

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



**Báo cáo thực tập cơ sở
Bài 9: Sao lưu hệ thống**

Giảng viên: Phạm Hoàng Duy

Sinh viên: Nguyễn Kim Bảo

Mã sinh viên: B22DCAT031

Hệ: Đại học chính quy

Hà Nội, 2/2025

1. Mục đích

- Bài thực hành này giúp sinh viên 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

2.1.1 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.
- SCP hoạt động bằng cách thiết lập một kết nối SSH giữa máy chủ cục bộ và máy chủ từ xa. Client SCP sẽ bắt đầu quá trình sao chép ở trong chế độ nguồn (source mode) hoặc chế độ đích (sink mode). Trong chế độ nguồn, client SCP yêu cầu và nhận tệp từ máy chủ từ xa. Còn trong chế độ đích, client báo hiệu cho máy chủ từ xa chuẩn bị nhận và ghi dữ liệu sắp tới. SCP sử dụng thông tin đăng nhập của SSH hoặc khóa công khai để xác thực. Client và server SCP giao tiếp qua một kênh bảo mật, đảm bảo tính bí mật và toàn vẹn của dữ liệu được truyền đi.
- Khi sử dụng client SCP, người dùng có thể bắt đầu quá trình truyền tệp qua câu lệnh SCP đơn giản. Giao thức hỗ trợ cả chế độ nguồn và chế độ đích, cho phép truyền ở cả hai hướng. Trong chế độ nguồn, chương trình SCP đọc tệp để tải, trong khi đó ở chế độ đích, nó xử lý dữ liệu tới từ máy chủ từ xa. Điều này đảm bảo dữ liệu được an toàn trong quá trình truyền
- SCP được sử dụng rộng rãi trong nhiều ngành công nghiệp khác nhau cho việc truyền file an toàn. Một vài trường hợp sử dụng phổ biến như: Truyền tệp giữa máy chủ cục bộ và máy chủ từ xa, truyền tệp giữa hai máy chủ từ xa, đăng tải tệp lên máy chủ web, tải xuống tệp từ máy chủ từ xa, truyền tệp giữa các hệ điều hành khác nhau,... SCP đặc biệt hữu dụng trong trường hợp an toàn là ưu tiên hàng đầu như trong các tổ chức tài chính, các tổ chức chăm sóc sức khỏe và cơ quan chính phủ.

2.1.2 FTP

- File Transfer Protocol (FTP) là một trong những giao thức cổ nhất trên mạng. FTP chạy trong tầng ứng dụng của giao thức TCP/IP. Do đó nó chung tầng với HTTP và POP. Các giao thức này thường được hỗ trợ bởi trình duyệt hoặc ứng dụng email để thực hiện chức năng của chúng. Ngoài ra cũng có các phần mềm chuyên dụng cho FTP
- Giả sử chúng ta muốn tải tệp lên máy chủ hoặc tải tệp xuống bằng FTP. Trong một kết nối FTP, hai kênh sẽ được mở. Đầu tiên, máy khách và máy chủ thiết lập một kênh điều khiển qua TCP cổng 21. Phía máy khách sẽ gửi lệnh tới máy chủ và máy chủ trả lại mã trạng thái. Sau đó cả hai có thể thiết lập một kênh dữ liệu qua TCP cổng 20. Kênh này chuyên dùng để truyền dữ liệu và giao thức giám sát lỗi trong quá trình này. Nếu một kết nối bị ngắt trong quá trình truyền, quá trình có thể tiếp tục sau khi tái thiết lập kết nối.
- Có sự khác biệt giữa FTP chủ động và FTP bị động. Trong phiên bản chủ động, máy khách thiết lập kết nối như đã nói ở trên qua TCP cổng 21 và báo cho máy chủ qua cổng mà máy chủ sẽ dùng để phản hồi. Tuy nhiên nếu tường lửa bảo vệ máy khách, máy chủ sẽ không thể phản hồi bởi tất cả các kết nối từ bên ngoài bị chặn. Vì lý do này, chế độ bị động được phát triển. Trong chế độ này máy chủ công bố một cổng mà máy khách có thể thiết lập kênh truyền dữ liệu. Vì máy khách là bên thiết lập kết nối, tường lửa sẽ không chặn quá trình truyền.
- FTP có nhiều câu lệnh và mã trạng thái khác nhau. Không phải tất cả các câu lệnh đều được thực thi trên máy chủ. Ví dụ, phía máy khách yêu cầu máy phía máy chủ tải lên hoặc tải xuống tệp, sắp xếp thư mục hoặc xóa tệp. Trong các trường hợp trên, máy chủ sẽ phản hồi với mã trạng thái từ đó cho biết câu lệnh được thực thi thành công hay không.
- Thường thì, ta cần thông tin xác thực để sử dụng FTP trên một máy chủ. Chúng ta cũng cần biết rằng FTP là một giao thức truyền bản rõ, đôi khi sẽ bị nghe lén nếu các trạng thái trong mạng được thiết lập đúng. Dù vậy, cũng có khả năng phía máy chủ cho phép sử dụng FTP với người dùng ẩn danh. Máy chủ khi đó sẽ cho phép mọi người dùng có thể đăng tải hoặc tải xuống file qua FTP mà không cần sử dụng mật khẩu. Tuy nhiên, điều này tiềm ẩn nhiều rủi ro bảo mật, nên các quyền truy cập thường bị hạn chế.

2.1.3 Ổ đĩa mạng

- Ổ đĩa mạng là bộ nhớ được chia sẻ trên một máy tính khác trong cùng một mạng, có thể là máy chủ hoặc máy tính cá nhân. Khi một ổ đĩa mạng được ánh xạ, nó sẽ xuất hiện trong File Explorer giống như một ổ đĩa cục bộ.
- Ổ đĩa mạng cho phép lưu trữ tập trung, tức cho phép nhiều người cùng truy cập cùng một dữ liệu mà không cần phải sao chép sang từng máy. Nó cũng có hệ

thông quyền truy cập với hai chế độ chỉ đọc hoặc đọc & ghi. Các quyền này được cấp bởi quản trị viên, quản trị viên có thể giám sát và sao lưu dữ liệu trên ổ đĩa mạng.

2.1.4 Net use

- Lệnh net use được sử dụng để kết nối, ngắt kết nối và quản lý ổ đĩa mạng trên Windows. Nó cho phép ánh xạ một thư mục chia sẻ trên mạng thành một ổ đĩa logic trên máy tính.
- Sử dụng net use để kết nối ổ đĩa mạng:
 - net use K: \\server\share /user:username password
 - K: ký tự ổ đĩa sẽ gán
 - \\server\share: địa chỉ thư mục chia sẻ trên mạng
 - /user:username password: Đăng nhập với tên người dùng và mật khẩu

2.1.5 Net view

- Lệnh net view được sử dụng để xem danh sách các máy tính hoặc tài nguyên chia sẻ trong mạng nội bộ.
- Sử dụng net view để xem danh sách máy tính trong mạng: net view
- Sử dụng net view để xem các thư mục chia sẻ trên một máy cụ thể: net view \\server

2.2 Tài liệu tham khảo

- Lab 8 pfSense firewall của CSSIA CompTIA Security+®
- [What is SCP Protocol? - SFTPCloud](#)
- [Hack The Box - Academy](#)
- [How to use Net Use command to map network drive](#)

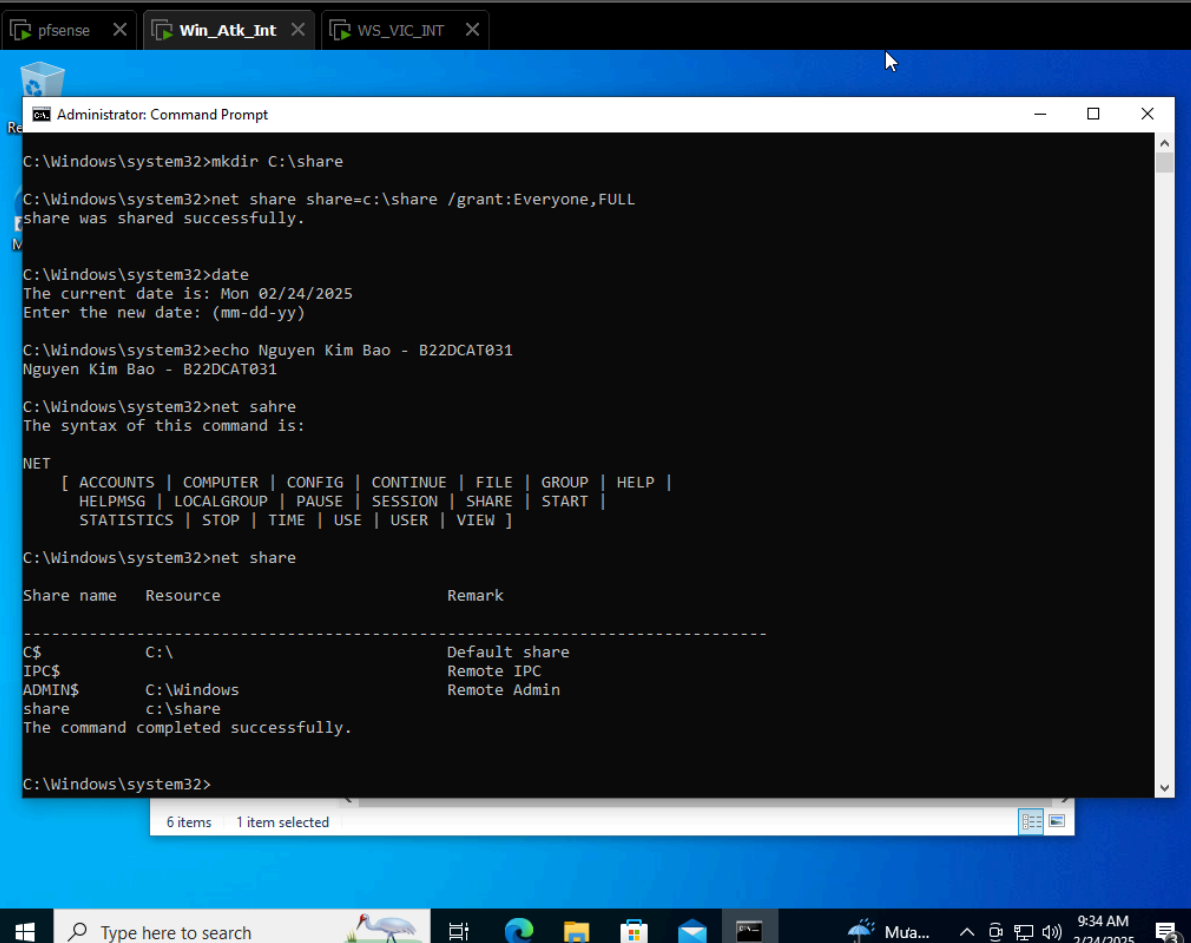
2.3 Chuẩn bị môi trường

- 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.
- Topo mạng như đã cấu hình trong bài 5. Trong bài này chỉ sử dụng các máy trong mạng Internal cho việc sao lưu.

2.4 Các bước thực hiện

2.4.1 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)



The screenshot shows a Windows 10 desktop environment. At the top, there are three browser tabs: 'pfsense', 'Win_Atk_Int', and 'WS_VIC_INT'. The main window is an 'Administrator: Command Prompt' with a black background and white text. The user is logged in as 'system32'. The following commands and their outputs are shown:

```
C:\Windows\system32>mkdir C:\share
C:\Windows\system32>net share share=c:\share /grant:Everyone,FULL
share was shared successfully.
C:\Windows\system32>date
The current date is: Mon 02/24/2025
Enter the new date: (mm-dd-yy)
C:\Windows\system32>echo Nguyen Kim Bao - B22DCAT031
Nguyen Kim Bao - B22DCAT031
C:\Windows\system32>net sahre
The syntax of this command is:
NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]
C:\Windows\system32>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:\Windows\system32>
```

At the bottom of the Command Prompt window, a status bar shows '6 items' and '1 item selected'. The Windows taskbar at the bottom includes the Start button, a search bar, task view, and several application icons. The system tray on the right shows the weather as 'Mưa...' (Rain), the time as '9:34 AM', and the date as '2/24/2025'.

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

```
C:\Users\Administrator>net use Z: \\192.168.100.5\share
Enter the user name for '192.168.100.5': kali
Enter the password for 192.168.100.5:
The command completed successfully.

C:\Users\Administrator>net use
New connections will be remembered.

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

C:\Users\Administrator>date
The current date is: Mon 02/24/2025
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo Nguyen Kim Bao - B22DCAT031
Nguyen Kim Bao - B22DCAT031

C:\Users\Administrator>
```

- Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows, 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
 - Chọn thư mục muốn sao lưu và đặt chính sách sao lưu.

```
C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>$Policy = New-WBPolicy
PS C:\Users\Administrator>$Fileset = New-WBFileSpec -FileSpec "C:\Users\Administrator"
PS C:\Users\Administrator>Add-WBFileSpec -Policy $Policy -FileSpec $Fileset
PS C:\Users\Administrator>
```

```
C:\Users\Admin>date
The current date is: Mon 02/24/2025
Enter the new date: (mm-dd-yy)

C:\Users\Admin>echo Nguyễn Kim Bảo - B22DCAT031
Nguyễn Kim Bảo - B22DCAT031
```

- Đặt thư mục sao lưu đích

```
Win_Atk_Int x WS_VIC_INT x pfsense x
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrator> $BackupLocation = New-WBBackupTarget -NetworkPath "\\192.168.100.5\share"
PS C:\Users\Administrator> Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
WARNING: The backed up data cannot be securely protected at this destination. Backups stored on a remote shared folder might be accessible by other people on the network. You should only save your backups to a location where you trust the other users who have access to the location or on a network that has additional security precautions in place.
WARNING: Backup or recovery of individual files or application data from DVDs or other removable media is not supported. You can only backup or recover full volumes from this media.
type.

Label          :
WBDisk          :
WBVolume        :
Path            : \\192.168.100.5\share
TargetType      : Network
InheritAcl      : True
PreserveExistingBackup : False
```

- Bắt đầu quá trình sao lưu

```
Win_Atk_Int x WS_VIC_INT x pfsense x
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrator> Start-WBBackup -Policy $Policy
Initializing the list of items to be backed up...
The backup operation completed.
PS C:\Users\Administrator> date
Monday, February 24, 2025 11:29:25 AM

PS C:\Users\Administrator> echo Nguyen Kim Bao - B22DCAT031
Nguyen
Kim
Bao
-
B22DCAT031
PS C:\Users\Administrator> dir z:

Directory: Z:\

Mode                LastWriteTime         Length Name
----                -
d-----          2/24/2025   9:36 AM             backup
d-----          2/24/2025  11:29 AM      WindowsImageBackup

PS C:\Users\Administrator>
```

- Minh chứng ở máy Window

```
Win_Atk_Int x WS_VIC_INT x pfsense x
Command Prompt
C:\Users\kali>echo %USERNAME%
NguyenKimBaoB22AT031
C:\Users\kali>date
The current date is: Mon 02/24/2025
Enter the new date: (mm-dd-yy)
C:\Users\kali>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.

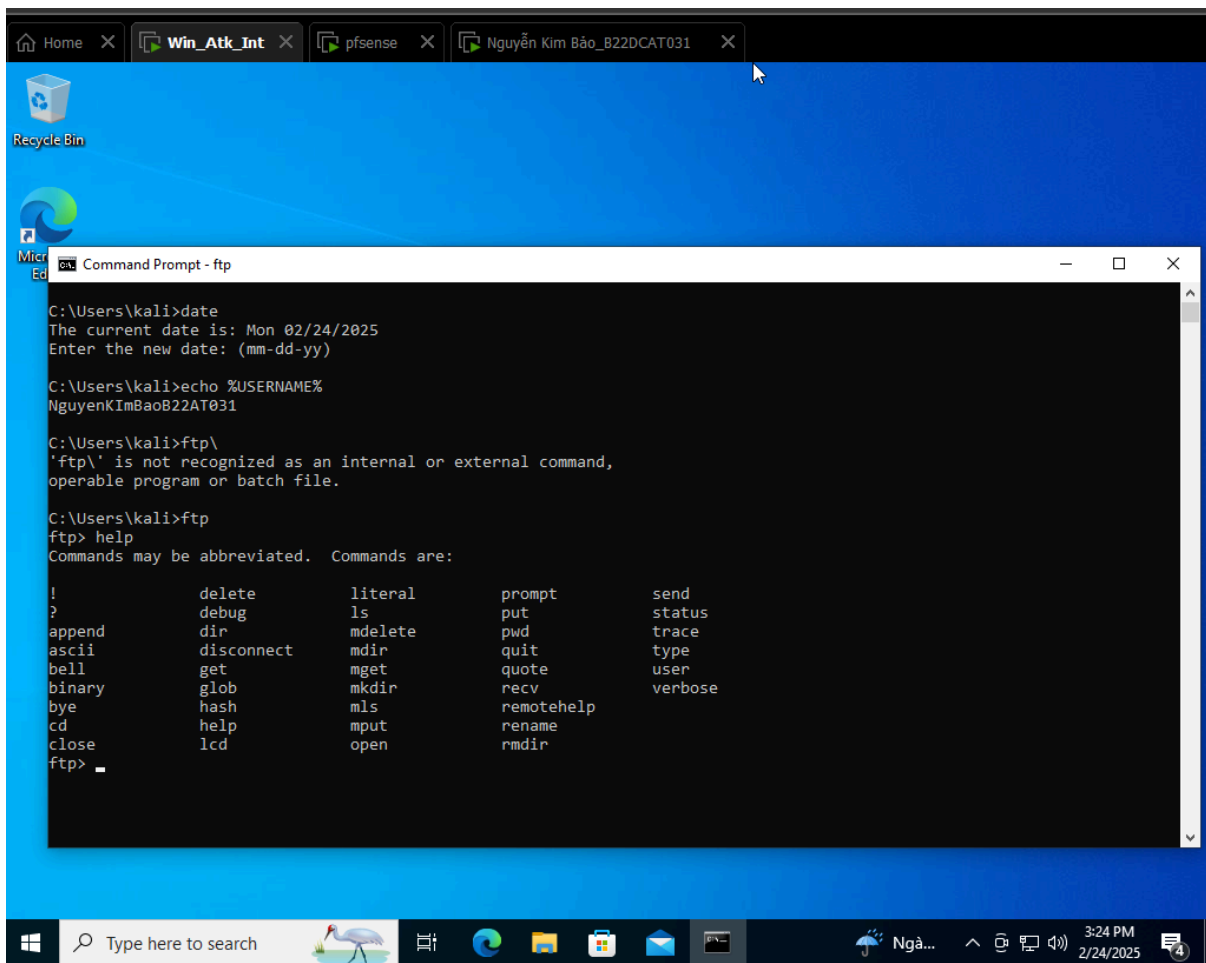
C:\Users\kali>dir c:\share
Volume in drive C has no label.
Volume Serial Number is E66E-F8C1

Directory of c:\share

02/24/2025  11:29 AM    <DIR>      .
02/24/2025  11:29 AM    <DIR>      ..
02/24/2025  09:36 AM    <DIR>      backup
02/24/2025  11:29 AM    <DIR>      WindowsImageBackup
               0 File(s)        0 bytes
               4 Dir(s)  44,053,090,304 bytes free
```

2.4.2 Sao lưu tệp lên FTP server

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



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

```
suffer2@NguyenKimBao-B22DCAT031:~$ sudo apt update && sudo apt install vsftpd -y
[sudo] password for suffer2:
Hit:1 http://vn.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://vn.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [866
kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [196
kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [1
51 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Compone
nts [212 B]
Get:9 http://vn.archive.ubuntu.com/ubuntu noble-updates/univ
[1,015 kB]
Get:10 http://vn.archive.ubuntu.com/ubuntu noble-updates/un
[254 kB]
Get:11 http://vn.archive.ubuntu.com/ubuntu noble-updates/un
[363 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/main
kB]
Get:13 http://vn.archive.ubuntu.com/ubuntu noble-updates/mul
ents [940 B]

C:\Users\Admin>date
The current date is: Mon 02/24/2025
Enter the new date: (mm-dd-yy)

C:\Users\Admin>echo Nguyễn Kim Bảo _ B22DCAT031
Nguyễn Kim Bảo _ B22DCAT031
```

```
suffer2@NguyenKimBao-B22DCAT031:~$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: ena
   Active: active (running) since Mon 2025-02-24 15:39:31 +07; 10s ago
     Process: 2949 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited>
   Main PID: 2951 (vsftpd)
      Tasks: 1 (limit: 2215)
     Memory: 712.0K (peak: 1.5M)
        CPU: 7ms
       CGroup: /system.slice/vsftpd.service
               └─2951 /usr/sbin/vsftpd /etc/vsftpd.conf

Feb 24 15:39:31 NguyenKimBao-B22DCAT031 systemd[1]: Starting vsftpd.service - v
Feb 24 15:39:31 NguyenKimBao-B22DCAT031 systemd[1]: Started vsftpd.service - vs
suffer2@NguyenKimBao-B22DCAT031:~$ date
Mon Feb 24 03:39:47 PM +07 2025
suffer2@NguyenKimBao-B22DCAT031:~$ echo Nguyen Kim Bao _ B22DCAT031
Nguyen Kim Bao _ B22DCAT031
suffer2@NguyenKimBao-B22DCAT031:~$
```

- 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 người dùng mới để sử dụng ftp và tạo thư mục /backup cho người dùng

```
suffer2@NguyenKimBao-B22DCAT031:~$ sudo useradd -m -d /backup -s /bin/bash NguyenKimBao_B22DCAT031
suffer2@NguyenKimBao-B22DCAT031:~$ sudo passwd NguyenKimBao_B22DCAT031
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
suffer2@NguyenKimBao-B22DCAT031:~$ sudo mkdir /backup
mkdir: cannot create directory '/backup': File exists
suffer2@NguyenKimBao-B22DCAT031:~$ sudo chown NguyenKimBao_B22DCAT031 /backup
suffer2@NguyenKimBao-B22DCAT031:~$ sudo chmod 755 /backup
suffer2@NguyenKimBao-B22DCAT031:~$ date
Mon Feb 24 03:42:49 PM +07 2025
suffer2@NguyenKimBao-B22DCAT031:~$ echo Nguyen Kim Bao _ B22DCAT031
Nguyen Kim Bao _ B22DCAT031
suffer2@NguyenKimBao-B22DCAT031:~$
```

- Tiến hành truy cập ftp và sao lưu tệp

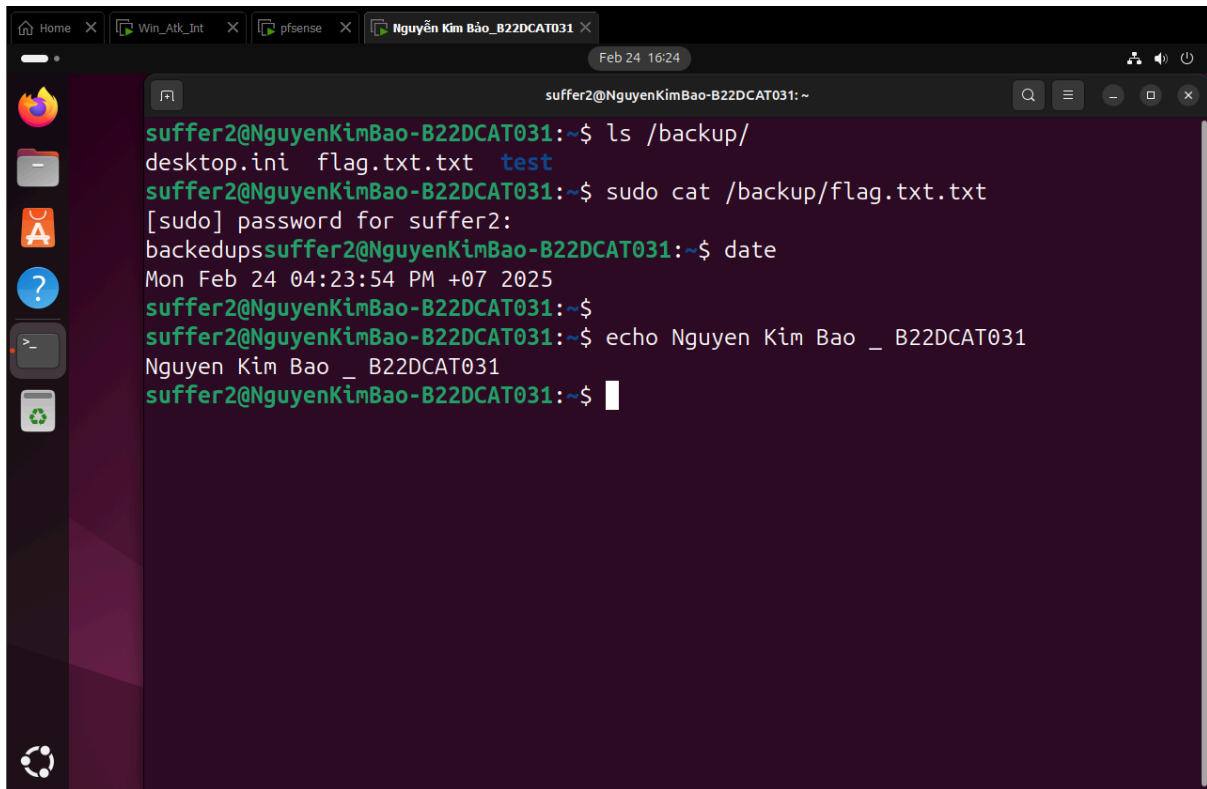
```
C:\Windows\system32>ftp 192.168.100.147
Connected to 192.168.100.147.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
User (192.168.100.147:(none)): NguyenKimBao_B22DCAT031
331 Please specify the password.
Password:
230 Login successful.
ftp> lcd C:\Users\kali\Documents\if you see me, that mean you back me up
Local directory now C:\Users\kali\Documents\if you see me, that mean you back me up.
ftp> mput *
Invalid command.
ftp> mput *
mput flag.txt.txt? y
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 9 bytes sent in 0.00Seconds 9000.00Kbytes/sec.
ftp> bye
221 Goodbye.

C:\Windows\system32>date
The current date is: Mon 02/24/2025
Enter the new date: (mm-dd-yy)

C:\Windows\system32>echo NguyenKimBao_B22DCAT031
NguyenKimBao_B22DCAT031

C:\Windows\system32>
```

- File flag.txt đã được sao lưu thành công sang máy Linux

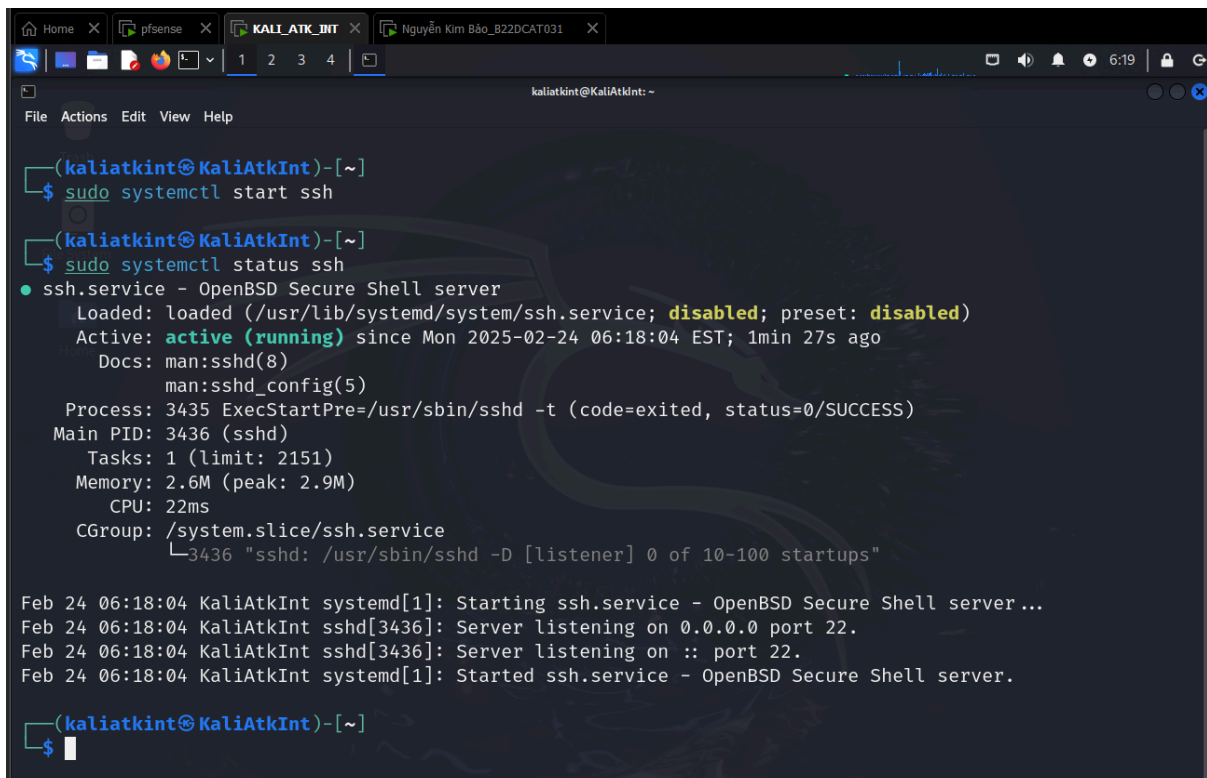


A terminal window titled 'suffer2@NguyenKimBao-B22DCAT031: ~' with a date/time indicator 'Feb 24 16:24'. The terminal shows the following commands and output:

```
suffer2@NguyenKimBao-B22DCAT031:~$ ls /backup/
desktop.ini  flag.txt.txt  test
suffer2@NguyenKimBao-B22DCAT031:~$ sudo cat /backup/flag.txt.txt
[sudo] password for suffer2:
backedupsuffer2@NguyenKimBao-B22DCAT031:~$ date
Mon Feb 24 04:23:54 PM +07 2025
suffer2@NguyenKimBao-B22DCAT031:~$
suffer2@NguyenKimBao-B22DCAT031:~$ echo Nguyen Kim Bao _ B22DCAT031
Nguyen Kim Bao _ B22DCAT031
suffer2@NguyenKimBao-B22DCAT031:~$
```

2.4.3 Sao lưu tệp sử dụng SCP

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



A terminal window titled 'kaliatmint@KaliAtkInt: ~' with a date/time indicator '6:19'. The terminal shows the following commands and output:

```
(kaliatmint@KaliAtkInt)-[~]
$ sudo systemctl start ssh
(kaliatmint@KaliAtkInt)-[~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Mon 2025-02-24 06:18:04 EST; 1min 27s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 3435 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 3436 (sshd)
      Tasks: 1 (limit: 2151)
     Memory: 2.6M (peak: 2.9M)
        CPU: 22ms
    CGroup: /system.slice/ssh.service
            └─3436 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 24 06:18:04 KaliAtkInt systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Feb 24 06:18:04 KaliAtkInt sshd[3436]: Server listening on 0.0.0.0 port 22.
Feb 24 06:18:04 KaliAtkInt sshd[3436]: Server listening on :: port 22.
Feb 24 06:18:04 KaliAtkInt systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(kaliatmint@KaliAtkInt)-[~]
$
```

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

```
kaliatkint@KaliAtkInt: ~  
File Actions Edit View Help  
$ ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa -N ""  
Generating public/private rsa key pair.  
Your identification has been saved in /home/kaliatkint/.ssh/id_rsa  
Your public key has been saved in /home/kaliatkint/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:xZVE0UDvIlrrI/yVoNoORbuLONrifD9K2JzkdZuagaM kaliatkint@KaliAtkInt  
The key's randomart image is:  
+--[RSA 4096]--+  
|             |  
|             |  
|             |  
|             |  
|             |  
|             |  
|             |  
|             |  
|             |  
|             |  
+--[SHA256]--+  
  
(kaliatkint@KaliAtkInt)-[~]  
$ date  
Mon Feb 24 06:26:14 EST 2025  
  
(kaliatkint@KaliAtkInt)-[~]  
$ echo Nguyen Kim Bao - B22DCAT031  
Nguyen Kim Bao - B22DCAT031  
  
(kaliatkint@KaliAtkInt)-[~]
```

```
suffer2@NguyenKimBao-B22DCAT031: ~  
File Actions Edit View Help  
Log Out...  
  
(kaliatkint@KaliAtkInt)-[~]  
$ ssh-copy-id suffer2@192.168.100.147  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kaliatkint/.ssh/id_rsa.pub"  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already  
installed  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install t  
he new keys  
suffer2@192.168.100.147's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'suffer2@192.168.100.147'"  
and check to make sure that only the key(s) you wanted were added.  
  
(kaliatkint@KaliAtkInt)-[~]  
$ ssh suffer2@192.168.100.147  
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.11.0-17-generic x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/pro  
  
Expanded Security Maintenance for Applications is not enabled.  
  
283 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable
```

```
Home X pfsense X KALI_ATK_INT X Nguyễn Kim Bao_B22DCAT031 X
1 2 3 4
suffer2@NguyễnKimBao-B22DCAT031: ~
File Actions Edit View Help

(kaliatkint@KaliAtkInt)-[~]
$ ssh suffer2@192.168.100.147
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.11.0-17-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

283 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Feb 18 22:08:54 2025 from 10.10.19.148
suffer2@NguyễnKimBao-B22DCAT031:~$ whoami
suffer2
suffer2@NguyễnKimBao-B22DCAT031:~$ date
Mon Feb 24 06:27:55 PM +07 2025
suffer2@NguyễnKimBao-B22DCAT031:~$ echo Nguyen Kim Bao _ B22DCAT031
Nguyen Kim Bao _ B22DCAT031
suffer2@NguyễnKimBao-B22DCAT031:~$
```

- 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

```
Home X pfsense X KALI_ATK_INT X KALI_ATK_EXT X Nguyễn Kim Bao_B22DCAT031 X
Feb 24 18:44
suffer2@NguyễnKimBao-B22DCAT031: ~/backup
suffer2@NguyễnKimBao-B22DCAT031:~/backup$ pwd
/home/suffer2/backup
suffer2@NguyễnKimBao-B22DCAT031:~/backup$ ls
flag.txt  thisistestbackupfolder.txt
suffer2@NguyễnKimBao-B22DCAT031:~/backup$ sudo scp /home/suffer2/backup/* kaliat
kint@192.168.100.3:/backup
kaliatkint@192.168.100.3's password:
flag.txt                                100% 14    14.5KB/s   00:00
thisistestbackupfolder.txt              100%  6    12.4KB/s   00:00
suffer2@NguyễnKimBao-B22DCAT031:~/backup$ date
Mon Feb 24 06:44:04 PM +07 2025
suffer2@NguyễnKimBao-B22DCAT031:~/backup$ echo Nguyen Kim Bao _ B22DCAT031
Nguyen Kim Bao _ B22DCAT031
suffer2@NguyễnKimBao-B22DCAT031:~/backup$
```

- Minh chứng

```
(kaliatkint@KaliAtkInt)-[~]  
$ ls ~/.ssh  
id_rsa id_rsa.pub known_hosts known_hosts.old  
  
(kaliatkint@KaliAtkInt)-[~]  
$ ls /backup  
flag.txt thisistestbackupfolder.txt  
  
(kaliatkint@KaliAtkInt)-[~]  
$ date  
Mon Feb 24 06:40:50 EST 2025  
  
(kaliatkint@KaliAtkInt)-[~]  
$ echo Nguyen Kim Bao - B22DCAT031  
Nguyen Kim Bao - B22DCAT031  
  
(kaliatkint@KaliAtkInt)-[~]  
$
```