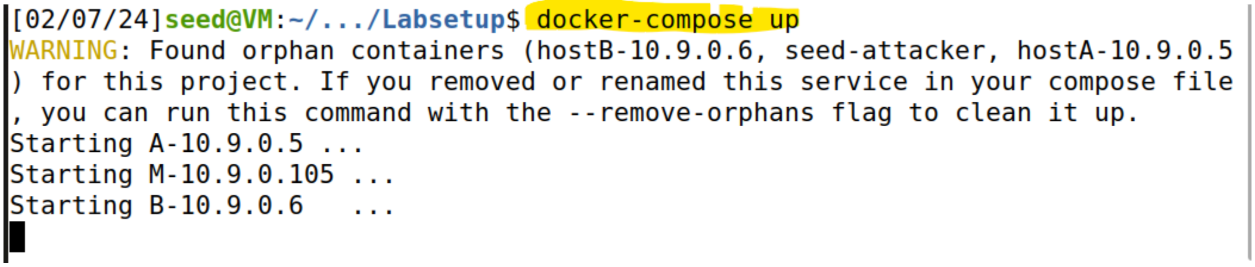
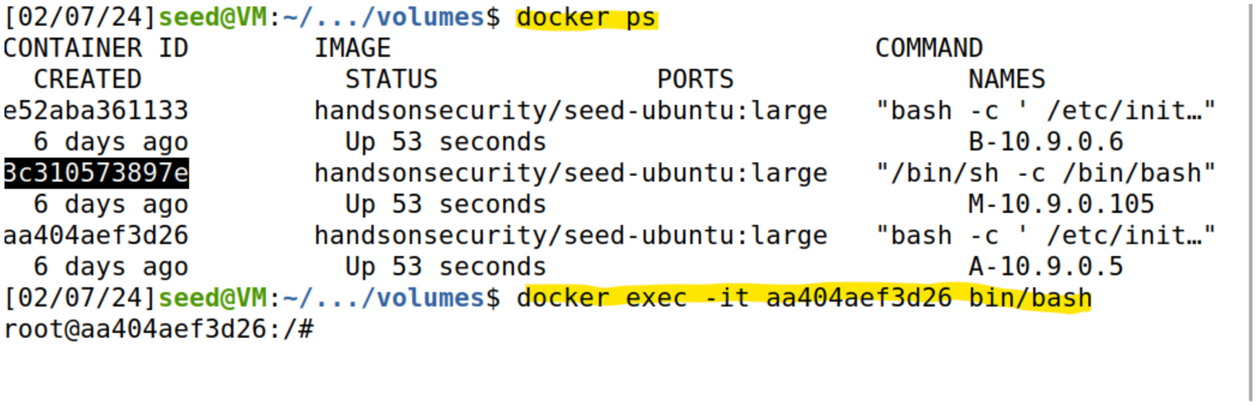
Cmpt280 _ Lab 4
Darion Kwasnitza - 3122890

1. **Setup Lan with Host A, Host B and Host M**

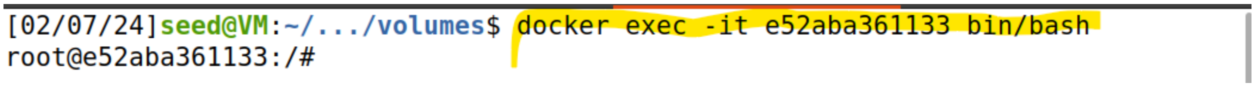


```
[02/07/24]seed@VM:~/.../Labsetup$ docker-compose up
WARNING: Found orphan containers (hostB-10.9.0.6, seed-attacker, hostA-10.9.0.5
) for this project. If you removed or renamed this service in your compose file
, you can run this command with the --remove-orphans flag to clean it up.
Starting A-10.9.0.5 ...
Starting M-10.9.0.105 ...
Starting B-10.9.0.6   ...
```

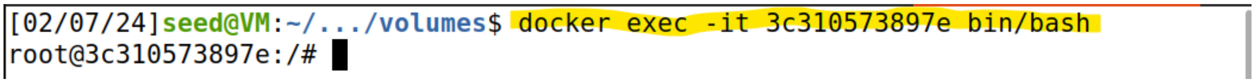
2. **Setup access to Host A, Host B and Host M using docker exec -it MAC bin/bash**



```
[02/07/24]seed@VM:~/.../volumes$ docker ps
CONTAINER ID        IMAGE                                COMMAND
  CREATED             STATUS              PORTS               NAMES
e52aba361133        handsonsecurity/seed-ubuntu:large   "bash -c ' /etc/init…"
  6 days ago          Up 53 seconds                           B-10.9.0.6
3c310573897e        handsonsecurity/seed-ubuntu:large   "/bin/sh -c /bin/bash"
  6 days ago          Up 53 seconds                           M-10.9.0.105
aa404aef3d26        handsonsecurity/seed-ubuntu:large   "bash -c ' /etc/init…"
  6 days ago          Up 53 seconds                           A-10.9.0.5
[02/07/24]seed@VM:~/.../volumes$ docker exec -it aa404aef3d26 bin/bash
root@aa404aef3d26:/#
```

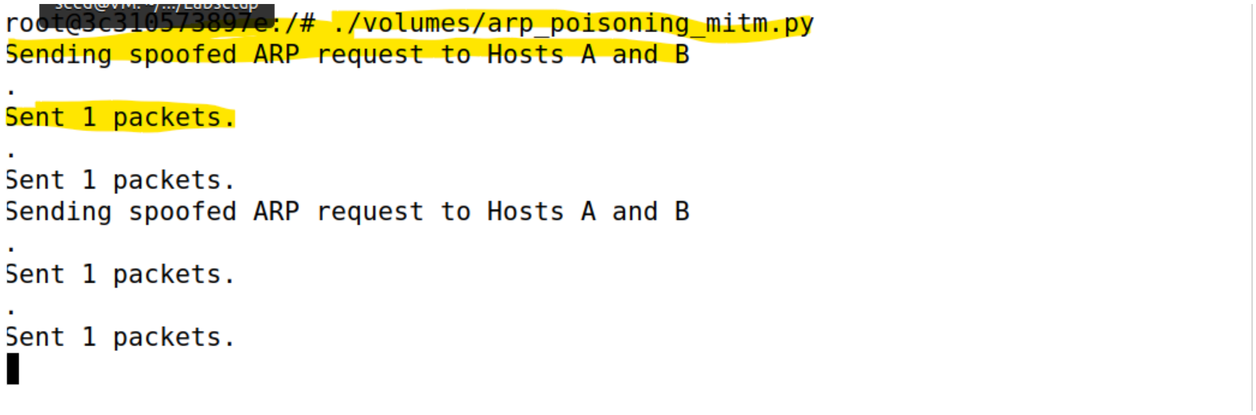


```
[02/07/24]seed@VM:~/.../volumes$ docker exec -it e52aba361133 bin/bash
root@e52aba361133:/#
```



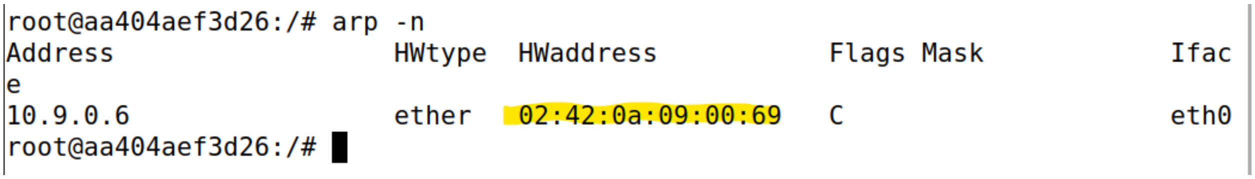
```
[02/07/24]seed@VM:~/.../volumes$ docker exec -it 3c310573897e bin/bash
root@3c310573897e:/#
```

3. **Launch attacker from Host M (Attacker) using ./volumes/arp_poisioning_mitm.py**

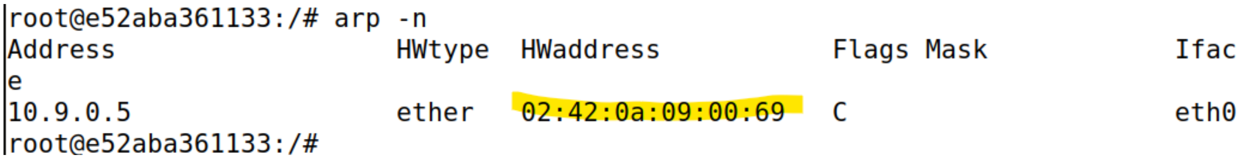


```
root@3c310573897e:/# ./volumes/arp_poisoning_mitm.py
Sending spoofed ARP request to Hosts A and B
.
Sent 1 packets.
.
Sent 1 packets.
Sending spoofed ARP request to Hosts A and B
.
Sent 1 packets.
.
Sent 1 packets.
```

4. **Check the ARP cache tables of Host A and Host B, HWaddress is changed for both to 02:42:0a:09:00:69, which is Host M HWaddress.**

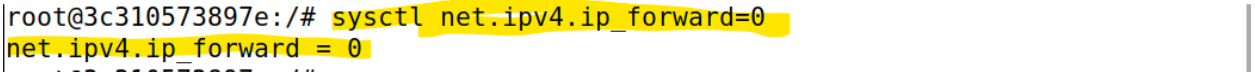


```
root@aa404aef3d26:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Ifac
e
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
root@aa404aef3d26:/# █
```

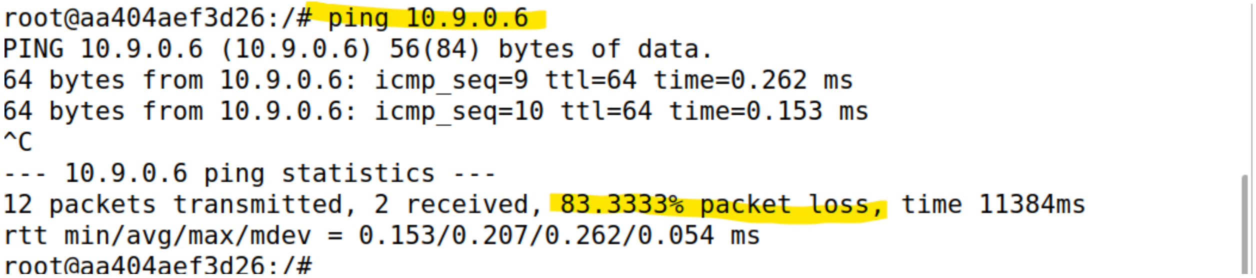


```
root@e52aba361133:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Ifac
e
10.9.0.5                 ether   02:42:0a:09:00:69   C                     eth0
root@e52aba361133:/#
```

5. **Stop IP forwarding on Host M using sysctl net.ipv4.io_forward=0, this results in packet loss between Host A and Host B**

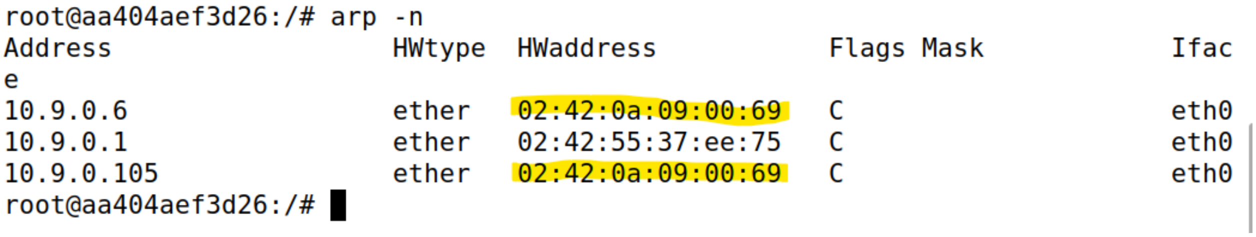


```
root@3c310573897e:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```



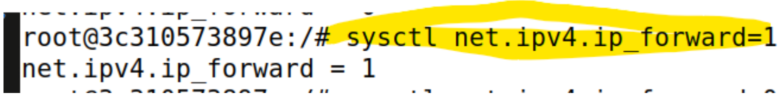
```
root@aa404aef3d26:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.262 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.153 ms
^C
--- 10.9.0.6 ping statistics ---
12 packets transmitted, 2 received, 83.3333% packet loss, time 11384ms
rtt min/avg/max/mdev = 0.153/0.207/0.262/0.054 ms
root@aa404aef3d26:/#
```

6. **The ARP cache tables are still manipulated, and my local machine is now manipulated as well.**

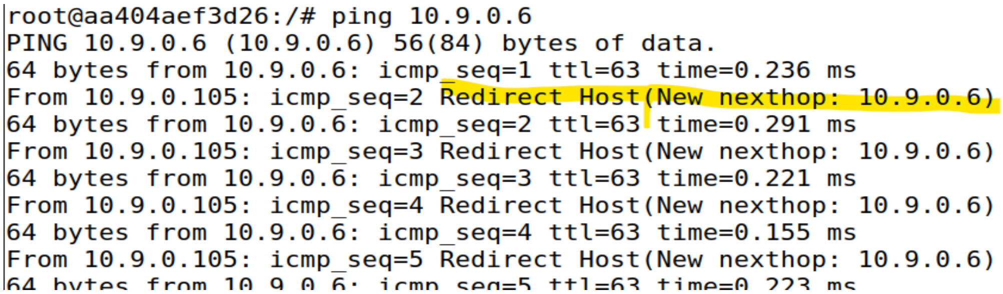


```
root@aa404aef3d26:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Ifac
e
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.1                 ether   02:42:55:37:ee:75   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
root@aa404aef3d26:/# █
```

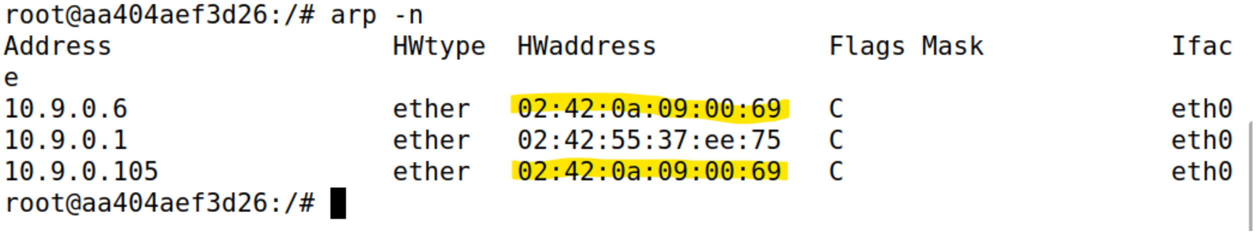
7. **Turn back on IP forwarding and ping Host B from Host A. If the packets are not directed to 10.9.0.6 then they become redirected to 10.9.0.6. The ARP cache of Host A has it's own HWaddress as 02:42:0a:09:00:69.**



```
root@3c310573897e:/# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

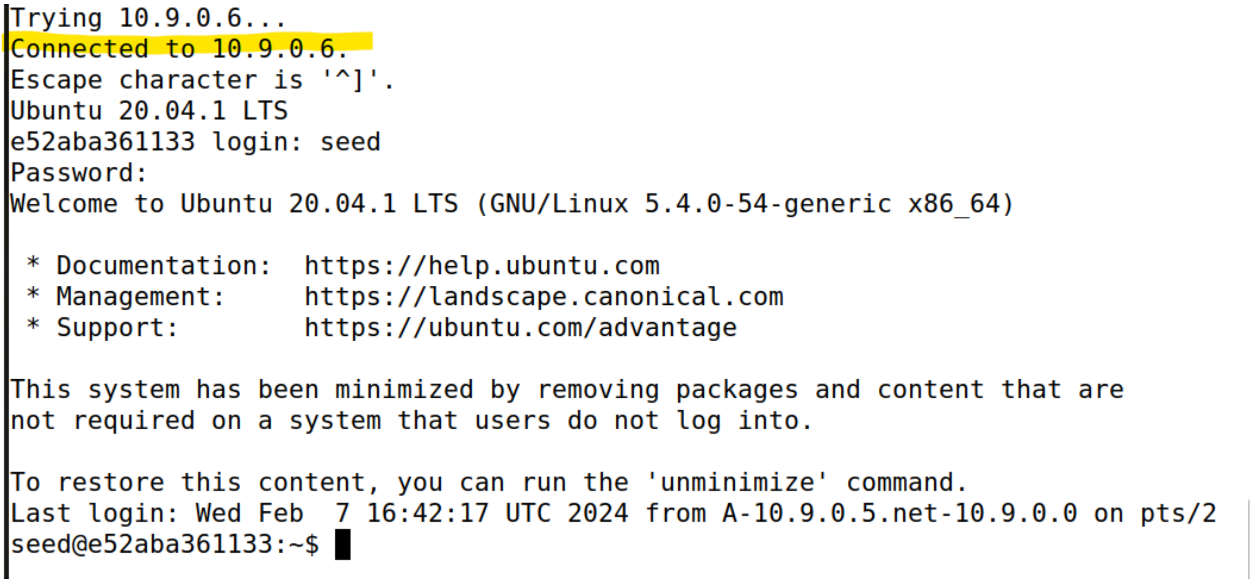


```
root@aa404aef3d26:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=63 time=0.236 ms
From 10.9.0.105: icmp_seq=2 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=2 ttl=63 time=0.291 ms
From 10.9.0.105: icmp_seq=3 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=3 ttl=63 time=0.221 ms
From 10.9.0.105: icmp_seq=4 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=4 ttl=63 time=0.155 ms
From 10.9.0.105: icmp_seq=5 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=5 ttl=63 time=0.223 ms
```



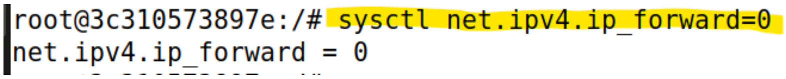
```
root@aa404aef3d26:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Ifac
e
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.1                 ether   02:42:55:37:ee:75   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
root@aa404aef3d26:/# 
```

8. **Make a telnet connection between Host A and Host B using telnet open 10.9.0.6**



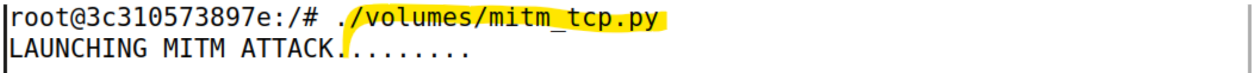
```
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
e52aba361133 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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 Feb  7 16:42:17 UTC 2024 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@e52aba361133:~$ 
```

9. **Inactivate IP forwarding on Host M**



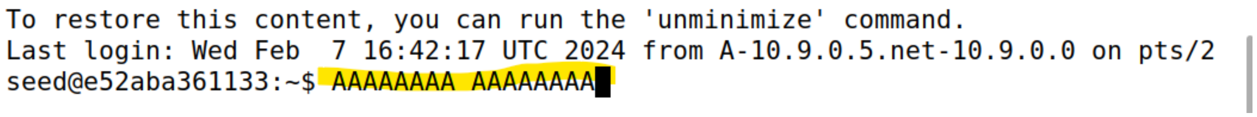
```
root@3c310573897e:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```

10. **Run attack code ./volumes/mitm_tcp.py**



```
root@3c310573897e:/# ./volumes/mitm_tcp.py
LAUNCHING MITM ATTACK.........
```

11. **Attempt to write "Network Security" on Host A, instead, everything typed is just A! This is because Host M has intercepted each packet going from Host A to Host B and has changed what is being seen on Host B's machine and being typed from Host A's machine.**



```
To restore this content, you can run the 'unminimize' command.
Last login: Wed Feb  7 16:42:17 UTC 2024 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@e52aba361133:~$ AAAAAAAA AAAAAAAA
```