BÁO CÁO BÀI THỰC HÀNH SỐ 7

**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

***Họ và tên sinh viên:*** ***Trần Kim Thiện***

***MSSV: 1050080076***

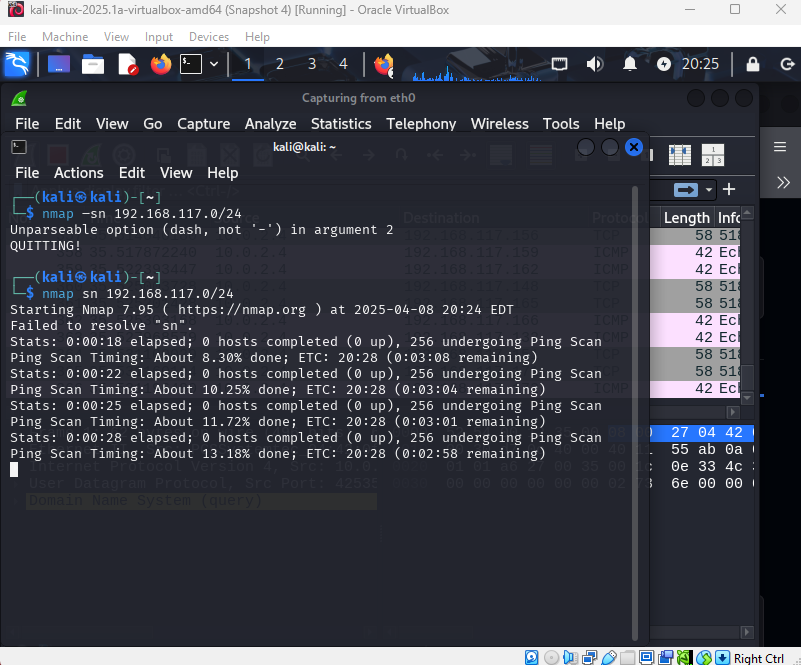
***Yêu cầu kết quả thực hành:***

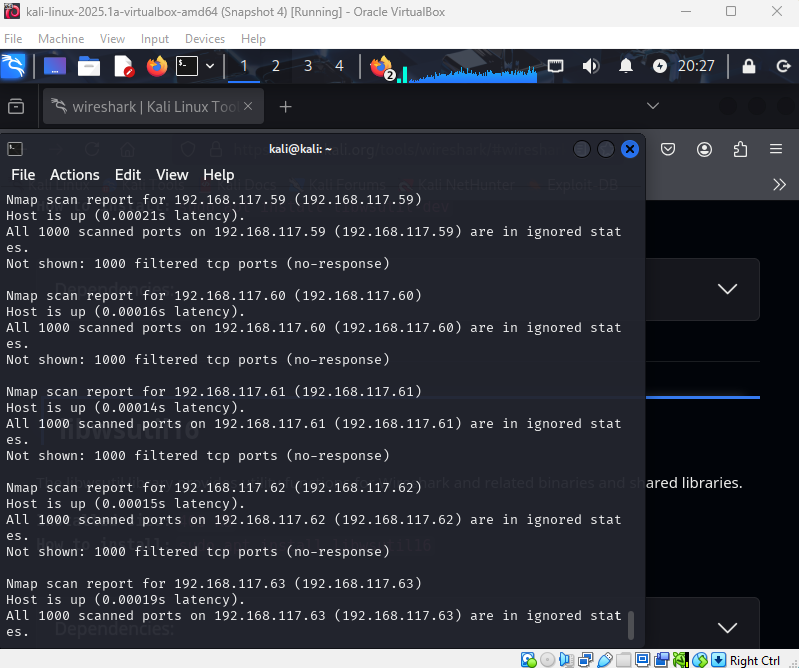
Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07

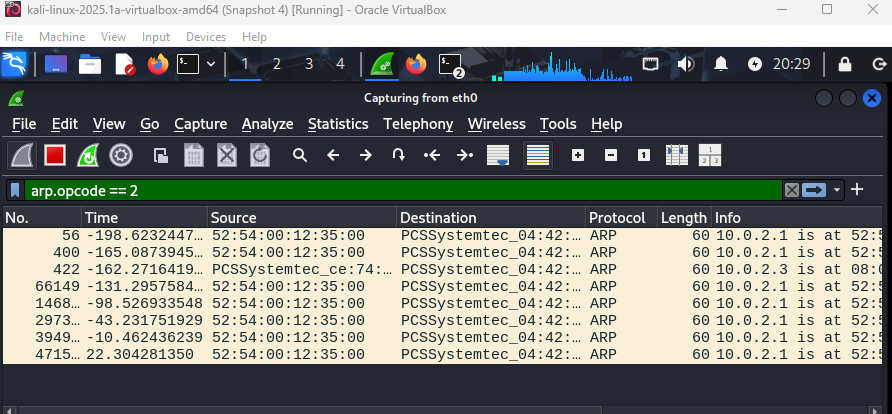
* Báo cáo kết quả thực hành
* File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.

**KẾT QUẢ THỰC HÀNH**

1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

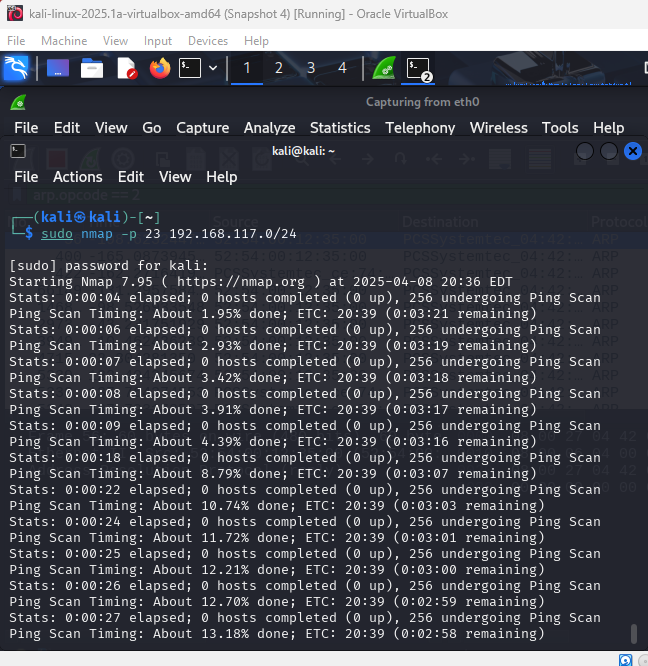


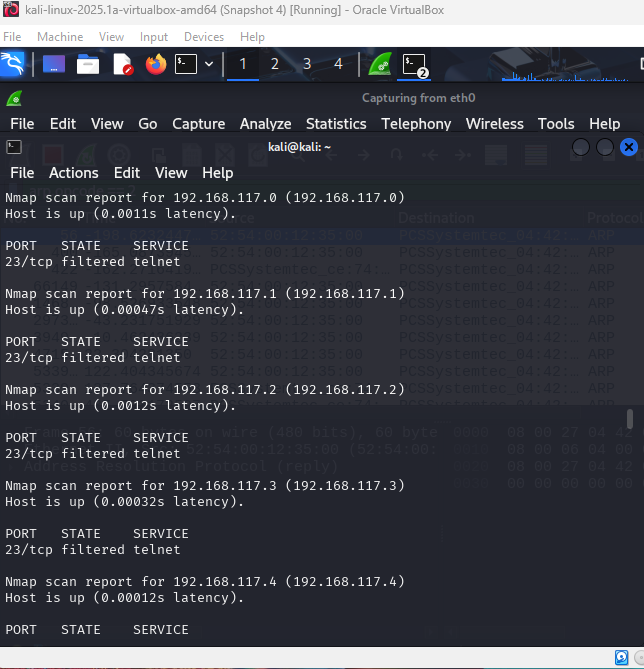
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì

Trên cửa sổ của Wireshark, ta 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

🡪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

* 1. **Kịch bản 2**
* Ảnh chụp kết quả thực hiện của nmap:

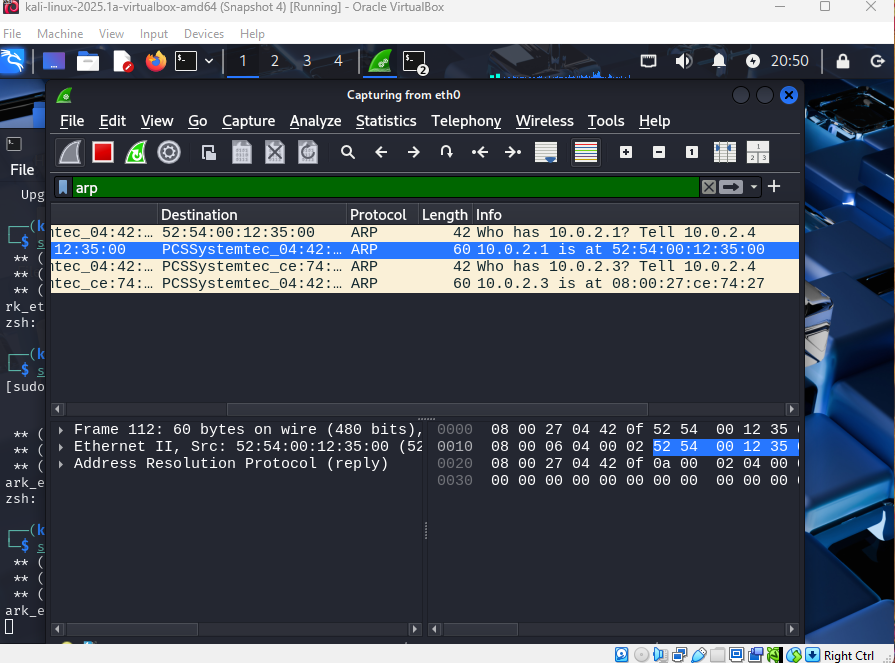




Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng filtered telnet.

* Ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

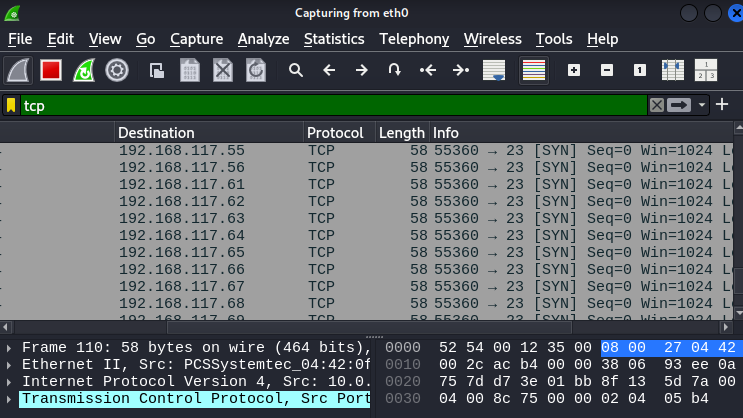
- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là ?



ARP Request: Máy có địa chỉ IP 10.0.2.4 (địa chỉ được hiển thị trong cột "Source" của các gói tin ARP Request) gửi đi các gói tin ARP Request để hỏi địa chỉ MAC của các máy có địa chỉ IP 10.0.2.1 và 10.0.2.3. Gói tin ARP Request có opcode là 1.

ARP Reply: Các máy có địa chỉ IP 10.0.2.1 và 10.0.2.3 sau đó trả lời bằng các gói tin ARP Reply, cung cấp địa chỉ MAC tương ứng của chúng. Gói tin ARP Reply có opcode là 2.

* Dựa trên đặc điểm lưu lượng ARP Request và ARP Reply này, kỹ thuật quét thăm dò được sử dụng là ARP Ping Scan.

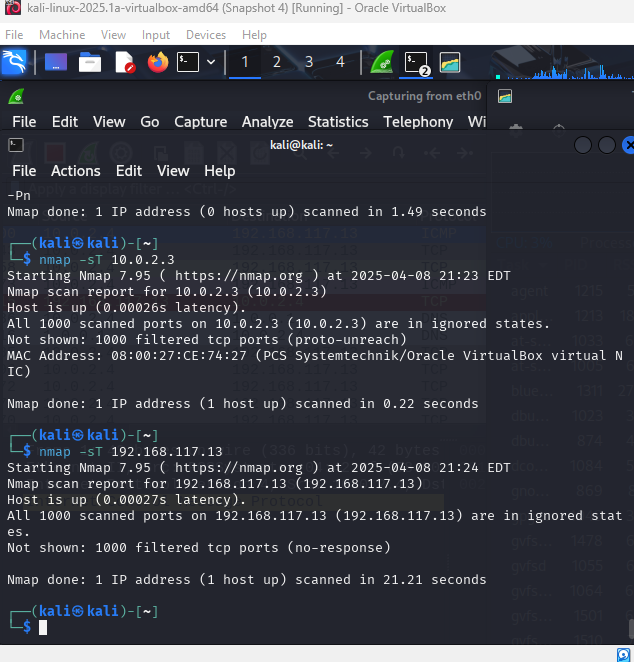


Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark ta có thể thấy gói tin TCP SYN được gửi từ cổng 23 từ địa chỉ 192.168.117.55 về máy tấn công

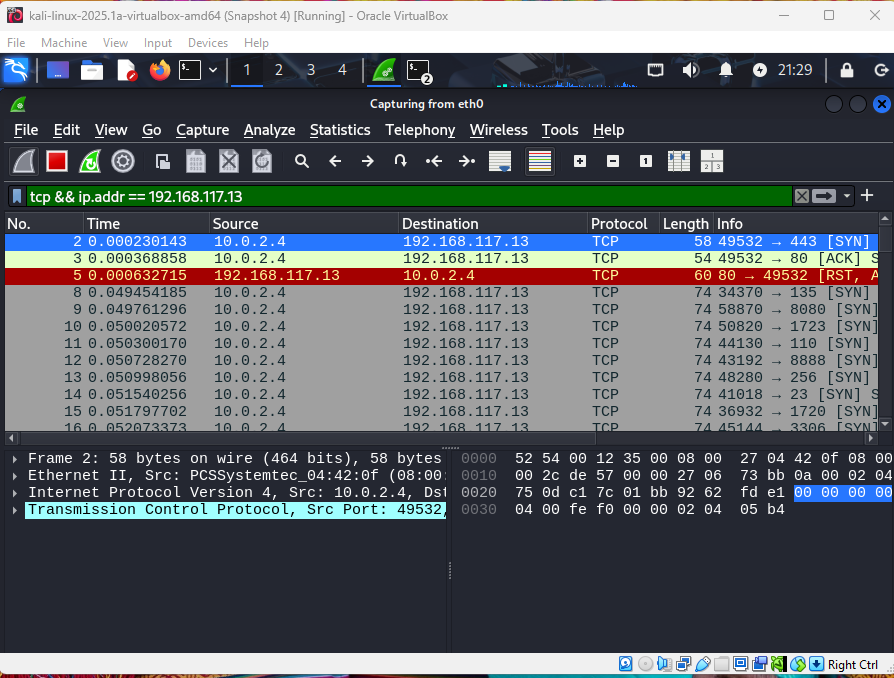
Gói tin mà ta thấy trong Wireshark là một gói tin TCP SYN được gửi từ cổng 23 của máy mục tiêu (192.168.117.55) về máy tấn công. Điều này là dấu hiệu cho thấy máy tấn công đã gửi một gói tin TCP SYN đến cổng 23 của máy mục tiêu, và máy mục tiêu đang phản hồi.

Kỹ thuật quét thăm dò:

* 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
  1. **Kịch bản 3**
* Ảnh chụp kết quả thực hiện của nmap:



* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì ?

**

Chúng ta có thể thấy một chuỗi tương tự các gói tin SYN, SYN/ACK, ACK và RST/ACK cho các cổng khác như 135 (msrpc), 445 (microsoft-ds) và 3389 (ms-wbt-server). Điều này cho thấy Nmap đang thăm dò nhiều cổng khác nhau trên máy mục tiêu.

Đặc điểm lưu lượng này (SYN -> SYN/ACK -> ACK -> RST) là dấu hiệu rõ ràng của kỹ thuật TCP Connect Scan (-sT). Trong kỹ thuật này, Nmap cố gắng thiết lập một kết nối TCP đầy đủ với từng cổng mục tiêu. Nếu cổng đang mở, quá trình bắt tay ba bước sẽ được hoàn thành (SYN, SYN/ACK, ACK), và sau đó Nmap sẽ gửi một gói tin RST để đóng kết nối. Nếu cổng đang đóng, máy mục tiêu sẽ trả lời bằng một gói tin RST ngay sau khi nhận được gói tin SYN.

* Đây là kỹ thuật quét thăm dò TCP Connect Scan.

1. **Thu thập thông tin hệ thống**

* Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì?

Để tìm kiếm máy chủ email trong một mạng, ta có thể sử dụng Nmap để quét các cổng dịch vụ email phổ biến

nmap -p 25,110,143,465,993,995 <địa\_chỉ\_mạng> / <mask>

nmap -p 25,110,143,465,993,995 192.168.100.0/24

* Giải thích các tham số sử dụng trong lệnh này?(1 điểm)

nmap: Lệnh gọi công cụ Nmap.

-p 25,110,143,465,993,995: Tham số này chỉ định các cổng cần quét.

25: SMTP (Simple Mail Transfer Protocol) - Giao thức truyền tải thư tín đơn giản.

110: POP3 (Post Office Protocol version 3) - Giao thức lấy thư từ máy chủ về máy khách.

143: IMAP (Internet Message Access Protocol) - Giao thức quản lý thư tín Internet.

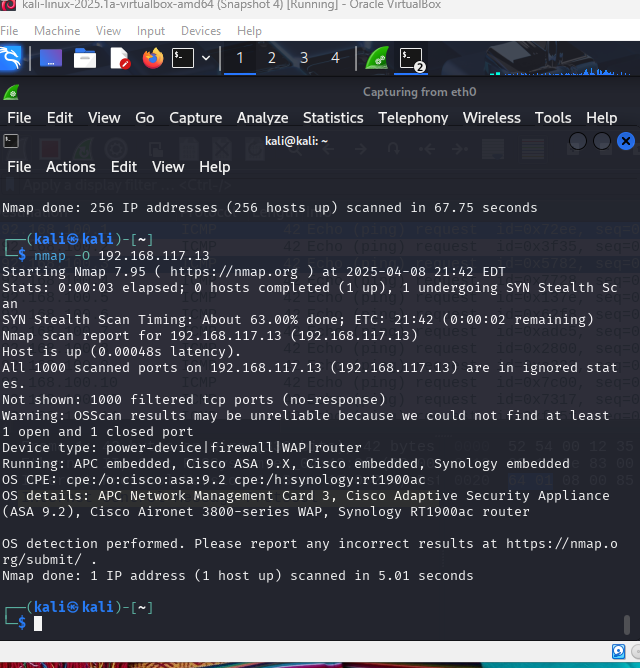
465: SMTPS (SMTP Secure) - SMTP qua SSL/TLS.

993: IMAPS (IMAP Secure) - IMAP qua SSL/TLS.

995: POP3S (POP3 Secure) - POP3 qua SSL/TLS.

**Thông tin hệ điều hành:**

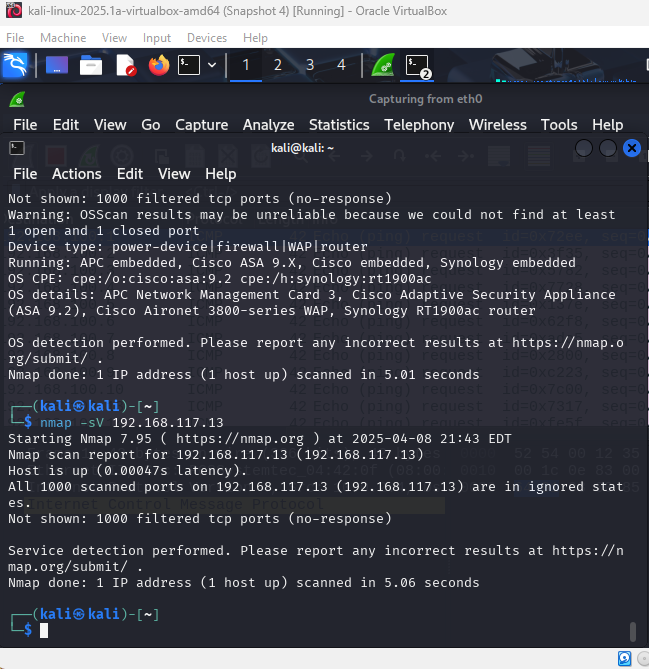
* Hình ảnh chụp kết quả của nmap:



* Nêu tên và phiên bản hệ điều hành: Cisco phiên bản 9.2

**Thông tin dịch vụ**

* Hình ảnh chụp kết quả của nmap:



* Danh sách dịch vụ

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | ssh | 22 | OpenSSH 7.6p1 Ubuntu 10 |
| 2 | http | 80 | Apache httpd 2.4.29 |
| 3 | rpcbind | 111 | (portmapper) 2-4 |

1. **Tìm kiếm thông tin về các lỗ hổng**

Báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ.

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
| OpenSSH 7.6p1 Ubuntu 10 | CVE-2018-15919 | Lỗ hổng từ chối dịch vụ trong quá trình phân tách quyền của OpenSSH do việc xử lý lỗi trong session\_pty\_cleanup có thể bị bỏ qua, dẫn đến việc giải phóng bộ nhớ sau khi sử dụng. |
| Apache httpd 2.4.29 | CVE-2019-0211 | Lỗ hổng double free trong module mod\_ssl khi sử dụng SSLVerifyClient với TLSv1.3. Lỗ hổng này có thể cho phép kẻ tấn công thực hiện tấn công từ chối dịch vụ hoặc có khả năng thực thi mã tùy ý |
| Microsoft Windows RPC | CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 | Đây là các lỗ hổng nghiêm trọng trong giao thức SMB (Server Message Block) v1 được sử dụng bởi Windows, cho phép kẻ tấn công từ xa thực thi mã tùy ý trên hệ thống mục tiêu. Mặc dù các cổng 49152-49155 thường được sử dụng cho RPC qua TCP/IP, các lỗ hổng SMB có thể liên quan đến các dịch vụ RPC nhất định |