BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: NGUYỄN BẢO TRÂN***

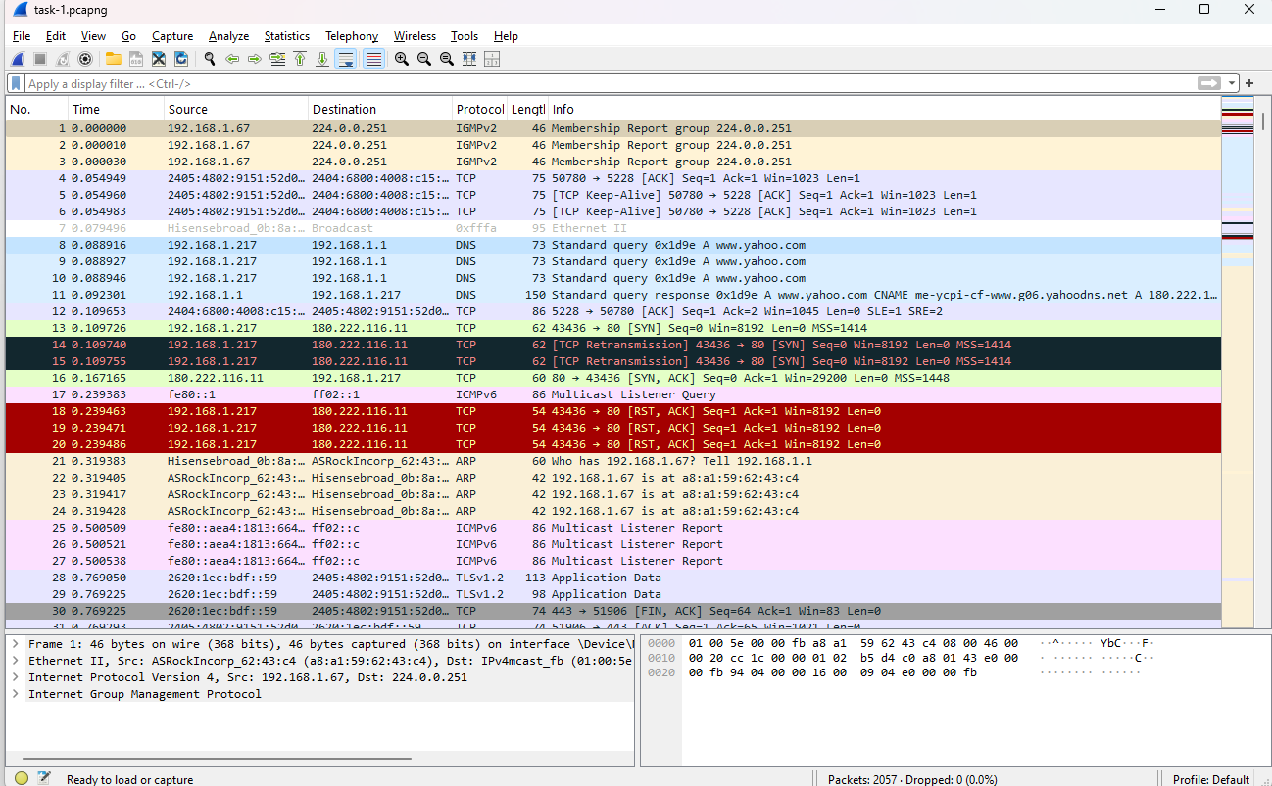
***MSSV: 1050080124***

**KẾT QUẢ THỰC HÀNH**

* **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
* **Kịch bản 1 : Ping Scan (ICMP Echo Scan)**



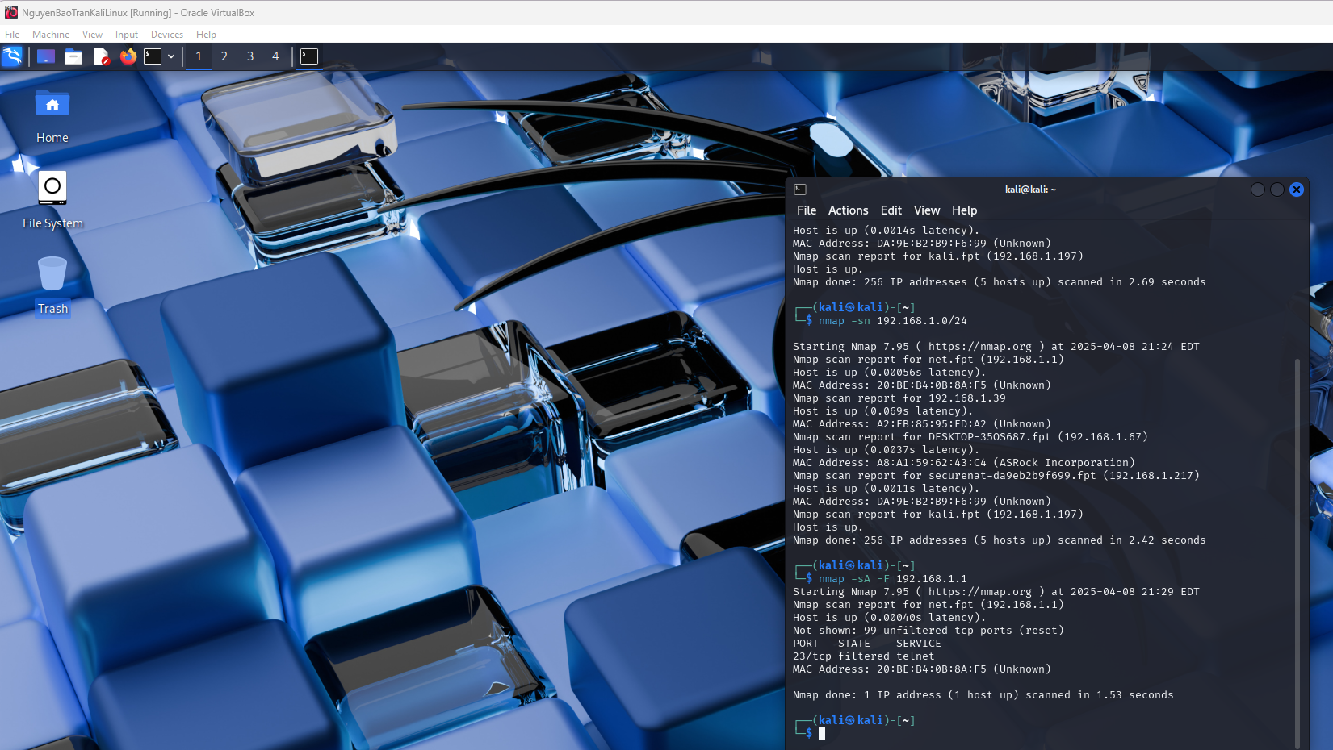
Thông qua quá trình phân tích lưu lượng trên máy do thám, em nhận thấy kỹ thuật quét được sử dụng là Ping Scan (ICMP Echo Scan) kết hợp với ARP Scan. Cụ thể, máy do thám đã gửi các gói ICMP Echo Request đến nhiều địa chỉ IP trong dải mạng nhằm xác định những thiết bị đang hoạt động. Đối với các IP chưa rõ địa chỉ MAC, máy tự động phát sinh các ARP Request để hỏi địa chỉ MAC tương ứng. Khi thiết bị trong mạng phản hồi bằng ICMP Echo Reply hoặc ARP Reply, điều đó cho thấy thiết bị đó đang tồn tại và sẵn sàng phản hồi. Dạng lưu lượng này là đặc trưng của lệnh nmap -sn khi thực hiện dò tìm các host đang "sống" trong mạng.



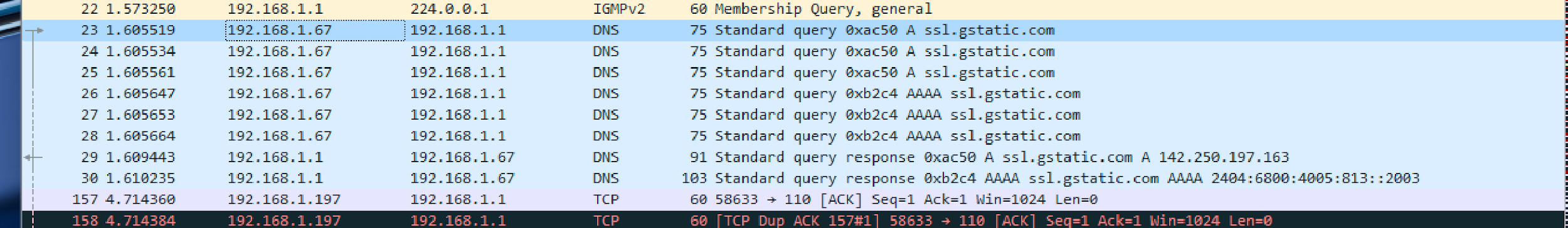
File 1:

https://drive.google.com/file/d/1w9PyuRis8ao8gN5WszSdt3a1-cF\_BKRJ/view?usp=sharing

* **Kịch bản 2 : TCP SYN Scan (nmap -sT)**



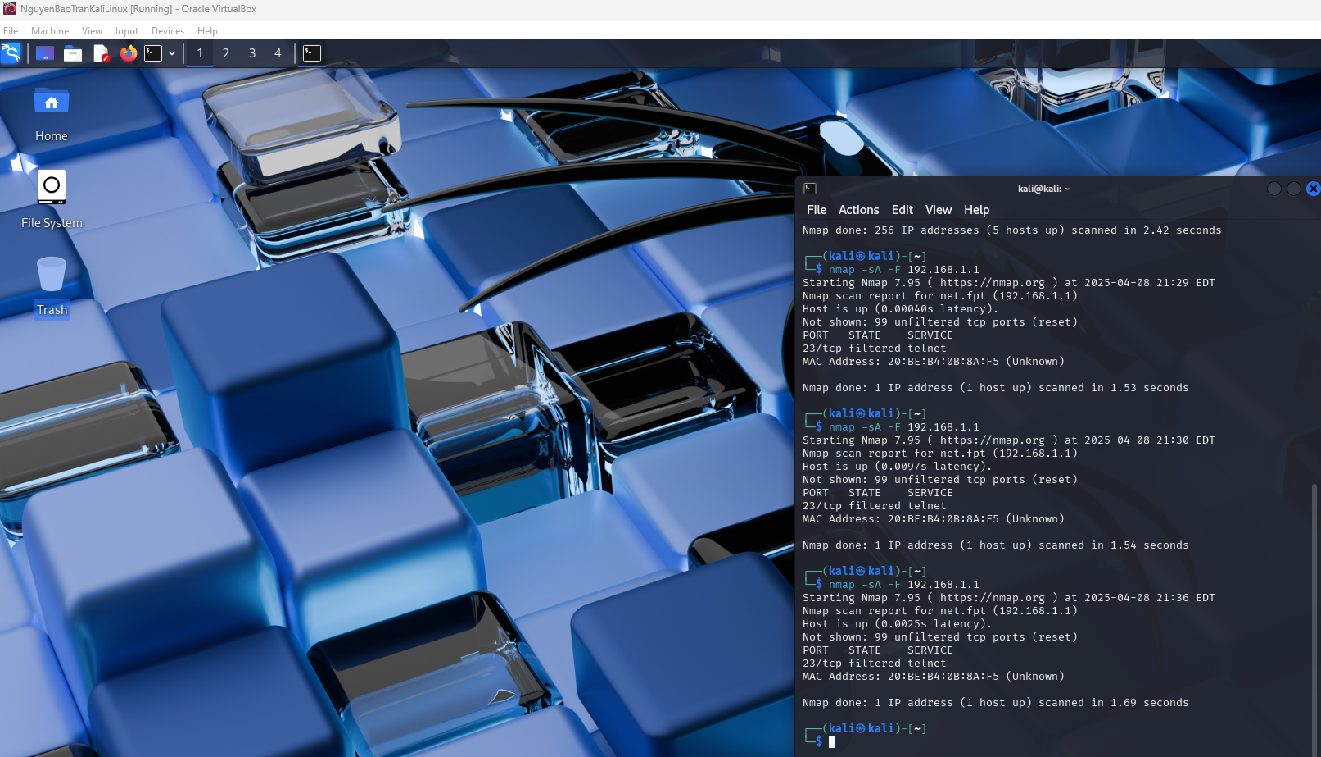
Trong kịch bản này, em đã sử dụng lệnh nmap -sS -F 192.168.1.1 từ máy do thám để thực hiện quét. Sau khi phân tích lưu lượng trong file task2.pcap, em xác định kỹ thuật được sử dụng là TCP SYN Scan, hay còn gọi là quét nửa mở (half-open scan). Cụ thể, máy do thám có địa chỉ IP 192.168.1.67 đã gửi các gói tin TCP mang cờ SYN đến nhiều cổng khác nhau trên máy mục tiêu 192.168.1.1. Khi một cổng trên máy đích đang mở, nó sẽ phản hồi bằng gói SYN-ACK. Thay vì hoàn tất quá trình bắt tay bằng cách gửi gói ACK, máy do thám sẽ gửi ngay một gói RST để hủy kết nối. Cách thức này giúp xác định cổng mở mà không thiết lập kết nối hoàn chỉnh, tránh bị phát hiện bởi một số hệ thống giám sát.



File 2:

https://drive.google.com/file/d/1u-xwlYu-uPUs7RWAI42nsRLESeJJvFAJ/view?usp=sharing

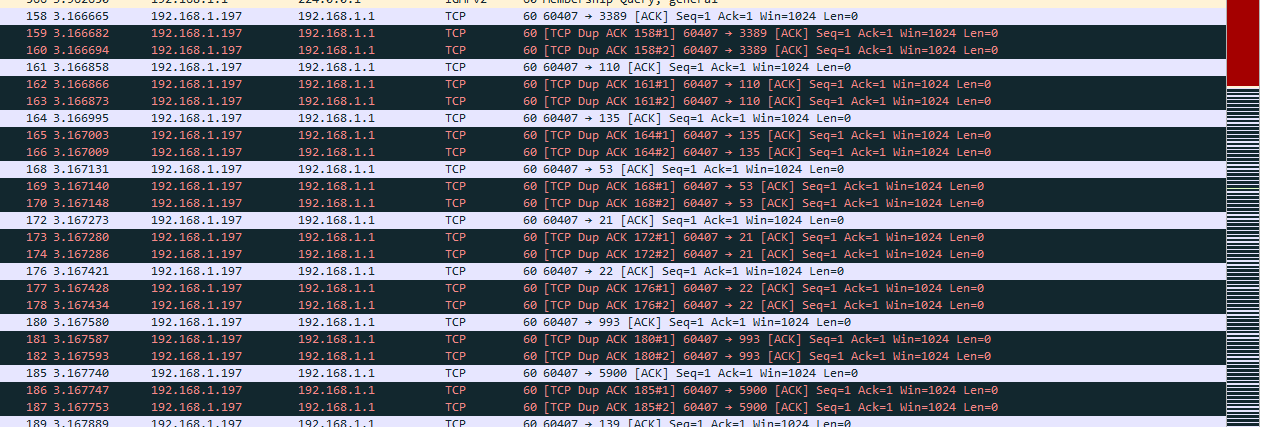
**Kịch bản 3 : TCP ACK Scan**



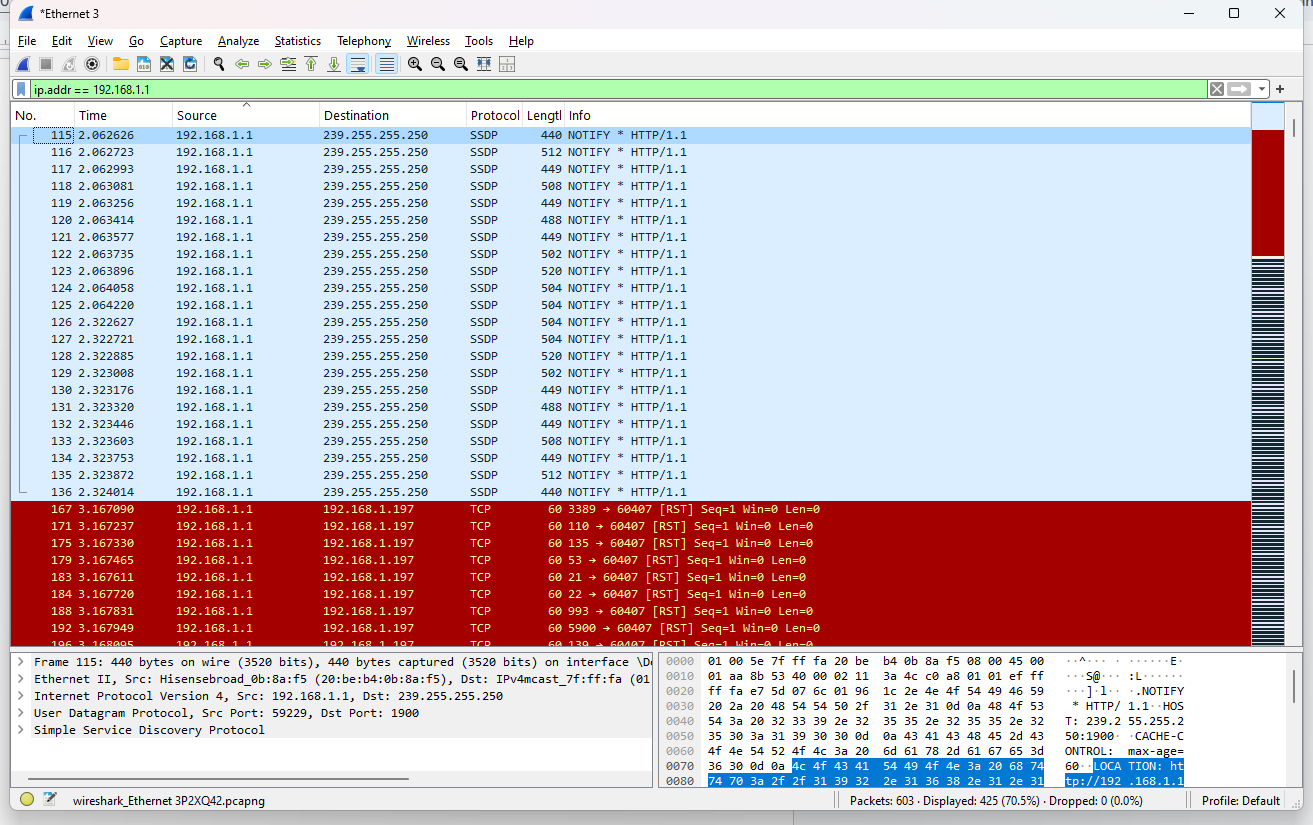
Trong kịch bản này, em sử dụng lệnh nmap -sA -F 192.168.1.1 từ máy do thám để kiểm tra trạng thái của firewall trên máy mục tiêu. Qua phân tích lưu lượng trong file task3.pcap, em xác định kỹ thuật quét được sử dụng là TCP ACK Scan. Cụ thể, máy do thám (ví dụ IP 192.168.1.6) đã gửi các gói TCP với cờ ACK đến nhiều cổng trên máy mục tiêu 192.168.1.67. Phân tích phản hồi cho thấy:

* Nếu máy mục tiêu phản hồi bằng gói TCP RST, điều đó cho thấy cổng tương ứng không bị lọc (unfiltered).
* Nếu không nhận được phản hồi, hoặc có dấu hiệu bị từ chối, có khả năng firewall đang chặn gói tin đến cổng đó.

192.168.1.197 đến 192.168.1.1



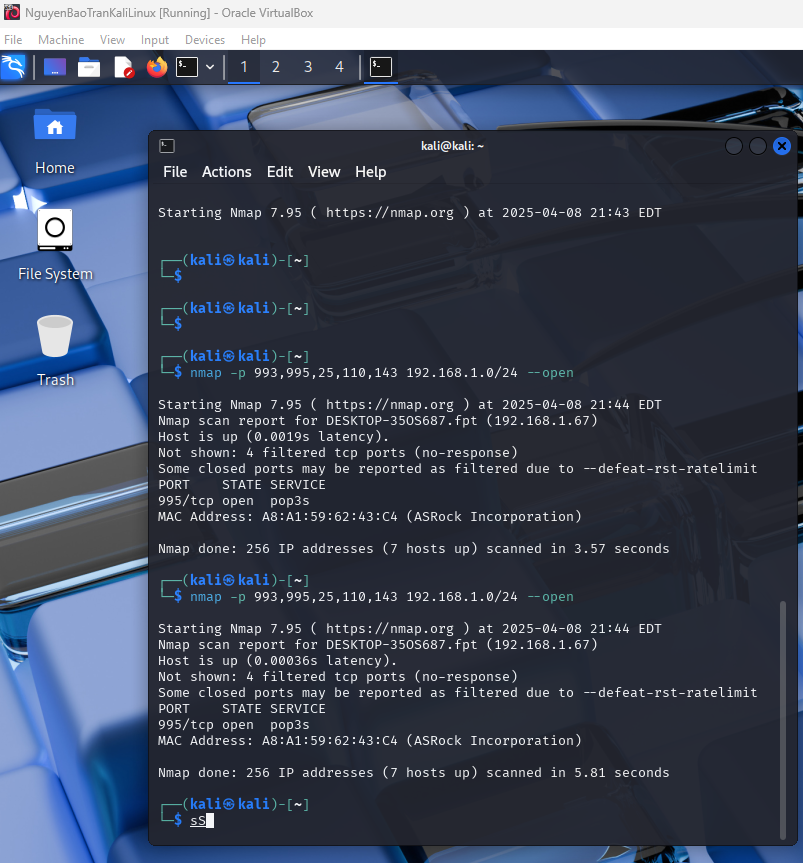
192.168.1.1 đến 192.168.1.197



**Thông tin hệ điều hành:**



**Thông tin dịch vụ:**



| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| --- | --- | --- | --- |
| 1 | POP3S | 995 | Chưa xác định |
|  |  |  |  |
|  |  |  |  |

File 3: https://drive.google.com/file/d/1RuBgcJH3eSB3zR3cLOT5R6M5kGu4hsx9/view?usp=sharing

* **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)** |
| --- | --- | --- |
| Dovecot 2.3.4.1 | CVE-2019-7524 | Lỗ hổng cho phép tấn công từ chối dịch vụ (DoS) qua xử lý sai MIME part trong một số email nhất định. |
| Apache HTTP Server 2.4.29 | CVE-2019-0211 | Cho phép người dùng không có đặc quyền nâng cao quyền trên hệ thống Unix nếu Apache chạy bằng mpm\_prefork. |
| OpenSSH 7.2p2 | CVE-2016-0777 | Tiết lộ thông tin nhạy cảm thông qua khai thác kênh bên (side-channel). |
| Samba 4.7.6 | CVE-2018-1050 | Lỗi khi xử lý yêu cầu SMB1 có thể bị khai thác để thực hiện DoS từ xa. |
| vsftpd 3.0.3 | CVE-2019-12815 | Lỗi khi xử lý lệnh LIST có thể gây tràn bộ nhớ, tiềm ẩn tấn công thực thi mã từ xa. |