LAB 6 Firewalls

57118219 贾志豪

Task 1.A

进行 make 操作，make 成功，并载入

```
[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$ lsmod |grep hello
hello                  16384  0
```

查看 message

```
[07/21/21]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
[    0.000000]   Hygon HygonGenuine
[    0.000000]   Centaur CentaurHauls
[    0.000000]   zhaoxin   Shanghai
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regi
sters'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'

...
[  152.493862] IPv6: ADDRCONF(NETDEV_CHANGE): veth6f7236d: link becomes ready
[  152.493906] br-2047ebf597e6: port 1(veth6f7236d) entered blocking state
[  152.493909] br-2047ebf597e6: port 1(veth6f7236d) entered forwarding state
[  152.599566] eth1: renamed from veth2d417d5
[  152.615525] IPv6: ADDRCONF(NETDEV_CHANGE): veth124b405: link becomes ready
[  152.615597] br-7e38166fe98d: port 4(veth124b405) entered blocking state
[  152.615598] br-7e38166fe98d: port 4(veth124b405) entered forwarding state
[ 1226.276589] hello: module license 'unspecified' taints kernel.
[ 1226.276590] Disabling lock debugging due to kernel taint
[ 1226.276617] hello: module verification failed: signature and/or required key
missing - tainting kernel
[ 1226.277128] Hello World!
```

查看信息

```
[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
```

Task 1.B

1.

加载 seedFilter，来过滤发给 114.114.114.114 的 udp 报文

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

访问失败

```
[07/21/21]seed@VM:~/.../Labsetup$ docksh 9a
root@9acd40c00ab7:/# dig @114.114.114.114 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @114.114.114.114 www.example.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

取消之后能够访问，能够成功访问

```
[07/21/21]seed@VM:~/.../packet_filter$ sudo rmmod seedFilter
[07/21/21]seed@VM:~/.../packet_filter$ lsmod | grep seedFilter
```

```
[07/21/21]seed@VM:~/.../Labsetup$ dig @114.114.114.114 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @114.114.114.114 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41165
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.com.        2551    IN      A       93.184.216.34

;; Query time: 36 msec
;; SERVER: 114.114.114.114#53(114.114.114.114)
;; WHEN: Wed Jul 21 23:12:17 EDT 2021
;; MSG SIZE  rcvd: 60
```

2.
集中 hook 函数的区别：

①PRE_ROUTING：
除了混杂模式，所有数据包都将经过这个钩子点，路由判决器之前调用
②LOCAL_IN：
在选路确定之后，且数据包的目的是本地主机
③FORWARD:
目的地是其它主机地数据包,即需要转发的
④LOCAL_OUT：
来自本机进程的数据包在其离开本地主机的过程中
⑤POST_ROUTING：
在数据包离开本地主机“上线”之前，需要被转发或者由本机产生的数据包都会经过这个点

使用 local_out

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

接收到从本机发出的报文

```
[ 1461.541481] *** LOCAL_OUT
[ 1461.541483]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 1461.541617] *** LOCAL_OUT
[ 1461.541619]     10.0.2.15  --> 114.114.114.114 (UDP)
[ 1461.545780] *** LOCAL_OUT
[ 1461.545782]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 1531.160401] *** LOCAL_OUT
[ 1531.160403]     10.0.2.15  --> 34.122.121.32 (TCP)
[ 1532.172784] *** LOCAL_OUT
[ 1532.172808]     10.0.2.15  --> 34.122.121.32 (TCP)
[ 1534.188420] *** LOCAL_OUT
[ 1534.188440]     10.0.2.15  --> 34.122.121.32 (TCP)
[ 1538.413442] *** LOCAL_OUT
[ 1538.413465]     10.0.2.15  --> 34.122.121.32 (TCP)
[ 1538.488429] *** LOCAL_OUT
[ 1538.488449]     10.0.2.15  --> 34.122.121.32 (TCP)
[ 1538.488695] *** LOCAL_OUT
[ 1538.488697]     10.0.2.15  --> 34.122.121.32 (TCP)
[ 1542.464228] *** LOCAL_OUT
[ 1542.464248]     10.0.2.15  --> 34.122.121.32 (TCP)
[ 1542.464375] *** LOCAL_OUT
[ 1542.464377]     10.0.2.15  --> 34.122.121.32 (TCP)
```

设置为 local_in

```
79    hook1.hook = printInfo;
80    hook1.hooknum = NF_INET_LOCAL_IN;
81    hook1.pf = PF_INET;
82    hook1.priority = NF_IP_PRI_FIRST;
83    nf register net hook(&init net, &hook1);
```

接收到，目的地为本机的报文

```
[ 2071.941804]     91.189.94.4  --> 10.0.2.15 (UDP)
[ 2075.681349] *** LOCAL_IN
[ 2075.681352]     127.0.0.1  --> 224.0.0.251 (UDP)
[ 2077.268019] *** LOCAL_IN
[ 2077.268022]     10.0.2.15  --> 224.0.0.251 (UDP)
[ 2097.485064] *** LOCAL_IN
[ 2097.485066]     192.168.60.1  --> 224.0.0.251 (UDP)
[ 2097.515365] *** LOCAL_IN
[ 2097.515367]     172.17.0.1  --> 224.0.0.251 (UDP)
[ 2097.630381] *** LOCAL_IN
[ 2097.630383]     10.9.0.1  --> 224.0.0.251 (UDP)
[ 2138.473104] *** LOCAL_IN
[ 2138.473124]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2138.474014] *** LOCAL_IN
[ 2138.474016]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2146.161719] *** LOCAL_IN
[ 2146.161739]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2146.162031] *** LOCAL_IN
[ 2146.162033]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2146.162150] *** LOCAL_IN
[ 2146.162151]     34.122.121.32  --> 10.0.2.15 (TCP)
```

设置 pre_routing

```
80    hook1.hook = printInfo;
81    hook1.hooknum = NF_INET_PRE_ROUTING;
82    hook1.pf = PF_INET;
83    hook1.priority = NF_IP_PRI_FIRST;
84    nf_register_net_hook(&init_net, &hook1);
```

所有的报文都会经过

```
[ 2362.226594] Registering filters.
[ 2431.149496] *** PRE_ROUTING
[ 2431.149499]     114.114.114.114  --> 10.0.2.15 (UDP)
[ 2431.468532] *** PRE_ROUTING
[ 2431.468557]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2431.469147] *** PRE_ROUTING
[ 2431.469162]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2431.783527] *** PRE_ROUTING
[ 2431.783548]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2431.783593] *** PRE_ROUTING
[ 2431.783600]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2431.784159] *** PRE_ROUTING
[ 2431.784161]     34.122.121.32  --> 10.0.2.15 (TCP)
[ 2479.779158] The filters are being removed.
```

设置为 post_routing

```
81    hook1.hook = printInfo;
82    hook1.hooknum = NF_INET_POST_ROUTING;
83    hook1.pf = PF_INET;
84    hook1.priority = NF_IP_PRI_FIRST;
85    nf register net hook(&init net, &hook1);
```

本机产生的和转发的数据包会被接收

```
[ 2816.196601] *** POST_ROUTING
[ 2816.196602]     10.0.2.15  --> 185.199.111.153 (TCP)
[ 2816.196878] wow
[ 2816.196879] *** POST_ROUTING
[ 2816.196894]     10.0.2.15  --> 185.199.111.153 (TCP)
[ 2816.197688] wow
[ 2816.197689] *** POST_ROUTING
[ 2816.197691]     10.0.2.15  --> 185.199.111.153 (TCP)
[ 2816.198659] wow
[ 2816.198660] *** POST_ROUTING
[ 2816.198661]     10.0.2.15  --> 185.199.111.153 (TCP)
[ 2816.198902] wow
[ 2816.198903] *** POST_ROUTING
[ 2816.198904]     10.0.2.15  --> 185.199.111.153 (TCP)
[ 2816.199664] wow
[ 2816.199665] *** POST_ROUTING
[ 2816.199667]     10.0.2.15  --> 185.199.111.153 (TCP)
[ 2816.199902] wow
[ 2816.199903] *** POST_ROUTING
[ 2816.199904]     10.0.2.15  --> 185.199.111.153 (TCP)
[ 2816.201107] wow
[ 2816.201109] *** POST_ROUTING
[ 2816.201111]     10.0.2.15  --> 185.199.111.153 (TCP)
```

Forward 设置

```
 81    hook1.hook = printInfo;
 82    hook1.hooknum = NF_INET_FORWARD;
 83    hook1.pf = PF_INET;
 84    hook1.priority = NF_IP_PRI_FIRST;
 85    nf_register_net_hook(&init_net, &hook1);
```

Router 得到转发报文，捕获数据

A ping 192.168.60.5，

```
root@b901c97e6d12:/# 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=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.096 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.073 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.074 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.079 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.068 ms
^C
--- 192.168.60.5 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6152ms
rtt min/avg/max/mdev = 0.067/0.082/0.122/0.018 ms
root@b901c97e6d12:/#
```

会接收转发的报文

```
[ 3077.656553] *** FORWARD
[ 3077.656555]     10.9.0.5  --> 192.168.60.5 (ICMP)
[ 3077.656569] wow
[ 3077.656569] *** FORWARD
[ 3077.656570]     10.9.0.5  --> 192.168.60.5 (ICMP)
[ 3077.656583] wow
[ 3077.656583] *** FORWARD
[ 3077.656584]     192.168.60.5  --> 10.9.0.5 (ICMP)
[ 3077.656590] wow
[ 3077.656590] *** FORWARD
[ 3077.656591]     192.168.60.5  --> 10.9.0.5 (ICMP)
[ 3078.687834] wow
[ 3078.687836] *** FORWARD
[ 3078.687838]     10.9.0.5  --> 192.168.60.5 (ICMP)
[ 3078.687851] wow
[ 3078.687852] *** FORWARD
[ 3078.687853]     10.9.0.5  --> 192.168.60.5 (ICMP)
[ 3078.687864] wow
[ 3078.687865] *** FORWARD
[ 3078.687866]     192.168.60.5  --> 10.9.0.5 (ICMP)
[ 3078.687870] wow
[ 3078.687870] *** FORWARD
[ 3078.687871]     192.168.60.5  --> 10.9.0.5 (ICMP)
```

3.

选择 pre_routing，所有数据报都将经过这个钩子点

Block telnet 10.9.0.1

代码如下：

```
78 unsigned int blocktelnet(void *priv, struct sk_buff *skb,
79                          const struct nf_hook_state *state)
80 {
81    struct iphdr *iph;
82    struct tcphdr *tcph;
83   // struct udphdr *udph;
84
85    u16  port   = 23;
86    char ip[16] = "10.9.0.1";
87    u32  ip_addr;
88
89    if (!skb) return NF_ACCEPT;
90
91    iph = ip_hdr(skb);
92    // Convert the IPv4 address from dotted decimal to 32-bit binary
93    in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);
94   // tcph=(void*)iph+iph->ihl*4;
95    //udph = udp_hdr(skb);
96    if (iph->protocol == IPPROTO_TCP )
97    {
98         tcph = tcp_hdr(skb);
99         if(tcph->dest==htons(23) && iph->daddr == ip_addr)
100         {
101               printk(KERN_WARNING "*** Dropping %pI4 (telnet), port %d\n",
    &(iph->daddr), port);
102                     return NF_DROP;
103         }
104    }
105    return NF_ACCEPT;
```

Hook 挂钩子

```
149    hook3.hook = blocktelnet;
150    hook3.hooknum = NF_INET_PRE_ROUTING;
151    hook3.pf = PF_INET;
152    hook3.priority = NF_IP_PRI_FIRST;
153    nf_register_net_hook(&init_net, &hook3);
```

结果如下：telnet 失败

```
root@634aaeb37176:/# telnet 10.9.0.1
Trying 10.9.0.1...
telnet: Unable to connect to remote host: Connection timed out
root@634aaeb37176:/#
```

Block ping

代码如下

```
108 unsigned int blockping(void *priv, struct sk_buff *skb,
109                        const struct nf_hook_state *state)
110 {
111    struct iphdr *iph;
112    struct iphdr *tcph;
113    struct udphdr *udph;
114
115    u16  port   = 53;
116    char ip[16] = "10.9.0.1";
117    u32  ip_addr;
118
119    if (!skb) return NF_ACCEPT;
120
121    iph = ip_hdr(skb);
122    // Convert the IPv4 address from dotted decimal to 32-bit binary
123    in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);
124
125    if (iph->protocol == IPPROTO_ICMP && iph->daddr == ip_addr)
126    {
127        printk(KERN_WARNING "*** Dropping %pI4 (icmp), port %d\n", &(iph-
    >daddr), port);
128            return NF_DROP;
129    }
130    return NF_ACCEPT;
131 }
```

挂钩子

```
155    hook4.hook = blockping;
156    hook4.hooknum = NF_INET_PRE_ROUTING;
157    hook4.pf = PF_INET;
158    hook4.priority = NF_IP_PRI_FIRST;
159    nf_register_net_hook(&init_net, &hook4);
```

结果如下，无响应

```
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.

^C
--- 10.9.0.1 ping statistics ---
248 packets transmitted, 0 received, 100% packet loss, time 253368ms

root@1b2d75c4969e:/#
```

Task 2.A

设置 iptables，双向

```
root@f0177cc39d4b:/# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@f0177cc39d4b:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@f0177cc39d4b:/# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCE
PT
root@f0177cc39d4b:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEP
T
root@f0177cc39d4b:/# iptables -P INPUT DROP
root@f0177cc39d4b:/# iptables -P OUTPUT DROP
```

Ping 可以正常进行

```
root@b901c97e6d12:/# 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=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.059 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.049/0.056/0.060/0.005 ms
```

Telnet 不通

```
root@b901c97e6d12:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
```

Task 2.B

设置 iptables 规则如下：

```
 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
    0     0 DROP       icmp --  eth1   *       0.0.0.0/0            0.0.0.0/0           icmptype
 0
   82  6888 DROP       icmp --  *      eth1    0.0.0.0/0            0.0.0.0/0           icmptype
 8
    6   504 ACCEPT     icmp --  eth0   *       0.0.0.0/0            0.0.0.0/0           icmptype
 0
    6   504 ACCEPT     icmp --  *      eth0    0.0.0.0/0            0.0.0.0/0           icmptype
 8
    0     0 ACCEPT     icmp --  eth1   *       0.0.0.0/0            0.0.0.0/0           icmptype
 8
    0     0 ACCEPT     icmp --  *      eth1    0.0.0.0/0            0.0.0.0/0           icmptype
 0
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0            0.0.0.0/0           icmptype
 8
    0     0 ACCEPT     icmp --  *      eth0    0.0.0.0/0            0.0.0.0/0           icmptype
 0
```

```
root@f0177cc39d4b:/# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

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

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

内部主机 ping 外，可以连通

```
root@634aaeb37176:/# 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=0.151 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.066 ms
^C
--- 10.9.0.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.066/0.108/0.151/0.042 ms
```

外部主机 ping 内部主机，ping 不通

```
root@b901c97e6d12:/# 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 ---
4 packets transmitted, 0 received, 100% packet loss, time 3085ms
```

10.9.0.5 ping router 可以通

```
root@b901c97e6d12:/# 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=0.066 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=0.049 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.055 ms
64 bytes from 10.9.0.11: icmp_seq=5 ttl=64 time=0.054 ms
64 bytes from 10.9.0.11: icmp_seq=6 ttl=64 time=0.049 ms
64 bytes from 10.9.0.11: icmp_seq=7 ttl=64 time=0.076 ms
64 bytes from 10.9.0.11: icmp_seq=8 ttl=64 time=0.049 ms
64 bytes from 10.9.0.11: icmp_seq=9 ttl=64 time=0.049 ms
64 bytes from 10.9.0.11: icmp_seq=10 ttl=64 time=0.049 ms
^C
--- 10.9.0.11 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9219ms
rtt min/avg/max/mdev = 0.049/0.054/0.076/0.008 ms
```

Telnet 都不通

```
root@b901c97e6d12:/# telnet 192.168.60.5
Trying 192.168.60.5...
```

```
root@634aaeb37176:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

Task 2.C

设置如下规则

```
root@f0177cc39d4b:/# iptables -A FORWARD -p tcp -s 192.168.60.5 --sport 23 -j ACCEPT
root@f0177cc39d4b:/# iptables -A FORWARD -p tcp -d 192.168.60.5 --dport 23 -j ACCEPT
root@f0177cc39d4b:/# iptables -P FORWARD DROP
```

10.9.0.5 可以 telnet 192.168.60.5

```
root@b901c97e6d12:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@b901c97e6d12:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
634aaeb37176 login: seed
```

10.9.0.5 Telnet 其他不通

```
634aaeb37176 login: seed^CConnection closed by foreign host.
root@b901c97e6d12:/# telnet 192.168.60.6
Trying 192.168.60.6...
```

内部 telnet 外部不通

```
root@1b2d75c4969e:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

内部可以互通

```
root@1b2d75c4969e:/# ping 192.168.60.7
PING 192.168.60.7 (192.168.60.7) 56(84) bytes of data.
64 bytes from 192.168.60.7: icmp_seq=1 ttl=64 time=0.090 ms
64 bytes from 192.168.60.7: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 192.168.60.7: icmp_seq=3 ttl=64 time=0.044 ms
^C
--- 192.168.60.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2041ms
rtt min/avg/max/mdev = 0.044/0.061/0.090/0.020 ms
```

Task 3.A

建立相关连接，结果如下：

Icmp 连接能持续 120s

```
root@f0177cc39d4b:/# conntrack -L
icmp     1 29 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=96 src=192.168.60.5
 dst=10.9.0.5 type=0 code=0 id=96 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

Udp 连接能持续 30s 左右

```
root@f0177cc39d4b:/# conntrack -L
tcp      6 235 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=23 dport=59490 sr
c=192.168.60.5 dst=10.9.0.5 sport=59490 dport=23 mark=0 use=1
udp      17 23 src=10.9.0.5 dst=192.168.60.5 sport=59106 dport=9090 [UNREPLIED]
src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59106 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
```

Tcp 能持续 120s 左右

```
root@f0177cc39d4b:/# conntrack -L
tcp      6 431997 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=36256 dport=90
90 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=36256 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

断开后

```
root@f0177cc39d4b:/# conntrack -L
tcp      6 118 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=36256 dport=9090 sr
c=192.168.60.5 dst=10.9.0.5 sport=9090 dport=36256 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

Task 3.B

设置如下的规则：

```
root@f0177cc39d4b:/# iptables -A FORWARD -p tcp -d 192.168.60.5 --dport 23 -j ACCEPT
root@f0177cc39d4b:/# iptables -A FORWARD -p tcp -s 192.168.60.5 --sport 23 -j ACCEPT
root@f0177cc39d4b:/# iptables -A FORWARD -p tcp -m conntrack --ctstate ESTABLISHED,R
ELATED -j ACCEPT

root@f0177cc39d4b:/# iptables -A FORWARD -p tcp --dport 23 --syn -m conntrack --ctst
ate NEW -j ACCEPT
```

10.9.0.5 Telnet 192.168.60.5 可以通

```
root@b901c97e6d12:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
634aaeb37176 login:
```

192.168.60.5 telnet 10.9.0.5 可行

```
root@634aaeb37176:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b901c97e6d12 login:
```

Task 4

设置如下的限制规则：

```
root@f0177cc39d4b:/# iptables -A FORWARD -s 10.9.0.5 -m limit \
> --limit 10/minute --limit-burst 5 -j ACCEPT
root@f0177cc39d4b:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@f0177cc39d4b:/#
```

一开始 5 个报速度很快，后面速度变慢，除开前 5 个包，后面大概 1 分钟 10 个包：

```
root@b901c97e6d12:/# 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=0.155 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.054 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.068 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.090 ms
64 bytes from 192.168.60.5: icmp_seq=37 ttl=63 time=0.058 ms
64 bytes from 192.168.60.5: icmp_seq=42 ttl=63 time=0.076 ms
^C
--- 192.168.60.5 ping statistics ---
47 packets transmitted, 12 received, 74.4681% packet loss, time 47214ms
rtt min/avg/max/mdev = 0.054/0.073/0.155/0.026 ms
```

去掉第二条规则后，所有报文全部接受，因为第一条规则被排除的默认处理为通过：

```
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.059 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.054 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.071 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.057 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.059 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.087 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.056 ms
64 bytes from 192.168.60.5: icmp_seq=22 ttl=63 time=0.065 ms
64 bytes from 192.168.60.5: icmp_seq=23 ttl=63 time=0.070 ms
^C
--- 192.168.60.5 ping statistics ---
23 packets transmitted, 23 received, 0% packet loss, time 22510ms
rtt min/avg/max/mdev = 0.054/0.068/0.115/0.017 ms
```

Task 5

192.168.60.5 会接收到 hello，发送三条只会接收到 1 条：

```
[07/22/21]seed@VM:~/.../Labsetup$ dockps
1b2d75c4969e  host2-192.168.60.6
b901c97e6d12  hostA-10.9.0.5
f0177cc39d4b  seed-router
634aaeb37176  host1-192.168.60.5
2eab082c4bf1  host3-192.168.60.7
[07/22/21]seed@VM:~/.../Labsetup$ docksh 63
root@634aaeb37176:/# nc -luk 8080
hello
```

```
seed@VM: ~/.../Labsetup
[07/22/21]seed@VM:~/.../Labsetup$ dockps
1b2d75c4969e  host2-192.168.60.6
b901c97e6d12  hostA-10.9.0.5
f0177cc39d4b  seed-router
634aaeb37176  host1-192.168.60.5
2eab082c4bf1  host3-192.168.60.7
[07/22/21]seed@VM:~/.../Labsetup$ docksh b9
root@b901c97e6d12:/# echo hello | nc -u 10.9.0.11 8080
```

设置每3个包为一个循环,第一条发给192.168.60.5,第二条发给192.168.160.6,第三条发给192.168.60.7

```
root@f0177cc39d4b:/# iptables -t nat -A PREROUTING -p udp --dport 8080 \
> -m statistic --mode nth --every 3 --packet 0 \
> -j DNAT --to-destination 192.168.60.5:8080
root@f0177cc39d4b:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic
--mode nth --every 3 --packet 1 -j DNAT --to-destination 192.168.60.6:8080
root@f0177cc39d4b:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic
--mode nth --every 3 --packet 2 -j DNAT --to-destination 192.168.60.7:8080
```

发了几条 echo 包，大致数量关系相等，随着次数的增加会参差不齐，第一条接受的会收到比其他两者较多一点的报文

```
root@634aaeb37176:/# nc -luk 8080
hello
hello
```

```
root@1b2d75c4969e:/# nc -luk 8080
hello
hello
```

```
root@2eab082c4bf1:/# nc -luk 8080
hello
hello
```

设置分发的概率为0.3

```
root@f0177cc39d4b:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic
--mode random --probability 0.3 -j DNAT --to-destination 192.168.60.5:8080
root@f0177cc39d4b:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic
--mode random --probability 0.3 -j DNAT --to-destination 192.168.60.6:8080
root@f0177cc39d4b:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic
--mode random --probability 0.3 -j DNAT --to-destination 192.168.60.7:8080
```

随着数量不断增加时，三者接受到的报文数量趋于相同

```
root@634aaeb37176:/# nc -luk 8080
hello
hello
hello
hello
hello
hello
```

```
root@1b2d75c4969e:/# nc -luk 8080
hello
hello
hello
hello
hello
hello
```

```
root@2eab082c4bf1:/# nc -luk 8080
hello
hello
hello
hello
hello
hello
```