**ICMP Redirect attack (Man in the middle attack)**

Name – Jagdeep Kainth

March 15, 2024

**Executive summary**

This report explains about the packet redirection functionality provided by internet Control Message protocol(ICMP). The report discussing about what presence of ICMP Redirect messages in the network usually tells. Man in the Middle attack are one of the most common and dangerous cyber-attack, that can be a great harm to the security and privacy of the network. In this attack, a attacker(malicious actor) tries to intercept and change the communication between two hosts , for example a user and a web application page or a client and a server or even two different devices communicating on the same network. The attacker can steal important information of the victim, alter that information, inject malware, steal credential, redirect traffic. There are some recommendations to prevent this attack from happening. Client can use secure communication protocols for this such as HTTPS and avoid using http Client should only consider using those web pages that has SSL(secure socket layer) certificate. Usage of SSH (secure shell), SFTP(Secure File Transfer Protocol) for file transfers are highly recommended. Using VPN, and applying strong encryption and authentication protocols, firewalls, antivirus software can protect against MITM attack.

[ Rublon Authors, December 14, 2023 ]

**Attack Description**

An error message that a router sends to the IP packet sender is known as an ICMP redirect. Redirects are used by routers to let senders know that their following packets sent to the same destination should use a different router if they think a packet is being routed wrongly. One may utilize ICMP redirection by attackers to alter the victim's path. The aim of this operation is to initiate an ICMP redirect attack against the victim, so that the malicious router container (10.9.0.111) will be used as the victim's router when it receives packets addressed to 192.168.60.5. Since the attacker controls the malicious router, the attacker has the ability to intercept packets, alter them, and then resend the altered packets.

In this lab experiment, we will create a virtualized environment using docker container in seed ubuntu virtual machine. The attacker (10.9.0.105) used the malicious router to gain access to victim (10.9.0.5) computer. The attacker will intercept the packets that were being send through legitimate router 10.9.0.11 to the network 192.168.60.11. The picture given below is the exact topology used in this experiment. [ Wenliang Du, 2020 ]

**A computer network diagram with numbers and symbols

Description automatically generated with medium confidence**

**Lab experiment**

**Setting up the environment**

Task 1- After unzip the lab folder and opening terminal, We will first go in the lab directory using cd command to run docker file using commands, such as docker-compose build and docker -compose up. To ensure that the victim computer will accept the ICMP redirect message. We will turn off the by default protection by simply using the command changing the value of net.ipv4.conf.all.accept\_redirect=1, which was 0 before.

**A screenshot of a computer

Description automatically generated**

Now on the victim, we will check IP route and we can see its going via 10.9.0.11 which is a legitimate server. Our goal in this experiment is to redirect the ICMP packet via malicious router which is 10.9.0.111. we will run a python script called redirect.py (code given at the end of document) from the attacker computer. After running the script we will verify that if the attack worked or not by using the command mtr -n 192.168.60.5 on the victim computer.

A screenshot of a computer

Description automatically generated

Before the attack

A screenshot of a computer

Description automatically generated

After the attack

A screenshot of a computer

Description automatically generated

From the table observations above we can see that now the ICMP redirect packet is going via the malicious router, hence we successfully completed the part 1 of the MITM attack.

Task 2 – now we will start the TCP Client and server program using netcat by using the following command nc -lp 9090 on the destination container( 192.168.60.5) and nc 192.168.60.5 9090 on the victim container.

By default the ip forwarding is enabled on the malicious router so that it should behave like a router and transfer packets to other hosts. We will change this setting so that we can intercept the packet during the MITM attack by setting the ipv4 forward limit to 0.

A screenshot of a computer screen

Description automatically generated

The last step is launching the mitm\_sample.py file

A screenshot of a computer program

Description automatically generated

The script is a prime example of a Man-in-the-Middle (MITM) attack tool, in which the attacker listens for targeted communication, intercepts it, and may even change its contents before forwarding it to the intended target. Often, the intention is to steal or alter data without the sender's or recipient's awareness.

**Recommendations**

This attack can be prevented by applying some measures by disabling the ICMP Redirect Acceptance which is a very common vulnerability in this attack. Company must disable this from all hosts and routers. This can be done by the command sysctl net.ipv4.conf.all.accept\_redirects=0 as we discussed during the lab. Usage of firewalls and antivirus software can be life saver in this attack, applying security tools can also prevent this attack from happening. It can block unauthorized and malicious connections from reaching your devices.

Make use of safe communication methods.   
The use of SSL/TLS and HTTPS has grown in popularity. In reality, 95% of Google websites use HTTPS, according to the company's January 2022 transparency report. All HTTPS connections aren't created equal, either. Always verify that the website you are viewing has a valid certificate issued by a reputable organization by looking at its certificate information. Additionally, you should refrain from opening attachments or following links from unidentified or dubious sources since they may direct you to dangerous websites. Additionally, you ought to employ additional safe protocols like VPN (Virtual Private Network) to encrypt all of your network traffic, SFTP (safe File Transfer Protocol) for file transfers, and SSH (Secure Shell) for remote access.

[ Rublon Authors, December 14, 2023]

**How MITM Attacks may be avoided using encryption**

* The most popular defense against a Man-in-the-Middle (MITM) attack is to encrypt communication.
* This is how the procedure operates: a server issues a digital certificate to identify the client during data transfers. After then, the client-server communication is encrypted.
* A key is required in encryption in order to both encrypt and decode shared messages between the sender and the recipient. That key is necessary for us to interpret the notes, and it is also necessary for the attackers. Nobody can access our information without the key. Data can be encrypted in two ways:
* Symmetric encryption encrypts and decrypts communications using a single encryption key that is exchanged in secret between the sender and the recipient. Because of its fast encryption speed, this approach is extensively utilized; nevertheless, a drawback is that we require a safe way to transfer the keys. The hacker can readily access our sent data if they manage to obtain the key. Data protection using symmetric encryption is the most extensively used and well-liked method.
* When using asymmetric encryption, two keys—the public and private keys—are needed to encrypt data. While the private key is solely known to the receiver and is used to decrypt data, the public key is broadcast via an open channel and is available to everyone.

There are a few specific ways that we can most likely stop MITM attacks:

* We can avert these kinds of attacks by utilizing Virtual Private Networks, or VPNs. VPNs are used in local area networks to provide a secure environment for the usage of sensitive data. [ Yathaarth Swaroop, September 18,2021 ]
* Steer clear of public networks when working on delicate or high-risk projects. Steer clear of public networks when performing sensitive chores like online banking or transactions involving sensitive information.  
  Auto fill-ins should not be used on websites that are identified as insecure. utilize multi-factor authentication wherever possible, and never allow any insecure website to utilize your auto-filled usernames or passwords since this poses a significant danger.
* by using a network intrusion detection system to secure the network and installing the appropriate antivirus software.
* To keep your passwords safe, always use Password Manager.

[ Yathaarth Swaroop, September 18,2021 ]

**Case reflection**

By performing the given experiment above and working on the report of MITM attack, I have learnt that MITM attack can’t be performed without changing the route of redirected packet via the malicious router. That means that the biggest vulnerability in this attack is using a unsecured network which does not have SSL certificate. ICMP redirect attack wont work if the victim container has turned on the countermeasure for not accepting redirect messages and the attack wont work that way. The attack also wont work if the malicious router settings are configured wrongly by means if its Ip forwarding is enabled .

**References**

1. [ Rublon Authors, December 14, 2023]

https://rublon.com/blog/how-to-prevent-man-in-the-middle-attacks-on-your-network/

1. [ Wenliang Du, 2020 ]

https://seedsecuritylabs.org/Labs\_20.04/Networking/ICMP\_Redirect/

1. [ Yathaarth Swaroop, September 18,2021 ]

https://www.encryptionconsulting.com/everything-about-man-in-the-middle-attack/

**Codes**

1. **Redirect.py**

#!/usr/bin/python3

from scapy.all import \*

# default ip addresses

ip = IP(src=”10.9.0.11”, dst=”10.9.0.5”)

icmp = ICMP(type=5, code=1)

icmp.gw = “10.9.0.111”

#triggering packet

ip2 = IP(src=”10.9.0.5”, dst=”192.168.69.5”)

# Send the malicious redirect

Send(ip/icmp/ip2/ICMP())

1. **mitm\_sample.py**

from scapy.all import \*

print("LAUNCHING MITM ATTACK.........")

def spoof\_pkt(pkt):

newpkt = IP(bytes(pkt[IP]))

del(newpkt.chksum)

del(newpkt[TCP].payload)

del(newpkt[TCP].chksum)

if pkt[TCP].payload:

data = pkt[TCP].payload.load

print("\*\*\* %s, length: %d" % (data, len(data)))

# Replace a pattern

newdata = data.replace(b'seedlabs', b'AAAAAAAA')

send(newpkt/newdata)

else:

send(newpkt)

f = 'tcp'

pkt = sniff(iface='eth0', filter=f, prn=spoof\_pkt)