fs2004
II Foro de Seguridad RedIRIS

Módulo Técnico

Carles Fragoso i Mariscal
Centre de Supercomputació de Catalunya (CESCA)

CENTRE DE SUPERCOMPUTACIÓ DE CATALUNYA
CESCA

red.es

RedIRIS

Módulo Técnico

- Agenda:
  - 25 de Marzo del 2004: 12:00-14:00 y 15:30-16:30 (3 horas).
- Ponente:
  - Carles Fragoso i Mariscal (Centre de Supercomputació de Catalunya).
- Descripción:
  - *"Este módulo pretende proporcionar aquellos conocimientos técnicos necesarios para poder afrontar la seguridad en la operativa diaria en nuestras infraestructuras de sistemas y comunicaciones.*
    El conocimiento del mundo 'underground' y sus motivaciones da paso a conocer el ciclo de vida de una intrusión y su correspondiente de detección y reacción. Todo ello con una visión práctica y ejemplos reales de incidentes en la comunidad académica."

Objetivos

- Adquirir conocimientos técnicos necesarios y terminología asociada para el tratamiento de incidentes de seguridad informática.
- Pasear por la cultura "*underground*" para conocer cuáles son los perfiles existentes de intrusos con sus principales motivaciones y los tipos de código maligno.
- Presentar algunas de las herramientas y técnicas comúnmente utilizadas por los intrusos y por los técnicos en seguridad informática.
- Estudiar las diferentes etapas del ciclo de vida de las intrusiones y la correspondiente de detección/reacción frente a estas.

Agenda

- Presentación.
- Introducción.
- Mundo "*underground*".
- Código malicioso: *"malware"*.
- Ciclo de vida de una intrusión.
- Ciclo de vida de la respuesta a incidentes.

Presentación

Carles Fragoso i Mariscal

- Técnico de redes, sistemas y seguridad del departamento de Comunicaciones y Operaciones del Centre de Supercomputació de Catalunya (CESCA): gestión de Anella Científica, alojamiento del nodo de RedIRIS en Catalunya, CATNIX y servicios Internet (news, proxy-caché, mail, DNS, acceso remoto, multicast, videoconferencia, VoIP, IPv6, etc).
- Ingeniero Técnico en Informática de Sistemas (EUIS/UAB).
- Máster en Redes y Servicios de Telecomunicaciones (MXST, URL/LaSalle).
- Profesor del Máster en Tecnologías de la Seguridad Informática (MTSI, esCERT-UPC/ICT).
- Cisco Certified Networking Associate (CCNA 640-607 #10538607).
- Cisco Certified Networking Professional (CCNP 640-901, 640-821, 640-811).
- SANS Institute GIAC Security Essentials Certified (GSEC #2852).
- En curso: Cisco CCNP (640-831), SANS GCIA/GSNA.

Centre de Supercomputació de Catalunya (CESCA)

Consell de Govern

President
Rafael Español

Vicepresident
Carles Solà

Secretari
Enric Banda

Vocals
Marta Aymerich
Oriol Ferran
Ramon Vilaseca
M. Teresa Costa
Joan Tugores
Lluís Ferrer
Josep Ferrer
M. Rosa Virós
Joan Batlle
Lluís Arola
Joan Viñas
Gabriel Ferraté
Lluís Calvo

28-01-04

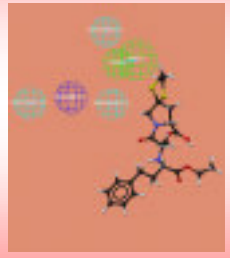
CENTRE DE SUPERCOMPUTACIÓ DE CATALUNYA
CESCA

Nuestros Servicios

+8,00

CAP
SED
ENTS +1
AGI² +3
TDX +1

SCF



+2 +4

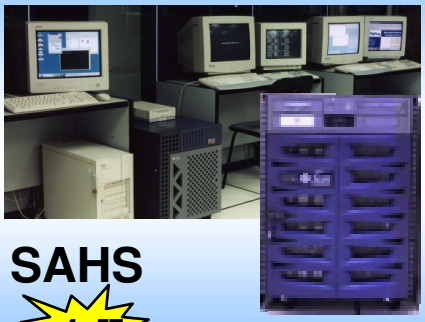
SxAC:
- DNS
- *Multicast*
- *News*
- *proxy-cache*
- *ftp-mirror*
- SAR
- SAD
- S24x7
- SCD
- SAV
- VIA
- SEG NUEVO

CESCA

ANT
JOCS
TAC
TSIUC

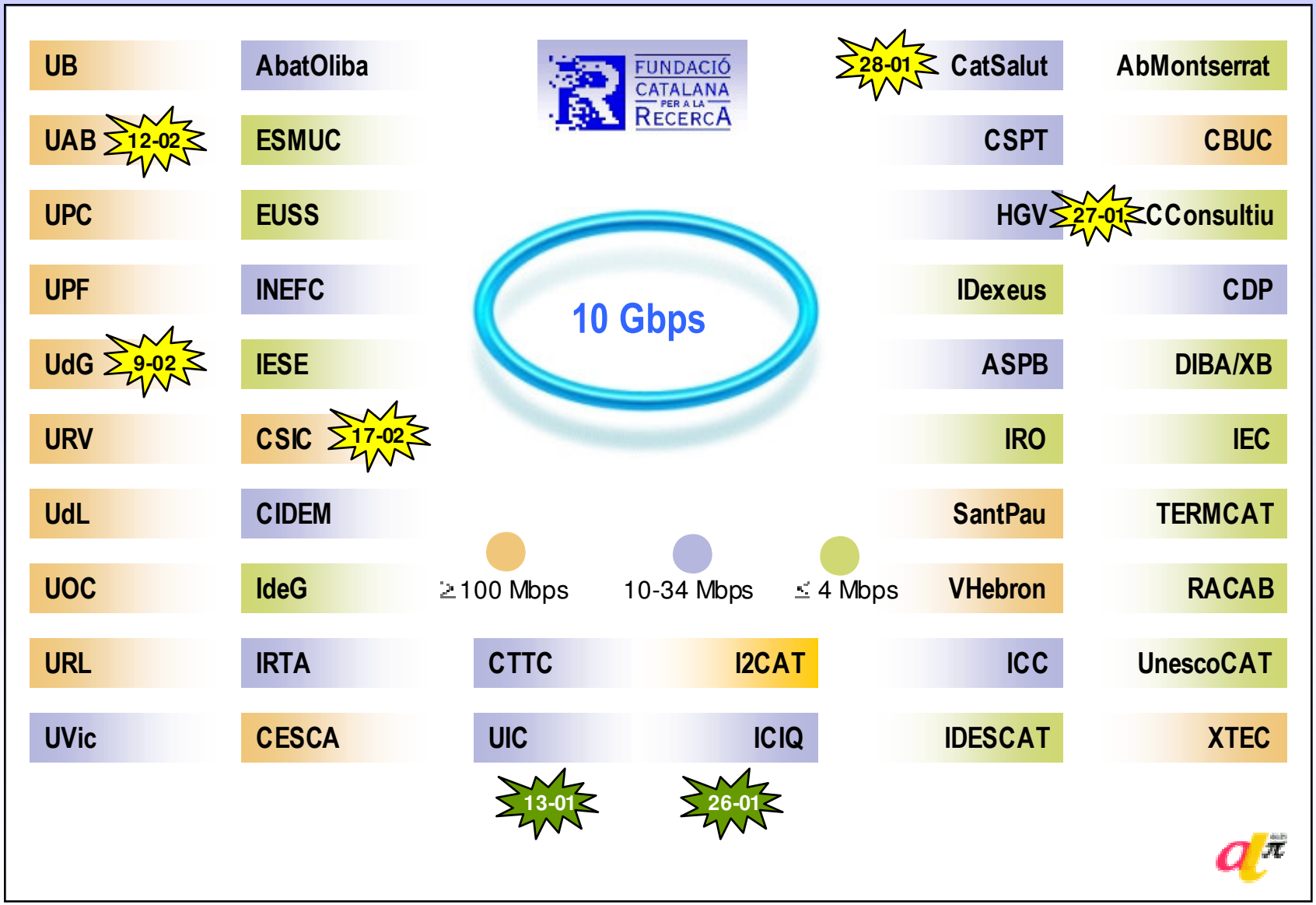
CATNIX +5 +2

RedIRIS
INTERNET2
GÉANT
6BONE



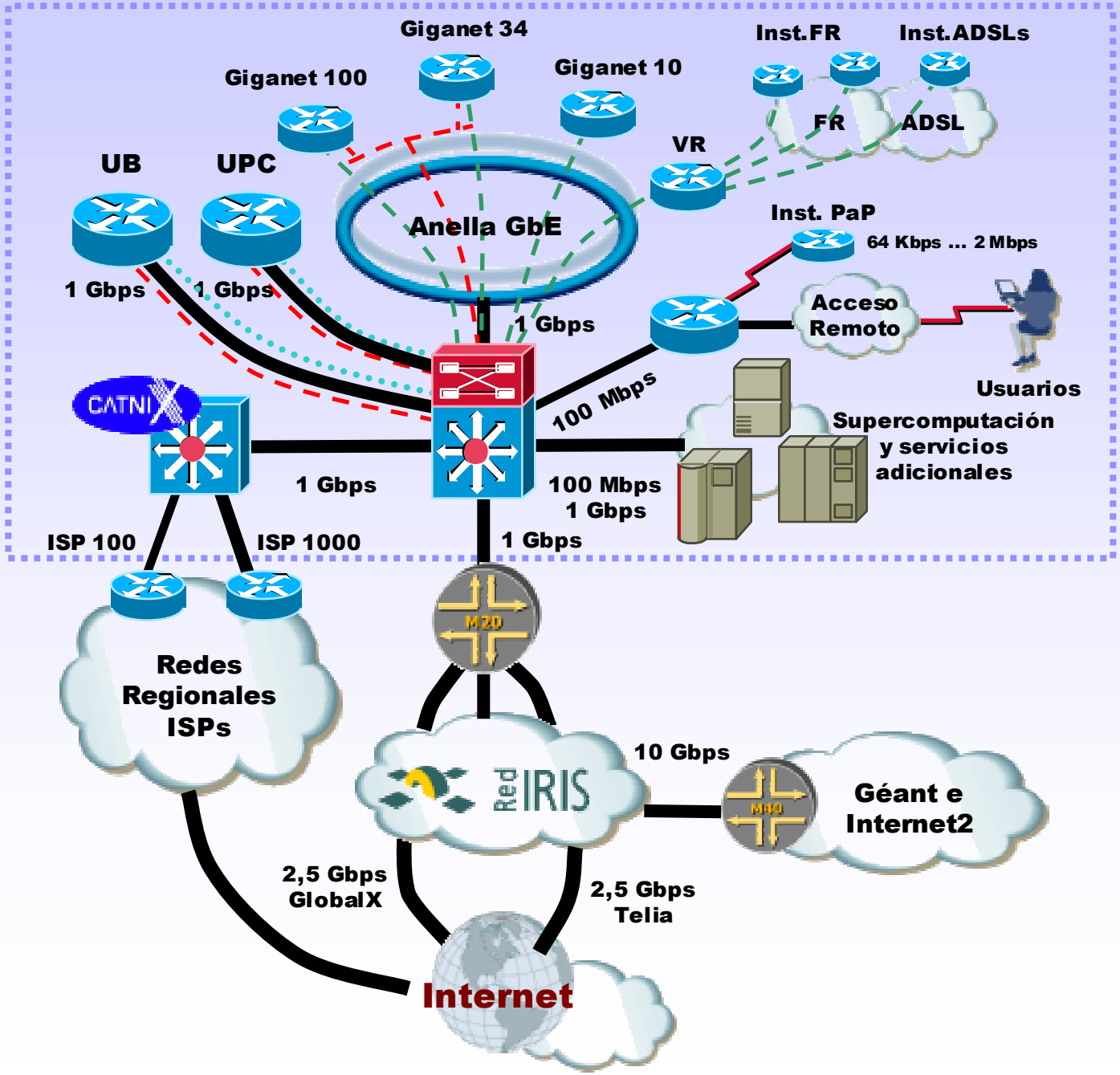
SAHS +4+57

La Anella Científica



CENTRE DE SUPERCOMPUTACIÓ DE CATALUNYA
CESCA

Topología Anella-GbE



SxAC – Servicios de Seguridad (SEG)

- Equip de Resposta a Incidents per a l'Anella Científica (ERIAC).
  - Coordinación de incidentes de seguridad para AC y CATNIX.
  - Notificación de alertas críticas de seguridad.
  - Soporte técnico en tecnologías de la seguridad informática.
- Grup de Treball en SEGuretat Informática (GTSEG).
  - Iniciativas y prácticas comunes en consenso.
- Uso de recursos especializados:
  - Módulo de Análisis de Red (Cisco NAM-2).
  - Módulo de Detección de Intrusos (Cisco IDSM-1)
- Proyectos:
  - Monitorización y análisis de tráfico (SMARTxAC).
  - Base de datos centralizada de gestión de incidentes (RT-IR).

Introducción

Sabias palabras de un padre...

*"The **wonderful** thing about the Internet is that you are connected to everyone else"*

*"The **terrible** thing about the Internet is that you are connected to everyone else"*

- Vinton Cerf

Reflexiones iniciales (I)

- La seguridad se ha convertido en un punto clave debido a la evolución de las tecnologías de la información y las comunicaciones.
- El modelo de seguridad inicial de la Internet basada en la confianza de su reducido número de miembros ha dejado de ser válido debido en gran parte a su penetración social.
- Existe una necesidad de redefinir el modelo y estrategia de seguridad implicando a todos los agentes (instituciones, proveedores de red y servicios, fabricantes, etc.) para actuar de forma coordinada y conjunta.

Reflexiones iniciales (II)

- El mundo electrónico no es tan diferente del mundo real aunque sí más desconocido al escapar del control de nuestros “sentidos”.
- En toda comunidad existen individuos malintencionados con diferentes intenciones/motivaciones:
  - Lucrativas, personales, ideológicas, etc.
- En las tecnologías de la información nuestros activos o bienes son:
  - Información, sistemas, infraestructura de comunicaciones y las propias personas.
- La supervivencia se basa en utilizar nuestros recursos en una lucha constante de adaptación frente a la sofisticación de esos individuos malintencionados y sus medios.

Mundo "*underground*"

Mundo *"underground"*

- Tipología de intruso.
- Motivaciones.
- Sofisticación vs Conocimiento.
- Vida social.
- Fuentes de información.
- Tendencias:

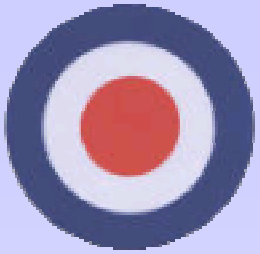
Conoce a tu enemigo (KYE)

"Know Your Enemy and know yourself; in a hundred battles, you will never be defeated. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are sure to be defeated in every battle"

- Sun Tzu (The Art of War)

"Si no puedes con tus enemigos, aprende de ellos" ☺

- Carlesun Fragotzu

¿Quién es  bjetivo?

- Dependiendo de los objetivos del intruso se realiza un proceso selectivo o no de los posibles objetivos.
- Los intrusos siguen la famosa *"ley del mínimo esfuerzo"* donde el objetivo será habitualmente aquel aparentemente más fácil de comprometer.
- El intruso puede seguir un proceso de tipo:
  - Específico: objetivo definido.
  - Subconjuntos: grupo de interés.
  - Aleatorio: ir de pesca.

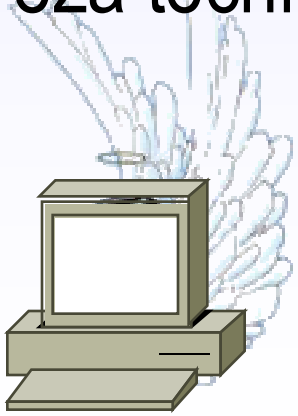
- Las instituciones pertenecientes a redes académicas y de investigación suelen ser un subconjunto bastante apetitoso al ser más abiertas y gozar de anchos de banda potentes.

"Underground"

- Utilizaremos "*underground*" como término genérico para englobar:
  - Miembros pertenecientes a la comunidad de intrusos.
  - Conjunto de herramientas utilizadas para ejercer actividades malignas (compromiso, infecciones, abuso de recursos, etc.).
  - Técnicas y estrategias de intrusión.
- El fenómeno "*hacker*" es quizás el más conocido aunque no el único (Ej."*warez scene*").
- Hay que tener en cuenta que esta comunidad dispone también de sus propias jergas.
  - Ej: *Phreax0ring* (*art of scaring*).
- Referencia: [UDG] Nomenclatura / Jerga.

¡Identifíquese Sr. Intruso!

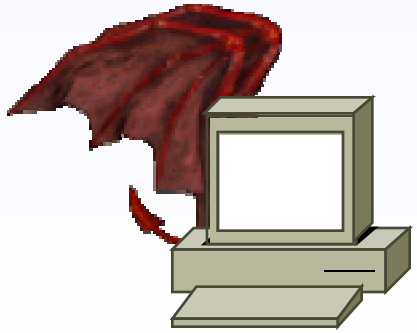
- Aunque el término "*hacker*" goza habitualmente de una connotación negativa, su origen pretende representar aquellos tecnófilos amantes del estudio de la seguridad informática.
- Existen múltiples definiciones y clasificaciones basadas en sus intenciones/motivaciones y nivel de destreza técnica.



Hacker **Cracker**

Whitehat **Blackhat**

Grayhat



Motivaciones

- Las intenciones y motivaciones de los intrusos/atacantes en tecnologías de la información son realmente variadas:
  - Lucrativas
    - *Robo y venta de información.*
    - *Uso de recursos ajenos con fines económicos (Ej. spam).*
  - Entretenimiento/vida social
    - *Aumento del ego/diversión.*
    - *Piratería (warez).*
    - *Pornografía (porn).*
    - *Juegos.*
  - Ideológicas
    - *Apología del terrorismo.*
    - *Políticas o religiosas.*

Cyberpiltrafillas™ ☺

(“*script kiddies*” o “*hacker wanabees*”)

- Destreza técnica: baja o nula.
- Motivaciones: entretenimiento/vida social.
- Edad: 10 años en adelante.
- Técnica: uso de programas o “*scripts*” desarrollados por verdaderos “*hackers*”.
- Conducta: sin código ético.

Hacker ☺

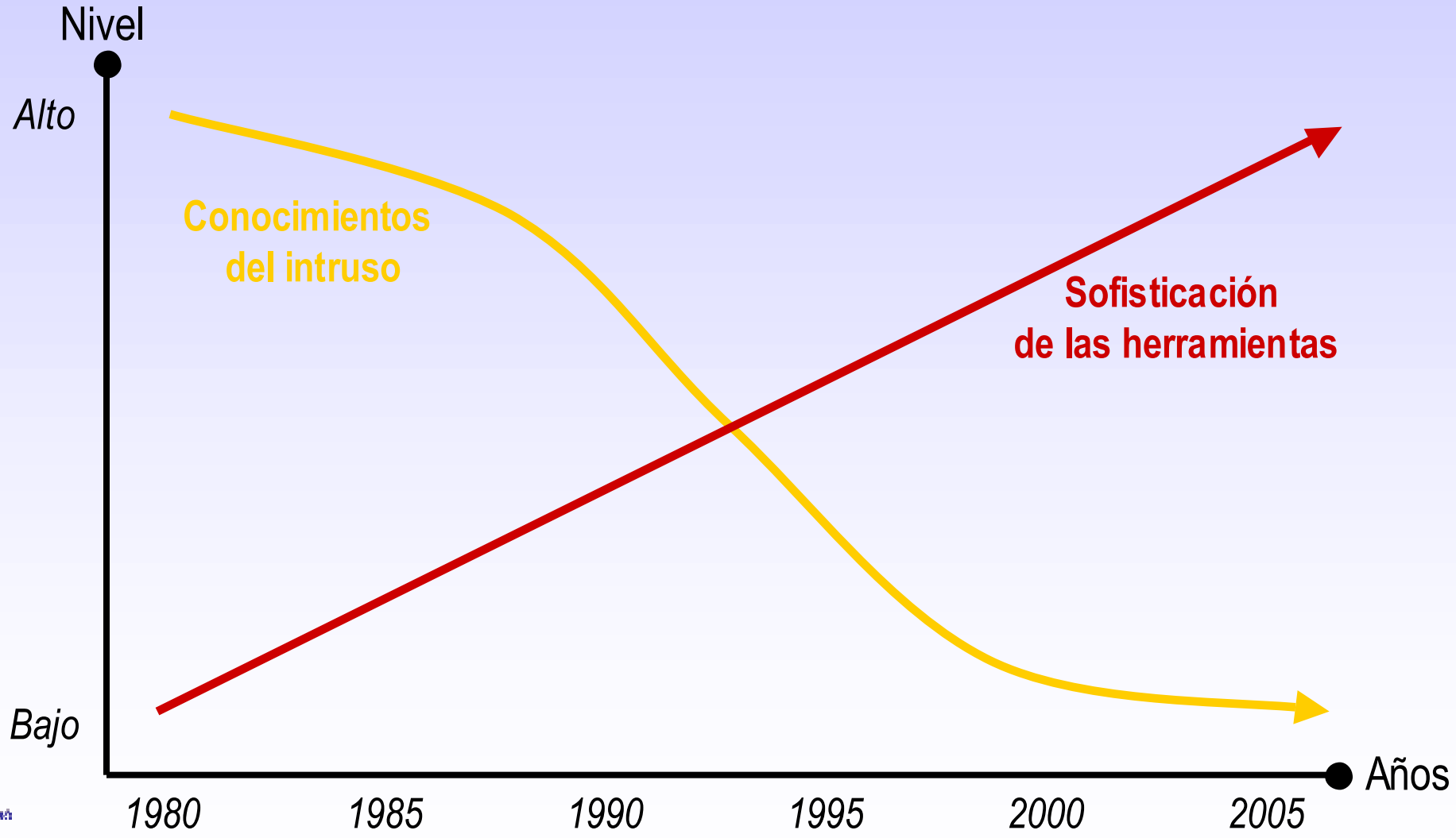
(i am l33t hax0r, ph33r my skl11z!!!)

- Destreza técnica: alta o muy alta.
- Motivaciones: aprendizaje y/o vida social (fama).
- Edad: 20 años en adelante.
- Técnica: código propio para aprovechar debilidades.
- Conducta: código ético donde se evita causar daño.

Cacharrería *"Hacker"*

- Existen mil y una herramientas disponibles en la red susceptibles de ser utilizadas intrusos informáticos:
  - *binder, cracker, flooder, mail bomber, nuker, card tool, password cracker, port scanner, sniffer, spoofer, trojan, virus, war dialer, log zapper / wipper, keyloggers, backdoor, vulnerabilities scanner, wardialers, rootkit, bouncer, exploit, worm, etc.*

Conocimientos vs Sofisticación



Intrusos vs Guardianes: Un paso adelante

- Según las estadísticas de los más prestigiosos *CSIRTs*, el volumen de incidentes de seguridad crece exponencialmente.
- Las herramientas disponibles son cada vez más sofisticadas, más numerosas y sobretodo más fáciles de utilizar.
- Las tecnologías, herramientas y cultura de la seguridad informática no ha avanzado a la misma velocidad.
- Técnicamente y legalmente gran parte de los delitos no llegan a ser imputados.

- Por ello se considera, que los *"hackers"* están actualmente un paso por delante de los que intentan defenderse de ellos.

Internet los cría y ellos se juntan

- En similitud con el mundo real, estos individuos también tienen vida social en la red donde se relacionan, intercambian experiencias:
  - Chat (IRC)/Mensajería instantánea.
  - Grupos de noticias.
  - Web loggers/Foros de discusión.
  - Correo electrónico/Listas de correo.
  - eZines/Concursos de Hacking.
- Algunos de estos puntos de encuentro pueden ser incluso los propios campos de batalla.
- También existen encuentros presenciales:
  - Convenciones/Fiestas (Con's/LAN Parties)

"Underground": fuentes de información

- Convenciones (*"Con's"*)
  - Defcon, BlackHat, CanSecWest, NoConName, etc.
- Fiestas (*"LAN Parties"*)
  - Campus Party, Linux Party, Fiberparty, etc.
- Chat (IRC)
  - Red Hispano, Undernet, EFNet, DALnet, etc.
- Listas de Correo
  - Hacking List, HackIndex, Pen-Testing, etc.
- Grupos de noticias
  - es.comp.hackers, entre otros.
- Web Loggers
  - Slashdot, Barrapunto, LinuxSecurity, etc.
- Concursos: Hackerslab, Boinas Negras, etc.

Internet Relay Chat (IRC)

- Red de servidores y clientes interconectados donde se accede a grupos de discusión (canales).
- Mecanismo preferido de contacto de la comunidad internauta: vida social, intercambio de conocimiento, herramientas, etc.
- Software Cliente:
  - mIRC, bitchX, ircii, irsii
- Software Servidor:
  - Unreal, UltimateIRC, ircd, Hybrid6/PTLink6.
- Referencias: [IRC]

La historia se repite: de *"Wardialers"* a *"Wardrivers"*

- Los módems como mecanismo de acceso remoto han sido tradicionalmente una puerta trasera sin demasiado control.
- Las redes inalámbricas WiFi se están convirtiendo en un 'deja-vu' del fenómeno *"wardialing"*.
- *"Wardialing"*
  - Popularizado en 1983 (película "Juegos de Guerra").
  - Proceso de escaneo telefónico en búsqueda de módems.
- *"Wardriving"*
  - Popularizado en 2001-2002 (fenómeno Antena Pringles™).
  - Proceso de escaneo en búsqueda de redes inalámbricas.

Guerras chateras: *"IRC Wars"*

- Los usuarios acceden a los canales e intentan conseguir privilegios de operador de canal para así poder tener el control del resto de individuos (*kick, ban, restricted channel*).
- Redes IRC:
  - Efnet, Undernet IRCNet DALnet QuakeNet IRC-Hispano
- Canales:
  - XDCC, ISO, WAREZ, MOVIEZ, DIVX, 0Day, PORN, MP3, VCD, DVD, Linux, BSD, etc.
- Uso habitual de herramientas de denegación de servicio, scripts para controlar clientes vulnerables, etc.
- El buen funcionamiento de la red es controlado por los administradores del servidor IRC (IRCops).
- Referencias: [IRC]

Piratería: *"Warez Scene"*

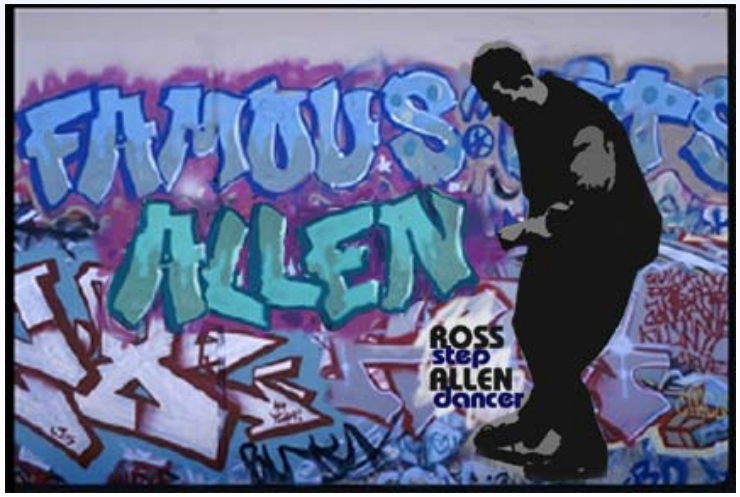
- Grupos cuyo objetivo es la distribución ilegal de programas, películas, música, juegos, etc.
- Utilizan prácticamente todos los mecanismos de transferencia de ficheros existentes:
  - FTP, Web, P2P, IRC XDCC, etc.
- Intentan distribuir sus contenidos al mayor número de personas posible en el menor tiempo y para ello necesitan utilizar recursos de espacio en disco/ancho de banda ajenos.
- Existen diferentes roles dependiendo de sus funciones:
  - Leechers / Lammers, Scanners, Uploaders, Pubers, Rooters, etc.

Denegación de Servicio: *"DoS'ers"*

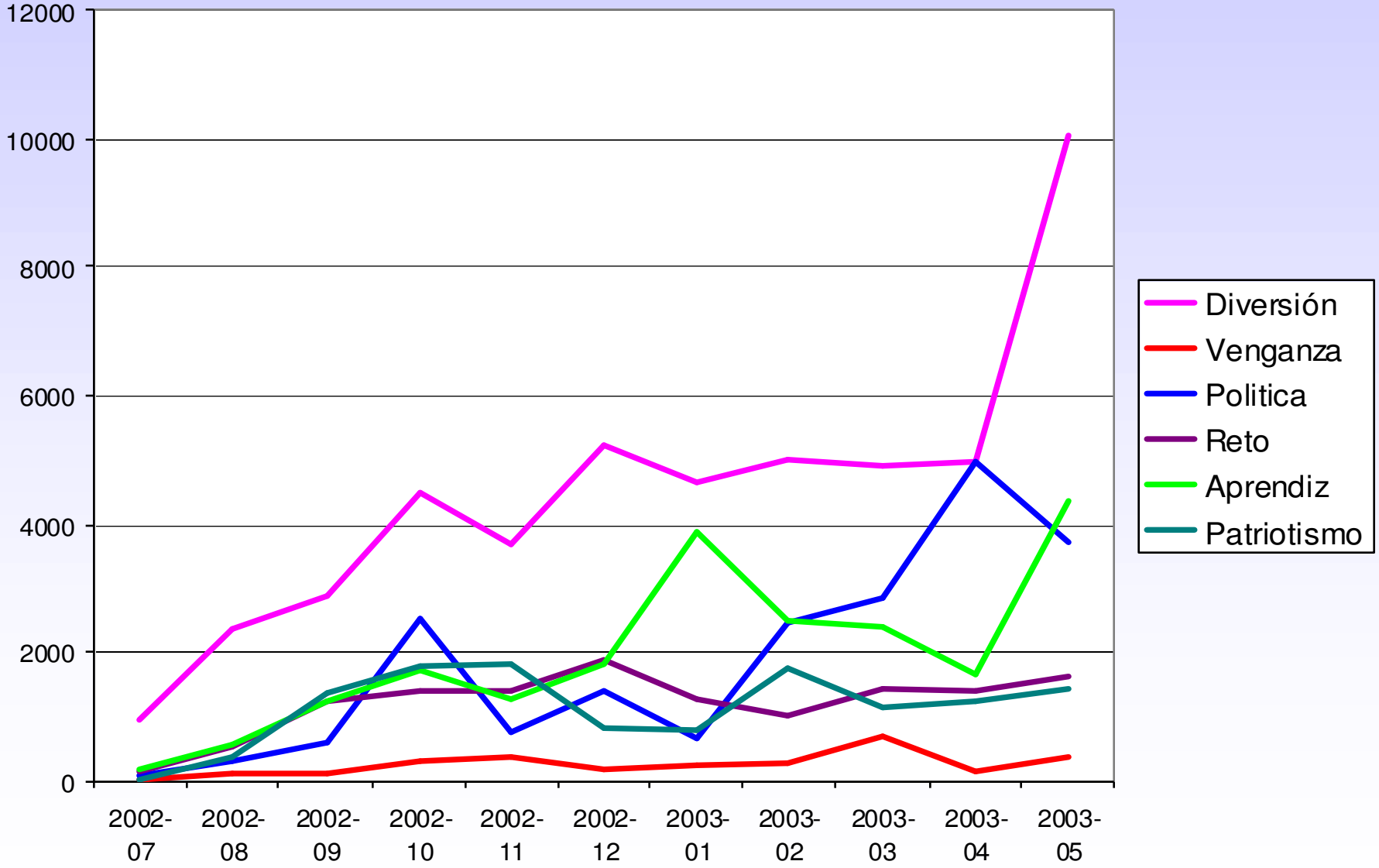
- Existen grupos de *"hackers"* cuyo objetivo es atentar contra la disponibilidad de los sistemas e infraestructura.
- Acaparan un gran número de sistemas comprometidos, habitualmente centenares, para conseguir un ancho de banda suficientemente destructivo.
- Ejercen el control de los sistemas mediante agentes y controladores de agentes para llevar a cabo los ataques de forma controlada y sincronizada:
  - Ej: Ataques entre bandas, ataques a gigantes de la red (Microsoft, Amazon, etc).

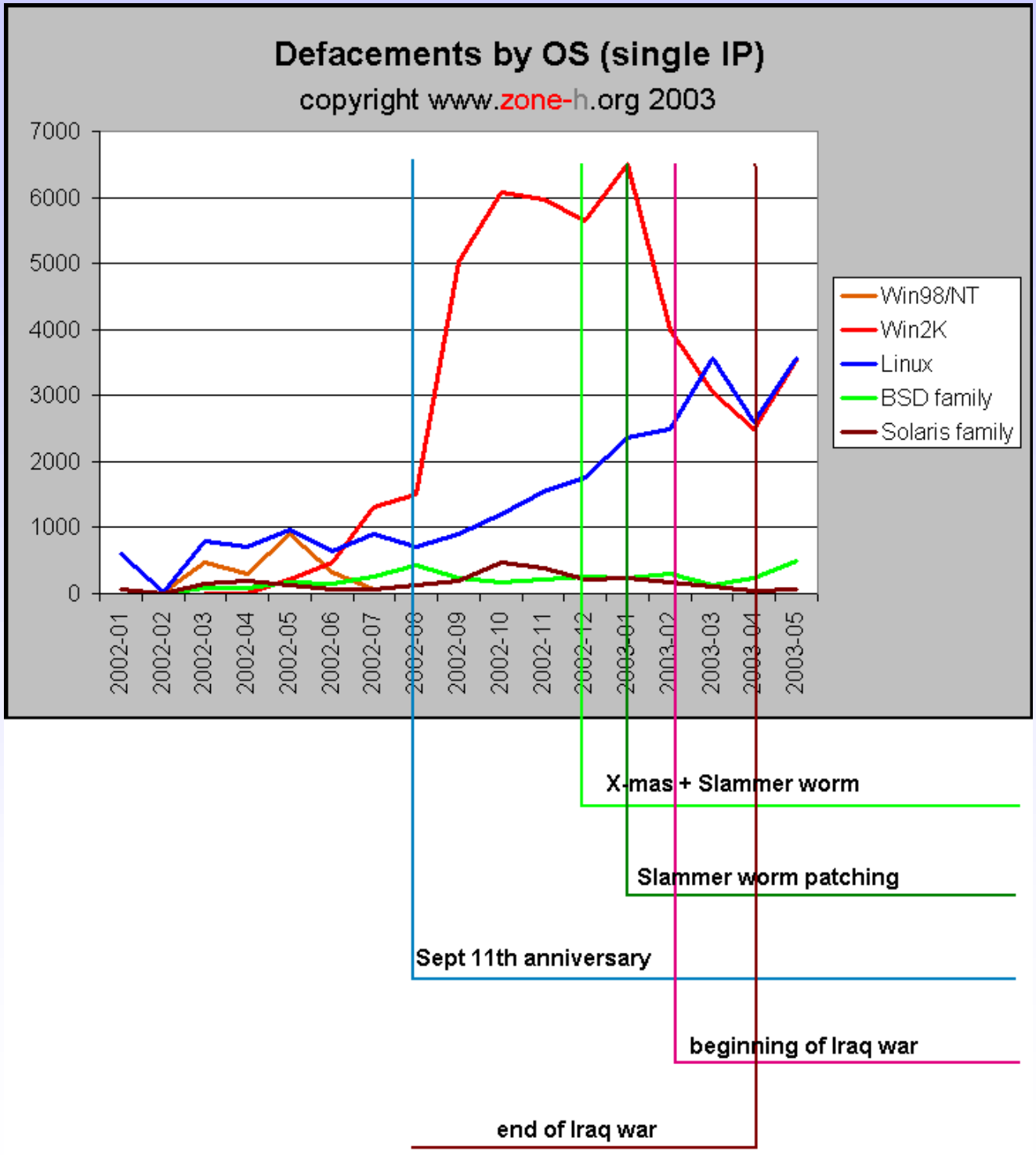
Graffiti en la red: *"Defacing"*

- Fenómeno similar al "Graffiti" que consiste en dejar huella en el máximo número de páginas web de entrada de sitios web.
- Suelen agruparse en bandas que luchan por tener más prestigio y estar más arriba en las listas *Top 10*.
- Habitualmente eligen la vulnerabilidad para luego escanear en búsqueda de servidores vulnerables a esta.
- Referencias:
  - [DFC] Zone-h, Alldas, etc.



"*Defacement*": motivaciones




Defacements by OS (single IP)
copyright www.zone-h.org 2003
7000
6000
5000
4000
3000
2000
1000
0
2002-01
2002-02
2002-03
2002-04
2002-05
2002-06
2002-07
2002-08
2002-09
2002-10
2002-11
2002-12
2003-01
2003-02
2003-03
2003-04
2003-05
Win98/NT
Win2K
Linux
BSD family
Solaris family
X-mas + Slammer worm
Slammer worm patching
Sept 11th anniversary
beginning of Iraq war
end of Iraq war

Código Malicioso: *"malware"*

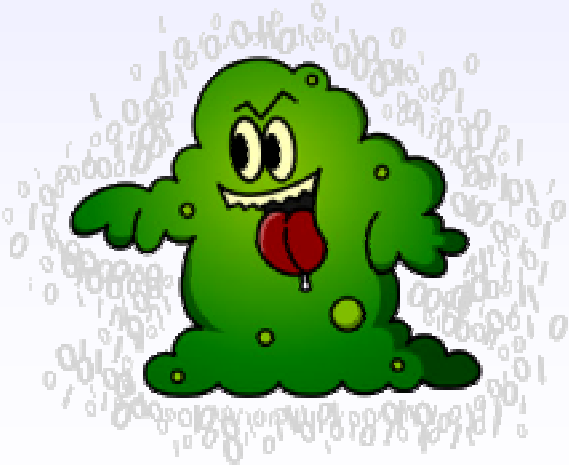
Código Malicioso: "*malware*"

- Programas diseñados con intenciones destructivas y/o intrusivas cuyo objetivo es la destrucción de los datos, ejecución de código y/u otros tipos de compromiso de la seguridad.
- Cada vez son armas de ataque más sofisticadas.
- Categorías básicas:
  - Virus (*virii*).
  - Troyanos (*trojans*).
  - Gusanos (*worms*).
  - Bombas lógicas (*logic bombs*).

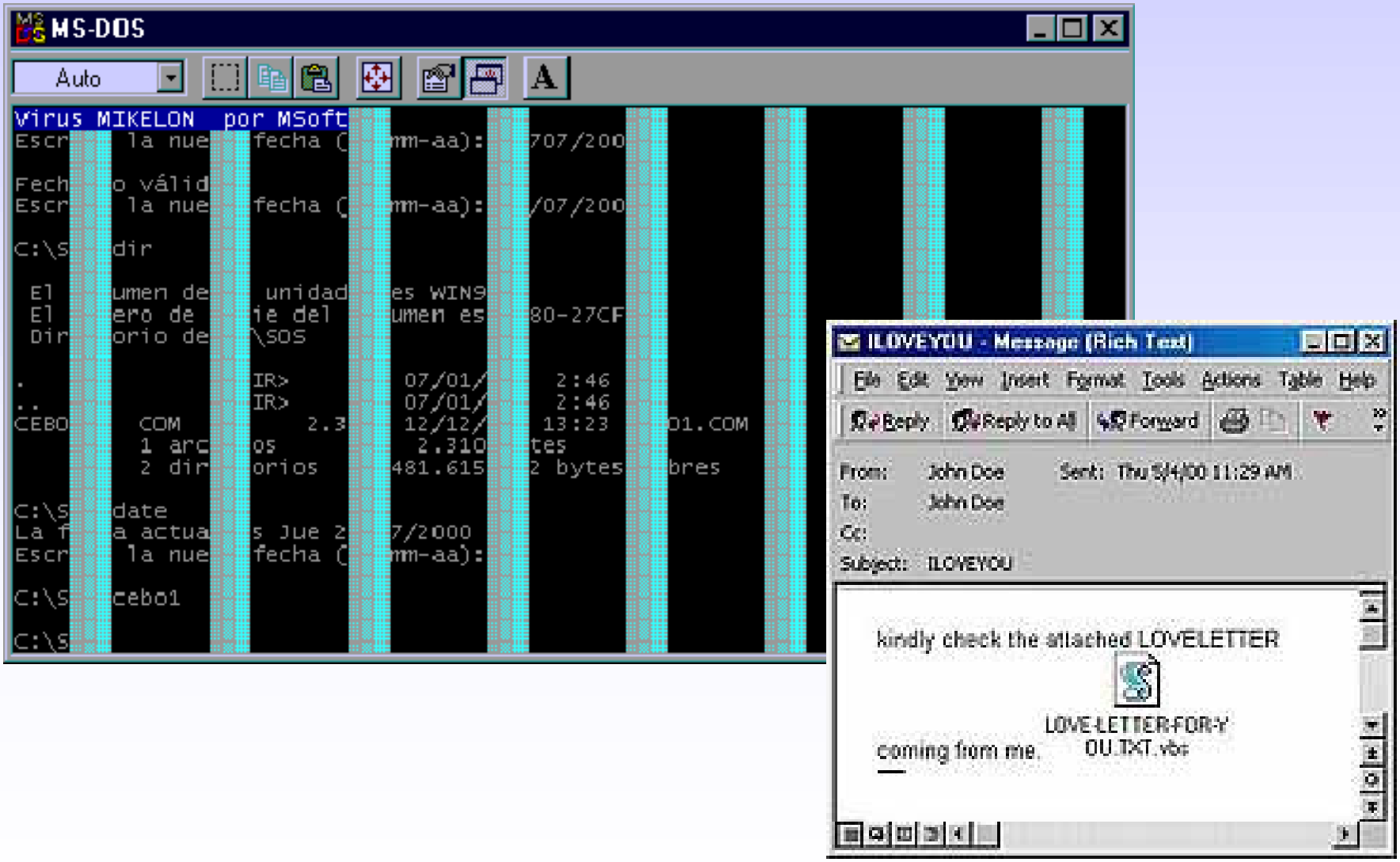
} Híbridos

Virus: *"virii"*

- Procedente del latín "veneno".
- Programa autocontenido creado para reproducirse y causar daños en el sistema infectado.
- Características:
  - Su función clásica es la de causar daño contagiando / destruyendo los archivos del sistema y / o inhabilitándolo.
  - Su objetivo lleva implícito una función de replicación.
- Mecanismos de infección:
  - Email, soportes extraíbles (FD, CD, etc).
- Tipos:
  - Adjuntos (ejecutables, macros de documentos).
  - Sobreescritura (autocontenidos).
  - Sistema de arranque.
- Referencias: [VIR] Virus Bulletin, AlertaAntivirus



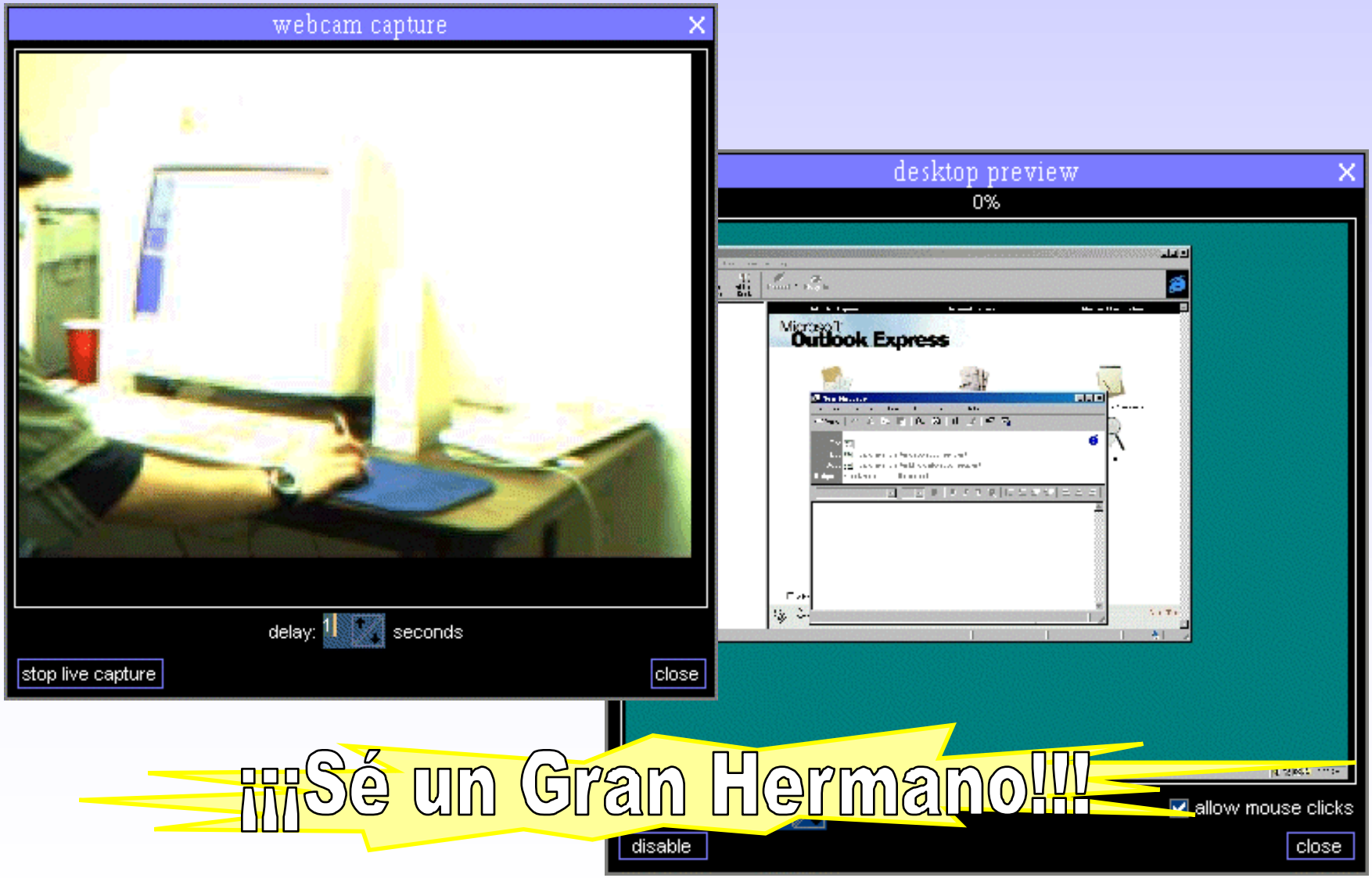
Virus: Barrotes y "I Love You"



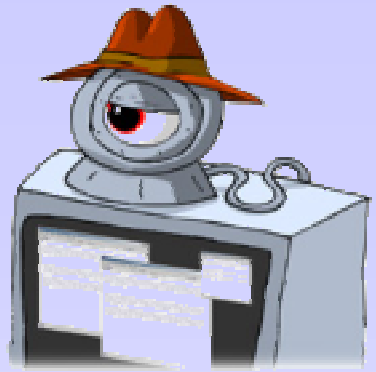
Troyanos: *"trojans"*

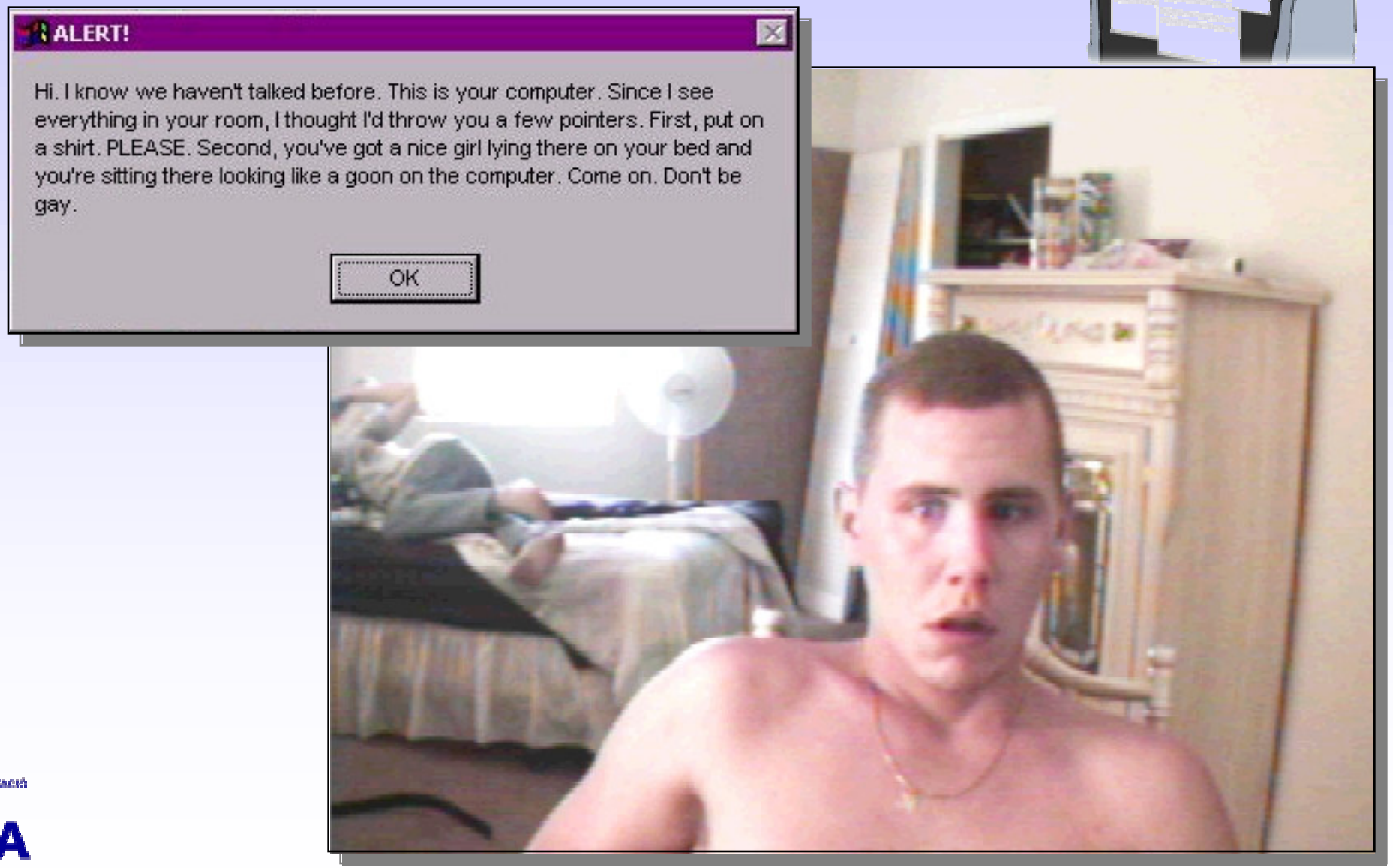
- Procede de la famosa historia romana del "Caballo de Troya".
- Programa creado para realizar acciones no autorizadas ocultado en el interior de un programa autorizado.
- Características:
  - No suelen contener funciones de autoreplicación.
  - Su objetivo no es causar daño sino proporcionar un mecanismo de acceso a los recursos del sistema de forma oculta.
- Mecanismos de infección:
  - Correo electrónico (programas de broma) y otros mecanismos de intercambio de ficheros.
- Referencias:
  - [TRJ] Listado de troyanos de Simovits y G-Lock.

Troyanos: Subseven



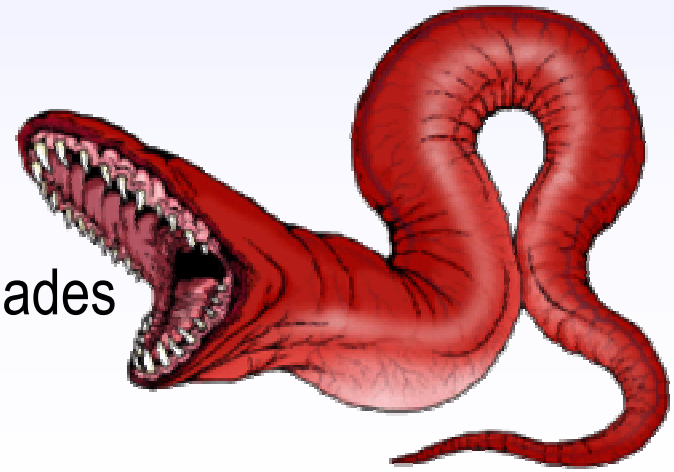
Troyanos: EmBOBado



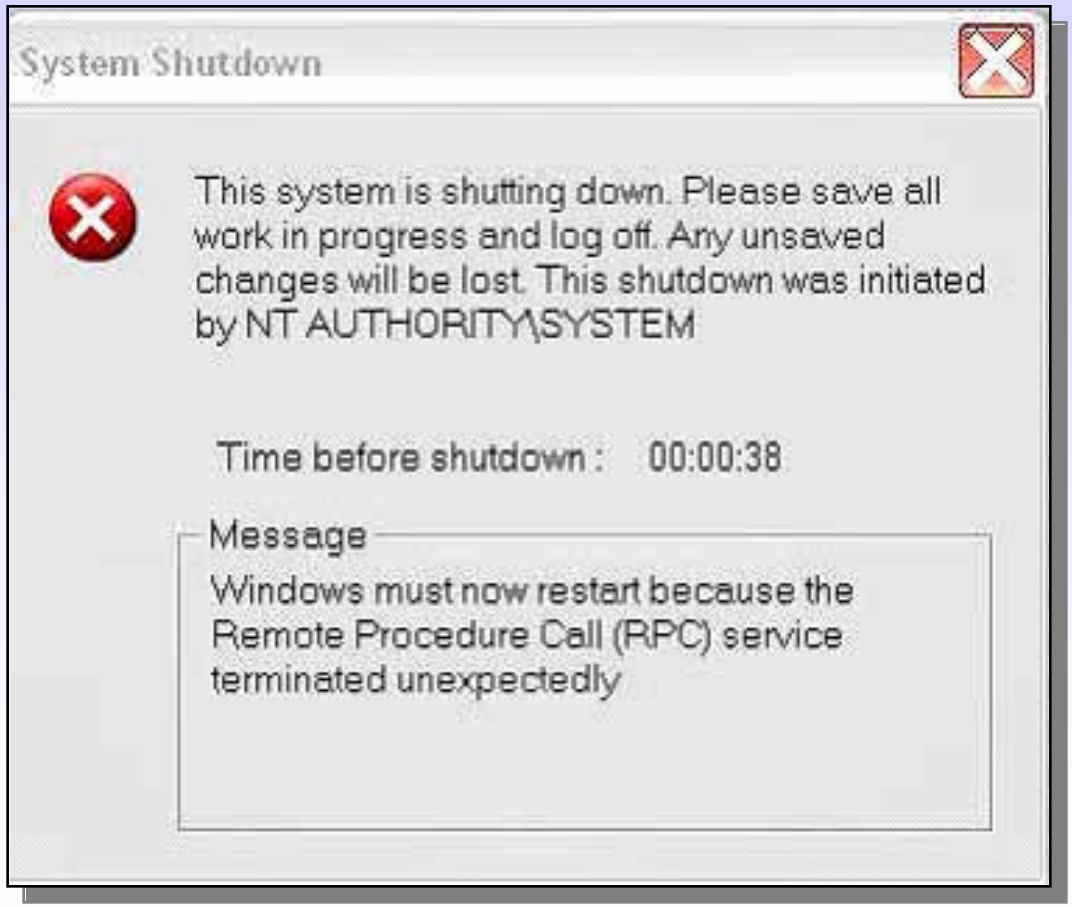


Gusanos: *"worms"*

- El primer gusano creado por Robert Morris se considera la primera gran amenaza que tuvo Internet.
- Programa autocontenido creado para propagarse de sistema a sistema degradando el rendimiento de sus recursos.
- Características:
  - Su función es básicamente auto replicarse.
  - Su objetivo no es causar daño aunque pueden adjuntar otro código maligno.
- Mecanismos de infección:
  - Correo electrónico, redes P2P, vulnerabilidades en servicios de red, etc.
- Referencias: [WRM] Networm.

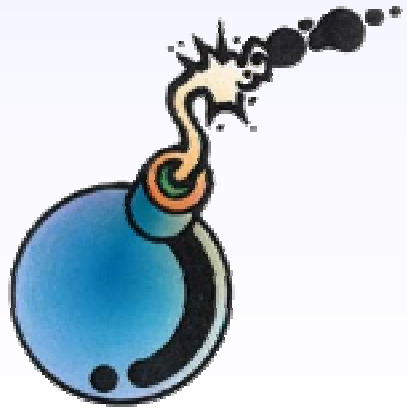


Gusanos: ¡¡¡Oh no Blaster!!!



Bomba lógica: *"logic bomb"*

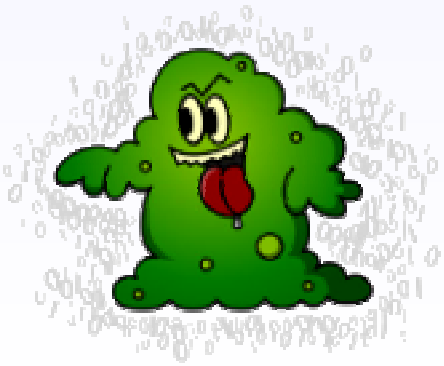
- Se asocian históricamente a código introducido por los programadores para acciones de chantaje o venganza.
- Código cuyo objetivo es realizar una determinado ataque o acción dañina al cumplirse una determinada condición.
- Características:
  - No dispone de funcionalidades de autoréplica.
  - Realiza acciones dañinas de forma condicional.

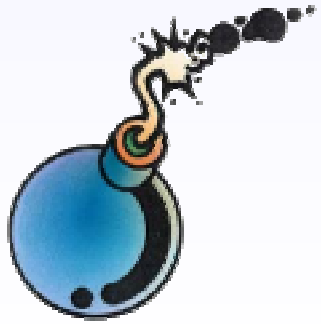


¿ Quién es quién ?

	Autorreplicación	Daños
Virus	Sí	Sí
Troyanos	No	No
Gusanos	Sí	No
Bomba lógica	No	Sí

– Cada vez el *"malware"* se ajusta más a un modelo híbrido.



Ciclo de vida de una intrusión

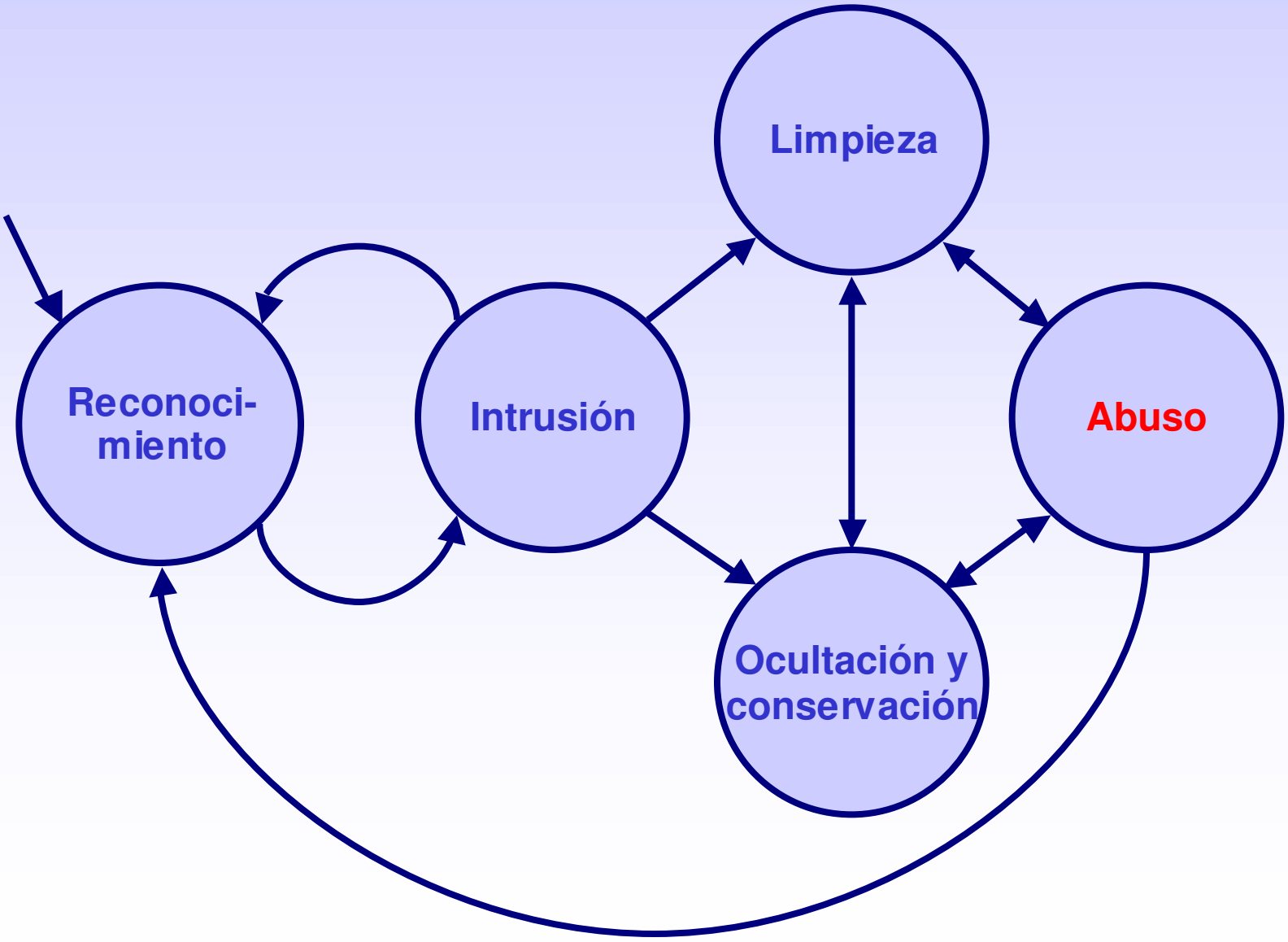
Introducción

- Como veremos a continuación, gran parte de las intrusiones suelen seguir un determinado número de etapas o un conjunto de ellas.
- Hay que tener en cuenta que un intruso además de abusar de los recursos comprometidos son habitualmente utilizados para nuevos ataques o intrusiones.
- El número de sistemas implicados puede dificultar en gran manera la investigación al rastrear un incidente.

Etapas de una intrusión (I)

- Reconocimiento:
  - Recopilación de información.
  - Sondeo (*scanning, fingerprinting*).
- Intrusión/Ataque:
  - Denegación de servicio.
  - Compromiso.
- Limpieza, ocultación y conservación.
- Abuso.

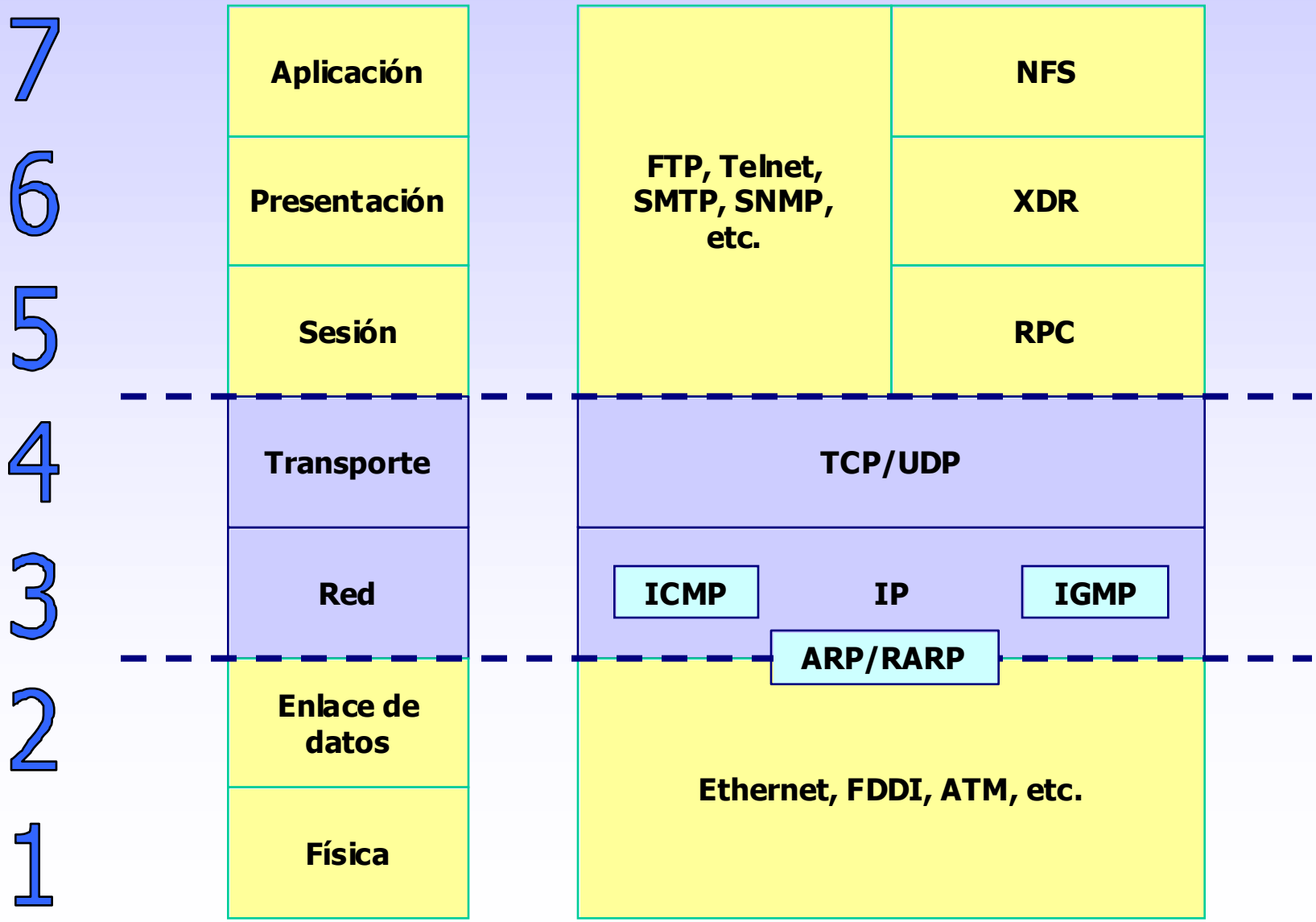
Etapas de una intrusión (II)



Reconocimiento

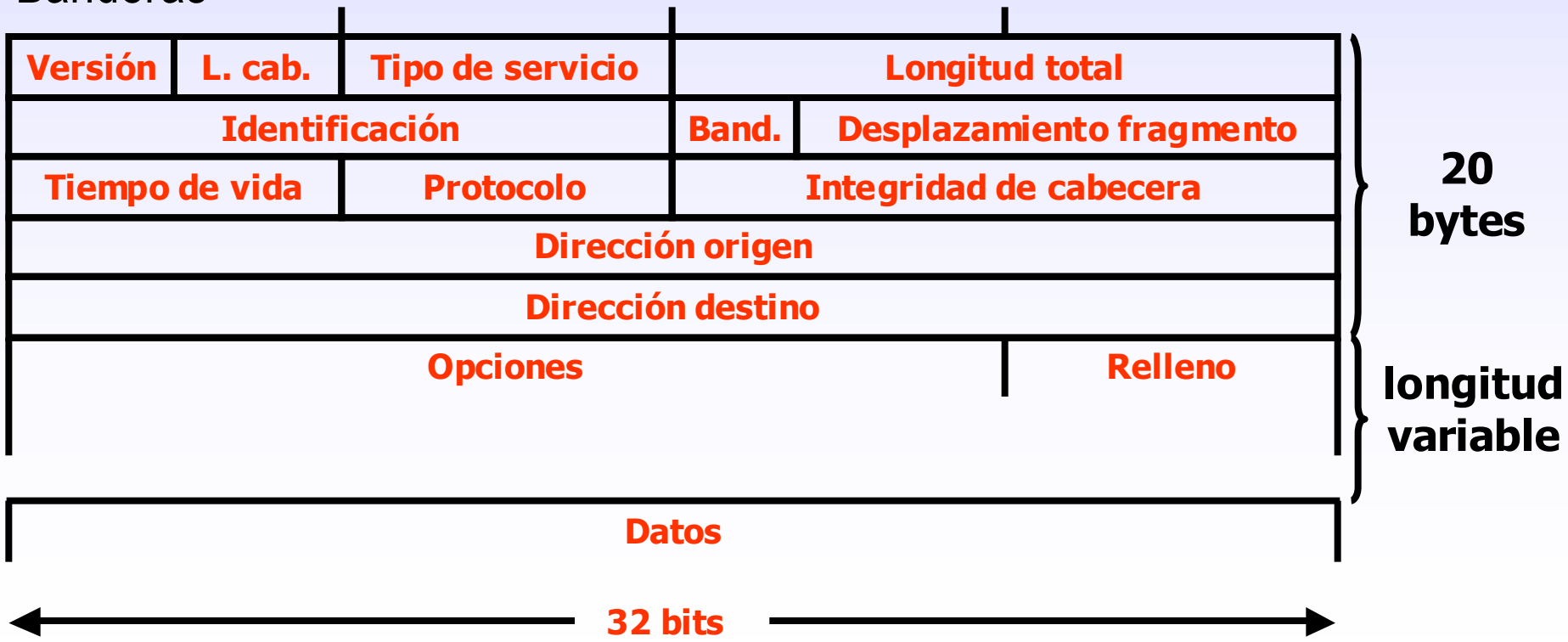
- Etapa consistente en la obtención de información útil sobre el objetivo de la intrusión (si está definido) o bien determinar una lista de posibles objetivos.
- Tipos:
  - Recopilación de información
    - Whois.
    - Web (buscadores, sitio web) → Google ☺
  - Sondeos
    - Escaneo.
    - Footprinting / Fingerprinting.

Pila TCP/IP en modelo OSI



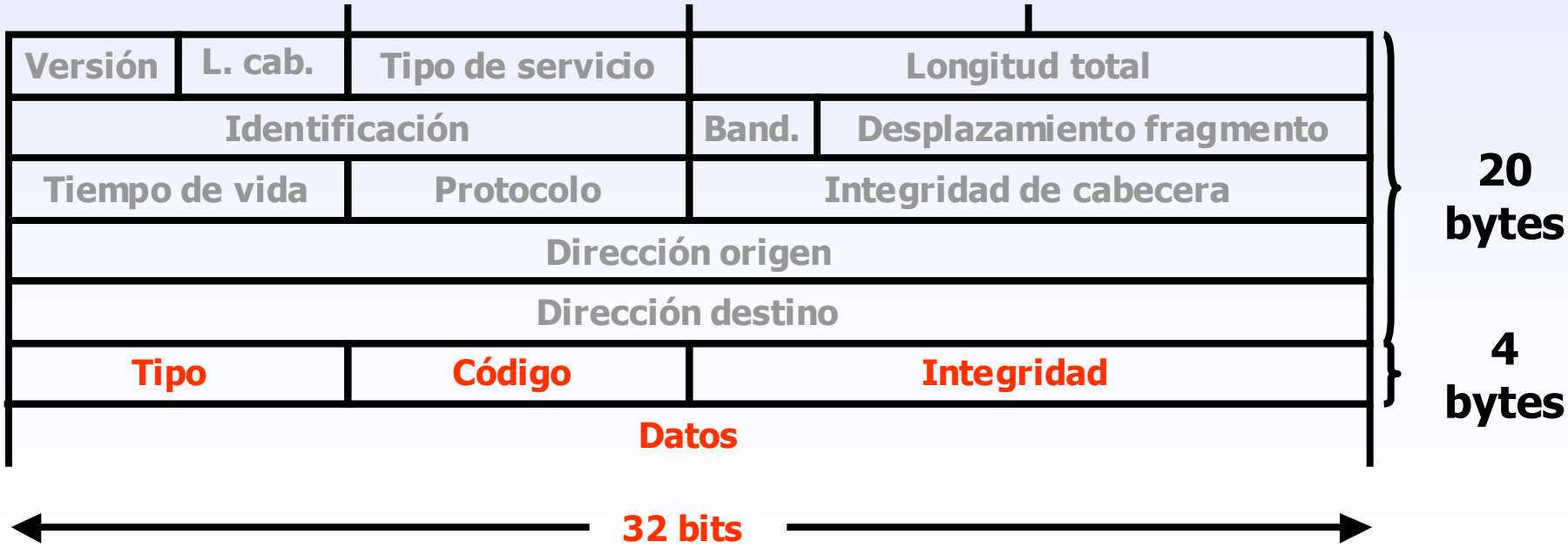
Internet Protocol (IP) versión 4

- Versión
- Longitud de cabecera
- Tipo de servicio
- Identificación
- Banderas
- Desplazamiento de fragmento
- Tiempo de vida
- Protocolo
- Integridad de cabecera
- Dirección origen y destino



Internet Control Message Protocol (ICMP)

- Considerado parte de la capa IP.
- Encargado de notificar mensajes de error o condiciones que requieran atención.
- Nunca responde a otro paquete de ICMP de error (evitar bucles).

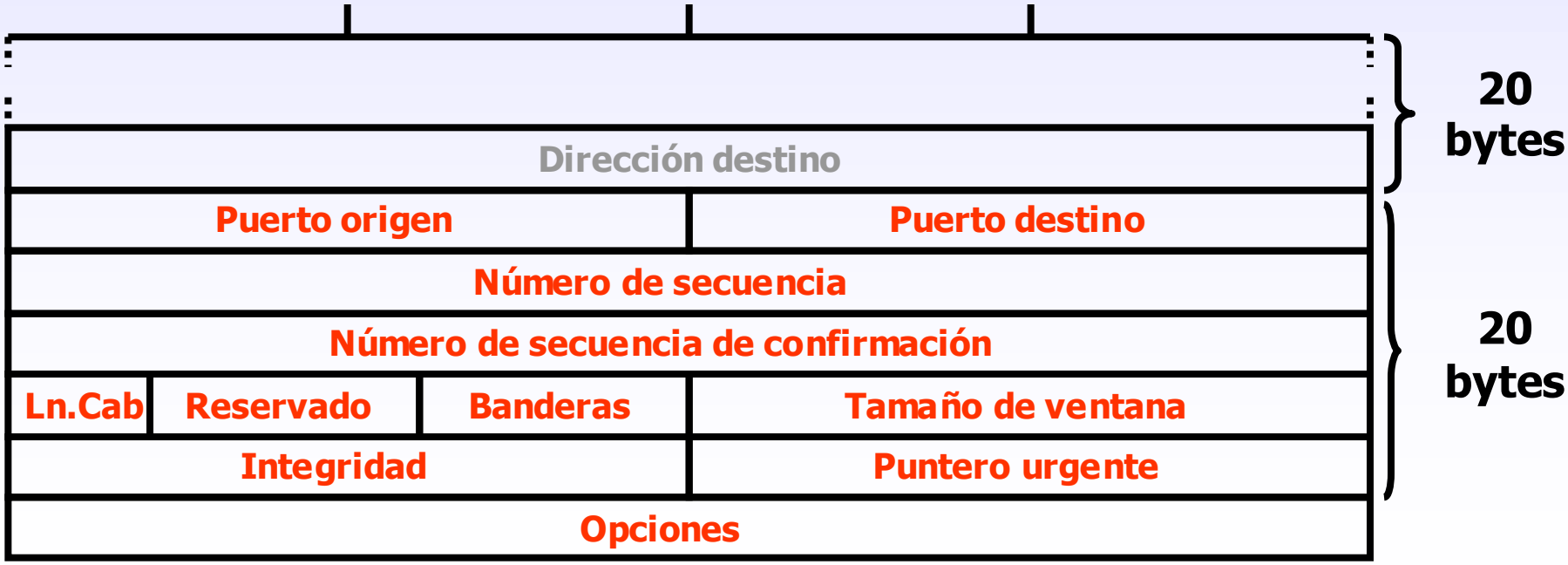


User Datagram Protocol (UDP)

- *RFC768*
- Protocolo de nivel de transporte no orientado a conexión.
- Es de tipo no-fiable (*send-and-pray*) pero más rápido, bueno si pequeñas perdidas pueden ser aceptables.
- Cada operación de envío genera un único datagrama.

Transport Control Protocol (TCP)

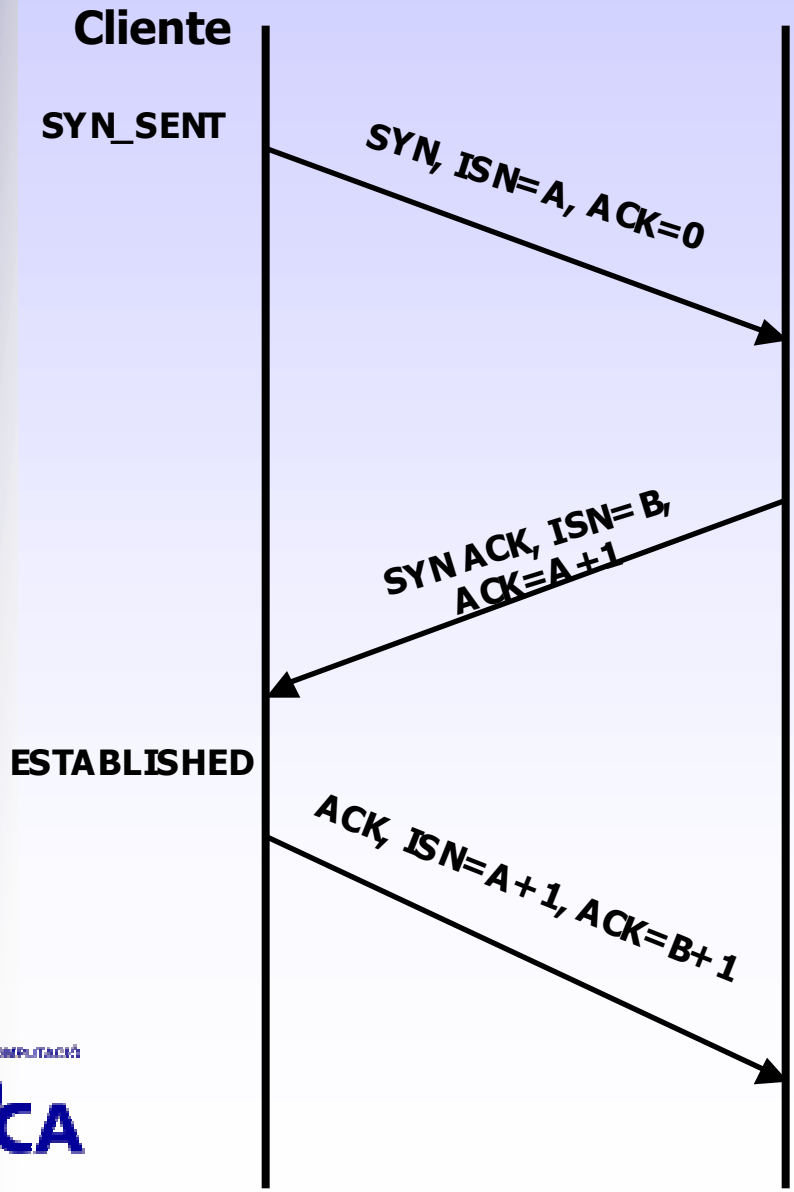
- *RFC793*
- Protocolo de nivel de transporte orientado a la conexión.
- Es de tipo fiable pero más lento debido al control de flujo.
- Permite realizar una transmisión ordenada y completa mediante números de secuencia.



Banderas TCP

- Synchronize (SYN): utilizado para iniciar una conexión, es decir, sincronización inicial de la secuencia.
- Acknowledgment (ACK): utilizado para la confirmación de recepción de un número particular de secuencia.
- Push (PSH): Informa al receptor que hay datos que la aplicación receptora debería leer.
- Urgent (URG): manifiesta la necesidad de procesar los datos del paquete con urgencia (prioridad).
- Finish (FIN): indica al sistema remoto la intención de finalizar.
- Reset (RST): utilizado para resetar una conexión (condiciones de error, timeouts, etc).

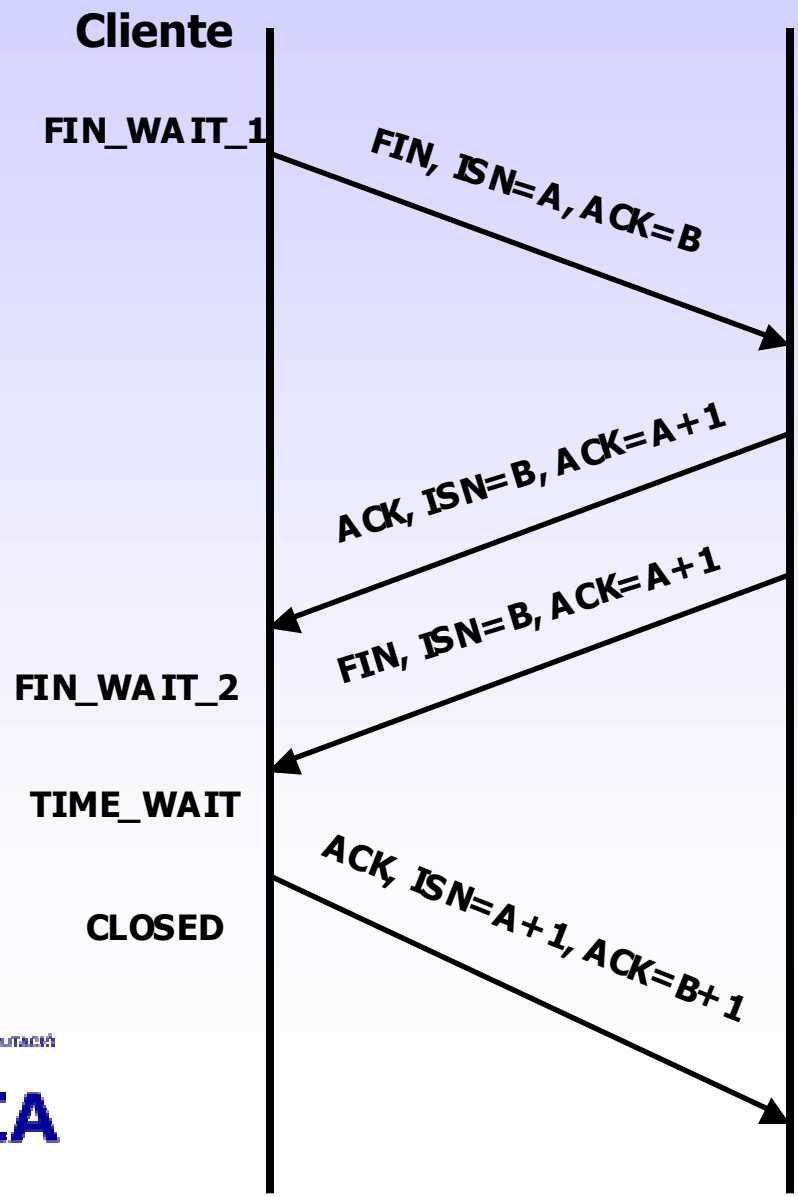
TCP: *"3-way handshake"*



- Pasos:
  - A pide establecimiento a B.
  - B confirma establecimiento a A.
  - A confirma la confirmación a B.

Fotografía propiedad de © ThinkGeek.com

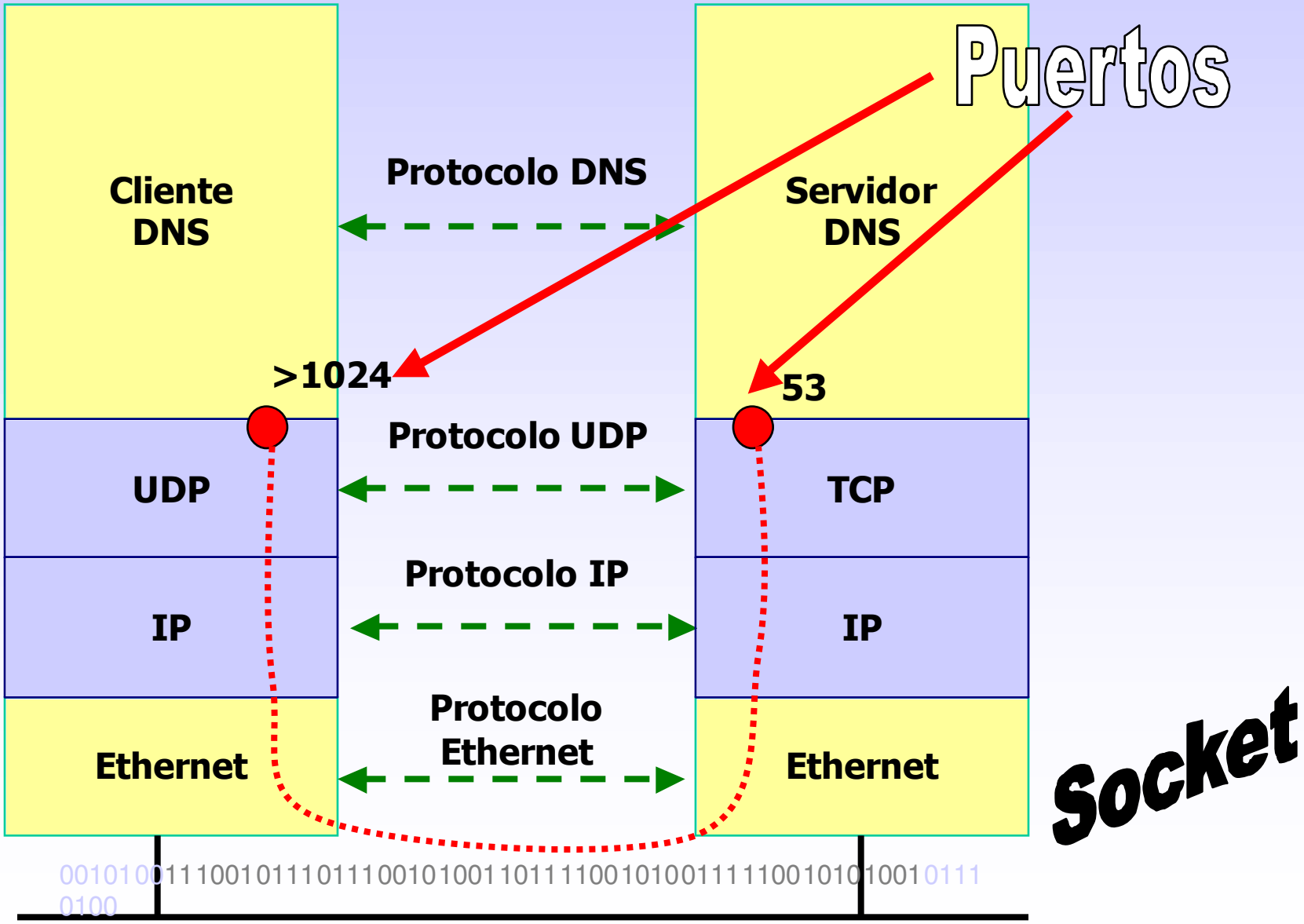
TCP: *"Graceful Finish"*



- Finalización full-duplex
- Pasos:
  - A pide finalización a B.
  - B confirma finalización a A.
  - B pide finalización a A.
  - A confirma finalización a B.

Fotografía propiedad de © ThinkGeek.com

Ejemplo: DNS


Puertos
Cliente DNS
Protocolo DNS
Servidor DNS
>1024
53
Protocolo UDP
UDP
TCP
Protocolo IP
IP
IP
Protocolo Ethernet
Ethernet
Ethernet
Socket

¿Qué está sucediendo?

```
08:45:43 router.test.com 648358: 7w0d:
    %SEC-6-IPACCESSLOGP: list 101 denied
    tcp 10.0.147.89(2789) -> 192.168.140.99(25), 1 packet
08:45:50 router.test.com 648361: 7w0d:
    %SEC-6-IPACCESSLOGP: list 101 denied
    tcp 10.0.147.89(2907) -> 192.168.140.217(25), 1 packet
08:47:03 router.test.com 648372: 7w0d:
    %SEC-6-IPACCESSLOGP: list 101 denied
    tcp 10.0.147.89(3698) -> 192.168.140.221(25), 1 packet
```

Sondeos: *"scanning"*

- Mecanismo de barrido por red que permite obtener información sobre los equipos y servicios disponibles.
- Tipos según su objetivo:
  - "Host scan": búsqueda centrada en máquinas.
  - "Port scan": búsqueda de servicios ofrecidos por máquina.
- Tipos según su mecanismo:
  - ICMP:
    - Echo Request, Timestamp, Address Mask.
  - Puertos (0-65536):
    - TCP
    - UDP

Sondeos: *"Portscanning" TCP/UDP*

- Puertos (0-65536):
  - TCP
    - CONNECT: fiable, lento y ruidoso.
      - Consiste en completar *"3-way-handshake"*.
    - SYN: menos fiable (posibles falsos positivos), rápido.
      - Consiste en enviar paquete SYN y escuchar la respuesta.
    - ACK: menos fiable (posibles falsos positivos), rápido.
      - Consiste en enviar paquetes SYN, ACK y escuchar la respuesta.
    - RST: rápido aunque poco utilizado.
      - Consiste en enviar paquetes RST y escuchar la respuesta.
    - XMAS/NULL/FIN: poco fiable (posibles falsos positivos / negativos)
      - Consiste en enviar paquetes con todos los flags / solo NULL / solo FIN.
  - UDP
    - Poco fiable al utilizar una técnica de escaneo inverso (posibles falsos positivos).

Sondeos: *"footprinting"*

- Los escaneos de puertos descritos tan solo indican la posible existencia de un servicio, pero no si es realmente es este y si es vulnerable.
  - Pregunta: ¿Cual es el servicio escuchando en el puerto 80?
- Es de gran importancia conocer la versión de los servicios para saber si son vulnerables.
- Tipos:
  - Banners.
  - Consultas de versión.
  - Consultas DNS.

Ejemplos: *"Banner grabbing"*

```
moeller@bluebird:~ > telnet bluebird
Trying 127.0.0.2...
Connected to bluebird.
Escape character is '^]'.
Welcome to SuSE Linux 7.1 (i386) - Kernel
2.2.18(2)
```

```
moeller@bluebird:~ > ftp bluebird

220 bluebird FTP server (Version 6.5/OpenBSD,
linux port 0.3.2) ready.
```

Mensaje necesario

```
moeller@bluebird:~ >telnet mailhub 25

220 mailhub ESMTP Server (Microsoft Exchange Internet
Mail Service 5.5.2656.59) ready
```

Ejemplos: consulta de versión

```
#rpcinfo -p server.domain.com
   program vers proto   port  service
    100000    4   tcp    111  rpcbind
    100000    4   udp    111  rpcbind
    100021    1   udp   4045  nlockmgr
    100229    1   tcp  32771  metad
    100230    1   tcp  32772  metamhd
    100024    1   udp  32772  status
    100024    1   tcp  32773  status
```

```
#nslookup -type=txt -class=chaos version.bind some.host.de
Server: some.host.es
Address: 192.168.1.7

version.bind   text =
        8.2.3-REL
```

Ejemplo: consulta DNS

Información completa de correspondencia IP-hostname

```
#nslookup
    >ls dominio.com
```

Información de registros HINFO, WKS

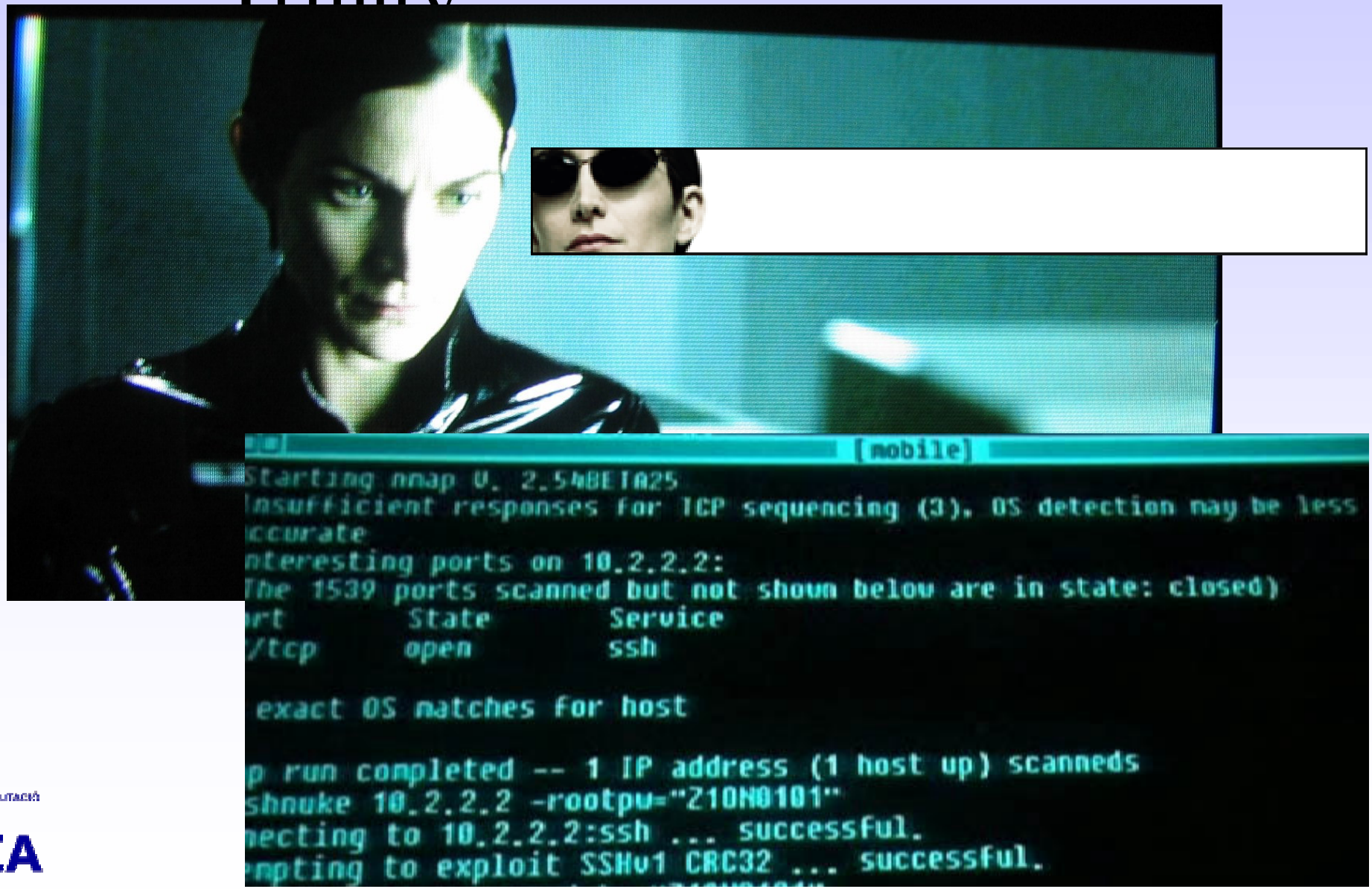
```
#nslookup -type=WKS host.dominio.com dns.dominio.com
#nslookup -type=HINFO host.dominio.com dns.dominio.com
```

¡En la variedad está el gusto!

Sondeos: *"fingerprinting"*

- A diferencia de las herramientas de "*footprinting*" que se centraban en la versión de los servicios, ahora pretendemos identificar la versión del sistema operativo.
- Las implementaciones de pila TCP/IP en los diferentes sistemas operativos y versiones de estos permiten diferenciarlas:
- Tipos:
  - Pasiva: necesidad de captura de paquetes. Ej: p0f.
  - Activa: son más ruidosas al necesitar sondear intensivamente la pila remota. Ej: nmap.

nmap: el ojito derecho de Trinity



Intrusión

- Etapa consistente en el ataque al sistema aprovechando sus debilidades con diversos objetivos:
  - conseguir acceso no autorizado, escalado de privilegios, denegación de servicio, etc.
- Tipos:
  - Configuración incorrecta.
  - Debilidades de diseño / protocolo.
  - Errores de programación:
    - Buffer overflow.
    - Format String bugs.

Configuración incorrecta

- Debilidades producidas por un fallo humano por parte del administrador o usuario del sistema.
- Ejemplos típicos:
  - Compartición de ficheros sin restricciones.
  - *Proxies* (*mail, web, socks*) no restringidos.
  - Cuentas sin contraseñas o de tipo débil.
  - Acceso abierto a base de datos de contraseñas.
  - Confianza total en contenidos dinámicos del navegador web o cliente de correo.

Debilidades de diseño / protocolo

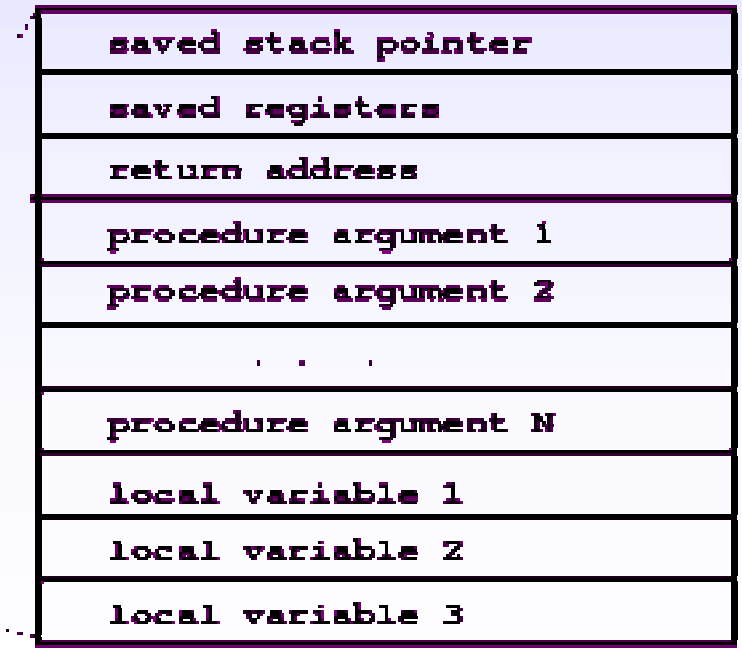
- Fallos básicos en el diseño del *software* o de los protocolos que no pueden ser solventados de forma trivial.
- Ejemplos:
  - Autenticación en texto claro en protocolos telnet / ftp.
    - Captura de credenciales por red.
  - Confianza en autenticación mediante dirección IP origen.
    - Falseado de cabecera de paquete IP.

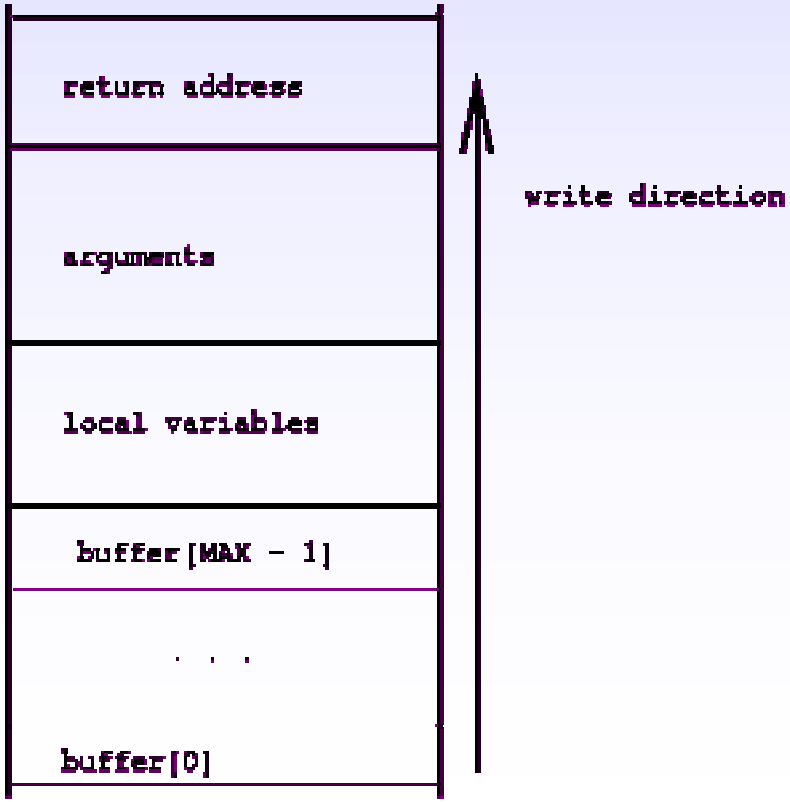
Errores de Programación

- Producidos por el programador típicamente por asumir o presuponer ciertas condiciones del entorno del programa.
- Los abusos proceden habitualmente de la falta de control en las variables de entrada:
  - *"Buffer overflow".*
  - Control de formato.

Ejemplo: *"Stack Smashing"*

- Contigüidad de los *buffers* de entrada con la pila.
- Al no haber control de *overflow* se escribe en el espacio adyacente ejecutando el código deseado.





Ejemplo: Demonio Linux IMAP

```
May 11 16:09:31 goodhost imapd[271]: connect from 1.2.3.4
May 11 16:09:42 goodhost imapd[271]: command stream end
of file, while reading line user=??? host=attack.net
May 11 16:40:36 goodhost imapd[271]: connect from 1.2.3.4
May 11 16:42:08 goodhost in.telnetd[603]: connect from
5.6.7.8
May 11 16:42:24 goodhost PAM_pwdb[606]: (login) session
opened for user codeking by (uid=0)
May 11 16:42:24 goodhost login[606]: LOGIN ON ttyp0 BY
codeking
May 11 17:16:36 goodhost in.telnetd[917]: connect from
  5.6.7.8 FROM badhost.com
May 11 17:17:11 goodhost PAM_pwdb[942]: (su) session
  opened for user rewt by codeking (uid=0)
```

"Exploit"

- También conocidos como *"xploit"*, son considerados la raíz de la cultura *"hacker"*.
- Código creado para aprovechar una vulnerabilidad existente en un servicio de un sistema informático.
- Cuando todavía no son públicos se les suele llamar "*0-day exploit*".
- Tipos:
  - Locales: necesidad de disponer de acceso local.
  - Remotos: explotables por red.

Curva de la vulnerabilidad

- Una instalación puntual de los parches es vital para reducir el número de incidentes.

Vulnerabilidades: fuentes

- Públicos de tipo *disclosure*:
  - VulnWatch List, BugTraq List, Full Disclosure
- Públicos de tipo general:
  - CERT/CC, US-CERT – Alerts and Bulletins
  - SANS Institute - Newsletters and Digests
  - SecurityFocus – Vulnerabilities
  - DoE, CIAC – Bulletins
- Públicos de fabricantes/proveedores (*software*, *hardware*):
  - Cisco PSIRT, Microsoft Security Bulletins, etc.
- Comerciales:
  - ALTAIR de esCERT/InetSecur, SANA de Hispasec
- Bases de Datos:
  - MITRE CVE, NIST CAT Metabase, etc.

Limpieza, ocultación y conservación

- Una vez realizada la intrusión, se realizan acciones para conservar el control del sistema sin levantar sospechas.
- Acciones:
  - Ocultación de actividad (red, procesos) → *Rootkits*
  - Limpieza de trazas → *Wiping / Zapping.*
    - *Ej: Unix: /var/adm o /var/log (wtmp, utmpx, wtmpx, lastlog).*
    - *Ej: Windows: Eventlog.*
  - Instalación de puertas traseras → *Backdoors.*
- Incluso algunos intrusos nos parchean amablemente el sistema. ☺

Ocultación: *"Rootkit"*

- "¿De verdad crees que es aire lo que respiras?"
  - Morpheus (1ª película de la saga Matrix)
- Herramienta que pretende ocultar al administrador la presencia de las actividades realizadas por el intruso.
- Habitualmente incorporan otras herramientas de abuso u ocultación: *sniffer, backdoor, log zapper / wipper, etc*.
- Tipología:
  - Sistema: reemplaza binarios modificados.
  - Núcleo: módulo cargado en el núcleo.
- Referencia: [RTK]

¡¡¡ Abusaaaandooo !!!

- Punto de partida para nuevos escaneos e intrusiones:
  - Instalación de *xploits*, *sniffers*, etc.
- Uso abusivo de recursos:
  - Almacenamiento: repositorio de software, películas, etc.
  - Capacidad de proceso: cracking de contraseñas.
  - Distribución de contenidos: "*warez*".
  - Denegación de servicio.

Denegación de Servicio: *DoS*

- Actividades cuyo objetivo es denegar el servicio, agotar o ralentizar los recursos de la victima mediante:
  - Agotamiento de recursos. Ej: SYN Flood.
  - Aprovechamiento de alguna vulnerabilidad. Ej: Ping de la muerte.
- Algunos tipos conocidos:
  - TCP SYN flood: agotamiento del espacio de conexiones.
  - UDP Flood: basado en saturación por tráfico de una máquina.
  - PING Flood: similar al anterior.
  - Smurf: efecto reflector sobre direcciones de broadcast.
  - Fraggle: abuso de servicios UDP.
- Herramientas: Stacheldraht, Tribe, Trin00, etc.
- Referencias: [DOS] CERT/CC, D.Dittrich.

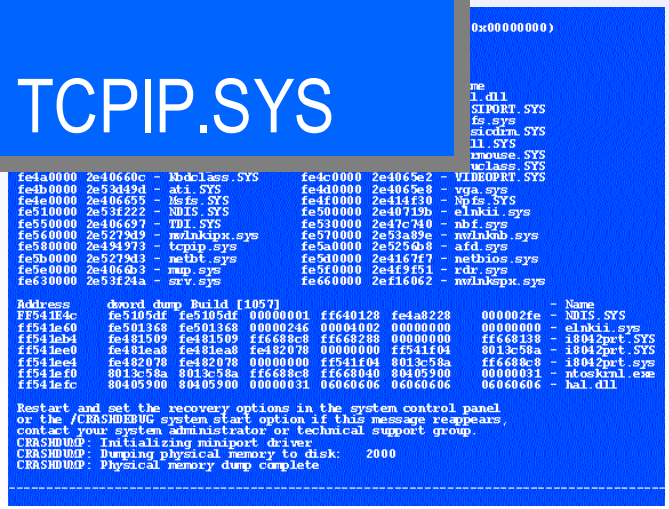
Ping de la muerte ☹

STOP: 0X0000001E

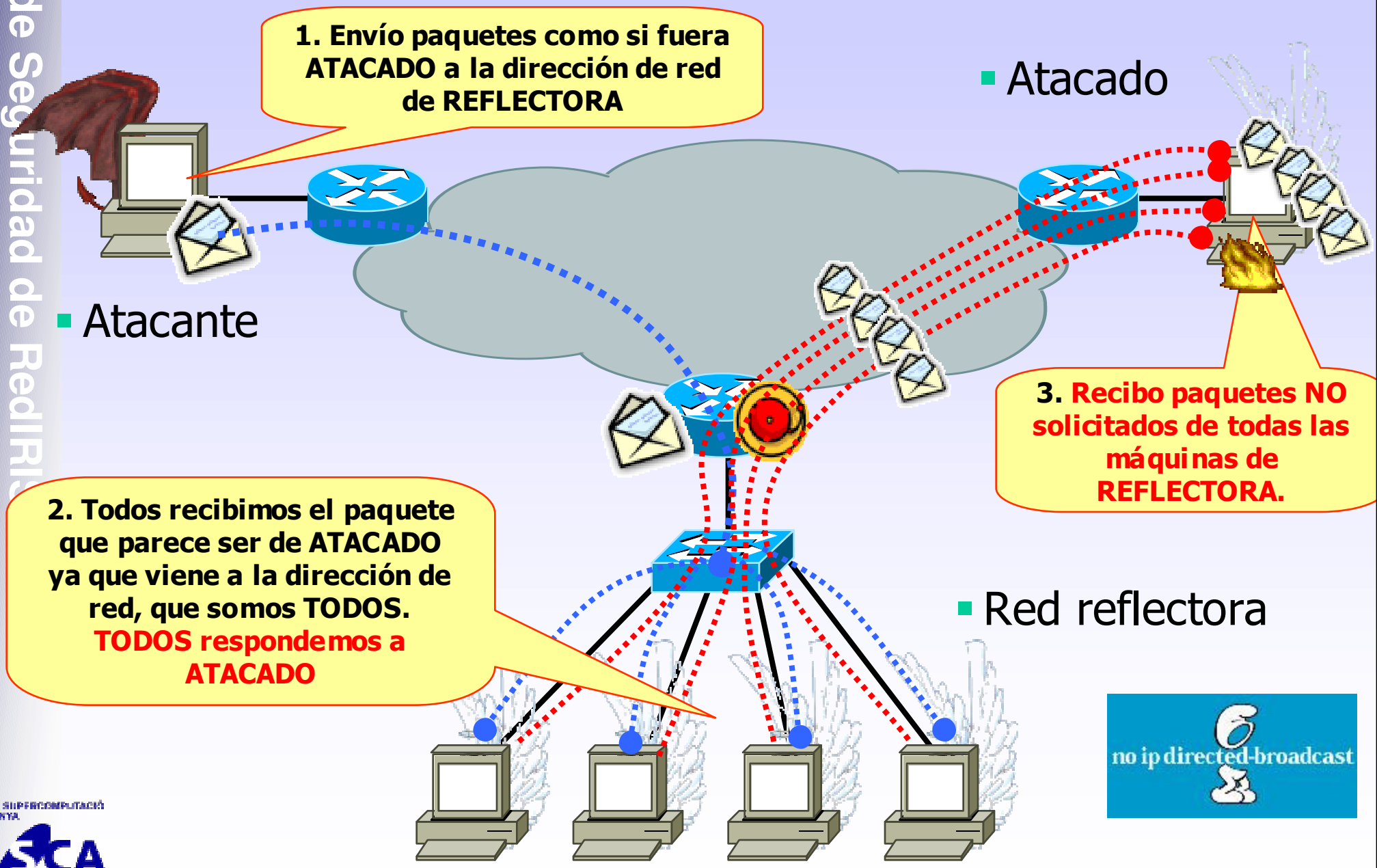
KMODE_EXCEPTION_NOT_HANDLED - TCPIP.SYS

STOP: 0x0000000A

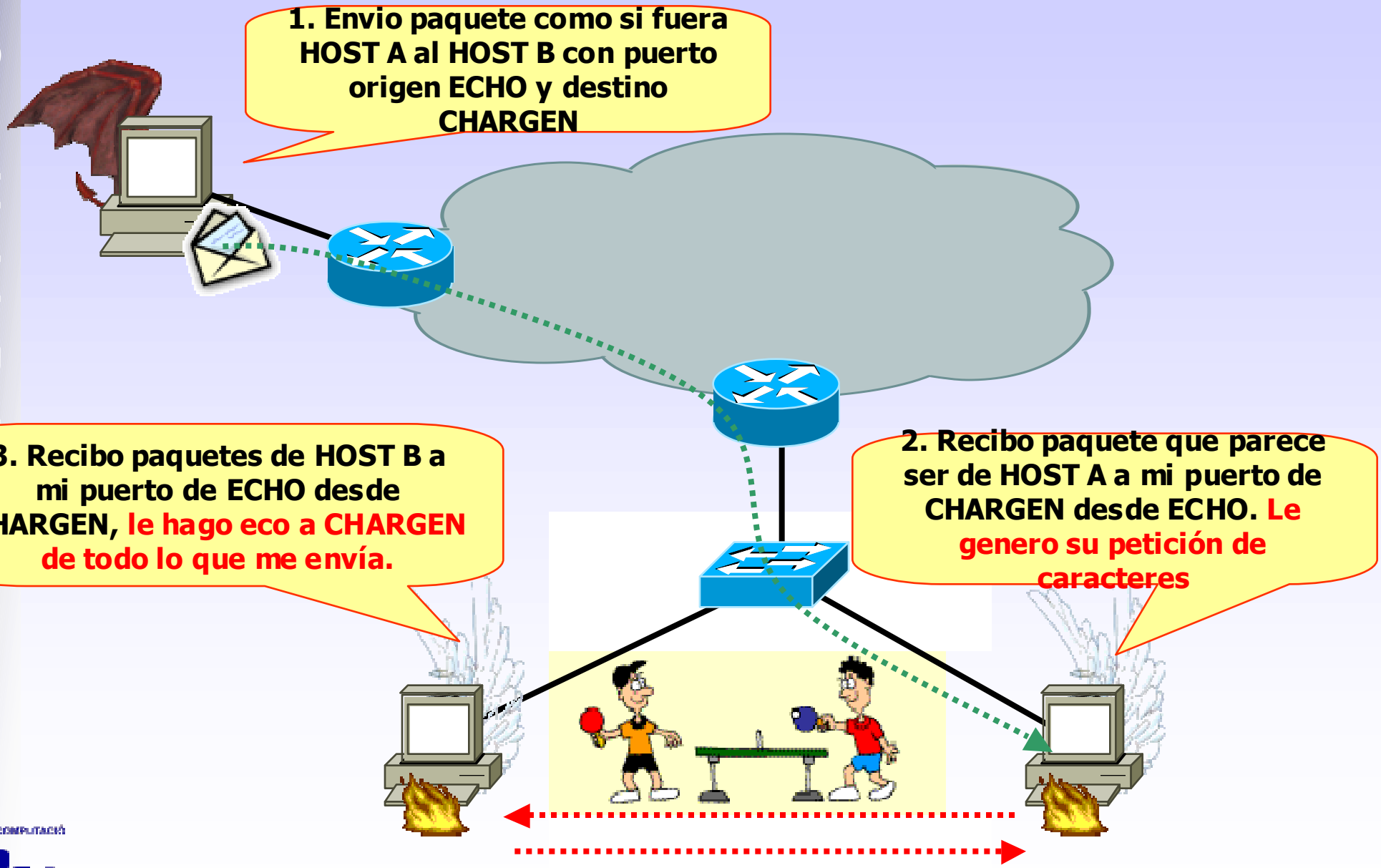
IRQL_NOT_LESS_OR_EQUAL - TCPIP.SYS



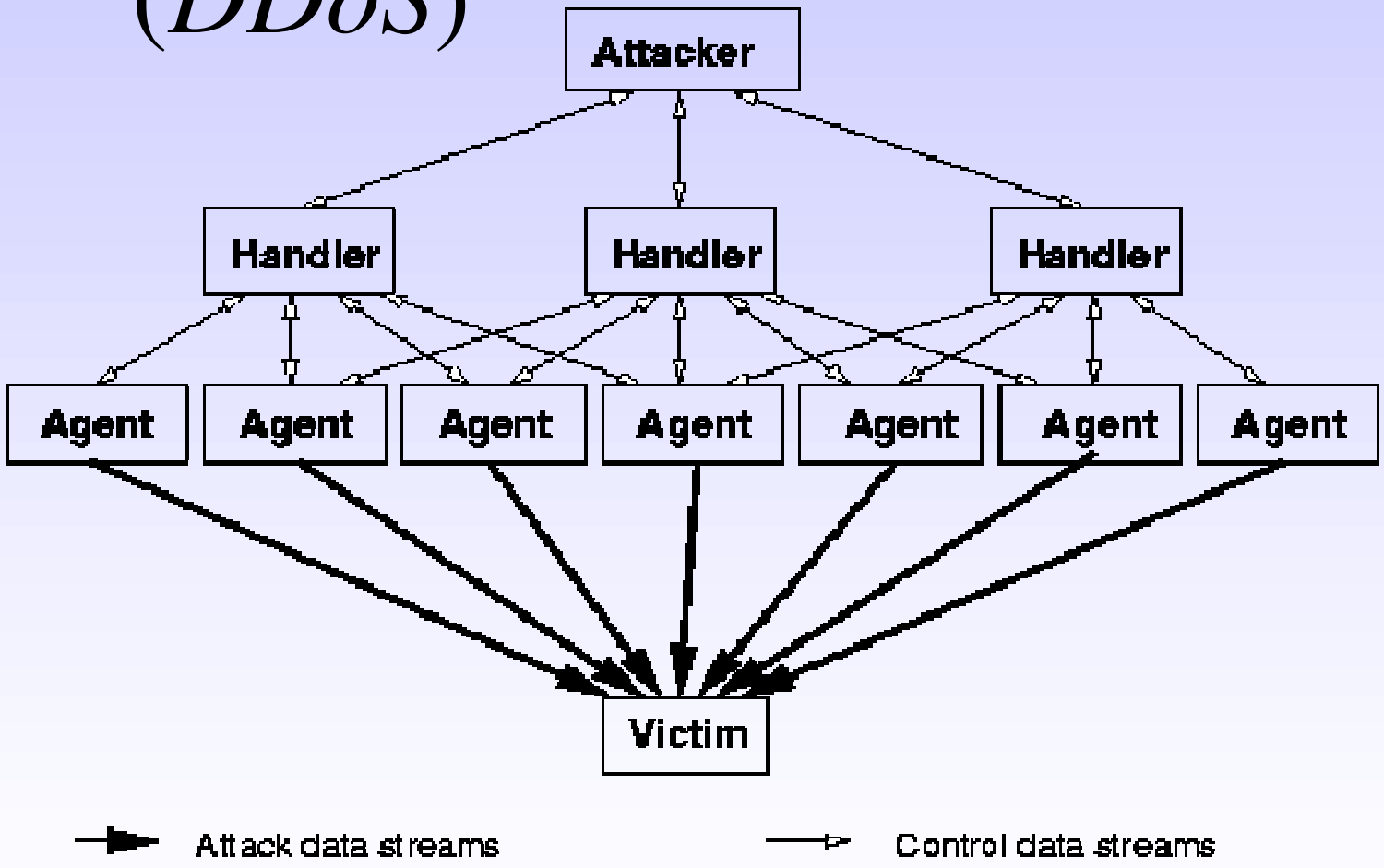
Smurfeando


1. Envío paquetes como si fuera ATACADO a la dirección de red de REFLECTORA
Atacado
Atacante
3. Recibo paquetes NO solicitados de todas las máquinas de REFLECTORA.
2. Todos recibimos el paquete que parece ser de ATACADO ya que viene a la dirección de red, que somos TODOS. TODOS respondemos a ATACADO
Red reflectora
no ip directed-broadcast

Ping UDP Pong



El temido *DoS* Distribuido (*DDoS*)



- Las ataques actuales de tipo DDoS suelen utilizar esencialmente el IRC como comunicación entre intruso y agentes.

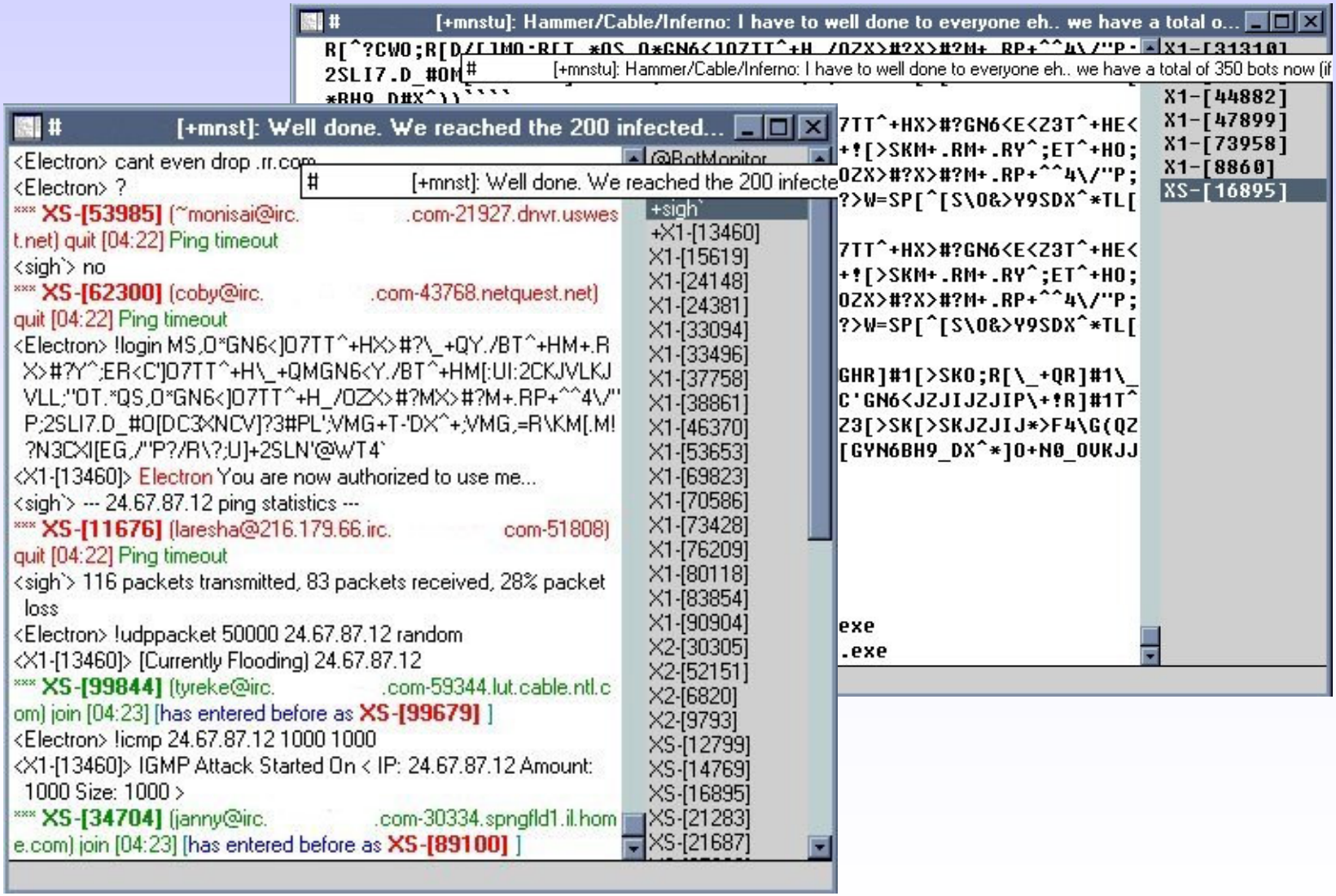
¿Qué es un *"bot"*?

- Bot es un termino genérico derivado de la palabra robot usado para describir un autómata o proceso automático.
- Son también conocidos como *zombies* o agentes y son controlados mediante un master.
- Suelen ser programas de pequeño tamaño viajando comprimidos en un ejecutable UPX.
- Uno de los primeros (1993) fué Eggdrop, todavía ampliamente conocido.
- Algunos bots troyanos tienen el nombre de sus autores: Subseven bot, Bionet bot, Attack bot, GT bot, Evil bot, Slack bot, etc.

La guerra de los bots: *"botnet"*

- Legión de bots propiedad de un determinado hacker o grupo.
- No suelen estar todos sus miembros activos siempre ya que no siempre están *"online"*.
- Su capacidad maligna está en función del ancho de banda agregado.
- Uso:
  - Distribución de *warez*.
  - Spamming.
  - Denegación de servicio.

Ejemplos: “botnet” (I)



Ciclo de vida de la respuesta a incidentes

Respuesta a incidentes

- Preparación y prevención.
- Detección y análisis.
- Contención, erradicación y recuperación.
- Reflexión y mejora:
  - Documentación y lecciones aprendidas.

Respuesta a incidentes (II)

Preparación y prevención

- En esta fase se aborda la seguridad preventiva.
- Técnicas:
  - Gestión de parches.
  - Seguridad de sistema/*host*.
  - Seguridad de red.
  - Prevención de código malicioso.
- Administrativas:
  - Política de seguridad y procedimientos operativos.
  - Planes de contingencia y de gestión de incidentes.
  - Formación y concienciación.

Detección y preanálisis

- Esta etapa consiste en la detección y/o identificación de la naturaleza del incidente.
- Es importante disponer del máximo de información posible: trazas (*logs*), capturas de tráfico.
- Se realiza un análisis minimalista, para así evaluar el riesgo rápidamente, intentando identificar el origen del incidente.
- Se debe realizar una primera toma de contacto con los implicados mediante notificaciones.
- Información:
  - Correlación con actividades en la red.
  - *"Tracing"* del origen.
  - Experiencias previas del CSIRT.

Regional Internet Registries (RIR)

- Delegados para la gestión de la asignación de direccionamiento IP por la IANA/ICANN para las diferentes regiones geográficas.
- Modelo descentralizado, estable y robusto que ha facilitado la evolución de IP en la arquitectura de direccionamiento y routing actual.
- Objetivos:
  - Conservación.
  - Agregación.
  - Registro.

RIPE NCC

ARIN
American Registry for Internet Numbers

APNIC

LACNIC

¡Ojo a las nuevas tecnologías!

- Actualmente o en corto plazo se desplegaran sobre nuestras infraestructuras nuevas tecnologías avanzadas.
- Conviene estudiarlas para conocer sus debilidades y la manera correcta de asegurarlas.
- Algunas de ellas son:
  - IPv6: protocolo IP de próxima generación.
  - ToIP/VoIP/Streaming/Videoconferencia: tecnologías multimedia.
  - WLAN: redes inalámbricas de área local.

Conclusiones

- Estar a la última en el conocimiento de la herramientas y técnicas utilizadas por los intrusos es cada vez más una necesidad al ser estas cada vez más sofisticadas, rápidas e inadvertidas.
- La seguridad no es un producto sino un proceso en ciclo de evolución constante donde la importancia reside en una buena política, procedimientos operativos y personal técnicamente competente.
- No existe la seguridad total pero una aproximación defensiva por capas puede reducir en gran manera el riesgo.

Bibliografía

- Klaus-Peter Kossakowski,
  "Handbook for Computer Incident Response Teams (CSIRTs)", CERT/CC.
- T.Grance et al, "Computer Security Incident Handling Guide (800-61)", NIST.
- Julia H.Allen, "The CERT Guide to System and Network Security Practices", Addison-Wesley.
- W.Richard Stevens, "TCP/IP Illustrated Guide – Volume 1 and 2", Addison-Wesley.
- Kenneth R.van Wyk, "Incident Response", O'Reilly.
- Ed.Skoudis, "Counter Hack", Prentice-Hall.
- S.Northcutt, "Inside Network Perimeter Security", New Riders.
- S.Northcutt, "Network Intrusion Detection", New Riders.
- Honeynet Project, "Know your Enemy", Addison-Wesley.

Agradecimientos

- Personal del Centre de Supercomputació de Catalunya.
- Organizadores del Foro:
  - Universidad de Santiago de Compostela (USC).
  - Red.ES/RedIRIS.
- Personal de IRIS-CERT de RedIRIS.
- Instructores/colaboradores SANS Institute:
  - Jess García, David Barroso.
- Asistentes al evento.
- Familia, amigos, etc.