FIB Facultat d'Informàtica de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA

CONCEPTES AVANÇATS DE SISTEMES OPERATIUS

Departament d'Arquitectura de Computadors

Ataques DDoS

(Seminaris de CASO)

Autors

Daniel Albert Sánchez

Àngel Casanova Rosell

Introducción

- **¿Qué es un ataque DDOS?**
  - El acrónimo significa ataque Distribuido de Denegación de Servicio.
- **Algunas de las víctimas de este tipo de ataques**
  - Yahoo
  - Amazon
  - Buy.com
  - eBay
  - CCN

Descripción de un ataque convencional

- Recopilación de información sobre la máquina víctima
  - SO, servicios, tipología de red …
- Utilización de los conocimientos obtenidos para entrar en la máquina víctima.
  - Usando bugs, fuerza bruta, etc.
- Una vez accedida a la máquina, conviene borrar las pistas que dejan los servicios sobre el acceso del atacante.
- También es usual que el atacante se deje algún mecanismo que le permita el acceso en futuras ocasiones.

Descripción de un ataque distribuido

- Diferencia con ataque tradicional:
  - Programas instalados en la máquina víctima que delegan el control de la misma al atacante.
  - Permiten el acceso remoto.
- La detección de un ataque distribuido mediante NIDS (Network Intrusion Detection Systems) es más complicada, puesto que es difícil saber el origen real del atacante.
  - Se suele utilizar IP Spoofing

Denegación de servicio

- La denegación de servicio DoS (Denial of Service), se produce cuando un determinado servicio no se encuentra disponible.
- Puede deberse a:
  - Que no haya conectividad en la red
  - Que no haya ancho de banda suficiente
  - Que no haya recursos en el sistema
  - Destrucción de la configuración del servicio
  - Ausencia física

Ataques DDoS

- Utilizar los ataques distribuidos para tomar el control de N máquinas y provocar de esta manera un ataque coordinado contra una tercera máquina.

- Básicamente se dividen en tres tipos:
  - DoS mediante UDP flood
  - DoS utilizando TCP syn flood
  - DoS mediante paquetes ICMP (ping)

Ataques DDoS

- DoS mediante UDP flood
  - Generar cantidades grandes de paquetes UDP a la víctima
  - Se suele acompañar de IP Spoofing
    - Denominamos IP Spoofing a la falsificación de la dirección IP remitente en un paquete.
    - De este modo se puede suplantar la identidad con algún fin.

Ataques DDoS

- DoS utilizando TCP syn flood
  - Susceptibles servicios que utilizan TCP (ftp, http, etc.)
  - Descripción del proceso:
    - El cliente envía una petición SYN
    - El servidor le responde con SYN-ACK
    - El cliente NO le responde con ACK
  - De este modo, la conexión queda “medio abierta”. Como puede aceptar un número de clientes limitado, al final se bloquea.
  - El atacante puede neutralizar el timeout

Ataques DDoS

- DoS mediante paquetes ICMP (ping)
  - Pretende agotar el ancho de banda de la víctima
    - El atacante envía paquetes ICMP echo request de forma continuada de tamaño grande (ping)
    - La víctima responde con ICMP echo reply (pong)
  - Sólo tiene buenos resultados si el atacante tiene un ancho de banda mucho mayor al ancho de banda de víctima

Ataques DDoS: Ejemplo #1

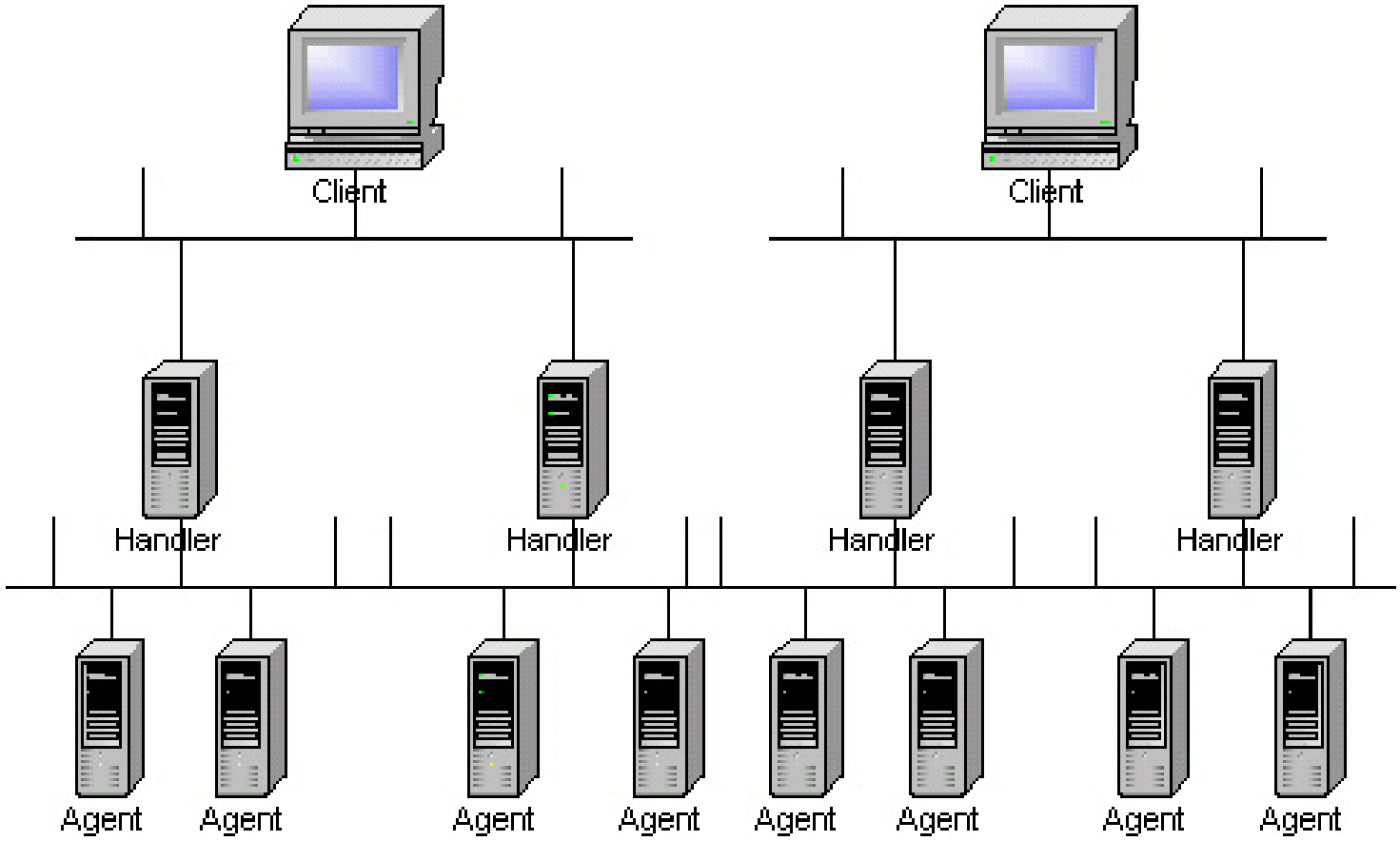
- El gusano Blaster
  - Aprovecha la vulnerabilidad de Windows XP, 2000, NT y 2003 en la RPC DCOM para instalarse en el sistema.
  - Tiene como segundo objetivo provocar un ataque DDoS a windowsupdate.com
    - De este modo, Microsoft no puede repartir el patch para protegerse ante el ataque
  - Intenta atacar direcciones IP aleatorias en busca de nuevas víctimas para infectar

Ataques DDoS: Ejemplo #2

- Ataque de un usuario a la red IRC-Hispano
  - Santiago G.A. 'Ronnie', de 26 años -> Autor del mayor ataque DDoS de España, llegando a afectar al 30% de los internautas españoles.
  - Realizó el ataque a modo de venganza (por estar baneado en un canal de la red).
  - Ataque masivo contra los nodos centrales de IRC Hispano iniciado en las fechas 24 y 25 de diciembre de 2002.
  - Utilizó un gusano llamado deloder

Notas generales

- En general, la estructura de un ataque DDoS es así:



Herramientas de denegación de servicio

- Facilitan el trabajo (El atacante puede ser un usuario inexperto)
- Algunas utilidades
  - Trinoo, sirve como modelo para el resto de herramientas
    - Encontrado por primera vez para Solaris 2.x, utilizando errores en RPC
  - TFN y TFN2K
    - Los primeros también se encontraron en Solaris 2.x
    - Se utilizan de los 3 tipos de ataques DDoS (ping, TCP y UDP)
  - Stacheldraht
    - Mejora Trinoo añadiendo encriptación a la comunicación
  - Otras herramientas
    - Shaft, Mstream, Wintrinoo, Trinity v2/Stacheldraht 1.666, etc.

Prevención

- Conviene tener el sistema siempre actualizado: así evitando al máximo la utilización por parte del atacante de bugs en servicios.
- Aumentando el nivel de seguridad: passwords seguras, instalando firewalls, desinstalando servicios sin utilizar, etc.
- Filtrando paquetes (Ingress filtering): Utilizando mecanismos en la red que impidan IP spoofing

Soluciones

- Solución compleja, puesto que es dificil detectar al atacante ya que el ataque no proviene de ningún lugar centralizado.
- Convendría un compromiso de toda la comunidad de Internet para tener los sistemas actualizados y seguros en la medida de lo posible.
- Identificar las máquinas Maestras (Handlers) para poder contactar con los ISP y buscar un remedio.
- Utilizar técnicas forenses para encontrar pistas
- El principal problema es net flood (inutilizar ancho de banda), puesto que syn flood ya no es problema.

Bibliografia

- http://www.rediris.es/rediris/boletin/57/enfoque2.html
- http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
- http://www.el-mundo.es/navegante/2003/08/29/seguridad/1062159692.html
- http://www.cisco.com/warp/public/707/newsflash.html
- http://www.argo.es/~jcea/artic/hispasec44.htm
- http://staff.washington.edu/dittrich/misc/ddos/