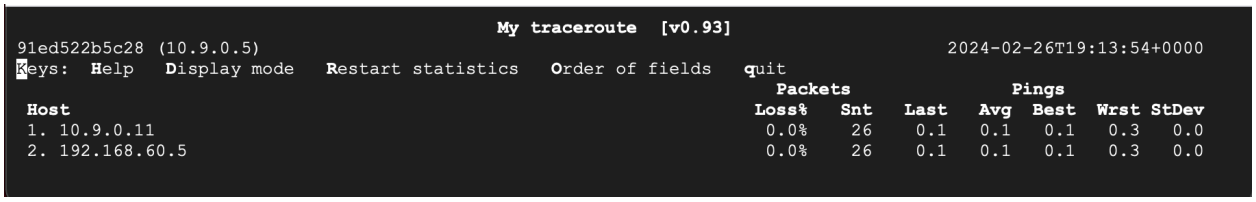
Nini Ola
Cyber Security
February 28 2024

Lab 3: ICMP Redirect

1. Task 1 :Launching ICMP Redirect Attack

a. Verification of attack success:

i. Picture before icmp attack

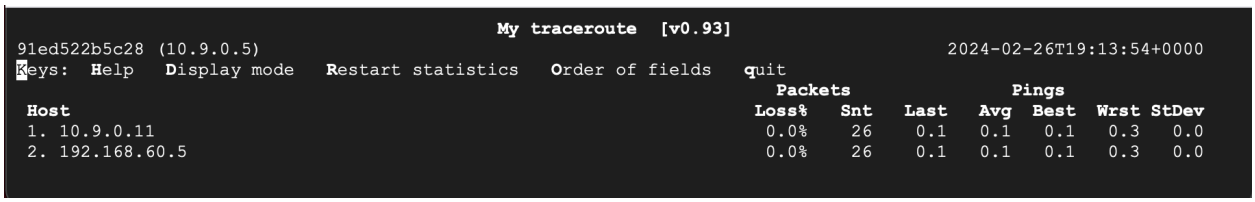


ii. Picture after icmp attack : the picture would have the attacker router in it so the ip addresses would be like below after running traceroute, the ip redirect would also show up in the cache of the victim.

1. 10.9.0.11
2. 192.168.60.5
3. 10.9.0111

b. **Question 1:** 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.

- **Output:** Here after flushing cache from previous experiment, and recreating the experiment, the attacker ip won't show up in the victims traceroute showing that the attack wasn't successful. It will look like the picture below

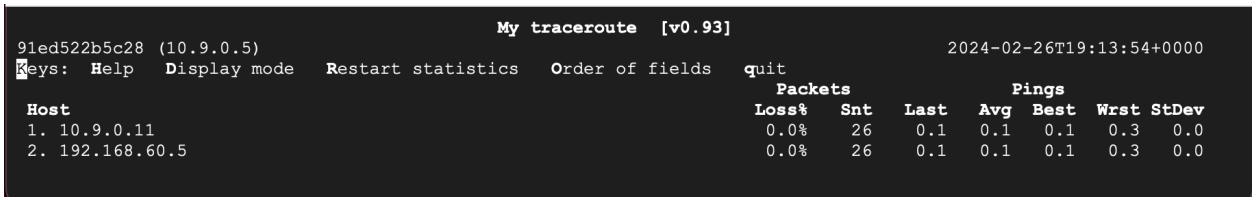


-

- **Explanation answer:** you cannot use icmp redirect attack to redirect to a remote machine, because icmp attacks are limited to redirecting within the same local network. If the target address is outside the local network, the attack wont work. Therefore the redirected address must be within the same local network as the sender

c. **Question 2:** 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.

- **Output**: here the cache of the victim won't be changed. The ip cache would look the same before and after the attack has been done



- **Explanation**: the icmp redirect attack wont work to redirect to a non-existent machine because the host will use the arp protocol to get the target mac address. If the target ip doesn;t exist the arp protocol won't return a mac address. As a result, the victim host will not update the routing table with a non-existent mac address , the current traffic continues and the redirect attack will fail.

d. **Question 3:** 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

- **Explanation** : The purpose of the entries are to disable the sending icmp redirect messages from the malicious router, they modify the kernel parameters related to sending ICMP redirects for different network interfaces:
- net.ipv4.conf.all.send_redirects=0: Disables sending ICMP redirects for all network interfaces.
- net.ipv4.conf.default.send_redirects=0: Disables sending ICMP redirects for the default network interface.
- net.ipv4.conf.eth0.send_redirects=0: Disables sending ICMP redirects for the eth0 network interface.

By setting these values to 0, the container instructs the kernel not to send ICMP redirects, which prevents it from attempting to redirect traffic.

- **Output when set to 1:** With the values set to 1, the victim host will receive ICMP redirect messages from the malicious router container. The victim will update its routing table based on the received ICMP redirects, potentially redirecting traffic through the malicious router.

2. **Task 2 : Launching the MITM Attack**
    a. **ATTACK success VERIFICATION**
        i. **OUTPUT :** Once the netcat connection has been established, you can verify the man in the middle attack is successful by typing on the victim's host and the message will be received on the malicious router in the form of a packet.
    b. **QUESTION 4:** In your MITM program, you only need to capture the traffic in one direction. Please indicate which direction, and explain why.

- **Explanation:** The direction is the traffic flowing from the victim to the target, the victim will send the message to the attacker not the target. This is because the attacker is hoping to capture information sent by the victim to the target and this direction allows this to happen. Intercepting from the victim to the target will allow the attacker to temper with the contents of the message, making the attack more efficient.

    c. **Question 5:** In the MITM program, when you capture the nc traffic from A (10.9.0.5), you can use A's IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion.
        i. **A's IP : Using A's IP address in the filter:**

- **Observation:** This filter captures traffic where the source or destination IP address is 10.9.0.5. It successfully captures traffic from host A to other hosts on the network.

        ii. **Using A's MAC address in the filter:**

- **Observation:** This filter captures traffic where the source MAC address is A's MAC address. It successfully captures traffic from host A to other hosts on the network.

Explanation answer: Both filtering options may initially appear to work but using A's IP address in the filter is the correct choice because it is more resilient to potential

changes to host A's network configuration. Filtering by IP address ensures that all traffic originating from host A, regardless of the source or destination IP addresses used, is captured. While filtering by MAC address may be less reliable if host A modifies its MAC address or uses multiple network interfaces.

- **Therefore, using A's IP address in the filter is preferred in a MITM attack.**