

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

---



**BÁO CÁO THỰC HÀNH**

**Bài 11: Sao lưu hệ thống**

**Họ và tên: Vũ Thành Long**

**Mã sinh viên: B21DCAT012**

**Nhóm: 06**

**Môn học: Thực tập cơ sở**

**Giảng viên giảng dạy: Nguyễn Hoa Cường**

**Hà Nội, 2024**

# Mục lục

I. Tìm hiểu lý thuyết.....	2
II. Mô tả cài đặt & kết quả .....	3
1. Sao lưu tới ổ đĩa mạng .....	3
2. Sao lưu tệp lên FTP server .....	10
3. Sao lưu tệp sử dụng SCP .....	15
III. Tài liệu tham khảo .....	21

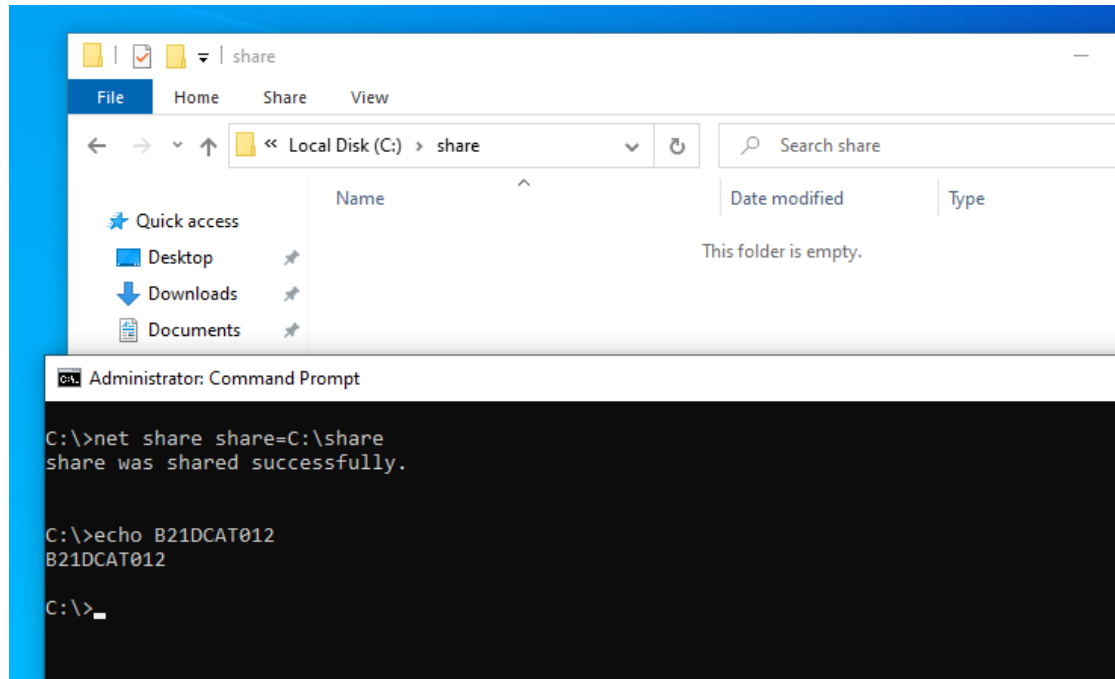
## I. Tìm hiểu lý thuyết:

- Giao thức sao chép an toàn (SCP) là một giao thức mạng để truyền các tệp một cách an toàn giữa máy chủ cục bộ và máy chủ từ xa hoặc giữa hai máy chủ từ xa.
- Theo các nhà phát triển OpenSSH vào tháng 4 năm 2019, SCP đã lỗi thời, không linh hoạt và không dễ sửa chữa; họ khuyến nghị sử dụng các giao thức hiện đại hơn như SFTP và rsync để truyền tệp.
- SCP sử dụng Secure Shell (SSH) để truyền dữ liệu và sử dụng các cơ chế tương tự để xác thực, do đó đảm bảo tính xác thực và tính bảo mật của dữ liệu trong quá trình truyền tải. Máy khách có thể gửi tệp tới máy chủ, đồng thời có thể yêu cầu tải xuống tệp hoặc thư mục từ máy chủ.
- Giao thức truyền tệp (FTP) là một giao thức mạng được sử dụng để truyền tệp từ máy chủ đến máy khách trên mạng máy tính.
- FTP được xây dựng trên kiến trúc mô hình máy khách-máy chủ. Người dùng FTP có thể tự xác thực bằng giao thức đăng nhập văn bản rõ ràng, thường ở dạng tên người dùng và mật khẩu, nhưng có thể kết nối ẩn danh nếu máy chủ được định cấu hình cho phép.
- FTP có thể hoạt động ở hai chế độ là chủ động và thụ động:
  - Ở chế độ chủ động, máy khách chờ (listen) kết nối từ máy chủ, trên cổng M của máy khách. Máy khách gửi máy chủ thông điệp PORT M để máy chủ biết máy khách đang chờ ở cổng nào. Máy chủ sau đó sẽ tạo kết nối từ cổng 20/21 của máy chủ đến cổng M của máy khách.
  - Chế độ thụ động được sử dụng trong trường hợp máy khách nằm sau tường lửa. Máy khách gửi thông điệp PASV đến máy chủ. Máy chủ sau đó gửi địa chỉ IP và cổng FTP đang mở của máy chủ để máy khách tạo kết nối đến máy chủ.
- Mặc định, dữ liệu trên FTP không được mã hoá, bao gồm tên đăng nhập và mật khẩu. Người dùng có thể bật SSL/TLS để mã hoá dữ liệu, tăng cường bảo mật cho quá trình truyền dữ liệu.
- Ổ đĩa mạng là ổ đĩa gắn trên một máy tính kết nối mạng, được thiết lập để người dùng trên cùng mạng có thể truy cập tài nguyên trên đó.
- Ổ đĩa mạng thường được sử dụng trong doanh nghiệp và trường học nhiều hơn là trong hộ gia đình.

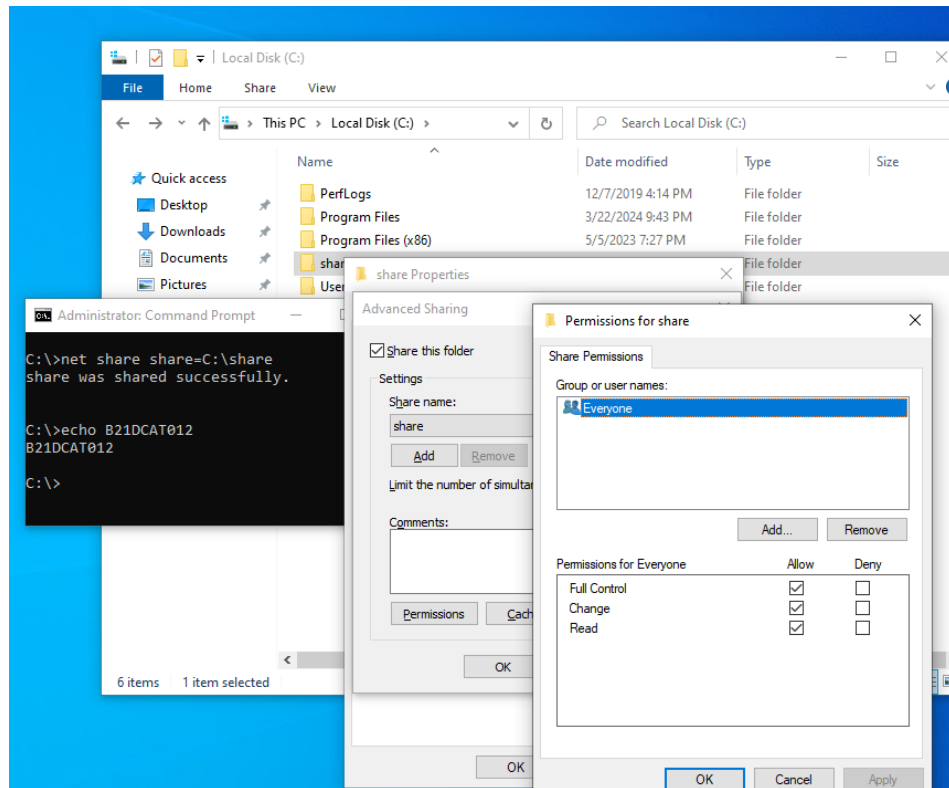
## II. Mô tả cài đặt & kết quả:

### 1. Sao lưu tới ổ đĩa mạng:

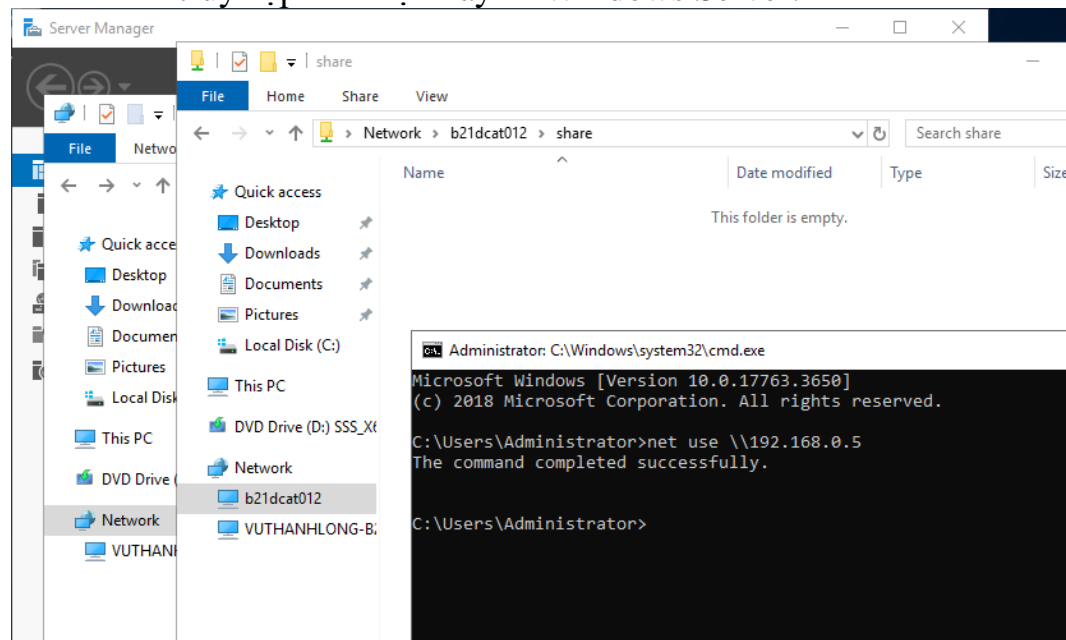
- Sinh viên chạy lệnh **net share share=C:\share** để tạo thư mục chia sẻ mới trên Windows 10 attack.



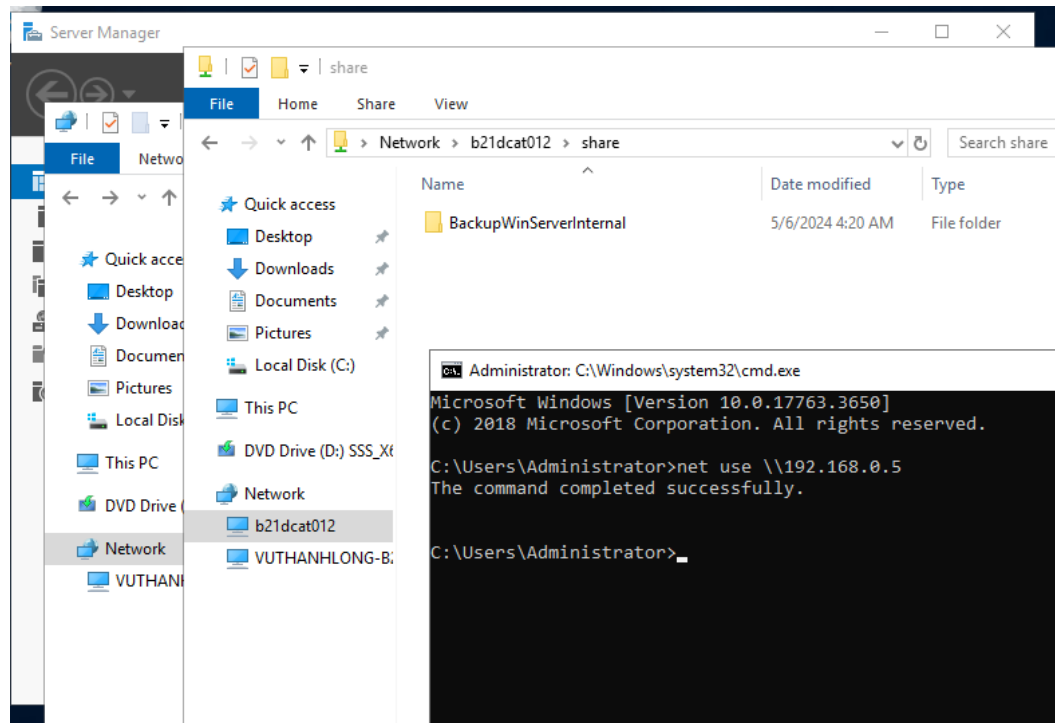
- Tiếp theo, sinh viên đặt quyền chỉnh sửa nội dung thư mục với tất cả người dùng.



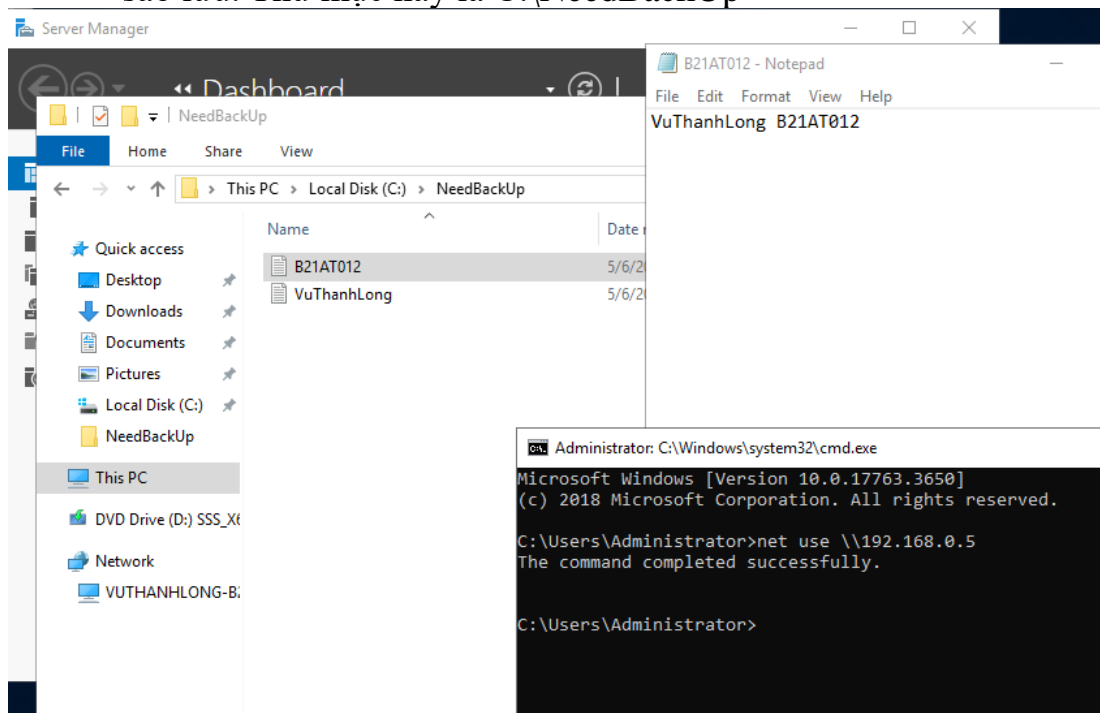
– Thử truy cập thư mục này từ Windows Server:



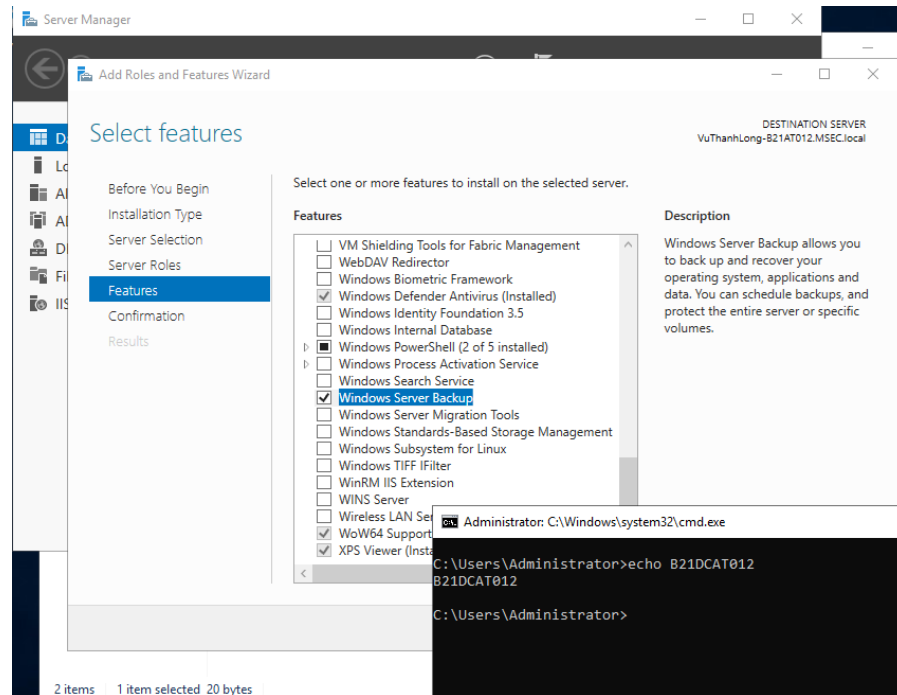
– Tại đây, sinh viên tạo một thư mục mới để chứa dữ liệu sắp sao lưu. Thư mục có tên BackupWinServerInternal.



- Tiếp theo, sinh viên tạo một thư mục chứa một số tệp cần được sao lưu. Thư mục này là C:\NeedBackUp



- Tiếp theo sinh viên bật tính năng Windows Server Backup ở Server Manager.



- Tiếp theo sinh viên thực hiện sao lưu. Thay vì sử dụng ntbackup, sinh viên sử dụng wadmin theo hướng dẫn của Microsoft.
- Sinh viên mở Command Prompt với quyền quản trị viên và chạy lệnh **wadmin start backup**
  - backupTarget:\\b21dcat012\share\BackupWinServerInternal**
  - include:C:\NeedBackUp**
- Nội dung lệnh có nghĩa là "Chạy sao lưu thư mục NeedBackUp với đích là thư mục BackupWinServerInternal.

```
Administrator: Command Prompt

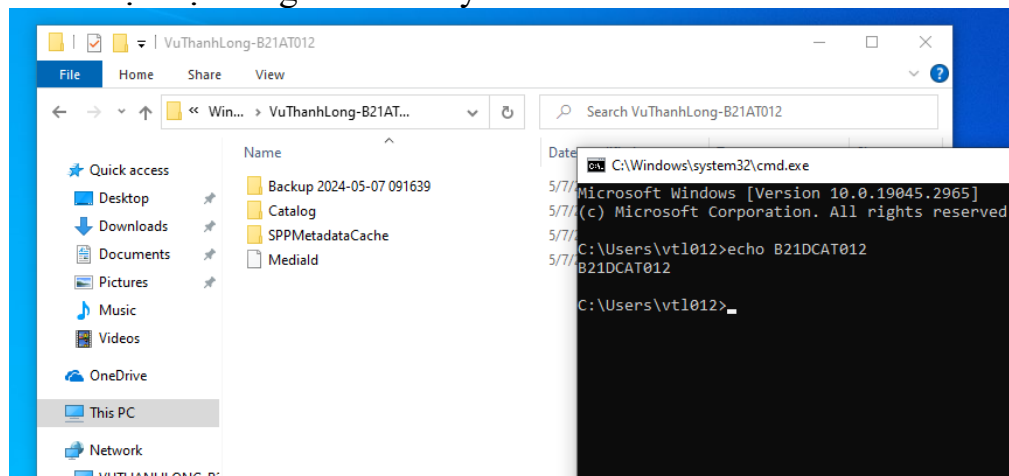
Note: The backed up data cannot be securely protected at this destination.
Backups stored on a remote shared folder might be accessible by other
people on the network. You should only save your backups to a location
where you trust the other users who have access to the location or on a
network that has additional security precautions in place.

Retrieving volume information...
This will back up (C:) (Selected Files) to \\b21dcat012\share\BackupWinServerInternal.
Do you want to start the backup operation?
[Y] Yes [N] No y

The backup operation to \\b21dcat012\share\BackupWinServerInternal is starting.
Creating a shadow copy of the volumes specified for backup...
Please wait while files to backup for volume (C:) are identified.
This might take several minutes.
Creating a shadow copy of the volumes specified for backup...
Please wait while files to backup for volume (C:) are identified.
This might take several minutes.
The backup of volume (C:) completed successfully.
Summary of the backup operation:
-----
The backup operation successfully completed.
The backup of volume (C:) completed successfully.
Log of files successfully backed up:
C:\Windows\Logs\WindowsServerBackup\Backup-07-05-2024_09-16-39.log

C:\Users\Administrator>
```

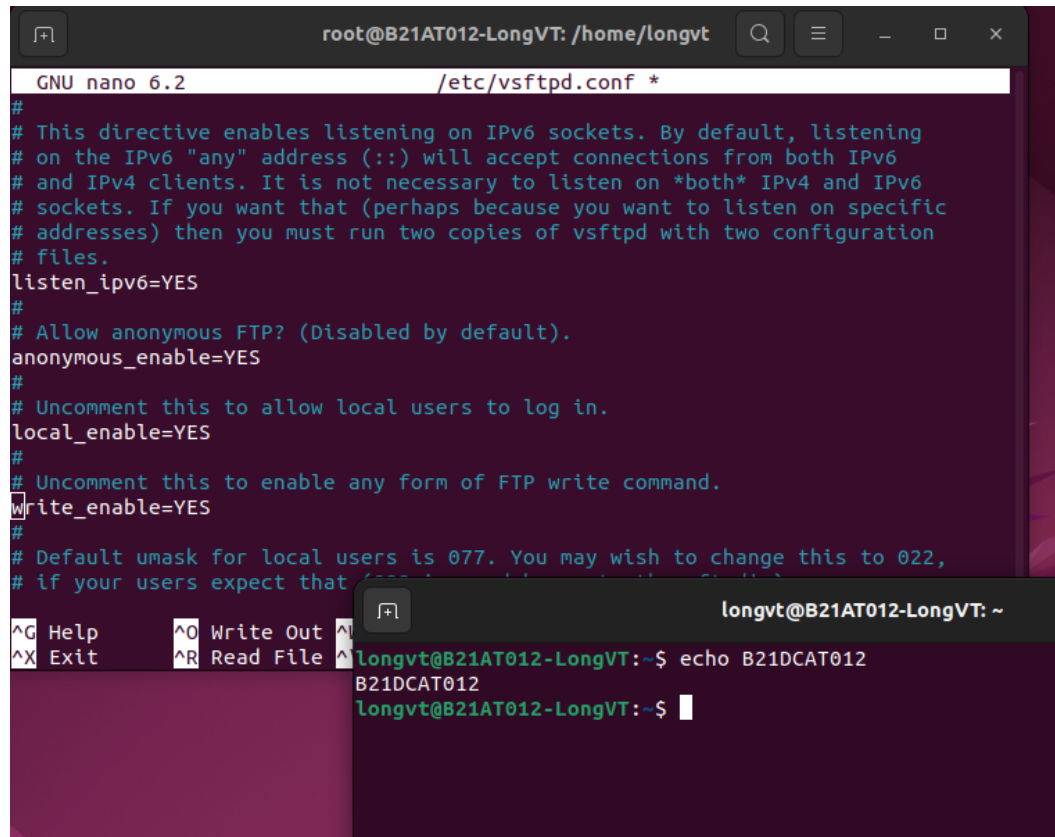
- Kết quả sao lưu thành công, từ Windows 10 có thể truy cập được nội dung sao lưu này.



## 2. Sao lưu tệp lên FTP server:

- Sinh viên khởi động dịch vụ FTP là vsftpd trên máy Ubuntu victim bằng lệnh **sudo systemctl start vsftpd** và **sudo systemctl enable vsftpd**.
- Tiếp theo, sinh viên chỉnh sửa nội dung tệp vsftpd.conf bật chế độ **write\_enable=YES** để cho phép FTP client tải lên các tệp mới.



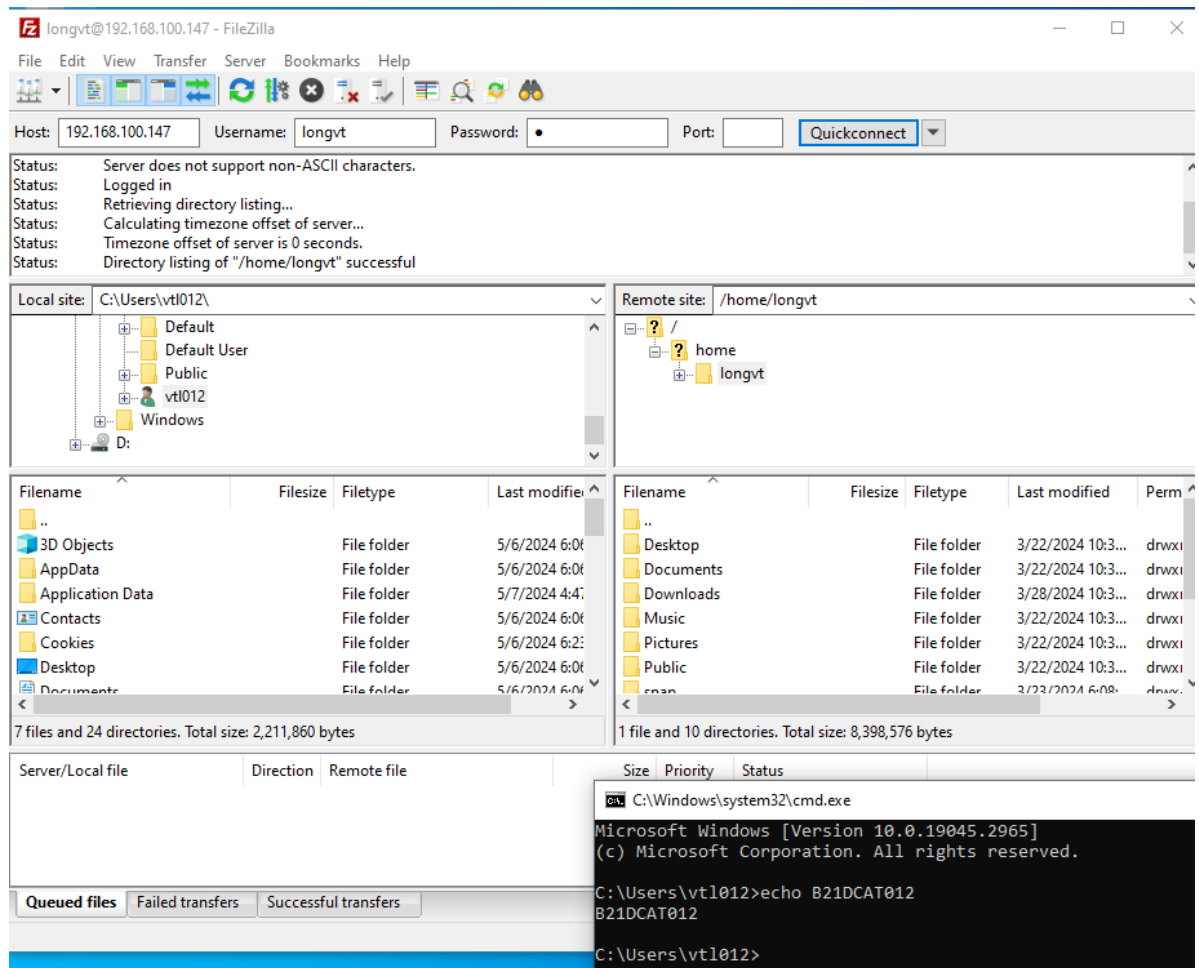


The screenshot shows a terminal window with two panes. The top pane is a nano editor editing `/etc/vsftpd.conf`. The configuration includes enabling IPv6 listening, anonymous FTP, local users, and write commands. The bottom pane shows a terminal session where the command `echo B21DCAT012` is executed, resulting in the output `B21DCAT012`.

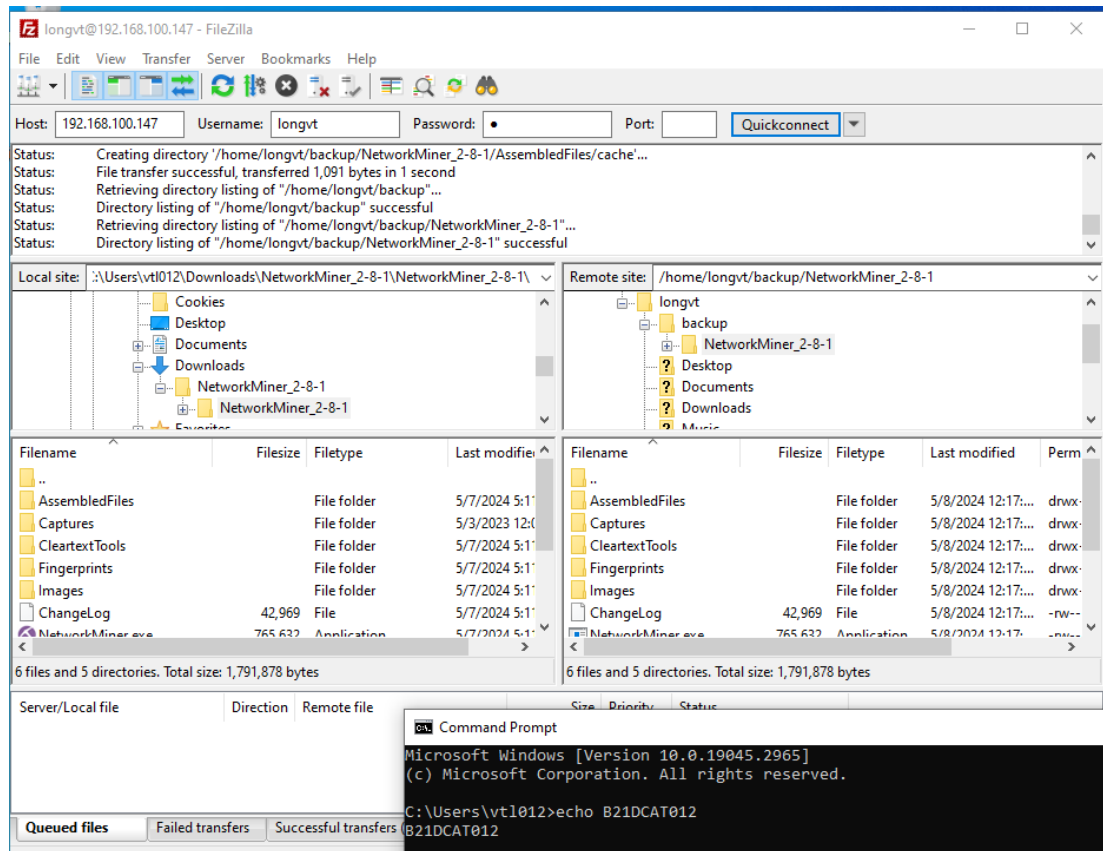
```
root@B21AT012-LongVT: /home/longvt
GNU nano 6.2 /etc/vsftpd.conf *
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (for example, via tar).
#
^G Help      ^O Write Out ^V
^X Exit      ^R Read File ^_

longvt@B21AT012-LongVT: ~
longvt@B21AT012-LongVT:~$ echo B21DCAT012
B21DCAT012
longvt@B21AT012-LongVT:~$
```

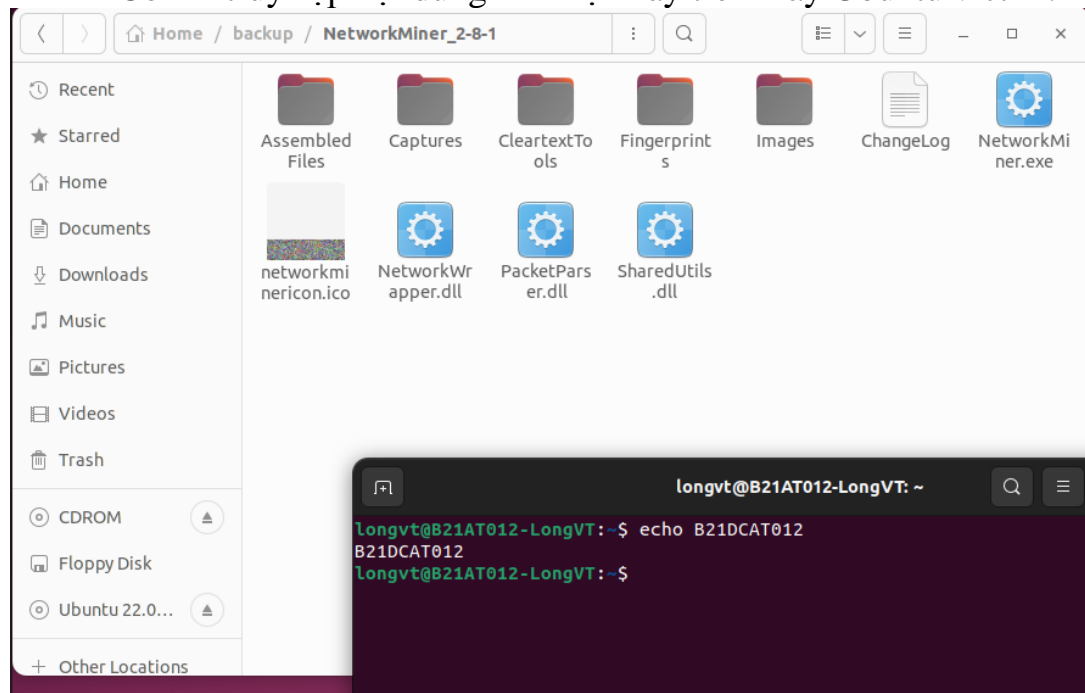
- Chạy FTP client trên Windows 7 attack, trong ví dụ là FileZilla. Chọn host là 192.168.100.147, tên đăng nhập và mật khẩu của một người dùng của Ubuntu victim. Cổng 21 và bấm Quickconnect.
- Riêng với phần bài này, vì tải tệp vào /backup cần quyền quản trị viên nên thay vào đó sinh viên sẽ tạo thư mục ~/backup.



- Sao chép thư mục NetworkMiner từ Windows 10 attack vào thư mục backup của Ubuntu Victim.



– Có thể truy cập nội dung thư mục này trên máy Ubuntu victim.



3. Sao lưu tệp sử dụng SCP:

- Để tạo Secure Shell Key mới, sinh viên chạy lệnh **ssh-keygen**.

```
kali@B21AT012-LongVT-Kali-Internal: ~  
File Actions Edit View Help  
  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$ echo B21DCAT012  
B21DCAT012  
  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$ ssh-keygen  
Generating public/private ed25519 key pair.  
Enter file in which to save the key (/home/kali/.ssh/id_ed25519):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/kali/.ssh/id_ed25519  
Your public key has been saved in /home/kali/.ssh/id_ed25519.pub  
The key fingerprint is:  
SHA256:mLWD8oMQ09GEPVzOD49p4cFNvtg9ZrWMSrNKVe7yKlo kali@B21AT012-LongVT-Kali-Internal  
The key's randomart image is:  
+--[ED25519 256]--+  
|  o..B...  .  
| oo = +  
| . . ..X O. .  
| . + o %ooo..  
| . S *O=O=O  
| + O. +O .  
| O E + .  
| O. =  
| ... oo..  
+---[SHA256]-----+  
  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$
```

- Thư mục mặc định chứa key là  
/ home/kali/.ssh

```
kali@B21AT012-LongVT-Kali-Internal: ~  
File Actions Edit View Help  
  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$ echo B21DCAT012  
B21DCAT012  
  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$ ls /home/kali/.ssh  
id_ed25519 id_ed25519.pub known_hosts known_hosts.old  
  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$
```

- Trên máy Ubuntu victim, tạo một tệp cần sao lưu là /home/longvt /Documents/B21AT012-LongVT- Backup. Trên máy Kali Internal, tạo thư mục /backup.
- Sinh viên khởi tạo máy chủ SSH trên Kali Internal sau đó chạy lệnh ssh [kali@192.168.100.3](mailto:kali@192.168.100.3) để truy cập máy Kali Internal.

```

longvt@B21AT012-LongVT: ~/Documents
longvt@B21AT012-LongVT:~/Documents$ ls
B21AT012-LongVT-Backup
longvt@B21AT012-LongVT:~/Documents$

```

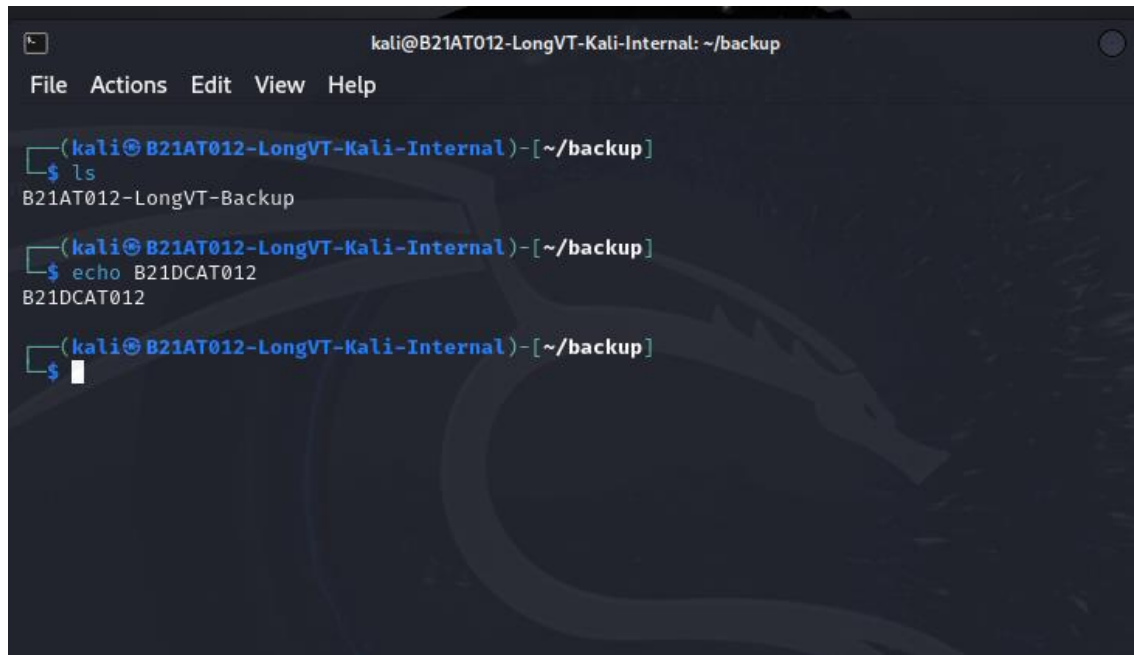
- Tiếp theo, sinh viên chạy lệnh **sudo scp copy** [longvt@192.168.100.147:/home/longvt/Documents/B21AT012-LongVT-Backup](mailto:longvt@192.168.100.147:/home/longvt/Documents/B21AT012-LongVT-Backup) /home/kali/backup để sao chép. Cấu trúc lệnh là scp copy <người dùng@máy nguồn><địa chỉ tệp tin> <địa chỉ thư mục đích>.
- Lần này sinh viên có thể sao lưu ra thư mục root nhờ dùng lệnh sudo.

```

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ sudo scp copy longvt@192.168.100.147:/home/longvt/Documents/B21AT012-LongVT-Backup /home/kali/backup
sudo: unable to resolve host B21AT012-LongVT-Kali-Internal: Temporary failure in name resolution
cp: cannot stat 'copy': No such file or directory
longvt@192.168.100.147's password:
B21AT012-LongVT-Backup                                100%  11    3.2KB/s   00:00
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$

```

- Trên máy Kali Internal có thể xem được tệp tin vừa được sao lưu.



The image shows a terminal window with a dark background and a faint dragon logo. The window title is 'kali@B21AT012-LongVT-Kali-Internal: ~/backup'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows three commands being executed in sequence: 'ls' which outputs 'B21AT012-LongVT-Backup', 'echo B21DCAT012' which outputs 'B21DCAT012', and a third command line with a cursor at the end.

```
kali@B21AT012-LongVT-Kali-Internal: ~/backup
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal) - [~/backup]
$ ls
B21AT012-LongVT-Backup

(kali@B21AT012-LongVT-Kali-Internal) - [~/backup]
$ echo B21DCAT012
B21DCAT012

(kali@B21AT012-LongVT-Kali-Internal) - [~/backup]
$
```

### III. Tài liệu tham khảo:

- wadmin Documentation: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin>
- Secure Shell Key: <https://www.geeksforgeeks.org/introduction-to-sshsecure-shell-keys/>