TCP Reset

In this task, the attacker wants to stop a telnet connection happening between two victims by exploiting the TCP Reset attack. Complete the script with the source/destination IPs, source/destination ports, flag and sequence number of the packets to send. To verify you have been successful, try to connect via telnet to the victim via a second host in the network.

Instructions on basic stuff

2) Build and turn on containers (dcbuild, dcup)
3) If for any reason it does not work, shut down all containers and remove them with the following commands
docker stop $(docker ps -a -q)
docker rm $(docker ps -a -q)
and get back to step 2
4) To see the name of the network interface, use ifconfig. The interface name of interest should start with “br-”. Alternatively, you can run docker network ls and look for the interface named “net-10.9.0.0”, extract its ID and add “br-” in front of it
5) To see the ID assigned to your containers, use dockps
6) To move into a container, use docksh ID
7) To create a file use touch name_file
8) To modify the file use nano (to save CTRL+O, CTRL+X)

[NOTE]
With our exploit we are sniffing packets in the network and extracting information from these sniffed packets. Thus, you should try to login with telnet with your exploit running in order to send packets in the network that can be sniffed. Packets can be exchanged by just typing on you keyboard when trying to login.