ICMP Redirect Attack Lab

2022

Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No: ICMP Attack
	Section: B	Date: 20/10/2022

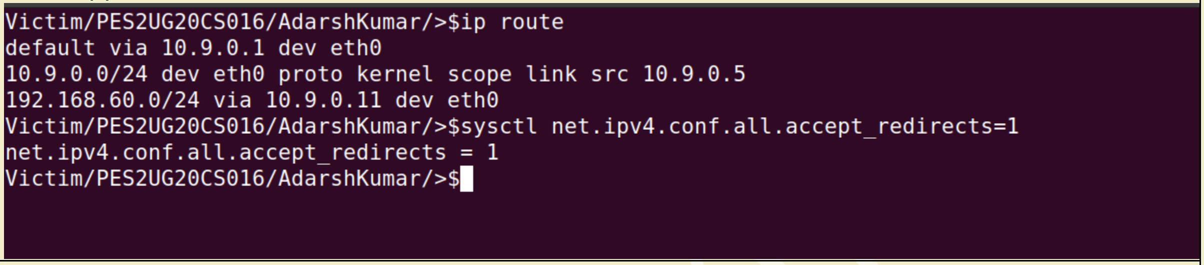
Task 1: Launching ICMP Redirect Attack

Screenshot of command

# ip route

# sysctl net.ipv4.conf.all.accept_redirects=1

We stopped the counter measure of the ICMP Redirect attack

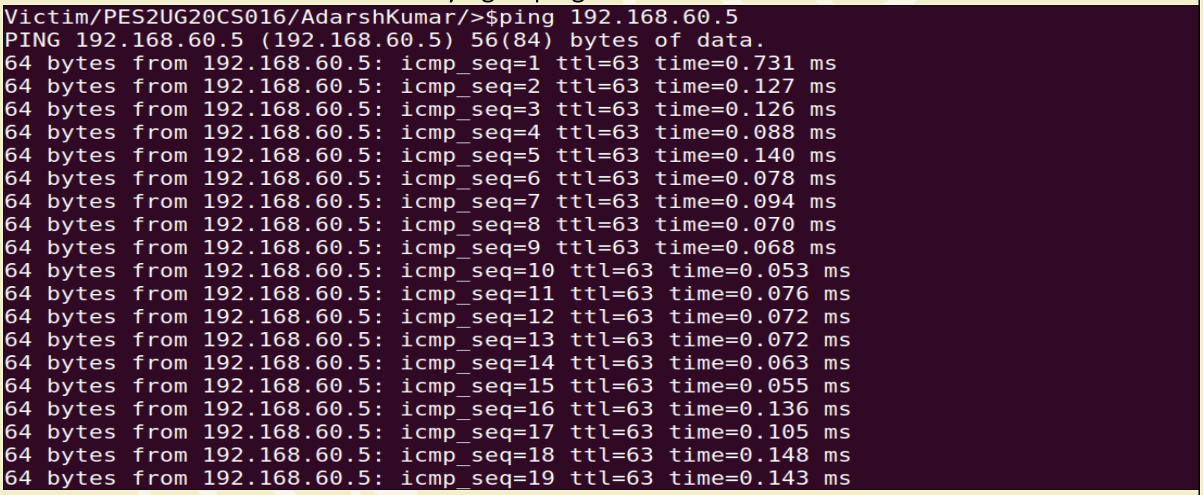


```
Victim/PES2UG20CS016/AdarshKumar/>$ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
192.168.60.0/24 via 10.9.0.11 dev eth0
Victim/PES2UG20CS016/AdarshKumar/>$sysctl net.ipv4.conf.all.accept_redirects=1
net.ipv4.conf.all.accept_redirects = 1
Victim/PES2UG20CS016/AdarshKumar/>$
```

Task 1A

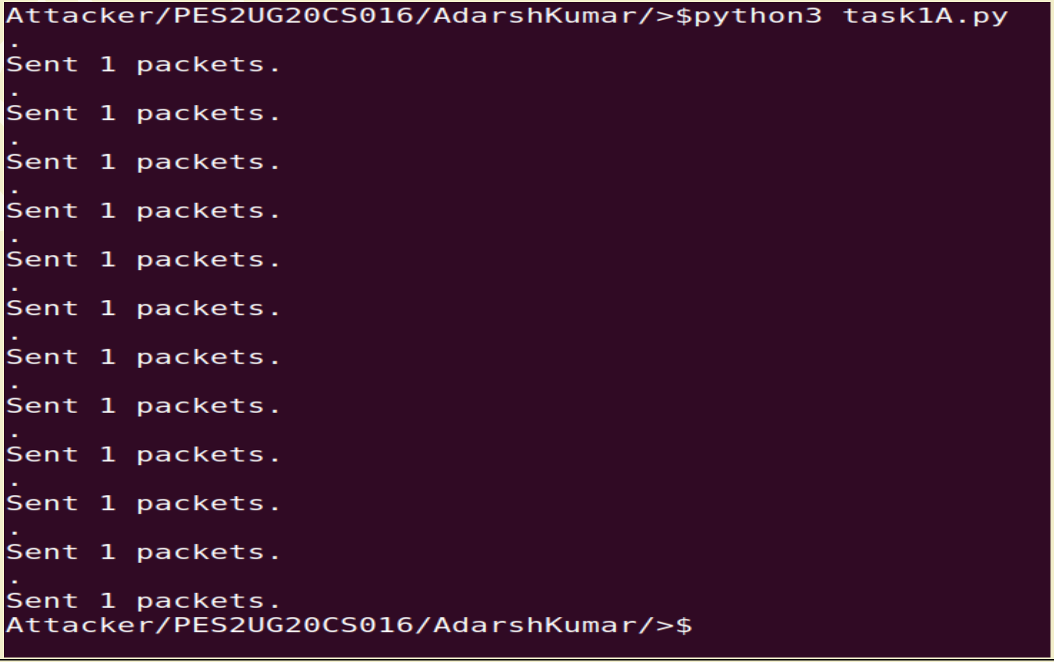
make the Victim Machine route its packets through the Malicious router

Here from victim’s terminal we are trying to ping host 192.168.60.5



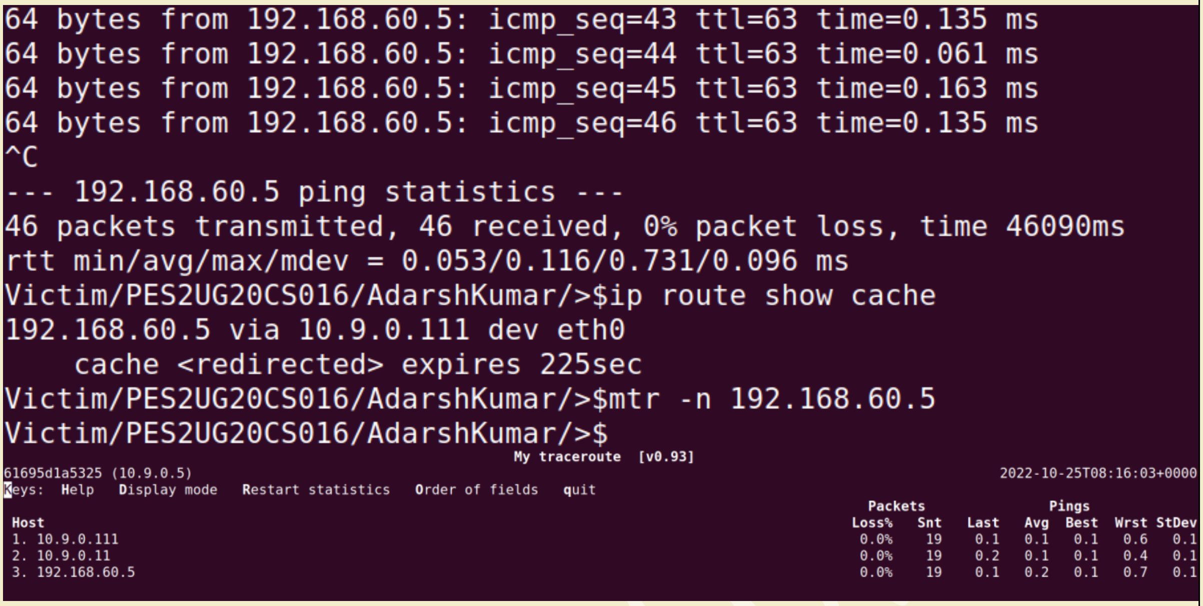
```
Victim/PES2UG20CS016/AdarshKumar/>$ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.731 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.127 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.088 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.140 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.078 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.070 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.068 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.053 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.076 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.055 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.136 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.105 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.148 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.143 ms
```

When the victim was pinging the host, we launched a ICMP redirect attack which sent redried message to the victim machine



```
Attacker/PES2UG20CS016/AdarshKumar/>$python3 task1A.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
Attacker/PES2UG20CS016/AdarshKumar/>$
```

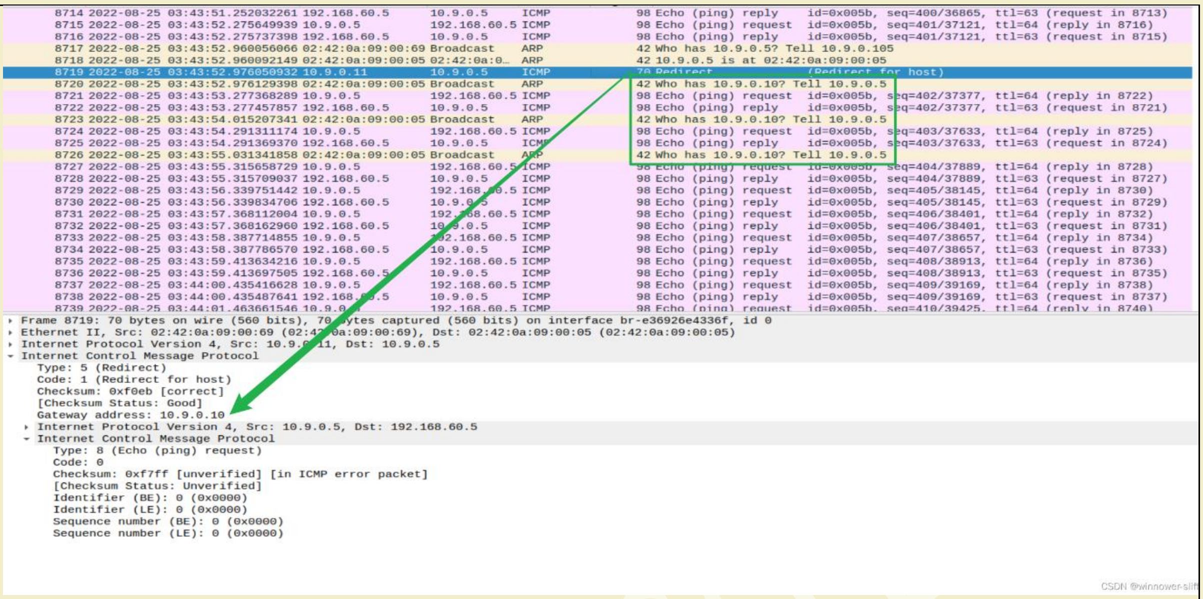
<table>
<tr>
<td></td>
<td>



```
64 bytes from 192.168.60.5: icmp_seq=43 ttl=63 time=0.135 ms
64 bytes from 192.168.60.5: icmp_seq=44 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=45 ttl=63 time=0.163 ms
64 bytes from 192.168.60.5: icmp_seq=46 ttl=63 time=0.135 ms
^C
--- 192.168.60.5 ping statistics ---
46 packets transmitted, 46 received, 0% packet loss, time 46090ms
rtt min/avg/max/mdev = 0.053/0.116/0.731/0.096 ms
Victim/PES2UG20CS016/AdarshKumar/>$ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 225sec
Victim/PES2UG20CS016/AdarshKumar/>$mtr -n 192.168.60.5
Victim/PES2UG20CS016/AdarshKumar/>$
                                   My traceroute  [v0.93]
61695d1a5325 (10.9.0.5)                                            2022-10-25T08:16:03+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                  Packets               Pings
 Host                                           Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.111                                   0.0%    19    0.1   0.1   0.1   0.6   0.1
 2. 10.9.0.11                                    0.0%    19    0.2   0.1   0.1   0.4   0.1
 3. 192.168.60.5                                 0.0%    19    0.1   0.2   0.1   0.7   0.1
```

We can see in the cache of the victim container that it is trying to reach host 198.168.60.5 from our malicious-Router 10.9.0.111 not from the genuine router 10.9.0.11 this can be also observed via mtr command clearly.

</td>
</tr>
<tr>
<td>Question 1:</td>
<td>Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gw is a computer not on the local LAN. Please show your experiment result, and explain your observation.</td>
</tr>
<tr>
<td>Solution</td>
<td>NO, we cannot use ICMP redirect attacks to redirect to a remote machine.
There are usually two situations in which an ICMP redirect occurs:
1) When the router receives data from an interface and needs to forward the data from the same interface;
2) When the router finds that the source IP address and the next hop belong to the same network segment when sending data to the remote network from an interface.
Both of these conditions require the redirected address to be on the same LAN as itself. If the redirected gateway points to an address not on the same LAN (eg 8.8.8.8), it will not be written to the victim's cache.
NOTE: (Since it has not been written, the screenshot is not shown)</td>
</tr>
<tr>
<td>Question 2:</td>
<td>Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation</td>
</tr>
<tr>
<td>Solution</td>
<td>I cannot use ICMP redirect attacks to redirect to a non-existing machine on the same network. I tried to direct the victim message to a non-existent URL 10.9.0.10, and the figure appeared:</td>
</tr>
</table>

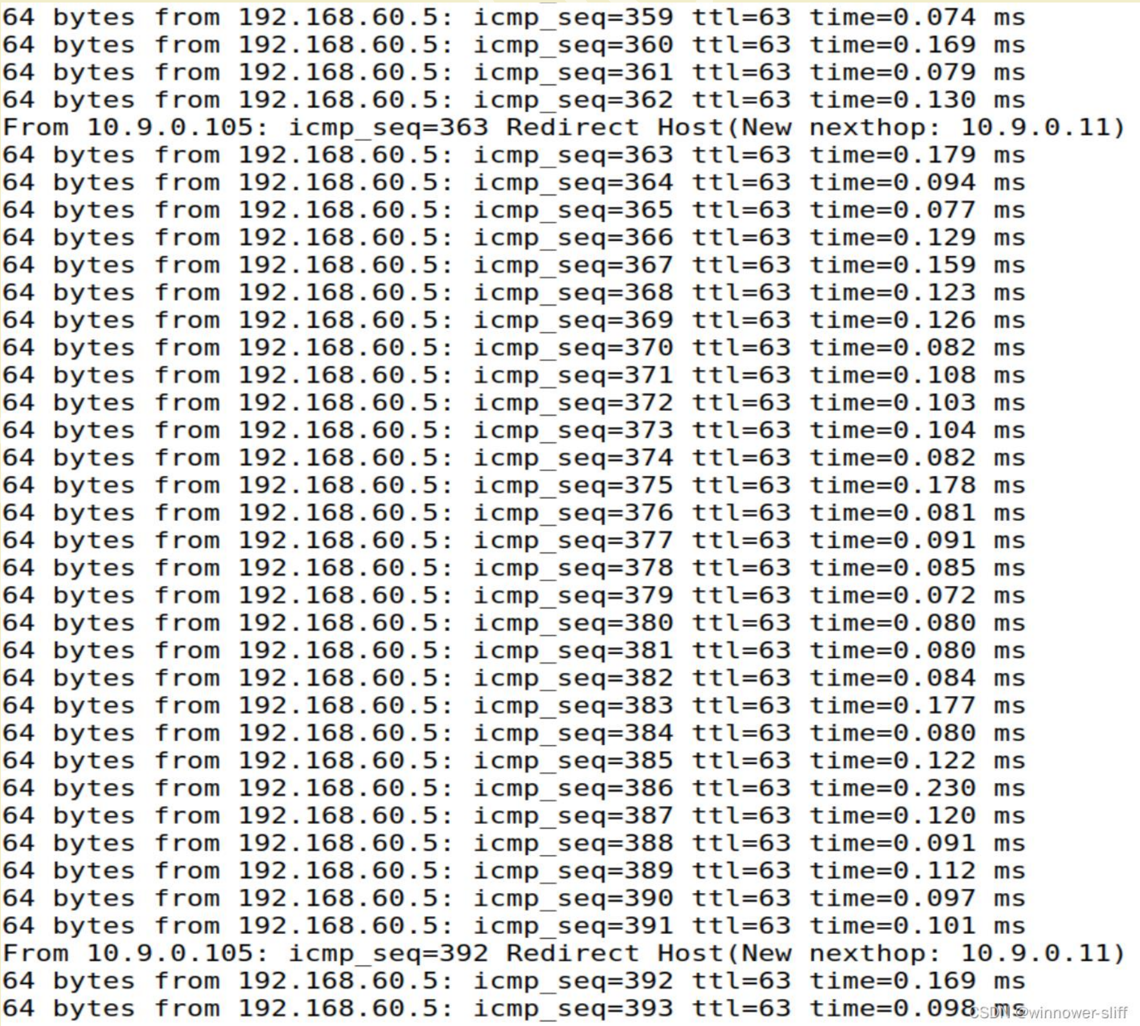


```
8714 2022-08-25 03:43:51.252032261 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=400/36865, ttl=63 (request in 8713)
8715 2022-08-25 03:43:52.275649939 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=401/37121, ttl=64 (reply in 8716)
8716 2022-08-25 03:43:52.275737398 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=401/37121, ttl=63 (request in 8715)
8717 2022-08-25 03:43:52.960056066 02:42:0a:09:00:69 Broadcast    ARP    42 Who has 10.9.0.5? Tell 10.9.0.105
8718 2022-08-25 03:43:52.960092149 02:42:0a:09:00:05 02:42:0a:0…  ARP    42 10.9.0.5 is at 02:42:0a:09:00:05
8719 2022-08-25 03:43:52.976050932 10.9.0.11         10.9.0.5     ICMP   70 Redirect             (Redirect for host)
8720 2022-08-25 03:43:52.976129398 02:42:0a:09:00:05 Broadcast    ARP    42 Who has 10.9.0.10? Tell 10.9.0.5
8721 2022-08-25 03:43:53.277368289 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=402/37377, ttl=64 (reply in 8722)
8722 2022-08-25 03:43:53.277457857 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=402/37377, ttl=63 (request in 8721)
8723 2022-08-25 03:43:54.015207341 02:42:0a:09:00:05 Broadcast    ARP    42 Who has 10.9.0.10? Tell 10.9.0.5
8724 2022-08-25 03:43:54.291311174 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=403/37633, ttl=64 (reply in 8725)
8725 2022-08-25 03:43:54.291369370 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=403/37633, ttl=63 (request in 8724)
8726 2022-08-25 03:43:55.031341858 02:42:0a:09:00:05 Broadcast    ARP    42 Who has 10.9.0.10? Tell 10.9.0.5
8727 2022-08-25 03:43:55.315658729 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=404/37889, ttl=64 (reply in 8728)
8728 2022-08-25 03:43:55.315709037 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=404/37889, ttl=63 (request in 8727)
8729 2022-08-25 03:43:56.339751442 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=405/38145, ttl=64 (reply in 8730)
8730 2022-08-25 03:43:56.339834706 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=405/38145, ttl=63 (request in 8729)
8731 2022-08-25 03:43:57.368112004 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=406/38401, ttl=64 (reply in 8732)
8732 2022-08-25 03:43:57.368162960 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=406/38401, ttl=63 (request in 8731)
8733 2022-08-25 03:43:58.387714855 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=407/38657, ttl=64 (reply in 8734)
8734 2022-08-25 03:43:58.387786570 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=407/38657, ttl=63 (request in 8733)
8735 2022-08-25 03:43:59.413634216 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=408/38913, ttl=64 (reply in 8736)
8736 2022-08-25 03:43:59.413697505 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=408/38913, ttl=63 (request in 8735)
8737 2022-08-25 03:44:00.435416628 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=409/39169, ttl=64 (reply in 8738)
8738 2022-08-25 03:44:00.435487641 192.168.60.5      10.9.0.5     ICMP   98 Echo (ping) reply    id=0x005b, seq=409/39169, ttl=63 (request in 8737)
8739 2022-08-25 03:44:01.463661546 10.9.0.5          192.168.60.5 ICMP   98 Echo (ping) request  id=0x005b, seq=410/39425, ttl=64 (reply in 8740)
```

```
▸ Frame 8719: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface br-e36926e4336f, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:69 (02:42:0a:09:00:69), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 10.9.0.11, Dst: 10.9.0.5
▾ Internet Control Message Protocol
    Type: 5 (Redirect)
    Code: 1 (Redirect for host)
    Checksum: 0xf0eb [correct]
    [Checksum Status: Good]
    Gateway address: 10.9.0.10
  ▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 192.168.60.5
  ▾ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7ff [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 0 (0x0000)
      Identifier (LE): 0 (0x0000)
      Sequence number (BE): 0 (0x0000)
      Sequence number (LE): 0 (0x0000)
```

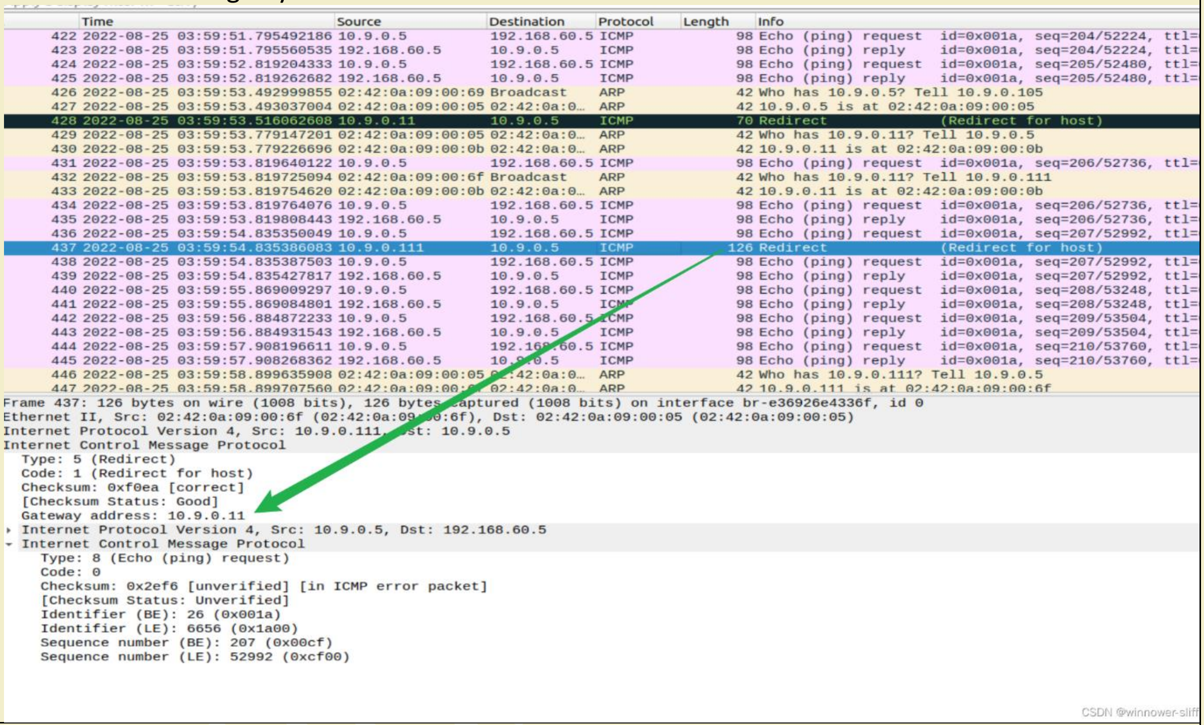
As can be seen from the figure, after receiving the reconnection, the victim will look for the MAC address of the target website through ARP, and at the same time maintain the original connection. However, since the MAC address of the target URL is not found, the original transmission is maintained.

During the experiment, I tried to direct the packet to 10.9.0.105, and found that IP forwarding was not turned on, so a redirect packet was sent to the victim. As shown in the figure:



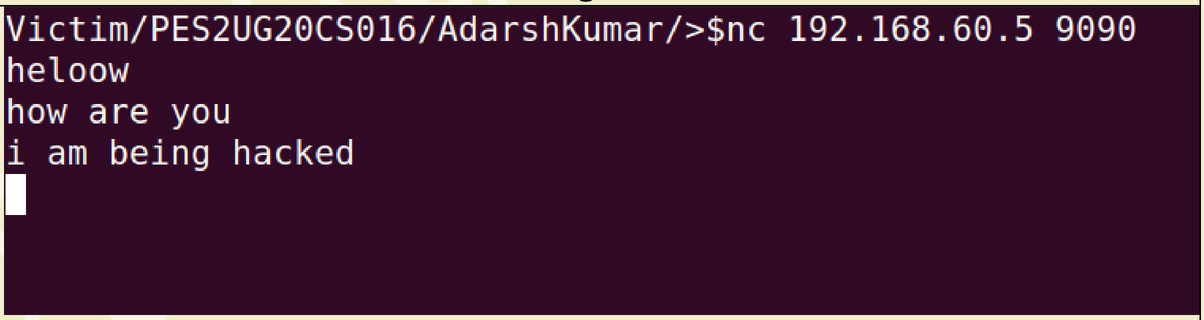
```
64 bytes from 192.168.60.5: icmp_seq=359 ttl=63 time=0.074 ms
64 bytes from 192.168.60.5: icmp_seq=360 ttl=63 time=0.169 ms
64 bytes from 192.168.60.5: icmp_seq=361 ttl=63 time=0.079 ms
64 bytes from 192.168.60.5: icmp_seq=362 ttl=63 time=0.130 ms
From 10.9.0.105: icmp_seq=363 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=363 ttl=63 time=0.179 ms
64 bytes from 192.168.60.5: icmp_seq=364 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=365 ttl=63 time=0.077 ms
64 bytes from 192.168.60.5: icmp_seq=366 ttl=63 time=0.129 ms
64 bytes from 192.168.60.5: icmp_seq=367 ttl=63 time=0.159 ms
64 bytes from 192.168.60.5: icmp_seq=368 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=369 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=370 ttl=63 time=0.082 ms
64 bytes from 192.168.60.5: icmp_seq=371 ttl=63 time=0.108 ms
64 bytes from 192.168.60.5: icmp_seq=372 ttl=63 time=0.103 ms
64 bytes from 192.168.60.5: icmp_seq=373 ttl=63 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=374 ttl=63 time=0.082 ms
64 bytes from 192.168.60.5: icmp_seq=375 ttl=63 time=0.178 ms
64 bytes from 192.168.60.5: icmp_seq=376 ttl=63 time=0.081 ms
64 bytes from 192.168.60.5: icmp_seq=377 ttl=63 time=0.091 ms
64 bytes from 192.168.60.5: icmp_seq=378 ttl=63 time=0.085 ms
64 bytes from 192.168.60.5: icmp_seq=379 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=380 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=381 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=382 ttl=63 time=0.084 ms
64 bytes from 192.168.60.5: icmp_seq=383 ttl=63 time=0.177 ms
64 bytes from 192.168.60.5: icmp_seq=384 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=385 ttl=63 time=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=386 ttl=63 time=0.230 ms
64 bytes from 192.168.60.5: icmp_seq=387 ttl=63 time=0.120 ms
64 bytes from 192.168.60.5: icmp_seq=388 ttl=63 time=0.091 ms
64 bytes from 192.168.60.5: icmp_seq=389 ttl=63 time=0.112 ms
64 bytes from 192.168.60.5: icmp_seq=390 ttl=63 time=0.097 ms
64 bytes from 192.168.60.5: icmp_seq=391 ttl=63 time=0.101 ms
From 10.9.0.105: icmp_seq=392 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=392 ttl=63 time=0.169 ms
64 bytes from 192.168.60.5: icmp_seq=393 ttl=63 time=0.098 ms
```

	At the same time, it can be associated with the previous question and the ARP poisoning experiment at the same time as SEED: it can deceive the existence of a non-existent URL to tell the victim, and direct the packet to the attacker's host, while hiding the attacker's real IP. address.
Question 3:	If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation
Solution	As shown in the figure, and the test results I got in the previous question, our malicious router sent the redirect message by itself:

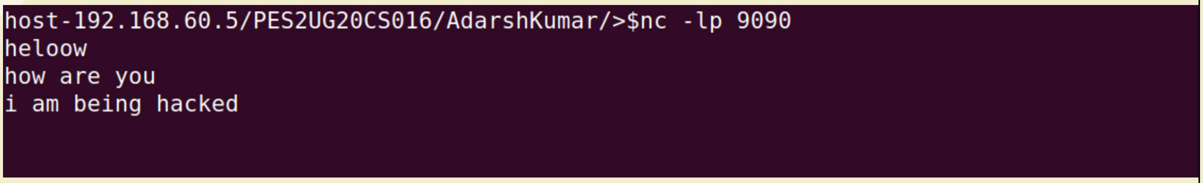


```
        Time                            Source              Destination   Protocol  Length  Info
    422 2022-08-25 03:59:51.795492186 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=204/52224, ttl=
    423 2022-08-25 03:59:51.795560535 192.168.60.5         10.9.0.5     ICMP          98 Echo (ping) reply    id=0x001a, seq=204/52224, ttl=
    424 2022-08-25 03:59:52.819204333 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=205/52480, ttl=
    425 2022-08-25 03:59:52.819262682 192.168.60.5         10.9.0.5     ICMP          98 Echo (ping) reply    id=0x001a, seq=205/52480, ttl=
    426 2022-08-25 03:59:53.492999855 02:42:0a:09:00:69 Broadcast       ARP           42 Who has 10.9.0.5? Tell 10.9.0.105
    427 2022-08-25 03:59:53.493037004 02:42:0a:09:00:05 02:42:0a:0…     ARP           42 10.9.0.5 is at 02:42:0a:09:00:05
    428 2022-08-25 03:59:53.516062608 10.9.0.11            10.9.0.5     ICMP          70 Redirect             (Redirect for host)
    429 2022-08-25 03:59:53.779147201 02:42:0a:09:00:05 02:42:0a:0…     ARP           42 Who has 10.9.0.11? Tell 10.9.0.5
    430 2022-08-25 03:59:53.779226696 02:42:0a:09:00:0b 02:42:0a:0…     ARP           42 10.9.0.11 is at 02:42:0a:09:00:0b
    431 2022-08-25 03:59:53.819640122 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=206/52736, ttl=
    432 2022-08-25 03:59:53.819725094 02:42:0a:09:00:6f Broadcast       ARP           42 Who has 10.9.0.11? Tell 10.9.0.111
    433 2022-08-25 03:59:53.819754620 02:42:0a:09:00:0b 02:42:0a:0…     ARP           42 10.9.0.11 is at 02:42:0a:09:00:0b
    434 2022-08-25 03:59:53.819764076 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=206/52736, ttl=
    435 2022-08-25 03:59:53.819808443 192.168.60.5         10.9.0.5     ICMP          98 Echo (ping) reply    id=0x001a, seq=206/52736, ttl=
    436 2022-08-25 03:59:54.835350049 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=207/52992, ttl=
    437 2022-08-25 03:59:54.835386083 10.9.0.111           10.9.0.5     ICMP         126 Redirect             (Redirect for host)
    438 2022-08-25 03:59:54.835387503 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=207/52992, ttl=
    439 2022-08-25 03:59:54.835427817 192.168.60.5         10.9.0.5     ICMP          98 Echo (ping) reply    id=0x001a, seq=207/52992, ttl=
    440 2022-08-25 03:59:55.869009297 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=208/53248, ttl=
    441 2022-08-25 03:59:55.869084801 192.168.60.5         10.9.0.5     ICMP          98 Echo (ping) reply    id=0x001a, seq=208/53248, ttl=
    442 2022-08-25 03:59:56.884872233 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=209/53504, ttl=
    443 2022-08-25 03:59:56.884931543 192.168.60.5         10.9.0.5     ICMP          98 Echo (ping) reply    id=0x001a, seq=209/53504, ttl=
    444 2022-08-25 03:59:57.908196611 10.9.0.5             192.168.60.5 ICMP          98 Echo (ping) request  id=0x001a, seq=210/53760, ttl=
    445 2022-08-25 03:59:57.908268362 192.168.60.5         10.9.0.5     ICMP          98 Echo (ping) reply    id=0x001a, seq=210/53760, ttl=
    446 2022-08-25 03:59:58.899635908 02:42:0a:09:00:05 02:42:0a:0…     ARP           42 Who has 10.9.0.111? Tell 10.9.0.5
    447 2022-08-25 03:59:58.899707560 02:42:0a:09:00:6f 02:42:0a:0…     ARP           42 10.9.0.111 is at 02:42:0a:09:00:6f
Frame 437: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface br-e36926e4336f, id 0
Ethernet II, Src: 02:42:0a:09:00:6f (02:42:0a:09:00:6f), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
Internet Protocol Version 4, Src: 10.9.0.111, Dst: 10.9.0.5
Internet Control Message Protocol
  Type: 5 (Redirect)
  Code: 1 (Redirect for host)
  Checksum: 0xf0ea [correct]
  [Checksum Status: Good]
  Gateway address: 10.9.0.11
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 192.168.60.5
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2ef6 [unverified] [in ICMP error packet]
    [Checksum Status: Unverified]
    Identifier (BE): 26 (0x001a)
    Identifier (LE): 6656 (0x1a00)
    Sequence number (BE): 207 (0x00cf)
    Sequence number (LE): 52992 (0xcf00)
```

Task 2: Launching the MITM Attack

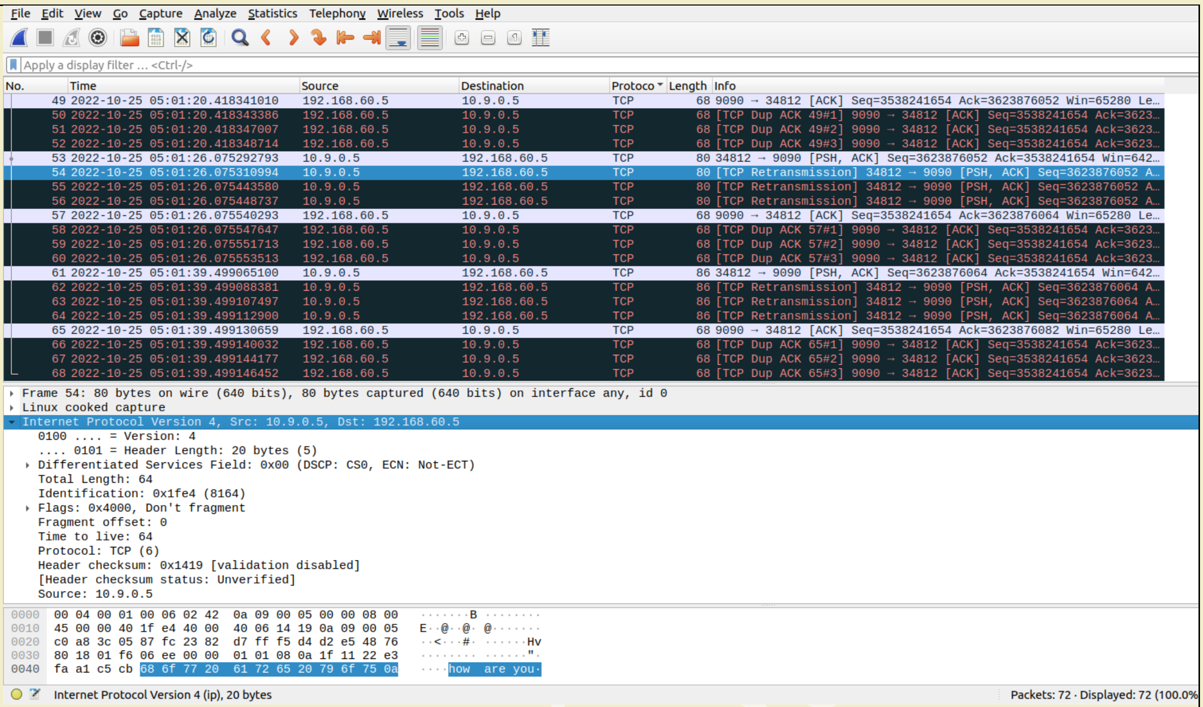


```
Victim/PES2UG20CS016/AdarshKumar/>$nc 192.168.60.5 9090
heloow
how are you
i am being hacked
```



```
host-192.168.60.5/PES2UG20CS016/AdarshKumar/>$nc -lp 9090
heloow
how are you
i am being hacked
```

Wireshark


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

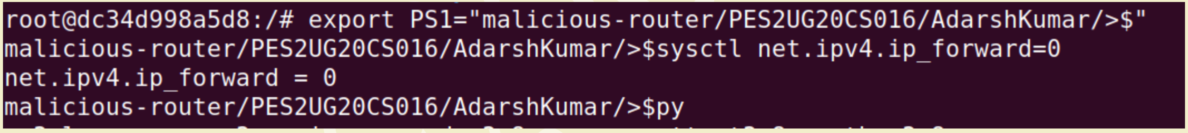
```
No.   Time                           Source         Destination    Protoco Length Info
   49 2022-10-25 05:01:20.418341010  192.168.60.5   10.9.0.5       TCP     68 9090 → 34812 [ACK] Seq=3538241654 Ack=3623876052 Win=65280 Le…
   50 2022-10-25 05:01:20.418343386  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 49#1] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   51 2022-10-25 05:01:20.418347007  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 49#2] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   52 2022-10-25 05:01:20.418348714  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 49#3] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   53 2022-10-25 05:01:26.075292793  10.9.0.5       192.168.60.5   TCP     80 34812 → 9090 [PSH, ACK] Seq=3623876052 Ack=3538241654 Win=642…
   54 2022-10-25 05:01:26.075310994  10.9.0.5       192.168.60.5   TCP     80 [TCP Retransmission] 34812 → 9090 [PSH, ACK] Seq=3623876052 A…
   55 2022-10-25 05:01:26.075443580  10.9.0.5       192.168.60.5   TCP     80 [TCP Retransmission] 34812 → 9090 [PSH, ACK] Seq=3623876052 A…
   56 2022-10-25 05:01:26.075448737  10.9.0.5       192.168.60.5   TCP     80 [TCP Retransmission] 34812 → 9090 [PSH, ACK] Seq=3623876052 A…
   57 2022-10-25 05:01:26.075540293  192.168.60.5   10.9.0.5       TCP     68 9090 → 34812 [ACK] Seq=3538241654 Ack=3623876064 Win=65280 Le…
   58 2022-10-25 05:01:26.075547647  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 57#1] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   59 2022-10-25 05:01:26.075551713  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 57#2] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   60 2022-10-25 05:01:26.075553513  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 57#3] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   61 2022-10-25 05:01:39.499065100  10.9.0.5       192.168.60.5   TCP     86 34812 → 9090 [PSH, ACK] Seq=3623876064 Ack=3538241654 Win=642…
   62 2022-10-25 05:01:39.499088381  10.9.0.5       192.168.60.5   TCP     86 [TCP Retransmission] 34812 → 9090 [PSH, ACK] Seq=3623876064 A…
   63 2022-10-25 05:01:39.499107497  10.9.0.5       192.168.60.5   TCP     86 [TCP Retransmission] 34812 → 9090 [PSH, ACK] Seq=3623876064 A…
   64 2022-10-25 05:01:39.499112900  10.9.0.5       192.168.60.5   TCP     86 [TCP Retransmission] 34812 → 9090 [PSH, ACK] Seq=3623876064 A…
   65 2022-10-25 05:01:39.499130659  192.168.60.5   10.9.0.5       TCP     68 9090 → 34812 [ACK] Seq=3538241654 Ack=3623876082 Win=65280 Le…
   66 2022-10-25 05:01:39.499140032  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 65#1] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   67 2022-10-25 05:01:39.499144177  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 65#2] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…
   68 2022-10-25 05:01:39.499146452  192.168.60.5   10.9.0.5       TCP     68 [TCP Dup ACK 65#3] 9090 → 34812 [ACK] Seq=3538241654 Ack=3623…

▸ Frame 54: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface any, id 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 192.168.60.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 64
    Identification: 0x1fe4 (8164)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x1419 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.9.0.5

0000  00 04 00 01 00 06 02 42  0a 09 00 05 00 00 08 00   ·······B ········
0010  45 00 00 40 1f e4 40 00  40 06 14 19 0a 09 00 05   E··@··@· @·······
0020  c0 a8 3c 05 87 fc 23 82  d7 ff f5 d4 d2 e5 48 76   ··<···#· ······Hv
0030  80 18 01 f6 06 ee 00 00  01 01 08 0a 1f 11 22 e3   ········ ······".
0040  fa a1 c5 cb 68 6f 77 20  61 72 65 20 79 6f 75 0a   ····how  are you·

Internet Protocol Version 4 (ip), 20 bytes                    Packets: 72 · Displayed: 72 (100.0%
```

We can see that TCP packet are retransmitted and the message is also present there.

Task 2B

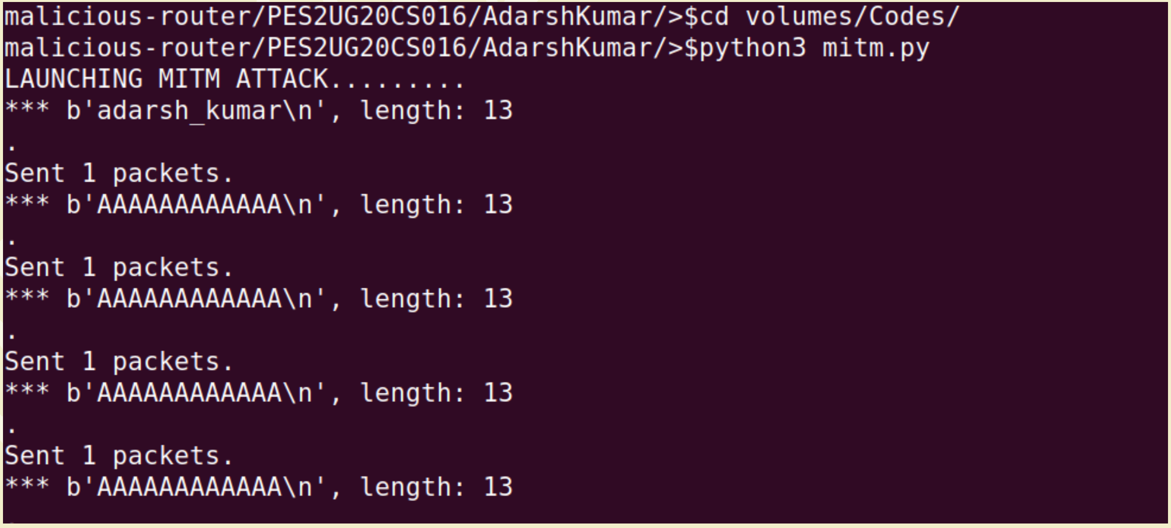
To launch the MITM Attack

Turning off IP forwarding on malicious router terminal



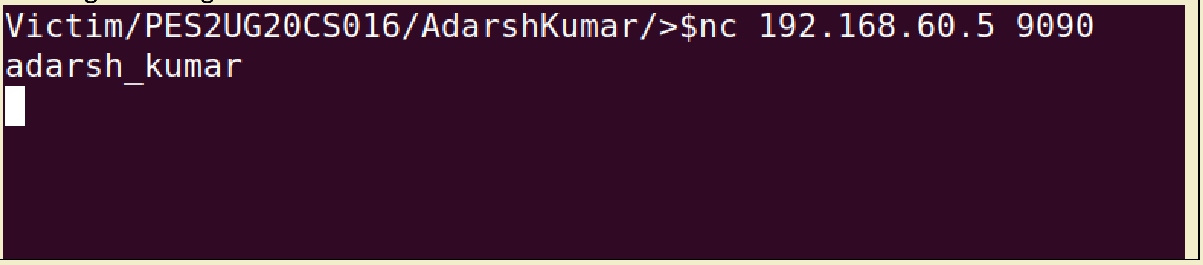
```
root@dc34d998a5d8:/# export PS1="malicious-router/PES2UG20CS016/AdarshKumar/>$"
malicious-router/PES2UG20CS016/AdarshKumar/>$sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
malicious-router/PES2UG20CS016/AdarshKumar/>$py
```

Now launching the man in the middle attack



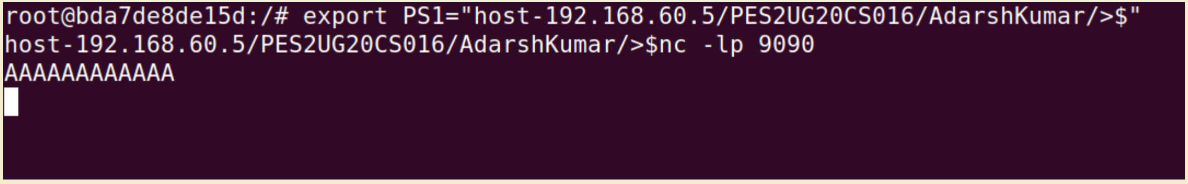
```
malicious-router/PES2UG20CS016/AdarshKumar/>$cd volumes/Codes/
malicious-router/PES2UG20CS016/AdarshKumar/>$python3 mitm.py
LAUNCHING MITM ATTACK.........
*** b'adarsh_kumar\n', length: 13
.
Sent 1 packets.
*** b'AAAAAAAAAAAA\n', length: 13
.
Sent 1 packets.
*** b'AAAAAAAAAAAA\n', length: 13
.
Sent 1 packets.
*** b'AAAAAAAAAAAA\n', length: 13
.
Sent 1 packets.
*** b'AAAAAAAAAAAA\n', length: 13
```

Sending a message from victim container to host



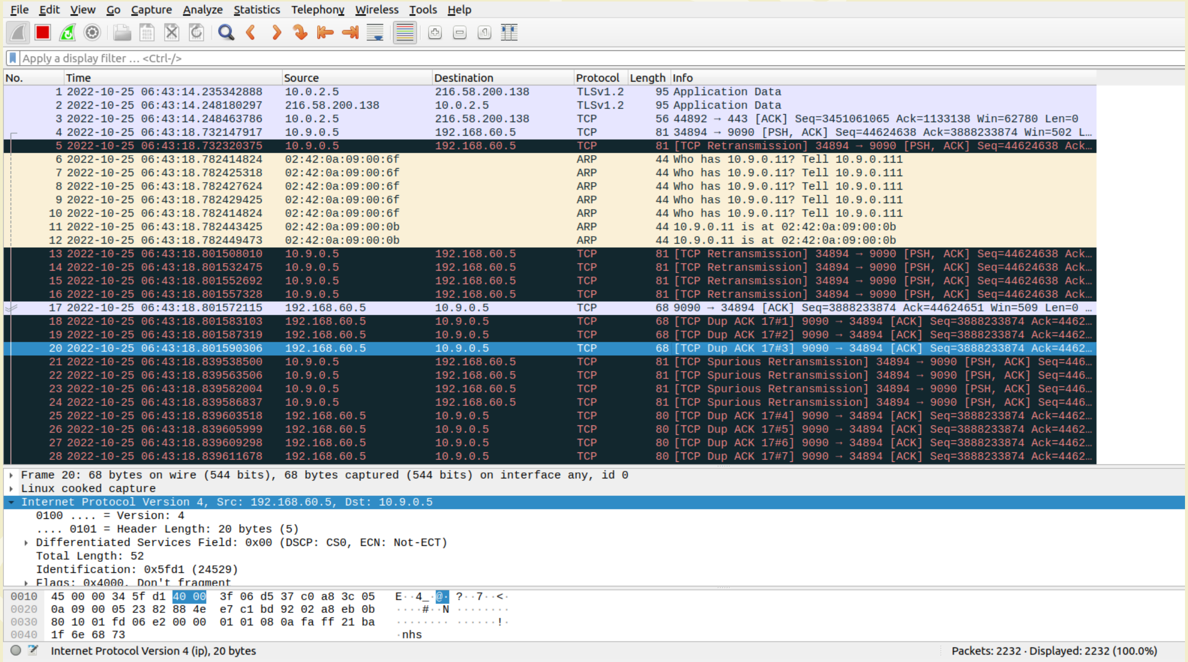
```
Victim/PES2UG20CS016/AdarshKumar/>$nc 192.168.60.5 9090
adarsh_kumar
█
```

As we can observe that the message is changed here that means our message might have been intersected in the middle and changed.



```
root@bda7de8de15d:/# export PS1="host-192.168.60.5/PES2UG20CS016/AdarshKumar/>$"
host-192.168.60.5/PES2UG20CS016/AdarshKumar/>$nc -lp 9090
AAAAAAAAAAAA
```

This confirmed that message is sent to the malleolus server and it was changed there.

Question 4:	In your MITM program, you only need to capture the traffic in one direction. Please indicate which direction, and explain why.
Solution	Because we only induce the sending direction to the victim host, only the victim will send the message to the malicious route, but not to the target host, so there is no need to formulate the message for the opposite direction (yes, but not necessary)
Question 5:	In the MITM program, when you capture the nc traffic from A (10.9.0.5), you can use A's IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion
Solution	MAC addresses should be used for filtering, because using IP can create forwarding storms. Which can be seen in the below Wireshark screenshot. 

```
No.  Time                           Source              Destination     Protocol Length Info
   1 2022-10-25 06:43:14.235342888  10.0.2.5            216.58.200.138  TLSv1.2    95 Application Data
   2 2022-10-25 06:43:14.248180297  216.58.200.138      10.0.2.5        TLSv1.2    95 Application Data
   3 2022-10-25 06:43:14.248463786  10.0.2.5            216.58.200.138  TCP        56 44892 → 443 [ACK] Seq=3451061065 Ack=1133138 Win=62780 Len=0
   4 2022-10-25 06:43:18.732147917  10.9.0.5            192.168.60.5    TCP        81 34894 → 9090 [PSH, ACK] Seq=44624638 Ack=3888233874 Win=502 L…
   5 2022-10-25 06:43:18.732320375  10.9.0.5            192.168.60.5    TCP        81 [TCP Retransmission] 34894 → 9090 [PSH, ACK] Seq=44624638 Ack…
   6 2022-10-25 06:43:18.782414824  02:42:0a:09:00:6f                   ARP        44 Who has 10.9.0.11? Tell 10.9.0.111
   7 2022-10-25 06:43:18.782425318  02:42:0a:09:00:6f                   ARP        44 Who has 10.9.0.11? Tell 10.9.0.111
   8 2022-10-25 06:43:18.782427624  02:42:0a:09:00:6f                   ARP        44 Who has 10.9.0.11? Tell 10.9.0.111
   9 2022-10-25 06:43:18.782429425  02:42:0a:09:00:6f                   ARP        44 Who has 10.9.0.11? Tell 10.9.0.111
  10 2022-10-25 06:43:18.782414824  02:42:0a:09:00:6f                   ARP        44 Who has 10.9.0.11? Tell 10.9.0.111
  11 2022-10-25 06:43:18.782443425  02:42:0a:09:00:0b                   ARP        44 10.9.0.11 is at 02:42:0a:09:00:0b
  12 2022-10-25 06:43:18.782449473  02:42:0a:09:00:0b                   ARP        44 10.9.0.11 is at 02:42:0a:09:00:0b
  13 2022-10-25 06:43:18.801508010  10.9.0.5            192.168.60.5    TCP        81 [TCP Retransmission] 34894 → 9090 [PSH, ACK] Seq=44624638 Ack…
  14 2022-10-25 06:43:18.801532475  10.9.0.5            192.168.60.5    TCP        81 [TCP Retransmission] 34894 → 9090 [PSH, ACK] Seq=44624638 Ack…
  15 2022-10-25 06:43:18.801552692  10.9.0.5            192.168.60.5    TCP        81 [TCP Retransmission] 34894 → 9090 [PSH, ACK] Seq=44624638 Ack…
  16 2022-10-25 06:43:18.801557328  10.9.0.5            192.168.60.5    TCP        81 [TCP Retransmission] 34894 → 9090 [PSH, ACK] Seq=44624638 Ack…
  17 2022-10-25 06:43:18.801572115  192.168.60.5        10.9.0.5        TCP        68 9090 → 34894 [ACK] Seq=3888233874 Ack=44624651 Win=509 Len=0 …
  18 2022-10-25 06:43:18.801583103  192.168.60.5        10.9.0.5        TCP        68 [TCP Dup ACK 17#1] 9090 → 34894 [ACK] Seq=3888233874 Ack=4462…
  19 2022-10-25 06:43:18.801587319  192.168.60.5        10.9.0.5        TCP        68 [TCP Dup ACK 17#2] 9090 → 34894 [ACK] Seq=3888233874 Ack=4462…
  20 2022-10-25 06:43:18.801590306  192.168.60.5        10.9.0.5        TCP        68 [TCP Dup ACK 17#3] 9090 → 34894 [ACK] Seq=3888233874 Ack=4462…
  21 2022-10-25 06:43:18.839538500  10.9.0.5            192.168.60.5    TCP        81 [TCP Spurious Retransmission] 34894 → 9090 [PSH, ACK] Seq=446…
  22 2022-10-25 06:43:18.839563506  10.9.0.5            192.168.60.5    TCP        81 [TCP Spurious Retransmission] 34894 → 9090 [PSH, ACK] Seq=446…
  23 2022-10-25 06:43:18.839582004  10.9.0.5            192.168.60.5    TCP        81 [TCP Spurious Retransmission] 34894 → 9090 [PSH, ACK] Seq=446…
  24 2022-10-25 06:43:18.839586837  10.9.0.5            192.168.60.5    TCP        81 [TCP Spurious Retransmission] 34894 → 9090 [PSH, ACK] Seq=446…
  25 2022-10-25 06:43:18.839603518  192.168.60.5        10.9.0.5        TCP        80 [TCP Dup ACK 17#4] 9090 → 34894 [ACK] Seq=3888233874 Ack=4462…
  26 2022-10-25 06:43:18.839605999  192.168.60.5        10.9.0.5        TCP        80 [TCP Dup ACK 17#5] 9090 → 34894 [ACK] Seq=3888233874 Ack=4462…
  27 2022-10-25 06:43:18.839609298  192.168.60.5        10.9.0.5        TCP        80 [TCP Dup ACK 17#6] 9090 → 34894 [ACK] Seq=3888233874 Ack=4462…
  28 2022-10-25 06:43:18.839611678  192.168.60.5        10.9.0.5        TCP        80 [TCP Dup ACK 17#7] 9090 → 34894 [ACK] Seq=3888233874 Ack=4462…

▸ Frame 20: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 192.168.60.5, Dst: 10.9.0.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x5fd1 (24529)
  ▸ Flags: 0x4000, Don't fragment

0010  45 00 00 34 5f d1 40 00  3f 06 d5 37 c0 a8 3c 05   E··4_·@· ?··7··<·
0020  0a 09 00 05 23 82 88 4e  e7 c1 bd 92 02 a8 eb 0b   ····#··N ········
0030  80 10 01 fd 06 e2 00 00  01 01 08 0a fa ff 21 ba   ········ ······!·
0040  1f 6e 68 73                                        ·nhs

Internet Protocol Version 4 (ip), 20 bytes                    Packets: 2232 · Displayed: 2232 (100.0%)
```