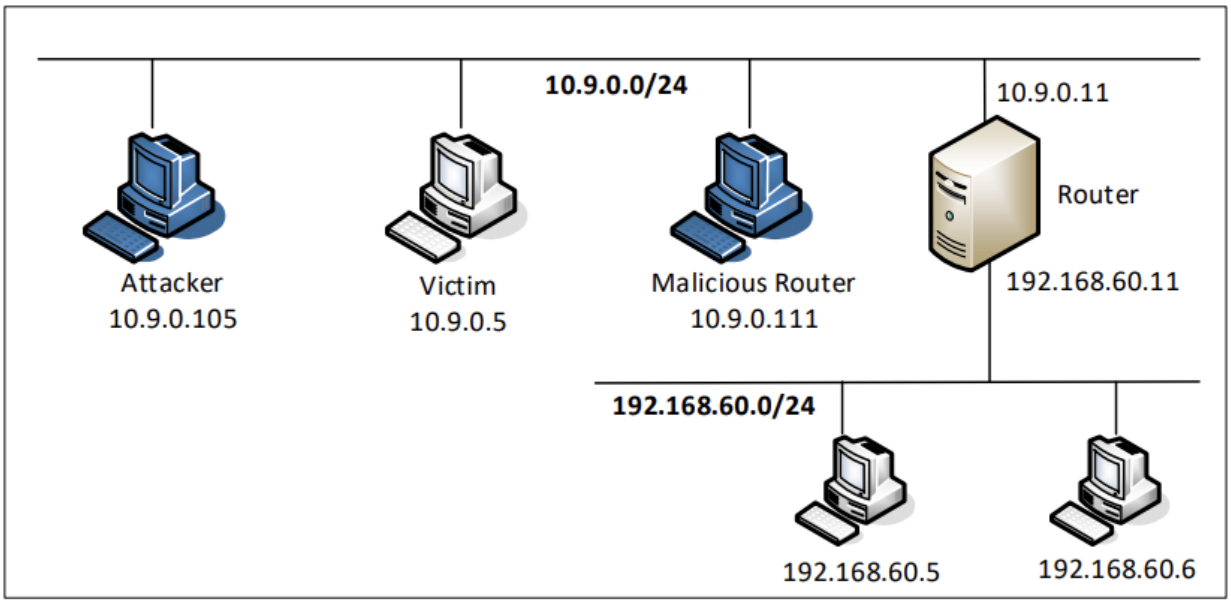
Nguyen Viet Hoang Nam

ITITIU19162

System and Network Security

Lab 4

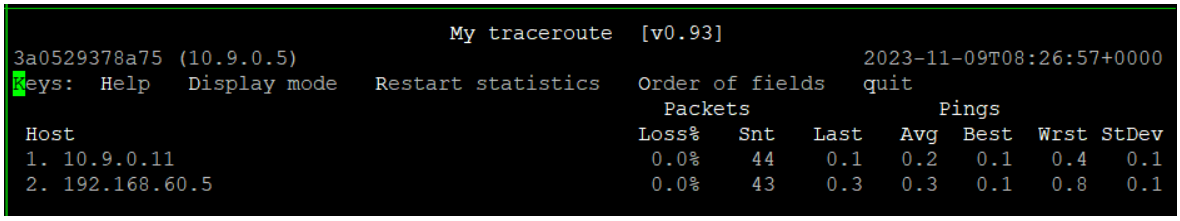


Task 1

Q1. 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.

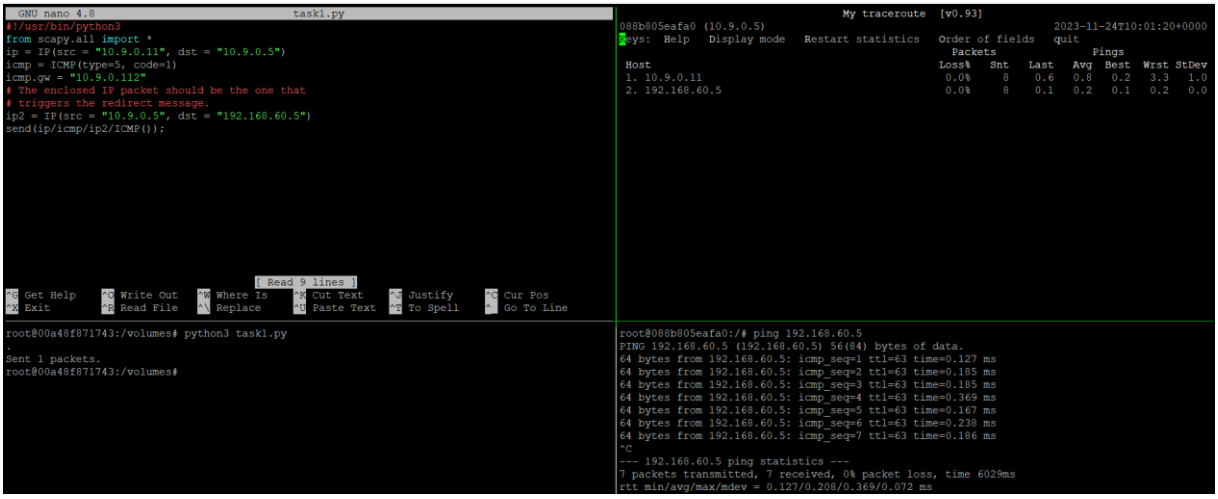
```
#!/usr/bin/python3
from scapy.all import *
ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
icmp = ICMP(type=5, code=1)
icmp.gw = "192.168.60.6"

# 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());
```



I changed the gateway to 192.168.60.6 and the attack was not succeed because ICMP redirect attacks typically aim to manipulate a host's routing table to redirect traffic within the local network, not to a remote machine outside the local network.

Q2. Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation.



The gateway was changed to 10.9.0.112 which was not exist in the local network and the attack result was unsuccessful because the victim routing cache table could not be updated as the non-exist IP gateway did not respond or reachable.

Q3. If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation.

Those are for determine whether the host should act as a router to forward packets between network interfaces or act as a standalone host and to control the sending of ICMP redirect messages on interfaces.