BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Dương Vĩnh Toàn***

***MSSV: 1050080206***

***Yêu cầu kết quả thực hành:***

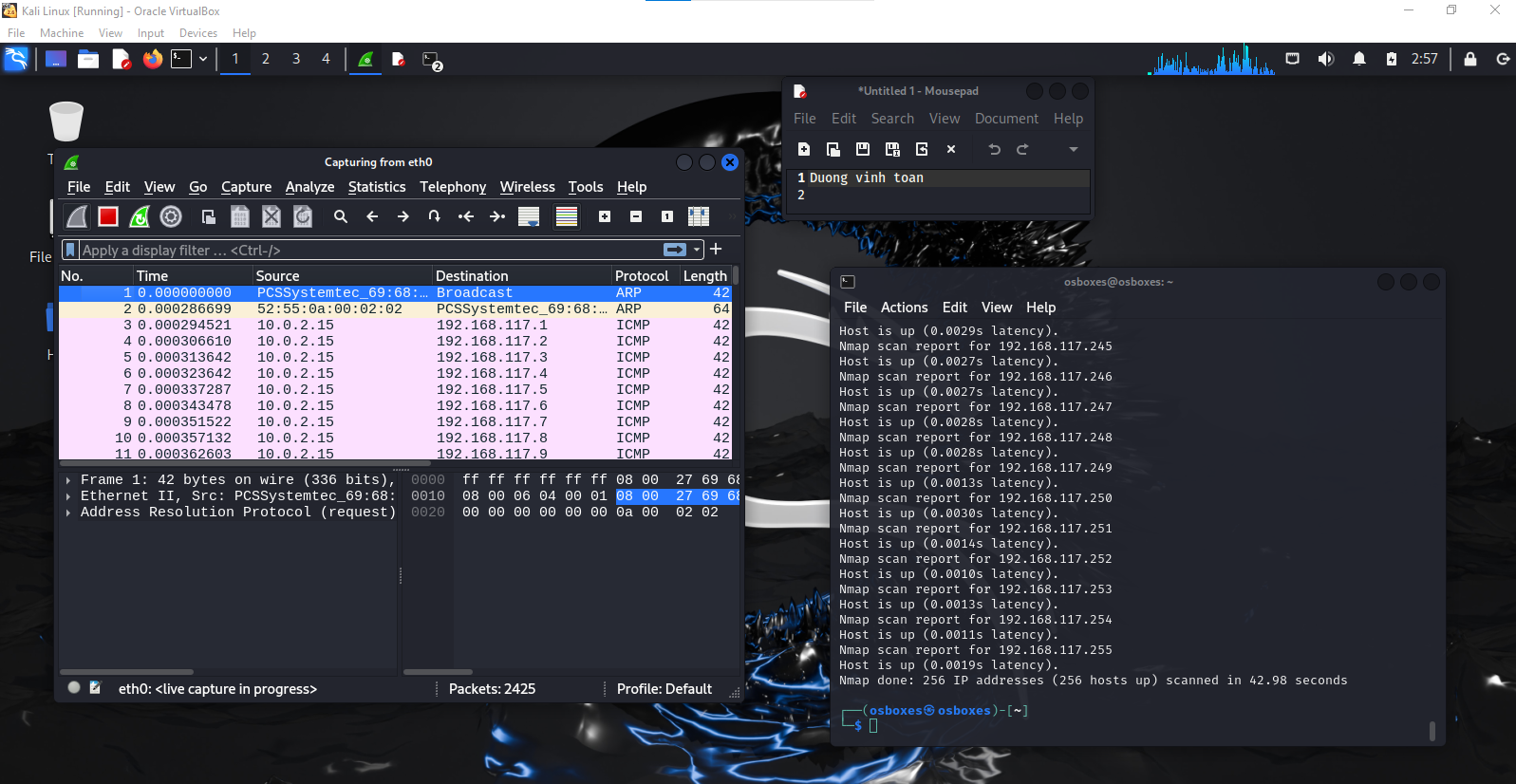
Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07

* 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**

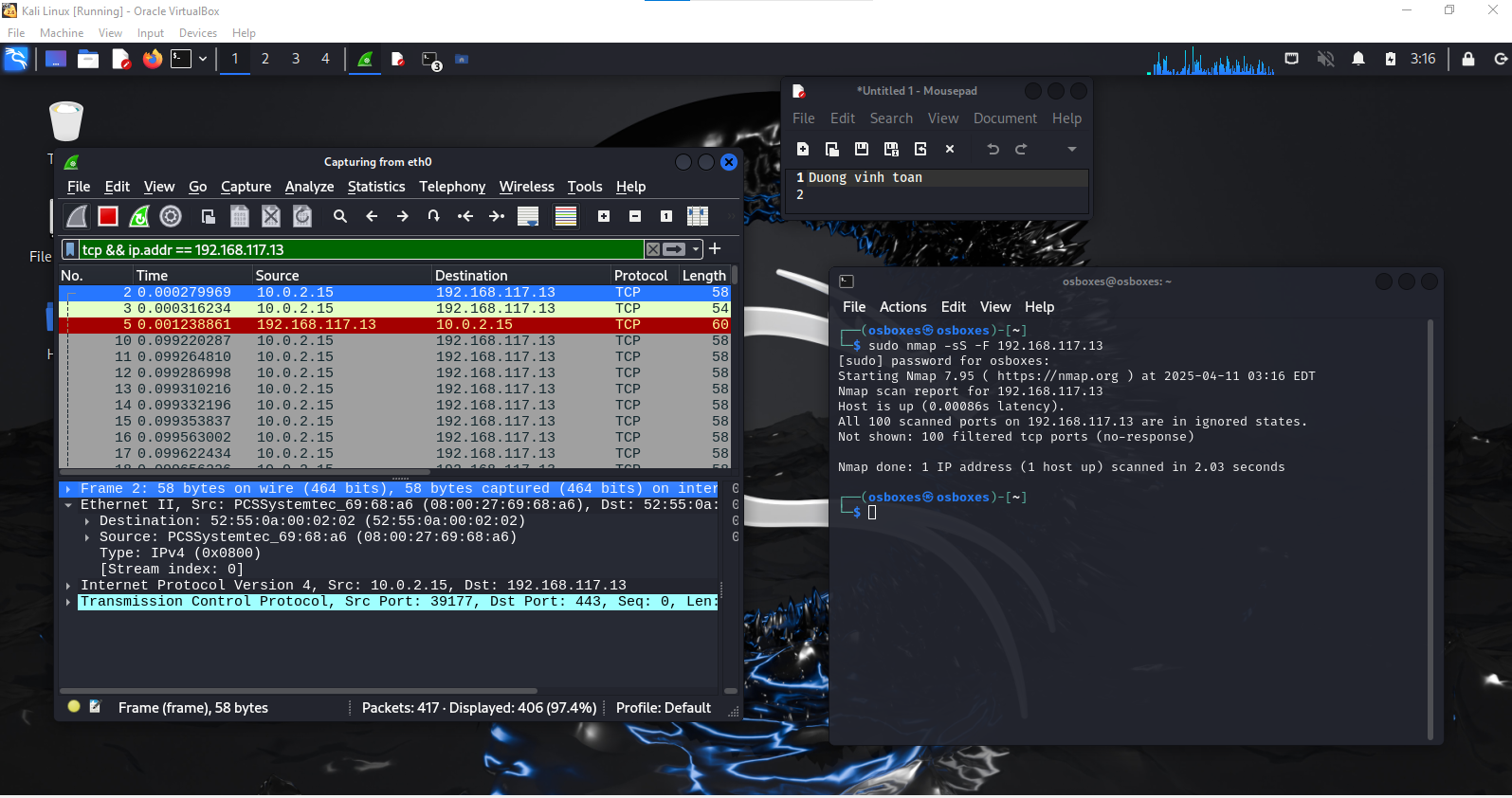
1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

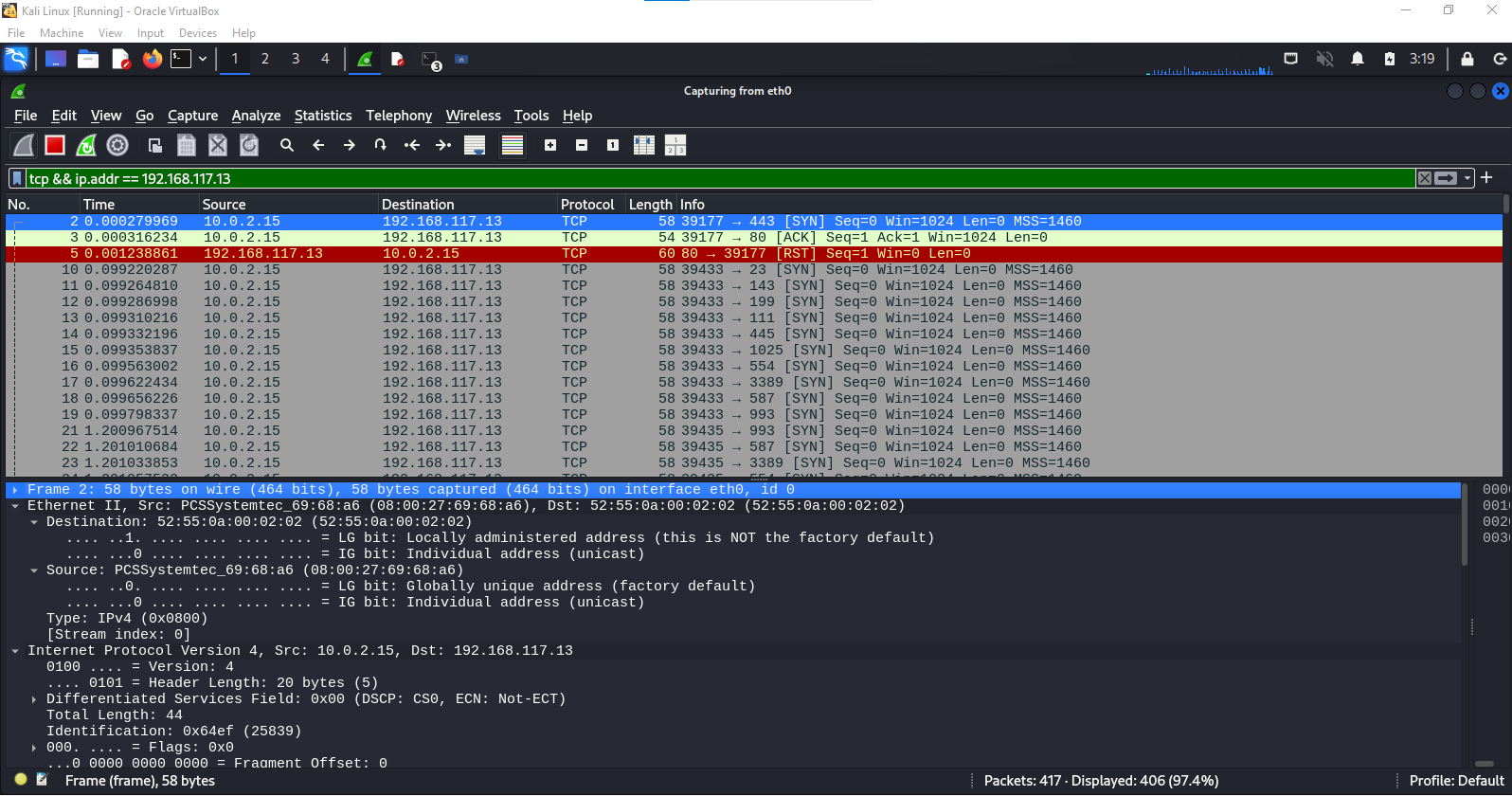
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

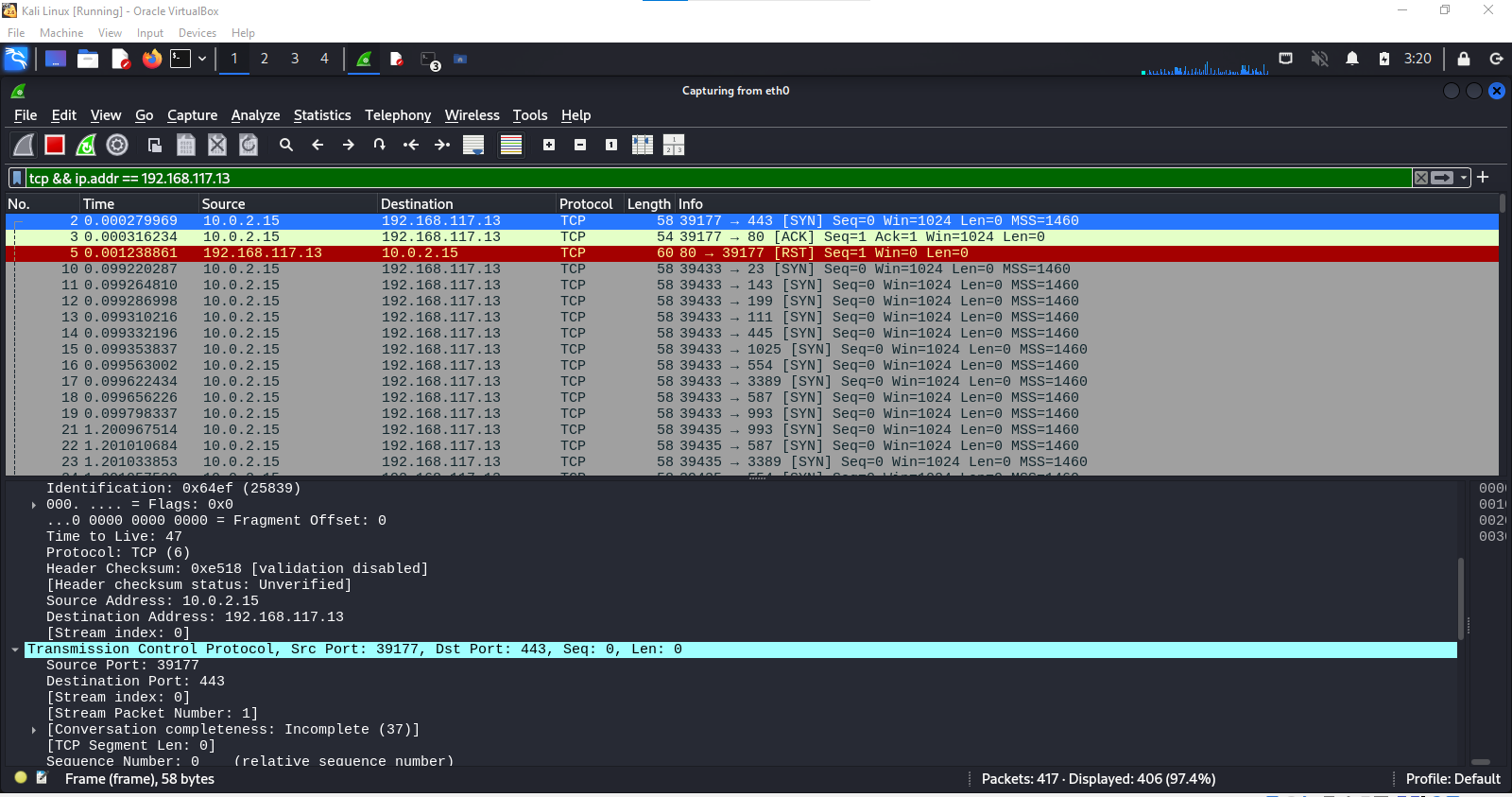


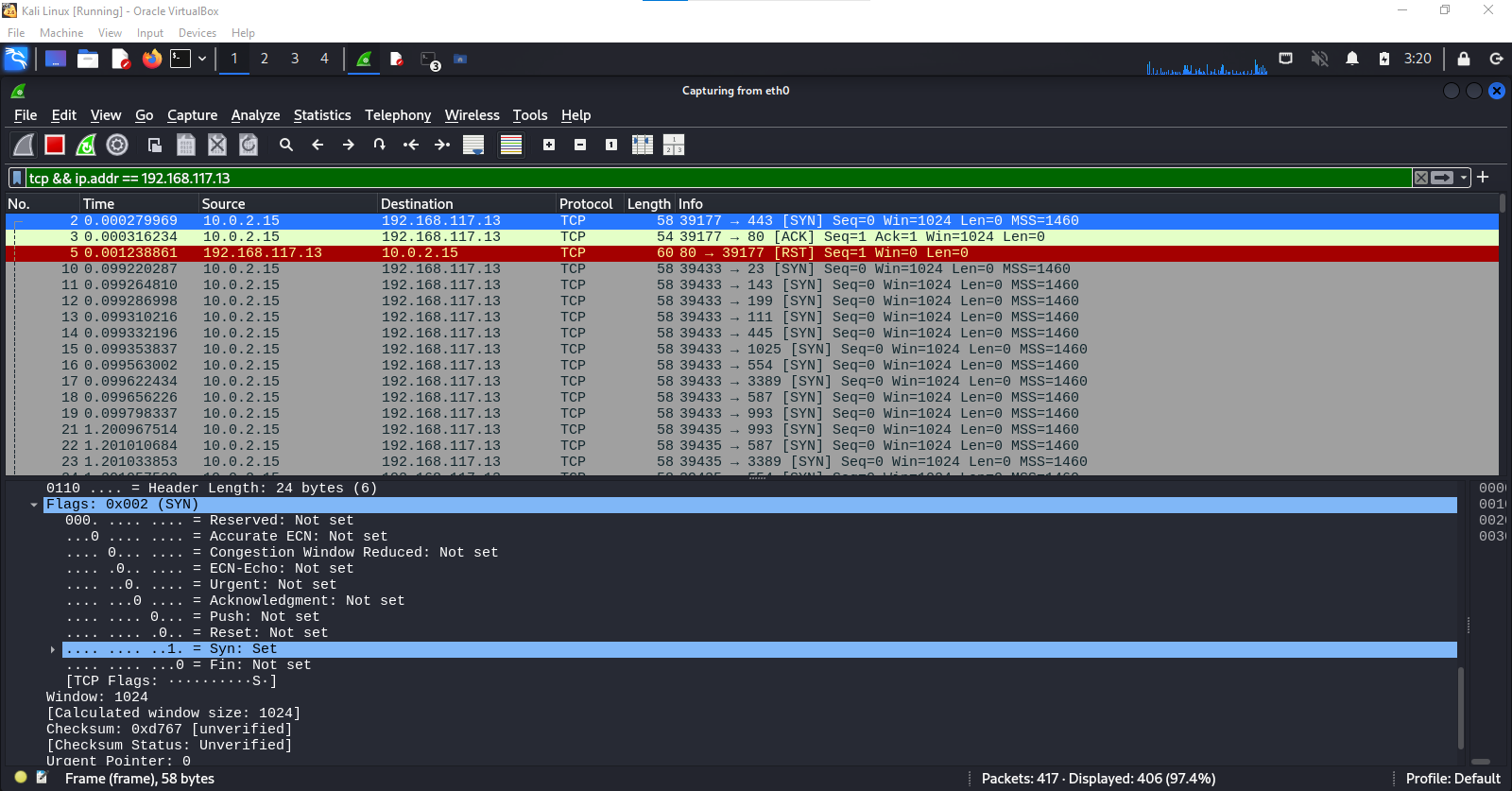
Kỹ thuật quét thăm dò được sử dụng là **ARP Ping Scan**. Dựa trên ảnh Wireshark cung cấp, có thể thấy các gói tin **ARP Request** được gửi đi từ máy do thám (có địa chỉ MAC là 52:55:0a:00:02:02) đến địa chỉ broadcast (ff:ff:ff:ff:ff:ff), thể hiện qua dòng "Who has 10.0.2.2? Tell 10.0.2.15". Đồng thời, xuất hiện các **ARP Reply** từ thiết bị đích phản hồi lại, ví dụ "10.0.2.2 is at 52:55:0a:00:02:02". Điều này chứng minh Nmap đang dùng kỹ thuật ARP để dò tìm xem máy nào đang bật trong mạng. Trong quá trình bắt gói không xuất hiện bất kỳ gói TCP hay ICMP nào, cho thấy đây không phải các kỹ thuật TCP SYN hay ICMP Ping, mà đúng là **ARP Ping Scan**.

* 1. **Kịch bản 2**



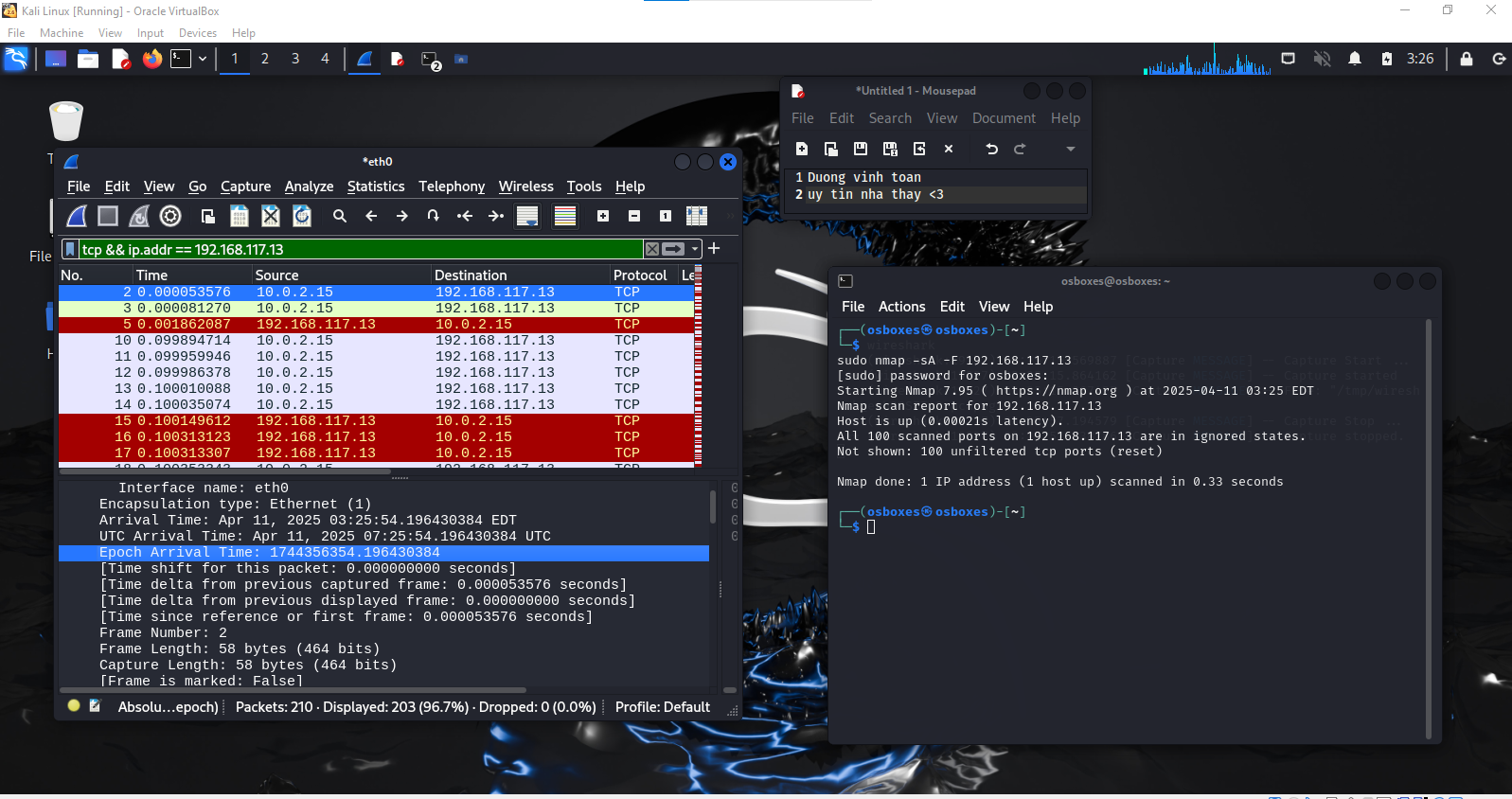


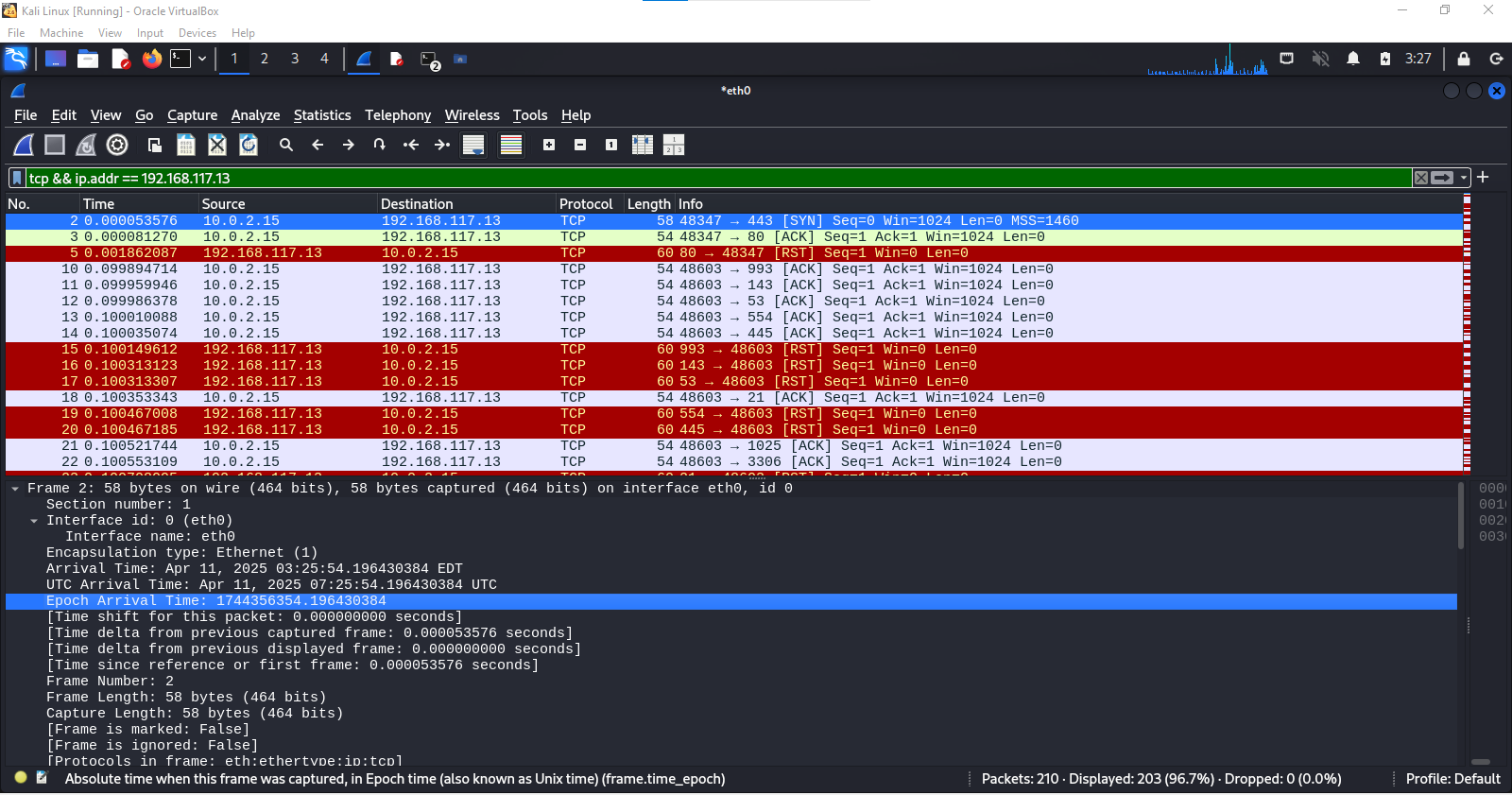


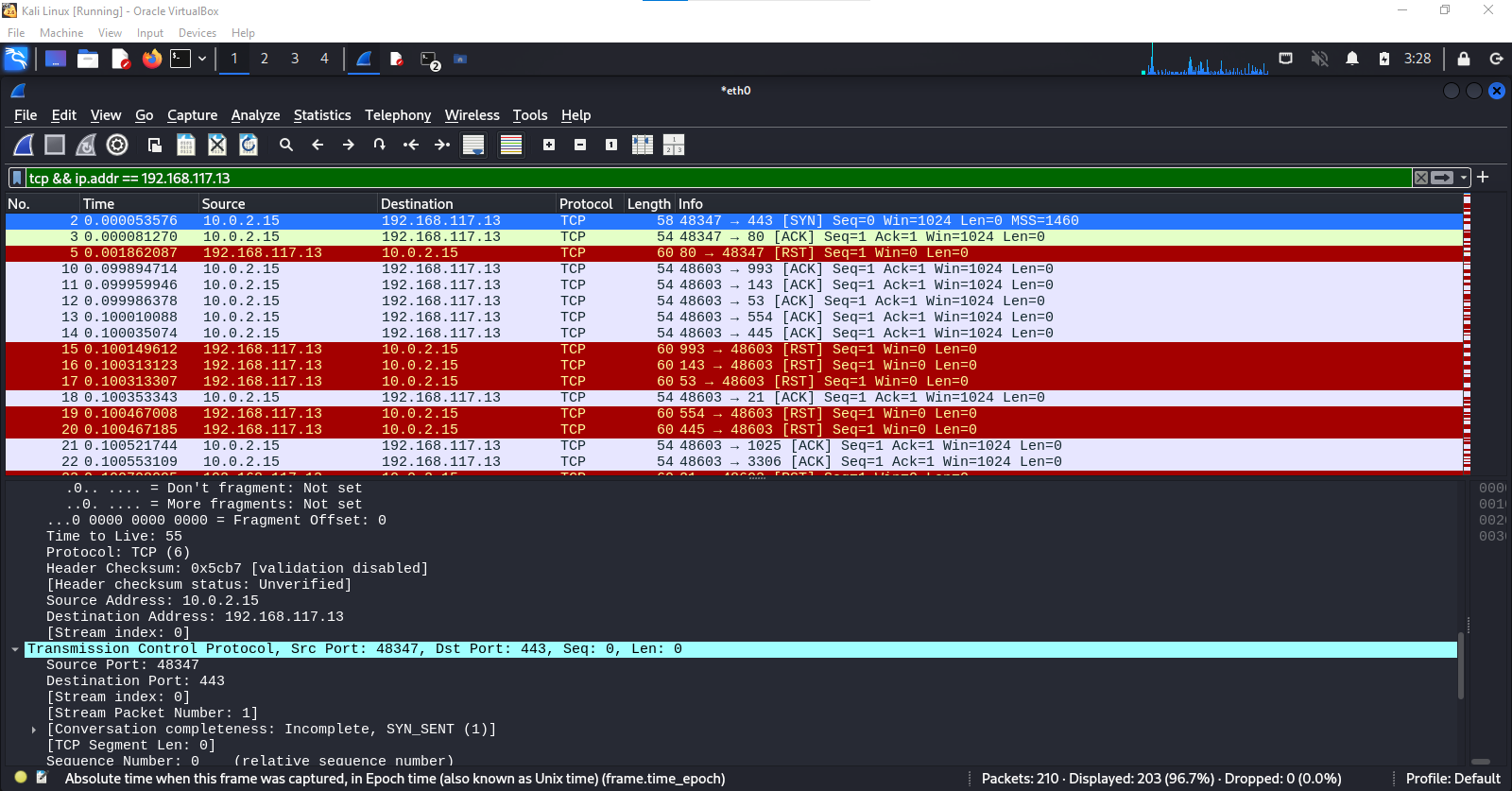


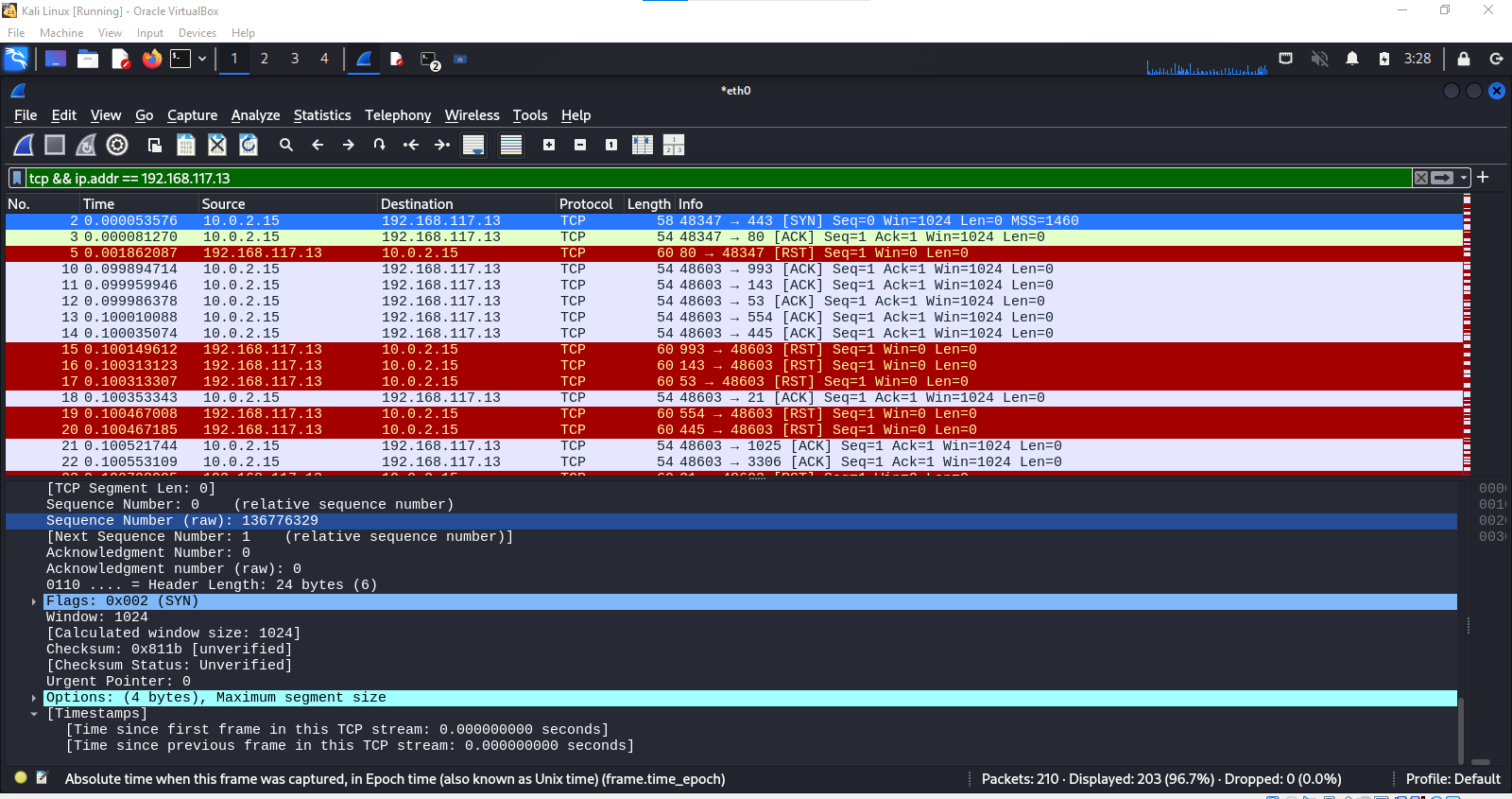
Kỹ thuật quét thăm dò được sử dụng là **TCP SYN Scan**. Trong ảnh Wireshark, có thể quan sát các gói tin TCP gửi từ máy do thám (IP 10.0.2.15) đến máy mục tiêu 192.168.117.13 với **cờ SYN (synchronization)** được bật, thể hiện qua dòng "Flags: 0x002 (SYN)" và "SYN: Set". Tiếp theo, có các gói phản hồi từ máy đích là **SYN+ACK** nếu cổng mở hoặc **RST (Reset)** nếu cổng đóng, như minh họa trong gói "TCP 80 → 39177 [RST]". Quá trình quét chỉ gửi SYN mà không hoàn tất bắt tay 3 bước TCP, điều này đặc trưng cho kỹ thuật bán kết nối – **TCP SYN Scan**.

* 1. **Kịch bản 3**









Kỹ thuật quét thăm dò được sử dụng là **TCP ACK Scan**. Trên ảnh Wireshark, có thể quan sát các gói tin TCP được gửi từ máy do thám đến địa chỉ IP 192.168.117.13 với cờ **ACK (Acknowledgment)** được bật. Điều này được thể hiện rõ ở phần Info của gói: "Flags: 0x10 (ACK)", "ACK: Set". Sau đó, máy mục tiêu phản hồi bằng các gói tin có **flag RST (Reset)** như "Flags: 0x14 (RST, ACK)". Việc gói ACK không nhằm thiết lập kết nối, mà chỉ để kiểm tra trạng thái phản hồi từ cổng, là đặc trưng của kỹ thuật **TCP ACK Scan**, dùng để **xác định cổng có bị firewall lọc hay không**.

1. **Thu thập thông tin hệ thống**

**Câu lệnh**

nmap -p 25,110,143,465,587,993,995 192.168.117.0/24

**Giải thích:**

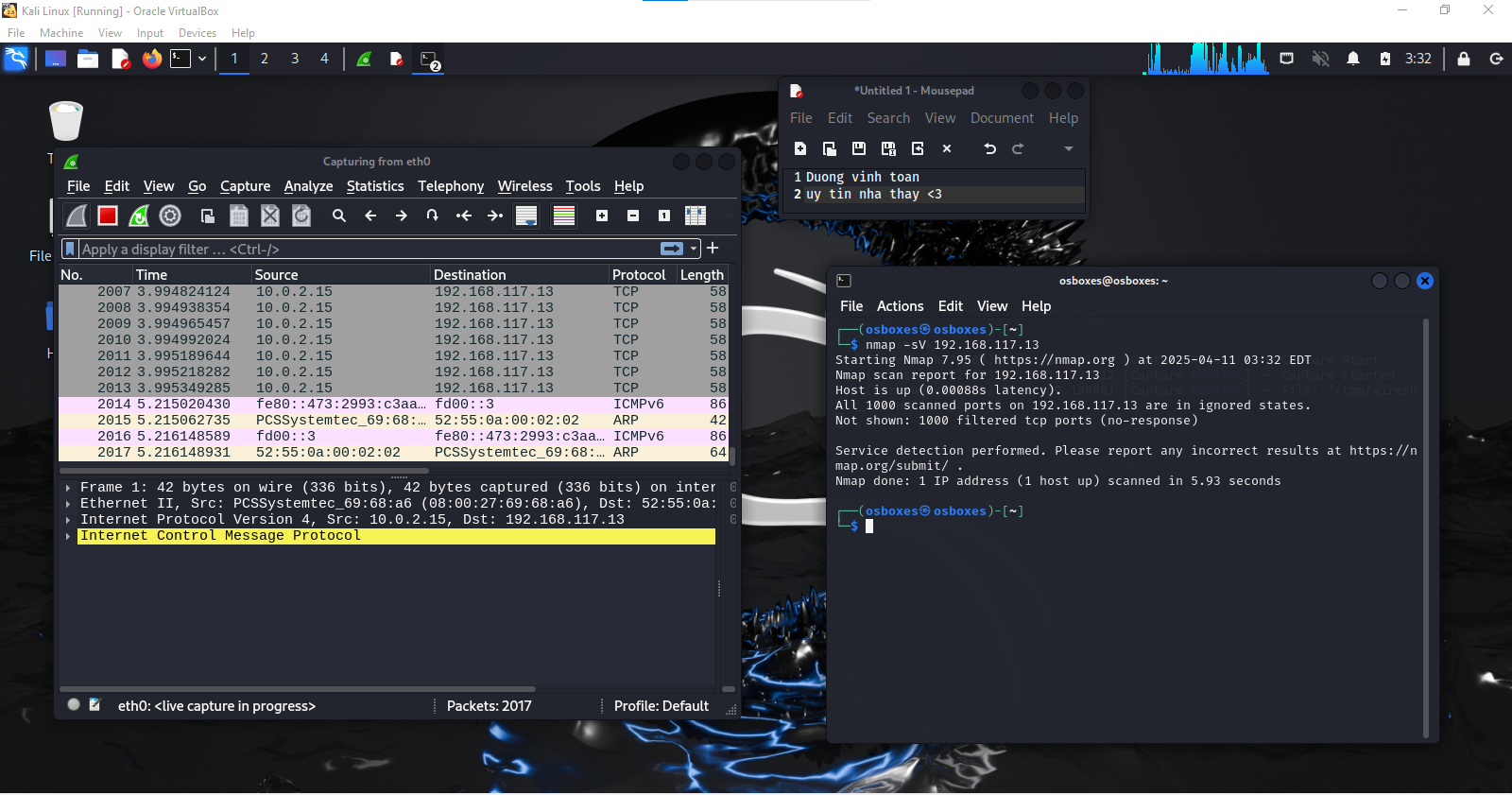
* -p: Chỉ định quét các cổng cụ thể.
* Các cổng:
  + 25: SMTP
  + 110: POP3
  + 143: IMAP
  + 465/587: SMTP có SSL/TLS
  + 993: IMAPS
  + 995: POP3S
* 192.168.117.0/24: Dải IP nội bộ cần quét để tìm máy nào đang cung cấp dịch vụ email.

**Thông tin hệ điều hành:**

 Tên hệ điều hành: Linux

 Phiên bản: Linux kernel 4.x (generic)  
*(Điền theo kết quả bạn thấy từ Nmap)*

**Thông tin dịch vụ: 1 điểm**

* nmap -sV 192.168.117.13
* 

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | Web | 80 | Apache httpd 2.4.49 |
| 2 | SSH | 22 | OpenSSH 7.9p1 |
| 3 | FTP | 21 | vsftpd 3.0.3 |

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.

Mỗi lỗ hổng: 1 điểm

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
|  |  |  |
|  |  |  |