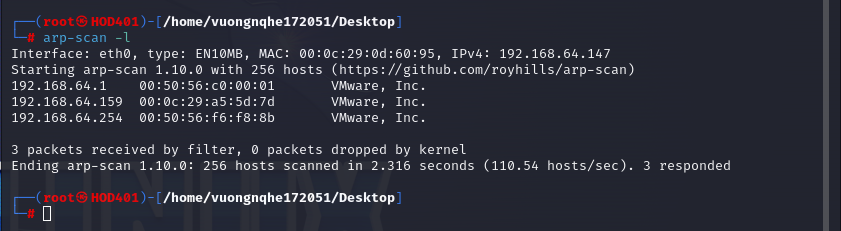
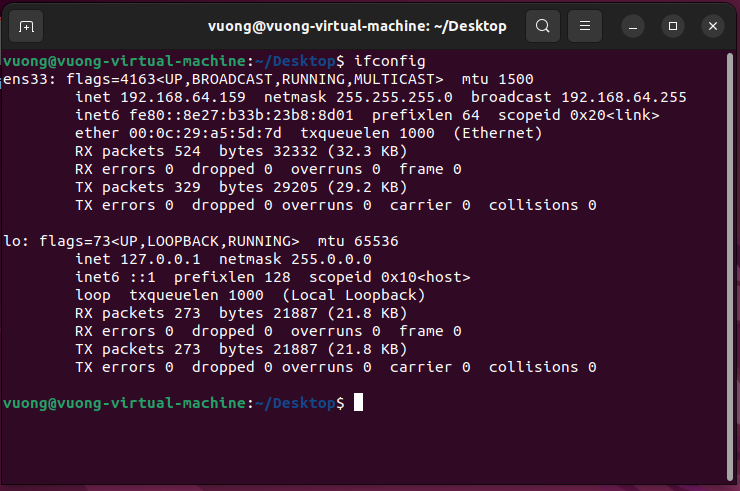
Lab-Project 11: yesman--Scanner Honeypot with scapy

**Finding the IP Address of the Target Machine:**

**\*** Tại máy Kali; sử dụng lệnh arp-scan -l tìm các máy cùng mạng

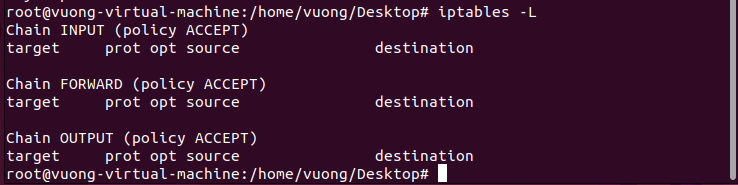
****



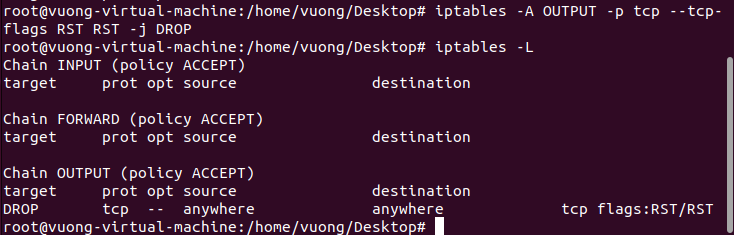
=> Tìm được IP của máy Ubuntu (máy target)

**Blocking ACK Packets on the Target Machine:**

**+** Sử dụng lệnh iptables liệt kê các quy tắc trong tường lửa:

****

**+** Chạy lênh: **iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP** để thêm quy tắc vào tường lửa và sử dụng lại lệnh iptables -L để kiểm tra

****

**Sniffing a Packet in scapy:**

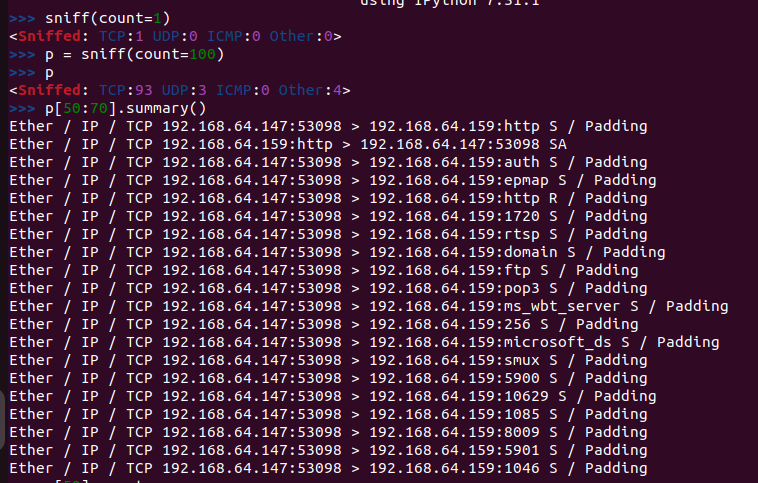
**\*** Trên máy Ubuntu (Target machine):

+ Mở **scapy** dưới quyền root, chạy lệnh **sniff(count=1)** để bắt 1 gói tin

**Sniffing 100 Packets in scapy:**

\* Trên máy Ubuntu (Target Machine)

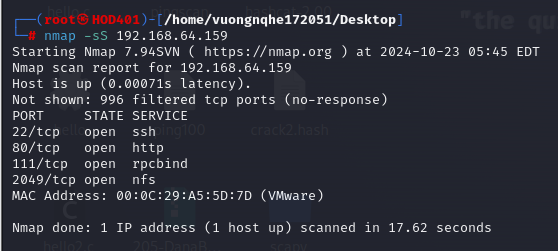
* Sử dụng lệnh **p=sniff(count=100)** để bắt 100 gói tin

****

**Scanning from the Scanner Machine**

\* Trên máy Kali:

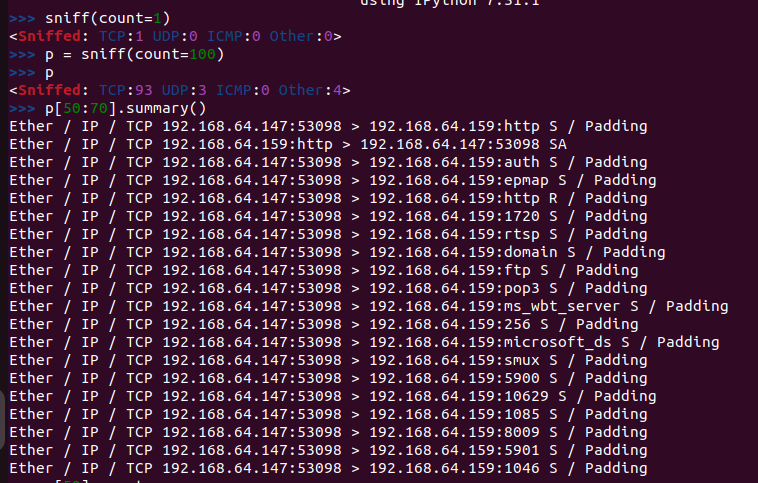
* Sử dụng command: **nmap -sS 192.168.64.159** để thực hiện SYN Scan

****

**Examining the Captured Packets**

**\*** Trên máy Ubuntu:

* Sau đó, sử dụng lệnh **p** kiểm tra các loại gói tin được gửi đến
* Sử dụng command **p[50:70].summary()** xem các gói 50 đến gói 70

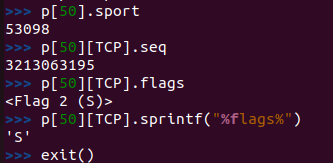
****

**+** Thực hiện các command sau:  
**p[50][TCP].sport**

**p[50][TCP].seq**

**p[50][TCP].flags**

**p[50][TCP].sprintf(“%flags%”)**

****

**Creating the yesman.py script**

**\*** Tại máy kali:

* Tạo 1 file **yesman.py** có đoạn code như dưới hình:

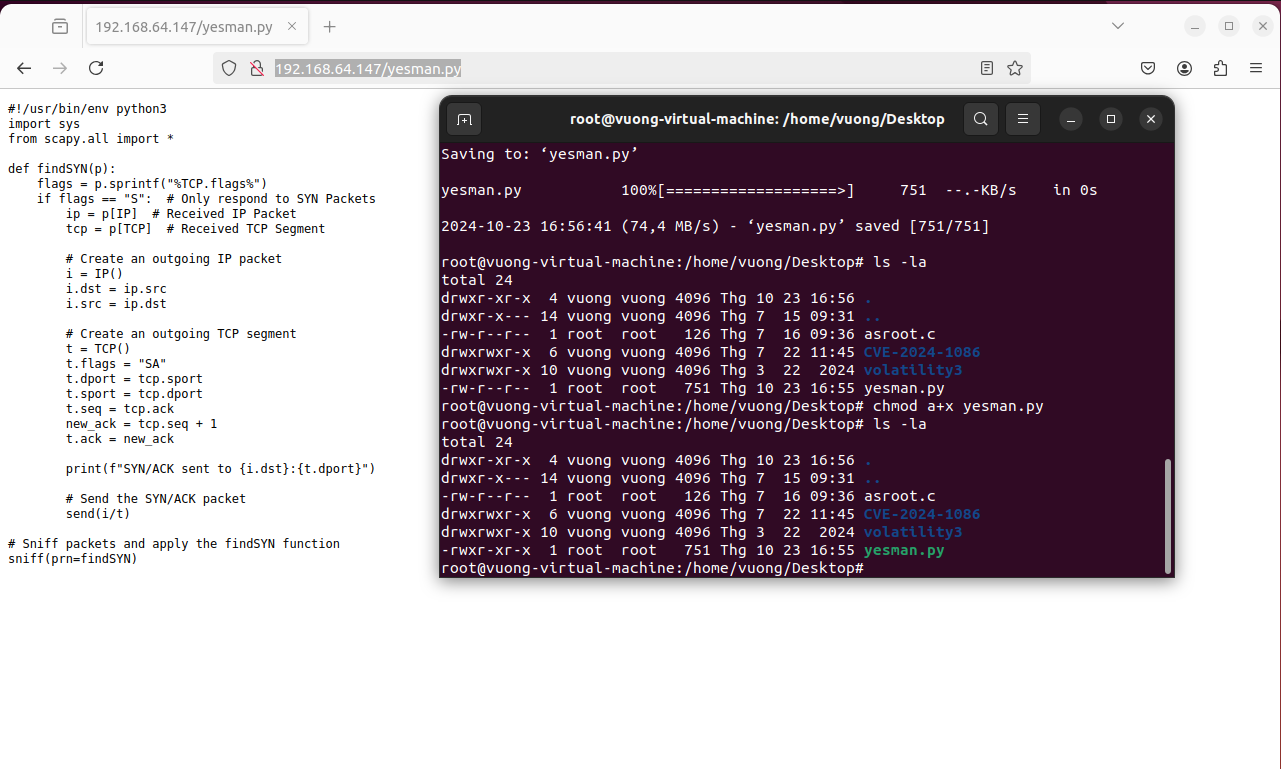
****

**(**Sửa code có sẵn trong bài tập thành python3**)**

* Copy file đã tạo vào thư mục **/var/www/html**

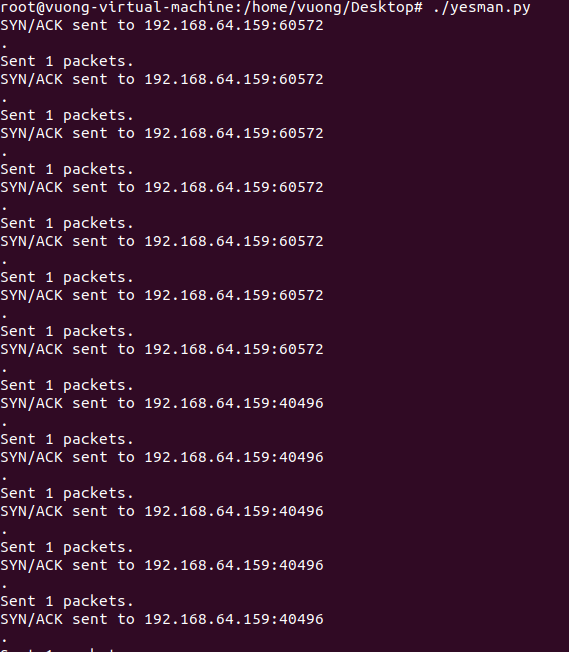
**\*** Trên máy Ubuntu:

* Truy cập vào trình duyệt, với đường dẫn: http://192 .168.64.147/yesman.py để cài đặt file yesman.py về máy
* Cấp quyền cho file yesman.py bằng lênh: **chmod a+x yesman.py**

****

**Starting yesman:**

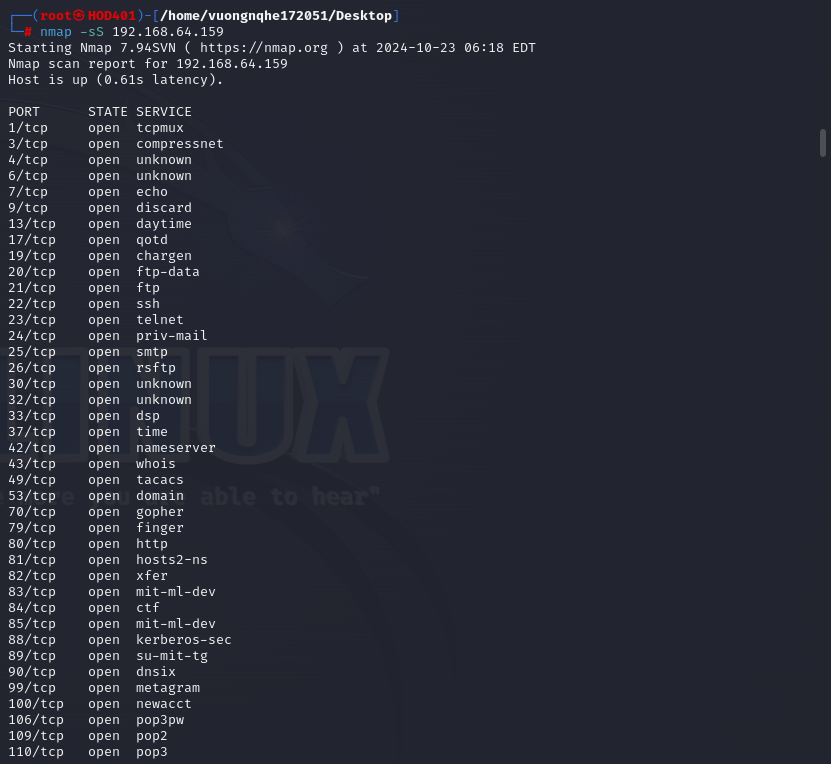
**\*** Trên máy Ubuntu, chạy file yesman.py bằng lệnh: **./yesman.py**

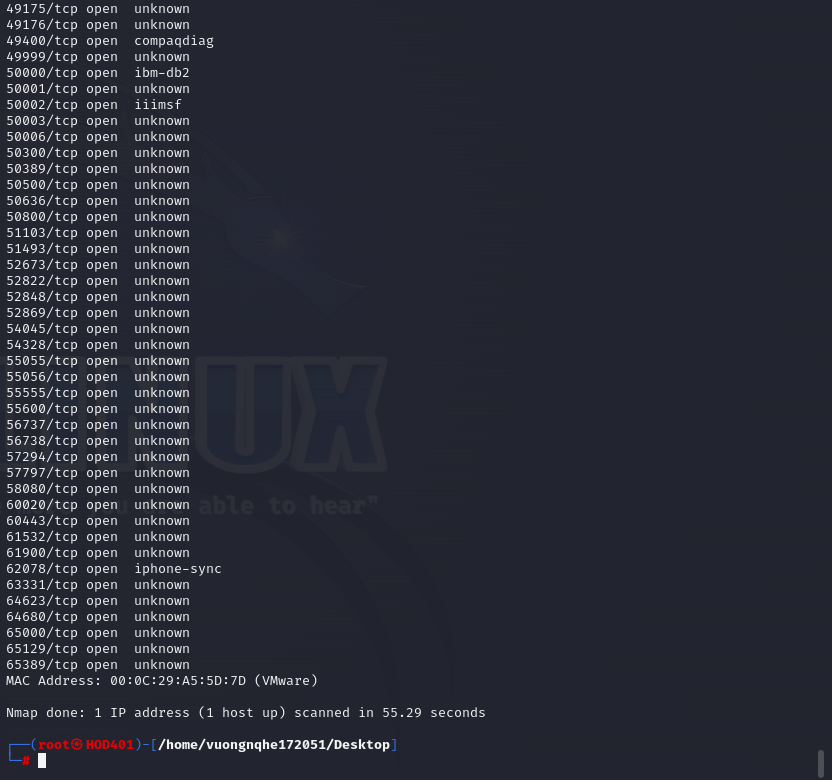
****

**Scanning the Protected Target Machine:**

**\*** Trên máy Kali:

* Sử dụng lệnh **nmap -sS 192.168.64.159** và thấy được kết quả như dưới:

****

****

**=>** Các cổng đều được quét