Ataques de denegación de servicios

DigitalHouse >
Coding School

Certified Tech Developer
The Ultimate Degree

Índice

1 Ataque de denegación de servicio (DoS)

Cuando hablamos de la **dimensión de disponibilidad** nos referimos a que la persona debe tener acceso a la información en el momento en que la necesite, en tiempo y forma.

“

La denegación de servicio consiste en la interrupción del acceso a los servicios (computadoras y redes) por parte de los usuarios legítimos.

”

Ataque de denegación de servicio (DoS)

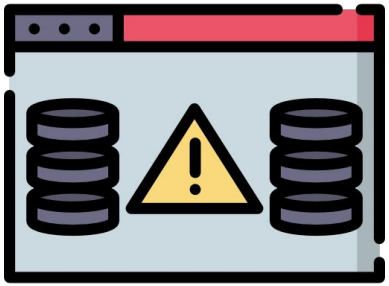
En un DoS lo que sucede es que se produce una gran cantidad de peticiones desde solamente una máquina o una dirección IP al servicio. Esto produce una saturación de los puertos, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones. Es aquí donde se produce la denegación del servicio.

Por otro lado, un DoS no solo puede ocurrir desde la red. El incremento del uso de recursos de manera sintética o forzada (como CPU o memoria), también puede producir un DoS. Es decir, no solo puede ocurrir saturando la red, sino que también se puede saturar otros recursos y producir el mismo efecto. Esto podría ocurrir desde la red o internamente en el servidor, con algún agente instalado programado para tal fin.

2 Ataque de denegación de servicio distribuido (DDoS)

Ataque de denegación de servicio distribuido (DoS)

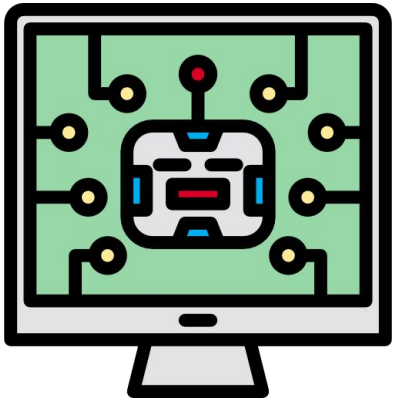
En un DDoS lo que sucede es que se produce una gran cantidad de peticiones al servicio, pero en este caso desde varios puntos o direcciones IP de conexión. Esto produce la saturación del puerto de destino, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones. Es aquí donde se produce el ataque de denegación de servicio distribuido.



bot - botnet

bot: es una **aplicación de software** que se encarga de realizar las tareas que tienen la característica de ser simples y repetitivas. Las mismas se realizarán a través de Internet. Estos bots trabajan mucho más rápido de lo que trabajaría una persona.

botnet: es un conjunto de dispositivos que están conectados a Internet y cuya seguridad ha sido comprometida por un atacante para instalar un bot programado para efectuar un ataque de DoS. Los dispositivos comprometidos quedan a la espera de que el atacante envíe una señal para comenzar el ataque.



Computadora Zombie

Una computadora zombie es una computadora que ha sido infectada por un virus, troyano o un gusano, y se utiliza de forma remota por un tercero para realizar ataques maliciosos —entre ellos está el ataque de denegación de servicio distribuido (DDoS)—.

3 Diferencia entre DoS y DDoS

“En DoS las peticiones se realizan desde solo una máquina o una dirección IP, como también puede ser desde algún agente instalado programado para tal fin. En DDoS las peticiones se realizan desde varios puntos o direcciones IP.”

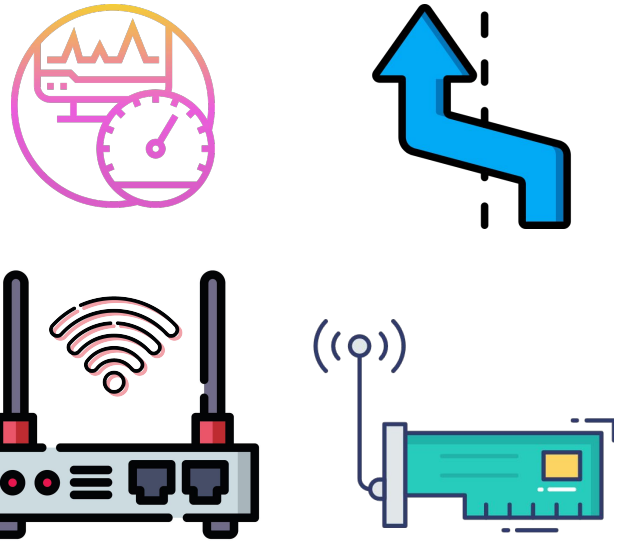
4 | ¿Cómo atacan?

Métodos de ataque

Consumen el ancho de banda.

Alteran las tablas de enrutamiento —la ruta por donde debe ir la información—. Por tal motivo, la información que se envía no llega a destino.

Fallas en los componentes físicos de una red.




DigitalHouse>
Coding School