2020

SERVICIOS DE RED E INTERNET

BENJAMIN GORDO CORTES

Contenido

Configura una máquina con Ubuntu Server 18.04 con funciones de servidor DHCP. un máximo de 200 hosts y uno de ellos será el de administrador (“administrator”) . 2

Ataca al servidor DHCP para consumir todo su pool de direcciones disponibles para los clientes. Utilizndo yersinia 4

Realiza lo mismo que en los apartados anteriores pero esta vez con una máquina Windows Server. Documenta todos los pasos realizados. 6

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 10

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.

Una vez tengamos nuestro Ubuntu server activo nos dispondremos a descargar el servicio de isc-dhcp-server con el comando apt install isc-dhcp-server

```
root@haze:/home/benja# apt install isc-dhcp-server
```

Una vez lo tengamos instalado configuramos la interfaz de red por la que queremos que le llegue la información modificando el archivo que está en ruta /etc/default/isc-dhcp-server.

```
root@haze:/home/benja# nano /etc/default/isc-dhcp-server_
```

```
  GNU nano 4.8                          /etc/default/isc-dhcp-server
# 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="enp0s3"
INTERFACESv6=""
```

Después configuraremos el archivo dhcp que está en la ruta /etc/dhcp/dhcpd.conf

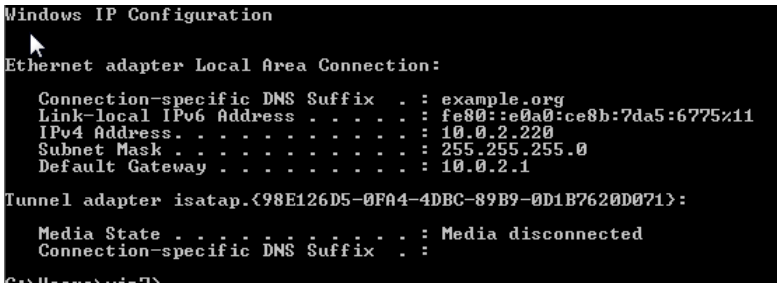
```
subnet 10.0.2.0 netmask 255.255.255.0 {
  range 10.0.2.20 10.0.2.220;
  default-lease-time 600;
  max-lease-time 7200;
```

También pondremos la Mac de la maquina administradora, para saber la Mac podremos una la cache arp. Una vez tengamos la Mac ponemos la configuración en el archivo dhcpd.conf

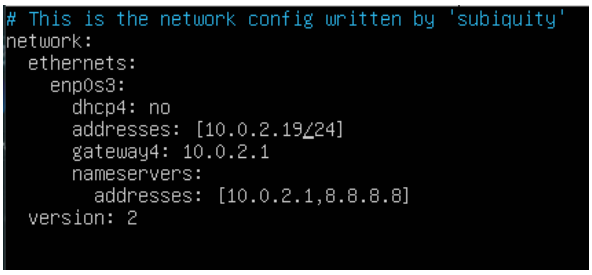
```
root@haze:/home/benja# arp -a
? (10.0.2.24) at 08:00:27:4a:2c:dc [ether] on enp0s3
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
```

```
host win7-admin {
   hardware ethernet 08:00:27:4a:2c:dc;
   fixed-address 10.0.2.220;
}
```

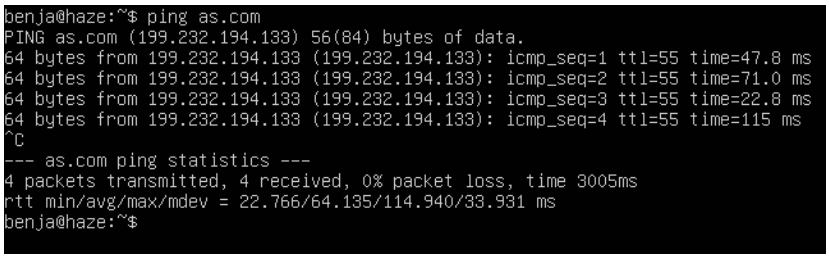
Si ahora metemos la maquina administradora podemos ver que nos pone la dirección que hemos puesto



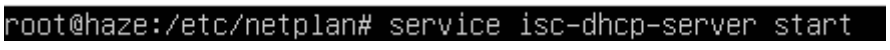
Después iremos a la configuración de red de nuestro servidor para poner una ip estática en la ruta /etc/netplan/00-installer-config.yaml

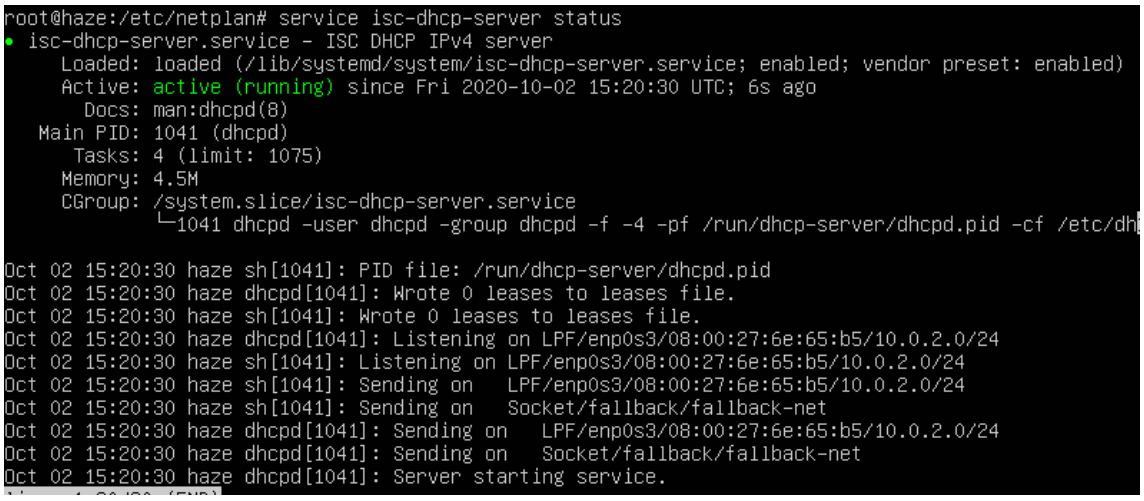


hacemos una comprobación de que el servidor tiene acceso a internet con el DNS.



Para poder iniciar el servicio usaremos el comando de service isc-dhcp-server start (para poder parar el servicio usamos stop y para reiniciar restart). También usaremos el comando service isc-dhcp-server status para comprobar que está activo el servicio.





Usaremos nmap para comprobar que el puerto 67/udp está abierto

```
root@haze:/home/benja# nmap -sU -p 67 10.0.2.19 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-06 08:08 UTC
Nmap scan report for 10.0.2.19
Host is up.

PORT   STATE         SERVICE
67/udp open|filtered dhcps
```

También meteremos otra maquina en la misma red y haremos una petición a dhcp con el comando dhclient -v y veremos quién nos la configuración de red. Como podemos ver la dirección 10.0.2.19 (Ubuntu server) nos da la configuración de red necesaria.

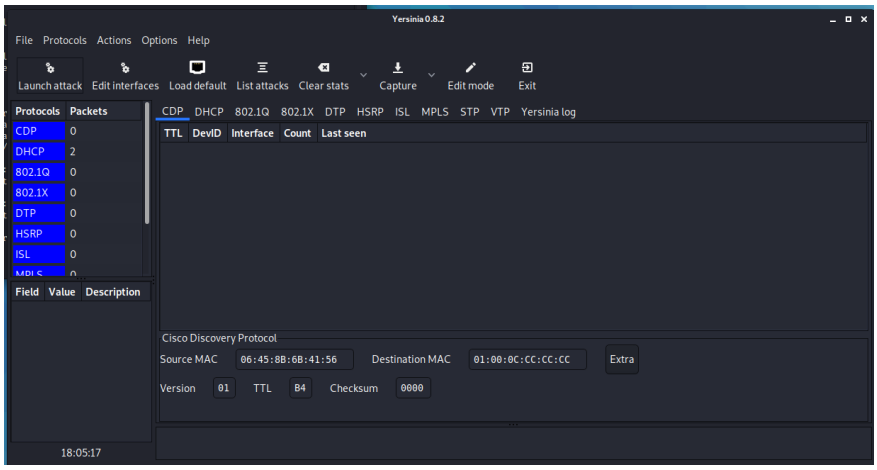
```
root@kali:/home/benja# dhclient -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:6c:6b:6d
Sending on   LPF/eth0/08:00:27:6c:6b:6d
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER of 10.0.2.23 from 10.0.2.19
DHCPREQUEST for 10.0.2.23 on eth0 to 255.255.255.255 port 67
DHCPACK of 10.0.2.23 from 10.0.2.19
bound to 10.0.2.23 -- renewal in 257 seconds.
```

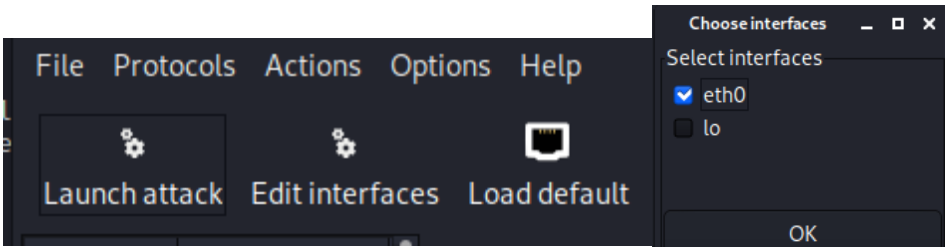
Ataca al servidor DHCP para consumir todo su pool de direcciones disponibles para los clientes. Para ello utiliza la herramienta Yersinia (https://tools.kali.org/vulnerability-analysis/yersinia) presente en Kali Linux. Documenta los comandos con los parámetros utilizando en el punto anterior explicando para qué valen, así como los resultados obtenidos.

Yersinia es una herramienta de seguridad utilizada que realiza ataques a la capa 2 (capa de enlace) utiliza diferentes protocolos como STP, DHCP, DTP… Sus ataques se basan en denegación de servicios, crear servidores falsos DHCP….

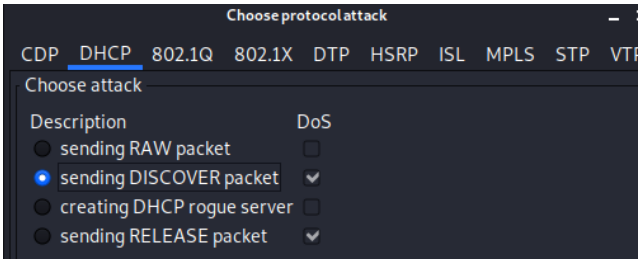
Abriremos un analizador de tráfico (wireshark) en 2º plano para ver qué es lo que sucede con el comando wireshark &. Una vez tengamos el analizador de tráfico preparado usaremos el comando yersinia -G para el entorno gráfico.



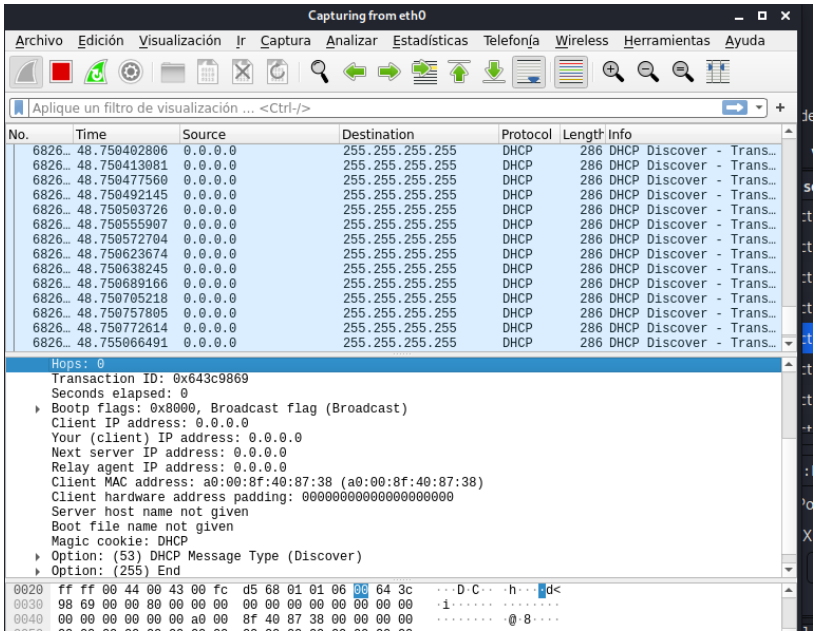
Una vez tengamos abierto yersinia configuraremos la interfaz que vamos a utilizar para realizar al ataque.



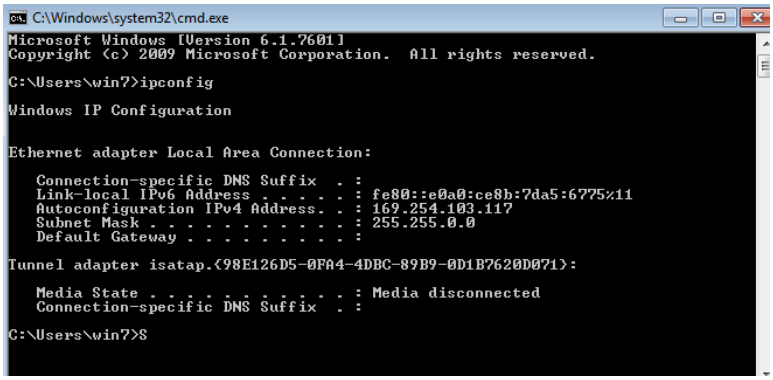
Ahora empezaremos el ataque dando a “Launch attack”, iremos a la pestaña de DHCP y escogeremos estas casillas para elegir el SENDING DISCOVER para poder agotar las direcciones.



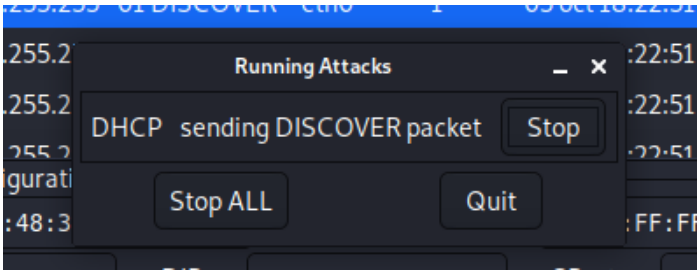
Si vamos a wireshark vemos las peticiones de la maquina al servidor.



Si añadimos una maquina veremos que le da ninguna configuración de red.

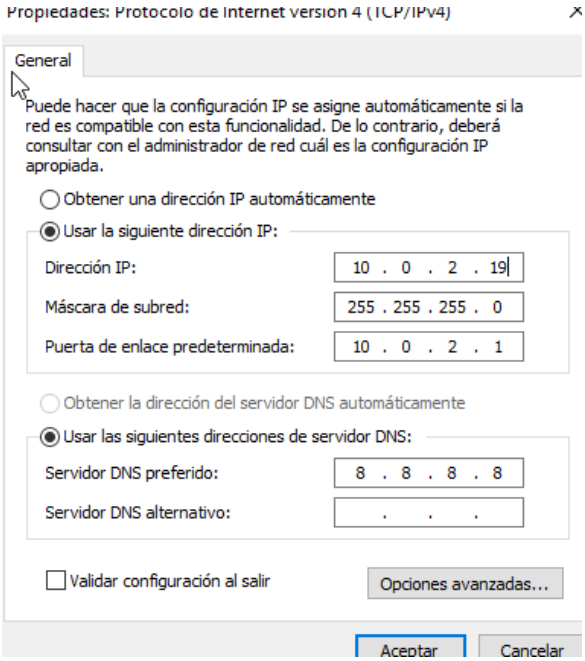


Para parar el ataque daremos a “list attacks” y daremos stop.

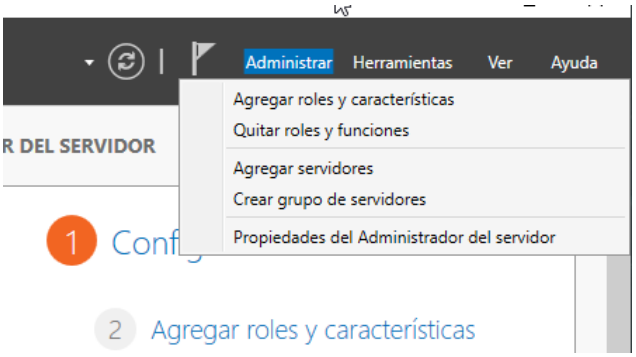


Realiza lo mismo que en los apartados anteriores pero esta vez con una máquina Windows Server. Documenta todos los pasos realizados.

Una vez tengamos instalados el Windows server 2016 lo primero que haremos será poner una ip estática.

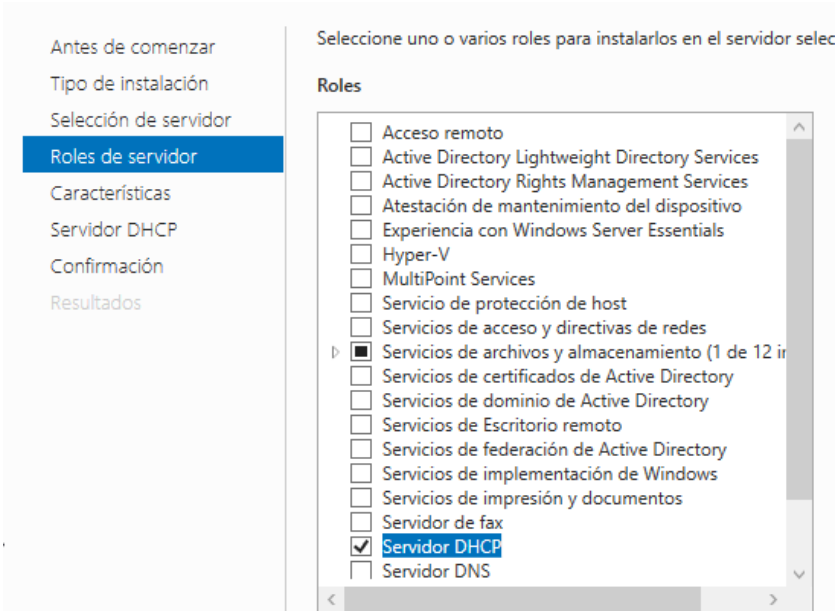


Después nos iremos a administración del servidor → administrar → agregar roles y características

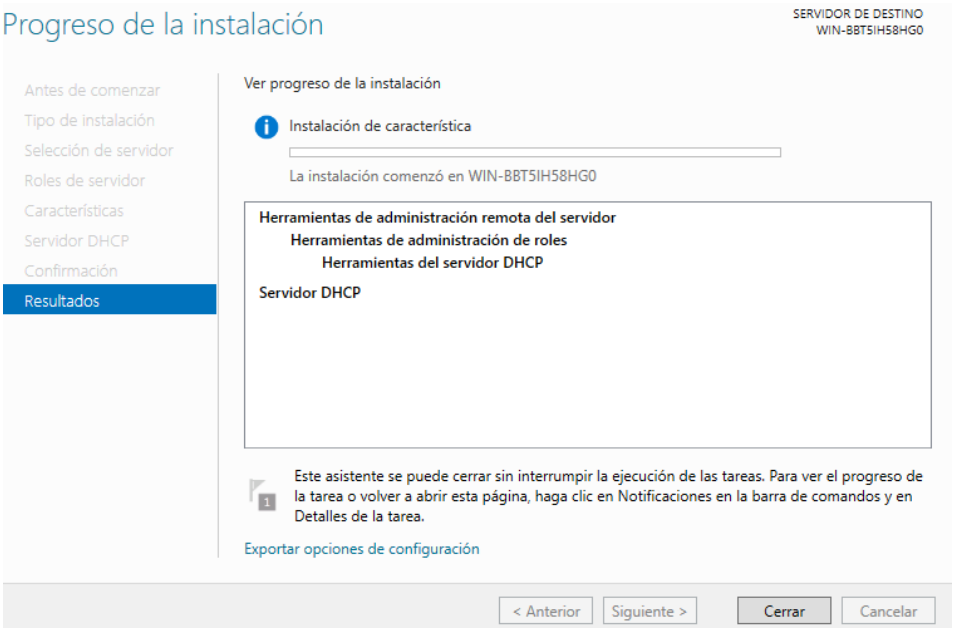


Seleccionaremos el servidor.

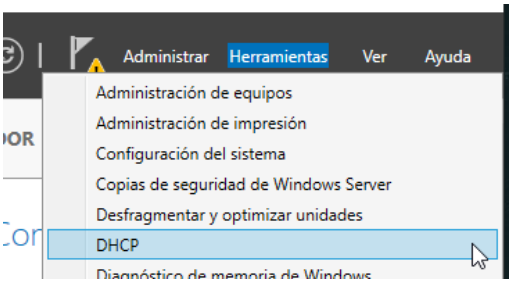
Escogemos el rol del servidor DHCP y agregamos las características.



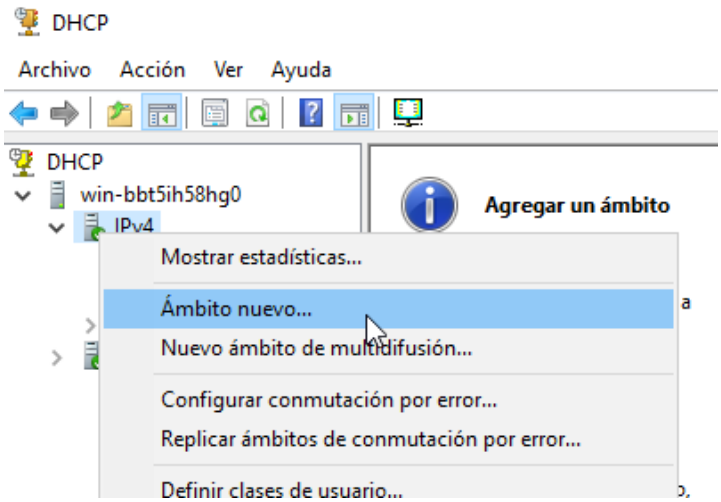
Una vez hayamos configurado todo daremos a instalar.

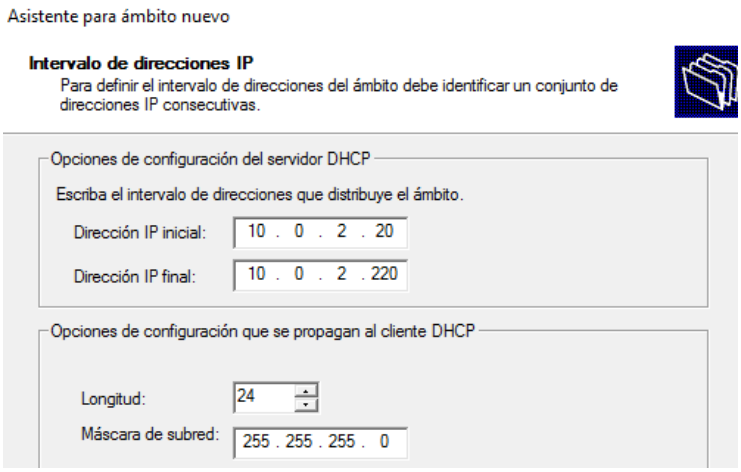


Ahora iremos al menú de herramientas y escogeremos dhcp y agregaremos un nuevo ámbito de direcciones asignables.

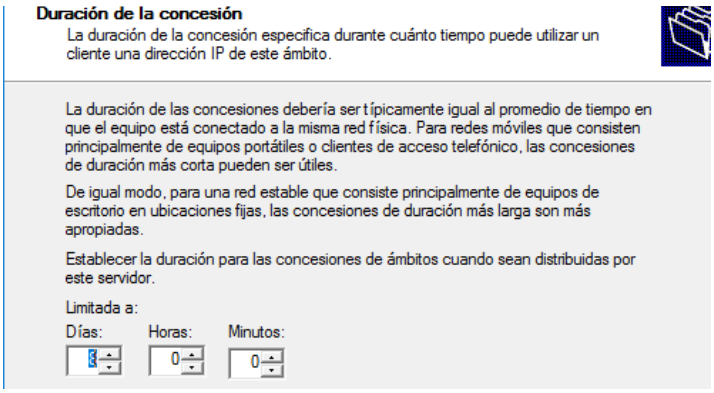


Daremos botón derecho sobre ipv4 y crearemos un nuevo ámbito.

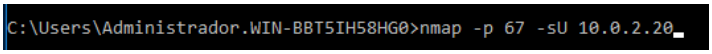




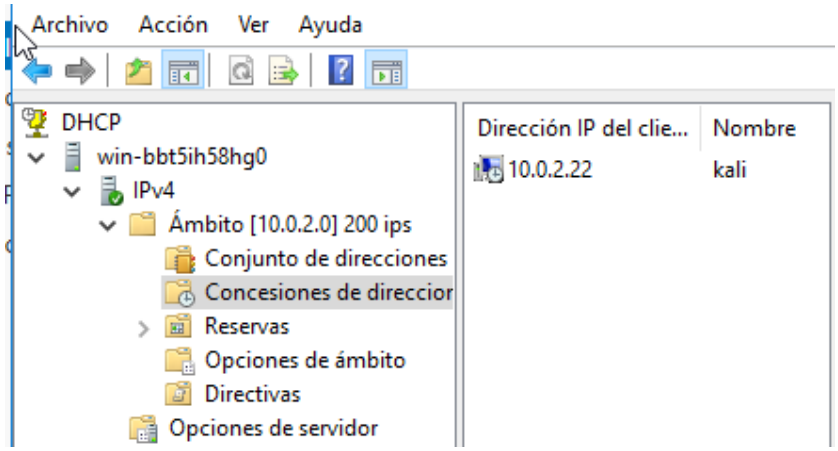
Al escoger el tiempo es importante saber el tiempo para que vamos a usarlo



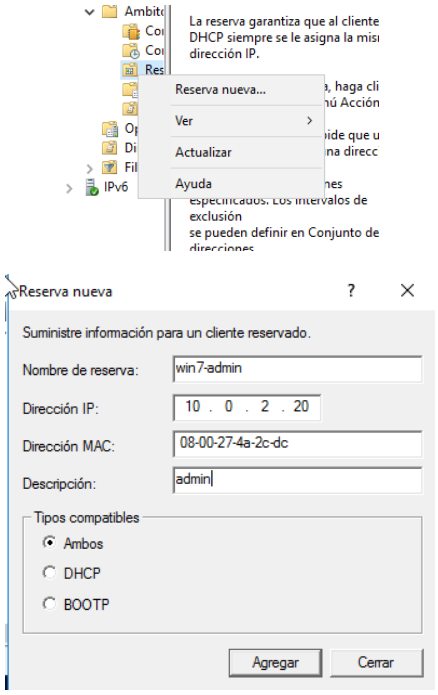
Para comprobar que funciona utilizaremos nmap para comprobar que el puerto está abierto



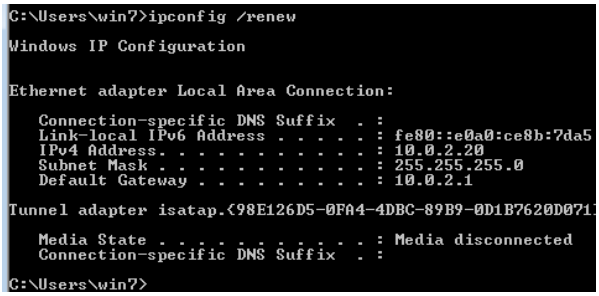
También agregare otra máquina para comprobar quien me da la interfaz de red. Vamos a la configuración de servidor dhcp y hay veremos la asignación de la ip.



Para poder hacer una reserva al servidor que así tenga una dirección para él, daremos botono derecho sobre reserva y damos a “nueva reserva”.

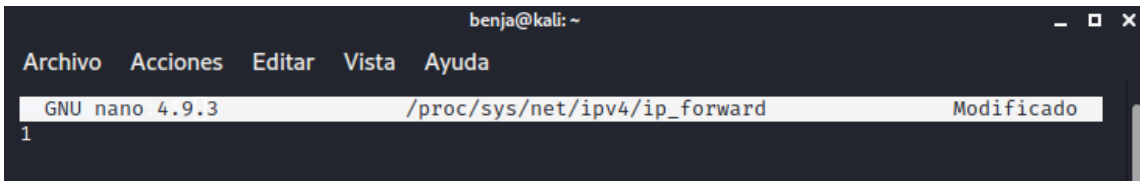


Ahora en la maquina administradora nos saldrá siempre esa ip

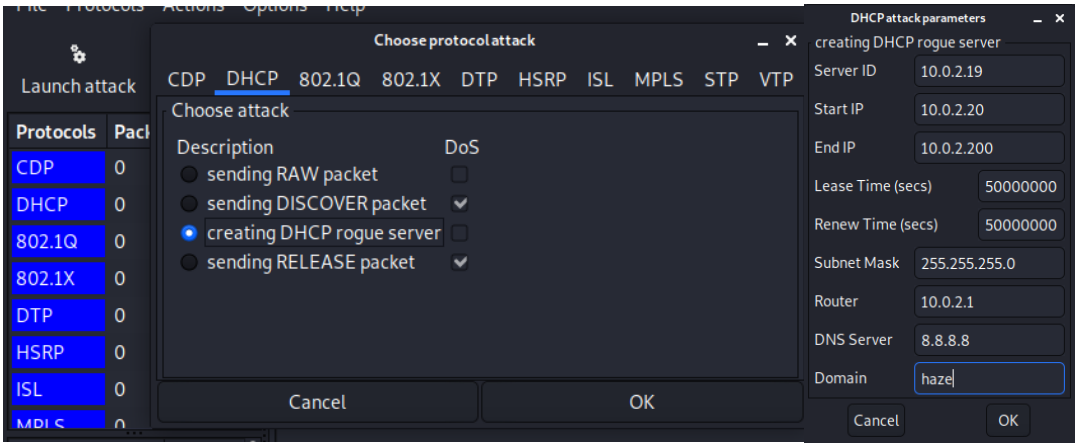


La empresa 4ck.es contrata nuestros servicios para comprobar la seguridad de la red interna de la organización. Una prueba fundamental en colocar un DHCP Rogue dentro de los segmentos de red donde se realizan las pruebas para realizar un ataque Man/Woman In The Middle. Configura un servidor DHCP malicioso 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

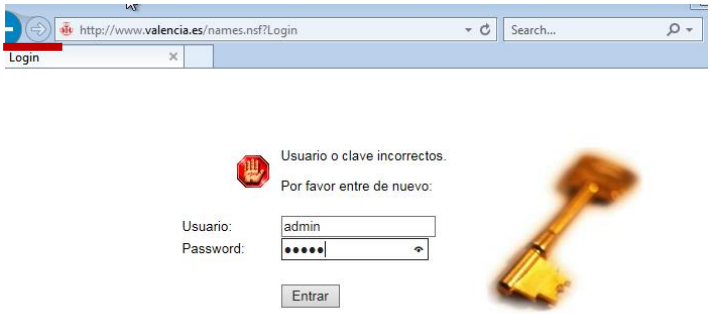
Para ello usaremos 3 máquinas virtuales un Windows 7 victima, Kali Linux maquina atacante (tarjeta de red en modo promiscuo) y un Ubuntu server que será el servidor DHCP. Primero pondremos a todas la maquinas en misma red y en la maquina Kali Linux activaremos el bit de enrutamiento que está en la ruta /proc/sys/net/ipv4/ip_forward y pondremos un 1. También abriremos un analizador de tráfico en mi caso wireshark.



Abriremos yersinia en el Kali Linux con el comando yersinia -G para el entorno gráfico. Dentro iremos a "Launch attack" → dhcp y escogeremos "creating DHCP rogue server".



Una vez le demos a ok comenzara el ataque. Si alguien que este en nuestra misma red accede a login sin cifrado (http), podremos sacar la contraseña y el usuario.



Una vez hayan dado a entrar, iremos a nuestro wireshark y usaremos el filtro del protocolo http. Si nos fijamos en los 4 paquetes en uno pone login, lo seleccionamos y miramos su contenido.