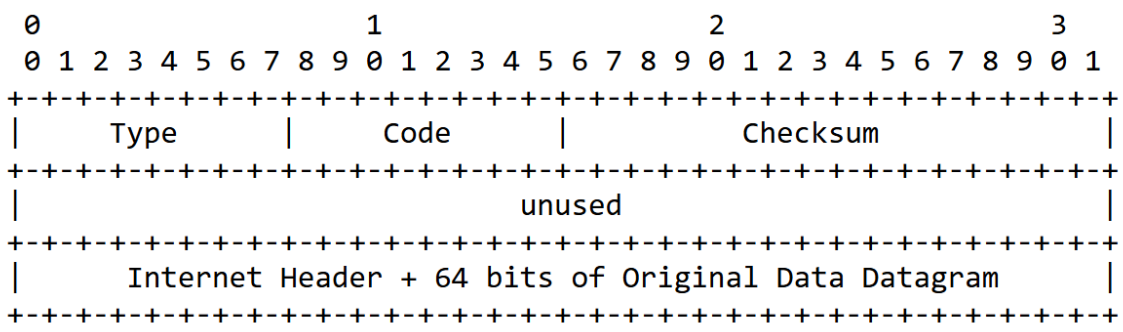
Nada Elshami

**ICMP Port Unreachable**

- Use hping3 to send one UDP segment to port 100XX on your partner's computer,
- Use one tcpdump command to capture the UDP segment (stimulus), and the ICMP message that was sent back (response).
- Save both packets in a file called **1ICMPPORT.pcap** using tcpdump filters and the –w and –c options

| |
|---|
| Your IP address (sender of ping): vm: 192.168.146.132, host: 10.16.47.227 |
| IP address of your partner (running tcpdump): vm: 10.0.2.15, host: 10.16.46.57 |
| **When is this kind of ICMP message sent?** |
| A port unreachable message is sent when a host receives a UDP packet that is destined for a closed port |
| **What is the ICMP message format for this kind of ICMP message? What are the type and code values?** |
| The answer to this question is as follows:<br>Destination Unreachable Message<br>  <br>ICMP port unreachable: type = 3, code = 3. |
| **What is the command you used to send the UDP segment?** |
| Hping3 –2 10003 –c 1 10.16.47.227 |
| **What is the tcpdump command you used to capture both packets? Include the filter you used to isolate the two packets.** |
| sudo tcpdump –i –eth0 –Xnvr 1ICMPPORT.pcap -c 2 'icmp or udp' |

```
┌──(mahimaavardini㉿mahimaa)-[~]
└─$ sudo tcpdump -i eth0 -Xnvr 1ICMPPORT.pcap -c 2 'icmp or udp'
reading from file 1ICMPPORT.pcap, link-type EN10MB (Ethernet), snapshot length 262144
14:15:59.613470 IP (tos 0x0, ttl 64, id 19351, offset 0, flags [none], proto UDP (17), length
 28)
    10.0.2.15.2559 > 0.0.39.19.0: UDP, length 0
        0x0000:  4500 001c 4b97 0000 4011 fc18 0a00 020f  E...K...@.......
        0x0010:  0000 2713 09ff 0000 0008 c2bd            ..'.........
14:15:59.614335 IP (tos 0xc0, ttl 255, id 58209, offset 0, flags [none], proto ICMP (1), leng
th 56)
    10.0.2.2 > 10.0.2.15: ICMP net 0.0.39.19 unreachable, length 36
        IP (tos 0x0, ttl 64, id 19351, offset 0, flags [none], proto UDP (17), length 28)
    10.0.2.15.2559 > 0.0.39.19.0: UDP, length 0
        0x0000:  45c0 0038 e361 0000 ff01 bf92 0a00 0202  E..8.a..........
        0x0010:  0a00 020f 0300 303b 0000 0000 4500 001c  ......0;....E...
        0x0020:  4b97 0000 4011 fc18 0a00 020f 0000 2713  K...@.........'.
        0x0030:  09ff 0000 0008 c2bd                      ........
```

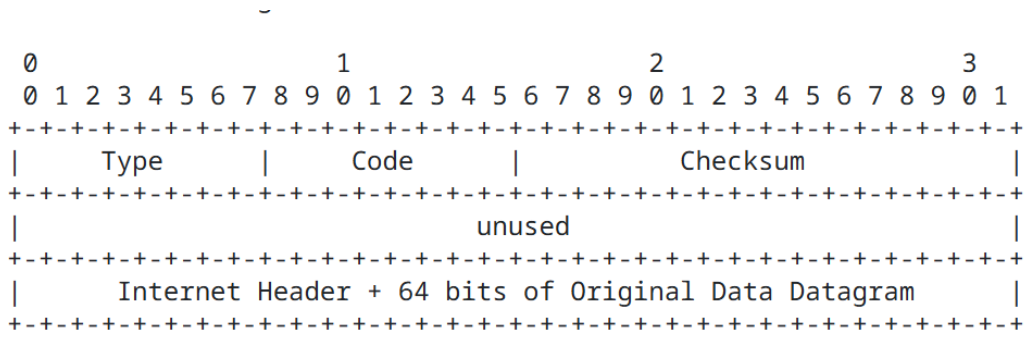
## 2. ICMP TTL Exceeded

- Use **ping** or **hping3** to send a packet to any host that will result in an **ICMP TTL exceeded** message being sent back to you. Use **tcpdump** to capture both packets (stimulus and response).
- Save both packets in a file called **2ICMPTTL.pcap** using tcpdump filters and the –w and –c options

**When is this kind of ICMP message sent?**

ICMP TTL Exceeded message is recieved when a packets time to live (TTL) field reaches zero before reaching its destination

**What is the ICMP message format for this kind of ICMP message? What are the type and code values?**




ICMP time exceeded: type=11 code=0

**What did you do to get this message (include the command you used to create the stimulus packet)?**

sudo hping3 -1 -t 1 -c 1 10.16.46.57

**What is the tcpdump command you used to capture both packets? Include the filter you used to isolate the two packets (stimulus and response).**

tcpdump –n –v -w 2ICMPTTL.pcap -c 2 –x

screenshot of the tcpdump output (hex and ASCII dump) showing the two packets (stimulus and response).

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -n -v -r  2ICMPTTL.pcap -c 2 -X
reading from file 2ICMPTTL.pcap, link-type EN10MB (Ethernet), snapshot length 262144
14:24:22.631326 IP (tos 0x0, ttl 1, id 64503, offset 0, flags [none], proto TCP (6), length 40)
    192.168.146.132.1078 > 10.16.42.107.0: Flags [none], cksum 0x216f (correct), win 512, length 0
        0x0000:  4500 0028 fbf7 0000 0106 3631 c0a8 9284  E..(......61....
        0x0010:  0a10 2a6b 0436 0000 06c1 b776 3ba7 06b9  ..*k.6.....v;...
        0x0020:  5000 0200 216f 0000                      P...!o..
14:24:22.631611 IP (tos 0x0, ttl 128, id 65514, offset 0, flags [none], proto ICMP (1), length 68)
    192.168.146.2 > 192.168.146.132: ICMP time exceeded in-transit, length 48
        IP (tos 0x0, ttl 1, id 64503, offset 0, flags [none], proto TCP (6), length 40)
    192.168.146.132.1078 > 10.16.42.107.0: Flags [none], cksum 0x216f (correct), win 512, length 0
        0x0000:  4500 0044 ffea 0000 8001 94f6 c0a8 9202  E..D............
        0x0010:  c0a8 9284 0b00 7cc2 0000 0000 4500 0028  ......|.....E..(
        0x0020:  fbf7 0000 0106 3631 c0a8 9284 0a10 2a6b  ......61......*k
        0x0030:  0436 0000 06c1 b776 3ba7 06b9 5000 0200  .6.....v;...P...
        0x0040:  216f 0000                                !o..
```

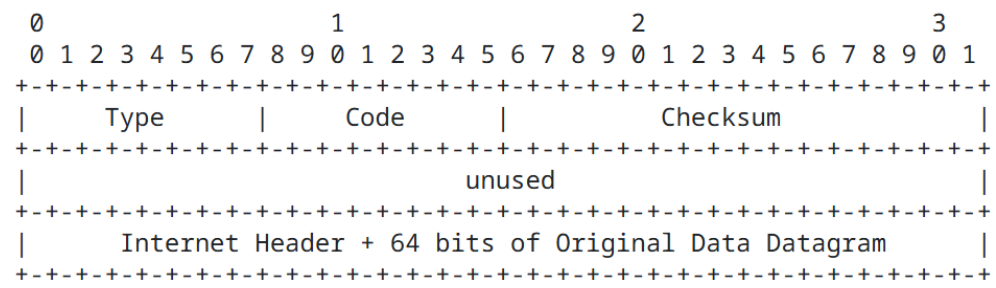
## 3. ICMP Admin Prohibited

- Use **nmap** or **hping3** to send a packet to any host that will result in an **ICMP admin prohibited** message being sent back to you. Use **tcpdump** to capture both packets (stimulus and response).
- Save both packets in a file called **3ICMPADMIN.pcap** using tcpdump filters and the –w and –c options

**When is this kind of ICMP message sent?**

An ICMP Admin prohibited message is sent when a firewall, router or security policy blocks a packet due to access restrictions

**What is the ICMP message format for this kind of ICMP message? What are the type and code values?**




ICMP admin prohibited: Type=3 code=13

**What did you do to get this message (include the command you used to create the stimulus packet)?**

We used the 3ICMPADMIN.pcap file provided by the professor. We opened it on wireshark and analyzed the packet and got the admin prohibted message

**What is the command you used to capture the ICMP message? Include the filter you used to isolate the two packets (stimulus and response).**

sudo tcpdump –w 3ICMPADMIN.PCAP -Xnv

screenshot of the tcpdump output (hex and ASCII dump) showing the two packets (stimulus and response).

```
┌──(mahimaavardini㉿mahimaa)-[~]
└─$ sudo tcpdump -r 3ICMPADMIN.pcap -Xnv
reading from file 3ICMPADMIN.pcap, link-type EN10MB (Ethernet), snapshot length 262144
09:55:15.720625 IP (tos 0x0, ttl 247, id 61110, offset 0, flags [none], proto ICMP (1), len
gth 96)
    205.211.94.158 > 192.168.1.209: ICMP host 141.117.126.20 unreachable - admin prohibited
 filter, length 76
        IP (tos 0x0, ttl 58, id 64020, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.209.34556 > 141.117.126.20.19: Flags [S], cksum 0xa5d1 (correct), seq 8288287
0, win 64240, options [mss 1460,sackOK,TS val 1289244460 ecr 0,nop,wscale 7], length 0
        0x0000:  4500 0060 eeb6 0000 f701 e5fa cdd3 5e9e  E..`.........^.
        0x0010:  c0a8 01d1 030d cb13 0011 0000 4500 003c  ............E..<
        0x0020:  fa14 4000 3a06 78a4 c0a8 01d1 8d75 7e14  ..@.:.x......u~.
        0x0030:  86fc 0013 04f0 b136 0000 0000 a002 faf0  .......6........
        0x0040:  a5d1 0000 0204 05b4 0402 080a 4cd8 4f2c  ............L.O,
        0x0050:  0000 0000 0103 0307 0000 0000 0000 0000  ................
09:55:18.289595 IP (tos 0x0, ttl 247, id 61117, offset 0, flags [none], proto ICMP (1), len
gth 96)
    205.211.94.158 > 192.168.1.209: ICMP host 141.117.126.20 unreachable - admin prohibited
 filter, length 76
        IP (tos 0x0, ttl 58, id 28350, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.209.37860 > 141.117.126.20.23: Flags [S], cksum 0x836d (correct), seq 1457351
375, win 64240, options [mss 1460,sackOK,TS val 1289247006 ecr 0,nop,wscale 7], length 0
        0x0000:  4500 0060 eebd 0000 f701 e5f3 cdd3 5e9e  E..`.........^.
        0x0010:  c0a8 01d1 030d cb13 0011 0000 4500 003c  ............E..<
        0x0020:  6ebe 4000 3a06 03fb c0a8 01d1 8d75 7e14  n.@.:........u~.
        0x0030:  93e4 0017 56dd 6acf 0000 0000 a002 faf0  ....V.j.........
        0x0040:  836d 0000 0204 05b4 0402 080a 4cd8 591e  .m..........L.Y.
        0x0050:  0000 0000 0103 0307 0000 0000 0000 0000  ................
```

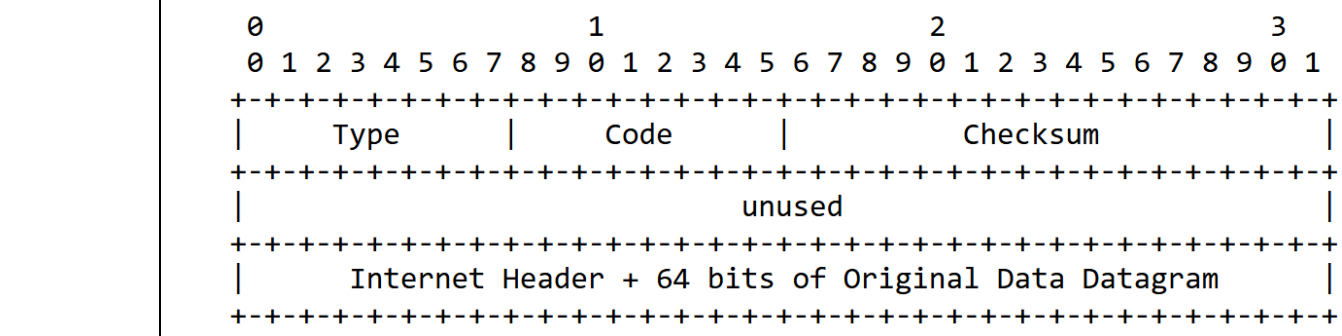
**4. ICMP Protocol Unreachable**

- Use **hping3** to send a packet to your partner's computer that will result in an **ICMP protocol unreachable** message being sent back to you. Use **tcpdump** to capture both packets (stimulus and response).
- Save both packets in a file called **4ICMPPROTO.pcap** using tcpdump filters and the –w and –c options

**When is this kind of ICMP message sent?**

ICMP Protocol Unreachable message is sent when a host does not support or recognize the protocol the packet was sent to.

**What is the ICMP message format for this kind of ICMP message? What are the type and code values?**




ICMP protocol unreachable : type = 3, code = 2

**What did you do to get this message (include the command you used to create the stimulus packet)?**

$ sudo hping3 -0 10.16.46.57 --ipproto 250 -c 1

**What is the command you used to capture the ICMP message? Include the filter you used to isolate the two packets (stimulus and response).**

sudo tcpdump -nv -X "host 10.16.46.57 or icmp" -r 4ICMPPROTO.pcap

screenshot of the tcpdump output (hex and ASCII dump) showing the two packets (stimulus and response).

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -nv -X "host 10.16.46.57 or icmp" -r 4ICMPPROTO.pcap

eading from file 4ICMPPROTO.pcap, link-type EN10MB (Ethernet), snapshot length 262144
3:14:57.802930 IP (tos 0x0, ttl 64, id 60415, offset 0, flags [none], proto unknown (250), le
20)
    192.168.146.132 > 10.16.46.57:  ip-proto-250 0
        0x0000:  4500 0014 ebff 0000 40fa 027b c0a8 9284  E.......@..{....
        0x0010:  0a10 2e39                                ...9
3:14:57.803959 IP (tos 0x0, ttl 128, id 337, offset 0, flags [none], proto ICMP (1), length 4
    192.168.146.2 > 192.168.146.132: ICMP 10.16.46.57 protocol 250 unreachable, length 28
        IP (tos 0x0, ttl 64, id 60415, offset 0, flags [none], proto unknown (250), length 20)
    192.168.146.132 > 10.16.46.57:  ip-proto-250 0
        0x0000:  4500 0030 0151 0000 8001 93a4 c0a8 9202  E..0.Q..........
        0x0010:  c0a8 9284 0302 fcfd 0000 0000 4500 0014  ............E...
        0x0020:  ebff 0000 40fa 027b c0a8 9284 0a10 2e39  ....@..{.......9
```