Ataque DHCP

Transcribed on August 2, 2025 at 10:50 AM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de los ataques IPV y en concreto un ataque llamado DHCP Starvation o agotamiento DHCP.

El ataque de agotamiento DHCP es una técnica utilizada por un atacante para consumir todas las direcciones IP disponibles que un servidor DHCP puede asignar.

Y funciona de esta forma.

Primero lo que hace es generar muchísimas peticiones, muchísimas solicitudes.

El atacante genera y envía una gran cantidad de peticiones DHCP falsas al servidor DHCP y para ello utiliza diferentes direcciones Mac que también son falsas.

Esto lleva a un agotamiento desde las direcciones IP, porque cada petición falsa lleva al servidor DHCP a asignar una dirección IP del pool de direcciones de disponibles a la dirección Mac que está falsificada.

Y como el atacante no tiene intención de usar realmente esas direcciones IP y debido a gran cantidad de peticiones, el pool de direcciones IP disponibles en el servidor DHCP se agota rápidamente.

Y esto provoca una denegación de servicio a clientes legítimos, porque una vez que todas las direcciones IP disponibles han sido asignadas a las direcciones Mac falsas, los dispositivos legítimos que intenten conectarse a la red y obtener una dirección IP a través del DHCP no van a poder hacerlo.

Y esto se debe a que el servidor DHCP ya no tiene direcciones IP disponibles para asignar, lo que efectivamente niega el acceso a la red a los usuarios legítimos.

Y además este ataque no requiere acceso físico a la red y puedes ejecutarlo de forma remota, lo que lo hace particularmente peligroso y difícil de detectada a tiempo.

En otras palabras, el objetivo del ataque es causar una interrupción en el servicio de red, impidiendo que los dispositivos legítimos se conecten a dicha red y accedan a los recursos esenciales, una delegación de servicio.

Bien, pues para protegernos de DHCP tenemos muchas técnicas, tenemos varias actuaciones que podemos hacer.

La primera es implementar el DHCP Snoopy.

El DHCP Snooping es una característica de seguridad que llevan los switches que filtran los mensajes DHCP no confiables y además previene que los servidores DHCP no autorizados asignen direcciones IP a los clientes y también se puede asignar para construir una pequeña base de datos de seguimiento de dispositivos y esto permite a los administradores de red saber qué dispositivos están conectados y a qué puerto del switch.

Otra técnica de mitigación puede ser limitar la tasa de peticiones DHCP, es decir, configurar los dispositivos de update para limitar la tasa a la que se aceptan las peticiones DHCP de cada cliente, reduciendo la efectividad de los ataques de agotamiento.

Además, esta configuración ayuda a prevenir también ataques de denegación de servicio y se puede configurar para proporcionar umbrales diferenciados basados en el rol o la ubicación del dispositivo en la red.

Otra técnica muy efectiva es vincular direcciones Mac con direcciones IP, es decir, utilizar reservas estáticas para dispositivos conocidos para asegurar que sólo los dispositivos autorizados puedan recibir una dirección IP del servidor DHCP.

La vinculación de Mac IP también facilita la administración de red al asegurar que los dispositivos de red críticos obtengan siempre la misma dirección IP.

Esto ya lo dijimos anteriormente, para los dispositivos críticos tenemos siempre que asignar una dirección IP manualmente.

Y finalmente, también podemos utilizar NAC, que es el control de acceso a la red.

Por lo tanto, implementar NAC para autenticar dispositivos antes de que se les permita el acceso a la red puede prevenir que dispositivos no autorizados hagan peticiones DHCP.

Y además, NAC no solo previene peticiones DHCP no autorizadas, sino que también puede imponer políticas de seguridad como antivirus y configuraciones de firewall antes de permitir el acceso a la red.

Bien, pues vamos a ver ahora cómo se implementa un ataque de agotamiento DHCP.

Aquí tengo, bueno, ya lo conocéis, son dos máquinas virtuales y una de ellas va a actuar como servidor DHCP y la otra será el atacante.

Bien, pues esta máquina va a actuar como el servidor DHCP.

¿Vamos a ver la IP que tiene aquí la veis?

Que va a ser la 5.

Bien, pues ahora lo que tenemos que proceder es a la instalación del servidor DHCP y para eso, pues bueno, como siempre sabéis, hacemos un apt update, como siempre, por si acaso.

Y después que vamos a instalar es el servidor de DHCP, que es también sencillo, apt install y le vamos a llamar isc thcp server Lo instalamos después.

Pues ya lo tenemos.

Instalamos.

Pues ya lo tenemos y ahora lo vamos a configurar.

Para eso hay que editar el siguiente fichero, está en etc dhtp dhcpd dhcpdh Este fichero es el que tenemos que editar con todos los parámetros para configurar el servidor DHCP.

Bien pues esta es la configuración que viene por defecto y tendremos que añadir la parte que corresponde con nuestra subnet, con nuestra arquitectura.

Bien pues nos podemos ir al final del fichero y aquí es donde voy a añadir todo lo relacionado con el DHCP o lo voy a poner directamente y ahora os explico qué hace más o menos cada línea, tampoco vamos a explicar aquí cómo funciona, pero sí que tengáis una idea.

Bueno pero para que también os sirva un poco de cómo funciona un DHCP os contaré lo que hace cada una de las líneas.

La primera, la segunda es 10.

211.

55.0 esta línea indica la declaración de una subred, que es la 10.211.350 y como ya vimos en subnetting aquí está permitiendo hasta 254 direcciones IP.

La siguiente línea y quizás la más importante porque es donde vamos a definir el rango de ips que podemos asignar aquí serán las IPs que podemos entregar a los dispositivos clientes, en este caso hemos puesto desde las 100 a las 105 para tener un poco de control, pero aquí podéis poner lo que queráis.

La siguiente de option domain name server especifica los DNS que los dispositivos clientes van a utilizar para la resolución de nombres de dominio, en este caso he puesto la típica de Google.

La siguiente, la de Optium routers, indica la dirección IP del router predeterminado, o sea el gateway y además este será el que todos los dispositivos clientes van a utilizar para acceder a cualquier red externa.

La siguiente, la de option broadcast define la dirección del broadcast para la subred, o sea aquí será donde se van a enviar los mensajes a todos los los dispositivos dentro de esta subnet.

El default list time establece el tiempo por defecto en segundos que una dirección IP se asigna a un dispositivo cliente si el cliente no solicita un tiempo específico, en este caso 600 segundos, unos 10 minutos es el tiempo por defecto y el max list time define el tiempo máximo en segundos que una dirección IP puede ser alquilada a un dispositivo cliente, en este caso son 7200 segundos que son dos horas, que es el máximo tiempo de conexión permitido.

Bien pues ya con esto sólo tenemos que almacenar la configuración, la guardamos y vamos a iniciar nuestro servidor DHCP y eso lo hacemos con sudo service isc dhcp server start Con esto ya lo tenemos en funcionamiento, pero para confirmar que funciona haremos un sudo service iscdhcp server como antes y ahora ponemos status y aquí nos está funcionando, está activo y un poco de log de lo que está pasando en este momento con este servicio.

Pues bien, hasta aquí ya tenemos montado nuestro pequeño servidor DHCP, ahora vámonos a la máquina que va a actuar como atacante.

En principio no nos va a hacer falta instalar ningún software adicional, pero sí que vamos a utilizar un script personalizado en Python y para ello tenemos que instalar también una librería que se llama Sky Scapi, es una librería muy interesante y muy práctica cuando queráis por ejemplo hacer algún tipo de operación relacionada con la red.

Es la más utilizada y la más recomendable cuando quieras crear un programa que gestione algo de una red desde Python.

Vamos a crear ese script para que lo veáis, no voy a explicaros en profundidad todo lo que hace, pero sí una vista general de cómo funciona y le voy a llamar pues dhcp attack python Bien pues así a nivel general básicamente lo que hace este programa es generar y enviar paquetes de descubrimiento DHCP, o sea lo que se llama el DHCP discover con direcciones Mac falsas.

Estos paquetes se van a utilizar en un ataque de agotamiento DHCP que es lo que haremos ahora.

Así que bueno, la primera línea que podéis ver que es el front, bueno es obvio, aquí lo que estamos es importando el scapi, también importamos la librería random porque es la que se va a basar para poder generar esas Mac falsas, que de hecho aquí podéis ver la función, La función random Mac lo que hace es eso justamente va a generar Mac aleatorias que comienzan con x x que son típicamente las más utilizadas para dispositivos virtuales.

Los últimos tres objetos de la dirección Mac se van a generar de forma aleatoria con la restricción de que el cuarto objeto sólo utiliza la mitad inferior de espacio, o sea X a xf.

Así que al final lo que tenemos una dirección Mac que digamos se convierte es una cadena hexadecimal separado por dos puntos, bueno ya sabéis cómo es el remoto de una dirección Mac, pues con esto tenemos una función que lo genera de forma aleatoria y esta es la función clave porque esta es la que va a realizar el ataque.

Aquí lo que hace primero con el com check ip address primera línea que veis que está false, eso lo que hace es que desactiva la comprobación de la dirección IP en scapi.

Bueno esto es algo interno de escapi, tampoco vamos a entrar mucho más en ello.

Después veis un bucle que es for 1 in range hasta 100, esto quiere decir que va a generar y enviar 100 paquetes de HTTP discover utilizando direcciones Mac falsas que se van a generar con el random Mac que ya hemos visto antes.

Esta fila sólo está diciendo que genere un encabezado Ethernet con la dirección de destino digamos para el broadcast.

Aquí establecemos las direcciones IP de origen y de destino para el paquete IP, como podéis ver el origen es sin IP y el destino es la dirección del broadcast.

Después tenemos los puertos UDP, aquí se definen los puertos de origen y destino para el protocolo UDP siguiendo las convenciones DHCP, es decir, el cliente envía desde el puerto 68 y el servidor escucha desde el puerto 67.

Esta parte de DHCP Option lo que hace es especificar que el paquete es un mensaje DHCP discover.

Esto bueno, podemos verlo aquí, aquí donde se asigna.

Y bien, finalmente pues nada, se imprime un mensaje para cada paquete enviado indicando que se ha enviado un DHCP discover con una dirección Mac falsa.

Bien pues ya sólo nos queda ejecutar este programa y ver cuáles son las consecuencias que tiene contra el servidor DHCP, pero antes tenemos que instalar la librería escape y para ello install scapi y la instalamos.

Vale pues ya tenemos listo el script para poder hacer la ejecución y ver cuáles son las consecuencias que tiene un DHCP Starvation o desgaste o agotamiento de las direcciones IP a un servidor DHCP.

Bien pues vamos a lanzar el script y ojo, tenemos que hacerlo como administrador porque utilizaremos cosas o digamos recursos del kernel asociados con la red, con lo cual tenemos que levantarlo como administrador, con lo cual hacemos un sudo y ahí está, veis, estamos lanzando ataques, creando diferentes paquetes con la Mac y bueno, vamos a comprobar si esto ha funcionado y a ver cuál ha sido la reacción de nuestro servidor DHCP.

Fijaros que ha tenido éxito, fijaros cómo va creando diferentes Mac con los primeros 3 bytes iguales pero el resto distinto.

Y esto os podéis imaginar que lo que está creando es un pequeño caos en el servidor de Edge de HCP, que bueno, a él le da igual, él simplemente quiere responder a todas las peticiones, pero claro tiene una limitación.

Bien pues de vuelta a nuestro servidor DHCP vamos a comprobar qué es lo que ha pasado a la pantalla para verlo más claro.

Y como siempre, la mejor forma de ver cualquier consecuencia de un ataque ya sabéis cuál es, y es la de comprobar los logs del sistema.

Entonces haremos un sudogreb y pondremos dhcp syslog.

Vamos a Porque es interesante, porque se está viendo perfectamente el éxito del ataque.

Aquí lo que se está mostrando es la actividad del servidor DHCP, indicando varios eventos que son muy importantes asociados con el manejo de las direcciones IP y las peticiones DHCP.

Aquí solamente hace un chequeo de que se ha inicializado todo bien para los diferentes protocolos EPV, EPV y correcto.

Bien.

Bueno, aquí hay una petición que no puede atender, pero bueno, esto tampoco es importante ahora.

Y vamos a ir bajando y veremos un poco lo que está ocurriendo.

A partir de aquí veremos.

Porque aquí es justo lo que nos interesa.

Aquí empieza el ataque de agotamiento de HCP.

Las múltiples líneas que veis aquí, comenzando con esta de la primera, desde aquí, son una serie de descubrimientos de HTTP, son peticiones de HTTP discover que provienen de diferentes direcciones Mac y todas comienzan por la que ya pusimos, ¿Acordáis?

Esto indica que es un ataque de agotamiento de HCP donde se generan peticiones desde direcciones Mac falsas para consumir todas las direcciones IP disponibles en ese servidor DHCP.

Y aquí, bueno, aquí intenta darla aquí más o menos lo está consiguiendo, está gestionándolas.

Pero justo a partir de aquí es cuando empieza a haber problemas.

Para ser más exactos, justo en este bloque aquí empieza a haber un problema, porque las líneas que indican no free lease muestran que el servidor DHCP ha agotado su reserva de direcciones IP que da el lease y no puede asignar direcciones nuevas a las peticiones entrantes.

Esto confirma que hemos tenido un éxito bastante grande en el ataque de agotamiento, ya que no hay direcciones impelibles para asignar a dispositivos legítimos que intenten conectarse a la red.

Y esto, claro, provocaría un pequeño caos porque nadie podría conectarse en ese momento, la máquina servidor DHTP no puede asignar direcciones IP, con lo cual ningún cliente nuevo legítimo de tu red podría acceder.

Bueno, podríamos bajar un poco más para ver cómo el ataque ha ido funcionando, pero nada, veis que al final no freelance, no hay ya forma, no puede estar entregando más direcciones IP a las peticiones que les van llegando desde múltiples, fijaos la cantidad de peticiones con diferentes Mac falsas que hemos generado con nuestro script.

Bien, pues la mejor forma de comprobarlo es mirar los logs.

Hay otro otro comando que suele venir instalado en Ubuntu que es DHCP, aquí nos debería de sacar un listado de todas las IPs que ha podido asignar, pero ¿Como hemos conseguido el ataque?

Pues en este momento no está entregando ninguna dirección IP, no está asignando IPs a ninguna Mac.

Aquí por ejemplo, desde el punto de vista de la defensa, algo interesante que podemos hacer, que nos puede sacar de algún apuro y comprobar realmente qué está pasando, es utilizar la herramienta nmap.

Bueno ya conocéis nmap, pero si usamos este comando, hacemos un nmap sn a la subred que tenemos que es la 55024, esto nos tendría que devolver las máquinas legítimas nada más, porque todo el resto son máquinas falsas, eran direcciones IP que no existen, con lo cual este nmap ha escaneado toda la red y como podéis ver funciona porque lo que nos está devolviendo son máquinas que sí que están en la red, podéis ver por ejemplo 7, la 5 también y esta también que es el gateway, con lo cual como podéis ver todo está funcionando bien, lo que pasa que digamos que hay como IPs fantasmas que están más que IP Mac fantasmas que están pidiendo que le asigne una IP, pero con nmap con este comando podríamos escanear y ver solamente aquellas que son legítimas, porque NAP sólo va a obtener respuesta de aquellas IP que sean reales, no de las falsas.

Pero bueno, ya sabéis que lo mejor para esto es monitorizarlo y aquí podríamos usar por ejemplo Wireshark para ver en T el tráfico, podemos filtrar por DHCP, bueno podemos hacer cantidad de cosas, o snort que ya lo conocéis, etc.

Bien, tenemos que recordar que el DHCP es un servicio crítico y que puede ser también vulnerable, vemos que es fácilmente entre comillas atacable y esto provocaría una delegación de servicio completa a tu red si no la sabes gestionar.

Por ese motivo es importante saber cómo protegernos de este tipo de ataques.

En definitiva, un ataque de agotamiento de DHCP evidencia la gran vulnerabilidad de los servicios de red críticos, incapacitando la asignación de direcciones IP a usuarios legítimos al saturar las que están disponibles.

Por este motivo es importante implementar medidas de seguridad muy robustas como el DHCP Snooping y la limitación de tasas de peticiones.

Y como siempre, tampoco olvidemos la monitorización, algo que tenemos que hacer siempre para prevenir cualquier tipo de ataque.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.