DHCP: Seguridad

DHCP Rogue Attack

- Este ataque consiste en **suplantar al servidor DHCP** de la red otorgando a los clientes **configuraciones maliciosas o inválidas**.
- El atacante responderá a los **DHCP DISCOVER** del cliente con una oferta y en los parámetros de configuración su propia **IP** como **puerta de enlace** (gateway) y como **servidor DNS** del cliente (víctima).
- La víctima, si recibe respuesta del atacante antes que del servidor legítimo, se configurará con los parámetros maliciosos.

Solicitud de configuración DHCP del cliente

- Cuando un cliente se conecta a una red y solicita una configuración DHCP con el comando **DHCP DISCOVER**, desconoce si habrá o no un servidor que le responderá.
    - En caso de que nadie le responda, se autoconfigurará una dirección **APIPA**. (168.254.0.0/16).
        - Las direcciones **APIPA** otorgan conectividad local.
        - Y cada 5 minutos volverá a enviar un **DHCP DISCOVER** en búsca de un nuevo servidor.
- El comando **DHCP DISCOVER** que envía el cliente tiene como destino una dirección de **broadcast** (255.255.255.255), por lo que es **recibido por todos los equipos de la red**.

Condición de carrera

- En el momento en el que el cliente envía el comando **DHCP Discover** se produce una **condición de carrera**.
- El atacante intentará responder al cliente con un **DHCP OFFER** malicioso **antes de que el servidor legítimo le haga una oferta**.
- El cliente aceptará la primera configuración que reciba.
    - El comando **DHCP REQUEST** enviado por un cliente y difundido por broadcast sirve tanto para aceptar una configuración, como para notificar al resto de servidores que han ofrecido una configuración que la suya ha sido rechazada.

La configuración maliciosa

- El atacante intentará establecerse como:
    - **Servidor DNS**: Controlando las **resoluciones de nombres a IP** solicitadas por el cliente y pudiendo redirigirlo a servidores falsos.
    - **Puerta de enlace** (gateway): Haciendo que todas las comunicaciones del cliente pasen a través de su equipo. **Man in the middle**.
- Otra opción sería otorgar configuraciones inválidas, que impidan que el cliente pueda conectarse a la red. **DDOS**.
    - Esto puede ocurrir de forma accidental, cuando por ejemplo alquien conecta a la red el router de su casa con el servicio DHCP activo y éste empieza a conceder configuraciones inválidas.

Prevención y detección del DHCP Rogue Attack

- Si encontramos un equipo que tiene problemas de conectividad y vemos que su **IP** está **fuera del rango de concesiones**, debemos sospechar que quizá haya un **servidor DHCP no autorizado en la red**.
- Una forma más activa de buscar servidores DHCP no autorizados consiste en utilizar un rastreador de paquetes. Se puede configurar una herramienta de **análisis de tráfico** para que nos avise si hay paquetes que provienen del puerto **UDP 67** de **equipos que no sean el servidor DHCP legítimo**.
- Se pueden inspeccionar **logs** los logs de la red en busca de ciertos eventos sospechosos.
- En el caso de **detectar un servidor DHCP malicioso** es crítico **actuar de forma rápida** y **eliminar los servidores DHCP no autorizados** o, al menos, **desactivar los puertos del switch** a los que esté conectado.

- Es posible que pase mucho tiempo antes de que se descubra un servidor **DHCP no autorizado**.
    - Un servidor malicioso puede pasar días o meses atendiendo a solicitudes y recopilando todo tipo de información.
- Los servidores **DHCP no autorizados** que se conecten por accidente suelen ser fácilmente detectables, puesto que suelen causar **problemas de conectividad** de los equipos.
- Hay que estar atento por si se producen **conflictos de direcciones IP**.
- Es vital **mantener la red** documentada. Saber dónde están los servidores y qué detalles de configuración tienen.
- Un **controlador de dominio** como **Active Directory** mantiene una base de datos segura de **servicios DHCP autorizados**. Si el servidor no está autorizado, no se agregará a la red.

DHCP Snooping

- La mejor forma de prevenir servidores DHCP maliciosos es activar **DHCP snooping** e **interfaces confiables** en los switches.
- Los switches modernos suelen traer **DHCP Snooping** integrado.
    - Buscan activamente paquetes de respuesta DHCP en una VLAN o en una interfaz específica.
    - Notificarán o bloquearán las respuestas DHCP de las **interfaces no confiables**.
- Esta es la **forma más eficaz** de evitar que se agreguen servidores DHCP no legítimos a un segmento de red.

Seguridad y prevención

- La seguridad requiere una **prevención activa y contínua**.
    - Se pueden llevar a cabo rutinas automatizadas o manuales para mantener la administración de la mejor forma posible.
    - Es **crítico** documentar la red y tener todos los equipos inventariados.
    - Se puede realizar un seguimiento de las solicitudes DHCP y de las ofertas, para descubrir servidores no autorizados.
- Este ataque funciona también en **redes wifi**, por lo que hay que tener cuidado al conectarse a las redes públicas.

DHCP Starvation Attack (Inanición DHCP)

- Los servidores **DHCP** cuentan con **rangos de direcciones IP limitados** para otorgar configuraciones a los clientes.
    - Un atacante puede falsear su dirección MAC (**MAC Spoofing**) y realizar **peticiones masivas de configuración**, dejando al servidor DHCP sin IPs disponibles que otorgar.
- Antes de otorgar una configuración, los servidores pueden intentar ver si la IP a conceder se encuentra actualmente en uso, utilizando el **protocolo ARP**.
    - Un atacante puede responder a las peticiones ARP del servidor diciendo que **la IP está en uso** por, por cada IP por la que pregunte el servidor.
    - De esta manera el servidor no podría realizar ninguna oferta de IPs.
- Es un ataque **DDOS**. Y se puede realizar en combinación con **DHCP Rogue** para hacerlo más efectivo.

Prevención y detección del DHCP Starvation Attack

- Muchas veces los administradores son sorprendidos por los ataques **DDOS**.
- Este tipo de ataques son fácilmente detectables utilizando **analizadores de tráfico** como el **Wireshark**.
    - En la primera variante del ataque tendríamos que buscar una inundación de segmentos TCP con el comando **DHCP DISCOVER** y con la **MAC** falsicada.
    - En la segunda variante podríamos hacer análisis del tráfico **ARP**.
- Una forma de controlar estos ataques es utilizando **seguridad de puertos en capa 2 en el switch**.
    - Limitando de este modo el número máximo de direcciones MAC permitidas por puerto.

Conclusiones generales

- Este tipo de ataques se pueden realizar de una forma muy sencilla utilizando herramientas como **yersinia**.
- Siempre es más fácil atacar una red que protegerla:

> *El atacante solo tiene que acertar una vez, el administrador siempre.*

- Disponer de las mejores defensas para prevenir los ataques es la mejor manera.

Fuentes

- DHCP Starvation attack withoud making any dhcp requests
- Rogue DHCP Server
- MicroNuggets: DHCP Starvation Attacks Explained
- DHCP Attacks and Defense Strategies
- Understanding and preventing dhcp starvation attacks