LAB 7

PHÂN TÍCH CÁC KỸ THUẬT DO THÁM HỆ THỐNG

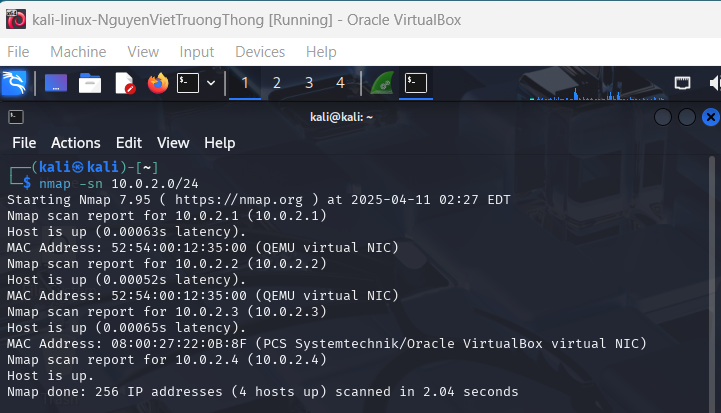
Họ và tên : Nguyễn Việt Trường Thông

MSSV : 1050080204

**KẾT QUẢ THỰC HÀNH**

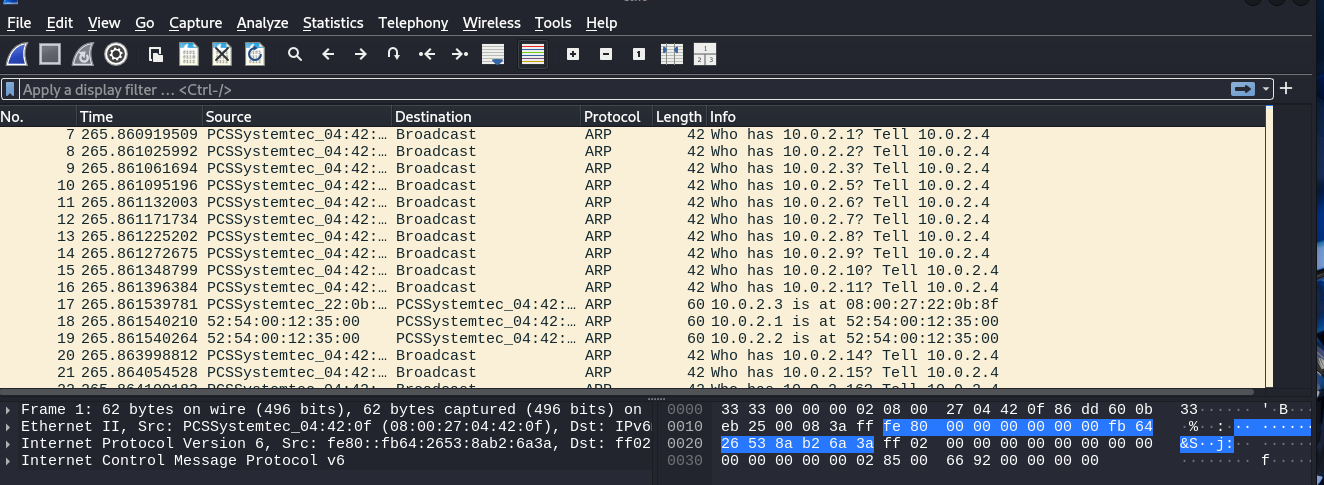
1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

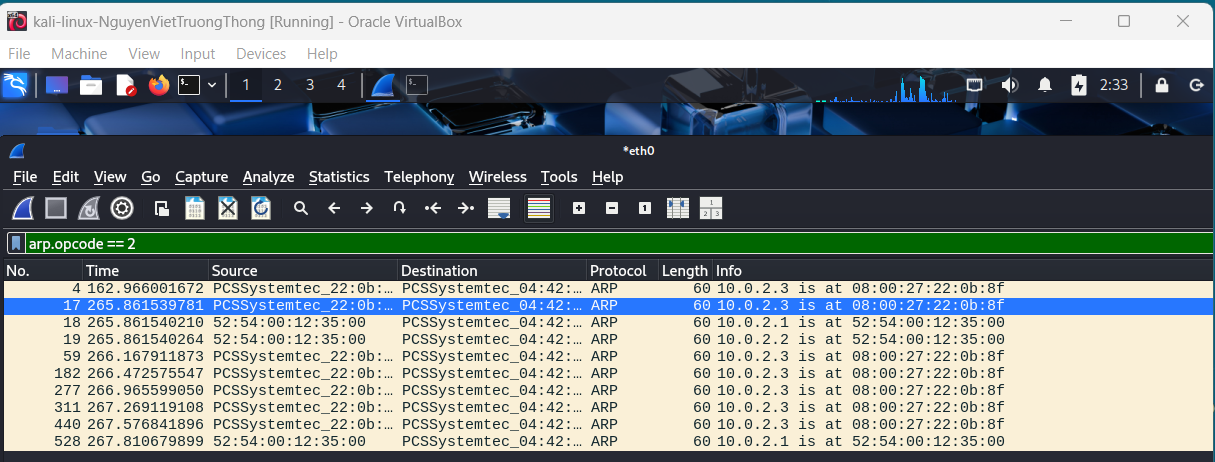
****

Phân tích lưu lượng:

* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm
* 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 10.0.2.0/24

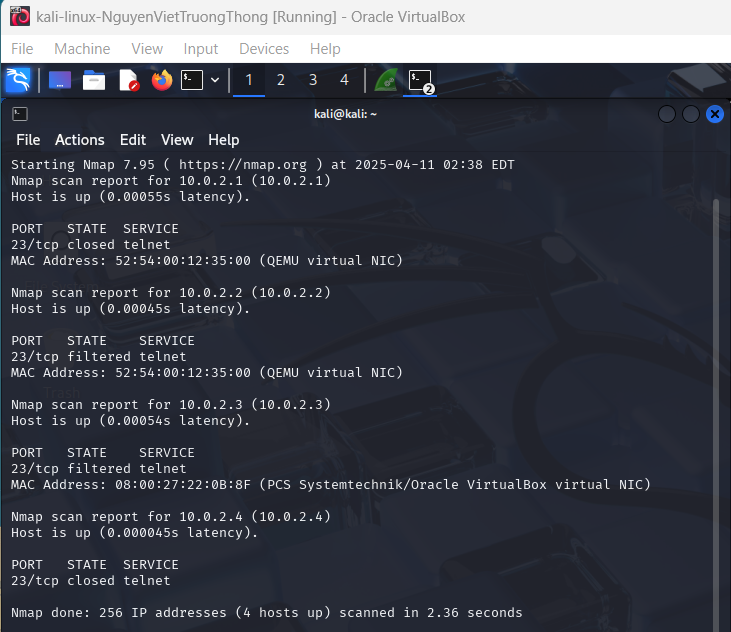


* Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc, chúng ta có thể thấy các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.



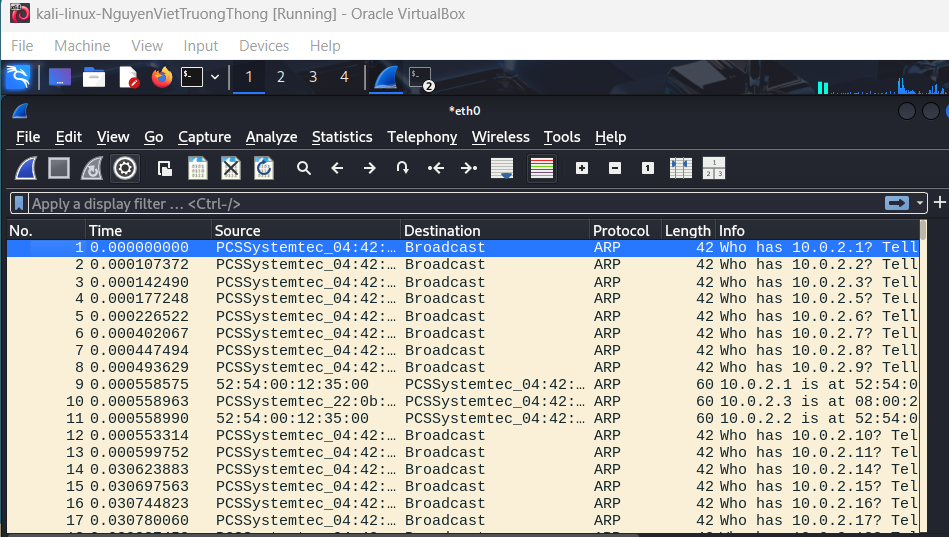
Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng đang hoạt động trong mạng.

* 1. **Kịch bản 2**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

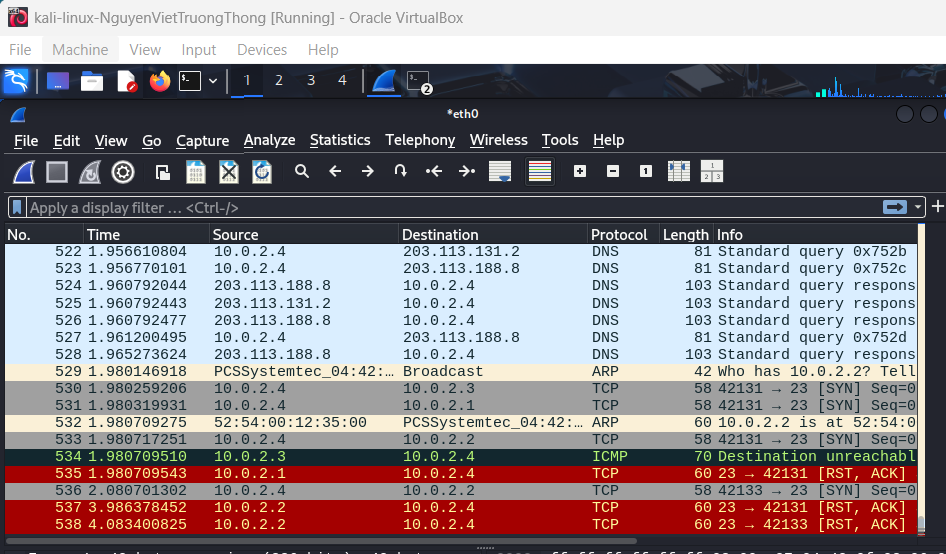


Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 10.0.2.1 và 10.0.2.0, 10.0.2.3, 10.0.2.4 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

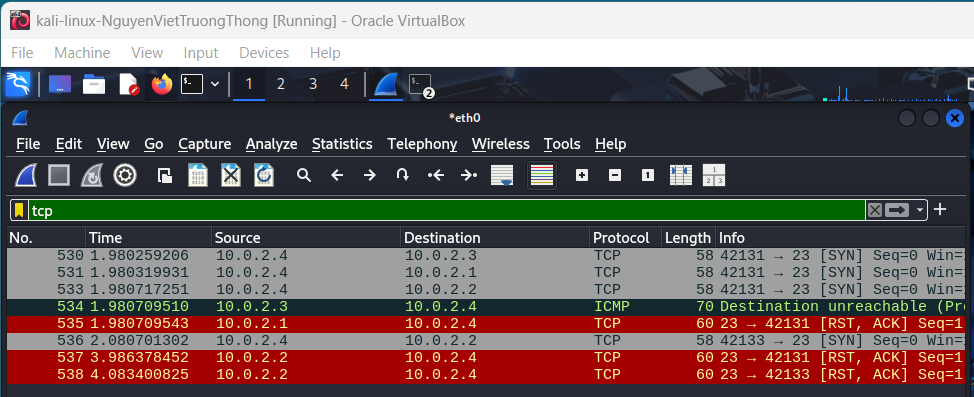
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm



* Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, 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 10.0.2.0/24.
* 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.

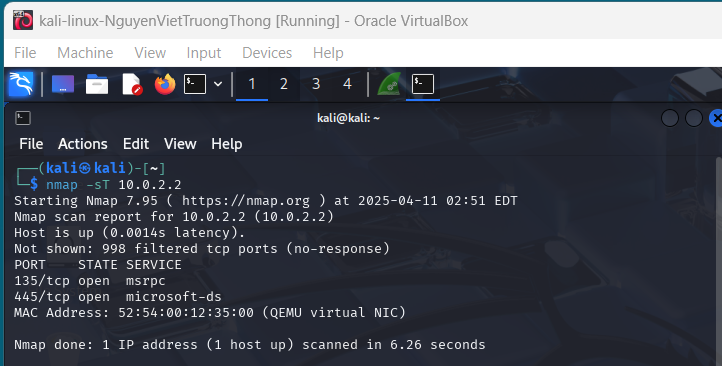


* - Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.117.13 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.117.10 trong kết quả trả về là địa chỉ của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

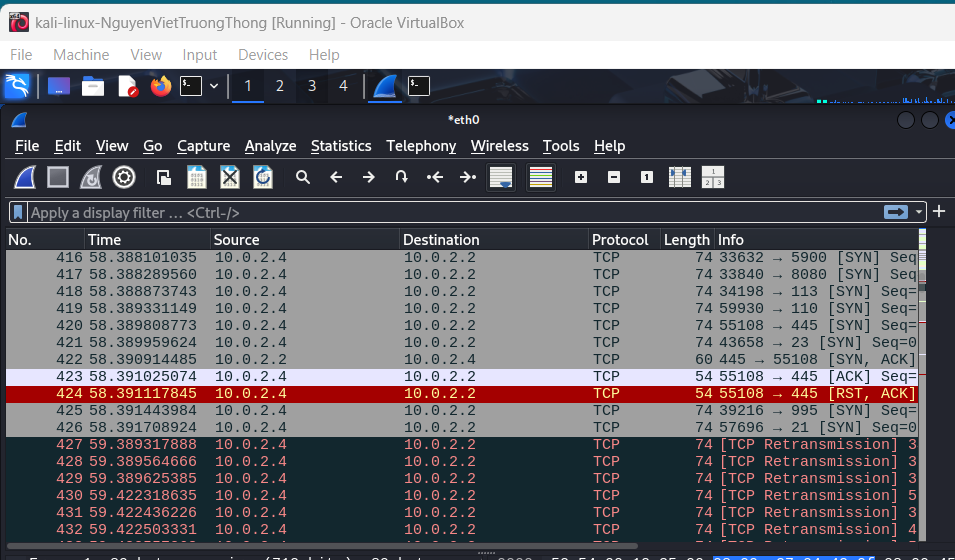
* 1. **Kịch bản 3**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

****

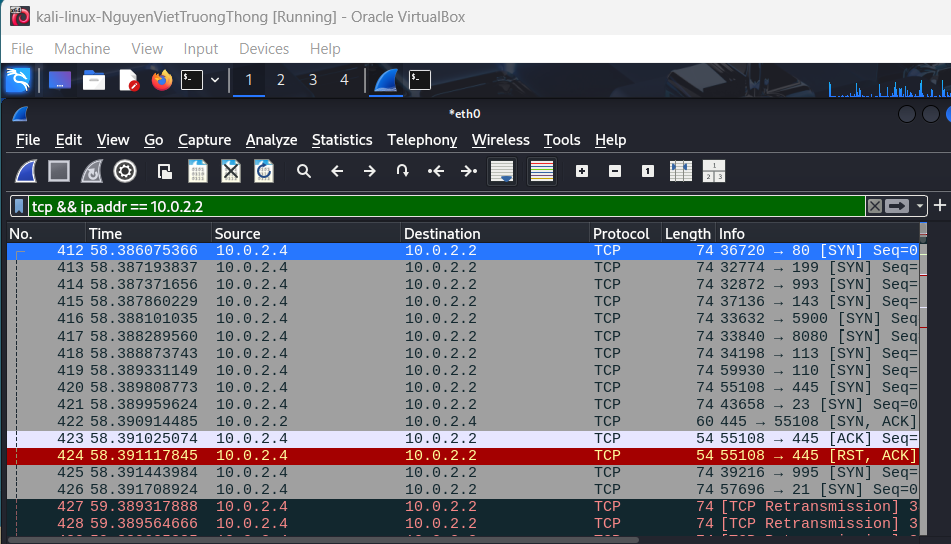
* Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 135, 445 trên máy mục tiêu 10.0.2.0 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.

Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

* Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 10.0.2.0 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói tin TCP SYN được gửi từ máy tấn công (10.0.2.1) tới máy mục tiêu là 10.0.2.0 Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.



* Sử dụng giá trị tcp && ip.addr == 10.0.2.0 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.



1. **Thu thập thông tin**

* Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này?(1 điểm)

nmap -p 25,110,143,465,587,993,995 --script banner <địa\_chỉ\_IP>

**25**: SMTP (gửi email)

**110**: POP3 (nhận email không mã hóa)

**143**: IMAP (nhận email không mã hóa)

**465**: SMTPS (SMTP qua SSL)

**587**: SMTP (gửi email có xác thực)

**993**: IMAPS (IMAP qua SSL)

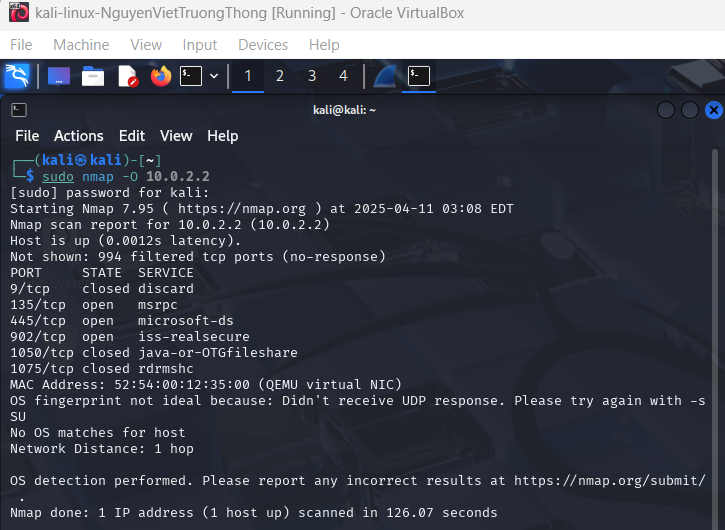
**995**: POP3S (POP3 qua SSL)

**--script banner**: sử dụng script banner để thu thập thông tin từ banner phản hồi của dịch vụ trên các cổng đó. Từ banner có thể xác định loại và phiên bản của máy chủ email.

**<địa\_chỉ\_IP>**: là địa chỉ IP đích mà bạn muốn quét để tìm máy chủ email.

**Thông tin hệ điều hành :**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm



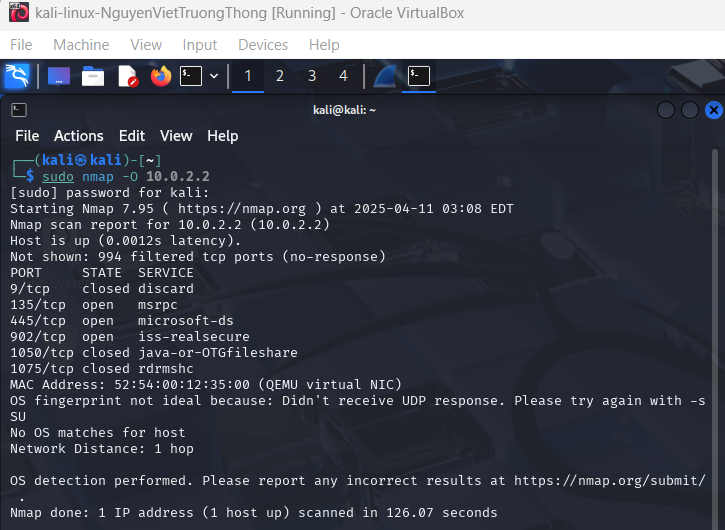
* Nêu tên và phiên bản hệ điều hành: 0.25 điểm

Hệ điều hành : Oracle VirtualBox

Phiên bản : Không xác định rõ

**Thông tin dịch vụ: 1 điểm**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm



* Danh sách dịch vụ: 0.75 điểm
* PORT 445/tcp : Microsoft-ds
* PORT 902/tcp : iss-realsecure
* PORT 1050/tcp : java-or-OTGfileshare

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Tên dịch vụ | Số hiệu cổng ứng  dụng | Tên phần mềm và phiên  bản |
| 1 | Microsoft-ds | 445 |  |
| 2 | iss-realsecure | 902 |  |
| 3 | java-or-OTGfileshare | 1050 |  |

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)** |
| SMB (Microsoft File Sharing) | CVE-2017-0144 | Lỗ hổng "EternalBlue" cho phép tấn công RCE trên Windows. |
| IBM RealSecure IDS/IPS | |  | | --- | |  |  |  | | --- | | CVE-2003-0230 | | Cho phép thực thi mã từ xa qua cổng 902 (phiên bản cũ). |