BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Phan Tân Phước***

***MSSV: 1050080070***

***Yêu cầu kết quả thực hành:***

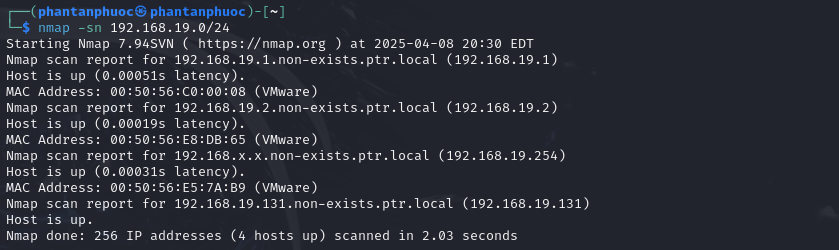
Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07

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

Lệnh này sử dụng Nmap với tùy chọn -sn, tức là thực hiện Ping Scan. Đây là kỹ thuật quét thăm dò (reconnaissance scan) để xác định host nào đang hoạt động (online) trong một dải mạng nhất định mà không quét cổng (no port scanning).

* Quét toàn bộ dải địa chỉ IP trong mạng con: /24 tương ứng với 256 địa chỉ IP từ 192.168.19.0 đến 192.168.19.255.
* Không kiểm tra cổng (Port scan): Tham số -sn yêu cầu Nmap chỉ kiểm tra xem host có đang hoạt động không (ping scan).
* Phản hồi cho thấy host hoạt động: Nmap trả về "Host is up" và thời gian phản hồi.



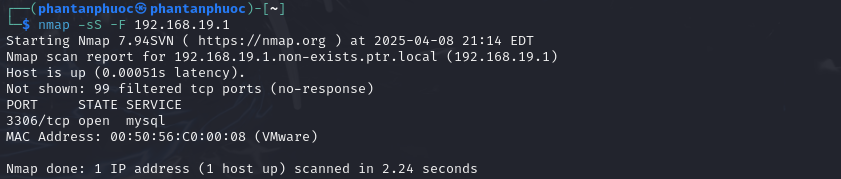
* Thời gian quét rất ngắn: Toàn bộ 256 IP được quét trong 2.03 giây.



*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*

* 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

Lệnh nmap -sS -F 192.168.19.1 được sử dụng để thực hiện quét thăm dò cổng (port scanning) bằng kỹ thuật SYN Scan (nửa kết nối) – một trong những kỹ thuật phổ biến và khó bị phát hiện hơn so với quét TCP thông thường.

* Sử dụng SYN scan – quét nửa kết nối (Stealth scan): Tham số -sS dùng kỹ thuật SYN scan – chỉ gửi gói TCP SYN mà không hoàn tất bắt tay 3 bước.
* Chỉ quét danh sách cổng phổ biến: Tham số -F dùng để quét nhanh, chỉ kiểm tra các cổng phổ biến (~100).
* Phản hồi cho biết có cổng đang mở (open port): 3306/tcp được báo là open – đây là cổng MySQL.



* Phần lớn cổng bị lọc (filtered): Nmap thông báo “99 filtered tcp ports (no-response)”.



* Thời gian quét nhanh và chỉ định rõ mục tiêu: Quét một địa chỉ IP cụ thể 192.168.19.1 và hoàn tất trong 2.24 giây.



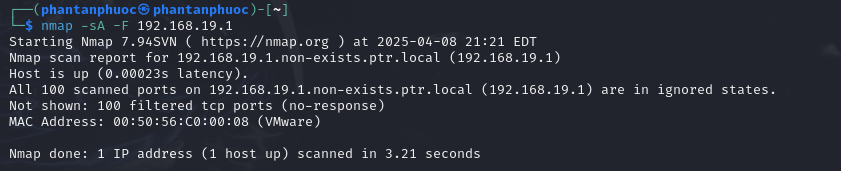
* Hiển thị MAC Address: Nmap thu được địa chỉ MAC: 00:50:56:C0:00:08 (VMware).



*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*

* 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

Nmap đang thực hiện một kỹ thuật quét đặc biệt gọi là ACK scan – dùng để xác định trạng thái của firewall (tường lửa) chứ không nhằm phát hiện cổng mở.

* Sử dụng kỹ thuật ACK scan: Tham số -sA là viết tắt của ACK scan, gửi các gói TCP với cờ ACK đã được bật.
* Kết quả cho biết tất cả cổng đều bị lọc: Mọi cổng đều không phản hồi → có khả năng bị tường lửa chặn hoàn toàn. Đây là điều mà ACK scan muốn xác định – giúp tin tặc hiểu được cơ chế bảo vệ của hệ thống.



* Không xác định được cổng mở/đóng: Không có dòng nào hiển thị port open hoặc closed, chỉ báo “filtered”.
* Quét nhanh các cổng phổ biến: Tham số -F chỉ quét danh sách ~100 cổng thông dụng nhất.
* Hiển thị địa chỉ MAC: Nmap thu được địa chỉ MAC 00:50:56:C0:00:08 (VMware).



*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*

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)

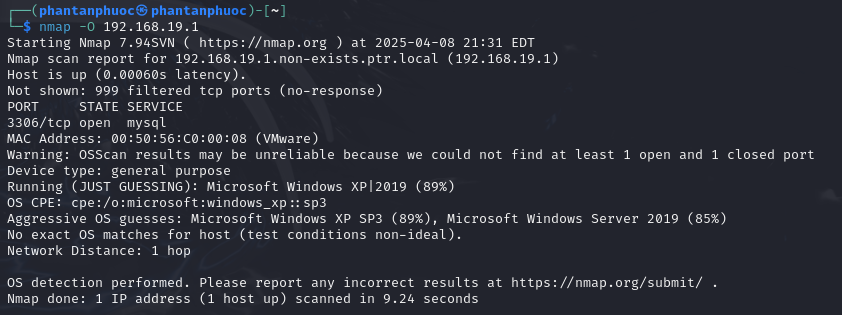
Lệnh quét thăm dò tìm kiếm máy chủ email là một kỹ thuật sử dụng công cụ Nmap để xác định xem một hệ thống có đang chạy các dịch vụ liên quan đến email hay không, thông qua việc kiểm tra các cổng mạng phổ biến của các giao thức email. Mục tiêu chính của kỹ thuật này là thu thập thông tin về các dịch vụ email đang hoạt động, từ đó hỗ trợ cho các bước phân tích bảo mật hoặc kiểm thử xâm nhập.

Xác định danh sách các cổng liên quan đến dịch vụ email cần kiểm tra.

* 25: SMTP – gửi email
* 110: POP3 – nhận email
* 143: IMAP – truy cập email
* 465: SMTPS – SMTP qua SSL
* 993: IMAPS – IMAP qua SSL
* 995: POP3S – POP3 qua SSL

**Thông tin hệ điều hành:**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm

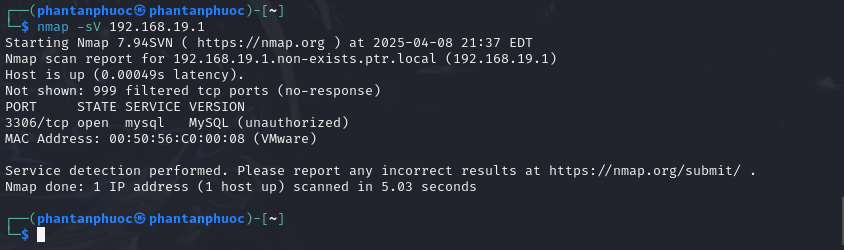


* Nêu tên và phiên bản hệ điều hành: 0.25 điểm

Tên hệ điều hành: Microsoft Windows XP 2019

**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 | Mysql | 3306/tcp | MySQL |
|  |  |  |  |
|  |  |  |  |

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)** |
| MySQL (unauthorized) – Không rõ phiên bản chính xác | CVE-2020-2579 | Lỗ hổng trong MySQL cho phép kẻ tấn công từ xa khai thác để thực thi mã tùy ý hoặc gây sập dịch vụ nếu cấu hình sai quyền truy cập |
|  |  |  |