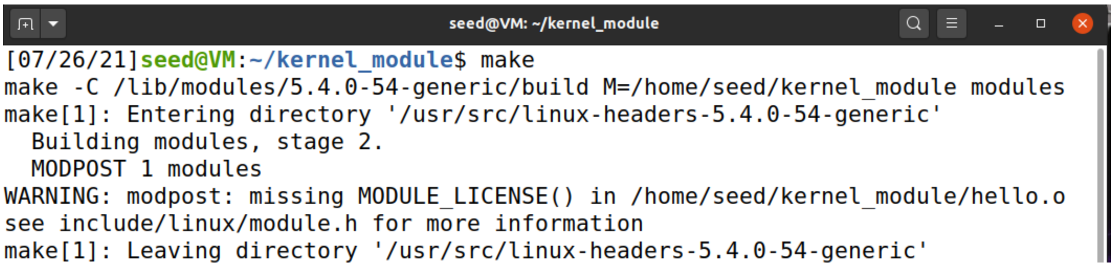
lab6-report

571118106 强珂阳

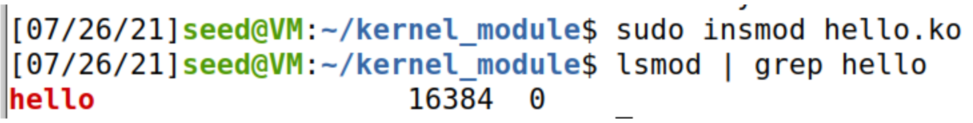
task 1.A Implement a Simple Kernel Module

编译 kernel_module

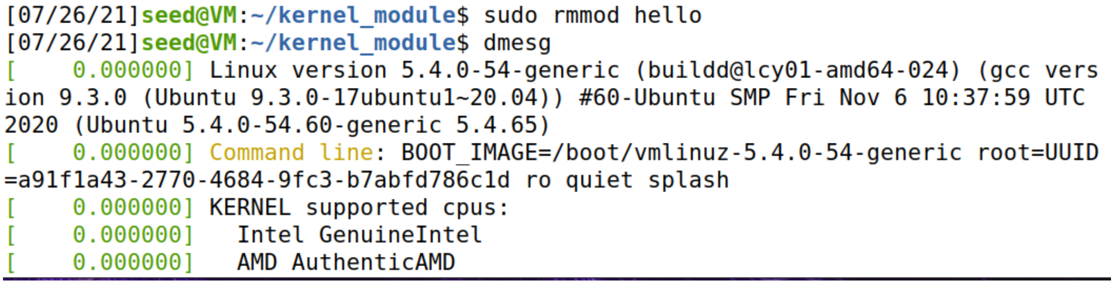


```
[07/26/21]seed@VM:~/kernel_module$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/kernel_module modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  Building modules, stage 2.
  MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/seed/kernel_module/hello.o
see include/linux/module.h for more information
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
```

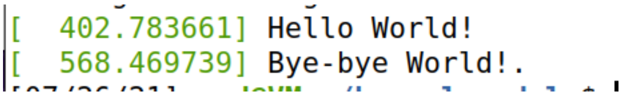
测试指令



```
[07/26/21]seed@VM:~/kernel_module$ sudo insmod hello.ko
[07/26/21]seed@VM:~/kernel_module$ lsmod | grep hello
hello                  16384  0
```



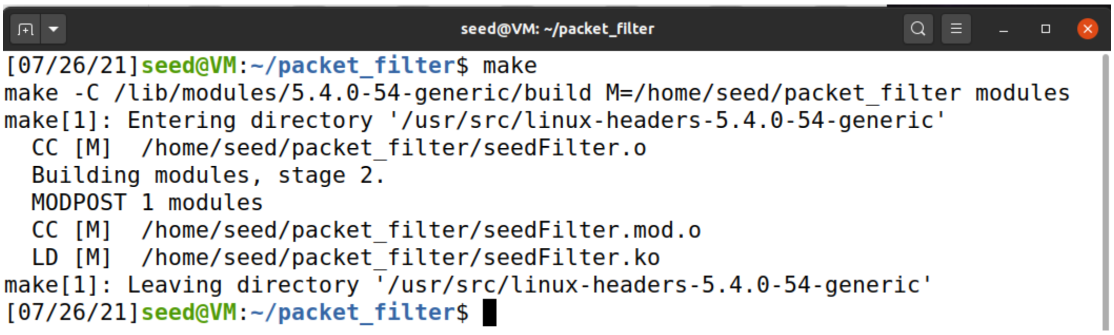
```
[07/26/21]seed@VM:~/kernel_module$ sudo rmmod hello
[07/26/21]seed@VM:~/kernel_module$ dmesg
[    0.000000] Linux version 5.4.0-54-generic (buildd@lcy01-amd64-024) (gcc vers
ion 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #60-Ubuntu SMP Fri Nov 6 10:37:59 UTC
2020 (Ubuntu 5.4.0-54.60-generic 5.4.65)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.4.0-54-generic root=UUID
=a91f1a43-2770-4684-9fc3-b7abfd786c1d ro quiet splash
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
```



```
[  402.783661] Hello World!
[  568.469739] Bye-bye World!.
```

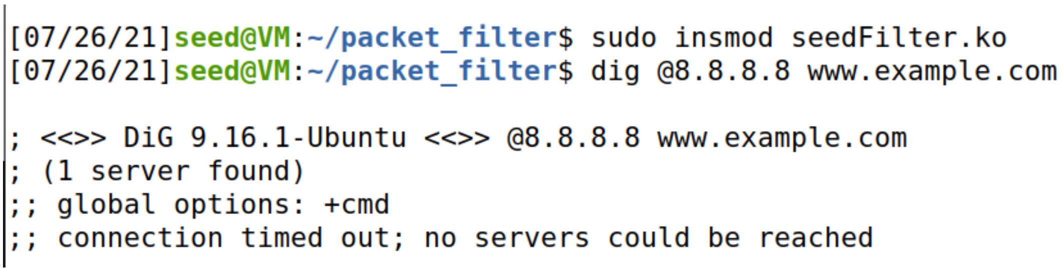
task 1.B Implement a Simple Firewall Using Netfilter

1.编译 packet_filter



```
[07/26/21]seed@VM:~/packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/packet_filter/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/packet_filter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[07/26/21]seed@VM:~/packet_filter$ 
```

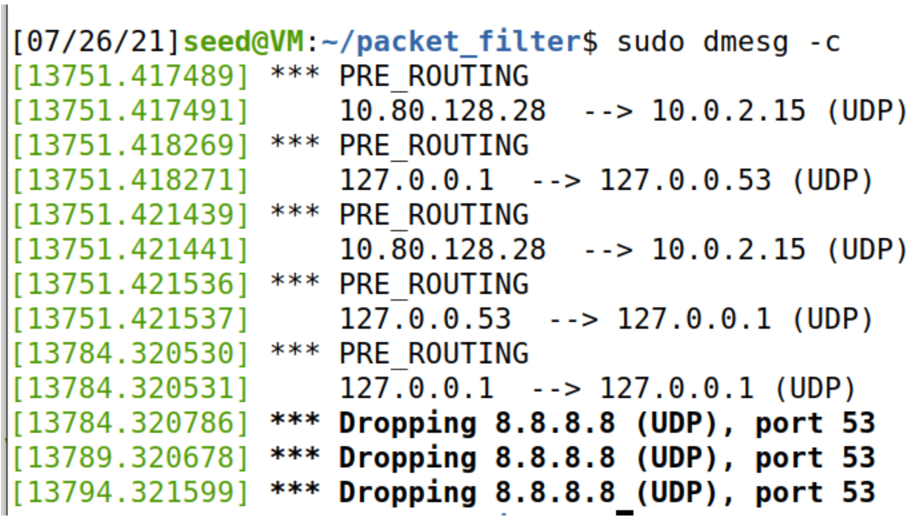
加载内核，并测试防火墙



```
[07/26/21]seed@VM:~/packet_filter$ sudo insmod seedFilter.ko
[07/26/21]seed@VM:~/packet_filter$ dig @8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

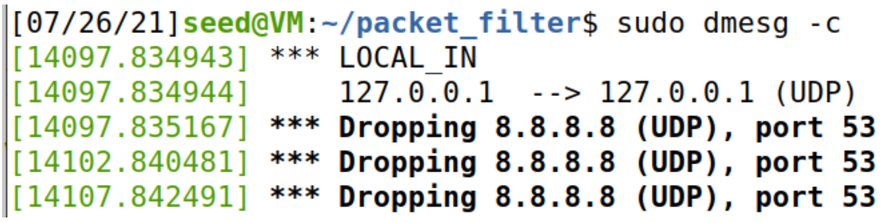
请求被阻止，说明正常工作。

2.修改代码的 hooknum，重新编译



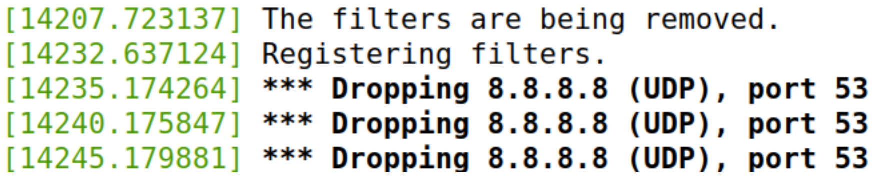
```
[07/26/21]seed@VM:~/packet_filter$ sudo dmesg -c
[13751.417489] *** PRE_ROUTING
[13751.417491]     10.80.128.28  --> 10.0.2.15 (UDP)
[13751.418269] *** PRE_ROUTING
[13751.418271]     127.0.0.1  --> 127.0.0.53 (UDP)
[13751.421439] *** PRE_ROUTING
[13751.421441]     10.80.128.28  --> 10.0.2.15 (UDP)
[13751.421536] *** PRE_ROUTING
[13751.421537]     127.0.0.53  --> 127.0.0.1 (UDP)
[13784.320530] *** PRE_ROUTING
[13784.320531]     127.0.0.1  --> 127.0.0.1 (UDP)
[13784.320786] *** Dropping 8.8.8.8 (UDP), port 53
[13789.320678] *** Dropping 8.8.8.8 (UDP), port 53
[13794.321599] *** Dropping 8.8.8.8 (UDP), port 53
```

数据包到达后，首先经过 NF_INET_PRE_ROUTING，决定发给本机还是转发。



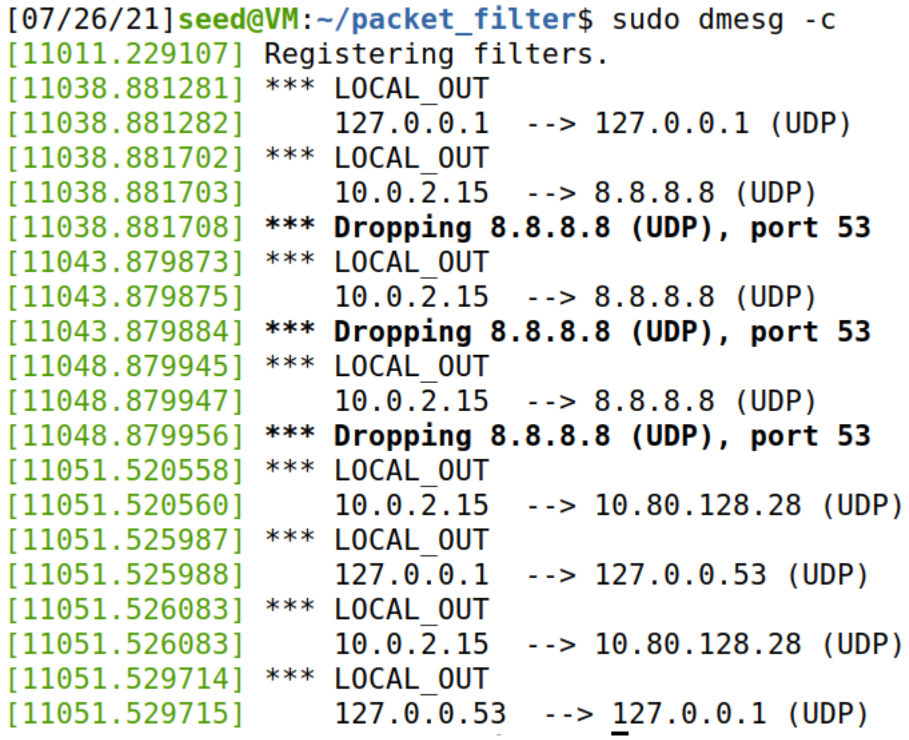
```
[07/26/21]seed@VM:~/packet_filter$ sudo dmesg -c
[14097.834943] *** LOCAL_IN
[14097.834944]     127.0.0.1  --> 127.0.0.1 (UDP)
[14097.835167] *** Dropping 8.8.8.8 (UDP), port 53
[14102.840481] *** Dropping 8.8.8.8 (UDP), port 53
[14107.842491] *** Dropping 8.8.8.8 (UDP), port 53
```

如果数据包发给本机，则会使用 NF_INET_LOCAL_IN 处理。



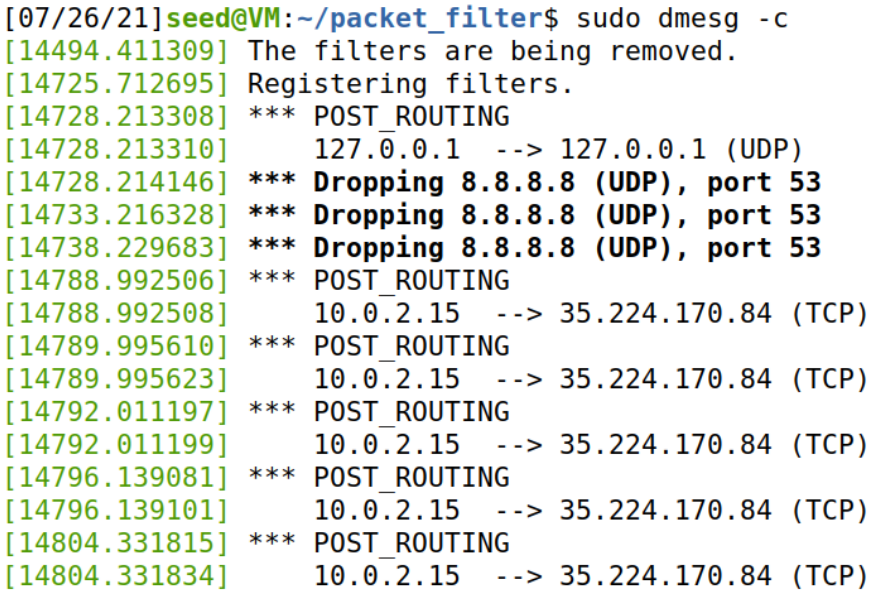
```
[14207.723137] The filters are being removed.
[14232.637124] Registering filters.
[14235.174264] *** Dropping 8.8.8.8 (UDP), port 53
[14240.175847] *** Dropping 8.8.8.8 (UDP), port 53
[14245.179881] *** Dropping 8.8.8.8 (UDP), port 53
```

如果数据包不是发给本机的，则会用 NF_INET_FORWARD 处理。



```
[07/26/21]seed@VM:~/packet_filter$ sudo dmesg -c
[11011.229107] Registering filters.
[11038.881281] *** LOCAL_OUT
[11038.881282]     127.0.0.1  --> 127.0.0.1 (UDP)
[11038.881702] *** LOCAL_OUT
[11038.881703]     10.0.2.15  --> 8.8.8.8 (UDP)
[11038.881708] *** Dropping 8.8.8.8 (UDP), port 53
[11043.879873] *** LOCAL_OUT
[11043.879875]     10.0.2.15  --> 8.8.8.8 (UDP)
[11043.879884] *** Dropping 8.8.8.8 (UDP), port 53
[11048.879945] *** LOCAL_OUT
[11048.879947]     10.0.2.15  --> 8.8.8.8 (UDP)
[11048.879956] *** Dropping 8.8.8.8 (UDP), port 53
[11051.520558] *** LOCAL_OUT
[11051.520560]     10.0.2.15  --> 10.80.128.28 (UDP)
[11051.525987] *** LOCAL_OUT
[11051.525988]     127.0.0.1  --> 127.0.0.53 (UDP)
[11051.526083] *** LOCAL_OUT
[11051.526083]     10.0.2.15  --> 10.80.128.28 (UDP)
[11051.529714] *** LOCAL_OUT
[11051.529715]     127.0.0.53  --> 127.0.0.1 (UDP)
```

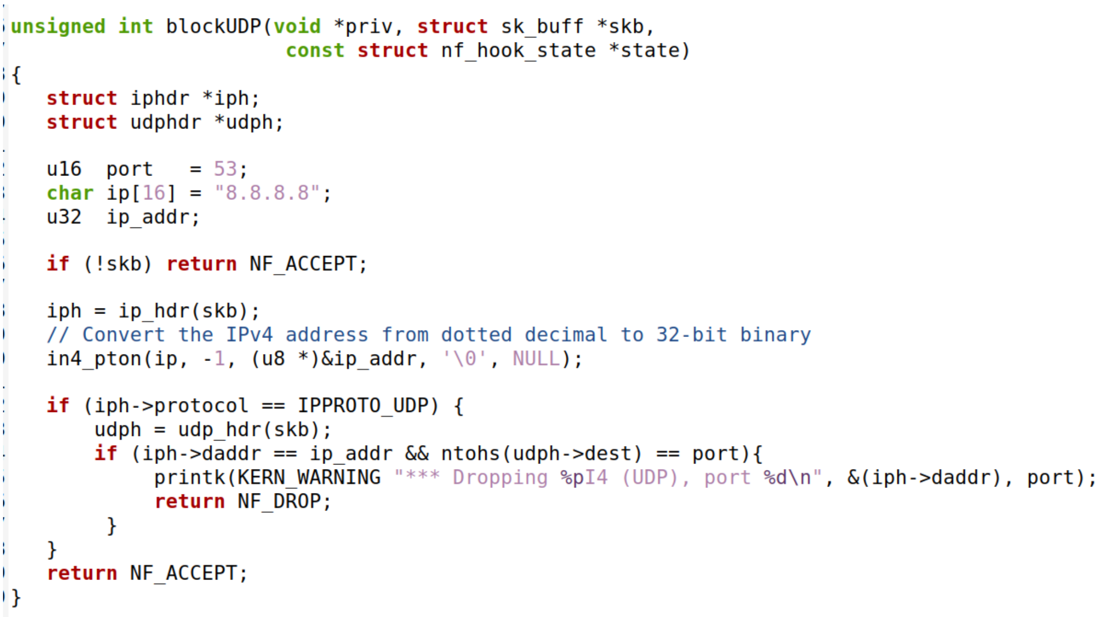
本机产生的数据包会第一个使用 NF_INET_LOCAL_OUT。



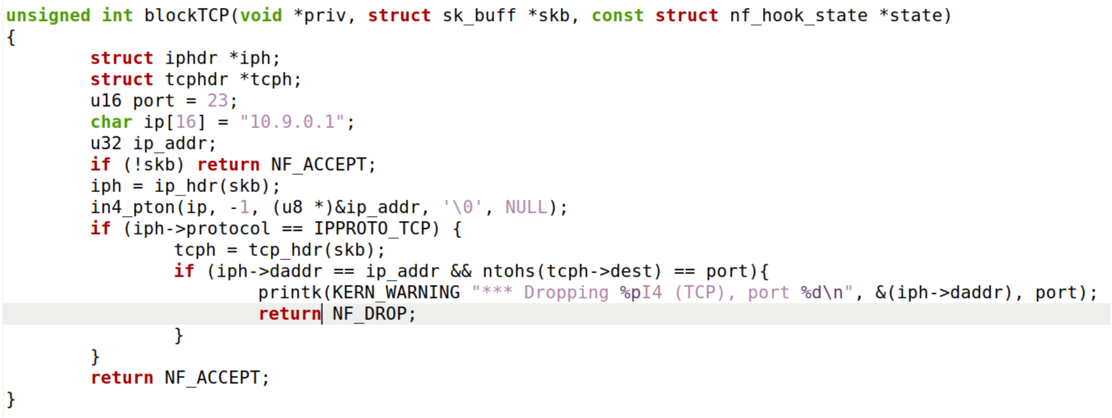
```
[07/26/21]seed@VM:~/packet_filter$ sudo dmesg -c
[14494.411309] The filters are being removed.
[14725.712695] Registering filters.
[14728.213308] *** POST_ROUTING
[14728.213310]     127.0.0.1  --> 127.0.0.1 (UDP)
[14728.214146] *** Dropping 8.8.8.8 (UDP), port 53
[14733.216328] *** Dropping 8.8.8.8 (UDP), port 53
[14738.229683] *** Dropping 8.8.8.8 (UDP), port 53
[14788.992506] *** POST_ROUTING
[14788.992508]     10.0.2.15  --> 35.224.170.84 (TCP)
[14789.995610] *** POST_ROUTING
[14789.995623]     10.0.2.15  --> 35.224.170.84 (TCP)
[14792.011197] *** POST_ROUTING
[14792.011199]     10.0.2.15  --> 35.224.170.84 (TCP)
[14796.139081] *** POST_ROUTING
[14796.139101]     10.0.2.15  --> 35.224.170.84 (TCP)
[14804.331815] *** POST_ROUTING
[14804.331834]     10.0.2.15  --> 35.224.170.84 (TCP)
```

本机向外发送的数据包会由 NF_INET_POST_ROUTING 处理发送。

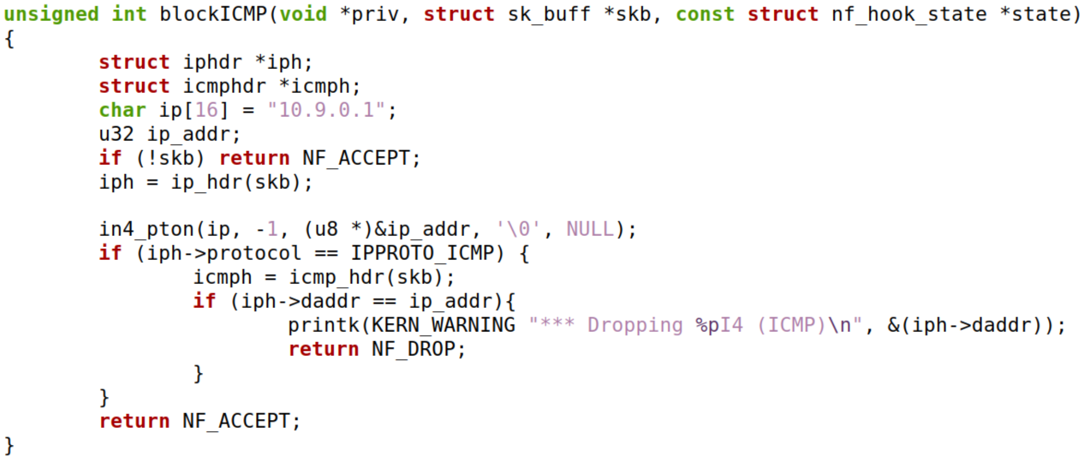
3.修改代码



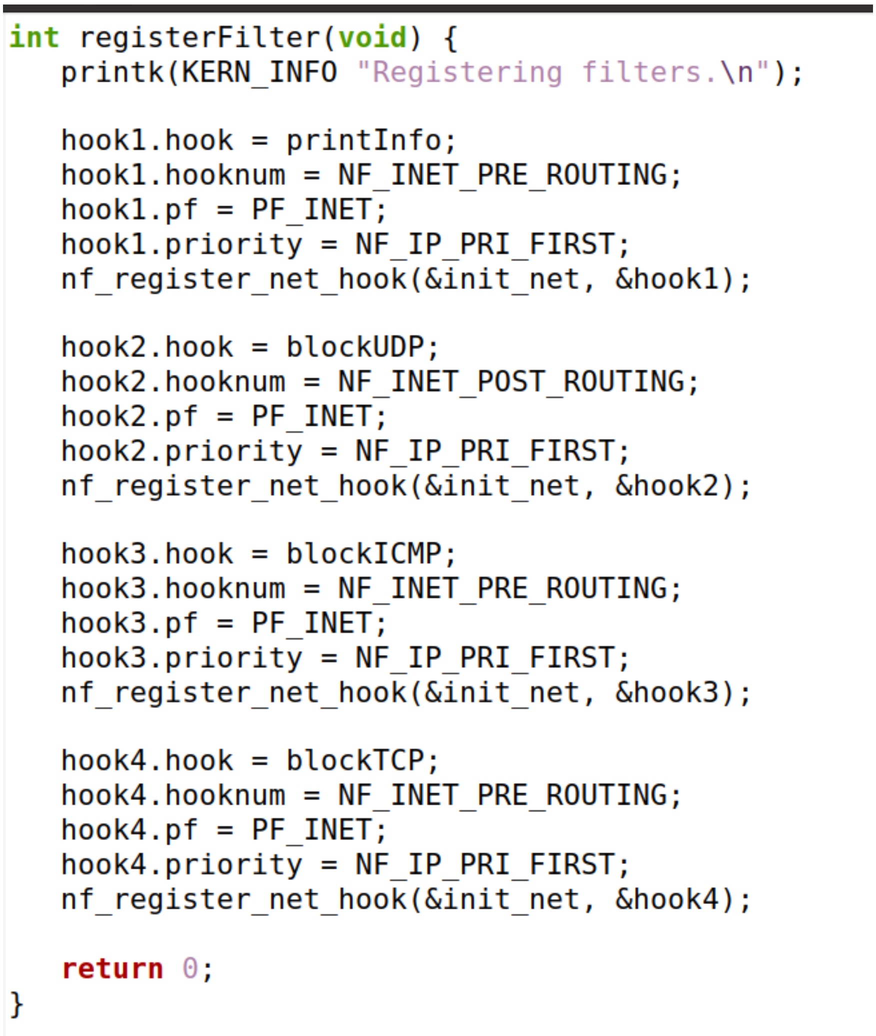
```
unsigned int blockUDP(void *priv, struct sk_buff *skb,
                       const struct nf_hook_state *state)
{
   struct iphdr *iph;
   struct udphdr *udph;

   u16  port   = 53;
   char ip[16] = "8.8.8.8";
   u32  ip_addr;

   if (!skb) return NF_ACCEPT;

   iph = ip_hdr(skb);
   // Convert the IPv4 address from dotted decimal to 32-bit binary
   in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);

   if (iph->protocol == IPPROTO_UDP) {
       udph = udp_hdr(skb);
       if (iph->daddr == ip_addr && ntohs(udph->dest) == port){
            printk(KERN_WARNING "*** Dropping %pI4 (UDP), port %d\n", &(iph->daddr), port);
            return NF_DROP;
        }
   }
   return NF_ACCEPT;
}
```



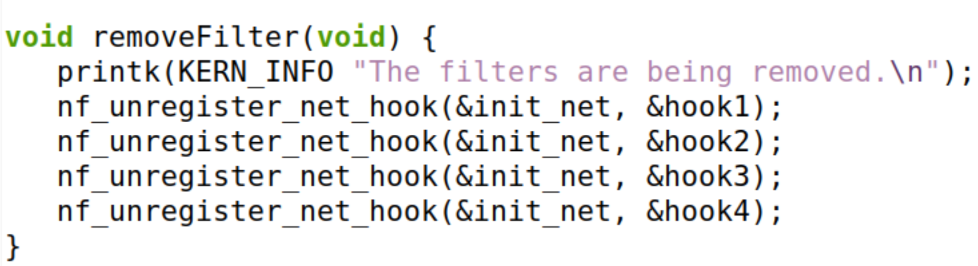
```
unsigned int blockTCP(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
        struct iphdr *iph;
        struct tcphdr *tcph;
        u16 port = 23;
        char ip[16] = "10.9.0.1";
        u32 ip_addr;
        if (!skb) return NF_ACCEPT;
        iph = ip_hdr(skb);
        in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);
        if (iph->protocol == IPPROTO_TCP) {
                tcph = tcp_hdr(skb);
                if (iph->daddr == ip_addr && ntohs(tcph->dest) == port){
                        printk(KERN_WARNING "*** Dropping %pI4 (TCP), port %d\n", &(iph->daddr), port);
                        return NF_DROP;
                }
        }
        return NF_ACCEPT;
}
```



```
unsigned int blockICMP(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
        struct iphdr *iph;
        struct icmphdr *icmph;
        char ip[16] = "10.9.0.1";
        u32 ip_addr;
        if (!skb) return NF_ACCEPT;
        iph = ip_hdr(skb);

        in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);
        if (iph->protocol == IPPROTO_ICMP) {
                icmph = icmp_hdr(skb);
                if (iph->daddr == ip_addr){
                        printk(KERN_WARNING "*** Dropping %pI4 (ICMP)\n", &(iph->daddr));
                        return NF_DROP;
                }
        }
        return NF_ACCEPT;
}
```

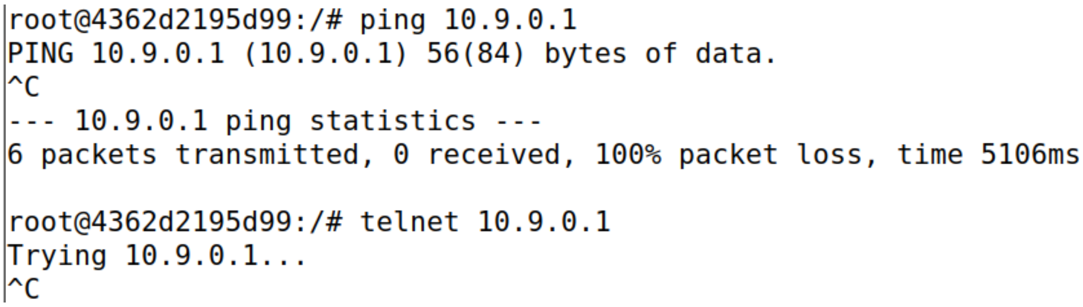


```
int registerFilter(void) {
   printk(KERN_INFO "Registering filters.\n");

   hook1.hook = printInfo;
   hook1.hooknum = NF_INET_PRE_ROUTING;
   hook1.pf = PF_INET;
   hook1.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook1);

   hook2.hook = blockUDP;
   hook2.hooknum = NF_INET_POST_ROUTING;
   hook2.pf = PF_INET;
   hook2.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook2);

   hook3.hook = blockICMP;
   hook3.hooknum = NF_INET_PRE_ROUTING;
   hook3.pf = PF_INET;
   hook3.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook3);

   hook4.hook = blockTCP;
   hook4.hooknum = NF_INET_PRE_ROUTING;
   hook4.pf = PF_INET;
   hook4.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook4);

   return 0;
}
```

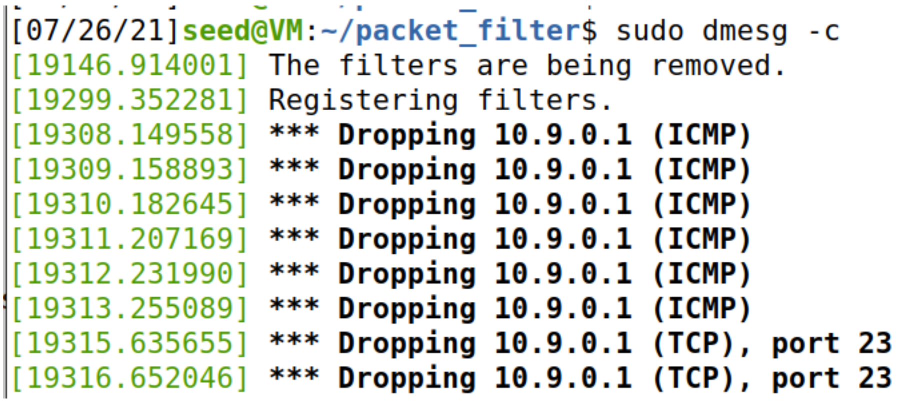


```
void removeFilter(void) {
   printk(KERN_INFO "The filters are being removed.\n");
   nf_unregister_net_hook(&init_net, &hook1);
   nf_unregister_net_hook(&init_net, &hook2);
   nf_unregister_net_hook(&init_net, &hook3);
   nf_unregister_net_hook(&init_net, &hook4);
}
```

用 A 分别 ping 和 telnet VM



```
root@4362d2195d99:/# ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
^C
--- 10.9.0.1 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5106ms

root@4362d2195d99:/# telnet 10.9.0.1
Trying 10.9.0.1...
^C
```

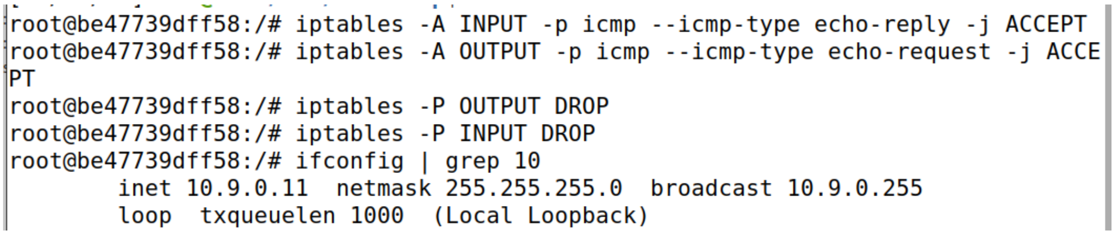


```
[07/26/21]seed@VM:~/packet_filter$ sudo dmesg -c
[19146.914001] The filters are being removed.
[19299.352281] Registering filters.
[19308.149558] *** Dropping 10.9.0.1 (ICMP)
[19309.158893] *** Dropping 10.9.0.1 (ICMP)
[19310.182645] *** Dropping 10.9.0.1 (ICMP)
[19311.207169] *** Dropping 10.9.0.1 (ICMP)
[19312.231990] *** Dropping 10.9.0.1 (ICMP)
[19313.255089] *** Dropping 10.9.0.1 (ICMP)
[19315.635655] *** Dropping 10.9.0.1 (TCP), port 23
[19316.652046] *** Dropping 10.9.0.1 (TCP), port 23
```

都被丢弃，说明阻止了其他计算机 ping VM、telnet 进入 VM。

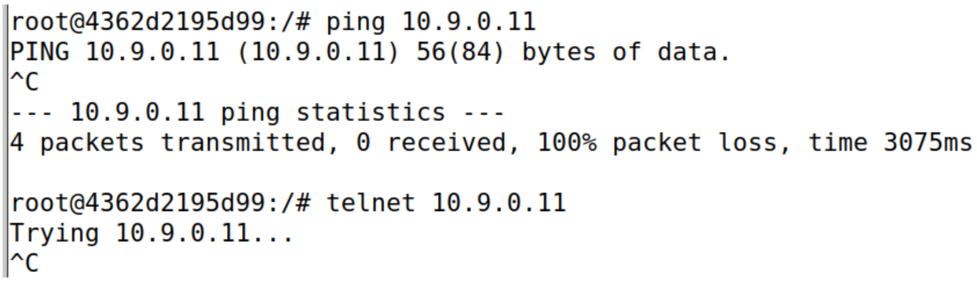
task 2.A Protecting the Router

在路由器上设置过滤机制并查看其 IP 地址



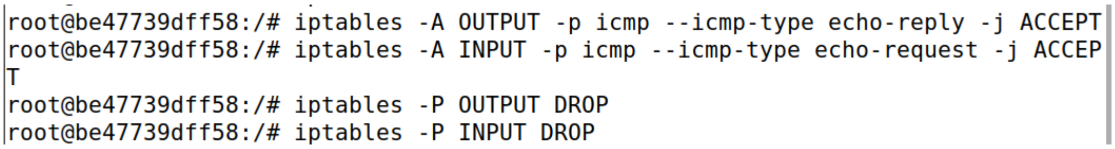
```
root@be47739dff58:/# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@be47739dff58:/# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCE
PT
root@be47739dff58:/# iptables -P OUTPUT DROP
root@be47739dff58:/# iptables -P INPUT DROP
root@be47739dff58:/# ifconfig | grep 10
        inet 10.9.0.11  netmask 255.255.255.0  broadcast 10.9.0.255
        loop  txqueuelen 1000  (Local Loopback)
```

在 A 上 ping、telnet 路由器均失败

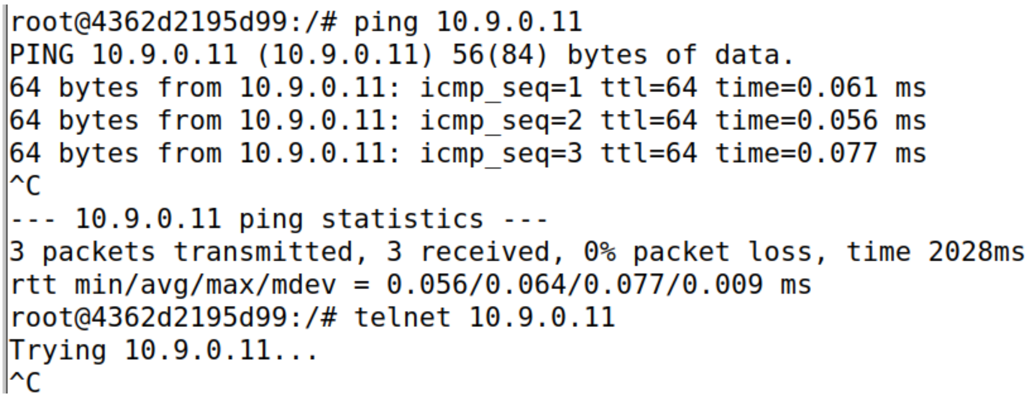


```
root@4362d2195d99:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3075ms

root@4362d2195d99:/# telnet 10.9.0.11
Trying 10.9.0.11...
^C
```

发现修改过滤机制，可以使 ping 通，telnet 不通



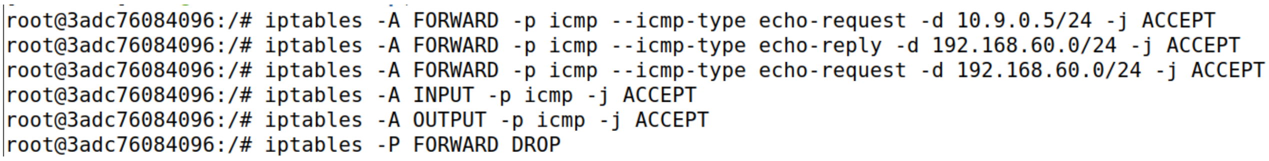
```
root@be47739dff58:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@be47739dff58:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEP
T
root@be47739dff58:/# iptables -P OUTPUT DROP
root@be47739dff58:/# iptables -P INPUT DROP
```



```
root@4362d2195d99:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.061 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.077 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.056/0.064/0.077/0.009 ms
root@4362d2195d99:/# telnet 10.9.0.11
Trying 10.9.0.11...
^C
```

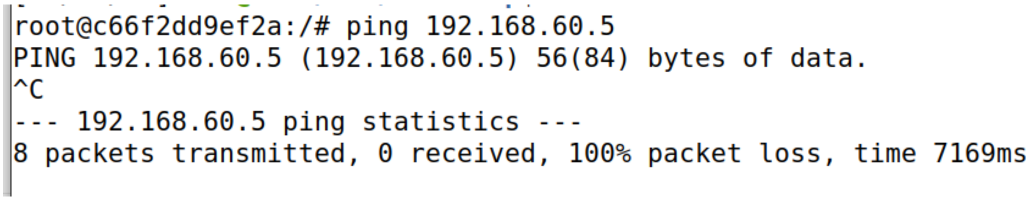
猜测前两条为允许其他主机 ping 路由器，后面两条为设置 INPUT 和 POUTPUT 默认丢包。

task 2.B Protecting the Internet Network



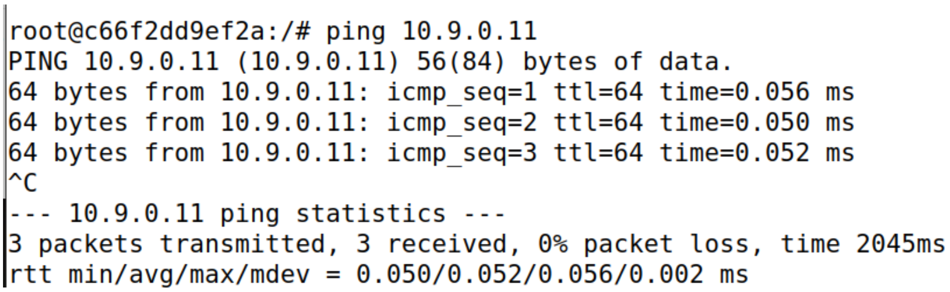
```
root@3adc76084096:/# iptables -A FORWARD -p icmp --icmp-type echo-request -d 10.9.0.5/24 -j ACCEPT
root@3adc76084096:/# iptables -A FORWARD -p icmp --icmp-type echo-reply -d 192.168.60.0/24 -j ACCEPT
root@3adc76084096:/# iptables -A FORWARD -p icmp --icmp-type echo-request -d 192.168.60.0/24 -j ACCEPT
root@3adc76084096:/# iptables -A INPUT -p icmp -j ACCEPT
root@3adc76084096:/# iptables -A OUTPUT -p icmp -j ACCEPT
root@3adc76084096:/# iptables -P FORWARD DROP
```

1.外部主机不能 ping 内部主机



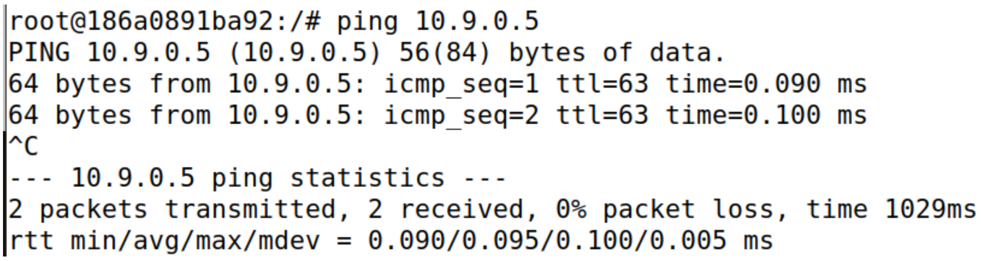
```
root@c66f2dd9ef2a:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
^C
--- 192.168.60.5 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7169ms
```

2.外部主机能 ping 路由器



```
root@c66f2dd9ef2a:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.052 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.050/0.052/0.056/0.002 ms
```

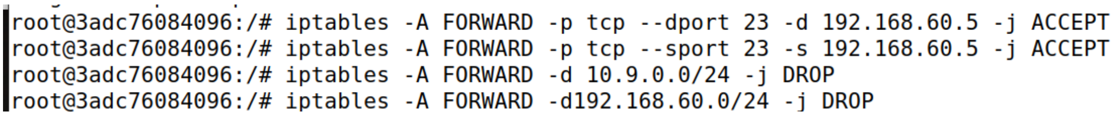
3.内部主机能 ping 外部主机



```
root@186a0891ba92:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.090 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.100 ms
^C
--- 10.9.0.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 0.090/0.095/0.100/0.005 ms
```

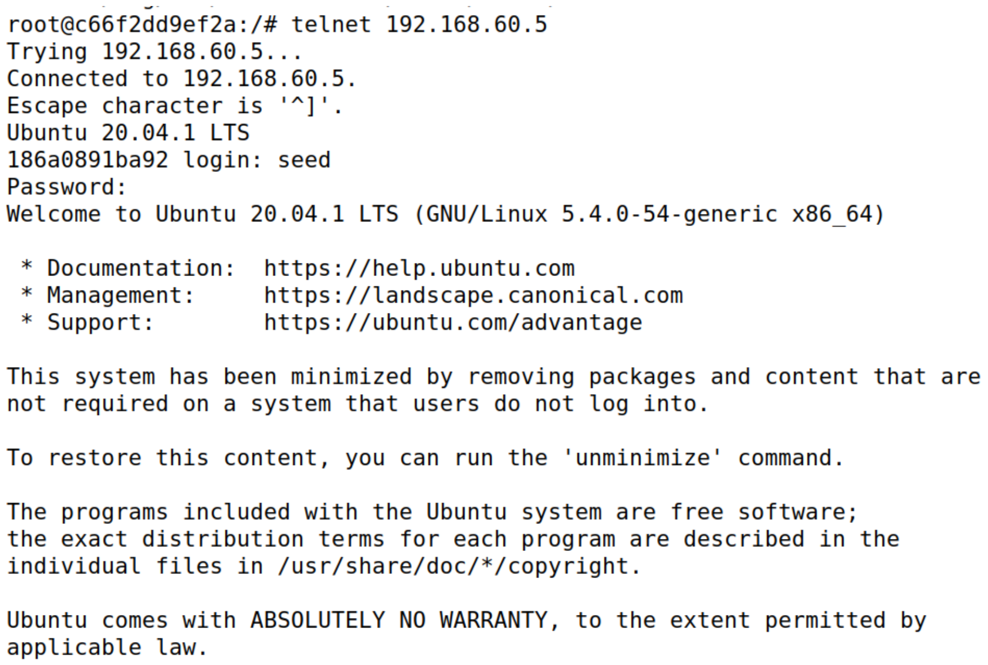
4.其他所有数据包被阻拦，见规则设置最后一条。

task 2.C Protecting Internal Servers



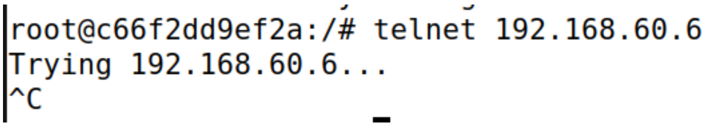
```
root@3adc76084096:/# iptables -A FORWARD -p tcp --dport 23 -d 192.168.60.5 -j ACCEPT
root@3adc76084096:/# iptables -A FORWARD -p tcp --sport 23 -s 192.168.60.5 -j ACCEPT
root@3adc76084096:/# iptables -A FORWARD -d 10.9.0.0/24 -j DROP
root@3adc76084096:/# iptables -A FORWARD -d192.168.60.0/24 -j DROP
```

1.外部主机可以 telnet 登录 192.168.60.5



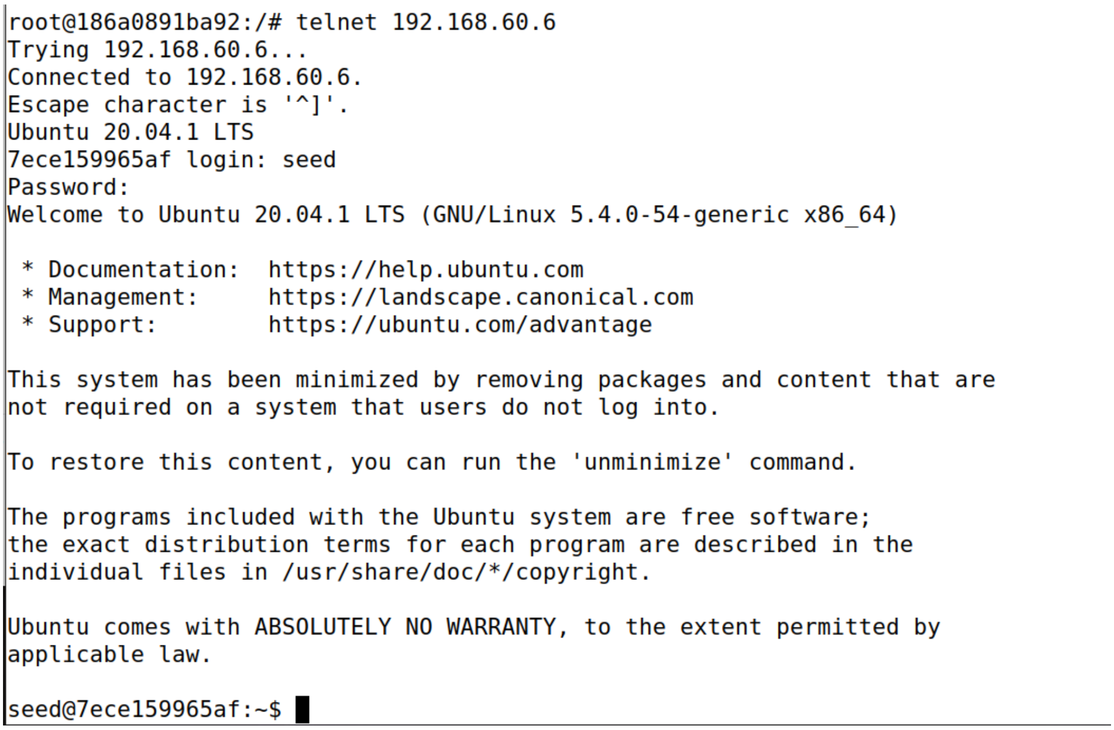
```
root@c66f2dd9ef2a:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
186a0891ba92 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.
```

2.无法登录其他内部主机（如 192.168.60.6）

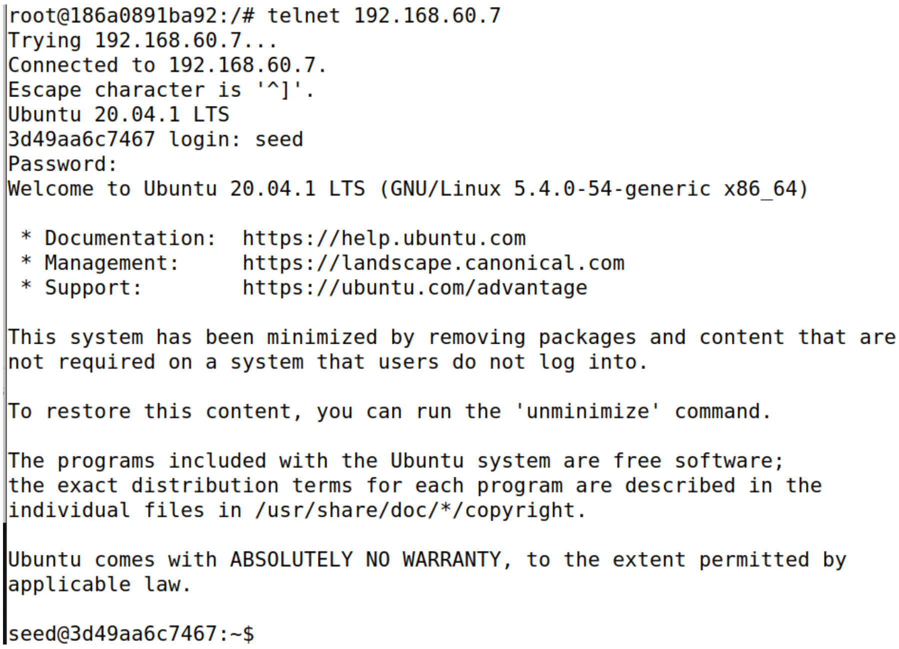


```
root@c66f2dd9ef2a:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
```

3.内部主机可以 telnet 登录其他内部主机

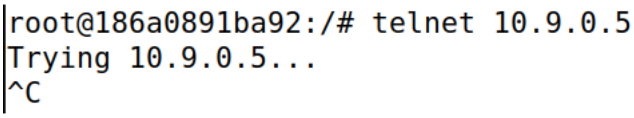


```
root@186a0891ba92:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7ece159965af login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

seed@7ece159965af:~$ █
```



```
root@186a0891ba92:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
3d49aa6c7467 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

seed@3d49aa6c7467:~$
```

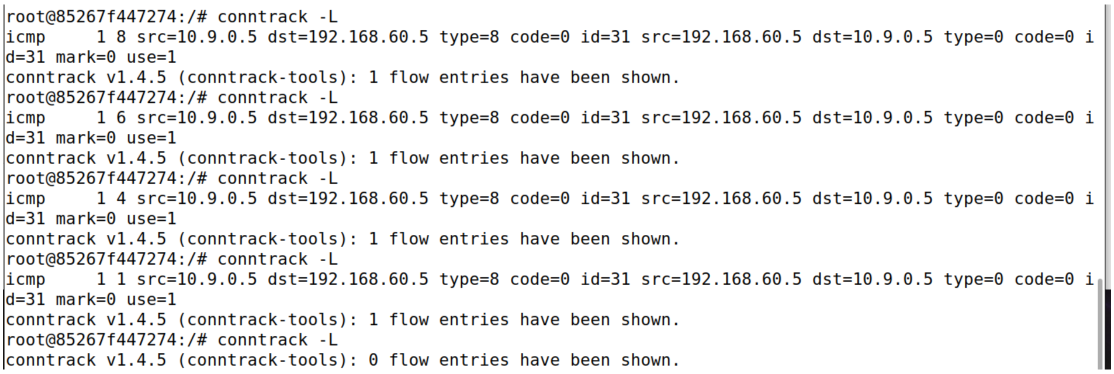
4.内部主机无法 telnet 登录外部主机



```
root@186a0891ba92:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
```

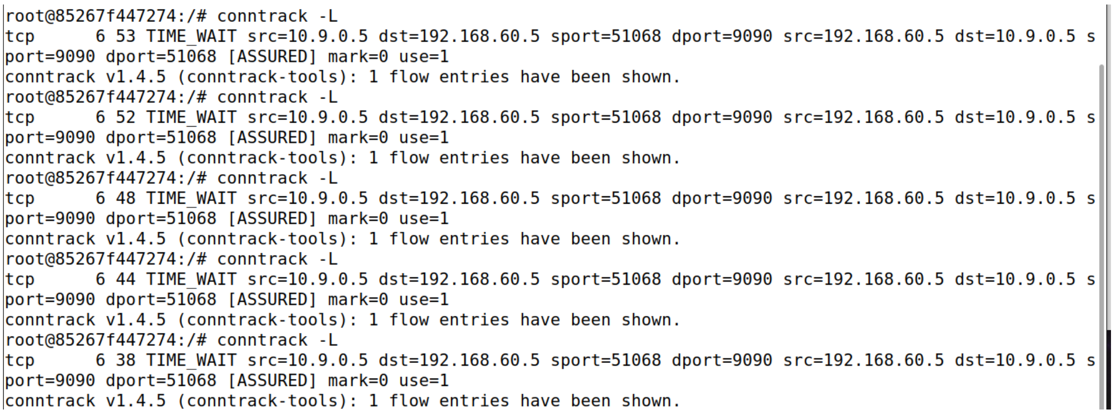
task 3.A Experiment with the Connection Tacking

icmp 连接状态保持 30 秒左右



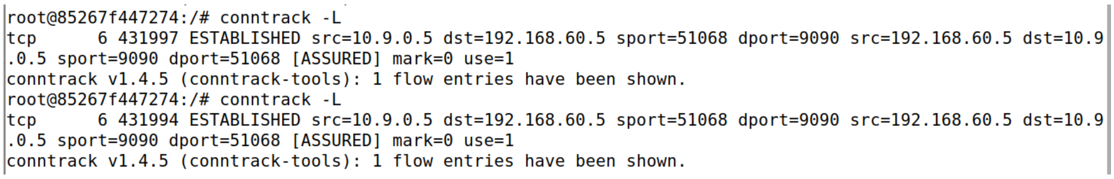
```
root@85267f447274:/# conntrack -L
icmp     1 8 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=31 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 i
d=31 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
icmp     1 6 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=31 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 i
d=31 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
icmp     1 4 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=31 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 i
d=31 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
icmp     1 1 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=31 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 i
d=31 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
```

udp 连接状态保持 60 秒左右



```
root@85267f447274:/# conntrack -L
tcp      6 53 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=51068 dport=9090 src=192.168.60.5 dst=10.9.0.5 s
port=9090 dport=51068 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
tcp      6 52 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=51068 dport=9090 src=192.168.60.5 dst=10.9.0.5 s
port=9090 dport=51068 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
tcp      6 48 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=51068 dport=9090 src=192.168.60.5 dst=10.9.0.5 s
port=9090 dport=51068 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
tcp      6 44 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=51068 dport=9090 src=192.168.60.5 dst=10.9.0.5 s
port=9090 dport=51068 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
tcp      6 38 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=51068 dport=9090 src=192.168.60.5 dst=10.9.0.5 s
port=9090 dport=51068 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

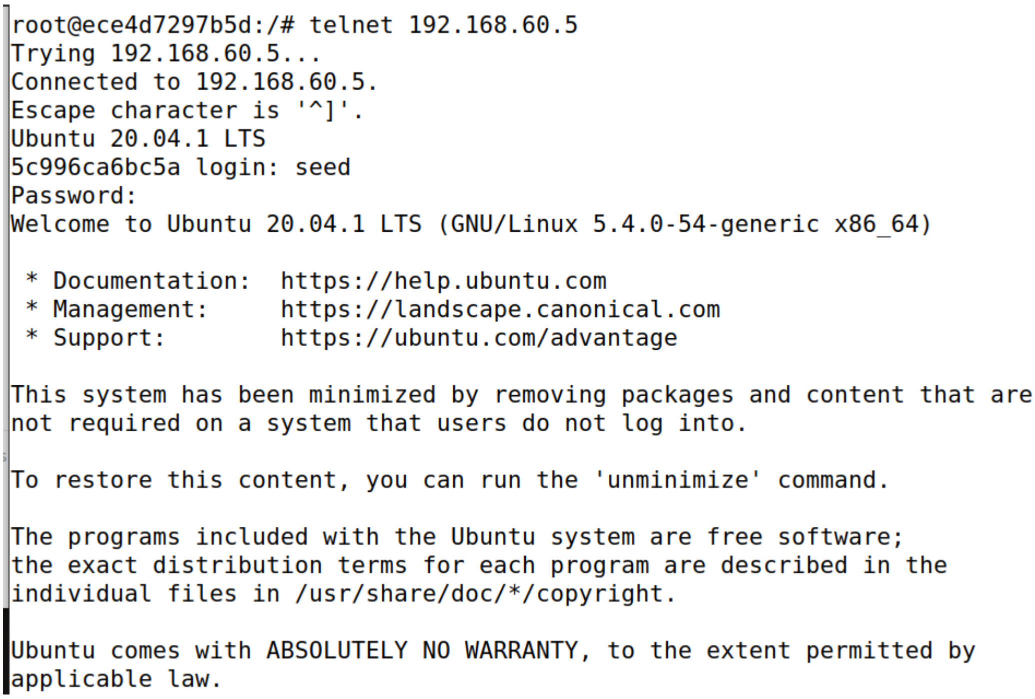
tcp 连接状态保持 432000 秒左右



```
root@85267f447274:/# conntrack -L
tcp      6 431997 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=51068 dport=9090 src=192.168.60.5 dst=10.9
.0.5 sport=9090 dport=51068 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@85267f447274:/# conntrack -L
tcp      6 431994 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=51068 dport=9090 src=192.168.60.5 dst=10.9
.0.5 sport=9090 dport=51068 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

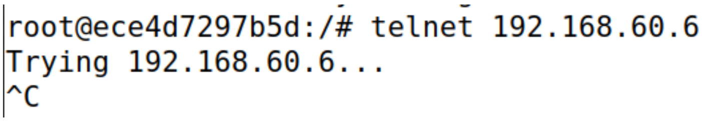
task 3.B Setting Up a Stateful Firewall

1.外部主机能 telnet 连接 192.168.60.5



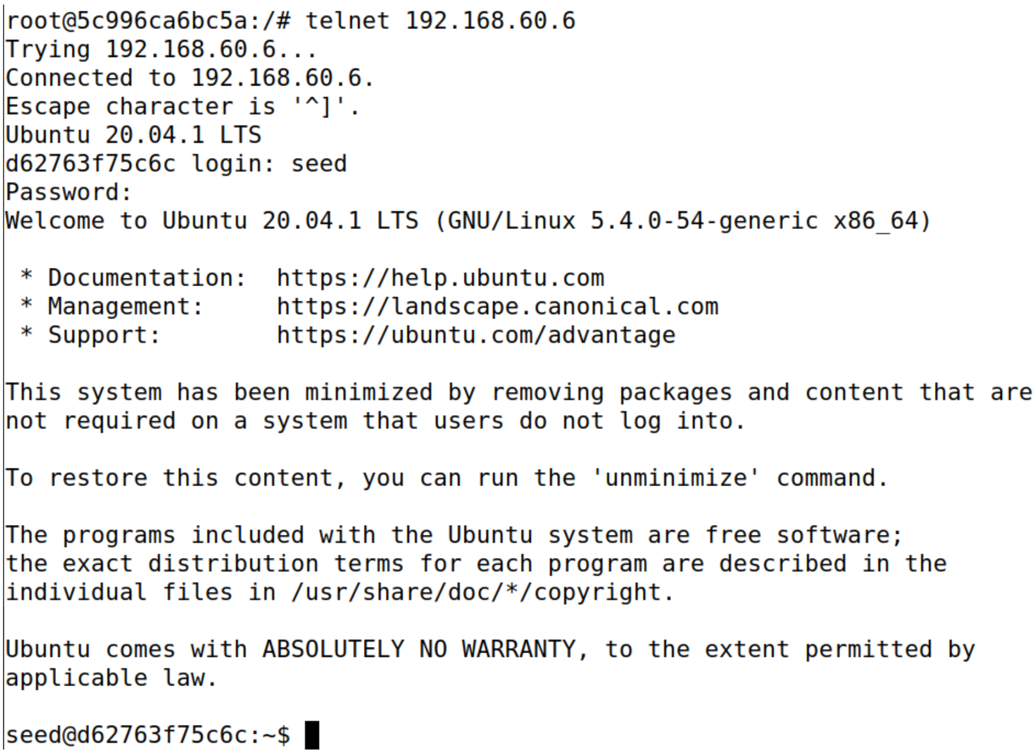
```
root@ece4d7297b5d:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
5c996ca6bc5a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.
```

2.外部主机无法访问内部主机

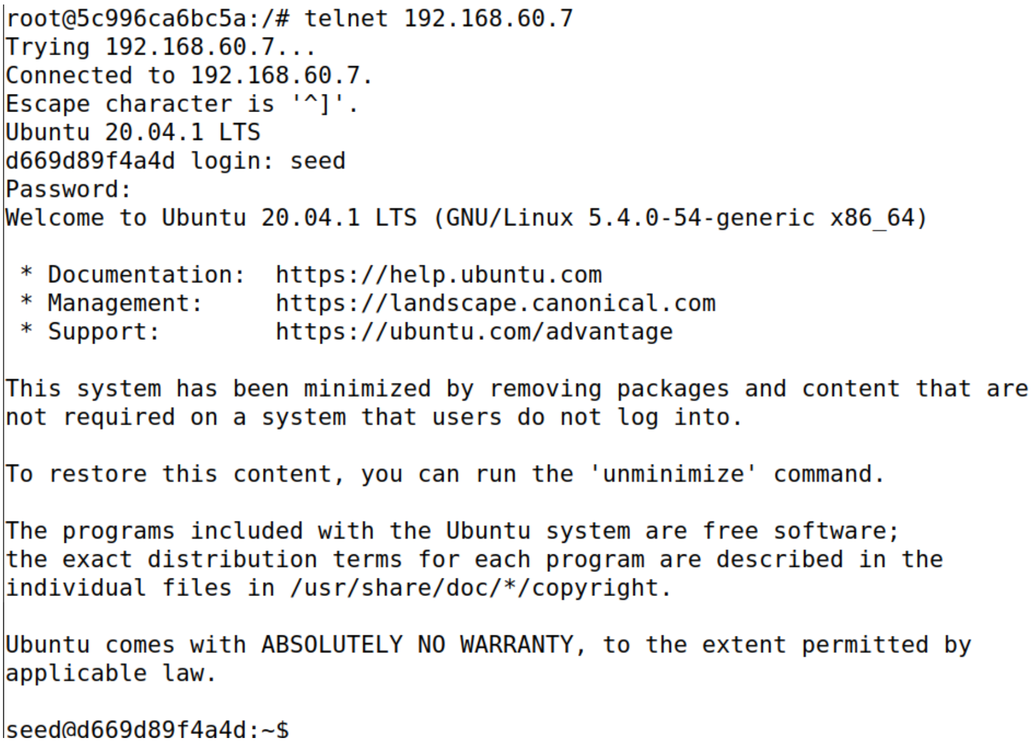


```
root@ece4d7297b5d:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
```

3.内部主机能访问内部主机

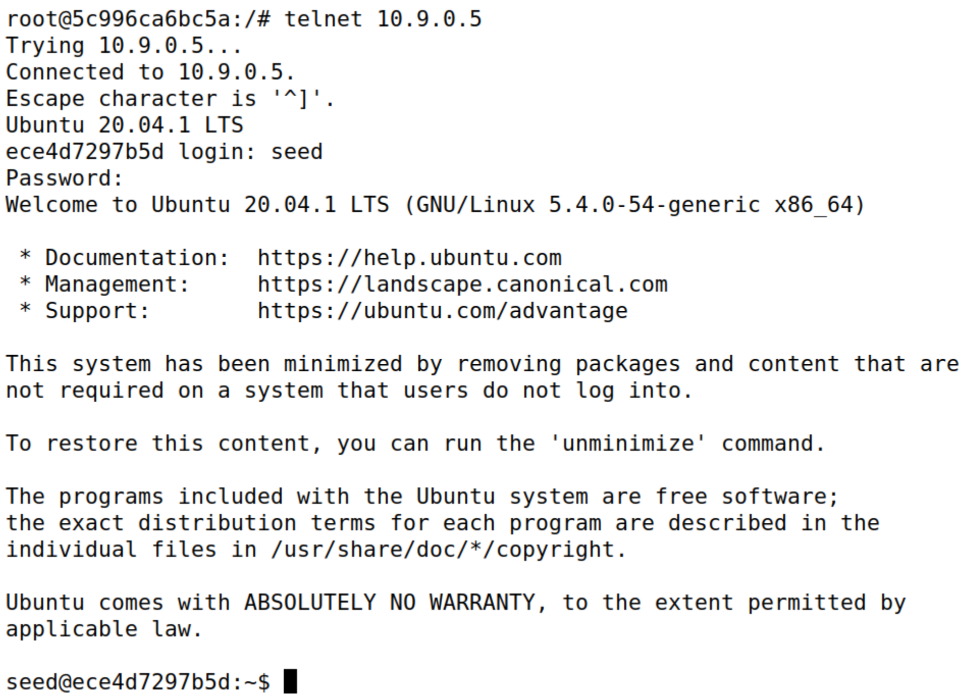


```
root@5c996ca6bc5a:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d62763f75c6c login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

seed@d62763f75c6c:~$
```



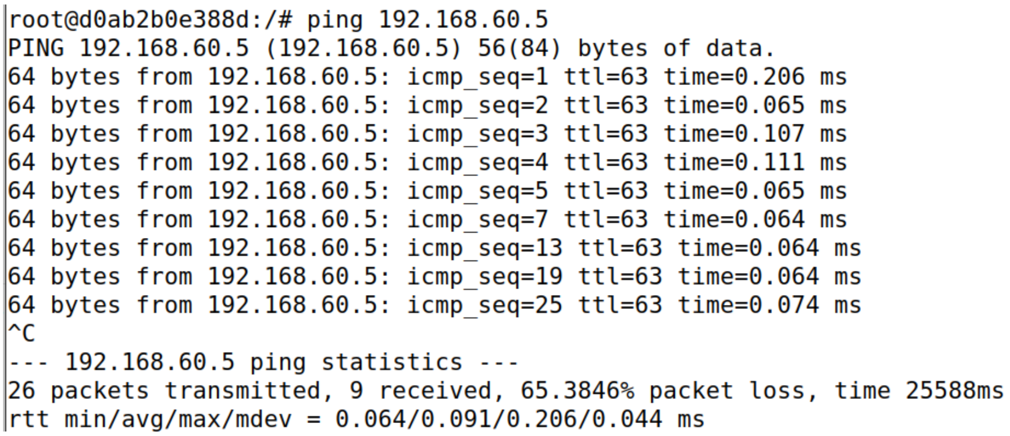
```
root@5c996ca6bc5a:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d669d89f4a4d login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

seed@d669d89f4a4d:~$
```

4.内部主机访问外部主机



```
root@5c996ca6bc5a:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ece4d7297b5d login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

seed@ece4d7297b5d:~$
```

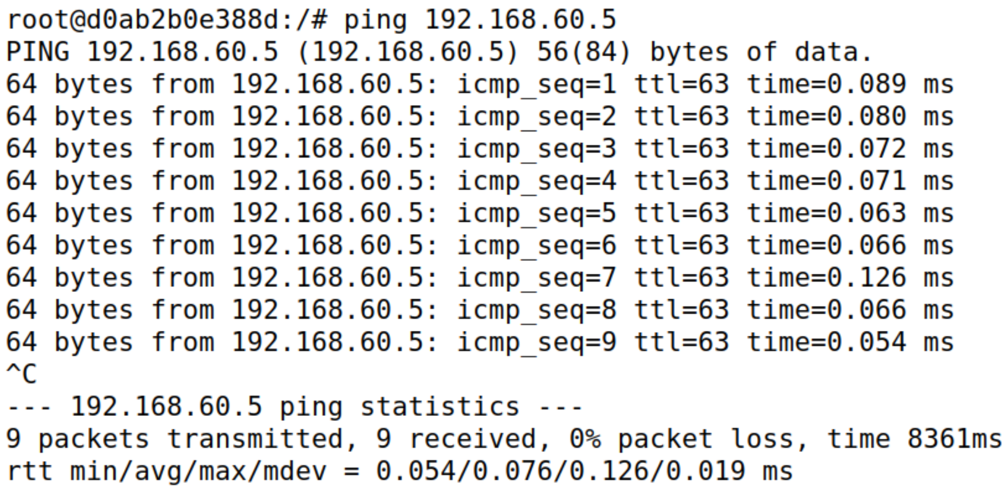
task 4 Limiting Network Traffic



```
root@d0ab2b0e388d:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.206 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.065 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.111 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.065 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.064 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.064 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.064 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.074 ms
^C
--- 192.168.60.5 ping statistics ---
26 packets transmitted, 9 received, 65.3846% packet loss, time 25588ms
rtt min/avg/max/mdev = 0.064/0.091/0.206/0.044 ms
```

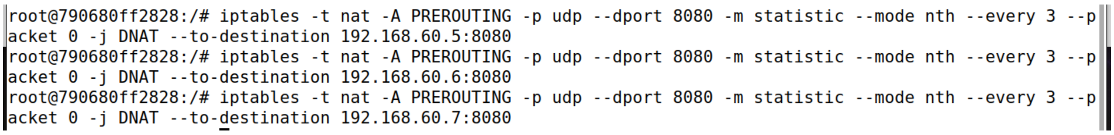
一开始会以正常速度发送，后面每隔 6s 发一个包。

如果只执行第一条命令，会议正常速度发送。



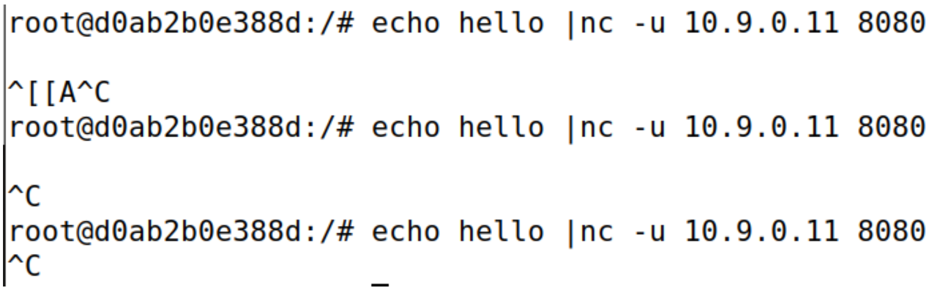
```
root@d0ab2b0e388d:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.089 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.071 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.054 ms
^C
--- 192.168.60.5 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8361ms
rtt min/avg/max/mdev = 0.054/0.076/0.126/0.019 ms
```

task 5 Load Balancing

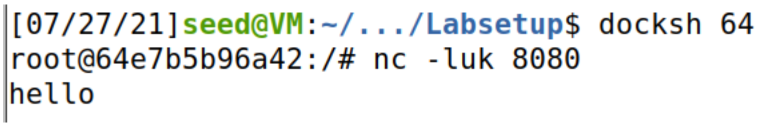


```
root@790680ff2828:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --p
acket 0 -j DNAT --to-destination 192.168.60.5:8080
root@790680ff2828:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --p
acket 0 -j DNAT --to-destination 192.168.60.6:8080
root@790680ff2828:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --p
acket 0 -j DNAT --to-destination 192.168.60.7:8080
```

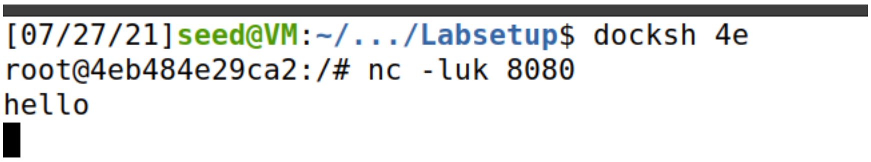
发送三次 hello，发现 host 按顺序各接收到一个



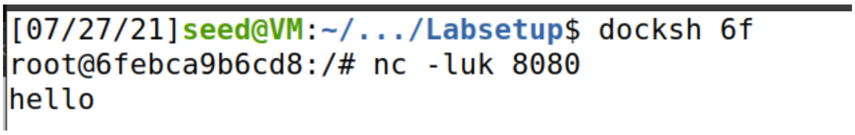
```
root@d0ab2b0e388d:/# echo hello |nc -u 10.9.0.11 8080

^[[A^C
root@d0ab2b0e388d:/# echo hello |nc -u 10.9.0.11 8080

^C
root@d0ab2b0e388d:/# echo hello |nc -u 10.9.0.11 8080
^C
```



```
[07/27/21]seed@VM:~/.../Labsetup$ docksh 64
root@64e7b5b96a42:/# nc -luk 8080
hello
```

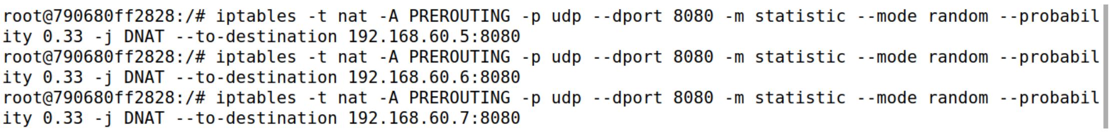


```
[07/27/21]seed@VM:~/.../Labsetup$ docksh 4e
root@4eb484e29ca2:/# nc -luk 8080
hello
```

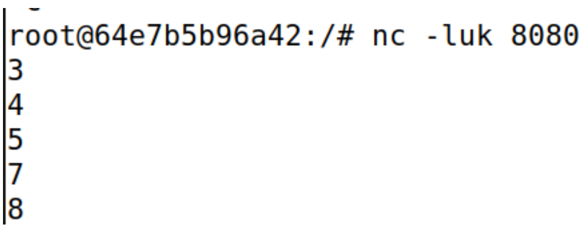


```
[07/27/21]seed@VM:~/.../Labsetup$ docksh 6f
root@6febca9b6cd8:/# nc -luk 8080
hello
```

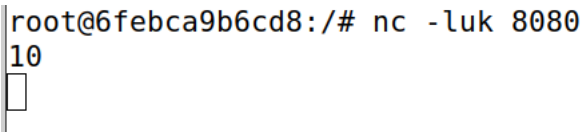
改为随机概率



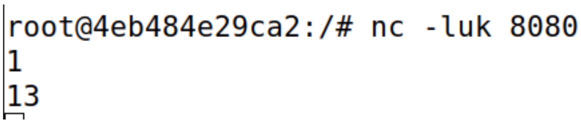
```
root@790680ff2828:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probabil
ity 0.33 -j DNAT --to-destination 192.168.60.5:8080
root@790680ff2828:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probabil
ity 0.33 -j DNAT --to-destination 192.168.60.6:8080
root@790680ff2828:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probabil
ity 0.33 -j DNAT --to-destination 192.168.60.7:8080
```



```
root@64e7b5b96a42:/# nc -luk 8080
3
4
5
7
8
```



```
root@6febca9b6cd8:/# nc -luk 8080
10
```



```
root@4eb484e29ca2:/# nc -luk 8080
1
13
```

在尝试的次数较少的时候差别还比较大，但由于概率都为 0.33，在次数多的时候会趋向于平衡。