

## BÁO CÁO BÀI TẬP

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

**Tên chủ đề: Lab 3**

*GVHD: ThS. Đỗ Hoàng Hiên*

### **1. THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT204.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đại Nghĩa	21521182	21521182@gm.uit.edu.vn
2	Hoàng Gia Bảo	21521848	21521848@gm.uit.edu.vn

### **1. NỘI DUNG THỰC HIỆN:<sup>1</sup>**

STT	Công việc	Kết quả tự đánh giá
1	Nguyễn Đại Nghĩa	100%
2	Hoàng Gia Bảo	0%

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

---

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

## BÁO CÁO CHI TIẾT

### Yêu cầu 1.1: Giới hạn gói tin đến dịch vụ DNS

Bước đầu em kiểm tra liệu trên máy victim đã lắng nghe trên port 53 hay chưa với câu lệnh “sudo netstat -tuln | grep ':53'”:

```
msfadmin@metasploit> sudo netstat -tuln | grep ':53'
```

Protocol	Local Address	Local Port	State
tcp	0.0.0.0	53760	LISTEN
tcp	192.168.82.200	53	LISTEN
udp	192.168.82.200	53	

Kết quả trên cho thấy rằng máy đang lắng nghe trên port 53 nhưng chỉ lắng nghe mỗi giao thức tcp.

Tiếp đến em sẽ sử dụng hping3 để gửi gói TCP SYN đến cổng 53 của máy victim với mức độ là 91 gói tin trong 10 giây thông qua câu lệnh “sudo hping3 -S -p 53 -i u109890 192.168.82.200”, kết quả nhận được như sau:

```

File Actions Edit View Help
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=50 win=5840 rtt=9.8 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=51 win=5840 rtt=9.6 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=52 win=5840 rtt=5.0 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=53 win=5840 rtt=6.4 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=54 win=5840 rtt=11.5 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=55 win=5840 rtt=11.6 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=56 win=5840 rtt=13.3 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=57 win=5840 rtt=7.9 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=58 win=5840 rtt=12.0 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=59 win=5840 rtt=6.4 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=60 win=5840 rtt=12.5 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=61 win=5840 rtt=4.3 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=62 win=5840 rtt=4.1 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=63 win=5840 rtt=4.1 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=64 win=5840 rtt=9.0 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=65 win=5840 rtt=5.7 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=66 win=5840 rtt=5.7 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=67 win=5840 rtt=10.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=68 win=5840 rtt=8.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=69 win=5840 rtt=13.0 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=70 win=5840 rtt=7.1 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=71 win=5840 rtt=4.1 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=72 win=5840 rtt=8.9 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=73 win=5840 rtt=8.9 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=74 win=5840 rtt=7.5 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=75 win=5840 rtt=4.3 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=76 win=5840 rtt=10.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=77 win=5840 rtt=8.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=78 win=5840 rtt=12.1 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=79 win=5840 rtt=4.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=80 win=5840 rtt=4.4 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=81 win=5840 rtt=4.4 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=82 win=5840 rtt=5.8 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=83 win=5840 rtt=10.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=84 win=5840 rtt=8.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=85 win=5840 rtt=12.1 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=86 win=5840 rtt=4.4 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=87 win=5840 rtt=4.4 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=88 win=5840 rtt=12.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=89 win=5840 rtt=4.4 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=90 win=5840 rtt=8.2 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=91 win=5840 rtt=8.0 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=92 win=5840 rtt=8.0 ms
len46 ip-192.168.82.200 ttl=63 DF id=0 sport=53 flags=SA seq=93 win=5840 rtt=12.4 ms
^C
- 192.168.82.200 hping statistic --
95 packets transmitted, 94 packets received, 2% packet loss
round-trip min/avg/max = 1.6/8.4/16.1 ms
[nghianguyen@kali]~$

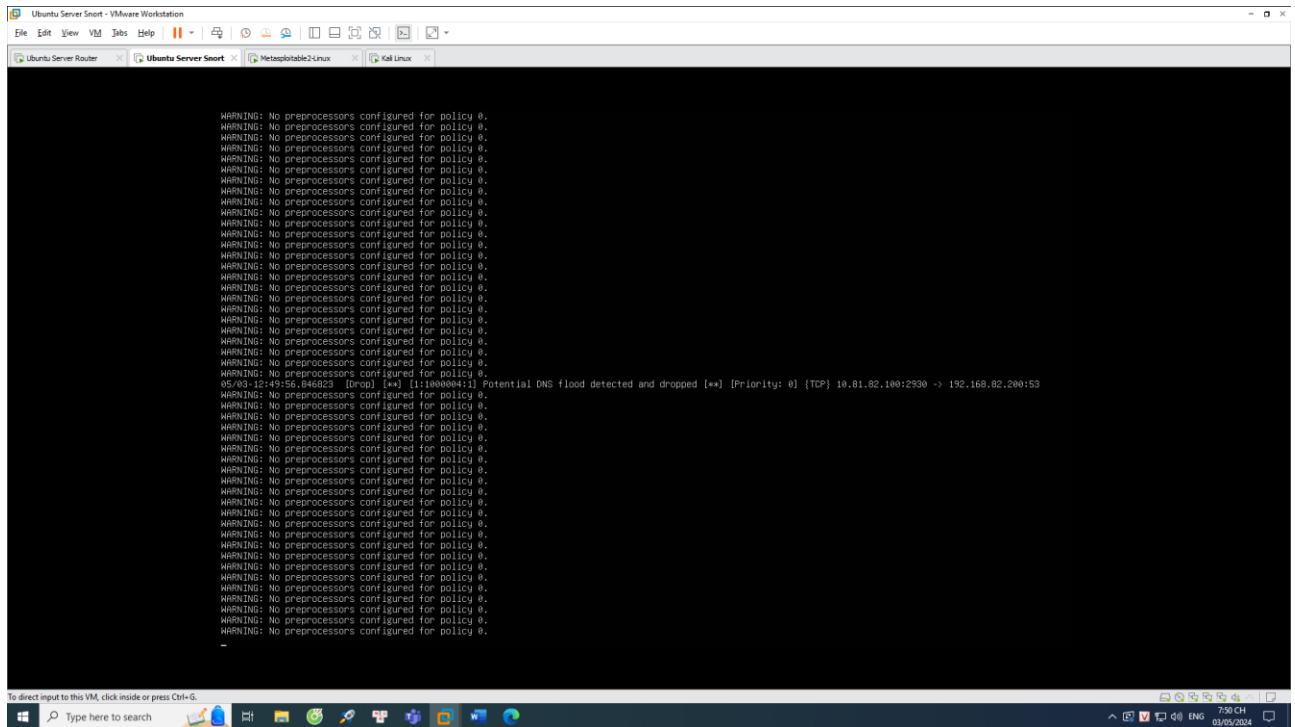
```

Từ hình ảnh trên thấy được rằng trước khi có rule thì em có thể gửi được hơn 90 gói tin trong vòng 10 giây.

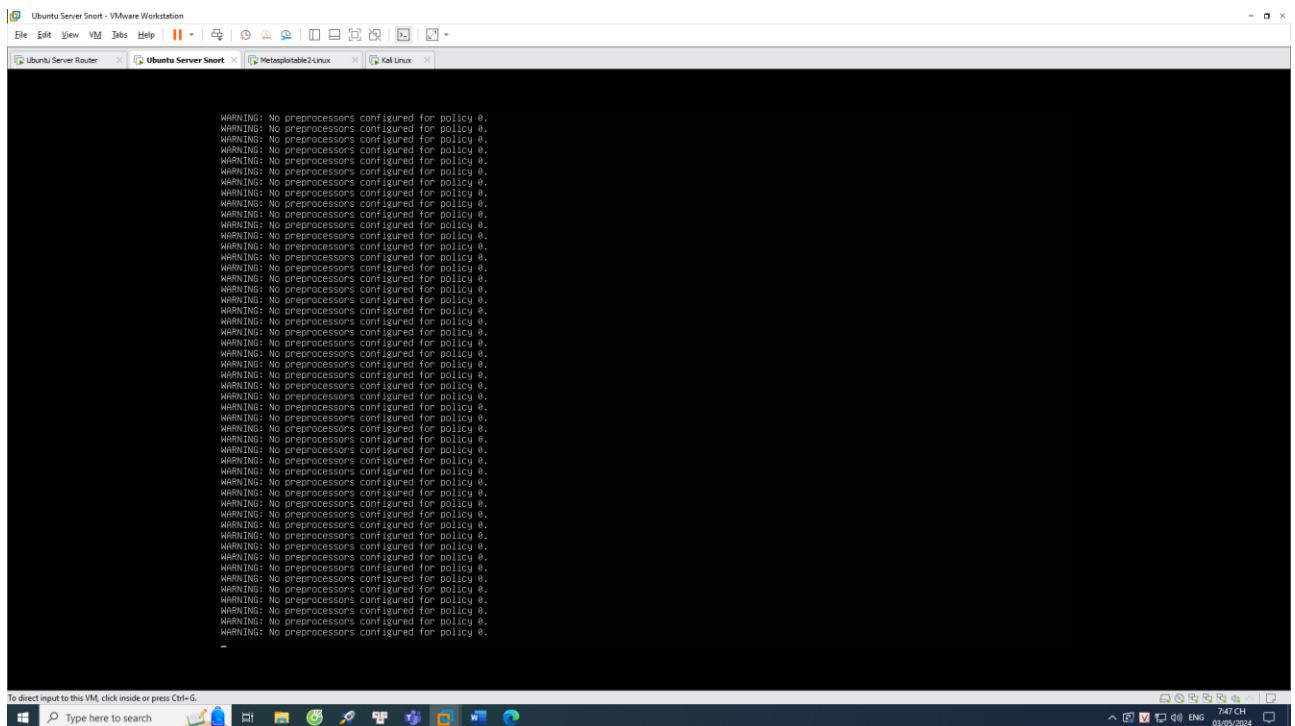
Bây giờ em sẽ bắt đầu áp dụng rule “drop udp any any -> 192.168.82.200 53 (msg:"Potential DNS flood detected and dropped"; threshold:type both, track by\_dst, count 90, seconds 10; sid:1000003; rev:001;) cho việc giới hạn gói udp đến dịch vụ DNS đến máy Victim.

Và “drop tcp any any -> 192.168.82.200 53 (msg:"Potential DNS flood detected and dropped"; threshold:type both, track by\_dst, count 90, seconds 10; sid:1000004; rev:001;) cho việc giới hạn gói tcp đến dịch vụ DNS đến máy Victim.

Em sẽ thực hiện kiểm tra rule trên bằng cách gửi đến victim 95 gói trong vòng 10 giây, sau một lúc chạy khoảng 10 giây thì trên màn hình snort có thông báo như sau:



Còn với việc em thử gửi 50 gói trong vòng 10 giây, thì em đã đợi khoảng gần 2 phút nhưng vẫn không có thông báo drop:



## Yêu cầu 1.2: Chỉ cho phép truy cập đến một số dịch vụ

Trước hết thì em xác định các dịch vụ trong đề bài tương ứng với các port như sau:

Telnet: 23

FTP: 21

SSH: 22

Web (HTTP): 80

Web (HTTPS): 443

Mail (SMTP): 25

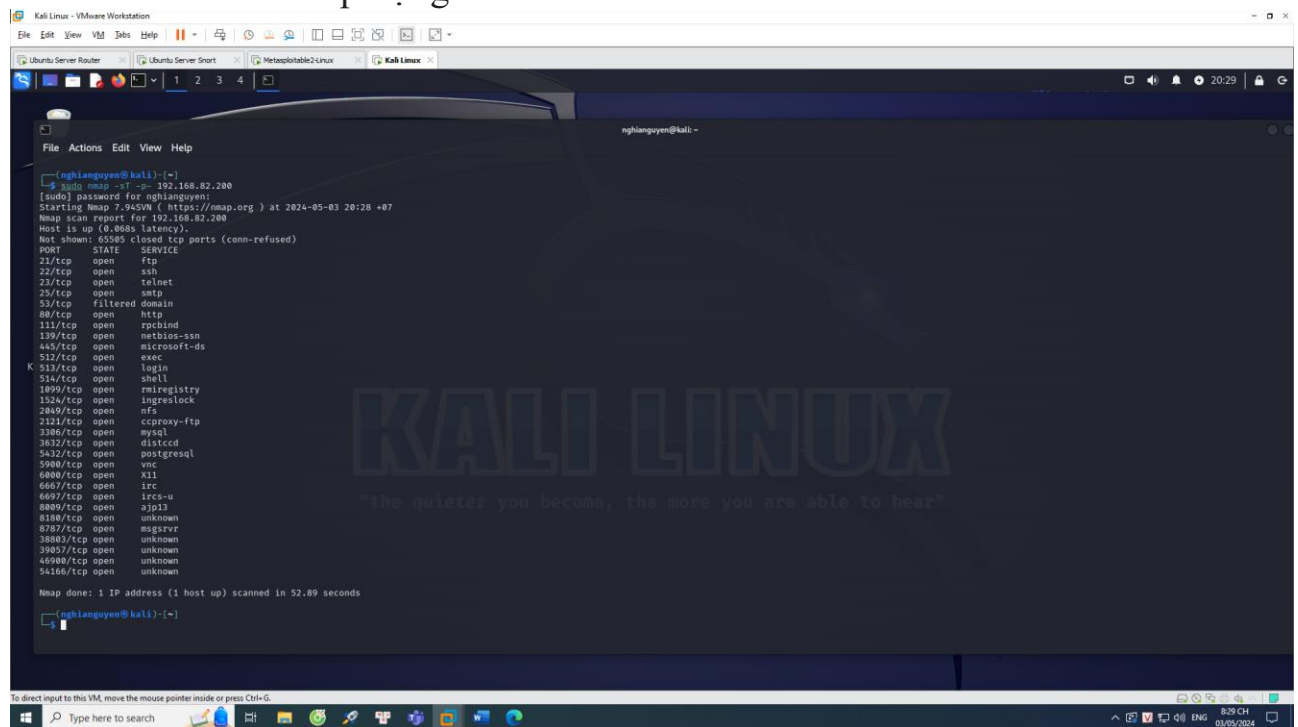
NetBIOS: 139

SMB: 445

MySQL: 3306

PostgreSQL: 5432

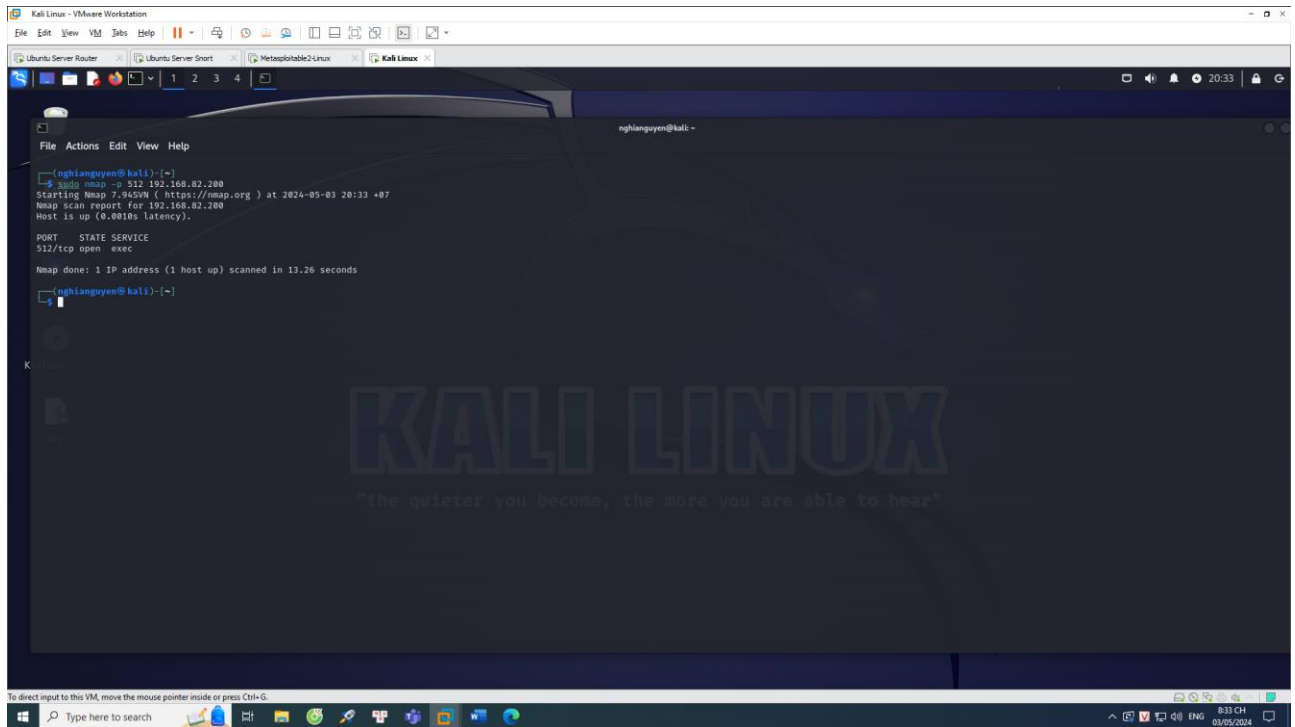
Em sẽ xem thử những port nào mà victim đang lắng nghe mà khác với các port trên để test thử trước khi áp dụng rule:



```
nghianguyen@kali:~$ sudo nmap -sT -p- 192.168.82.200
[sudo] password for nghianguyen:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 20:28 +07
Nmap scan report for 192.168.82.200
Host is up (0.000s latency).
Not shown: 65585 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    filtered domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1399/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8080/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38883/tcp open  unknown
39857/tcp open  unknown
46900/tcp open  unknown
54166/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 52.89 seconds
nghianguyen@kali:~$
```

Phía trên là các port đang lắng nghe của victim, em sẽ chọn port 512 để test bằng công cụ nmap:

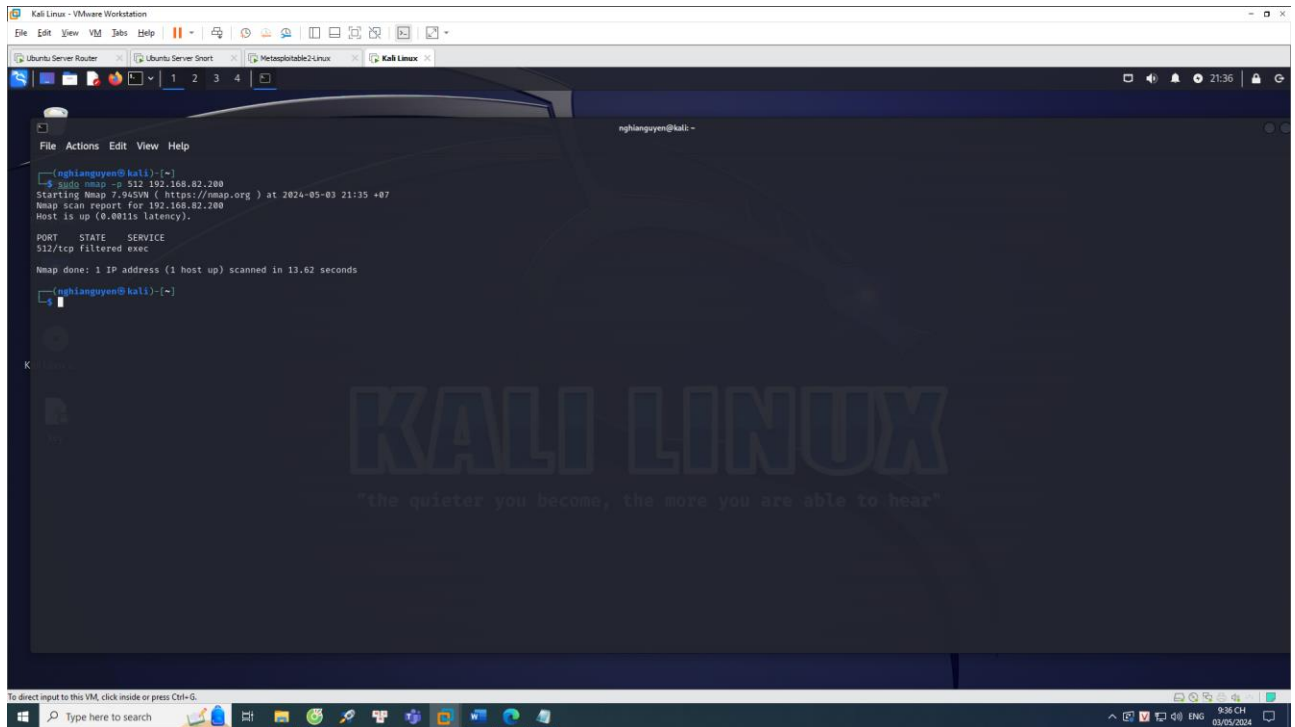


Vậy thì trước khi áp dụng rule, em có thể scan tới port 512 của victim.

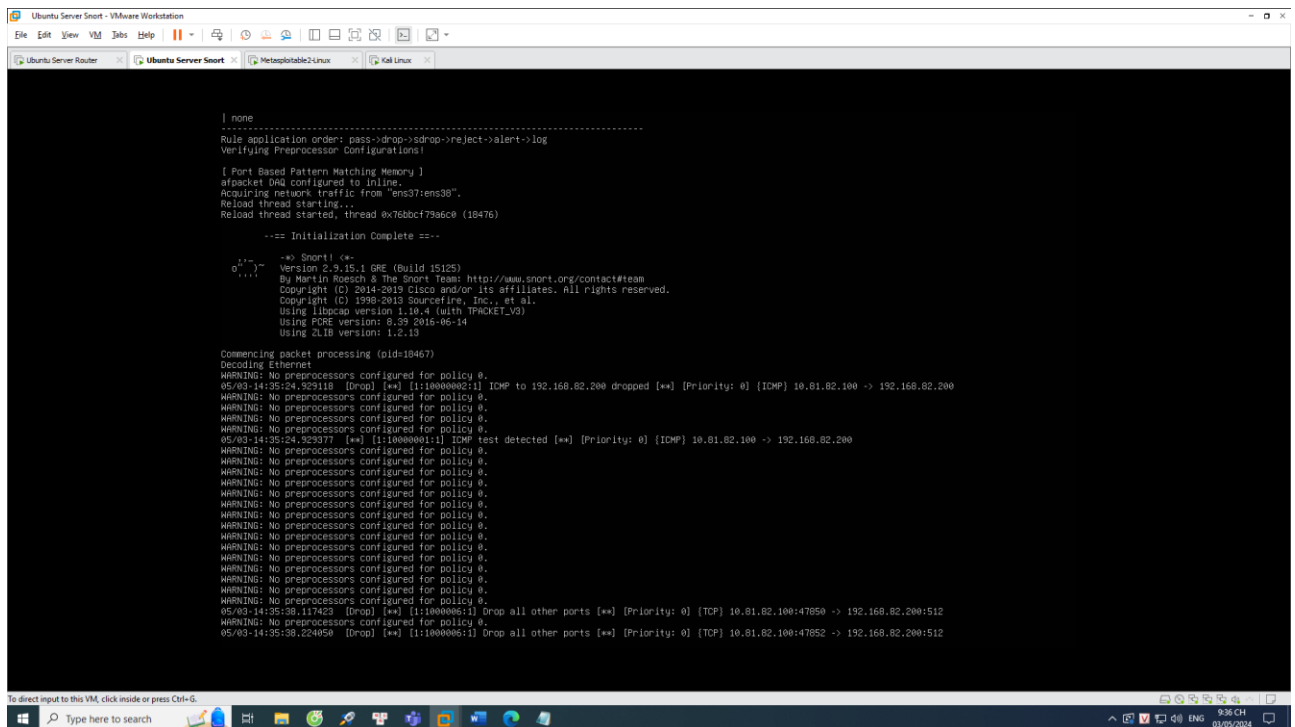
Bây giờ em sẽ tiến hành viết rule như sau: “pass tcp any any -> 192.168.82.200 \$ALLOWED\_PORTS (msg:" Allow specified ports"; sid:1000005; rev:001;)”. Tiếp đến là rule: “drop tcp any any -> 192.168.82.200 any (msg:"Drop all other ports"; sid:1000006; rev:001;)”.

Với ALLOWED\_PORTS là biến mà em định nghĩa trong file “/etc/snort/nhom7-snort.conf”, với nội dung là “portvar ALLOWED\_PORTS [21,22,23,25,80,139,443,445,3306,5432]”.

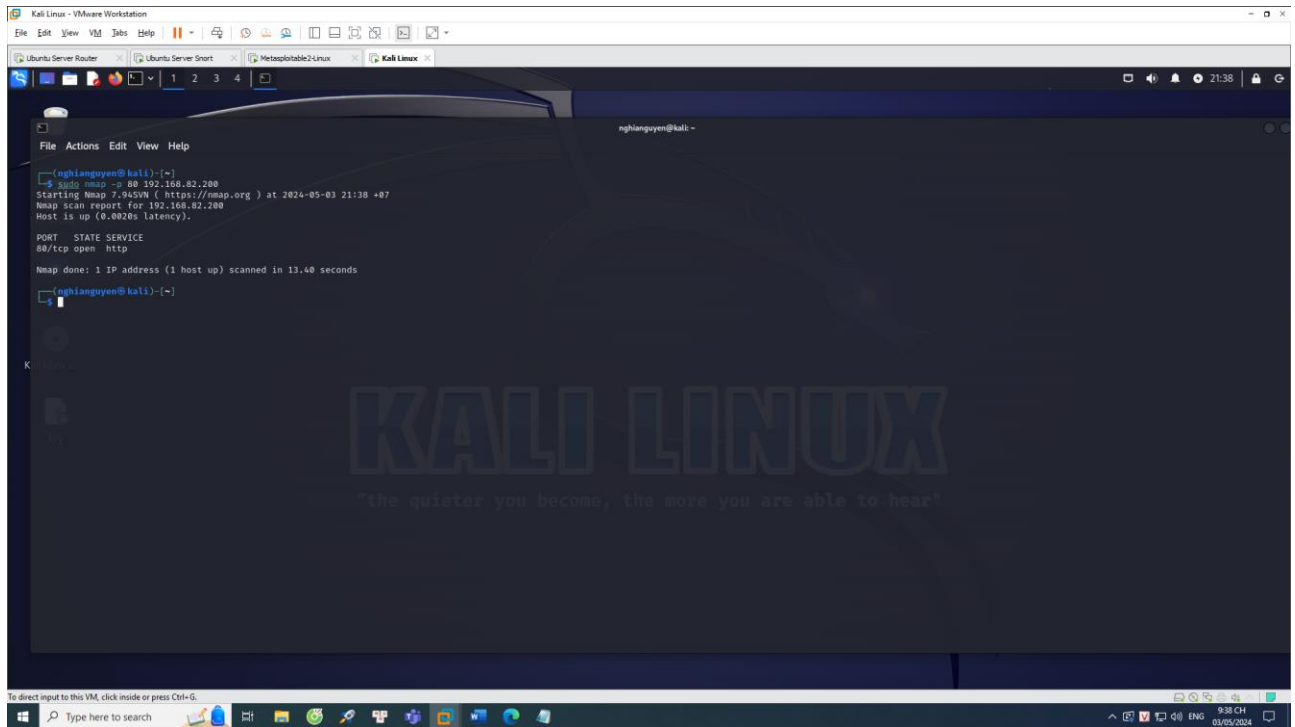
Sau khi áp dụng rule thì em sẽ thử test lại với port 512 vừa này, kết quả nhận được:



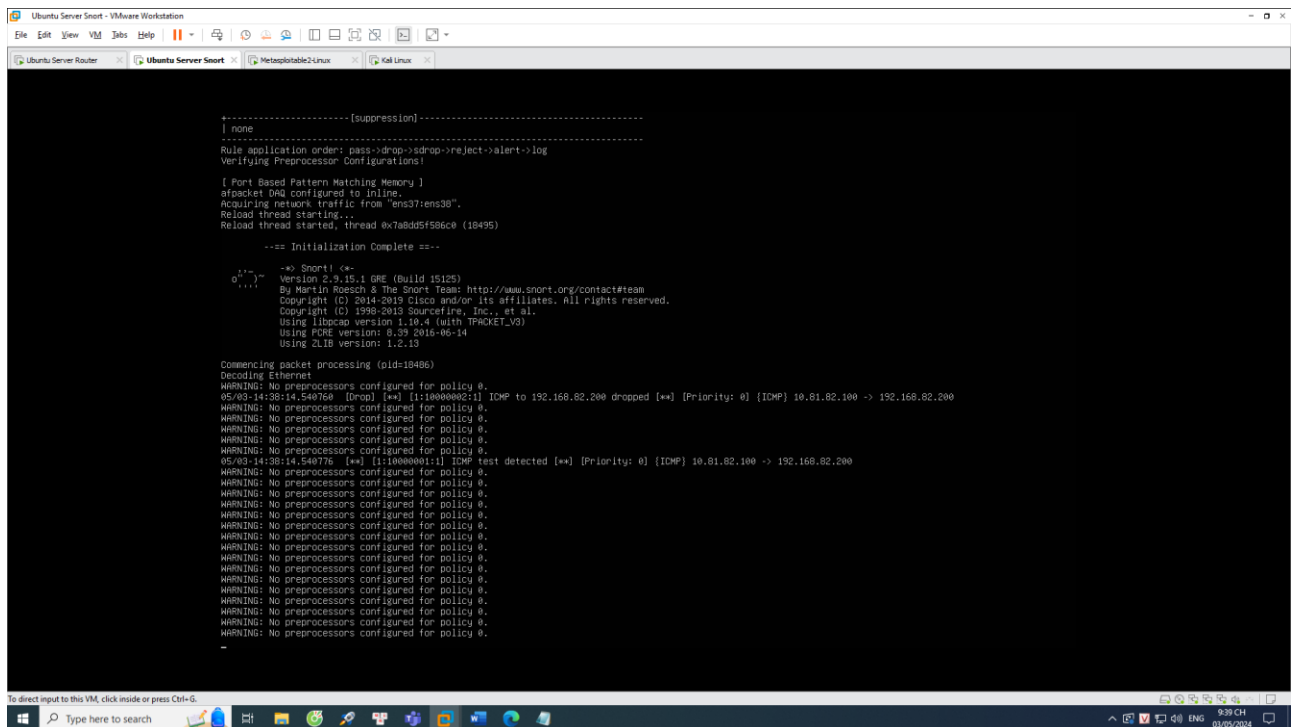
Thông báo trên terminal snort:



Bây giờ em sẽ test thử trên port được cho phép là port 80:



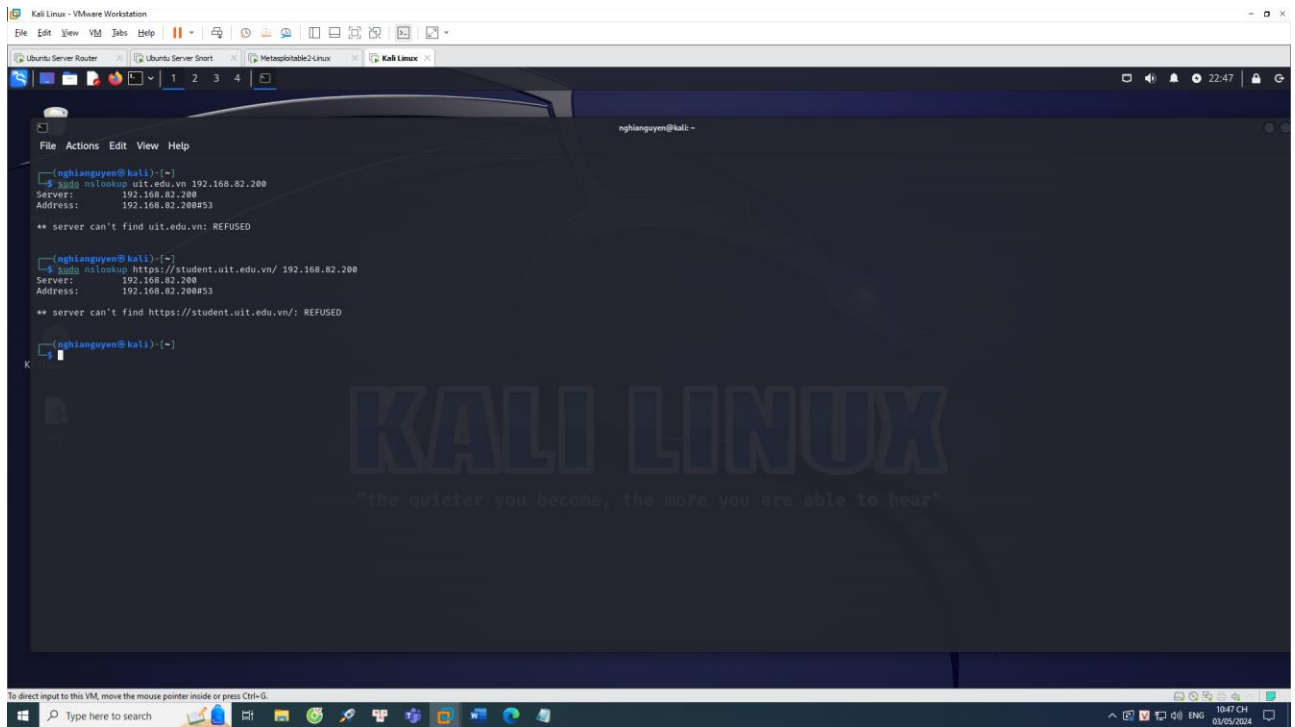
Kết quả là vẫn quét được, còn terminal của snort thì không báo lỗi:





## Yêu cầu 1.3: Chỉ cho phép các truy vấn DNS đến các tên miền thuộc quản lý của UIT

Trước khi viết rule thì em sẽ thử nslookup đến uit.edu.vn:



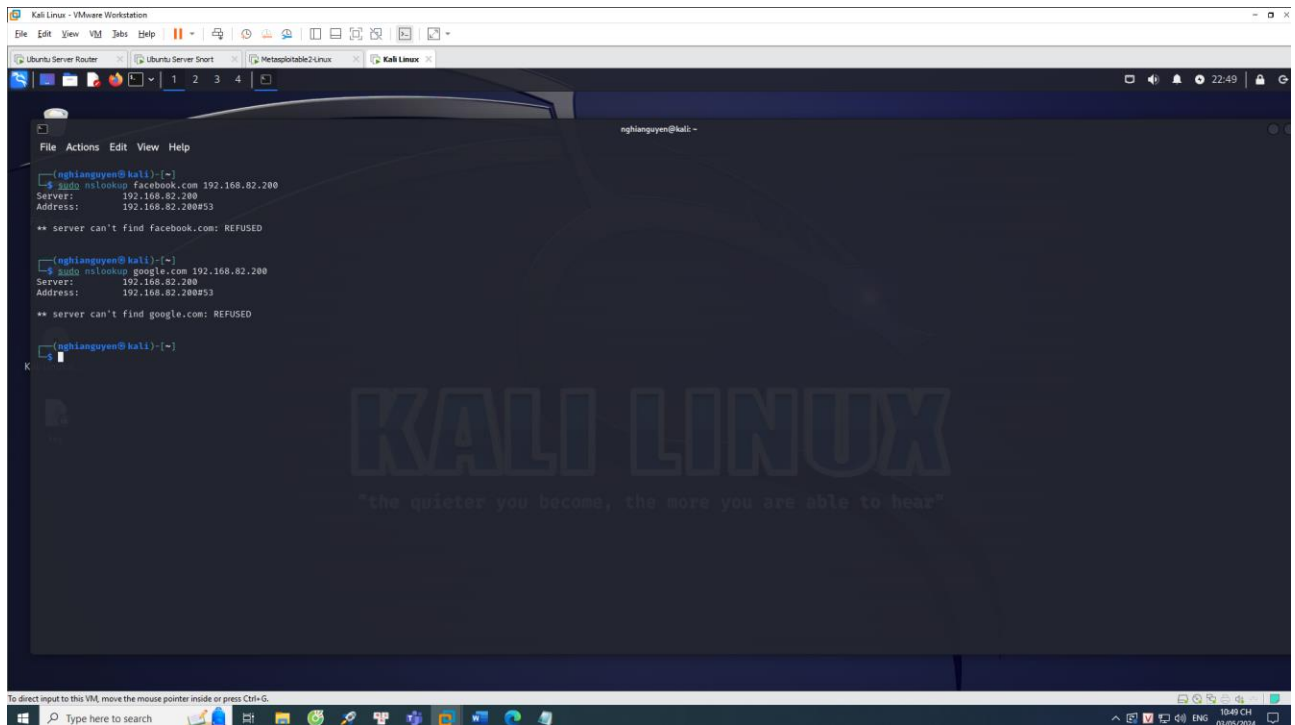
```
(nghianguyen@kali):~$ nslookup uit.edu.vn 192.168.82.200
Server:      192.168.82.200
Address:     192.168.82.200#53
** server can't find uit.edu.vn: REFUSED

(nghianguyen@kali):~$ nslookup https://student.uit.edu.vn/ 192.168.82.200
Server:      192.168.82.200
Address:     192.168.82.200#53
** server can't find https://student.uit.edu.vn/: REFUSED

(nghianguyen@kali):~$
```

Mặc dù là không trả về kết quả, nhưng mà nhìn chung thì vẫn đã gửi được yêu cầu DNS tới máy victim.

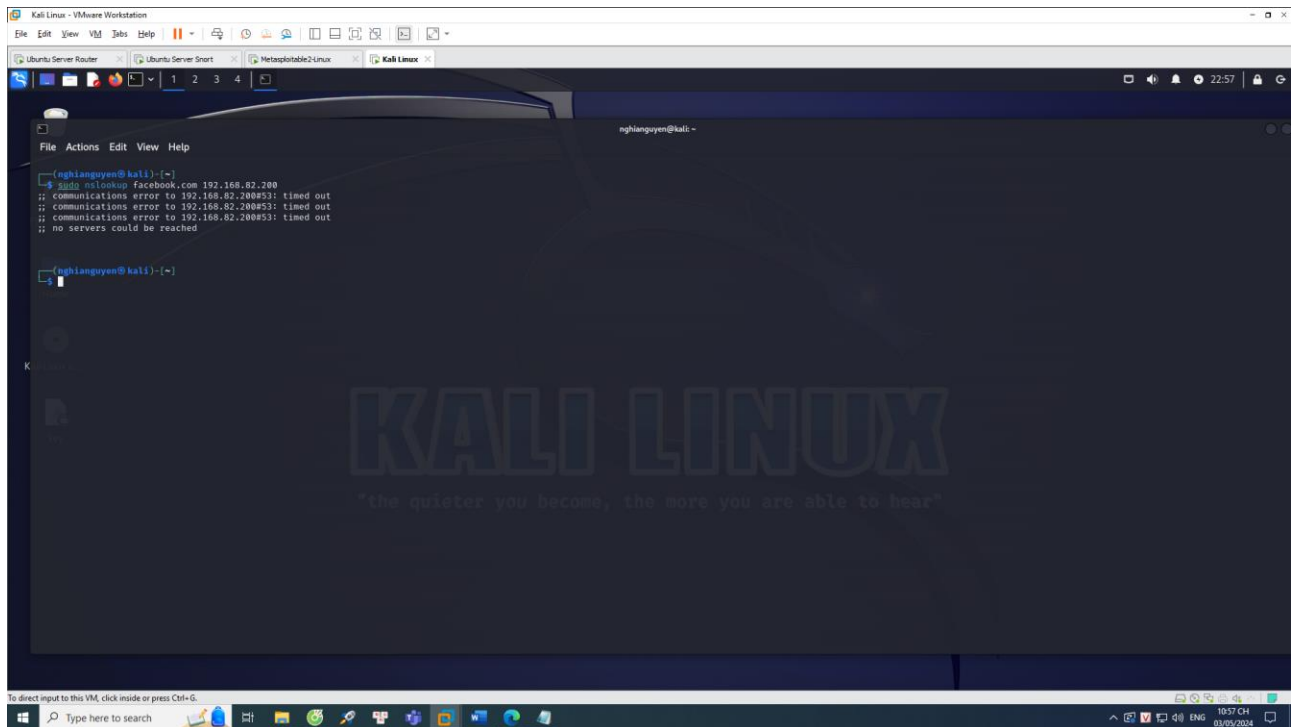
Nslookup đến các tên miền không phải quản lý của uit:



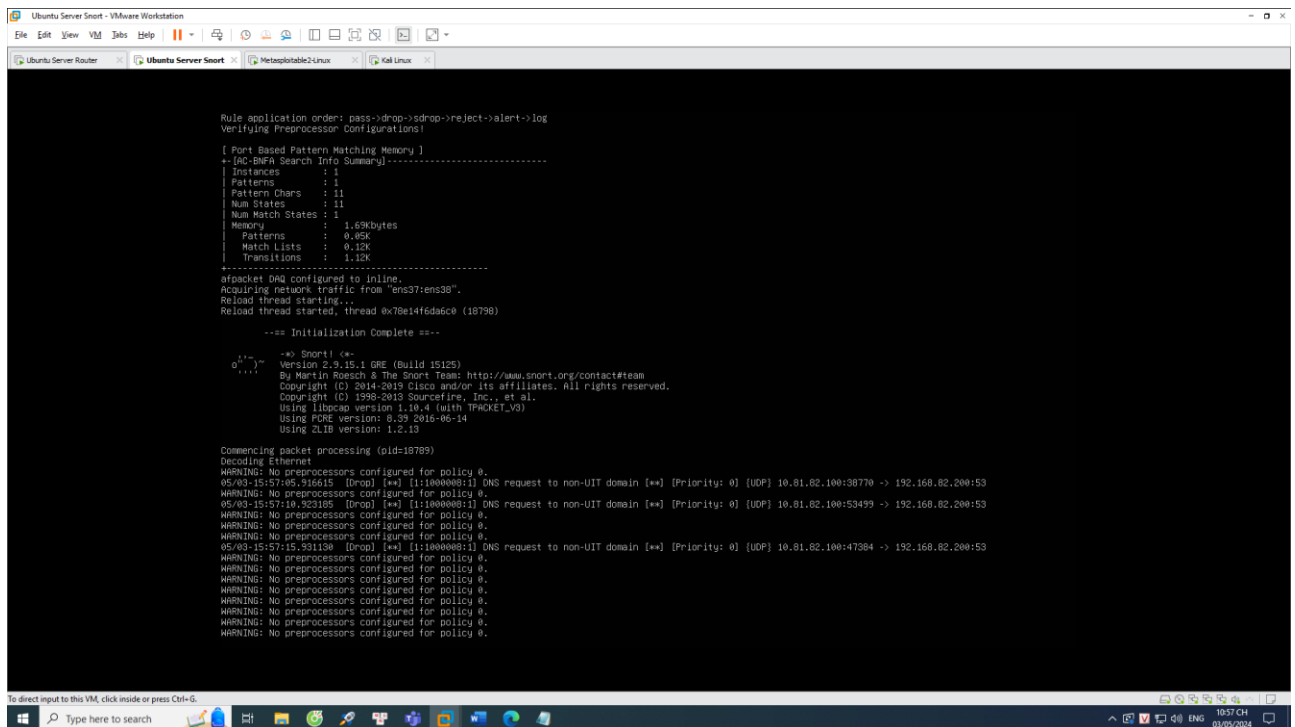
Kết quả là vẫn gửi yêu cầu được.

Bây giờ em sẽ tiến hành viết rule như sau: “pass udp any any -> 192.168.82.200 53 (msg:"UIT domain"; content:"|01 00 00 01 00 00 00 00 00|"; pcre:"/[^.]\*uit.edu.vn/"; sid:1000007; rev:001;)”. Và thêm 1 rule chặn các gói tin gửi tới port 53: “drop udp any any -> 192.168.82.200 53 (msg:" Blocked DNS request to non-UIT domain"; sid:1000008; rev:001;)”.

Sau khi áp dụng rule vào thì em tiến hành nslookup tới các tên miền không phải quản lí của uit:



Kết quả trên terminal của snort:



Khi sử dụng tên miền của uit:

