



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. Utilizando 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 (“administrador”) 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

```
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : example.org
    Link-local IPv6 Address . . . . . : fe80::e0a0:ce8b:7da5:6775%11
    IPv4 Address. . . . . : 10.0.2.220
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Tunnel adapter isatap.{98E126D5-0FA4-4DBC-89B9-0D1B7620D071}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

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

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.0.2.19/24]
      gateway4: 10.0.2.1
      nameservers:
        addresses: [10.0.2.1,8.8.8.8]
      version: 2
```

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

```
benja@haze:~$ ping as.com
PING as.com (199.232.194.133) 56(84) bytes of data:
64 bytes from 199.232.194.133 (199.232.194.133): icmp_seq=1 ttl=55 time=47.8 ms
64 bytes from 199.232.194.133 (199.232.194.133): icmp_seq=2 ttl=55 time=71.0 ms
64 bytes from 199.232.194.133 (199.232.194.133): icmp_seq=3 ttl=55 time=22.8 ms
64 bytes from 199.232.194.133 (199.232.194.133): icmp_seq=4 ttl=55 time=115 ms
^C
--- as.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 22.766/64.135/114.940/33.931 ms
benja@haze:~$
```

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.

```
root@haze:/etc/netplan# service isc-dhcp-server start
```

```
root@haze:/etc/netplan# 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 Fri 2020-10-02 15:20:30 UTC; 6s ago
     Docs: man:dhcpd(8)
   Main PID: 1041 (dhcpd)
      Tasks: 4 (limit: 1075)
     Memory: 4.5M
    CGroup: /system.slice/isc-dhcp-server.service
            └─1041 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dh

Oct 02 15:20:30 haze sh[1041]: PID file: /run/dhcp-server/dhcpd.pid
Oct 02 15:20:30 haze dhcpd[1041]: Wrote 0 leases to leases file.
Oct 02 15:20:30 haze sh[1041]: Wrote 0 leases to leases file.
Oct 02 15:20:30 haze dhcpd[1041]: Listening on LPF/enp0s3/08:00:27:6e:65:b5/10.0.2.0/24
Oct 02 15:20:30 haze sh[1041]: Listening on LPF/enp0s3/08:00:27:6e:65:b5/10.0.2.0/24
Oct 02 15:20:30 haze sh[1041]: Sending on LPF/enp0s3/08:00:27:6e:65:b5/10.0.2.0/24
Oct 02 15:20:30 haze sh[1041]: Sending on Socket/fallback/fallback-net
Oct 02 15:20:30 haze dhcpd[1041]: Sending on LPF/enp0s3/08:00:27:6e:65:b5/10.0.2.0/24
Oct 02 15:20:30 haze dhcpd[1041]: Sending on Socket/fallback/fallback-net
Oct 02 15:20:30 haze dhcpd[1041]: Server starting service.
```

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
```

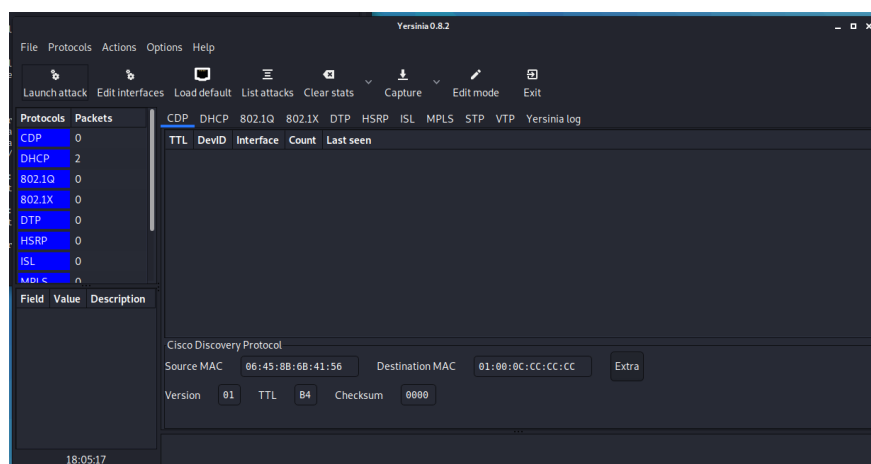
También meteremos otra maquina en la misma red y haremos una petición a dhcp con el comando dhclient -v y veremos quién nos la configuración de red. Como podemos ver la dirección 10.0.2.19 (Ubuntu server) nos da la configuración de red necesaria.

```
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/

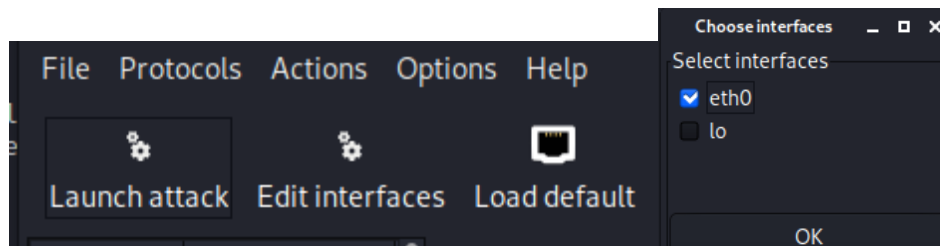
Listening on LPF/eth0/08:00:27:6c:6b:6d
Sending on   LPF/eth0/08:00:27:6c:6b:6d
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER of 10.0.2.23 from 10.0.2.19
DHCPREQUEST for 10.0.2.23 on eth0 to 255.255.255.255 port 67
DHCPACK of 10.0.2.23 from 10.0.2.19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

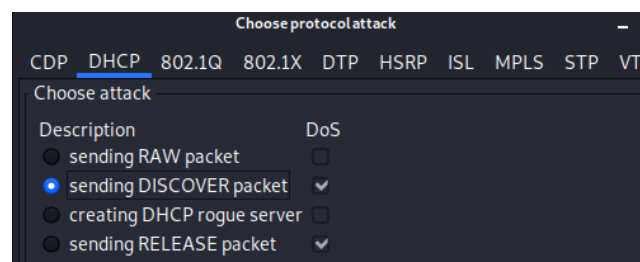
Abriremos un analizador de tráfico (wireshark) en 2º plano para ver qué es lo que sucede con el comando wireshark &. Una vez tengamos el analizador de tráfico preparado usaremos el comando yersinia -G para el entorno gráfico.



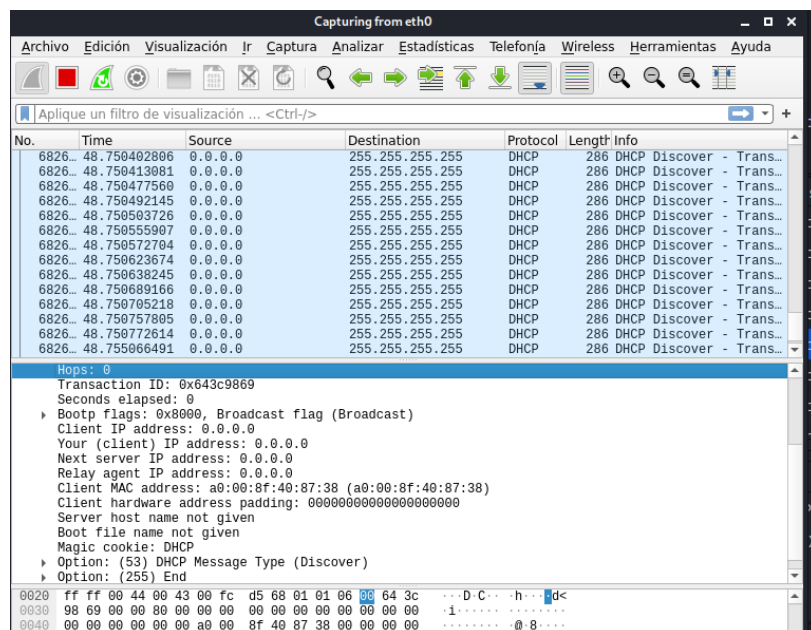
Una vez tengamos abierto yersinia configuraremos la interfaz que vamos a utilizar para realizar al ataque.



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.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\win7>ipconfig

Windows IP Configuration

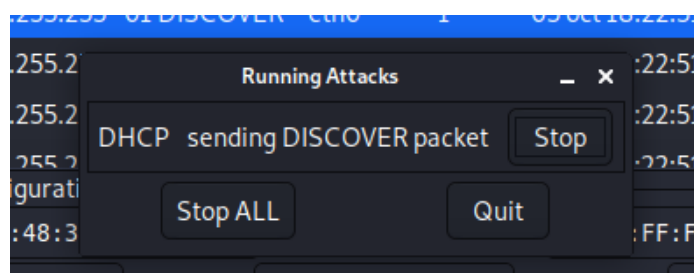
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e0a0:ce8b:7da5:6775%11
    Autoconfiguration IPv4 Address. . : 169.254.103.117
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{98E126D5-0FA4-4DBC-89B9-0D1B7620D071}:

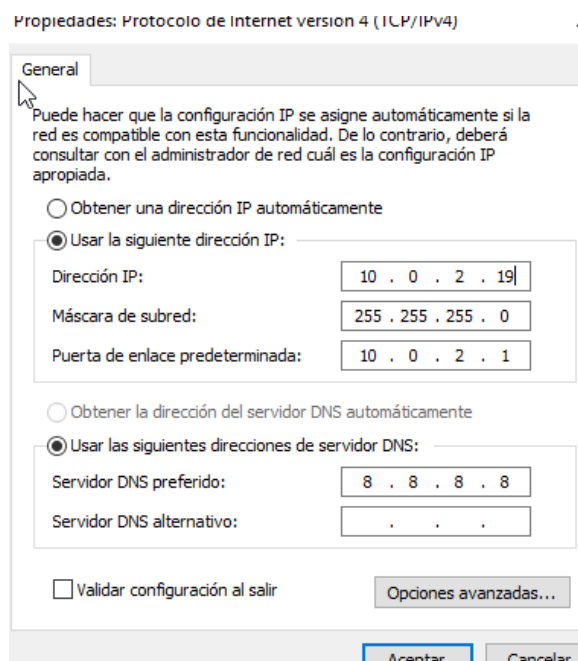
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
C:\Users\win7>S
```

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

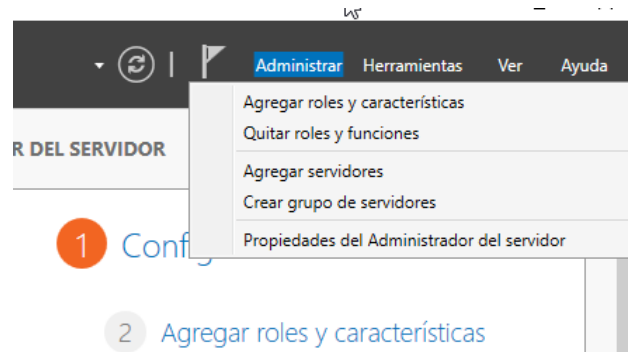


Realiza lo mismo que en los apartados anteriores pero esta vez con una máquina Windows Server. Documenta todos los pasos realizados.

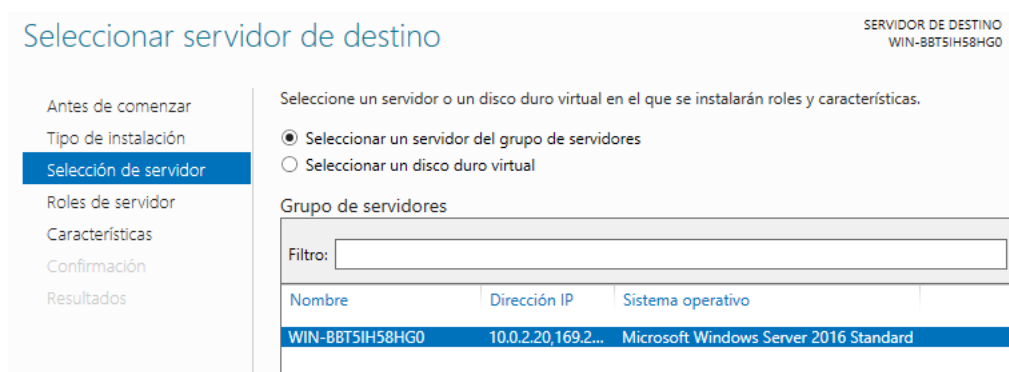
Una vez tengamos instalados el Windows server 2016 lo primero que haremos será poner una ip estática.



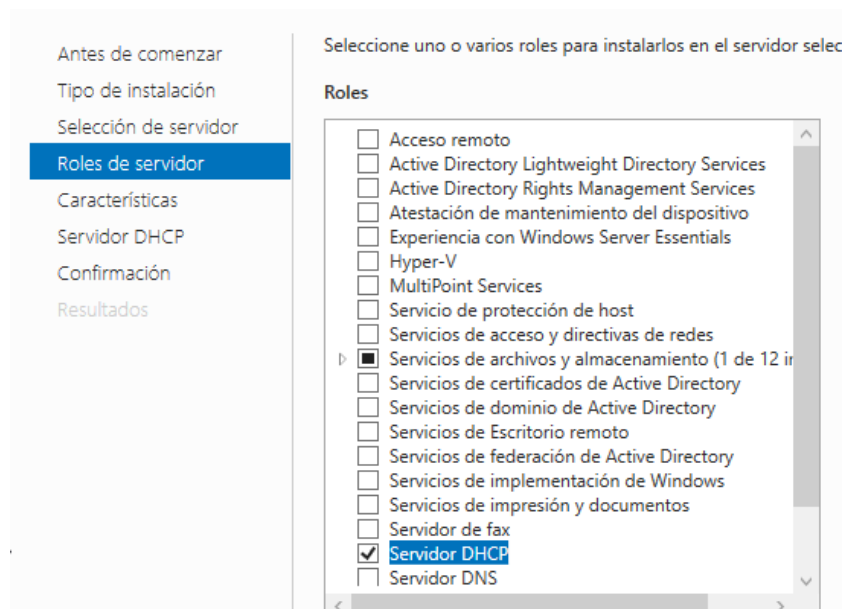
Después nos iremos a administración del servidor → administrar → agregar roles y características



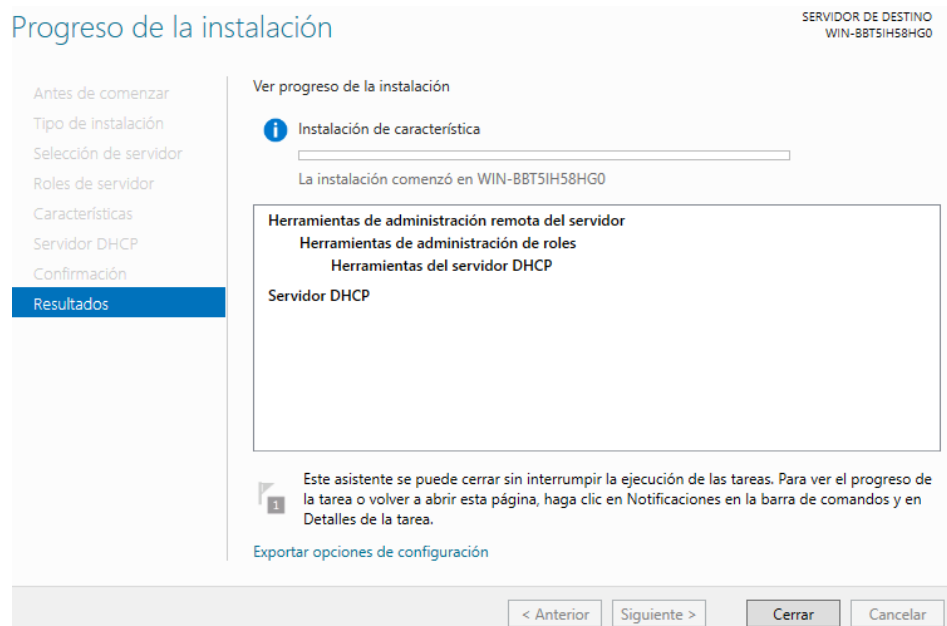
Seleccionaremos el servidor.



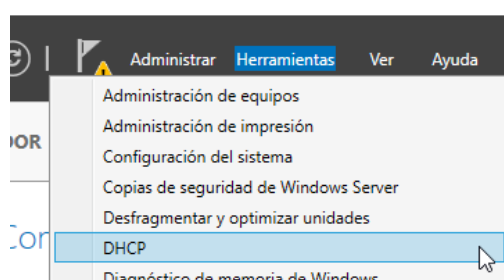
Escogemos el rol del servidor DHCP y agregamos las características.



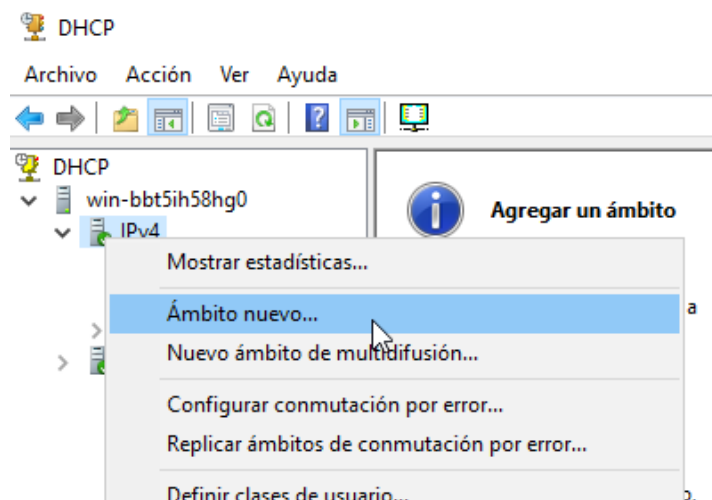
Una vez hayamos configurado todo daremos a instalar.



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.



Asistente para ámbito nuevo

Intervalo de direcciones IP

Para definir el intervalo de direcciones del ámbito debe identificar un conjunto de direcciones IP consecutivas.



Opciones de configuración del servidor DHCP

Escriba el intervalo de direcciones que distribuye el ámbito.

Dirección IP inicial: 10 . 0 . 2 . 20

Dirección IP final: 10 . 0 . 2 . 220

Opciones de configuración que se propagan al cliente DHCP

Longitud: 24

Máscara de subred: 255 . 255 . 255 . 0

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

Duración de la concesión

La duración de la concesión especifica durante cuánto tiempo puede utilizar un cliente una dirección IP de este ámbito.



La duración de las concesiones debería ser típicamente igual al promedio de tiempo en que el equipo está conectado a la misma red física. Para redes móviles que consisten principalmente de equipos portátiles o clientes de acceso telefónico, las concesiones de duración más corta pueden ser útiles.

De igual modo, para una red estable que consiste principalmente de equipos de escritorio en ubicaciones fijas, las concesiones de duración más larga son más apropiadas.

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

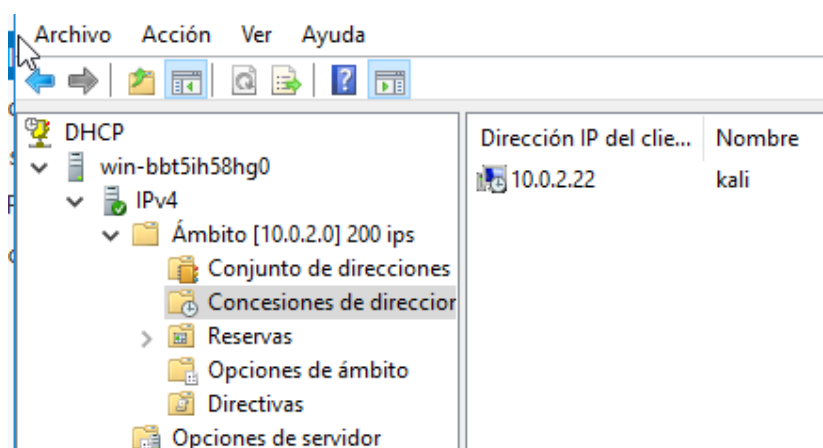
Limitada a:

Días: 8 Horas: 0 Minutos: 0

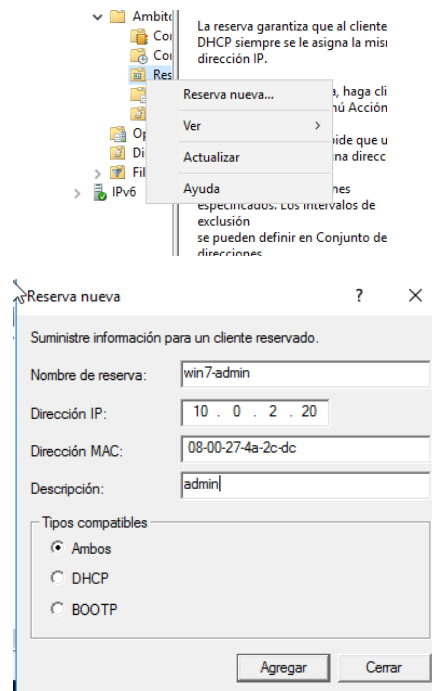
Para comprobar que funciona utilizaremos nmap para comprobar que el puerto está abierto

```
C:\Users\Administrador.WIN-BBT5IH58HG0>nmap -p 67 -sU 10.0.2.20
```

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 botón derecho sobre reserva y damos a “nueva reserva”.



Ahora en la maquina administradora nos saldrá siempre esa ip

```
C:\Users\win7>ipconfig /renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e0a0:ce8b:7da5
    IPv4 Address. . . . . : 10.0.2.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

Tunnel adapter isatap.{98E126D5-0FA4-4DBC-89B9-0D1B7620D071}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

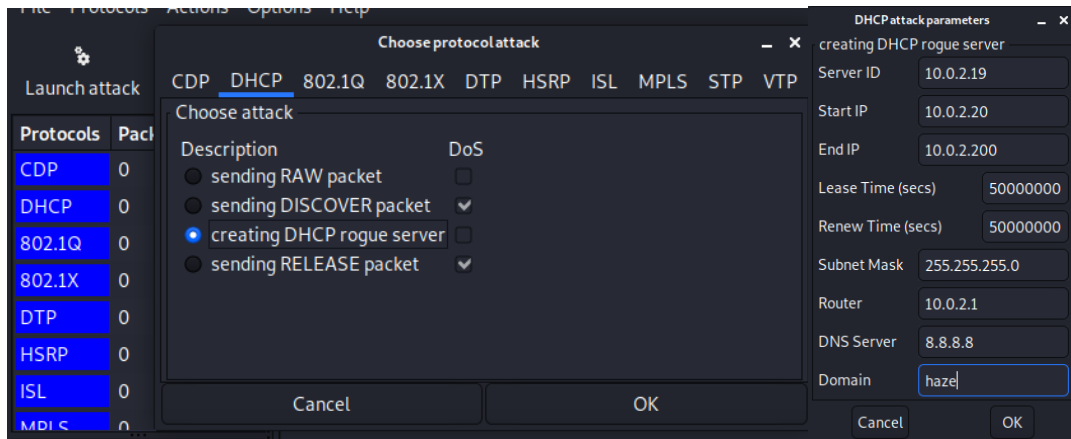
C:\Users\win7>
```

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>

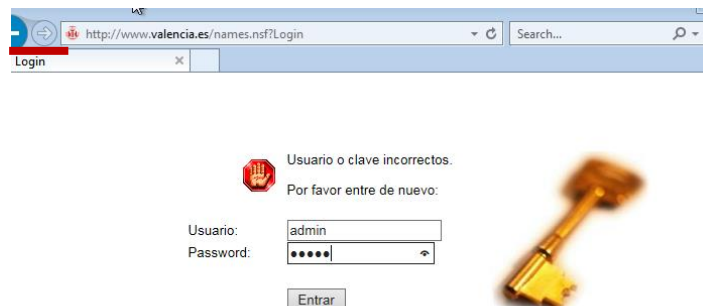
Para ello usaremos 3 máquinas virtuales un Windows 7 víctima, Kali Linux máquina atacante (tarjeta de red en modo promiscuo) y un Ubuntu server que será el servidor DHCP. Primero pondremos a todas las máquinas en misma red y en la máquina Kali Linux activaremos el bit de enrutamiento que está en la ruta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

```
benja@kali: ~
Archivo Acciones Editar Vista Ayuda
GNU nano 4.9.3 /proc/sys/net/ipv4/ip_forward Modificado
1
```

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.

