BÁO CÁO LAB 4

Môn: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

GVTH: ĐỖ HOÀNG HIỂN

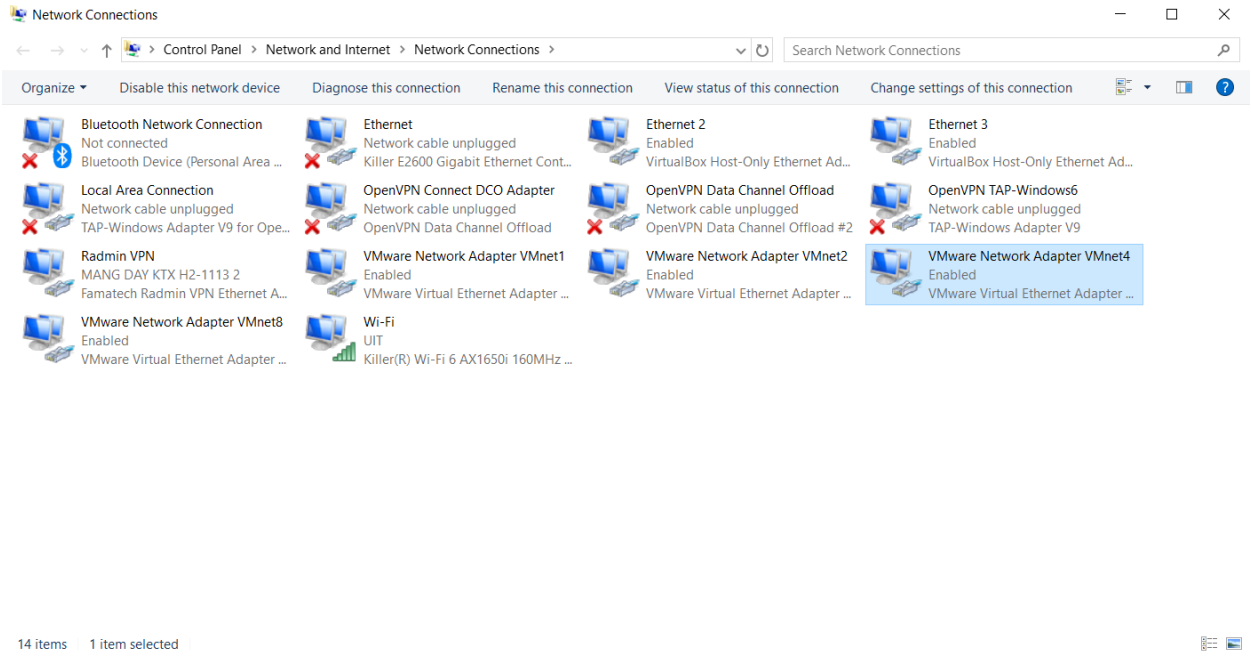
Sinh viên thực hiện	**Sinh viên 1** MSSV: 21522573 Họ tên: Phạm Thanh Tâm **Sinh viên 2** MSSV: 21520514 Họ tên: Nguyễn Văn Anh Tú
Lớp	**NT204.O21.ATCL**
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc *(nếu là nhóm)*	**[Sinh viên 1]**: **[Sinh viên 2]**:
Link Video thực hiện *(nếu có yêu cầu)*	
Ý kiến *(nếu có)* *+ Khó khăn gặp phải* *+ Đề xuất, góp ý…*	
Điểm tự đánh giá *(bắt buộc)*	10 /**10**

[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

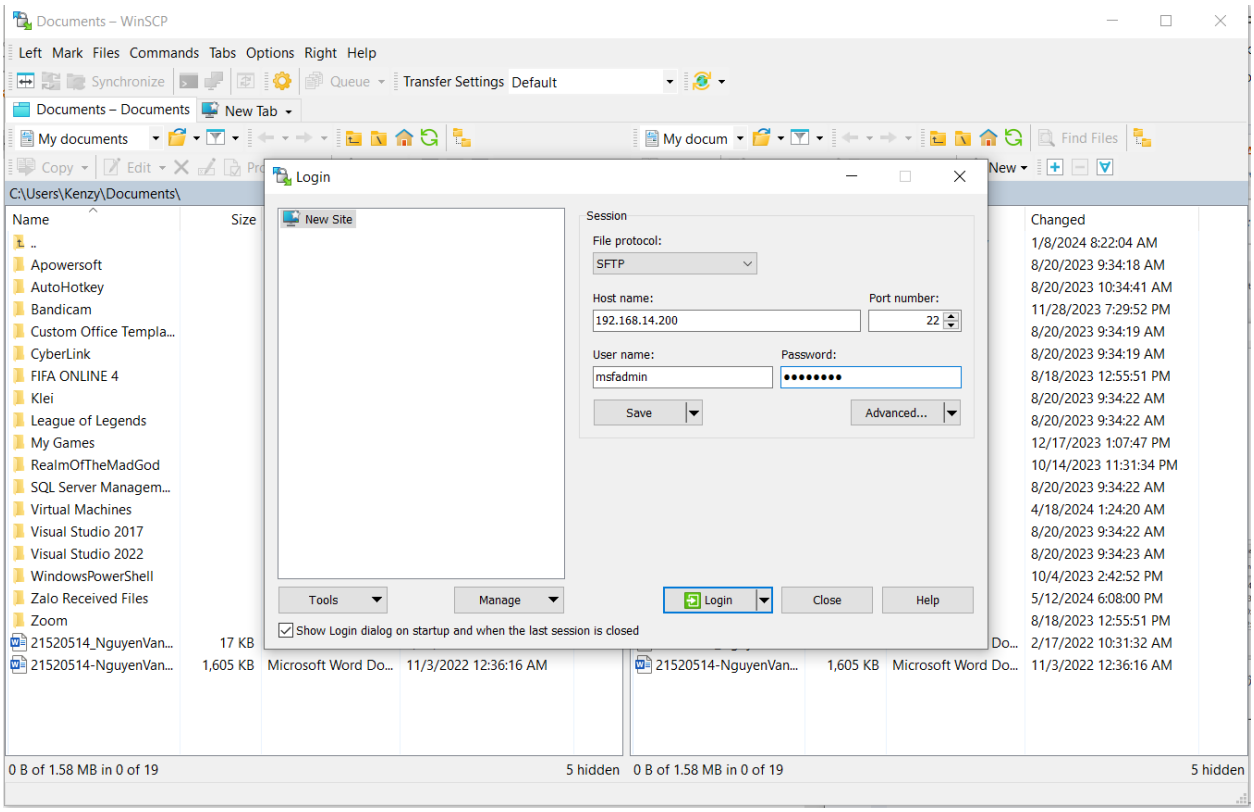
BÁO CÁO CHI TIẾT

Các yêu cầu cần thiết

Enable card mạng VMnet 4

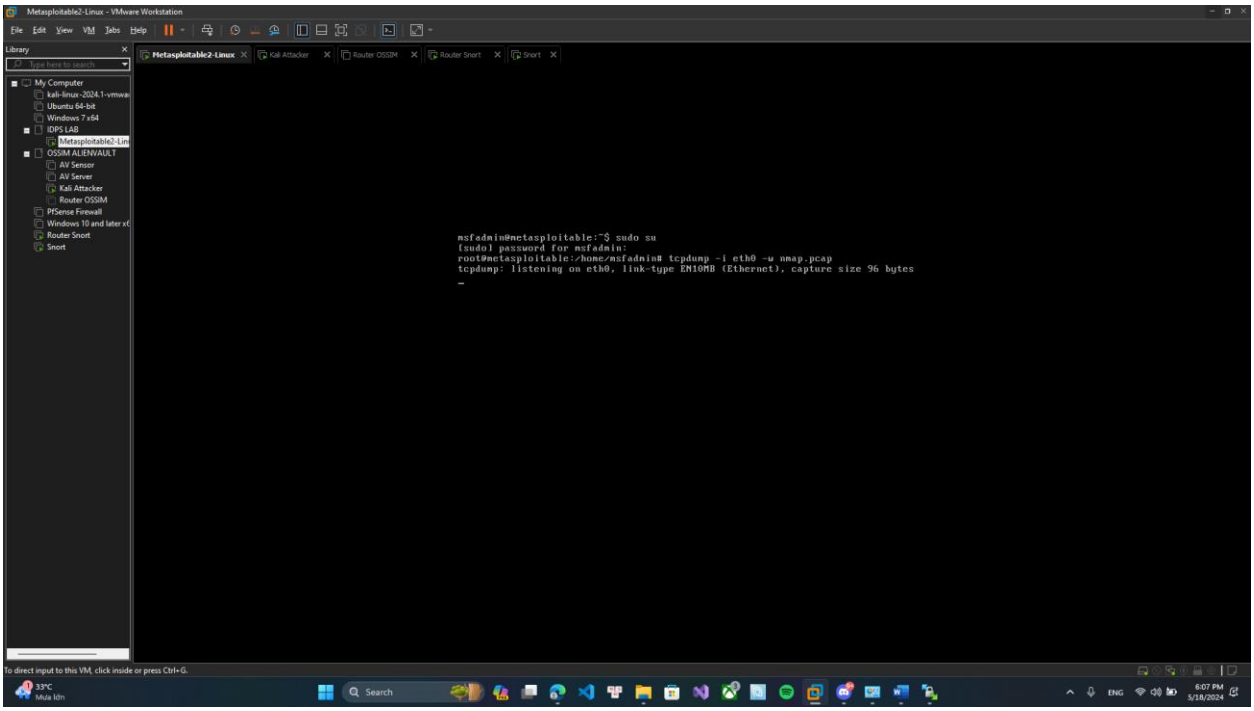


Kết nối tới máy Metasploit bằng WinSCP

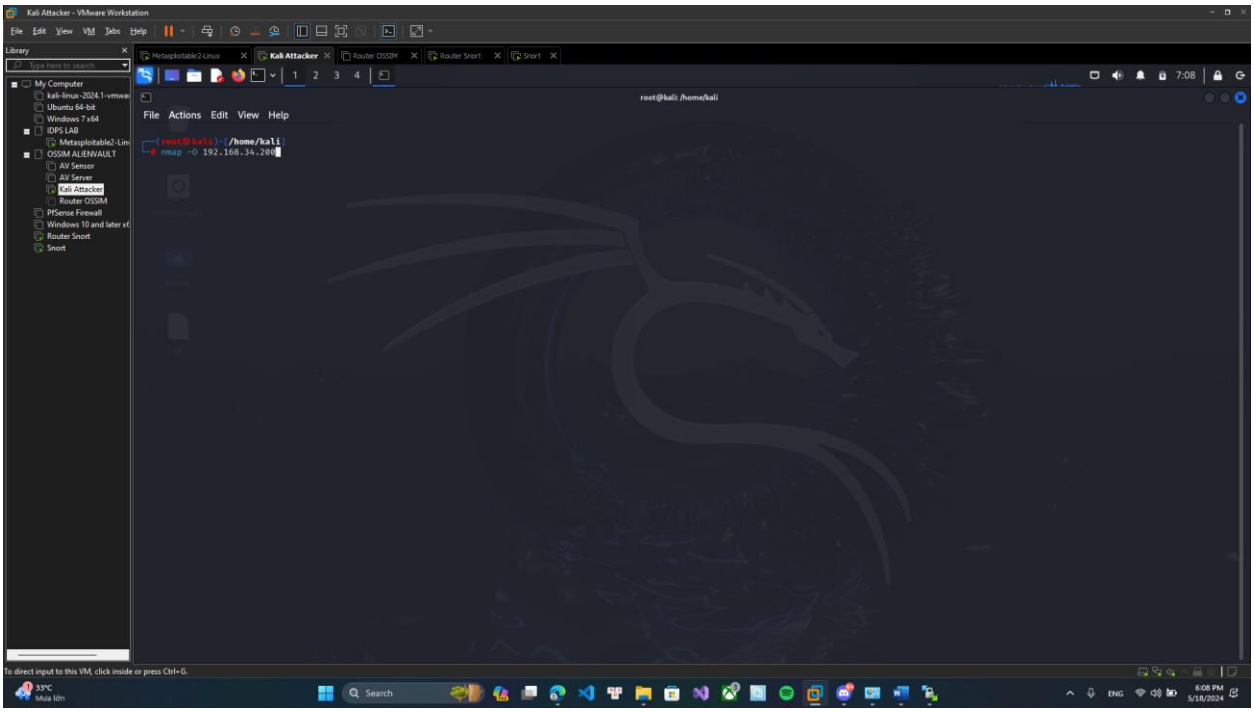


Yêu cầu 1.1: Ngăn chặn công cụ nmap dò quét thông tin hệ điều hành

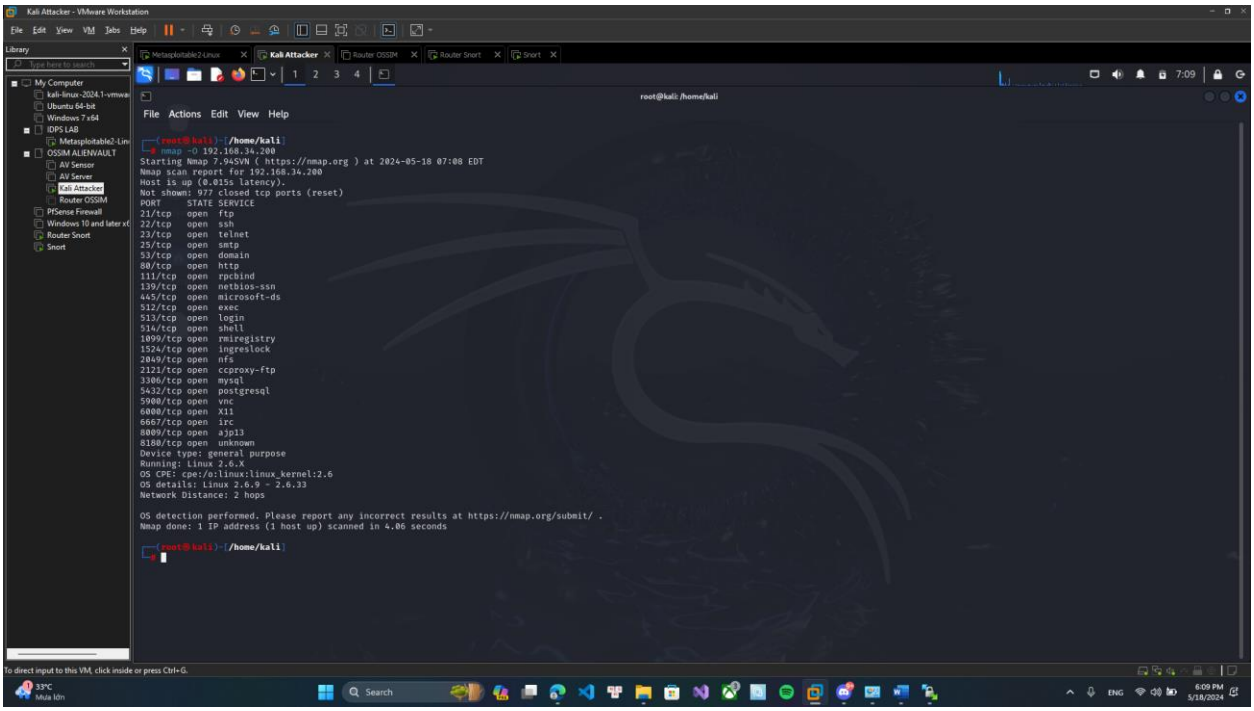
- Trên máy Victim Metasploitable sử dụng lệnh : tcpdump -i eth0 -w nmap.pcap



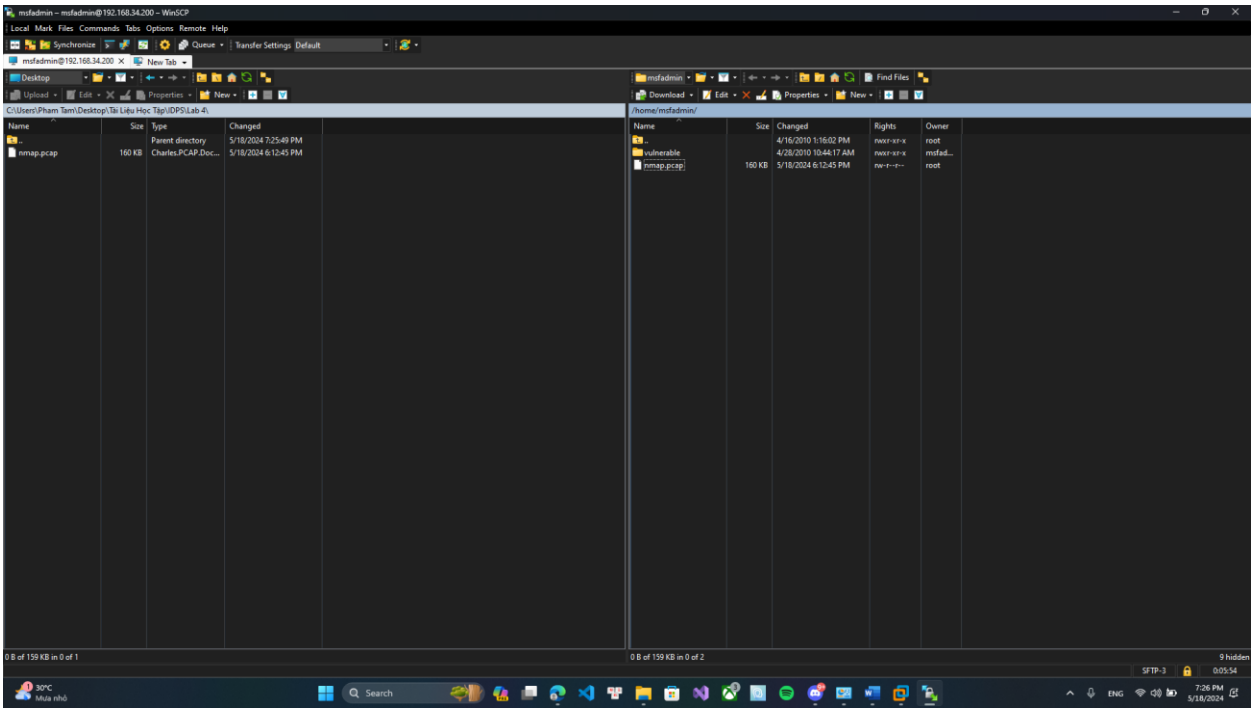
- Trong lúc đang lắng nghe thì qua máy Kali attack vào máy Victim :



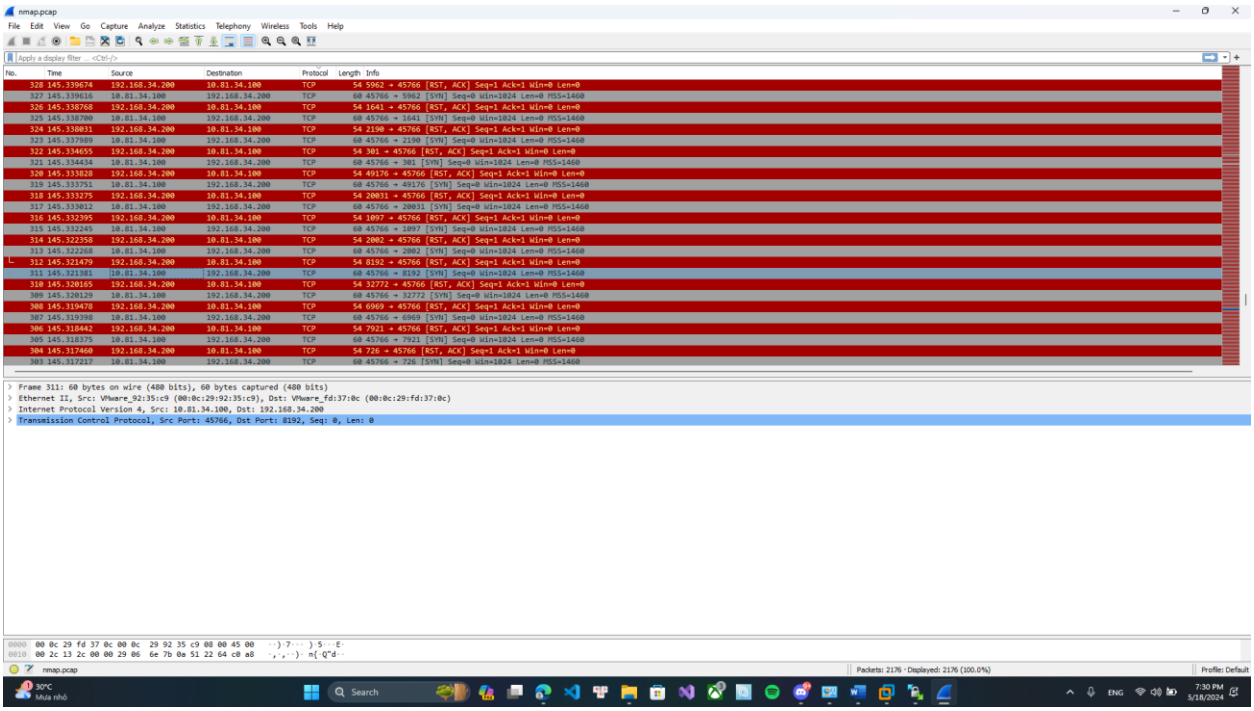
- Thực hiện Scan OS trên máy Kali: nmap -O 192.168.7.200



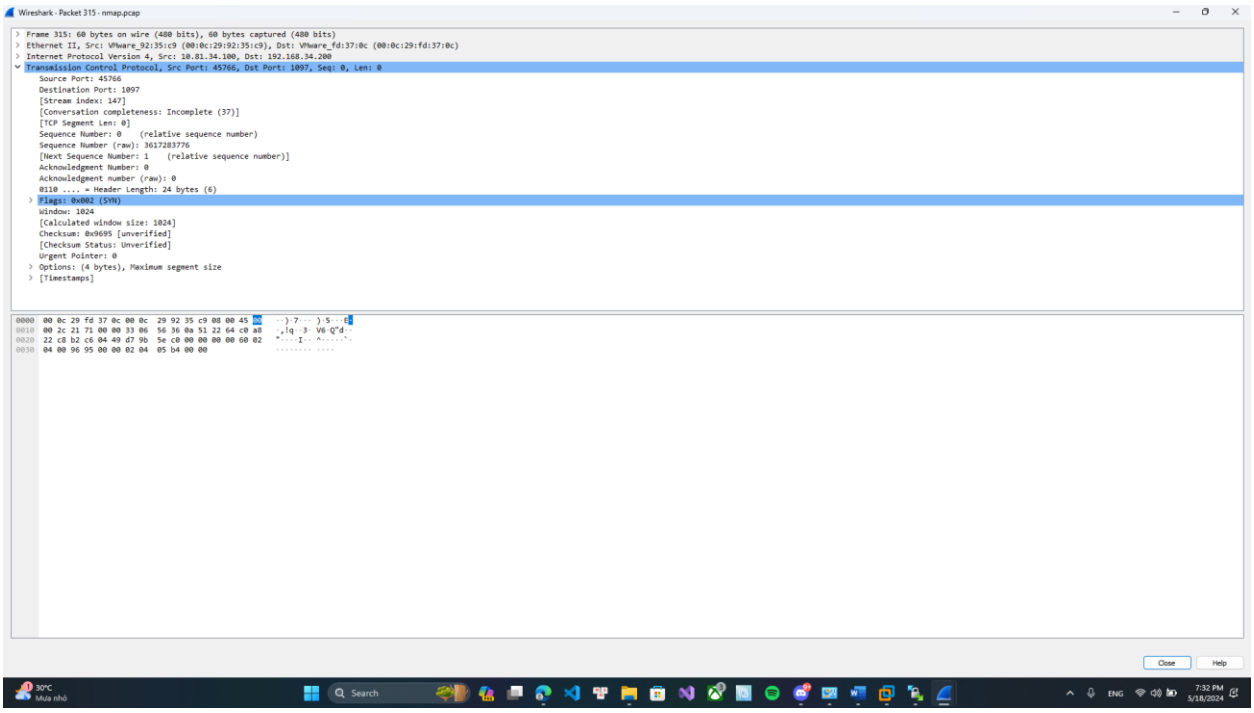
- Tải file nmap.pcap về máy thật:



- Mở file nmap.pcap bằng wireshark ta thấy rất nhiều gói SYN được gửi đến ip của Metasploitable (192.168.34.200) :



- Ta thử chọn 1 gói để phân tích:

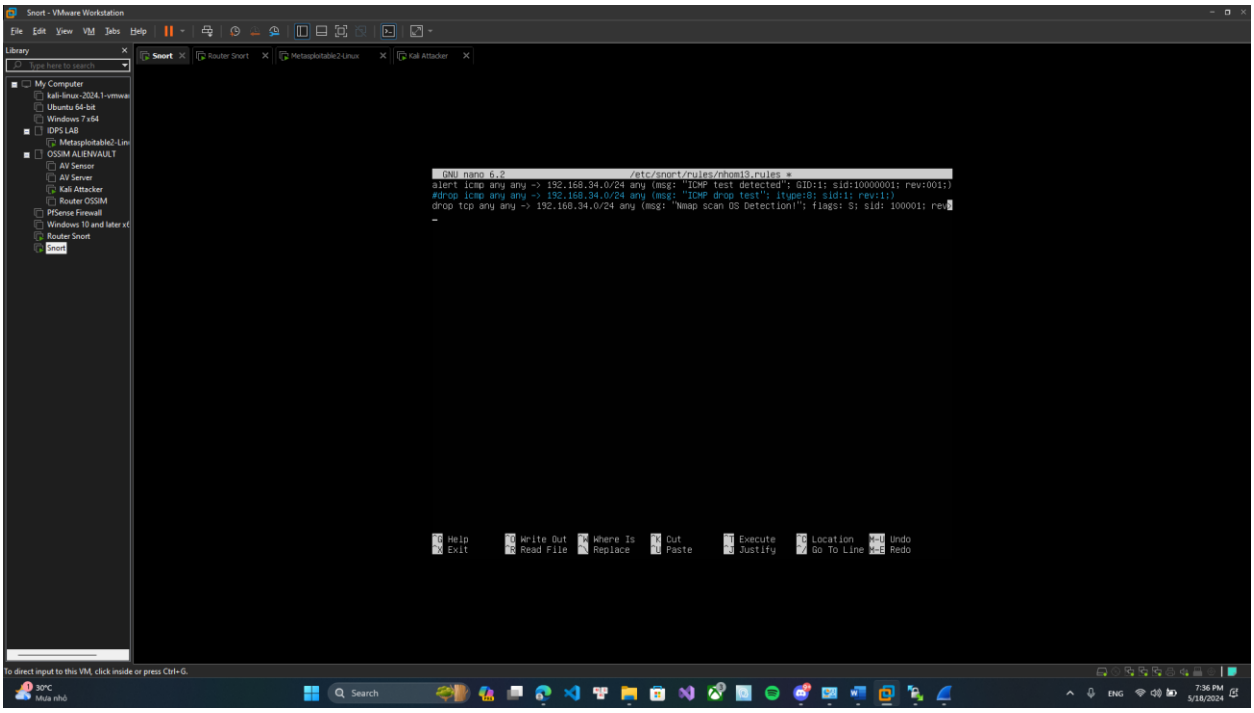


- Tất cả các gói đều có 1024 byte và TCP Segment Len là 0

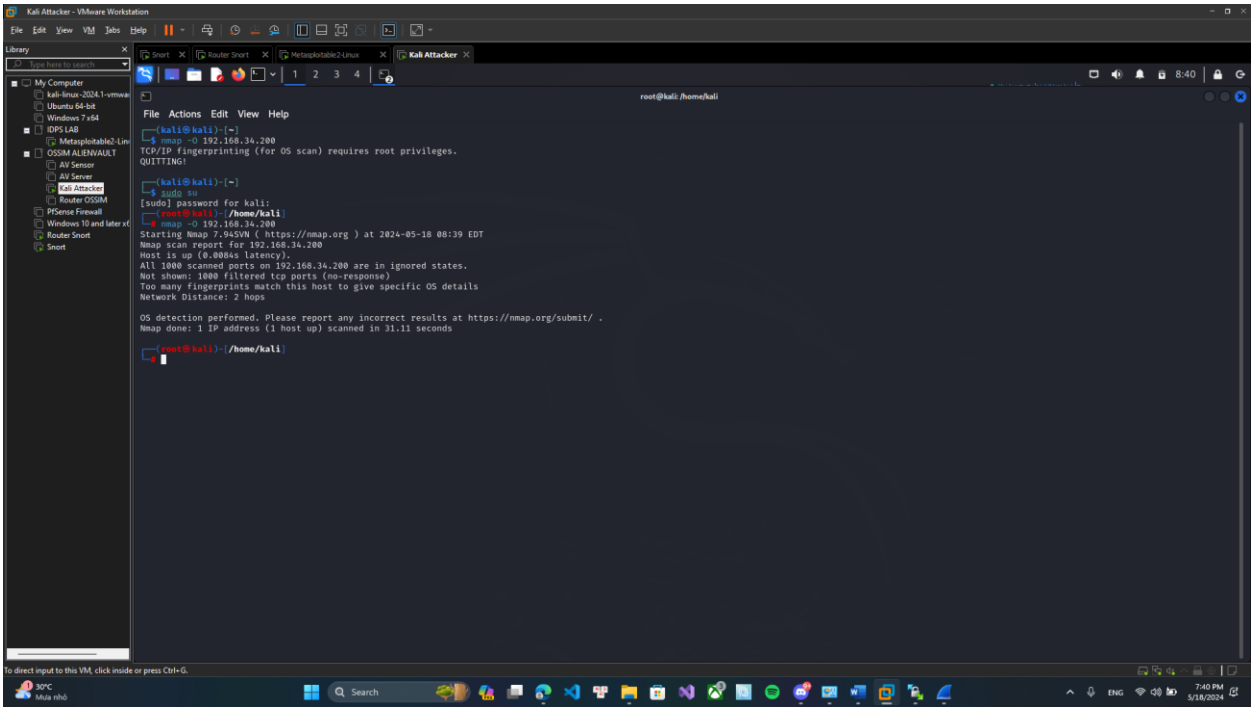
=> Đây là dấu hiệu của việc máy đã bị Scan port và để ngăn chặn việc này ta cần chặn scan port

- Thêm rule cho máy Snort:

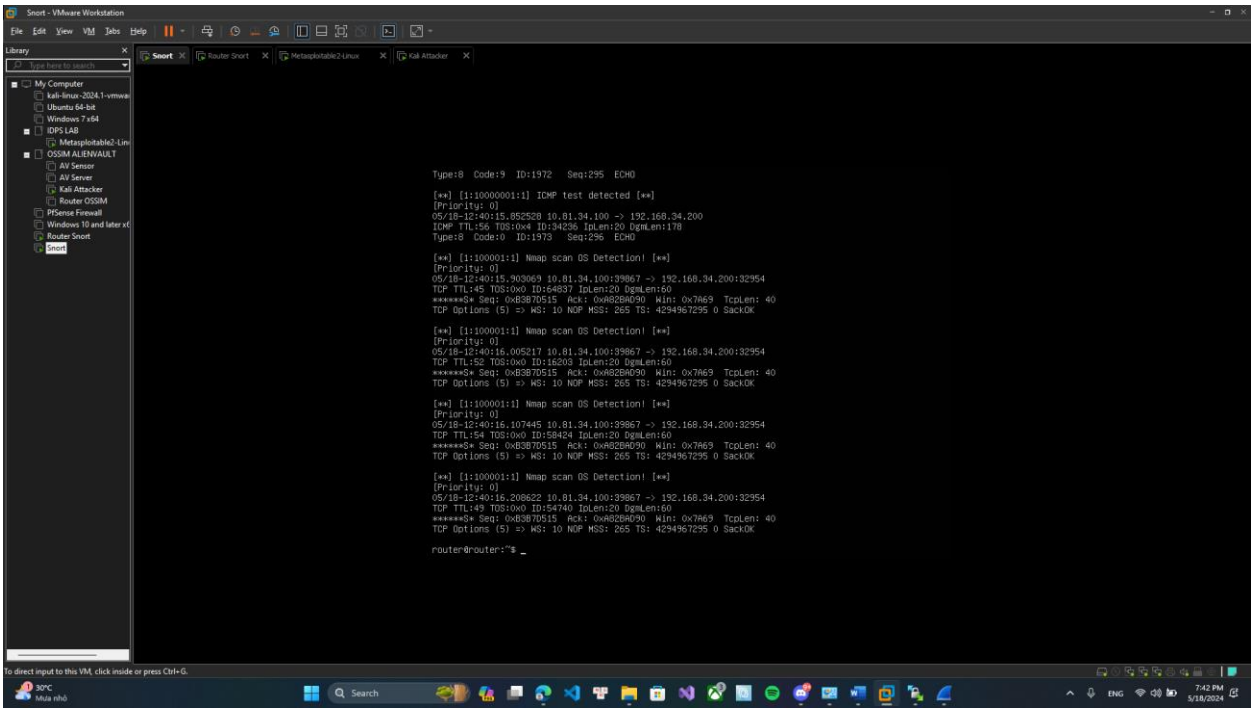
“drop tcp any any ->192.168.34.0/24 any (msg: “Nmap scan OS Detection!”; flags: S; sid: 100001; rev: 1;)



- Không thể scan được nữa sau khi set rule:

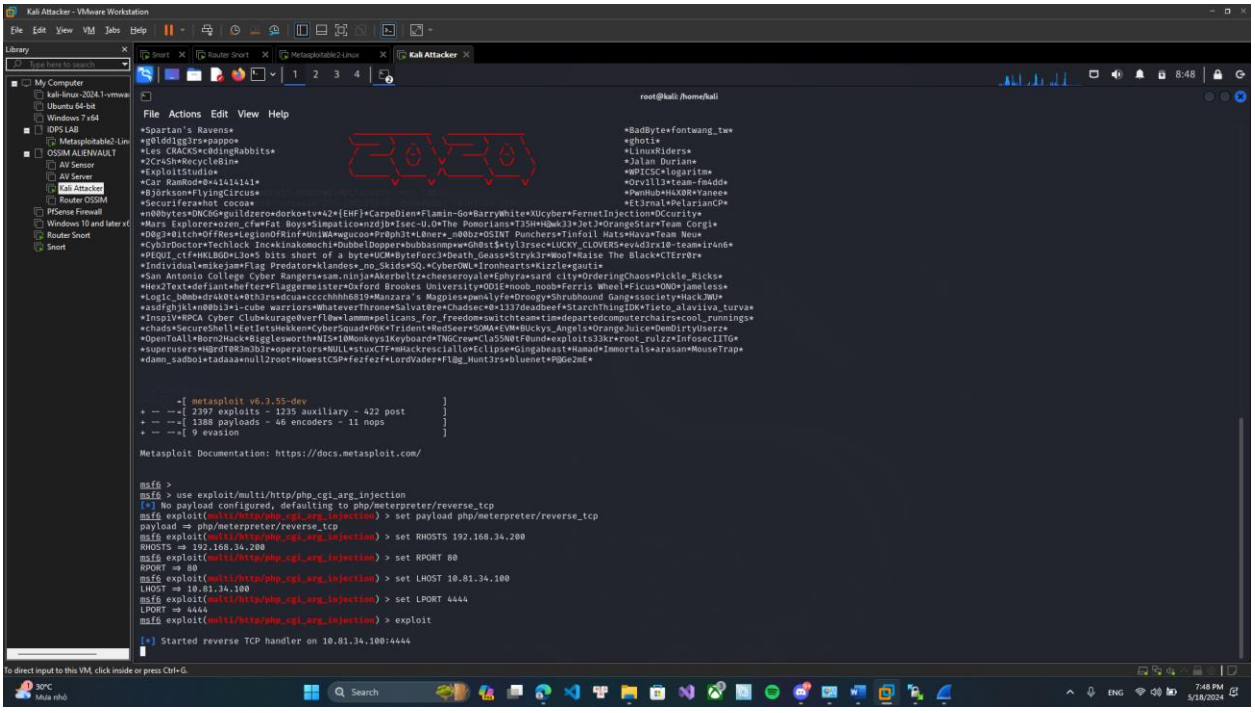


- Log mà Snort đã phát hiện ra đồng thời chặn:

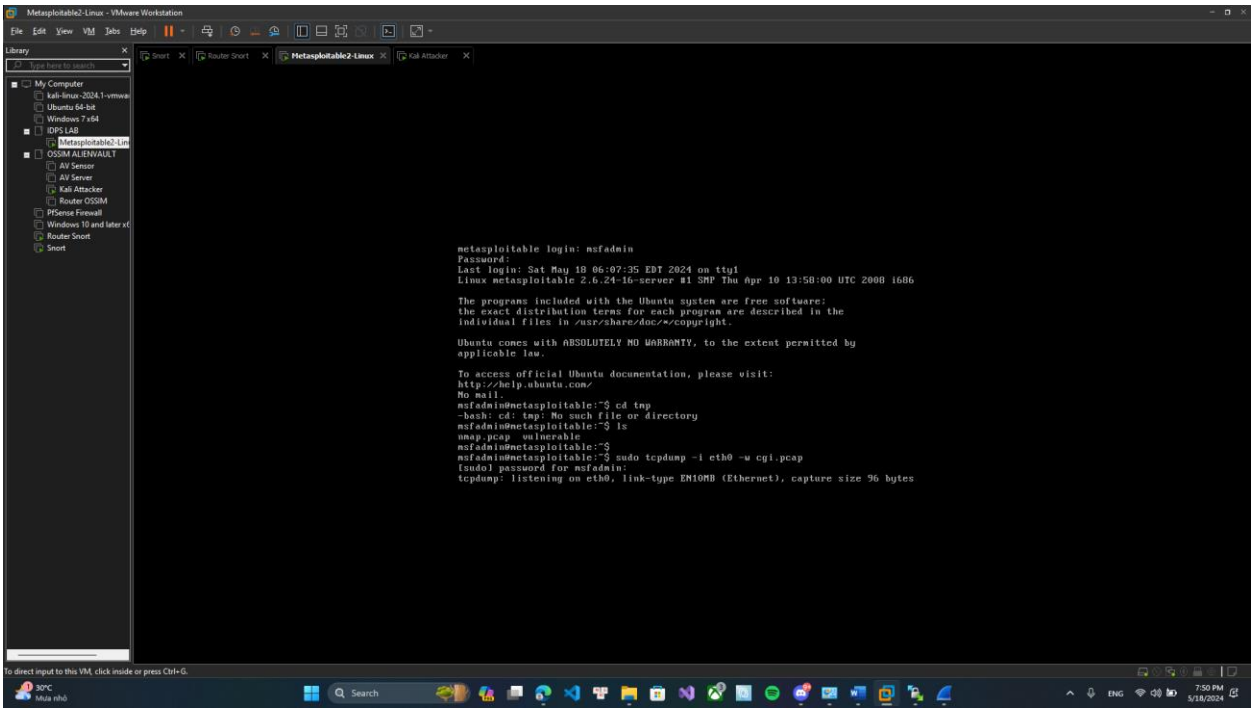


Yêu cầu 1.2: Ngăn chặn lỗ hổng PHP CGI Argument

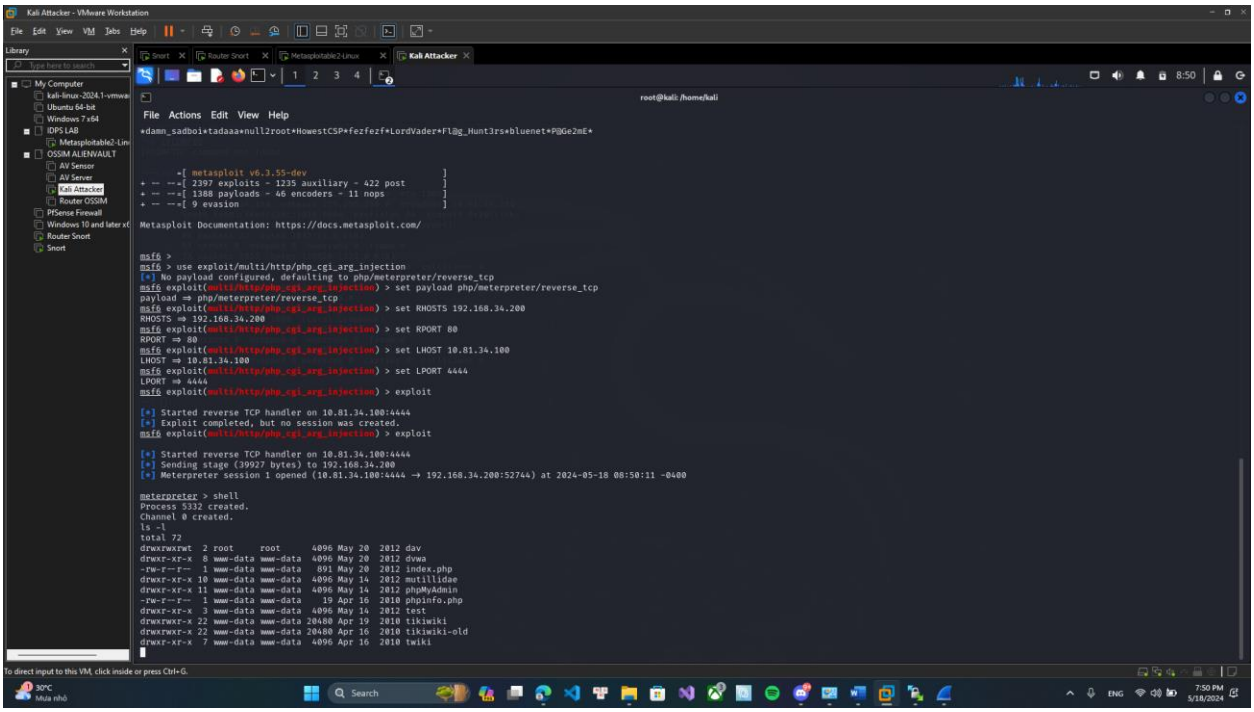
- Trên máy Kali tiến hành attack PHP CGI Argument:



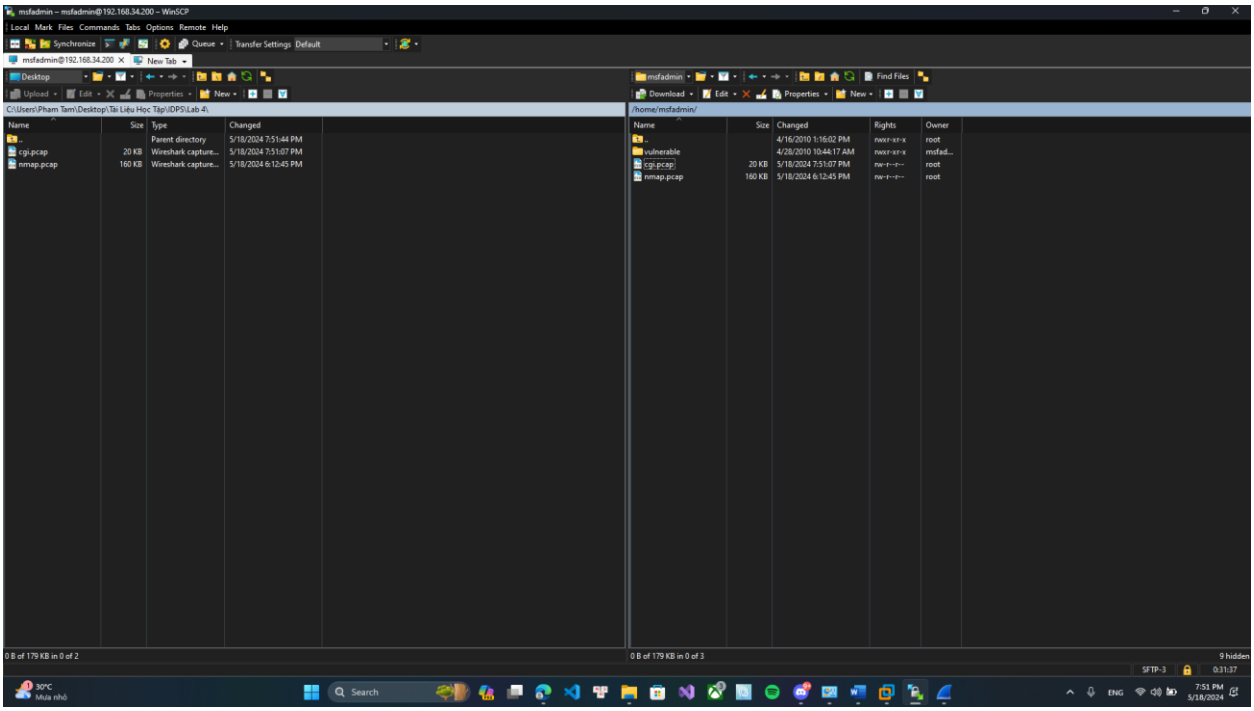
- Đồng thời trên máy victim đang lắng nghe:



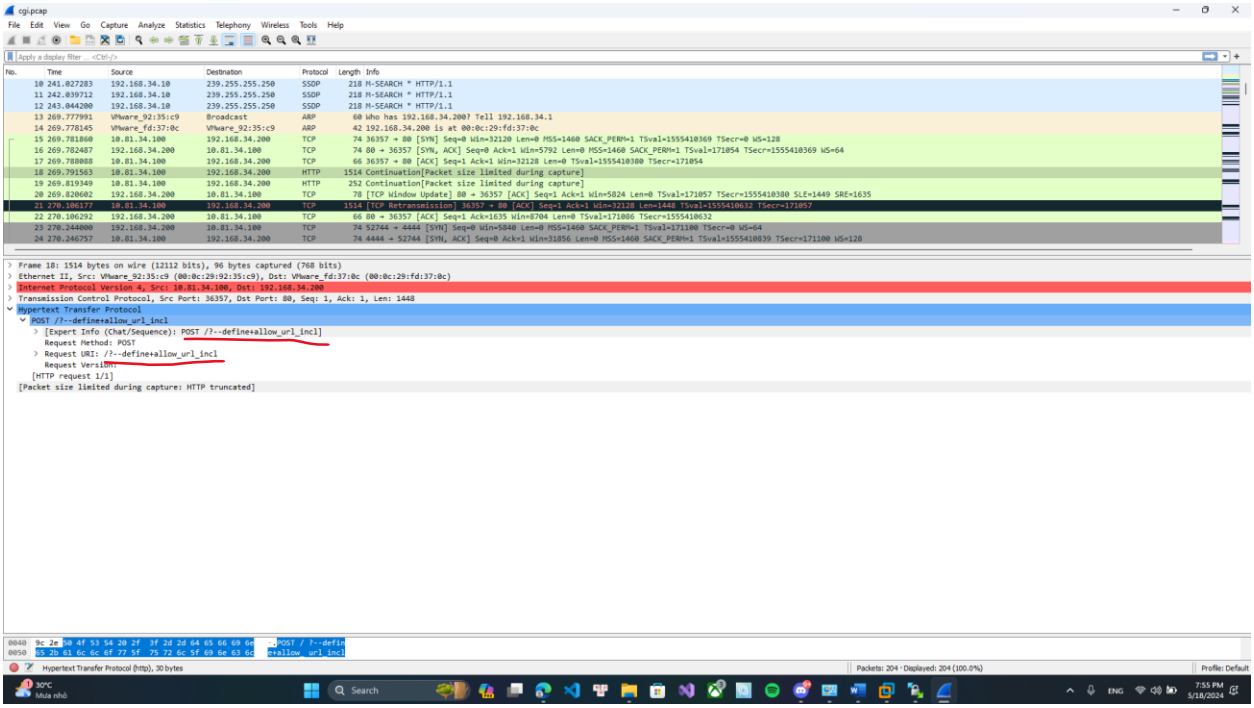
- Attack thành công:



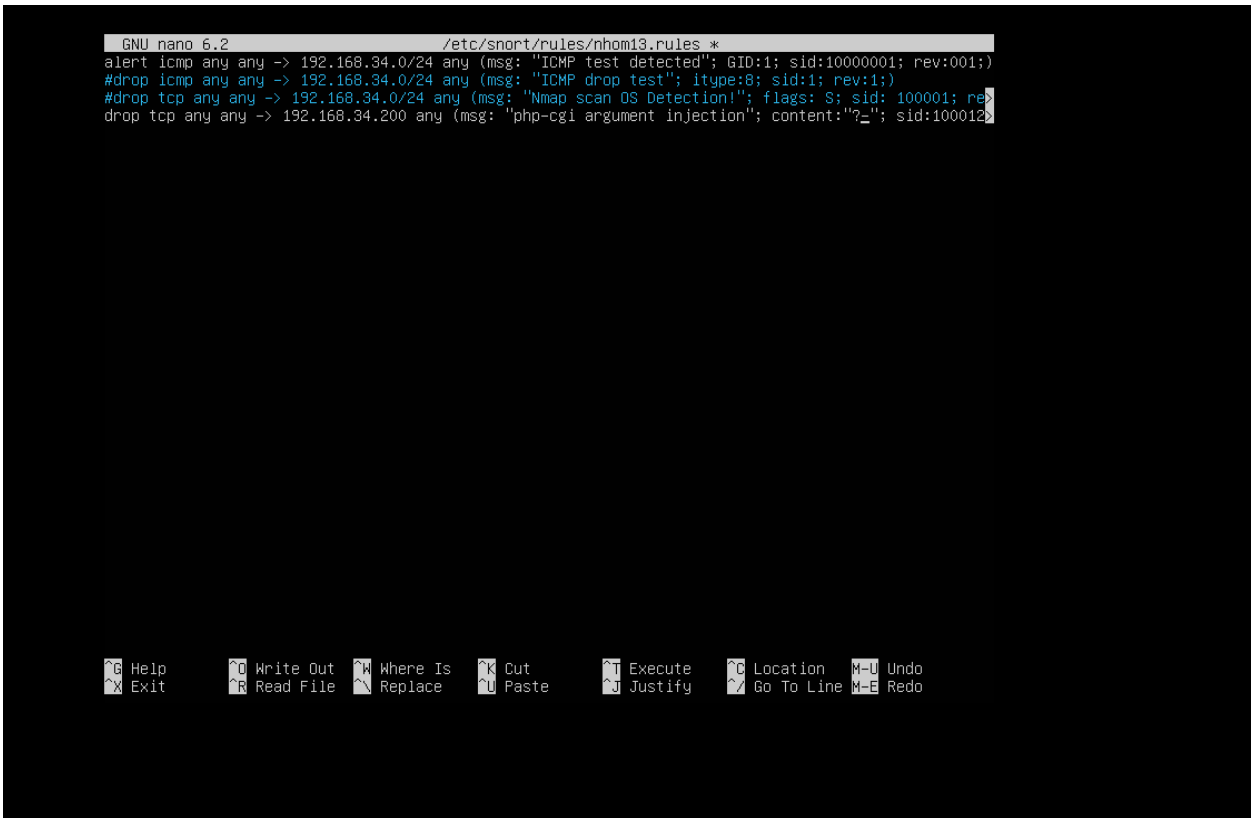
- Lấy file cgi.pcap về máy thật để phân tích:



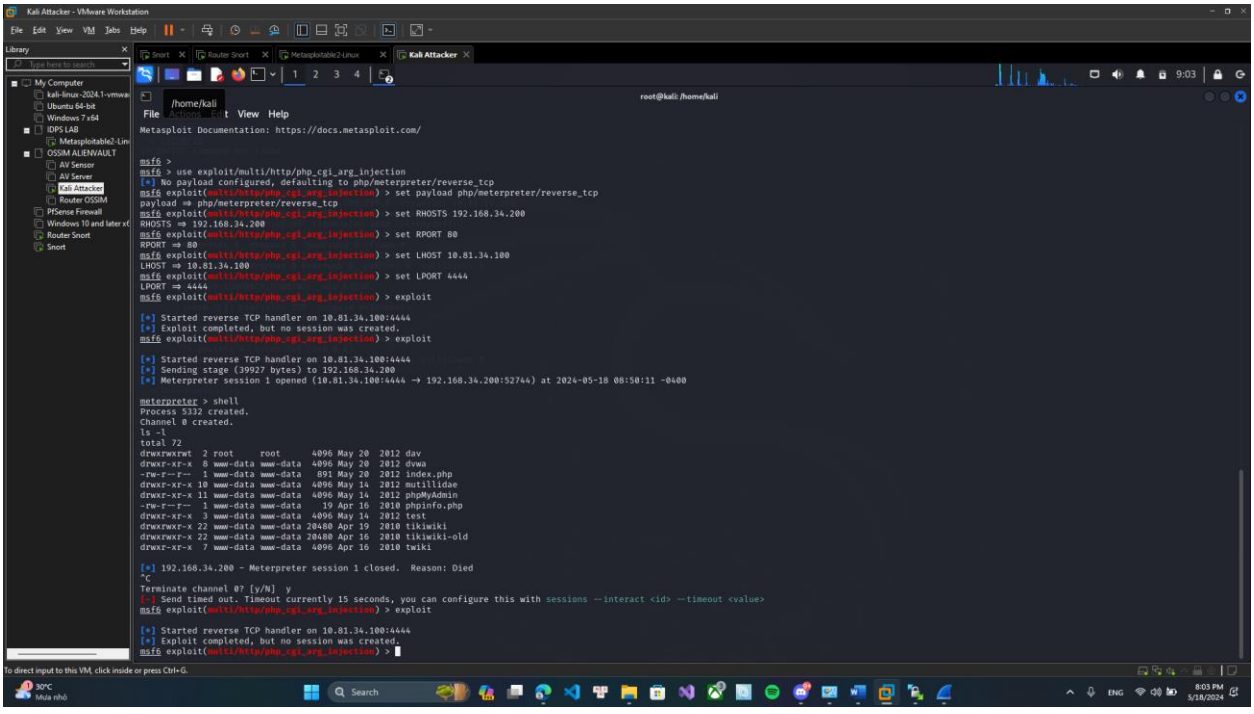
- Dựa trên phân tích ta thấy có yêu cầu HTTP đáng ngờ khi mà nó yêu cầu POST với tham số không hợp lệ: :



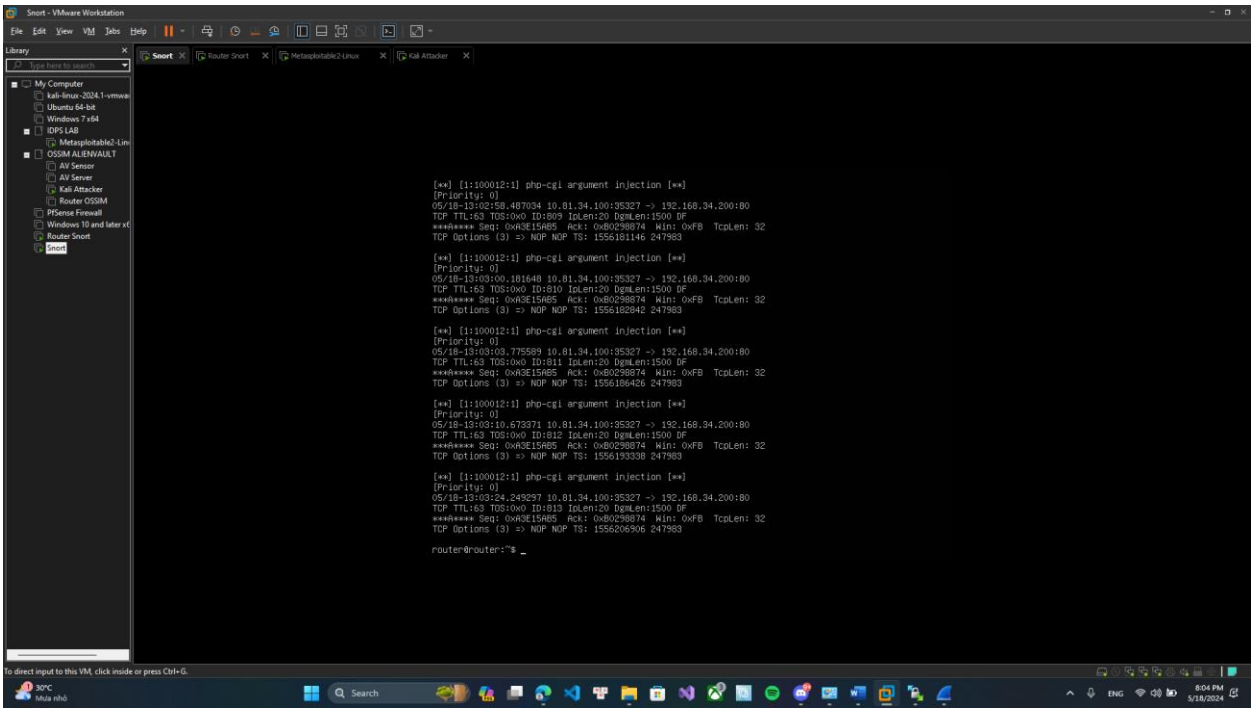
- Ta thêm rule vào Snort:



- Attack đã bị block:

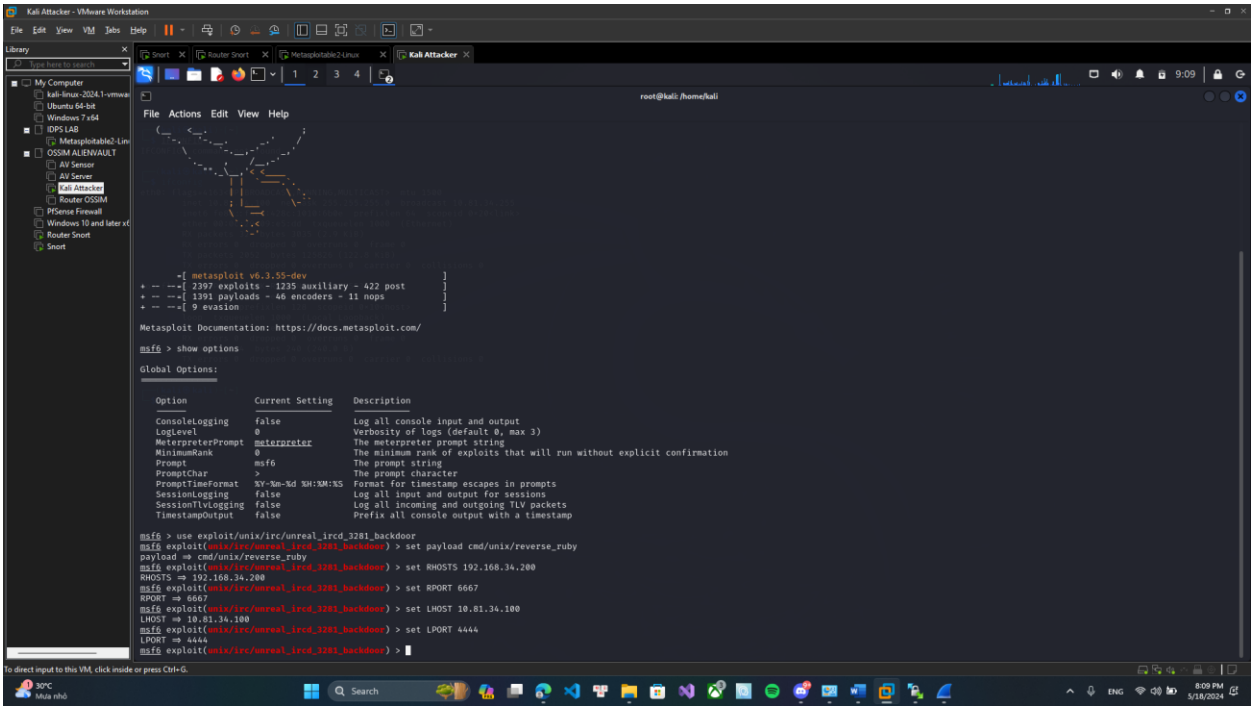


- Log trả về:

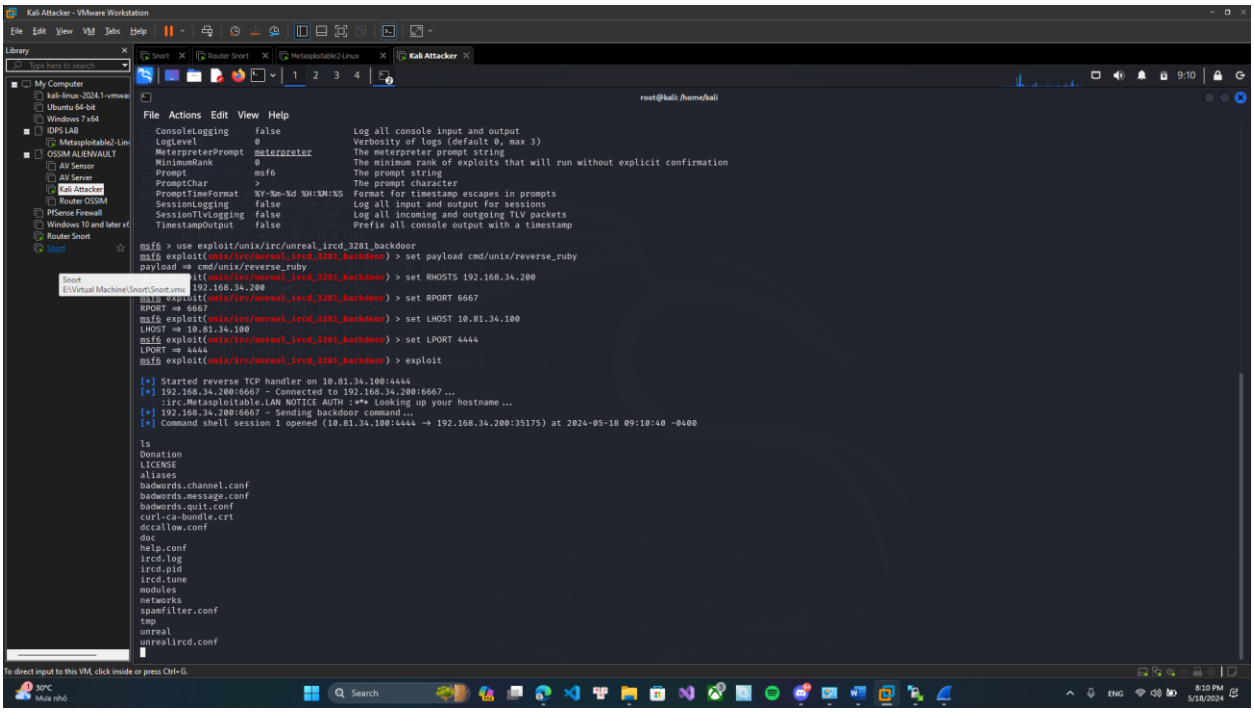


Yêu cầu 1.3: Ngăn chặn lỗ hổng UnrealIRCD 3.2.8.1 Backdoor Command Execution

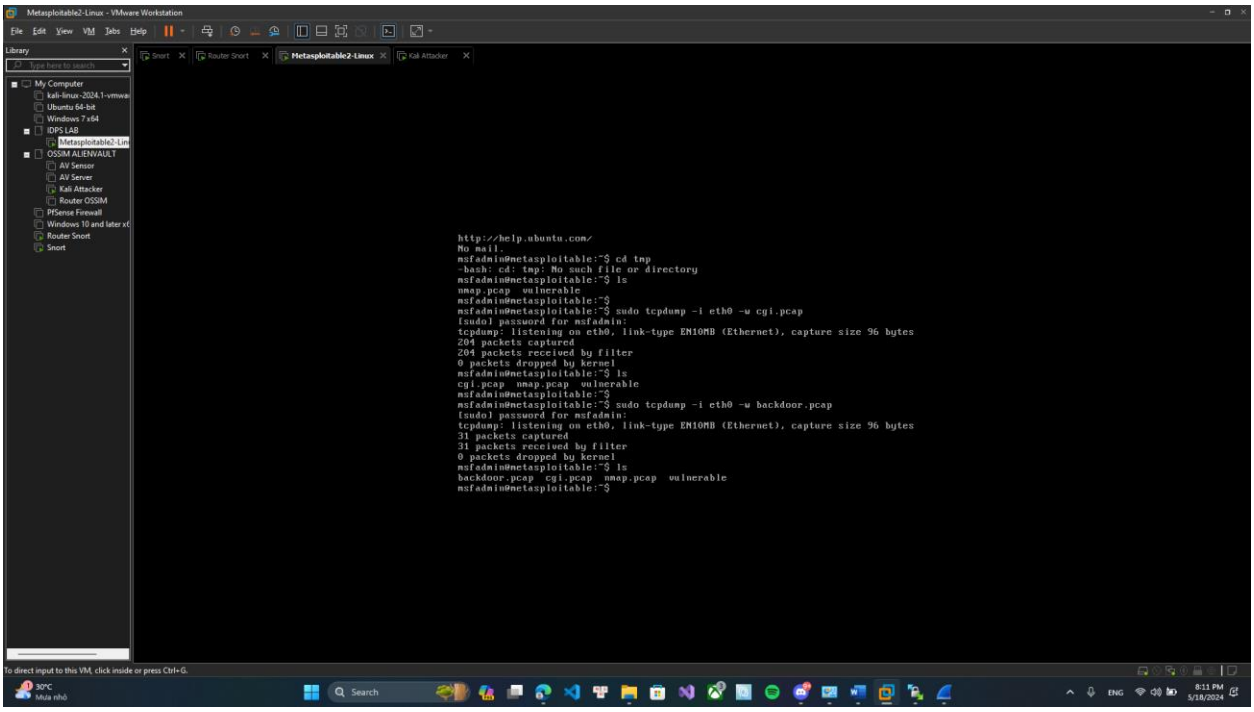
- Set up tấn công:



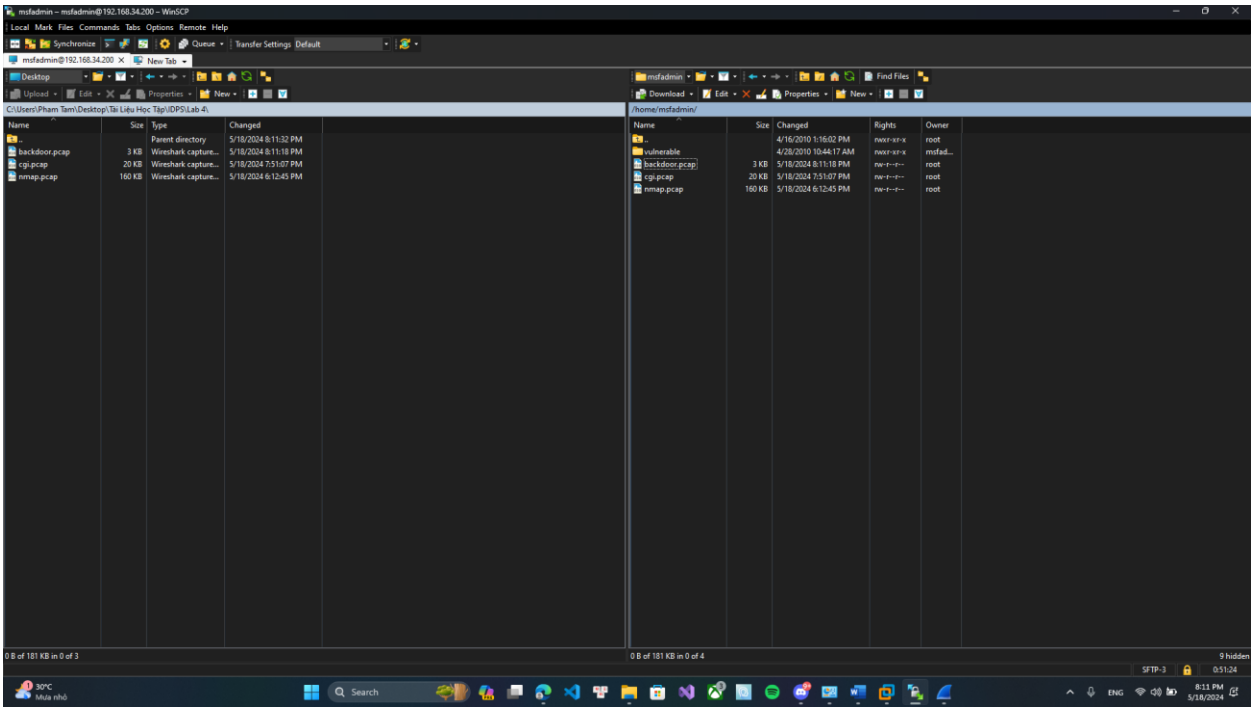
- Attack thành công:



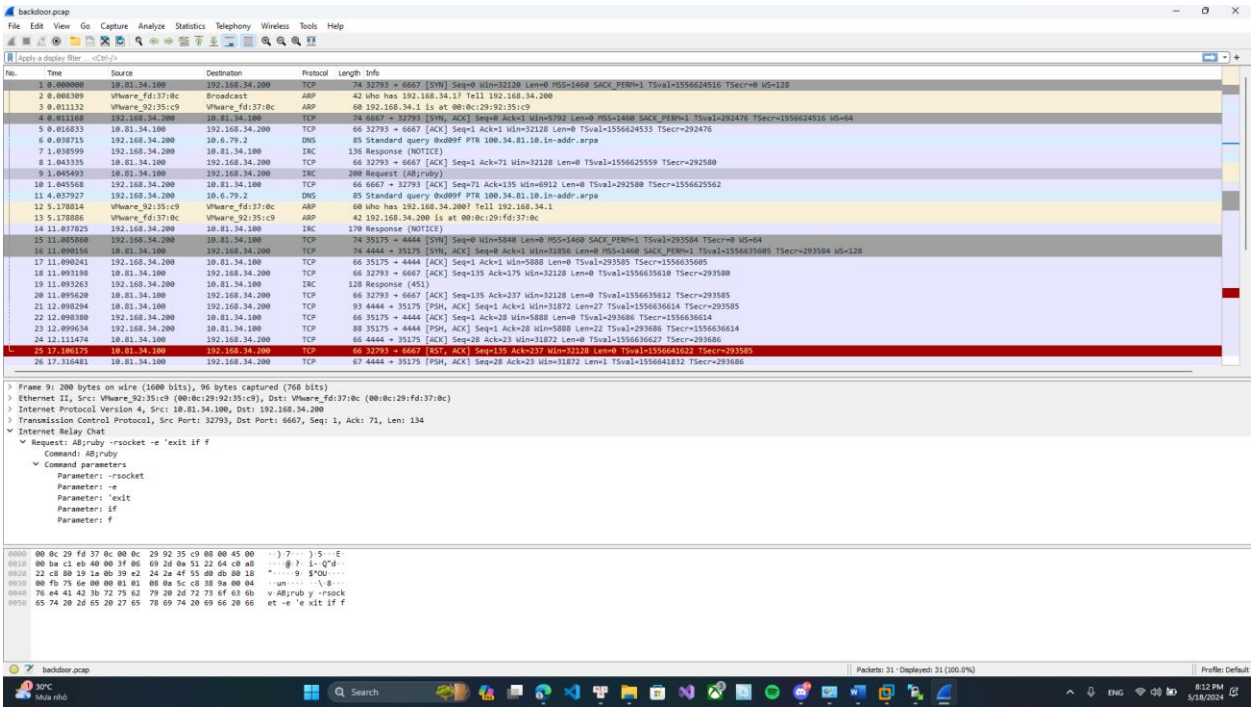
- Máy victim cũng đã bắt được pcap:



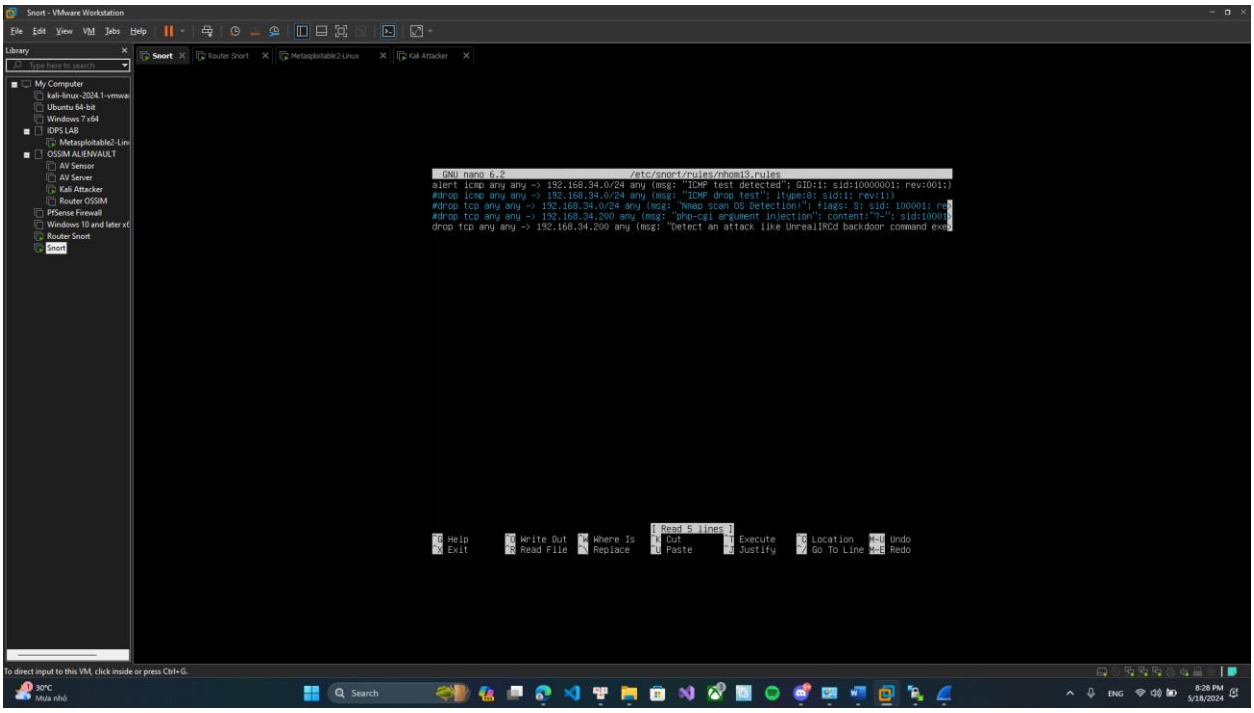
- Chuyển file pcap qua máy thật :



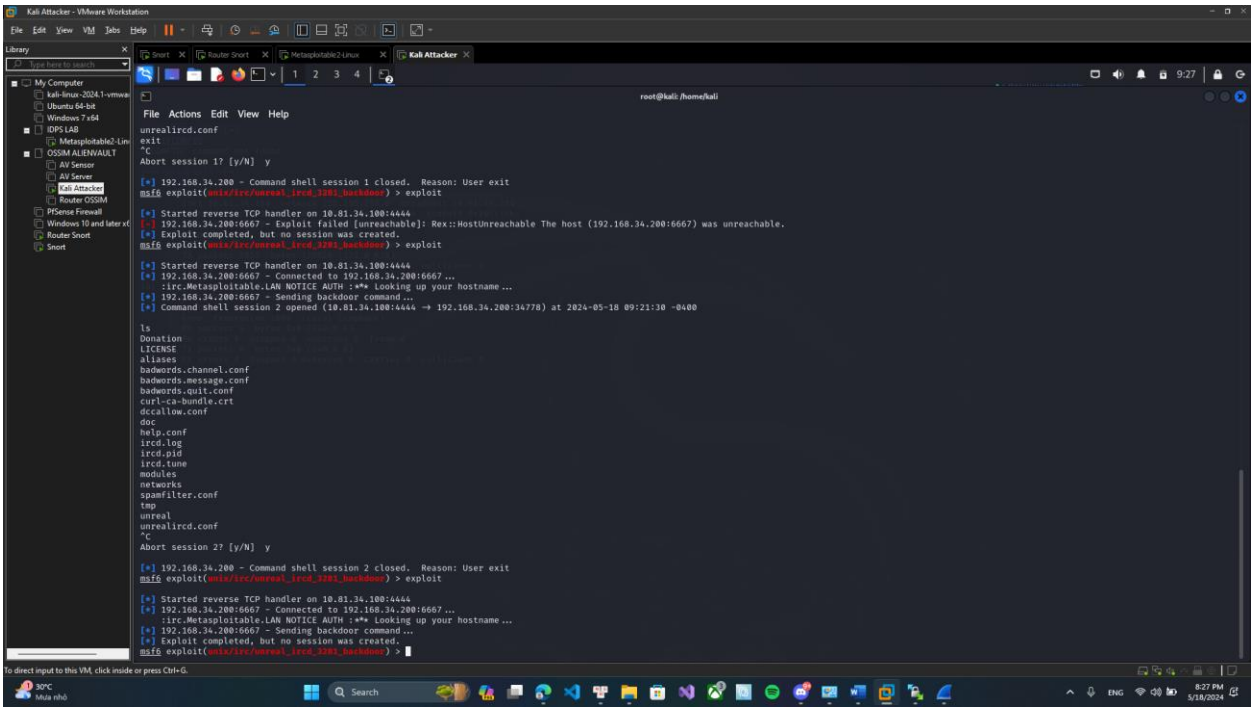
- Qua phân tích ta thấy gói tin có payload là AB, đây là dấu hiệu rõ ràng của attack UnrealIRCd, nơi kẻ tấn công sử dụng chuỗi AB để thực thi các lệnh Unix :



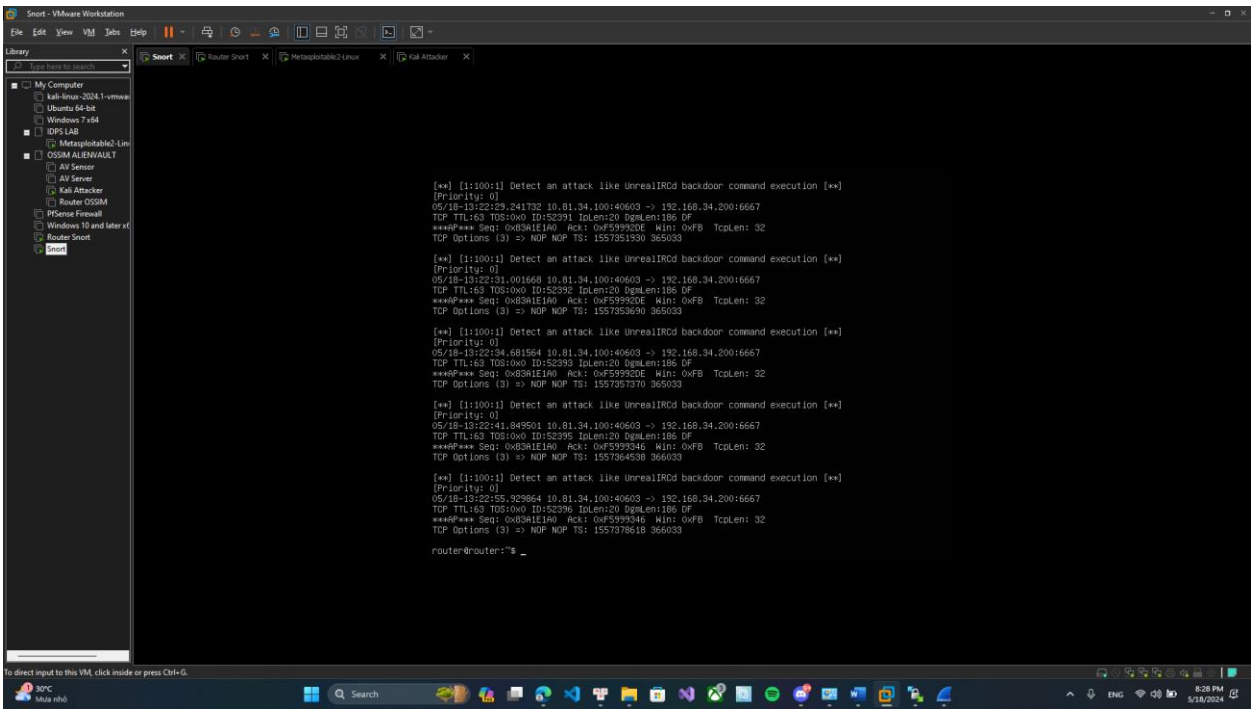
- Ta sẽ set Rule trên Snort: drop tcp any any -> $HOME_NET any (msg:"Detect an attack like UnrealIRCd backdoor command execution"; flow:to_server,established; content:"AB|3B|"; depth:3; sid:17; rev:1;)



- Tấn công đã bị chặn:


Kali Attacker - VMware Workstation
root@kali: /home/kali
File Actions Edit View Help
unrealircd.conf
exit
^C
Abort session 1? [y/N] y
[*] 192.168.34.200 - Command shell session 1 closed. Reason: User exit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 10.81.34.100:4444
[-] 192.168.34.200:6667 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.34.200:6667) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 10.81.34.100:4444
[*] 192.168.34.200:6667 - Connected to 192.168.34.200:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.34.200:6667 - Sending backdoor command ...
[*] Command shell session 2 opened (10.81.34.100:4444 -> 192.168.34.200:34778) at 2024-05-18 09:21:30 -0400
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
^C
Abort session 2? [y/N] y
[*] 192.168.34.200 - Command shell session 2 closed. Reason: User exit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 10.81.34.100:4444
[*] 192.168.34.200:6667 - Connected to 192.168.34.200:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.34.200:6667 - Sending backdoor command ...
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >

- Log ghi lại:


Snort - VMware Workstation
[**] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
[Priority: 0]
05/18-13:22:29.241732 10.81.34.100:40603 -> 192.168.34.200:6667
TCP TTL:63 TOS:0x0 ID:52391 IpLen:20 DgmLen:186 DF
AP Seq: 0x83A1E1A0 Ack: 0xF59992DE Win: 0xFB TcpLen: 32
TCP Options (3) => NOP NOP TS: 1557351930 365033
[**] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
[Priority: 0]
05/18-13:22:31.001668 10.81.34.100:40603 -> 192.168.34.200:6667
TCP TTL:63 TOS:0x0 ID:52392 IpLen:20 DgmLen:186 DF
AP Seq: 0x83A1E1A0 Ack: 0xF59992DE Win: 0xFB TcpLen: 32
TCP Options (3) => NOP NOP TS: 1557353690 365033
[**] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
[Priority: 0]
05/18-13:22:34.681564 10.81.34.100:40603 -> 192.168.34.200:6667
TCP TTL:63 TOS:0x0 ID:52393 IpLen:20 DgmLen:186 DF
AP Seq: 0x83A1E1A0 Ack: 0xF59992DE Win: 0xFB TcpLen: 32
TCP Options (3) => NOP NOP TS: 1557357370 365033
[**] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
[Priority: 0]
05/18-13:22:41.849501 10.81.34.100:40603 -> 192.168.34.200:6667
TCP TTL:63 TOS:0x0 ID:52395 IpLen:20 DgmLen:186 DF
AP Seq: 0x83A1E1A0 Ack: 0xF5999346 Win: 0xFB TcpLen: 32
TCP Options (3) => NOP NOP TS: 1557364530 366033
[**] [1:100:1] Detect an attack like UnrealIRCd backdoor command execution [**]
[Priority: 0]
05/18-13:22:55.929864 10.81.34.100:40603 -> 192.168.34.200:6667
TCP TTL:63 TOS:0x0 ID:52396 IpLen:20 DgmLen:186 DF
AP Seq: 0x83A1E1A0 Ack: 0xF5999346 Win: 0xFB TcpLen: 32
TCP Options (3) => NOP NOP TS: 1557378618 366033
router@router:~$