ARP Cache Poisoning

+

Man-In-The-Middle Attack

Submitted By:
Fahim Morshed
SID: 1605077

There are **two main** steps of this attack. Following are the steps briefly:

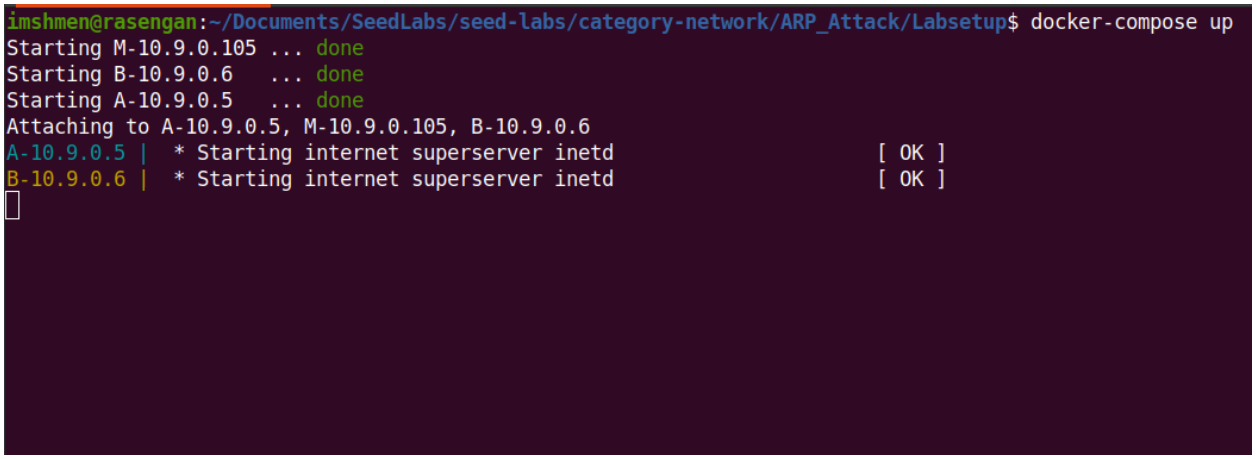
- **Poisoning the ARP cache table of the victims:**
    1. Create A raw socket to receive and send arp packets only: At first I created a raw socket that will only respond to ARP packets.
    2. Create ARP Request packets for victims: Let's assume we know the IP addresses of our victims but we need to know the hardware addresses. For that purpose I broadcasted ARP request packets to discover the MAC addresses of the victim IPs.
    3. Getting the MAC addresses of the victims: After receiving the ARP request packets that I broadcasted the victims will reply with their MAC addresses.
    4. Create ARP Reply packets for victims: Now we'll craft ARP reply packets and send them to the victim machines. In the ARP reply packets the source IP will be of the victims but the source MAC address will be mine (of the attacker).
    5. Keep victims arp cache poisoned: Finally we need to send the ARP reply packets continuously to the victims. Because after some delay the devices are going to resolute ARP again and again. We need to keep their ARP cache poisoned.

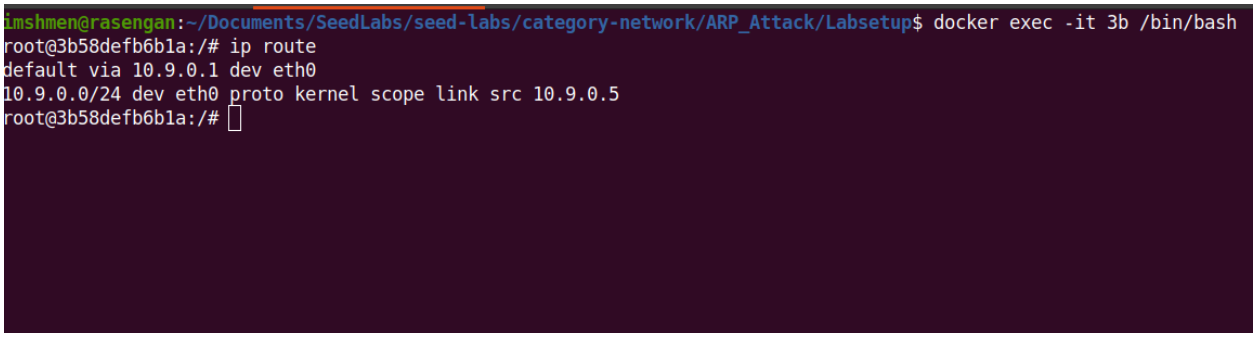
- **Being the man in the middle:**
    1. Create A raw socket to receive and send icmp packets packets only: Now we need to be the man in the middle in their communication. So to intercept the packets in the communication we are going to open a socket to receive the ICMP packets which pass us.
    2. Receive all the packets in the transmission channel: If our attack is successful we will receive all the packets between our victims. Now if the ip_forwarding is on in my (attacker) machine the machine will act as a router and forward the packets to the original IP.
    3. Read the packets and relay them back to the original destination: To be actually the man in the middle I will turn the ip_forwarding off and then intercept the packets. After intercepting the packet I sent the packets to their original destination to conceal my interception.

Snapshot of the steps of the attack :

Now attack snapshots is shown below sequentially:

1. **Setup:** The following pictures demonstrate the simulation setup. We will run 3 docker containers. Container A, B are victim hosts and container M is attacker. Their IP addresses along with their MAC addresses are also shown in the snapshots.





```
imshmen@rasengan:~/Documents/SeedLabs/seed-labs/category-network/ARP_Attack/Labsetup$ docker exec -it 63 /bin/bash
root@6372b19e94ed:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.6
root@6372b19e94ed:/#
```

```
imshmen@rasengan:~/Documents/SeedLabs/seed-labs/category-network/ARP_Attack/Labsetup$ docker exec -it df /bin/bash
root@df4696b6b6b5:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.105
root@df4696b6b6b5:/#
```

2. **Before attacking:** The following pictures demonstrate the arp cache table and the states of A, B and M before the attack. We will see the ARP cache table absolutely fine and if A pings B, M receives nothing.

```
root@3b58defb6b1a:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
root@3b58defb6b1a:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
root@3b58defb6b1a:/#
```

```
root@6372b19e94ed:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.6
root@6372b19e94ed:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.5                 ether   02:42:0a:09:00:05   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
root@6372b19e94ed:/#
```

```
root@df4696b6b6b5:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.105
root@df4696b6b6b5:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
10.9.0.5                 ether   02:42:0a:09:00:05   C                     eth0
root@df4696b6b6b5:/#
```

```
root@3b58defb6b1a:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
root@3b58defb6b1a:/# 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=0.150 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.086 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.103 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.106 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.101 ms
64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.120 ms
64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.123 ms
64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.157 ms
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.107 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.138 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.117 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.117 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.133 ms
```

```
root@6372b19e94ed:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.6
root@6372b19e94ed:/# 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
05:21:39.822303 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 9, length 64
05:21:39.822341 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 9, length 64
05:21:40.850375 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 10, length 64
05:21:40.850416 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 10, length 64
05:21:41.870371 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 11, length 64
05:21:41.870410 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 11, length 64
05:21:42.898349 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 12, length 64
05:21:42.898389 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 12, length 64
05:21:43.918302 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 13, length 64
05:21:43.918348 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 13, length 64
05:21:44.946239 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 14, length 64
05:21:44.946260 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 14, length 64
05:21:45.966346 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 15, length 64
05:21:45.966387 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 15, length 64
05:21:46.990299 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 16, length 64
05:21:46.990324 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 16, length 64
05:21:48.018298 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 17, length 64
05:21:48.018344 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 17, length 64
```

```
root@df4696b6b6b5:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.105
root@df4696b6b6b5:/# 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
```

3. **After attacking:** Now we'll launch the attack. First we'll run the spoof script to poison A and B's arp cache. We'll see that their cache is poisoned and if they communicate their packets will go through M. After that we'll turn the IP forwarding off and see that the communication is stopped but M will continue to receive packets. This proves that ARP cache poisoning and Man in the middle attack is successful in this process. Finally we'll relay the packets to their original IP destination to conceal our identity by running the sniffing script. Notice these in the snapshots below.

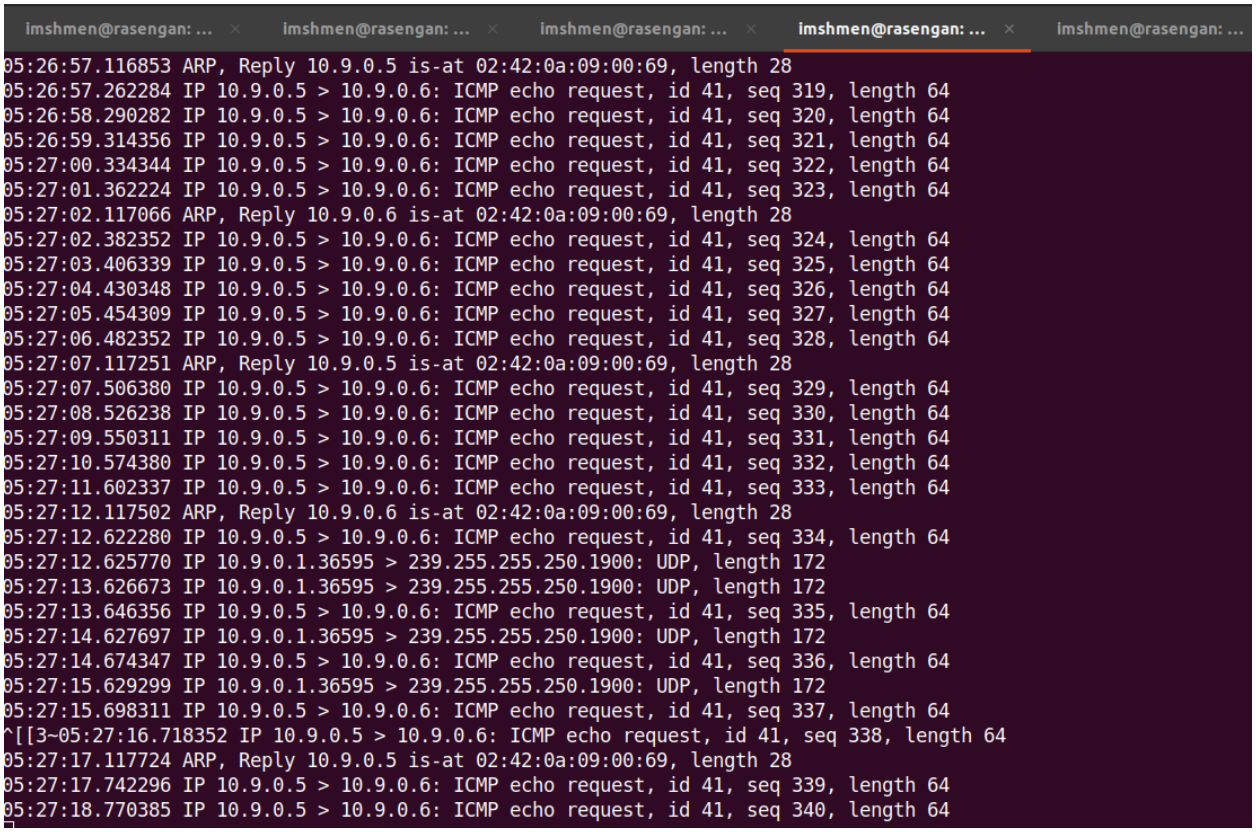
```
root@df4696b6b6b5:/volumes/mitm# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.105
root@df4696b6b6b5:/volumes/mitm# ./spoof/spoof
[*] Attacker MAC address: 02:42:0A:09:00:69
[+] Got index '9' from interface 'eth0'
[+] ETHER packet created
[+] Packet sent to broadcast
[*] Listening for target response...
[+] Got response from victim
[*] Sender MAC address: 02:42:0A:09:00:05
[*] Sender ip address: 10.09.00.05
[*] Target MAC address: 02:42:0A:09:00:69
[*] Target ip address: 10.09.00.06
[*] Victim's MAC address: 02:42:0A:09:00:05
[+] ETHER packet created
[+] Packet sent to broadcast
[*] Listening for target response...
[+] Got response from victim
[*] Sender MAC address: 02:42:0A:09:00:06
[*] Sender ip address: 10.09.00.06
[*] Target MAC address: 02:42:0A:09:00:69
[*] Target ip address: 10.09.00.05
[*] Victim's MAC address: 02:42:0A:09:00:06
[+] SPOOFED Packet sent to '10.9.0.6'
[+] SPOOFED Packet sent to '10.9.0.5'
[+] SPOOFED Packet sent to '10.9.0.6'
[+] SPOOFED Packet sent to '10.9.0.5'
[+] SPOOFED Packet sent to '10.9.0.6'
[+] SPOOFED Packet sent to '10.9.0.5'
```

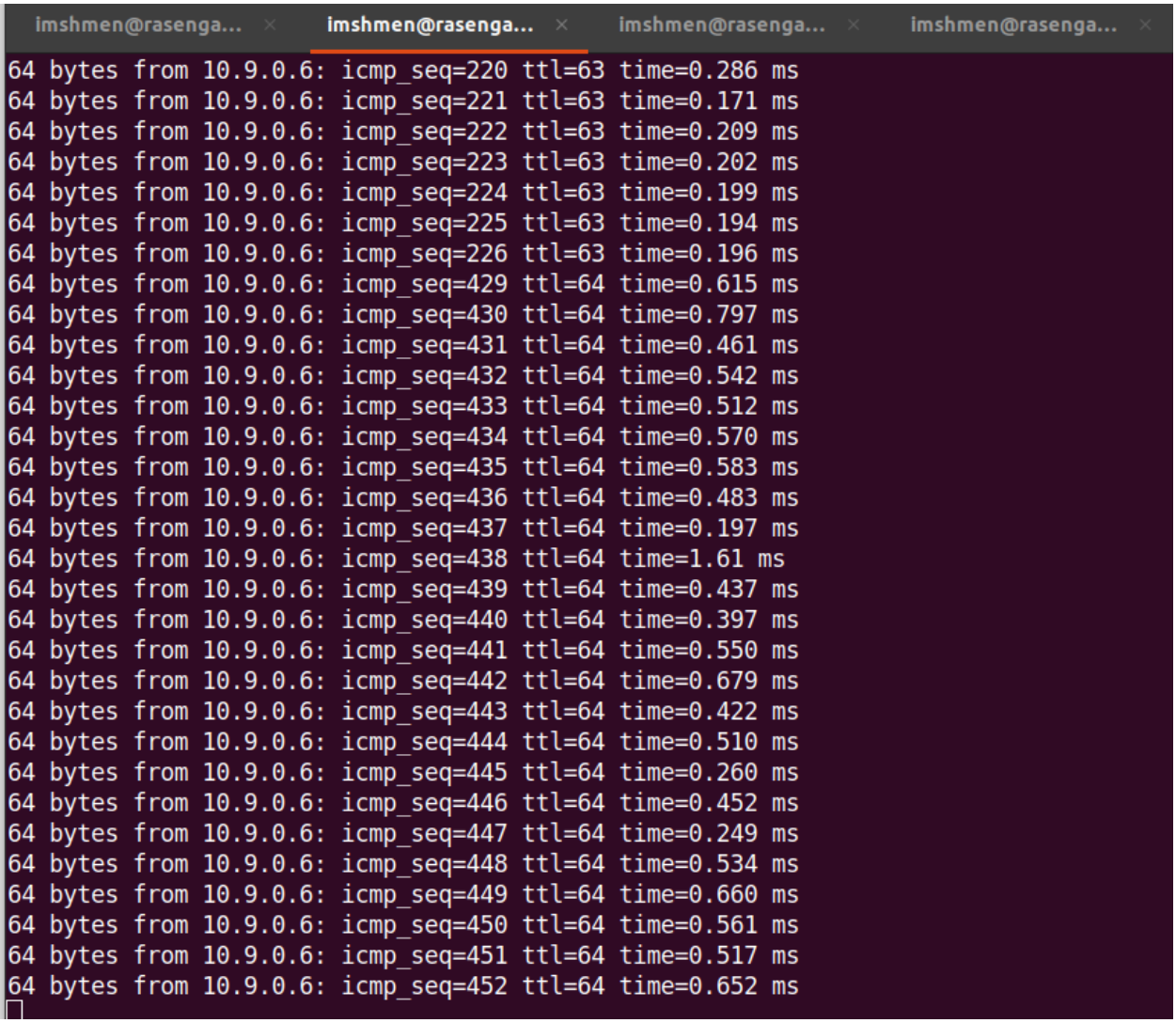
```
root@3b58defb6b1a:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
root@3b58defb6b1a:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
root@3b58defb6b1a:/#
```

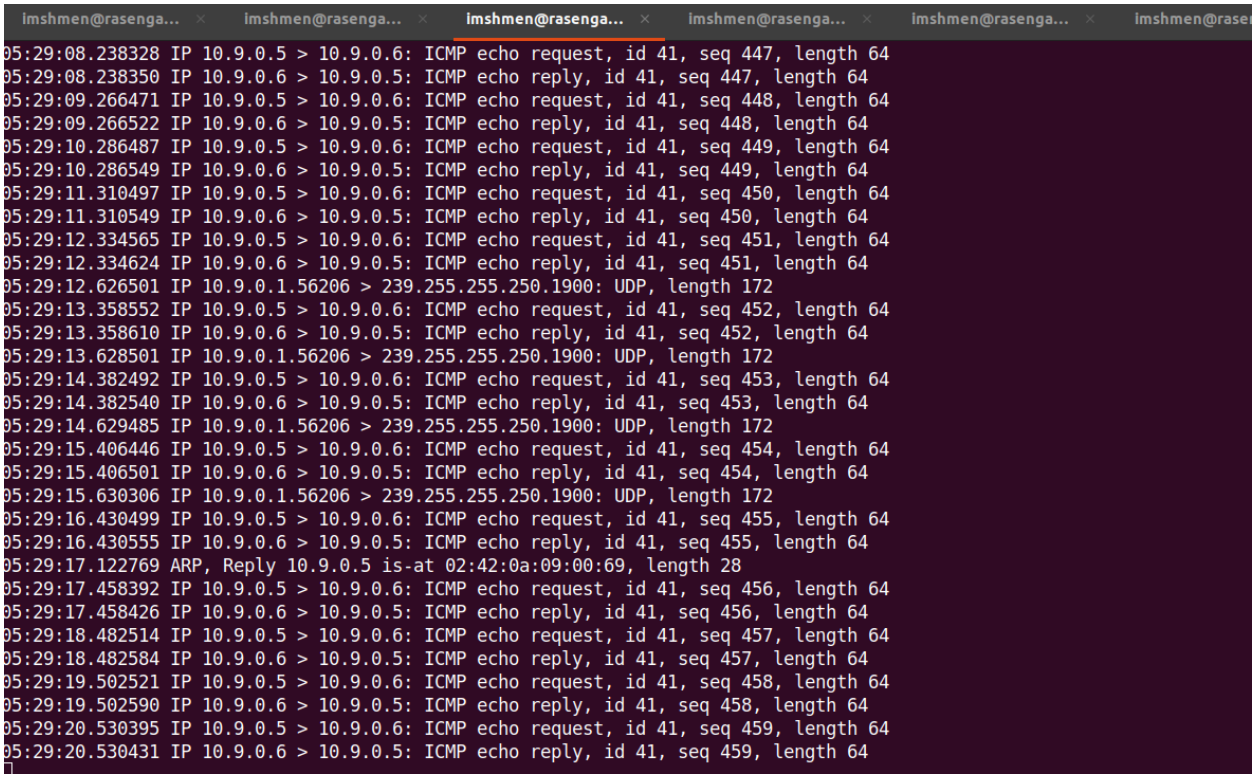
```
root@6372b19e94ed:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.6
root@6372b19e94ed:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
10.9.0.5                 ether   02:42:0a:09:00:69   C                     eth0
root@6372b19e94ed:/#
```

```
root@df4696b6b6b5:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.105
root@df4696b6b6b5:/# 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
05:23:12.622867 IP 10.9.0.1.44108 > 239.255.255.250.1900: UDP, length 172
05:23:13.623879 IP 10.9.0.1.44108 > 239.255.255.250.1900: UDP, length 172
05:23:14.624728 IP 10.9.0.1.44108 > 239.255.255.250.1900: UDP, length 172
05:23:15.625667 IP 10.9.0.1.44108 > 239.255.255.250.1900: UDP, length 172
05:23:57.108177 ARP, Request who-has 10.9.0.5 (ff:ff:ff:ff:ff:ff) tell 10.9.0.6, length 28
05:23:57.108282 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
05:23:57.108664 ARP, Request who-has 10.9.0.6 (ff:ff:ff:ff:ff:ff) tell 10.9.0.5, length 28
05:23:57.108739 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:06, length 28
05:23:57.109054 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:23:58.066291 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 144, length 64
05:23:58.066353 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 144, length 64
05:23:58.066430 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 144, length 64
05:23:58.066450 IP 10.9.0.105 > 10.9.0.6: ICMP redirect 10.9.0.5 to host 10.9.0.5, length 92
05:23:58.066456 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 144, length 64
05:23:59.086316 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 145, length 64
05:23:59.086369 IP 10.9.0.105 > 10.9.0.5: ICMP redirect 10.9.0.6 to host 10.9.0.6, length 92
05:23:59.086376 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 145, length 64
05:23:59.086456 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 145, length 64
05:23:59.086472 IP 10.9.0.105 > 10.9.0.6: ICMP redirect 10.9.0.5 to host 10.9.0.5, length 92
05:23:59.086477 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 145, length 64
05:24:00.110332 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 146, length 64
05:24:00.110383 IP 10.9.0.105 > 10.9.0.5: ICMP redirect 10.9.0.6 to host 10.9.0.6, length 92
05:24:00.110391 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 146, length 64
05:24:00.110475 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 146, length 64
05:24:00.110501 IP 10.9.0.105 > 10.9.0.6: ICMP redirect 10.9.0.5 to host 10.9.0.5, length 92
05:24:00.110506 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 146, length 64
```

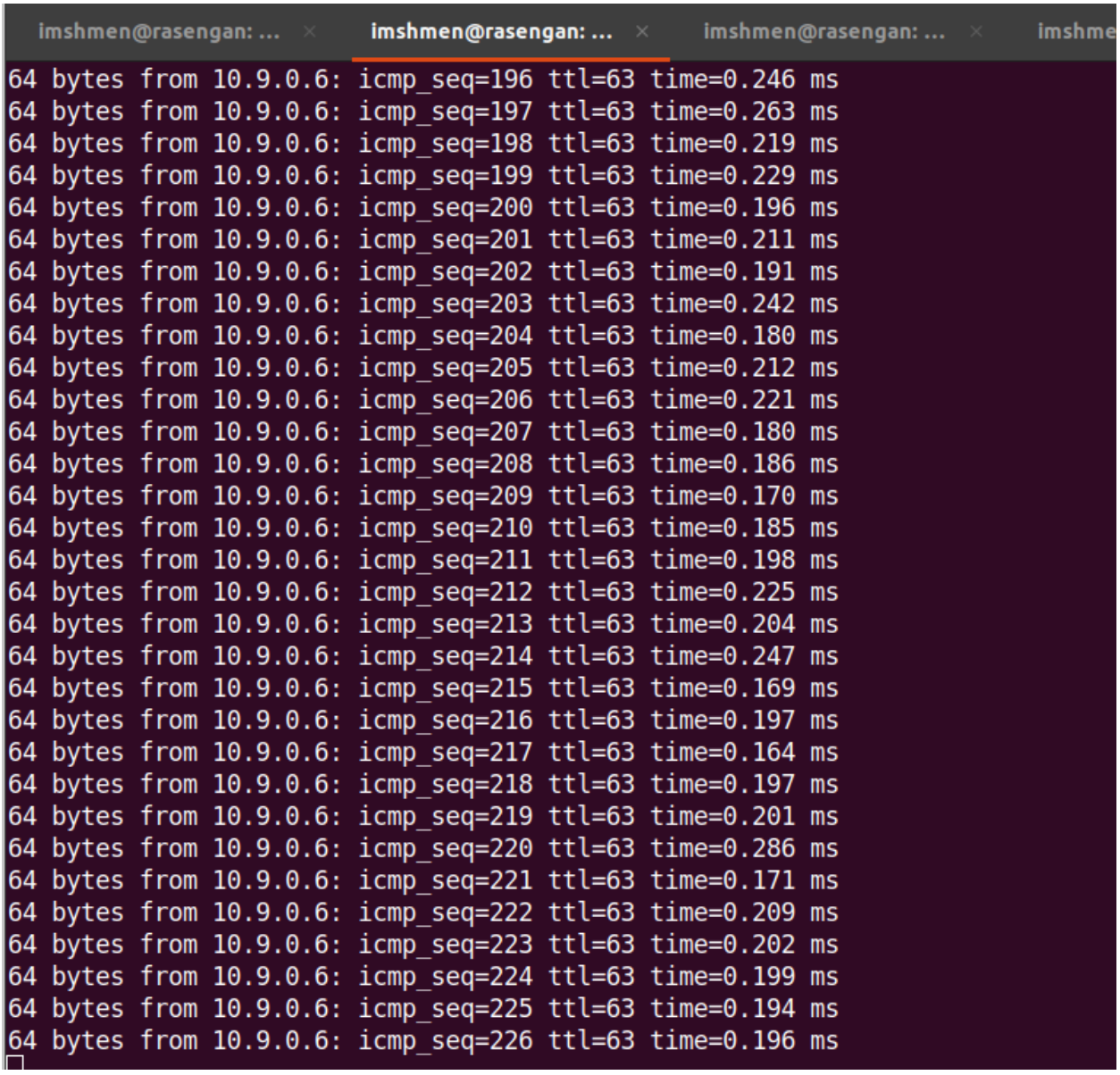
```
root@df4696b6b6b5:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.105
root@df4696b6b6b5:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@df4696b6b6b5:/#
```

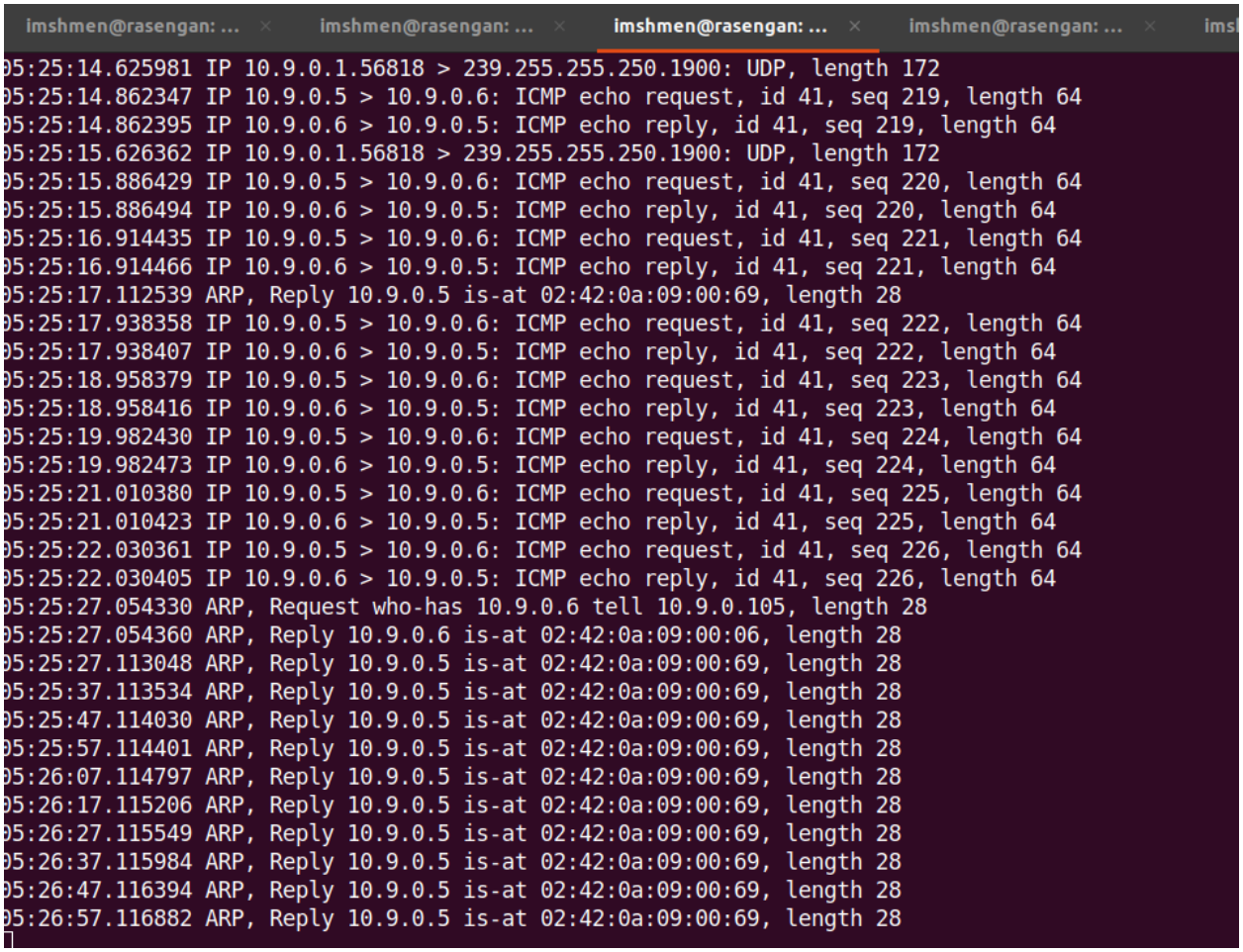

imshmen@rasengan: ...
imshmen@rasengan: ...
imshmen@rasengan: ...
imshmen@rasengan: ...
imshmen@rasengan: ...
05:26:57.116853 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:26:57.262284 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 319, length 64
05:26:58.290282 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 320, length 64
05:26:59.314356 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 321, length 64
05:27:00.334344 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 322, length 64
05:27:01.362224 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 323, length 64
05:27:02.117066 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
05:27:02.382352 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 324, length 64
05:27:03.406339 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 325, length 64
05:27:04.430348 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 326, length 64
05:27:05.454309 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 327, length 64
05:27:06.482352 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 328, length 64
05:27:07.117251 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:27:07.506380 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 329, length 64
05:27:08.526238 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 330, length 64
05:27:09.550311 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 331, length 64
05:27:10.574380 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 332, length 64
05:27:11.602337 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 333, length 64
05:27:12.117502 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
05:27:12.622280 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 334, length 64
05:27:12.625770 IP 10.9.0.1.36595 > 239.255.255.250.1900: UDP, length 172
05:27:13.626673 IP 10.9.0.1.36595 > 239.255.255.250.1900: UDP, length 172
05:27:13.646356 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 335, length 64
05:27:14.627697 IP 10.9.0.1.36595 > 239.255.255.250.1900: UDP, length 172
05:27:14.674347 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 336, length 64
05:27:15.629299 IP 10.9.0.1.36595 > 239.255.255.250.1900: UDP, length 172
05:27:15.698311 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 337, length 64
^[[3~05:27:16.718352 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 338, length 64
05:27:17.117724 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:27:17.742296 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 339, length 64
05:27:18.770385 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 340, length 64


imshmen@rasenga...
imshmen@rasenga...
imshmen@rasenga...
imshmen@rasenga...
64 bytes from 10.9.0.6: icmp_seq=220 ttl=63 time=0.286 ms
64 bytes from 10.9.0.6: icmp_seq=221 ttl=63 time=0.171 ms
64 bytes from 10.9.0.6: icmp_seq=222 ttl=63 time=0.209 ms
64 bytes from 10.9.0.6: icmp_seq=223 ttl=63 time=0.202 ms
64 bytes from 10.9.0.6: icmp_seq=224 ttl=63 time=0.199 ms
64 bytes from 10.9.0.6: icmp_seq=225 ttl=63 time=0.194 ms
64 bytes from 10.9.0.6: icmp_seq=226 ttl=63 time=0.196 ms
64 bytes from 10.9.0.6: icmp_seq=429 ttl=64 time=0.615 ms
64 bytes from 10.9.0.6: icmp_seq=430 ttl=64 time=0.797 ms
64 bytes from 10.9.0.6: icmp_seq=431 ttl=64 time=0.461 ms
64 bytes from 10.9.0.6: icmp_seq=432 ttl=64 time=0.542 ms
64 bytes from 10.9.0.6: icmp_seq=433 ttl=64 time=0.512 ms
64 bytes from 10.9.0.6: icmp_seq=434 ttl=64 time=0.570 ms
64 bytes from 10.9.0.6: icmp_seq=435 ttl=64 time=0.583 ms
64 bytes from 10.9.0.6: icmp_seq=436 ttl=64 time=0.483 ms
64 bytes from 10.9.0.6: icmp_seq=437 ttl=64 time=0.197 ms
64 bytes from 10.9.0.6: icmp_seq=438 ttl=64 time=1.61 ms
64 bytes from 10.9.0.6: icmp_seq=439 ttl=64 time=0.437 ms
64 bytes from 10.9.0.6: icmp_seq=440 ttl=64 time=0.397 ms
64 bytes from 10.9.0.6: icmp_seq=441 ttl=64 time=0.550 ms
64 bytes from 10.9.0.6: icmp_seq=442 ttl=64 time=0.679 ms
64 bytes from 10.9.0.6: icmp_seq=443 ttl=64 time=0.422 ms
64 bytes from 10.9.0.6: icmp_seq=444 ttl=64 time=0.510 ms
64 bytes from 10.9.0.6: icmp_seq=445 ttl=64 time=0.260 ms
64 bytes from 10.9.0.6: icmp_seq=446 ttl=64 time=0.452 ms
64 bytes from 10.9.0.6: icmp_seq=447 ttl=64 time=0.249 ms
64 bytes from 10.9.0.6: icmp_seq=448 ttl=64 time=0.534 ms
64 bytes from 10.9.0.6: icmp_seq=449 ttl=64 time=0.660 ms
64 bytes from 10.9.0.6: icmp_seq=450 ttl=64 time=0.561 ms
64 bytes from 10.9.0.6: icmp_seq=451 ttl=64 time=0.517 ms
64 bytes from 10.9.0.6: icmp_seq=452 ttl=64 time=0.652 ms


imshmen@rasenga...
imshmen@rasenga...
imshmen@rasenga...
imshmen@rasenga...
imshmen@rasenga...
05:29:08.238328 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 447, length 64
05:29:08.238350 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 447, length 64
05:29:09.266471 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 448, length 64
05:29:09.266522 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 448, length 64
05:29:10.286487 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 449, length 64
05:29:10.286549 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 449, length 64
05:29:11.310497 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 450, length 64
05:29:11.310549 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 450, length 64
05:29:12.334565 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 451, length 64
05:29:12.334624 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 451, length 64
05:29:12.626501 IP 10.9.0.1.56206 > 239.255.255.250.1900: UDP, length 172
05:29:13.358552 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 452, length 64
05:29:13.358610 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 452, length 64
05:29:13.628501 IP 10.9.0.1.56206 > 239.255.255.250.1900: UDP, length 172
05:29:14.382492 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 453, length 64
05:29:14.382540 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 453, length 64
05:29:14.629485 IP 10.9.0.1.56206 > 239.255.255.250.1900: UDP, length 172
05:29:15.406446 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 454, length 64
05:29:15.406501 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 454, length 64
05:29:15.630306 IP 10.9.0.1.56206 > 239.255.255.250.1900: UDP, length 172
05:29:16.430499 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 455, length 64
05:29:16.430555 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 455, length 64
05:29:17.122769 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:29:17.458392 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 456, length 64
05:29:17.458426 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 456, length 64
05:29:18.482514 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 457, length 64
05:29:18.482584 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 457, length 64
05:29:19.502521 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 458, length 64
05:29:19.502590 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 458, length 64
05:29:20.530395 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 459, length 64
05:29:20.530431 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 459, length 64

```
root@df4696b6b6b5:/volumes/mitm# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.105
root@df4696b6b6b5:/volumes/mitm# ./sniff/sniff
Starting...
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:06
Echo request sent from 02:42:0A:09:00:69 to 02:42:0A:09:00:05
```


imshmen@rasengan: ...
imshmen@rasengan: ...
imshmen@rasengan: ...
imshme
64 bytes from 10.9.0.6: icmp_seq=196 ttl=63 time=0.246 ms
64 bytes from 10.9.0.6: icmp_seq=197 ttl=63 time=0.263 ms
64 bytes from 10.9.0.6: icmp_seq=198 ttl=63 time=0.219 ms
64 bytes from 10.9.0.6: icmp_seq=199 ttl=63 time=0.229 ms
64 bytes from 10.9.0.6: icmp_seq=200 ttl=63 time=0.196 ms
64 bytes from 10.9.0.6: icmp_seq=201 ttl=63 time=0.211 ms
64 bytes from 10.9.0.6: icmp_seq=202 ttl=63 time=0.191 ms
64 bytes from 10.9.0.6: icmp_seq=203 ttl=63 time=0.242 ms
64 bytes from 10.9.0.6: icmp_seq=204 ttl=63 time=0.180 ms
64 bytes from 10.9.0.6: icmp_seq=205 ttl=63 time=0.212 ms
64 bytes from 10.9.0.6: icmp_seq=206 ttl=63 time=0.221 ms
64 bytes from 10.9.0.6: icmp_seq=207 ttl=63 time=0.180 ms
64 bytes from 10.9.0.6: icmp_seq=208 ttl=63 time=0.186 ms
64 bytes from 10.9.0.6: icmp_seq=209 ttl=63 time=0.170 ms
64 bytes from 10.9.0.6: icmp_seq=210 ttl=63 time=0.185 ms
64 bytes from 10.9.0.6: icmp_seq=211 ttl=63 time=0.198 ms
64 bytes from 10.9.0.6: icmp_seq=212 ttl=63 time=0.225 ms
64 bytes from 10.9.0.6: icmp_seq=213 ttl=63 time=0.204 ms
64 bytes from 10.9.0.6: icmp_seq=214 ttl=63 time=0.247 ms
64 bytes from 10.9.0.6: icmp_seq=215 ttl=63 time=0.169 ms
64 bytes from 10.9.0.6: icmp_seq=216 ttl=63 time=0.197 ms
64 bytes from 10.9.0.6: icmp_seq=217 ttl=63 time=0.164 ms
64 bytes from 10.9.0.6: icmp_seq=218 ttl=63 time=0.197 ms
64 bytes from 10.9.0.6: icmp_seq=219 ttl=63 time=0.201 ms
64 bytes from 10.9.0.6: icmp_seq=220 ttl=63 time=0.286 ms
64 bytes from 10.9.0.6: icmp_seq=221 ttl=63 time=0.171 ms
64 bytes from 10.9.0.6: icmp_seq=222 ttl=63 time=0.209 ms
64 bytes from 10.9.0.6: icmp_seq=223 ttl=63 time=0.202 ms
64 bytes from 10.9.0.6: icmp_seq=224 ttl=63 time=0.199 ms
64 bytes from 10.9.0.6: icmp_seq=225 ttl=63 time=0.194 ms
64 bytes from 10.9.0.6: icmp_seq=226 ttl=63 time=0.196 ms


imshmen@rasengan: ...
imshmen@rasengan: ...
imshmen@rasengan: ...
imshmen@rasengan: ...
05:25:14.625981 IP 10.9.0.1.56818 > 239.255.255.250.1900: UDP, length 172
05:25:14.862347 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 219, length 64
05:25:14.862395 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 219, length 64
05:25:15.626362 IP 10.9.0.1.56818 > 239.255.255.250.1900: UDP, length 172
05:25:15.886429 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 220, length 64
05:25:15.886494 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 220, length 64
05:25:16.914435 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 221, length 64
05:25:16.914466 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 221, length 64
05:25:17.112539 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:25:17.938358 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 222, length 64
05:25:17.938407 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 222, length 64
05:25:18.958379 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 223, length 64
05:25:18.958416 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 223, length 64
05:25:19.982430 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 224, length 64
05:25:19.982473 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 224, length 64
05:25:21.010380 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 225, length 64
05:25:21.010423 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 225, length 64
05:25:22.030361 IP 10.9.0.5 > 10.9.0.6: ICMP echo request, id 41, seq 226, length 64
05:25:22.030405 IP 10.9.0.6 > 10.9.0.5: ICMP echo reply, id 41, seq 226, length 64
05:25:27.054330 ARP, Request who-has 10.9.0.6 tell 10.9.0.105, length 28
05:25:27.054360 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:06, length 28
05:25:27.113048 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:25:37.113534 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:25:47.114030 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:25:57.114401 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:26:07.114797 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:26:17.115206 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:26:27.115549 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:26:37.115984 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:26:47.116394 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28
05:26:57.116882 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:69, length 28

Conclusion:

Now I conclude that with the snapshots given and the justification logic given, my attack was successful.