acenswhitepapers

Definición y métodos, de Ataques DoS.

acens .com
the hosting company

Calle San Rafael, 14
28108 Alcobendas (Madrid)
902 90 10 20
www.acens.com

Definición

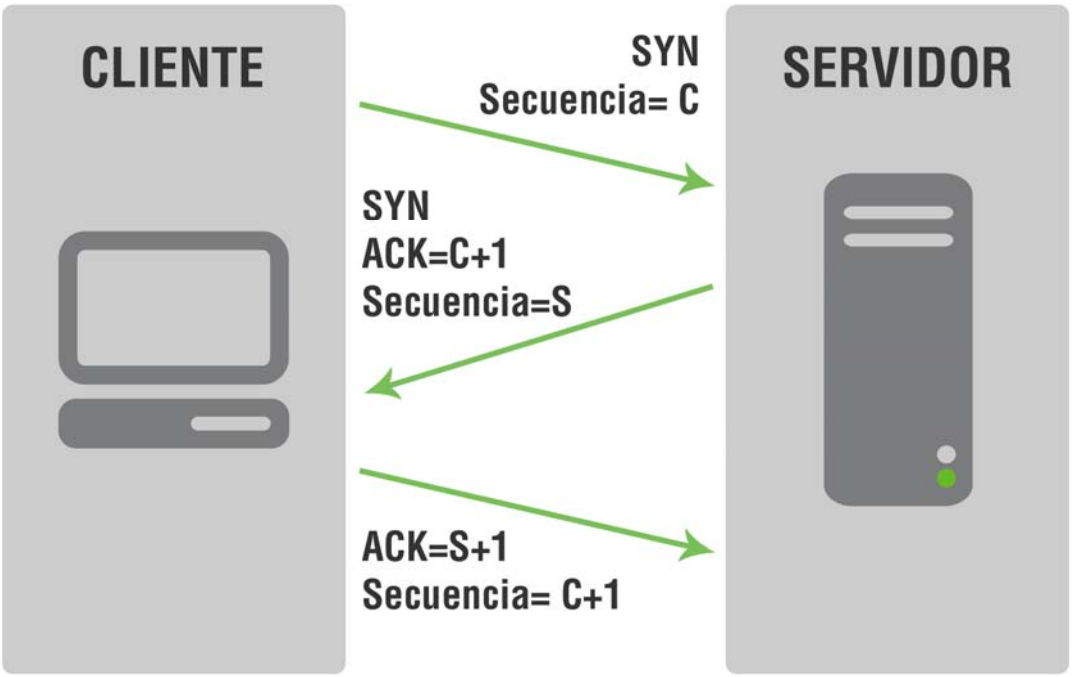
Un ataque de denegación de servicio, también llamado ataque DoS (Denial of Service) es un ataque a un sistema de red que provoca que un servicio sea inaccesible a los usuarios que hacen uso de él. El problema principal, y más importante, que causa este tipo de ataques es la pérdida de conectividad de la red por el consumo del ancho de banda de la red víctima, provocando así que ese servicio esté caído hasta que se consigue controlar el ataque.

Cuando se realiza un ataque de este tipo, lo que se hace es hacer multitud de peticiones simultáneas, que lo que hacen es saturar los puertos con muchos flujos de información, haciendo que el servidor se sature y no pueda servir tal cantidad de peticiones de información, de ahí su nombre de "denegación", ya que no es capaz de servir tal cantidad de petición de datos.

Para poder lograr hacer un ataque de este tipo, es necesario una gran cantidad de computadores activos en todo el mundo. Hay ocasiones en que los usuarios de esos computadores participan de forma voluntaria en el ataque, pero también se puede dar el caso de que los propios usuarios no sepan que están formando parte del ataque que se está realizando, ya que ni siquiera sabrán que están infectados. Al conjunto de equipos que participan en el ataque sin saber que forman parte de él , se le denomina red de equipos zombies.

Realizar un ataque de este tipo, se puede hacer de numerosas formas, aunque básicamente siempre consiste en lo siguiente.

Consumo de los recursos de los que dispone el servicio atacado, como puede ser el ancho de banda, el espacio en disco o consumir toda la capacidad de proceso del procesador.
Alteración de la información de configuración, como puede ser las rutas de encaminamiento.
Alteración en la información del estado, como puede ser la interrupción de sesiones.
Interrupción de componentes físicos de red.
Impedir la comunicación entre el usuario y la víctima, de manera que ya no se podrán poner en contacto de forma adecuada.



Métodos de ataque

Como ya hemos descrito anteriormente, en un ataque de denegación de servicio se impide el buen funcionamiento de la red que sufre ese ataque. Hay varios tipos de ataques, pero todos estos tipos tienen una cosa en común: utilizan el protocolo TCP/IP para conseguir dejar tumbada a la red.

Inundación SYN

El método “inundación SYN” es una forma de realizar un ataque de negación de servicio, en el cual , un atacante envía una sucesión de peticiones SYN al sistema, es decir, mandan un alto número de peticiones de información hasta que logran saturarlo.

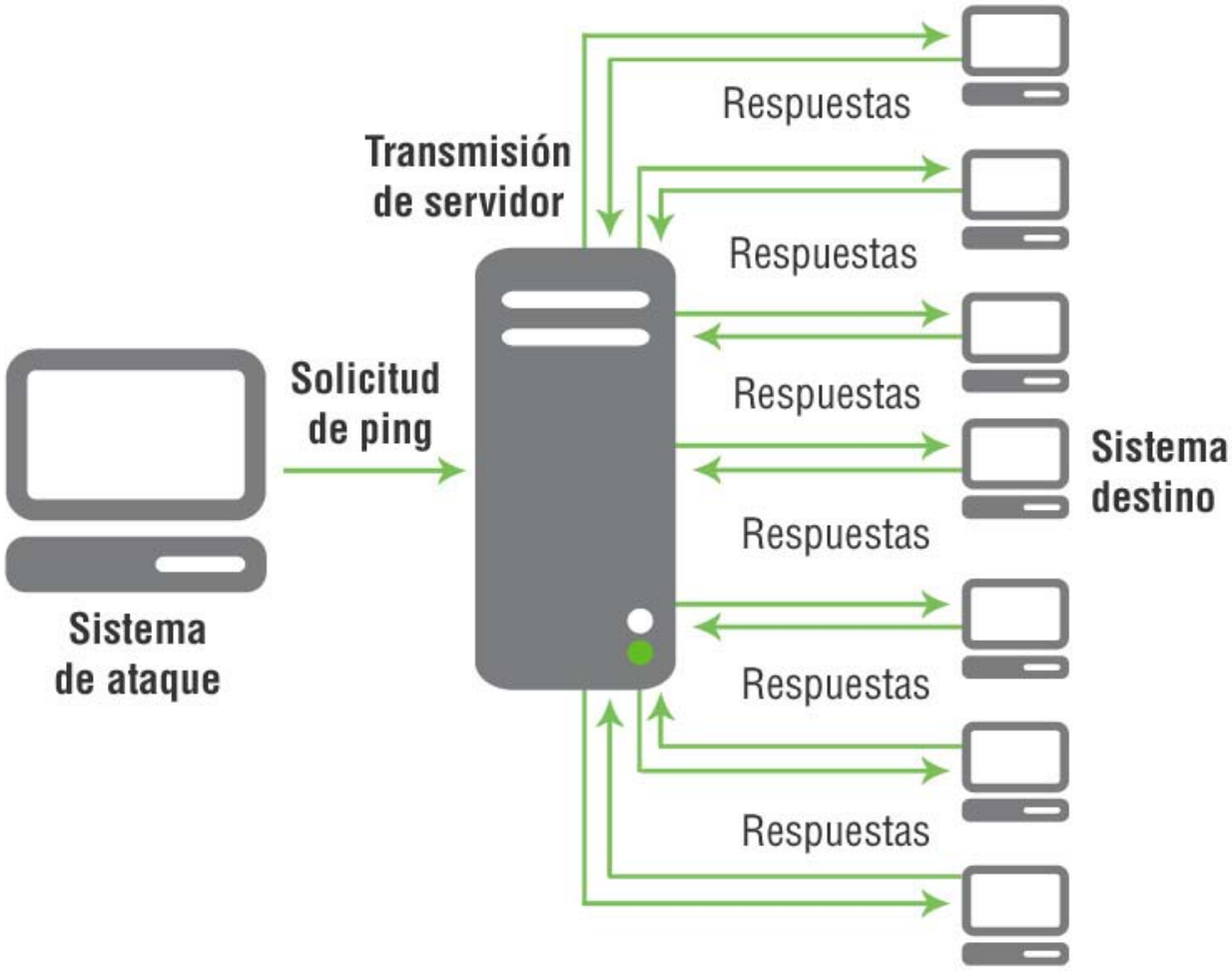
El funcionamiento normal de una conexión de una petición normal entre un cliente y un servidor, se lleva por medio del intercambio de mensajes. El proceso de este intercambio suele ser el siguiente:
El cliente que quiere realizar la conexión, manda un mensaje SYN al servidor.
El servidor de destino, recibe ese mensaje y responde enviando una respuesta SYN-ACK al cliente que ha realizado la petición.
El cliente que ha recibido la respuesta del servidor, responde al mismo con el mensaje ACK, iniciándose de esta manera la conexión.

A este proceso se le conoce como “Apretón de manos de tres vías del TCP”.

Conociendo ya los pasos para realizar la conexión, este tipo de ataques, lo que hace es enviar un número elevado de peticiones de conexión al servidor, pero en la petición SYN que se manda, el atacante lo que hace es cambiar la dirección de origen.

El servidor al recibir la petición de conexión responde, como hemos comentado anteriormente, enviando la señal SYN-ACK, y se queda a la espera de recibir la respuesta ACK del cliente. Al haber indicado direcciones falsas de origen, estas respuestas no llegarán nunca al servidor, por lo que este se quedará a la espera de estas respuestas consumiendo los recursos de la máquina y limitando el número de conexiones que se pueden hacer, causando de esa forma el problema.

Para este tipo de ataques, existe un mecanismo de caducidad que posibilita rechazar los paquetes una vez transcurrido un determinado período de tiempo. No obstante, cuando la cantidad de paquetes SYN es bastante considerable, si el equipo de destino utiliza todos los recursos para almacenar las solicitudes en cola, corre el riesgo de volverse inestable, lo que puede provocar la caída o el reinicio del sistema.



Inundación ICMP

Inundación ICMP es otra de las técnicas utilizadas para provocar un ataque de denegación de servicio. Este tipo de ataque, lo que busca es agotar el ancho de banda de la víctima, y para este fin, el atacante lo que hace es enviar un número elevado de paquetes ICMP echo request de gran tamaño hacia la víctima, haciendo que la víctima tenga que responder a su vez con paquetes ICMP echo reply causando una sobrecarga en la red y en el sistema de la víctima.

En este tipo de ataque, influye la relación entre la capacidad de procesamiento del atacante y de la víctima, ya que si la capacidad del atacante es mucho mayor que el de la víctima, esta no podrá manejar todo el tráfico generado, apareciendo de esa forma el problema de denegación de servicio.

SMURF

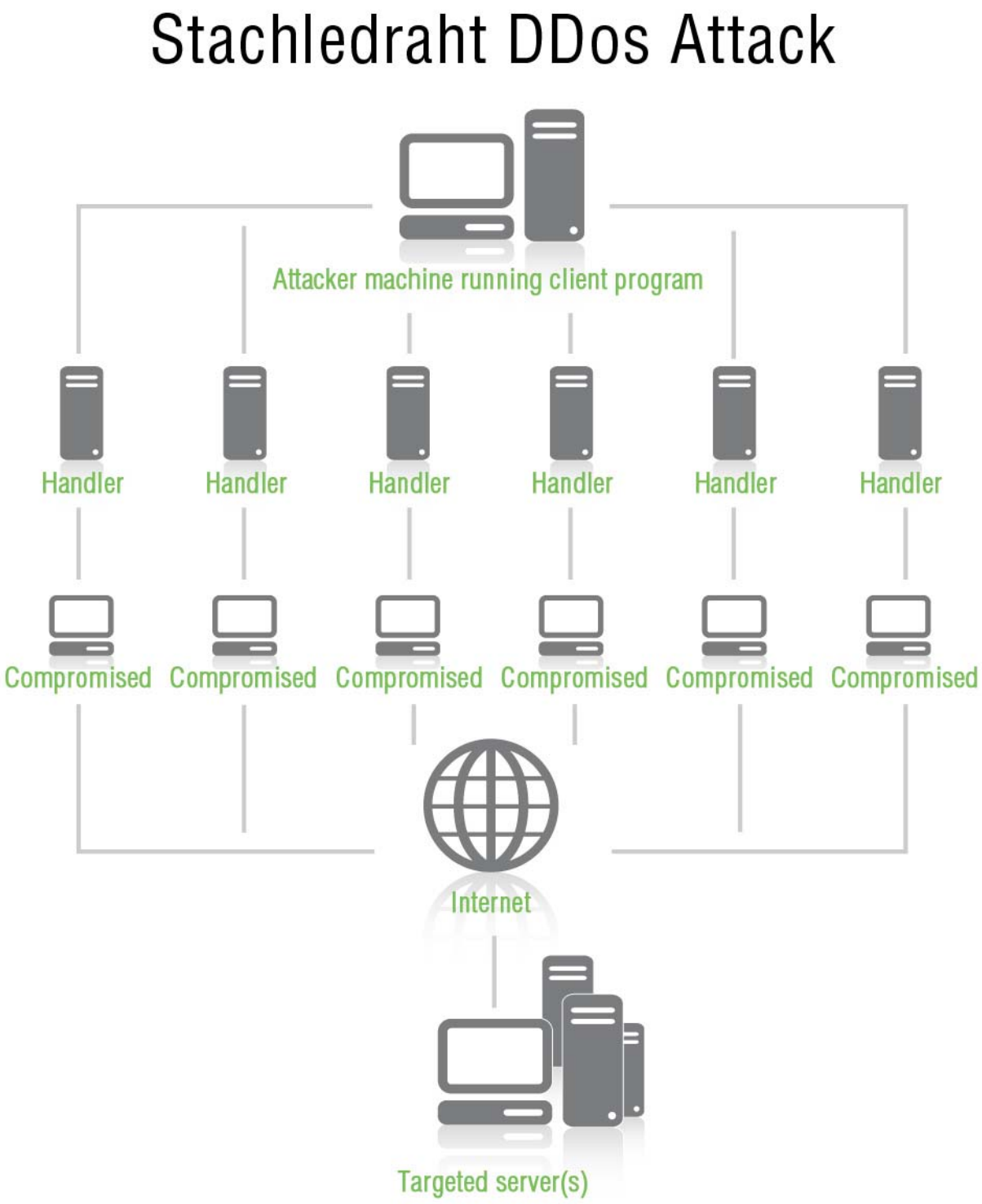
El ataque por medio de Smurf, es una variante del ataque por inundación ICMP, pero en este tipo de ataque intervienen tres elementos: el atacante, el intermediario y la víctima.

En el ataque Smurf, el atacante dirige paquetes ICMP tipo "echo request" a una dirección IP de broadcast, usando como dirección IP origen, la dirección de la víctima. Se espera que los equipos conectados respondan a la petición, usando “Echo reply”, a la máquina origen.

La gravedad del ataque vendrá dada por el número de intermediarios que pueda formar parte del ataque. Esta forma de ataque puede incluso provocar el mismo mal que el que se quiere hacer a la víctima.

A continuación, vamos a ver las etapas de este tipo de ataque.

El equipo atacante, envía una solicitud de ping a uno o varios servidores de difusión mientra que falsifica las direcciones IP de origen (dirección a la que el servidor debe de responder) y proporciona la dirección IP de un equipo de destino.
El servidor transmite la solicitud a toda la red.
Todos los equipos de la red, envían una respuesta al servidor de difusión.
El servidor redirecciona la respuesta al equipo de destino.



Inundación UDP

El tipo de ataque UDP consiste en generar gran cantidad de paquetes UDP contra la víctima (el protocolo UDP no requiere conexión, lo contrario que pasa con el protocolo TCP de los casos anteriores). Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP spoofing.

El caso más conocido de inundación UDP es el "Chargen Denial of Service Attack" la implementación de este ataque es sencilla: Es suficiente con establecer una comunicación entre el servicio “chargen” de una máquina y el servicio “echo” de otra. El servicio chargen genera caracteres mientras que el servicio echo reenvía los datos que recibe. El cracker envía paquetes UDP al puerto 19 (chargen) de una de las víctimas dando la dirección IP y el puerto de origen de la otra. En este caso, puerto de origen UDP 7 (echo). La inundación UDP lleva a la saturación del ancho de banda entre ambas máquinas. Una red completa puede ser la víctima de una inundación UDP.