BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Trần Anh Tuấn***

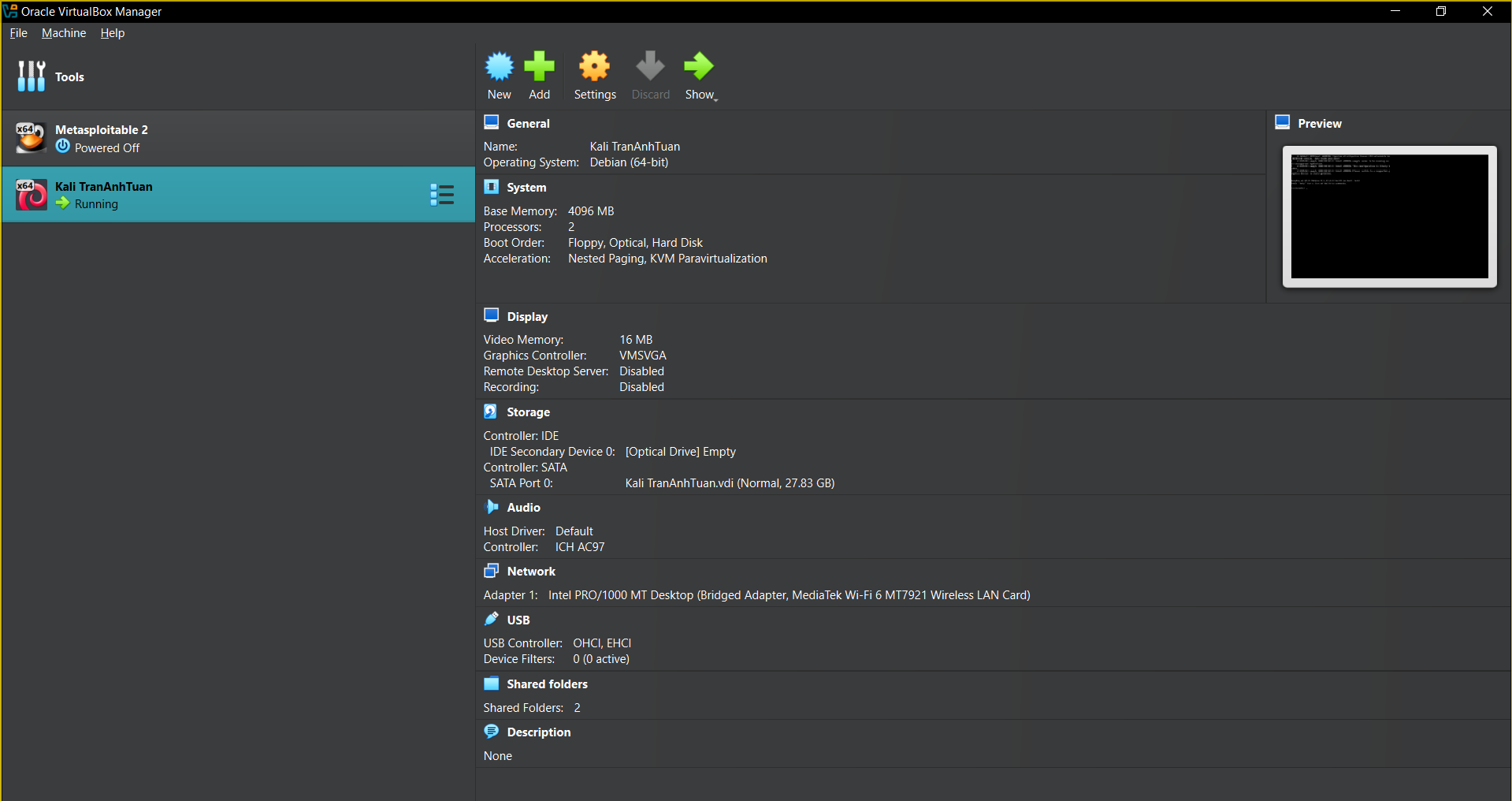
***MSSV: 1050080289***

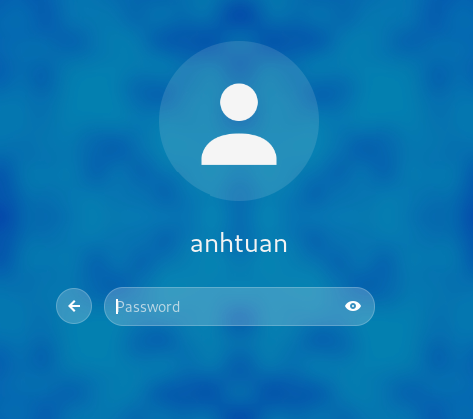
**KẾT QUẢ THỰC HÀNH**

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

**1.1. Kịch bản 1**

**Bước 1:** Truy cập máy ảo



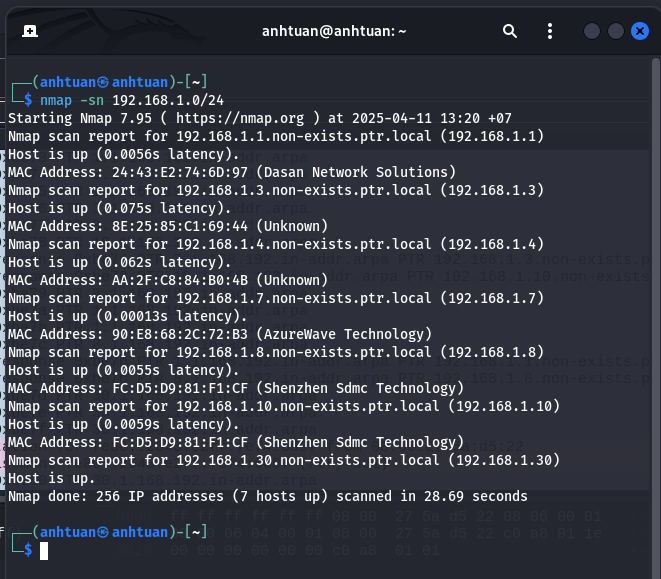


**Bước 2:** Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn card mạng để bắt gói tin.

**Bước 3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

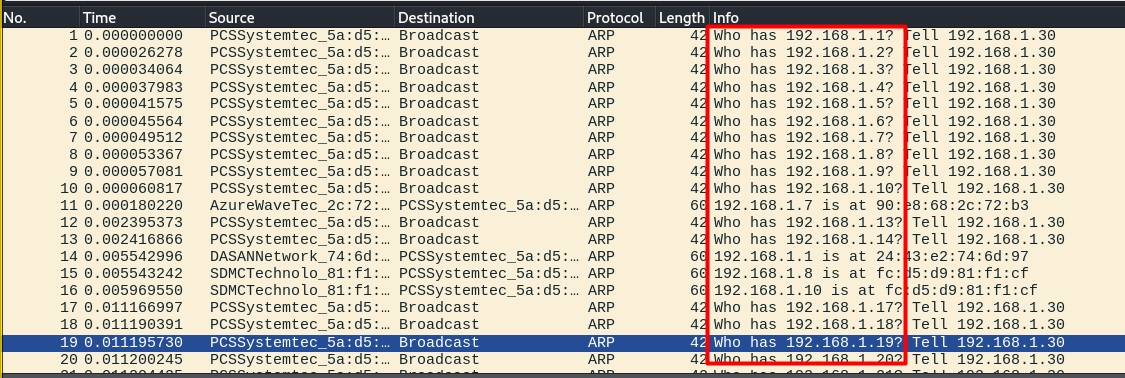
**nmap –sn 192.168.1.0/24**

**Bước 4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau:



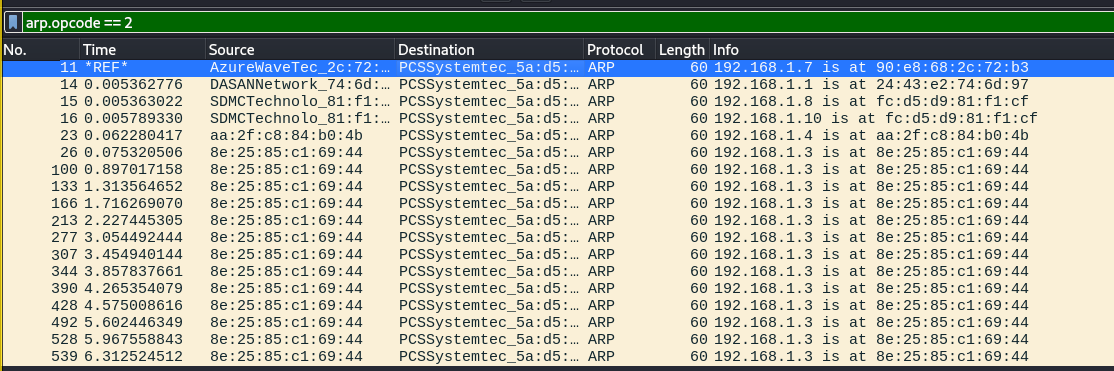
Có thể thấy ngoài địa chỉ 192.168.1.30 là địa chỉ của máy tấn công thì còn 6 nút mạng nữa đang hoạt động có địa chỉ là 192.168.1.1, 192.168.1.3, 192.168.1.4, 192.168.1.7, 192.168.1.8, 192.168.1.10.

**Bước 5:** Dừng bắt gói tin trên Wireshark



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 192.168.1.0/24

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.

**1.2. Kịch bản 2**

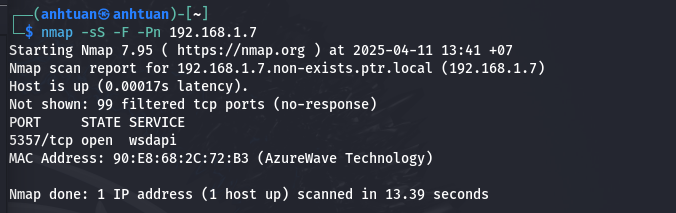
**Bước 1:** Truy cập máy ảo

**Bước 2:** Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn card mạng để bắt gói tin.

**Bước 3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

**nmap –sS –F 192.168.1.7**

**Bước 4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau đây. Kết quả cho thấy cổng dịch vụ 5357 trên máy mục tiêu 192.168.1.7 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp dịch vụ tương ứng là wsdapi.



**Bước 5:** Dừng bắt gói tin trên Wireshark

**Phân tích lưu lượng:**

Khi sử dụng lệnh **nmap -sS -F 192.168.1.7** để quét cổng, Wireshark đã ghi nhận lưu lượng từ máy tấn công (192.168.1.30) gửi đến máy mục tiêu (192.168.1.7).

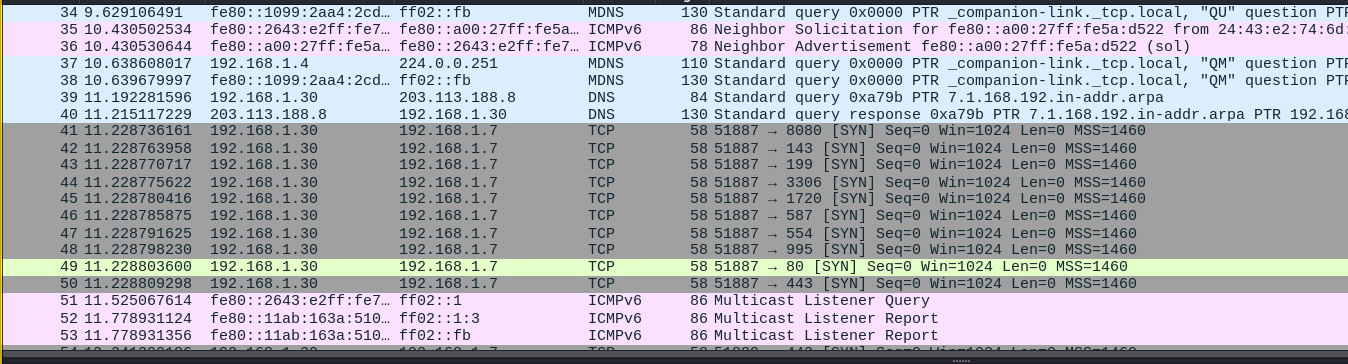
- Các gói tin TCP có cờ SYN được gửi đến các cổng như: 5357, 80, 443.

- Đây là đặc trưng của kỹ thuật TCP SYN scan: chỉ gửi SYN mà không hoàn tất quá trình bắt tay TCP.

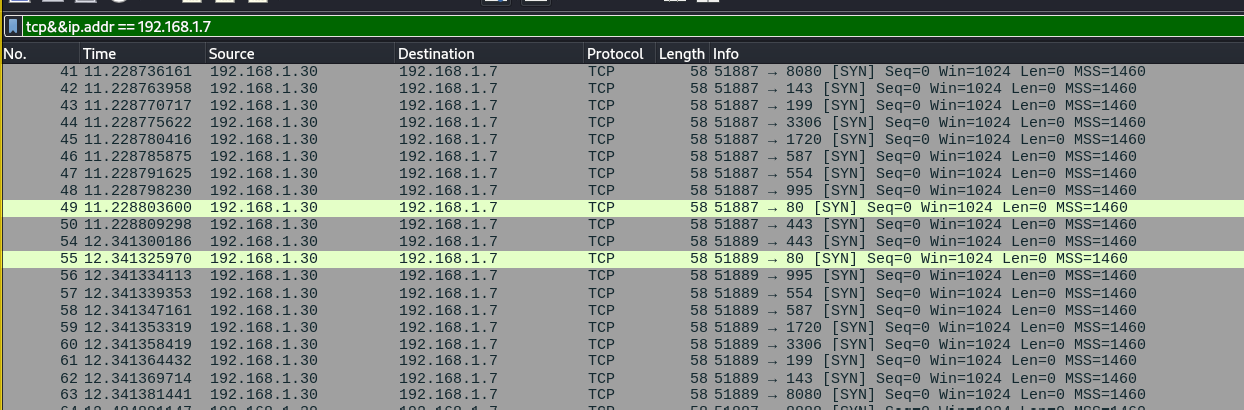
- Mục tiêu là xác định xem cổng có đang mở hay không mà tránh bị phát hiện bởi hệ thống giám sát.

- Một số cổng không phản hồi có thể do bị lọc hoặc đóng.

- Trong trường hợp cổng mở, máy mục tiêu thường sẽ phản hồi SYN-ACK, nhưng điều này không thấy rõ trong ảnh chụp (có thể do lọc hoặc chưa hiển thị hết).



Sử dụng bộ lọc `tcp && ip.addr == 192.168.1.7` trong Wireshark, ta ghi nhận được nhiều gói tin TCP với cờ SYN được gửi từ máy do thám (192.168.1.30) đến máy mục tiêu (192.168.1.7). Các gói tin được gửi đến nhiều cổng khác nhau như: 80, 443, 8080, 5357,...



Đây là đặc trưng của kỹ thuật TCP SYN Scan – một kỹ thuật quét "nửa mở", chỉ gửi gói SYN mà không hoàn tất quá trình bắt tay TCP. Mục đích là dò tìm các cổng đang mở mà vẫn giảm khả năng bị phát hiện.

**1.3. Kịch bản 3**

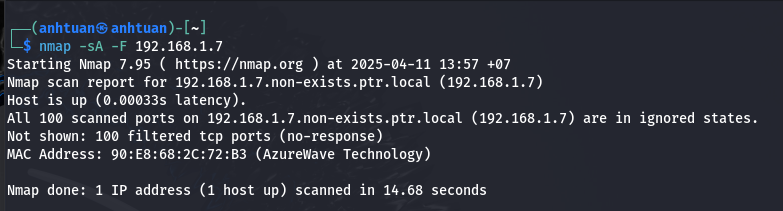
**Bước 1:** Truy cập máy ảo

**Bước 2:** Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn card mạng để bắt gói tin.

**Bước 3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

**nmap –sA –F 192.168.1.7**

**Bước 4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau đây.



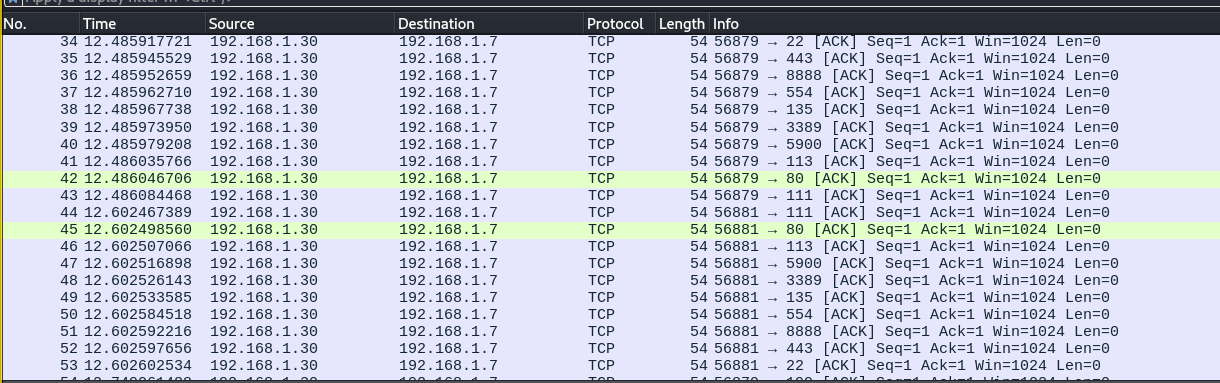
Kết quả cho thấy TẤT CẢ các cổng bị filtered, tức là:

* Không có cổng nào trả lời.
* Có thể có firewall hoặc thiết bị lọc đang chặn gói ACK.

**Bước 5:** Dừng bắt gói tin trên Wireshark

**Phân tích lưu lượng:**

* Gói tin **TCP** từ máy do thám đến nhiều cổng đích.
* Chỉ chứa **cờ ACK**, không có SYN hay FIN.
* **Không có dữ liệu** (Len = 0).
* **Không nhận được phản hồi** từ máy mục tiêu → các cổng **bị lọc (filtered)**.



Chỉ thấy **gói TCP ACK gửi đi** từ 192.168.1.30 → 192.168.1.7.

**Không thấy bất kỳ phản hồi nào từ 192.168.1.7**.

**Kết luận:** Tất cả các cổng đều đang ở trạng thái **filtered**, và firewall đã **chặn phản hồi** từ máy mục tiêu.

**2. Thu thập thông tin hệ thống**

nmap -sS -p 25,110,143,465,587,993,995 192.168.100.0/24

**Giải thích tham số**:

-sS: quét TCP SYN (stealth scan)

* -p 25,110,143,465,993,995: Chỉ định quét các cổng liên quan đến dịch vụ email:
  + 25: SMTP (gửi email).
  + 110: POP3 (nhận email).
  + 143: IMAP (nhận email).
  + 465: SMTPS (SMTP qua SSL).
  + 587 Submission (SMTP với xác thực)
  + 993: IMAPS (IMAP qua SSL).
  + 995: POP3S (POP3 qua SSL).

**Thông tin hệ điều hành:**

- Hình ảnh chụp kết quả của nmap:

- Nêu tên và phiên bản hệ điều hành:

**Thông tin dịch vụ:**

- Hình ảnh chụp kết quả của nmap:

- Danh sách dịch vụ:

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

**3. 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:

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