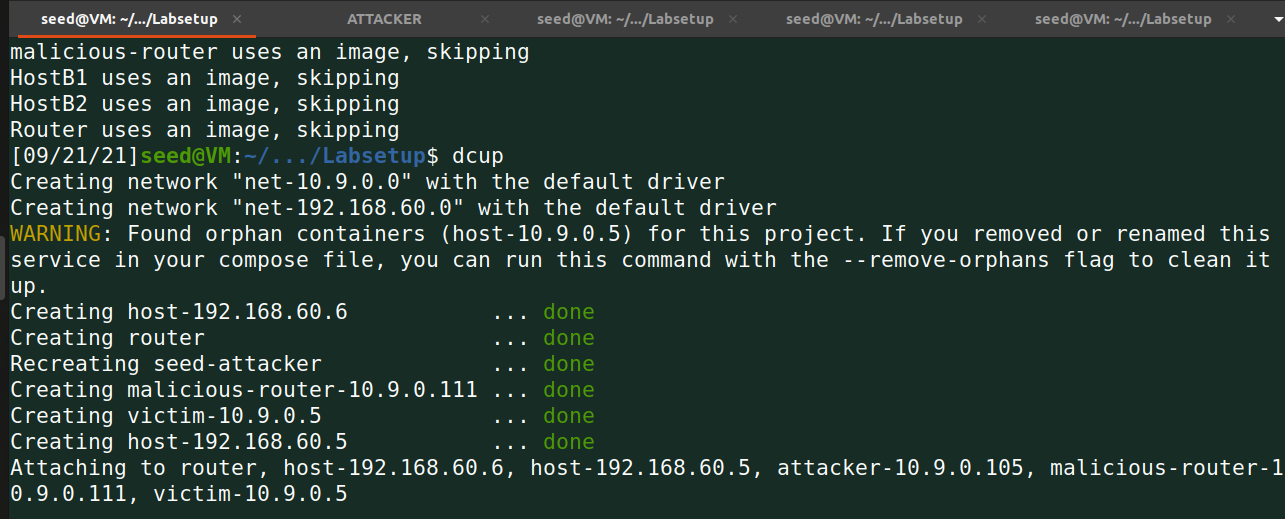
Lab-4 Report: ICMP Redirect Attack

Shrikant Kale - 700727822

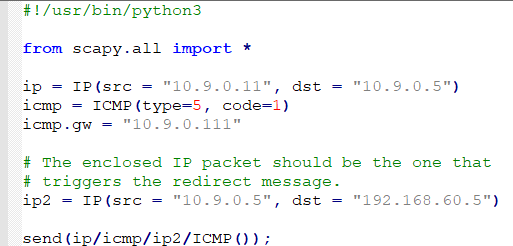
1. **Lab Environment Setup**

* Created Lab environment using docker containers.
* To execute docker container, I have used docker-compose commands.
  + dcbuild (docker-compose build) – to build the docker container image
  + dcup (docker-compose up) – to run the docker container
  + dcdown (docker-compose down) – to shut down the container

****

1. **Task 1: Launching ICMP Redirect Attack**
   * + - **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**

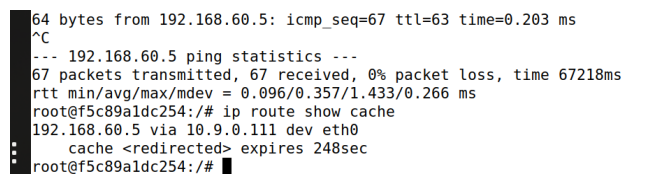
**The following is the code to perform ICMP redirect to Victim:**

****

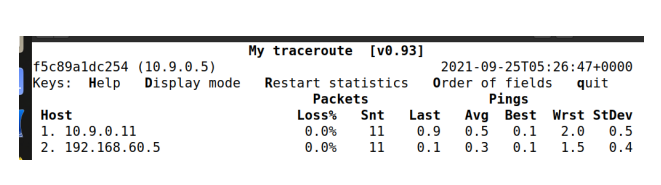
**Running iproute on victim computer**

****

**Route changing worked after using ip route show cache**

****

**- DOING A TRACEROUTE ON THE VICTIM MACHINE, AND SEE WHETHER THE PACKET IS REROUTED OR NOT**

****

* **If you look at thedocker-compose.ymlfile, you will find the following entries forthe malicious router container. What are the purposes of these entries? Please change their value to1, and launch the attack again. Please describe and explain your observation**
  + **After setting the below changes the victim container to will not accept ICMP redirect messages.**

**Sysctls:- net.ipv4.conf.all.send\_redirects=0**

**- net.ipv4.conf.default.send\_redirects=0**

**- net.ipv4.conf.eth0.send\_redirects=0**