

Universidad Tecnológica del Valle del Mezquital

1er. Encuentro de Informática

26 julio 2001

Seguridad en Redes

Dr. Roberto Gómez Cárdenas

DCC del ITESM-CEM

rogomez@campus.cem.itesm.mx

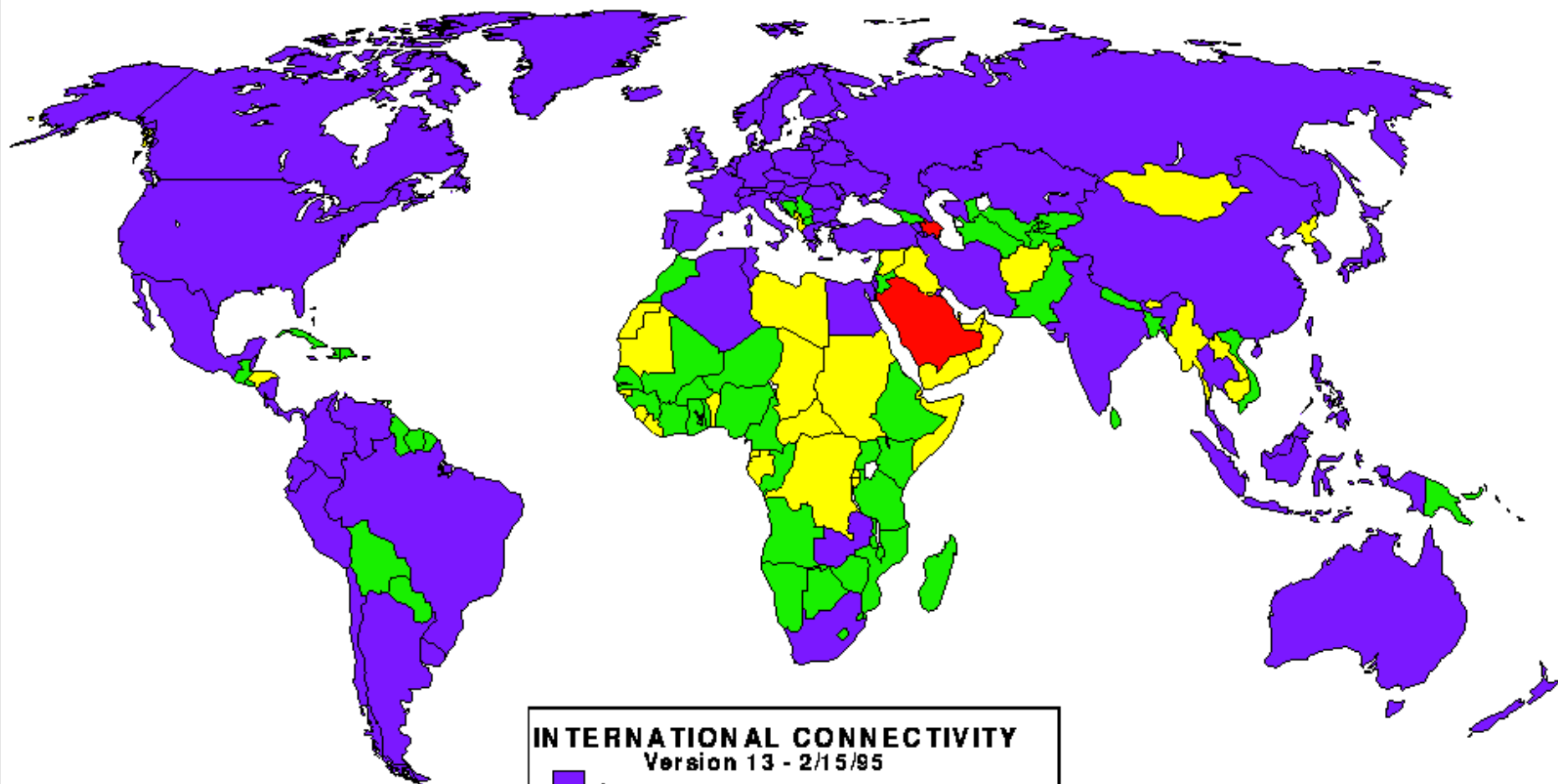
<http://webdia.cem.itesm.mx/dia/ac/rogomez>

La invencibilidad depende de uno mismo; la vulnerabilidad del enemigo, de él.

La invencibilidad reside en la defensa; la posibilidad de la victoria en el ataque.

Sun Tzu

"El arte de la guerra"



INTERNATIONAL CONNECTIVITY

Version 13 - 2/15/95

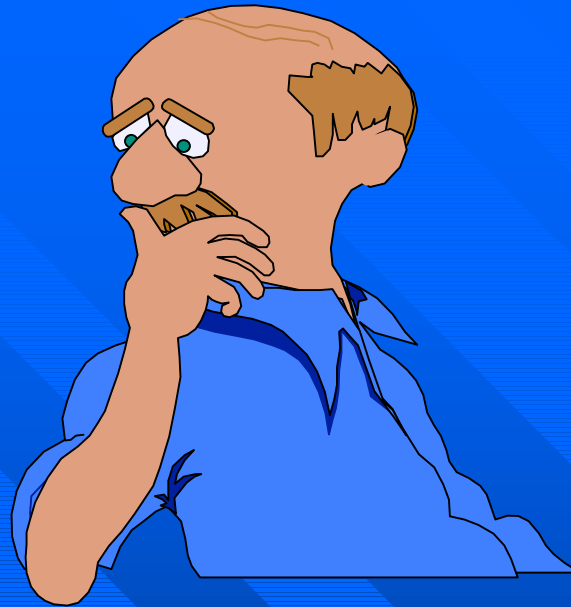
- Internet
- Bitnet but not Internet
- EMail Only (UUCP, FidoNet)
- No Connectivity

This map may be obtained via anonymous ftp
from <ftp://cs.wisc.edu/connectivity/table/directory>

Copyright © 1995
Larry Landweber
and the Internet Society.
Unlimited permission to
copy or use is hereby granted
subject to inclusion of
this copyright notice.

El riesgo

- Desafortunadamente, este gran crecimiento incluirá (incluye) individuos deshonestos cuyo pasatiempo es introducirse en sistemas
- Ninguna institución está libre del asecho de estos individuos.
- Todo el mundo alguna vez ha sido afectado por algún problema de seguridad computacional.



¿¿De que o de quien me debo
preocupar??

¿¿hay peligro??

El Hacker: La Vieja Guardia



- Origen del término a finales de los 60.
- Programador con alto dominio de su profesión, capaz de solucionar problemas a través de hacks (segmentos de código muy ingenioso).
- Verdaderos conocedores de la tecnología de cómputo y telecomunicaciones (85-93).
- La búsqueda del conocimiento siempre fue su fuerza impulsora.

El cracker



- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas computacionales. Una vez logrado el acceso produce daños a los recursos del sistema atacado.
- No necesariamente tiene el mismo nivel de conocimientos que el hacker

La nueva generación o los “Scripters”

- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al inframundo.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy “cool”.



El Hacker: La Visión del Resto de los Usuarios

- ¿Qué es eso?
- Eso pasa solo en las películas.
- Así como los de "The Net"
- Yo soy hacker.
- Yo apenas sé como se usa una computadora.
- Bill Gates se va a encargar de ellos.

Hackers más Famosos.

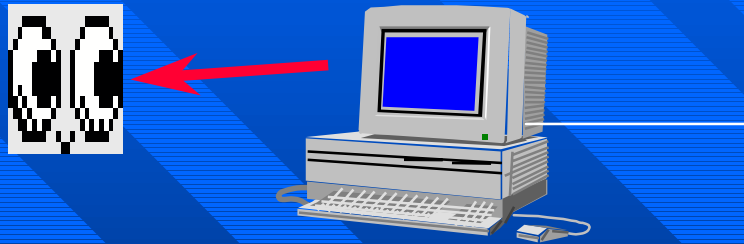
(www.discovery.com/area/technology/hackers/hackers.html).



[illegible]

Tipos de Ataques

Ataques Pasivos.



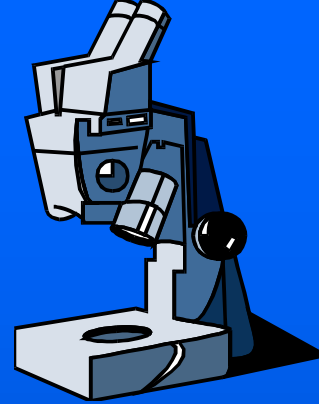
Ataques Activos.



Principales Ataques

- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Stack overflow
- Pepena
- Bombas lógicas
- Dedos inexpertos
- Falsificación
- Usurpación
- Sniffers
- Spam y hoaxes
- Grafiti
- Ingeniería Social
- Negación de servicio

Virus



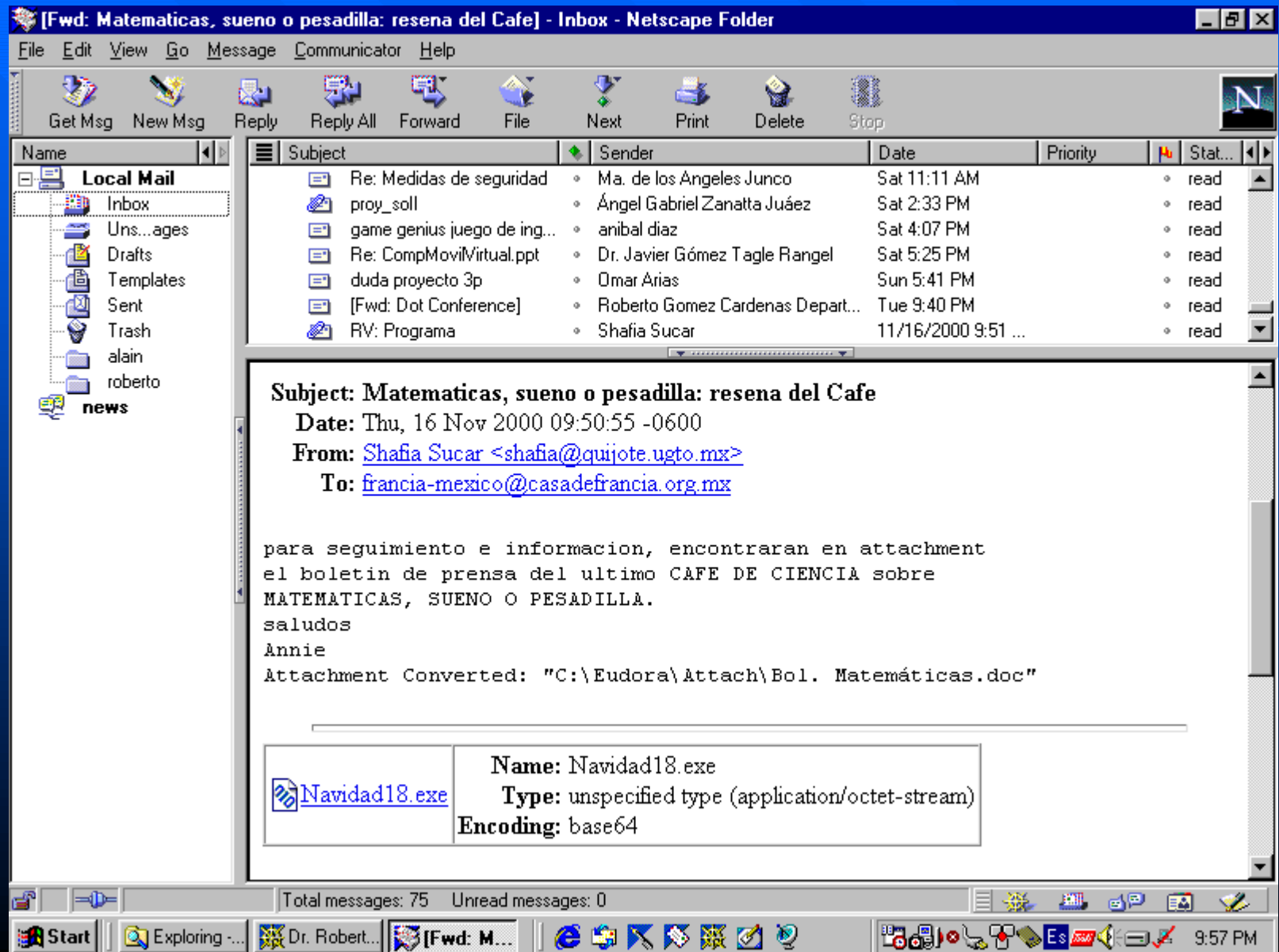
- Un virus se define como una porción de código de programación cuyo objetivo es implementarse a si mismo en un archivo ejecutable y multiplicarse sistemáticamente de un archivo a otro.
- Además de esto, los virus están diseñados para realizar una acción concreta en los sistemas informáticos..
 - la simple aparición de un mensaje en la pantalla
 - destrucción de toda la información

Los gusanos

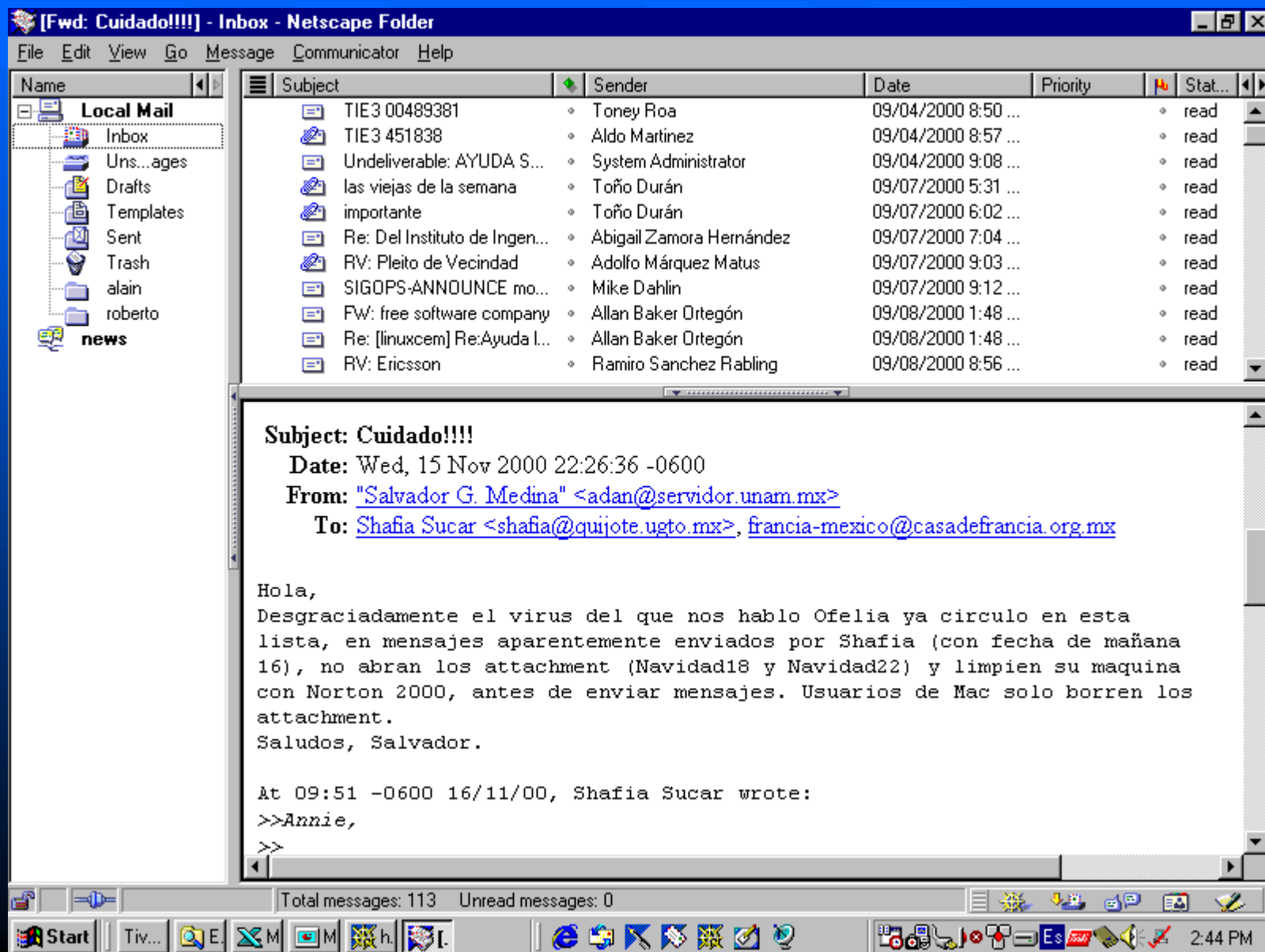
Es un programa que produce copias de sí mismo de un sistema a otro a través de la red; en las máquinas que se instala, produce enormes sobre-cargas de procesamiento que reducen la disponibilidad de los sistemas afectados.



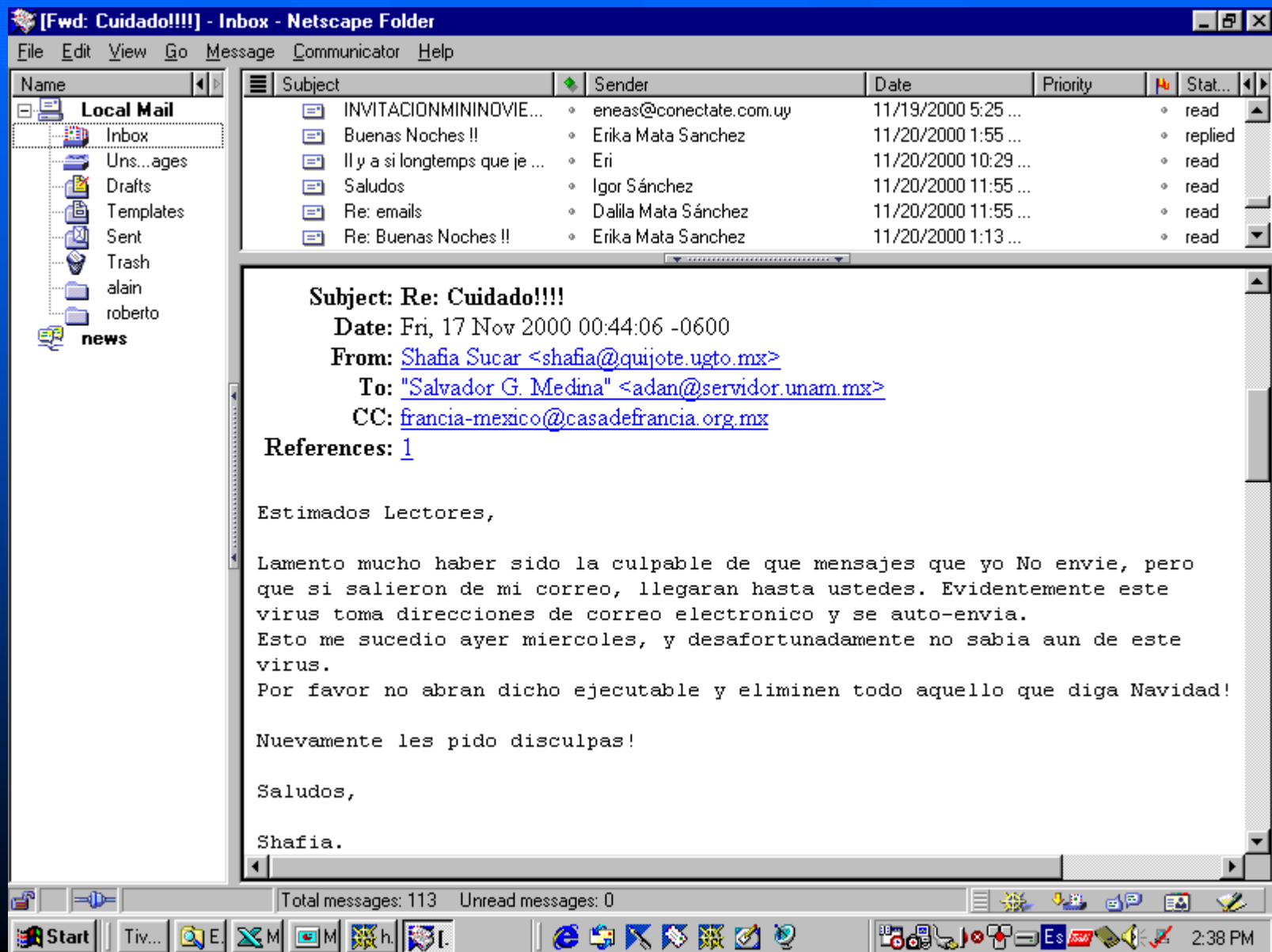
El gusano navidad.exe (1)



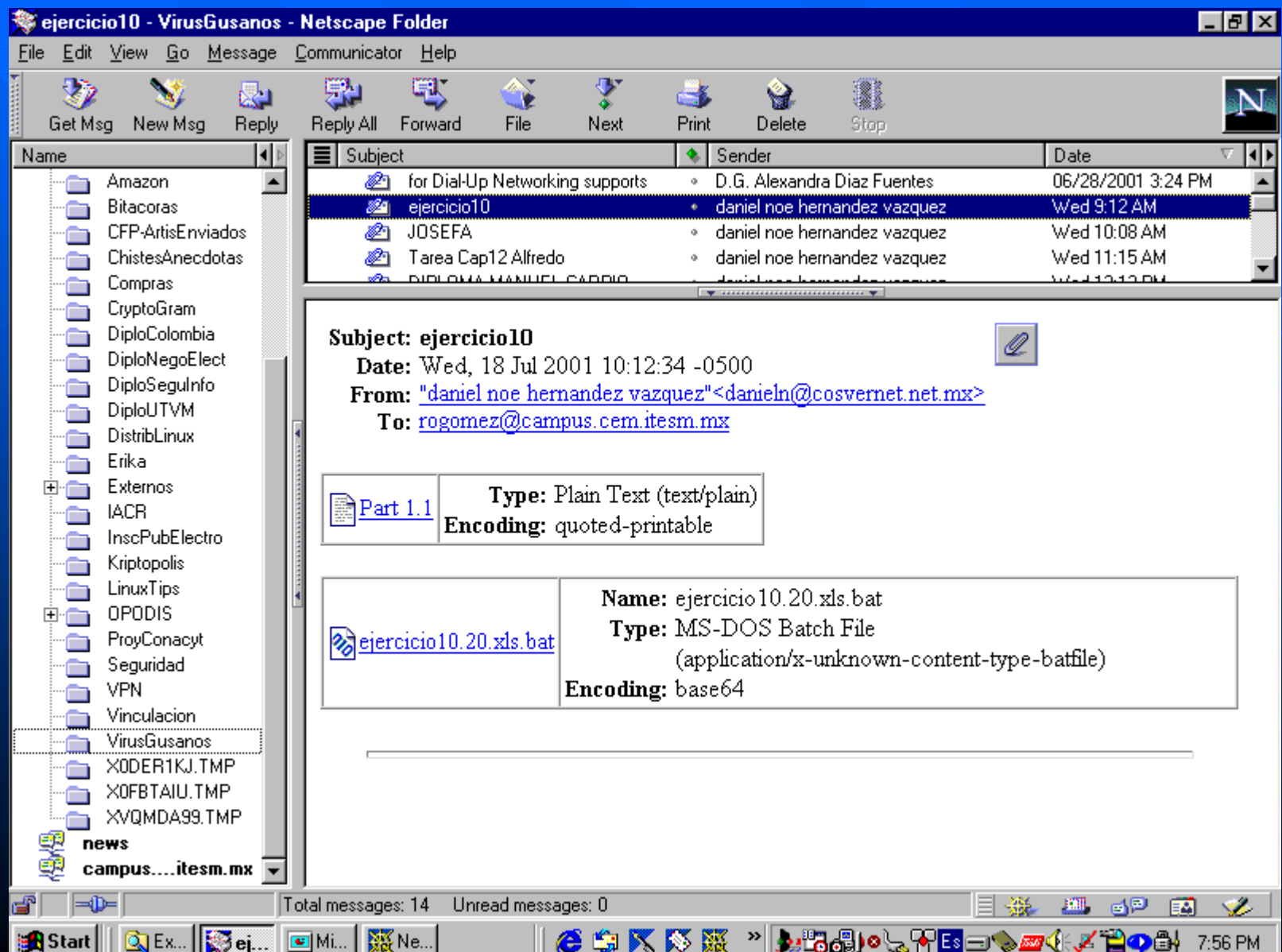
El gusano navidad.exe (2)



El gusano navidad.exe (3)



Lo último: W32.Sircam.Worm

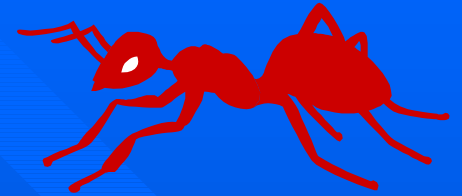


El Caballo de Troya

- Objetivo principal: recuperación información confidencial de un organismo o un usuario
- Se basa en substituir un programa de servicio común por uno alterado por el intruso para recuperar información



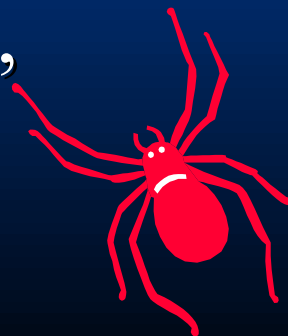
Bugs



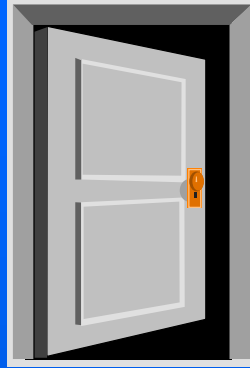
- Un bicho (Bug) es cualquier error introducido accidentalmente en un programa



- Estos errores se vuelven un problema cuando los programas afectados son de vital importancia para el funcionamiento del sistema, por ejemplo: Sistemas operativos, Protocolos de comunicación, etc.



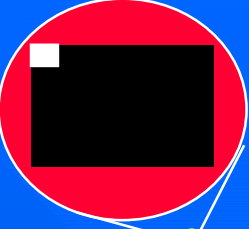
Trapdoors



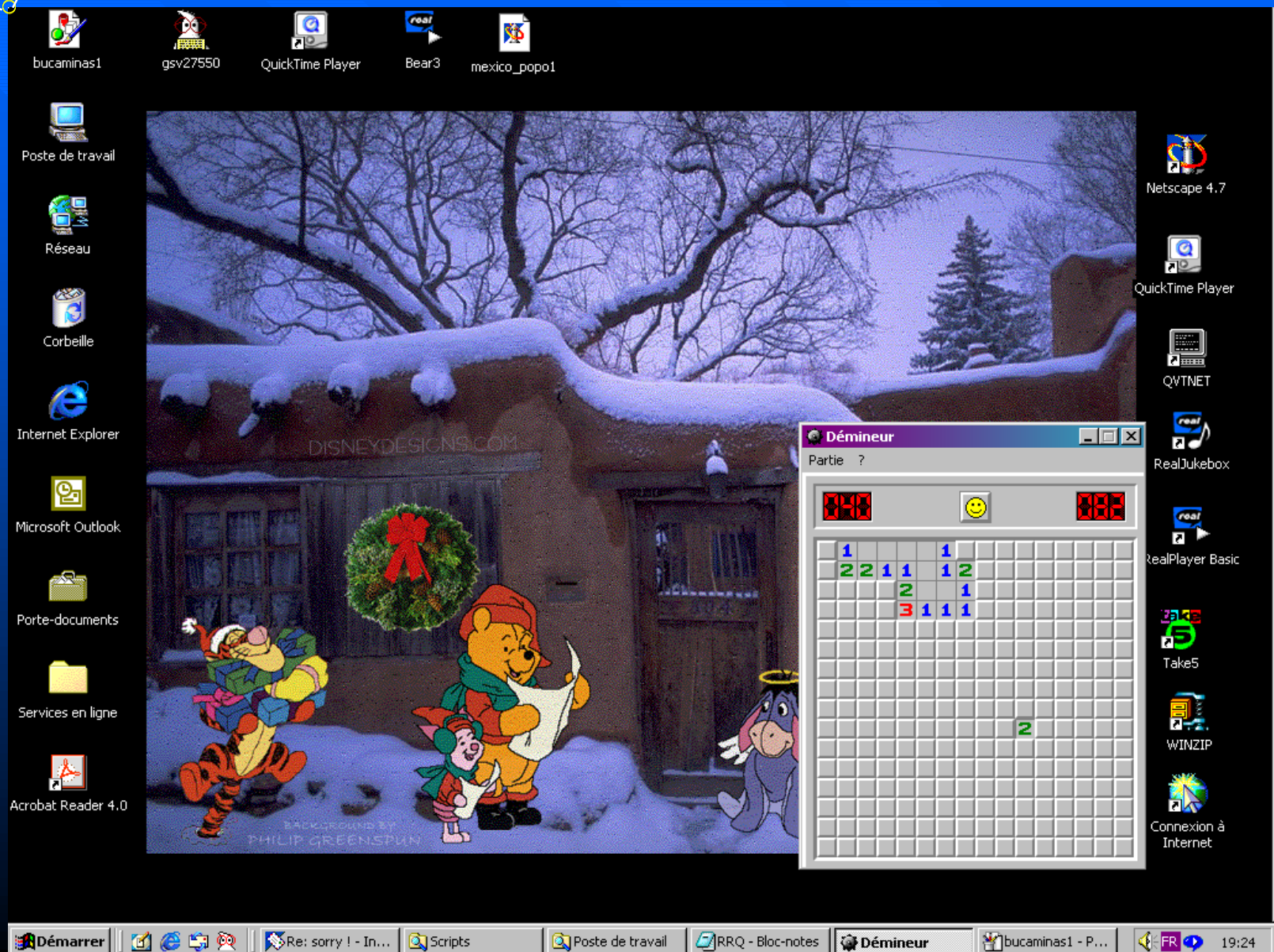
- Es frecuentemente creado por el diseñador del sistema; sin embargo, en ocasiones existe por accidente.
- Algunas veces es creado durante las pruebas de implementación de un sistema y después es olvidado.
- Otras veces, es usado por el proveedor para “atar” al cliente que compro dicho sistema.

Ejemplo Backdoor

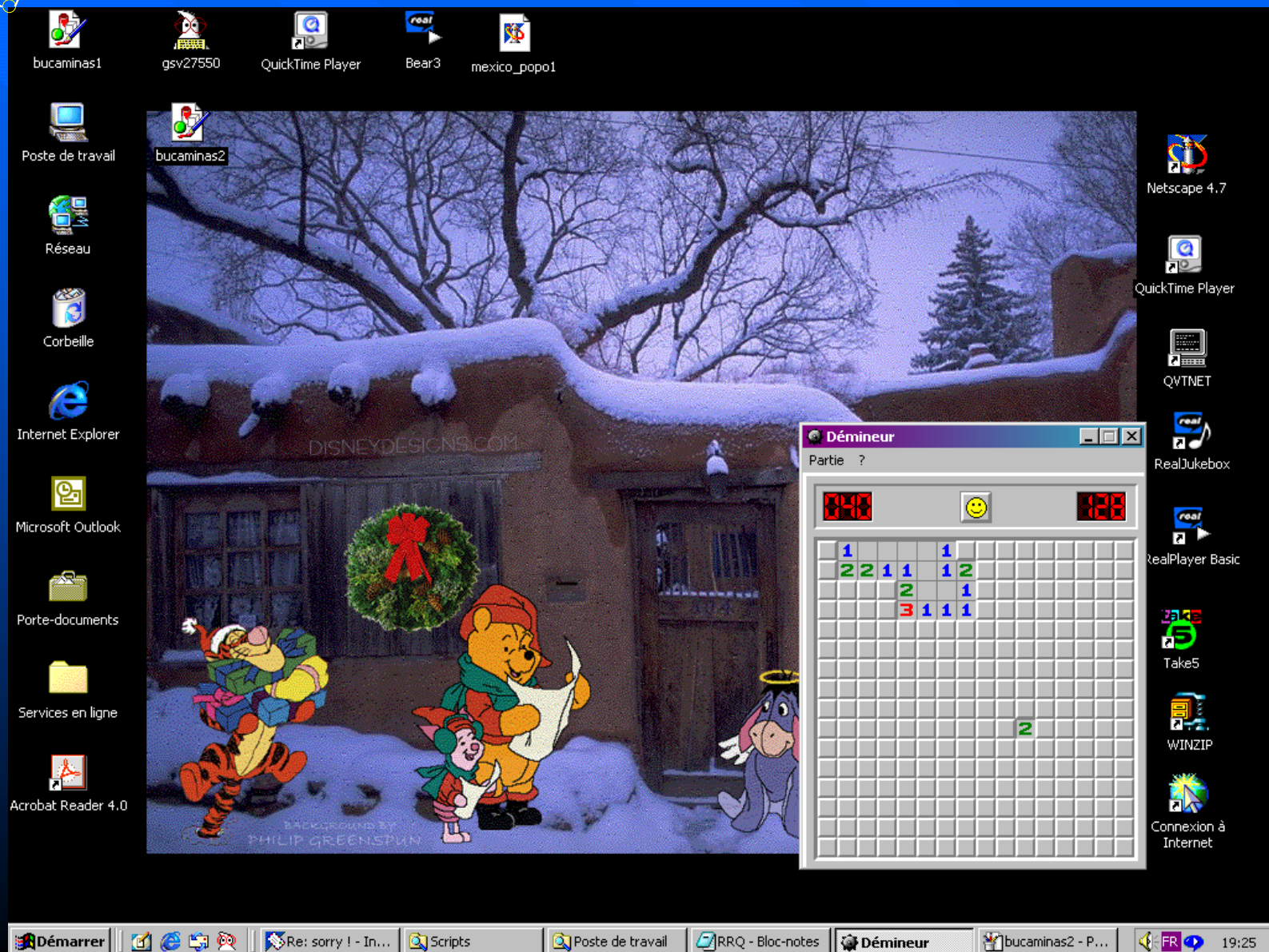
- Programa buscaminas de Windows 2000
- Correr Minesweeper, teclear “xyzzy” y presionar Shift + Enter.
- Buscar un pixel blanco en la parte superior izquierda de la pantalla
 - si no se ve configurar pantalla
 - conforme se mueve el raton por las celdas del buscaminas el pixel desaparece y aparece: desaparece cuando hay una mina en la celda y viceversa



Trapdoor en buscaminas (2)



Trapdoor en buscaminas (3)



Trapdoor en buscaminas (4)

The screenshot shows a Windows XP desktop with a Disney-themed background featuring Winnie the Pooh, Tigger, and Eeyore in a snowy setting. The desktop has several icons on the left (bucaminas1, Poste de travail, Réseau, Corbeille, Internet Explorer, Microsoft Outlook, Porte-documents, Services en ligne, Acrobat Reader 4.0) and top (bucaminas1, gsv27550, QuickTime Player, Bear3, mexico_popo1). On the right, there are icons for Netscape 4.7, QuickTime Player, QVTNET, RealJukebox, RealPlayer Basic, Take5, WINZIP, and Connexion à Internet. A Minesweeper game window titled "Démineur" is open, showing a 10x10 grid with numbers and a message: "Vous avez fait le meilleur temps du niveau intermédiaire. Entrez votre nom." with a text box containing "rogomez" and an "OK" button. The taskbar at the bottom shows the Start button and several open applications: Re: sorry ! - In..., Scripts, Poste de travail, RRQ - Bloc-notes, Démineur, bucaminas3 - P..., and FR.

Desktop icons (left to right, top to bottom):

- bucaminas1
- Poste de travail
- Réseau
- Corbeille
- Internet Explorer
- Microsoft Outlook
- Porte-documents
- Services en ligne
- Acrobat Reader 4.0

Desktop icons (top to bottom, left to right):

- bucaminas1
- gsv27550
- QuickTime Player
- Bear3
- mexico_popo1
- bucaminas2
- bucaminas3

Desktop icons (right side, top to bottom):

- Netscape 4.7
- QuickTime Player
- QVTNET
- RealJukebox
- RealPlayer Basic
- Take5
- WINZIP
- Connexion à Internet

Minesweeper game window (Démineur):

Partie ?

Vous avez fait le meilleur temps du niveau intermédiaire. Entrez votre nom.

rogomez

OK

Taskbar (bottom):

- Démarrer
- Re: sorry ! - In...
- Scripts
- Poste de travail
- RRQ - Bloc-notes
- Démineur
- bucaminas3 - P...
- FR
- 19:29

El stack o buffer overflow

- Ataque se remonta al año de 1988.
- Se dan a conocer los detalles de dicho ataque en noviembre 1996 (Phrack Magazine, número 49).
- Se produce una situación de desbordamiento del búfer cuando un usuario o un proceso intenta introducir en el búfer más datos de los originalmente permitidos.
- Aprovechando esta situación se puede conseguir acceder fraudulentamente al sistema.

Stack/buffer overflow

```
main()
```

```
{
```

```
:
```

```
count = read(fd, bytes, buf)
```

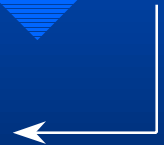
```
:
```

```
}
```



Variables locales
al main

SP



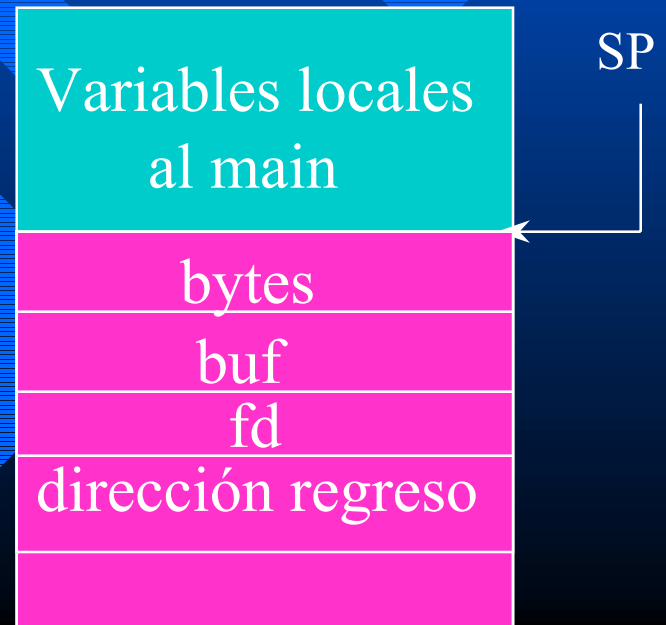
Stack

Stack/buffer overflow

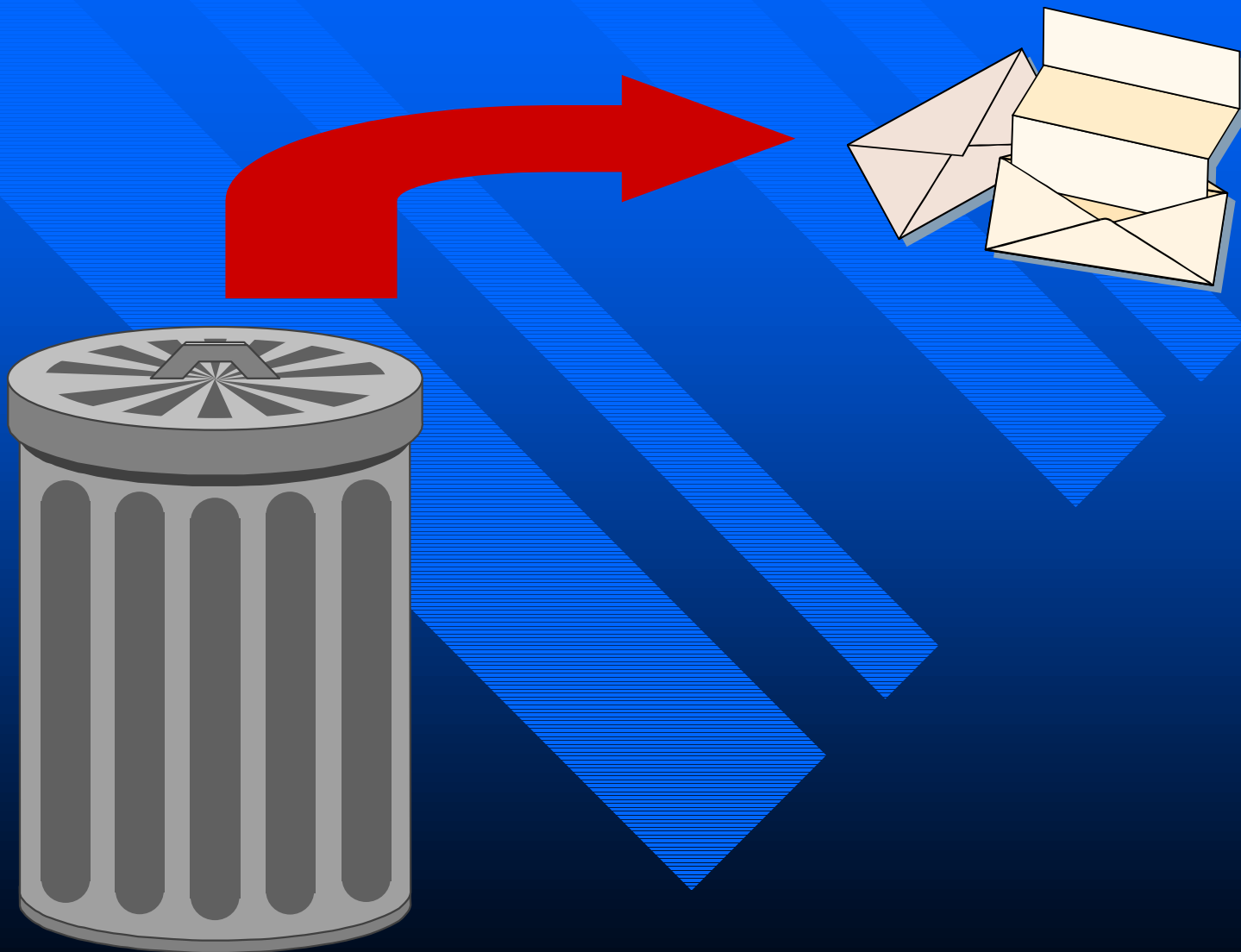
```
main()
{
    :
    count = read(fd, bytes, buf)
    :
}
```



```
main()
{
    :
    count = read(fd, bytes, buf)
    :
}
```



Pepena



Bomba lógica

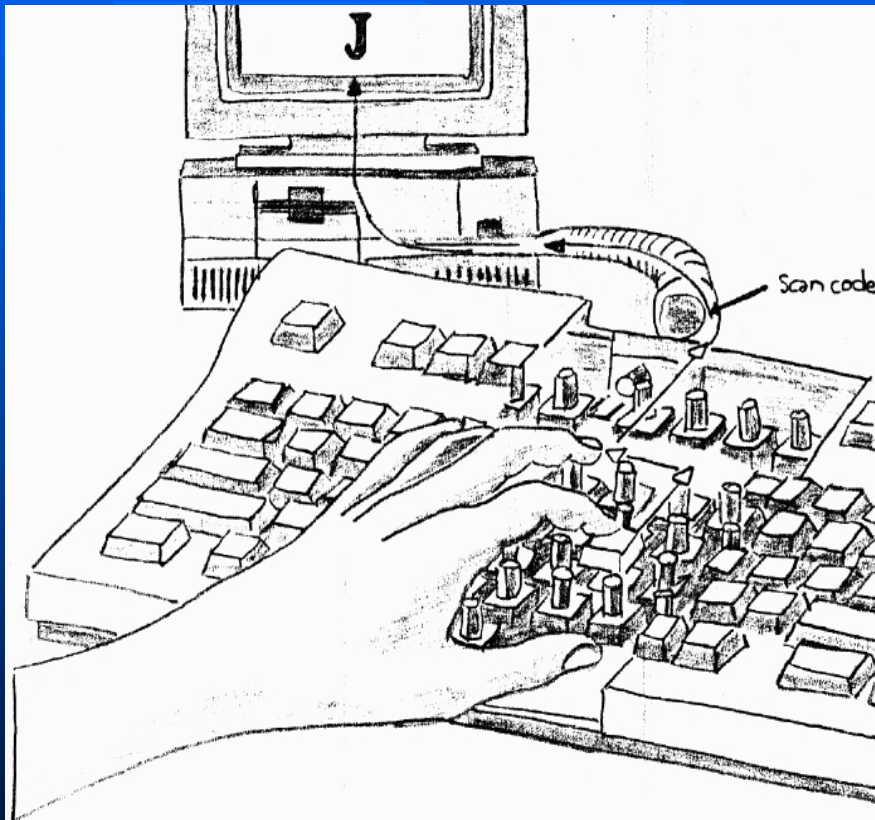
- Una bomba lógica es una modificación en un programa que lo obliga a ejecutarse de manera diferente bajo ciertas circunstancias
- Bajo condiciones normales, el programa se comporta como previsto y, la bomba no puede ser detectada.

- Un ejemplo de pseudocódigo es:

```
IF Profesor = jvazquez THEN salario == Horas * Rango * 1.1  
ELSE salario == Horas * Rango
```



Dedos inexpertos

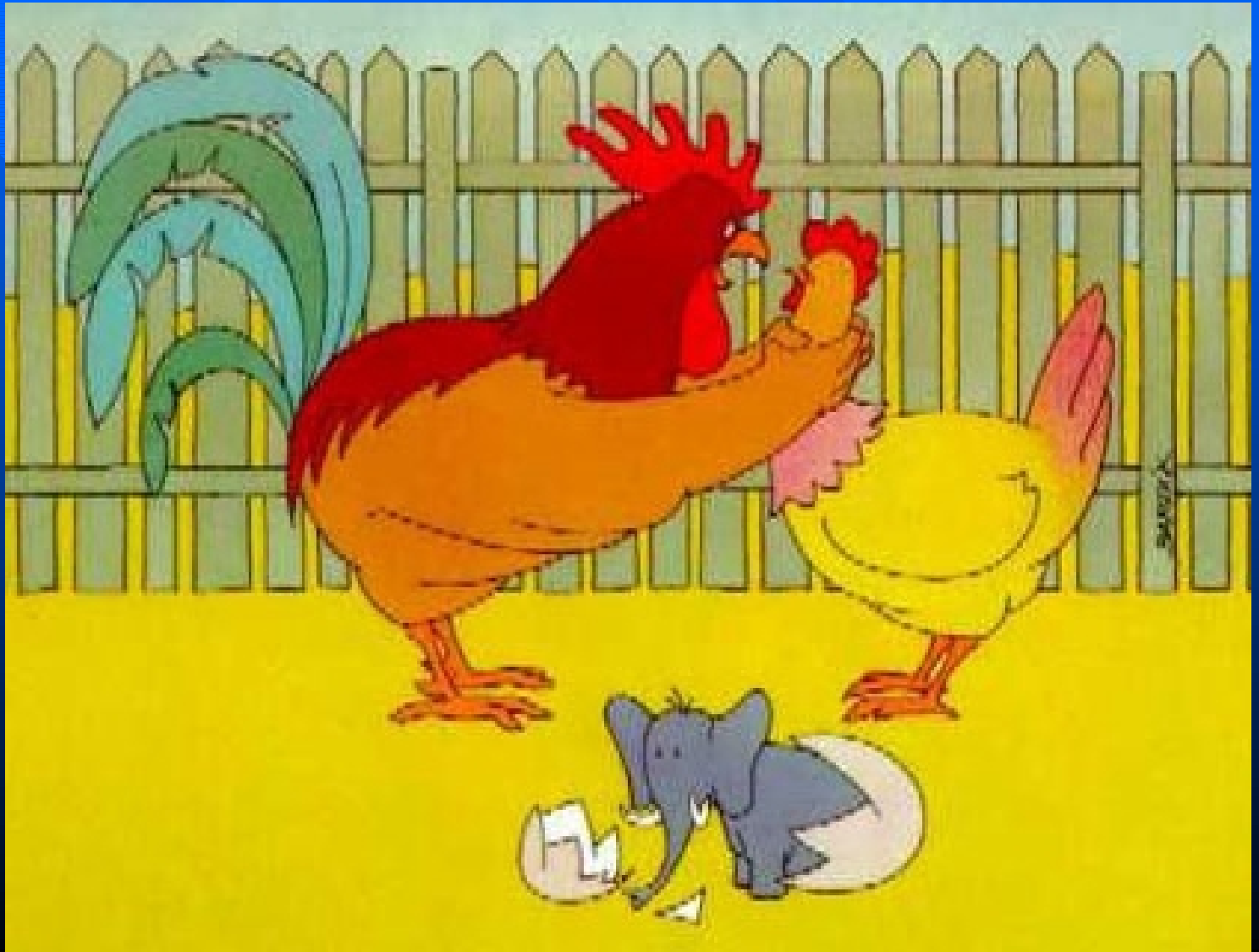


Falsificación

- El atacante escribe información falsa haciéndose pasar por la víctima.
- Va muy ligado a la usurpación de personalidad.

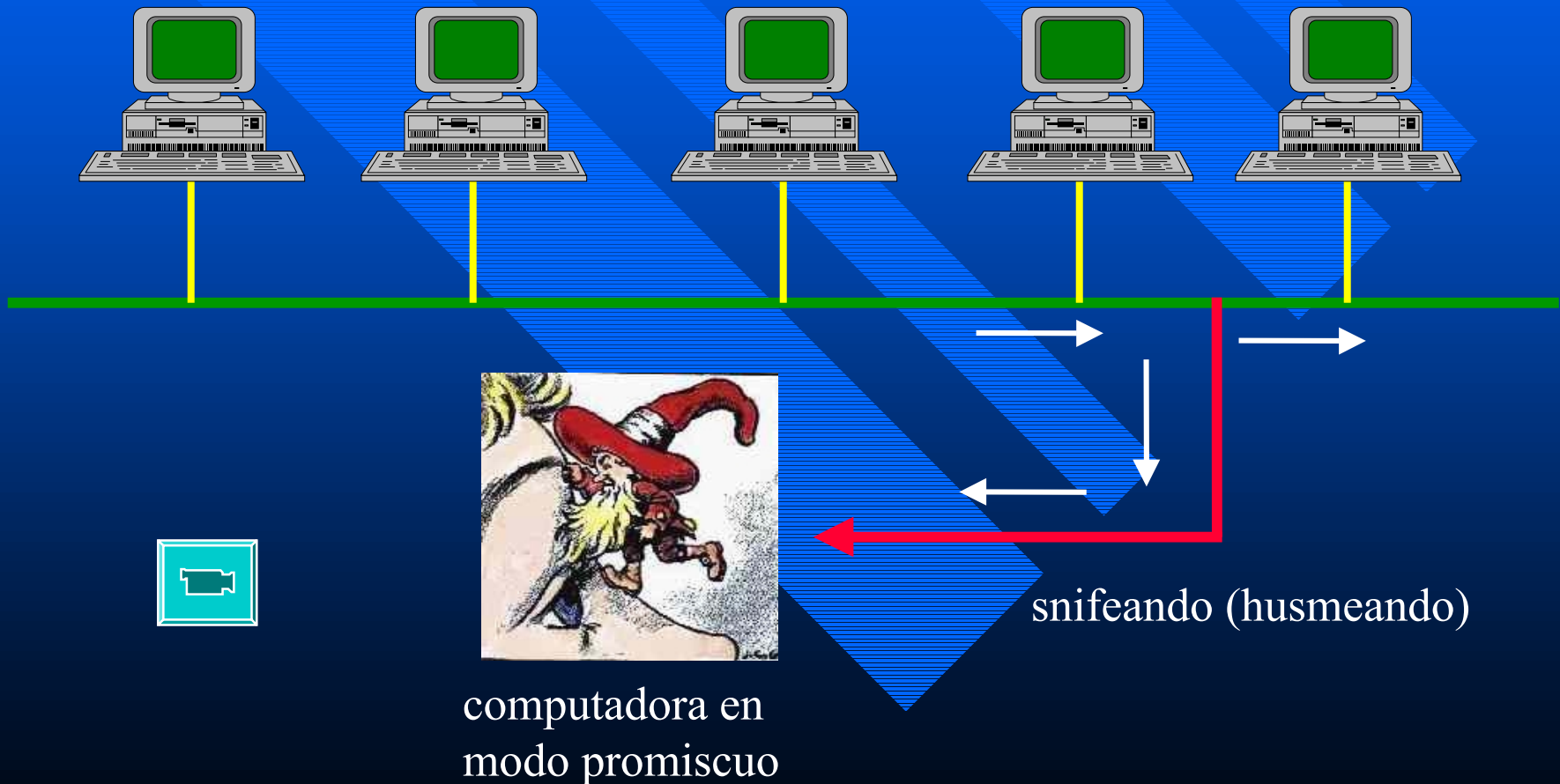


Usurpación

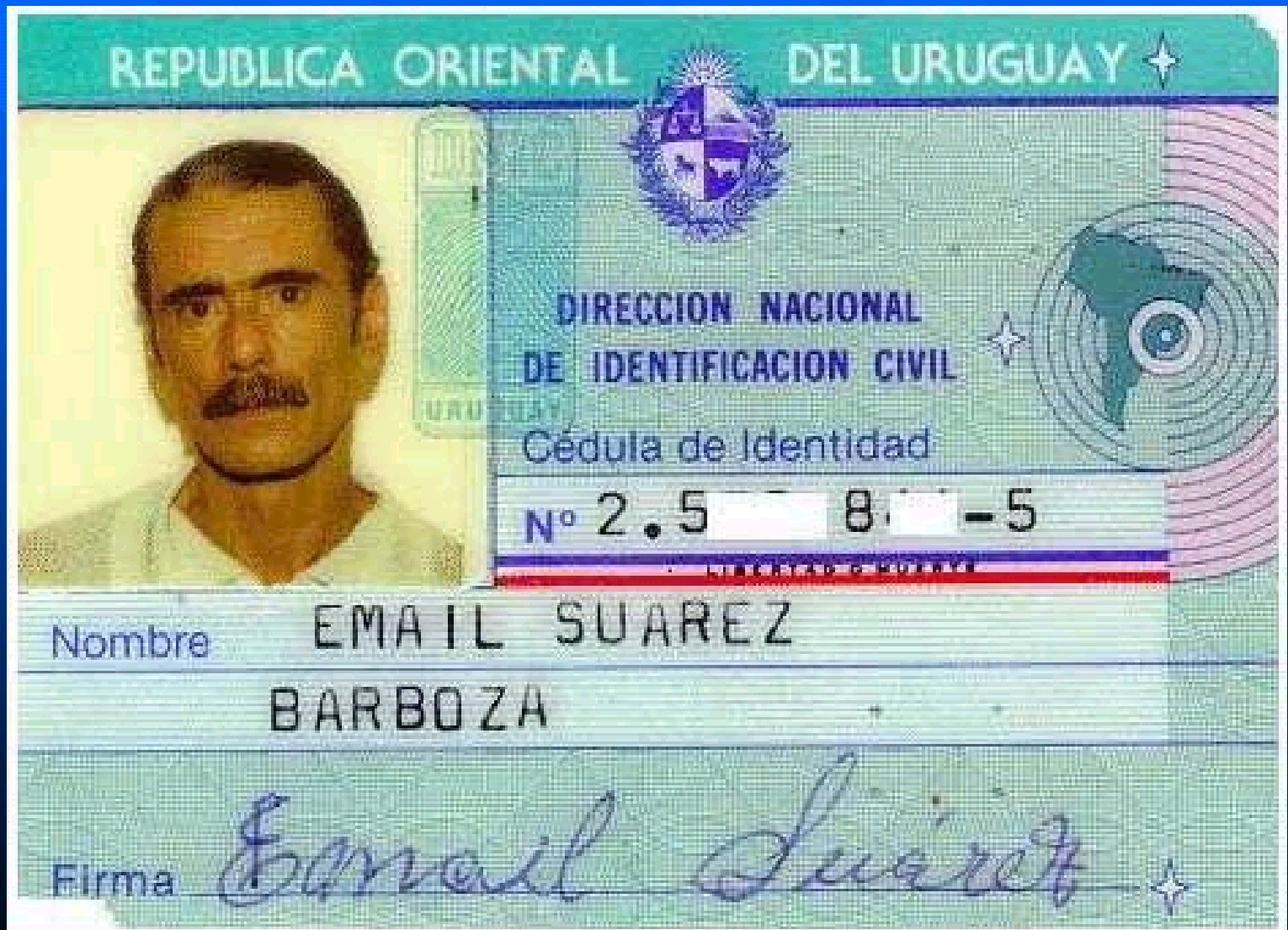


Sniffers

¿Cómo se comunican dos computadoras en una red local?



¿Quién es e-mail?



Spam

■ Cada vez recibimos más correos no deseados:

- Ventas.
- Insultos.
- Bombardeos.
- Pornografía
- Hoax

Hoax

Arq. Xxxxxx wrote:

> Unanse a esta buena causa:

>

> SE TRATA DE LA PEQUEDA LLAMADA JESSICA MYDEK
TIENE SIETE ANOS DE

> EDAD Y SUFRE DE UN AGUDO Y MUY RARO CASO DE
CARCINOMA CEREBRAL.

> ESTA ENFEREMEDAD TERMINAL PROVOCA LA APARICION
DE DIVERSOS TUMORES

> MALIGNOS EN EL CEREBRO.

>

>

Hoax

- LOS DOCTORES LE HAN PRONOSTICADO A JESSICA SEIS MESES DE VIDA, Y
- > COMO PARTE DE SUS ULTIMOS DESEOS ELLA QUIZO INICIAR UNA CADENA DE
 - > E-MAILS INFORMANDO DE SU CONDICION Y ENVIAR EL MENSAJE A LA
 - > GENTE PARA QUE VIVA AL MAXIMO Y DISFRUTEN DE CADA MOMENTO DE SU VIDA,
 - > UNA OPORTUNIDAD QUE ELLA NUNCA TENDRA.
 - >
 - > ADICIONALMENTE, LA SOCIEDAD AMERICANA DE LUCHA CONTRA EL CANCER,
 - > JUNTO CON OTRAS EMPRESAS PATROCINADORAS, ACORDARON DONAR TRES
 - > CENTAVOS QUE SERAN DESTINADOS A LA INVESTIGACION DEL CANCER POR

Hoax

CADA

- > PERSONA QUE ENVIE ESTE MENSAJE.
- > POR FAVOR, DENLE A JESSICA Y A TODAS LAS VICTIMAS DEL CANCER UNA
- > OPORTUNIDAD.
- >
- > Lo unico que tienen que hacer para incrementar el numero de personas en
- > esta cadena es:
- >
- > Primero: dirija este e-mail a ACS@aol.com
- > Segundo: en la parte donde dice CC agregue los e-mails de todos los
- > amigos y colegas que conozca
- >
- > Saludos cordiales,
- > Alfonso



Ingeniería Social.

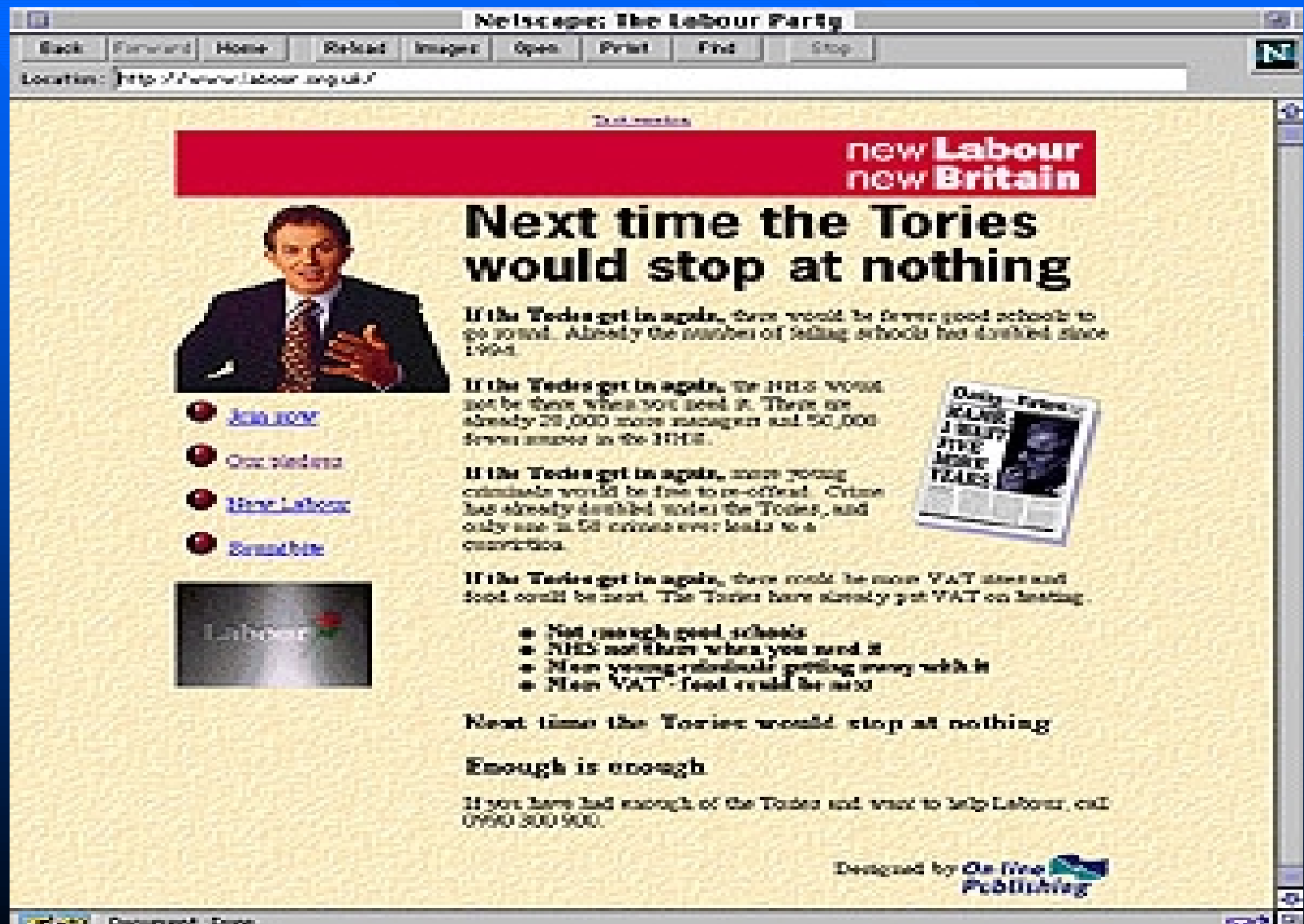
- Es una de las formas más comunes para penetrar sistemas de “alta seguridad”.
- Se basa en ataques como:
usurpación de identidad, pepena, inocencia de la gente, relaciones humanas, etc.



Graffiti

- Consiste en substituir páginas de un organismo por otras.
- El objetivo es dañar la reputación de la empresa
- Este tipo de ataques no tiene un periodo de duración grande

Partido Laboral (Original).



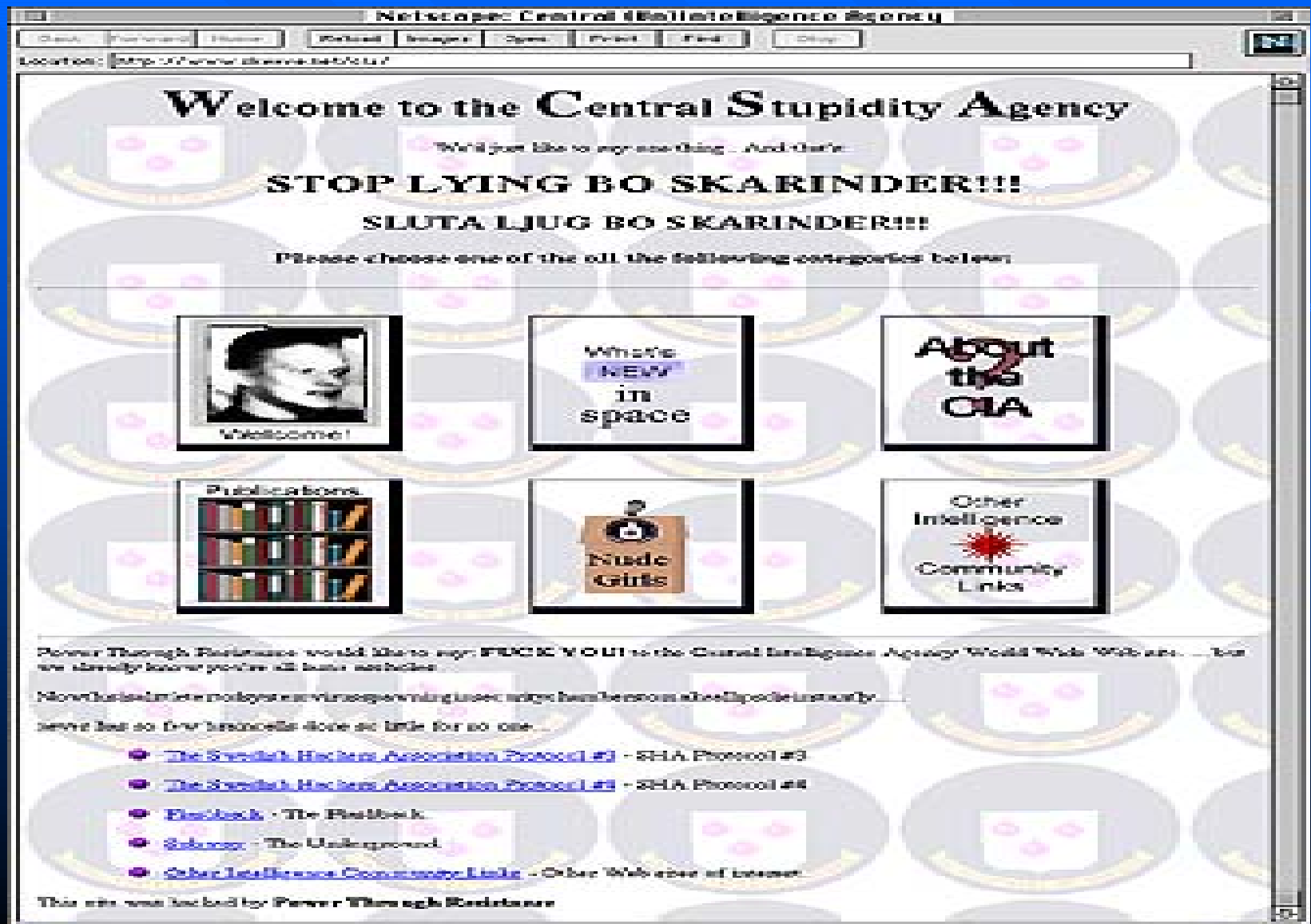
Partido Laboral (Hackeado).



Central Intelligence Agency (Original).



Central Intelligence Agency (Hacked).



Negación de servicio

- Su objetivo principal es impedir que un organismo proporcione el servicio para el que fue creado.
- Generalmente se basa en un ataque a una sola máquina
- Muy difícil de evitar

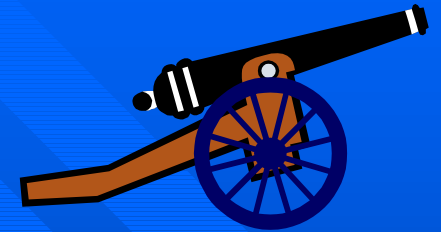
¿Cómo me protejo?

Dos aspectos a cubrir:
el administrativo y el técnico

Seguridad Computacional

El conjunto de políticas y mecanismos que nos permiten garantizar la *confidencialidad*, la *integridad* y la *disponibilidad* de los recursos de un sistema.

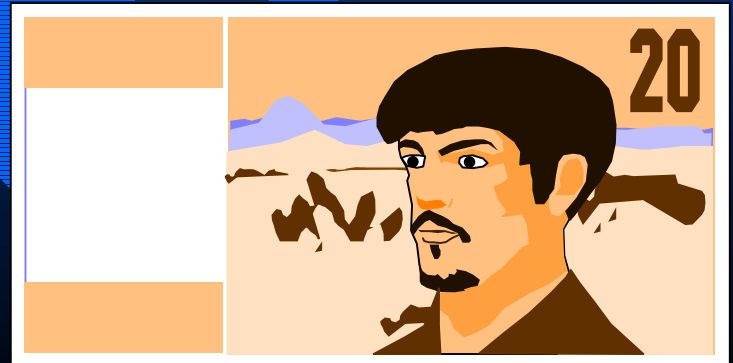
Confidencialidad



Un sistema posee la propiedad de *confidencialidad* si, la información manipulada por éste no es disponible ni puesta en descubierto para usuarios, entidades o procesos no autorizados.

Integridad

Un sistema posee la propiedad de integridad si los datos manipulados por éste no son alterados o destruidos por usuarios, entidades o procesos no autorizados.



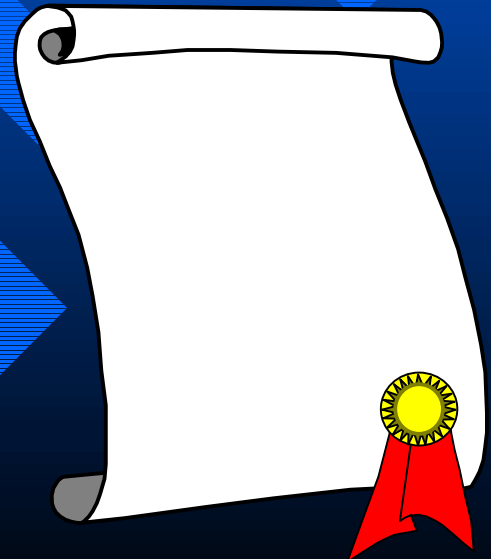
Disponibilidad

Un sistema posee la propiedad de *disponibilidad* si, la información es accesible (está disponible) en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.



Política de Seguridad

- Definición del conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Depende de los objetivos y metas de la organización.

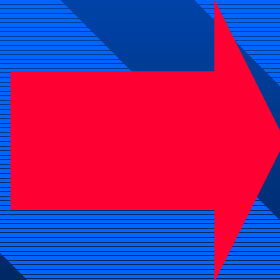


Paradigmas

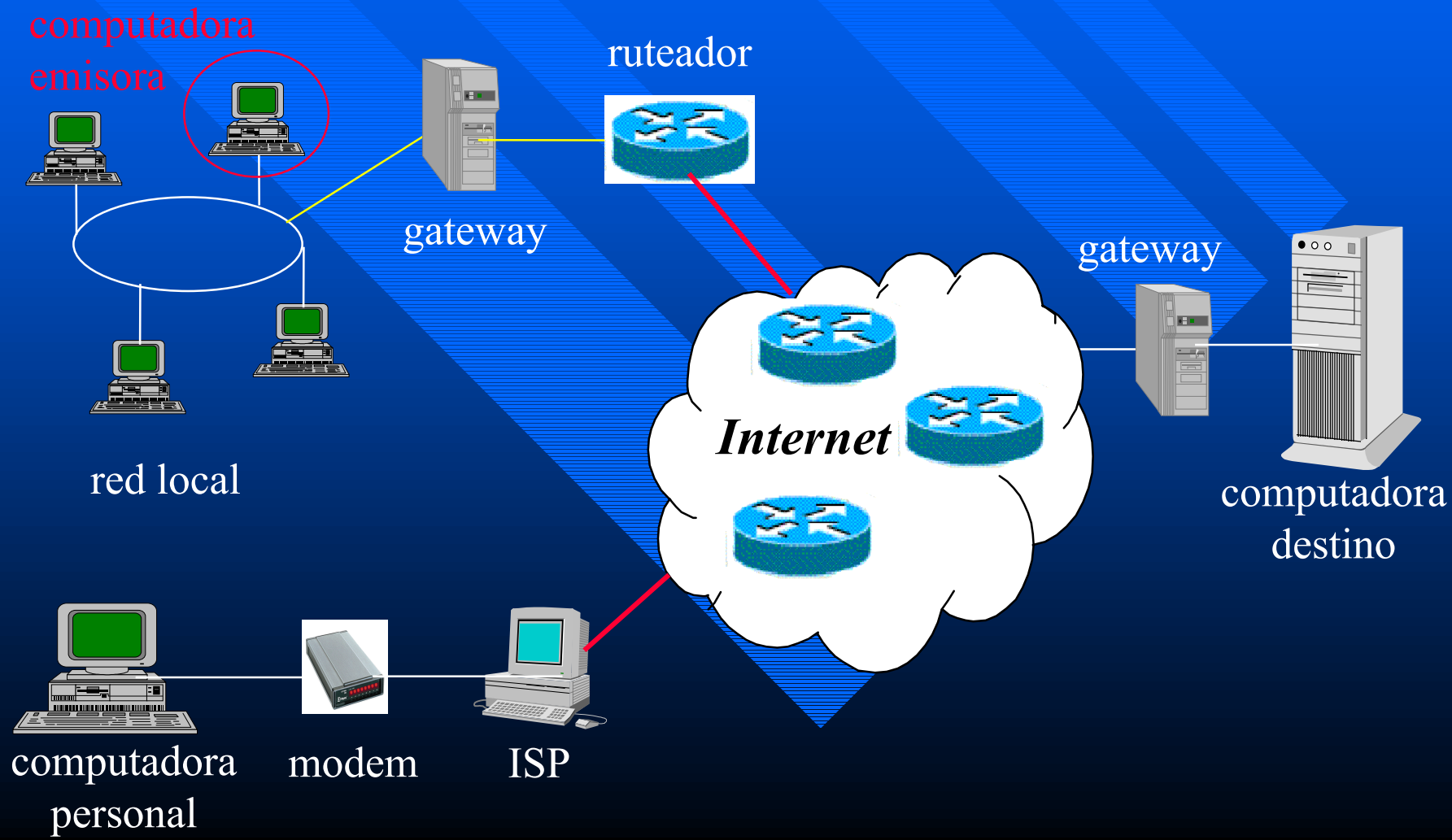
Existen varios paradigmas:

- 1) *Paranoico*: Nada está permitido.
- 2) *Prudente*: Lo que no está expresamente permitido, está prohibido.
- 3) *Permisivo*: Lo que no está expresamente prohibido, está permitido.
- 4) *Promiscuo*: Todo está permitido.

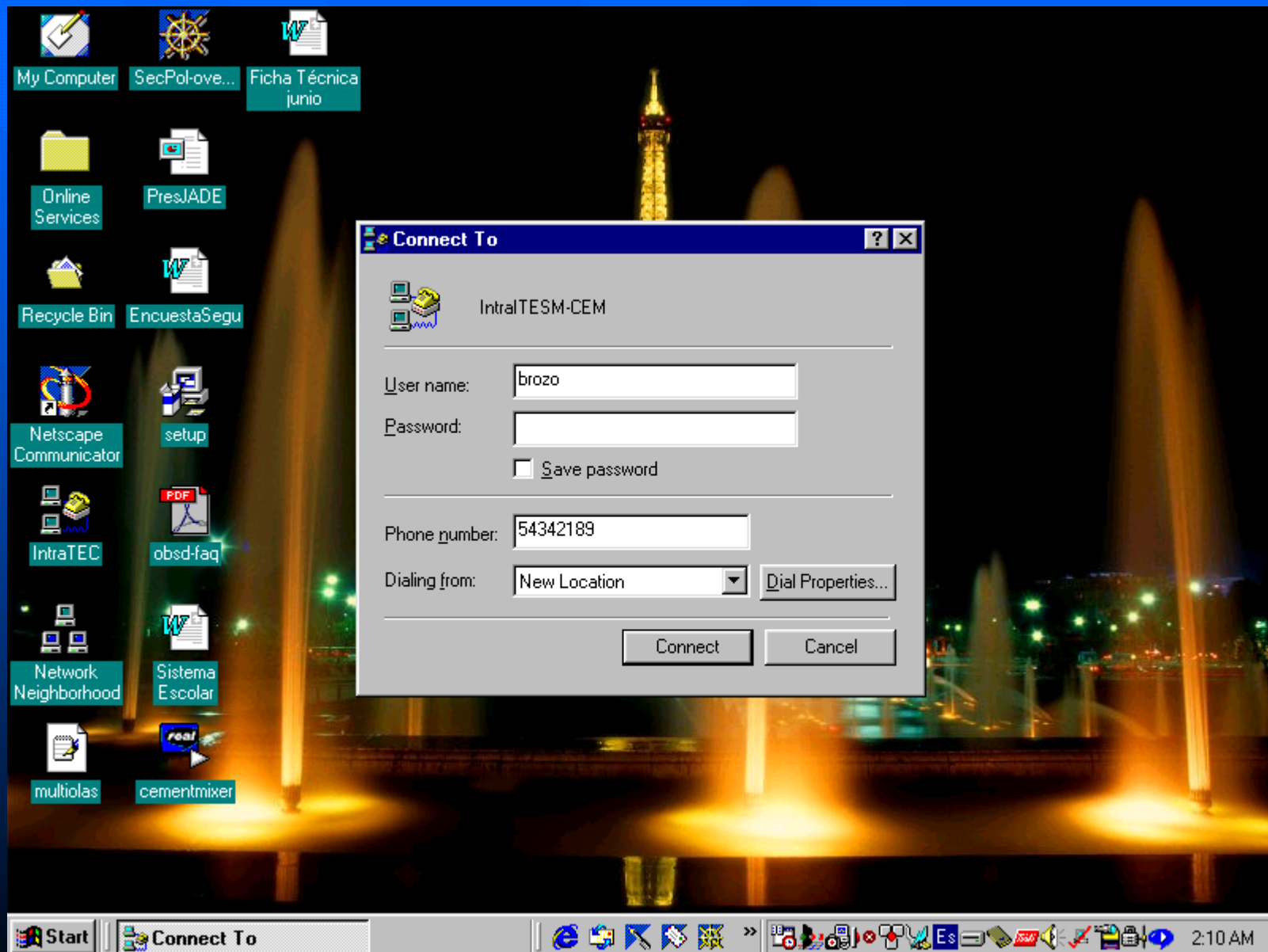
Aspectos Técnicos (definir perímetros)



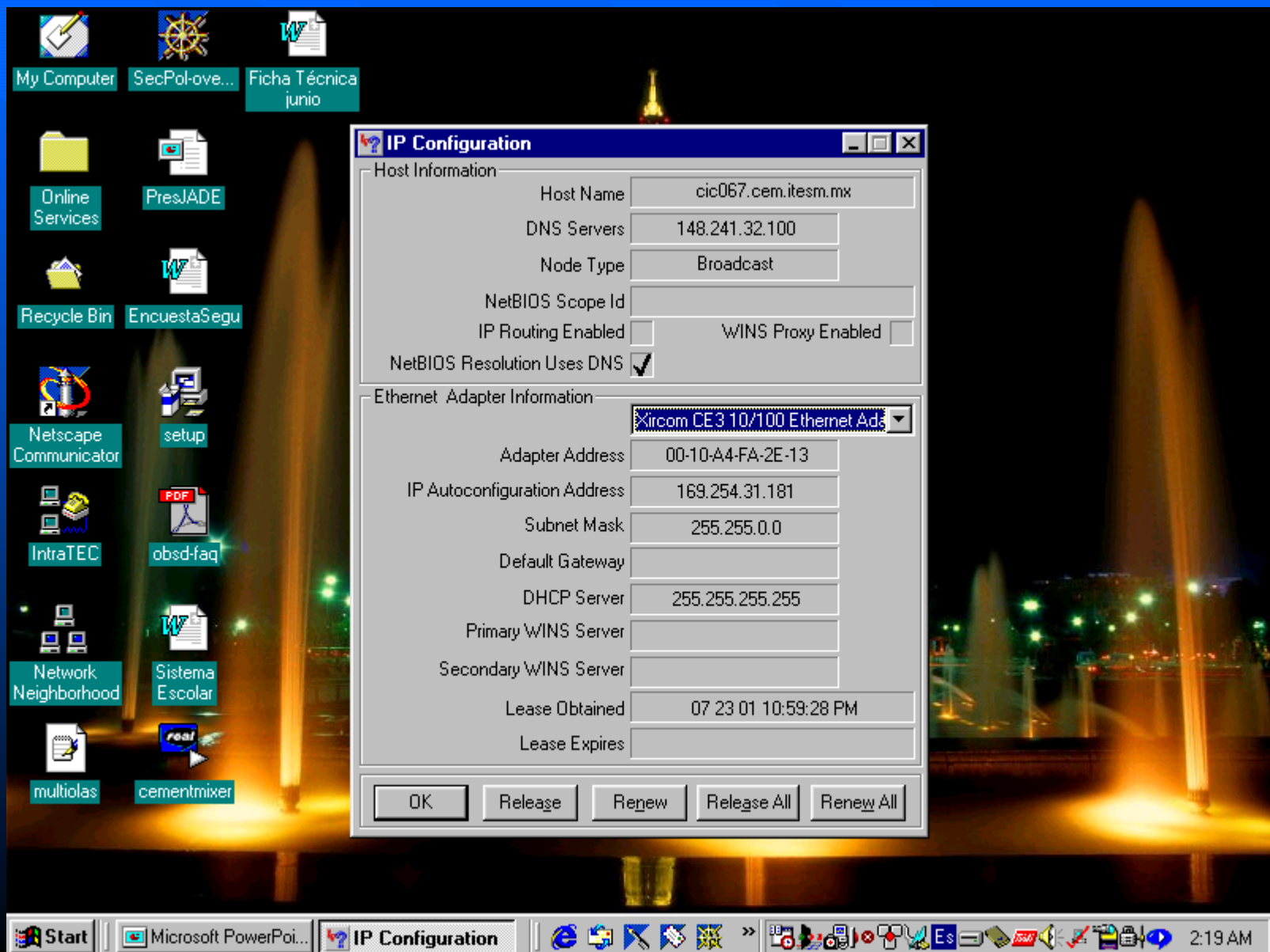
¿Cómo se comunica una computadora con otra?



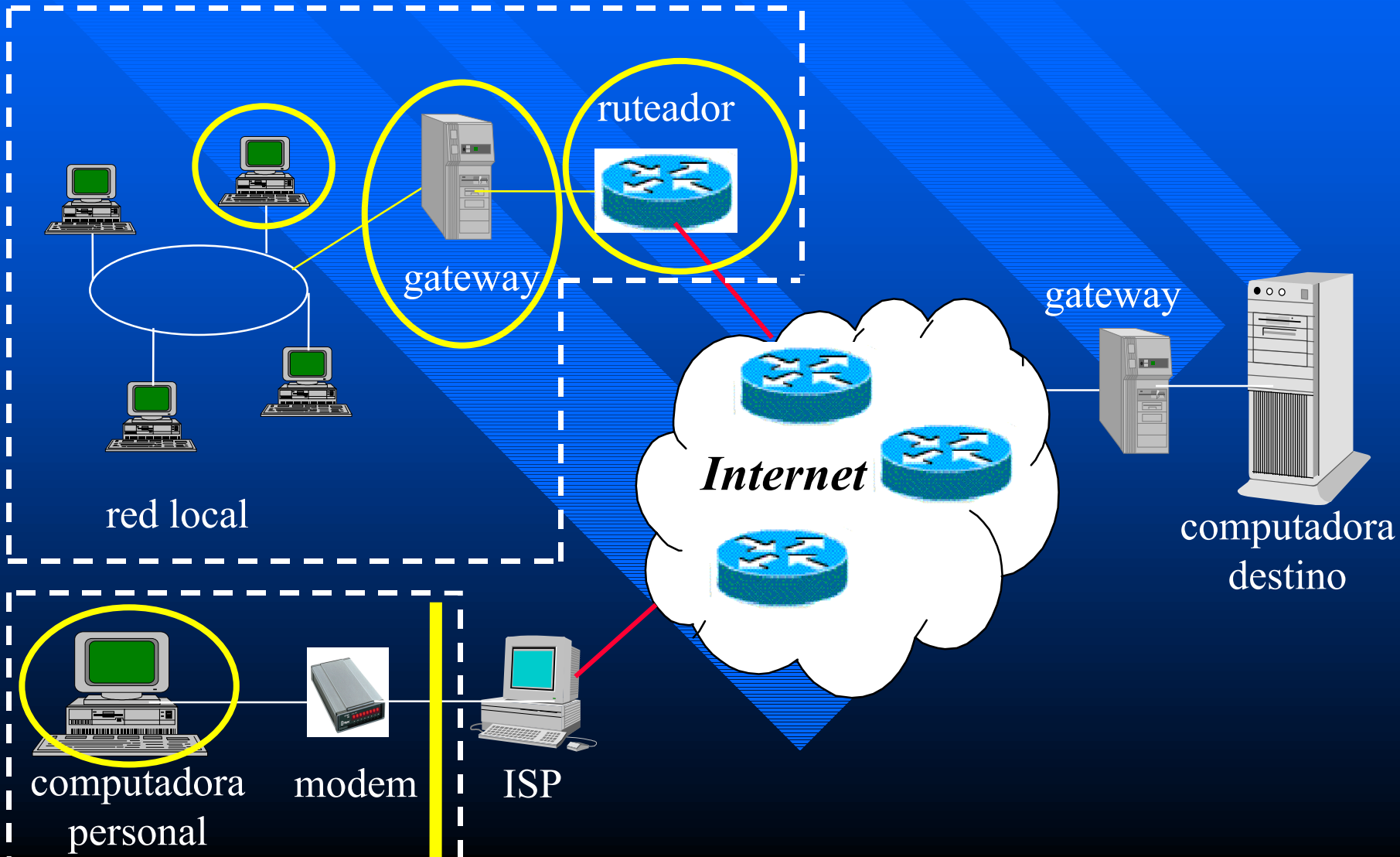
Conexión a través de un ISP



Conexión via gateway



¿Donde poner los perímetros?

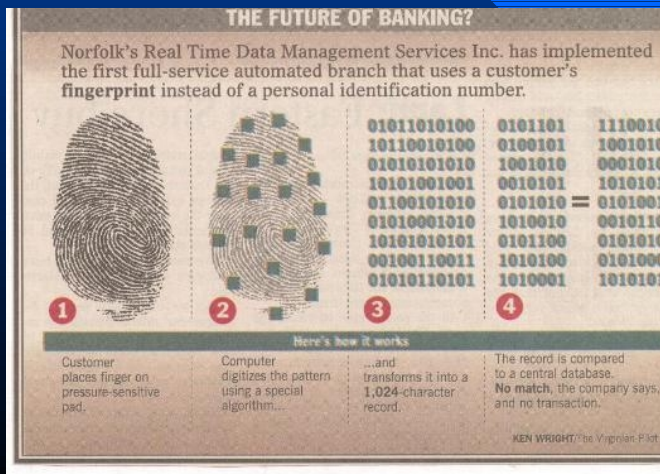


¿En qué consiste el perímetro?

- ¿Quien quiere entrar?
 - autenticación
- ¿A donde puede ir?
 - control de acceso
- Rechazar lo no deseado
 - filtros y firewalls
- ¿Qué quiere hacer adentro?
 - proxies
- Cerrando las puertas traseras
 - cerrando los servicios

Autenticación

- La autenticación se refiere a demostrar la identidad de las entidades involucradas en una comunicación.
- Evita que alguien tome la identidad de otro. Generalmente toma dos formas.



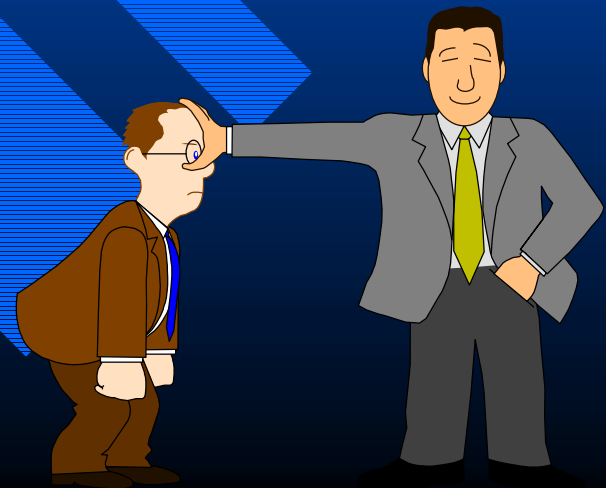
<http://totaleclipsed.hypermart.net/>



KNOCKIN' ON HEAVEN'S DOOR

Control de acceso

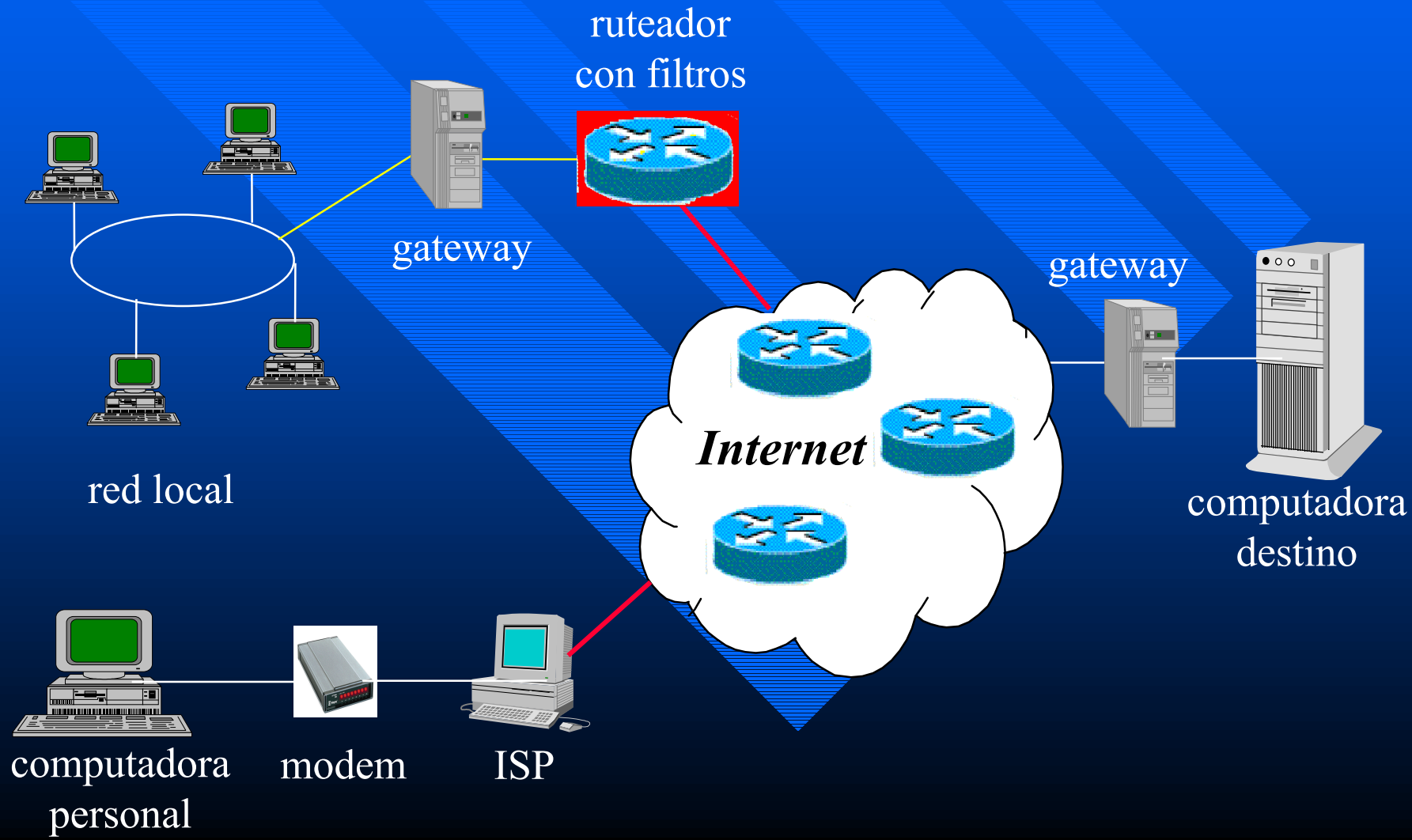
- Permite definir quién puede tener acceso a ciertos recursos, dependiendo de los privilegios o atributos que posea.
- Permite proteger los recursos del sistema contra el uso no autorizado.
- Se aplica a los usuarios y procesos que ya han sido autenticados.



Filtrando la información

- Examinar los paquetes que van hacia afuera o vienen entrando a la red.
- Se definen reglas que permiten dejar pasar el paquete o descartarlo.
- Las reglas se fijan en función de las direcciones, protocolos y puertos, básicamente.
- Programación del ruteador para filtrar paquetes.

Integrando un filtro



¿Qué es un firewall?

Podemos definirlo como una colección de componentes colocados entre dos redes, que en conjunto poseen las siguientes propiedades:

- Todo el tráfico de afuera hacia adentro, y viceversa, debe pasar por el firewall.
- Sólo tráfico autorizado, como establecido previamente en las políticas de la organización, puede pasar a través del firewall.

Esquema general Firewall



Ejemplo reglas de acceso

Demonstration - FireWall-1 Security Policy

File Edit View Manage Policy Window Help

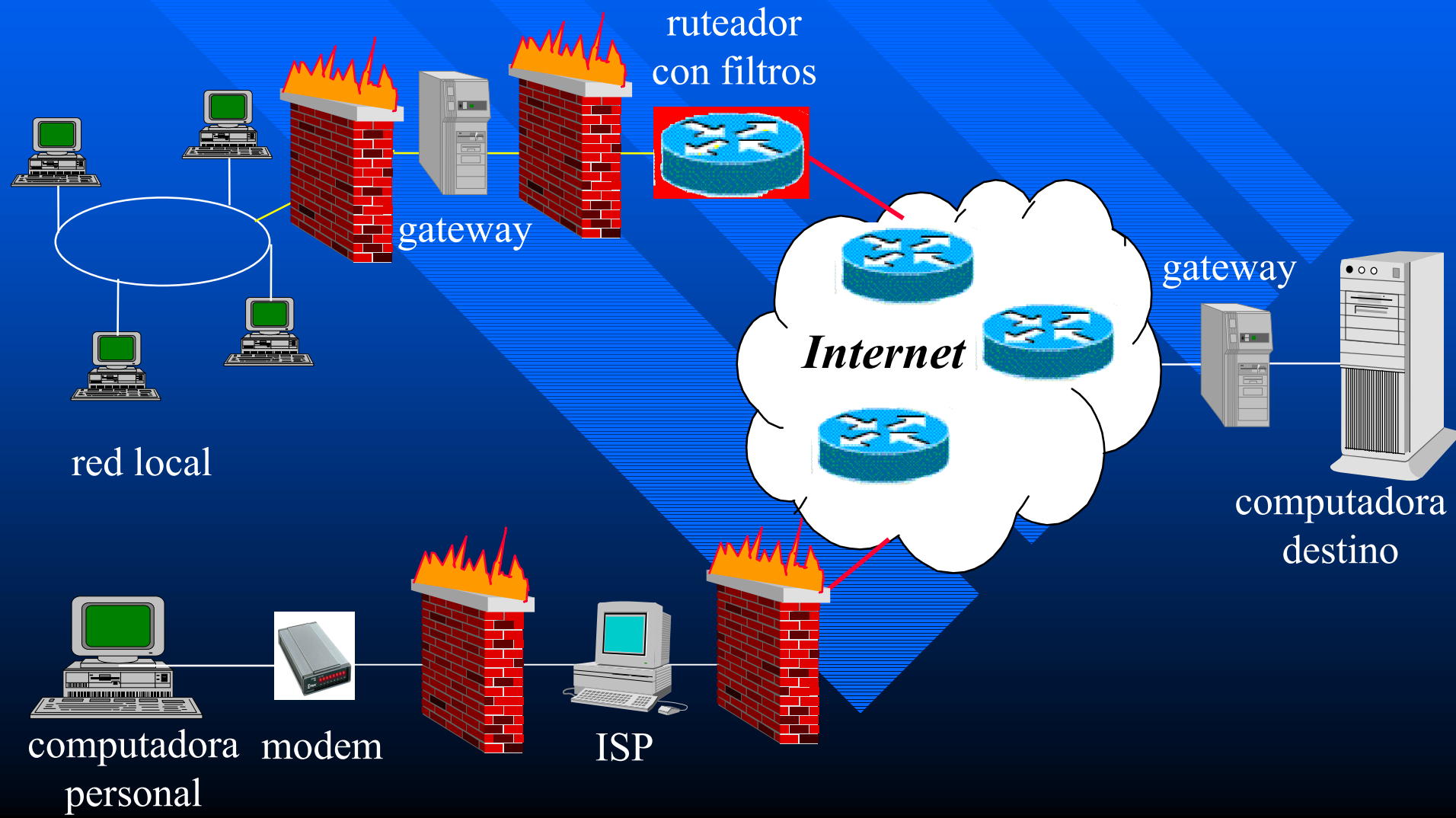
Security Policy | Address Translation | Generate an alert for suspicious activity

No.	Source	Destination	Service	Action	Track	Install C
1	Any	Web_Server	http	accept	Short	Gateway
2	Local_Net	Any	Any	accept	Short	Gateway
3	Any	Any	Any	drop	Alert	Gateway

With three simple rules, you have implemented access control for your network.



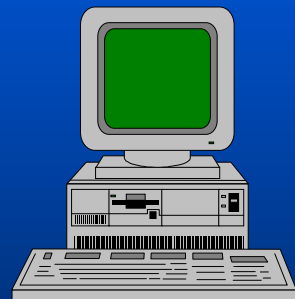
Integrando el firewall



¿Qué quiere hacer adentro: proxies?

- Es un intermediarios entre cliente y servidor.
- Un servidor proxy realiza una conexión con un servidor de alguna aplicación, de la parte de un cliente.
- Desde el punto de vista del cliente, hace la conexión con el proxy, pensando que ésta es con el servidor.

Esquema general aplicación cliente/servidor

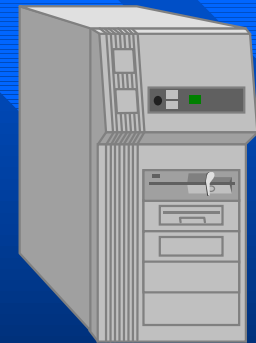


Cliente

1. cliente realiza una petición



3.. servidor responde al cliente

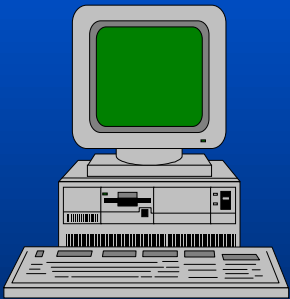


Servidor

2. servidor toma la petición y la procesa

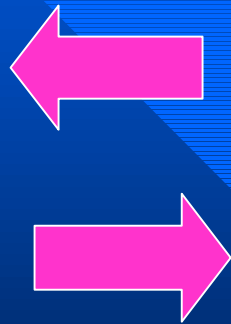
Esquema general cliente/servidor con proxy

1. cliente realiza petición al servidor



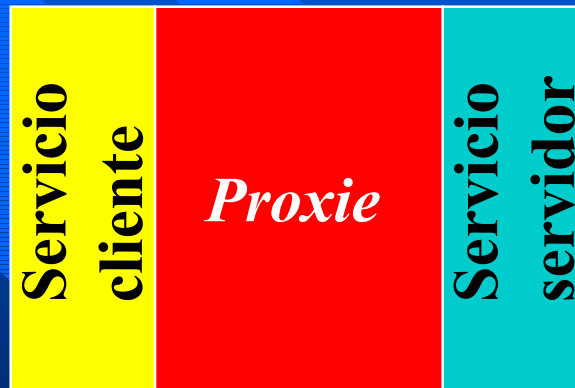
Cliente

7. proxy le responde al cliente.



2. el proxy toma la petición y realiza un chequeo

6. proxy toma la respuesta y la verifica

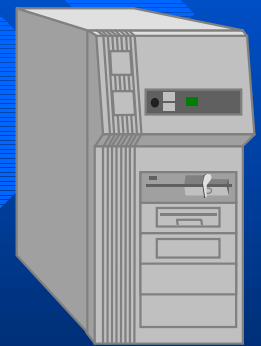


3. después del chequeo se envía la petición al servidor

5. servidor envía respuesta al cliente

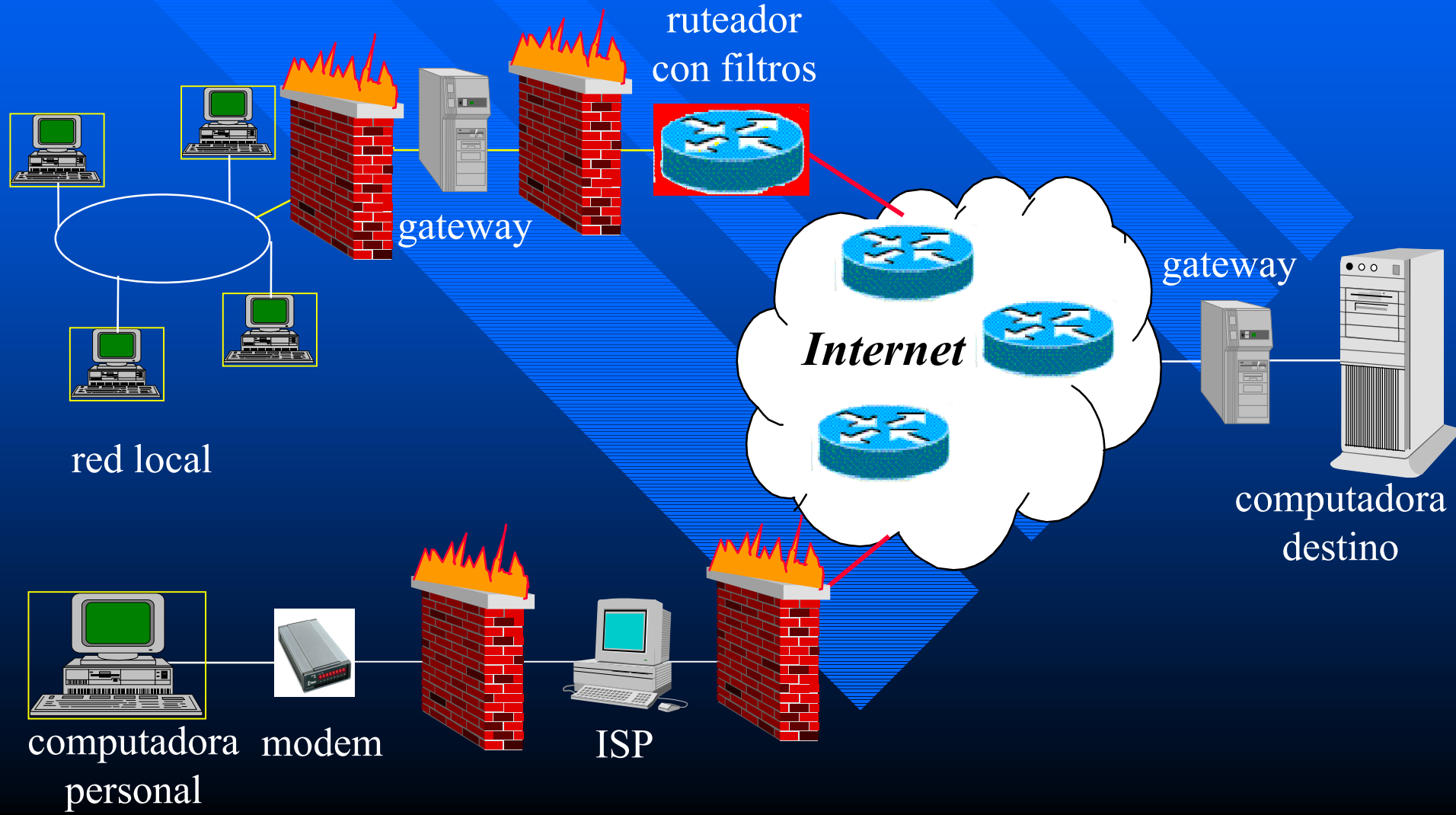


4. servidor toma la petición "depurada" y la procesa



Servidor

Integrando todo

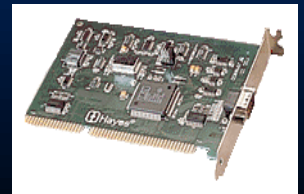


Cerrando puertas traseras (servicios)

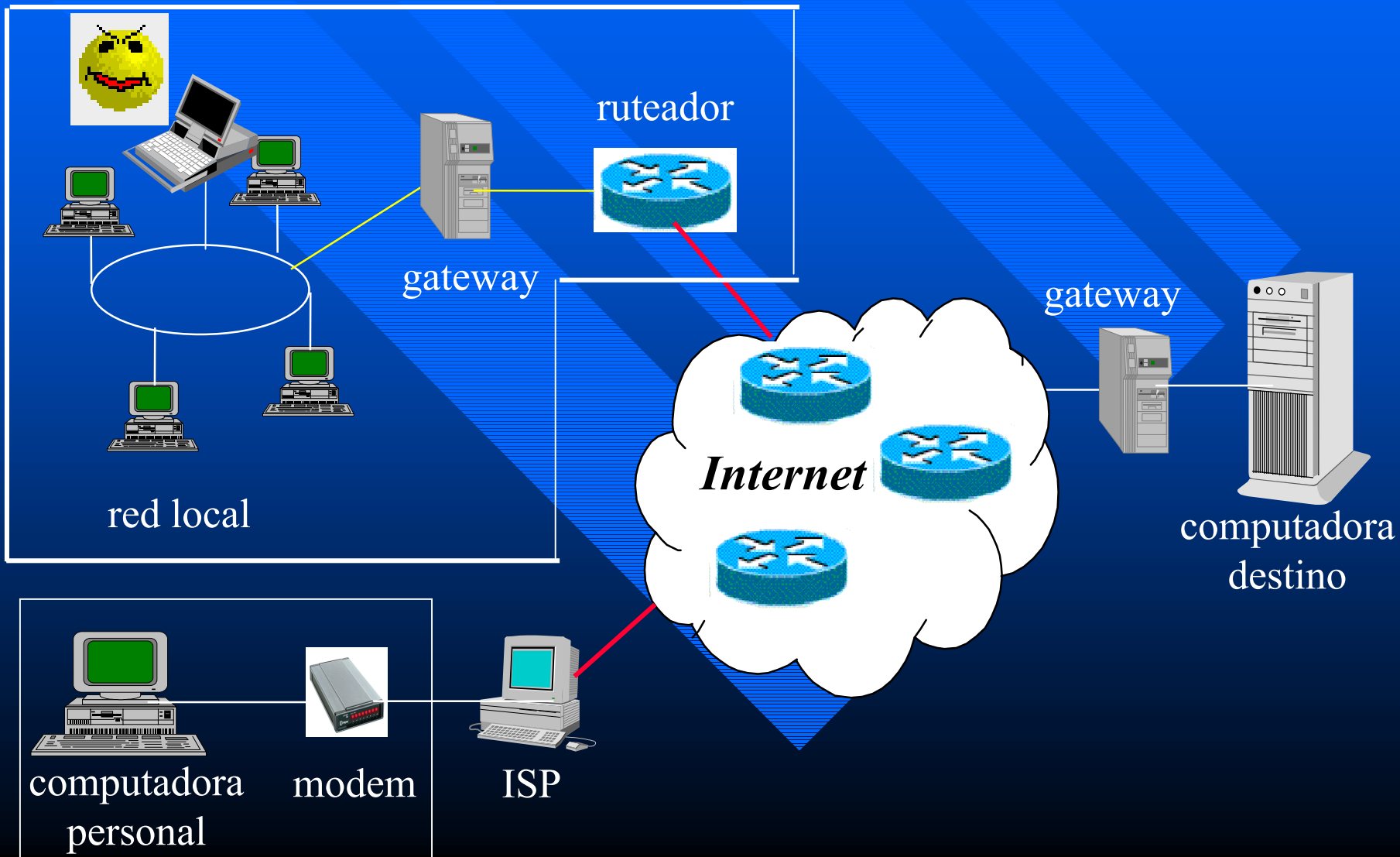
- Muchos servicios no se utilizan
 - correo (sendmail), transferencia de archivos (ftp), conexiones remotas (telnet) etc
- La mayor parte de los sistemas operativos lo instalan por default.
- Muchos de estos servicios son usados por los intrusos para introducirse al sistema.
- Es importante que los responsables de los sistemas se aseguren que estos servicios estan cerrados.

Cerrando puertas traseras (conexiones)

- Hoy en día la mayor parte de las computadoras cuentan con una tarjeta fax/modem.
- Algunos usuarios se pueden conectar a internet sin pasar por los perímetros definidos.
- Es importante que el usuario este consiente de que esto puede poner en peligro la seguridad.
 - políticas de seguridad
- Los encargados de seguridad deben supervisar que lo anterior no sea posible.



Ya establecí mi perímetro: ¿eso es todo?



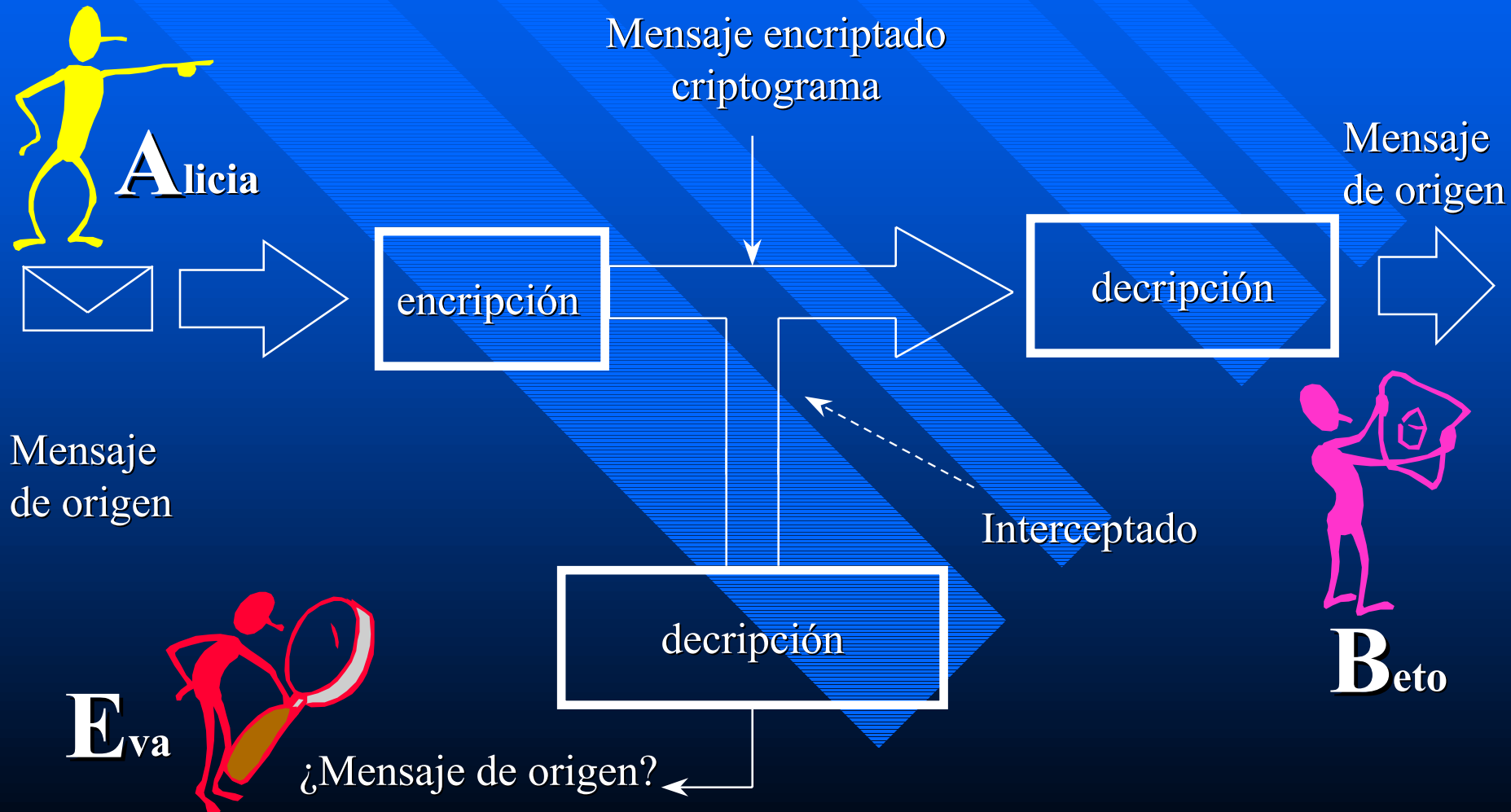
Integridad de Datos.

- Los datos no deben seguir modificaciones.
- Utilizar herramientas que me permitan verificar si algunos archivos han sido modificados.
- Existen diferentes herramientas en el mercado que realizan lo anterior.

Confidencialidad.

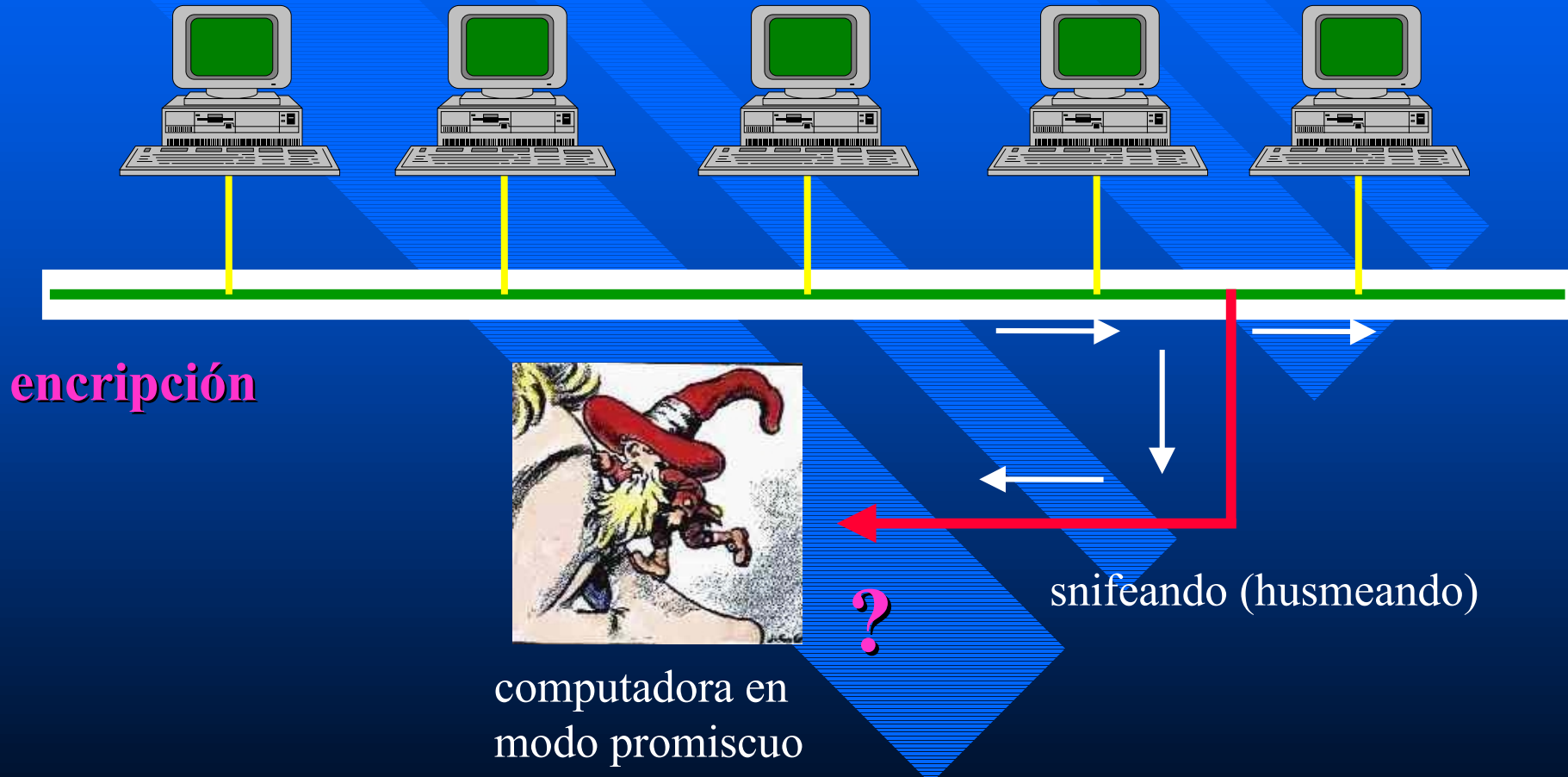
- Servicio que garantiza la privacidad de los datos:
 - En local.
 - En conexiones.
 - En modo no conectado.
 - En campos selectos.
 - En flujo de datos.
- Principal mecanismo para implementar este mecanismo es la criptologia

Proceso encriptación/decriptación





Protegiendome de sniffers

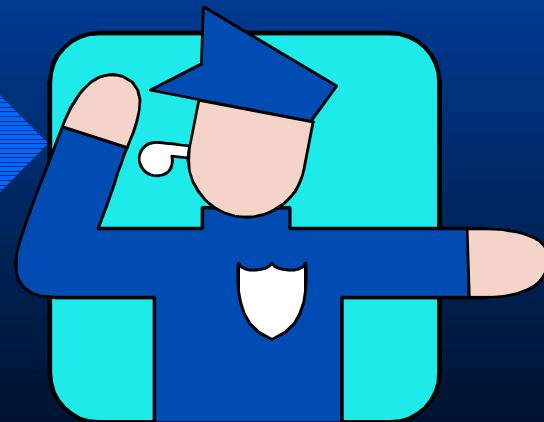


Precauciones a tomar en cuenta

- Los passwords
- Los discos e información compartida
- Los permisos
- Los “botes de basura”
- Los programas SetUID

¿Y si contratamos vigilantes?

los detectores de intrusos
IDS



IDS

- Intrusion Detection Systems.
- Busca automatizar la detección y eliminación de intrusos.
- Se define un intento de intrusión a la posibilidad, no autorizada, de
 - acceder información,
 - manipular información,
 - dejar un sistema fuera de alcance o sin posibilidad de uso.

IDS (cont)

- Asumen que un intruso puede detectarse examinando varios parámetros como:
 - tráfico de la red, -ubicación del usuario,
 - uso de CPU y E/S, -diferentes actividades usuario.
- Se dividen en
 - Detección Intrusos basados en reglas.
 - Detección Intrusos basados en estadísticas.

Desventajas IDS

■ Falsos positivos

- No se detecto una intrusión, siendo que alguien intentó entrar

■ Falsos negativos

- Se dio una alarma siendo que se hizo una operación normal.

*Si se cae un árbol y nadie oye (se percata que se cayó) entonces,
¿¿en realidad se cayó??*

¿Cómo se si todo esta bien?

- Usar herramientas de detección de vulnerabilidades
- Son herramientas para ayudar a los administradores a auditar sus redes para valorar y/o incrementar el nivel de seguridad
- La mayoría de las herramientas de seguridad disponibles hoy en dia se desarrollaron en universidades o las crearon especialistas independientes

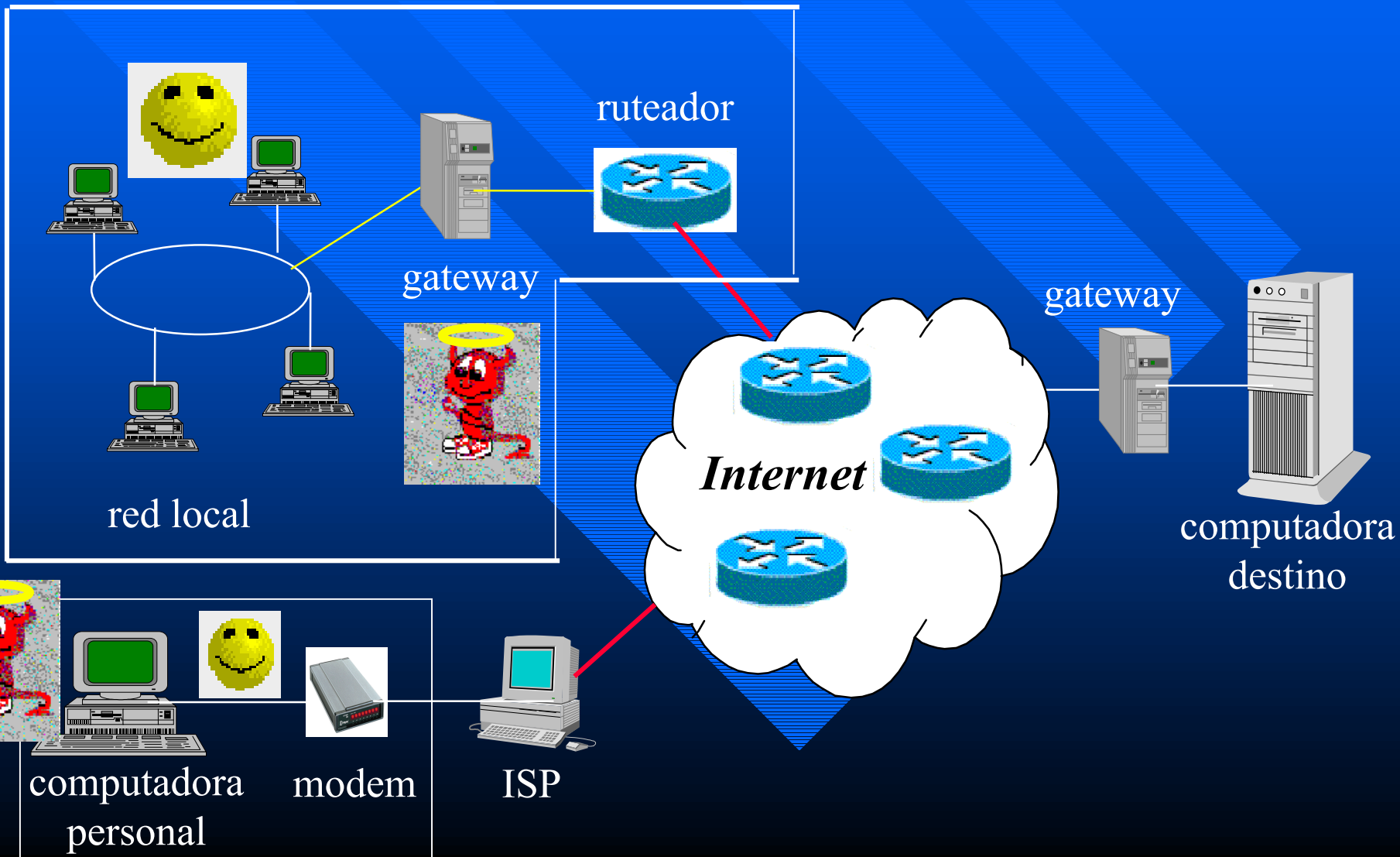
Vulnerabilidad

- Debilidad de un sistema informático que permite que sus propiedades de sistema seguro sean violadas.
- La debilidad puede originarse en el diseño, la implementación o en los procedimientos para operar y administrar el sistema.
- En el argot de la seguridad computacional una vulnerabilidad también es conocida como un *hoyo*.

Herramientas detección vulnerabilidades

- Encargadas de encontrar de forma automática vulnerabilidades de los sistemas
- Pequeño problema:
 - también las puede usar el intruso para ver cuáles son las debilidades del sistema que desea atacar

¿¿Ya termine??



Referencias

- *Hacking Exposed*; McClure, Scambray y Kurtz, Mc. Graw Hill
- *Unix System Security*; D.A. Curry, Addison Wesley
- *Seguridad en Windows 2000*; Jeff Schmidt, Pearson Education
- *Network Intrusión Detection*; Northcutt, Ed. New Riders, 2da. edición
- *Network Security*; Kaufman, Perlman y Speciner, Ed. Prentice Hall

Referencias

- *Applied Cryptography Protocols, Algorithms and Source in C*; B. Schneier, John Wiley & Sons
- *Firewalls and Internet Security*, William R. Cheswick and Steven M. Bellovin, Addison Wesley Professional Computing Series, 1995, 5a, edición.
- *Practical Unix & Internet Security*, S. Garfinkel, G. Spafford, O'Reilly, 1996, 2da. edición
- Revista: Sys Admin Unix Journal
- Revista: Dr. Doob's

Algunas ligas interesantes

- <http://www.cert.org>
- <http://www.sans.org>
- <http://www.kriptograma.org>
- <http://www.packetstorm.com>
- <http://www.snort.org>
- <http://www.tripwire.com>
- <http://www.linux.org>
- <http://www.microsoft.com>
- <http://webdia.cem.itesm.mx/dia/ac/rogomez>

Conclusiones

- Los ataques existen, no es ficción.
- La información corre peligro.
- Es importante estar consciente de lo anterior y tomar acciones al respecto.
- La seguridad al 100% no existe, todo es posible franquear.
 - se trata de dificultar la tarea del intruso

Gracias por su atención

¿preguntas?