MỤC LỤC

1. [Tìm hiểu lý thuyết 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark0)
   1. [SCP 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark1)
   2. [FTP 2](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark2)
   3. [Ổ đĩa mạng 4](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark3)
   4. [Net use 5](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark4)
   5. [Net view 6](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark5)
2. [Nội dung thực hành 7](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark6)
   1. [Sao lưu tới ổđĩa mạng 8](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark7)
   2. [Sao lưu tệp lên FTP Server 16](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark8)
   3. [Sao lưu tệp sử dụng SCP 19](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark9)
3. [Tài liệu tham khảo 22](file:///C:\Users\Acer\Downloads\Bài-thực-hành-10_Nguyễn-Huy-Quang_B20DCAT144.docx#_bookmark10)

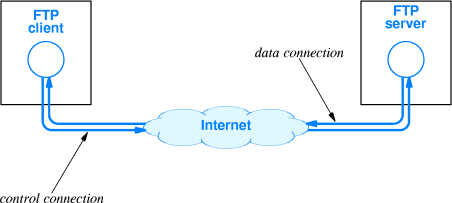
### Tìm hiểu lý thuyết

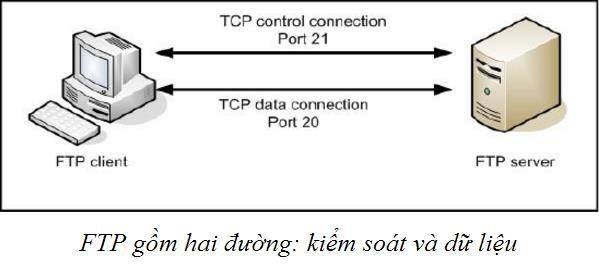
### SCP

* + - SCP (Secure copy) là một giao thức truyền file, giúp chuyển các file máy tính một cách an toàn từ máy chủ cục bộ sang máy chủ từ xa. Nó hoạt động trên kỹ thuật giao thức Secure Shell (SSH).
    - Giao thức SCP là một giao thức mạng truyền file, hỗ trợ các tính năng mã hóa và xác thực. Nó dựa trên giao thức sao chép từ xa của Berkeley Software Distribution (BSD) (RCP – Remote Copy Protocol), chạy trên cổng 22 sử dụng giao thức SSH.
    - SCP có thể được gọi là sự kết hợp của RCP và SSH hơn là một giao thức vì quá trình truyền file được thực hiện bằng RCP và xác thực và mã hóa được cung cấp bởi Giao thức SSH.
    - SCP duy trì tính bí mật của dữ liệu được chuyển và bảo vệ tính xác thực bằng cách chặn những kẻ đánh cắp gói trích xuất thông tin có giá trị từ các gói dữ liệu.
    - Giao thức SSH hỗ trợ bao gồm các thuộc tính cơ bản như quyền và dấu thời gian cho file được tải lên. Trong khi đó, FTP phổ biến không hỗ trợ việc bao gồm thuộc tính ngày / dấu thời gian.
    - Máy khách cung cấp cho máy chủ tất cả các file sẽ được tải lên. Một yêu cầu tải xuống các file và thư mục được gửi bởi máy khách.
    - Máy chủ cung cấp cho máy khách tất cả các thư mục con và file có sẵn để tải xuống. Vì quá trình tải xuống được kiểm soát bởi máy chủ, nên có nhiều rủi ro về bảo mật khi được kết nối với một máy chủ độc hại.
    - Mặt khác, chương trình SCP thực hiện giao thức SCP như một ứng dụng khách hoặc một daemon dịch vụ. Chương trình máy chủ SCP và máy khách SCP là một và giống nhau. Một ví dụ điển hình của chương trình SCP là chương trình SCP dòng lệnh có sẵn với hầu hết các triển khai SSH.

### FTP

* + - FTP (File Transfer Protocol): Giao thức truyền tải tập tin được dùng trong việc trao đổi dữ liệu mạng thông qua giao thức TCP/IP, thường hoạt động trên cổng 20 và 21. Với giao thức này, các máy client trong mạng có thể truy cập vào máy chủ FTP để truyền và nhận dữ liệu dù ở xa.



* + - Mô hình hoạt động của giao thức FTP:
      * Giao thức FTP hoạt động dựa trên mô hình cơ bản của việc truyền và nhận dữ liệu từ máy Client đến máy Server. Quá trình truyền nhận giữa máy Client và máy Server lại được tạo từ hai tiến trình TCP Logic là Control Connection và Data Connection.
      * Control Connection: Đây là phiên làm việc TCP logic đầu tiên được tạo ra khi quá trình truyền dữ liệu bắt đầu. Tuy nhiên, tiến trình này chỉ kiểm soát các thông tin điều khiển đi qua nó, ví dụ như các tập lệnh. Quá trình này sẽ được duy trì trong suốt quá trình phiên làm việc diễn ra.
      * Data Connection: Khác với tiến trình Control Connection, Data Connection là một kết nối dữ liệu TCP được tạo ra với mục đích chuyên

biệt là truyền tải dữ liệu giữa máy Client và máy Server. Kết nối sẽ tự động ngắt khi quá trình truyền tải dữ liệu hoàn tất.

* + - Các phương thức truyền dữ liệu trong giao thức FTP: FTP có 3 phương thức truyền tải dữ liệu là stream mode, block mode, và compressed mode.
      * Stream mode: Phương thức này hoạt động dựa vào tính tin cậy trong việc truyền dữ liệu trên giao thức TCP. Dữ liệu sẽ được truyền đi dưới dạng các byte có cấu trúc không liên tiếp. Thiết bị gửi chỉ đơn thuần đẩy luồng dữ liệu qua kết nối TCP tới phía nhận mà không có một trường tiêu đề nhất định.
      * Block mode: Là phương thức truyền dữ liệu mang tính quy chuẩn hơn. Với phương thức này, dữ liệu được chia thành nhiều khối nhỏ và được đóng gói thành các FTP blocks. Mỗi block sẽ chứa thông tin về khối dữ liệu đang đượcgửi.
      * Compressed mode: Phương thức truyền sử dụng kỹ thuật nén dữ liệu khá đơn giản là “run-length encoding”. Với thuật toán này, các đoạn dữ liệu bị lặp sẽ được phát hiện và loại bỏ để giảm chiều dài của toàn bộ thông điệp khi gửi đi.

### Ổ đĩa mạng

* + - Đây là một tên gọi khác của thiết bị lưu trữ kết nối mạng với tên gọi chuyên ngành là Network Attached Storage (NAS).
    - Không chỉ dành riêng cho các văn phòng quy mô lớn, công nghệ hiện đại đã cho ra đời các ổ đĩa cứng nhỏ gọn, giá cả phải chăng giúp người dùng sao lưu tự động và chia sẻ lưu trữ cho mạng Internet gia đình.
    - Dù là ổ đĩa cứng mạng hay NAS đều sẽ được trang bị bộ xử lý tích hợp, hệ điều hành và nhiều ổ đĩa cứng. Đồng thời phải có khoang trống hay cổng giao tiếp để thực hiện nâng cấp dung lượng, nên thiết bị này thích hợp cho việc lưu trữ, chia sẻ tập tin.
    - Ổ đĩa mạng được kết nối trực tiếp vào mạng bằng cáp ethernet mà không cần phải thông qua PC, đĩa cứng mạng và các thiết bị NAS nhằm hạn chế tối đa về lỗi bảo mật.
    - Bên cạnh đó, vì không cần sử dụng thiết bị chủ hay PC, nên thiết bị không lệ thuộc vào năng lực làm việc của bộ xử lý. Cũng chính vì thế, các văn phòng nhỏ thường là người dùng chủ yếu của NAS.
    - Hạn chế lớn nhất của NAS chính là tốc độ. Theo một khảo sát, Tốc độ truyền tải trên mạng (trong khoảng 11 đến 100 Mb/giây) chậm hơn nhiều lần tốc độ truyền tải của ổ đĩa cứng gắn trong lẫn gắn ngoài (đạt 480 Mb/giây với giao tiếp USB 2.0).
    - Đa phần thiết bị NAS hiện nay vẫn đủ nhanh để các nhóm làm việc nhỏ thực hiện yêu cầu sao lưu và chia sẻ máy tính. Và hầu hết các thiết bị NAS có thể hỗ trợ máy tính hoạt động trên hệ điều hành Windows và Mac, riêng đối với

Linux vẫn còn tồn tại nhiều hạn chế.

### Net use

* + - Lệnh net use là lệnh Command Prompt được sử dụng để kết nối, xóa và cấu hình kết nối với các tài nguyên được chia sẻ, chẳng hạn như ổ đĩa được ánh xạ và máy inmạng.
    - Tính khả dụng của net use: Lệnh này có sẵn trong Command Prompt trên Windows 10, Windows 8, Windows 7, Windows Vista và Windows XP, cũng như trong các phiên bản Windows cũ hơn và trong hệ điều hành Windows Server.
    - Cú pháp lệnh net use chung:

net use [{devicename | \*}] [\\computername\sharename[\volume] [{password | \*}]] [/user:[domainname\]username] [/user:[dotteddomainname\]username] [/user:[username@dotteddomainname] [/home {devicename | \*} [{password | \*}]] [/persistent:{yes | no}] [/smartcard] [/savecred] [/delete] [/help] [/?]

* + - Các option trong net use:

|  |  |
| --- | --- |
| **Tùy chọn** | **Mô tả** |
| net use | Chỉ thực thi lệnh net use để hiển thị thông tin chi tiết về  các ổ đĩa và thiết bị hiện được ánh xạ. |
| device name | Sử dụng tùy chọn này để chỉ định ký tự ổ hoặc cổng  máy in mà người dùng muốn ánh xạ tài nguyên mạng |
| \\ computername \ sharename | Điều này chỉ định tên của máy tính, computername, và tài nguyên được chia sẻ, sharename, như một thư mục được chia sẻ hoặc một máy in dùng chung được kết nối  với computername. |
| volumn | Sử dụng tùy chọn này để chỉ định volume khi kết nối  với NetWare server. Client Service for NetWare hoặc Gateway Service for Netware phải được cài đặt. |
| password | Đây là mật khẩu cần thiết để truy cập tài nguyên được  chia sẻ trên computername |
| /user | Sử dụng tùy chọn lệnh net này để chỉ định một  username để kết nối với tài nguyên. |
| domainname | Chỉ định một domain khác với domain người dùng  đang sử dụng |

|  |  |
| --- | --- |
| username | Sử dụng tùy chọn này với /user để chỉ định tên người  dùng sẽ sử dụng để kết nối với tài nguyên được chia sẻ. |
| dotteddomainname | Tùy chọn này chỉ định domain đủ điều kiện nơi  username đang tồn tại. |
| /home | Tùy chọn lệnh net use này ánh xạ thư mục chính của người dùng hiện tại thành ký tự ổ devicename hoặc ký  tự ổ có sẵn tiếp theo với \*. |
| /persistent | Sử dụng tùy chọn này để kiểm soát độ ổn định của các  kết nối được tạo bằng lệnh net use |
| /smartcard | Switch này cho lệnh net use sử dụng thông tin đăng  nhập có trên smart card có sẵn |
| /savecred | Tùy chọn này lưu trữ password và thông tin user để sử  dụng vào lần tiếp theo |
| /delete | Lệnh net use này được sử dụng để hủy kết nối mạng |
| /help | Để hiển thị thông tin trợ giúp chi tiết cho lệnh net use. |
| /? | Hiển thị cú pháp lệnh |

### Net view

* + - Hiển thị danh sách miền, máy tính hoặc tài nguyên đang được chia sẻ bởi máy tính được chỉ định. Được sử dụng mà không có tham số, chế độ xem net hiển thị danh sách các máy tính trong miền hiện tại của người dùng
    - Các phiên bản áp dụng: Windows Server 2003, Windows Vista, Windows XP, Windows Server 2008, Windows 7, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2000, Windows Server 2012, Windows 8 .
    - Cú pháp:

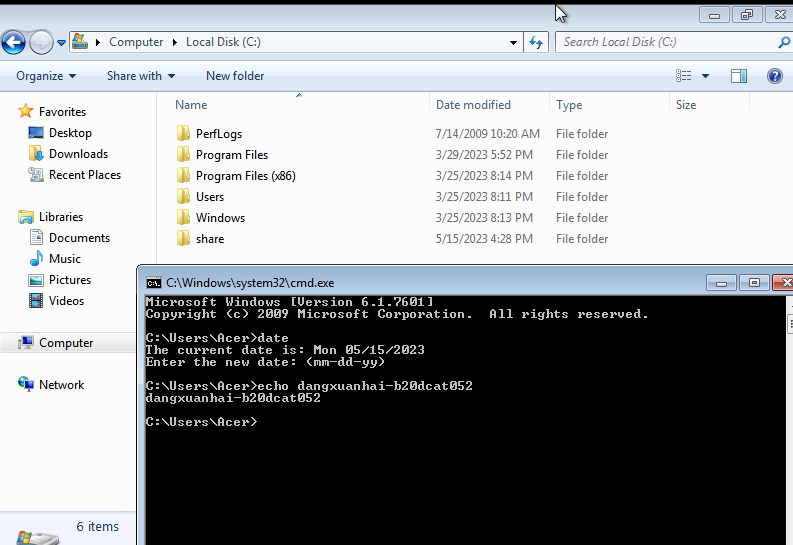
net view [\\ComputerName [/CACHE] | [/ALL] | /DOMAIN[:DomainName]] Trong đó, các tham số có ý nghĩa như sau:

|  |  |
| --- | --- |
| Tham số | Mô tả |
| \\ComputerName | Chỉ định máy tính có chứa các tài nguyên được  chia sẻ mà người dùng muốn xem |
| /CACHE | Hiển thị cài đặt bộ đệm ẩn máy khách ngoại tuyến  cho các tài nguyên trên máy tính được chỉ định. |
| /ALL | Hiển thị tất cả các chia sẻ chứa ký tự $ |
| /domain[:DomainName] | Chỉ định miền mà người dùng muốn xem các máy  tính khả dụng. Nếu người dùng bỏ qua DomainName, / domain sẽ hiển thị tất cả các miền trong mạng. |

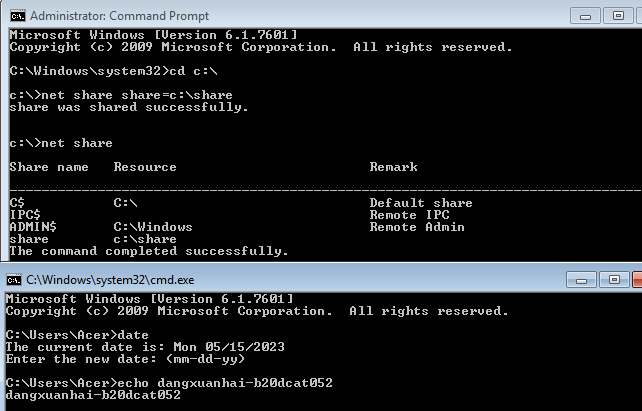
# Nội dung thực hành

* 1. **Sao lưu tới ổ đĩa mạng**

## Trên máy trạm Windows attack trong mạng Internal, tạo thư mục share



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



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

• Dùng câu lệnh net use để kiểm tra lại

A picture containing text, screenshot, font, software

Description automatically generated

A picture containing text, screenshot, software, font

Description automatically generated

• Trên máy Windows server Internal, có thể thấy được ổ đĩa mạng đã được chia sẻ

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated with medium confidence

• Mở các quyền với thư mục share

A screenshot of a computer

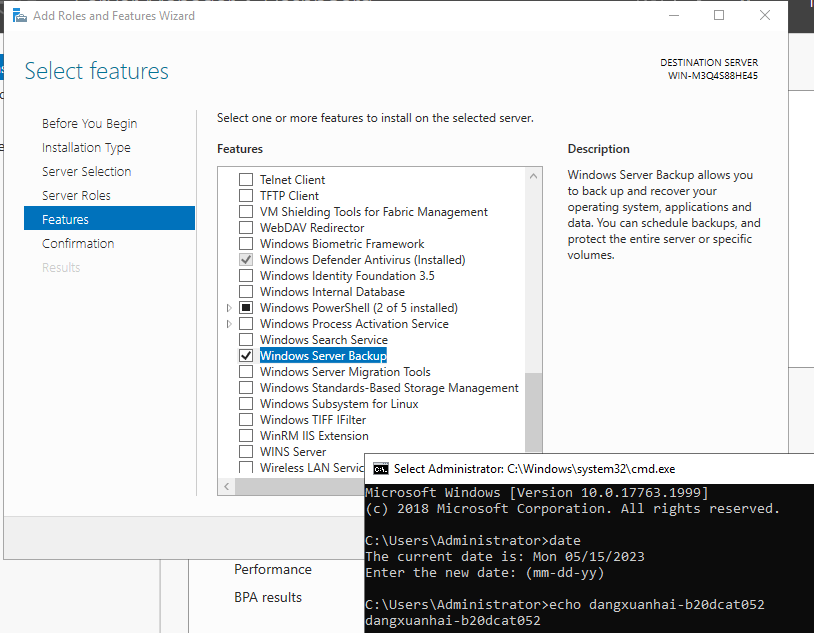
Description automatically generated

* Quay lại tạo thư mục trong Z, hệ thống đã cho tạo thư mục bên trong do ta đã cấp quyền Full Control

A screenshot of a computer

Description automatically generated

Sao lưu hệ thống bằng chương trình sao lưu của Windows Server + Mở Server Manager => Add Role and Features => Windows Server Backup



A screenshot of a computer

Description automatically generated with medium confidence

+ Tool -> Windows Server Backup => Chuột phải Local Backup chọn

Backup Once

A screenshot of a computer

Description automatically generated

+ Chọn Different Option

A screenshot of a computer

Description automatically generated

+ Chọn Custom

A screenshot of a computer

Description automatically generated

+ Tạo một thư Backup trong This PC để tiến hành Backup

A screenshot of a computer

Description automatically generated

+ Chọn tới thư mục Backup vừa tạo

A screenshot of a computer error

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

+ Tại cửa sổ Specify Remote Folder, tại mục Location nhập

\\192.168.100.5\share

A screenshot of a computer

Description automatically generated

+ Tiến hành sao lưu

A screenshot of a computer

Description automatically generated

+ Quá trình sao lưu đã diễn ra thành công

A screenshot of a computer

Description automatically generated

+ Trên máy Windows 7, mở folder WindowsImageBackup đã nhận từ máy

Windows Server

A computer screen shot of a computer

Description automatically generated with low confidence

A computer screen shot of a computer

Description automatically generated with low confidence

+ Kiểm tra, minh chứng kết quả, mở cmd và gõ lệnh sau

net user

dir

A screenshot of a computer screen

Description automatically generated with medium confidence

**2. Sao lưu tệp lên FTP Server**

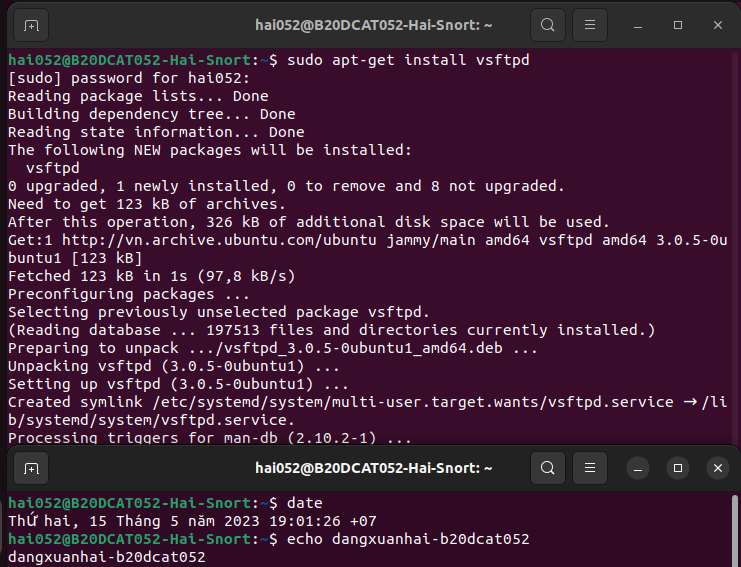
- Trên máy Windows Server Victim cài đặt FTP Server

A screenshot of a computer

Description automatically generated

-Trên máy Linux victim Internal, cài đặt FTP Server

*sudo apt-get install vsftpd*



- Chỉnh sủa file /etc/vsftpd.conf

sudo nano /etc/vsftpd.conf

A screenshot of a computer

Description automatically generated

- Khởi động tường lửa, allow cổng

sudo ufw enable

A screenshot of a computer

Description automatically generated

sudo ufw allow 20:21/tcp

A screenshot of a computer program

Description automatically generated with medium confidence

- Khởi động lại vsftpd

systemctl restart vsftpd

A screenshot of a computer

Description automatically generated with medium confidence

- Trên máy Windows server ta tạo mới 1 thư mục dạng zip

A screenshot of a computer

Description automatically generated

- Trên máy Windows Server Victim, tiến hành sao lưu tới thư mục trên máy

Linux trong mạng Internal sử dụng FTP Client

ftp 192.168.100.147

A screenshot of a computer

Description automatically generated

- Sau khi kết nối thành công, tiến hành backup bằng lệnh put

A screenshot of a computer

Description automatically generated

- Kiểm tra bằng lệnh dir

A screenshot of a computer screen

Description automatically generated with medium confidence

- Trên máy Linux Victim kiểm tra lại bằng lệnh ls

A screenshot of a computer program

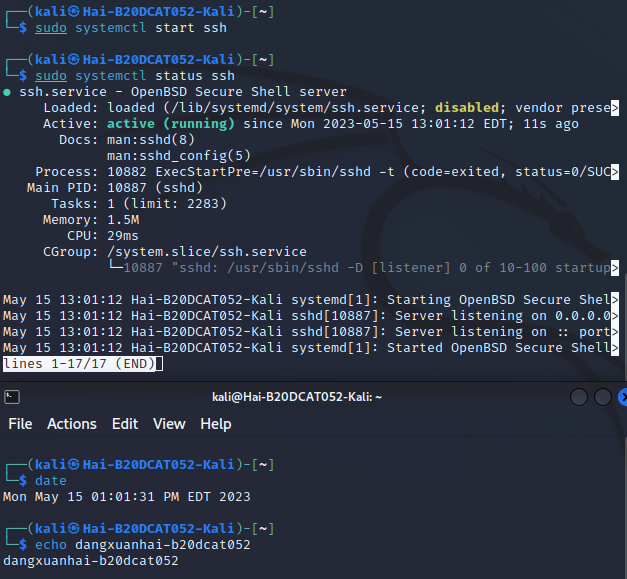
Description automatically generated with medium confidence

**3. Sao lưu tệp sử dụng SCP**

- Trên máy Kali Linux Internal, tiến hành cấu hình ssh server

systemctl start ssh

systemctl status ssh



- Tạo Secure Shell Keys trên máy Kali Linux

ssh-keygen –t rsa

A screenshot of a computer program

Description automatically generated with medium confidence

ls ~/.ssh

A screenshot of a computer

Description automatically generated

cat ~/.ssh/id\_rsa.pub

A screenshot of a computer program

Description automatically generated with medium confidence

cat ~/.ssh/id\_rsa



Trong máy Linux victim, gõ lệnh scp để copy các file cần sao lưu sang máy

Kali Linux

scp Hai-B20DCAT052-SCP.txt [Hai-B20DCAT052-Kali@192.168.100.3:Backup](mailto:Hai-B20DCAT052-Kali@192.168.100.3:Backup)

A screenshot of a computer program

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated with medium confidence

Trên máy Kali Attack trong mạng Internal kiểm tra bằng lệnh ls

A screenshot of a computer program

Description automatically generated with medium confidence

A screenshot of a computer screen

Description automatically generated with medium confidence