



ATAQUES DDOS

La seguridad de Internet en Jaque



Índice

- Introducción
- Ataques DOS
- Ataques DOS Distribuidos
- Herramientas DDOS
- Soluciones
- Historia



ATAQUES DDOS

Introducción



- **Internet se ha convertido en la última década en una revolución tecnológica y social por diversos motivos:**

- Accesibilidad: Es accesible desde casi cualquier punto del planeta y en cualquier momento.
- Información: Es la mayor fuente de información del mundo y está desplazando a los medios de comunicación tradicionales: periódicos, radio, televisión...
- Comunicación y conectividad: Gracias a servicios como el e-mail, chats, grupos de noticias... permiten la comunicación de millones de personas de una manera económica.
- Anonimato: La conexión a Internet es relativamente anónima y permite a los usuarios ser prácticamente invisibles al resto.




- **Esas propias ventajas de Internet son su talón de Aquiles:**

- La accesibilidad y el anonimato permiten que sea muy difícil identificar la ubicación física o la identidad de los posibles atacantes a un sistema.
- La información permite que muchas personas se puedan formar para atacar a las vulnerabilidades de los sistemas. Lo único que necesitan es acceso a internet y un poco de predisposición para aprender.
- La comunicación permite coordinar a diferentes personas para realizar un ataque. Y la conectividad permite distribuir el software malicioso de manera rápida. Es precisamente esta característica que hace más vulnerable a Internet ya que un programa malicioso que aproveche una vulnerabilidad de un sistema operativo en pocas horas se puede distribuir por miles de equipos.



ATAQUES DDOS

Ataques DOS

- 
- **Podríamos definir los ataques DOS (Denegation Of Service) como la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.**
 - **Los ataques DOS nacen como una consecuencia natural de la propia arquitectura de Internet. No es necesario tener grandes conocimientos para realizar este tipo de ataques y no es tan arriesgado como realizar un ataque directo contra un servidor: este tipo de ataques utilizan otros equipos intermedios para luego poder borrar rastros.**
 - Por ejemplo: Si un servidor tiene un ancho de banda de 1mbps y un usuario tiene un ancho de banda de 30mbps, este usuario podría denegar el servicio del servidor haciéndole muchas peticiones y agotando su ancho de banda.

- **Existen tres tipos básicos de denegación de servicio:**

- **Consumo de recursos:** El atacante intenta consumir los recursos del servidor hasta agotarlos: ancho de banda, tiempo de cpu, memoria, disco duro...
- **Destrucción o alteración de la configuración:** Se intenta modificar la información de la máquina. Este tipo de ataques necesitan de técnicas más sofisticadas.
- **Destrucción o alteración física de los equipos:** Se intenta denegar el servicio destruyendo físicamente el servidor o algunos de sus componentes, cortando el cable de conexión, o el cable de la red eléctrica.

Nosotros nos centraremos en el primer tipo de ataques.



FIG. 1 - Ataques DOS

Los sistemas de DOS más utilizados:

- Mail Bombing: El primer sistema de denegación de servicio fue el denominado *mail bombing*, consistente en el envío masivo de mensajes a una máquina hasta saturar el servicio.
- Smurfing: Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de *ping*. Esta trama lleva como dirección de origen la dirección IP de la víctima (usando IP Spoofing) y como dirección de destino la dirección broadcast de la red atacada. De esta forma todos los equipos de la red contestan a la víctima de tal modo que pueden llegar a saturar su ancho de banda. (FIG. 2)
- SYN Flood: El sistema atacante utiliza una IP inexistente y envía multitud de tramas SYN de sincronización a la víctima. Como la víctima no puede contestar al peticionario (porque su IP es inexistente) las peticiones llenan la cola de tal manera que las solicitudes reales no puedan ser atendidas. (FIG. 3)

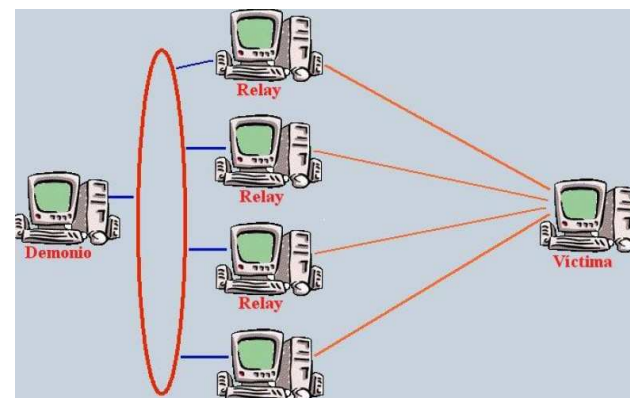


FIG. 2 - Smurfing

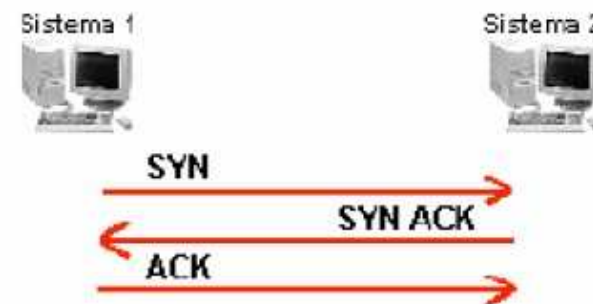


FIG. 3 – SYN Flood



ATAQUES DDOS

Ataques DOS Distribuidos

- **Podemos definir el ataque DDOS como** *un ataque de denegación de servicio (DOS) dónde existen múltiples focos distribuidos y sincronizados que focalizan su ataque en un mismo destino.*
- **Es decir, el ataque DDOS es una ampliación del concepto DOS sumándole la capacidad de acceso simultáneo y desde cualquier punto del mundo que ofrece Internet.** (FIG. 4)

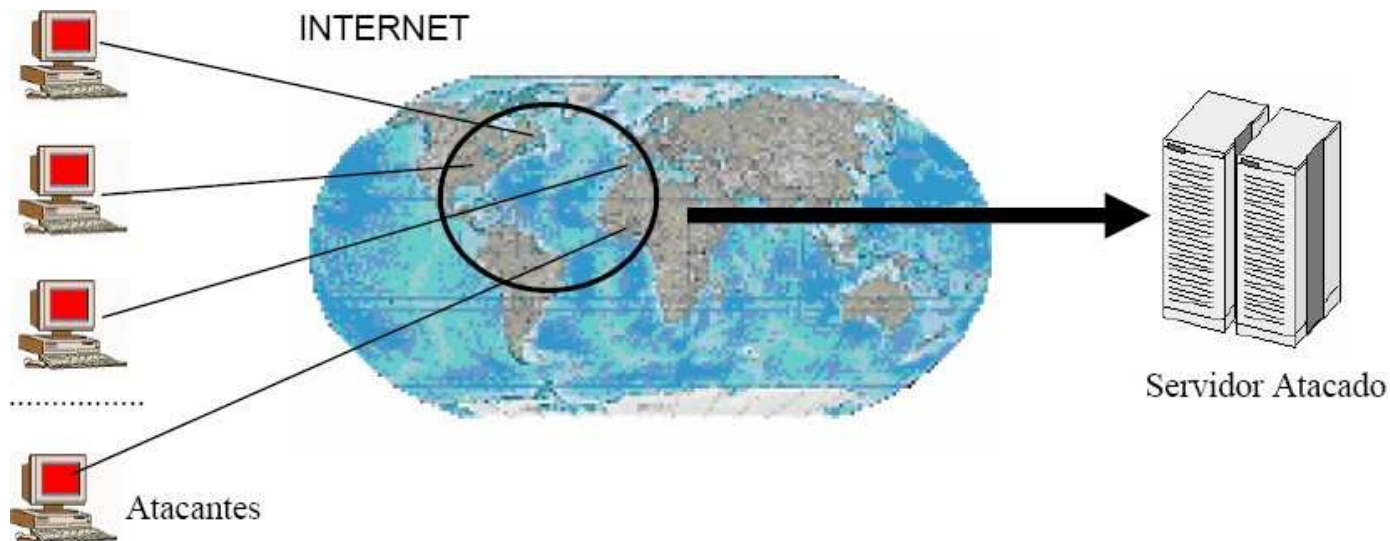




FIG. 5 – Esquema general de DDOS

- 
- **Existen diferentes tipos de ataques DDOS pero todos tienen en común un gran consumo de ancho de banda. Aquí está el gran peligro de este tipo de ataques que tienen dos vertientes:**
 - Denegación del servicio: Es su objetivo principal, hacer que un sistema no pueda cumplir su cometido.
 - Saturación de la red: Debido a que los paquetes de estos ataques comparten las mismas rutas que el resto de comunicaciones.

 - **El crecimiento del número de nodos conectados y la mejora del ancho de banda hacen que existan cada vez más atacantes potenciales. Se puede dar el caso de cientos de atacantes coordinados pero este fenómeno no se da en la realidad:**
 - ▶ Es muy arriesgado para un atacante usar su propio equipo.
 - ▶ Es muy difícil coordinar a muchos atacantes.

- 
- **En la práctica el método utilizado es:** *(FIG. 6)*
 - Uno o varios hackers buscan sistemas vulnerables. Esto es fácil ya que:
 - Cada vez hay más nodos conectados permanentemente a internet.
 - Muchos equipos carecen de las actualizaciones críticas de sus sistemas operativos o éstos son antiguos.
 - El desconocimiento de muchos de los usuarios hace que no sean conscientes de que sus equipos están infectados por algún programa malicioso.
 - Se realiza un ataque sobre esos nodos y se les instala el programa. Estos son los nodos “masters”, es decir, los que tienen una conexión directa con el atacante.
 - A su vez el programa instalado en estos nodos busca un segundo nivel de nodos (“slaves”) que serán los encargados de realizar el ataque final.
 - Los atacantes dan la orden de manera sincronizada para que todos los nodos slave ataquen al sistema “víctima”.

- La gran ventaja de este sistema es que permite mantener el anonimato de los atacantes ya que analizan el trafico de los nodos slave y cuando detectan que están siendo analizados cierran la conexión, posteriormente limpian cualquier prueba en el master y finalmente cierran su conexión con el master.

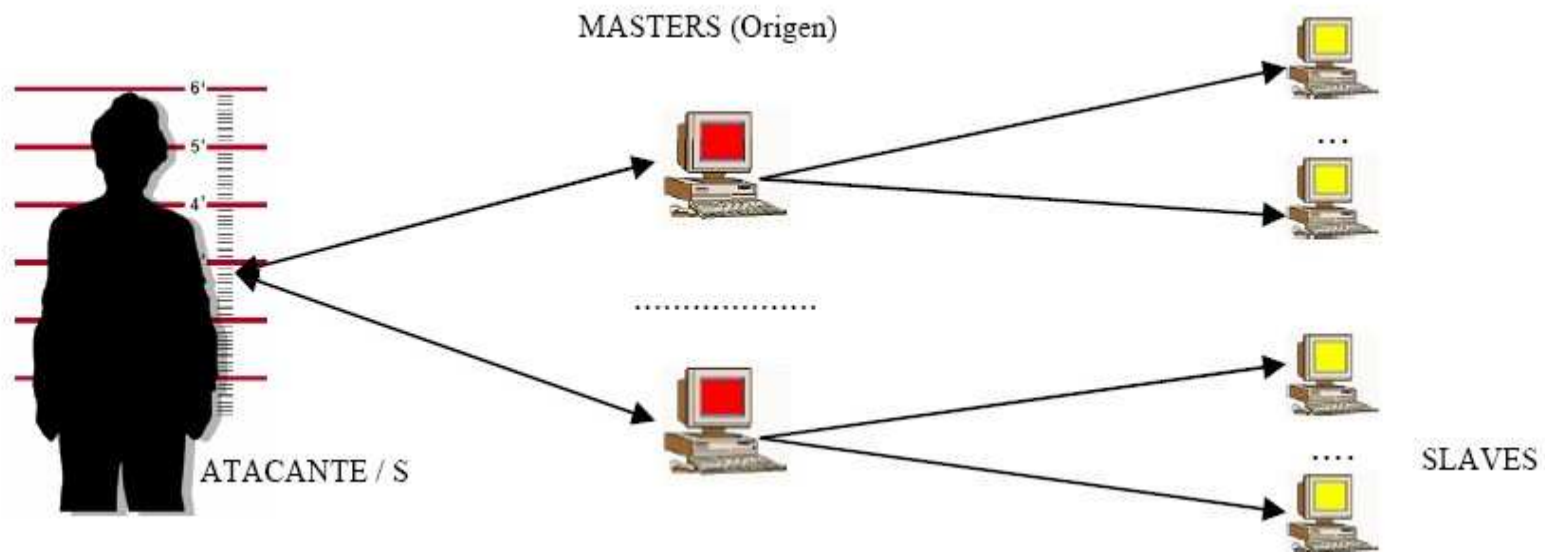
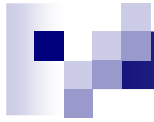


FIG. 6 – Jerarquía de nodos atacantes



ATAQUES DDOS

Herramientas



- La proliferación de herramientas ha ido creciendo gracias a la aparición de comunidades de intrusos que, con mucha organización y muy poco tiempo de respuesta, consiguen pasar de una versión beta a su versión final en tiempos récords.
- Esto hace que la dificultad para enfrentarse a ellos resulte cada vez mayor.
- Las herramientas usadas para crear ataques DDOS son cada vez más sencillas y fáciles de usar para usuarios poco expertos, esto hace que también aumente el número de ataques y los daños que producen.



Trinoo

- Trinoo es la primera herramienta de ataque distribuido conocida.
- Los primeros “demons” trinoo fueron encontrados en maquinas solaris, al parecer infectadas por vulnerabilidades sobre los RPC.
- Trinoo aprovecha vulnerabilidades y errores conocidos de distintos SO para su contagio.
- Después de su fase de contagio la Red Trinoo está lista para recibir los comandos y actuar en consecuencia.
- Los puntos débiles de Trinoo está en que la transmisión de comandos usa una patrón fácilmente reconocible por programas de detección y el almacenaje de las IP comprometidas en ficheros no encriptados.



TFN y TFN2K

- Estas herramientas son la evolución natural del Trinoo.
- Las herramientas TFN (Tribe Food Network), implementa la mayoría de ataques DDOS conocidos.
- La diferencia fundamental con Trinoo es que la sincronización de la red ya no viaja en TCP o UDP sino por ICMP echo reply, para conseguir de esta manera una mayor dificultad a la hora de ser detectados por monitorizadores de la red.
- Su punto débil es que no comprueba el origen del paquete ICMP, por ello un solo paquete ICMP con los datos correctos puede dejarlo fuera de combate.




TFN2K

- TFN2K es la más sofisticada herramienta descubierta hasta el momento. Entre sus características más novedosas destacan:
 1. La comunicación entre maestro y esclavo está encriptada.
 2. Los paquetes de comandos y los ataques propiamente dichos, pueden ser enviados de una forma aleatoria utilizando TCP, UDP, ICMP.
 3. El maestro es capaz de falsificar su propia dirección IP lo que hace complicado prevenir este tipo de ataques.
 4. La comunicación es totalmente "silenciosa". Ningún comando es reconocido con el envío de un paquete aceptando o diciendo haber entendido su contenido.
 5. Los comandos utilizados no están basados en cadenas.
 6. Comprobación de la autenticidad de los mensajes recibidos, aprovechando características del mecanismo de encriptación.



ATAQUES DDOS

Soluciones

- 
- Si analizamos el funcionamiento de los DDOS nos daremos cuenta que no existen soluciones 100% fiables contra ellos.
 - Sin embargo si podemos defendernos de sus efectos. Y el modo de defensa debe cumplir las 5 requisitos básicos
 1. Una solución distribuida para un problema distribuido
 2. La solución no debe penalizar el tráfico de usuarios legítimos
 3. Solución robusta y universal (amenazas internas y externas)
 4. El sistema debe ser viable es su aplicación
 5. Debe ser una solución incremental
 - Las soluciones actuales se basan en firewalls clásicos y sistemas de detección de intrusos
 - Organismos como CISCO recomiendan soluciones sencillas como modificar el tamaño de la pila de TCP o disminuir el tiempo de espera de establecimiento de las conexiones.



ATAQUES DDOS

Historia de los ataques DDOS

- La evolución del número de ataques a servidores web, ha ido en aumento desde el su inicio.

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

Total incidents reported (1988-2003): **319,992**



Ataque sobre los DNS raiz

- Según los expertos la redundancia de los datos en los servidores DNS, y su distribución por el mundo, hace que el sistema de resolución de nombres se mantenga operativo desde el punto de vista del usuario siempre que haya al menos 5 servidores operativos.
- El 21 de Octubre de 2002, se intentó un ataque sobre 11 de los 13 servidores raiz de DNS. Este ataque sin embargo solo logró la caída de 7 servidores.
- Cuando el ataque fue detectado, los responsables de administración de las diferentes máquinas tomaron medidas para la recuperación y la prevención del ataque.
- Durante 1 hora el ataque estuvo apunto de tener efectos reales sobre Internet, y provocar grandes perdidas economicas



MyDoom

- El virus MyDoom ha sido uno de los más extendidos (1 million de máquinas afectadas según F-Secure).
- Su propagación a sido una de las más rápidas, en 4 segundos ya era una verdadera epidemia.
- Inicialmente este virus fue concebido para hacer un ataque DDoS sobre el servidor de SCO (www.sco.com), aunque existen teorías de que su verdadera intención era la recopilación de direcciones de e-mail para Spam.
- El ataque tuvo la SCO en jaque durante 1 semana hasta que SCO cambió su dominio (www.thescogroup.com).
- Su predecesor MyDoom.B no llegó a tener el mismo impacto ya sea por su menor propagación o por la capacidad de respuesta de su objetivo (www.microsoft.com), que cambió sus servidores solo 2 segundos despues del inicio del ataque.



Blaster y Sasser

- Blaster ha sido uno de los últimos virus con gran expansión por la red.
- Su objetivo era un DDoS sobre los servidores de Microsoft. Especialmente contra el sitio www.windowsupdate.com
- Su infección se producía por una vulnerabilidad de Windows.
- Aunque el número de ordenadores infectados resulto ser bastante grande 1,2 millones, no provocó grandes problemas.
- La semana pasada se ha descubierto el virus Sasser que, al igual que Blaster, aprovecha las vulnerabilidades de Windows para su distribución por la red. Sus consecuencias estan siendo menores que las de Blaster y a día de hoy está en fase de desinfección.