HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

BÀI THỰC HÀNH 10

THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 3/2022

Bài 10: Sao lưu hệ thống

1.1 Mục đích

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

1. Sao lưu tới ổ đĩa mạng
2. Sao lưu tệp lên FTP server
3. Sao lưu tệp sử dụng SCP

1.2 Nội dung thực hành

1.2.1 Tìm hiểu lý thuyết

- ✓ SCP – Secure copy (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.
- ✓ FTP - Giao thức truyền tệp hay FTP cho phép người dùng truyền tệp từ máy này sang máy khác từ xa. Hạn chế của việc sử dụng FTP là dữ liệu được gửi dưới dạng văn bản không được mã hóa.
- ✓ oỔ đĩa mạng - Ổ đĩa mạng là bộ nhớ trên máy tính khác được gán ký tự ổ đĩa. 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.
- ✓ Net use - Lệnh net use có thể được sử dụng để ánh xạ các ổ đĩa của hệ thống từ xa.
- ✓ Net view - Lệnh net view sẽ hiển thị danh sách các mạng chia sẻ của hệ thống.

1.2.2 Chuẩn bị môi trường

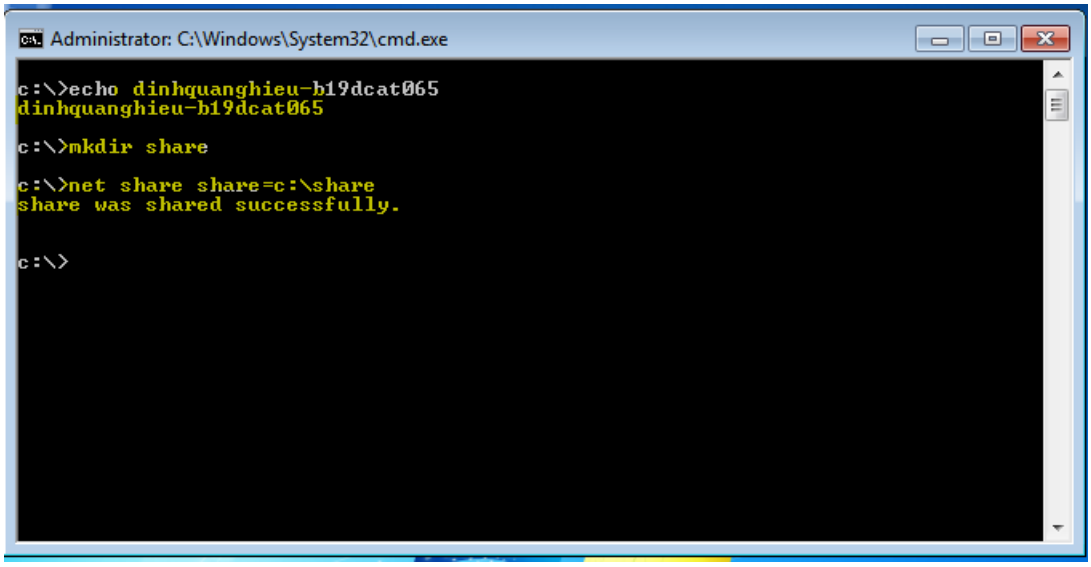
- ✓ Phần mềm VMWare Workstation.
- ✓ Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 05 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
- ✓ Topo mạng như đã cấu hình trong bài 5. Trong bài này chỉ sử dụng các máy trong mạng Internal cho việc sao lưu

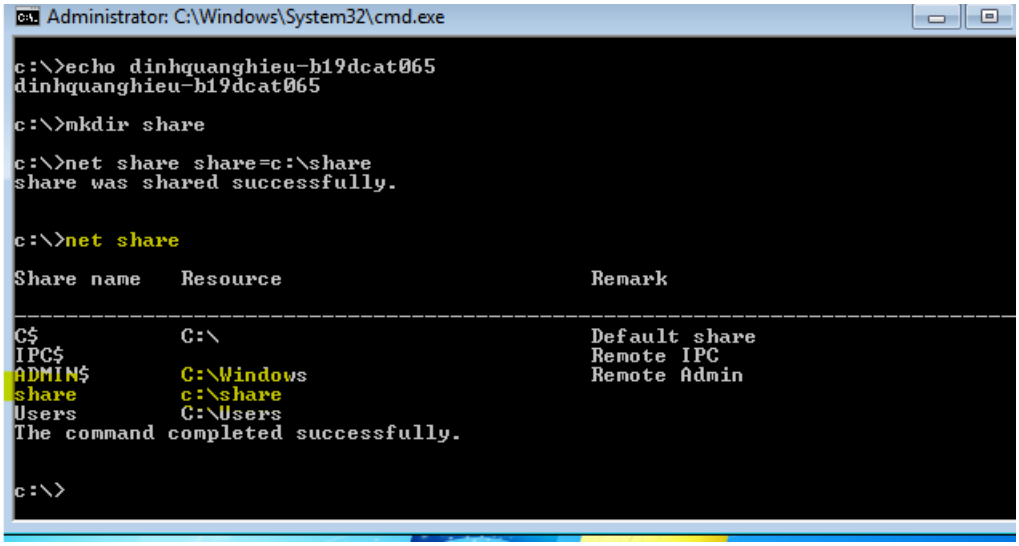
1.2.3 Các bước thực hiện và kết quả cần đạt

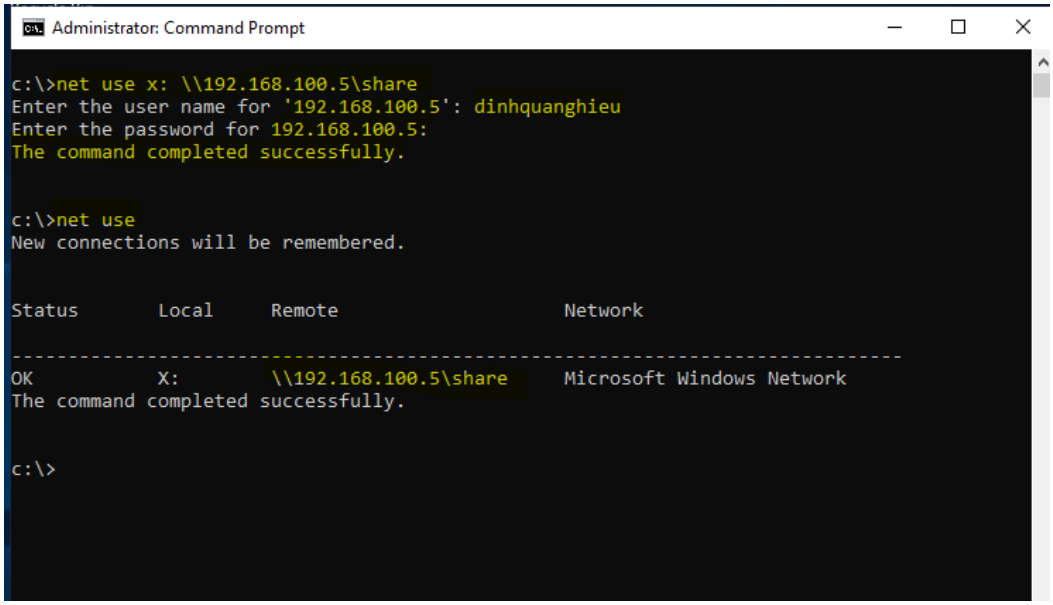
1.2.3.1 Sao lưu tới ổ đĩa mạng

a) Các bước thực hiện

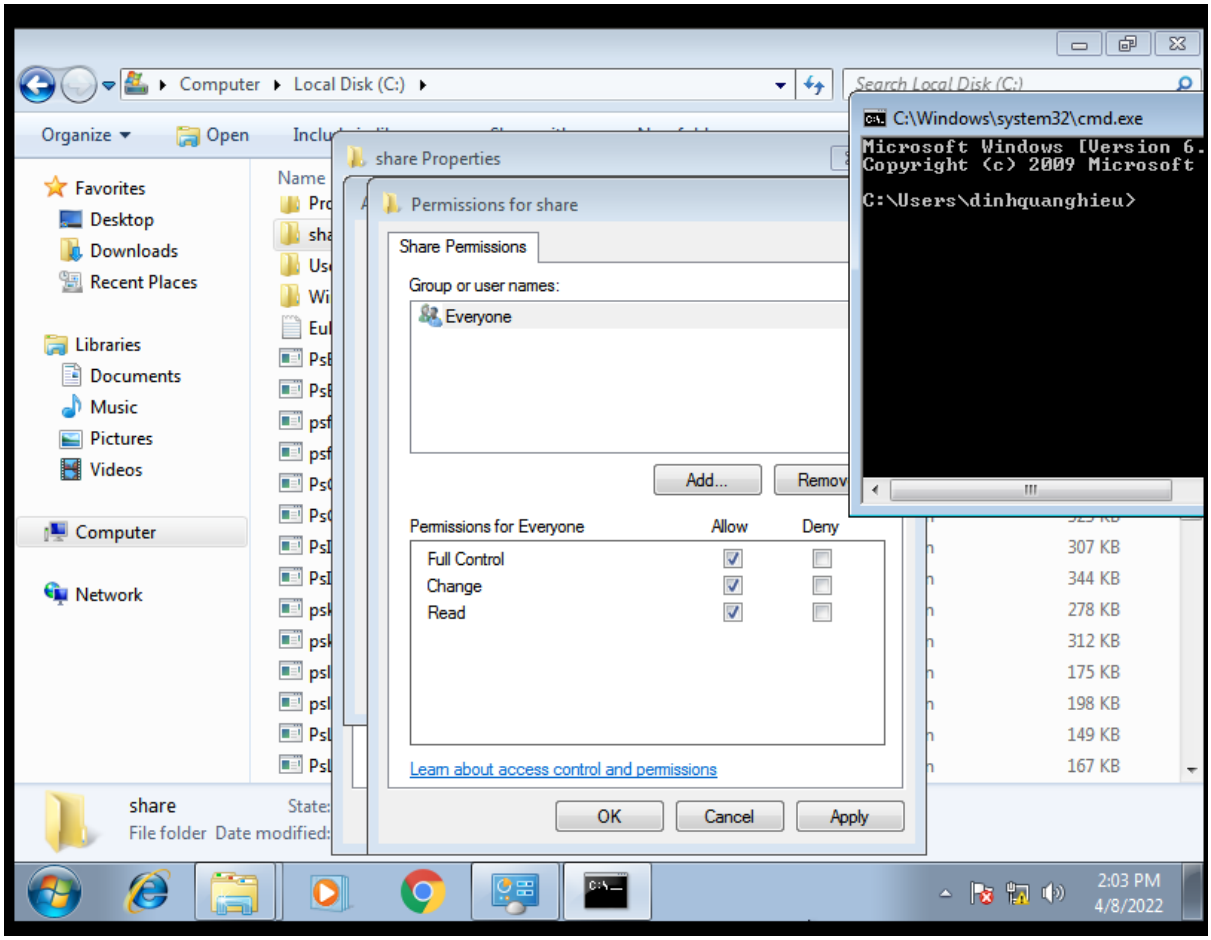
- ➢ Trên máy trạm Windows attack trong mạng Internal, tạo thư mục share rồi chia sẻ qua mạng (C:\net share share=c:\share)

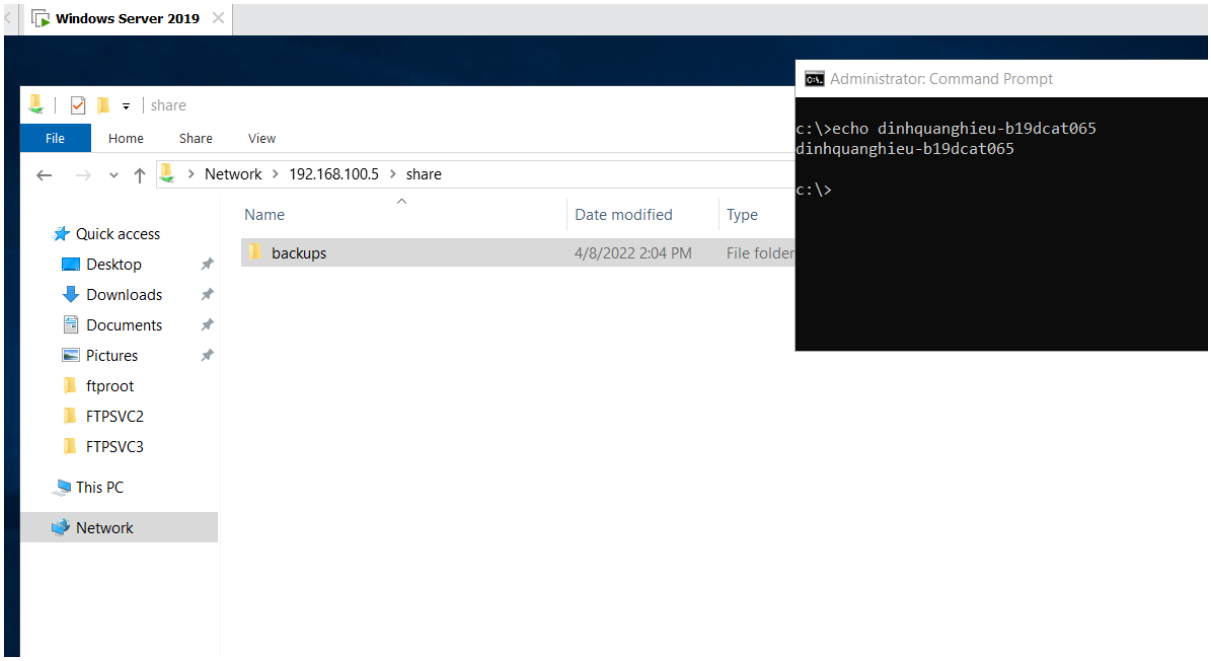

Administrator: C:\Windows\System32\cmd.exe
c:\>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
c:\>mkdir share
c:\>net share share=c:\share
share was shared successfully.
c:\>


Administrator: C:\Windows\System32\cmd.exe
c:\>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
c:\>mkdir share
c:\>net share share=c:\share
share was shared successfully.
c:\>net share
Share name Resource Remark
C$ C:\ Default share
IPC$ Remote IPC
ADMIN$ C:\Windows Remote Admin
share c:\share
Users C:\Users
The command completed successfully.
c:\>

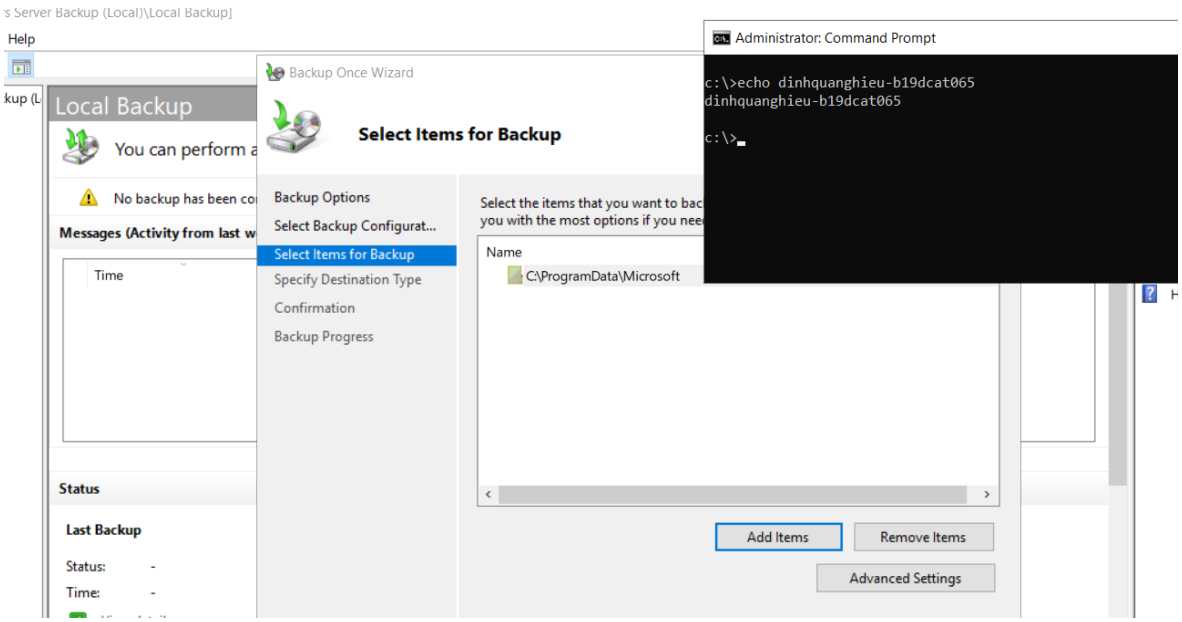

Administrator: Command Prompt
c:\>net use x: \\192.168.100.5\share
Enter the user name for '192.168.100.5': dinhquanghieu
Enter the password for 192.168.100.5:
The command completed successfully.
c:\>net use
New connections will be remembered.
Status Local Remote Network
OK X: \\192.168.100.5\share Microsoft Windows Network
The command completed successfully.
c:\>

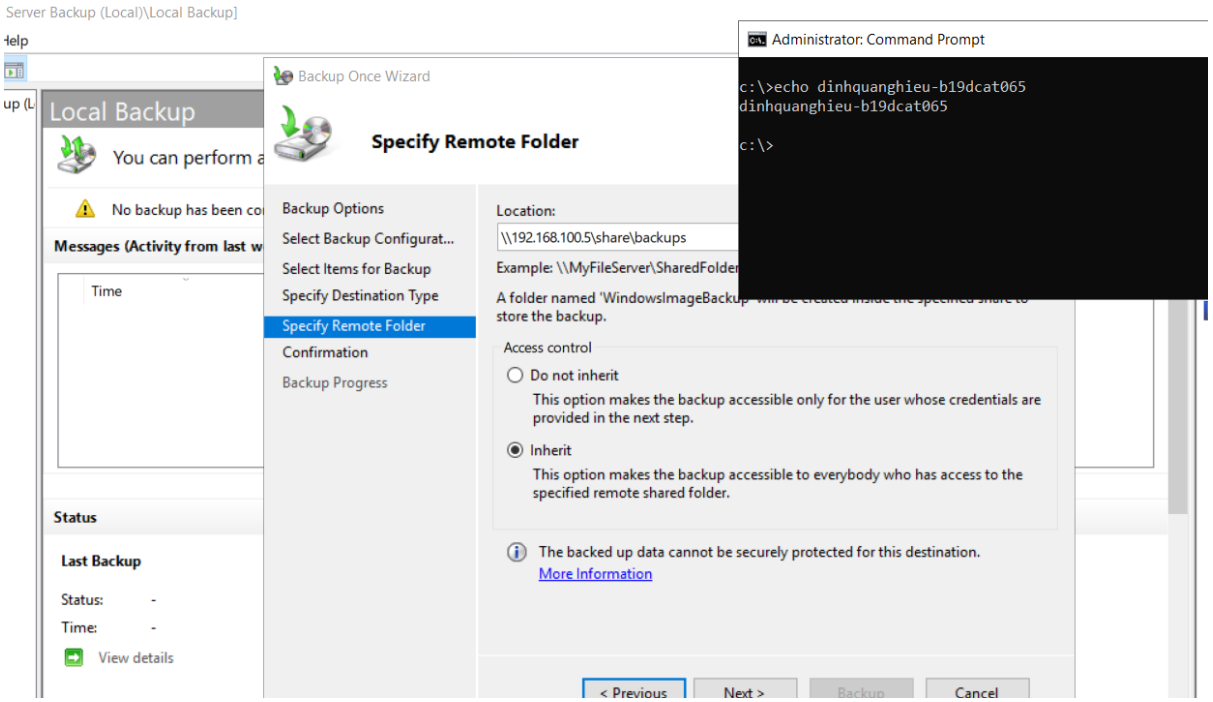
- Trên máy Windows attack trong mạng Internal, cấu hình thư mục ở đĩa mạng cho phép sao lưu tệp và thư mục từ máy khác nếu không tạo được thư mục trên máy Windows server

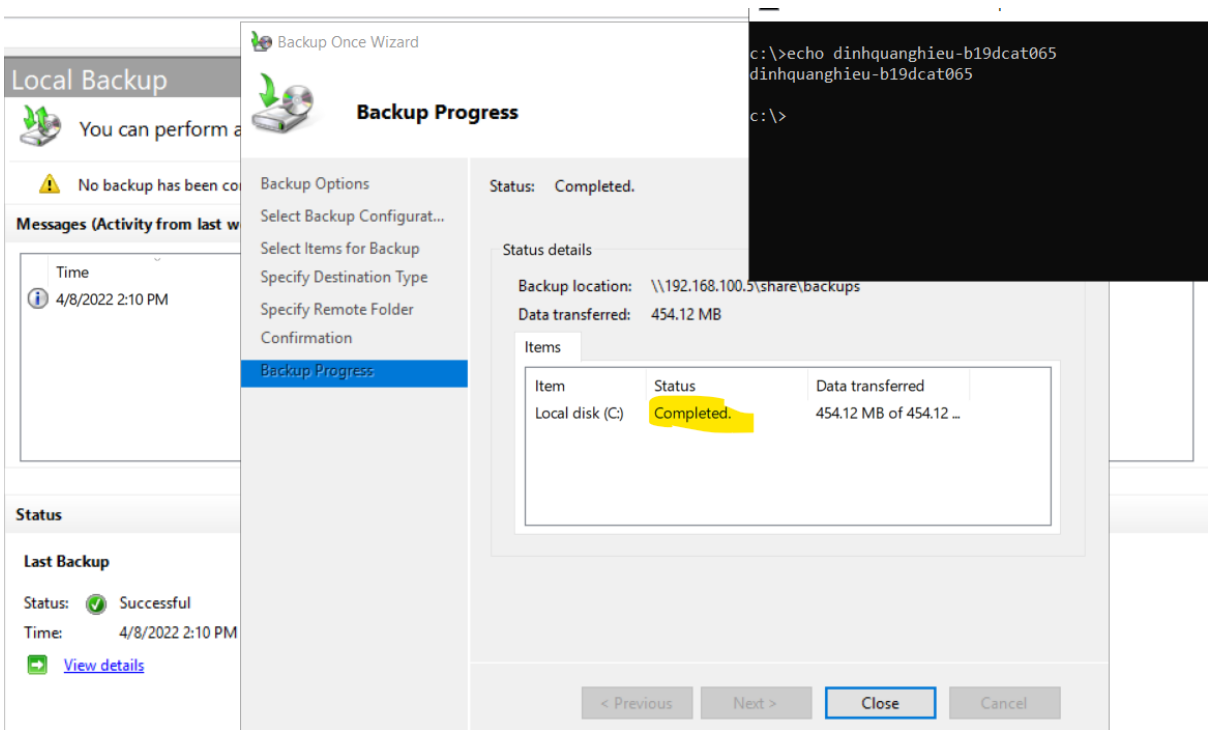


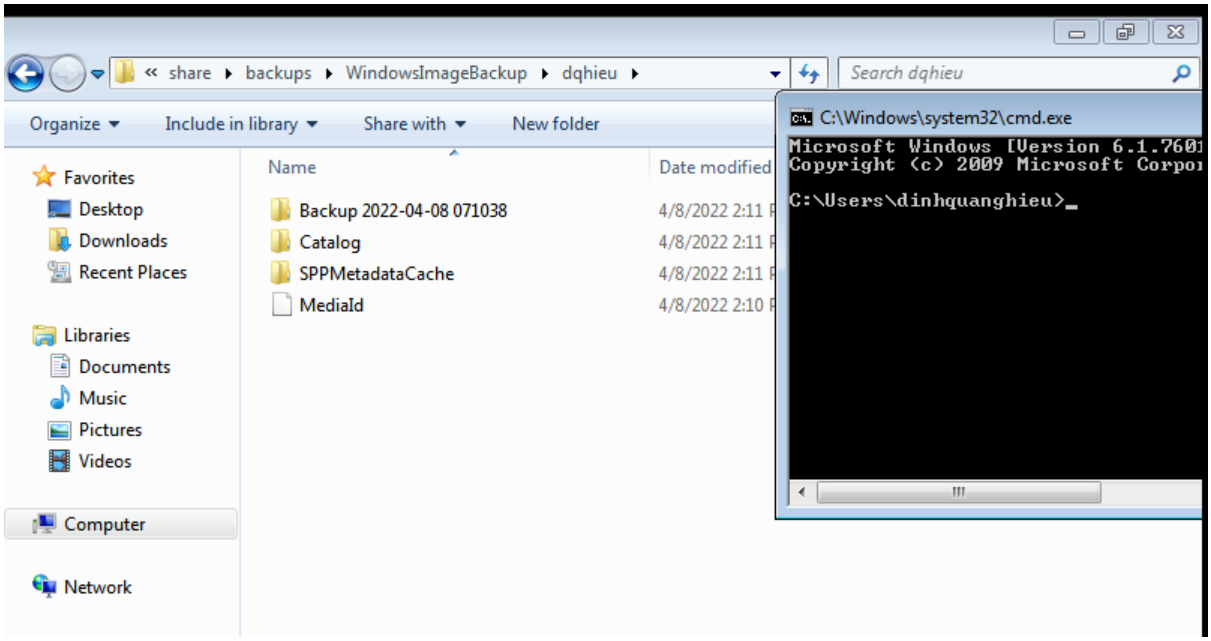


- Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2003, nếu sử dụng Win khác thì có thể download ntbackup để sử dụng), sau đó chọn 1 thư mục để sao lưu và đích là thư mục ổ mạng đã chia sẻ trên máy Windows attack trong mạng Internal
- Vào Server Manager -> Tools -> Windows Server Backup -> Chuột phải Local Backups -> Backup Once
- Ở cửa sổ Backup Once Wizard: Different options -> Custom -> Chọn file muốn backups -> Chọn kiểu file muốn backups đến -> Chọn đường dẫn file để backups -> Backup




Server Backup (Local)\Local Backup]
Help
Local Backup
You can perform a
No backup has been co
Messages (Activity from last w
Time
Status
Last Backup
Status:
Time:
View details
Backup Once Wizard
Specify Remote Folder
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Specify Remote Folder
Confirmation
Backup Progress
Location:
\\192.168.100.5\share\backups
Example: \\MyFileServer\SharedFolder
A folder named 'WindowsImageBackup
store the backup.
Access control
Do not inherit
This option makes the backup accessible only for the user whose credentials are provided in the next step.
Inherit
This option makes the backup accessible to everybody who has access to the specified remote shared folder.
The backed up data cannot be securely protected for this destination.
More Information
< Previous
Next >
Backup
Cancel
Administrator: Command Prompt
c:\>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
c:\>


Local Backup
You can perform a
No backup has been co
Messages (Activity from last w
Time
4/8/2022 2:10 PM
Status
Last Backup
Status: Successful
Time: 4/8/2022 2:10 PM
View details
Backup Once Wizard
Backup Progress
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Specify Remote Folder
Confirmation
Backup Progress
Status: Completed.
Status details
Backup location: \\192.168.100.5\share\backups
Data transferred: 454.12 MB
Items
Item
Status
Data transferred
Local disk (C:)
Completed.
454.12 MB of 454.12 ...
< Previous
Next >
Close
Cancel
c:\>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
c:\>



b) Kết quả cần đạt được

Minh chứng:

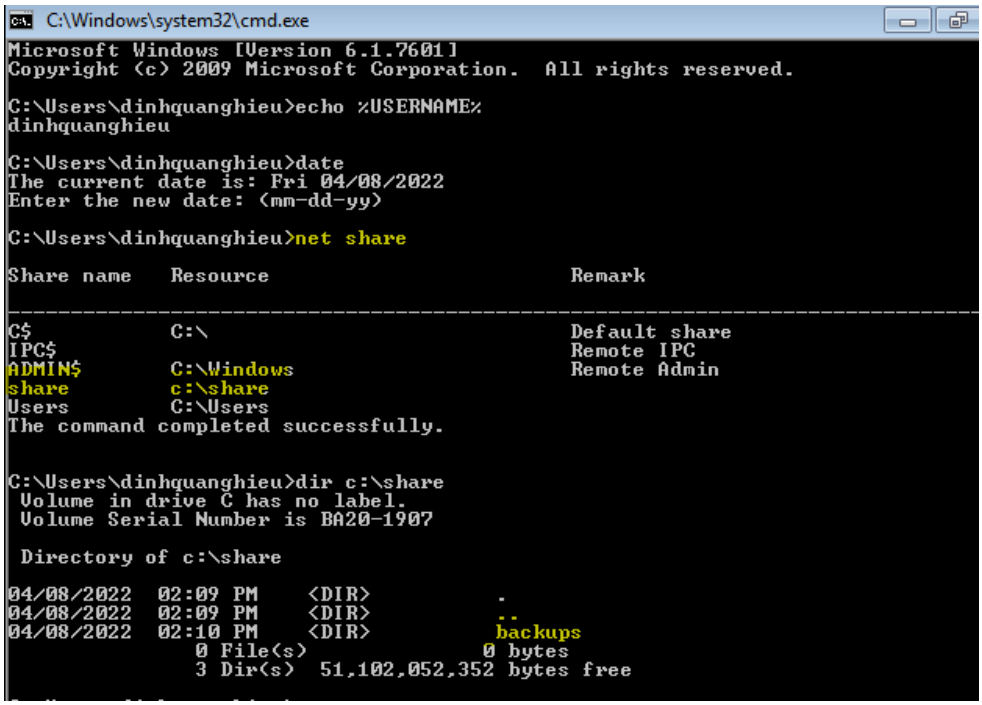
- Chụp ảnh minh chứng màn hình với các lệnh trong cmd trong máy Windows attack:

    + echo %USERNAME%

    + date

    +net share

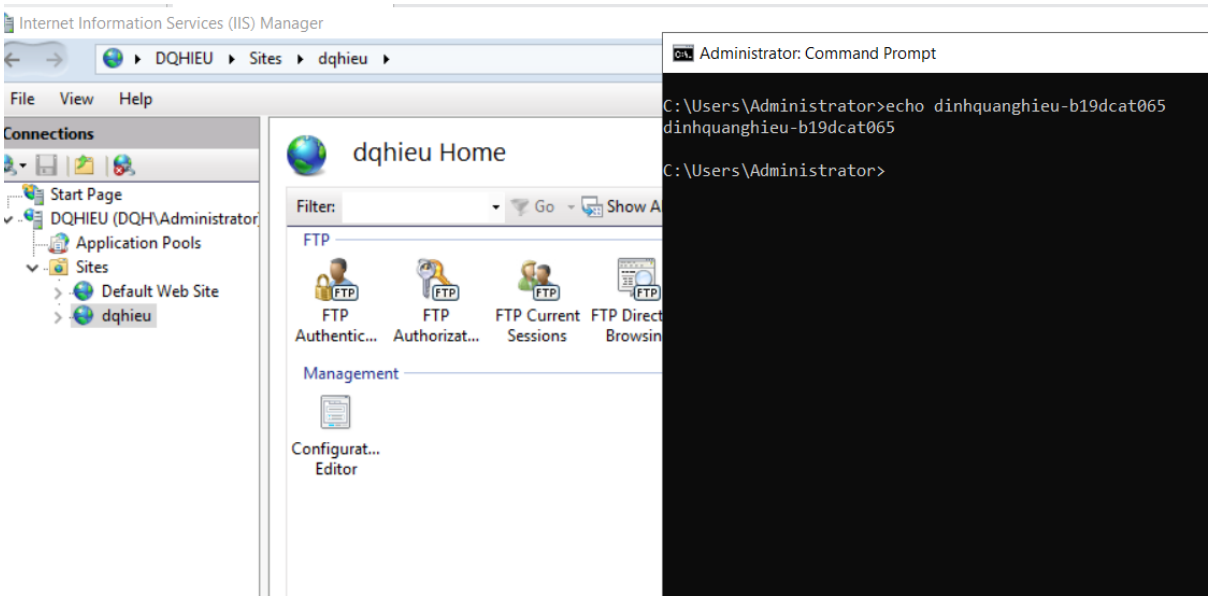
    + dir c:\share



1.2.3.2 Sao lưu tệp lên FTP server

a) Các bước thực hiện

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



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

```
dinhquanghieu-b19dcat065@ubuntu:~$ sudo apt-get install vsftpd
[sudo] password for dinhquanghieu-b19dcat065:
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 0 not upgraded.
Need to get 115 kB of archives.
After this operation, 336 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 vsftpd amd64 3.0.3-3
ubuntu2 [115 kB]
Fetched 115 kB in 1s (74.5 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 222718 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-3ubuntu2_amd64.deb ...
Unpacking vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for systemd (229-4ubuntu21.31) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up vsftpd (3.0.3-3ubuntu2) ...
```

```
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw allow 20:21/tcp
Rules updated
Rules updated (v6)
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw allow 990/tcp
Rules updated
Rules updated (v6)
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw allow 35000:40000/tcp
Rules updated
Rules updated (v6)
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw allow 22
Rules updated
Rules updated (v6)
dinhquanghieu-b19dcat065@ubuntu:~$
```

dinhquanghieu-b19dcat065@ubuntu: ~

```
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw reload
Firewall reloaded
dinhquanghieu-b19dcat065@ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
20:21/tcp                  ALLOW       Anywhere
990/tcp                    ALLOW       Anywhere
35000:40000/tcp            ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
22                         ALLOW       Anywhere
20:21/tcp (v6)             ALLOW       Anywhere (v6)
990/tcp (v6)               ALLOW       Anywhere (v6)
35000:40000/tcp (v6)       ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)

dinhquanghieu-b19dcat065@ubuntu:~$
```

```
dinhquanghieu-b19dcat065@ubuntu: ~
  GNU nano 2.5.3              File: /etc/vsftpd.conf                    Modified

#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
write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

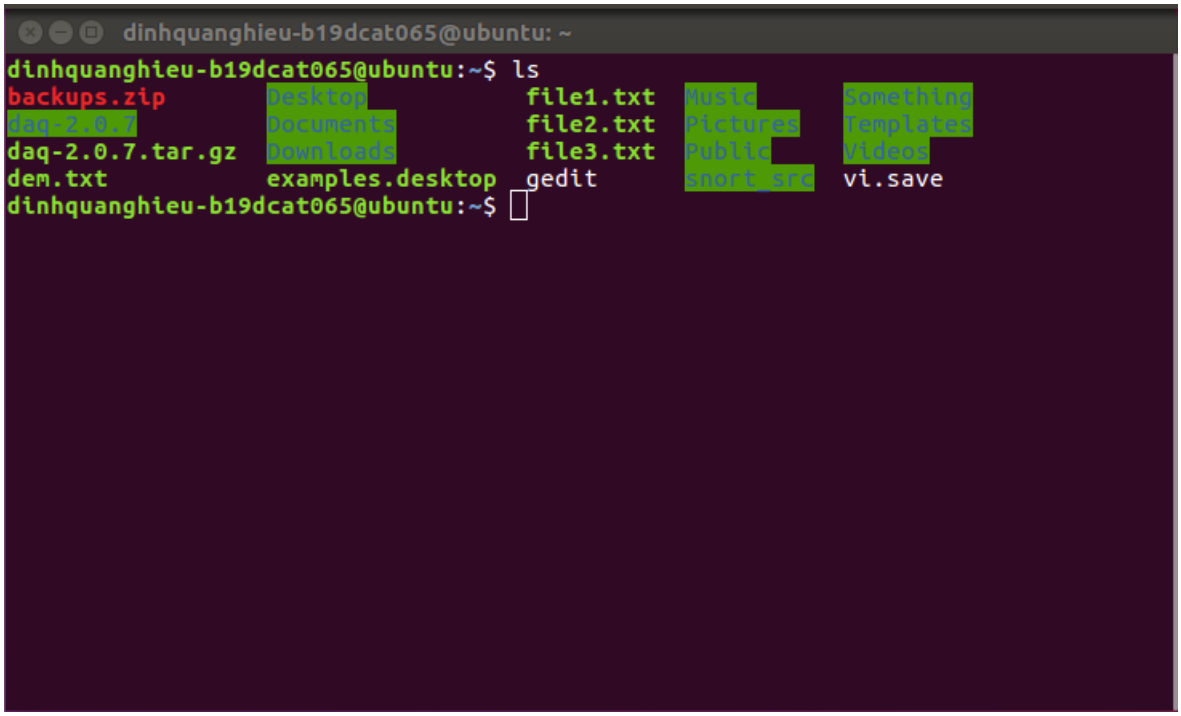
- Sao lưu 1 thư mục trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client, sau khi kết nối tới ftp server

```
C:\Users\Administrator\Desktop>ftp 192.168.100.147
Connected to 192.168.100.147.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
User (192.168.100.147:(none)): dinhquanghieu-b19dcat065
331 Please specify the password.
Password:
230 Login successful.
ftp> put backups.zip
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 331869916 bytes sent in 5.28Seconds 62842.25Kbytes/sec.
ftp>
```

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065

C:\Users\Administrator>
```



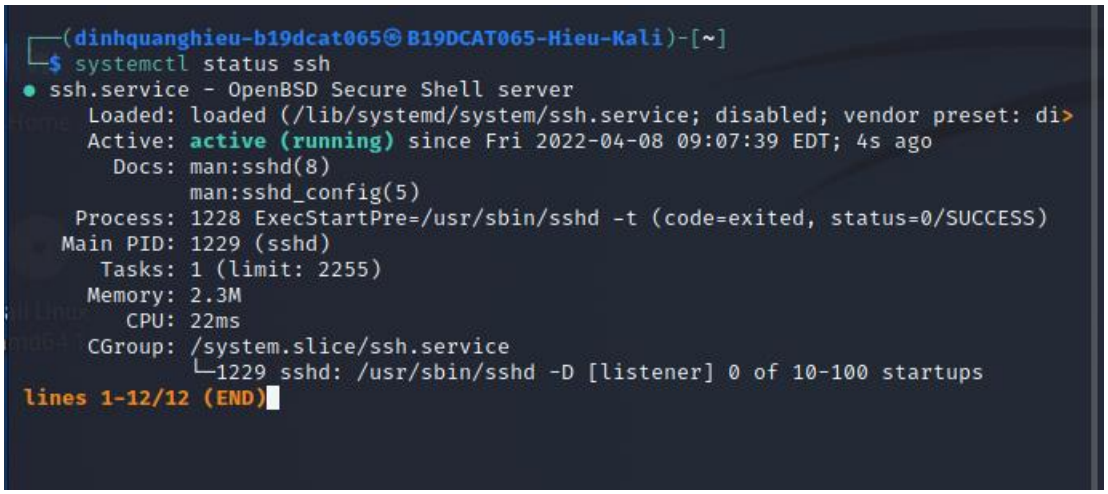
b) Kết quả cần đạt được

Cài đặt và sao lưu thành công. Tên người dùng phải là “tên sinh viên_mã sinh viên”. Thực hiện viết báo cáo cho bài thực hành theo các bước đã mô tả bên trên.

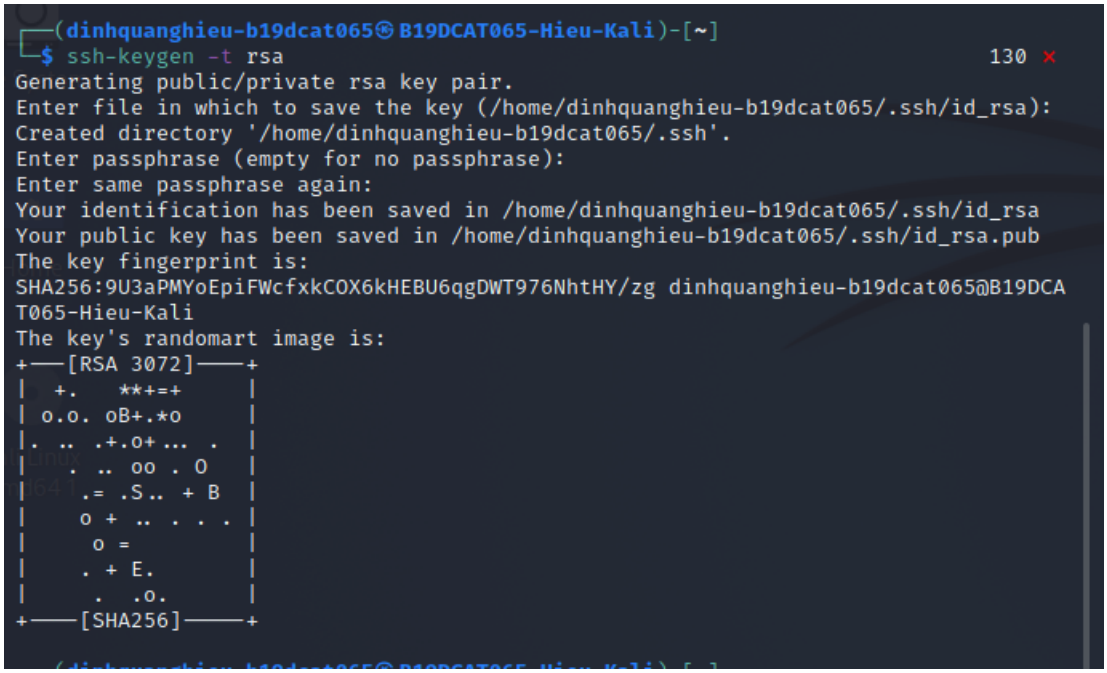
1.2.3.3 Sao lưu tệp sử dụng SCP

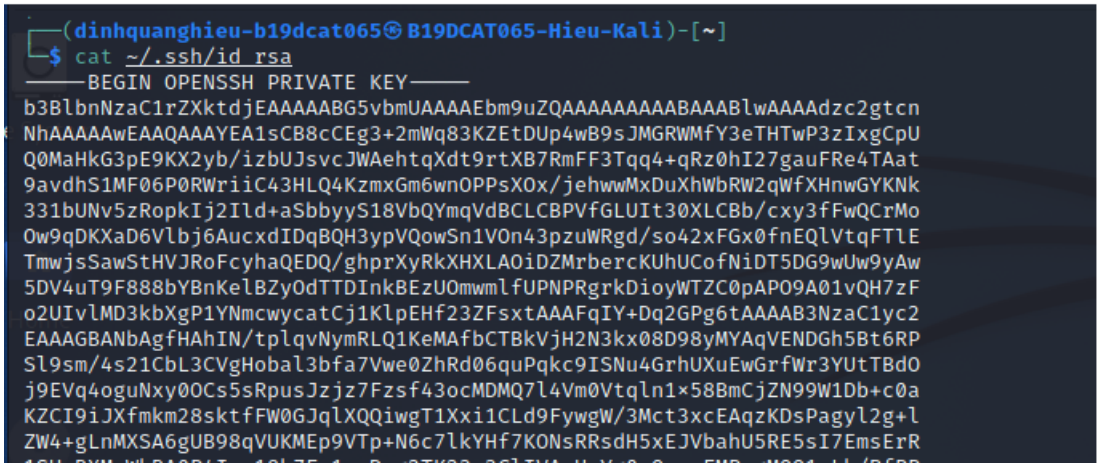
a) Thực hiện cấu hình

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

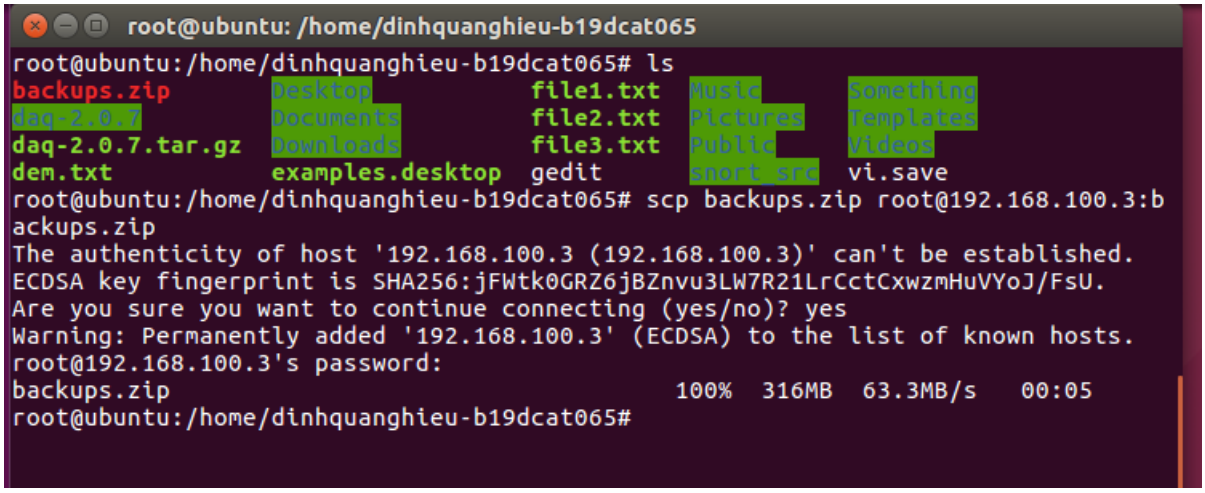


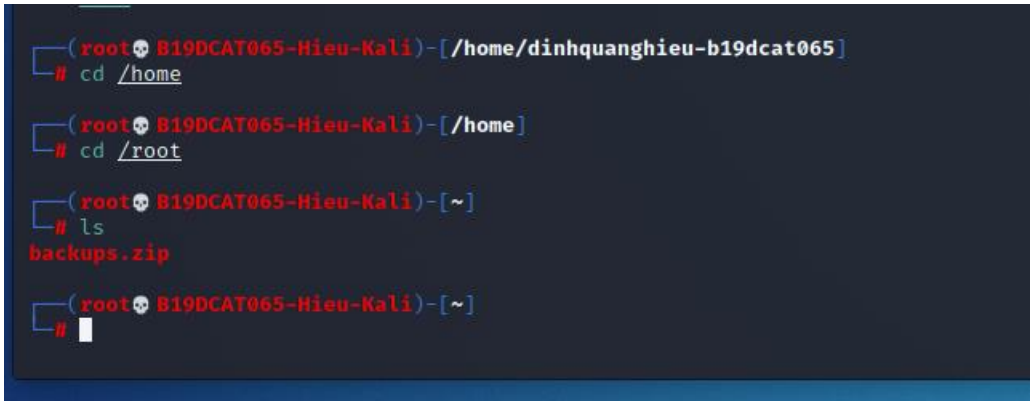
- Tiếp tục, tạo Secure Shell Keys trên máy Kali Linux đó





- 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





b) Kết quả cần đạt được

Sao lưu thành công. Tên người dùng phải đặt là “tên sinh viên_mã sinh viên” . Thực hiện viết báo cáo cho bài thực hành theo các bước đã mô tả bên trên.