Cmpt 280 - Assignment 5
Darion Kwasnitza - 3122890

Setting up lab environment using docker-compose up

```
[02/28/24]seed@VM:~/.../Labsetup$ docker-compose up
WARNING: Found orphan containers (B-10.9.0.6, M-10.9.0.105, A-10.9.0.5, hostA-10
.9.0.5, hostB-10.9.0.6) for this project. If you removed or renamed this service
 in your compose file, you can run this command with the --remove-orphans flag t
o clean it up.
Starting host-192.168.60.5           ... done
Starting victim-10.9.0.5             ... done
Starting router                      ... done
Starting malicious-router-10.9.0.111 ... done
Starting host-192.168.60.6           ... done
Starting attacker-10.9.0.105         ... done
Attaching to victim-10.9.0.5, host-192.168.60.6, attacker-10.9.0.105, malicious-
router-10.9.0.111, host-192.168.60.5, router
```

Setting up the victim machine (able to use d7 because it is unique)

```
[02/28/24]seed@VM:~/.../Labsetup$ docksh d7
root@d734fbe110c8:/#
```

Setting up the attacker machine (able to use 2c because it is unique)

```
[02/28/24]seed@VM:~/.../Labsetup$ docksh 2c
root@2caa4ab90ddd:/#
```

Pinging 198.168.60.5 from the victim machine

```
root@d734fbe110c8:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.130 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.065 ms
```

Launching the attack from the attacker's machine using .volumes/icmp_redirect.py

```
Sent 1 packets.
root@2caa4ab90ddd:/# ./volumes/icmp_redirect.py
.
Sent 1 packets.
root@2caa4ab90ddd:/# ./volumes/icmp_redirect.py
.
Sent 1 packets.
```

Checking the ip route show cache on the victim machine, evidence of a redirection via 10.9.0.111. Successfully completed task 1.

```
root@d734fbe110c8:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 288sec
```

Question 1.

I wasn't able to do this, so I can conclude that ICMP redirect attacks can only occur on networks connected like LAN, for example. When I tried to do this, nothing happened when I ran the attack, and no IP route cache was shown.

Question 2.

No, I also couldn't do this because the machine does not exist, and it does not even have an IP address to redirect. However, if the machine were on the same network theoretically, it still wouldn’t work. The attack did not work when I inputted a random machine that did not exist.

Question 3.

When I changed them all to 1, I expected drastic change. However, I didn’t see a change. I assume it was supposed to redirect all IP addresses, but I couldn’t tell because I only have one machine running. I did some research online, and it confirms that there should be more hosts that are affected by this attack, not just one.

All of the work I have done above is my own