Firewall Exploration Lab

57118135 许皓钦

Task1

Task1.A

根据实验所给代码进行 make。

```
[07/25/21]seed@VM:~$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/hello.o
  Building modules, stage 2.
  MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/seed/hello.o
see include/linux/module.h for more information
  CC [M]  /home/seed/hello.mod.o
  LD [M]  /home/seed/hello.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[07/25/21]seed@VM:~$
```

make 后得到的全部文件如下。

用 insmod 命令载入模块，用 lsmod 命令查看，用 rmmod 命令将其从内核中卸载，用 dmesg 命令查看日志。

```
[07/25/21]seed@VM:~$ sudo insmod hello.ko
[07/25/21]seed@VM:~$ lsmod | grep hello
hello                  16384  0
[07/25/21]seed@VM:~$ sudo rmmod hello
[07/25/21]seed@VM:~$ dmesg
```

成功出现了期望的结果。

```
[ 4857.959321] Hello World!
[ 4882.062047] Bye-bye World!.
```

Task1.B

Task1.B.1

用所给代码进行 make。

```
[07/25/21]seed@VM:~$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/seedFilter.mod.o
  LD [M]  /home/seed/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[07/25/21]seed@VM:~$
```

用 insmod 命令载入模块，用 lsmod 命令查看。

```
[07/25/21]seed@VM:~$ sudo insmod seedFilter.ko
[07/25/21]seed@VM:~$ lsmod | grep seedFilter
seedFilter             16384  0
[07/25/21]seed@VM:~$
```

发送请求，发现请求被阻塞，达到预期结果。

```
[07/25/21]seed@VM:~/Desktop$ 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

[07/25/21]seed@VM:~/Desktop$
```

Task1.B.2

将 printfo 挂在不同 hook 上，先修改第 78 行处代码，然后重新 make

并加载内核，再发送请求，最后看日志，结果如下。

NF_INET_LOCAL_OUT：在数据包以其方式离开主机之前调用。

```
77    hook1.hook = printInfo;
78    hook1.hooknum = NF_INET_LOCAL_OUT;
79    hook1.pf = PF_INET;
80    hook1.priority = NF_IP_PRI_FIRST;
```

```
[07/25/21]seed@VM:~$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/seedFilter.mod.o
  LD [M]  /home/seed/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[07/25/21]seed@VM:~$ sudo insmod seedFilter.ko
[07/25/21]seed@VM:~$ lsmod | grep seedFilter
seedFilter             16384  0
[07/25/21]seed@VM:~$
```

```
[07/25/21]seed@VM:~/Desktop$ 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

[07/25/21]seed@VM:~/Desktop$
```

```
[ 8202.266500] *** Dropping 8.8.8.8 (UDP), port 53
[ 8204.104175] *** LOCAL_OUT
[ 8204.104176]     192.168.43.35  --> 192.168.43.1 (UDP)
[ 8204.127242] *** LOCAL_OUT
[ 8204.127244]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 8204.127348] *** LOCAL_OUT
[ 8204.127349]     192.168.43.35  --> 192.168.43.1 (UDP)
[ 8204.148540] *** LOCAL_OUT
[ 8204.148542]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 8205.182237] *** LOCAL_OUT
[ 8205.182239]     192.168.43.35  --> 224.0.0.251 (UDP)
[ 8207.268125] *** LOCAL_OUT
[ 8207.268127]     192.168.43.35  --> 8.8.8.8 (UDP)
[ 8207.268138] *** Dropping 8.8.8.8 (UDP), port 53
[ 8212.265268] *** LOCAL_OUT
[ 8212.265269]     192.168.43.35  --> 8.8.8.8 (UDP)
[ 8212.265279] *** Dropping 8.8.8.8 (UDP), port 53
[ 8220.101275] *** LOCAL_OUT
[ 8220.101276]     192.168.43.35  --> 192.168.43.1 (UDP)
```

NF_INET_PRE_ROUTING:在做出任何路由决策之前调用。

```
76
77    hook1.hook = printInfo;
78    hook1.hooknum = NF_INET_PRE_ROUTING;
79    hook1.pf = PF_INET;
80    hook1.priority = NF_IP_PRI_FIRST;
81    nf_register_net_hook(&init_net, &hook1);
82
83    hook2.hook = blockUDP;
```

```
[ 8440.001197] *** Dropping 8.8.8.8 (UDP), port 53
[ 8444.440209] *** PRE_ROUTING
[ 8444.440211]     192.168.43.1  --> 192.168.43.35 (UDP)
[ 8444.441098] *** PRE_ROUTING
[ 8444.441099]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 8444.466461] *** PRE_ROUTING
[ 8444.466463]     192.168.43.1  --> 192.168.43.35 (UDP)
[ 8444.466668] *** PRE_ROUTING
[ 8444.466669]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 8444.997828] *** Dropping 8.8.8.8 (UDP), port 53
[ 8445.263108] *** PRE_ROUTING
[ 8445.263110]     192.168.43.35  --> 224.0.0.251 (UDP)
[ 8450.000378] *** Dropping 8.8.8.8 (UDP), port 53
[ 8496.306068] *** PRE_ROUTING
[ 8496.306090]     192.168.43.1  --> 192.168.43.35 (UDP)
```

NF_INET_LOCAL_IN:在发送到网络堆栈之前调用。

```
76
77    hook1.hook = printInfo;
78    hook1.hooknum = NF_INET_LOCAL_IN;
79    hook1.pf = PF_INET;
80    hook1.priority = NF_IP_PRI_FIRST;
81    nf_register_net_hook(&init_net, &hook1);
82
```

```
[ 8636.506693] *** LOCAL_IN
[ 8636.506694]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 8636.506895] *** Dropping 8.8.8.8 (UDP), port 53
[ 8639.462848] *** LOCAL_IN
[ 8639.462849]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 8639.469534] *** LOCAL_IN
[ 8639.469536]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 8639.635807] *** LOCAL_IN
[ 8639.635822]     192.168.43.1  --> 192.168.43.35 (UDP)
[ 8639.636082] *** LOCAL_IN
[ 8639.636083]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 8639.636103] *** LOCAL_IN
[ 8639.636104]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 8641.507801] *** Dropping 8.8.8.8 (UDP), port 53
[ 8646.507019] *** Dropping 8.8.8.8 (UDP), port 53
```

NF_INET_FORWARD:向其他主机转发报文时调用。

```
77    hook1.hook = printInfo;
78    hook1.hooknum = NF_INET_FORWARD;
79    hook1.pf = PF_INET;
80    hook1.priority = NF_IP_PRI_FIRST;
81    nf_register_net_hook(&init_net, &hook1);
82
```

```
[ 8701.349620]     192.168.43.35  --> 224.0.0.251 (UDP)
[ 8735.822616] The filters are being removed.
[ 8744.209262] Registering filters.
[ 8836.252815] *** Dropping 8.8.8.8 (UDP), port 53
[ 8841.251725] *** Dropping 8.8.8.8 (UDP), port 53
[ 8846.251224] *** Dropping 8.8.8.8 (UDP), port 53
```

NF_IP_POST_ROUTING:数据包离开主机并进入不同的网络之后调用。

```
77    hook1.hook = printInfo;
78    hook1.hooknum = NF_INET_POST_ROUTING;
79    hook1.pf = PF_INET;
80    hook1.priority = NF_IP_PRI_FIRST;
81    nf_register_net_hook(&init_net, &hook1);
82
```

```
[ 8991.615600] The filters are being removed.
[ 9004.647652] Registering filters.
[ 9038.621793] *** POST_ROUTING
[ 9038.621794]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 9038.621983] *** Dropping 8.8.8.8 (UDP), port 53
[ 9043.619555] *** Dropping 8.8.8.8 (UDP), port 53
[ 9048.620289] *** Dropping 8.8.8.8 (UDP), port 53
```

Task1.B.3

下面代码是实现防止其他计算机 telnet 到 VM 的 hook。

```
74 unsigned int telnetFilter(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
75 {
76
77            struct iphdr *iph;
78            struct tcphdr *tcph;
79            iph = ip_hdr(skb);
80            tcph = (void *)iph+iph->ihl*4;
81
82            if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(23))
83            {
84                printk(KERN_INFO "Dropping telent packet 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]);
85                return NF_DROP;
86            }
87            else
88            {
89                return NF_ACCEPT;
90            }
91 }
```

下面代码是实现防止其他计算机 ping 到 VM 的 hook。

```
93 unsigned int pingFilter(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
94 {
95
96             struct iphdr *iph;
97             iph = ip_hdr(skb);
98
99             if(iph->protocol == IPPROTO_ICMP )
100            {
101                printk(KERN_INFO "Dropping telent packet 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]);
102                return NF_DROP;
103            }
104            else
105            {
106                return NF_ACCEPT;
107            }
108 }
```

```
126    hook3.hook = telnetFilter;
127    hook3.hooknum = NF_INET_LOCAL_IN;
128    hook3.pf = PF_INET;
129    hook3.priority = NF_IP_PRI_FIRST;
130    nf_register_net_hook(&init_net, &hook3);
131
132    hook4.hook = pingFilter;
133    hook4.hooknum = NF_INET_LOCAL_IN;
134    hook4.pf = PF_INET;
135    hook4.priority = NF_IP_PRI_FIRST;
136    nf_register_net_hook(&init_net, &hook4);
137
138    return 0;
139 }
140
141
142 void removeFilter(void) {
143    printk(KERN_INFO "The filters are being removed.\n");
144    nf_unregister_net_hook(&init_net, &hook1);
145    nf_unregister_net_hook(&init_net, &hook2);
146    nf_unregister_net_hook(&init_net, &hook3);
147    nf_unregister_net_hook(&init_net, &hook4);
148 }
```

编译并加载内核。

```
[07/25/21]seed@VM:~$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/seedFilter.mod.o
  LD [M]  /home/seed/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[07/25/21]seed@VM:~$ sudo insmod seedFilter.ko
[07/25/21]seed@VM:~$ lsmod | grep seedFilter
seedFilter             16384  0
```

此时 telnet 和 ping 均未成功。

```
root@f77b0ec7ca9c:/# telnet 10.9.0.1
Trying 10.9.0.1...
telnet: Unable to connect to remote host: Connection timed out
root@f77b0ec7ca9c:/# 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 ---
68 packets transmitted, 0 received, 100% packet loss, time 68612ms

root@f77b0ec7ca9c:/#
```

查看日志发现 telnet 包都被 drop 掉了。

```
[15099.063114] Dropping telent packet to 10.9.0.1
[15100.089748] Dropping telent packet to 10.9.0.1
[15101.115651] Dropping telent packet to 10.9.0.1
[15102.141451] Dropping telent packet to 10.9.0.1
[15103.157533] Dropping telent packet to 10.9.0.1
[15104.184205] Dropping telent packet to 10.9.0.1
[15105.208285] Dropping telent packet to 10.9.0.1
[15106.232315] Dropping telent packet to 10.9.0.1
[15107.266631] Dropping telent packet to 10.9.0.1
[15108.289228] Dropping telent packet to 10.9.0.1
[15109.314272] Dropping telent packet to 10.9.0.1
[15110.330581] Dropping telent packet to 10.9.0.1
```

Task2

Task2.A

在路由器里设置如下规则。

```
root@d19383e9a65c:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@d19383e9a65c:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEP
T
root@d19383e9a65c:/# iptables -P OUTPUT DROP
root@d19383e9a65c:/# iptables -P INPUT DROP
root@d19383e9a65c:/#
```

此时从 10.9.0.5 ping 路由器能通，但是 telnet 不行。

```
root@ebc788016f94:/# 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=0.090 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=0.112 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 0.049/0.083/0.112/0.026 ms
root@ebc788016f94:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@ebc788016f94:/#
```

清除写入的规则。

```
root@d19383e9a65c:/# iptables -F
root@d19383e9a65c:/# iptables -P OUTPUT ACCEPT
root@d19383e9a65c:/# iptables -P INPUT ACCEPT
root@d19383e9a65c:/#
```

Task2.B

在路由器里设置如下规则。

```
root@d19383e9a65c:/# iptables -A FORWARD -i eth0 -o eth1 -p icmp --icmp-typ
e echo-request -j DROP
root@d19383e9a65c:/# iptables -A FORWARD -s 10.9.0.11 -p icmp --icmp-type e
cho-request -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -o eth0 -p icmp --icmp-type echo-r
equest -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth1 -o eth0 -p icmp --icmp-typ
e echo-request -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth1 -o eth0 -p icmp --icmp-typ
e echo-reply -j ACCEPT
root@d19383e9a65c:/# iptables -P FORWARD DROP
root@d19383e9a65c:/#
```

此时，外部主机不能 ping 内网。

```
root@ebc788016f94:/# 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 ---
14 packets transmitted, 0 received, 100% packet loss, time 13309ms

root@ebc788016f94:/#
```

外部主机可以 ping 路由器。

```
root@ebc788016f94:/# 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=0.053 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.050 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.049 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.049/0.051/0.053/0.001 ms
root@ebc788016f94:/#
```

内部主机可以 ping 外网。

```
root@4b92ed003733:/# 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=0.150 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.060 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.060 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.145 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.061 ms
^C
--- 10.9.0.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.060/0.095/0.150/0.042 ms
root@4b92ed003733:/#
```

无论是内网 telnet 外网还是外网 telnet 内网都失败。

```
root@ebc788016f94:/# telnet 192.168.60.5
Trying 192.168.60.5...
telnet: Unable to connect to remote host: Connection timed out
root@ebc788016f94:/#
```

```
root@4b92ed003733:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@4b92ed003733:/#
```

清除规则。

```
root@d19383e9a65c:/# iptables -F
root@d19383e9a65c:/# iptables -P OUTPUT ACCEPT
root@d19383e9a65c:/# iptables -P INPUT ACCEPT
root@d19383e9a65c:/#
```

Task2.C

在路由器里设置如下规则。

```
root@d19383e9a65c:/# iptables -A FORWARD -i eth0 -o eth1 -d 192.168.60.5 -p
 tcp --dport 23 -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth1 -o eth0 -s 192.168.60.5 -p
 tcp --sport 23 -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth0 -o eth1 -j DROP
root@d19383e9a65c:/# iptables -A FORWARD -i eth1 -o eth1 -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth1 -o eth0 -j DROP
root@d19383e9a65c:/# iptables -P FORWARD DROP
root@d19383e9a65c:/#
```

外网主机能 telnet 192.168.60.5。

```
root@ebc788016f94:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
4b92ed003733 login:
```

外网主机不能 telnet 内网其他主机。

```
root@ebc788016f94:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@ebc788016f94:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
```

外网主机无法 ping 内网主机。

```
root@ebc788016f94:/# 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 ---
10 packets transmitted, 0 received, 100% packet loss, time 9222ms

root@ebc788016f94:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
^C
--- 192.168.60.6 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8176ms

root@ebc788016f94:/# ping 192.168.60.7
PING 192.168.60.7 (192.168.60.7) 56(84) bytes of data.
^C
--- 192.168.60.7 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9221ms

root@ebc788016f94:/#
```

内网主机可以 ping 所有内网主机 。

```
root@4b92ed003733:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
64 bytes from 192.168.60.6: icmp_seq=1 ttl=64 time=0.102 ms
64 bytes from 192.168.60.6: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 192.168.60.6: icmp_seq=3 ttl=64 time=0.047 ms
^C
--- 192.168.60.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.047/0.066/0.102/0.025 ms
root@4b92ed003733:/# 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=0.119 ms
64 bytes from 192.168.60.7: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 192.168.60.7: icmp_seq=3 ttl=64 time=0.074 ms
^C
--- 192.168.60.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2058ms
rtt min/avg/max/mdev = 0.050/0.081/0.119/0.028 ms
root@4b92ed003733:/#
```

内网主机无法访问外网主机。

```
root@4b92ed003733:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
^C
--- 10.9.0.5 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 16380ms

root@4b92ed003733:/#
```

清除规则。

```
root@d19383e9a65c:/# iptables -P FORWARD ACCEPT
root@d19383e9a65c:/# iptables -F
root@d19383e9a65c:/#
```

Task3

Task3.A

在 10.9.0.5 上 ping192.168.60.5。

```
root@ebc788016f94:/# 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=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.070 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.117 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.059 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.061 ms
```

在路由器上查看跟踪信息，可知持续时间为 30s。

```
root@d19383e9a65c:/# conntrack -L
icmp     1 29 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=59 src=192.168
.60.5 dst=10.9.0.5 type=0 code=0 id=59 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

在 192.168.60.5 上开一个 UDP 服务器，在 10.9.0.5 上发送报文。

```
root@ebc788016f94:/# nc -u 192.168.60.5 9090
123
456
```

```
root@4b92ed003733:/# nc -lu 9090
123
456
```

查看路由器跟踪信息，可知持续时间为 30s。

```
root@d19383e9a65c:/# conntrack -L
udp      17 26 src=10.9.0.5 dst=192.168.60.5 sport=38485 dport=9090 [UNREPL
IED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=38485 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@d19383e9a65c:/#
```

在 192.168.60.5 上开一个 TCP 服务器，在 10.9.0.5 上发送报文。

```
root@ebc788016f94:/# nc 192.168.60.5 9090
123
```

```
root@4b92ed003733:/# nc -l 9090
123
```

查看路由器跟踪信息，可知持续时间为 432000s。

```
root@d19383e9a65c:/# conntrack -L
tcp      6 431997 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=59336 dpo
rt=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59336 [ASSURED] mark
=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@d19383e9a65c:/#
```

Task3.B

在路由器里设置如下规则。

```
root@d19383e9a65c:/# iptables -A FORWARD -p tcp -m conntrack --ctstate ESTA
BLISHED,RELATED -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth0 -o eth1 -d 192.168.60.5 -p
 tcp --dport 23 --syn -m conntrack --ctstate NEW -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth0 -o eth1 -p tcp --syn -m co
nntrack --ctstate NEW -j DROP
root@d19383e9a65c:/# iptables -A FORWARD -i eth1 -o eth1 -p tcp --syn -m co
nntrack --ctstate NEW -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -i eth1 -o eth0 -p tcp --syn -m co
nntrack --ctstate NEW -j ACCEPT
root@d19383e9a65c:/# iptables -P FORWARD DROP
root@d19383e9a65c:/#
```

外部主机可以 telnet192.168.60.5。

```
root@ebc788016f94:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
4b92ed003733 login:
```

外部主机不能 telnet 到内网其他主机。

```
root@ebc788016f94:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@ebc788016f94:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
```

内网主机可以 telnet 到任意内网或外网主机。

```
root@4b92ed003733:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fedad57c1059 login: ^CConnection closed by foreign host.
root@4b92ed003733:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ebc788016f94 login: ^CConnection closed by foreign host.
root@4b92ed003733:/#
```

清除规则。

```
root@d19383e9a65c:/# iptables -P FORWARD ACCEPT
root@d19383e9a65c:/# iptables -F
root@d19383e9a65c:/#
```

Task4

在路由器里设置如下规则。

```
root@d19383e9a65c:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/mi
nute --limit-burst 5 -j ACCEPT
root@d19383e9a65c:/#
```

在 10.9.0.5 上 ping192.168.60.5，没有丢包现象。

```
root@ebc788016f94:/# 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=0.068 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.093 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=6 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=8 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.078 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.060 ms
^C
--- 192.168.60.5 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9194ms
rtt min/avg/max/mdev = 0.060/0.066/0.093/0.010 ms
root@ebc788016f94:/#
```

在路由器里加入第二条规则。

```
root@d19383e9a65c:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/mi
nute --limit-burst 5 -j ACCEPT
root@d19383e9a65c:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@d19383e9a65c:/#
```

继续在 10.9.0.5 上 ping192.168.60.5，能 ping 通但有丢包现象。

```
root@ebc788016f94:/# 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=0.100 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.077 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=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.061 ms
^C
--- 192.168.60.5 ping statistics ---
24 packets transmitted, 8 received, 66.6667% packet loss, time 23557ms
rtt min/avg/max/mdev = 0.060/0.068/0.100/0.013 ms
root@ebc788016f94:/#
```

清除规则。

```
root@d19383e9a65c:/# iptables -P FORWARD ACCEPT
root@d19383e9a65c:/# iptables -F
root@d19383e9a65c:/#
```

Task5

轮询模式:

在 192.168.60.5, 192.168.60.6, 192.168.60.7 上 8080 端口都开一个 UDP 服务器。

```
[07/25/21]seed@VM:~/Desktop$ dockps
ebc788016f94  hostA-10.9.0.5
fedad57c1059  host2-192.168.60.6
d19383e9a65c  seed-router
4b92ed003733  host1-192.168.60.5
cba397bae487  host3-192.168.60.7
[07/25/21]seed@VM:~/Desktop$ docksh 4b
root@4b92ed003733:/# nc -luk 8080
```

```
seed@VM: ~/Desktop
[07/25/21]seed@VM:~/Desktop$ docksh fe
root@fedad57c1059:/# nc -luk 8080
```

```
seed@VM: ~/Desktop
[07/25/21]seed@VM:~/Desktop$ docksh cb
root@cba397bae487:/# nc -luk 8080
```

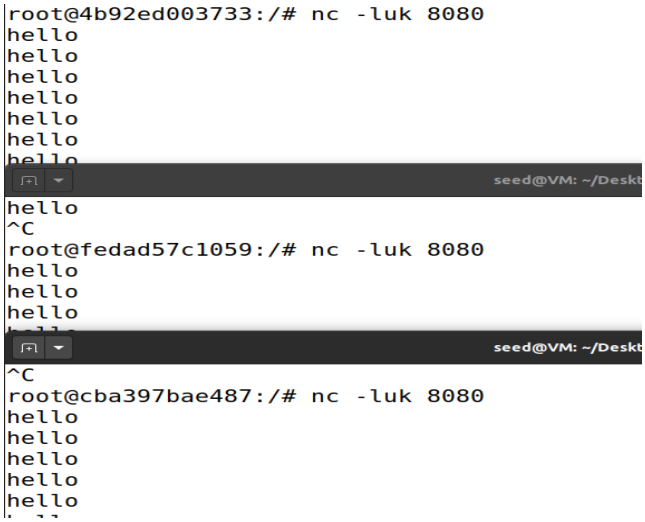
在路由器里设置如下规则。

```
root@d19383e9a65c:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statis
tic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@d19383e9a65c:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statis
tic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.6:8080
root@d19383e9a65c:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statis
tic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.7:8080
root@d19383e9a65c:/#
```

在 10.9.0.5 上输入足够多的 echo hello | nc -u 10.9.0.11 8080，观察三个服务器 hello 的数量。

```
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^[[A
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/#
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
root@ebc788016f94:/# ^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
```

在输入了 75 次 echo hello | nc -u 10.9.0.11 8080 后，192.168.60.5，192.168.60.6，192.168.60.7 里的 hello 数量为 50：15：10。



清除规则。

```
root@d19383e9a65c:/# iptables -t nat -P PREROUTING ACCEPT
root@d19383e9a65c:/# iptables -F
```

随机模式:

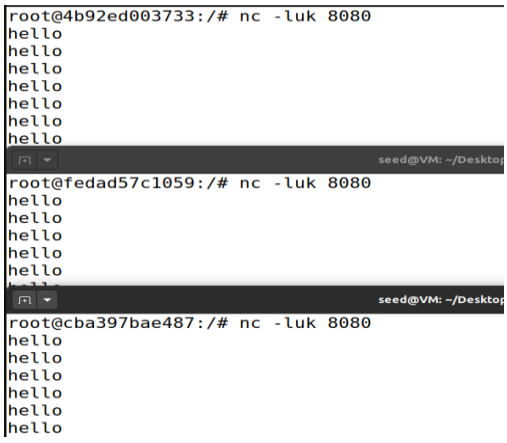
在路由器里设置如下规则。

```
root@d19383e9a65c:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statis
tic --mode random --probability 0.33 -j DNAT --to-destination 192.168.60.5:8080
root@d19383e9a65c:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statis
tic --mode random --probability 0.5 -j DNAT --to-destination 192.168.60.6:8080
root@d19383e9a65c:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -j DNAT -
-to-destination 192.168.60.7:8080
root@d19383e9a65c:/#
```

在 10.9.0.5 上输入足够多的 echo hello | nc -u 10.9.0.11 8080，观察三个服务器 hello 的数量。

```
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
root@ebc788016f94:/# echo hello | nc -u 10.9.0.11 8080
^C
```

在输入了 84 次 echo hello | nc -u 10.9.0.11 8080 后，192.168.60.5，192.168.60.6，192.168.60.7 里的 hello 数量为 54：19：11。



清除规则。

```
root@d19383e9a65c:/# iptables -t nat -P PREROUTING ACCEPT
root@d19383e9a65c:/# iptables -F
root@d19383e9a65c:/#
```