Lab1

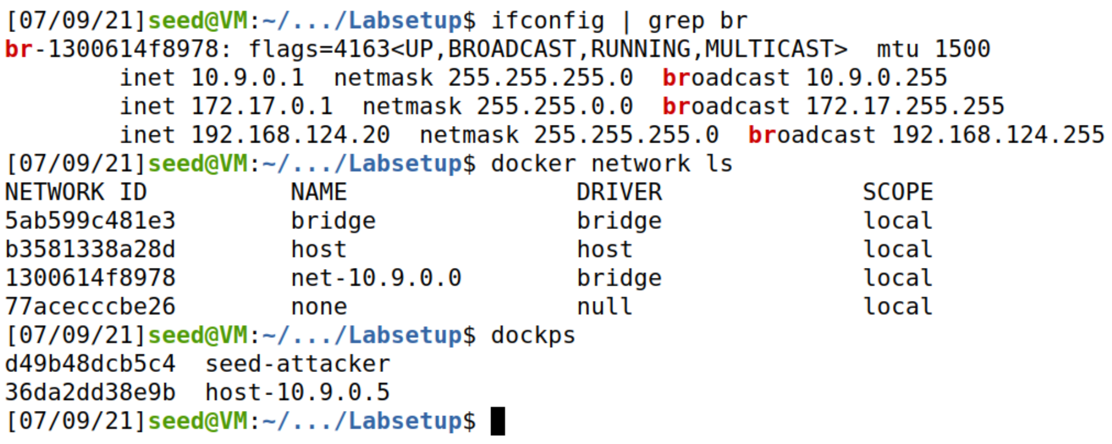
57118232 谢隆文

Task 1.1：Sniffing Packets

Task 1.1A

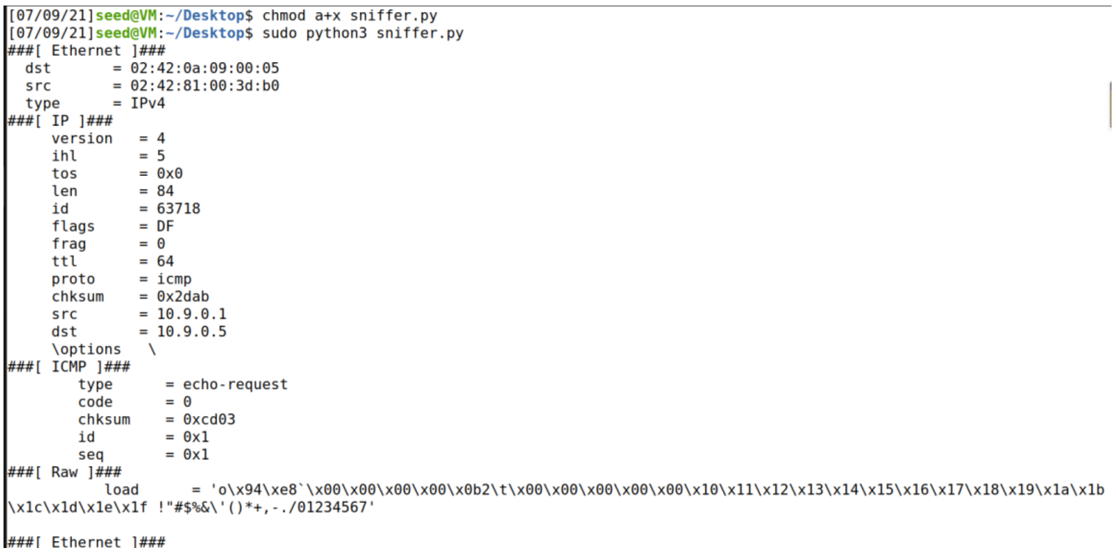
sniff.py

from scapy.all import *
def print_pkt(pkt):
pkt.show()
pkt = sniff(iface='br- 1300614f8978', filter='icmp', prn=print_pkt)
启动 docker，查看网络 id



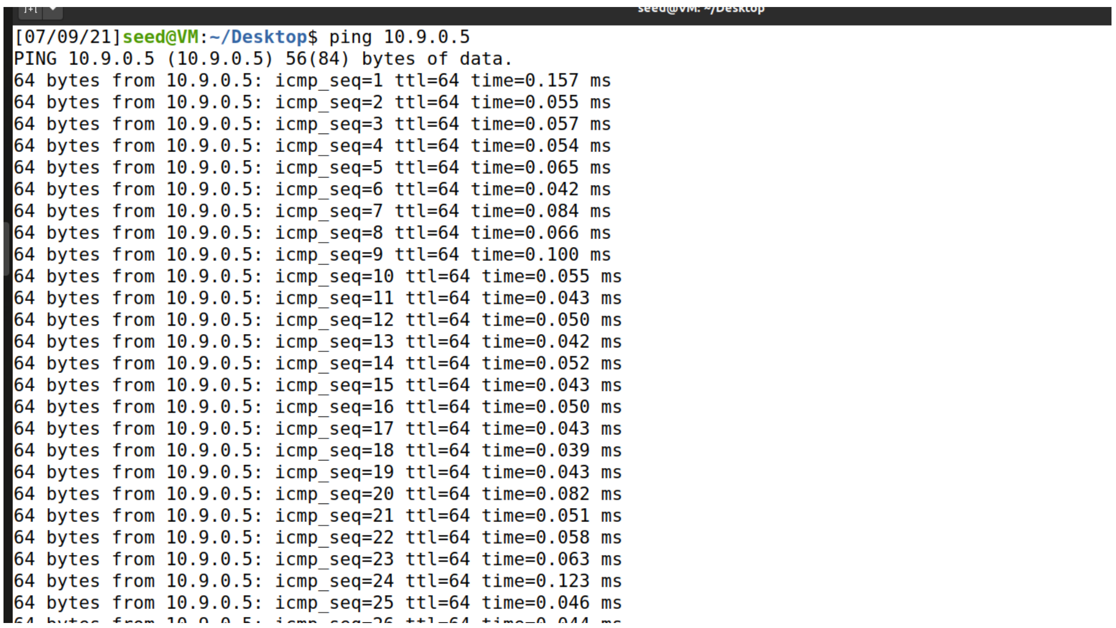
```
[07/09/21]seed@VM:~/.../Labsetup$ ifconfig | grep br
br-1300614f8978: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.1  netmask 255.255.255.0  broadcast 10.9.0.255
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet 192.168.124.20  netmask 255.255.255.0  broadcast 192.168.124.255
[07/09/21]seed@VM:~/.../Labsetup$ docker network ls
NETWORK ID          NAME                DRIVER              SCOPE
5ab599c481e3        bridge              bridge              local
b3581338a28d        host                host                local
1300614f8978        net-10.9.0.0        bridge              local
77acecccbe26        none                null                local
[07/09/21]seed@VM:~/.../Labsetup$ dockps
d49b48dcb5c4  seed-attacker
36da2dd38e9b  host-10.9.0.5
[07/09/21]seed@VM:~/.../Labsetup$ 
```

以 root 权限运行



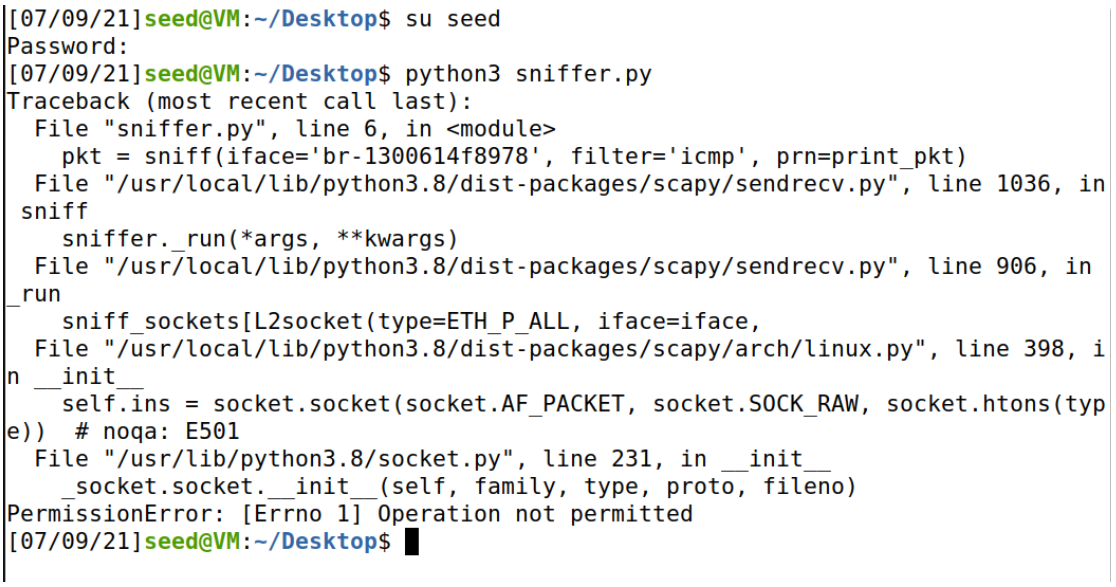
```
[07/09/21]seed@VM:~/Desktop$ chmod a+x sniffer.py
[07/09/21]seed@VM:~/Desktop$ sudo python3 sniffer.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:81:00:3d:b0
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 63718
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x2dab
     src       = 10.9.0.1
     dst       = 10.9.0.5
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0xcd03
        id        = 0x1
        seq       = 0x1
###[ Raw ]###
           load      = 'o\x94\xe8`\x00\x00\x00\x00\x0b2\t\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b
\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
```



```
[07/09/21]seed@VM:~/Desktop$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.157 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.057 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=0.054 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=0.065 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=64 time=0.042 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=64 time=0.084 ms
64 bytes from 10.9.0.5: icmp_seq=8 ttl=64 time=0.066 ms
64 bytes from 10.9.0.5: icmp_seq=9 ttl=64 time=0.100 ms
64 bytes from 10.9.0.5: icmp_seq=10 ttl=64 time=0.055 ms
64 bytes from 10.9.0.5: icmp_seq=11 ttl=64 time=0.043 ms
64 bytes from 10.9.0.5: icmp_seq=12 ttl=64 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=13 ttl=64 time=0.042 ms
64 bytes from 10.9.0.5: icmp_seq=14 ttl=64 time=0.052 ms
64 bytes from 10.9.0.5: icmp_seq=15 ttl=64 time=0.043 ms
64 bytes from 10.9.0.5: icmp_seq=16 ttl=64 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=17 ttl=64 time=0.043 ms
64 bytes from 10.9.0.5: icmp_seq=18 ttl=64 time=0.039 ms
64 bytes from 10.9.0.5: icmp_seq=19 ttl=64 time=0.043 ms
64 bytes from 10.9.0.5: icmp_seq=20 ttl=64 time=0.082 ms
64 bytes from 10.9.0.5: icmp_seq=21 ttl=64 time=0.051 ms
64 bytes from 10.9.0.5: icmp_seq=22 ttl=64 time=0.058 ms
64 bytes from 10.9.0.5: icmp_seq=23 ttl=64 time=0.063 ms
64 bytes from 10.9.0.5: icmp_seq=24 ttl=64 time=0.123 ms
64 bytes from 10.9.0.5: icmp_seq=25 ttl=64 time=0.046 ms
```

非 root 权限下，运行 sniffer 抓包无效



```
[07/09/21]seed@VM:~/Desktop$ su seed
Password:
[07/09/21]seed@VM:~/Desktop$ python3 sniffer.py
Traceback (most recent call last):
  File "sniffer.py", line 6, in <module>
    pkt = sniff(iface='br-1300614f8978', filter='icmp', prn=print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in
 sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 906, in
_run
    sniff_sockets[L2socket(type=ETH_P_ALL, iface=iface,
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398, i
n __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(typ
e))  # noqa: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[07/09/21]seed@VM:~/Desktop$ 
```

Task 1.1B

只抓取 ICMP 报文，见 Task 1.1A 所示。

捕获任何来自特定 IP 的 TCP 数据包，目的端口为 23。

#!/usr/bin/evn python3

from scapy.all import *

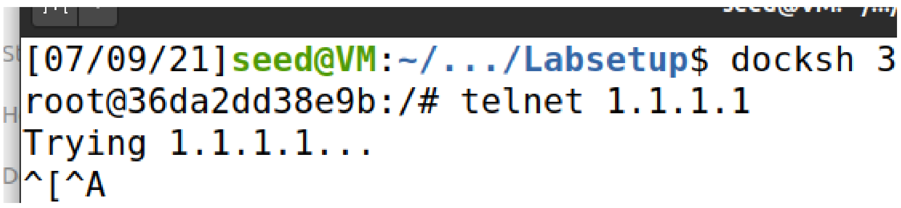
def print_pkt(pkt):

pkt.show()

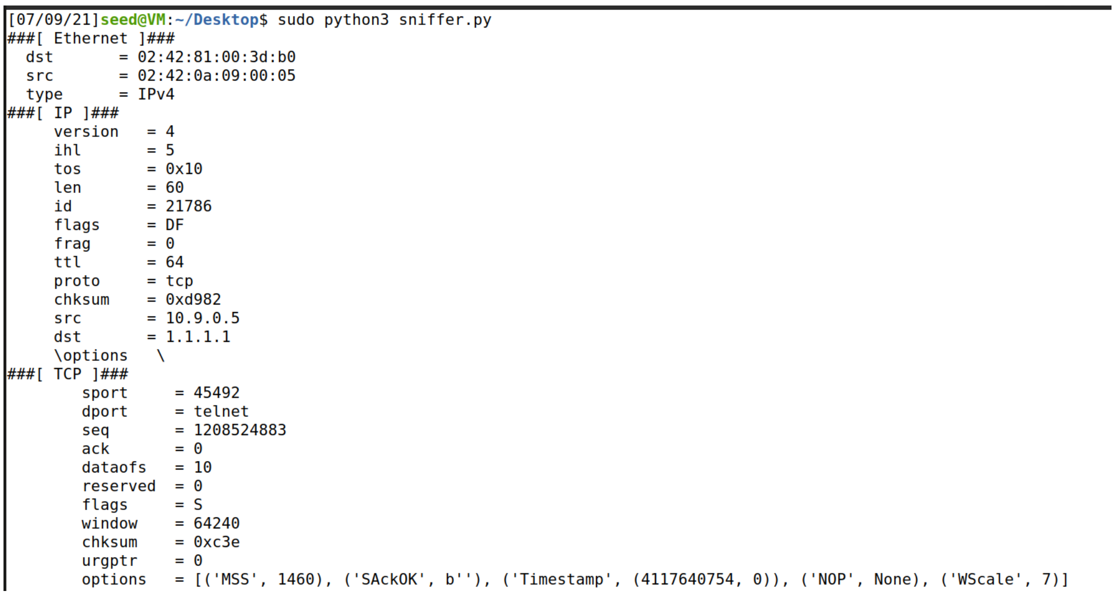
pkt = sniff(iface='br-1300614f8978', filter='tcp port 23 and host 10.9.0.5',

prn=print_pkt)

利用 docksh 获取 host 的 shell，telnet 任意一个 IP 地址建立连接。



```
[07/09/21]seed@VM:~/.../Labsetup$ docksh 3
root@36da2dd38e9b:/# telnet 1.1.1.1
Trying 1.1.1.1...
^[^A
```

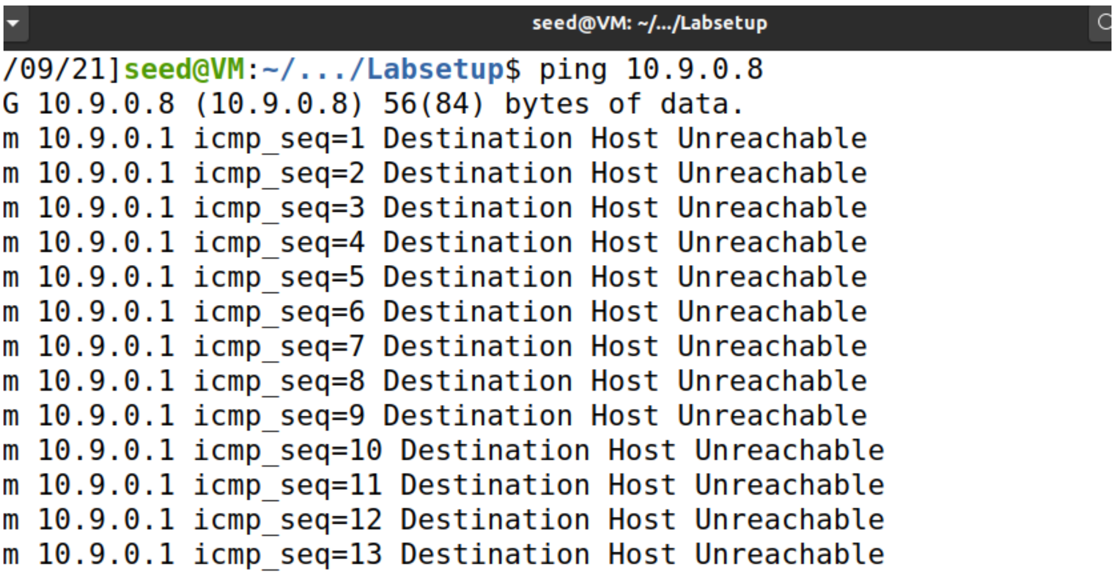


```
[07/09/21]seed@VM:~/Desktop$ sudo python3 sniffer.py
###[ Ethernet ]###
  dst       = 02:42:81:00:3d:b0
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 60
     id        = 21786
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xd982
     src       = 10.9.0.5
     dst       = 1.1.1.1
     \options   \
###[ TCP ]###
        sport     = 45492
        dport     = telnet
        seq       = 1208524883
        ack       = 0
        dataofs   = 10
        reserved  = 0
        flags     = S
        window    = 64240
        chksum    = 0xc3e
        urgptr    = 0
        options   = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (4117640754, 0)), ('NOP', None), ('WScale', 7)]
```

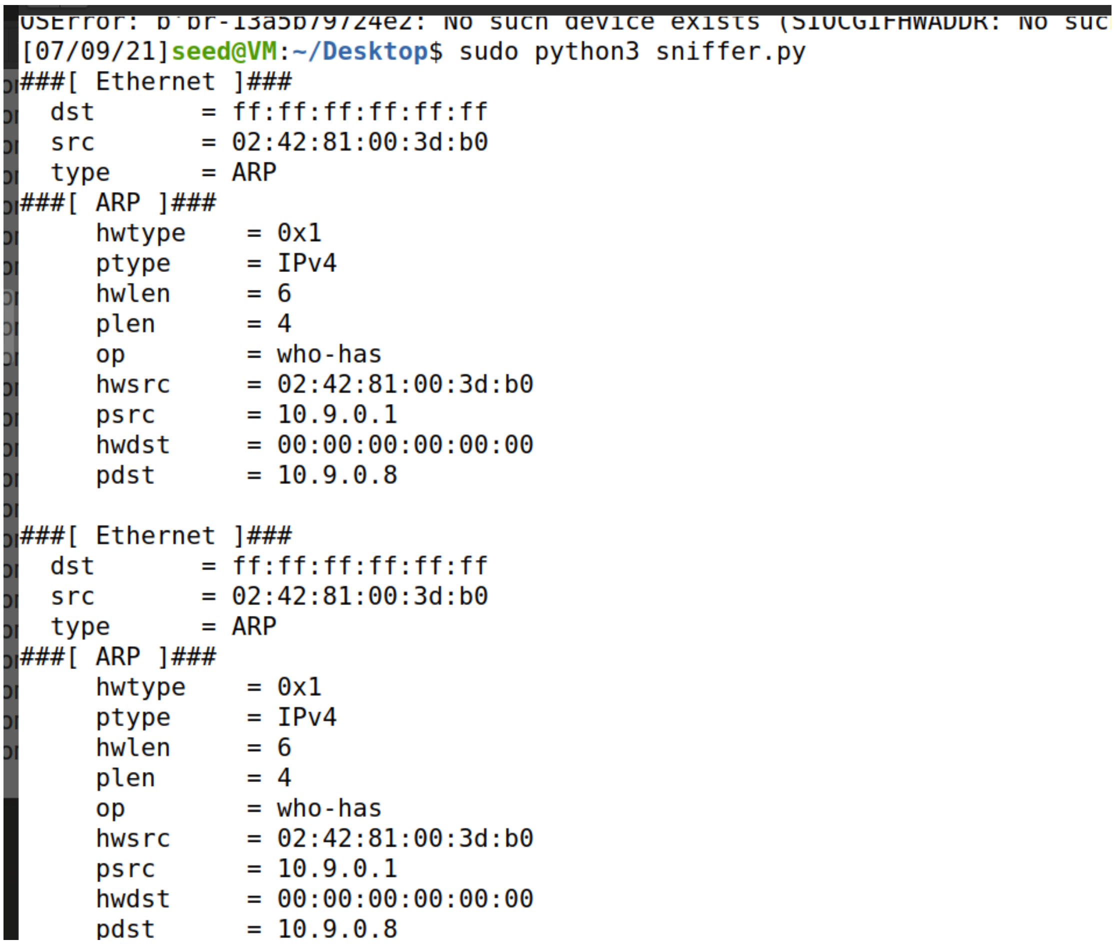
捕获来自或去特定子网的数据包。

```
#!/usr/bin/evn python3
from scapy.all import *
def print_pkt(pkt):
pkt.show()
pkt = sniff(iface='br-13a5b79724e2', filter='host 10.9.0.8', prn=print_pkt)
```

直接 ping 10.9.0.8，可得到捕获的数据包。



```
/09/21]seed@VM:~/.../Labsetup$ ping 10.9.0.8
G 10.9.0.8 (10.9.0.8) 56(84) bytes of data.
m 10.9.0.1 icmp_seq=1 Destination Host Unreachable
m 10.9.0.1 icmp_seq=2 Destination Host Unreachable
m 10.9.0.1 icmp_seq=3 Destination Host Unreachable
m 10.9.0.1 icmp_seq=4 Destination Host Unreachable
m 10.9.0.1 icmp_seq=5 Destination Host Unreachable
m 10.9.0.1 icmp_seq=6 Destination Host Unreachable
m 10.9.0.1 icmp_seq=7 Destination Host Unreachable
m 10.9.0.1 icmp_seq=8 Destination Host Unreachable
m 10.9.0.1 icmp_seq=9 Destination Host Unreachable
m 10.9.0.1 icmp_seq=10 Destination Host Unreachable
m 10.9.0.1 icmp_seq=11 Destination Host Unreachable
m 10.9.0.1 icmp_seq=12 Destination Host Unreachable
m 10.9.0.1 icmp_seq=13 Destination Host Unreachable
```



```
OSError: b'br-13a5b79724e2: No such device exists (SIOCGIFHWADDR: No suc
[07/09/21]seed@VM:~/Desktop$ sudo python3 sniffer.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:81:00:3d:b0
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 02:42:81:00:3d:b0
     psrc      = 10.9.0.1
     hwdst     = 00:00:00:00:00:00
     pdst      = 10.9.0.8

###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:81:00:3d:b0
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 02:42:81:00:3d:b0
     psrc      = 10.9.0.1
     hwdst     = 00:00:00:00:00:00
     pdst      = 10.9.0.8
```

Task 1.2：Spoofing ICMP Packets

如下程序实现构造一个 ICMP echo-request 包，可以指定任意 IP 地址，本次实验指定 114.114.114.114 为源地址（伪造），10.1.0.5 为目的地址。

from scapy.all import *

a = IP()

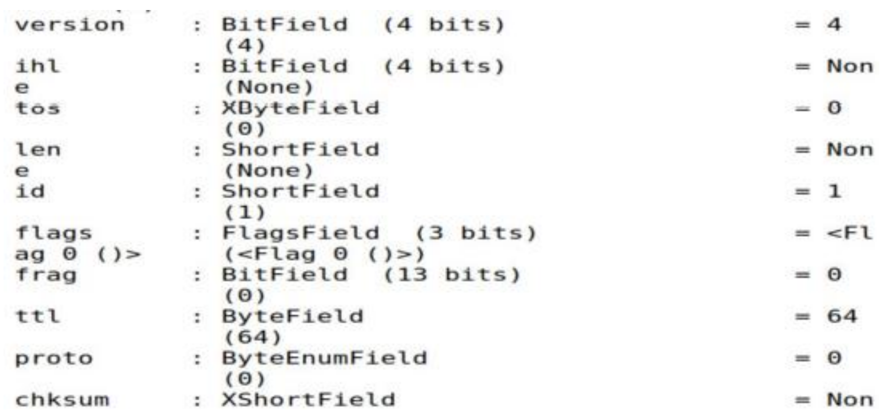
a.dst = '10.9.0.3'

b = ICMP()

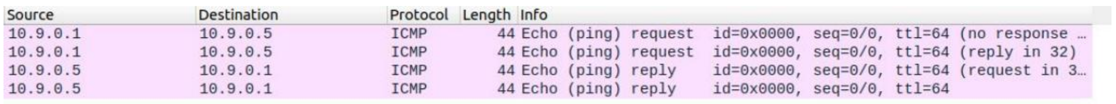
p = a/b

send(p)

ls(a)



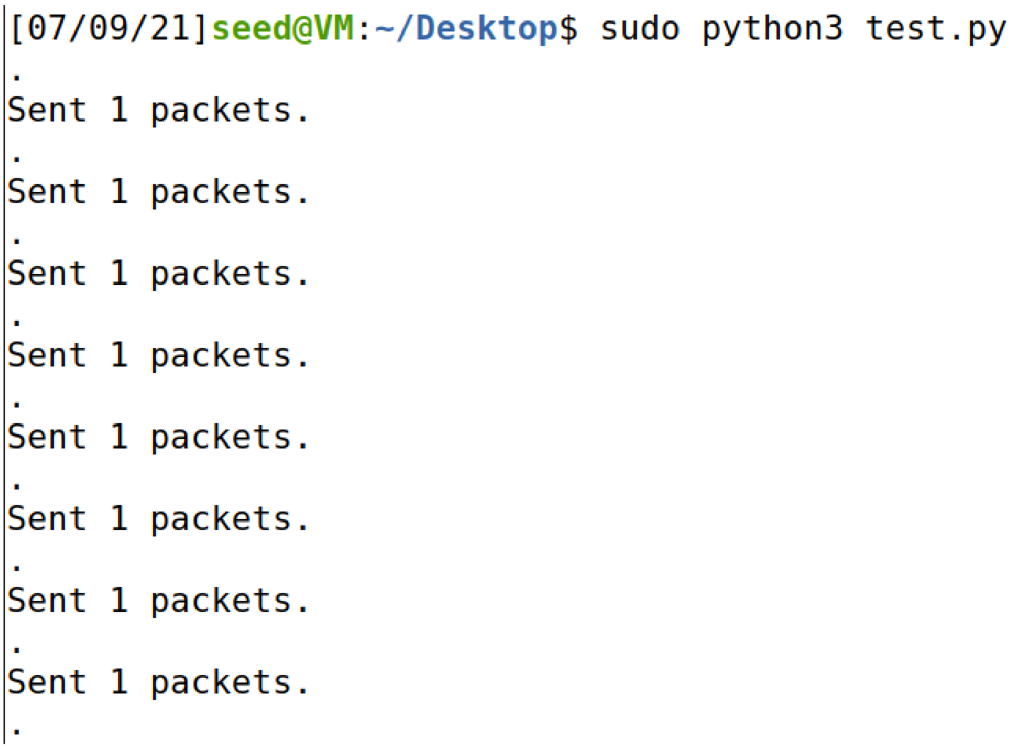
```
version      : BitField  (4 bits)                       = 4
               (4)
ihl          : BitField  (4 bits)                       = Non
e              (None)
tos          : XByteField                               = 0
               (0)
len          : ShortField                               = Non
e              (None)
id           : ShortField                               = 1
               (1)
flags        : FlagsField  (3 bits)                     = <Fl
ag 0 ()>       (<Flag 0 ()>)
frag         : BitField  (13 bits)                      = 0
               (0)
ttl          : ByteField                                = 64
               (64)
proto        : ByteEnumField                            = 0
               (0)
chksum       : XShortField                              = Non
```



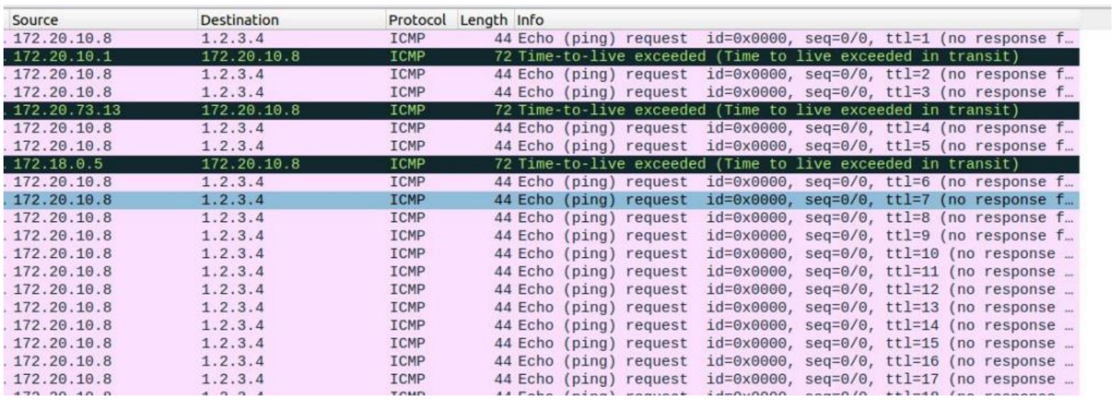
```
Source        Destination   Protocol Length Info
10.9.0.1      10.9.0.5      ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (no response …
10.9.0.1      10.9.0.5      ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 32)
10.9.0.5      10.9.0.1      ICMP         44 Echo (ping) reply    id=0x0000, seq=0/0, ttl=64 (request in 3…
10.9.0.5      10.9.0.1      ICMP         44 Echo (ping) reply    id=0x0000, seq=0/0, ttl=64
```

Task 1.3：Traceroute

```
from scapy.all import *
a = IP()
b = ICMP()
a.dst = '1.2.3.4'
for i in range(30):
a.ttl = i + 1
p = a / b
send(p)
```



```
[07/09/21]seed@VM:~/Desktop$ sudo python3 test.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
```



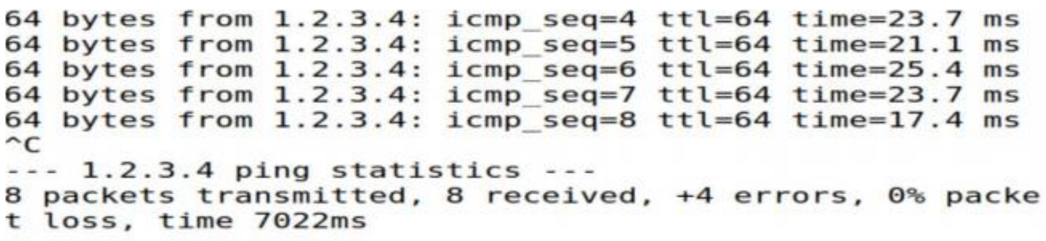
```
Source        Destination   Protocol Length Info
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=1 (no response f…
172.20.10.1   172.20.10.8   ICMP         72 Time-to-live exceeded (Time to live exceeded in transit)
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=2 (no response f…
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=3 (no response f…
172.20.73.13  172.20.10.8   ICMP         72 Time-to-live exceeded (Time to live exceeded in transit)
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=4 (no response f…
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=5 (no response f…
172.18.0.5    172.20.10.8   ICMP         72 Time-to-live exceeded (Time to live exceeded in transit)
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=6 (no response f…
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=7 (no response f…
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=8 (no response f…
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=9 (no response f…
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=10 (no response …
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=11 (no response …
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=12 (no response …
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=13 (no response …
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=14 (no response …
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=15 (no response …
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=16 (no response …
172.20.10.8   1.2.3.4       ICMP         44 Echo (ping) request  id=0x0000, seq=0/0, ttl=17 (no response …
```

Task 1.4：Sniffing and-then Spoofing

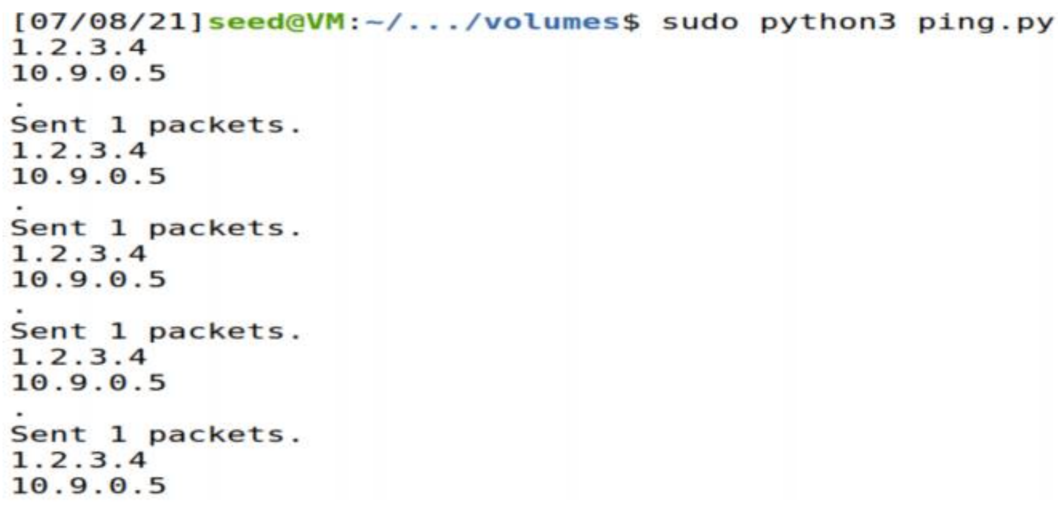
```
from scapy.all import *
```

```
def spoof_pkt(pkt):
a = IP()
b = ICMP()
a.dst = '10.9.0.5'
p = a/b
send(p)
pkt = sniff(iface='br-13a5b79724e2', filter='icmp and host 10.9.0.5',
prn=spoof_pkt
```

ping 1.2.3.4（不存在主机）



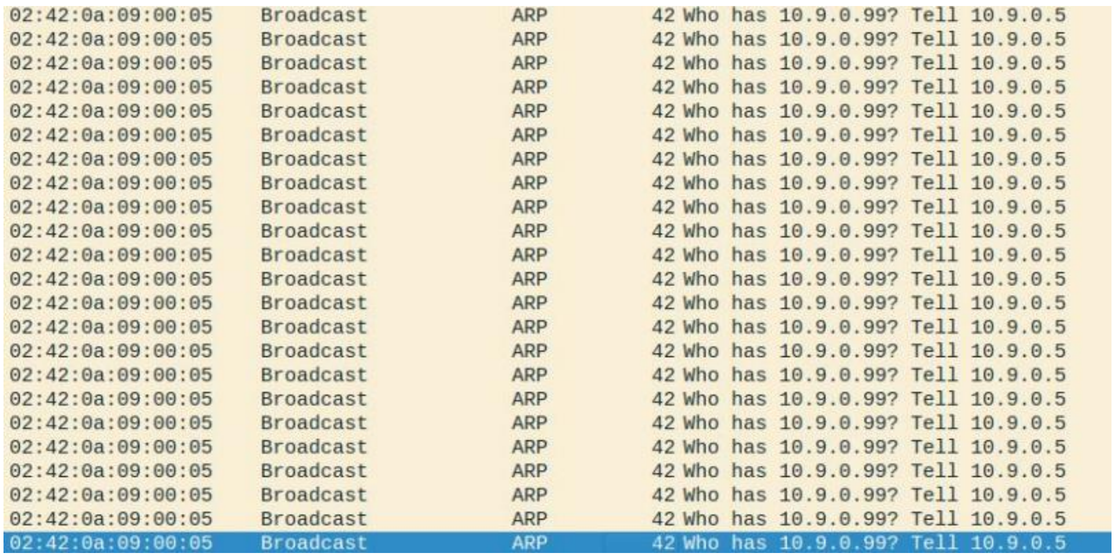
```
64 bytes from 1.2.3.4: icmp_seq=4 ttl=64 time=23.7 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=64 time=21.1 ms
64 bytes from 1.2.3.4: icmp_seq=6 ttl=64 time=25.4 ms
64 bytes from 1.2.3.4: icmp_seq=7 ttl=64 time=23.7 ms
64 bytes from 1.2.3.4: icmp_seq=8 ttl=64 time=17.4 ms
^C
--- 1.2.3.4 ping statistics ---
8 packets transmitted, 8 received, +4 errors, 0% packe
t loss, time 7022ms
```



```
[07/08/21]seed@VM:~/.../volumes$ sudo python3 ping.py
1.2.3.4
10.9.0.5
.
Sent 1 packets.
1.2.3.4
10.9.0.5
.
Sent 1 packets.
1.2.3.4
10.9.0.5
.
Sent 1 packets.
1.2.3.4
10.9.0.5
.
Sent 1 packets.
1.2.3.4
10.9.0.5
```

user 将 10.9.0.1 当做网关，将该报文传递给 10.9.0.1，因为实际上 1.2.3.4.不可达，所以只有 ping.py 会发回伪造报文给 10.9.0.5，造成 1.2.3.4 可以 ping 通的假象。

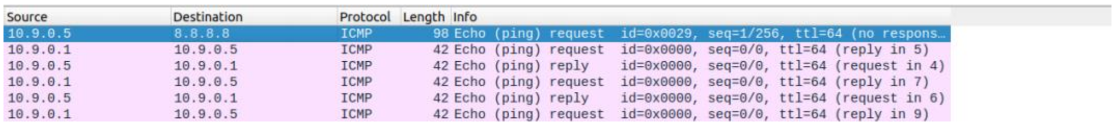
ping 10.9.0.99（本局域网内不存在）



```
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
02:42:0a:09:00:05    Broadcast    ARP    42 Who has 10.9.0.99? Tell 10.9.0.5
```

局域网内不存在的主机，一直在利用 MAC 地址进行广播，但是得不到响应。

ping 8.8.8.8（互联网上存在）



```
Source        Destination   Protocol  Length Info
10.9.0.5      8.8.8.8       ICMP      98 Echo (ping) request  id=0x0029, seq=1/256, ttl=64 (no respons…
10.9.0.1      10.9.0.5      ICMP      42 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 5)
10.9.0.5      10.9.0.1      ICMP      42 Echo (ping) reply    id=0x0000, seq=0/0, ttl=64 (request in 4)
10.9.0.1      10.9.0.5      ICMP      42 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 7)
10.9.0.5      10.9.0.1      ICMP      42 Echo (ping) reply    id=0x0000, seq=0/0, ttl=64 (request in 6)
10.9.0.1      10.9.0.5      ICMP      42 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 9)
```

user 将报文发送给网关后，ping 命令的报文会被 10.9.0.1 发送到互联网上，经由互联网交给 8.8.8.8，由于 8.8.8.8 真实存在，所以最后会有两个 echo-reply，一个来自 8.8.8.8。另外一个由 piny.py 伪造。