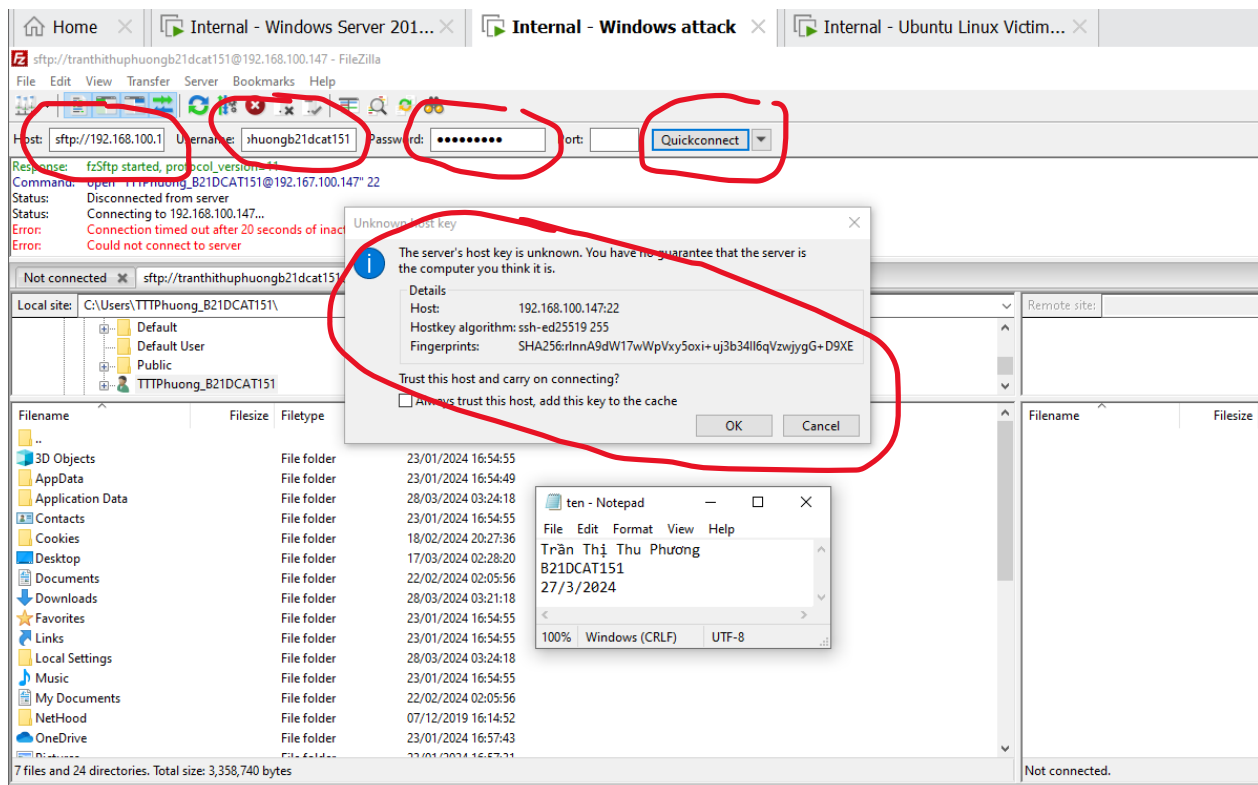
Bài 11: Sao lưu hệ thống

```
extr
tranthithuphuongb21dcat151@slave-1:~$ sudo systemctl start vsftpd.service
tranthithuphuongb21dcat151@slave-1:~$ sudo systemctl status vsftpd.service
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
   Active: active (running) since Wed 2024-03-27 13:29:01 PDT; 2min 36s ago
   Main PID: 3083 (vsftpd)
     Tasks: 1 (limit: 2281)
    CGroup: /system.slice/vsftpd.service
            └─3083 /usr/sbin/vsftpd /etc/vsftpd.conf

Mar 27 13:29:01 slave-1 systemd[1]: Starting vsftpd FTP server...
Mar 27 13:29:01 slave-1 systemd[1]: Started vsftpd FTP server.
lines 1-10/10 (END)
```

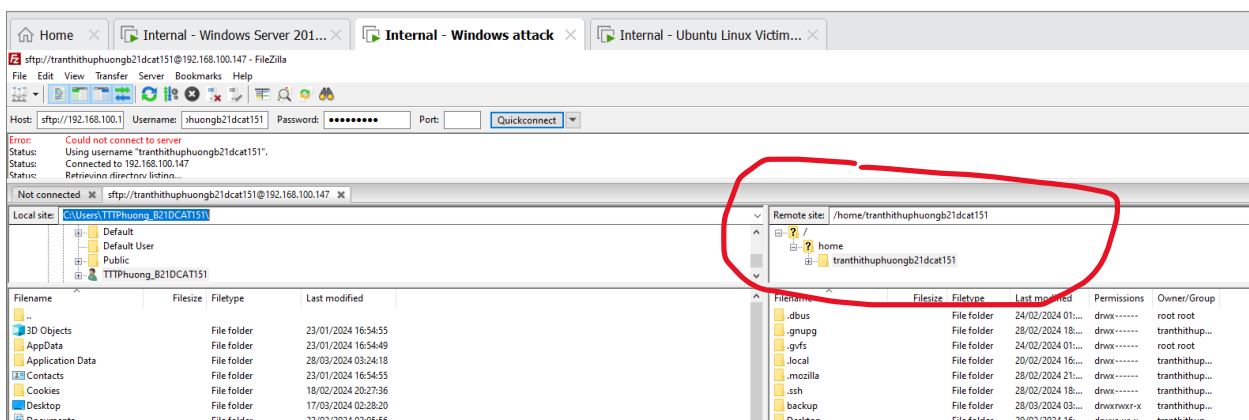
Bật dịch vụ ftp

- 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/tranthithuphuongb21dcat151/backup

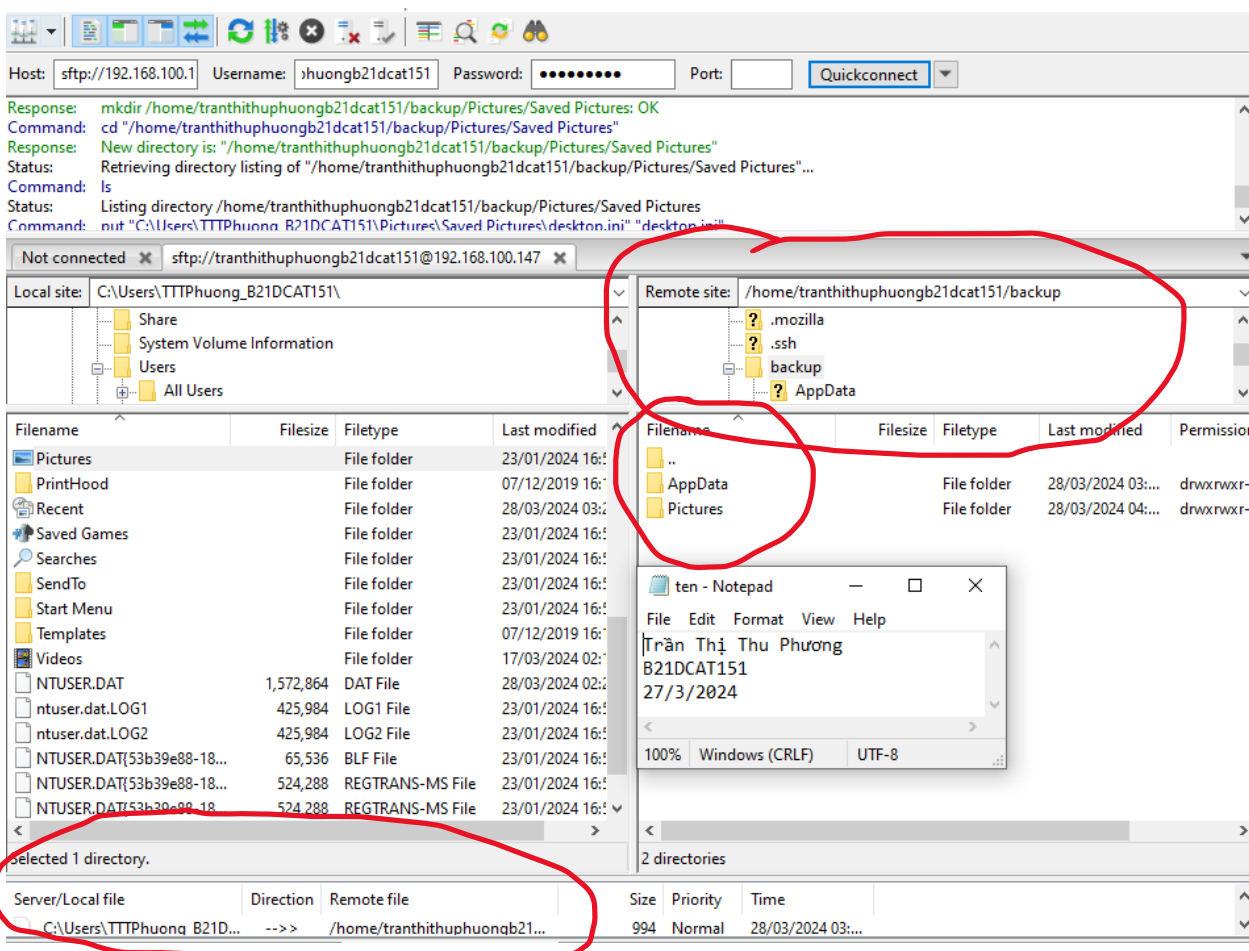


Kết nối đến ftp server

Bài 11: Sao lưu hệ thống



Kết quả sau khi kết nối



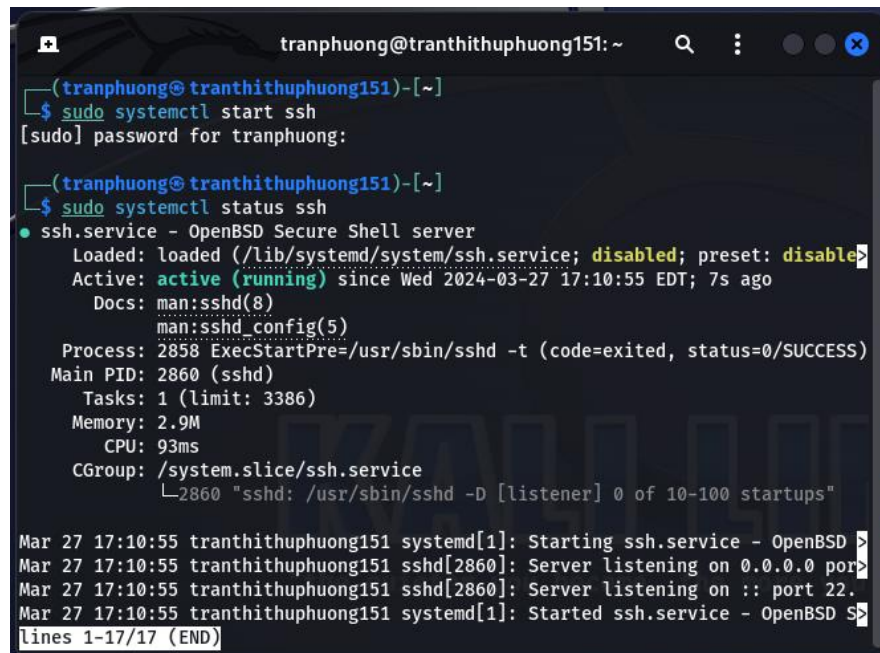
Sao lưu 1 thư mục trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client


```
tranthithuphuongb21dcat151@slave-1:~$ ls
backup  Desktop  Downloads  Pictures  sinhvien  Templates
demo    Documents Music      Public    snap      Videos
tranthithuphuongb21dcat151@slave-1:~$ cd backup
tranthithuphuongb21dcat151@slave-1:~/backup$ ls
AppData  Pictures
tranthithuphuongb21dcat151@slave-1:~/backup$
```

Kiểm tra thư mục backup trong Ubuntu (Minh chứng)

2.2.4. Sao lưu tệp sử dụng SCP

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

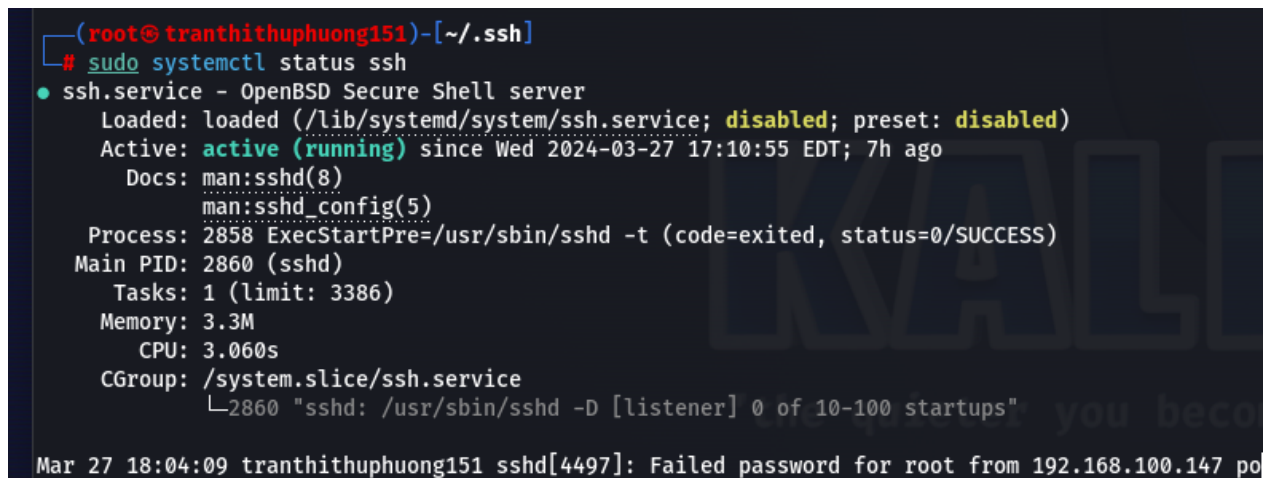


```
tranhphuong@tranthithuphuong151: ~
(tranhphuong@tranthithuphuong151)-[~]
$ sudo systemctl start ssh
[sudo] password for tranphuong:

(tranhphuong@tranthithuphuong151)-[~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Wed 2024-03-27 17:10:55 EDT; 7s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2858 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 2860 (sshd)
      Tasks: 1 (limit: 3386)
     Memory: 2.9M
        CPU: 93ms
    CGroup: /system.slice/ssh.service
            └─2860 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 27 17:10:55 tranthithuphuong151 systemd[1]: Starting ssh.service - OpenBSD
Mar 27 17:10:55 tranthithuphuong151 sshd[2860]: Server listening on 0.0.0.0 por
Mar 27 17:10:55 tranthithuphuong151 sshd[2860]: Server listening on :: port 22.
Mar 27 17:10:55 tranthithuphuong151 systemd[1]: Started ssh.service - OpenBSD S
lines 1-17/17 (END)
```

Kiểm tra dịch vụ ssh đã bật hay chưa

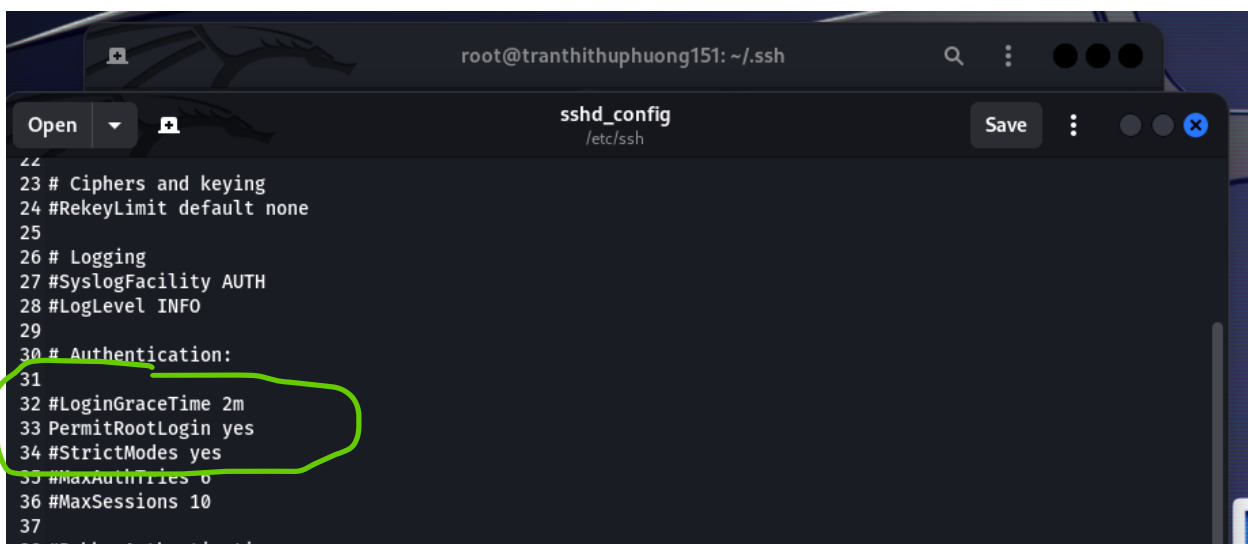


```
(root@tranthithuphuong151)-[~/ssh]
# sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Wed 2024-03-27 17:10:55 EDT; 7h ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2858 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 2860 (sshd)
      Tasks: 1 (limit: 3386)
     Memory: 3.3M
        CPU: 3.060s
    CGroup: /system.slice/ssh.service
            └─2860 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 27 18:04:09 tranthithuphuong151 sshd[4497]: Failed password for root from 192.168.100.147 po
```

Bật dịch vụ ssh

Bài 11: Sao lưu hệ thống



```
root@tranthithuphuong151: ~/.ssh
sshd_config
/etc/ssh
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
```

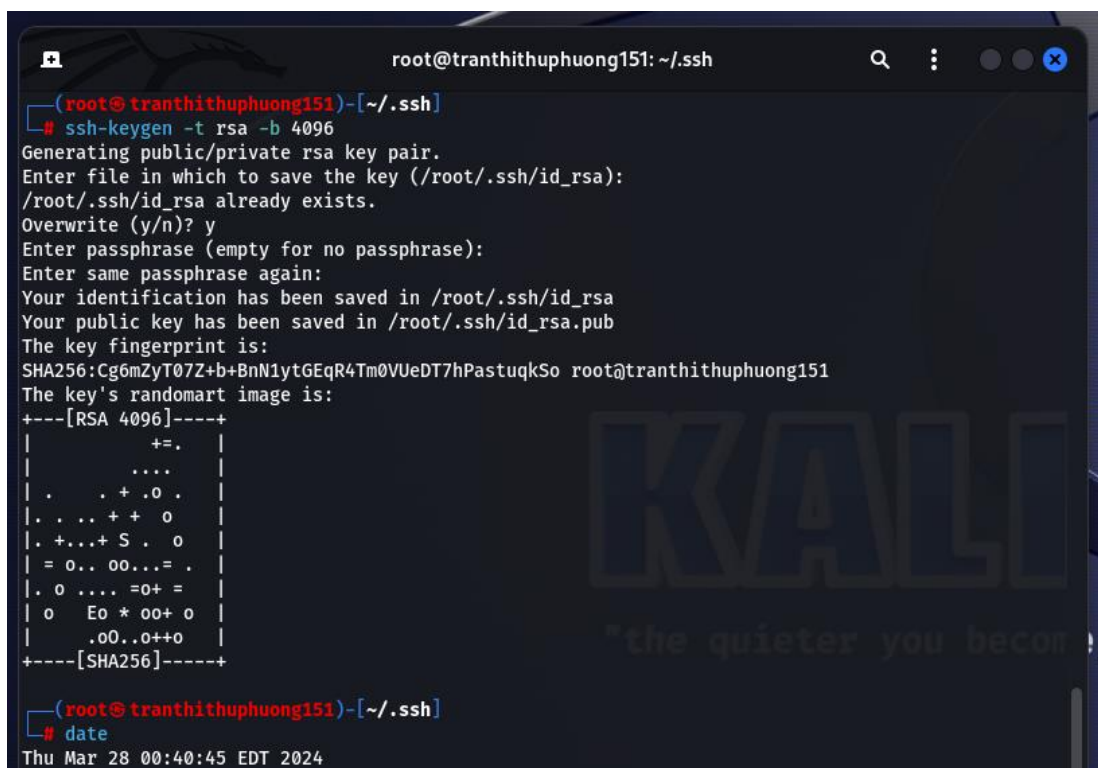
Cấu hình ssh cho phép truy cập vào tài khoản root trên Kali



```
(root@tranthithuphuong151)~[~/.ssh]
# sudo service ssh restart
```

Khởi động lại dịch vụ ssh

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



```
root@tranthithuphuong151: ~/.ssh
(root@tranthithuphuong151)~[~/.ssh]
# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
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:Cg6mZyT07Z+b+BnN1ytGEqR4Tm0VUeDT7hPastuqkSo root@tranthithuphuong151
The key's randomart image is:
+---[RSA 4096]-----+
|          +=.      |
|          ....     |
| . . . . + .0 .    |
| | . . . . + + 0   |
| | . + . . + S . 0 |
| | = 0 . . 00 . . = |
| | . 0 . . . . =0+ = |
| | 0  Eo * 00+ 0   |
| | .00 . .0+ +0   |
+---[SHA256]-----+
(root@tranthithuphuong151)~[~/.ssh]
# date
Thu Mar 28 00:40:45 EDT 2024
```

Tạo Secure Shell Keys trên máy Kali Linux

Bài 11: Sao lưu hệ thống

- 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

```
tranthithuphuongb21dcat151@slave-1: ~  
File Edit View Search Terminal Help  
tranthithuphuongb21dcat151@slave-1:~$ touch TranThiThuPhuong_B21DCAT151.txt  
tranthithuphuongb21dcat151@slave-1:~$ ls  
backup  Documents  Music      sinhvien  TranThiThuPhuong_B21DCAT151.txt  
demo    Downloads  Pictures  snap      Videos  
Desktop file1.txt  Public    Templates  
tranthithuphuongb21dcat151@slave-1:~$ date  
Wed Mar 27 21:57:49 PDT 2024  
tranthithuphuongb21dcat151@slave-1:~$ scp TranThiThuPhuong_B21DCAT151.txt root@192.168.100.3:  
/root/  
root@192.168.100.3's password:  
TranThiThuPhuong_B21DCAT151.txt          100%  0    0.0KB/s   00:00  
tranthithuphuongb21dcat151@slave-1:~$
```

Sao lưu file vào thư mục root

```
tranthithuphuongb21dcat151@slave-1:~$ ls  
backup  Desktop  Downloads  Music      Public  snap      TranThiThuPhuong_B21DCAT151.txt  
demo    Documents file1.txt  Pictures  sinhvien Templates Videos  
tranthithuphuongb21dcat151@slave-1:~$ scp -r /backup root@192.168.100.3:/root/  
root@192.168.100.3's password:  
/backup: No such file or directory  
tranthithuphuongb21dcat151@slave-1:~$ scp -r ./backup root@192.168.100.3:/root/  
root@192.168.100.3's password:  
IconCache.db                100% 34KB 930.8KB/s   00:00  
results.xml                 100% 48KB  7.8MB/s   00:00  
NetworkDiagnostics.debugreport.xml 100% 6092 2.0MB/s   00:00  
ResultReport.xml           100% 37KB 10.2MB/s   00:00  
results.xml                100% 388 135.3KB/s   00:00  
latest.cab                 100% 12KB  4.0MB/s   00:00  
Connected Devices Platform certificates.sst 100% 654 281.7KB/s   00:00  
L.TTTPhuong_B21DCAT151.cdpresource 100% 54 18.7KB/s   00:00  
ActivitiesCache.db         100% 1024KB 20.7MB/s   00:00
```

Sao lưu thư mục backup vào thư mục root trên máy Kali

```
(root@tranthithuphuong151)~  
# ls  
TranThiThuPhuong_B21DCAT151.txt  backup  
  
(root@tranthithuphuong151)~  
# cd backup  
  
(root@tranthithuphuong151)~/backup  
# ls  
AppData  Pictures  
  
(root@tranthithuphuong151)~/backup  
# date  
Thu Mar 28 01:11:41 EDT 2024  
  
(root@tranthithuphuong151)~/backup  
# echo "Tran Thi Thu Phuong - B21DCAT151"  
Tran Thi Thu Phuong - B21DCAT151
```

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>