Ataque DDoS

Un ataque de Denegación de Servicio Distribuido (DDoS) busca sobrepasar la capacidad de un recurso de red como un sitio web o un servidor, enviando un volumen masivo de solicitudes maliciosas. El objetivo principal es interrumpir el servicio y hacerlo inaccesible para los usuarios legítimos. En algunos casos, los atacantes pueden exigir un rescate para detener el ataque. Por lo general este tipo de ataques se utilizan para desacreditar o dañar el negocio de un competidor. Para enviar una cantidad extremadamente grande de solicitudes al recurso víctima, el hacker utiliza una “red zombi” de computadoras afectadas.

¿Cómo funciona?

Todos recursos de red tienen un límite finito de solicitudes que pueden atender al mismo tiempo. Además del límite de capacidad del servidor, el canal que conecta el servidor a internet tiene un ancho de banda capacidad limitada. Cuando hay una cantidad de solicitudes que pasa los límites de capacidad los servicios se ven afectados, de la siguiente manera:

- El ataque consume todo el ancho de banda disponible.
- El servidor se ve abrumado por la cantidad de solicitudes y no puede procesarlas todas

¿Cómo detectar un ataque DDoS?

No existe una forma de detectar un ataque DDoS, pero hay señales que pueden ayudar a identificarlo.

- Aumento inusual y repentino del tráfico web.
- Rendimiento irregular o red lento
- El sitio web se desconecta por completo

¿Cómo evitarlo?

- Desarrollar una estrategia de defensa.
- Identificar brechas de seguridad y evaluar posibles amenazas en la configuración.

¿Cómo protegerse contra un ataque DDoS?

- Realizar un análisis de riesgo de forma periódica.
- Organizar un equipo de respuesta contra ataques DDoS.
- Incorporar herramientas de detección y prevención de intrusiones.
- Evaluar la eficacia de la estrategia de defensa.