Rogue DHCP – Yersinia + Metasploit + dnschef

Introducción del Ataque

El ataque Rogue DHCP utiliza un servidor DHCP falso para distribuir configuraciones de red maliciosas a las víctimas dentro de una red local. En combinación con herramientas como dnschef y Yersinia, este ataque permite redirigir el tráfico DNS de las víctimas hacia páginas web controladas por el atacante o sitios de su elección, facilitando ataques de phishing, robo de credenciales o interceptación de tráfico.

Funcionamiento del Ataque

- **Preparación del Entorno**: Configura un servidor DHCP falso en la máquina atacante utilizando herramientas como ***Metasploit***. Este servidor distribuirá configuraciones maliciosas (como puertas de enlace predeterminadas o servidores DNS) a los dispositivos de la red.
- **Utiliza Yersinia: I**nterrumpir las comunicaciones normales entre clientes y el servidor DHCP legítimo. Esto se logra mediante el envío de paquetes de desautenticación (Deauthentication) a los clientes conectados al punto de acceso, forzándolos a reconectarse. Durante el proceso de reconexión, el servidor DHCP falso responderá antes que el servidor legítimo, ofreciendo configuraciones maliciosas.
- **Ejecución del Ataque:** Cuando una víctima solicita una configuración de red, el servidor DHCP falso responde y entrega los parámetros maliciosos. Entre estos parámetros, el servidor DHCP proporciona una dirección DNS controlada por el atacante.
- **Redirección de Tráfico:** En el servidor atacante, se configura dnschef para actuar como un servidor DNS personalizado. ***dnschef*** intercepta las consultas DNS de la víctima y redirige las solicitudes a páginas web específicas o réplicas de sitios legítimos alojadas por el atacante.
- **Manipulación del Usuario:** Al acceder a las páginas web, la víctima es redirigida al contenido diseñado por el atacante, permitiendo acciones como robo de credenciales o la ejecución de scripts maliciosos.

Herramientas usadas

- **Metasploit:** Un marco de trabajo para pruebas de penetración que incluye módulos para configurar un servidor DHCP malicioso.
- **Yersinia**: Una herramienta avanzada para manipular y explotar protocolos de red como DHCP, STP, CDP, entre otros. Facilita la ejecución de ataques al protocolo DHCP, incluyendo el envenenamiento de tablas de direcciones y la generación de respuestas masivas falsas para saturar la red.
- **dnschef:** Una herramienta utilizada para realizar redirecciones DNS, permitiendo al atacante controlar las solicitudes DNS de las víctimas.
- **Wireshark (Opcional):** Un analizador de tráfico de red que permite verificar que las respuestas del servidor DHCP falso y las redirecciones DNS están funcionando correctamente.

Pasos

Metasploit

Teniendo en cuenta que la ip de la máquina atacante es 192.168.1.114.

Vamos a configurar Metasploit para crear un servidor DHCP falso, y así engañar a los nuevos usuarios que se conecten a la red.

1. **Habilitar la interfaz de red virtual**: Utiliza la misma tarjeta de red física (eth0) pero con la IP específica 192.168.1.115. Esto permite que tu máquina atacante utilice esa dirección IP para servir como un servidor DHCP falso.

   sudo ifconfig eth0:1 192.168.1.115 netmask 255.255.255.0

2. **Habilitar el reenvío de paquetes IP:** Permite que la máquina pueda reenviar paquetes entre interfaces, actuando como un router.

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

3. **Configurar la puerta de enlace predeterminada:** Establece la dirección 192.168.137.1 como puerta de enlace predeterminada para la interfaz virtual eth0:1.

route add default gw 192.168.1.137 eth0:1

4. **Iniciar Metasploit y cargar el módulo DHCP:** Esto abre Metasploit y carga el módulo auxiliar para configurar un servidor DHCP falso.

msfconsole -q -x 'use auxiliary/server/dhcp'

Dentro de Metasploit, configura las siguientes opciones para usar la IP de tu máquina atacante (192.168.1.114):

1. Configurar la dirección IP de la máquina atacante como el **host principal del servidor DHCP.**
    a. Esto significa que el módulo de Metasploit escuchará en la IP 192.168.1.114 para atender las solicitudes DHCP de los dispositivos en la red.
    b. La máquina atacante es la que está ejecutando el servidor DHCP falso, por lo que debe estar configurada para recibir las solicitudes desde los dispositivos que buscan una dirección IP en la red.

set srvhost 192.168.1.114

2. Configurar la **máscara de subred** del servidor DHCP
    a. En este caso, la máscara 255.255.255.0 divide la red en un rango que incluye las IPs desde 192.168.1.1 hasta 192.168.1.254.
    b. Define cómo los dispositivos en la red deben comunicarse. Usar esta máscara asegura que todos los dispositivos con direcciones IP dentro del rango 192.168.1.x puedan comunicarse directamente entre sí.

set netmask 255.255.255.0

3. Configurar la **puerta de enlace predeterminada** que se asignará a los dispositivos que obtengan una dirección IP del servidor DHCP
    a. En este caso, la puerta de enlace es 192.168.1.1.
    b. La puerta de enlace es necesaria para que los dispositivos puedan comunicarse con redes externas. Si 192.168.1.1 es la dirección del router principal de tu red, esta configuración permite que las víctimas usen el router para el tráfico externo mientras el atacante intercepta el tráfico DNS.

set router 192.168.1.1

4. Configurar la máquina atacante (192.168.1.114) como el **servidor DNS** para los dispositivos que obtengan una dirección IP del servidor DHCP
    a. Esto es clave para interceptar y redirigir las solicitudes DNS de las víctimas. Por ejemplo, se puede usar una herramienta como *dnschef* en la máquina del atacante para responder con direcciones IP falsas y redirigir a las víctimas a páginas controladas.

set dnsserver 192.168.1.114

5. Definir la **primera dirección IP** del rango que será asignada por el servidor DHCP.
    a. En este caso, las direcciones IP comenzarán en 192.168.1.200. Esto evita conflictos con otras direcciones IP que ya puedan estar en uso en la red, como las del router (192.168.1.1) o de tu máquina atacante (192.168.1.114).

set DHCPIPSTART 192.168.1.200

6. Definir la **última dirección IP** del rango que será asignada por el servidor DHCP.
    a. Esto establece un rango de direcciones IP (192.168.1.200 a 192.168.1.250) que pueden ser asignadas dinámicamente a las víctimas. El rango debe ser suficientemente amplio para cubrir el número esperado de dispositivos que se conectarán al servidor.

set DHCPIPEND 192.168.1.250

7. Configurar un **nombre de dominio ficticio** que se asignará a los dispositivos que obtengan una dirección IP del servidor DHCP.
    a. Este dominio (atck.local) es una etiqueta arbitraria que puede usarse para identificar las máquinas que reciben configuraciones del servidor DHCP. También puede ser útil para que las víctimas vean algo menos sospechoso en sus configuraciones de red.

set DOMAINNAME atck.local

8. Comprobar que la configuración es correcta

show options

```
Name         Current Setting  Required  Description
----         ---------------  --------  -----------
BROADCAST                     no        The broadcast address to send to
DHCPIPEND    192.168.1.200    no        The last IP to give out
DHCPIPSTART  192.168.1.100    no        The first IP to give out
DNSSERVER    192.168.1.114    no        The DNS server IP address
DOMAINNAME   atck.local       no        The optional domain name to assign
FILENAME                      no        The optional filename of a tftp boot server
HOSTNAME                      no        The optional hostname to assign
HOSTSTART                     no        The optional host integer counter
NETMASK      255.255.255.0    yes       The netmask of the local subnet
ROUTER       192.168.1.1      no        The router IP address
SRVHOST      192.168.1.114    yes       The IP of the DHCP server
```

9. Por último, iniciar el servidor DHCP

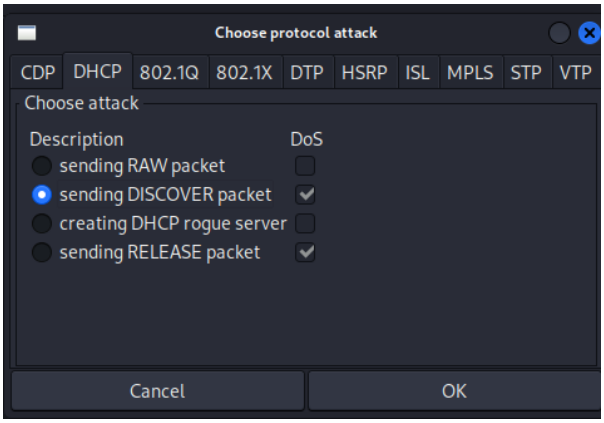
Run

Yersinia

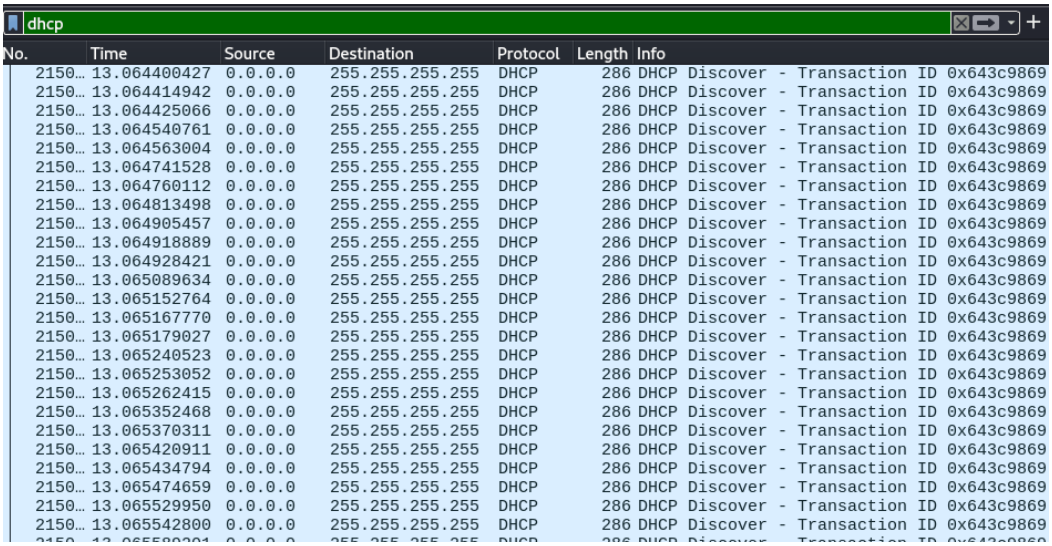
1. Iniciar Yersinia en modo interactivo como administrador

sudo yersinia -G

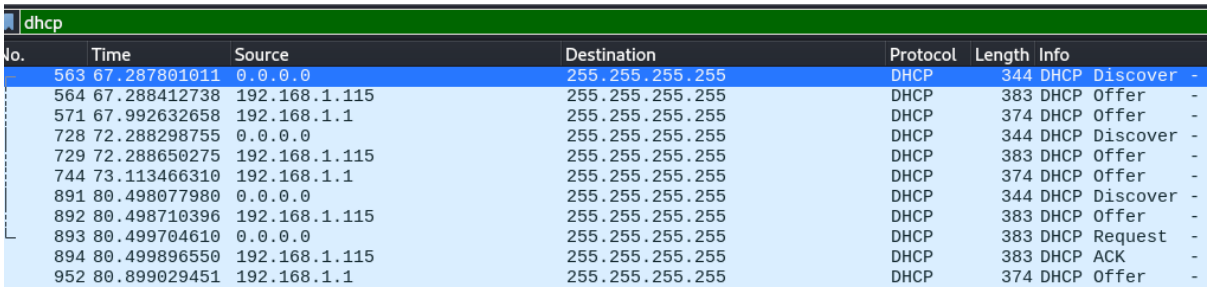
2. Seleccionar el protocolo DHCP
3. Lanzar el ataque DISCOVER DHCP



4. Para comprobar el funcionamiento nos fijamos en wireshark
    - Yersinia envía múltiples solicitudes DHCP Discover falsificadas usando direcciones MAC generadas aleatoriamente.
    - Esto inunda el servidor DHCP legítimo, obligándolo a responder con DHCP Offer para cada solicitud.
    - Como los clientes legítimos también dependen del servidor, este podría quedarse sin direcciones IP disponibles, impidiendo que otros dispositivos se conecten a la red.



Wireshark (opcional)



1. **Inicio de la búsqueda (DHCP Discover):**
    a. El cliente, con dirección inicial `0.0.0.0`, envía un paquete **DHCP Discover** a la dirección de broadcast (`255.255.255.255`). Este paquete es visible en la línea número 563.
    b. El cliente está indicando que busca un servidor DHCP que le proporcione una configuración de red.
2. **Respuestas de los servidores DHCP (DHCP Offer):**
    a. El primer **DHCP Offer** llega desde tu servidor DHCP falso con IP `192.168.1.115` (línea 564). Este paquete ofrece al cliente una dirección IP y configuración de red.
    b. Poco después, el servidor DHCP legítimo del router (IP `192.168.1.1`) responde también con su **DHCP Offer** (línea 571).
    c. Ambos servidores compiten ofreciendo direcciones IP al cliente, pero el cliente solo aceptará la primera respuesta completa que reciba.
3. **Aceptación de la oferta (DHCP Request):**
    a. En la línea 729, el cliente envía un paquete **DHCP Request** indicando que acepta la oferta del servidor `192.168.1.115`. Este paso confirma que el

cliente ha elegido la configuración de red proporcionada por tu servidor DHCP falso.

4. **Confirmación de la configuración (DHCP ACK):**
    a. En la línea 744, tu servidor DHCP falso responde con un paquete **DHCP ACK**, confirmando la asignación de la configuración al cliente.
    b. Este paquete incluye la dirección IP asignada y otros parámetros como la puerta de enlace, máscara de subred y servidor DNS.
5. **Reacción del servidor legítimo:**
    a. A pesar de que el servidor legítimo envía otro **DHCP Offer** en la línea 952, el cliente ya está configurado con los parámetros de tu servidor DHCP falso, por lo que ignora cualquier respuesta posterior.

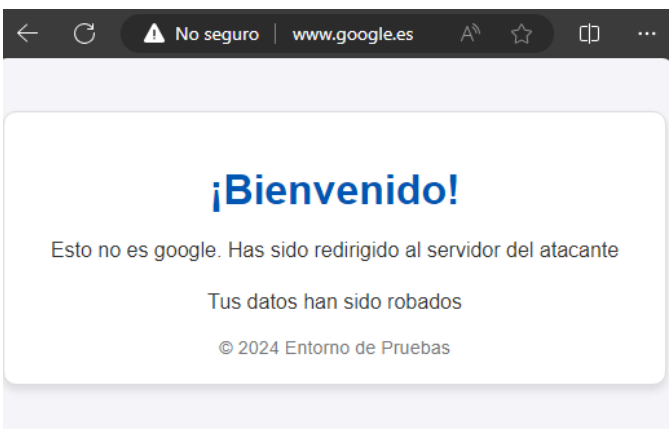
Dnschef

Con el comando **dnschef** es posible configurar un servidor DNS falso que interceptará las consultas DNS del cliente y redirigirá cualquier solicitud para dominios que coincidan con `google.es` a la dirección IP `192.168.1.114` (la dirección IP de la máquina atacante), que será un simple servidor apache.

```
sudo ./dnschef.py -i 192.168.1.114 --fakeip 192.168.1.114 --

fakedomains google.es
```

- **Interceptación de consultas DNS**: Cuando el cliente conectado al servidor DHCP realiza una consulta DNS para resolver google.es, en lugar de dirigirse a un servidor DNS legítimo, la consulta se envía a **dnschef**, que actúa como un servidor DNS falso.
- **Respuesta con IP falsa**: dnschef está configurado para responder a cualquier consulta relacionada con google.es con la dirección IP 192.168.1.114, independientemente de la IP real del dominio.
- **Servidor Apache**: En la máquina atacante, el servidor Apache puede estar configurado para servir una página web personalizada o incluso para capturar información del cliente.
- **Redirección a tu servidor**: Dado que 192.168.1.114 es la IP de la máquina atacante, cualquier intento del cliente de acceder a google.es será redirigido al servidor Apache en esa IP.



¿Por qué funciona el ataque?

Un ataque de DHCP Rogue (servidor DHCP falso) funciona explotando la naturaleza del protocolo DHCP, que asigna dinámicamente direcciones IP y otros parámetros de red a los dispositivos que se conectan. Al introducir un servidor DHCP malicioso en la red, el atacante puede proporcionar configuraciones de red controladas, redirigiendo el tráfico de las víctimas a través de su máquina para realizar ataques de intermediario (Man-in-the-Middle).

En este escenario, el servidor DHCP falso está configurado para responder más rápidamente que el servidor legítimo, aumentando la probabilidad de que el cliente acepte su oferta. Una vez que el cliente utiliza la configuración proporcionada por el atacante, su tráfico puede ser redirigido o interceptado.

1. **Solicitud de configuración por parte del cliente:**
    a. Cuando un dispositivo se conecta a la red, envía un mensaje **DHCP Discover** en busca de servidores DHCP disponibles.
2. **Respuesta de servidores DHCP:**
    a. Tanto el servidor DHCP legítimo como el servidor DHCP falso (controlado por el atacante) pueden responder con un mensaje **DHCP Offer**, ofreciendo parámetros de red al cliente.
3. **Selección de la oferta por el cliente:**
    a. El cliente acepta la primera oferta que recibe enviando un mensaje **DHCP Request** al servidor correspondiente.
4. **Confirmación del servidor:**
    a. El servidor seleccionado responde con un **DHCP ACK**, confirmando la asignación de la configuración de red.