

Báo cáo bài thực hành số 10

Môn học

Thực tập cơ sở

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

Mã SV: B19DCAT141

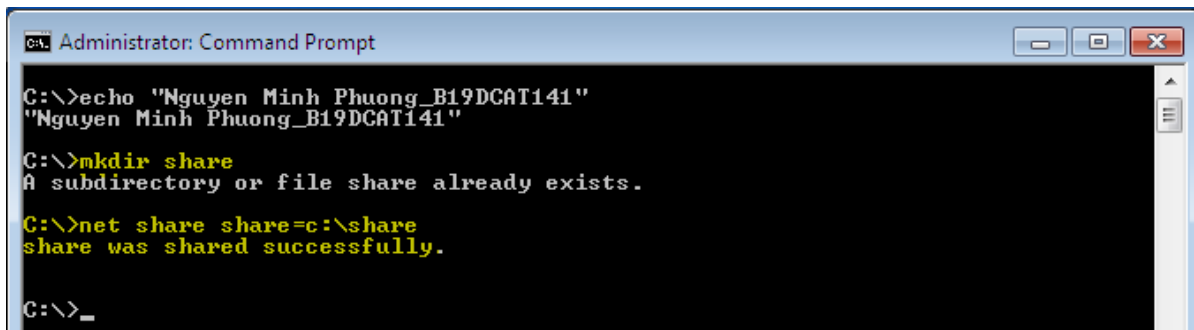
I. Lý thuyết:

- 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.
- Ổ 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 được 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.

II. Thực hành:

1. 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)



```
Administrator: Command Prompt
C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"
C:\>mkdir share
A subdirectory or file share already exists.
C:\>net share share=c:\share
share was shared successfully.
C:\>_
```

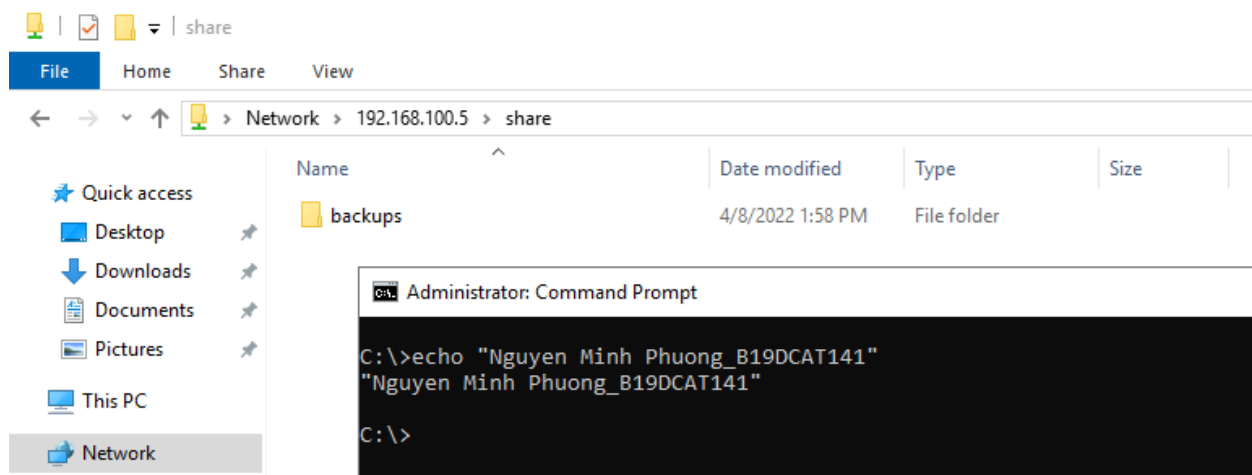
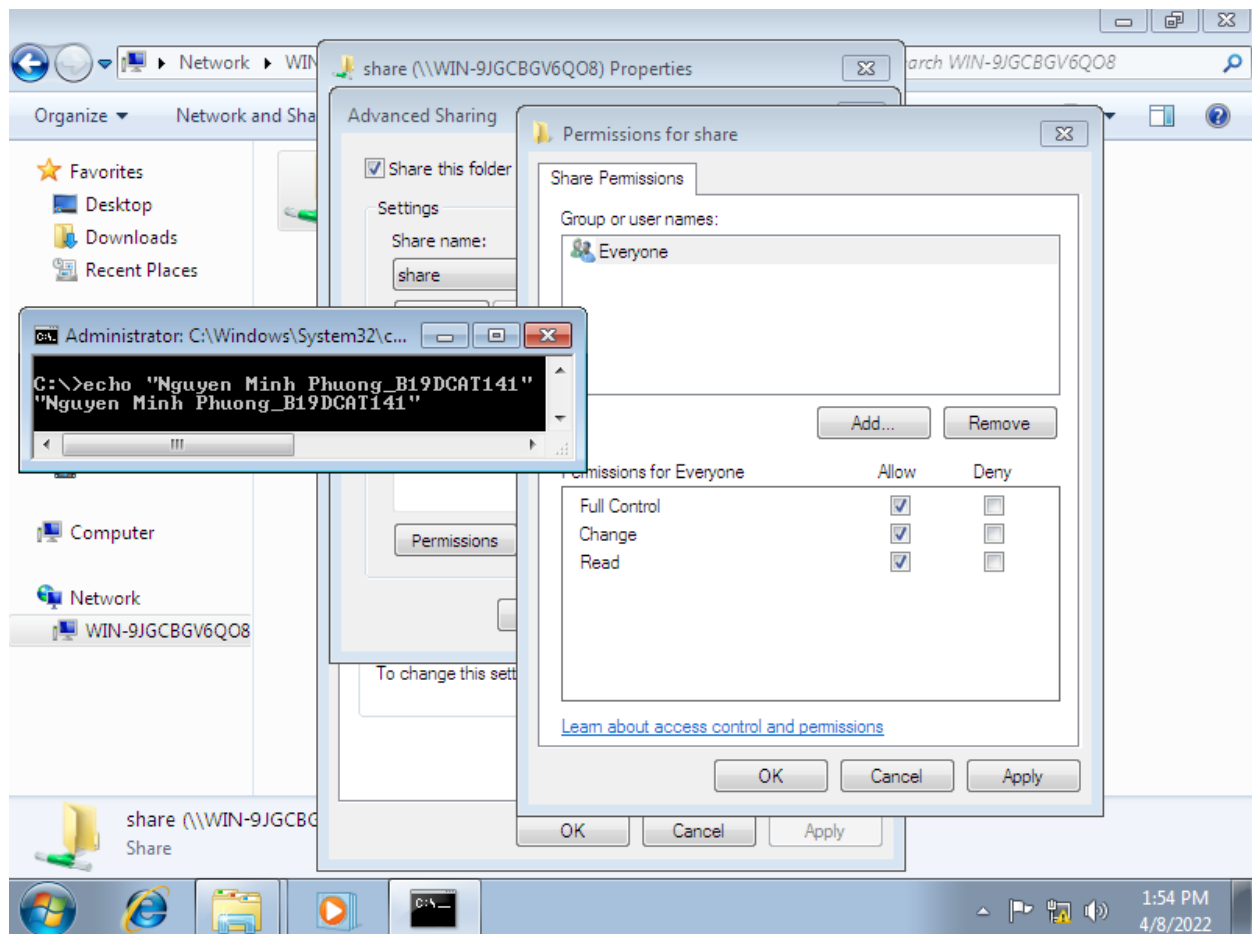
```
Administrator: Command Prompt
C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"
C:\>net share
Share name      Resource          Remark
-----
C$              G:\              Default share
IPC$            C:\Windows       Remote IPC
ADMIN$          C:\share         Remote Admin
share           c:\share
The command completed successfully.
```

```
Administrator: Command Prompt
C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"
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:\>_
```

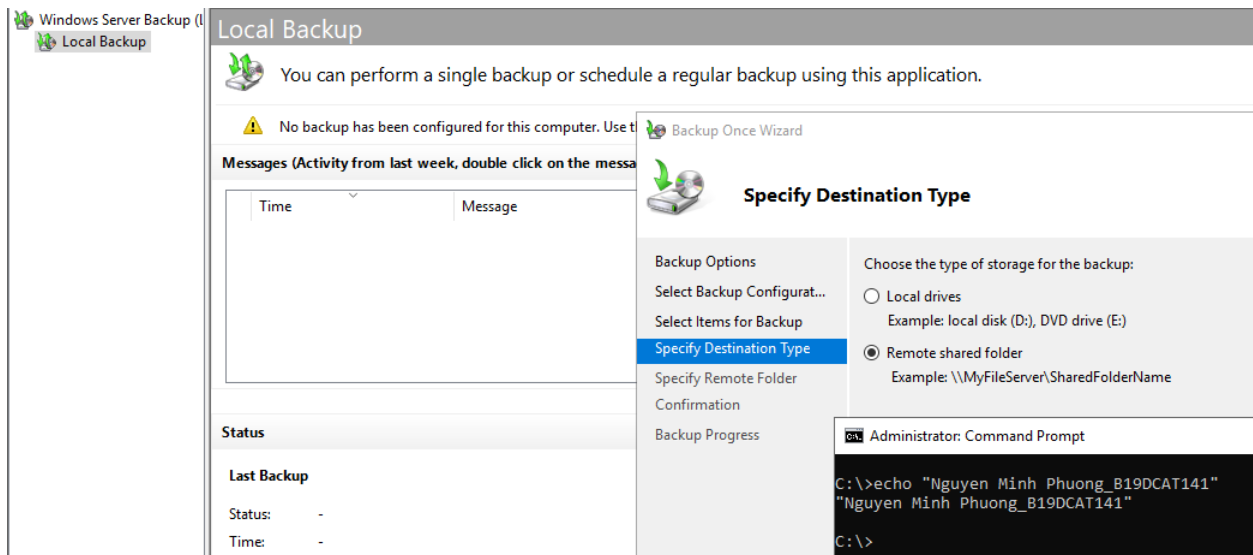
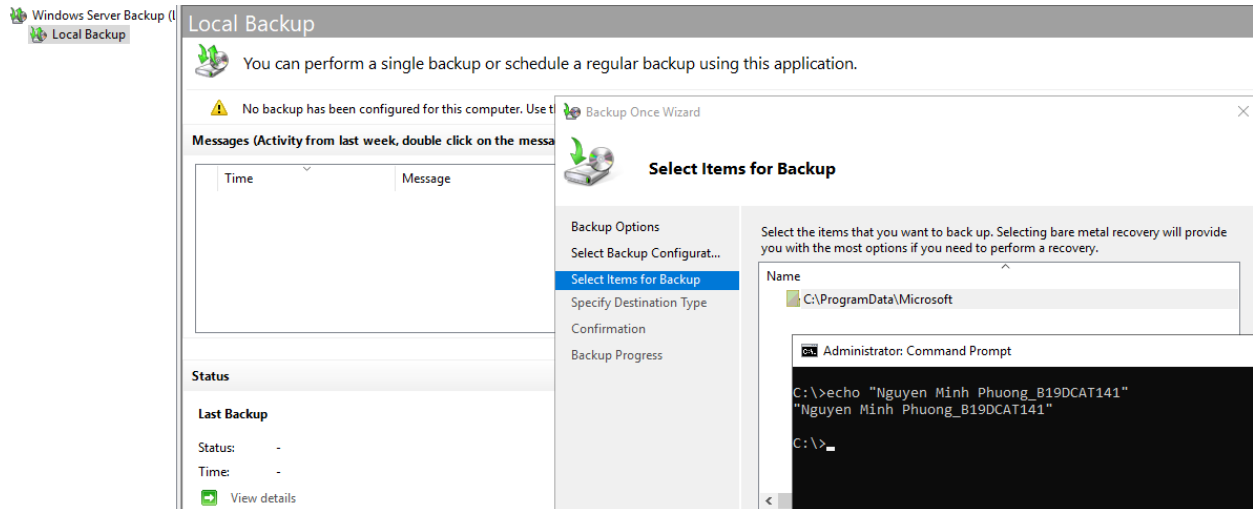
- Trên máy Windows attack trong mạng Internal, cấu hình thư mục ổ đĩa mạng cho phép sao lưu tệp và thư mục từ máy khác nếu không tạo được thư mục trên máy Windows server



- 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



Windows Server Backup (L)
Local Backup

Local Backup

You can perform a single backup or schedule a regular backup using this application.

No backup has been configured for this computer. Use the Backup Once Wizard

Messages (Activity from last week, double click on the message)

Time	Message

Status

Last Backup

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\SharedFolderName

Administrator: Command Prompt

```
C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"
C:\>
```

Windows Server Backup (L)
Local Backup

Local Backup

You can perform a single backup or schedule a regular backup using this application.

No backup has been configured for this computer. Use the Backup Once Wizard

Messages (Activity from last week, double click on the message)

Time	Message
4/8/2022 2:10 PM	Backup

Status

Last Backup

Status: ✔ Successful

Time: 4/8/2022 2:10 PM

[View details](#)

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: 447.45 MB

Item	Status	Data transferred
Local disk (C:)	Completed.	447.45 MB of 447.45...

Administrator: Command Prompt

```
C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"
C:\>
```

WIN-A2EVBIJU5T

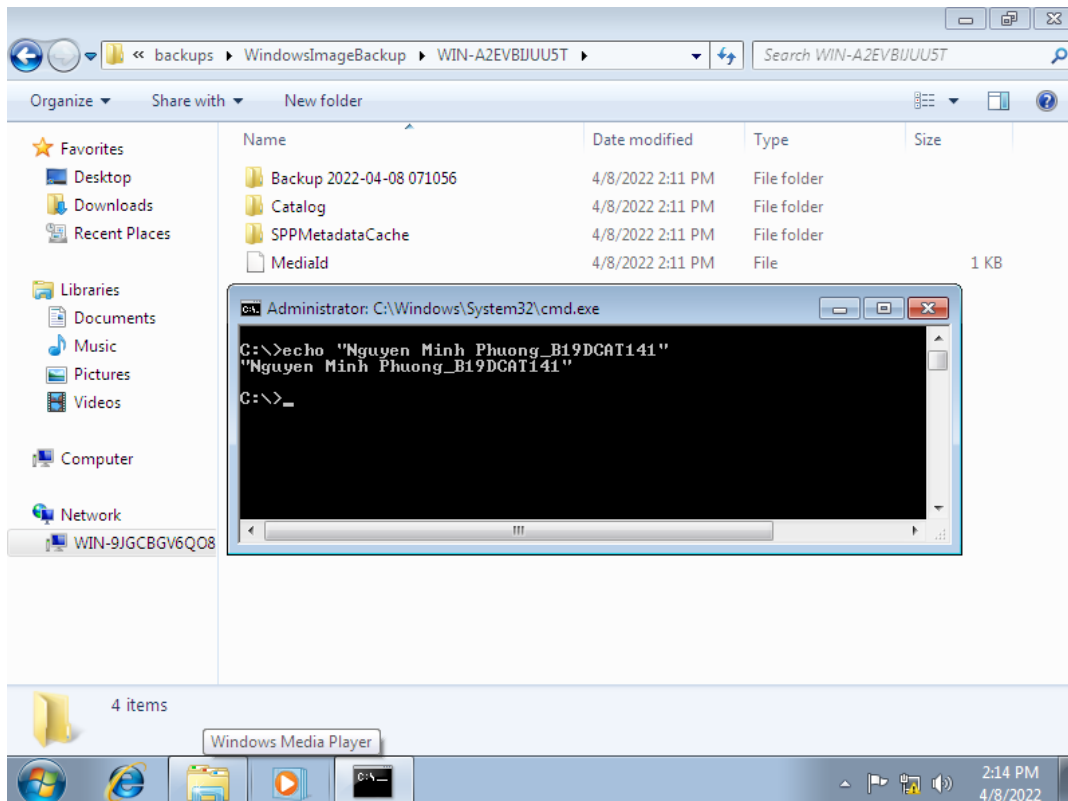
File Home Share View

Network > 192.168.100.5 > share > backups > WindowsImageBackup > WIN-A2EVBIJU5T

Name	Date modified	Type	Size
Backup 2022-04-08 071056	4/8/2022 2:11 PM	File folder	
Catalog	4/8/2022 2:11 PM	File folder	
SPPMetadataCache	4/8/2022 2:11 PM	File folder	
MediaId	4/8/2022 2:11 PM	File	1 KB

Administrator: Command Prompt

```
C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"
C:\>
```



```
Administrator: C:\Windows\System32\cmd.exe

C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"

C:\>echo %USERNAME%
phuong-b19dcat141

C:\>date
The current date is: Fri 04/08/2022
Enter the new date: (mm-dd-yy)

C:\>net share

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

C:\>dir c:\share
Volume in drive C has no label.
Volume Serial Number is A495-8EDE

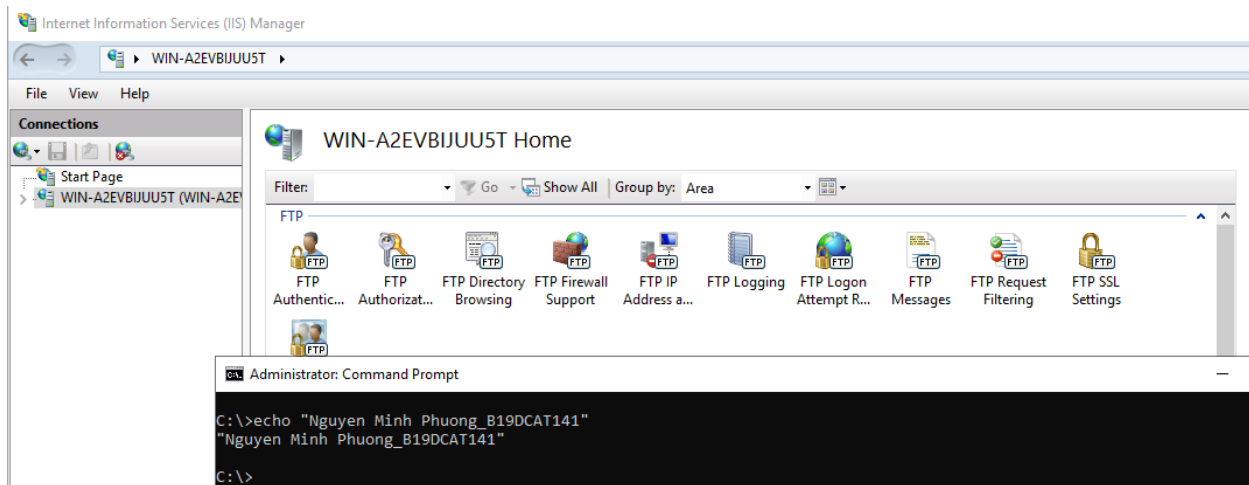
Directory of c:\share

04/08/2022  01:58 PM    <DIR>          .
04/08/2022  01:58 PM    <DIR>          ..
04/08/2022  02:11 PM    <DIR>          backups
0 File(s)      0 bytes
3 Dir(s)      56,435,052,544 bytes free

C:\>_
```

2. Sao lưu tệp bên FTP Server:

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



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

```
phuong-b19dcat141@ubuntu: ~  
phuong-b19dcat141@ubuntu:~$ sudo apt-get install vsftpd  
[sudo] password for phuong-b19dcat141:  
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 440 not upgraded.  
Need to get 126 kB of archives.  
After this operation, 371 kB of additional disk space will be used.  
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main i386 vsftpd i386 3.0.3-3ubuntu2 [126 kB]  
Fetched 126 kB in 1s (68.1 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 179834 files and directories currently installed.)  
Preparing to unpack .../vsftpd_3.0.3-3ubuntu2_i386.deb ...  
Unpacking vsftpd (3.0.3-3ubuntu2) ...  
Processing triggers for systemd (229-4ubuntu21.16) ...  
Processing triggers for ureadahead (0.100.0-19) ...  
Processing triggers for man-db (2.7.5-1) ...  
Setting up vsftpd (3.0.3-3ubuntu2) ...  
Processing triggers for systemd (229-4ubuntu21.16) ...  
Processing triggers for ureadahead (0.100.0-19) ...
```

```
phuong-b19dcat141@ubuntu:~$ sudo ufw allow 20:21/tcp  
Rules updated  
Rules updated (v6)  
phuong-b19dcat141@ubuntu:~$ sudo ufw allow 990/tcp  
Rules updated  
Rules updated (v6)
```



```

phuong-b19dcat141@ubuntu:~$ sudo ufw allow 35000:40000/tcp
Rules updated
Rules updated (v6)
phuong-b19dcat141@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
phuong-b19dcat141@ubuntu:~$ sudo ufw reload
Firewall reloaded
phuong-b19dcat141@ubuntu:~$ sudo ufw status
Status: active

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

```

```

phuong-b19dcat141@ubuntu: ~
GNU nano 2.5.3 File: /etc/vsftpd.conf Modified
#
# 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
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
# Activate logging of uploads/downloads.
xferlog_enable=YES
#

```

- 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

Administrator: Command Prompt - ftp 192.168.100.147

```
C:\>echo "Nguyen Minh Phuong_B19DCAT141"
"Nguyen Minh Phuong_B19DCAT141"

C:\>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)): phuong-b19dcat141
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>
```

```
phuong-b19dcat141@ubuntu: ~
phuong-b19dcat141@ubuntu:~$ ls
backups.zip  Documents  examples.desktop  Pictures  Templates
Desktop      Downloads  Music             Public    Videos
phuong-b19dcat141@ubuntu:~$
```

3. Sao lưu tệp sử dụng SCP

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

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help
(kali@b19dcat141-phuong-kali)-[~]
$ sudo systemctl start ssh
[sudo] password for kali:

(kali@b19dcat141-phuong-kali)-[~]
$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor prese>
   Active: active (running) since Fri 2022-04-08 03:47:39 EDT; 9s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1445 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCC>
   Main PID: 1446 (sshd)
    Tasks: 1 (limit: 2265)
   Memory: 2.4M
      CPU: 22ms
   CGroup: /system.slice/ssh.service
           └─1446 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 08 03:47:39 b19dcat141-phuong-kali systemd[1]: Starting OpenBSD Secure S>
Apr 08 03:47:39 b19dcat141-phuong-kali sshd[1446]: Server listening on 0.0.0>
Apr 08 03:47:39 b19dcat141-phuong-kali sshd[1446]: Server listening on :: po>
Apr 08 03:47:39 b19dcat141-phuong-kali systemd[1]: Started OpenBSD Secure Sh>

(kali@b19dcat141-phuong-kali)-[~]
$
```

130 x

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

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help

(kali@b19dcat141-phuong-kali)-[~]
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:zh06A5CE/u0M9LqgulVxhR/t5Yly1QzrXz0eQgVp9bA kali@b19dcat141-phuong-kali
The key's randomart image is:
+--[RSA 3072]--+
| .. ... .+=+.. |
| .. .... . o++o. |
| . + .. o =o.E.. |
| . .+ o +.o . |
| o.o. So. .. o. |
| .o o+ o .....+ |
| o = * . ..o |
| o .. o o . |
| =. .. |
+--[SHA256]--+
```

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help

(kali@b19dcat141-phuong-kali)-[~]
$ ls ~/.ssh
id_rsa id_rsa.pub known_hosts

(kali@b19dcat141-phuong-kali)-[~]
$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDR6/1LoXAgGY7Y7PuAqTL461DpHA5NdGDapA2LV
KvS8DYUT/Ivjy9An4Ct2AzR6Yz0SvNazChTx2uhXX3lWs7UzIFHcnRwohN+KFYAnAMvNDck5BPVL2
BZ/4pjNPjx4D1CIaUZA08UCdg8/P60oz0+t6wRCgg6P8ztL4C4MSvMlR/ctXH+wQaoI5vw8iRfLoT
qgzU6otxVA6vCnkyRtv0quP0CARILhz8mMH85ESb6WP9/qRUmVLAMIt2TALsBFSmV5hAeS5MbuQhk
OM6hP1FLvqY0UdMQrpiIPj2gbQJ9yIaHNy/BsU2cL26VeJWWwcmZR1Bk4Nxf/E6NWL+Jgs4hmkR0b
uNNIJic6vT93m1RPmLtpbkF0MftgbBdlrkm1jl19b2QuUl1ijhYmRK1EDxr+SNxI78IUtQ2pYUpzZ
Q1rkPAXy8vaNzRLs6bi63tUdxIcn4FW7UuvuJDzFDbZ9VnUubEusERK5it6c0NbLoYWO44PBKQOZZ
Iqnp9hVN83m8= kali@b19dcat141-phuong-kali

(kali@b19dcat141-phuong-kali)-[~]
$ cat ~/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABBQ3eZ0gh
7ZG5/uQM1+m0AnAAAAEAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQgQDR6/1LoXAg
GY7Y7PuAqTL461DpHA5NdGDapA2LVKvS8DYUT/Ivjy9An4Ct2AzR6Yz0SvNazChTx2uhXX
3lWs7UzIFHcnRwohN+KFYAnAMvNDck5BPVL2BZ/4pjNPjx4D1CIaUZA08UCdg8/P60oz0+
t6wRCgg6P8ztL4C4MSvMlR/ctXH+wQaoI5vw8iRfLoTqgzU6otxVA6vCnkyRtv0quP0CAR
ILhz8mMH85ESb6WP9/qRUmVLAMIt2TALsBFSmV5hAeS5MbuQhkOM6hP1FLvqY0UdMQrpiI
Pj2gbQJ9yIaHNy/BsU2cL26VeJWWwcmZR1Bk4Nxf/E6NWL+Jgs4hmkR0buNNIJic6vT93m
1RPmLtpbkF0MftgbBdlrkm1jl19b2QuUl1ijhYmRK1EDxr+SNxI78IUtQ2pYUpzZQ1rkPA
```

- 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

```
phuong-b19dcat141@ubuntu: ~  
phuong-b19dcat141@ubuntu:~$ scp backups.zip kali@192.168.100.3:backups.zip  
The authenticity of host '192.168.100.3 (192.168.100.3)' can't be established.  
ECDSA key fingerprint is SHA256:0itnXxd60V8o2Gqyg9c3UuQjJ08XEVq2cIW30GtFdiE.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.100.3' (ECDSA) to the list of known hosts.  
kali@192.168.100.3's password:  
backups.zip                               100%   0   0.0KB/s   00:00
```

```
kali@b19dcat141-phuong-kali: ~  
File Actions Edit View Help  
  
(kali@ b19dcat141-phuong-kali)-[~]  
$ ls  
backups.zip  python-cairo_1.16.2-2ubuntu2_amd64.deb  
Desktop      python-gobject-2_2.28.6-14ubuntu1_amd64.deb  
Documents    python-gtk2_2.24.0-5.1ubuntu2_amd64.deb  
Downloads    Templates  
Music        Videos  
password     zenmap-7.91-1.noarch.rpm  
Pictures     zenmap-7.91-1.noarch.rpm.1  
Public
```

III. Kết quả:

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