Ping Flood Attack

Transcribed on August 2, 2025 at 10:27 AM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a esta nueva sesión.

En esta nueva sesión vamos a tratar el tema del ataque Pin Flute o inundación de Ping, el cual es un ataque de denegación de servicio o DOS y también veremos por encima algunas de sus técnicas para mitigarlo.

Un Ping Flood es un tipo de ataque en el que se inundan de manera masiva y repetitiva a un objetivo con solicitudes de ECOICMP, que es el protocolo de control de mensajes de Internet muy asociado al ping, y son enviadas desde una fuente malintencionada hacia la víctima con una frecuencia tan alta que sobrecargan la capacidad de respuesta.

El objetivo principal del ataque es abrumar al sistema objetivo con una gran cantidad de tráfico de red, lo que puede provocar una saturación de los recursos de red y una disminución significativa en el rendimiento global del sistema.

Además este tipo de ataque es relativamente simple de ejecutar, pero puede causar daños considerables al servicio y disponibilidad de los recursos de red, afectando a usuarios legítimos y dificultando el funcionamiento normal de los sistemas.

Ahí tenéis un pequeño gráfico con todo el flujo de ataque de un Pink Flute.

Bien, pues vamos a la parte práctica y Como antes comenté, PIN Float es un ataque de denegación de servicio 1 2 que se enfoca en saturar a la víctima.

Competiciones del PIN Bien, ya hicimos uno parecido en otro módulo, pero aquí vamos a hacerlo un poco más en profundidad y ver en detalle cómo se utiliza con diferentes parámetros y la herramienta que utilizaré será HPIN, que bueno ya sabes, si no la tienes instalada pues tendrías que instalarla en tu equipo.

Bien, yo la tengo ya instalada en mi máquina y como siempre, como he hecho en otras prácticas, pues estaré en dos máquinas, esta será la primera que será la máquina atacante que tiene la dirección 17, acaba en 17 y la otra acaba en 5, es la máquina que he usado en otras en otros vídeos.

Bien, enviar un ataque de Pin Float con HPIN es bastante sencillo, fijaros, este sería el comando, voy a limpiar la pantalla para hacerlo más fácil y haríamos un hpin 3 flood run bueno voy a poner delante sudo por si no hay ningún tipo de problema, haremos un sudo con HTTP run, ahora os cuento que es claro source y después ponemos guión guión el protocolo ICMP y la dirección IP que vamos a tocar en este caso es la 2 11 5 5 punto 5 qué hemos hecho aquí, fijaros, comando hp y después float, esta es la clave porque esto es lo que diferencia lo que hemos hecho antes con HP y aquí lo estamos ya integrando en un

Después veis el comando run source, esto es que utiliza direcciones IP de fuentes aleatorias para cada paquete enviado y esto dificulta que la víctima o los dispositivos de red como cortafuegos o ids o ips puedan bloquear el ataque basándose en la dirección IP de la fuente, o sea, está emulando diferentes IPs para que no pueda ser capturado.

Y después ya ICMP indica a HPIN que genere paquetes ICMP y además específicamente el eco request que son los que se utilizan por el comando pin estándar.

Hay muchas formas de poder ver este ataque, podemos monitorizar los recursos por ejemplo de red, de CPU, de memoria, ancho de banda, etc.

Bien pues ahora vuelvo a la máquina número uno que es el servidor que va a ser atacado con el pink fluid y voy a ver la forma de visualizar el ataque para que podáis comprender cómo se está produciendo contra la máquina y qué efectos está teniendo sobre ella.

Pues ya de paso os comento una herramienta bastante útil que se llama Etherape que lo que hace es visualizar la red y así podemos ver cómo está ocurriendo el ataque, casi viendo la arquitectura en tiempo real.

Bien pues haremos un sudo apt update como siempre y luego ya haremos el sudo apt install fm que es así sudo apt installed Y ya lo tenemos instalado.

Bien pues vamos a proceder a lanzar la aplicación de delay sudo y ya lo tenemos aquí en la pantalla, vamos a abrir un poco para verlo mejor así lo primero será comprobar que la captura se está realizando a través de la tarjeta de AND que estamos utilizando, en este caso eth.

Aquí en capture podemos ir a interface y vemos que está en eth, bien etle tiene muchas más opciones pero no es el caso, ahora lo dejaré para que sea lo mínimo y captures toda la información y lo veamos en pantalla.

Bien, pues ahora voy a ir a la máquina 1 para lanzar el Pink Flute con HP 3.

Bien, pues lo que hacemos ahora es lanzar el ataque de Pink Fluid y veréis que empezará a trabajar.

Aquí va.

Vale, ahora lo ideal es irnos la otra máquina que es la que nos muestra la actividad, fijaros con el Pink Fruit incluso hay problemas para que nos muestre Etherape, fijaros que lo que está pasando, está intentando dibujarlo pero está dando un tipo de error porque está saturando la máquina, fijaros que está intentando dibujar todo, aunque este es el tráfico de Internet, con Etherape no podríamos visualizar el ataque, hay que buscar otra forma de ver qué está pasando.

Eso sí, se puede configurar, se puede adaptar para algún tipo de ataque, pero ahora mismo la máquina está totalmente congestionada por el ataque que está recibiendo del Pink Float y eso lo podemos ver porque la máquina se nota que va un poco lenta y si abrimos el System Monitor, que hasta aquí nos ha dejado ver, veréis cómo está la CPU, está al 100% de capacidad, están totalmente saturadas y también ocurre con la red, fijaros qué tráfico más inusual de red cuando no estamos haciendo nada, lo que pasa que está intentando responder a esos PIN que está recibiendo, con lo cual está totalmente saturado, procurando intentar corresponder a los eco request que está enviando el Ping Float Attack, Fijaros arriba la CPU que está totalmente al máximo porque está intentando dar salida a todas esas conexiones que están pidiendo del PIN.

Bien, aunque aquí en este caso no ha funcionado demasiado bien a la hora de dibujar la red, sí que os lo quería explicar para que tengáis a Ether en el radar, porque es una aplicación muy buena para ir dibujando los diferentes saltos.

Lo que veis ahí son las conexiones hacia Internet, también es lo que está dibujando, depende del protocolo y cada color corresponde a un protocolo específico.

Entonces bueno, que sepáis que esta aplicación existe y que es súper útil para ir viendo y dibujando el tráfico D, pero en este caso no ha funcionado bien para dibujar todos los nodos, porque no es que no puede con tanta información, de hecho fijaros de fondo como está decidiendo nodos, nodos, nodos y tendría que dibujar cada uno de estos nodos, algo que es totalmente imposible de hacer.

Fijaos la cantidad de IPs que está recibiendo el pin flu, y claro, la única forma de verlo es viendo la saturación de la máquina, que cada vez va peor, cada vez está más al 100% y también podéis ver el tema de la red.

Y lo mismo ocurre con la memoria, fijaros que la RAM también está a tope, está usando toda la máquina ahora mismo para intentar responder a esos PIN, que es algo totalmente imposible que no lo puede hacer, con lo cual en un momento dado la máquina llegará incluso a pararse o a provocar algún tipo de error por no poder dar servicio, y eso es justamente un ataque de denegación de servicio.

Pues bien, algunas de las medidas de mitigación y de protección podrían ser por ejemplo, la limitación de tasa, que es la primera, que es el Rate Limited, con esto es configurar los cortafuegos y los routers para limitar el número de solicitudes y CMP permitidas por segundo desde una única fuente o hacia un único destino.

Después tenemos las ya conocidas Listas de control de acceso o ACL, pues podríamos configurar ACL para bloquear o restringir el tráfico ICMP entrante o hacia direcciones IP específicas que no deberían estar recibiendo o enviando pings.

Después tenemos la detección de anomalías, utilizar sistemas de detección de intrusiones como los IDS y y los sistemas de prevención de intrusiones como los IPS que ya hemos visto.

Estos pueden identificar patrones de tráfico inusual, como por ejemplo una inundación ICMP.

Y esto ya lo vimos en el módulo de los IDS y de los ips.

De modo práctico, el ataque de pin fling representa una amenaza considerable para la disponibilidad de la red, al inundar a un objetivo con paquetes excesivos de peticiones de ECOP y CMP y esto provoca una congestión en la red y una interrupción en los servicios.

Estrategias de mitigación como la limitación de tasa, las ACL y la detección de anomalías son fundamentales para defenderse contra este tipo de ataques y preservar la funcionalidad de nuestra red.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.