3. Protección de Datos

7. Denegación de Servicio

7.1 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 conectividadpermite 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.

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.

Un ataque de denegación de servicio (Denial of Service) se caracteriza por intentar evitar el uso legítimo de un bien, servicio o recurso.

Un DDoS (Distributed DoS) consiste en la utilización de muchos atacantes para lograr un DoS.

Pero, ¿cómo es posible lanzar este tipo de ataques en Internet?

- Las técnicas de diseño de la Internet actual se centran en ser eficiente en el transporte de paquetes de fuente a destino. Se trata de un modelo extremo a extremo: la red proporciona un servicio best-effort
- Es responsabilidad de los extremos utilizar los protocolos convenientes para garantizar calidad de servicio, transporte robusto y fiable o seguridad.

- Si uno de los extremos se comporta de manera malintencionada puede provocar daños al otro extremo
- Dado el diseño de la red intermedia (Internet) no se actuará contra el host malicioso.
- Consecuencias de estos ataques:
    - Suplantación de direcciones IP: IP Spoofing
    - Ataques de denegación de servicio distribuido (DDoS)

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.

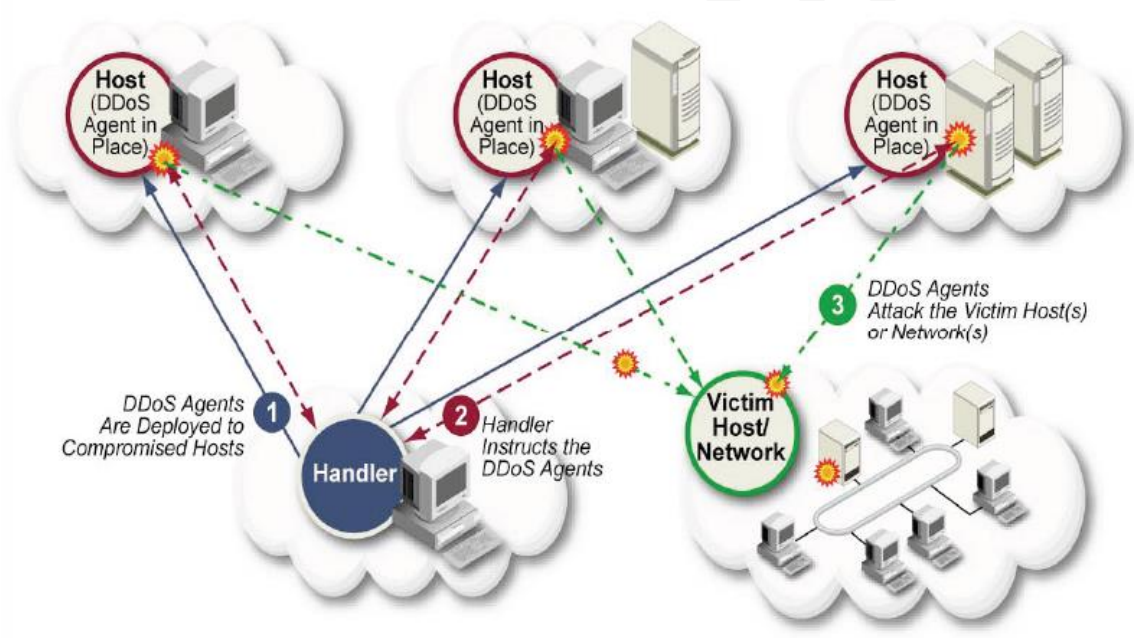
7.2 Internet y DDoS

Las características de Internet hacen que sea relativamente sencillo lanzar ataques DDoS usando esta infraestructura. Entre otras tenemos:

- La seguridad en Internet es altamente interdependiente
- Los recursos en Internet son limitados: Ancho de banda, CPU, memoria, espacio en disco
- La inteligencia y los recursos no son gestionados de manera coordinada
- No es obligatorio llevar un registro de la actividad
- El control es distribuido

Aunque pueden existir diferentes tipos de ataque, cuando se lleva a cabo un ataque DDoS, podemos identificar unas fases comunes:

- Reclutamiento de los agentes que realizarán el ataque:
    - Búsqueda de vulnerabilidades.
    - Utilización de la vulnerabilidad para acceder a la máquina.
    - Infección de la máquina con el código del ataque. De esta forma, el atacante está construyendo lo que suele denominarse como Botnet
- Utilización de las máquinas comprometidas para ejecutar el ataque.



7.2.1 Motivaciones de los ataques DDoS

Detrás de los DDoS puede haber diversos motivos que enumeramos aquí:

- Provocar un daño en la víctima.
- Razones personales
- Ganar prestigio. Los atacantes suelen alardear de sus logros para conseguir renombre dentro de su comunidad.
- Motivos económicos. Se han registrado ataques DDoS que han inutilizado infraestructuras de empresas a las que se les ha exigido dinero a cambio de terminar el ataque.
- Razones políticas

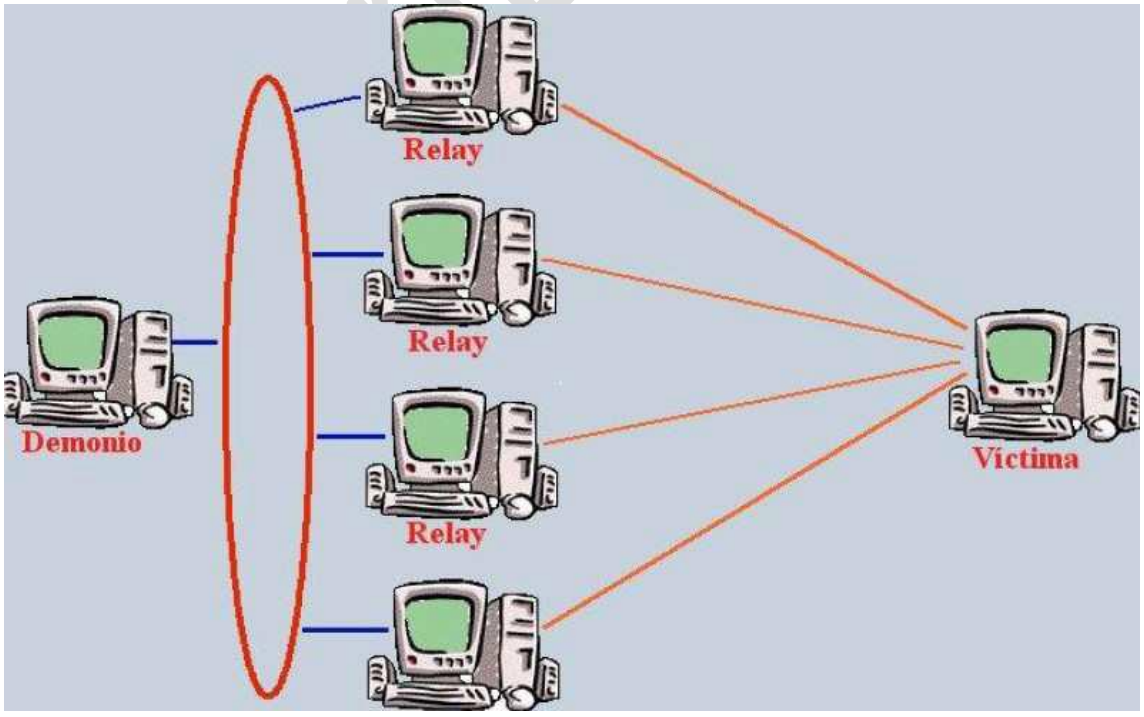
7.3 Ataques DoS Clásicos

Dentro de estos ataques podemos dividir en las siguientes categorías:

- **Ataques lógicos o software**: consiste en enviar al equipo remoto una serie de datagramas mal construidos para aprovechar algún error conocido en dicho sistema. Son fáciles de evitar actualizando el SW a versiones que corrijan dichos fallos o añadiendo reglas al FW para filtrar paquetes mal construidos.
    - Ping of Death
    - Teardrop
    - Land
- **Ataques de inundación (flood)**: consisten en bombardear un sistema con un flujo continuo de tráfico que acaba por consumir todos los recursos del mismo y el BW de la red del sistema atacado.
    - TCP SYN
    - Smurf IP
    - UDP Flood
    - ICMP Flood

Los sistemas de DOS más utilizados:

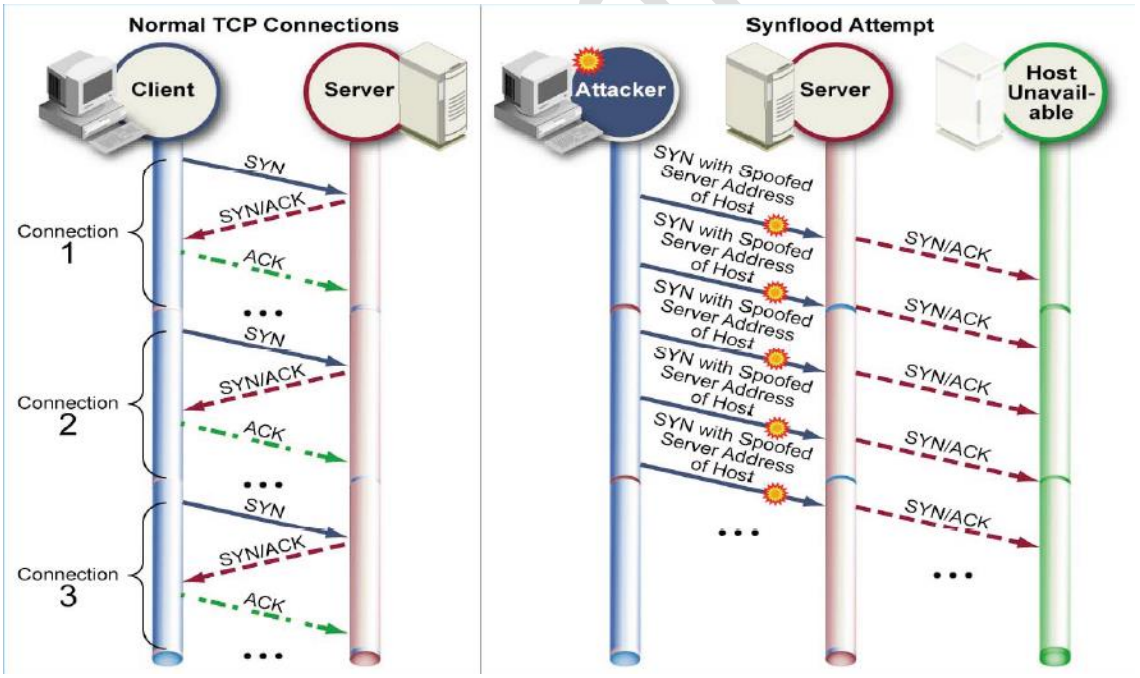
- Mail Bombing: El primer sistema de denegación de servicio fue el denominado mail bombing, consistente en el envío masivo de mensajes a una máquina hasta saturar el servicio.
- Smurfing: Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de ping. Esta 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.



    - Es muy simple pero desgraciadamente muy efectivo.

- Aprovecha las direcciones IP de broadcasting y los paquetes ICMP ECHO Request/Reply (PING)
- No existe una protección total contra este ataque, por lo que sigue siendo muy peligroso.
- Este ataque necesita al menos tres protagonistas: el atacante, el atacado y un conjunto de redes intermediarias que se utilizan para el ataque.
- El atacante busca redes (a ser posible grandes, con más de 30 hosts), que tengan dirección IP de broadcasting (X.Y.Z.255, o X.Y.255.255, o incluso mejor, X.255.255.255).
- Falsifica un paquete IP poniendo como dirección Origen la de la víctima, y envía un paquete ICMP ECHO Request (PING) a la dirección de broadcast de las redes intermediarias seleccionadas.
- Los centenares (o miles) de hosts de esas direcciones de broadcasting responderán a quien ellos creen ser el origen (en realidad la desprevenida víctima) con un paquete ICMP de respuesta al PING, colapsando la línea de ese servidor.
- Si este proceso se repite cada pocos segundos el efecto es devastador.

- 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.



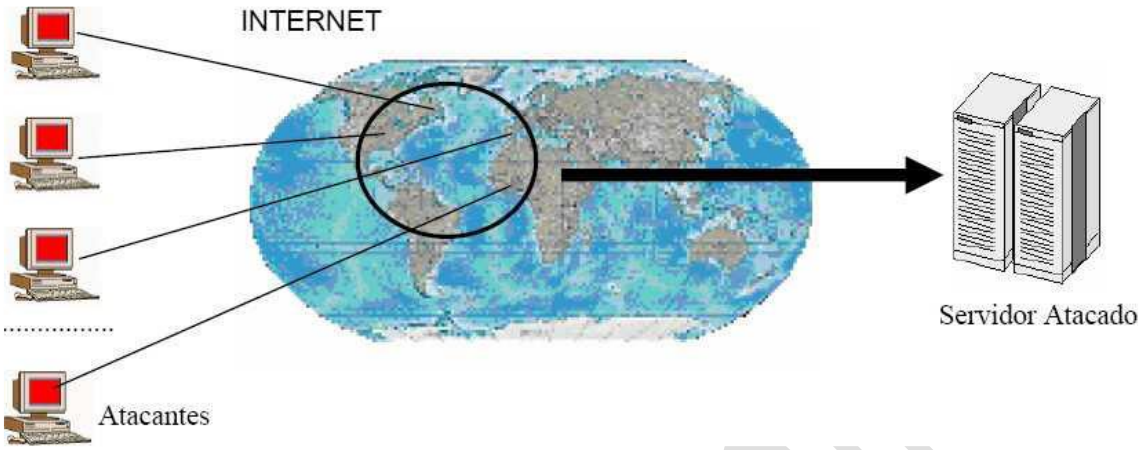
- El esquema del establecimiento de conexión TCP es,
  1) C ---------- NSc, Syn ---------- >> S
  2) C <<------- NSc+1, Ack, Syn, NSs ---------- S
  3) C ---------- NSs+1, Ack ---------->> S
- Normalmente los pasos 1,2 y 3 se producen consecutiva y rápidamente. El servidor suele establecer un timeout de 75 segundos entre el paso 2 y la respuesta del ciente del paso 3.

- El ataque TCP Syn se basa en falsificar (spoof) el IP origen del paso 1, poniendo el IP de un host legal pero inalcanzable (unreacheable)
- Por tanto nadie responderá al paso 2, y el servidor deberá esperar 75 segundos en un estado muy incómodo, con su socket a medio abrir, sus bufferes reservados, etc..
- Además TCP suele tener una cola finita y no muy grande (de 6 a 15 entradas) para estas conexiones en trámite, por lo que si enviamos varias decenas de estas peticiones de conexión TCP falsas colapsaremos la cola haciendo que el servidor tenga que rechazar el resto de peticiones “legales” que le estén llegando.
- Si además repetimos esa tanda de peticiones cada 80 segundos (un poco más de 75s, para que dé tiempo de que se desbloqueen las anteriores), conseguiremos parar el servicio TCP.
- Este ataque es difícil de evitar, ya que se basa en una debilidad intrínseca de TCP.

7.4 Ataques DDoS

Podemos definir el ataque DDOS como un ataque de denegación de servicio (DOS) donde 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.



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:

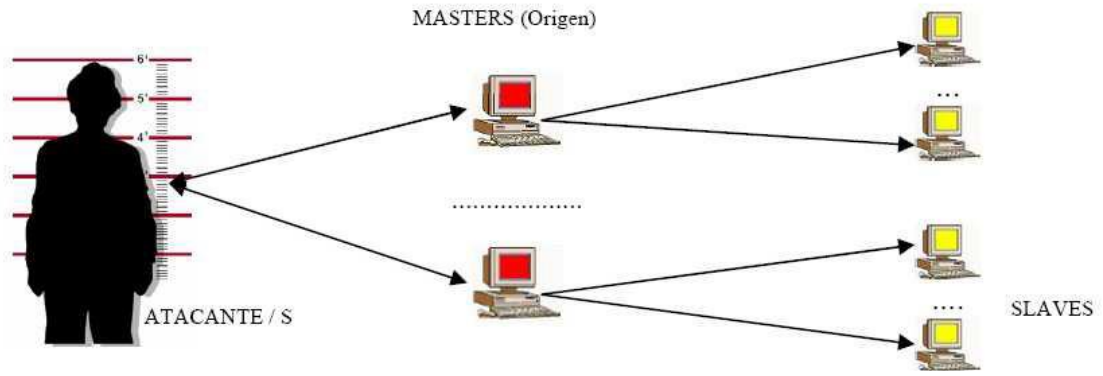
- Denegación del servicio: Es su objetivo principal, hacer que un sistema no pueda cumplir su cometido.
- Saturación de la red: Debido a que los paquetes de estos ataques comparten las mismas rutas que el resto de comunicaciones.

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:

- 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 “victima”.



La gran ventaja de este sistema es que permite mantener el anonimato de los atacantes ya que analizan el tráfico 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.

7.5 Herramientas en Ataques DDoS

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.

Veamos algunos ejemplos clásicos:

Trinoo

Trinoo es la primera herramienta de ataque distribuido conocida.

Los primeros "demons" trinoo fueron encontrados en máquinas 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.

El punto débil de Trinoo está en que la transmisión de comandos usa un patrón fácilmente reconocible por programas de detección y el almacenaje de las IP comprometido 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 fue la más sofisticada herramienta descubierta hasta el momento.

Entre sus características más novedosas destacaban:

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.

7.6 Soluciones a Ataques DDoS:

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 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.