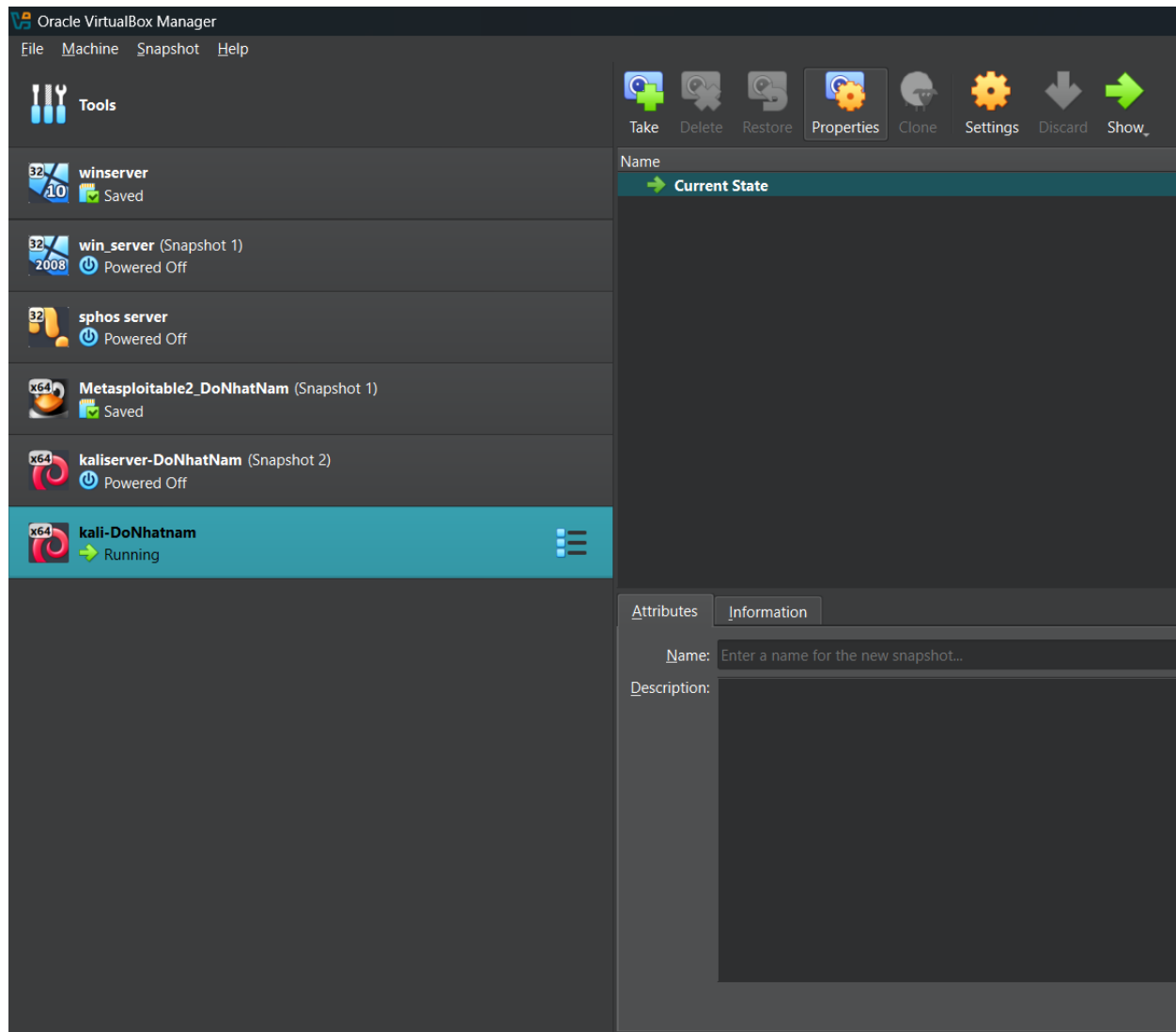


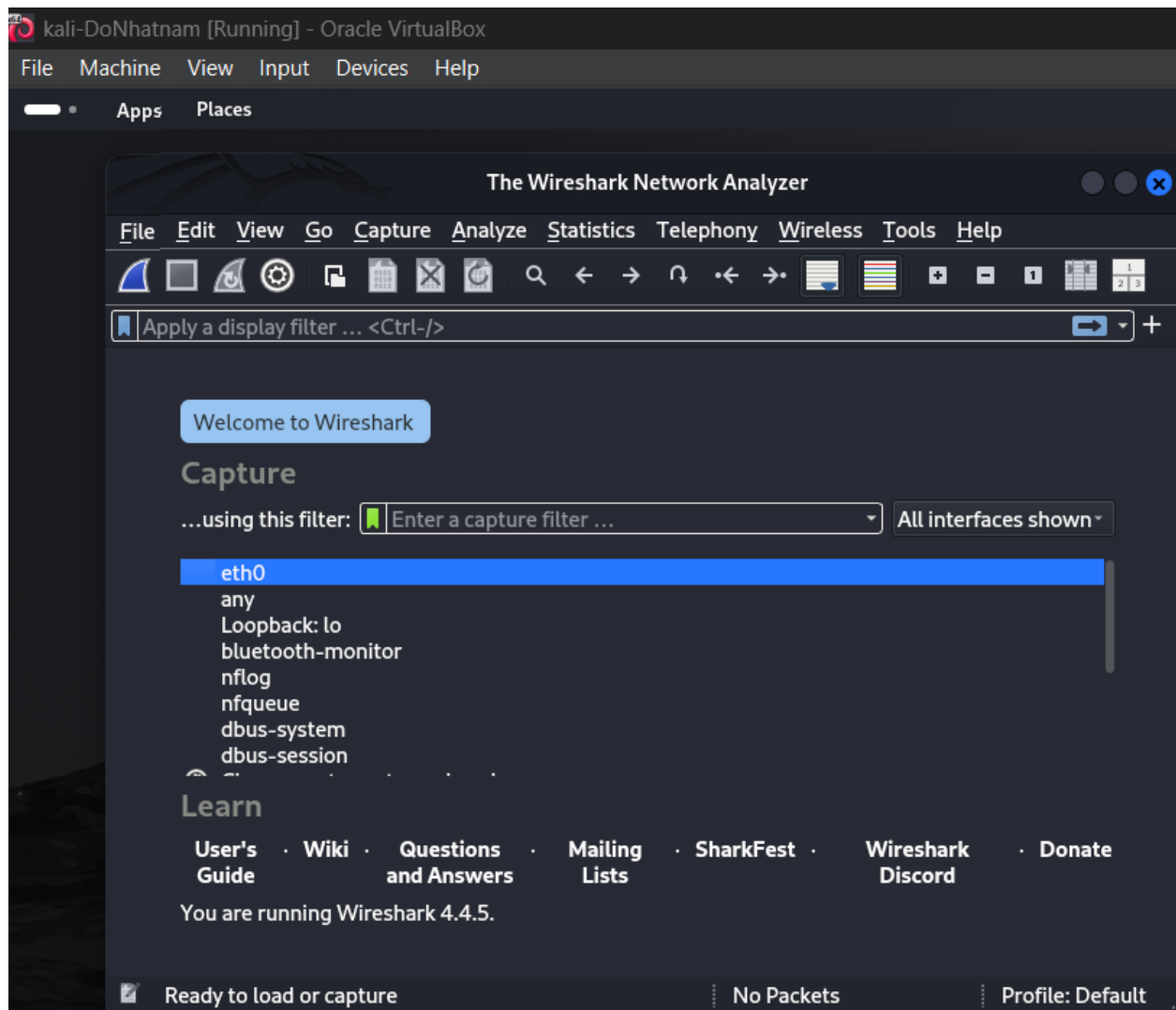
# BÀI TẬP LAP 7

## PHÂN TÍCH CÁC KỸ THUẬT DO THÁM HỆ THỐNG

***B1: Truy cập máy ảo Attack***



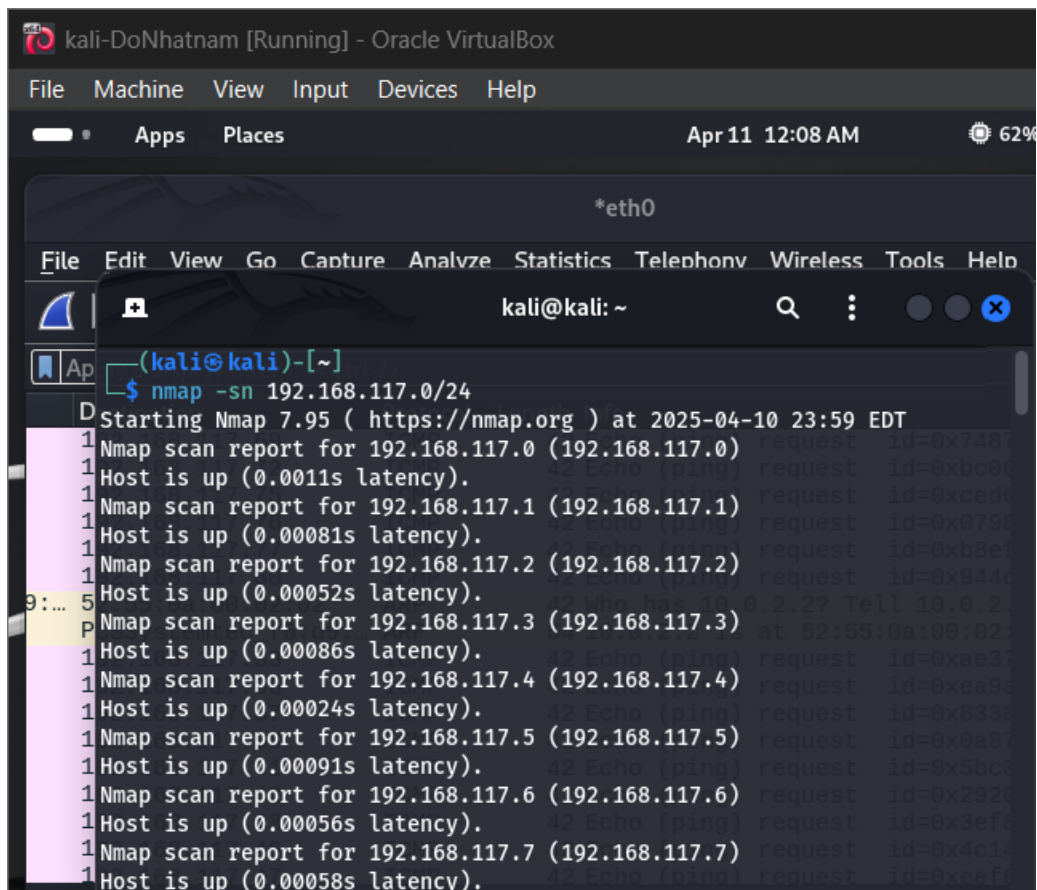
***B2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn các mạng để bắt gói tin.***



**B3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau

```
nmap -sn 192.168.117.0/24
```

**B4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau



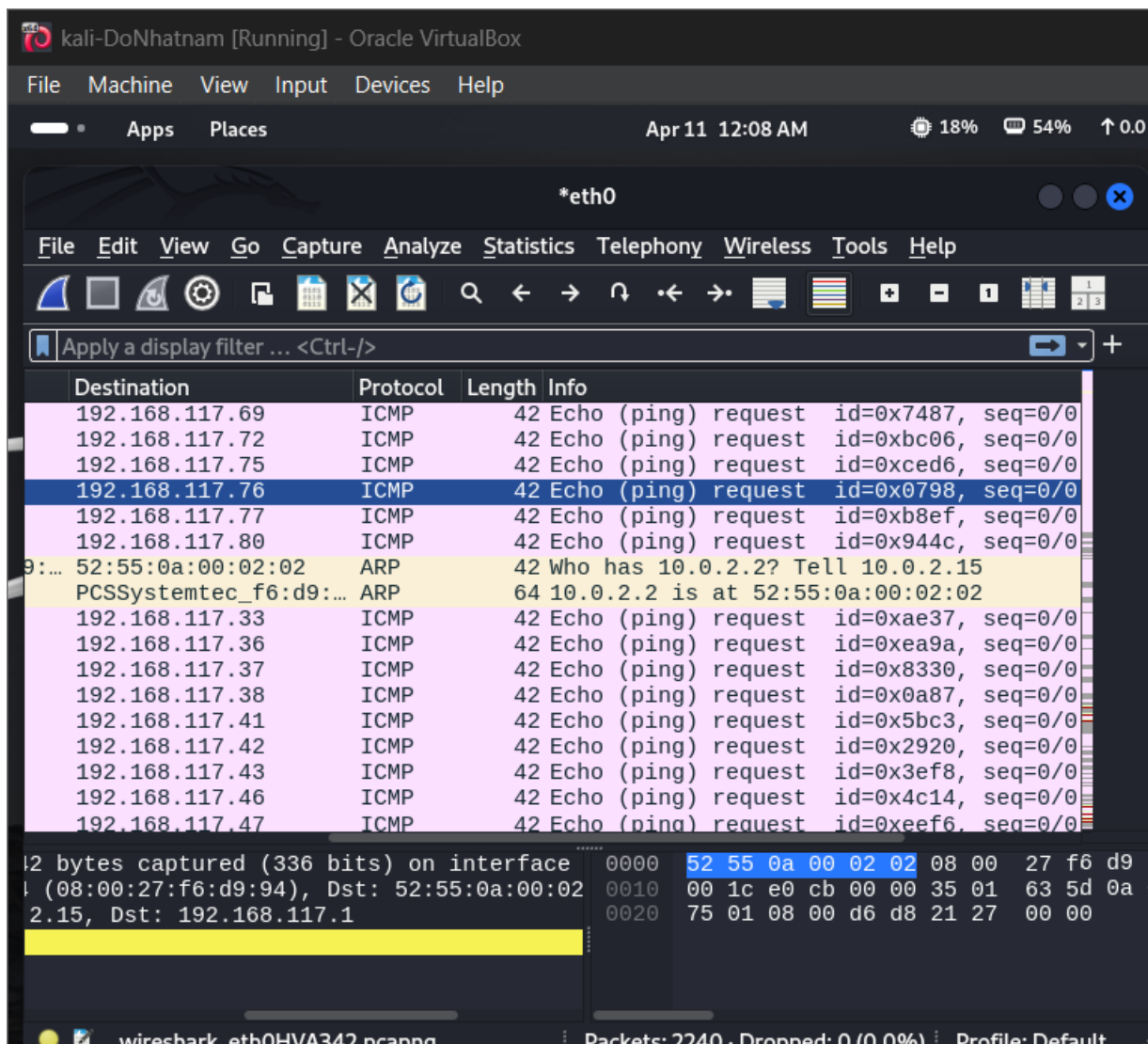
```
kali-DoNhatnam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apr 11 12:08 AM 62%
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
kali@kali: ~
(kali@kali)~[~]
$ nmap -sn 192.168.117.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 23:59 EDT
1 Nmap scan report for 192.168.117.0 (192.168.117.0)
1 Host is up (0.0011s latency).
1 Nmap scan report for 192.168.117.1 (192.168.117.1)
1 Host is up (0.00081s latency).
1 Nmap scan report for 192.168.117.2 (192.168.117.2)
1 Host is up (0.00052s latency).
1 Nmap scan report for 192.168.117.3 (192.168.117.3)
1 Host is up (0.00086s latency).
1 Nmap scan report for 192.168.117.4 (192.168.117.4)
1 Host is up (0.00024s latency).
1 Nmap scan report for 192.168.117.5 (192.168.117.5)
1 Host is up (0.00091s latency).
1 Nmap scan report for 192.168.117.6 (192.168.117.6)
1 Host is up (0.00056s latency).
1 Nmap scan report for 192.168.117.7 (192.168.117.7)
1 Host is up (0.00058s latency).
```

Có thể thấy ngoài địa chỉ 192.168.117.10 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang hoạt động có địa chỉ là 192.168.117.2, 192.168.117.3 và 192.168.117.13

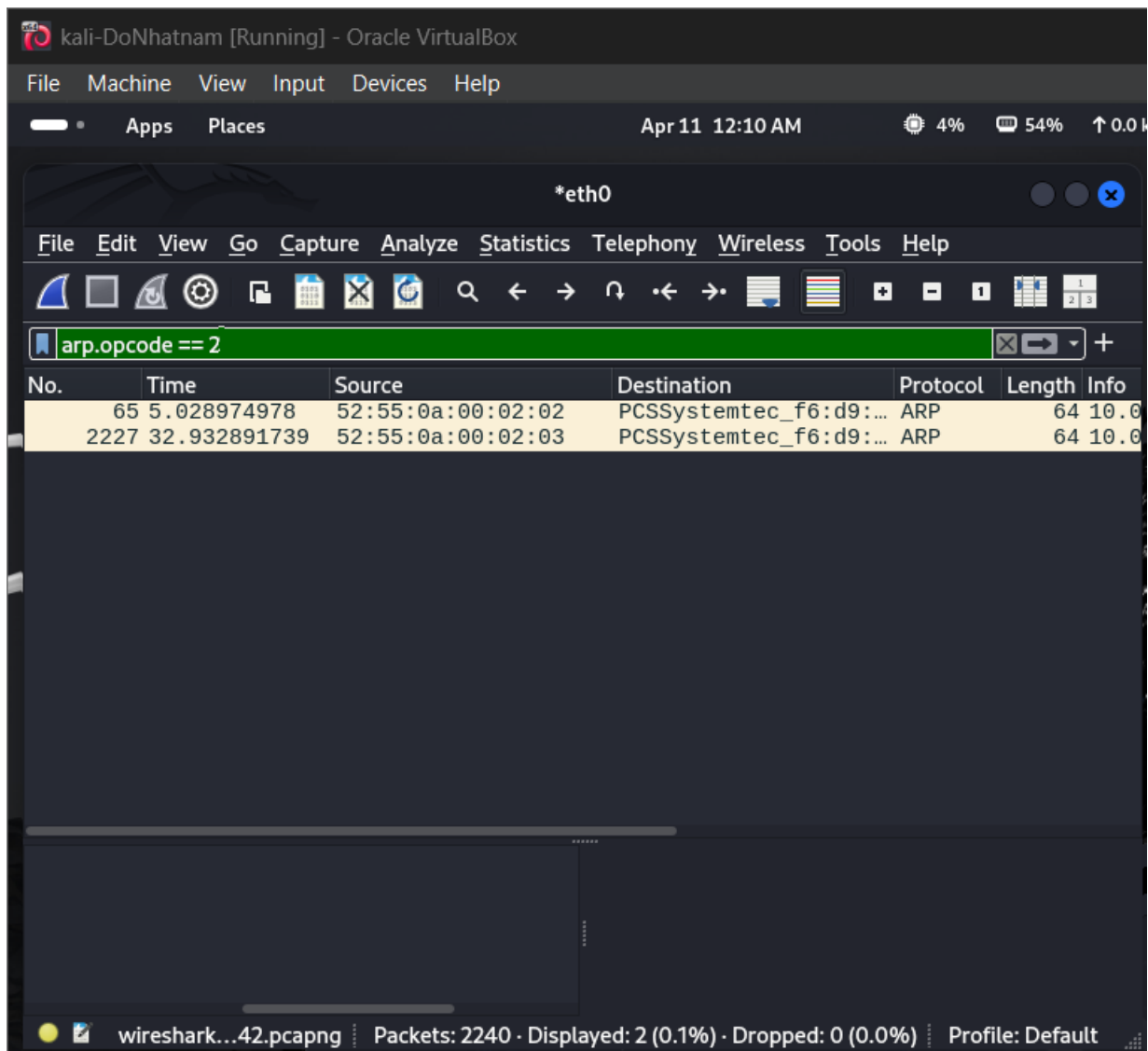
### ***B5: Dừng bắt gói tin trên Wireshark***

Phân tích lưu lượng:

Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.117.0/24



Trên cửa sổ của Wireshark, sử dụng giá trị `arp.opcode == 2` cho bộ lọc, chúng ta có thể thấy các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.



Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng đang hoạt động trong mạng.

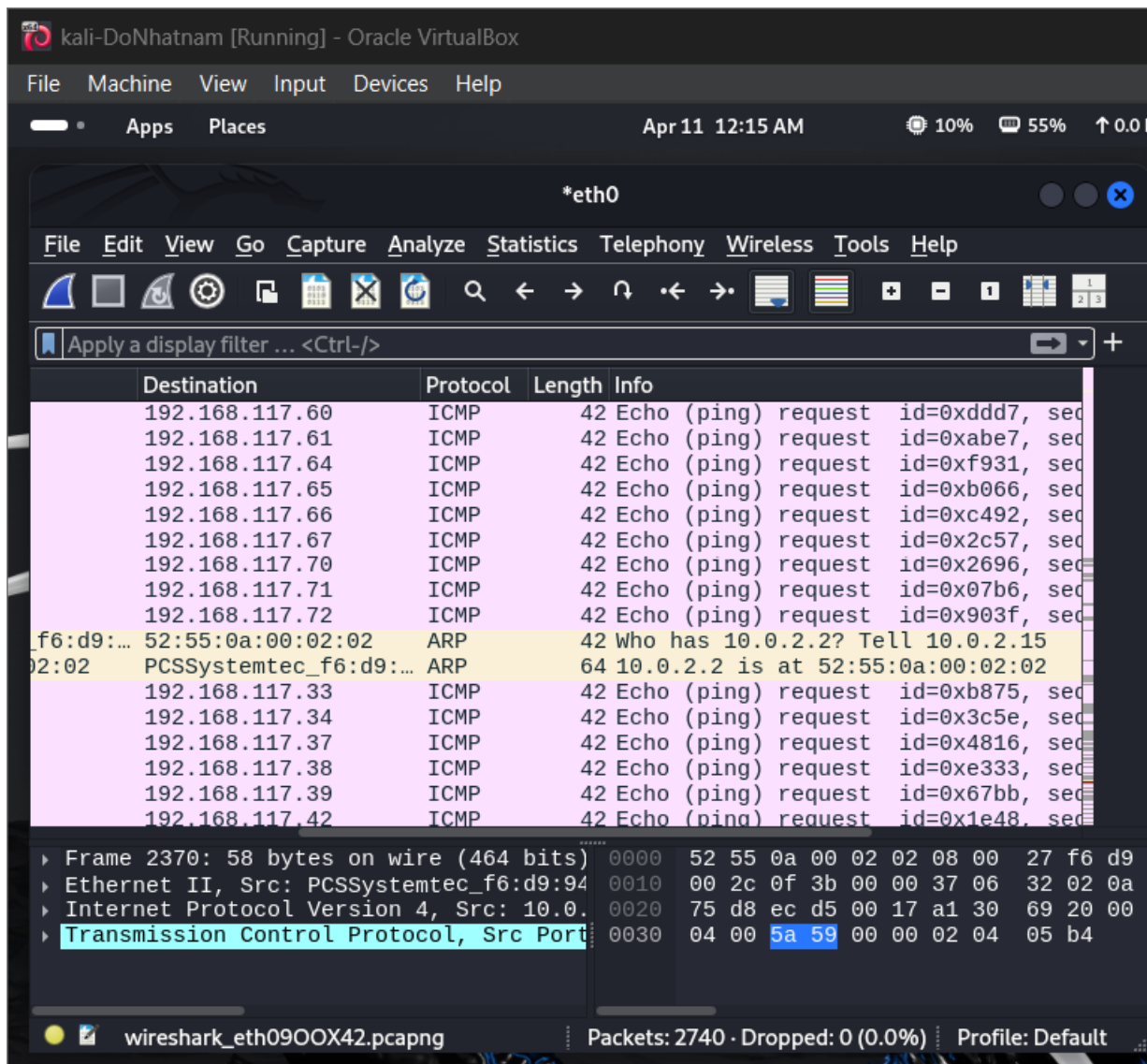
## 2.2. Quét thăm dò dịch vụ

**B3:** Mở cửa sổ *Terminal 2*, sử dụng *Nmap* để quét mạng với lệnh sau:

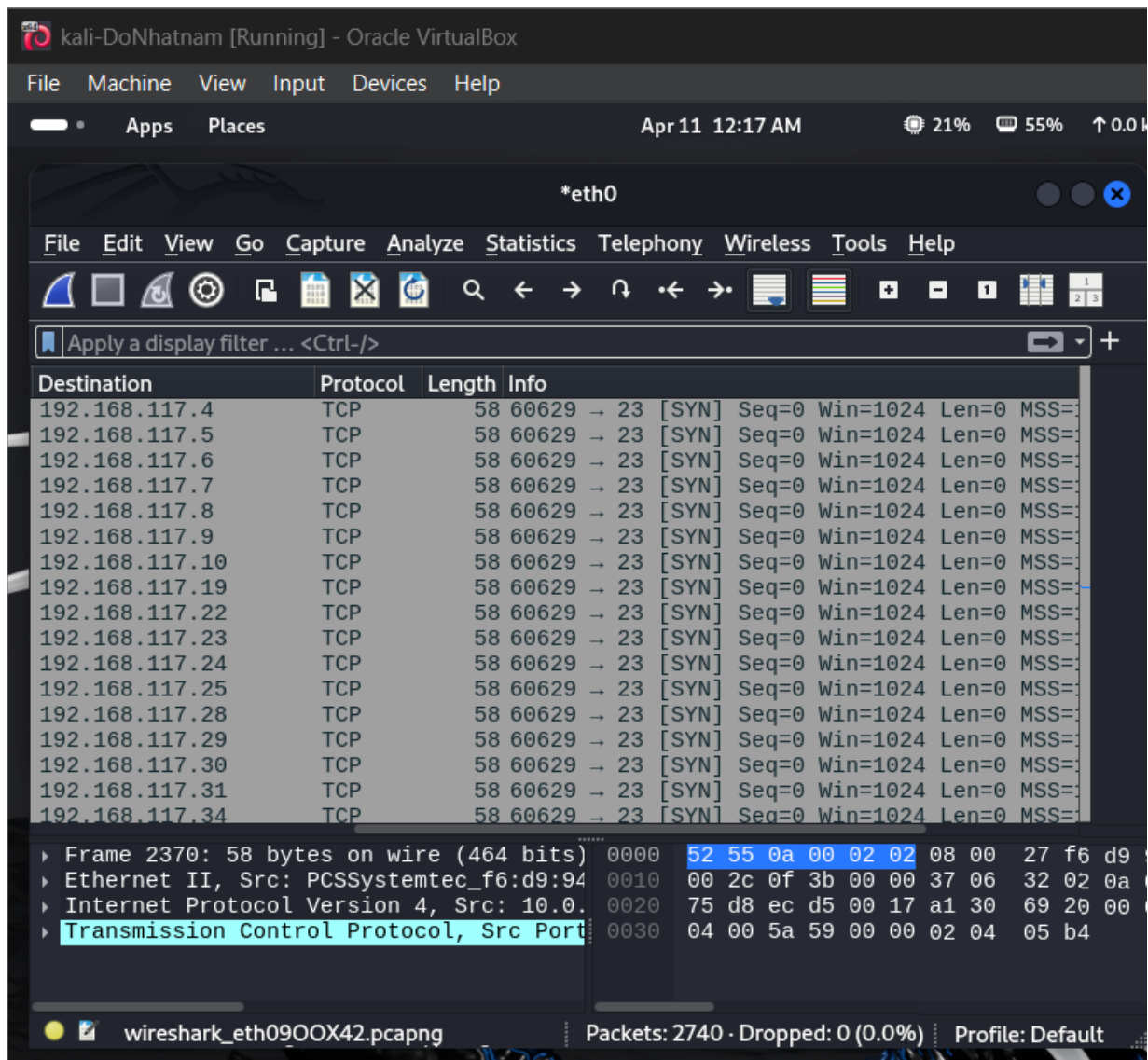
```
sudo nmap -p 23 192.168.117.0/24
```

B4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.117.13 và 192.168.117.10 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.



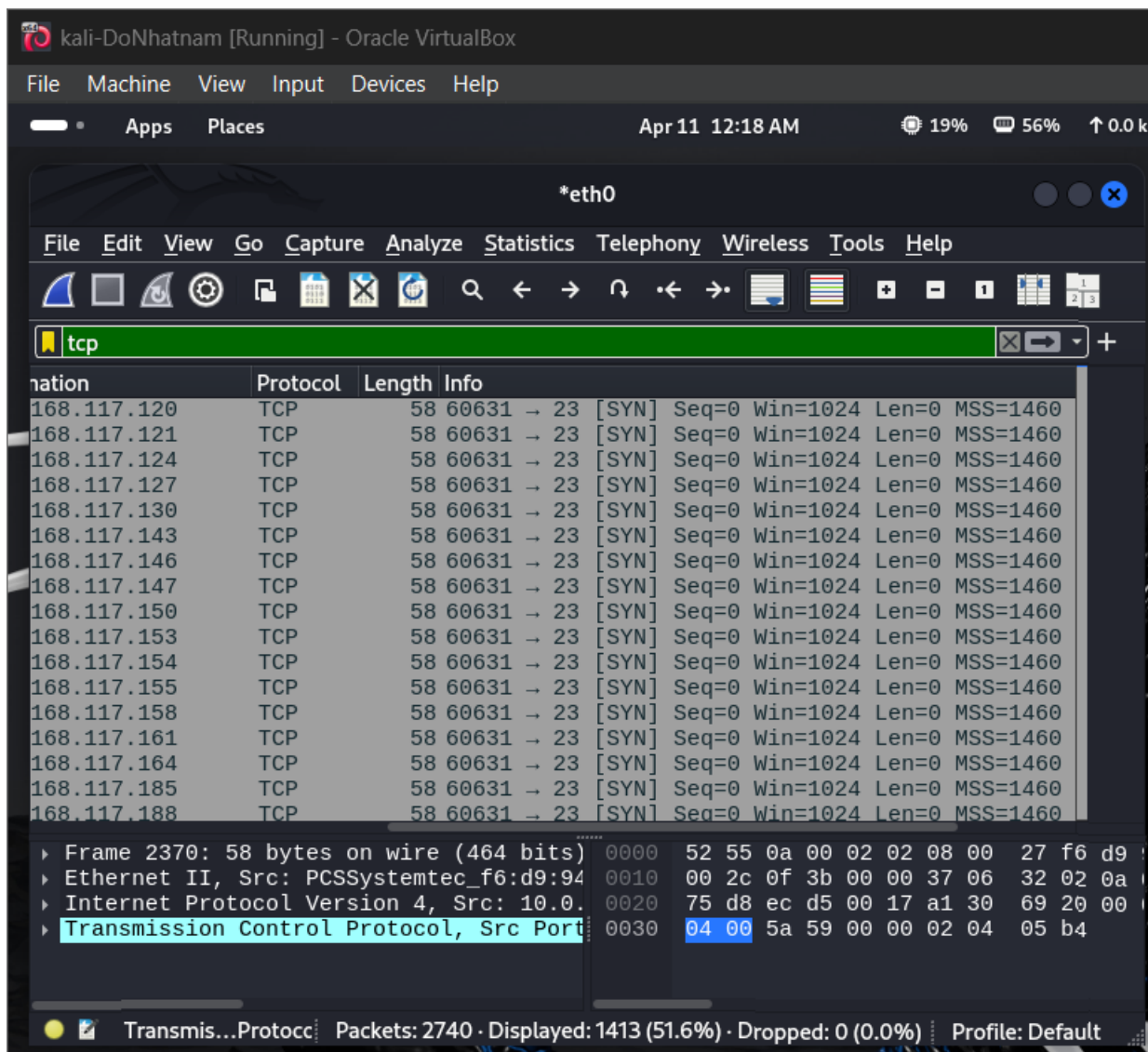


Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 23 của các máy đang hoạt động.



- Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.117.13 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.117.10 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Telnet)





Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

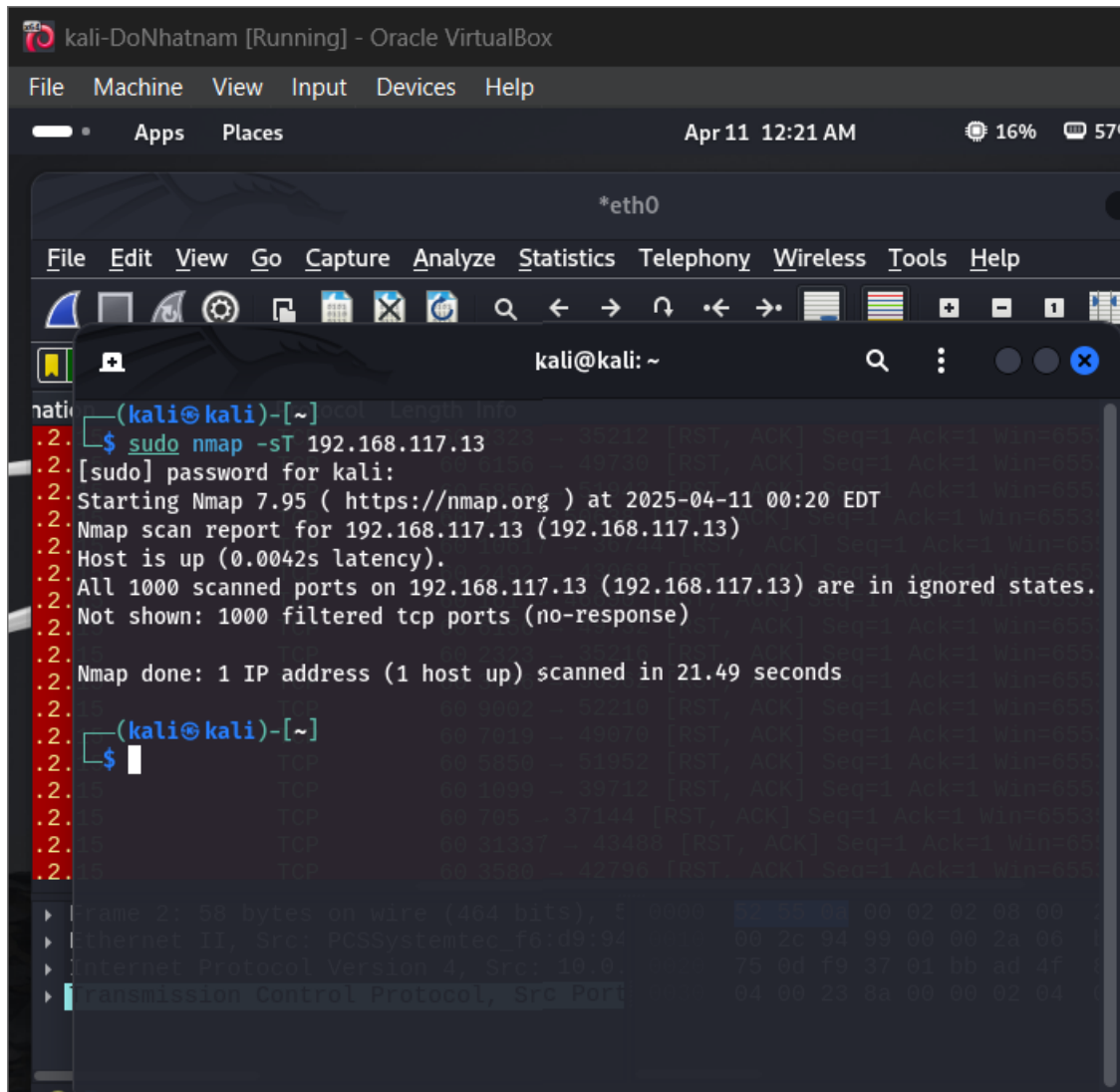
## 2.3. Quét cổng dịch vụ

**B3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

```
nmap -sT 192.168.117.13
```

**B4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 22, 23, 53 trên máy mục tiêu 192.168.117.13 có

*trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns*



The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window is titled 'kali-DoNhatnam [Running] - Oracle VirtualBox'. The menu bar includes File, Machine, View, Input, Devices, and Help. The status bar shows 'Apr 11 12:21 AM', '16%' CPU usage, and '57%' memory usage. The terminal window has a title bar '\*eth0' and a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The terminal shows the following commands and output:

```
(kali@kali)-[~]
└─$ sudo nmap -sT 192.168.117.13
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 00:20 EDT
Nmap scan report for 192.168.117.13 (192.168.117.13)
Host is up (0.0042s latency).
All 1000 scanned ports on 192.168.117.13 (192.168.117.13) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds
```

The terminal also shows a list of TCP ports and their corresponding RST, ACK, Seq, and Win values:

```
(kali@kali)-[~]
└─$
TCP 60 8002 54210 [RST, ACK] Seq=1 Ack=1 Win=655
TCP 60 7019 49070 [RST, ACK] Seq=1 Ack=1 Win=655
TCP 60 8000 51952 [RST, ACK] Seq=1 Ack=1 Win=655
TCP 60 1000 39712 [RST, ACK] Seq=1 Ack=1 Win=655
TCP 60 700 37144 [RST, ACK] Seq=1 Ack=1 Win=655
TCP 60 31337 43400 [RST, ACK] Seq=1 Ack=1 Win=655
TCP 60 3500 42796 [RST, ACK] Seq=1 Ack=1 Win=655
```

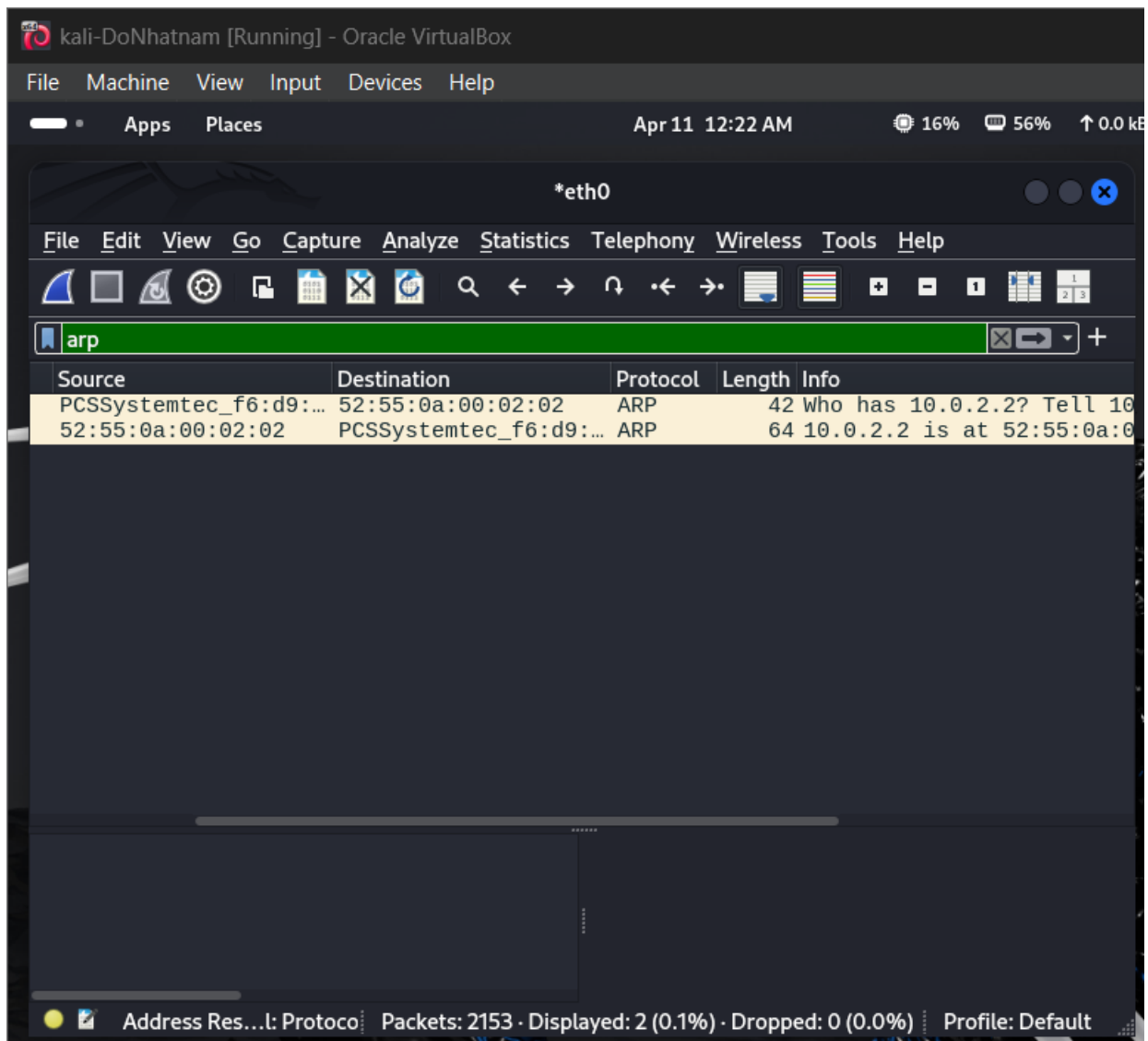
The terminal also shows a packet capture in Wireshark, with the following details:

```
Frame 2: 58 bytes on wire (464 bits), 5 packets
Ethernet II, Src: PCSSystemtec f8:d9:94, 00:2c:94:99:00:00:2a:00
Internet Protocol Version 4, Src: 192.168.117.10, 75:0d:f9:37:01:bb:ad:4f
Transmission Control Protocol, Src Port: 8000, 04:00:23:8a:00:00:02:04
```

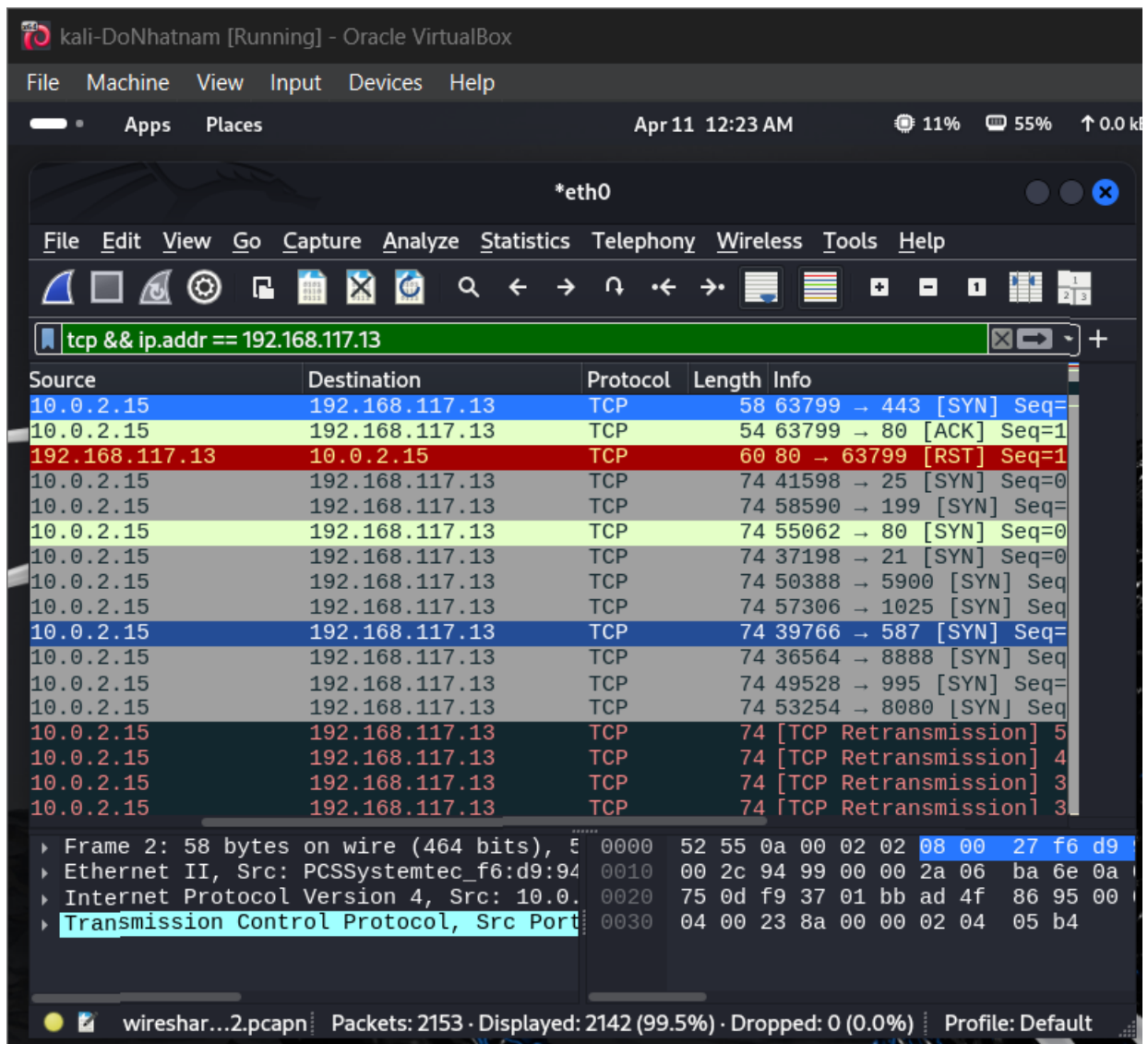
## ***B5: Dừng bắt gói tin trên Wireshark***

Phân tích lưu lượng:

Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 192.168.117.13 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói 8 tin TCP SYN được gửi từ máy tấn công (192.168.117.10) tới máy mục tiêu là 192.168.117.13. Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.



- Sử dụng giá trị `tcp && ip.addr == 192.168.117.13` ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 53 đã được thiết lập (các gói tin 12, 16, 17 của quá trình bắt tay 3 bước) nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST(gói tin 30) để hủy kết nối này



Tiếp tục phân tích trên các cổng ứng dụng khác, ta thấy hiện tượng xảy ra tương tự với các cổng ứng dụng 22, 23. Điều này cho thấy máy do thám đã thực hiện hành vi quét cổng với kỹ thuật TCP Connection Scan - Danh sách các cổng ứng dụng trên máy mục tiêu có thiết lập kết nối với máy do thám trùng khớp với kết quả trả về của lệnh quét nmap trên máy do thám.

### 3.1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap

#### 3.1.1. Kịch bản 1

Thực hiện lệnh quét nmap -sn Dia\_chi\_mang/Mat\_na trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là task1.pcap.

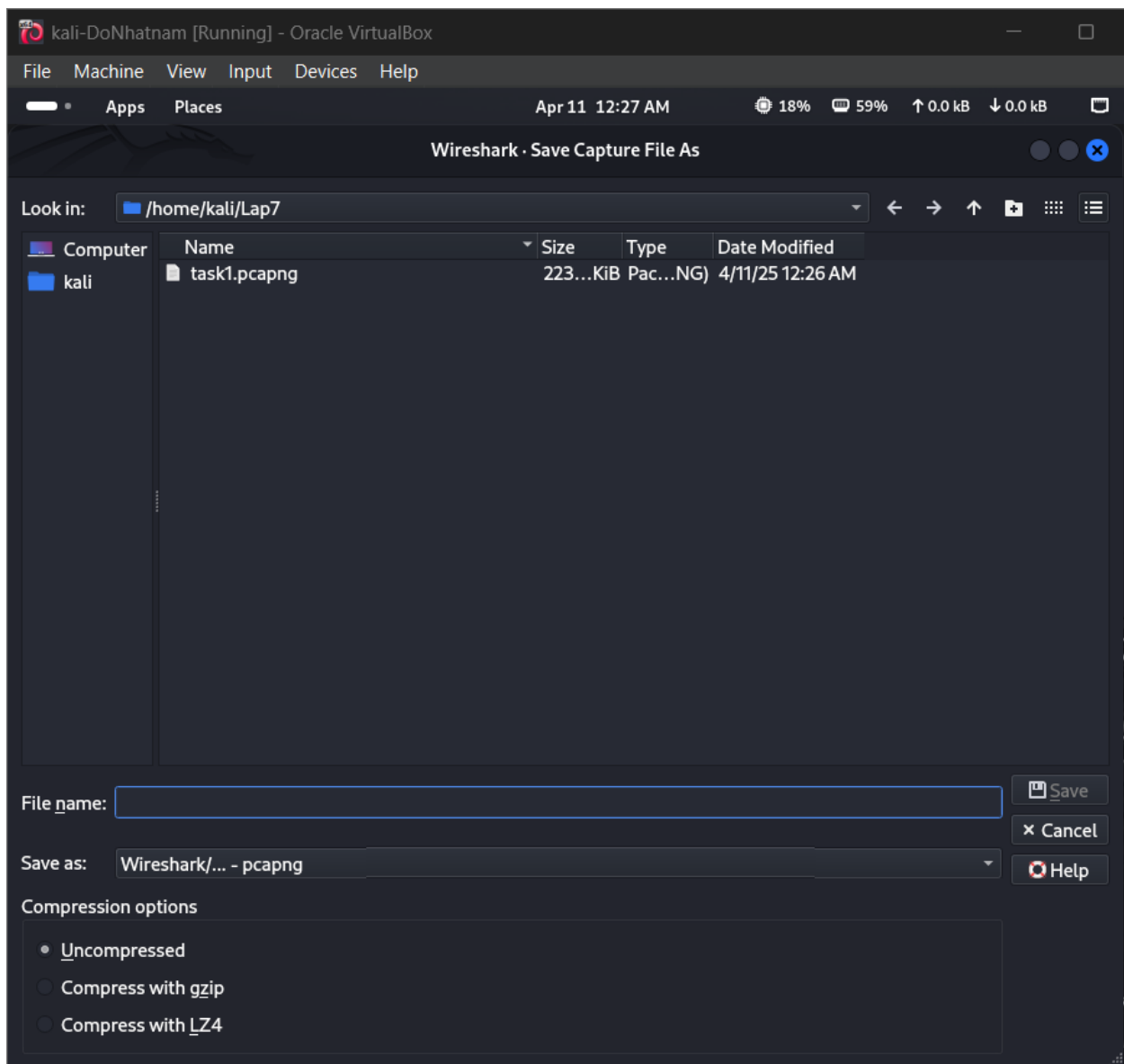
Trả lời: Khi thực hiện lệnh sudo nmap -sn 192.168.117.0/24 trên máy do thám, kỹ thuật quét được sử dụng là Ping Scan hay còn gọi là Host Discovery. Đây là kỹ thuật nhằm xác định những máy chủ nào đang hoạt động trong một dải mạng nhất định mà không thực hiện quét các cổng dịch vụ. Trong quá trình này, Nmap sẽ gửi các gói ICMP Echo Request tương tự như lệnh ping hoặc kết hợp gửi thêm các gói TCP SYN đến cổng 443 và TCP ACK đến cổng 80, tùy thuộc vào cấu hình và quyền của người dùng. Nếu máy mục tiêu phản hồi bằng ICMP Echo Reply hoặc gửi lại gói RST khi không có dịch vụ đang chạy tại cổng đó thì Nmap sẽ xác định rằng máy chủ đó đang hoạt động. Ngược lại, nếu không có phản hồi hoặc phản hồi bằng ICMP unreachable thì máy chủ được coi là không hoạt động hoặc bị lọc bởi tường lửa. Trên máy do thám khi bắt lưu lượng mạng bằng công cụ như Wireshark hoặc tcpdump, ta có thể quan sát thấy các gói ICMP Echo Request được gửi tới từng địa chỉ IP trong dải mạng và các phản hồi ICMP Echo Reply từ những máy chủ đang bật. Nếu không thấy phản hồi, Nmap có thể chuyển sang sử dụng các gói TCP để tiếp tục kiểm tra. Như vậy, kỹ thuật quét được sử dụng trong lệnh nmap -sn là Ping Scan với mục đích chính là phát hiện các thiết bị đang hoạt động trong mạng.

kali-DoNhatnam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

```
(kali@kali)-[~]  
$ nmap -sn 192.168.117.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 00:57 EDT  
Nmap scan report for 192.168.117.0 (192.168.117.0)  
Host is up (0.00049s latency).  
Nmap scan report for 192.168.117.1 (192.168.117.1)  
Host is up (0.00055s latency).  
Nmap scan report for 192.168.117.2 (192.168.117.2)  
Host is up (0.00038s latency).  
Nmap scan report for 192.168.117.3 (192.168.117.3)  
Host is up (0.00058s latency).  
Nmap scan report for 192.168.117.4 (192.168.117.4)  
Host is up (0.00041s latency).  
Nmap scan report for 192.168.117.5 (192.168.117.5)  
Host is up (0.00043s latency).  
Nmap scan report for 192.168.117.6 (192.168.117.6)  
Host is up (0.00075s latency).  
Nmap scan report for 192.168.117.7 (192.168.117.7)  
Host is up (0.00054s latency).  
Nmap scan report for 192.168.117.8 (192.168.117.8)  
Host is up (0.00019s latency).  
Nmap scan report for 192.168.117.9 (192.168.117.9)  
Host is up (0.00031s latency).  
Nmap scan report for 192.168.117.10 (192.168.117.10)
```

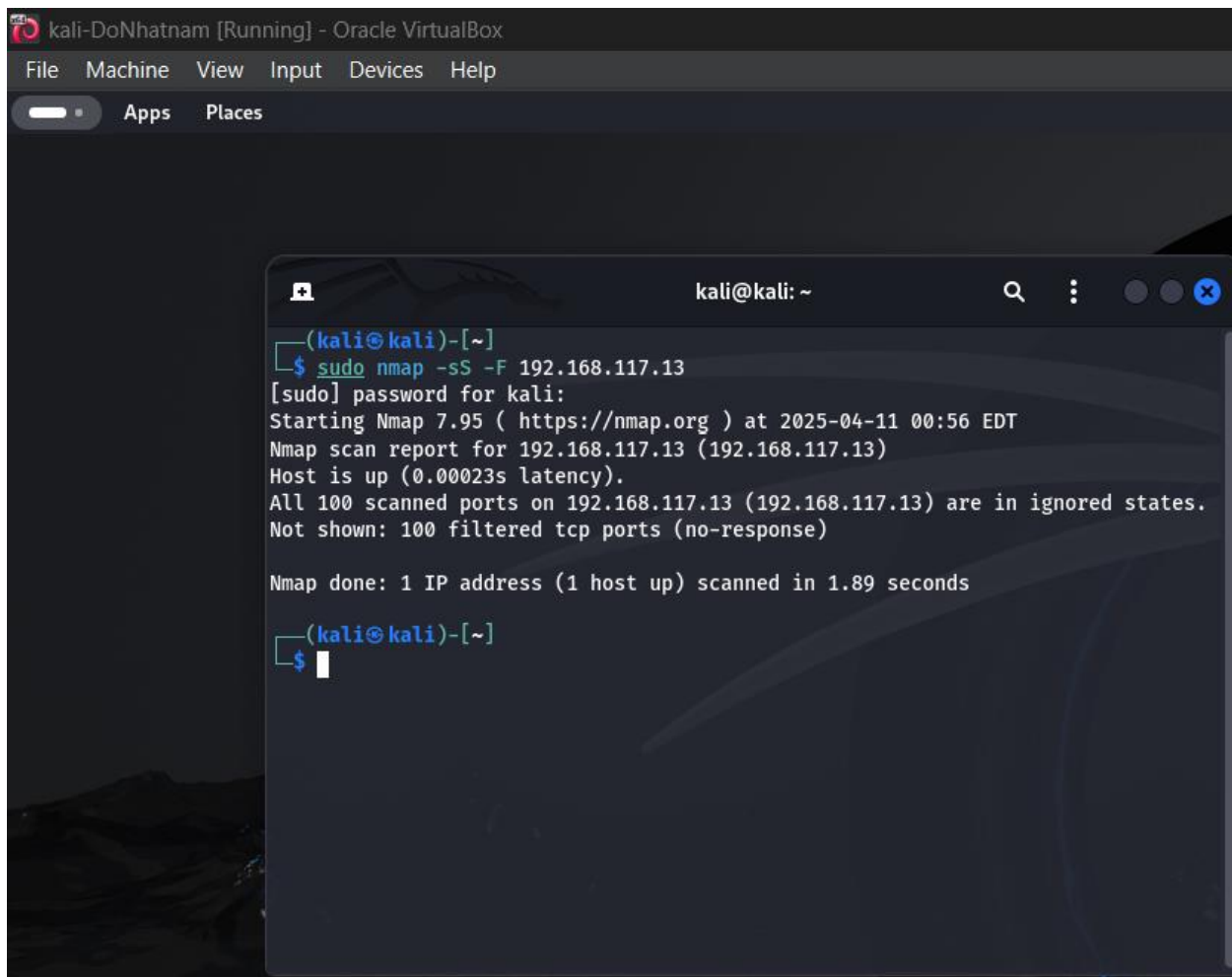


### 3.1.2. Kịch bản 2

Thực hiện lệnh quét `nmap -sS -F Địa_chỉ_IP_máy_mục_tujuan` trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là `task2.pcap`.

Trả lời: Khi thực hiện lệnh `sudo nmap -sS -F 192.168.117.13` trên máy do thám, kỹ thuật quét được sử dụng là TCP SYN Scan, hay còn gọi là quét nửa mở (Half-open scan). Đây là một kỹ thuật quét phổ biến vì nó nhanh, hiệu quả và ít bị phát hiện hơn so với các phương pháp khác. Trong quá trình quét, Nmap gửi các gói TCP có cờ SYN đến các cổng

trên máy mục tiêu để bắt đầu tiến trình bắt tay TCP. Nếu máy mục tiêu phản hồi bằng gói SYN-ACK, điều đó cho thấy cổng đang mở, và ngay sau đó Nmap sẽ gửi một gói RST để hủy kết nối trước khi hoàn tất quá trình bắt tay, do đó gọi là quét nửa mở. Nếu cổng đóng, máy mục tiêu sẽ phản hồi bằng gói RST. Nếu không có phản hồi hoặc nhận được thông báo ICMP unreachable, có thể xác định rằng cổng đang bị lọc bởi tường lửa. Khi bắt lưu lượng trên máy do thám bằng công cụ như tcpdump hoặc Wireshark, ta có thể quan sát thấy các gói SYN được gửi đi, SYN-ACK hoặc RST được nhận về, và các gói RST được gửi lại từ máy do thám, xác nhận rằng kỹ thuật TCP SYN Scan đã được sử dụng trong quá trình quét.



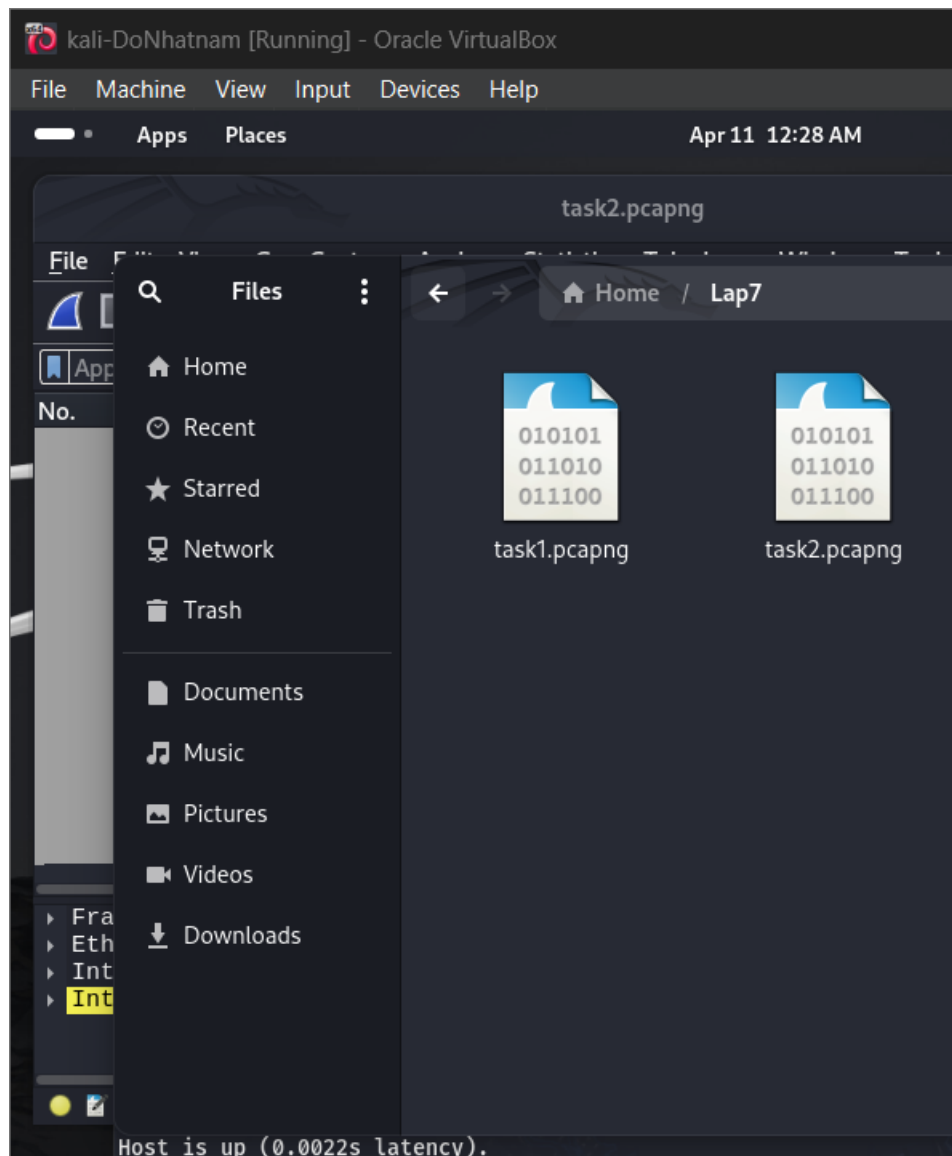
```
kali-DoNhatnam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places

kali@kali: ~
(kali@kali)-[~]
$ sudo nmap -sS -F 192.168.117.13
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 00:56 EDT
Nmap scan report for 192.168.117.13 (192.168.117.13)
Host is up (0.00023s latency).
All 100 scanned ports on 192.168.117.13 (192.168.117.13) are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds

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



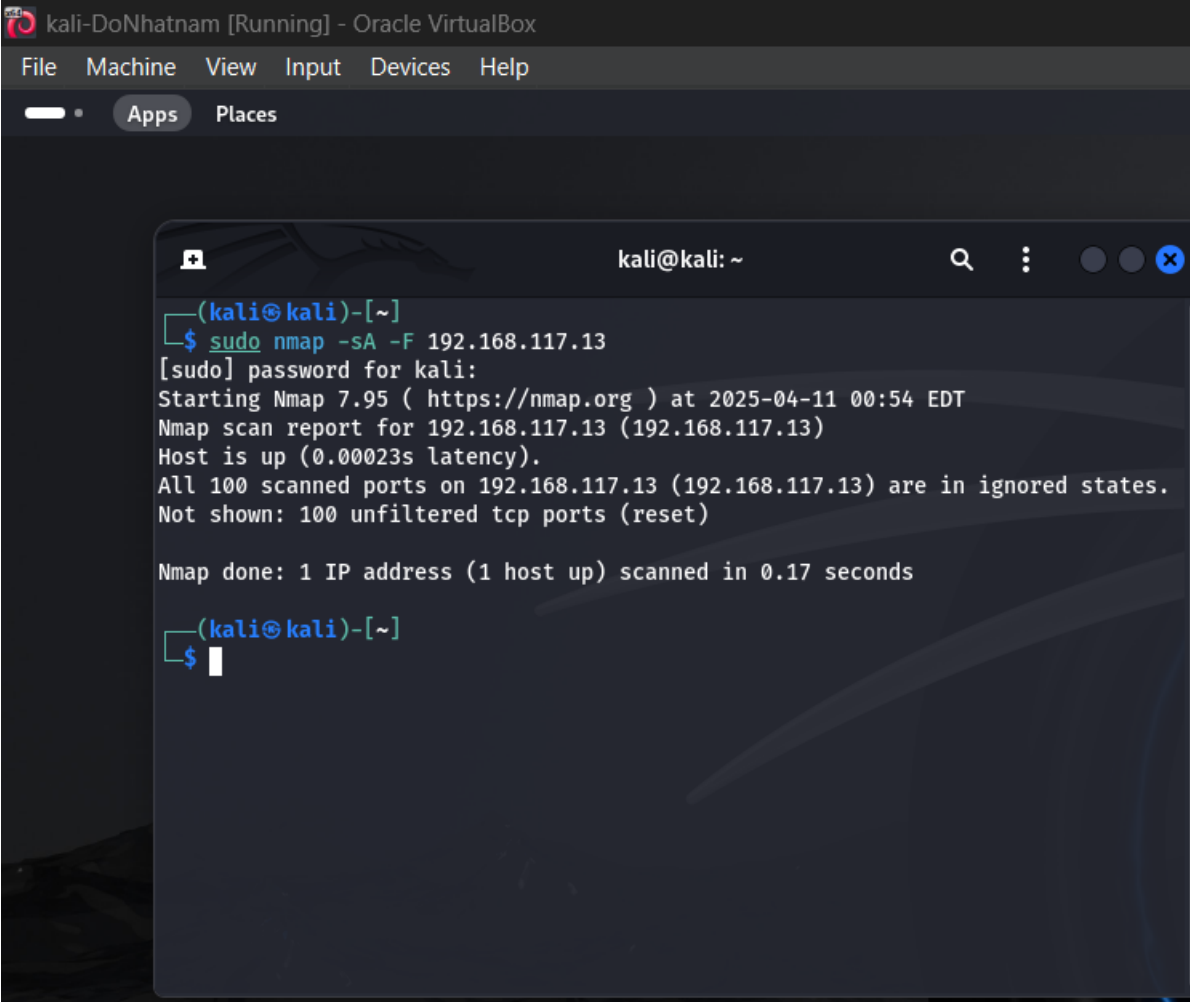


### 3.1.3. Kịch bản 3

Thực hiện lệnh quét `nmap -sA -F Địa_chi_IP_máy_mục_tujuan` trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là `task3.pcap`.

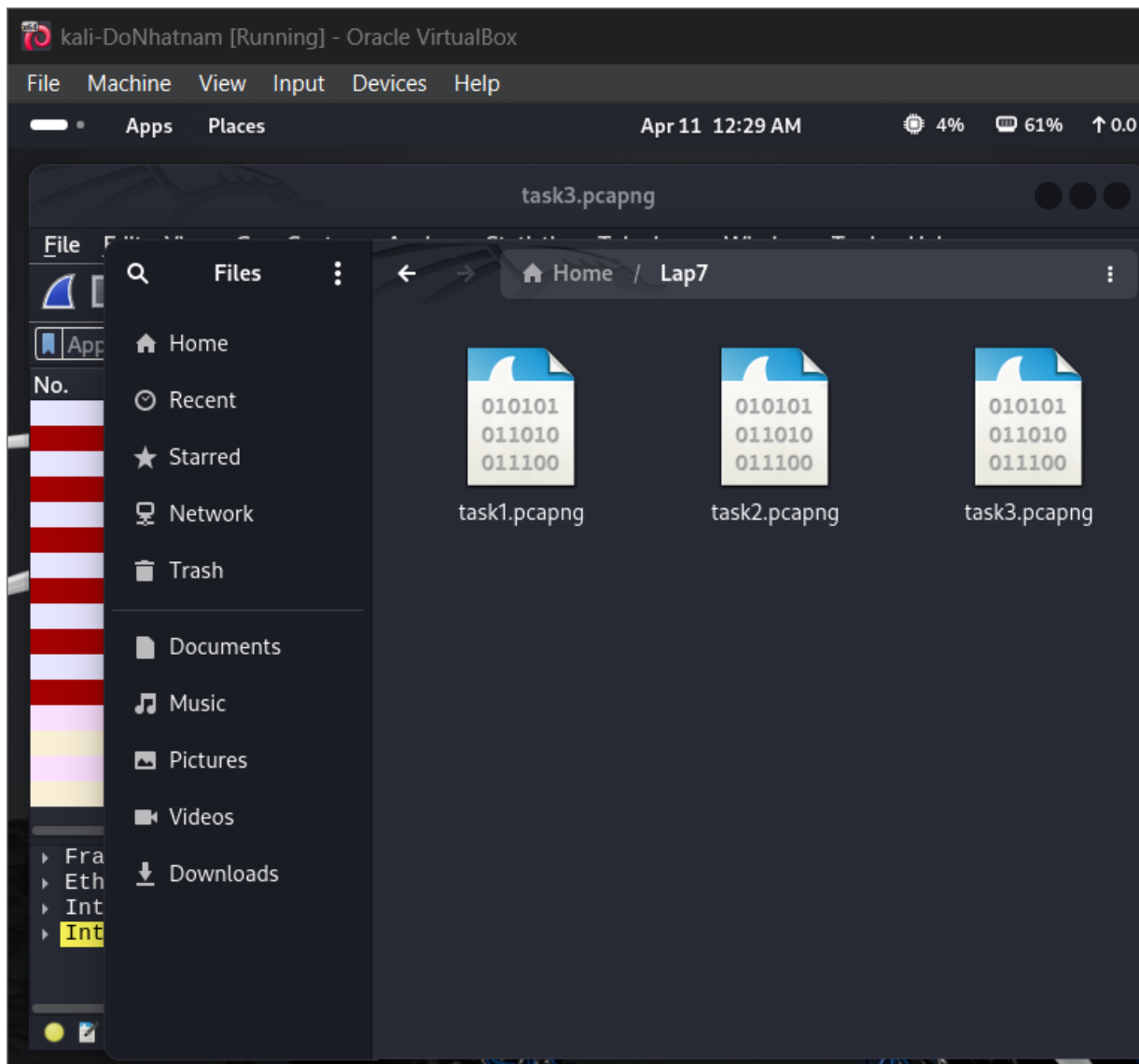
Trả lời: Khi thực hiện lệnh `sudo nmap -sA -F 192.168.117.13` trên máy do thám, ta đang sử dụng kỹ thuật quét ACK Scan. Đây là một kỹ thuật quét nhằm xác định xem các cổng trên máy mục tiêu có được lọc bởi tường lửa hay không, chứ không nhằm xác định trạng thái mở hoặc đóng của cổng. Trong quá trình quét, Nmap sẽ gửi các gói tin TCP có

cờ ACK đến các cổng đích. Nếu nhận được phản hồi là gói RST từ máy mục tiêu, điều đó cho thấy cổng không bị lọc. Ngược lại, nếu không có phản hồi hoặc nhận được thông báo lỗi ICMP unreachable, thì có thể kết luận rằng cổng đã bị lọc. Để phân tích kỹ thuật quét này, ta có thể sử dụng công cụ tcpdump hoặc Wireshark để bắt và lưu lại lưu lượng mạng trên máy do thám.



The screenshot shows a Kali Linux virtual machine window titled "kali-DoNhatnam [Running] - Oracle VirtualBox". Inside the VM, a terminal window is open with the prompt "kali@kali: ~". The user has entered the command `sudo nmap -sA -F 192.168.117.13`. The terminal output shows the Nmap scan results for 192.168.117.13, indicating that the host is up and all 100 scanned ports are in ignored states.

```
(kali@kali)-[~]  
$ sudo nmap -sA -F 192.168.117.13  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 00:54 EDT  
Nmap scan report for 192.168.117.13 (192.168.117.13)  
Host is up (0.00023s latency).  
All 100 scanned ports on 192.168.117.13 (192.168.117.13) are in ignored states.  
Not shown: 100 unfiltered tcp ports (reset)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds  
  
(kali@kali)-[~]  
$
```



### 3.2. Thu thập thông tin hệ thống

Sử dụng nmap để xác định nút mạng trong mạng 192.168.100.0 /24 cung cấp dịch vụ email. Sử dụng nmap để quét, thu thập thông tin về hệ điều hành và các dịch vụ trên nút mạng này. Sử dụng Wireshark để bắt lưu trên máy do thám. Hãy cho biết thông tin các dịch vụ đang được cung cấp trên máy mục tiêu. Lưu lại file lưu lượng trên máy do thám với tên là task4.pcap.

Trả lời: Khi sử dụng Nmap để xác định các nút mạng trong dải địa chỉ 192.168.100.0/24 có cung cấp dịch vụ email, ta thực hiện lệnh `nmap -p`

25,110,143,465,587,993,995 192.168.100.0/24 trên máy do thám. Đây là các cổng tiêu chuẩn của các dịch vụ email như SMTP, POP3, IMAP và các biến thể mã hóa SSL/TLS của chúng. Sau khi xác định được máy chủ nào đang mở các cổng này, tức là có khả năng đang cung cấp dịch vụ email, ta tiếp tục sử dụng lệnh `nmap -A <Địa_chỉ_IP_máy_mục_tujuan>` để quét sâu hơn, thu thập thông tin về hệ điều hành, các dịch vụ đang chạy, phiên bản phần mềm và các cấu hình liên quan. Trong khi thực hiện các lệnh này, ta đồng thời sử dụng Wireshark trên máy do thám để bắt và lưu lại lưu lượng mạng nhằm phục vụ việc phân tích sau này. Trong quá trình phân tích file .pcap thu được từ Wireshark, ta có thể kiểm tra các gói tin TCP liên quan đến các cổng email đã liệt kê để xác định dịch vụ cụ thể như SMTP (cổng 25 hoặc 587), POP3 (cổng 110 hoặc 995), IMAP (cổng 143 hoặc 993), cũng như quan sát thông tin banner hoặc phản hồi từ phía máy chủ, từ đó xác định được phần mềm đang sử dụng ví dụ như Postfix, Exim, Dovecot hay Microsoft Exchange. Như vậy, thông qua việc quét Nmap và phân tích lưu lượng bằng Wireshark, ta có thể xác định được IP của nút mạng đang cung cấp dịch vụ email trong mạng 192.168.100.0/24 cũng như thu thập chi tiết các dịch vụ và hệ điều hành mà máy mục tiêu đang sử dụng.

kali-DoNhatnam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apr 11 1:04 AM 19% 58% ↑ 0.0 kB

kali@kali: ~

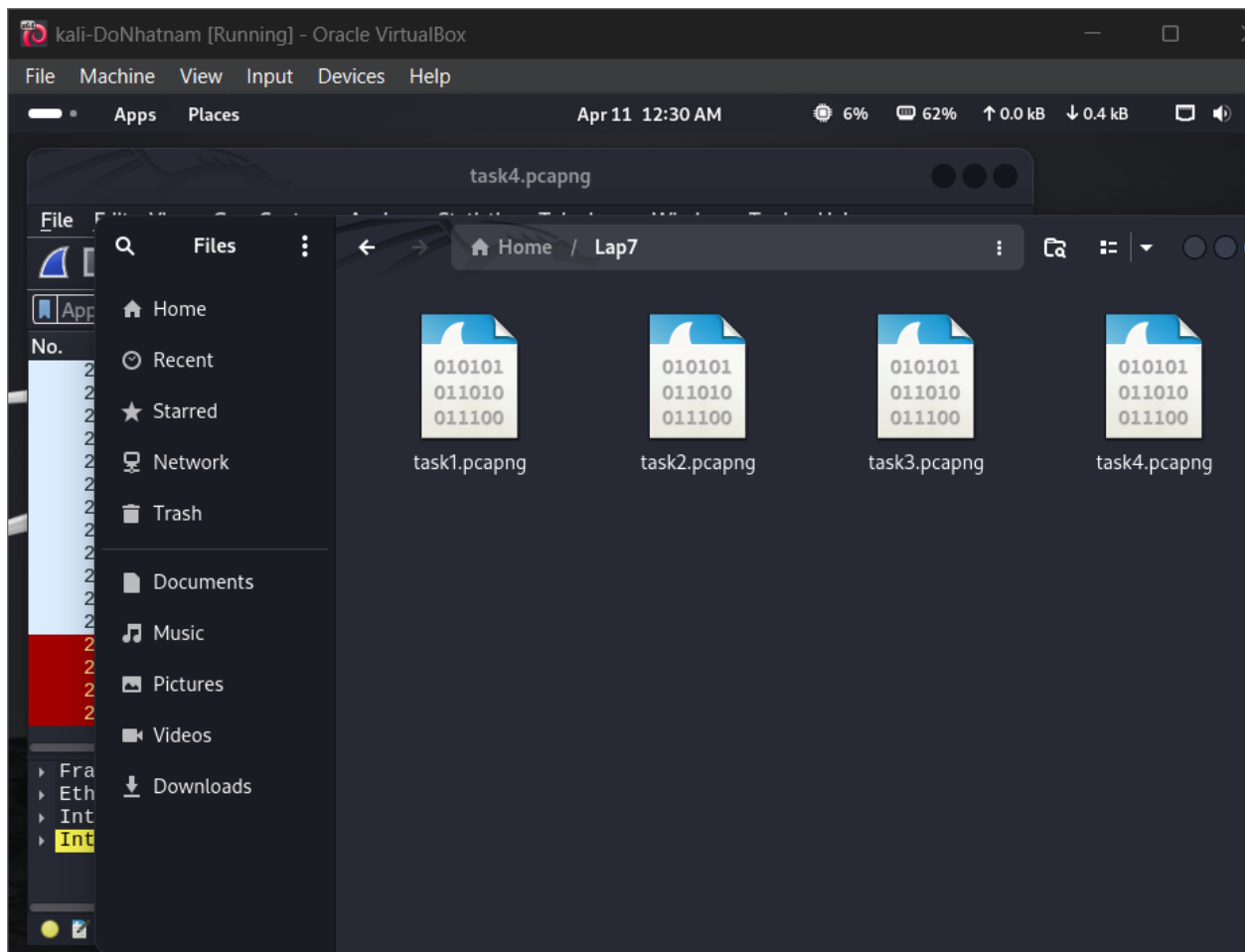
```
$ sudo nmap -p 25,110,143,465,587,993,995 192.168.100.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 01:02 EDT
Nmap scan report for 192.168.100.0 (192.168.100.0)
Host is up (0.00086s latency).
PORT      STATE SERVICE
25/tcp    filtered smtp
110/tcp    filtered pop3
143/tcp    filtered imap
465/tcp    filtered smtps
587/tcp    filtered submission
993/tcp    filtered imaps
995/tcp    filtered pop3s

Nmap scan report for 192.168.100.1 (192.168.100.1)
Host is up (0.00074s latency).
PORT      STATE SERVICE
25/tcp    filtered smtp
110/tcp    filtered pop3
143/tcp    filtered imap
465/tcp    filtered smtps
587/tcp    filtered submission
993/tcp    filtered imaps
```

File Edit View Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length
4791	44.825763695	10.0.2.15	192.168.100.183	TCP	58
4792	44.828955540	10.0.2.15	192.168.100.184	TCP	58
4793	44.831397290	10.0.2.15	192.168.100.185	TCP	58
4794	44.834227213	10.0.2.15	192.168.100.186	TCP	58
4795	44.904386575	10.0.2.15	192.168.100.189	TCP	58
4796	44.912659912	10.0.2.15	192.168.100.192	TCP	58
4797	44.915619935	10.0.2.15	192.168.100.195	TCP	58
4798	44.919266782	10.0.2.15	192.168.100.196	TCP	58
4799	44.923318827	10.0.2.15	192.168.100.197	TCP	58
4800	44.925774987	10.0.2.15	192.168.100.198	TCP	58
4801	44.928273383	10.0.2.15	192.168.100.201	TCP	58
4802	44.931196208	10.0.2.15	192.168.100.202	TCP	58
4803	44.933777137	10.0.2.15	192.168.100.203	TCP	58
4804	44.936771211	10.0.2.15	192.168.100.204	TCP	58
4805	45.018975457	10.0.2.15	192.168.100.207	TCP	58
4806	45.019333383	10.0.2.15	192.168.100.210	TCP	58
4807	45.019333383	10.0.2.15	192.168.100.213	TCP	58



### 3.3. Tìm kiếm thông tin về các lỗ hổng

Dựa vào kết quả quét ở phần 2, hãy lập báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ. Thông tin về các lỗ hổng có thể tìm kiếm trên <https://www.cvedetails.com/>

Phần mềm dịch vụ (tên dịch vụ, tên phần mềm, phiên bản)	Số CVE	Mô tả ngắn gọn về lỗ hổng
SSH - OpenSSH 7.2p2	CVE-2016-10012	Lỗi trong xử lý X11 forwarding có thể bị khai thác để nâng quyền

Telnet - GNU inetutils 1.9.4	CVE-2019-0053	Lỗi tràn bộ đệm có thể cho phép thực thi mã từ xa
DNS - BIND 9.10.3	CVE-2016-2776	Lỗi trong xử lý gói tin DNS có thể gây tấn công từ chối dịch vụ