**LAB 2: ICMP Redirect Attack Lab**

Sending an ICMP redirect message to the sender of an IP packet is an error message delivered by a router. Senders of packets to the same destination may be advised to use an alternative router by a router if it suspects the packet is being routed wrongly. In order to modify a victim's route, ICMP redirect can be utilized by attackers.Using an ICMP redirect attack, the malicious router container (10.9.0.111) will act as the victim's router when packets are sent to 192.168.60.5. This is the goal of this work.

This means that the attacker is able to intercept and modify packets that are being sent out by the malicious router that is controlled by the attacker.

Task 1: Initializing and setting up the container.

Text

Description automatically generated

Text

Description automatically generated Text

Description automatically generated

We'll be attacking the victim container from the attacker container for this operation. The victim will connect to the 192.168.60.0/24 network via the router container (192.168.60.11). As shown in the below figure we ping the destination from the victim side.

Text, table

Description automatically generated with medium confidence

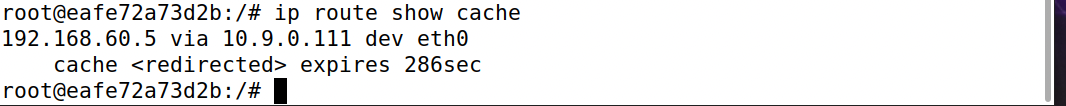
And we launch the attack from the attacker machine.

Text

Description automatically generated

Nowwe run ip route on the victim container to check the cache and we got the following output. The routing table is unaffected by ICMP redirect packets, but the routing cache is.

Until the entries expire, the routing cache overwrites the routing table.



Now we do a traceroute on the victim machine and we check if the packets are rerouted or not using the following command: mtr -n 192.168.60.5 and we can see that the packets are being re-routed to the malicious router

A picture containing text

Description automatically generated

**Questions:**

1. In this case, the IP address assigned to icmp-gw is a computer that is not on the local LAN, therefore we are trying to divert the ICMP attack to a remote machine. A look at the figure below shows that it didn't work out.

Text

Description automatically generated with low confidence



Text

Description automatically generated

1. Here I assigned the IP address to a local computer that is either offline or non-existing and we can see from the figures below that we cannot redirect ICMP attacks to a non-existing machine on the same network.

Text

Description automatically generated



Text

Description automatically generated

1. The below figure shows that I have changed the entries to ‘1’. These are countermeasures. The purpose of these entries are to disable the sending of ICMP redirect requests

Text

Description automatically generated

The below figure shows that after launching the attack it does not redirect to the malicious router but to the normal router.

Text

Description automatically generated

Task 2:

We repeat the steps of task 1 and we get the cache.

From destination server we start listening. Start the netcat server on the container 192.168.60.5

Text

Description automatically generated

From Victim server we connect to the server and When we send a message, we get it at the destination.

Text

Description automatically generated



IP forwarding is enabled in the malicious router's configuration, allowing it to act as a router and forward traffic to other computers. It is imperative that we stop forwarding IP packets when we begin the MITM attack in order for us to intercept and modify the packet. We can accomplish this by disabling the rogue router's IP forwarding. And we do it using the command: sysctl net.ipv4.ip\_forward=0

Text

Description automatically generated

Now we launch the mitm attack from the malicious router container. It is a sniffer. It captures the packet which victim sends to the destination.

Text

Description automatically generated with low confidence

Graphical user interface, text, application, chat or text message

Description automatically generated

Text, letter

Description automatically generated

**Questions**:

1. In your MITM program, we capture the traffics in one direction. which is source to destination
2. I launched the attack using both and I tried capturing the traffic from both A’s IP address and MAC address as shown below. Here I got the output for both scenarios and therefore IP addresses are not reliable for MITM attacks due to the ARP protocol. Now the problematic one would be using the IP address instead of MAC address.

Text

Description automatically generated

Text, letter

Description automatically generated

