Reverse Shell

Through the TCP Session Hijacking attack, an attacker can hijack an existing TCP connection (session) between two victims by injecting malicious contents into this session. If this connection is a telnet session, attackers can inject malicious commands (e.g. deleting an important file) into this session, causing the victims to execute the malicious commands. In this task, the attacker wants to run a reverse shell from the victim machine to give the attack the shell access to the victim machine.

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]
To have a bash shell on a remote machine connect back to the attacker’s machine, the attacker needs a process waiting for some connection on a given port. To do so, you can use netcat

```
+-------------------------------------------------------+
| On 10.9.0.1 (attcker)                                 |
|                                                       |
| $ nc -lnv 9090                                        |
| Listening on 0.0.0.0 9090                             |
| Connection received on 10.9.0.5 49382                 |
| $ <--+ This shell runs on 10.9.0.5                    |
|                                                       |
+-------------------------------------------------------+
```