

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



Môn: Thực tập cơ sở

BÁO CÁO THỰC TẬP CƠ SỞ
Bài 9: Sao lưu hệ thống

<i>Họ và tên giảng viên:</i>	<i>PGS.TS.Đỗ Xuân Chợt</i>
<i>Họ và tên:</i>	<i>Phạm Thanh Tùng</i>
<i>Mã sinh viên:</i>	<i>B20DCAT171</i>
<i>Lớp:</i>	<i>D20CQAT03-B</i>
<i>Số điện thoại:</i>	<i>0856915668</i>

Hà Nội 2023

1. Mục đích:

- Giúp sinh viên nắm được công cụ và cách thức sao lưu hệ thống, bao gồm:
 - o Sao lưu tới ổ đĩa mạng
 - o Sao lưu tệp lên FTP server
 - o Sao lưu tệp sử dụng SCP

2. Nội dung thực hành:

2.1. Tìm hiểu lý thuyết:

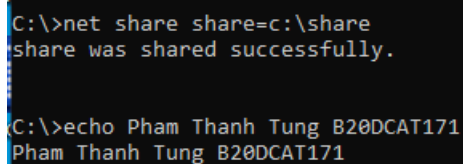
- SCP – Secure copy (SCP) là một phương tiện truyền tệp một cách an toàn giữa một máy chủ cục bộ và một máy chủ từ xa hoặc giữa hai máy chủ từ xa, dựa trên giao thức Secure Shell (SSH). Các tệp có thể được tải lên bằng giao thức SSH với SCP. Các tệp sẽ được mã hóa khi gửi qua mạng
- FTP - Giao thức truyền tệp hay FTP cho phép người dùng truyền tệp từ máy này sang máy khác từ xa. Hạn chế của việc sử dụng FTP là dữ liệu được gửi dưới dạng văn bản không được mã hóa
- Ổ đĩa mạng - Ổ đĩa mạng là bộ nhớ trên máy tính khác được gán ký tự ổ đĩa. Trong một số trường hợp, người dùng sẽ chỉ có quyền truy cập đọc vào ổ đĩa mạng, vì vậy họ sẽ không thể lưu trữ bất kỳ tệp nào. Nếu quyền ghi tồn tại, người dùng có thể lưu trữ tệp
- Net use - Lệnh net use có thể được sử dụng để ánh xạ các ổ đĩa của hệ thống từ xa.
- Net view - Lệnh net view sẽ hiển thị danh sách các mạng chia sẻ của hệ thống.
- Tài liệu tham khảo:

Lab 8 pfsense firewall của CSSIA CompTIA Security+®

2.2. Các bước thực hiện

2.2.1. 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)



```
C:\>net share share=c:\share
share was shared successfully.

C:\>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
```

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

```
C:\>net use x: \\192.168.100.5\share
Enter the user name for '192.168.100.5': B20DCAT171
Enter the password for 192.168.100.5:
The command completed successfully.
```

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

Status	Local	Remote	Network
OK	X:	\\192.168.100.5\share	Microsoft Windows Network

The command completed successfully.

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

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

Status	Local	Remote	Network
OK	X:	\\192.168.100.5\share	Microsoft Windows Network

The command completed successfully.

```
C:\>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
```

- 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, sau đó chọn 1 thư mục để sao lưu và đích là thư mục ở mạng đã chia sẻ trên máy Windows attack trong mạng Internal



Confirmation

Backup Options

Select Backup Configurat...

Select Items for Backup

Specify Destination Type

Specify Remote Folder

Confirmation

Backup Progress

A backup of the items below will now be created and saved to the specified destination.

File excluded: None

Backup destination: \\192.168.100.5\share

Advanced option: VSS Copy Backup

Backup items

Name

C:\Users\Administrator

Administrator: C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.17763.737]

(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Administrator>

```
C:\Users\B20DCAT171>net share

Share name      Resource                Remark
-----
C$              C:\                    Default share
IPC$            C:\                   Remote IPC
ADMIN$          C:\Windows             Remote Admin
share           C:\Share
The command completed successfully.

C:\Users\B20DCAT171>dir c:\share
Volume in drive C has no label.
Volume Serial Number is 5616-F716

Directory of c:\share

03/07/2023  09:35 PM    <DIR>          .
03/07/2023  09:35 PM    <DIR>          ..
03/07/2023  08:52 PM             58 Hello.txt.txt
03/07/2023  09:35 PM    <DIR>          WindowsImageBackup
                1 File(s)              58 bytes
                3 Dir(s)  43,577,905,152 bytes free

C:\Users\B20DCAT171>

C:\Windows\system32\cmd.exe - date

Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\B20DCAT171>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\B20DCAT171>date
The current date is: Tue 03/07/2023
Enter the new date: (mm-dd-yy) 
```

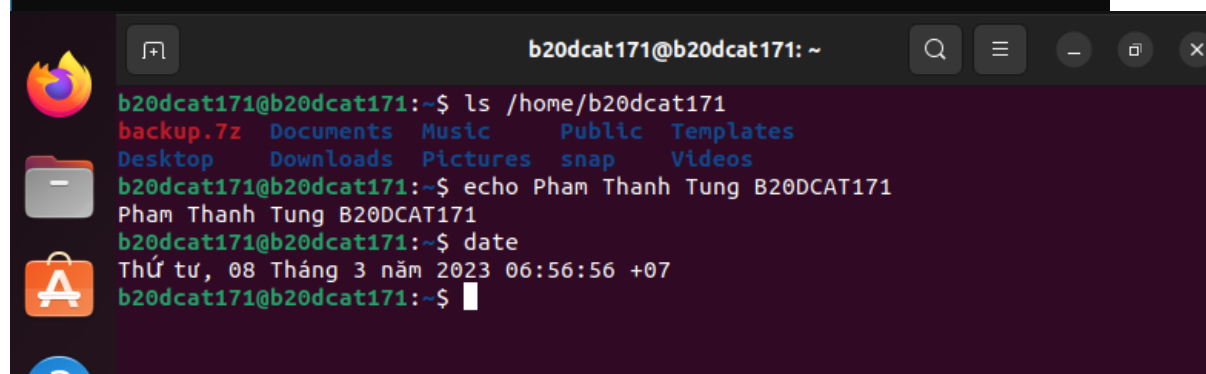
2.3. Sao lưu tệp lên FTP server

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

```
C:\>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)): b20dcat171
331 Please specify the password.
Password:
230 Login successful.
ftp> bin
200 Switching to Binary mode.
ftp> put backup.7z
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 4498754 bytes sent in 0.03Seconds 145121.10Kbytes/sec.
ftp>
```

```
C:\Users\B20DCAT171>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
```

```
C:\Users\B20DCAT171>date
The current date is: Wed 03/08/2023
Enter the new date: (mm-dd-yy)
```



```
b20dcat171@b20dcat171: ~
b20dcat171@b20dcat171:~$ ls /home/b20dcat171
backup.7z  Documents  Music      Public  Templates
Desktop    Downloads  Pictures   snap    Videos
b20dcat171@b20dcat171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
b20dcat171@b20dcat171:~$ date
Thứ tư, 08 Tháng 3 năm 2023 06:56:56 +07
b20dcat171@b20dcat171:~$
```

2.4.Sao lưu tệp sử dụng SCP

- Trên máy Kali Linux trong mạng Internal, cấu hình SSH server.
- Tiếp tục, tạo Secure Shell Keys trên máy Kali Linux đó

```
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:EsFnEyLHxhaYLfjhoovqfPVmZdLsgDyxUFGD052JxjE root@B20DCAT171-Tung-K
ali
The key's randomart image is:
+--[RSA 3072]--+
| ..0@E=.o      |
| . =*BB*+      |
| o.=+o .       |
| ..o. .        |
| . .o = S      |
| . * + =       |
| .. . o *      |
+-----+

kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
└─$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

(kali@B20DCAT171-Tung-Kali)-[~]
└─$ date
Tue Mar 7 07:06:08 PM EST 2023
```

- 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

```
root@b20dcat171:/home/b20dcat171# scp backup.7z kali@192.168.100.3:/home/kali/b
ackup
kali@192.168.100.3's password:
backup.7z                               100% 4393KB  56.9MB/s   00:00
root@b20dcat171:/home/b20dcat171# echo Pham Thanh Tung B20DCA171
Pham Thanh Tung B20DCA171
root@b20dcat171:/home/b20dcat171# date
Thứ tư, 08 Tháng 3 năm 2023 07:58:59 +07
root@b20dcat171:/home/b20dcat171#
```

```
(kali@B20DCAT171-Tung-Kali)-[~]
└─$ ls /home/kali
backup  Documents  key_rsa      Music  Pictures  Templates
Desktop Downloads  key_rsa.pub  password Public     Videos

(kali@B20DCAT171-Tung-Kali)-[~]
└─$

kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
└─$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

(kali@B20DCAT171-Tung-Kali)-[~]
└─$ date
Tue Mar 7 07:06:08 PM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
└─$
```