Chapter 6 实验报告

57118238 刘欣宇

Task1.A：

加载内核的测试：

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

```
[07/21/21]seed@VM:~/.../kernel_module$ sudo insmod hello.ko
[07/21/21]seed@VM:~/.../kernel_module$ modinfo hello.ko
filename:       /home/seed/Desktop/kernel_module/hello.ko
srcversion:     75A5408065DE2CED836C338
depends:
retpoline:      Y
name:           hello
vermagic:       5.4.0-54-generic SMP mod_unload
```

查看 dmesg：

```
[07/21/21]seed@VM:~/.../kernel_module$ sudo insmod hello.ko
[07/21/21]seed@VM:~/.../kernel_module$ sudo rmmod hello
[07/21/21]seed@VM:~/.../kernel_module$ dmesg
```

```
[90229.699900] Hello World!
[90231.692751] Bye-bye World!.
```

Task1.B：

1、加载内核之前：

```
[07/21/21]seed@VM:~/.../packet_filter$ dig @8.8.8.8 www.example

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 38478
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.                   IN      A

;; AUTHORITY SECTION:
.                       86394   IN      SOA     a.root-servers.net. nstld.verisi
gn-grs.com. 2021072104 1800 900 604800 86400

;; Query time: 56 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jul 21 23:42:31 EDT 2021
;; MSG SIZE  rcvd: 115
```

加载内核之后:

```
^C[07/21/21]seed@VM:~/.../packet_filter$ dig @8.8.8.8 www.example

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

2、

(1)挂载在 NF_INET_PRE_ROUTING 上，所有数据包都经过，在路由判决前被调用:

```
[91991.570920] *** PRE_ROUTING
[91991.571354]     192.168.88.1  --> 192.168.88.255 (UDP)
[91992.077134] *** PRE_ROUTING
[91992.077856]     192.168.88.1  --> 224.0.0.251 (UDP)
[92024.917257] *** PRE_ROUTING
[92024.917892]     192.168.88.2  --> 192.168.88.128 (UDP)
[92024.928116] *** PRE_ROUTING
[92024.928172]     127.0.0.1  --> 127.0.0.53 (UDP)
[92024.936780] *** PRE_ROUTING
[92024.936828]     192.168.88.2  --> 192.168.88.128 (UDP)
[92024.937692] *** PRE_ROUTING
[92024.937743]     127.0.0.53  --> 127.0.0.1 (UDP)
[92024.939545] *** PRE_ROUTING
[92024.939567]     127.0.0.1  --> 127.0.0.53 (UDP)
[92024.945651] *** PRE_ROUTING
[92024.945669]     192.168.88.2  --> 192.168.88.128 (UDP)
[92024.951183] *** PRE_ROUTING
[92024.951196]     192.168.88.2  --> 192.168.88.128 (UDP)
[92024.951442] *** PRE_ROUTING
[92024.951454]     127.0.0.53  --> 127.0.0.1 (UDP)
[92055.923585] The filters are being removed.
```

(2)挂载在 NF_INET_LOCAL_IN 上，经过路由判决后发往本机的数据包将通过该钩子点:

```
[07/22/21]seed@VM:~/.../packet_filter$ sudo dmesg -c
[92216.966140] Registering filters.
[92222.157729] *** LOCAL_IN
[92222.157740]     127.0.0.1  --> 127.0.0.1 (UDP)
[92222.158399] *** Dropping 8.8.8.8 (UDP), port 53
[92227.158773] *** Dropping 8.8.8.8 (UDP), port 53
[92232.160862] *** Dropping 8.8.8.8 (UDP), port 53
[92261.370964] The filters are being removed.
```

(3)挂载在 NF_INET_FORWARD，需要被转发的数据包会通过该钩子点:

```
[07/22/21]seed@VM:~/.../packet_filter$ sudo dmesg -c
[92691.566292] Registering filters.
[92694.918760] *** Dropping 8.8.8.8 (UDP), port 53
[92699.932935] *** Dropping 8.8.8.8 (UDP), port 53
[92704.933976] *** Dropping 8.8.8.8 (UDP), port 53
[92798.575557] The filters are being removed.
```

(4)挂载在 NF_INET_LOCAL_OUT，本机产生的数据包第一个到达的钩子点：

```
[07/22/21]seed@VM:~/.../packet_filter$ sudo dmesg -c
[92868.338467] Registering filters.
[92871.036660] *** LOCAL_OUT
[92871.036678]     127.0.0.1  --> 127.0.0.1 (UDP)
[92871.037361] *** LOCAL_OUT
[92871.037375]     192.168.88.128  --> 8.8.8.8 (UDP)
[92871.037394] *** Dropping 8.8.8.8 (UDP), port 53
[92876.040341] *** LOCAL_OUT
[92876.040379]     192.168.88.128  --> 8.8.8.8 (UDP)
[92876.040463] *** Dropping 8.8.8.8 (UDP), port 53
[92881.038416] *** LOCAL_OUT
[92881.038453]     192.168.88.128  --> 8.8.8.8 (UDP)
[92881.038494] *** Dropping 8.8.8.8 (UDP), port 53
[92924.906806] *** LOCAL_OUT
[92924.906822]     192.168.88.128  --> 192.168.88.2 (UDP)
[92924.915677] *** LOCAL_OUT
[92924.915693]     127.0.0.1  --> 127.0.0.53 (UDP)
[92924.915975] *** LOCAL_OUT
[92924.915991]     192.168.88.128  --> 192.168.88.2 (UDP)
[92924.920401] *** LOCAL_OUT
[92924.920417]     127.0.0.53  --> 127.0.0.1 (UDP)
[92924.920701] *** LOCAL_OUT
[92924.920716]     127.0.0.1  --> 127.0.0.53 (UDP)
[92924.921027] *** LOCAL_OUT
[92924.921043]     192.168.88.128  --> 192.168.88.2 (UDP)
[92924.924556] *** LOCAL_OUT
[92924.924573]     127.0.0.53  --> 127.0.0.1 (UDP)
[92966.433144] The filters are being removed.
```

(5)挂载在 NF_INET_POST_ROUTING，需要被转发或是本机产生的数据包都会经过这个钩子点：

```
[07/22/21]seed@VM:~/.../packet_filter$ sudo dmesg -c
[93019.388483] Registering filters.
[93022.085394] *** POST_ROUTING
[93022.085406]     127.0.0.1  --> 127.0.0.1 (UDP)
[93022.086909] *** Dropping 8.8.8.8 (UDP), port 53
[93027.080926] *** Dropping 8.8.8.8 (UDP), port 53
[93032.082980] *** Dropping 8.8.8.8 (UDP), port 53
[93078.229250] The filters are being removed.
```

3、增加的 ping 过滤代码：

```
unsigned int pingFilter(void *priv, struct sk_buff * skb, const struct
nf_hook_state *state){

            struct iphdr *iph;
            struct tcphdr *tcph;
            iph = ip_hdr(skb);
            tcph = (void *)iph+iph->ihl*4;

            if(iph->protocol == IPPROTO_ICMP && ((((unsigned char *)&iph-
>daddr)[0]==10 && ((unsigned char *)&iph->daddr)[1]==9 && ((unsigned char
*)&iph->daddr)[2]==0 && ((unsigned char *)&iph->daddr)[3]==1)
              ))
              {
                printk(KERN_INFO "Dropping ping packdt to %d.%d.%d.%d\n",
                ((unsigned char *)&iph->daddr)[0],
                ((unsigned char *)&iph->daddr)[1],
                ((unsigned char *)&iph->daddr)[2],
                ((unsigned char *)&iph->daddr)[3]);
                return NF_DROP;
            }else{
                return NF_ACCEPT;
            }
}
```

增加的 telnet 过滤代码：

```
unsigned int telnetFilter(void *priv, struct sk_buff * skb, const struct
nf_hook_state *state){

            struct iphdr *iph;
            struct tcphdr *tcph;
            iph = ip_hdr(skb);
            tcph = (void *)iph+iph->ihl*4;

            if((iph->protocol == IPPROTO_TCP && (tcph->dest == htons(23)))
&& ((((unsigned char *)&iph->daddr)[0]==10 && ((unsigned char *)&iph->daddr)-
[1]==9 && ((unsigned char *)&iph->daddr)[2]==0 && ((unsigned char *)&iph-
>daddr)[3]==1))){
                printk(KERN_INFO "Dropping telent packdt to %d.%d.%d.%d\n",
                ((unsigned char *)&iph->daddr)[0],
                ((unsigned char *)&iph->daddr)[1],
                ((unsigned char *)&iph->daddr)[2],
                ((unsigned char *)&iph->daddr)[3]);
                return NF_DROP;
            }else{
                return NF_ACCEPT;
            }
```

挂载，在挂载时我都选择了 NF_INET_PRE_ROUTING：

```
hook3.hook = telnetFilter;
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 = pingFilter;
hook4.hooknum = NF_INET_PRE_ROUTING;
hook4.pf = PF_INET;
hook4.priority = NF_IP_PRI_FIRST;
nf_register_net_hook(&init_net, &hook4);
```

编译加载内核模块后，在 10.9.0.5 主机上进行 ping 和 telnet 命令：

```
[07/22/21]seed@VM:~/.../Labsetup$ docksh 19
root@190bcc1a5a7b:/# 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 ---
5 packets transmitted, 0 received, 100% packet loss, time 4079ms

root@190bcc1a5a7b:/# telnet 10.9.0.1
Trying 10.9.0.1...
^C
root@190bcc1a5a7b:/#
```

卸载内核模块后查看内核日志缓冲区：

```
[95631.139783] Dropping ping packdt to 10.9.0.1
[95632.149388] Dropping ping packdt to 10.9.0.1
[95633.169693] Dropping ping packdt to 10.9.0.1
[95634.193416] Dropping ping packdt to 10.9.0.1
[95635.219223] Dropping ping packdt to 10.9.0.1
[95642.524370] Dropping telent packdt to 10.9.0.1
[95643.538038] Dropping telent packdt to 10.9.0.1
[95645.554552] Dropping telent packdt to 10.9.0.1
[95649.616320] Dropping telent packdt to 10.9.0.1
[95656.020894] The filters are being removed.
```

Task2.A：

在 router 上设置：

```
root@0261df2e536c:/# iptables -A INPUT -p icmp -j ACCEPT
root@0261df2e536c:/# iptables -A OUTPUT -p icmp -j ACCEPT
root@0261df2e536c:/# iptables -P OUTPUT DROP
root@0261df2e536c:/# iptables -P INPUT DROP
```

此时可以 ping 通 router，但是不能 telnet：

```
root@190bcc1a5a7b:/# 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=0.157 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.387 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.430 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.119 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3049ms
rtt min/avg/max/mdev = 0.119/0.273/0.430/0.136 ms
root@190bcc1a5a7b:/# telnet 10.9.0.11
Trying 10.9.0.11...
^C
```

Task2.B：

规则如下：

```
root@0261df2e536c:/# iptables -A FORWARD -p icmp --icmp-type echo-request -d 10.
9.0.5/24 -j ACCEPT
root@0261df2e536c:/# iptables -A FORWARD -p icmp --icmp-type echo-reply -d 192.1
68.60.0/24 -j ACCEPT
root@0261df2e536c:/# iptables -A FORWARD -p icmp --icmp-type echo-request -d 192
.168.60.0/24 -j DROP
root@0261df2e536c:/# iptables -A INPUT -p icmp -j ACCEPT
root@0261df2e536c:/# iptables -A OUTPUT -p icmp -j ACCEPT
root@0261df2e536c:/# iptables -P FORWARD DROP
```

所有设置显示：

```
root@0261df2e536c:/# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             10.9.0.0/24          icmp echo-request
ACCEPT     icmp --  anywhere             192.168.60.0/24      icmp echo-reply
DROP       icmp --  anywhere             192.168.60.0/24      icmp echo-request

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere
```

从外网 10.9.0.5 ping 网关 10.9.0.11：

```
root@190bcc1a5a7b:/# 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=0.853 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.440 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.468 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.500 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3061ms
rtt min/avg/max/mdev = 0.440/0.565/0.853/0.167 ms
```

从外网 10.9.0.5 ping 内网 192.168.60.5，不通：

```
root@190bcc1a5a7b:/# 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 ---
6 packets transmitted, 0 received, 100% packet loss, time 5101ms
```

从外网 10.9.0.5 telnet 内网 192.168.60.5，不通：

```
root@190bcc1a5a7b:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
```

从内网 192.168.60.5 ping 外网 10.9.0.5，能 ping 通：

```
root@d18be91f2d45:/# 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=0.476 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.507 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.291 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.698 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.286 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=63 time=0.174 ms
^C
--- 10.9.0.5 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5080ms
rtt min/avg/max/mdev = 0.174/0.405/0.698/0.174 ms
```

从内网 192.168.60.5 telnet 外网 10.9.0.5，不通：

```
root@d18be91f2d45:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
```

Task2.C

设置规则：

```
root@0261df2e536c:/# iptables -A FORWARD -p tcp --dport 23 -d 192.168.60.5 -j AC
CEPT
root@0261df2e536c:/# iptables -A FORWARD -p tcp --sport 23 -s 192.168.60.5 -j AC
CEPT
root@0261df2e536c:/# iptables -A FORWARD -d 10.9.0.0/24 -j DROP
root@0261df2e536c:/# iptables -A FORWARD -d 192.168.60.0/24 -j DROP
```

规则列表：

```
root@0261df2e536c:/# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.60.5         tcp dpt:telnet
ACCEPT     tcp  --  192.168.60.5         anywhere             tcp spt:telnet
DROP       all  --  anywhere             10.9.0.0/24
DROP       all  --  anywhere             192.168.60.0/24

Chain OUTPUT (policy DROP)
target     prot opt source               destination
```

外部主机 10.9.0.5 可以 telnet 内部主机 192.168.60.5：

```
root@190bcc1a5a7b:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d18be91f2d45 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
```

外部主机 10.9.0.5 不可以 telnet 内部主机 192.168.60.6，没有响应：

```
root@190bcc1a5a7b:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
```

内部主机 192.168.60.5 可以 telnet 内部主机 192.168.60.6：

```
root@d18be91f2d45:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
639d75c0f0b2 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

内部主机 192.168.60.5 不可以 telnet 外部主机 10.9.0.5：

```
root@d18be91f2d45:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
```

Task3.A：

ICMP，连接的生命周期仅几十秒：

```
root@0261df2e536c:/# conntrack -L
icmp     1 29 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=47 src=192.168.60.5
 dst=10.9.0.5 type=0 code=0 id=47 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
icmp     1 24 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=47 src=192.168.60.5
 dst=10.9.0.5 type=0 code=0 id=47 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
icmp     1 22 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=47 src=192.168.60.5
 dst=10.9.0.5 type=0 code=0 id=47 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
icmp     1 20 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=47 src=192.168.60.5
 dst=10.9.0.5 type=0 code=0 id=47 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
icmp     1 14 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=47 src=192.168.60.5
 dst=10.9.0.5 type=0 code=0 id=47 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
```

UDP，类似于 ICMP，连接的生命周期仅几十秒，一旦一段时间内没有数据包交换，连接将中止：

```
root@0261df2e536c:/# conntrack -L
udp      17 26 src=10.9.0.5 dst=192.168.60.5 sport=46418 dport=9090 [UNREPLIED]
src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=46418 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
udp      17 22 src=10.9.0.5 dst=192.168.60.5 sport=46418 dport=9090 [UNREPLIED]
src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=46418 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
udp      17 21 src=10.9.0.5 dst=192.168.60.5 sport=46418 dport=9090 [UNREPLIED]
src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=46418 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
udp      17 16 src=10.9.0.5 dst=192.168.60.5 sport=46418 dport=9090 [UNREPLIED]
src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=46418 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
```

TCP，可以明显观察到 TCP 连接的生命周期十分长：

```
root@0261df2e536c:/# conntrack -L
tcp      6 431998 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=35702 dport=90
90 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=35702 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
tcp      6 431994 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=35702 dport=90
90 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=35702 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@0261df2e536c:/# conntrack -L
tcp      6 431978 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=35702 dport=90
90 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=35702 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

Task3.B：

```
root@0261df2e536c:/# iptables -F
root@0261df2e536c:/# iptables -A FORWARD -p tcp -m conntrack --ctstate ESTABLISH
ED,RELATED -j ACCEPT
root@0261df2e536c:/# iptables -A FORWARD -p tcp --dport 23 -d 192.168.60.5 --syn
 -m conntrack --ctstate NEW -j ACCEPT
root@0261df2e536c:/# iptables -A FORWARD -p tcp --dport 23 -d 10.9.0.0/24 --syn
-m conntrack --ctstate NEW -j ACCEPT
```

10.9.0.5 telnet 192.168.10.5 成功：

```
[07/22/21]seed@VM:~/.../Labsetup$ docksh fd
root@fd4c56775264:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
327f8c7660f8 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

10.9.0.5 telnet 192.168.10.6 失败:

```
root@fd4c56775264:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
```

内网 192.168.10.5 telnet 10.9.0.5，192.168.60.6 都能成功:

```
root@327f8c7660f8:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fd4c56775264 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

Task4:

有第二条规则时:

```
root@0261df2e536c:/# iptables -A FORWARD -s 10.9.0.5 -m limit \
> --limit 10/minute --limit-burst 5 -j ACCEPT
root@0261df2e536c:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@0261df2e536c:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  hostA-10.9.0.5.net-10.9.0.0  anywhere             limit: avg
 10/min burst 5
DROP       all  --  hostA-10.9.0.5.net-10.9.0.0  anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@0261df2e536c:/#
```

此时超出的会丢弃 5 个:

```
root@190bcc1a5a7b:/# 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=0.507 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.171 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.158 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.174 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.688 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.305 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.305 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.671 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.684 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.300 ms
64 bytes from 192.168.60.5: icmp_seq=37 ttl=63 time=0.313 ms
^C
--- 192.168.60.5 ping statistics ---
38 packets transmitted, 11 received, 71.0526% packet loss, time 37847ms
rtt min/avg/max/mdev = 0.158/0.388/0.688/0.201 ms
```

没有第二条:

```
root@0261df2e536c:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute
--limit-burst 5 -j ACCEPT
root@0261df2e536c:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  hostA-10.9.0.5.net-10.9.0.0  anywhere             limit: avg
 10/min burst 5

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

没有第二条时，限制是无效的:

```
root@190bcc1a5a7b:/# 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=0.173 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.222 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.167 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.352 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.662 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.379 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.339 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.679 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.659 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.344 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.388 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.345 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.199 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.168 ms
^C
--- 192.168.60.5 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13228ms
rtt min/avg/max/mdev = 0.167/0.362/0.679/0.176 ms
```

第二条是需要的，不然对于限制条件外的报文没有处理。

Task5：

Hello 被发送到 192.168.60.5：

```
[07/23/21]seed@VM:~/.../Labsetup$ docksh 1f
root@1fd7944d7677:/# nc -luk 8080
hello
```

设置命令，每三条数据中，第一个发送给 192.168.60.5:8080，第二个发送给 192.168.60.6:8080，第三个发送给 192.168.60.7:8080：

```
root@f930507b1c7a:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-des
tination 192.168.60.5:8080
root@f930507b1c7a:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode nth --every 3 --packet 1 -j DNAT --to-des
tination 192.168.60.6:8080
root@f930507b1c7a:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode nth --every 3 --packet 2 -j DNAT --to-des
tination 192.168.60.7:8080
root@f930507b1c7a:/#
```

结果如图：

```
seed@VM: ~/.../Labsetup
1fd7944d7677  host1-192.168.60.5
f930507b1c7a  seed-router
f5da2b251913  host3-192.168.60.7
9307309820bb  hostA-10.9.0.5
2fd6b41fed77  host2-192.168.60.6
[07/23/21]seed@VM:~/.../Labsetup$ docksh 1f
root@1fd7944d7677:/# nc -luk 8080
hello
different_hello
different_hello
```

```
seed@VM: ~/.../Labsetup
1fd7944d7677  host1-192.168.60.5
f930507b1c7a  seed-router
f5da2b251913  host3-192.168.60.7
9307309820bb  hostA-10.9.0.5
2fd6b41fed77  host2-192.168.60.6
[07/23/21]seed@VM:~/.../Labsetup$ docksh 2f
root@2fd6b41fed77:/# nc -luk 8080
different_hello
```

```
seed@VM: ~/.../Labsetup
f930507b1c7a  seed-router
f5da2b251913  host3-192.168.60.7
9307309820bb  hostA-10.9.0.5
2fd6b41fed77  host2-192.168.60.6
[07/23/21]seed@VM:~/.../Labsetup$ docksh f5
root@f5da2b251913:/# nc -luk 8080
different_hello
```

开放三个端口，设置转发概率大概为 0.33 以期望均衡：

```
root@f930507b1c7a:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode random --probability 0.33 -j DNAT --to-de
stination 192.168.60.5:8080
root@f930507b1c7a:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode random --probability 0.33 -j DNAT --to-de
stination 192.168.60.6:8080
root@f930507b1c7a:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode random --probability 0.33 -j DNAT --to-de
stination 192.168.60.7:8080
```

转发效果：

```
f5da2b251913  host3-192.168.60.7
9307309820bb  hostA-10.9.0.5
2fd6b41fed77  host2-192.168.60.6
[07/23/21]seed@VM:~/.../Labsetup$ docksh 1f
root@1fd7944d7677:/# nc -luk 8080
hello
different_hello
different_hello
different_hello2
different_hello2
```

seed@VM: ~/.../Labsetup

```
f5da2b251913  host3-192.168.60.7
9307309820bb  hostA-10.9.0.5
2fd6b41fed77  host2-192.168.60.6
[07/23/21]seed@VM:~/.../Labsetup$ docksh 2f
root@2fd6b41fed77:/# nc -luk 8080
different_hello
different_hello2
different_hello2
```

```
f5da2b251913  host3-192.168.60.7
9307309820bb  hostA-10.9.0.5
2fd6b41fed77  host2-192.168.60.6
[07/23/21]seed@VM:~/.../Labsetup$ docksh f5
root@f5da2b251913:/# nc -luk 8080
different_hello
different_hello2
```