

BÁO CÁO THỰC HÀNH

Môn học: Hệ thống nhúng mạng không dây

Buổi báo cáo: Lab 3

Tên chủ đề: Introduction Netfilter and Iptables

GVHD: Nguyễn Văn Bảo

Ngày thực hiện: xx/xx/2024

THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT131.021.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Đình Luân	21521105	21521105@gm.uit.edu.vn

1. ĐÁNH GIÁ KHÁC:

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	3 ngày
Link Video thực hiện (nếu có)	
Ý kiến (nếu có) + Khó khăn + Đề xuất ...	
Điểm tự đánh giá	8

BÁO CÁO CHI TIẾT

1. Sửa lại file nkmod.c để hook chỉ DROP các gói tin UDP.

Địa chỉ máy ubuntu là 192.168.110.132

```
static struct nf_hook_ops *nf_hook_ex_ops = NULL;

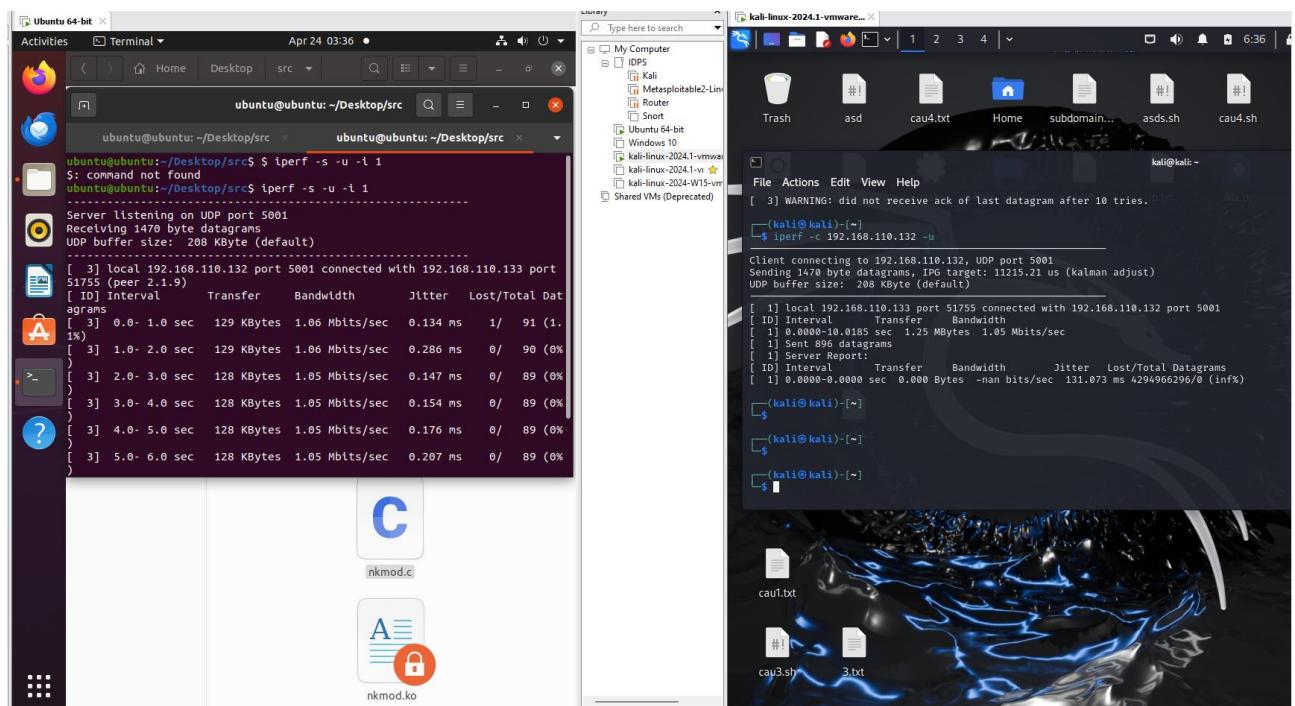
static unsigned int nf_hook_ex(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    struct iphdr *iph;
    if(!skb)
        return NF_ACCEPT;
    iph = ip_hdr(skb);
    if (iph->protocol == 17) {
        printk(KERN_INFO "Dropped received packet \n");
        return NF_DROP;
    }
    return NF_ACCEPT;
}
```

Sửa giá trị iph->protocol thành 17 (UDP)

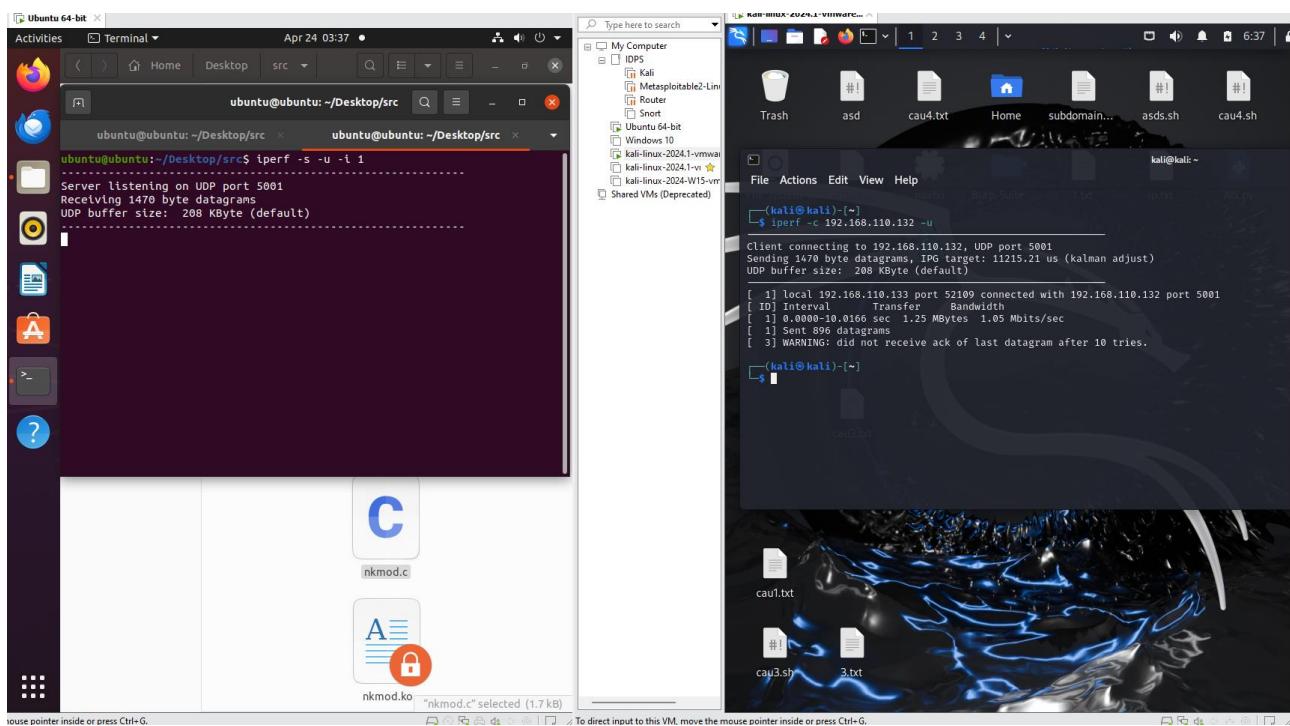
Trên máy Ubuntu khởi động UDP server bằng lệnh \$ iperf -s -u -i 1

Máy còn lại bắt đầu UDP client để kết nối tới máy Ubuntu, sử dụng lệnh \$ iperf -c 192.168.110.132 -u

Trước khi sử dụng module, ta có thể kết nối bình thường đến máy ubuntu



Sau khi sử dụng module, ta không còn kết nối được với máy ubuntu:



Xem file log:

```
ubuntu@ubuntu:~/Desktop/src$ dmesg | tail
[ 933.797378] Dropped received packet
[ 933.809361] Dropped received packet
[ 945.698564] Dropped received packet
[ 945.698573] Dropped received packet
[ 950.704055] Dropped received packet
[ 950.704061] Dropped received packet
[ 955.709180] Dropped received packet
[ 955.709185] Dropped received packet
[ 960.713579] Dropped received packet
[ 960.713591] Dropped received packet
ubuntu@ubuntu:~/Desktop/src$
```

2. DROP các packet có source IP đến từ địa chỉ máy client, chặng hạn như 192.168.20.22, ACCEPT tất cả các packet còn lại.

Địa chỉ máy client: 192.168.110.133

Ta sửa code:

```

static struct nf_hook_ops *nf_hook_ex_ops = NULL;

static unsigned int nf_hook_ex(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    struct iphdr *iph;
    if(!skb)
        return NF_ACCEPT;

    char sipaddr[16];
    char target[16] = "192.168.110.133";
    iph = ip_hdr(skb);
    snprintf(sipaddr, 16, "%pI4", &iph->saddr);

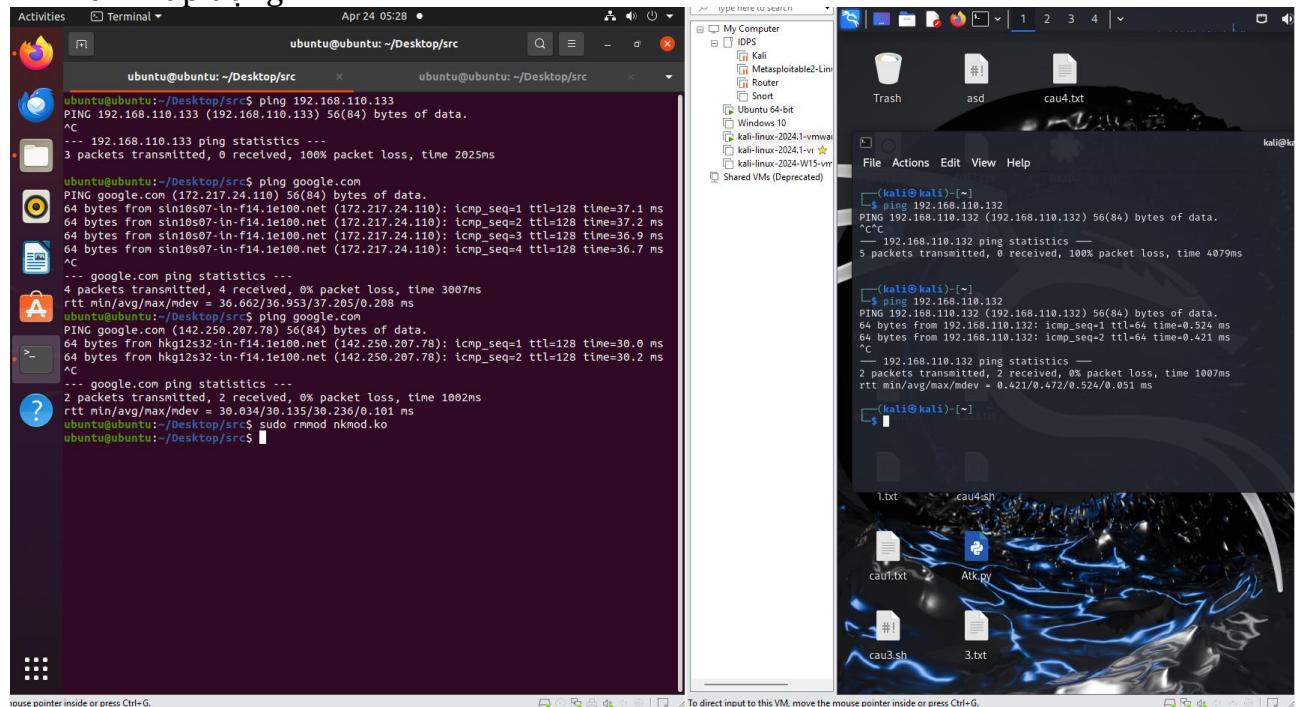
    if (memcmp(&sipaddr, &target, sizeof(sipaddr))) {
        return NF_ACCEPT;
    }
    printk(KERN_INFO "Dropped packet from 192.168.110.133 \n");
    return NF_DROP;
}

```

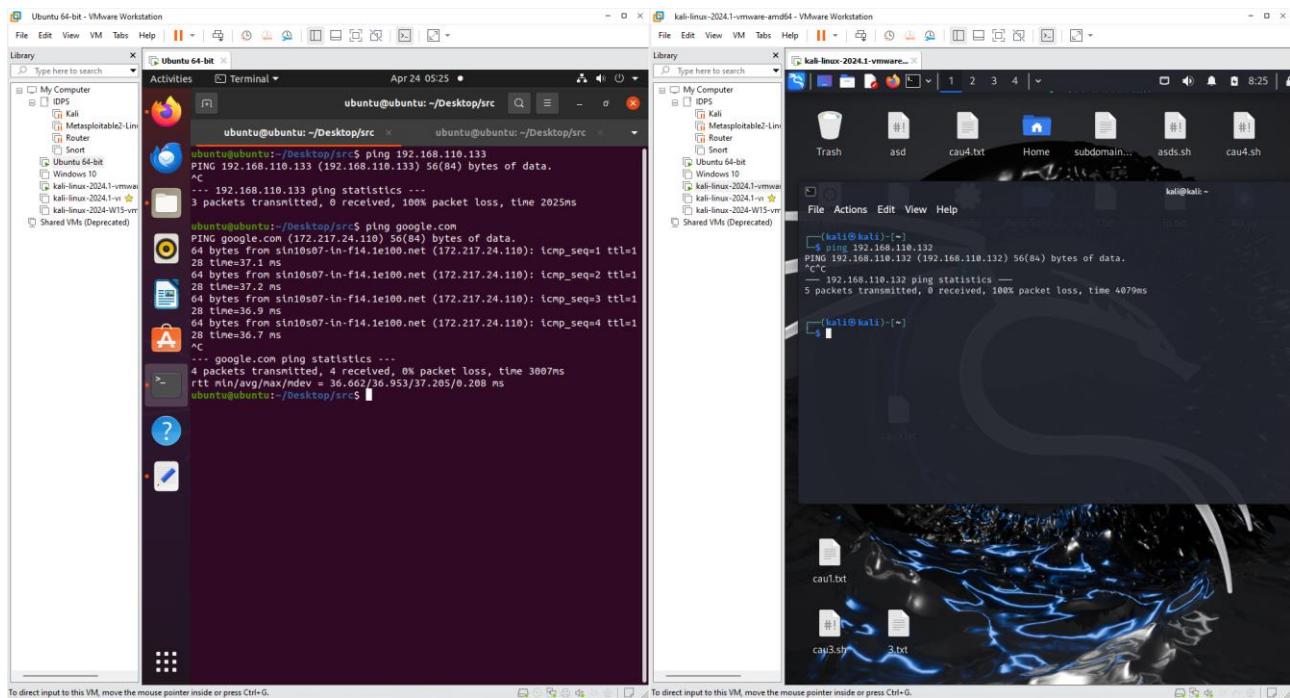
Kiểm tra:

Trước khi áp dụng thì máy kali vẫn ping được tới máy ubuntu nhưng sau khi áp dụng thì máy kali không ping được tới máy ubuntu

Trước khi áp dụng:



Sau khi áp dụng:



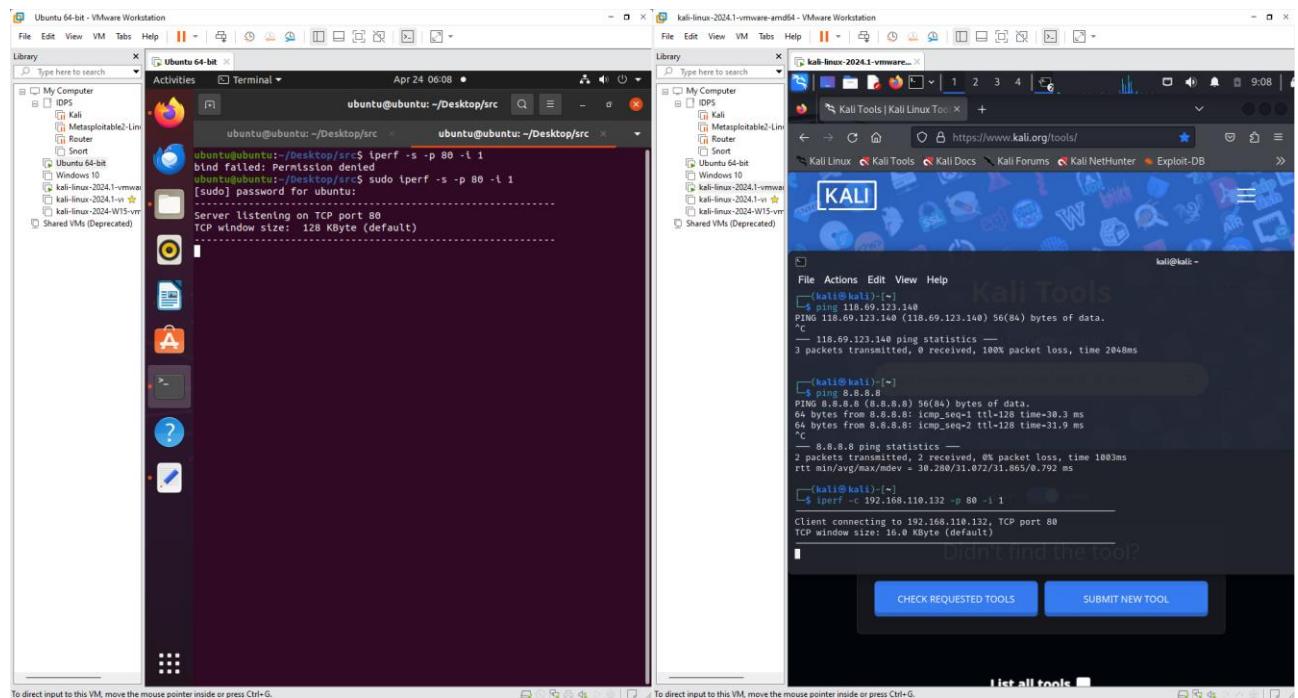
```
ubuntu@ubuntu:~/Desktop/src$ dmesg | tail
[ 7561.925410] Dropped packet from 192.168.110.133
[ 7561.935489] Dropped packet from 192.168.110.133
[ 7561.935616] Dropped packet from 192.168.110.133
[ 7561.953706] Dropped packet from 192.168.110.133
[ 7561.953736] Dropped packet from 192.168.110.133
[ 7561.953845] Dropped packet from 192.168.110.133
[ 7561.955819] Dropped packet from 192.168.110.133
[ 7561.957619] Dropped packet from 192.168.110.133
[ 7561.980404] Dropped packet from 192.168.110.133
[ 7562.009393] Dropped packet from 192.168.110.133
ubuntu@ubuntu:~/Desktop/src$
```

3. DROP các gói tin TCP và UDP đi đến với địa chỉ port đích là 80.

```
static unsigned int nf_hook_ex(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    struct iphdr *iph;
    struct tcphdr *tcp;
    struct udphdr *udp;
    if(!skb)
        return NF_ACCEPT;
    iph = ip_hdr(skb);
    tcp = tcp_hdr(skb);
    udp = udp_hdr(skb);
    if(iph->protocol == 6){
        int dest_porttcp = (unsigned int) ntohs(tcp->dest);
        if(dest_porttcp == 80){
            printk(KERN_INFO "Dropped a TCP packet \n");
            return NF_DROP;
        }
    }
    if(iph->protocol == 17){
        int dest_portudp = (unsigned int) ntohs(udp->dest);
        if(dest_portudp == 80){
            printk(KERN_INFO "Dropped a UDP packet \n");
            return NF_DROP;
        }
    }
    return NF_ACCEPT;
}
```

Kiểm tra:

- + Máy ubuntu: iperf -s -p 80 -i 1
- + Máy client: iperf -c 192.168.110.132 -p 80 -i 1



```
ubuntu@ubuntu:~/Desktop/src$ dmesg | tail
[ 9901.202234] Dropped a TCP packet
[ 9902.226290] Dropped a TCP packet
[ 9903.249535] Dropped a TCP packet
[ 9904.274173] Dropped a TCP packet
[ 9905.296661] Dropped a TCP packet
[ 9906.320109] Dropped a TCP packet
[ 9908.338327] Dropped a TCP packet
[ 9912.496747] Dropped a TCP packet
[ 9920.691366] Dropped a TCP packet
[ 9936.816584] Dropped a TCP packet
ubuntu@ubuntu:~/Desktop/src$ dmesg | tail
[ 9902.226290] Dropped a TCP packet
[ 9903.249535] Dropped a TCP packet
[ 9904.274173] Dropped a TCP packet
[ 9905.296661] Dropped a TCP packet
[ 9906.320109] Dropped a TCP packet
[ 9908.338327] Dropped a TCP packet
[ 9912.496747] Dropped a TCP packet
[ 9920.691366] Dropped a TCP packet
[ 9936.816584] Dropped a TCP packet
[ 9970.609159] Dropped a TCP packet
ubuntu@ubuntu:~/Desktop/src$
```

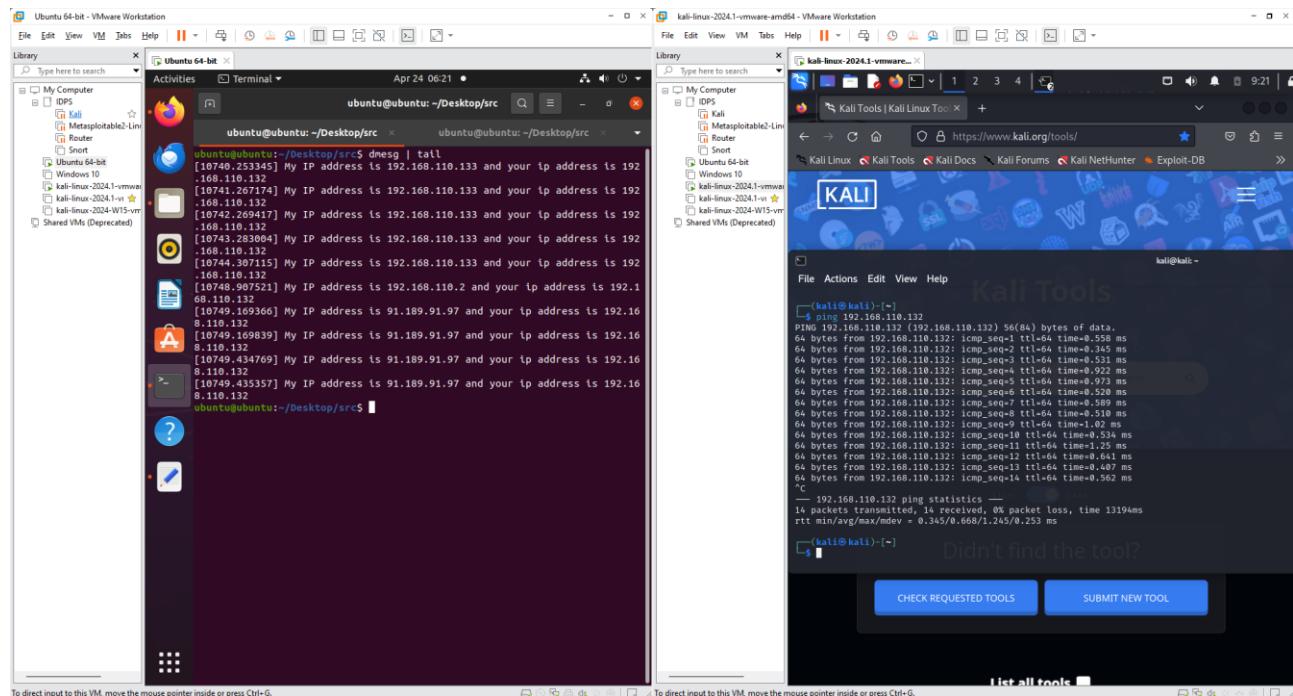
4. Tìm cách để in ra địa chỉ nguồn và địa chỉ đích của các gói tin khi thực hiện một tác vụ bất kỳ.

```

3 static unsigned int nf_hook_ex(void *priv, struct sk_buff *skb, const
4   struct nf_hook_state *state)
5 {
6     struct iphdr *iph;
7     iph=ip_hdr(skb);
8     char sipaddr[16];
9     char dipaddr[16];
10    sprintf(sipaddr,16,"%pI4",&iph->saddr);
11    sprintf(dipaddr,16,"%pI4",&iph->daddr);
12    printk(KERN_INFO "My IP address is %s and your ip address is
13      %s",sipaddr,dipaddr);
14    return NF_ACCEPT;
15 }
16

```

Kiểm tra: ping từ máy kali có địa chỉ 192.168.110.133 tới máy ubuntu có địa chỉ 192.168.110.132



5. Chỉ cho phép các gói tin đi đến uit.edu.vn (biết trước địa chỉ IP) đi ra ngoài, DROP tất cả còn lại

Ip của uit.edu.vn là:

```

$ nmap uit.edu.vn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 08:32 EDT
Nmap scan report for uit.edu.vn (118.69.123.140)
Host is up (0.0071s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
541/tcp   open  uucp-rlogin

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds

```

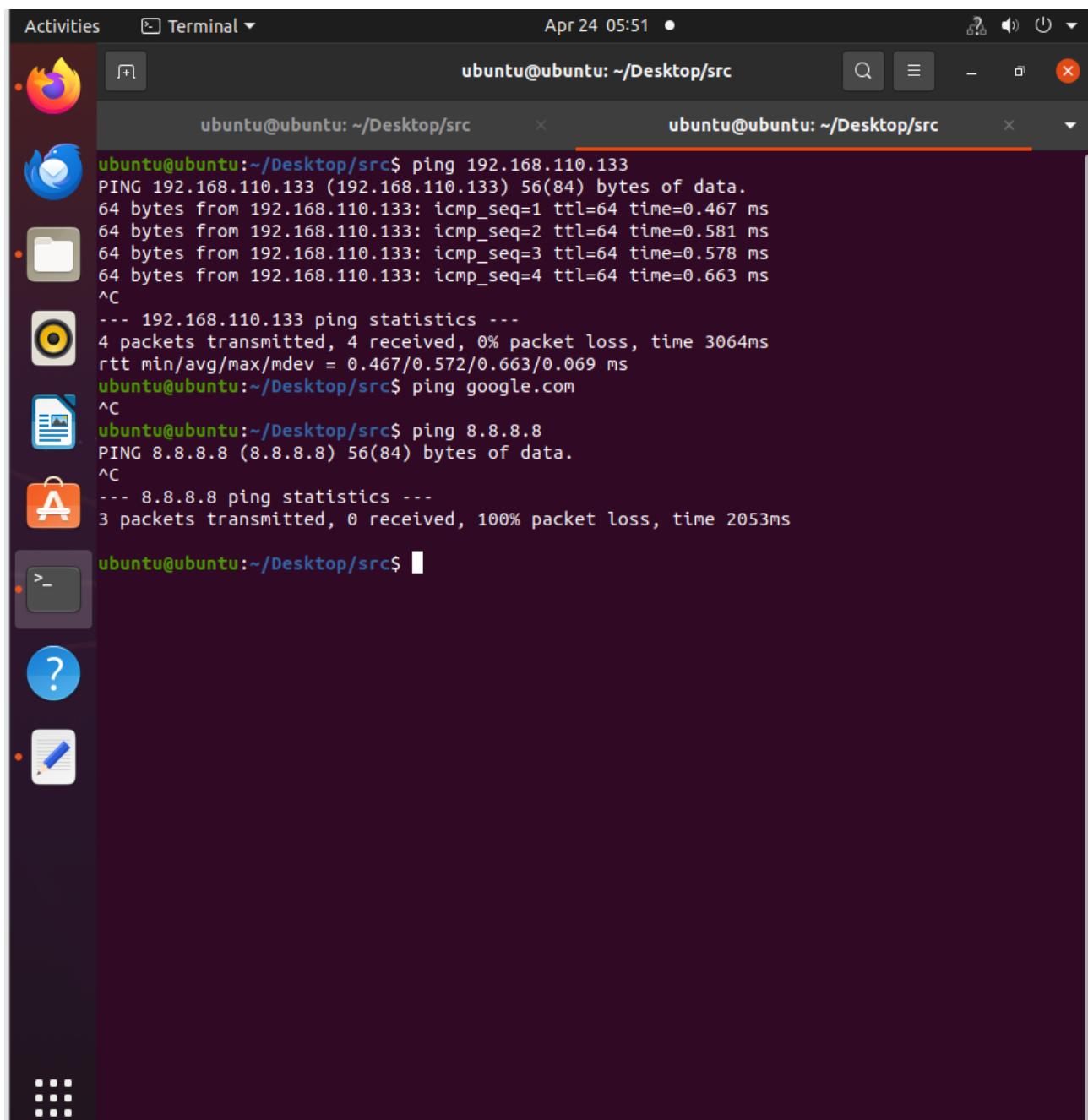
Tuy nhiên ta không thể ping tới địa chỉ này, có lẽ do trường đã chặn.

```
(kali㉿kali)-[~]
$ ping 118.69.123.140
PING 118.69.123.140 (118.69.123.140) 56(84) bytes of data.
^C
--- 118.69.123.140 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms
```

Nên em thay thế bằng địa chỉ của máy kali:

```
!3 static unsigned int nf_hook_ex(void *priv, struct sk_buff *skb, const struct
  nf_hook_state *state)
!4 {
!5     struct iphdr *iph;
!6     if(!skb)
!7         return NF_ACCEPT;
!8
!9
!0     char sipaddr[16];
!1     char target[16] = "192.168.110.133";
!2     iph = ip_hdr(skb);
!3     sprintf(sipaddr, 16, "%pI4", &iph->saddr);
!4
!5
!6     if (memcmp(&sipaddr, &target, sizeof(sipaddr))) {
!7         printk(KERN_INFO "Dropped packet \n");
!8         return NF_DROP;
!9     }
!10 }
!11 return NF_ACCEPT;
!12 }
```

Kết quả: ta có thể ping được tới máy kali nhưng không thể ping tới các địa chỉ khác:



6. Chặn các gói tin Echo Request đến từ máy client.

Ping từ máy kali tới máy ubuntu trước khi cài đặt rule:

```
(kali㉿kali)-[~]
$ ping 192.168.110.132
PING 192.168.110.132 (192.168.110.132) 56(84) bytes of data.
64 bytes from 192.168.110.132: icmp_seq=1 ttl=64 time=0.535 ms
64 bytes from 192.168.110.132: icmp_seq=2 ttl=64 time=0.333 ms
^X64 bytes from 192.168.110.132: icmp_seq=3 ttl=64 time=0.661 ms
64 bytes from 192.168.110.132: icmp_seq=4 ttl=64 time=0.358 ms
```

Cài đặt rule:

```

ubuntu@ubuntu:~/Desktop/src$ sudo iptables -F
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source          destination
      0    0  DROP        icmp -- any    any    anywhere       anywhere        icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source          destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source          destination
ubuntu@ubuntu:~/Desktop/src$
```

Kiểm tra

```

ubuntu@ubuntu:~/Desktop/src$ sudo iptables -F
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source          destination
      0    0  DROP        icmp -- any    any    anywhere       anywhere        icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source          destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source          destination
ubuntu@ubuntu:~/Desktop/src$
```

Kiểm tra bằng wireshark:

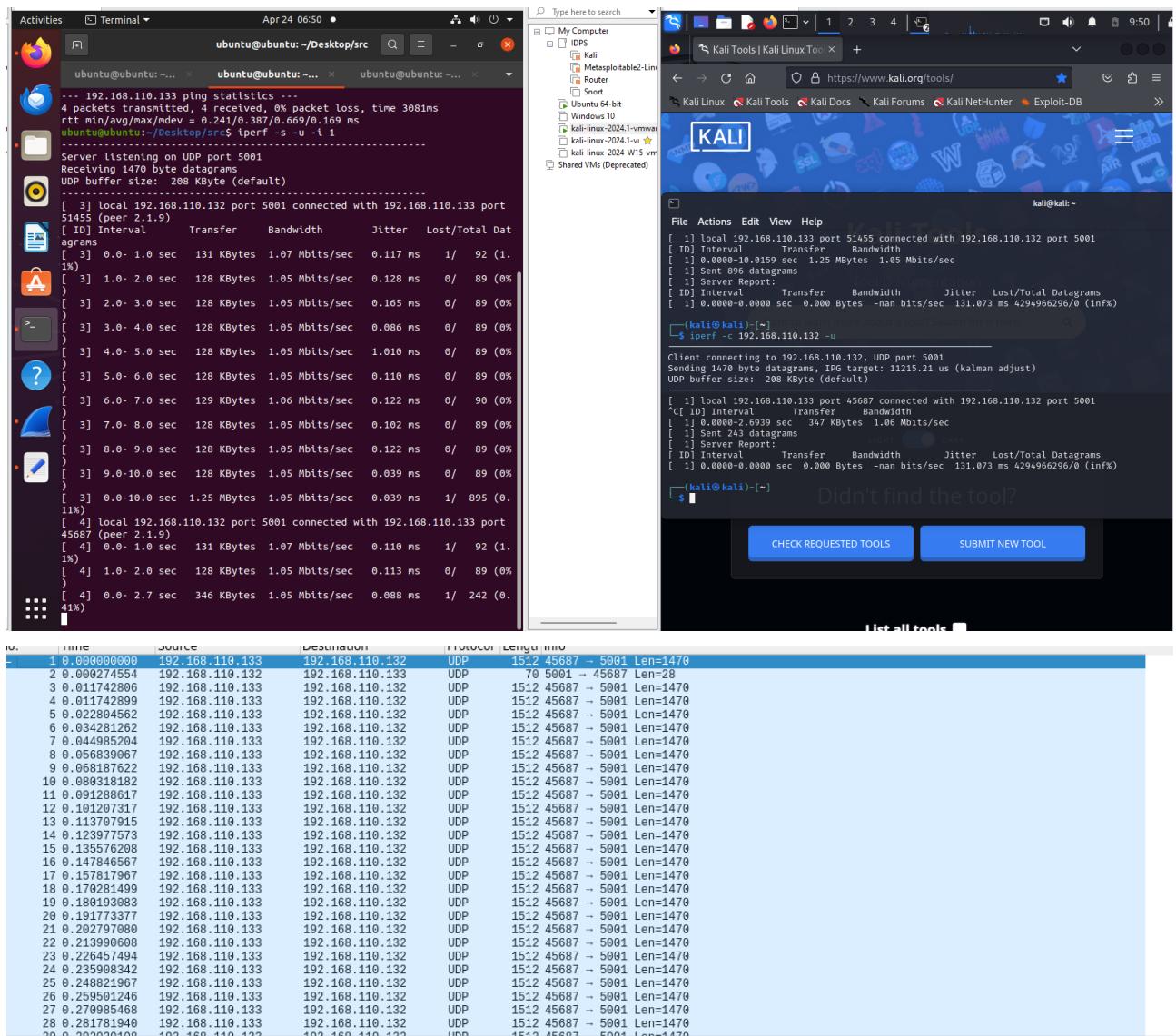
30 1.987488084	192.168.110.133	192.168.110.132	ICMP	98 Echo (ping) request id=0x9cf0, seq=2/512, ttl=64 (no response found!)
31 3.011212190	192.168.110.133	192.168.110.132	ICMP	98 Echo (ping) request id=0x9cf0, seq=3/768, ttl=64 (no response found!)
32 4.034911794	192.168.110.133	192.168.110.132	ICMP	98 Echo (ping) request id=0x9cf0, seq=4/1024, ttl=64 (no response found!)
33 5.058871231	192.168.110.133	192.168.110.132	ICMP	98 Echo (ping) request id=0x9cf0, seq=5/1280, ttl=64 (no response found!)
34 6.082931565	192.168.110.133	192.168.110.132	ICMP	98 Echo (ping) request id=0x9cf0, seq=6/1536, ttl=64 (no response found!)

7. Cấm tất cả các gói tin UDP và TCP có port đích là 80 đến từ bất kỳ máy tính nào.

Trước khi thiết lập rule:

Sử dụng iperf để khởi động UDP Server bằng lệnh: "iperf -s -u -i 1"

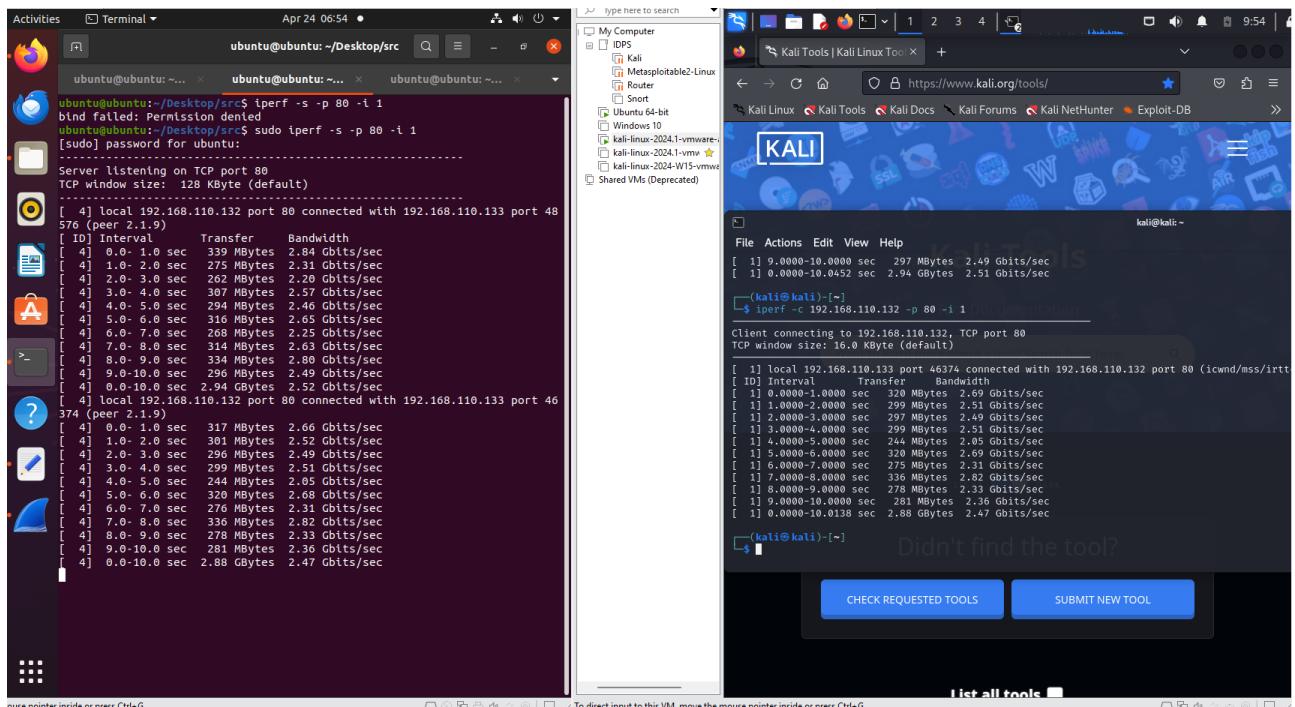
Sử dụng iperf để kết nối tới UDP Server bằng lệnh: "iperf -c 192.168.110.132 -u"



Ta có thể nhận được gói tin UDP

Kiểm tra với server tcp ở port 80:

- + Máy ubuntu: iperf -s -p 80 -i 1
- + Máy client: iperf -c 192.168.110.132 -p 80 -i 1



Cài đặt luật

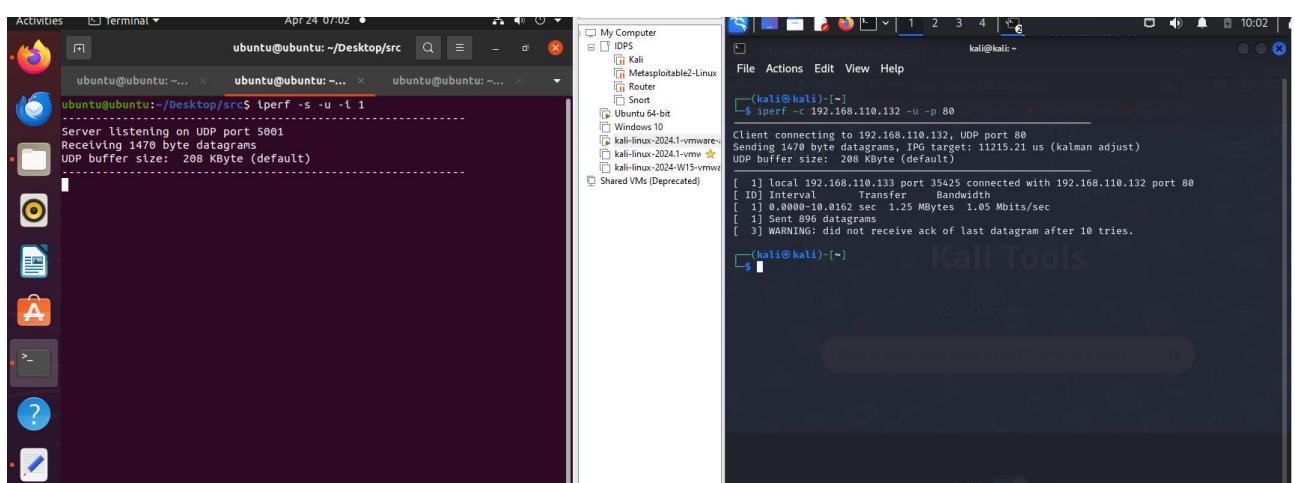
```
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -A INPUT -p TCP --dport 80 -j DROP
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -A INPUT -p UDP --dport 80 -j DROP
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 1 packets, 229 bytes)
 pkts bytes target     prot opt in     out      source          destination
   14  1176  DROP       icmp  --  any    any     anywhere        anywhere
     0     0  DROP       tcp   --  any    any     anywhere        anywhere
     0     0  DROP       udp   --  any    any     anywhere        anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination

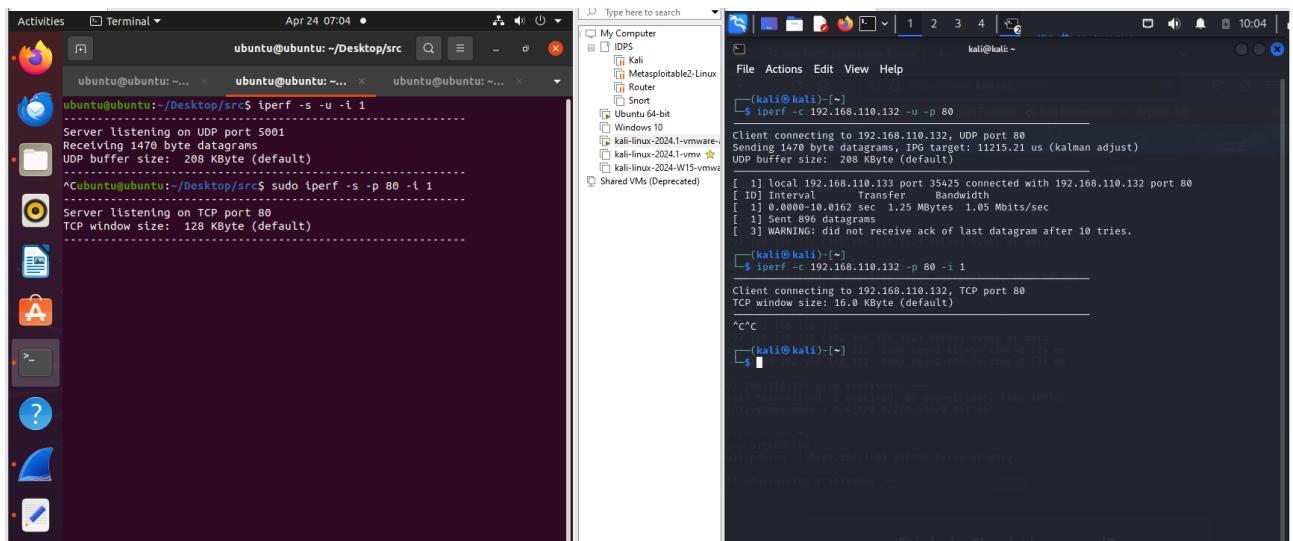
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
ubuntu@ubuntu:~/Desktop/src$
```

Kết quả:

UDP:



TCP:



Wireshark:

Index	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.110.133	192.168.110.132	TCP	74	53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=2467083224 TSecr=0 ...
2	1.012667289	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission] 53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSva...
3	2.036679655	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission] 53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSva...
4	3.058956876	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission] 53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSva...
5	4.082837298	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission] 53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSva...
6	5.107977076	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission] 53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSva...
7	5.172579598	VMware_14:65:2e	VMware_29:65:57	ARP	60	Who has 192.168.110.132? Tell 192.168.110.133
8	5.172595135	VMware_29:65:57	VMware_14:65:2e	ARP	42	192.168.110.132 is at 00:0c:29:29:a6:57
9	7.124651227	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission] 53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSva...
10	11.315376726	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission] 53884 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSva...
11	79.3659223320	192.168.110.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

8. Xoá tất cả rules, thiết đặt chặn các traffic từ máy Ubuntu đến địa chỉ IP máy client và ngược lại, các hoạt động khác bình thường.

Xoá tất cả các rules:

```
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -F
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
ubuntu@ubuntu:~/Desktop/src$
```

Trước khi cài đặt route 2 máy có thể giao tiếp bình thường

Ip máy ubuntu: 192.168.110.132

Ip máy kali: 192.168.110.133

```
ubuntu@ubuntu:~/Desktop/src$ ping 192.168.110.132
PING 192.168.110.132 (192.168.110.132) 56(84) bytes of data.
64 bytes from 192.168.110.132: icmp_seq=1 ttl=64 time=0.022 ms
64 bytes from 192.168.110.132: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 192.168.110.132: icmp_seq=3 ttl=64 time=0.046 ms
^C
--- 192.168.110.132 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.022/0.034/0.046/0.009 ms
ubuntu@ubuntu:~/Desktop/src$
```

Ta cài đặt rule:

```
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -F
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -A INPUT -s 192.168.110.133 -d 192.168.110.132 -j DROP
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -A OUTPUT -s 192.168.110.132 -d 192.168.110.133 -j DROP
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
      0     0  DROP       all    --  any    any    192.168.110.133   ubuntu
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
      0     0  DROP       all    --  any    any    ubuntu             192.168.110.133
ubuntu@ubuntu:~/Desktop/src$
```

Kiểm tra: 2 máy đều có thể ping tới google nhưng không thể ping cho nhau → Ngoại trừ các traffic giữa 2 máy thì tất cả vẫn hoạt động bình thường

```
ubuntu@ubuntu:~/Desktop/src$ ping 192.168.110.133
PING 192.168.110.133 (192.168.110.133) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
^C
--- 192.168.110.133 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4074ms

ubuntu@ubuntu:~/Desktop/src$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=29.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=30.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=30.1 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 29.854/29.995/30.066/0.099 ms
ubuntu@ubuntu:~/Desktop/src$
```

```
(kali㉿kali)-[~] $ ping 192.168.110.132 icmp_seq=1 ttl=64 time=0.424 ms
PING 192.168.110.132 (192.168.110.132) 56(84) bytes of data.
^C192.168.110.132 ping statistics —
— 192.168.110.132 ping statistics — loss, time 1007ms
3 packets transmitted, 0 received, 100% packet loss, time 2050ms

(kali㉿kali)-[~] $ ping 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=30.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=30.3 ms
^C
— 8.8.8.8 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 30.332/30.602/30.872/0.270 ms

(kali㉿kali)-[~]
```

9. Xoá rule câu số 8, thiết lập lệnh không cho phép client SSH vào máy Ubuntu. Hãy chứng minh điều đó?

Xoá rule câu số 8:

```
Chain INPUT (policy ACCEPT)
num  target      prot opt source                      destination
Chain FORWARD (policy ACCEPT)
num  target      prot opt source                      destination
Chain OUTPUT (policy ACCEPT)
num  target      prot opt source                      destination
ubuntu@ubuntu:~/Desktop/src$
```

Ta ssh từ máy kali tới ubuntu :

```
(kali㉿kali)-[~]
$ ssh ubuntu@192.168.110.132
The authenticity of host '192.168.110.132 (192.168.110.132)' can't be established.
ED25519 key fingerprint is SHA256:r8r6QTTTe4nnZ4P9rr7Tfd3ozih3VCjmCqg/W4BfJ60c.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.110.132' (ED25519) to the list of known hosts.
ubuntu@192.168.110.132's password: 
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-105-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: dev = 0 https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.
uit.edu.vn
0 updates can be applied immediately. 0 of data.

31 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.      CHECK REQUESTED TOOLS      SUBMIT NEW TOOL

ubuntu@ubuntu:~$
```

Ta vẫn có thể kết nối bình thường

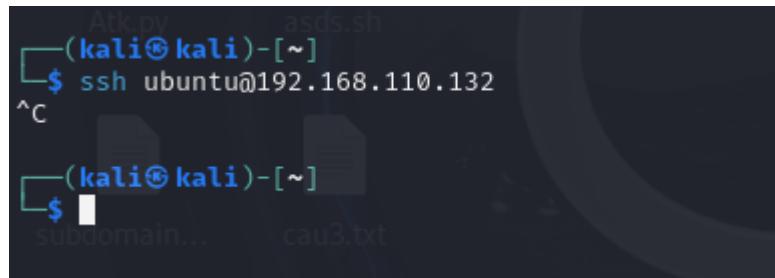
Cài đặt Rules:

```
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
ubuntu@ubuntu:~/Desktop/src$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    DROP       tcp  --  anywhere       anywhere        tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination
ubuntu@ubuntu:~/Desktop/src$
```

Kết quả:



Ta kiểm tra bằng wireshark thì thấy có các gói tin tcp retransmission, tức là gói tin tcp ssh đã bị chặn:

81	27.129352493	192.168.110.133	192.168.110.132	TCP	242	[TCP Retransmission]	56134 -- 22	[FIN, PSH, ACK]	Seq=1 ACK=1 Win=249 Len=176 TStamp=246...
82	27.963318391	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission]	57984 -- 22	[SYN]	Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TS...
83	28.977934963	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission]	57984 -- 22	[SYN]	Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TS...
84	29.999543824	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission]	57984 -- 22	[SYN]	Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TS...
85	31.026035300	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission]	57984 -- 22	[SYN]	Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TS...
86	32.047276230	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission]	57984 -- 22	[SYN]	Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TS...
87	33.070891177	192.168.110.133	192.168.110.132	TCP	74	[TCP Retransmission]	57984 -- 22	[SYN]	Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TS...

10. Tìm hiểu và trình bày về cuộc tấn công Deny of Service (DoS), thiết lập rule để phòng chống cuộc tấn công này.

Lý thuyết về DoS:

Tấn công DoS (Denial of Service) nhắm vào việc làm cho một dịch vụ, hệ thống hoặc tài nguyên mạng trở nên không khả dụng cho người dùng hợp lệ. Điều này có thể đặc biệt nguy hiểm đối với các dịch vụ trực tuyến, doanh nghiệp và tổ chức mà hoạt động của họ phụ thuộc nhiều vào tính liên tục của dịch vụ mạng.

Dưới đây là một số chi tiết về tấn công DoS:

- Nguyên lý hoạt động: Khi bắt đầu một cuộc tấn công DoS, kẻ tấn công gửi một lượng lớn yêu cầu đến một dịch vụ hoặc hệ thống cụ thể, đòi hỏi một lượng lớn tài nguyên. Điều này có thể làm cho hệ thống không thể xử lý được, làm cho dịch vụ trở nên không khả dụng.
- Các phương pháp tấn công: Có nhiều phương pháp để thực hiện tấn công DoS, bao gồm gửi lượng lớn gói tin đến máy chủ (như tấn công UDP flood hoặc SYN flood), lợi dụng lỗ hổng bảo mật để làm cho hệ thống gặp lỗi, hoặc thực hiện tấn công từ chối dịch vụ (tấn công DoS) bằng cách tiêu tốn tài nguyên của máy chủ, hệ thống mạng, hoặc ứng dụng.
- Loại tấn công DDoS: Tấn công DoS thường được mở rộng thành tấn công DDoS (Distributed Denial of Service), trong đó, không chỉ một mà nhiều hệ thống được sử dụng để tấn công một mục tiêu. Điều này làm cho việc phát hiện và ngăn chặn tấn công trở nên khó khăn hơn.
- Hậu quả: Các hậu quả của tấn công DoS có thể rất nghiêm trọng, bao gồm thiệt hại về tài chính, mất dữ liệu quan trọng, ảnh hưởng đến uy tín của doanh nghiệp hoặc tổ chức, và gây ra sự không hài lòng từ phía người dùng.

Các cách thức thực hiện tấn công DoS phổ biến:

- Tấn công DDoS (Distributed Denial of Service): Đây là phiên bản mở rộng của tấn công DoS, nơi nhiều hệ thống (thường là botnet) được sử dụng để gửi lượng lớn yêu cầu đến một hệ thống hoặc dịch vụ, làm quá tải và làm cho nó trở nên không khả dụng.

2. Tấn công UDP Flood: Tấn công này thường làm cho hệ thống không thể xử lý lượng lớn gói tin UDP (User Datagram Protocol), làm cho dịch vụ trở nên không khả dụng.
3. Tấn công SYN Flood: Tấn công này tập trung vào việc gửi một lượng lớn gói tin SYN (Synchronize) đến máy chủ, làm cho máy chủ phải mất nhiều tài nguyên để xử lý các kết nối SYN, và cuối cùng không thể đáp ứng yêu cầu từ người dùng hợp lệ.
4. Tấn công HTTP Flood: Trong loại tấn công này, kẻ tấn công gửi một lượng lớn yêu cầu HTTP đến máy chủ web, làm cho nó không thể xử lý và đáp ứng các yêu cầu từ người dùng thật.
5. Tấn công Smurf: Trong tấn công này, kẻ tấn công gửi các gói tin ICMP Echo Request đến một địa chỉ IP broadcast, làm cho tất cả các máy trong mạng đều phản hồi lại địa chỉ IP đó, gây ra quá tải cho hệ thống mục tiêu.

Script dùng để chặn Tấn công dos:

```

1#!/bin/bash
2
3# Xóa tất cả các quy tắc iptables hiện có
4iptables -F
5
6# Thiết lập các chính sách mặc định
7iptables -P INPUT DROP
8iptables -P FORWARD DROP
9iptables -P OUTPUT ACCEPT
10
11# Cho phép các kết nối đã thiết lập và liên quan
12iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
13
14# Giới hạn số lượng gói tin TCP mới mỗi giây từ một địa chỉ IP
15iptables -A INPUT -p tcp --syn -m connlimit --connlimit-above 20 --connlimit-mask 32 -j DROP
16
17# Giới hạn số lượng kết nối TCP đồng thời từ một địa chỉ IP
18iptables -A INPUT -p tcp --syn -m conntrack --ctstate NEW -m recent --name tcpattack --set
19iptables -A INPUT -p tcp --syn -m conntrack --ctstate NEW -m recent --name tcpattack --update --seconds 60 --hitcount 10 -j DROP
20
21# Giới hạn số lượng yêu cầu ICMP mỗi giây từ một địa chỉ IP
22iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
23iptables -A INPUT -p icmp -j DROP
24
25|

```

Cài đặt:

```

ubuntu@ubuntu:~/Desktop$ sudo iptables -L --line-number
Chain INPUT (policy DROP)
num target     prot opt source          destination
1  ACCEPT      all  --  anywhere        anywhere        ctstate RELATED,ESTABLISHED
2  DROP        tcp  --  anywhere        anywhere
3  DROP        tcp  --  anywhere        anywhere
4  DROP        tcp  --  anywhere        anywhere
5  ACCEPT      icmp --  anywhere       anywhere        icmp echo-request limit: avg 1/sec burst 5
6  DROP        icmp --  anywhere       anywhere
sk: 255.255.255.255

Chain FORWARD (policy DROP)
num target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
num target     prot opt source          destination
ubuntu@ubuntu:~/Desktop$ 

```