BÁO CÁO BÀI THỰC HÀNH SỐ 1

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

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

***MSSV: 0850080047***

***Yêu cầu kết quả thực hành:***

Đóng gói các kết quả vào file nén có tên theo định dạng HoTenSV\_MSSV\_Lab01.zip

* 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.

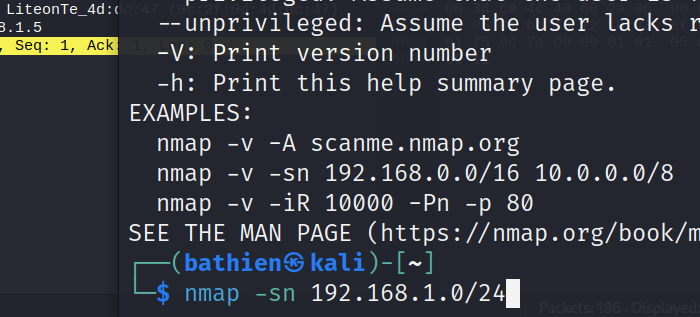
**KẾT QUẢ THỰC HÀNH**

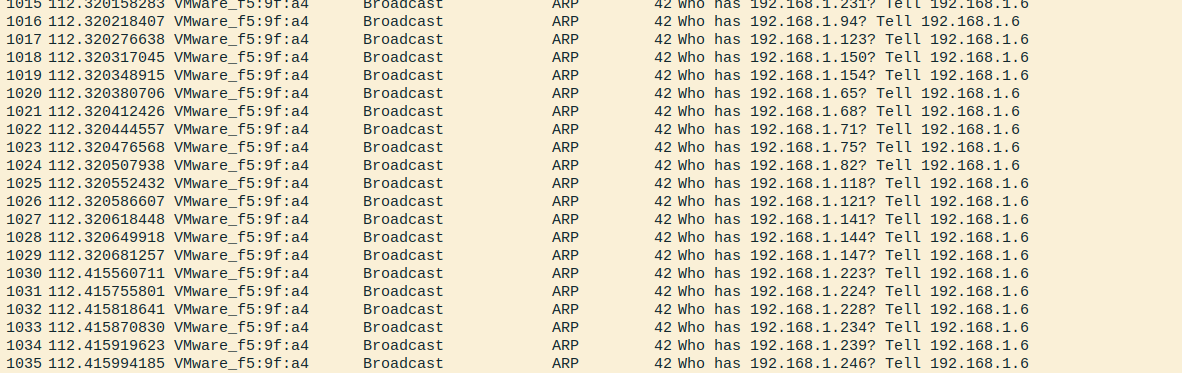
1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

* 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? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

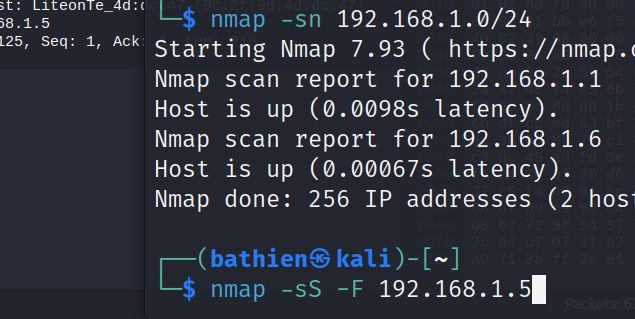


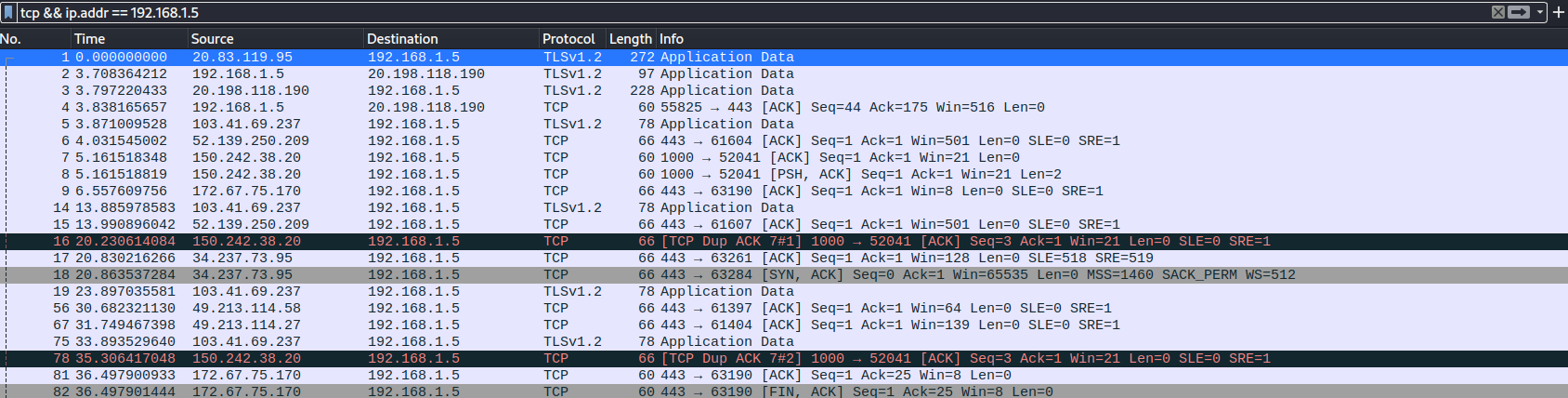


* Kỹ thuật ARP ping được sử dụng bởi nmap. Kỹ thuật này được sử dụng để tìm kiếm các thiết bị mạng bằng cách gửi yêu cầu ARP request và chờ đợi các thiết bị phản hồi với địa chỉ MAC của chúng.
  1. **Kịch bản 2**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

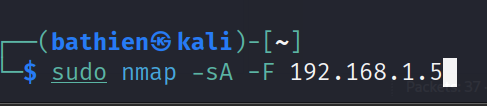


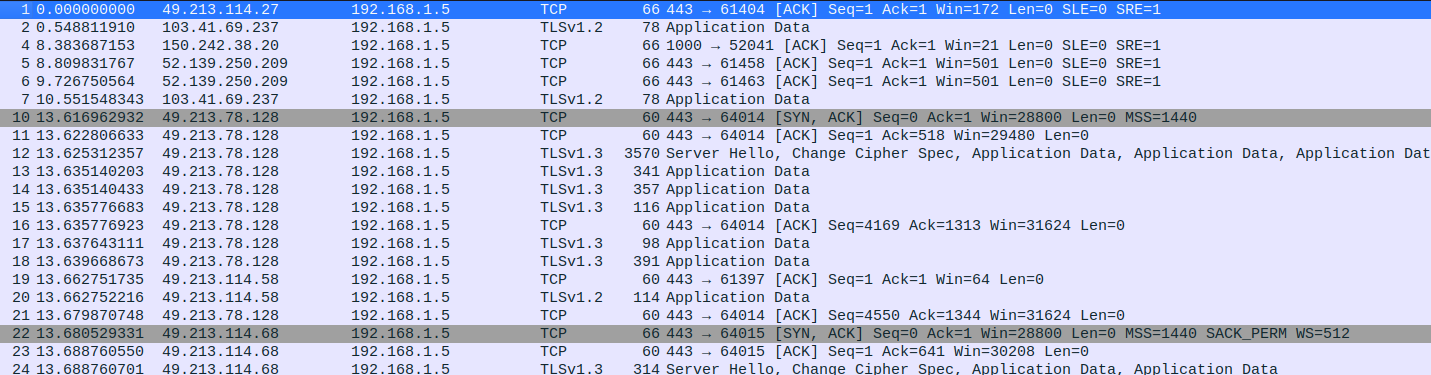


* Dựa trên kết quả bắt gói tin của file task2.pcap, ta thấy các gói tin gửi đi bởi nmap có chứa cờ SYN, điều này cho thấy rằng nmap đã sử dụng kỹ thuật quét TCP SYN scan để quét các cổng trên máy mục tiêu. Kỹ thuật quét này thường được sử dụng để quét mạng nhanh chóng và ẩn danh, bởi vì nó không hoàn thành quá trình kết nối TCP hoàn chỉnh với máy mục tiêu. Thay vào đó, nó gửi các gói tin SYN và đợi phản hồi từ máy mục tiêu để xác định cổng nào đang mở.
  1. **Kịch bản 3**
* 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? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*





* Lệnh quét nmap "-sA" được sử dụng để thực hiện quét ACK scan. Kỹ thuật này sử dụng các gói tin ACK để xác định xem một máy chủ có đang mở một cổng hay không. Nếu máy chủ gửi trả lời RST, có nghĩa là cổng đó không mở. Nếu không có phản hồi, có thể xác định rằng cổng đó đang được mở hoặc bị chặn bởi firewall.

1. **Thu thập thông tin hệ thống**

* 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)
* Lệnh là : nmap -p 25 --script smtp-enum-users <địa chỉ IP hoặc tên miền>

Trong đó:

+ -p 25 : là chỉ ddingj số cổng quét là 25, giao thức SMTP

+ --script smtp-enum-users : để thực hiện thăm dò và tìm kiếm danh sách người dùng trên máy chủ email. Kịch bản này sẽ thử liệt kê các tài khoản người dùng trên máy chủ bằng cách sử dụng một số tên người dùng thông thường như "root", "admin", "test", vv…

+ địa chỉ ip hoặc tên miền : Địa chỉ IP hoặc tên miền của máy chủ email cần quét.

**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

**Thông tin dịch vụ: 1 điểm**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* Danh sách dịch vụ: 0.75 điểm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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)** |
|  |  |  |
|  |  |  |