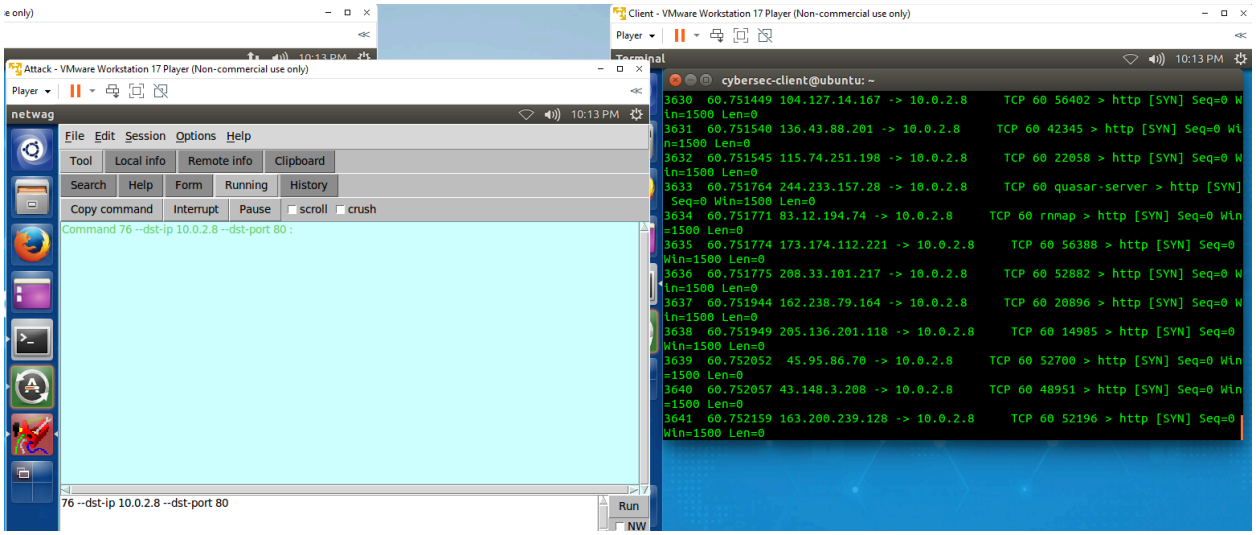
Task 1 - Syn Flooding

1. Observe the attack and take screenshots of the attack scenario



2. Comment on your observation

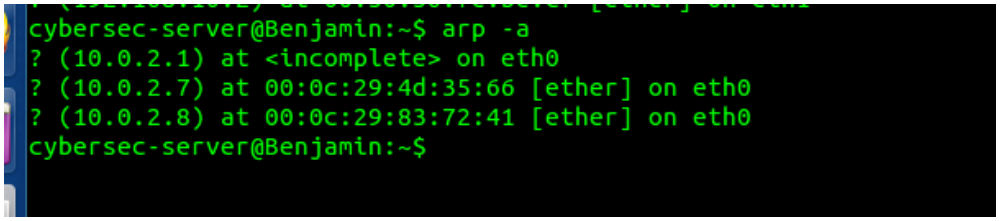
   The program continuously sends packets to the allocated ip address (10.0.2.8) resulting in continuous SYN processes. They happen at a really rapid speed as the terminal always had a constant feed.

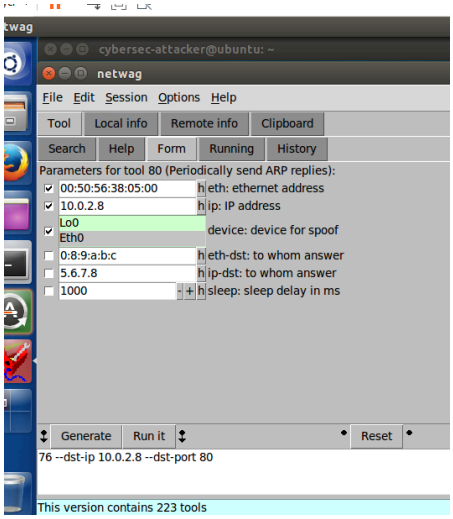
3. Categorize this attack in terms of severityu and how it is linked to DDoS attack.

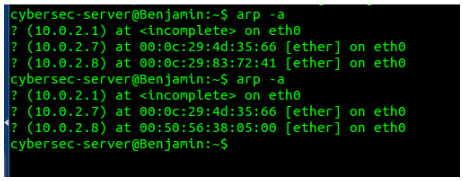
   This attack can be very severe as it can overwhelm servers if done from multiple attacks. This can result in DDoS attacks if the servers cannot handle the rapid requests resulting In overloading of server processes.

Task 2 - ARP cache poisoning

1. Observe the attack and take screenshots of the attack scenario







2. Comment on your observation

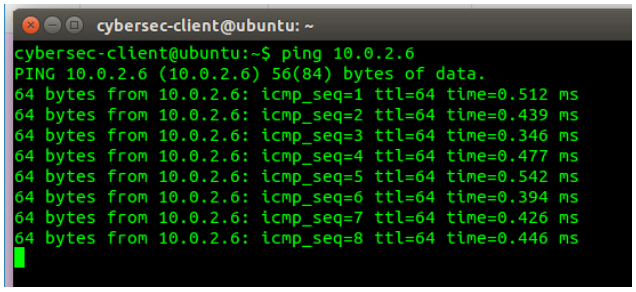
The ARP details were modified due to the poisoned packet being sent to the server.

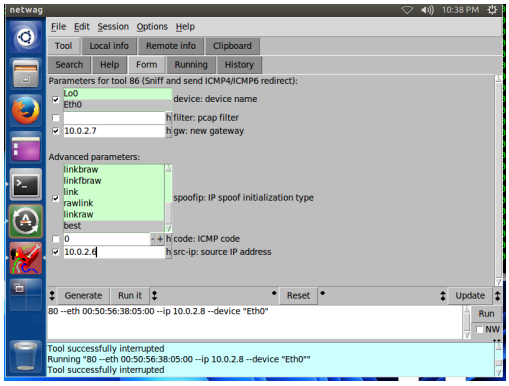
3. Briefly describe how you can mitigate this attack

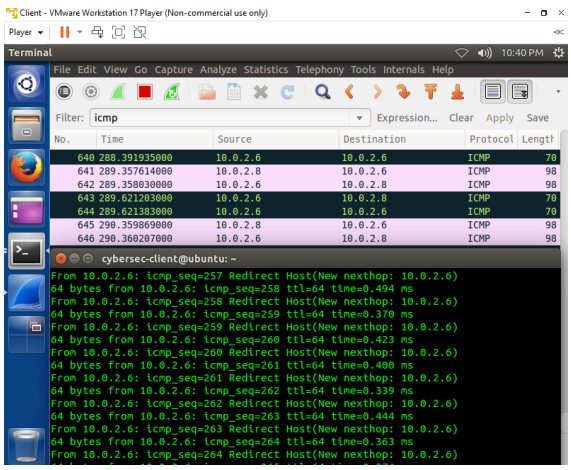
Packet Filtering is a good way to identify poisoned ARP packets preventing them from affecting the system.

Task 3 - ICMP Redirect

1. Observe the attack and take screenshots of the attack scenario







2. Comment on your observation

   Datapackets are being transferred/redirected to the host using the direct path rather than the fastest route.

3. Briefly describe how you can mitigate this attack

- Use a secure routing protocol
- Editing the etc/sysctl File to restrict the redirection