

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ



BÀI 10:
SAO LƯU HỆ THỐNG

Giảng viên : Nguyễn Ngọc Diệp

Sinh viên : Nguyễn Đức Anh

Mã sinh viên : B21DCAT031

Hệ : Đại học chính quy

Hà Nội, 4/2024

Table of Contents

1. Mục đích	3
2. Nội dung thực hành	3
2.1 Tìm hiểu lý thuyết	3
2.2 Tài liệu tham khảo	5
2.3 Chuẩn bị môi trường	5
2.4 Các bước thực hiện	5
a. Sao lưu tới ổ đĩa mạng.....	5
b. Sao lưu tệp lên FTP server	10
c. Sao lưu tệp sử dụng SCP	13
3. Kết quả đạt được	15

1. Mục đích

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. Nội dung thực hành

2.1 Tìm hiểu lý thuyết

a. SCP – Secure copy (SCP)

SCP (Secure Copy) là một công cụ dòng lệnh được sử dụng để sao chép và truyền tệp tin giữa các máy tính trong mạng với mức độ bảo mật cao. SCP sử dụng giao thức SSH (Secure Shell) để mã hóa dữ liệu trước khi truyền đi, giúp bảo vệ dữ liệu khỏi bị đánh cắp hoặc thay đổi trong quá trình truyền tải.

SCP hoạt động tương tự như công cụ sao chép (copy) dòng lệnh của hệ điều hành Unix/Linux, tuy nhiên nó cung cấp thêm tính năng bảo mật. Khi bạn sử dụng SCP để sao chép tệp tin, dữ liệu sẽ được mã hóa trước khi gửi đến máy chủ đích thông qua SSH. Do đó, dù có ai gián điệp trong mạng cũng không thể đọc được nội dung của tệp tin.

SCP có thể hoạt động ở hai chế độ: sao chép từ local lên remote hoặc ngược lại.

SCP là một công cụ rất hữu ích cho các quản trị viên hệ thống hoặc những người làm việc với nhiều máy tính trong mạng. Nó giúp họ có thể sao chép các tệp tin lớn, các script, hoặc các tệp tin nhạy cảm một cách nhanh chóng và an toàn.

Ngoài ra, SCP còn có thể kết hợp với các lệnh dòng lệnh khác để tạo ra các tác vụ tự động hoặc định kỳ. Ví dụ, bạn có thể sử dụng SCP kết hợp với Cron để sao chép các tệp tin định kỳ từ một máy tính đến một máy chủ khác.

Tuy nhiên, việc sử dụng SCP cũng có một số hạn chế. SCP chỉ có thể sao chép tệp tin một cách tuần tự, không thể sao chép nhiều tệp tin cùng lúc. Nếu bạn muốn sao chép nhiều tệp tin, bạn phải sử dụng một vòng lặp hoặc một lệnh tổng hợp khác để sao chép chúng.

Ngoài SCP, còn có một số công cụ khác để sao chép tệp tin qua SSH như rsync, lftp, ncftp,... Tuy nhiên, mỗi công cụ có những ưu điểm và hạn chế riêng, tùy thuộc vào mục đích sử dụng và tình huống cụ thể.

b. FTP - Giao thức truyền tệp

FTP (File Transfer Protocol) là một giao thức truyền tệp dùng để truyền tệp tin giữa các máy tính trên mạng. Giao thức này được thiết kế để truyền tệp tin theo hai hướng: từ máy chủ về máy khách (download) và từ máy khách lên máy chủ (upload). FTP sử dụng mô hình kiến trúc máy chủ - máy khách để truyền dữ liệu.

Trong giao thức FTP, khi một máy khách yêu cầu truyền một tệp tin từ máy chủ, nó kết nối đến máy chủ thông qua cổng điều khiển (port 21) bằng cách sử dụng tài khoản và mật khẩu xác thực. Sau khi xác thực thành công, máy khách và máy chủ thiết lập kết nối dữ liệu trực tiếp để truyền tệp tin. Kết nối dữ liệu có thể được thiết lập bằng một trong hai phương

thức: Active hoặc Passive.

Phương thức Active yêu cầu máy khách mở một cổng để chờ máy chủ kết nối trở lại, trong khi Passive yêu cầu máy chủ mở một cổng để chờ máy khách kết nối. Khi kết 4 nối dữ liệu được thiết lập, máy khách và máy chủ có thể truyền dữ liệu theo hướng đơn chiều hoặc đồng thời.

FTP còn có một số chức năng khác như cho phép tạo thư mục mới, xóa thư mục, đổi tên thư mục, đổi tên tệp tin, xóa tệp tin, hiển thị danh sách các tệp tin và thư mục trên máy chủ, v.v.

Tuy nhiên, việc sử dụng FTP cũng có một số hạn chế. Ví dụ, FTP không cung cấp tính năng mã hóa dữ liệu, do đó dữ liệu có thể bị đánh cắp hoặc bị thay đổi khi được truyền qua mạng. Ngoài ra, FTP cũng không hỗ trợ các tính năng như đồng bộ hóa dữ liệu, sao lưu dữ liệu tự động, hoặc quản lý phiên làm việc. Do đó, các công nghệ mới như SFTP (Secure File Transfer Protocol) hay FTPS (FTP over SSL/TLS) được phát triển để thay thế cho FTP và cung cấp tính năng bảo mật và đầy đủ hơn cho việc truyền tệp tin trên mạng.

c. Ổ đĩa mạng

Ổ đĩa mạng (Network Attached Storage hay NAS) là một thiết bị lưu trữ dữ liệu được kết nối vào mạng để các thiết bị khác trong mạng có thể truy cập và chia sẻ dữ liệu từ đó. NAS thường được dùng cho các mục đích lưu trữ và chia sẻ dữ liệu giữa các máy tính trong một doanh nghiệp hoặc gia đình.

NAS thường được thiết kế với một số khe cắm ổ đĩa cứng, nơi mà người dùng có thể cài đặt ổ đĩa cứng để lưu trữ dữ liệu. NAS thường được cài đặt và quản lý thông qua giao diện web hoặc phần mềm quản lý để người dùng có thể thực hiện các tác vụ quản lý như tạo thư mục, xóa thư mục, di chuyển tệp tin, cấu hình chia sẻ dữ liệu, v.v.

NAS cũng cung cấp một số tính năng đáng chú ý như sao lưu dữ liệu, phân quyền truy cập dữ liệu, mã hóa dữ liệu và chia sẻ tệp tin qua mạng. Ngoài ra, NAS còn có thể được cấu hình để truy cập từ xa qua Internet, cho phép người dùng truy cập dữ liệu từ bất kỳ đâu trên thế giới mà không cần phải có truy cập trực tiếp vào máy tính của mình.

Tuy nhiên, để sử dụng được NAS, người dùng cần phải có kiến thức cơ bản về mạng và quản lý hệ thống. Ngoài ra, NAS cũng có giá thành cao hơn so với một ổ đĩa di động thông thường, do đó, việc lựa chọn NAS cần phải cân nhắc đến nhu cầu sử dụng và khả năng tài chính của mỗi người dùng.

d. Net use

"Net use" là một lệnh trong hệ điều hành Windows được sử dụng để kết nối và ngắt kết nối với các tài nguyên mạng như máy chủ, ổ đĩa mạng, máy in, v.v. thông qua đường mạng.

Khi sử dụng lệnh "Net use", người dùng có thể kết nối với các tài nguyên mạng thông qua các giao thức khác nhau như SMB, NFS, FTP, v.v. Bằng cách kết nối với các tài nguyên mạng này, người dùng có thể truy cập vào các tệp tin và thư mục được chia sẻ từ các máy tính khác trong mạng.

e. Net view

"Net view" là một lệnh trong hệ điều hành Windows được sử dụng để hiển thị danh sách các máy tính và tài nguyên mạng có sẵn trên mạng. Lệnh này cho phép người dùng kiểm tra xem có bao nhiêu máy tính đang hoạt động trên mạng, tài nguyên được chia sẻ từ các máy tính đó, và tên của các nhóm làm việc trong mạng.

2.2 Tài liệu tham khảo

- Lab 8 pfsense firewall của CSSIA CompTIA Security+®.

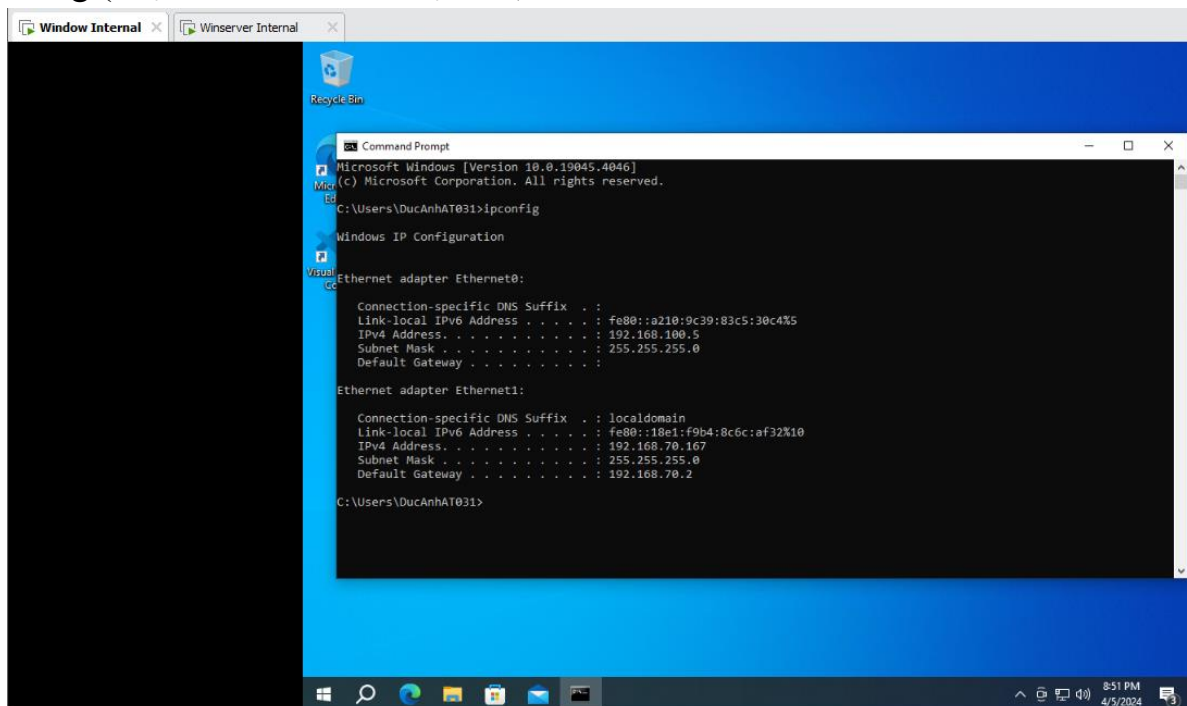
2.3 Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- 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.
- Topo mạng như đã cấu hình trong bài 5.

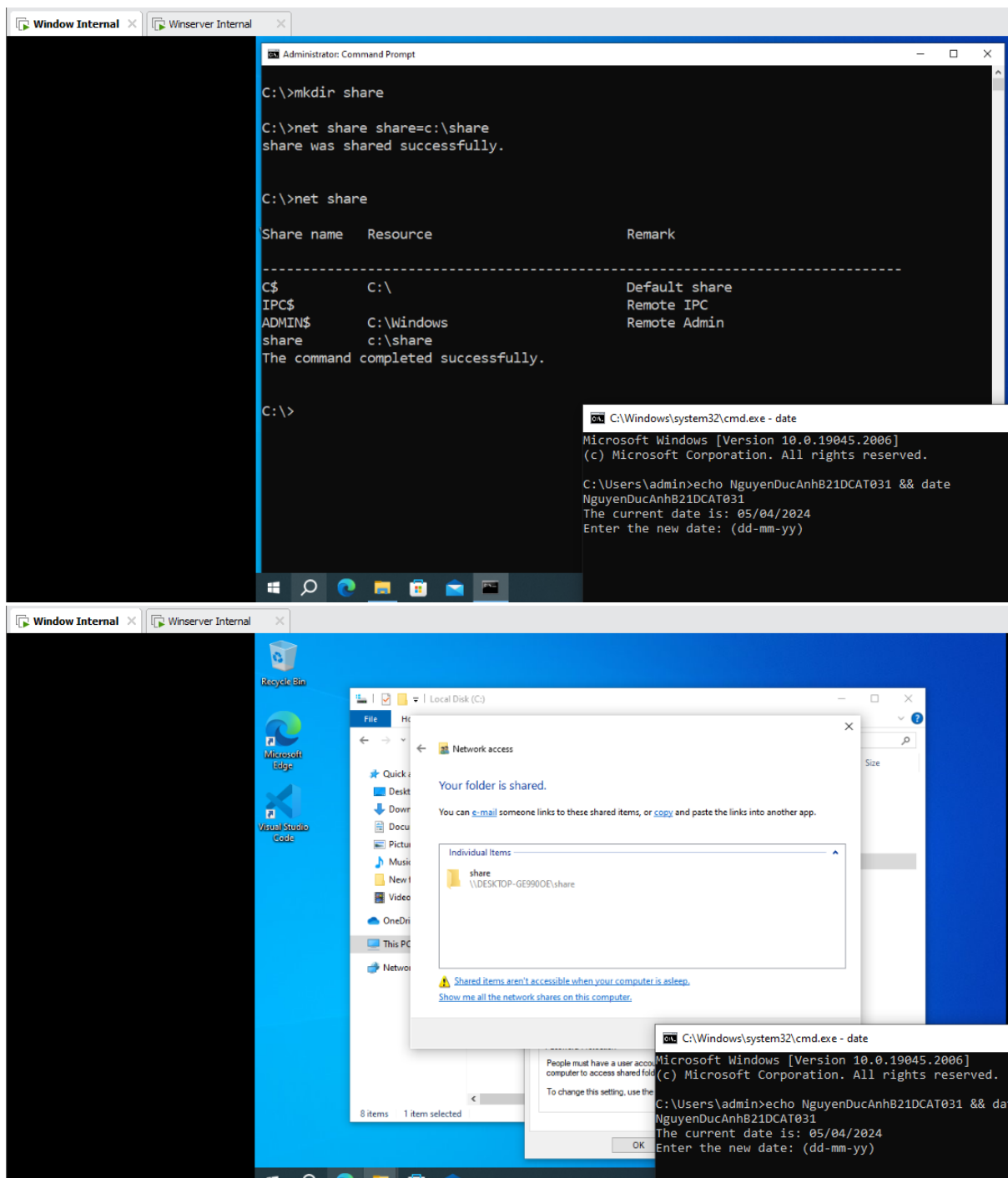
2.4 Các bước thực hiện

a. Sao lưu tới ổ đĩa mạng

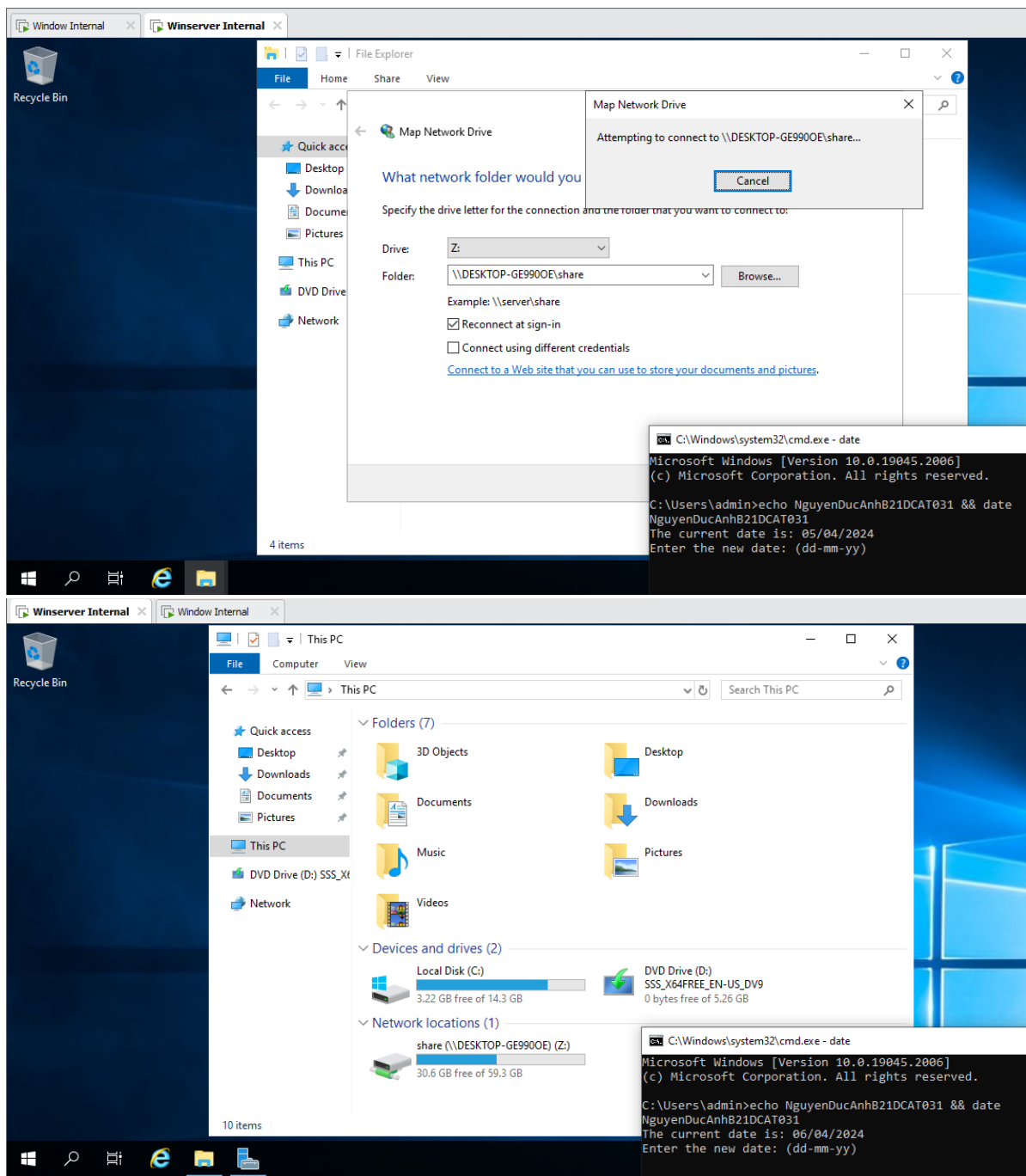
Trên máy trạm Windows attack trong mạng Internal, tạo thư mục share rồi chia sẻ qua mạng (C:\net share share=c:\share)



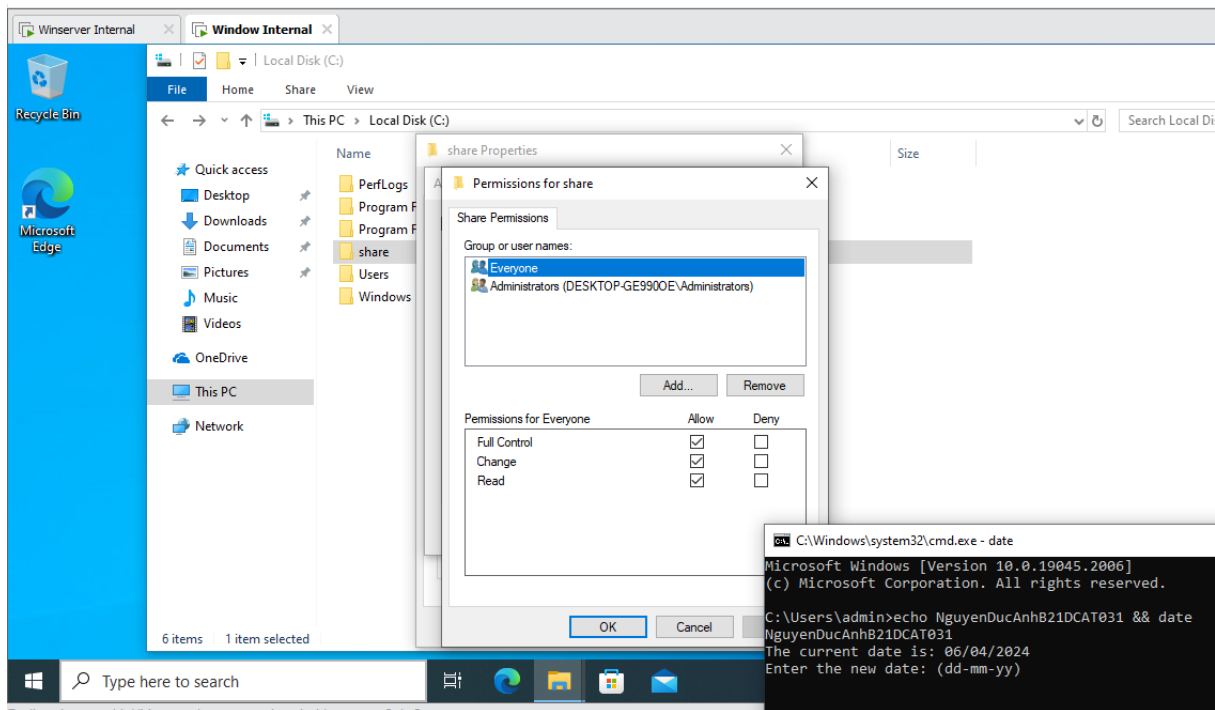
IP máy Windows Attack



Trên máy Windows server ở mạng Internal, cấu hình map ổ đĩa mạng trên máy

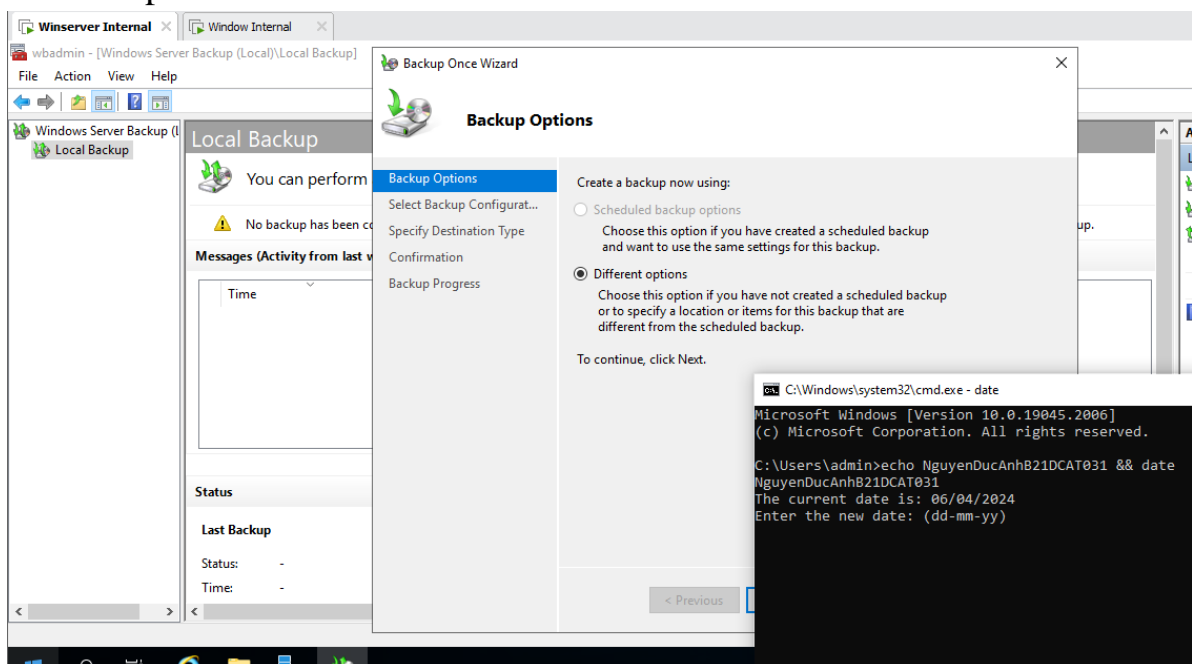


Trên máy Windows attack trong mạng Internal, cấu hình thư mục ở đĩa mạng cho phép sao lưu tệp và thư mục từ máy khác nếu không tạo được thư mục trên máy Windows server

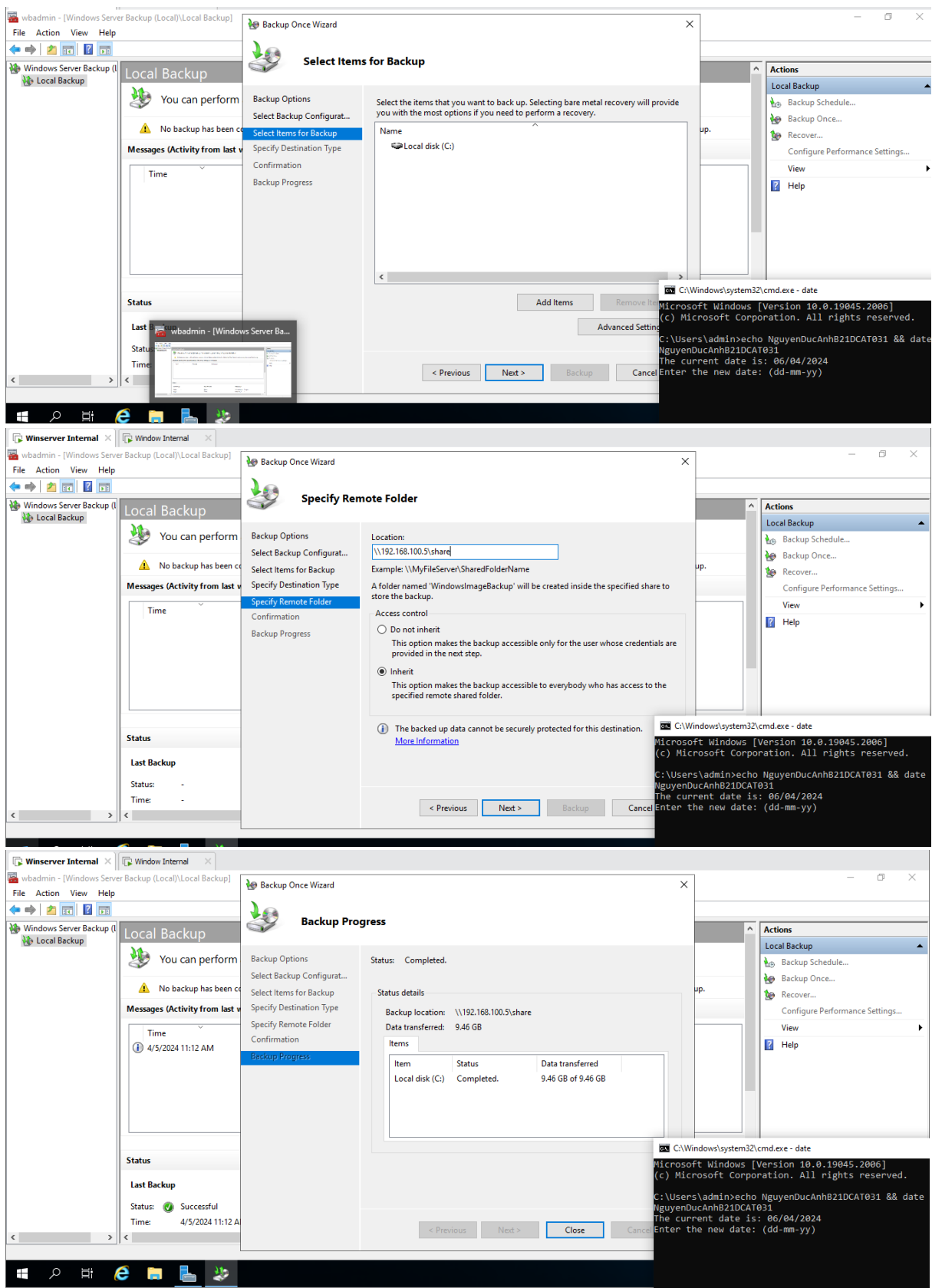


Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2019, nếu sử dụng Win khác thì có thể download ntbackup để sử dụng), sau đó chọn 1 thư mục để sao lưu và đích là thư mục ổ mạng đã chia sẻ trên máy Windows attack trong mạng Internal:

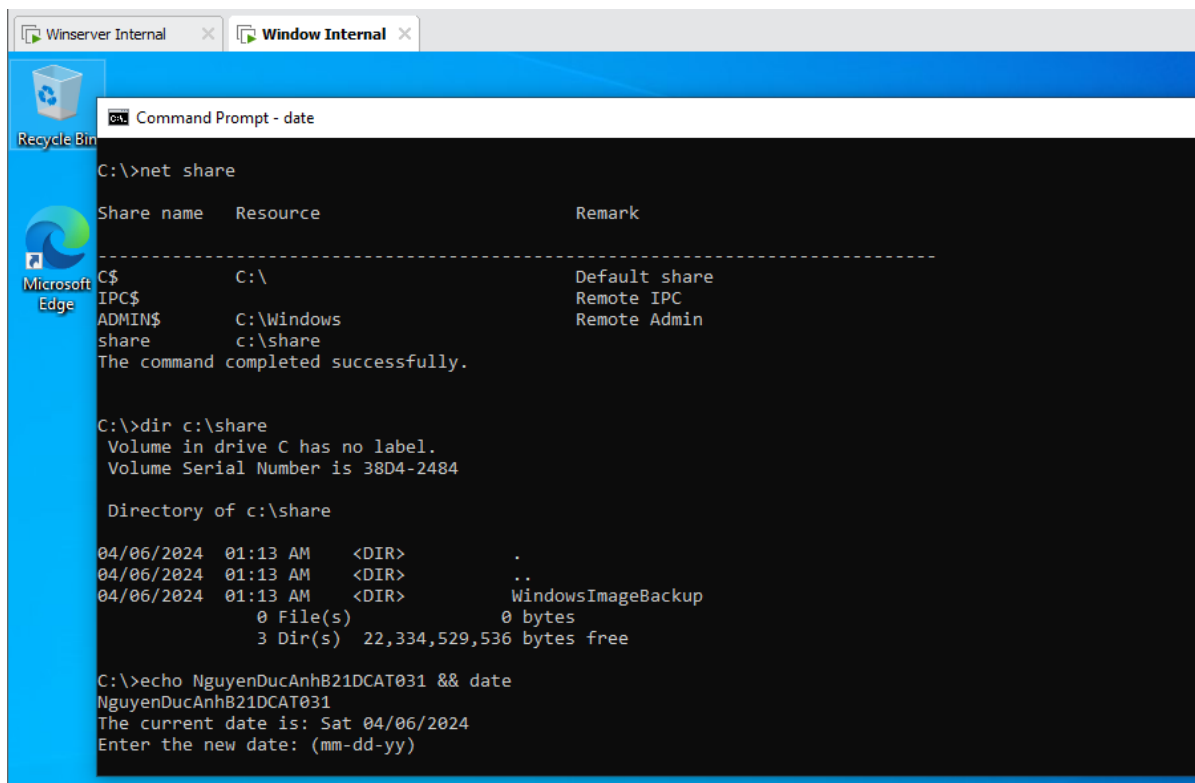
- Vào Server Manager -> Tools -> Windows Server Backup -> Chuột phải Local Backups -> Backup Once



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



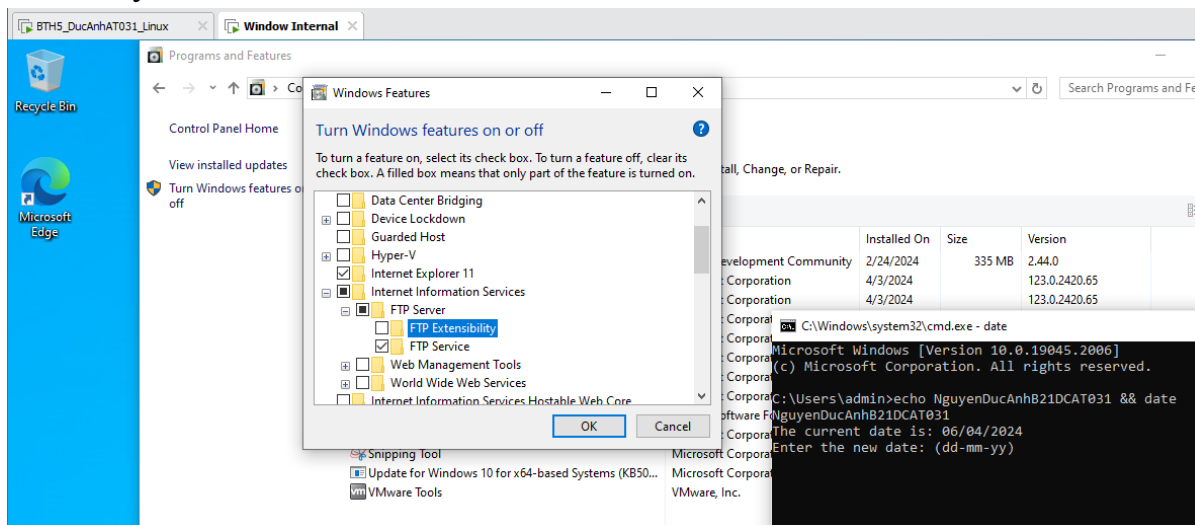
Đã backup xong.



Kiểm tra lại trên máy Windows Attack

b. Sao lưu tệp lên FTP server

Trên máy Windows Attack, cấu hình FTP client



Trên máy Linux trong mạng Internal, cài đặt FTP Server

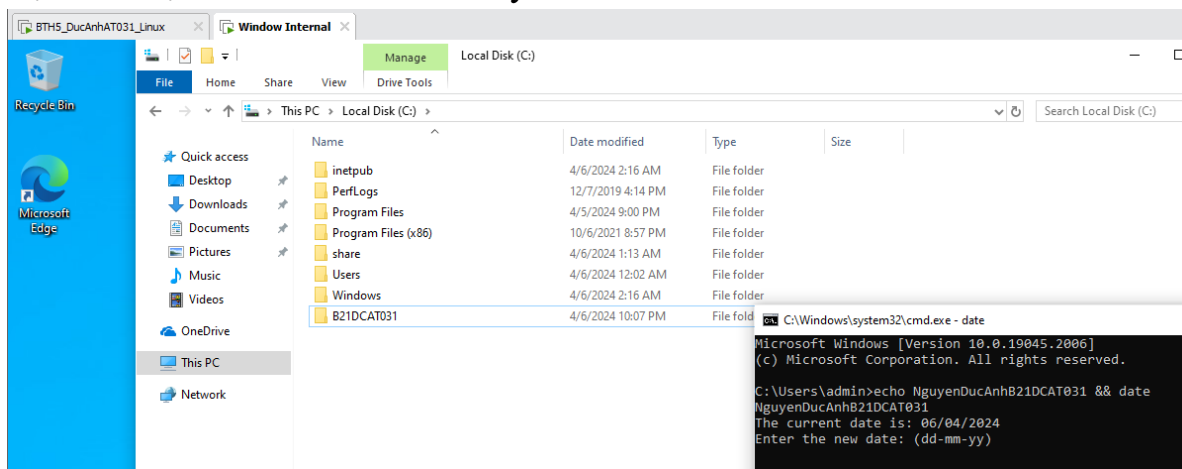
```
BTMS_DucAnhAT031_Linux x Window Internal x
Terminal
ducanhat031@ducanhat031: ~
E: Invalid operation get
ducanhat031@ducanhat031:~$ sudo apt install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 191 not upgraded.
Need to get 115 kB of archives.
After this operation, 336 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu xenial/main amd64 vsftpd amd64 3.0.3-3ubuntu2 [115 kB]
Fetched 115 kB in 0s (501 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 181711 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-3ubuntu2_amd64.deb ...
Unpacking vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for systemd (229-4ubuntu21.28) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for systemd (229-4ubuntu21.28) ...

ducanhat031@ducanhat031:~$ service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
   Active: active (running) since T7 2024-04-06 21:46:19 +07; 14min ago
   Main PID: 2660 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─2660 /usr/sbin/vsftpd /etc/vsftpd.conf

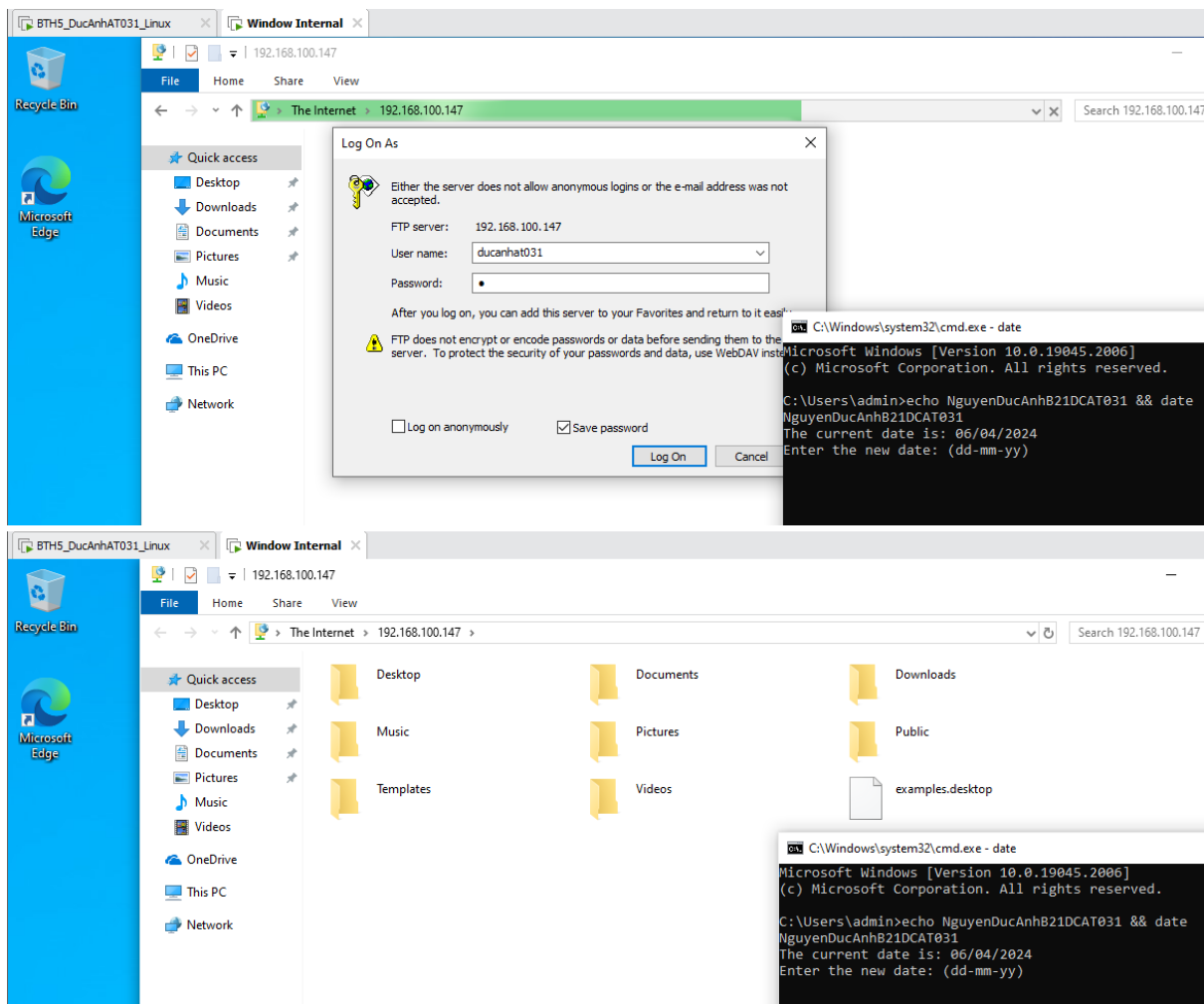
Th04 06 21:46:19 ducanhat031 systemd[1]: Starting vsftpd FTP server...
Th04 06 21:46:19 ducanhat031 systemd[1]: Started vsftpd FTP server.

ducanhat031@ducanhat031:~$
```

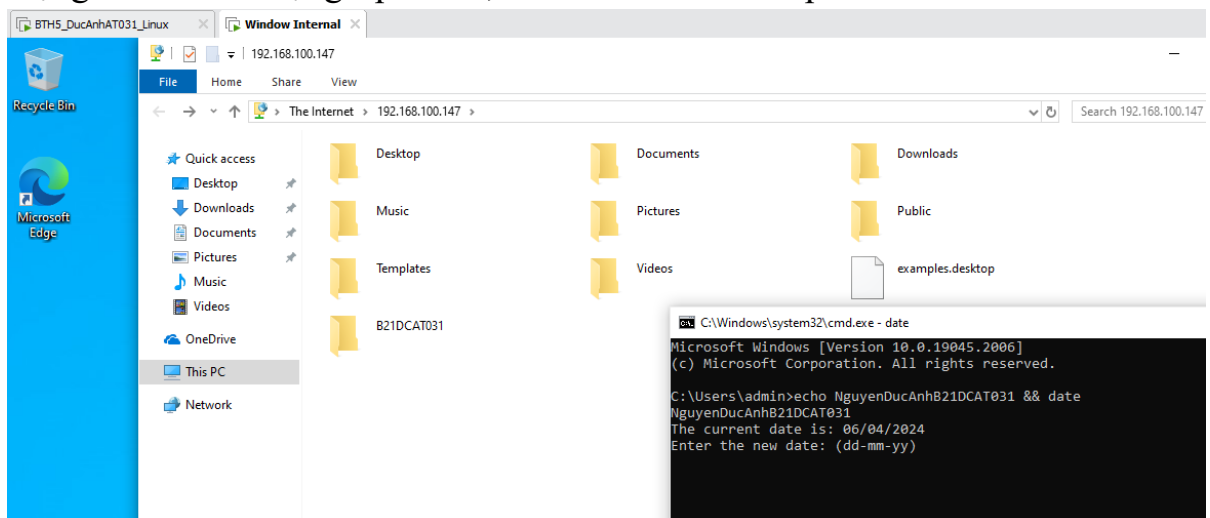
Tạo thư mục B21DCAT031 ở máy Windows Attack



Trên máy Windows Attack ở mạng Internal, cài đặt ftp client và đăng nhập quan máy linux Internal 192.168.100.147



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



Kiểm tra thấy folder B21DCAT031 trên máy Linux.

```

ducanhat031@ducanhat031:~$ ls -l
total 48
drwx----- 2 ducanhat031 ducanhat031 4096 Th04  6 22:18 B21DCAT031
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 14 17:43 Desktop
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Documents
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Downloads
-rw-r--r--  1 ducanhat031 ducanhat031 8980 Th03 12 13:14 examples.desktop
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Music
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Pictures
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Public
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Templates
drwxr-xr-x  2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Videos
ducanhat031@ducanhat031:~$

```

c. Sao lưu tệp sử dụng SCP

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

The screenshot shows a Kali Linux desktop with a terminal window open. The terminal displays the command `systemctl status ssh` and its output, showing that the SSH service is active and running. Below the status output, the terminal shows the logs for the SSH service, indicating that it started successfully on April 6, 2024, at 11:29:26 EDT.

```

ducanhat031@DucAnhB21AT031: ~
File Actions Edit View Help

(ducanhat031@DucAnhB21AT031)-[~]
$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: >
   Active: active (running) since Sat 2024-04-06 11:29:26 EDT; 7s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2693 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCC>
   Main PID: 2696 (sshd)
     Tasks: 1 (limit: 2152)
    Memory: 3.0M (peak: 3.3M)
       CPU: 21ms
    CGroup: /system.slice/ssh.service
           └─2696 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

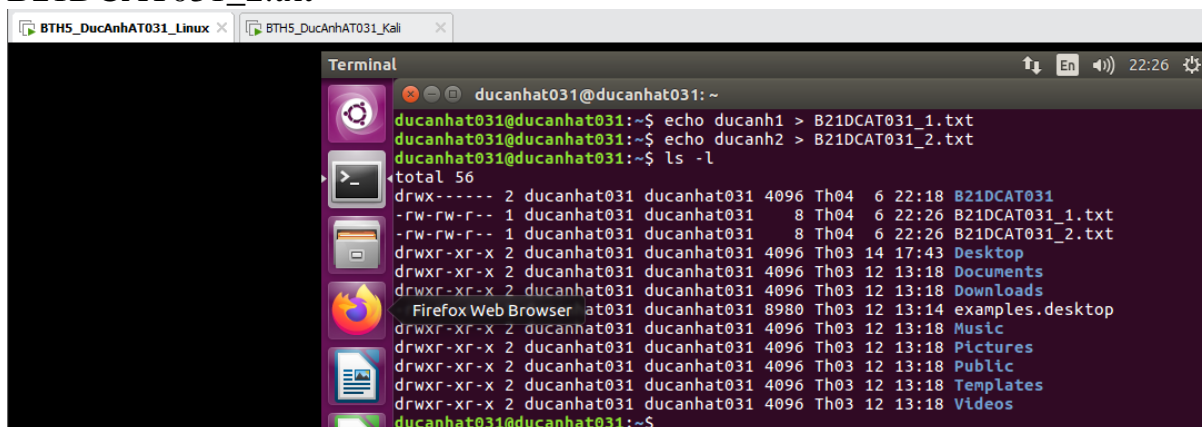
Apr 06 11:29:25 DucAnhB21AT031 systemd[1]: Starting ssh.service - OpenBSD Se>
Apr 06 11:29:26 DucAnhB21AT031 sshd[2696]: Server listening on 0.0.0.0 port >
Apr 06 11:29:26 DucAnhB21AT031 sshd[2696]: Server listening on :: port 22.
Apr 06 11:29:26 DucAnhB21AT031 systemd[1]: Started ssh.service - OpenBSD Sec>
lines 1-17/17 (END)

```

Tạo Secure Shell Key trên máy Kali linux:

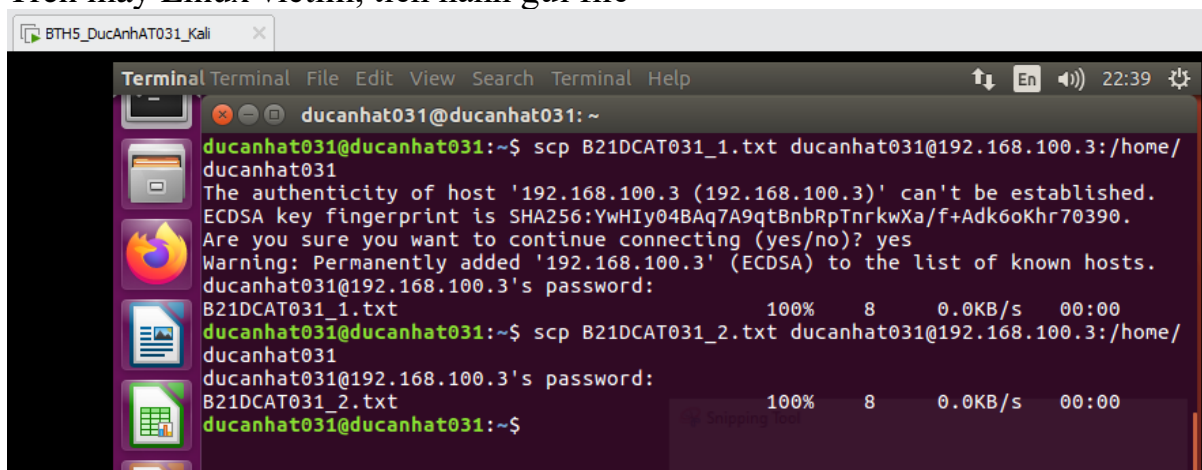
```
(ducanhat031@DucAnhB21AT031)~  
$ ssh-keygen  
Generating public/private ed25519 key pair.  
Enter file in which to save the key (/home/ducanhat031/.ssh/id_ed25519):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/ducanhat031/.ssh/id_ed25519  
Your public key has been saved in /home/ducanhat031/.ssh/id_ed25519.pub  
The key fingerprint is:  
SHA256:KliexcdFi3bSuuv83viiwByXzj86GWJUuWkEaUq03o50 ducanhat031@DucAnhB21AT031  
The key's randomart image is:  
+--[ED25519 256]--+  
|  
| . . . .  
| . . +O.  
| . + = .  
| . oo=B +  
| . o S+ %  
| + o o.. E o  
| . + . . =.+ o  
| . . o.. *+ .  
| . +O====  
+---[SHA256]-----+
```

Trên máy Linux victim, tạo 2 file text lần lượt là B21DCAT031_1.txt và B21DCAT031_2.txt



```
BTH5_DucAnhAT031_Kali  
Terminal  
ducanhat031@ducanhat031: ~  
ducanhat031@ducanhat031:~$ echo ducanh1 > B21DCAT031_1.txt  
ducanhat031@ducanhat031:~$ echo ducanh2 > B21DCAT031_2.txt  
ducanhat031@ducanhat031:~$ ls -l  
total 56  
drwx----- 2 ducanhat031 ducanhat031 4096 Th04 6 22:18 B21DCAT031  
-rw-rw-r-- 1 ducanhat031 ducanhat031 8 Th04 6 22:26 B21DCAT031_1.txt  
-rw-rw-r-- 1 ducanhat031 ducanhat031 8 Th04 6 22:26 B21DCAT031_2.txt  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 14 17:43 Desktop  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Documents  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Downloads  
Firefox Web Browser at031 ducanhat031 8980 Th03 12 13:14 examples.desktop  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Music  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Pictures  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Public  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Templates  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Th03 12 13:18 Videos  
ducanhat031@ducanhat031:~$
```

Trên máy Linux victim, tiến hành gửi file



```
BTH5_DucAnhAT031_Kali  
Terminal  
ducanhat031@ducanhat031: ~  
ducanhat031@ducanhat031:~$ scp B21DCAT031_1.txt ducanhat031@192.168.100.3:/home/  
ducanhat031  
The authenticity of host '192.168.100.3 (192.168.100.3)' can't be established.  
ECDSA key fingerprint is SHA256:YwHIy04BAq7A9qtBnbRpTnrkXa/f+Adk6oKhr70390.  
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.  
ducanhat031@192.168.100.3's password:  
B21DCAT031_1.txt 100% 8 0.0KB/s 00:00  
ducanhat031@ducanhat031:~$ scp B21DCAT031_2.txt ducanhat031@192.168.100.3:/home/  
ducanhat031  
ducanhat031@192.168.100.3's password:  
B21DCAT031_2.txt 100% 8 0.0KB/s 00:00  
ducanhat031@ducanhat031:~$
```


Tiến hành kiểm tra trên máy Kali linux.

```
ducanhat031@DucAnhB21AT031: ~  
File Actions Edit View Help  
  
(ducanhat031@DucAnhB21AT031)-[~]  
$ ls -l  
total 84  
-rw-r--r-- 1 ducanhat031 ducanhat031 8 Apr 6 11:39 B21DCAT031_1.txt  
-rw-r--r-- 1 ducanhat031 ducanhat031 8 Apr 6 11:39 B21DCAT031_2.txt  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Desktop  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Documents  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Downloads  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Music  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Pictures  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Public  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Templates  
drwxr-xr-x 2 ducanhat031 ducanhat031 4096 Mar 7 04:09 Videos  
-rw-r--r-- 1 tcpdump tcpdump 6231 Apr 2 11:51 eth0_NguyenDucAnh031.pcap  
-rw-r--r-- 1 ducanhat031 ducanhat031 19500 Apr 3 07:18 eth0_anhnd031_ftp.pcap  
-rw-r--r-- 1 tcpdump tcpdump 2027 Apr 2 12:19 eth1_NguyenDucAnh.pcap  
-rw-r--r-- 1 tcpdump tcpdump 1768 Apr 2 12:24 eth1_NguyenDucAnh031.pcap  
-rw-r--r-- 1 ducanhat031 ducanhat031 4216 Apr 3 06:53 eth1_anhnd031_ftp.pcap
```

3. Kết quả đạt được

- Học cách sao lưu tới ổ đĩa mạng.
- Sao lưu tệp qua FTP Server
- Chia sẻ file an toàn bằng SCP (Secure Copy)