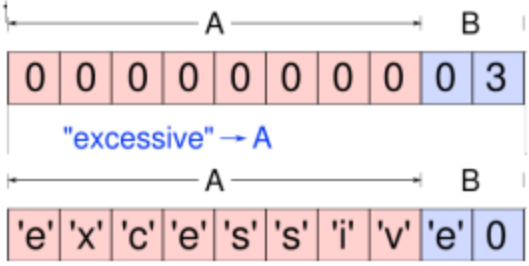
- **Desbordamiento**
  - *Buffer Overflow*
  - Un programa no gestiona adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada para los mismos (habitualmente un **buffer**)
    - Datos sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original
  - En las arquitecturas actuales no hay separación entre memoria de datos y programa
    - La sobreescritura en la memoria de programa podría ocasionar una alteración del



- **Desbordamiento de Montículo**
  - *Heap Overflow*
  - **Montículo:** usada para ubicar la memoria dinámica en tiempo de ejecución
    - No hay direcciones de retorno como en pila
  - Ataque consiste en sobrescribir ciertas variables que contienen direcciones o estructuras que a su vez contienen direcciones
    - Apuntar al código del atacante
  - Ejemplo: iOS Jailbreaking
  - Misma prevención que en pila

- **Lógica de programa**
  - *Off-by-One Error*
  - El programador no considera todos los casos en la lógica de su programa
  - Ejemplo: OpenSSH (2002)

```
if (id < 0 || id > channels_alloc)
```

    - ¿Qué ocurre si id = channels_alloc?

- **Validación de entrada de datos**
  - *Input Validation Attack*
  - El programador no revisa convenientemente los datos proporcionados por el usuario y los pasa a la aplicación
  - Resultados:
    - Denegación de servicio por datos excesivos
    - Ejecución de comandos arbitrarios

- **Validación de entrada de datos**
  - Ejemplo: IIS4 (*Canonicalization Attack*)
    - Bloqueado por servidor:

```
http://victima.com/scripts/../../../../winnt/system32/cmd.exe?/c+dir
```

    - No bloqueado por servidor:

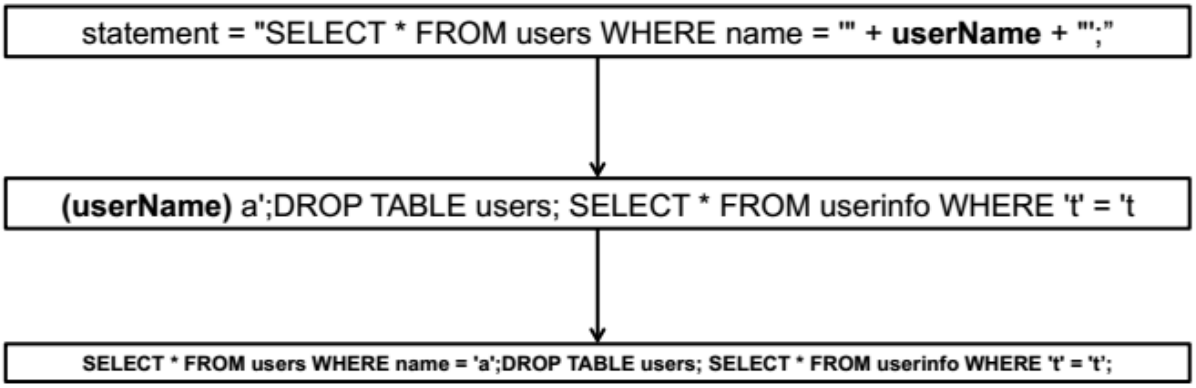
```
http://victima.com/scripts/..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir
```

- **Troyano**
  - Modelo cliente-servidor (el troyano es el servidor)
    - **Conexión directa:** cliente se conecta al servidor
      - Necesario conocer la IP de la máquina infectada
      - La conexión puede ser retenida por el cortafuegos
    - **Conexión inversa:** servidor se conecta al cliente
      - Necesario configurar la IP del cliente en el servidor antes de la infección
        - Se puede utilizar un servidor intermedio (IP fija, anonimato)
      - Es menos probable que la conexión sea retenida por el cortafuegos

- **Rootkit**
  - Conjunto de programas (*kit*) que permiten el acceso continuo y oculto a un atacante
    - Puerta trasera
    - Módulo de ocultación de huellas (puede implicar modificación de herramientas básicas del sistema)
  - **Diferencia con Troyano:** el atacante lo despliega desde el interior del sistema y con privilegios de Administrado (*root*)

- **Gusano**
  - Gusano ILoveYou (2000)
    - Creado por Onel de Guzmán (Filipinas)
    - Escrito en VBScript y aprovechaba
      - Ingeniería Social
      - Microsoft Outlook
    - Varias mutaciones
    - Afectó a 50.000 ordenadores durante días
      - CIA, Pentágono, Parlamento Británico
      - 80% empresas españolas
      - Pérdidas totales de $8.700 millones

- **Inyección código SQL**
  - **Caracteres incorrectamente delimitados (“escapados”)**
    - Se pueden añadir comentarios para bloquear el resto de sentencias SQL (--,({,/*)

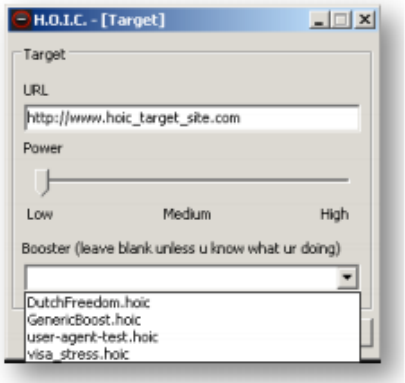


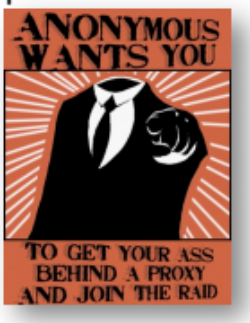
DDoS

- **LOIC**
  - Low Orbit Ion Cannon
  - Creado por Praetox Technologies
  - TCP flood y UDP flood
  - Botnet voluntario
    - Los usuarios legítimos ejecutan el programa
  - Incidentes Anonymous:
    - Project Chanology: Iglesia de la Cienciología (2008)
    - Operation Payback: instituciones que bloquearon a Wikileaks (2010)
    - Operation Megaupload: instituciones que cerraron Megaupload (2012)
  - Nuevas versiones
    - JS LOIC (Javascript)
    - Low Orbit Web Cannon

DDoS

- **HOIC**
  - High Orbit Ion Cannon
  - Lanzado en 2012 por Anonymous
  - Ataques se limitan a HTTP
  - Uso de scripts (boosters) con patrones de ataque
  - Técnicas de aleatorización del ataque para evitar la detección





Honeypots

- **Puro**
  - Sistema de producción completo como cebo
  - Monitorización en el enlace con la red

- **Alta Interacción**
  - Gran cantidad de servicios instalados
  - Monitorización pasa más desapercibida
  - Sistemas de Investigación
- **Baja Interacción**
  - Escasos servicios instalados (los más comúnmente atacados)
  - Sistemas de producción

Wi-Fi

- **“Descubrimiento y revelación de secretos”**
  - Delito tipificado por código penal
    - Romper claves Wi-Fi
    - Escuchar tráfico de redes abiertas
  - **Penas:**
    - Cárcel: 1 a 4 años
    - Multas: 12 a 24 meses