

**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.
- ✓ 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 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

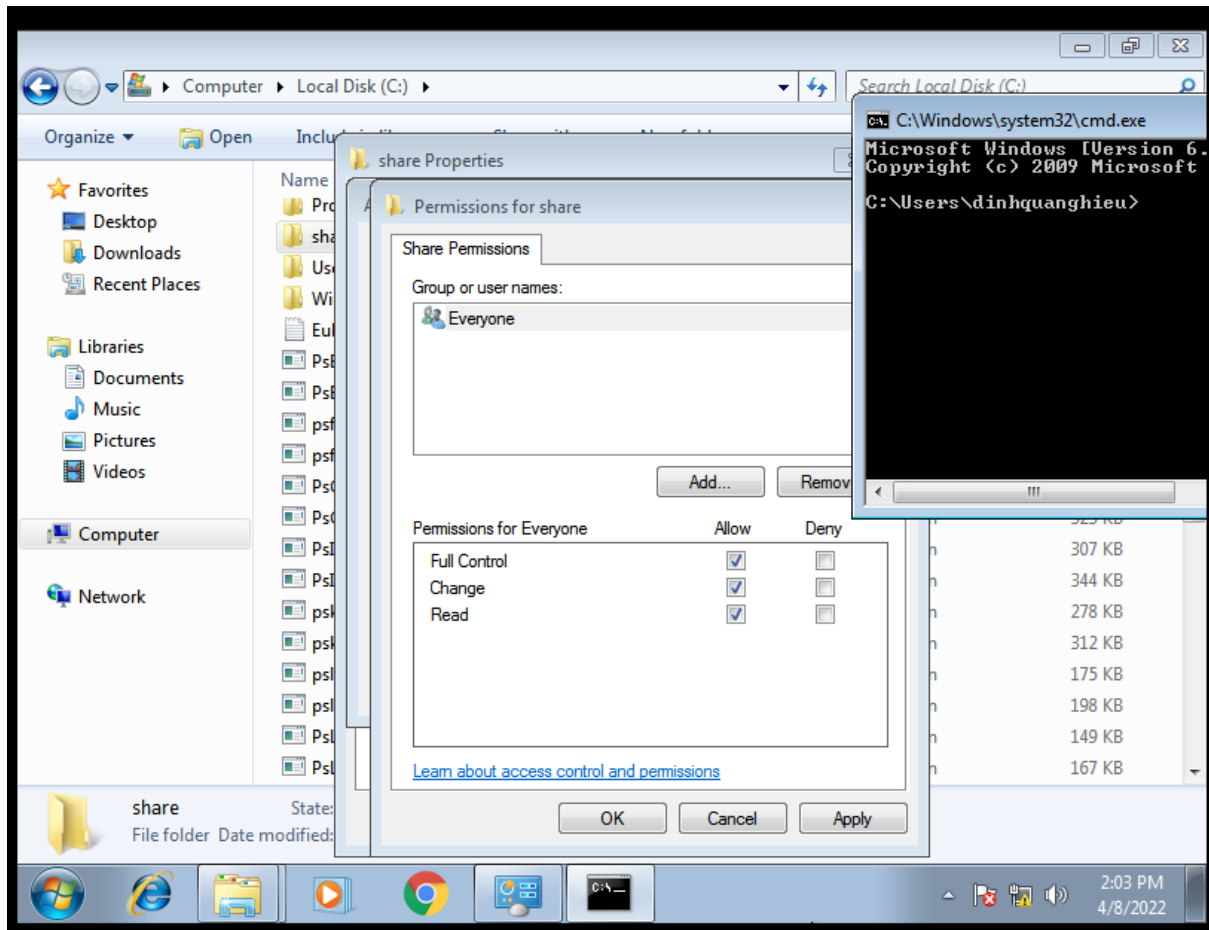
c:\>net use x: \\192.168.100.5\share
Enter the user name for '192.168.100.5': dinhquanghieu
Enter the password for 192.168.100.5:
The command completed successfully.

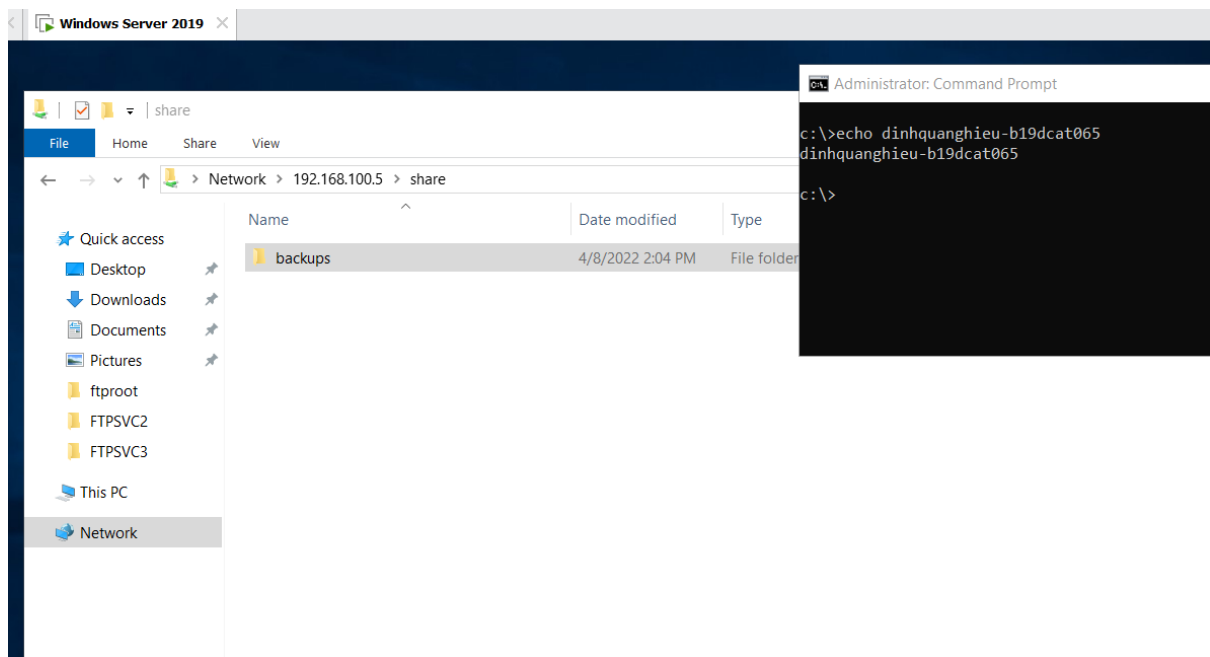
c:\>net use
New connections will be remembered.

Status      Local      Remote          Network
-----
OK          X:         \\192.168.100.5\share  Microsoft Windows Network
The command completed successfully.

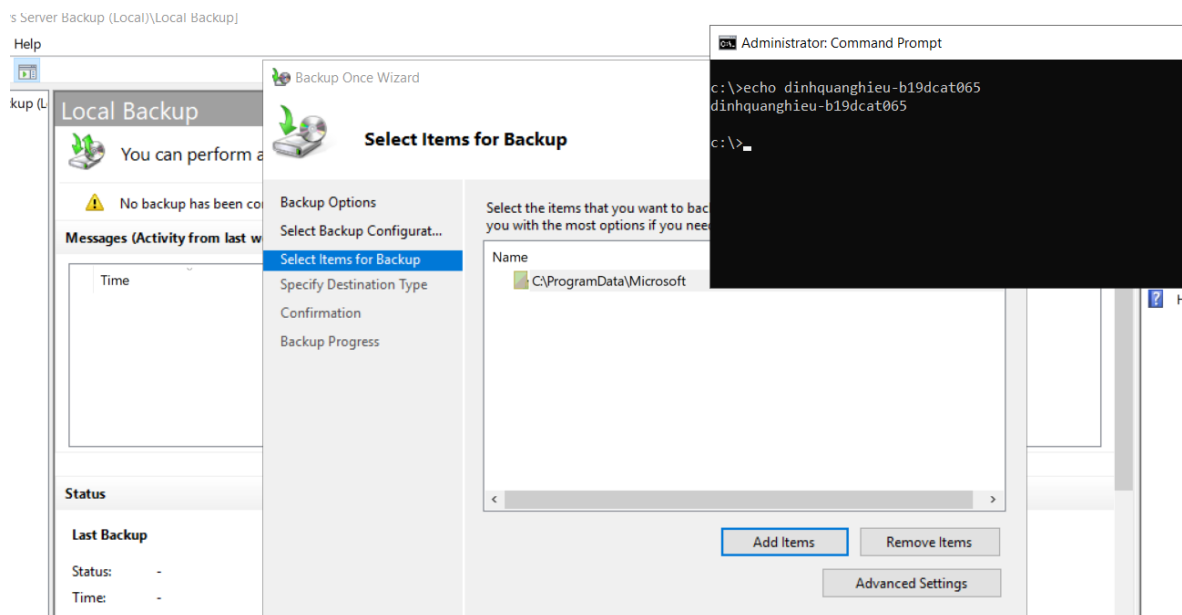
c:\>
```

- 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



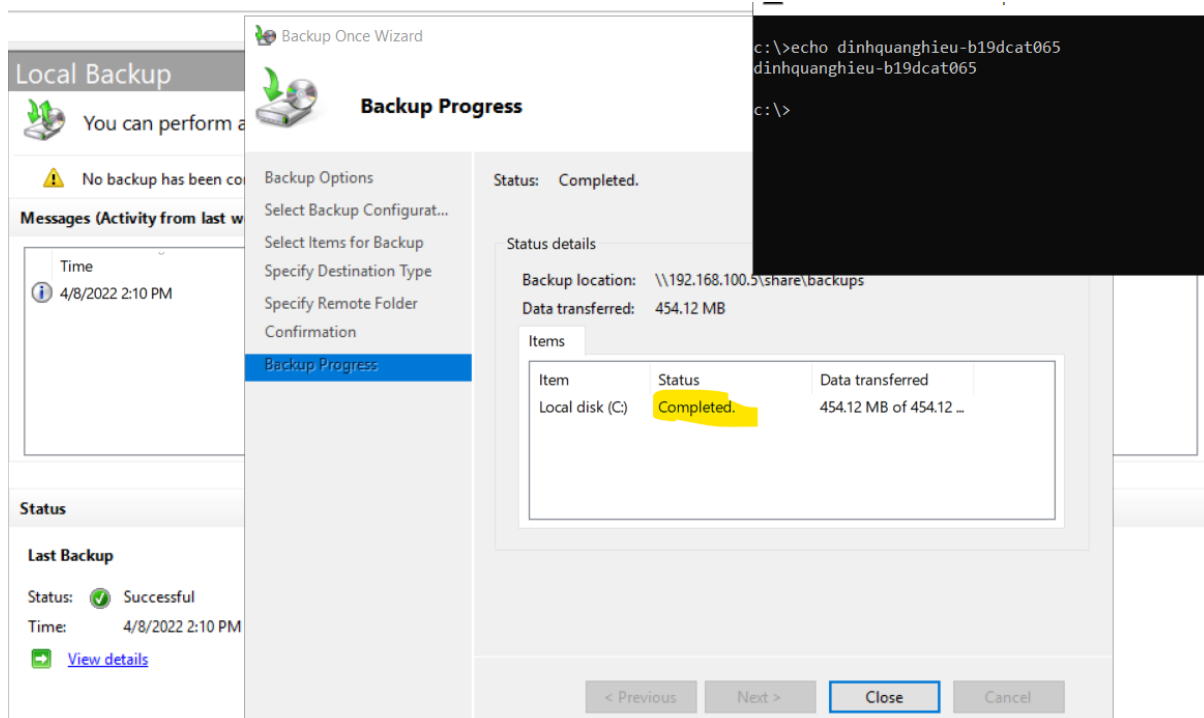
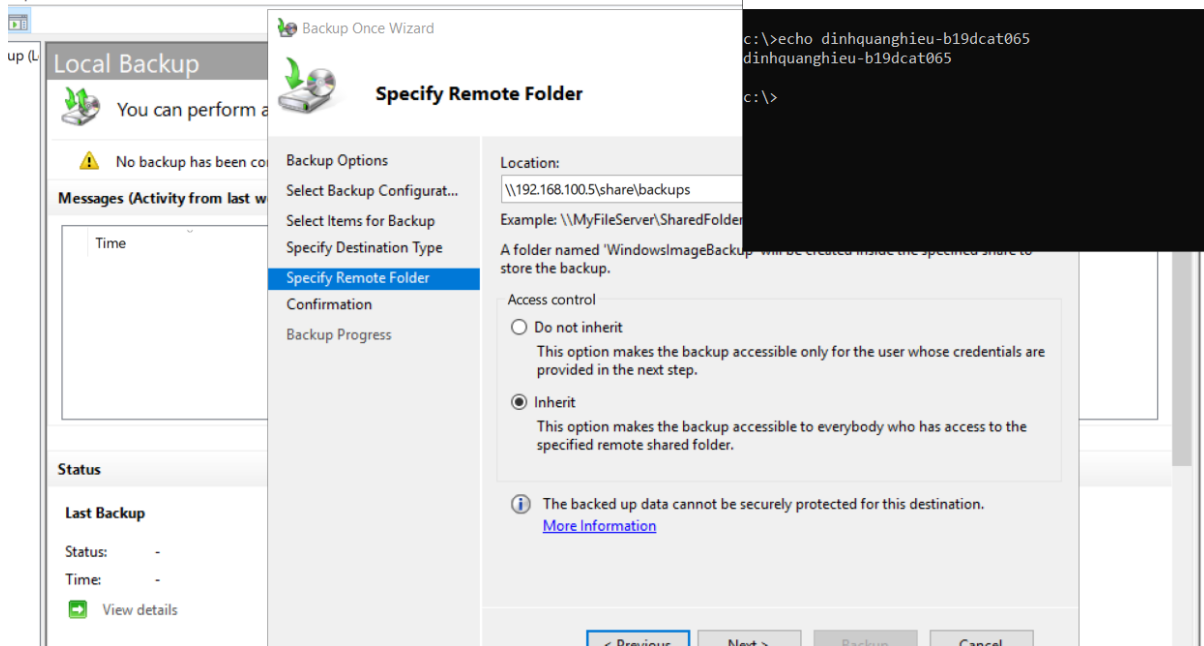


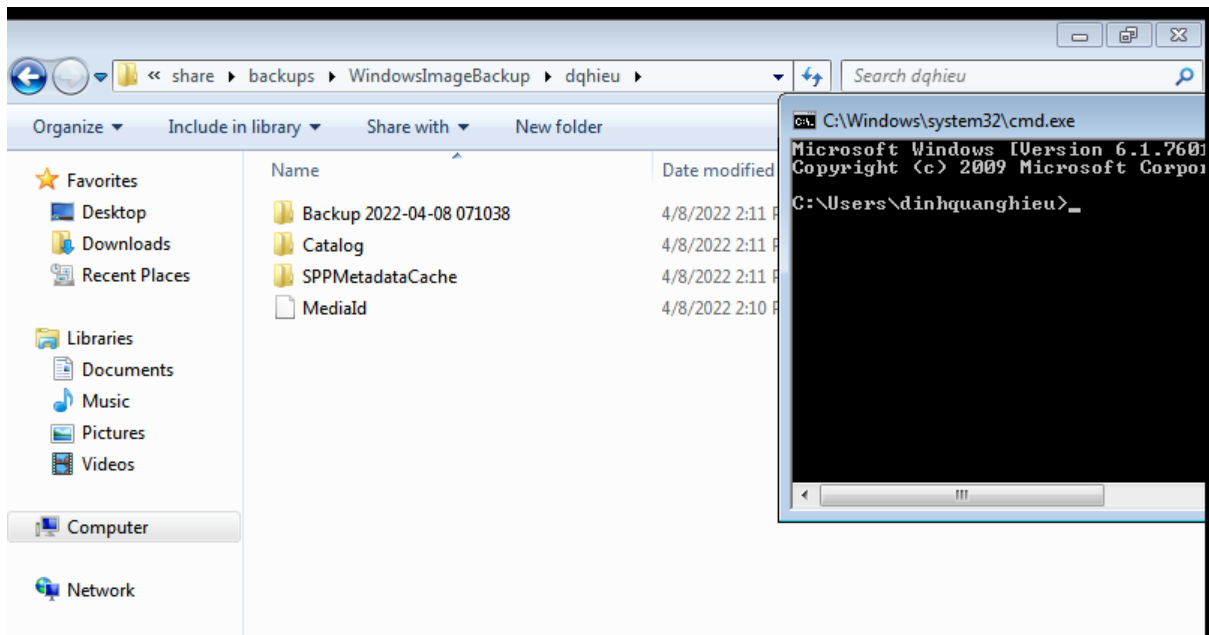
- Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2003, nếu sử dụng Win khác thì có thể download ntbackup để sử dụng), sau đó chọn 1 thư mục để sao lưu và đích là thư mục ổ mạng đã chia sẻ trên máy Windows attack trong mạng 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



Help

up (L





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

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\dinhquanghieu>echo %USERNAME%
dinhquanghieu

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

C:\Users\dinhquanghieu>net share

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

C:\Users\dinhquanghieu>dir c:\share
Volume in drive C has no label.
Volume Serial Number is BA20-1907

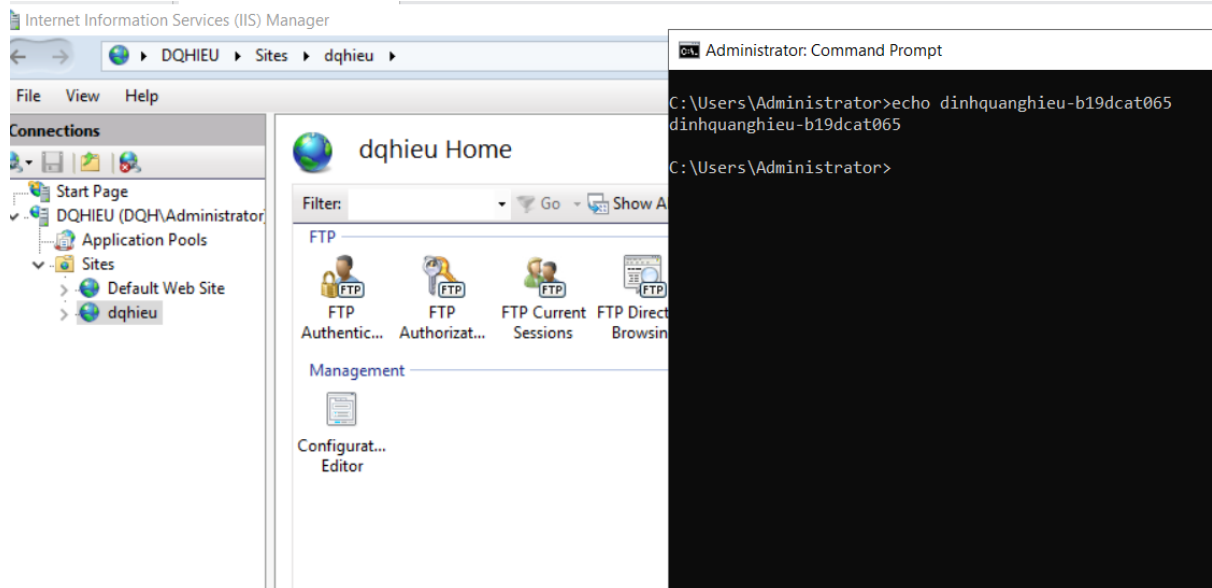
Directory of c:\share

04/08/2022  02:09 PM    <DIR>      .
04/08/2022  02:09 PM    <DIR>      ..
04/08/2022  02:10 PM    <DIR>      backups
               0 File(s)      0 bytes
               3 Dir(s)  51,102,052,352 bytes free
```

### 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 3.0.3-3ubuntu2 [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>
```

```
dinhquanghieu-b19dcat065@ubuntu: ~  
dinhquanghieu-b19dcat065@ubuntu:~$ ls  
backups.zip      Desktop          file1.txt        Music            Something  
daq-2.0.7        Documents        file2.txt        Pictures         Templates  
daq-2.0.7.tar.gz Downloads        file3.txt        Public           Videos  
dem.txt          examples.desktop gedit            snort_src       vi.save  
dinhquanghieu-b19dcat065@ubuntu:~$
```

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.

```
(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]  
$ systemctl status ssh  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: di  
   Active: active (running) since Fri 2022-04-08 09:07:39 EDT; 4s ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Process: 1228 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  
    Main PID: 1229 (sshd)  
       Tasks: 1 (limit: 2255)  
      Memory: 2.3M  
         CPU: 22ms  
    CGroup: /system.slice/ssh.service  
            └─1229 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups  
lines 1-12/12 (END)
```

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

```
(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/dinhquanghieu-b19dcat065/.ssh/id_rsa):
Created directory '/home/dinhquanghieu-b19dcat065/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/dinhquanghieu-b19dcat065/.ssh/id_rsa
Your public key has been saved in /home/dinhquanghieu-b19dcat065/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:9U3aPMYoEpiFWcfxkCOX6kHEBU6qgDWT976NhtHY/zg dinhquanghieu-b19dcat065@B19DCA
T065-Hieu-Kali
The key's randomart image is:
+--[RSA 3072]--+
| +.  **+=+ |
| o.o. oB+.*o |
| .. .+.o+ ... |
| .. .. oo . 0 |
| .. .S.. + B |
| o + .. . . |
| o = |
| . + E. |
| . .o. |
+--[SHA256]--+
```

```
(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]
$ ls ~/.ssh
id_rsa id_rsa.pub

(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]
$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDWwIHxwISDf7aZarzcPkS0NSnjAH2wkwZFYx9jd5MdPA
/fmJgAKLRDQxoeQbekT0pfbJv+LNtQmy9wLYB6G2pd232u1cHtGYUXd0qrj6pHPSEjbuBq4VF7hMBq31q9
2FLUwXTo/RFauKILjcctDgrObEabrCc48+xc7H+N6HDAzE05eFZtFbapZ9cefAZgo2TffVtQ2/nNGimQiP
YiV35pJtvlJLXxvBiapV0EIsIE9V8YtQi3fRcsIFv9zHLd8XBAKsyg7D2oMpdoPpWVuPoC5zF0gOoFAff
KLVCjBKfVU6fjen05ZGB3+yjjbEUBHR+cRCVW2oVOURObCOxJrBK0dULGgVzKFpAQND+CGmtfJGRcdcsA6
INkytt6twpSFQKh82INPkMb3BTD3IDDKNXi5P0XzzxtgGcp6UFnI51NMMieQETNQ6bCaV9Q809GCuQOKjJ
ZNkLSKA870DTW9AfvmWjZQi+UwPerTeA/Vg2ZzDJxq0KPUqWkQd/bdkWzG0= dinhquanghieu-b19dcat
065@B19DCAT065-Hieu-Kali

(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]
$
```

```
(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]
$ cat ~/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAadzC2gtcn
NhAAAAAwEAAQAAAYEA1sCB8cCEg3+2mWq83KZEtdUp4wB9sJMGRWMfY3eTHTwP3zIxgCpU
Q0MaHkG3pE9KX2yb/izbUJsvcJWAehtqXdt9rtXB7RmFF3Tqq4+qRz0hI27gauFRe4TAat
9avdhS1MF06P0RWriiC43HLQ4KzmxGm6wnOPPsXOX/jehwwMxDuXhWbRW2qWfXHNwGYKNk
331bUNv5zRopkIj2Ild+aSbbyyS18VbQYmqVdBCLCBPVfGLUIt30XLCBb/cxy3fFwQCrMo
0w9qDKXaD6Vlbj6AucxdIDqBQH3ypVQowSn1V0n43pzuWRgd/so42xFGx0fnEQlVtqFTLE
TmwjsSawStHVJRofcyhaQEDQ/ghprXyRkXHXLA0iDZMrbercKUHUCofNiDT5DG9wUw9yAw
5DV4uT9F888bYBnKelBzy0dTTDInkBEzU0mwmlfUPNPRgrkDioyWTZC0pAP09A01vQH7zF
o2UIvLMD3kbXgP1YNmcwycatCj1KlpEHf23ZFsxtAAAFqIY+Dq2GPG6tAAAAB3NzaC1yc2
EAAAAGBANbAgfHAIIN/tplqvNymRLQ1KeMAfbCTBkvjH2N3kx08D98yMYAqVENDGh5Bt6RP
Sl9sm/4s21CbL3CVgHobal3bfa7Vwe0Zhrd06quPqkc9ISNu4GrhUXuEwGrfWr3YUtTBd0
j9EVq4oguNxy0OCs5sRpusJzjz7Fzsf43ocMDMQ7L4Vm0Vtqln1x58BmCjZN99W1Db+c0a
KZCI9iJXfmkm28sktfFW0GJqLXQqiWgT1Xxi1CLd9FywgW/3Mct3xcEAqzKDsPagyl2g+l
ZW4+gLnMXSA6gUB98qVUKMEp9VTp+N6c7LkYHf7KONsRRsdH5xEJVBahU5RE5sI7EmsErR
-----
```

- 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

```
root@ubuntu: /home/dinhquanghieu-b19dcat065
root@ubuntu:/home/dinhquanghieu-b19dcat065# ls
backups.zip      Desktop          file1.txt        Music            Something
daq-2.0.7        Documents        file2.txt        Pictures         Templates
daq-2.0.7.tar.gz Downloads        file3.txt        Public           Videos
dem.txt          examples.desktop gedit            snort_src       vi.save
root@ubuntu:/home/dinhquanghieu-b19dcat065# scp backups.zip root@192.168.100.3:b
ackups.zip
The authenticity of host '192.168.100.3 (192.168.100.3)' can't be established.
ECDSA key fingerprint is SHA256:jFWtk0GRZ6jBZnvu3LW7R21LrCctCxwzmHuVYoJ/FsU.
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.
root@192.168.100.3's password:
backups.zip                                100% 316MB 63.3MB/s 00:05
root@ubuntu:/home/dinhquanghieu-b19dcat065#
```

```
(root@B19DCAT065-Hieu-Kali)-[/home/dinhquanghieu-b19dcat065]
# cd /home

(root@B19DCAT065-Hieu-Kali)-[/home]
# cd /root

(root@B19DCAT065-Hieu-Kali)-[~]
# ls
backups.zip

(root@B19DCAT065-Hieu-Kali)-[~]
#
```

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.