Denegación de Servicio (DoS)

Curso 2013/14

Grado Gestión Informática Empresarial

Asignatura Auditoría y Seguridad Informática

Profesores Alfredo Cuesta Infante
alfredo.cuesta@ajz.ucm.es
Alberto Herrán González
aherran@ajz.ucm.es

Contenidos

Denegación de Servicio (DoS)

Definición

La denegación de servicio, *Denial of Service*, o *DoS* es

- un ataque desde la red
- cuya acción impide el uso autorizado de redes, sistemas o aplicaciones
- mediante el agotamiento de sus recursos.

Clasificación mediante blanco del ataque

Blanco del ataque	**Recurso agotado**	**Ejemplo**
Redes	Ancho de banda	*ping flood*
Sistemas	Software que gestiona la red	*SYN spoofing*
Aplicaciones	Una aplicación de red concreta	Firefox

Clasificación mediante número de hosts empleados

- Desde un único host, directamente contra el atacado.
- Utilizando intermediarios:
  - Ataque distribuido, *DDoS* *Distributed DoS*.
  - Ataque por reflexión *Reflection attack*.
  - Ataque con amplificación *Amplifier attack*.

DoS – Ping flood

Ataque básico

Opción flood del ping de Linux: ejecutar `ping -f` contra una IP destino...PERO:

- La IP de la fuente (atacante) se identifica en el paquete ICMP. Por tanto:
- ↓ El atacante es descubierto, y lo que es peor...
- ↓ el eco de cada paquete vuelve hacia él, por lo que también se satura su equipo.
- El atacante intentará lanzar ping *imitando*, *spoofing*, otra dirección fuente.

Spoofing de la dirección fuente

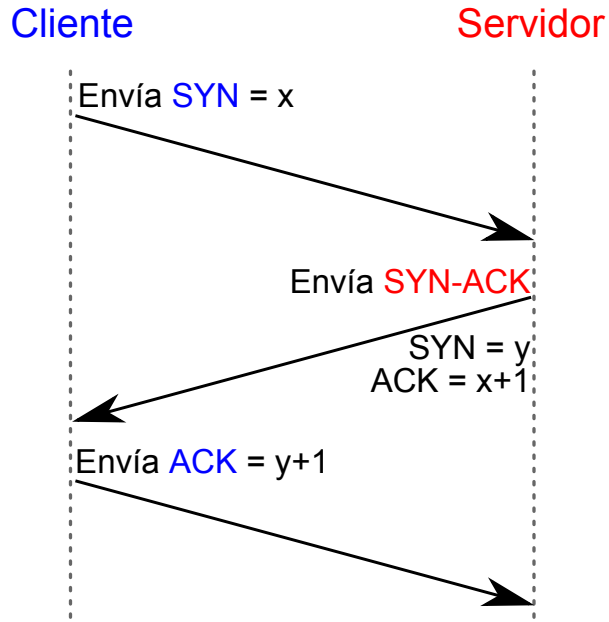
1. El atacante genera paquetes ICMP con diferentes direcciones fuente.
2. El atacado comienza a responder a cada paquete.
3. Cada paquete respondido llega al host *real*, aquel cuya IP había sido imitada.
4. Si existe, puesto que no ha enviado nada, envía un mensaje de error de vuelta. Si no existe entonces el paquete puede acabar volviendo a su origen.

Resultado:

- El atacante no se identifica,
- no satura su red,
- al atacar desde varias IP rebaja las posibilidades de ser rechazado por IDSs,
- y logra que el atacado tenga aún más tráfico que sólo generado por el ping.

DoS – SYN spoofing

Es un ataque contra los recursos del sistema, en concreto contra el código del SO que gestiona las peticiones de conexión TCP.



Protocolo SYN-ACK para conexiones TCP

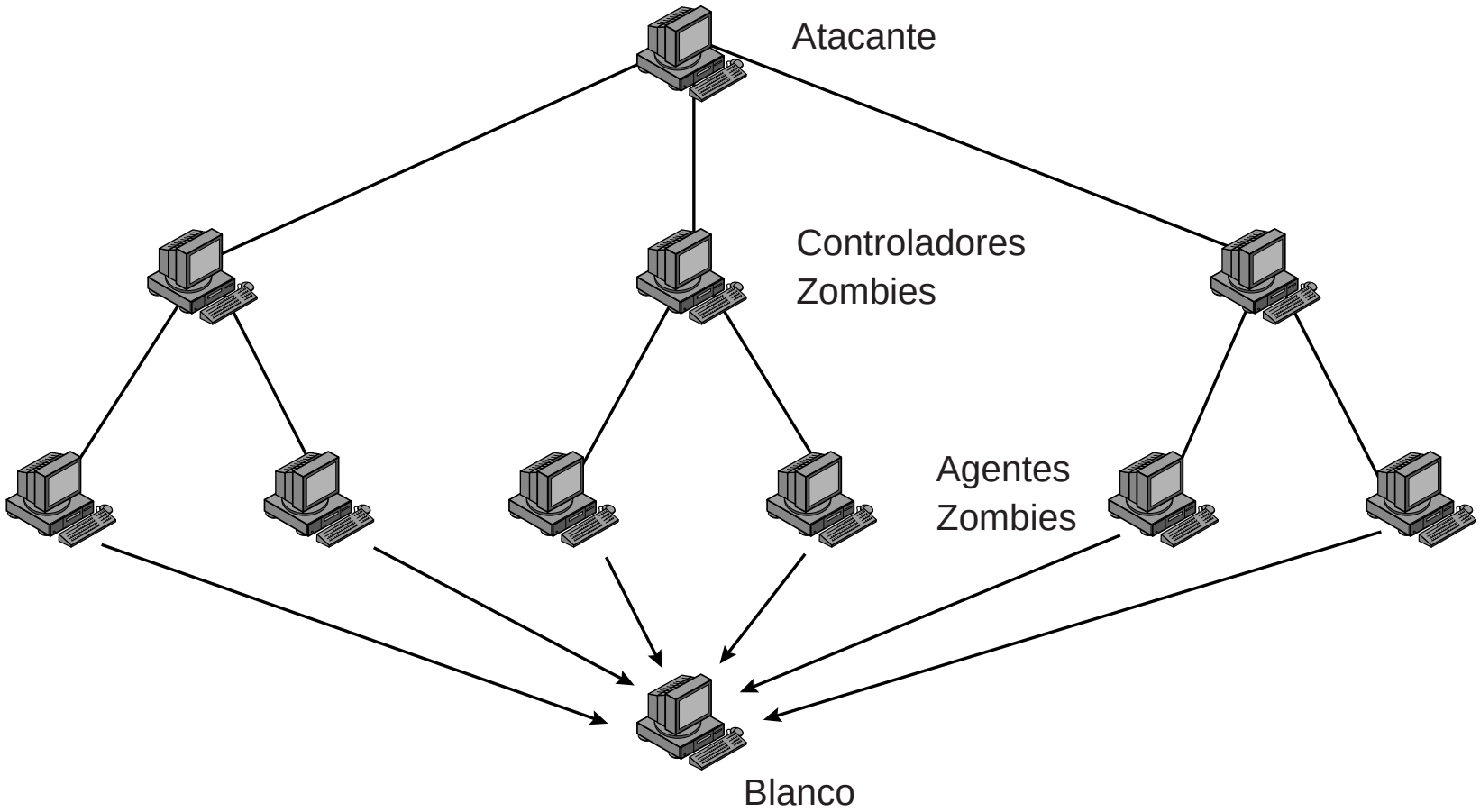
1. El cliente envía la señal SYN; una secuencia x.
   - **El servidor almacena los detalles de la petición en una tabla llamada 'TCP connections'**
2. El servidor devuelve la señal SYN y la ACK:
   ACK $= x + 1$
   SYN $=$ una secuencia diferente y
3. El cliente envía la señal ACK $= y + 1$.
4. El servidor marca la petición TCP como *establecida*.

Descripción del ataque

1. El atacante genera muchas señales SYN con direcciones fuente falsas.
2. El servidor almacena cada una de ellas en la tabla TCP connections y envía señales SYN-ACK a los hosts propietarios de dichas direcciones.
3. Como no recibe ningún ACK de vuelta la tabla del servidor se llena.
   Esta tabla no suele tener mucho espacio porque normalmente las peticiones se despachan rápidamente.

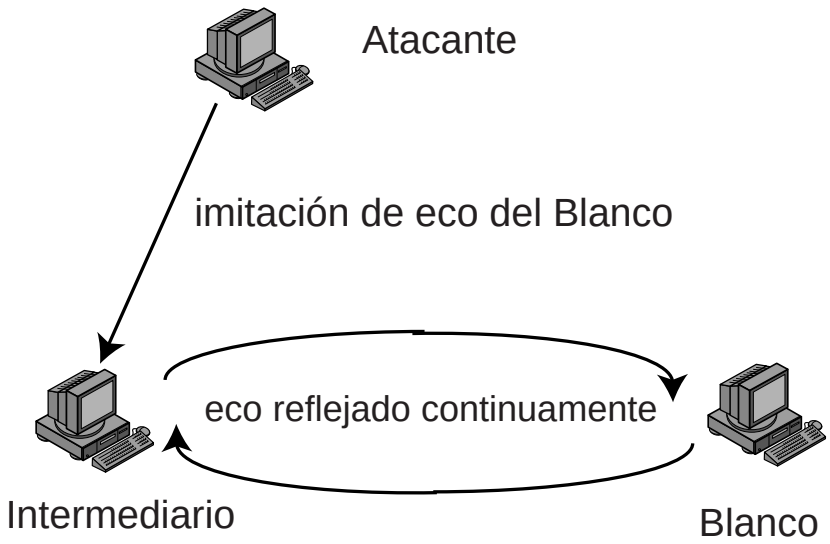
- ¡ Las peticiones legítimas se quedan sin atender !

DDoS



Zombi: Host en el que se detecta y aprovecha una brecha en su SO para instalar una puerta de atrás y controlar su comportamiento en remoto.

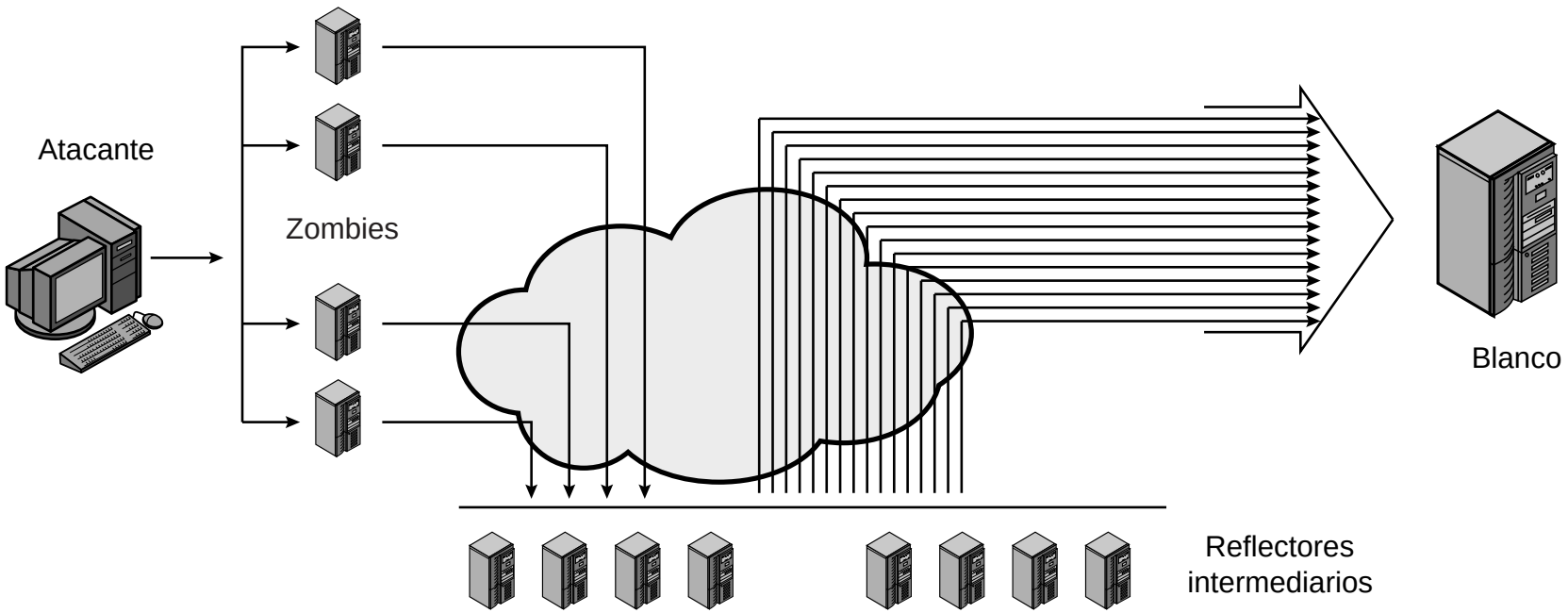
Ataque por reflexión



- En un DDoS los intermediarios son *zombies*; hosts que NO tienen un comportamiento normal.
- En un ataque por reflexión el intermediario no sufre ninguna modificación.
  De hecho se necesita que funcione normalmente para obtener el ataque deseado.

Ataque con amplificación

- Los paquetes ICMP se envian a una red usando la dirección IP de *broadcast* imitando la dirección fuente del host atacado.
- La dirección IP de broadcast es una dirección lógica a la cual todos los hosts de una red están conectados → lo que se envía a esa dirección es recibido por todos.
- Todos los hosts conectados a la red responden a la dirección de la fuente.

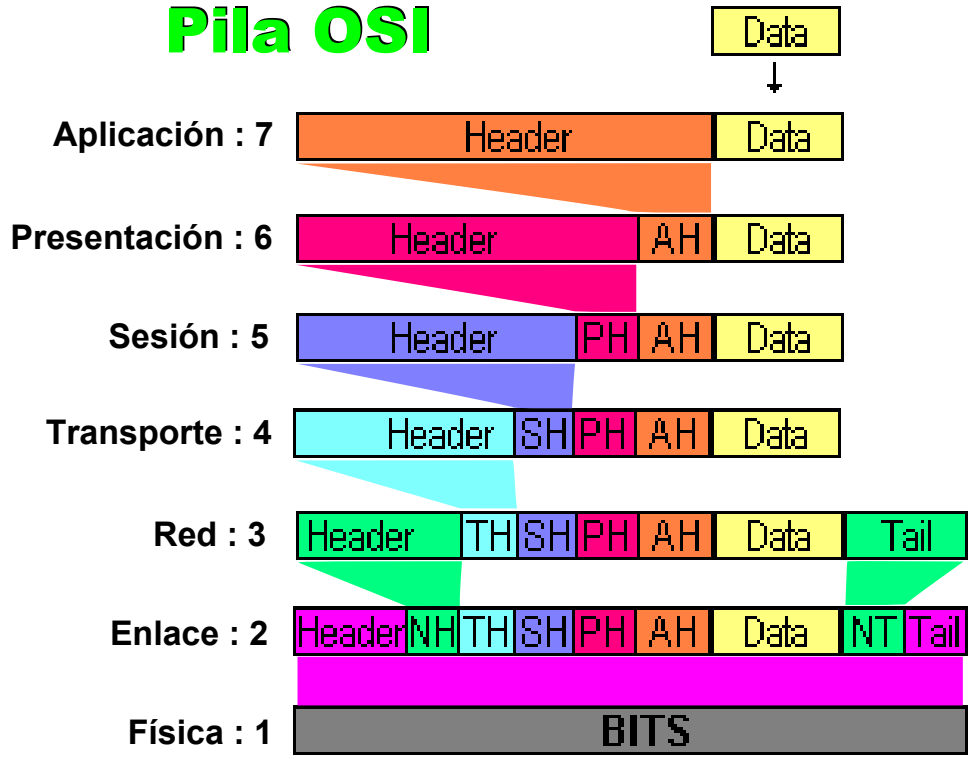


Ha habido dos programas famosos de este tipo: *Smurf* y *Fraggle*


Pero ¿cómo se hace *spoofing*?

Sockets

- En general un *socket* es un programa que facilita la comunicación entre otros dos.
- Los SO utilizan sockets para que las aplicaciones puedan comunicarse con el Kernel cuando se trata de enviar y recibir datos por un red.
- Estos sockets se programan siguiendo un protocolo de transporte: TCP, UDP ...



¿Se pueden inyectar/leer paquetes IP desde una aplicación directamente a la red? **SÍ**

Raw sockets

- *Raw Sockets* son programas para leer directamente de la tarjeta de red.
  Wireshark o cualquier otro *sniffer*, por ejemplo.
- Igualmente se puede crear un programa para componer a voluntad paquetes de red e inyectarlos directamente en la tarjeta.
  En YouTube hay varios tutoriales.

Defensas contra un DoS

- Es imposible impedir por completo un DoS.
  - Si el atacante es un usuario legítimo.
  - Si se produce un acceso legitimo pero con un gran demanda.
- La propuesta usual es tener exceso de ancho de banda y distrubuir servidores replicados. Resulta una solución muy costosa pero siempre será necesaria, al menos en parte.

En general hay 3 líneas de defensa:

1. **Prevención:** El filtrado de paquetes ICMP se debe implementar lo más cerca posible del atacante, y siempre antes o en el mismo punto de acceso del ISP.
   En caso de un SYN flood, un opción es utilizar SYN cookies*.
   Otra opción es tirar las peticiones TCP incompletas si se llena la tabla.
   Si es un ataque con amplificación, bloquear el uso de la IP de broadcast.
2. **Detección y Filtrado:** La detección y filtrado es una tarea de los sistemas IDS y cortafuegos instalados.
3. **Identificación y Trazado:** Al igual que antes, esta tarea se lleva a cabo por los IDS.

*** SYN Cookie** es información importante de la petición TCP que se codifica y se utiliza como secuencia en la señal SYN que envía el servidor.
El cliente envía el ACK = información codificada e incrementada. Cuando el servidor recibe el ACK reconstruye la información de la petición (que antes estaba en la tabla).
Este método se suele emplear sólo cuando la tabla llena.

ISP : Internet Service Provider Es la empresa que proporciona la conexión a Internet
ICMP : Internet Control Message Protocol Es el protocolo que utiliza el ping.

Otros ataques

en menor detalle

- Redes privadas virtuales
- Seguridad en redes WiFi
- Desbordamiento de memoria

★ Seguridad en aplicaciones web y bases de datos $\Longrightarrow$ *Última práctica*

Redes privadas virtuales (VPN)

Motivación

En la transparencia anterior el cortafuegos separa la DMZ de la intranet, pero...

- ¿qué ocurre si se algún empleado teletrabaja?,
- ¿si hay varias sucursales o franquicias se deben implementar clones de la intranet?

En ambos casos se recurre a Internet:

- En el primer caso es abusrdo pensar que la intranet llegará hasta el domicilio
- En el segundo sería muy costoso y fácil de cometer errores

Solución

- Para acceder por Internet hay que asegurar la confidencialidad, integridad y autenticación de las comunicaciones.
- Estas características las preserva la criptografía.
- Para una comunicación continuada se emplean redes privadas virtuales, *VPN* o *Virtual Private Networks*.

Seguridad en redes WiFi

Puntos débiles

1. Interferencias electromagnéticas.
2. Mayor potencia de emisión → mayor número de posibles atacantes.
3. Todo el mundo tiene acceso al medio
   → conviene cifrar las conexiones
   → el cifrado debe ser eficaz.
4. Es fácil inyectar y acceder al tráfico de la red.
5. Hay que proteger también los dispositivos cliente (ataque *Evil Twin*)

Defensas

1. Replicar puntos de acceso,
   aumentar potencia.
2. Reducir la potencia,
   contraseñas de al menos 20 caracteres.
3. Utilizar WPA-2.
   WEP se revienta en menos de 15 min!
4. Para redes personales
   → Filtrado por dirección MAC
   Para LAN de empresas
   → WIDS (*Wireless IDS*)
5. Borrar redes ocultas de la lista de redes preferidas.

Ataque de punto de acceso falso (*Evil Twin*)

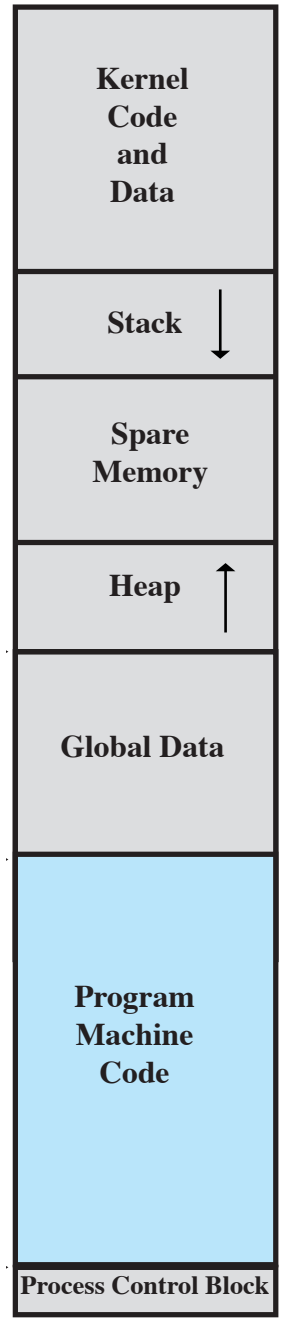
- Todos los clientes guardan una lista de las redes a las que conectarse cada vez que la detectan.
- Un atacante se podría hacer pasar por una de estas redes para acceder al dispositivo, pero... **¿Los clientes anuncian su lista de redes preferidas?**
- Hay un caso especial en el que sí. Cuando en la lista de redes preferidas hay una red *oculta* el cliente tiene que preguntar por ella!
- El *Evil Twin* se hace pasar por esta red.

Desbordamiento de memoria

Los ataques por desbordamiento de memoria consisten en:

- acceder a posiciones reservadas de memoria,
- escribiendo en ellas desbordando sus límites,
- de modo que se logre **reescribir el código fuente**,
- generalmente con otro código malicioso.

- Son ataques que precisan muchos conocimientos de informática
  Lenguajes de programación, compiladores, arquitectura y estructura de los procesadores...
- Las zonas protegidas son:
  - Pila, *Stack*
  - Montón, *Heap*
  - Datos globales, *Global data*



Defensas

- **Al compilar**
  - Marcar las opciones de verificación y protección de escritura.
  - Usar lenguajes de programación de alto-nivel.
  - Escribir los programas con políticas de *código seguro*.
- **Al ejecutar**
  - Aleatorizar la asignación de memoria
  - Impedir ejecución de código cuando este se encuentra almacenado en zonas reservadas de memoria