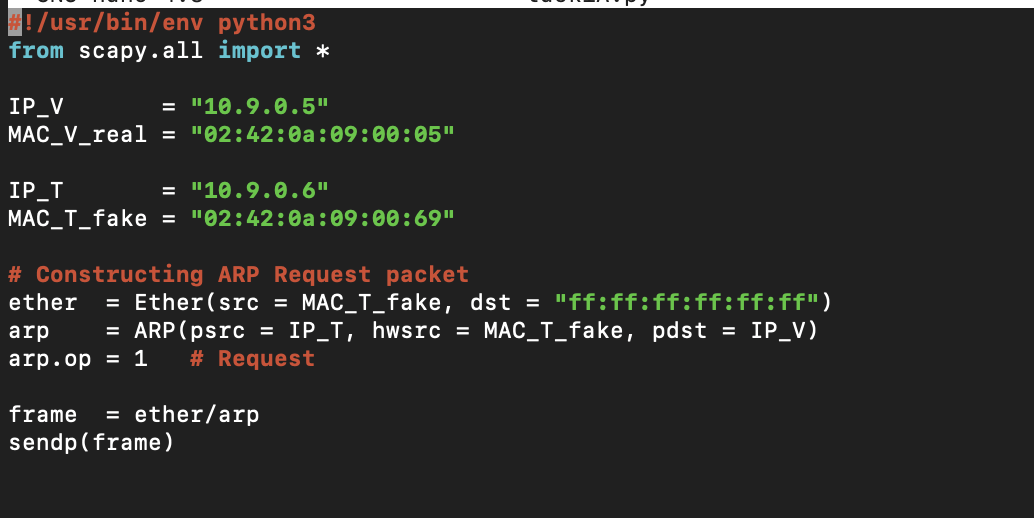
**Task 1.A**

Code:



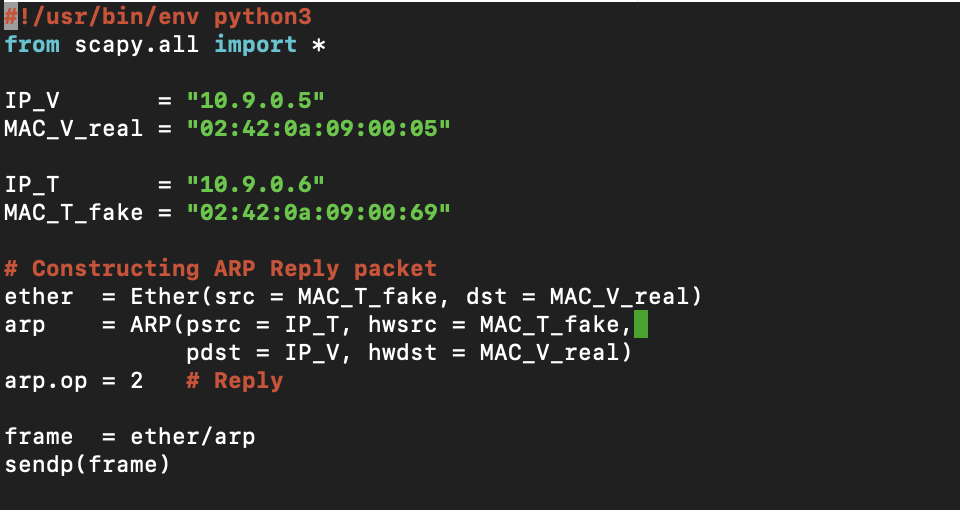
Result:



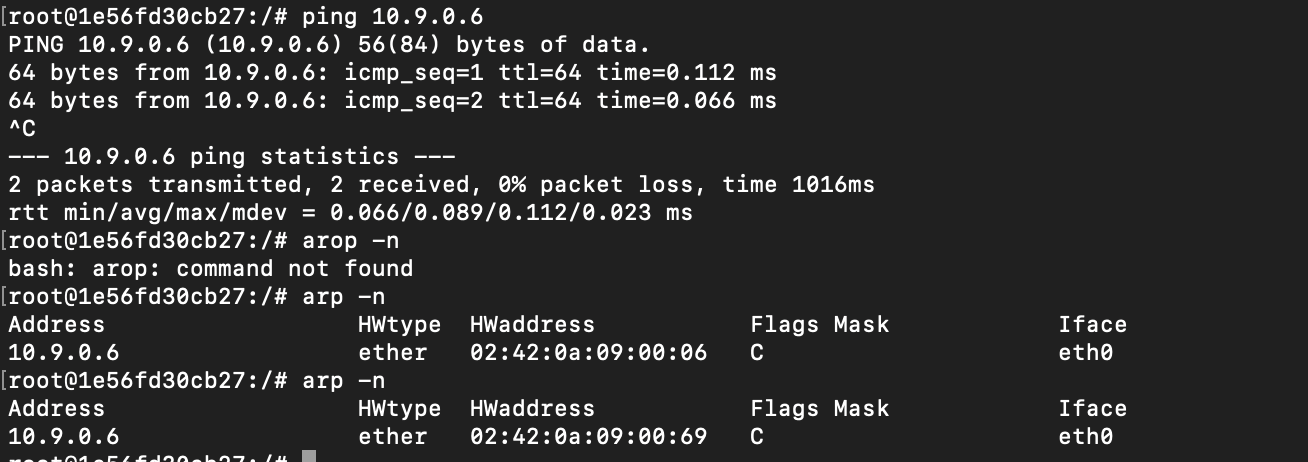
Observations: Here we broadcast ARP request with fake mac address.

**Task 1.B**

Code:

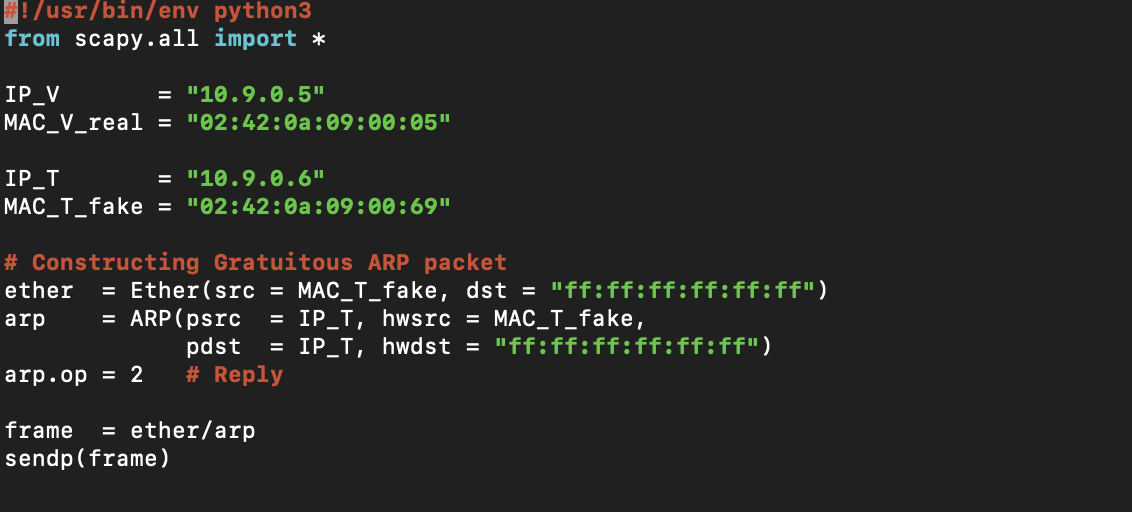


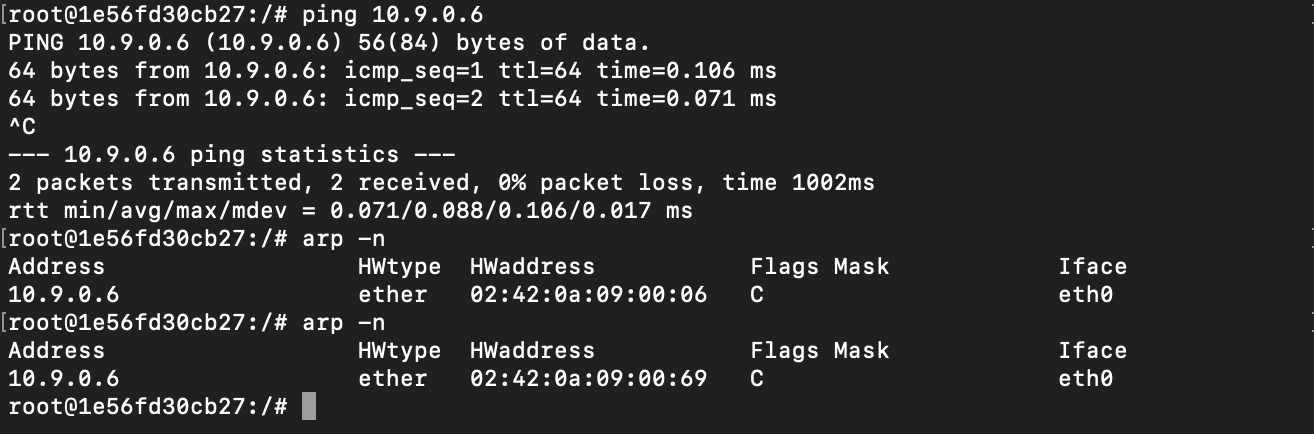
Result:



Observations:  
Here we have to first get the ip address to poision to the cache then only it will give the result we are looking for as there was no response expected. Else, it will do nothing. Thus, I am using ping to get the ip in arp cache.

**Task 1.C**

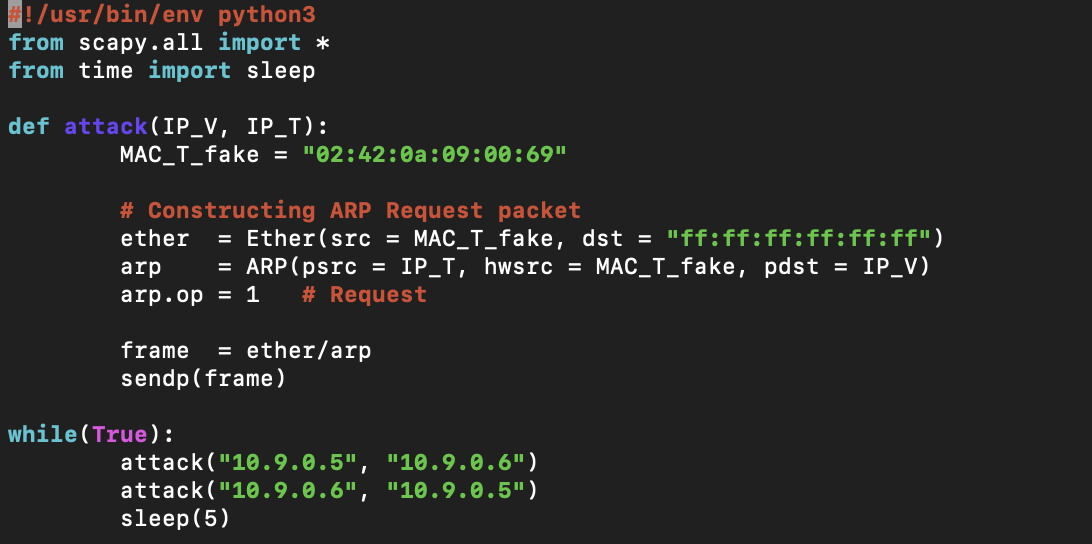
Code:  


Result:  


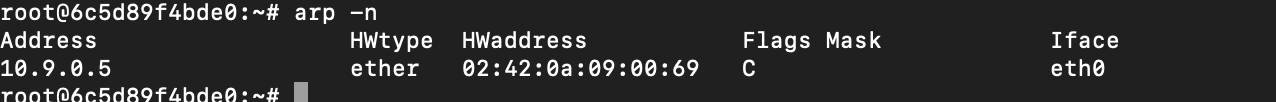
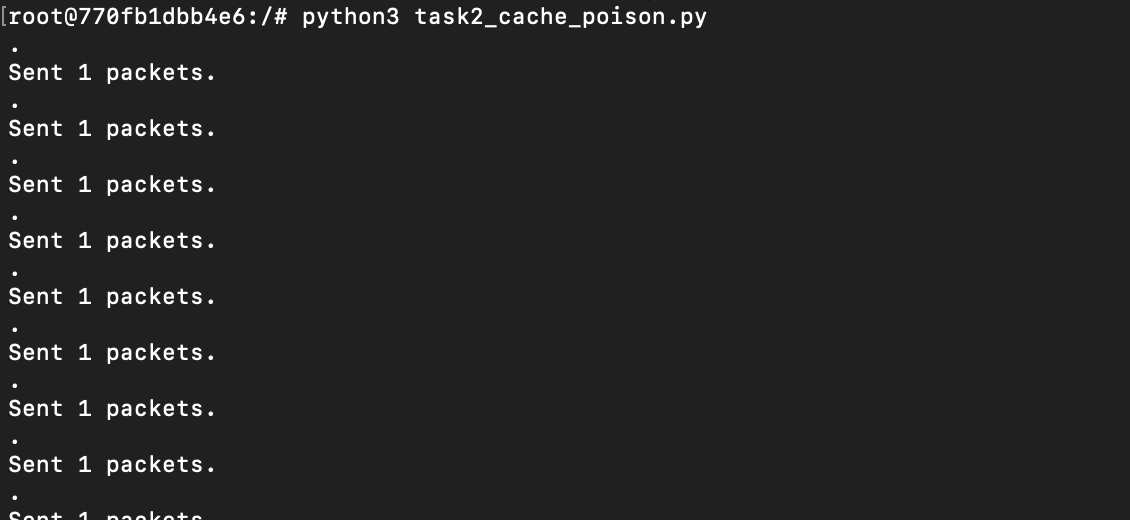
Observations:

Similarly to Task 1.B there was no response expected, so we have to ping first then poison. Good part about this method is we dont need the destination ip and mac addresses.

**Task 2.1**

Code:  


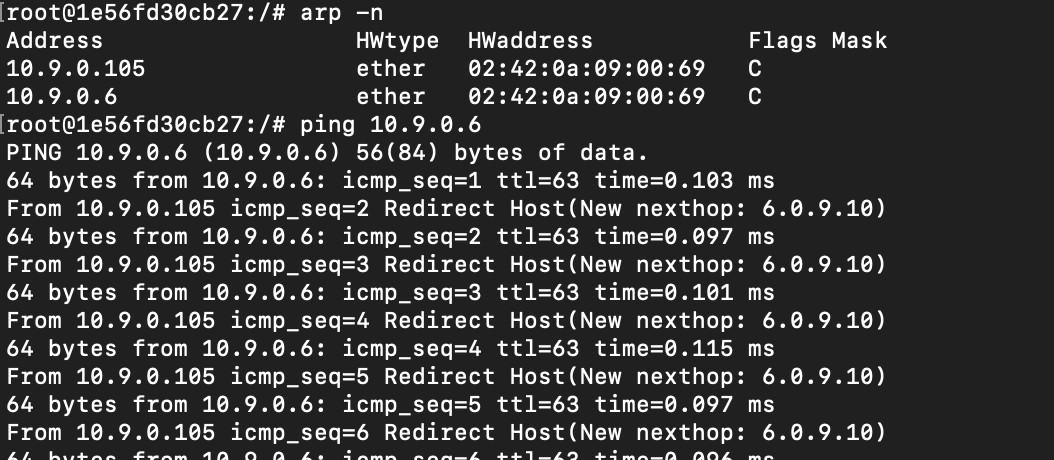
Result:



Observation:  
We see arp cache of both Host A and B poisioned with mac address of attacker every 5 sec using ARP request as the cache can expire or change anytime.

**Task 2.2 Using Port Forwarding**

Result:



Observations:  
We see packet going through attacker.

**Task 2.3 No Port Forwarding**

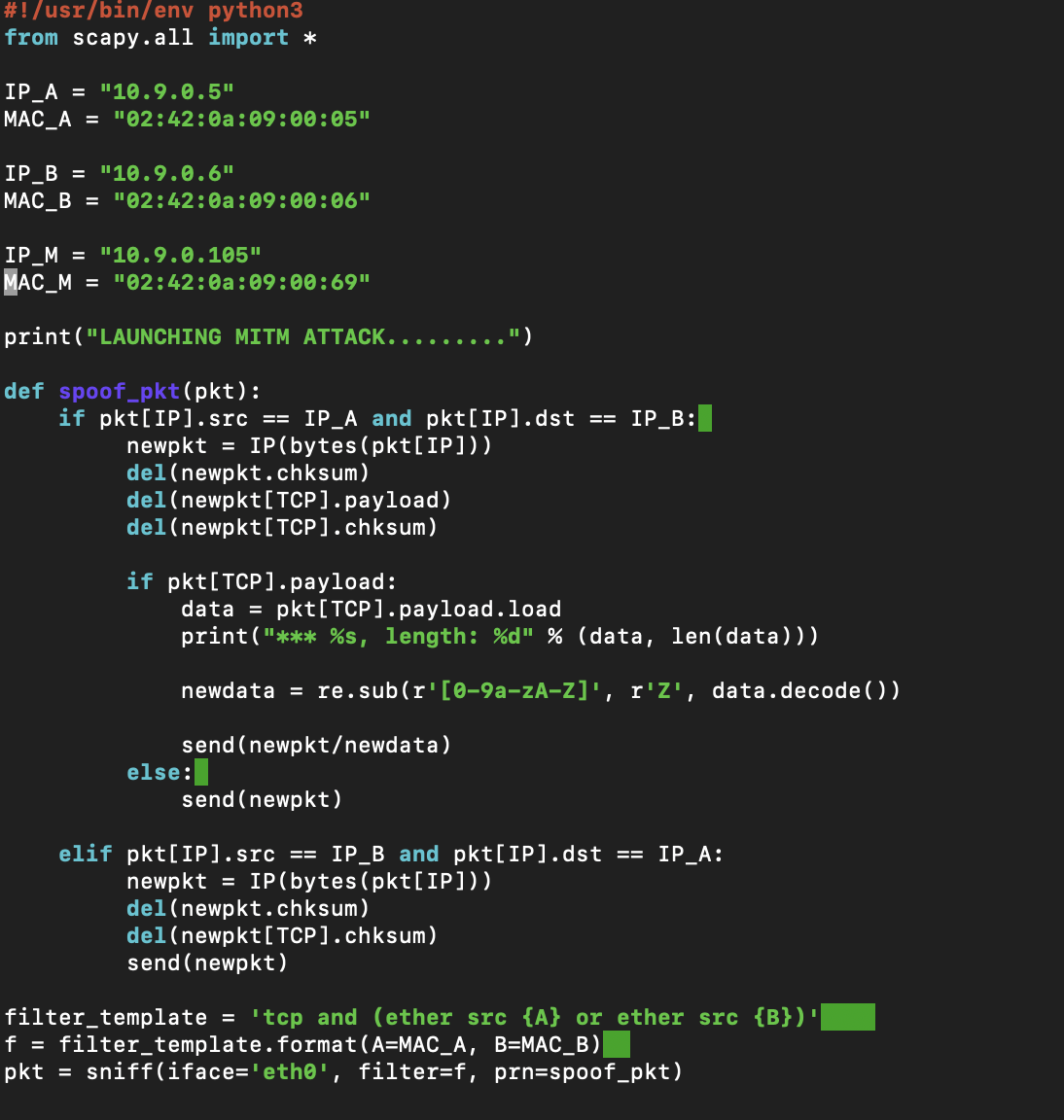
Result:

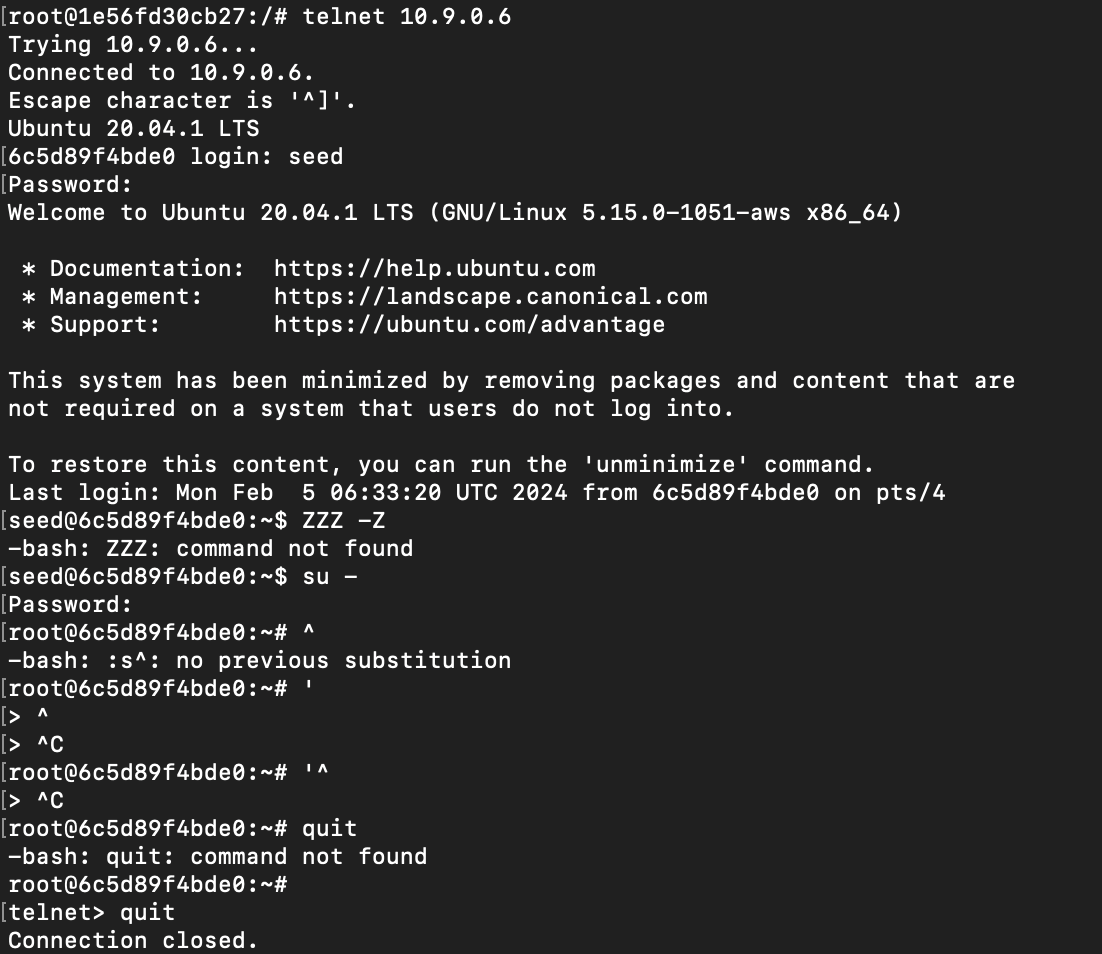
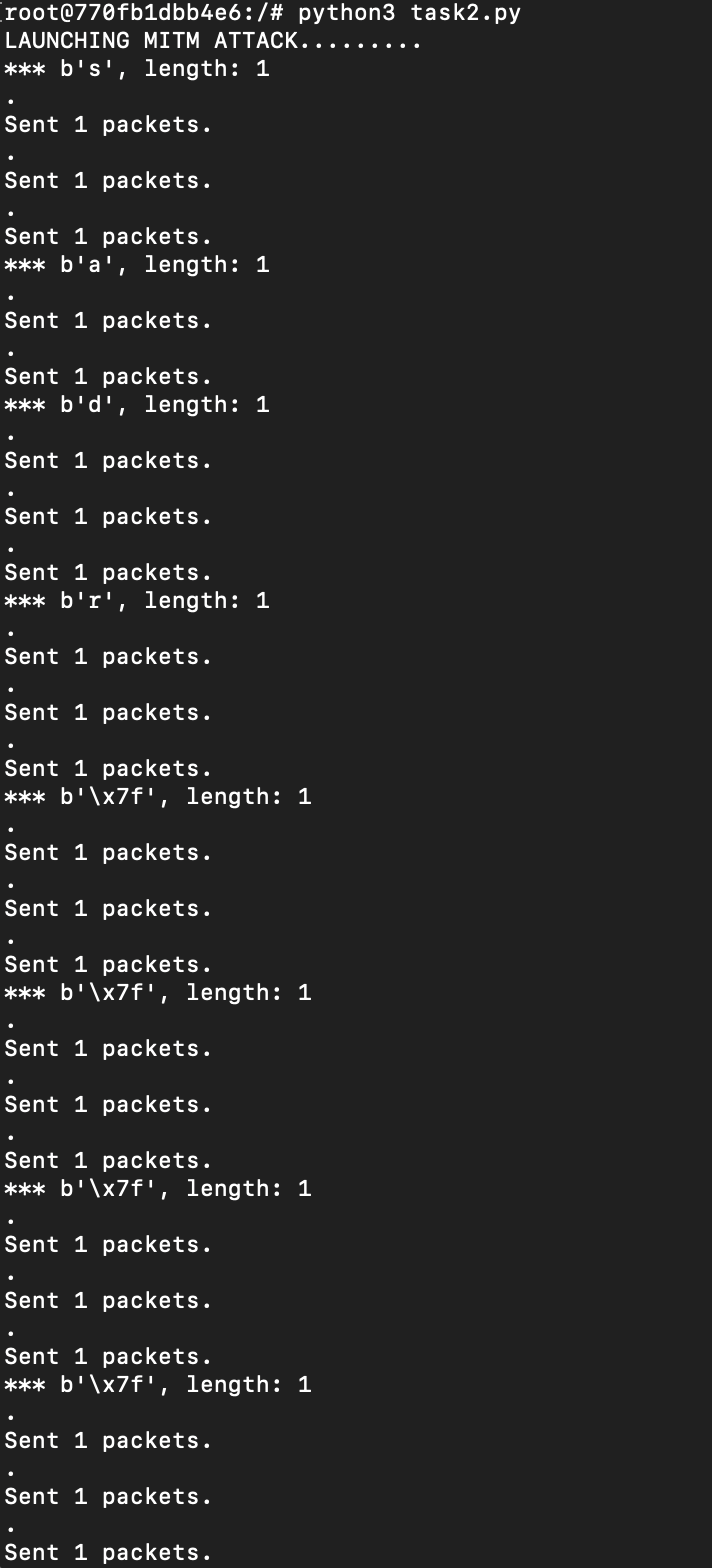


Observations:  
Since there is no port forwarding we dont have a way to go to host B.

**Task 2.4**

Code:

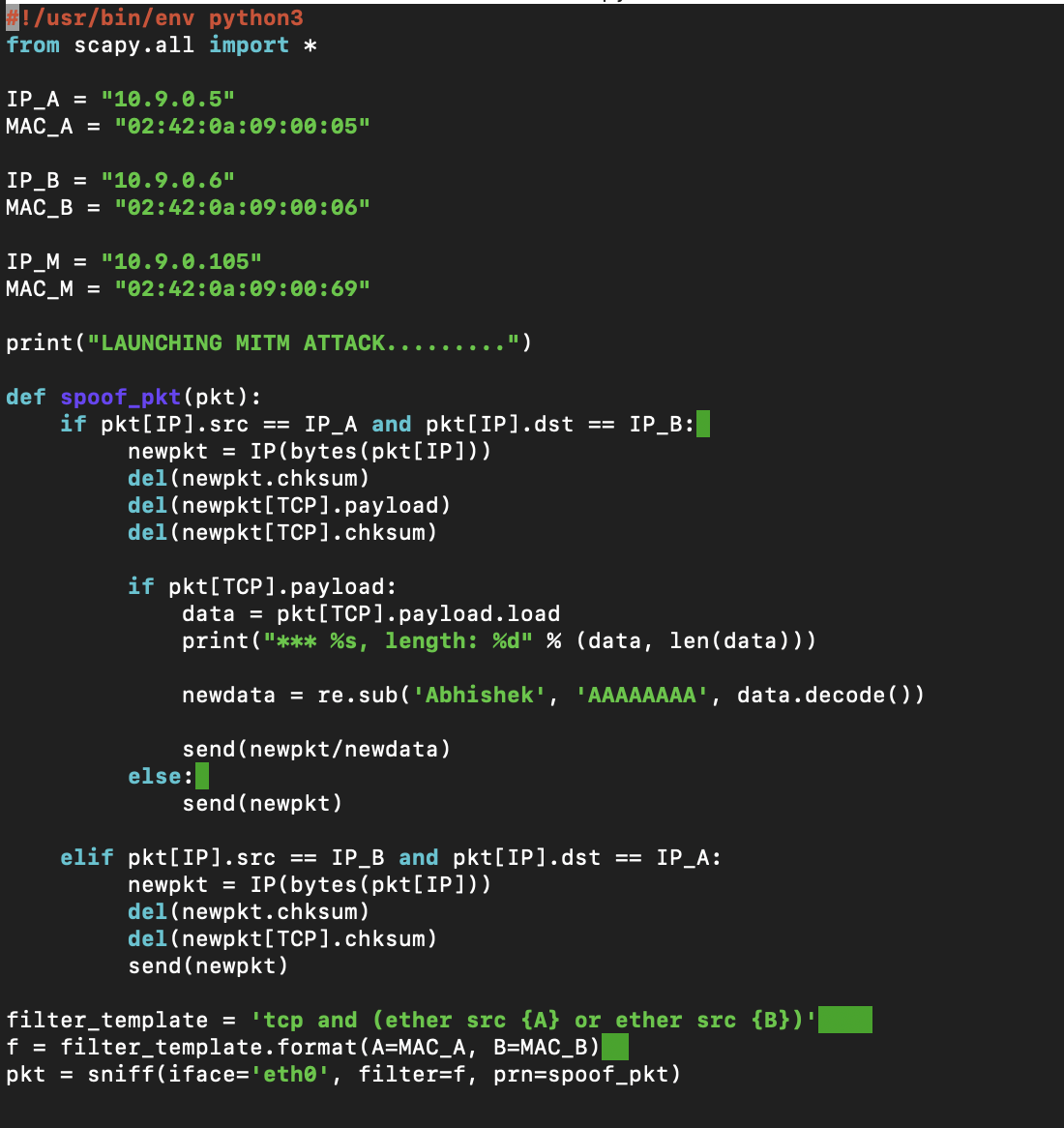


Result:  


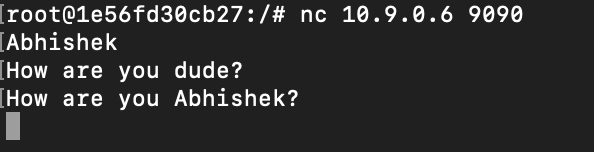
Observations:

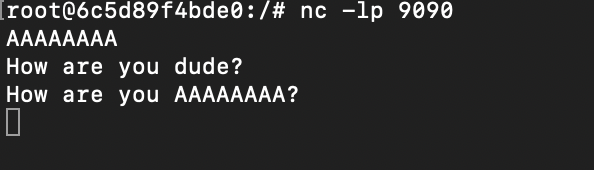
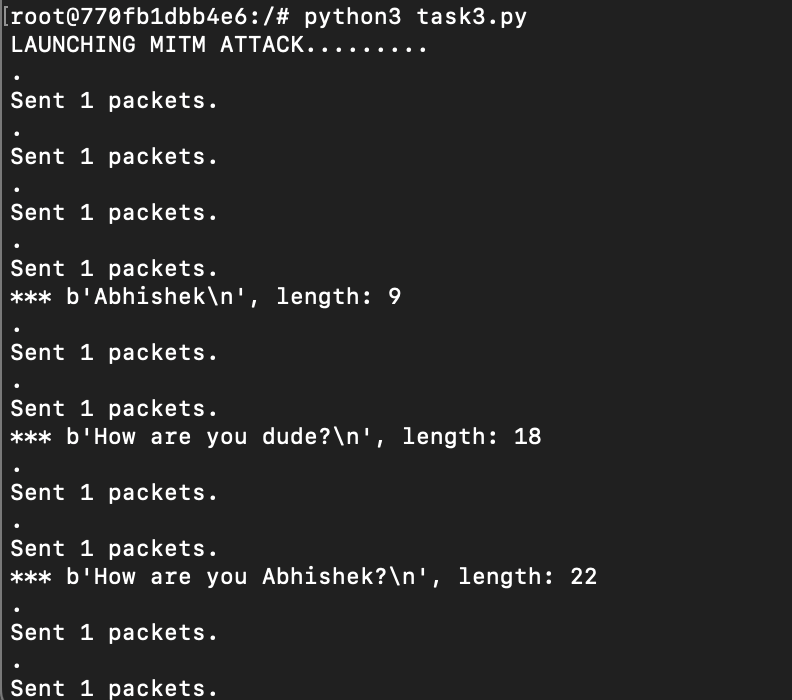
We just see ‘Z’ for all characters and numbers and special character are preserved.

**Task 3**

Code:

Result:





Observations:

We see that my first name Abhishek is changed to AAAAAAAA. There is slight change in code from task 2. We turn ip forwarding on for connection the we turn it off so that we can send required packet.