lab1-report

571118106 强珂阳

task 1.1A

root 权限下运行

sniffer.py
~/Desktop/Labs_20.04/Network Security/Packet Sniffing and Spoofing Lab/Labsetup/volumes

```python
#!/usr/bin/env python3
from scapy.all import *
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface='br-97c502071b88', filter='icmp', prn=print_pkt)
```

seed@VM: ~/.../Labsetup

```
root@VM:/volumes# ./sniffer.py
###[ Ethernet ]###
  dst       = 02:42:9a:c8:10:d6
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 49766
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x642b
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
```

用没有 root 权限的 host 并修改相应代码

seed@VM: ~/.../volumes

```
[07/07/21]seed@VM:~/.../volumes$ sniffer.py
Traceback (most recent call last):
  File "./sniffer.py", line 5, in <module>
    pkt = sniff(iface='eth0', 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
[07/07/21]seed@VM:~/.../volumes$
```

对比以上两种情况，发现没有 root 权限不能运行该代码

task 1.1B

1. filter=`icmp`结果同 1.1A

2. 捕获来自特定 IP，目标端口为 23 的任何 tcp 数据包

```
#!/usr/bin/env python3
from scapy.all import *
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface='br-97c502071b88', filter='ip src 10.9.0.5 and tcp and dst port 23',
prn=print_pkt)
```

```
bash: dockps: command not found
root@VM:/volumes# sniffer.py
^Croot@VM:/volumes# sniffer.py
###[ Ethernet ]###
  dst       = 02:42:9a:c8:10:d6
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 60
     id        = 17487
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xe245
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
###[ TCP ]###
        sport     = 55266
```

3. 捕获来自或前往特定子网的数据包

```
#!/usr/bin/env python3
from scapy.all import *
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface='br-97c502071b88', filter='net 10.9.0.0/16', prn=print_pkt)
```

```
root@VM:/volumes# ls
sniffer.py
root@VM:/volumes# sniffer.py
###[ Ethernet ]###
  dst       = 02:42:9a:c8:10:d6
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 64155
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x2bf6
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
```

task 1.2

伪造源地址为 110.110.110.110

```python
#!/usr/bin/env python3
from scapy.all import *
a=IP()
a.src='110.110.110.110'
a.dst='10.9.0.5'
b=ICMP()
p=a/b
send(p)
ls(a)
```

用 wireshark 可以发现捕获到该报文

843	2021-07-08 09:2…	110.110.110.110	10.9.0.5	ICMP	44	Echo (ping) request id=0x0000,
844	2021-07-08 09:2…	110.110.110.110	10.9.0.5	ICMP	44	Echo (ping) request id=0x0000,

task 1.3

```python
#!/usr/bin/env python3
from scapy.all import *
a = IP()
b = ICMP()
a.dst = '58.192.118.142'
for i in range(50):
        a.ttl = i + 1
        send(a/b)
ls(a)
```

连接东南大学官网，由于不联网，所以将 ttl 设置成较大的数依旧显示没有响应

No.	Time	Source	Destination	Protocol	Length	Info
39	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=39 (no response …
40	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=40 (no response …
41	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=41 (no response …
42	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=42 (no response …
43	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=43 (no response …
44	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=44 (no response …
45	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=45 (no response …
46	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=46 (no response …
47	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=47 (no response …
48	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=48 (no response …
49	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=49 (no response …
50	2021-07-08 09:4…	0.0.0.0	58.192.118.142	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=50 (no response …

task 1.4

```python
#!/usr/bin/env python3
from scapy.all import *
def spoof_pkt(pkt):
        pkt.show()
        a = IP()
        a.src = pkt[IP].dst
        a.dst = pkt[IP].src
        b = ICMP()
        b.type = 0
        b.id = pkt[ICMP].id
        b.seq = pkt[ICMP].seq
        p = a/b
        send(p)
pkt = sniff(iface='br-97c502071b88', filter = 'icmp[icmptype] == icmp-echo', prn = spoof_pkt)
```

ping 1.2.3.4

可以看到有伪造的 1.2.3.4 发出响应报文

No.	Time	Source	Destination	Protocol	Length	Info
365	2021-07-08 11:4…	10.9.0.5	1.2.3.4	ICMP	100	Echo (ping) request id=0x0029, seq=20/5120, ttl=64 (no respo…
366	2021-07-08 11:4…	1.2.3.4	10.9.0.5	ICMP	44	Echo (ping) reply id=0x0029, seq=20/5120, ttl=64
367	2021-07-08 11:4…	1.2.3.4	10.9.0.5	ICMP	44	Echo (ping) reply id=0x0029, seq=20/5120, ttl=64
368	2021-07-08 11:4…	10.9.0.5	1.2.3.4	ICMP	100	Echo (ping) request id=0x0029, seq=21/5376, ttl=64 (no respo…
369	2021-07-08 11:4…	10.9.0.5	1.2.3.4	ICMP	100	Echo (ping) request id=0x0029, seq=21/5376, ttl=64 (no respo…
370	2021-07-08 11:4…	1.2.3.4	10.9.0.5	ICMP	44	Echo (ping) reply id=0x0029, seq=21/5376, ttl=64
371	2021-07-08 11:4…	1.2.3.4	10.9.0.5	ICMP	44	Echo (ping) reply id=0x0029, seq=21/5376, ttl=64
372	2021-07-08 11:4…	10.9.0.5	1.2.3.4	ICMP	100	Echo (ping) request id=0x0029, seq=22/5632, ttl=64 (no respo…
373	2021-07-08 11:4…	10.9.0.5	1.2.3.4	ICMP	100	Echo (ping) request id=0x0029, seq=22/5632, ttl=64 (no respo…
374	2021-07-08 11:4…	1.2.3.4	10.9.0.5	ICMP	44	Echo (ping) reply id=0x0029, seq=22/5632, ttl=64
375	2021-07-08 11:4…	1.2.3.4	10.9.0.5	ICMP	44	Echo (ping) reply id=0x0029, seq=22/5632, ttl=64
376	2021-07-08 11:4…	10.9.0.5	1.2.3.4	ICMP	100	Echo (ping) request id=0x0029, seq=23/5888, ttl=64 (no respo…

ping 10.9.0.99

局域网内没有 icmp 报文，所以没有欺骗报文

242	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
243	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
244	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
245	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
246	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
247	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
248	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
249	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
250	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
251	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
252	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
253	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
254	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
255	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
256	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
257	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
258	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
259	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
260	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
261	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
262	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
343	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
344	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5
345	2021-07-08 11:5…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.99? Tell 10.9.0.5

ping 8.8.8.8

可以看到有伪造的 8.8.8.8 发出响应报文

2084	2021-07-08 12:0…	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x0031, seq=7/1792, ttl=64 (no respon…
2085	2021-07-08 12:0…	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x0031, seq=7/1792, ttl=64 (reply in …
2086	2021-07-08 12:0…	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x0031, seq=7/1792, ttl=64 (request i…
2087	2021-07-08 12:0…	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x0031, seq=7/1792, ttl=64
2088	2021-07-08 12:0…	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x0031, seq=8/2048, ttl=64 (no respon…
2089	2021-07-08 12:0…	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x0031, seq=8/2048, ttl=64 (reply in …
2090	2021-07-08 12:0…	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x0031, seq=8/2048, ttl=64 (request i…
2091	2021-07-08 12:0…	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x0031, seq=8/2048, ttl=64
2092	2021-07-08 12:0…	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x0031, seq=9/2304, ttl=64 (no respon…
2093	2021-07-08 12:0…	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x0031, seq=9/2304, ttl=64 (reply in …
2094	2021-07-08 12:0…	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x0031, seq=9/2304, ttl=64 (request i…
2095	2021-07-08 12:0…	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x0031, seq=9/2304, ttl=64