ĐẠI HỌC DUY TÂN
BAN SAU ĐẠI HỌC

OAN TOÀN VÀ BẢO MẬT THÔNG TIN
BÀI THỰC HÀNH CÁ NHÂN

TỔNG HỢP CÁC BÀI TẬP

Giáo viên giảng dạy : PGS-TS. Nguyễn Gia Như

Học viên thực hiện: Ks. Ngô Thanh Lợi

Đà Nẵng, Tháng 3 năm 2025

BÀI TẬP 1 WIRESHARK & NMAP

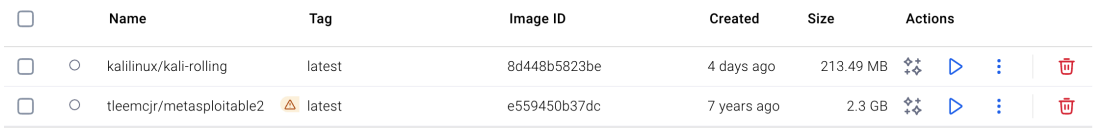
1.1 Setup evniroment

Trong phạm vi bài tập thực hành cá nhân về Wirshark, NMap sẽ triển khai trên mạng được giả lập mạng ở hai OS Kali Linux & Metasploitable2 trên MacOS; sau đó tiến hành cài đặt các package Wirshark, NMap trên Kalilinux để triển khai các bài tập thực hành.

❖ Cài đặt Kali Linux. Metasploitable2 và thiết lập mạng

➢ Chuẩn bị docker image Kali Linux, Metasploitable2

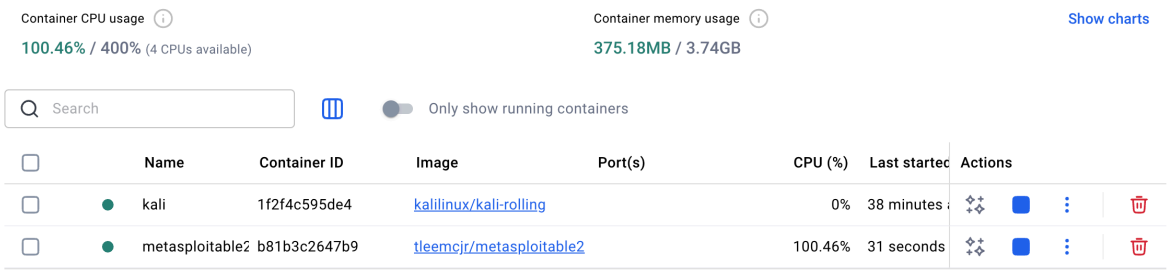
```
# thanhloi@LoiNT-MacOS Isa676-InformationSecurity
docker pull kalilinux/kali-rolling
docker pull tleemcjr/metasploitable2
```



	Name	Tag	Image ID	Created	Size	Actions
☐	kalilinux/kali-rolling	latest	8d448b5823be	4 days ago	213.49 MB	
☐	tleemcjr/metasploitable2	latest	e559450b37dc	7 years ago	2.3 GB	

➢ Chuẩn bị Run image Kali-Linux, Metasploitable2 trong container & thiết lập mang với pentest

```
# thanhloi@LoiNT-MacOS Isa676-InformationSecurity;
docker network create loint-pentest
docker run -it --name kali --network loint-pentest --privileged
kalilinux/kali-rolling /bin/bash
docker run -d --net loint-pentest --name metasploitable2 -h victim
tleemcjr/metasploitable2 /bin/sh -c "/bin/services.sh && tail -f
/dev/null"
┌──(root㉿attacker)-[/]
└─# apt update
└─# apt install -y iputils-ping
└─# apt install iproute2 -y
└─# apt install net-tools -y
# Trong container Kali, cài đặt tcpdump, nmap, hoặc metasploit-framework
để tạo lưu lượng mạng
└─# apt update && apt install tcpdump nmap metasploit-framework -y
#ping metasploitable2 have IP: 172.18.0.3
└─# ping 172.18.0.3
```




```
└─# ping 172.18.0.3
PING 172.18.0.3 (172.18.0.3) 56(84) bytes of data.
64 bytes from 172.18.0.3: icmp_seq=1 ttl=64 time=0.226 ms
64 bytes from 172.18.0.3: icmp_seq=2 ttl=64 time=0.075 ms
64 bytes from 172.18.0.3: icmp_seq=3 ttl=64 time=0.044 ms
64 bytes from 172.18.0.3: icmp_seq=4 ttl=64 time=0.047 ms
64 bytes from 172.18.0.3: icmp_seq=5 ttl=64 time=0.038 ms
64 bytes from 172.18.0.3: icmp_seq=6 ttl=64 time=0.214 ms
64 bytes from 172.18.0.3: icmp_seq=7 ttl=64 time=0.174 ms
64 bytes from 172.18.0.3: icmp_seq=8 ttl=64 time=0.048 ms
64 bytes from 172.18.0.3: icmp_seq=9 ttl=64 time=0.048 ms
64 bytes from 172.18.0.3: icmp_seq=10 ttl=64 time=0.213 ms
64 bytes from 172.18.0.3: icmp_seq=11 ttl=64 time=0.168 ms
64 bytes from 172.18.0.3: icmp_seq=12 ttl=64 time=0.144 ms
64 bytes from 172.18.0.3: icmp_seq=13 ttl=64 time=0.219 ms
```

- Cài đăt Wireshark trong Kaliliux và kiểm tra kết nối Metasploitable2

```
# thanhloi@LoiNT-MacOS Isa676-InformationSecurity;
docker exec -it attacker bash
┌──(root㉿attacker)-[/]
└─# apt update
└─# apt install wireshark
# Result: wireshark is already the newest version (4.4.7-1).
└─# dpkg-reconfigure wireshark-common
└─# sudo wireshark &
```

- Cài đặt Namp trong Kaliliux và kiểm tra kết nối Metasploitable2

```
# thanhloi@LoiNT-MacOS Isa676-InformationSecurity;
docker exec -it attacker bash
┌──(root㉿attacker)-[/]
└─# apt update
└─# apt install -y nmap
└─# nmap --version
# Result: Nmap version 7.95 ( https://nmap.org )
```

- Cài đăt Wireshark MacOS với guideline: Installing Wireshark under macOS và Containershark Extcap Plugin cho Wireshark

1.2 Sử dụng Wirshark để kiểm tra và phân tích gói tin

1.2.1 Giới thiệu Wirshark và những ứng dụng

Wireshark là phần mềm mã nguồn mở, miễn phí, dùng kiểm tra và phân tích lưu lượng mạng. Nó hỗ trợ giao thức packet capture qua ***pcap/tshark***, có giao diện GUI mạnh, dùng trên Windows, Linux, macOS. Wireshark được xem như "đồng hồ vạn năng" của mạng – giúp nhìn rõ hoạt động bên trong, luồng traffic, cấu trúc gói tin và các lỗi xảy ra.

Các ứng dụng của Wirshark trong bảo mật thông tin

- Phát hiện xâm nhập & giám sát sự cố
  - Phát hiện các kết nối lạ, session hijacking, traffic C2 malware.
  - Dùng filter như tcp.flags.syn == 1 để phát hiện SYN-Flood hoặc port scan
- Forensics mạng
  - Bắt và giữ file pcap để phục vụ điều tra incident.
  - Khôi phục lưu lượng truy cập, xem file bằng Xplico/Zeek sau khi capture
- Phân tích mã độc & reverse engineering
  - Phát hiện backdoor/malware C2 thong qua bất thường protocol.
  - Phân tích payload gói tin, xác định kiểu mã hóa, phát hiện DNS tunneling...
- 3.4 Xác thực và máy chủ web
  - Xem TLS handshake (ClientHello), phân tích chứng chỉ, debug lỗi SSL/TLS
  - Debug các lỗi HTTP/HTTPS, kiểm tra response codes, phân tích nội dung header/meta.
- 3.5 Kiểm thử xâm nhập (Pentesting)
  - Trong lab pentest, dùng Wireshark để quan sát kết quả khi tấn công.
  - Phân tích traffic trong exploitation, reverse shell, capture flag…

1.2.2 Kiểm tra các gói tin

Sử dụng Wireshark hoặc tcpdump trong container Kali để bắt và phân tích lưu lượng giữa Kali (172.18.0.2) và Metasploitable2 (172.18.0.3)

- Sử dụng tcpdump trong container Kali để lưu gữ gói tin ở file **capture.pcap**

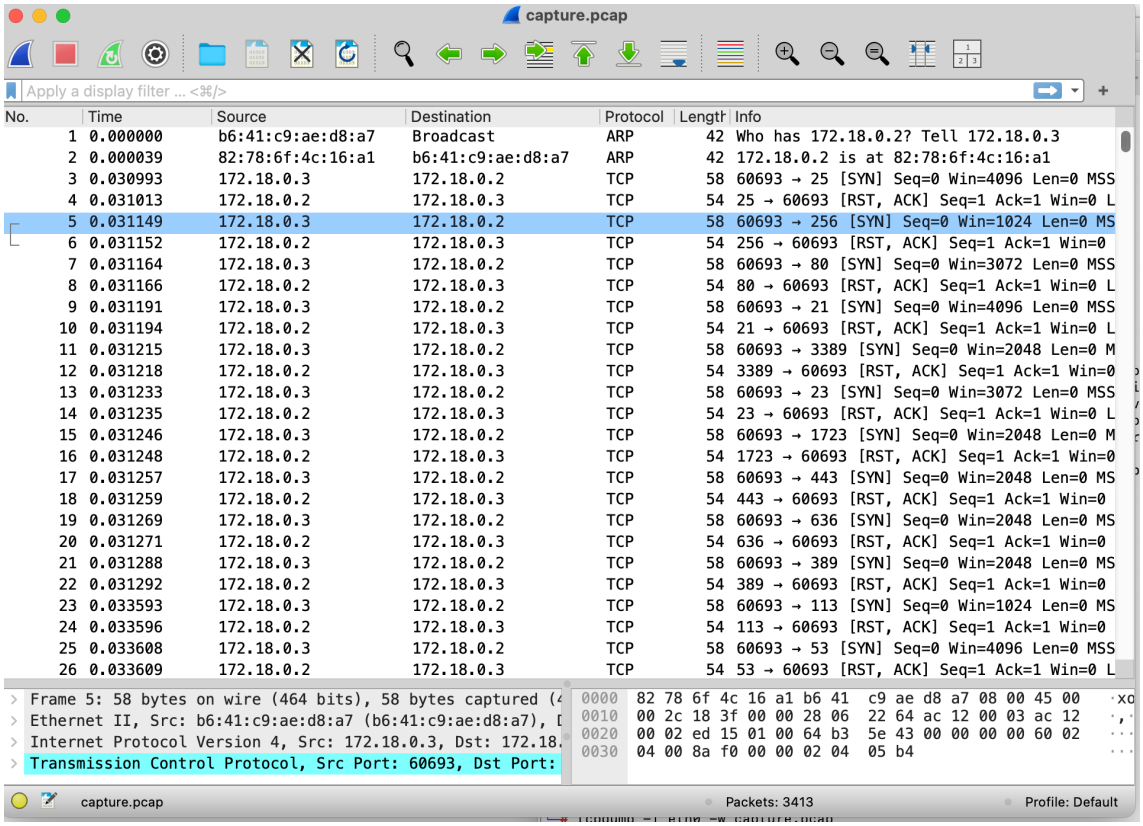
```
┌──(root㉿attacker)-[/]
└─# tcpdump -i eth0 -w capture.pcap
#tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length
262144 bytes
```

❖ Tạo lưu lượng mạng từ terminal của **Metasploitable2** or **Kali** để tcpdump lưu giữ gói tin

```
msfadmin@victim:~$ nmap 172.18.0.2
```

❖ Tải file capture.pcap từ kali về MacOS để phân tích với Wirshark

```
# thanhloi@LoiNT-MacOS Isa676-InformationSecurity;
docker cp kali:/capture.pcap ~/capture.pcap
open -a Wireshark ~/capture.pcap
```



❖ Tuỳ chọn xem các gói tin với Edgeshark giúp đơn giản hoá xem gói tin

➢ Cài đặt Docker Compose và run Edgeshark

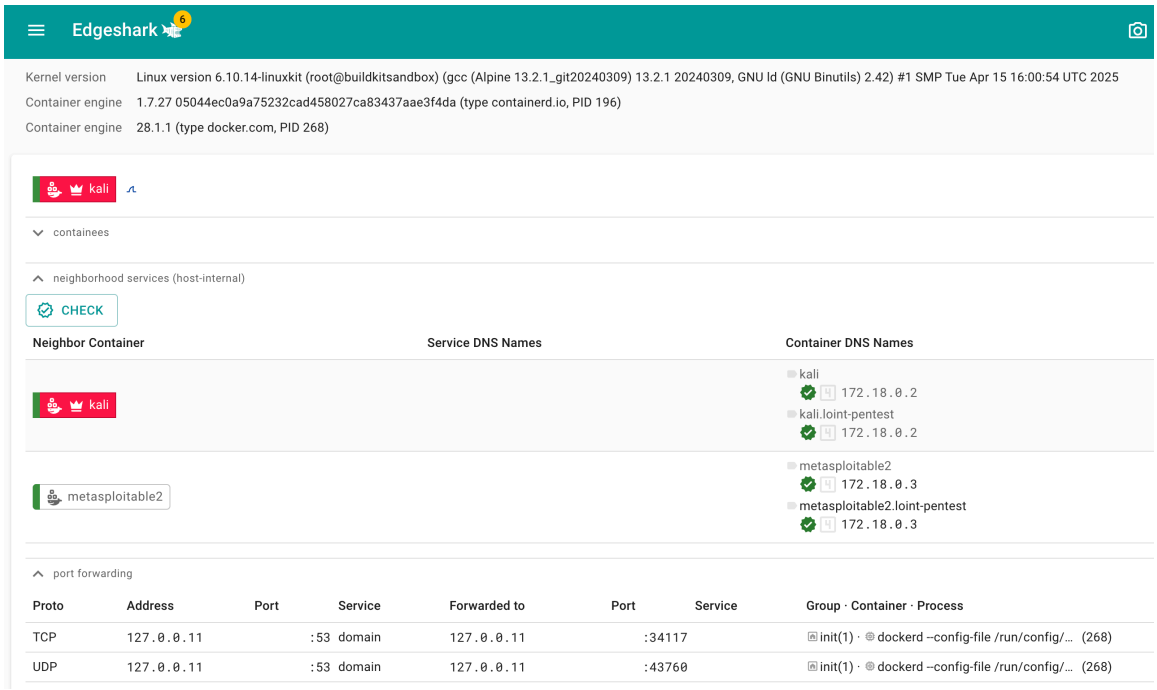
```
# thanhloi@LoiNT-MacOS Isa676-InformationSecurity;
brew install docker-composewget -q --no-cache -O -
https://github.com/siemens/edgeshark/raw/main/deployments/wget/docker-
compose.yaml | docker compose -f - up
```

➢ Cài đặt Cài plugin cshargextcap và packetflix-handler của Siemen

```
# thanhloi@LoiNT-MacOS Isa676-InformationSecurity;
tar -xzf cshargextcap-<version>-darwin-<arch>.tar.gz
sudo mv cshargextcap /Applications/Wireshark.app/Contents/MacOS/extcap/
mkdir -p /tmp/pflix-handler && cd /tmp/pflix-handler
curl -sLO https://github.com/srl-
labs/containerlab/files/14278951/packetflix-handler.zip
```

```
unzip packetflix-handler.zip
sudo mv packetflix-handler.app /Applications
sudo xattr -r -d com.apple.quarantine /Applications/packetflix-
handler.app
```

➢ Kiểm tra Edgeshark từ url *http://localhost:5001* với các host, mạng trong docker container



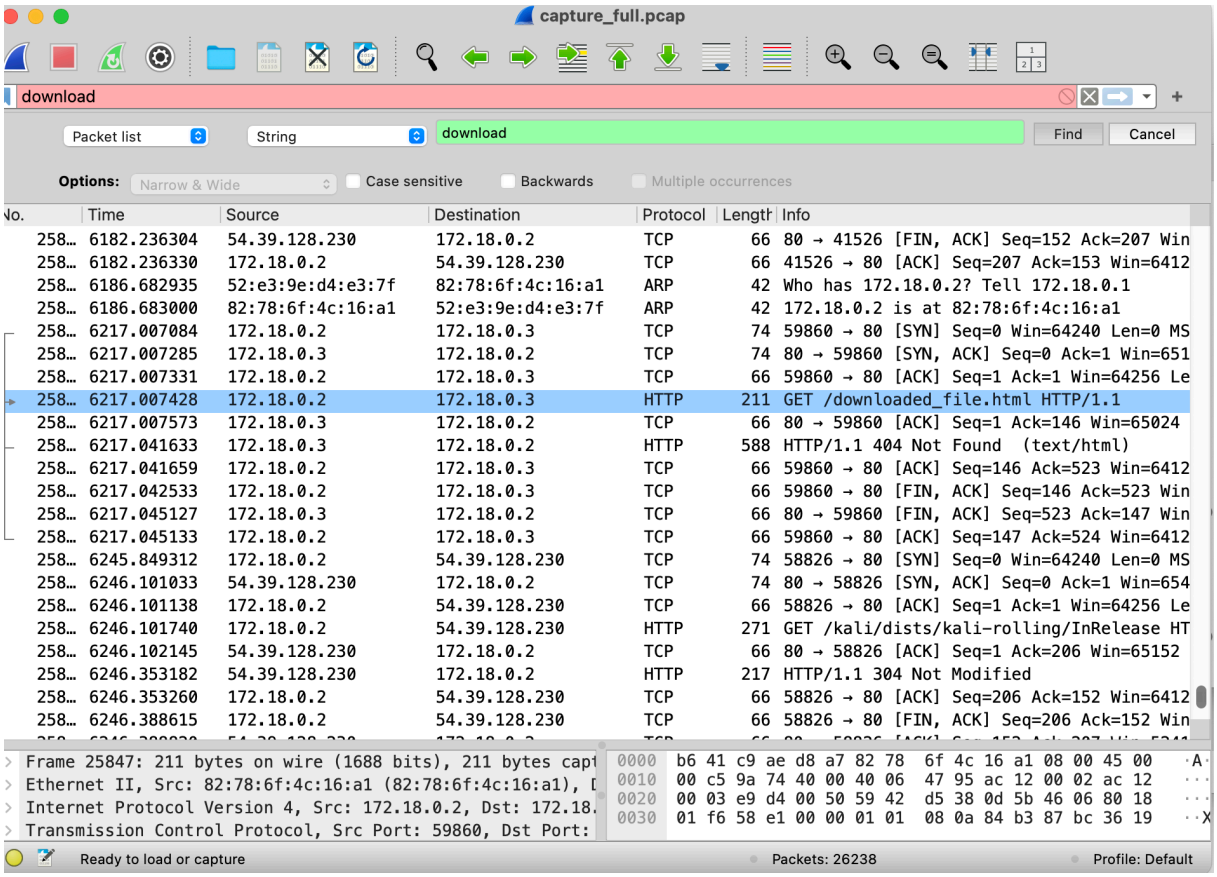
❖ Kịch bản bắt các gói tin được download từ internet vào container Kali, hoặc từ **Metasploitable2** về **kali** với Edgeshark; phân tích chúng bằng Wireshark

➢ Tạo lưu lượng mạng từ Metasploitable2

o Tạo lưu lượng mạng từ container Kali:

```
┌──(root㉿attacker)-[/]
└─# apt update && apt install wget curl -y
└─# curl http://172.18.0.3/downloaded_file.html -o downloaded_file.html
```

➢ Bắt gói tin bằng Edgeshark



1.3. Sử dụng NMAP để khám phá & kiểm tra bảo mật mạng

1.3.1 Giới thiệu NMAP và những ứng dụng

Nmap (Network Mapper) là một công cụ mã nguồn mở mạnh mẽ và phổ biến được sử dụng để quét mạng và kiểm tra bảo mật. Được phát triển bởi Gordon Lyon (bút danh Fyodor) vào năm 1997, Nmap ban đầu được thiết kế để khám phá các máy chủ và dịch vụ trên mạng, nhưng hiện đã trở thành một công cụ đa năng trong lĩnh vực an ninh mạng. Nmap hỗ trợ nhiều nền tảng, bao gồm Linux, Windows, macOS, và được sử dụng rộng rãi bởi các chuyên gia bảo mật, quản trị viên mạng, và cả tin tặc để phân tích mạng và tìm kiếm lỗ hổng.

Nmap hoạt động bằng cách gửi các gói tin (packets) đến các máy chủ mục tiêu và phân tích phản hồi để thu thập thông tin về:

- ❖ Các máy chủ đang hoạt động (host discovery).
- ❖ Các cổng (ports) mở trên máy chủ.
- ❖ Dịch vụ (services) chạy trên các cổng (như HTTP, SSH, FTP).
- ❖ Hệ điều hành và phiên bản phần mềm.
- ❖ Các đặc điểm mạng khác như tường lửa, thiết bị định tuyến.

Nmap được điều khiển qua dòng lệnh, nhưng cũng có giao diện đồ họa (Zenmap) dành cho người dùng muốn thao tác dễ dàng hơn.Các tính năng chính của Nmap

- ❖ Khám phá máy chủ (Host Discovery): Xác định các thiết bị đang hoạt động trong mạng.
- ❖ Quét cổng (Port Scanning): Kiểm tra trạng thái các cổng (mở, đóng, hoặc bị lọc) trên máy chủ.
- ❖ Phát hiện dịch vụ và phiên bản (Service/Version Detection): Xác định dịch vụ (như Apache, SSH) và phiên bản phần mềm chạy trên các cổng.
- ❖ Phát hiện hệ điều hành (OS Detection): Dự đoán hệ điều hành và phiên bản dựa trên đặc điểm mạng.
- ❖ Quét kịch bản (Nmap Scripting Engine - NSE): Sử dụng các script Lua để thực hiện các tác vụ nâng cao như phát hiện lỗ hổng, tấn công brute-force, hoặc thu thập thông tin chi tiết.
- ❖ Phân tích tường lửa và IDS/IPS: Kiểm tra cấu hình tường lửa hoặc hệ thống phát hiện xâm nhập (IDS/IPS).
- ❖ Hỗ trợ nhiều giao thức: Nmap hỗ trợ TCP, UDP, ICMP, và các giao thức khác.

1.3.2 Các thao tác với NMAP

Điều kiện tiền đề đã dựng thành công mạng "***loint-pentest***" với 2 host "***kali*** " & "***metasploitable2*** ". Kiểm tra một số lệnh phổ biến NMAP từ "**kali**" host

- ❖ Khám phá mạng : "***nmap -ns <subnet>***" giúp quản trị viên mạng xác định tất cả các thiết bị đang hoạt động trong mạng, bao gồm máy chủ, máy trạm, thiết bị IoT, hoặc thiết bị không xác định. Ví dụ kiểm tra mạng "***loint-pentest***" và thông tin host "***metasploitable2***"

```
┌──(root㉿1f2f4c595de4)-[/]
└─# nmap -sn 172.18.0.0/16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 08:08 UTC
Nmap scan report for 172.18.0.1
Host is up (0.000092s latency).
MAC Address: DE:49:76:9A:82:24 (Unknown)
Nmap scan report for metasploitable2.loint-pentest (172.18.0.3)
Host is up (0.000070s latency).
MAC Address: FA:1C:59:6D:89:75 (Unknown)
Nmap scan report for 1f2f4c595de4 (172.18.0.2)
Host is up.
Stats: 0:05:46 elapsed; 8193 hosts completed (3 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 99.93% done; ETC: 08:13 (0:00:00 remaining)
Stats: 0:05:48 elapsed; 12289 hosts completed (3 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 0.73% done
Stats: 0:05:48 elapsed; 12289 hosts completed (3 up), 4096 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 1.10% done; ETC: 08:15 (0:01:30 remaining)
```

```
┌──(root㉿1f2f4c595de4)-[/]
└─# nmap 172.18.0.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 08:06 UTC
Nmap scan report for metasploitable2.loint-pentest (172.18.0.3)
Host is up (0.000013s latency).
Not shown: 979 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: FA:1C:59:6D:89:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

- ❖ Kiểm tra bảo mật (Security Auditing)
  - ➢ Phát hiện cổng mở: Nmap xác định các cổng mở có thể là điểm yếu để tin tặc khai thác

```
┌──(root㉿1f2f4c595de4)-[/]
└─# nmap -p 1-65535 172.18.0.0/16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 08:15
Nmap scan report for 172.18.0.1
Host is up (0.0000020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
111/tcp   open  rpcbind
64873/tcp open  unknown
MAC Address: DE:49:76:9A:82:24 (Unknown)

Nmap scan report for metasploitable2.loint-pentest (172.18.0
Host is up (0.0000030s latency).
Not shown: 65510 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33553/tcp open  unknown
```

```
┌──(root㉿1f2f4c595de4)-[/]
└─# nmap -p 1-65535 172.18.0.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 08:16 UTC
Nmap scan report for metasploitable2.loint-pentest (172.18.0.3)
Host is up (0.0000030s latency).
Not shown: 65510 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33553/tcp open  unknown
MAC Address: FA:1C:59:6D:89:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

- Phát hiện lỗ hổng: Sử dụng Nmap Scripting Engine (NSE) để tìm các lỗ hổng cụ thể, như cấu hình sai của dịch vụ SMB cho thấy các lỗ hổng tiềm năng:

```
┌──(root㉿1f2f4c595de4)-[/]
└─# nmap --script smb-vuln* 172.18.0.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 08:22 UTC
Nmap scan report for metasploitable2.loint-pentest (172.18.0.3)
Host is up (0.0000040s latency).
Not shown: 979 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: FA:1C:59:6D:89:75 (Unknown)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
```

- Cổng 139 (netbios-ssn) và 445 (microsoft-ds): Đây là các cổng chuẩn cho dịch vụ SMB trên Linux và các hệ thống tương tự. Các lỗ hổng SMB phổ biến có thể bao gồm:
  - MS17-010 (EternalBlue): Lỗ hổng nghiêm trọng cho phép thực thi mã từ xa.
  - SMB Signing Disabled: Dễ bị tấn công Man-in-the-Middle.
  - Lỗ hổng trong cấu hình chia sẻ file và quyền truy cập.
- Các dịch vụ khác mở và lỗ hổng của metasploitable2
  - FTP (21/tcp): Có thể có lỗ hổng do cấu hình yếu hoặc sử dụng tài khoản mặc định.
  - SSH (22/tcp): Có thể bị tấn công brute-force nếu mật khẩu yếu.
  - Telnet (23/tcp): Giao thức không mã hóa, dễ bị nghe lén và tấn công.
  - SMTP (25/tcp): Có thể bị lợi dụng để gửi thư rác hoặc tấn công relay.
  - MySQL (3306/tcp), PostgreSQL (5432/tcp):
  - VNC (5900/tcp): Có thể bị truy cập trái phép nếu không có bảo mật.
  - Các dịch vụ khác như RPC, exec, login, shell, rmiregistry, ingreslock, ajp13, irc

➢ **Kiểm tra tường lửa:** Kiểm tra xem tường lửa có chặn các cổng hoặc giao thức cụ thể hay không.

```
┌──(root㉿1f2f4c595de4)-[/]
└─# nmap -sA 172.18.0.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 08:27 UTC
Nmap scan report for metasploitable2.loint-pentest (172.18.0.3)
Host is up (0.0000040s latency).
All 1000 scanned ports on metasploitable2.loint-pentest (172.18.0.3) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: FA:1C:59:6D:89:75 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

- Host is up (0.0000040s latency): Nmap xác nhận rằng host 172.18.0.3 (container metasploitable2) đang hoạt động. Độ trễ rất thấp (0.0000040 giây) cho thấy kết nối mạng giữa **kali** và **metasploitable2** trong mạng **loint-pentest** là tốt và container đang chạy.
- All 1000 scanned ports are in ignored states. Not shown: 1000 unfiltered tcp ports (reset):
  - **Unfiltered ports**: Kết quả cho thấy tất cả 1000 cổng TCP được quét đều ở trạng thái "unfiltered" (không bị lọc). Điều này có nghĩa là các gói tin ACK gửi đến các cổng này nhận được phản hồi RST (reset), cho thấy các cổng không bị tường lửa chặn.
  - Ignored states: Tất cả cổng đều "unfiltered" (nhận RST), chúng được liệt kê là "ignored" trong báo cáo chính, và chi tiết được cung cấp ở dòng "Not shown".

- **Ý nghĩa**: Kết quả này cho thấy không có tường lửa chặn các cổng TCP trên metasploitable2, nhưng nó không xác định được trạng thái cụ thể của các cổng (mở, đóng, hay lọc) vì -sA không được thiết kế để xác định trạng thái cổng mà chỉ kiểm tra tường lửa.

BÀI TẬP 2 TÀI LIỆU & ĐỀ TÀI THAM KHẢO

[1] Ứng dụng thị giác máy tính và trí tuệ nhân tạo phát hiện đối tượng trên ảnh phục vụ công tác bảo vệ bí mật nhà nước. Tạp chí KH&CN Duy Tân số 01(68)

[2] Hybrid propulsion based on fuel cells. Tạp chí KH&CN Duy Tân số 01(68)

[3] YOLOv8 vs Faster R-CNN: A Comparative Analysis. Keylabs.ai, 15-Jan-2024

[4] Ảnh hưởng của tạp chất CR đến tính chất quang và từ tính của vật liệu sắt điện không chì $BO_{0.5}$ TIO_3 Tạp chí khoa học số 2/2026 -Trường Đại học Thủ Đô

[5] On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives. Springer Nature, Journal of Network and Systems Management (2022).

[6] How Blockchain Technology could Transform the Online Gaming Industry. Author: Julius Nave, University of Twente

[7] https://jsrd.thanhdo.edu.vn/index.php/khpt/structure-and-presentation

[8] Simon Peyton Jones. How to Write a Great Research Paper. Microsoft Research, Cambridge