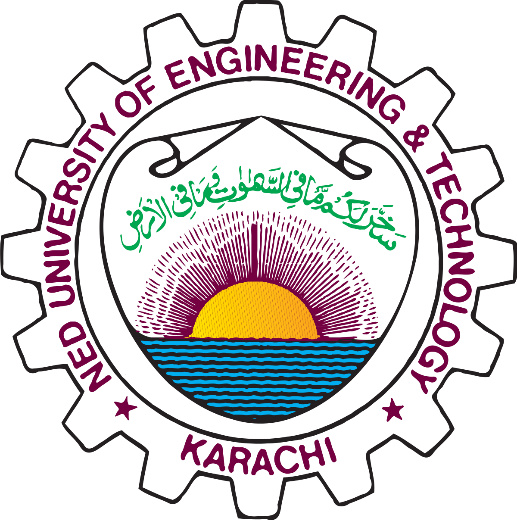
**CT-541 – NETWORK SECURITY**MS-IS 004 2019/20– Evening Fall 2019

**NS Assignment-02**

**ICMP REDIRECT**



**STUDENT NAME: MUHAMMAD UMAR TARIQ**

**STUDENT ID: IS 004 2019/20**

**COURSE INSTRUCTOR: Dr. MUBASHIR M KHAN**

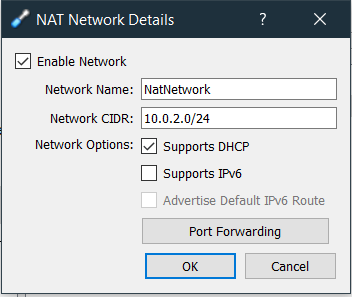
**DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY**

**NED UNIVERSITY, KARACHI CAMPUS**

**Virtual Machines Configured in Host-Only Networking Mode:**

**Windows Hosts Do not support the ICMP redirects. So we need NATNetwork**

1. Attacker Virtual Machine VM1 IP: 10.0.2.4
2. Victim VM2 IP: 10.0.2.5
3. Victim VM3 IP: 10.0.2.6
4. ACTUAL DEFAULT GATEWAY: 10.0.2.1

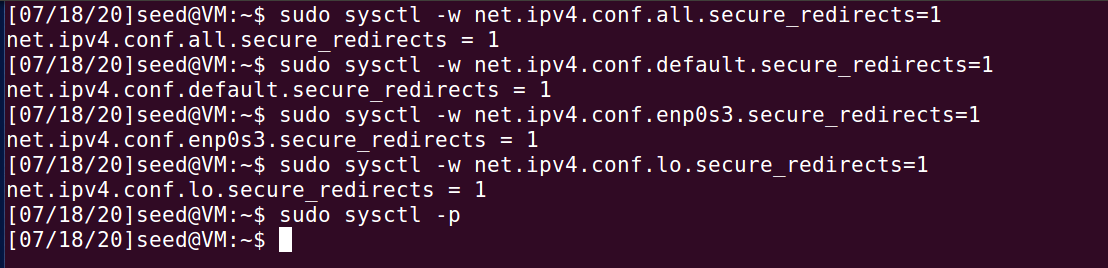


Step1: **Set Ubuntu Secure Redirects Feature to 1, on the attacker**

Since to Accept ICMP redirects ONLY FOR gateways LISTED in our default gateway list (enabled by default) we need to

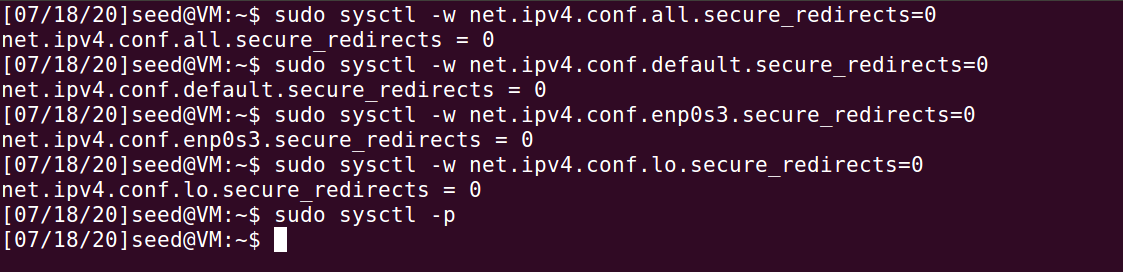
net.ipv4.conf.all.secure\_redirects = 1

similiarly, and remember to restart sysctl file. With new config.



Run sysctl -p for restarting this file after each configuration.

Step 2: **Modify Victim VM2 /etc/sysctl.conf file**



Step3: **VM3 will act as observer. Where we run the wireshark to observe traffic packets. We can also insert actual default gateway IP here. For demonstration purposes we enter the vm3 ip. So we can run wireshark to see icmp redirect messages in the wireshark packet capture.**

Step4: From Attacker VM1 terminal, Run:

Gateway example.

Command runs From Attacker VM1, to Victim VM2, the third IP is for observer machine on which we will run Wireshark:

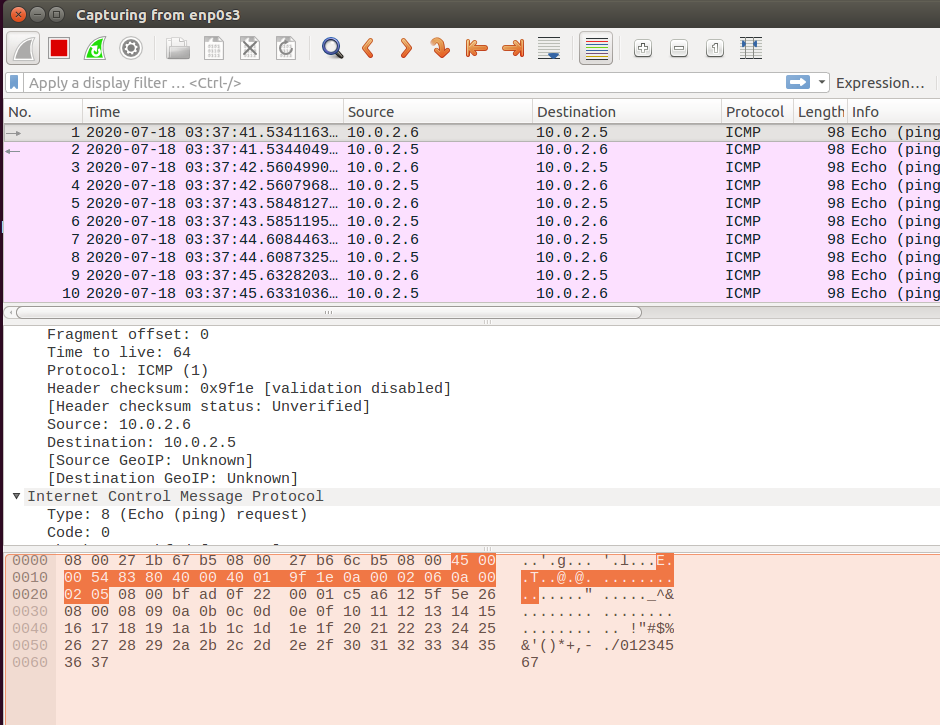
Sudo netwox 86 --device "enp0s8" --filter "src host VICTIMIP" --gw VICTIM\_REDIRECTED\_GATEWAY\_ATTACKERS\_IP --code 1 --src-ip ACTUAL\_GATEWAY\_OF\_VICTIM

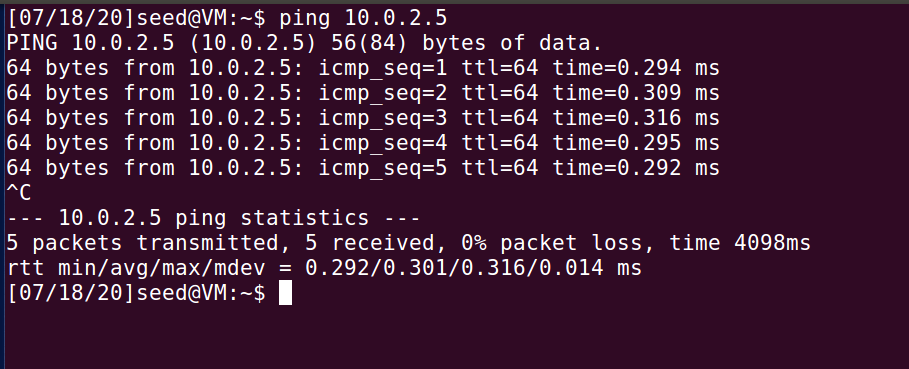
Sudo netwox 86 --device "enp0s8" --filter "src host 192.168.56.102" --gw 192.168.56.101 --code 1 --src-ip 192.168.56.1

**We can also use attacker’s ip as the gateway. This is done using:**

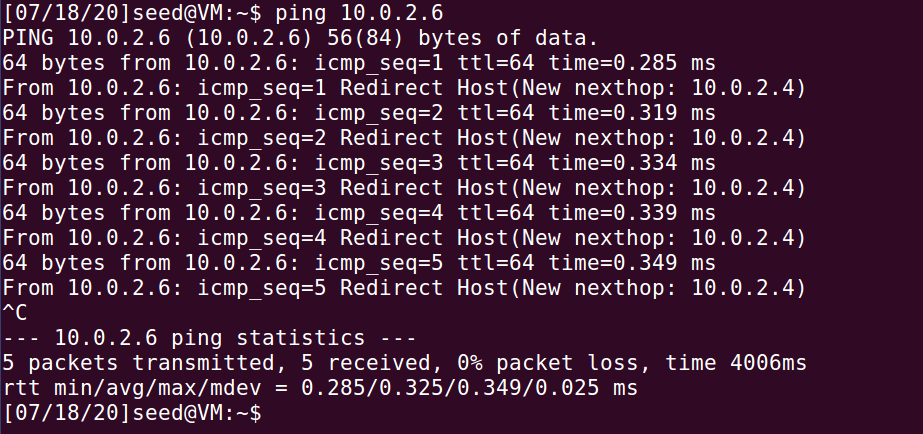
**sudo netwox 86 --device "enp0s3" --filter "src host 10.0.2.5" --gw 10.0.2.4 --spoofip "raw" --code 0 --src-ip 10.0.2.6**

**Before Attack:**Wireshark And Ping Before the Attack, Observing from VM3(10.0.2.6) Source and Victim is VM2(10.0.2.5) Destination:

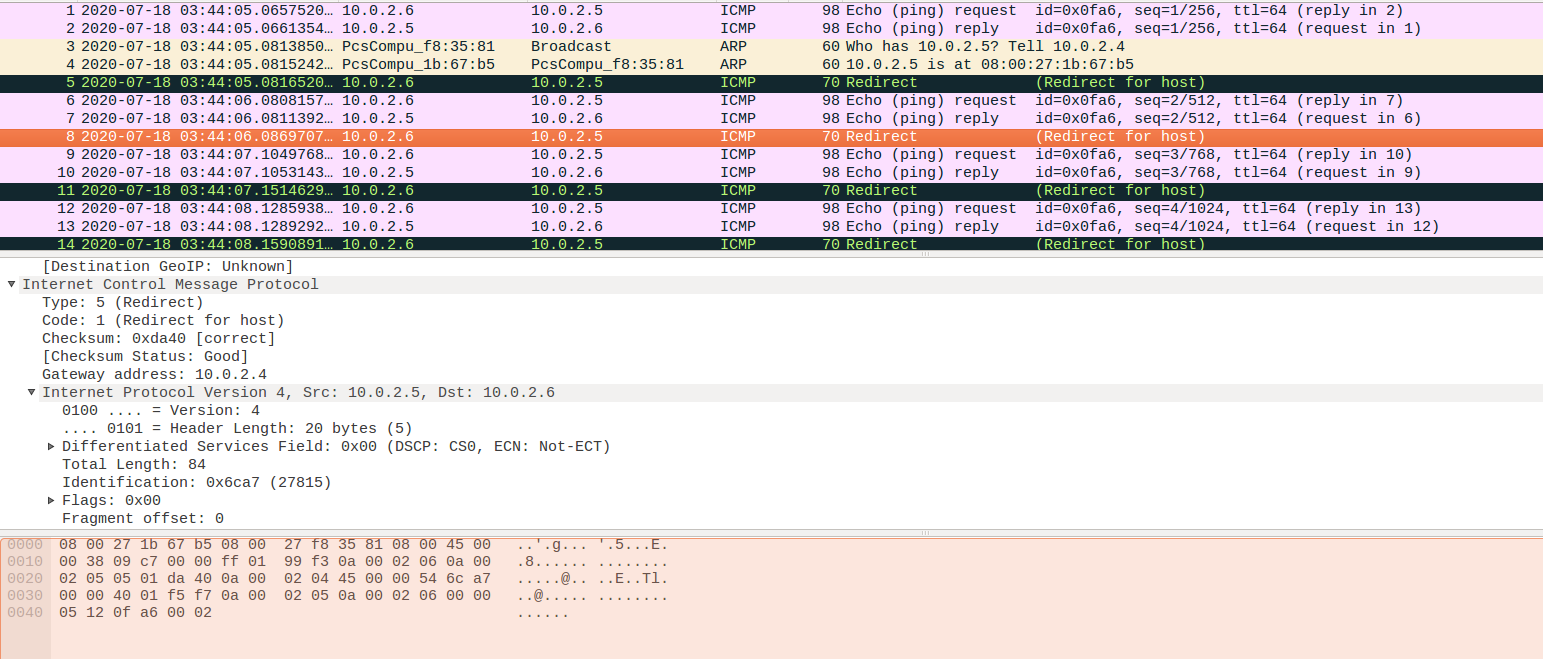




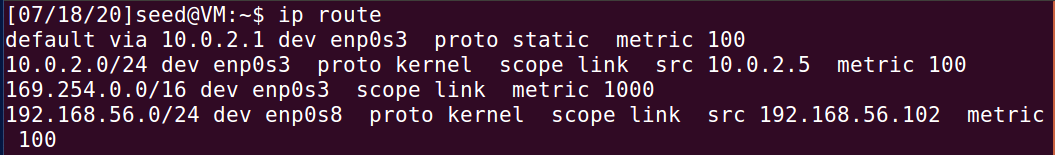
After Attack, **We Ping VM3 from VM2, Now Note The Redirect Host(New Next Hop)**:



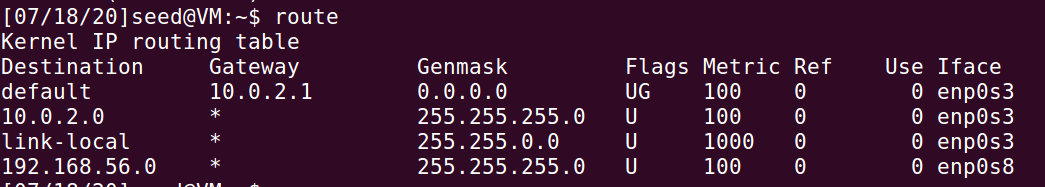
Also from VM3, we can see the ICMP Redirect and changed Gateway:



**ICMP Redirect Attack Mitigation / Security Defence Mechanisms**:



Route



These tables will not show this attack

if forwarding is disabled (we are not a router) value of net.ipvX.conf.all.accept\_redirects will be ORed interface-specific value e.g. net.ipvX.conf.eth0.accept\_redirects. send\_redirects is always ORed.

Full fix would be then:

Log in to your Linux server or desktop and open a terminal window. From that terminal, issue the command:

sudo nano /etc/sysctl.conf

The first option to look for is:

#net.ipv4.ip\_forward=1

Change that line to:

net.ipv4.ip\_forward=0

The next line to edit is:

#net.ipv4.conf.all.send\_redirects = 0

Change that to:

net.ipv4.conf.all.send\_redirects = 0

Add the following line under that:

net.ipv4.conf.default.send\_redirects = 0

Look for the line:

#net.ipv4.conf.all.accept\_redirects = 0

Change that to:

net.ipv4.conf.all.accept\_redirects = 0

Add the following line under that:

net.ipv4.conf.default.accept\_redirects = 0

Finally, add the following lines to the bottom of the file:

net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1

net.ipv4.tcp\_syncookies = 1

net.ipv4.tcp\_max\_syn\_backlog = 2048

net.ipv4.tcp\_synack\_retries = 3

net.ipv4.netfilter.ip\_conntrack\_tcp\_timeout\_syn\_recv=45

The above lines do the following:

Enable Bad Error Message Protection

Enable SYN cookies to ensure a server avoids dropping connections when the SYN queue fills up

Increase the SYS backlog queue size to 2048

close the SYN\_RECV state connections earlier

Lowers the timeout value for SYN\_RECV to help in reducing the SYN flood attack

Save and close the file.

How to reload the configuration

You can reload the configuration issue the command:

sudo sysctl -p

One caveat to the sysctl -p command is I found it didn't load the tcp\_max\_syn\_backlog properly. It wasn't until a reboot that the 2048 value was added. So, after running the sudo sysctl -p command, issue the command:

sudo less /proc/sys/net/ipv4/tcp\_max\_syn\_backlog

Make sure the value presented is 2048.

If the value is anything less, reboot the server.

At this point, your Linux server should be better protected against SYN attacks and IP address spoofing. Enjoy that newfound security.