Universidad
Nacional Autónoma de México

Facultad de Ciencias

Redes de computadoras

Lecturas

Alumno David Pérez Jacome

Profesor: El Paulo

2023

Resumenes de lecturas de la materia..

¿Qué es un ataque DDoS en la capa de aplicación?

Estos ataques a la capa 7, a diferencia de los ataques a la capa de red como la Amplificación del DNS, son especialmente eficaces debido a que consumen recursos del servidor además de los recursos de la red.
Un ataque a la capa de aplicación crea más daño con menos ancho de banda total.

Cuando un usuario envía una solicitud para entrar en una cuenta en línea, como una cuenta de Gmail, la cantidad de datos y recursos que debe utilizar el ordenador del usuario es mínima y desproporcionada en comparación con la cantidad de recursos que se consumen en el proceso de comprobación de las credenciales de inicio de sesión, la carga de los datos relevantes del usuario desde una base de datos y el posterior envío de una respuesta con la página web solicitada.

Distinguir entre el tráfico de ataque y el tráfico normal es difícil, especialmente en el caso de un ataque a la capa de aplicación, como una botnet que lleva a cabo un ataque de inundación HTTP contra el servidor de una víctima. Ya que cada bot en una botnet realiza solicitudes de red aparentemente legítimas, el tráfico no está falsificado y puede parecer que tiene un origen "normal".

Los ataques a la capa de aplicación requieren una estrategia adaptativa que incluya la capacidad de limitar el tráfico en base a determinados conjuntos de reglas, que pueden fluctuar con regularidad. Hay herramientas como un WAF que, configuradas correctamente, pueden mitigar la cantidad de tráfico falso que se pasa a un servidor de origen, lo que disminuye considerablemente el impacto del intento de DDoS.

Con otros ataques como las inundaciones SYN o ataques de reflexión como la amplificación NTP, se pueden utilizar estrategias para dejar caer el tráfico de forma bastante eficiente, siempre que la propia red tenga el ancho de banda para recibirlos. Por desgracia, la mayoría de las redes no pueden recibir un ataque de amplificación de 300 Gbps, y todavía menos redes pueden enrutar y servir adecuadamente el volumen de solicitudes de la capa de aplicación que puede generar un ataque L7.

Un método es aplicar un desafío al dispositivo que realiza la solicitud de red para comprobar si es un bot o no. Esto se realiza mediante una prueba muy parecida a la prueba CAPTCHA que es habitual encontrar al crear una cuenta en línea. Al tener un requisito como un reto computacional de JavaScript, se pueden mitigar muchos ataques.

Otras vías para detener las inundaciones HTTP incluyen el uso de un firewall de aplicaciones web, la gestión y el filtrado del tráfico a través de una base de datos de reputación de IP, y el análisis de la red sobre la marcha por parte de los ingenieros.

¿Qué es un ataque DDoS de inundación HTTP?

¿Qué es un ataque DDoS de inundación HTTP? Un ataque de inundación HTTP es un tipo de ataque volumétrico de denegación de servicio distribuido (DDoS) diseñado para saturar un servidor objetivo con solicitudes HTTP. Una vez que el objetivo ha sido saturado con solicitudes y es incapaz de responder al tráfico normal, se producirá una denegación de servicio para las solicitudes adicionales de los usuarios reales.

Los ataques de inundación HTTP son un tipo de ataque DDoS a la "capa 7". La capa 7 es la capa de aplicación del modelo OSI, y hace referencia a protocolos de Internet como el HTTP. HTTP es la base de las peticiones de Internet basadas en el navegador, y se suele utilizar para cargar páginas web o enviar contenidos de formularios por Internet. Mitigar los ataques a la capa de aplicación es especialmente complejo, ya que el tráfico malicioso es difícil de distinguir del tráfico normal.

Ataque HTTP GET - En esta forma de ataque, se coordinan varios ordenadores u otros dispositivos para enviar múltiples solicitudes de imágenes, archivos o algún otro activo desde un servidor objetivo. Cuando el objetivo se vea inundado con solicitudes y respuestas entrantes, se producirá una denegación de servicio a las solicitud adicionales que vengan de fuentes de tráfico legítimas.

Ataque HTTP POST - Normalmente, cuando se envía un formulario en un sitio web, el servidor debe gestionar la solicitud entrante y enviar los datos a una capa de persistencia, casi siempre una base de datos. El proceso de gestionar los datos del formulario y ejecutar los comandos necesarios de la base de datos es relativamente intensivo en comparación con la cantidad de potencia de procesamiento y el ancho de banda que se necesita para enviar la solicitud POST. Este ataque utiliza la disparidad en el consumo relativo de recursos, al enviar muchas solicitudes POST directamente a un servidor objetivo hasta que se sature su capacidad y se produzca una denegación de servicio.

Como se ha mencionado anteriormente, mitigar los ataques a la capa 7 es algo complejo y que, con frecuencia, es una tarea multifacética. Un método es implementar un desafío a la máquina solicitante para comprobar si es un bot o no, de forma muy parecida a la prueba captcha que es habitual encontrar al crear una cuenta en línea. Al tener un requisito como un reto computacional de JavaScript, se pueden mitigar muchos ataques.