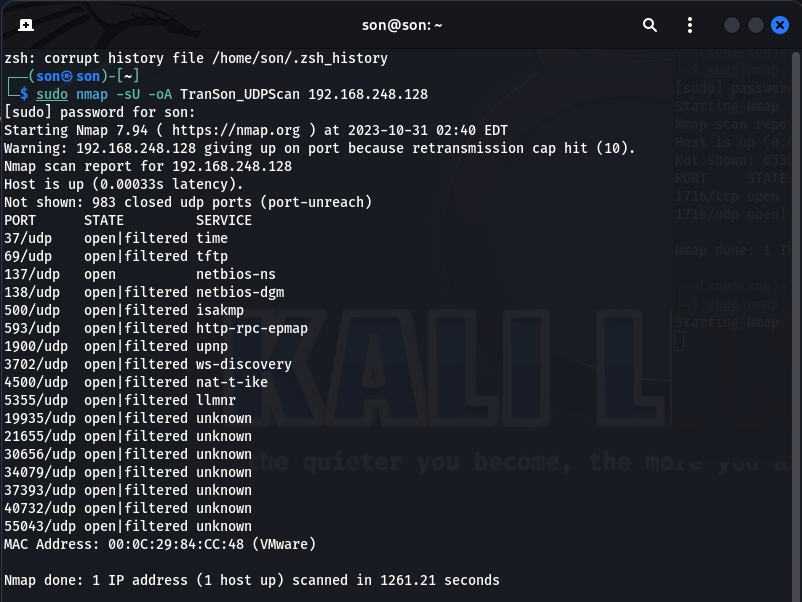
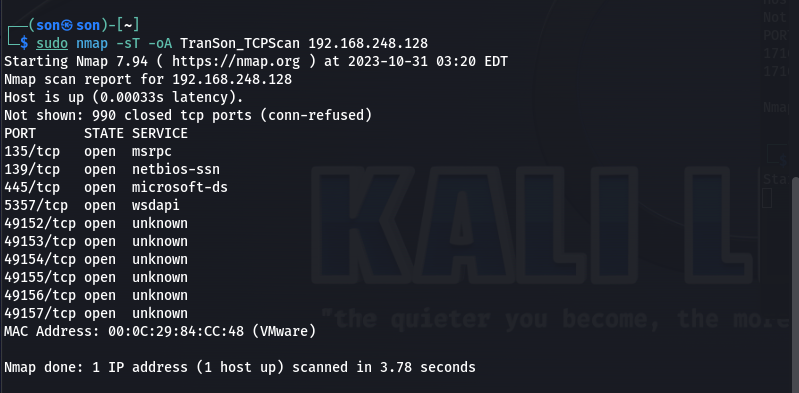
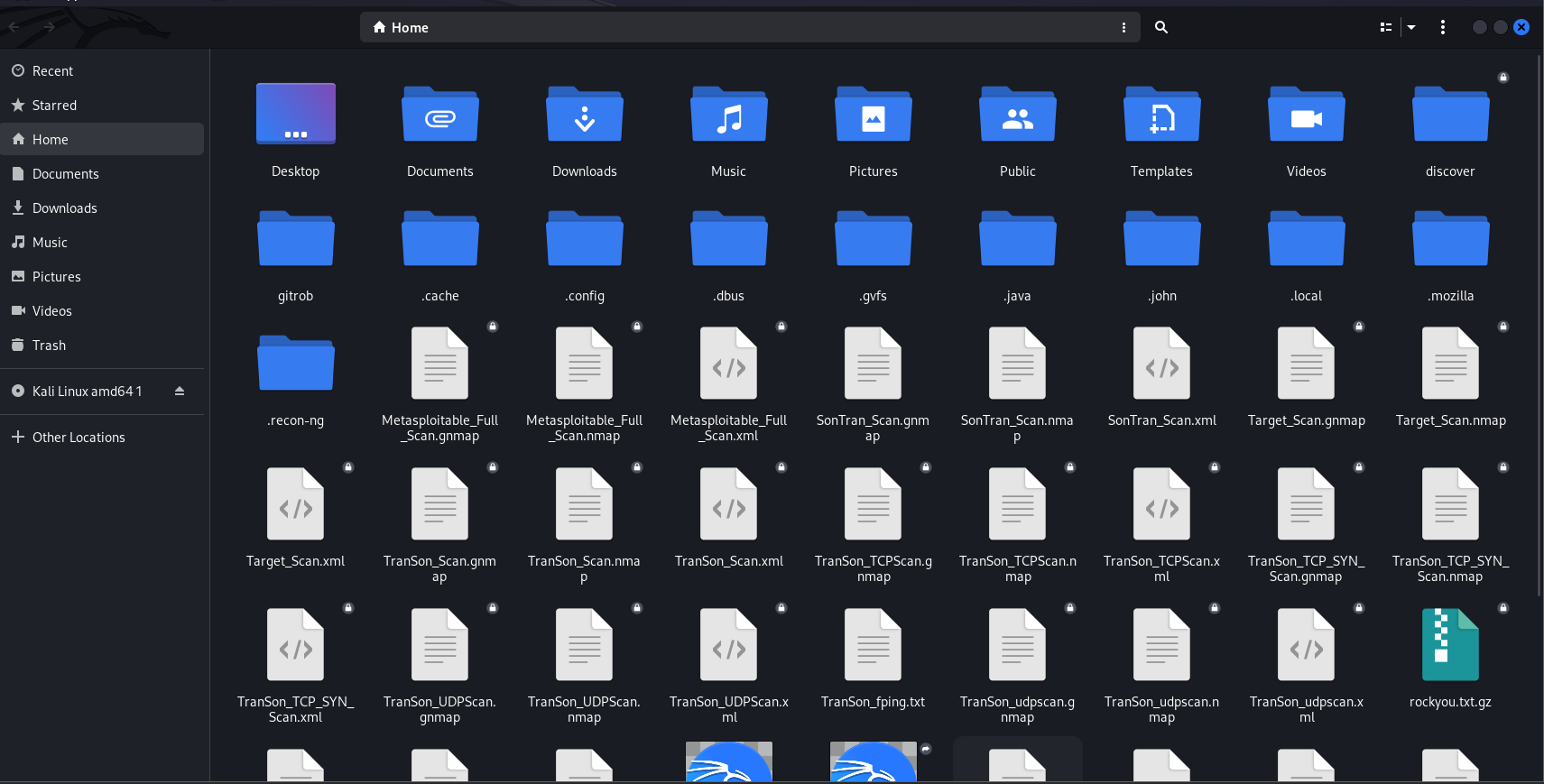
### **Save the output**

For each of the nmap commands below, you will need to save the output using the -oA flag, with a filename that includes your first initial, last name, and the scan type.



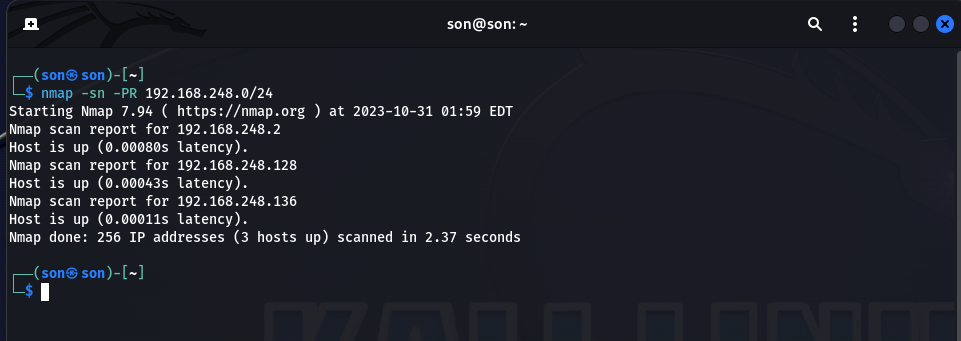






### **Host Discovery**

Use the proper nmap switch to determine which IP / hosts are alive on your network. Take a screenshot of the output.



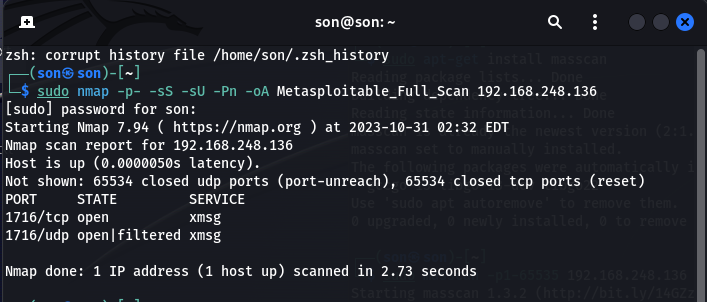
Trong đó:

- `sn` chỉ định quét mạng mà không quét các cổng.

- `PR` chỉ định sử dụng giao thức ARP để xác định các địa chỉ IP/hosts hoạt động.

### **Full Port Scan**

After locating the Metasploitable target in the previous step, conduct a full scan of all the ports on the target system and take a screenshot of the output. Be sure to include TCP and UDP results.



Trong đó:

- `-p-` chỉ định quét tất cả các cổng.

- `-sS` là loại quét TCP SYN Scan.

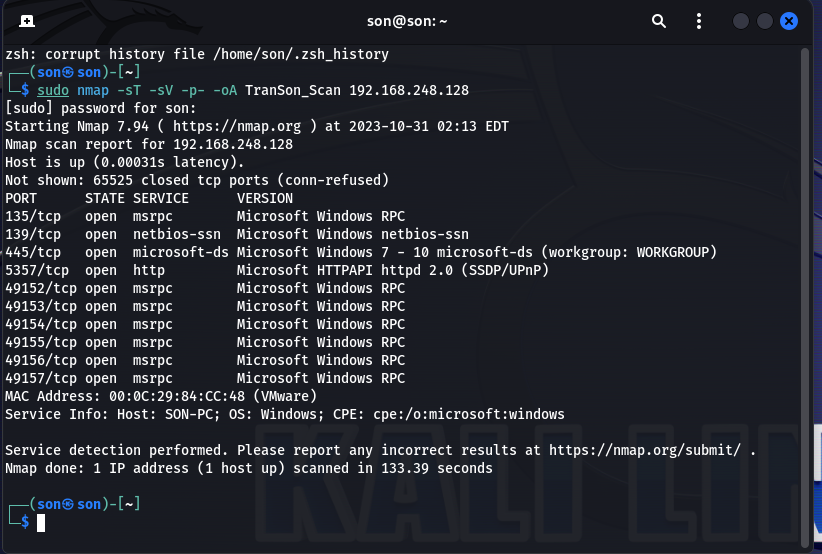
- `-sU` là loại quét UDP Scan.

- `-Pn` tắt việc kiểm tra tính sống của hệ thống mục tiêu.

- `-oA Metasploitable\_Full\_Scan` chỉ định tên tệp kết quả đầu ra.

### **TCP Connect Scan**

Using the proper nmap command, launch a TCP Connect scan against the target. This scan also needs to determine the operating system and the detailed service version information for each of the ports open on the system. Take a screenshot of the output.



Trong đó:

- `sT` là loại quét TCP Connect scan.

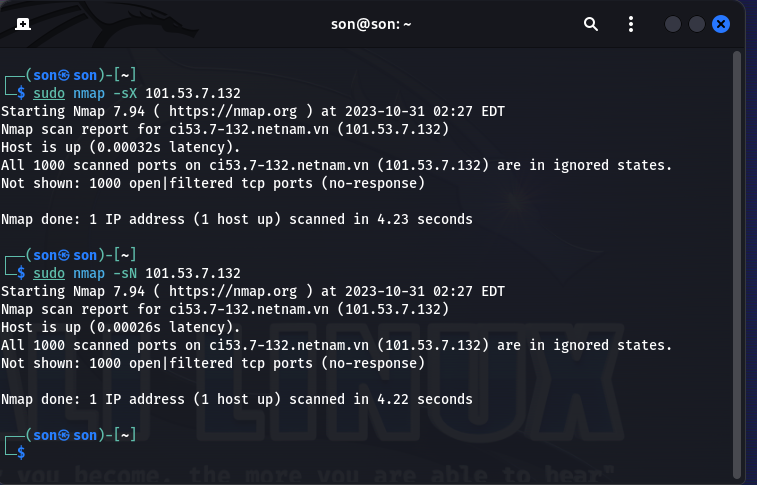
- `sV` cho phép xác định phiên bản dịch vụ chi tiết.

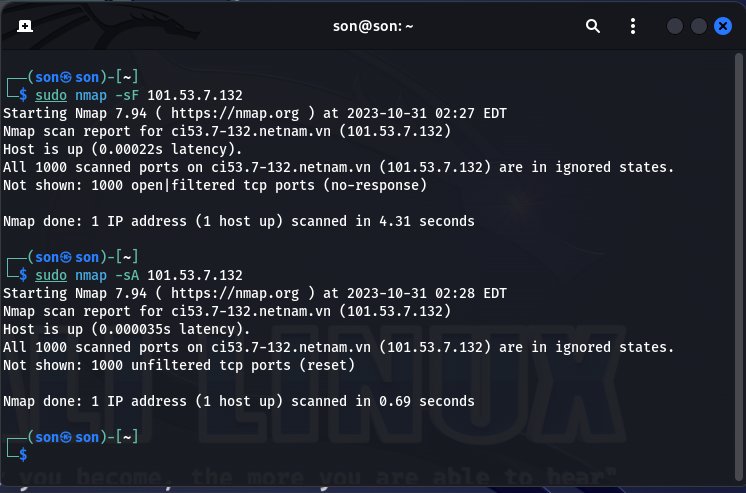
- `-p-` chỉ định quét tất cả các cổng.

- `oA Target\_Scan` chỉ định tên tệp kết quả đầu ra.

### **Violate the TCP Protocol**

Run an NMAP scan that violates the TCP protocol. Take a screenshot of the output. Examples of scans that violate the TCP protocol include FIN, Xmas tree, Null, Ack, etc.





-sX: Quét Xmas tree (vi phạm giao thức TCP).

-sN: Quét Null (vi phạm giao thức TCP).

-sF: Quét FIN (vi phạm giao thức TCP).

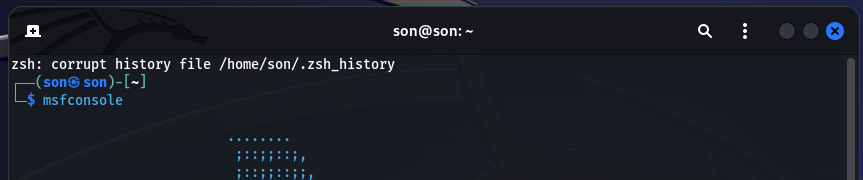
-sA: Quét Ack (vi phạm giao thức TCP).

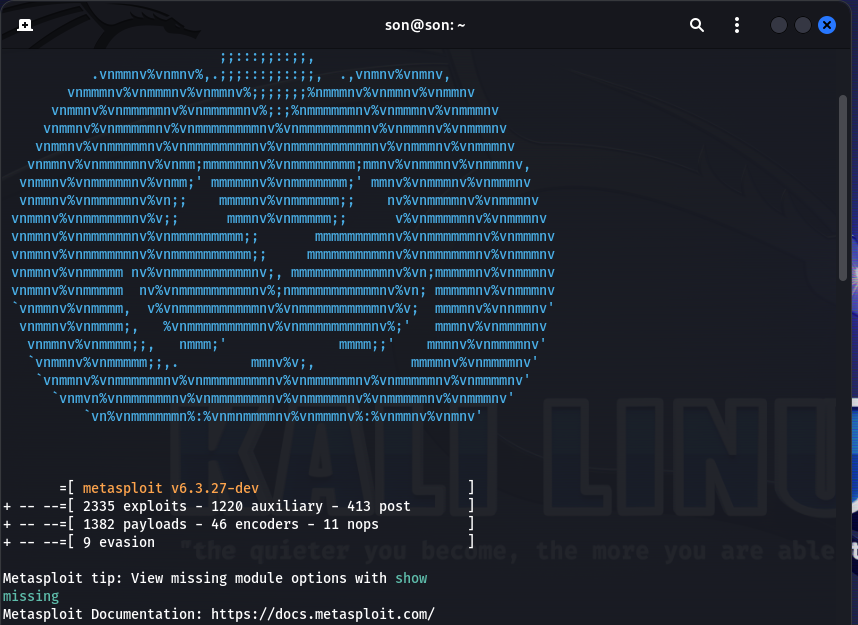
### **Choose your own port scanner**

Run a different port scanner against the Metasploitable machine and take a screenshot of the output. This will give you an opportunity to take a look at and evaluate other tools and utilities.

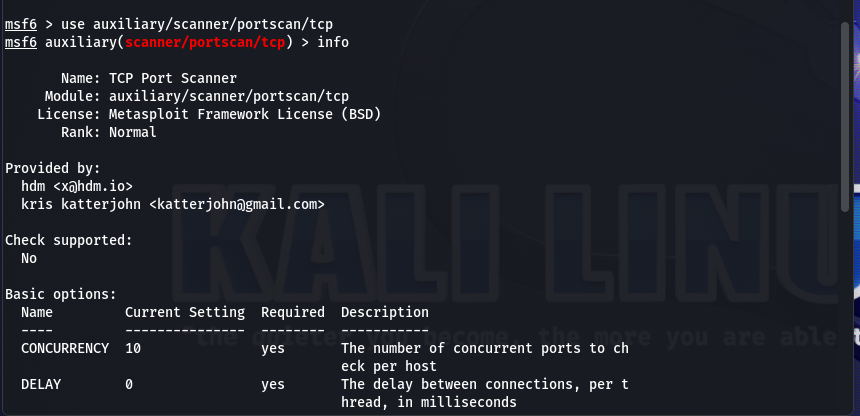
Tool sử dụng là : Metasploit Framework

Nhập msfconsole để khởi động Metasploit Framework





Trong giao diện Metasploit, sử dụng module auxiliary/scanner/portscan/tcp để quét cổng TCP. Chạy lệnh sau để xem thông tin về module:



Đặt các tùy chọn cho module auxiliary/scanner/portscan/tcp. => Chạy module để thực hiện quét cổng bằng lệnh run. Đây là kết quả sau khi quét.

