



# Ataques

Roberto Gómez Cárdenas

[rogomez@campus.cem.itesm.mx](mailto:rogomez@campus.cem.itesm.mx)

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



# 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 “Script-Kidies”

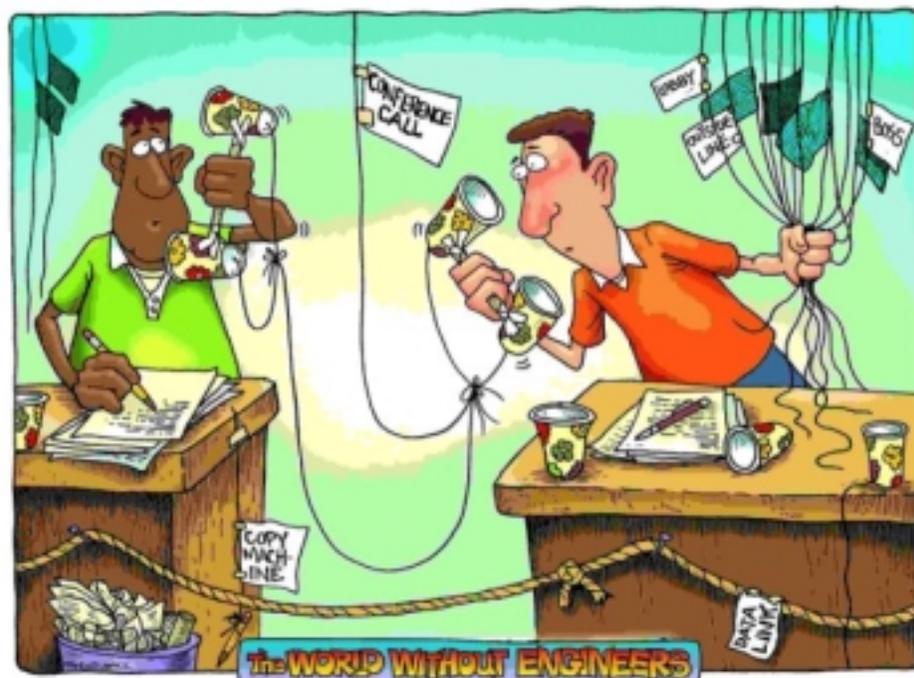
- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al inframundo.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy “cool”.





# El Phreaker

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas telefónicos privados.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado, o se beneficia del mismo.





# Hackers más famosos





# ¿Qué hicieron?

- Kevin Poulsen
  - In 1990 Poulsen took over all telephone lines going into Los Angeles area radio station KIIS-FM to win a call-in contest.
- Johan Helsingius
  - Operated the world's most popular anonymous remailer, called penet.fi, until he closed up shop in September 1996.
- Kevin Mitnick
  - The first hacker to have his face immortalized on an FBI "Most Wanted" poster.
- Cap Crunch (John Draper)
  - Figured out how to make free phone calls using a plastic prize whistle he found in a cereal box.



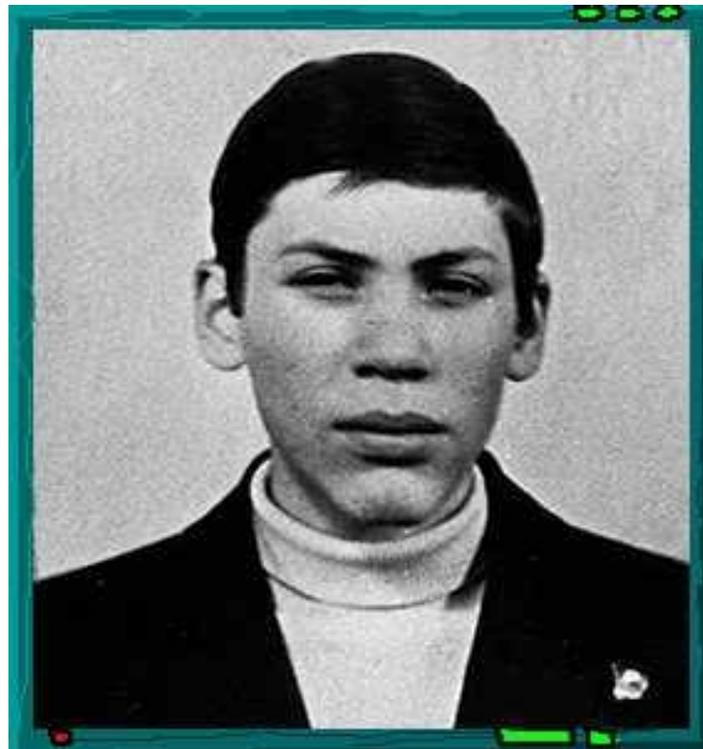
# ¿Son todos?

- Phiber Optik (Mark Abene)
  - Inspired thousands of teenagers around the country to "study" the internal workings of our nation's phone system.
- Otros:
  - Steve Wozniak
  - Tsutomu Shimomura
  - Linus Torvalds





# Vladimir Levin (Russian Hacker).



- **Hacked the City Bank \$ 10,000,000**



# Kevin Mitnick





# ¿Qué es un ataque?

- Acción o acciones que previenen cualquier parte de un sistema de información automatizado, de funcionar de acuerdo con su propósito definido.
- Esto incluye cualquier acción que causa la destrucción, modificación o retraso del servicio no autorizado.



## Otra definición ...

- El acto de tratar agresivamente, de evitar controles de seguridad de un sistema. el hecho de que se haga un ataque no necesariamente significa que tendrá éxito.
- El grado de éxito depende de la vulnerabilidad del sistema o actividad y la efectividad de las medidas de protección existentes.



# Aclaración ataque

- No es un ataque físico (aunque puede ser).
- Un ataque no se realiza en un solo paso.
- Depende de los objetivos del atacante.
- Puede consistir de varios pasos antes de llegar a su objetivo.



# Definición threat

- A threat is any circumstance or event which has the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.
- Common use today is from the press, which uses the word to describe people who “break into” computers for various purposes. (BBD)



# Ataque Asincrónico (Asynchronous Attack)

- Intento de aprovechar el intervalo entre un acto defensivo y un ataque para provocar que el acto defensivo sea inoperante.
- Ejemplo:
  - tarea sistema operativo puede ser interrumpida para verificar un parámetro almacenado,
  - el atacante gana control y cambia el valor del parámetro
  - el sistema operativo gana control de nuevo y continua su trabajo usando el parámetro maliciosamente alterado
  - ejemplo de ataque TOC/TOU



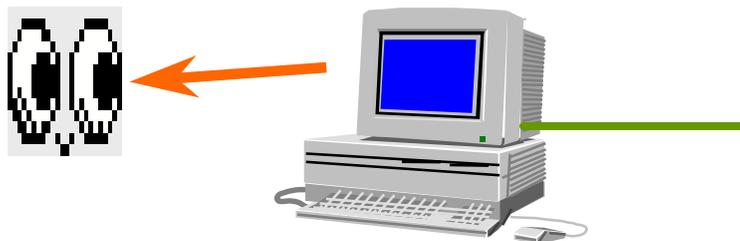
# Anatomía de un Ataque

- Blanco conocido.
- ¿Quién quiero ser hoy?
- ¿Dónde está la puerta?
- ¿Cómo entro?
- ¿Quién me vigila?
- Estoy en control. Me perteneces.
- ¿A dónde mas puedo ir?

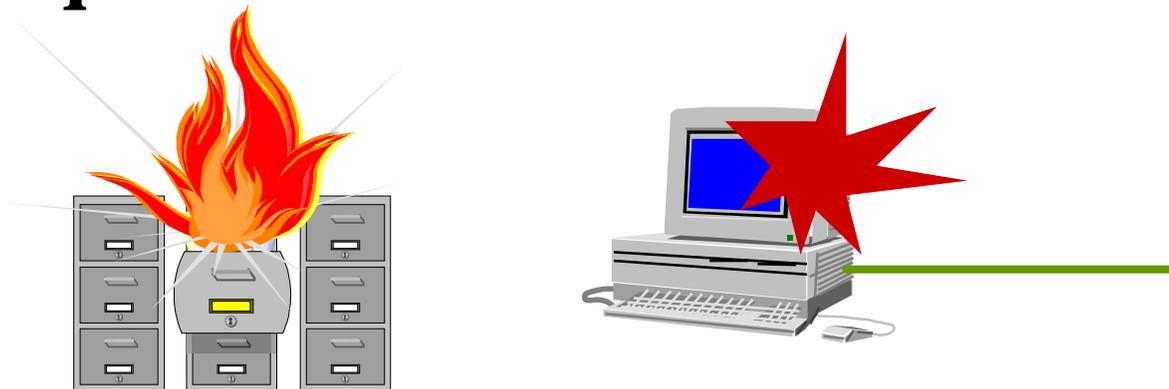


# Tipos de Ataques

## Ataques Pasivos.



## Ataques Activos.





# Principales Ataques

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

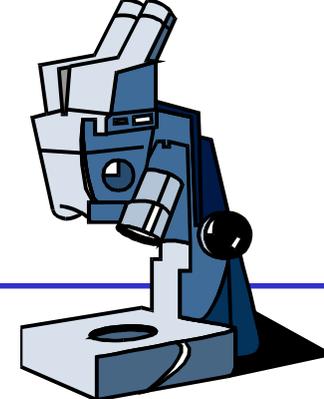


# Códigos Malicioso y virus

- Malicious Code and Virus
  - existen distinciones técnicas entre los diferentes tipos de programas maliciosos
  - el termino “virus” se refiere a todos estos tipos de programas entre los que se incluyen los virus per se, los caballos de troya, los gusanos “worms”, entre otros.
- El termino Jargon
  - vocablo empleado por hackers y crackers para hacer referencia a programas malignos.
  - ejmplos: Sig virus, GP virus, worm, caballo de Troya, back door, bomb, etc.



# Virus

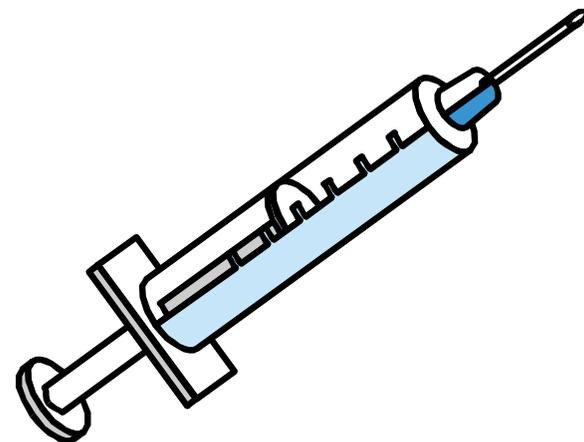


- Un virus se define como una porción de código de programación cuyo objetivo es implementarse a si mismo en un archivo ejecutable y multiplicarse sistemáticamente de un archivo a otro.
- Además de esta función primaria de "invasión" o "reproducción", los virus están diseñados para realizar una acción concreta en los sistemas informáticos.



# Virus

- Esta acción puede ir desde la simple aparición de un mensaje en la pantalla, hasta la destrucción de toda la información contenida en el sistema.



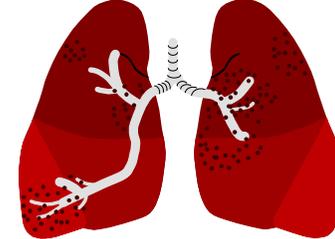


# ¿Cómo actúa un virus?

- El ciclo de los virus informático es muy similar al de los biológicos (lo que justifica su nombre).
- Este ciclo está compuesto por los siguientes pasos:
  - Infección
  - Expansión
  - Explosión



# Infección

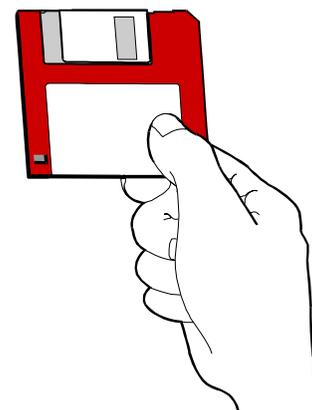


- Al ejecutar un archivo infectado (el código del virus se ha implantado en el archivo anteriormente) comienza la fase de infección.
- Se duplica e implanta en otros archivos ejecutables.
- Comienza la "invasión" del sistema informático.
- La víctima, aún no es consciente de la existencia del virus ya que este permanece oculto y sin causar daños apreciables.



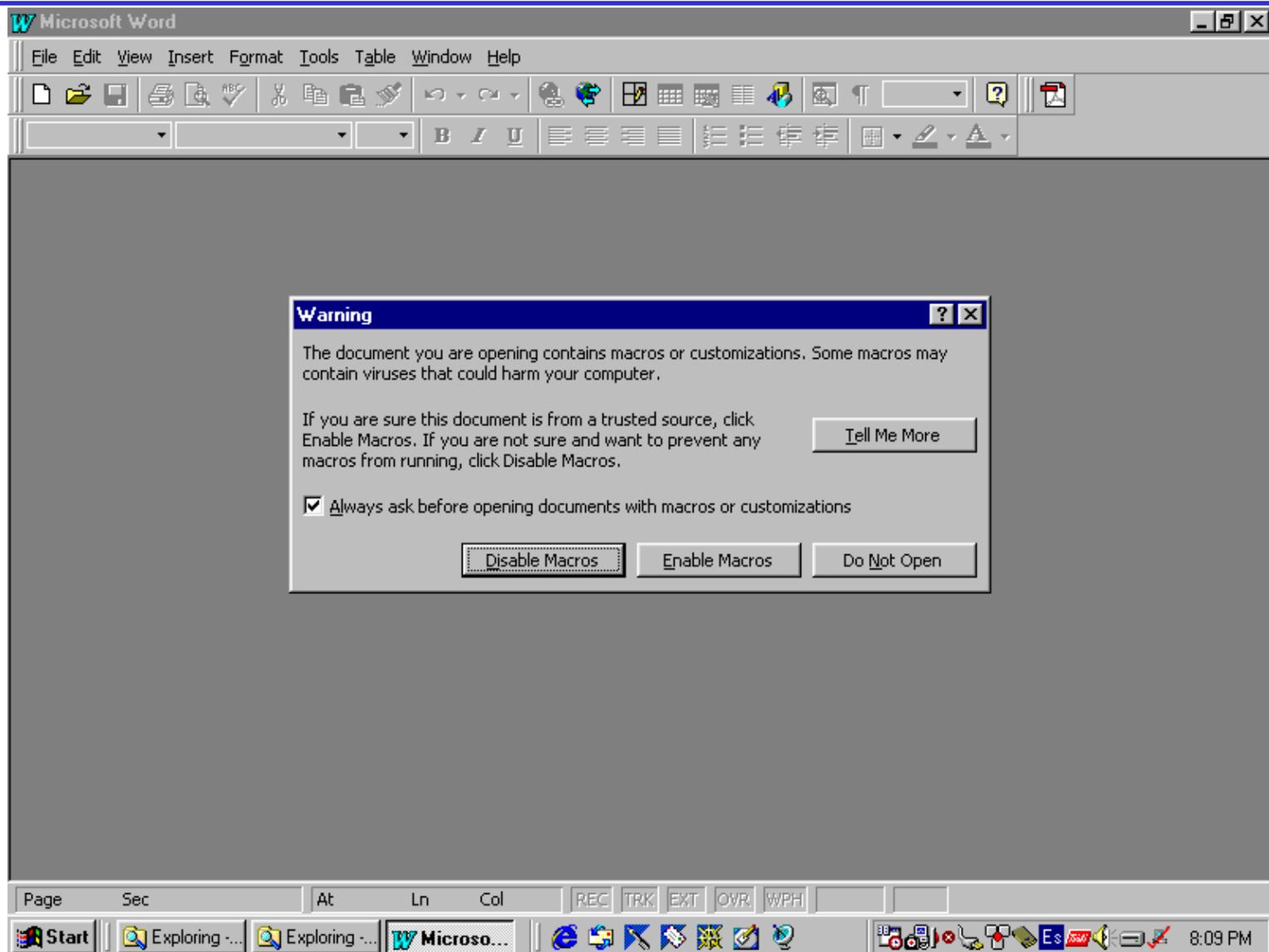
# Expansión

- El virus pasará a otros ordenadores, a través de redes informáticas, disquetes y CDs que contengan archivos infectados, software en Internet, archivos adjuntos a mensaje electrónicos, etc
- En todos los casos es necesario un medio de transmisión.





# Ejemplo expansión





# Explosión

- Si el virus no ha sido detectado y destruido por algún *programa antivirus*, en un momento determinado o bajo determinadas circunstancias, tomará el control del ordenador infectado, ejecutando la acción para la que fue programado.
- En este momento, debido a los trágicos efectos que pueden llegar a ocasionar, se hará evidente su existencia.





# Características virus

- Son muy pequeños.
- Casi nunca incluyen nombre del autor.
- Casi nunca incluyen registro.
- Casi nunca incluyen mensajes.
- Casi nunca incluyen la fecha de creación o modificación.
- Se reproducen así mismos y toman el control.



# Atributos para que un programa se considere un virus

- Modificación de códigos de software a través del enlace en las estructuras del programa virus con las estructuras de otros programas.
- Facultad de ejecutar la modificación en varios programas.
- Facultad para reconocer programas ya infectados de no infectados.





# Atributos de un virus

- Posibilidad de impedir que vuelva a ser modificado el mismo programa al reconocer que ya está infectado o marcado.
- El software modificado asimila los atributos anteriores para a su vez, iniciar el proceso con otros programas y en otros discos.



# ¿Cómo funciona un virus?

- Generalmente se inicia cuando de alguna manera el virus se copia en la memoria RAM.
- A partir de ahí los virus buscan alojarse, copiarse o almacenarse en cualquier medio disponible (discos flexibles, discos duros, o cintas).



# Clasificación virus (de acuerdo a su objetivo principal)

- Virus Cauticos
- Virus Crecidos
- Virus Descarados
- Virus Estadísticos
- Virus Físicos
- Virus Juguetones
- Virus Malditos
- Virus Misteriosos
- Virus Mutantes
- Virus Resentidos
- Virus Simples
- Virus Supervisores
- Virus Temporales
- Virus Vengadores
- Virus Viajeros
- Virus Kernel
- Virus de Código Fuente



# Tipos de virus

- Boot sector
- Macros.
- Ejecutables



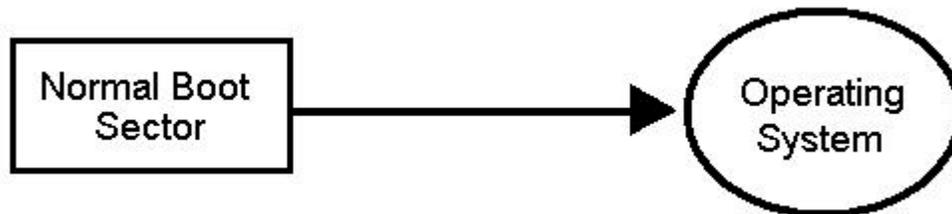
# Virus tipo boot sector

- Normalmente ejecuta su código malicioso cuando el sistema es iniciado.
- Después regresa el control de proceso de inicio al sector de arranque del disco duro
- De esta forma puede concluir el proceso normal de inicio, pero con un pequeño parásito agregado.

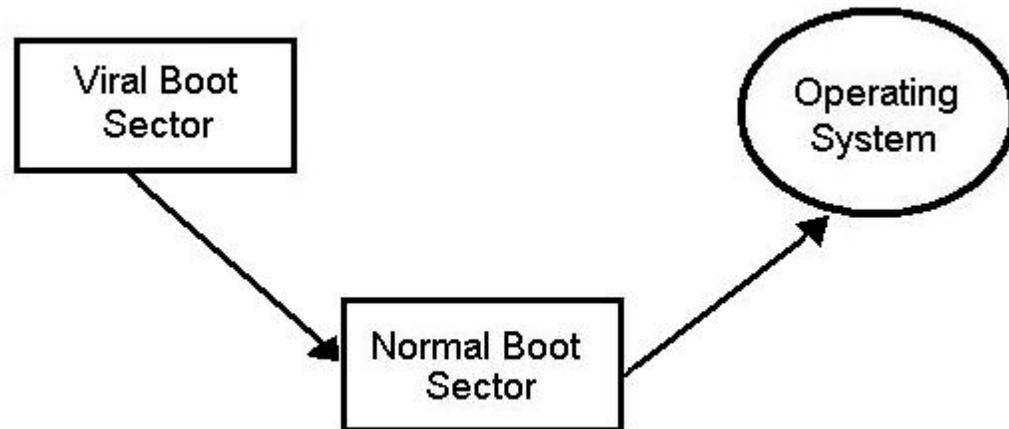


# Esquema virus boot sector

Proceso normal de arranque:



Proceso infectado por el Boot Sector Virus:





# Virus tipo macros

- Algunos documentos pueden encontrarse infectados por un virus que no es mas que un macro.
- Un macro esta constituido por una serie de instrucciones que ejecutan código malicioso dentro de un sistema.
- Este macro es ejecutado al abrir el documento infectado como puede ser un archivo de Microsoft Word, un archivo de Microsoft Excel, entre otros.

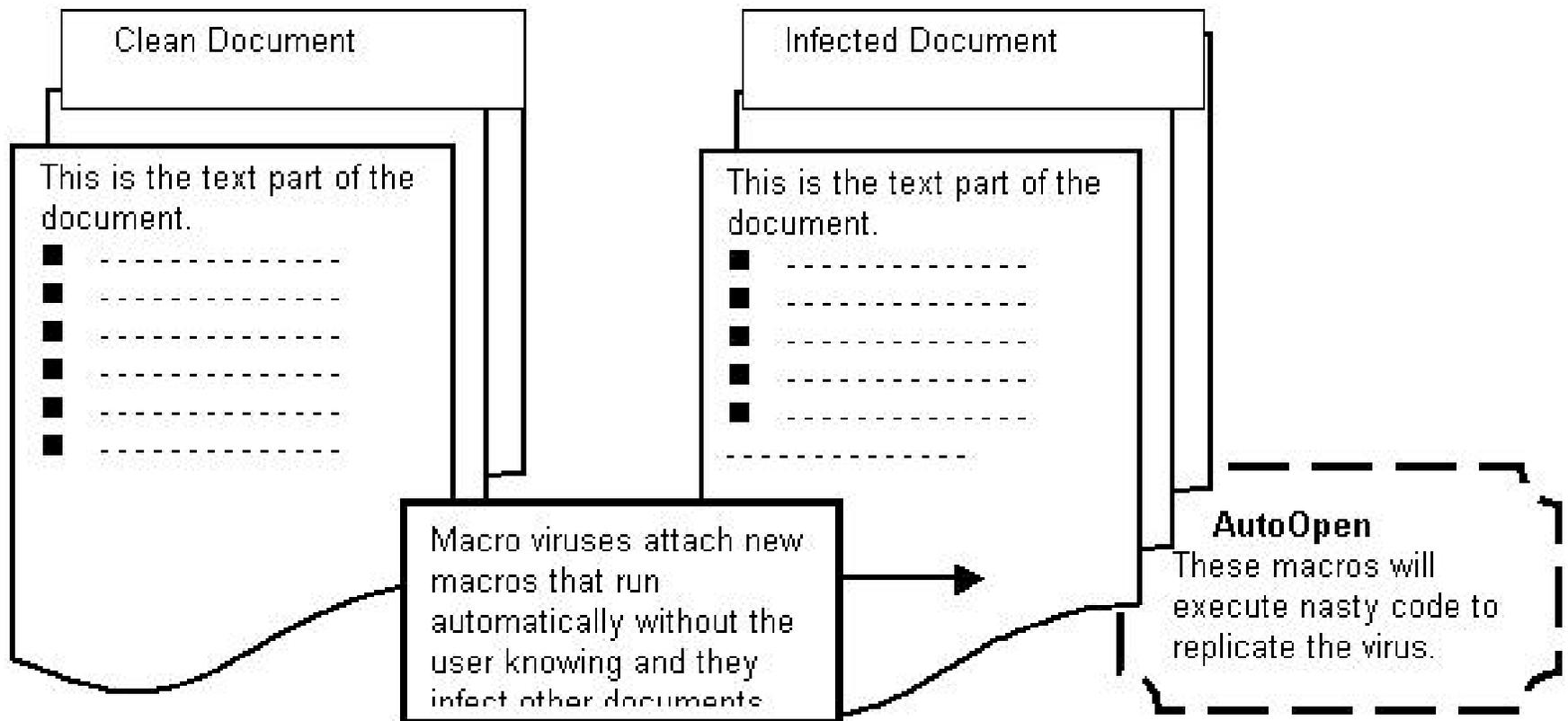


# Reproducción virus tipo macros

- Los virus tipo macro pueden reproducirse por medio del uso de correo electrónico.
- Dentro de sus instrucciones puede estar alguna que utilice el directorio de correos electrónicos guardado en Microsoft Outlook
  - así, enviarse a sí mismo a todas las personas que son conocidas por el dueño del sistemas infectado.



# Funcionamiento virus tipo macro





# Virus ejecutables

- Estos virus se ubican en un archivo ejecutable normal.
- Al ser ejecutado el programa, además de correr las rutinas propias, ejecuta las rutinas del virus.
- Algunos virus poseen la característica de establecerse en una parte de la memoria no volátil de un sistema (NRAM)
  - se conocen como virus de tipo TSR (Terminate and Stay Resident)
  - esto hace que el virus se mantenga vivo aun y cuando el sistema se apaga y vuelve a encender.



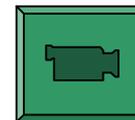
# Ejemplos de virus

- El caballo de Troya
- El pakistaní
- El cascada
- El Alabama
- El Jerusalén
- El Miguel Angel
- El ping pong
- El Viena
- El natas
- El dos piernas
- El stoned noit
- El DARK AVEGER
- El ping pong
- El I love you
- El trojan
- El killer



# ¿Qué no hace un virus?

- Destruir dispositivos de una computadora.
- Reproducirse sin la ayuda de un medio de transmisión.





# Variantes relacionadas con virus

- En ocasiones de habla de estas variantes como si de virus se tratara, cuando en realidad son conceptualmente diferentes.
- Algunos antivirus pueden detectarlos.
- Estas variantes son:
  - Troyanos
  - Gusanos
  - Bomba lógica



# 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.



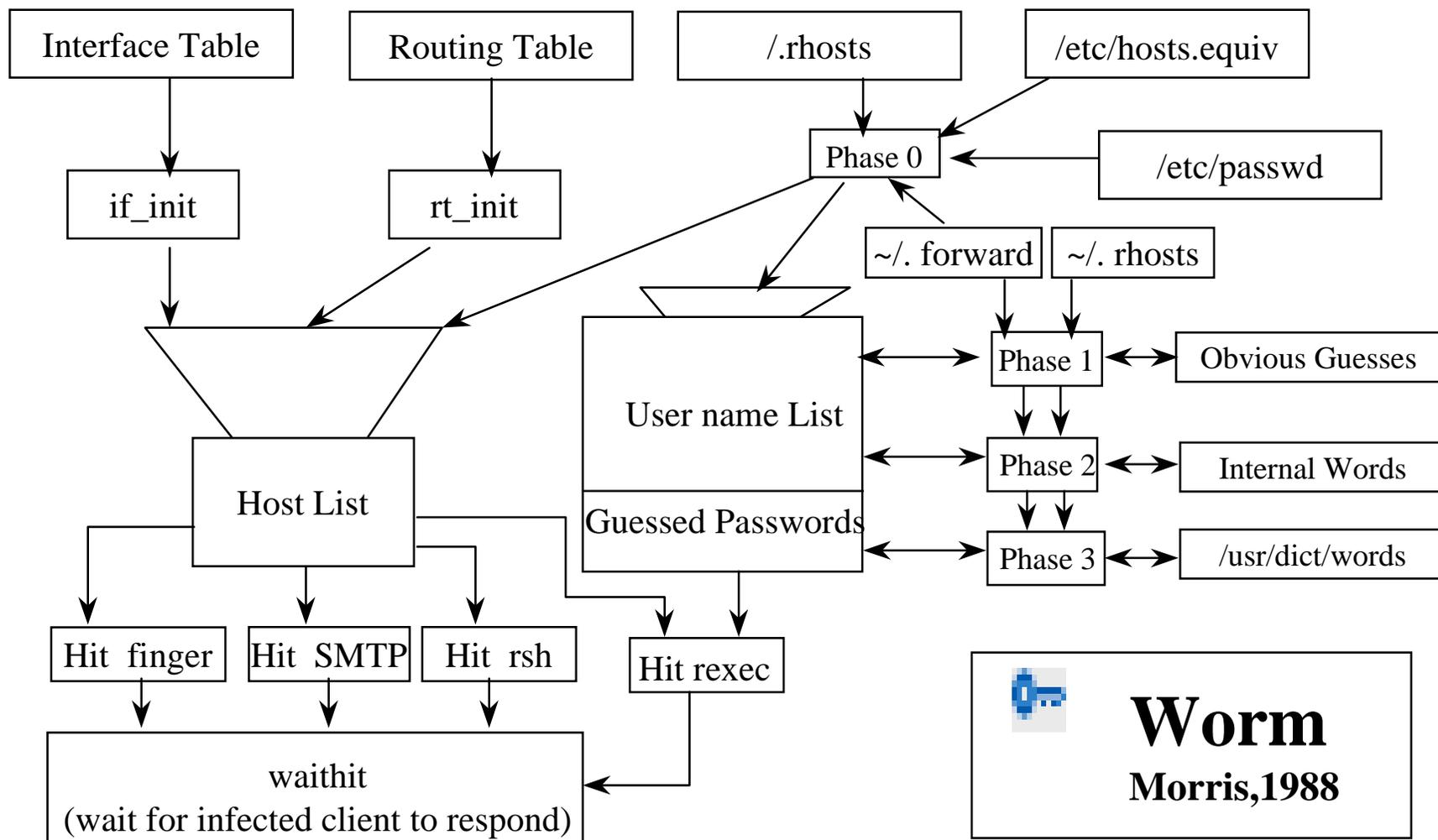


# El gusano de Internet

- Tarde: 2-nov-1988 un programa que se autoreplicaba fue liberado en Internet.
- Este programa se fue auto-copiando de máquina en máquina causando que estas máquinas se sobrecargan y dejaran de proporcionar servicio a sus usuarios.
- A pesar de que el sistema solo atacaba dos tipos de sistemas (Sun o VAX) se propago rapidamente



# El gusano de Morris, 1988 ...





# ¿Qué hacía el gusano?

- Explotaba tres vulnerabilidades de las versiones de Unix derivadas de BSD
  - máquina atacante enviaba un script de shell a la victima y lo ejecutaba
  - shell compilaba y ejecutaba un programa enC
  - programa se conectaba con la máquina atacante de nuevo via TCP
  - bajaba el programa objeto precompilado que implementaba al gusano mismo
  - intentaba ligar el programa en la victima y correrlo
  - en este punto la víctima se convierte en atacante y empieza a realizar lo mismo en otras máquinas



# Vulnerabilidades explotadas

- (1) Programa rsh y la función de biblioteca rexec
  - proporcionan acceso a un shell en una máquina remota
  - rexec requiere de autenticación
  - rsh permite el acceso a máquinas confiables
- (2) El programa fingerd
  - proporcionar información acerca de un usuario
  - programa lee una línea de entrada del sistema remoto
- (3) La función debug del programa sendmail
  - facilidad de enviar correo a un programa de tal forma que el programa es ejecutado con el cuerpo del mensaje como entrada



# ¿Qué no hacía?

- Borrar sistemas archivos aparte de los creados por el mismo.
- Modificar archivos existentes en un sistema infectado.
  - no era un virus, se propagaba copiándose y compilándose en sistemas remotos, no modificando otros programas para propagarse
- Instalar programar a ser ejecutados por usuarios sospechosos más tarde.
- Registrar o transmitir passwords decriptados.
  - intentaba decriptar passwords a nivel local



## ¿Qué no hacía?

- Tratar de contar con privilegios de superusuarios.
  - no atacaba alguna cuenta en especial
- Propagarse vía UUCP, X.25, BITNET o DECNET,
  - se propagaba vía TCP.
- Infectar sistemas System V Unix
  - a menos que estos fueran modificados para usar programas de red BSD como sendmail, fingerd y rexec



# Ejemplos de gusanos modernos

---

- Happy99
- Melissa
- ExploreZip
- Navidad



# El gusano navidad.exe (1)

[Fwd: Matematicas, sueño o pesadilla: resena del Cafe] - Inbox - Netscape Folder

File Edit View Go Message Communicator Help

Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop

Name	Subject	Sender	Date	Priority	Stat...
Local Mail					
Inbox					
Uns...ages					
Drafts					
Templates					
Sent					
Trash					
alain					
roberto					
news					
	Re: Medidas de seguridad	Ma. de los Angeles Junco	Sat 11:11 AM		read
	proy_soll	Ángel Gabriel Zanatta Juárez	Sat 2:33 PM		read
	game genius juego de ing...	anibal diaz	Sat 4:07 PM		read
	Re: CompMoviVirtual.ppt	Dr. Javier Gómez Tagle Rangel	Sat 5:25 PM		read
	duda proyecto 3p	Omar Arias	Sun 5:41 PM		read
	[Fwd: Dot Conference]	Roberto Gomez Cardenas Depart...	Tue 9:40 PM		read
	RV: Programa	Shafia Sucar	11/16/2000 9:51 ...		read

**Subject: Matematicas, sueño o pesadilla: resena del Cafe**  
**Date:** Thu, 16 Nov 2000 09:50:55 -0600  
**From:** [Shafia Sucar <shafia@quijote.ugto.mx>](mailto:shafia@quijote.ugto.mx)  
**To:** [francia-mexico@casadefrancia.org.mx](mailto:francia-mexico@casadefrancia.org.mx)

para seguimiento e informacion, encontraran en attachment el boletin de prensa del ultimo CAFE DE CIENCIA sobre MATEMATICAS, SUEÑO O PESADILLA.  
saludos  
Annie  
Attachment Converted: "C:\Eudora\Attach\Bol. Matemáticas.doc"

 [Navidad18.exe](#)  
**Name:** Navidad18.exe  
**Type:** unspecified type (application/octet-stream)  
**Encoding:** base64

Total messages: 75 Unread messages: 0

Start Exploring... Dr. Robert... [Fwd: M... 9:57 PM





# El gusano navidad.exe (3)

[Fwd: Cuidado!!!!] - Inbox - Netscape Folder

File Edit View Go Message Communicator Help

Name	Subject	Sender	Date	Priority	Stat...
Local Mail					
Inbox					
Uns...ages					
Drafts					
Templates					
Sent					
Trash					
alain					
roberto					
news					

**Subject: Re: Cuidado!!!!**  
**Date:** Fri, 17 Nov 2000 00:44:06 -0600  
**From:** [Shafia Sucar <shafia@quijote.ugto.mx>](mailto:shafia@quijote.ugto.mx)  
**To:** "Salvador G. Medina" <adan@servidor.unam.mx>  
**CC:** [francia-mexico@casadefrancia.org.mx](mailto:francia-mexico@casadefrancia.org.mx)  
**References:** [1](#)

Estimados Lectores,

Lamento mucho haber sido la culpable de que mensajes que yo No envie, pero que si salieron de mi correo, llegaran hasta ustedes. Evidentemente este virus toma direcciones de correo electronico y se auto-envia. Esto me sucedio ayer miercoles, y desafortunadamente no sabia aun de este virus. Por favor no abran dicho ejecutable y eliminen todo aquello que diga Navidad!

Nuevamente les pido disculpas!

Saludos,

Shafia.

Total messages: 113 Unread messages: 0

Start | Tiv... | E. | M | h. | I. | Es | 2:38 PM



## Lo bueno y lo malo de navidad

- Nombre: W95/Navidad@m worm.
- Alias: Navidad.
- Tipo: Ejecutable Windows 32.
- En la semana del 6 al 12 de noviembre del 2000 se recibieron múltiples reportes de la aparición del gusano denominado "Navidad".
- Navidad llega por correo electrónico en un anexo llamado NAVIDAD.EXE, generalmente este correo proviene de una persona que el usuario conoce y a quien se envió recientemente algún mensaje.



## Lo bueno y lo malo de navidad

- Lo malo del Navidad es que contiene rutinas destructivas que se activan, al menos en teoría, el 25 de diciembre.
- Lo bueno es que debido a errores en el procedimiento de instalación, quizá nunca llegue a activarse la rutina destructora.
- Lo malo es que después de instalarse, no funcionará prácticamente ningún programa del usuario



## Eliminado el gusano

- Lo malo es que Navidad no puede eliminarse como un virus porque no lo es, tiene que eliminarse en forma manual.
- Lo malo es que tan pronto se instala, el Navidad vigila cada mensaje que el usuario recibe para contestarlo enviando el anexo NAVIDAD.EXE.
- Lo bueno es que el Navidad solo funciona con Outlook.
- Lo bueno es que es muy sencillo de erradicar.



## Erradicando navidad.exe

- Basta borrar los archivos NAVIDAD.EXE (en donde se encuentre) y el archivo WINSVRC.VXD de la ruta C:\WINDOWS\SYSTEM.
- Finalmente se eliminan las llaves del registry de Windows con las que el Navidad pretende ejecutarse en el siguiente arranque del sistema.
- Las llaves correctas deben verse así:
  - HKEY\_CLASSES\_ROOT\exefile\shell\open\command  
@="\"%1\" %\*"
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Win32BaseServiceMOD" = ""



# Otro ejemplo virus/gusano

[Fwd: US PRESIDENT AND FBI SECRETS =PLEASE VISIT => (<http://www.2600.COM>)<=] - Inbox - Netscape Folder

File Edit View Go Message Communicator Help

Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop

Name	Subject	Sender	Date	Priority
Local Mail				
Inbox	Partido para maniana	Victor Manuel Romero Medina	Fri 9:34 AM	
Unsent Messages	!TarNeta Burundis de Eri!	Eri	Fri 6:11 AM	
Drafts	Repercusiones de la encef...	Juan A. Montaña Hirose	Fri 10:47 AM	
Templates	Re: OPODIS 2001	Raul Jacinto Montes	Fri 12:06 PM	
Sent	[Fwd: FW: Pregunta]	Roberto Gomez Cardenas Departa...	Fri 4:06 PM	
Trash	[Fwd: Backdoor en juego B...	Roberto Gomez Cardenas Departa...	Mon 6:10 PM	
alain	[Fwd: Discovery Online, Ha...	Roberto Gomez Cardenas Departa...	Tue 2:06 PM	
roberto	[Fwd: US PRESIDENT AN...	Roberto Gomez Cardenas Departa...	7:20 PM	
news				

**Subject:** US PRESIDENT AND FBI SECRETS =PLEASE VISIT =>  
<http://WWW.2600.CO> M<=  
**Date:** Tue, 9 Jan 2001 10:38:04 -0500  
**From:** [Lula Frye <frye@hq.acm.org>](mailto:frye@hq.acm.org)  
**To:** ['Roberto Gomez Cardenas' <rogomez@campus.cem.itesm.mx>](mailto:rogomez@campus.cem.itesm.mx)

BUOUOUEJIPU

 [IIBODUAE.JPG.vbs](#)

**Name:** IIBODUAE.JPG.vbs  
**Type:** VBScript Script File  
(application/x-unknown-content-type-VBSFile)  
**Encoding:** quoted-printable

Total messages: 131 Unread messages: 0

Start Fin... Ex... Mi... Pr... [F... 7:17 PM



# ¿Cuál es el problema?

rem =====

rem "Plan Colombia" virus v1.0

rem by Sand Ja9e Gr0w (www.colombia.com)

rem Dedicated to all the people that want to be hackers or crackers, in Colombia

rem This program is also a protest act against the violence and corruption that

rem Colombia lives I always wanting that all this finishes, I have said...

rem Santa fe de Bogotá 2000/09

rem I dedicate to all you the song "GoodBye" of Andreas Bochelli

rem =====

rem Thanks God..!

rem A greeting for "Lina María" from "Santa fe de Bogotá"

rem A greeting for "Tizo" from "Spain"

rem And One kicked of tail to my friends, "eL ChE" and "ThE SpY"

rem okay, ok...

rem my baby start here...



# ¿Y que hace?

On Error Resume Next

```
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow,polyn
```

```
eq=""
```

```
ctr=0
```

```
:
```

```
:
```

```
for each f1 in fc
```

```
  s=lcase(f1.name)
```

```
  if (ext="vbs") or (ext="vbe") then
```

```
    set ap=fso.OpenTextFile(f1.path,2,true)
```

```
    ap.write vbscopy
```

```
    ap.close
```

```
  else
```

# ¿borra archivos?



```
if(ext="js") or (ext="jse") or (ext="css") or (ext="wsh") or (ext="sct")
    or (ext="hta") then
    set ap=fso.OpenTextFile(f1.path,2,true)
    ap.write vbscopy
    ap.close
    bname=fso.GetBaseName(f1.path)
    set cop=fso.GetFile(f1.path)
    cop.copy(folderspec&"\"&bname&".vbs")
    fso.DeleteFile(f1.path)
else
    :
    :

rem bye net connection ...      :-(
Set WSHNetwork=Nothing

end sub
```



# Viendo las consecuencias ...

Find: Files named \*.vbs

File Edit View Options Help

Name & Location | Date | Advanced

Named: \*.vbs

Containing text:

Look in: (C:)

Include subfolders

Find Now

Stop

New Search

Browse...

Name	In Folder	Size	Type	Modified
reload	C:\WINDOWS	13KB	VBScript Script File	01/10/2001 7:04 PM
BG_RES1.JPG	C:\WINDOWS\OPTIONS\CABS\TOUR\RESOUR...	13KB	VBScript Script File	01/10/2001 7:04 PM
STHBOX.JPG	C:\WINDOWS\OPTIONS\CABS\TOUR\RESOUR...	13KB	VBScript Script File	01/10/2001 7:04 PM
CSEL	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
BG_OVR.JPG	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
BG_TOUR.JPG	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
Sm1	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
Sm2	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
Sm3	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
Sm4	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
Sm5	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
Sm6	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
SM	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
TOUR	C:\WINDOWS\OPTIONS\CABS\TOUR\OVERVIE...	13KB	VBScript Script File	01/10/2001 7:04 PM
BG_CONT.JPG	C:\WINDOWS\OPTIONS\CABS\TOUR\IMAGES	13KB	VBScript Script File	01/10/2001 7:04 PM
CE	C:\WINDOWS\OPTIONS\CABS\TOUR\COMPRESS	13KB	VBScript Script File	01/10/2001 7:04 PM
MASTER	C:\WINDOWS\OPTIONS\CABS\CONTENT\ZDNET	13KB	VBScript Script File	01/10/2001 7:04 PM
FINNCS	C:\WINDOWS\OPTIONS\CABS\CONTENT\W.S.I	13KB	VBScript Script File	01/10/2001 7:04 PM

542 file(s) found

Monitoring New Items

Start Find: Files nam... Exploring - FigurasL... 7:12 PM



# Lo último: W32.Sircam.Worm

**ejercicio10 - VirusGusanos - Netscape Folder**

File Edit View Go Message Communicator Help

Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop

Name	Subject	Sender	Date
Amazon	for Dial-Up Networking supports	D.G. Alexandra Diaz Fuentes	06/28/2001 3:24 PM
Bitacoras	<b>ejercicio10</b>	daniel noe hernandez vazquez	Wed 9:12 AM
CFP-ArtisEnviados	JOSEFA	daniel noe hernandez vazquez	Wed 10:08 AM
ChistesAnecdotas	Tarea Cap12 Alfredo	daniel noe hernandez vazquez	Wed 11:15 AM
Compras	DIPLOMA MANUEL CARRIO	daniel noe hernandez vazquez	Wed 11:15 AM

**Subject:** ejercicio10  
**Date:** Wed, 18 Jul 2001 10:12:34 -0500  
**From:** "daniel noe hernandez vazquez" <danieln@cosvernet.net.mx>  
**To:** [rogomez@campus.cem.itesm.mx](mailto:rogomez@campus.cem.itesm.mx)

**Part 1.1** Type: Plain Text (text/plain)  
Encoding: quoted-printable

**ejercicio10.20.xls.bat**  
Name: ejercicio10.20.xls.bat  
Type: MS-DOS Batch File  
(application/x-unknown-content-type-batfile)  
Encoding: base64

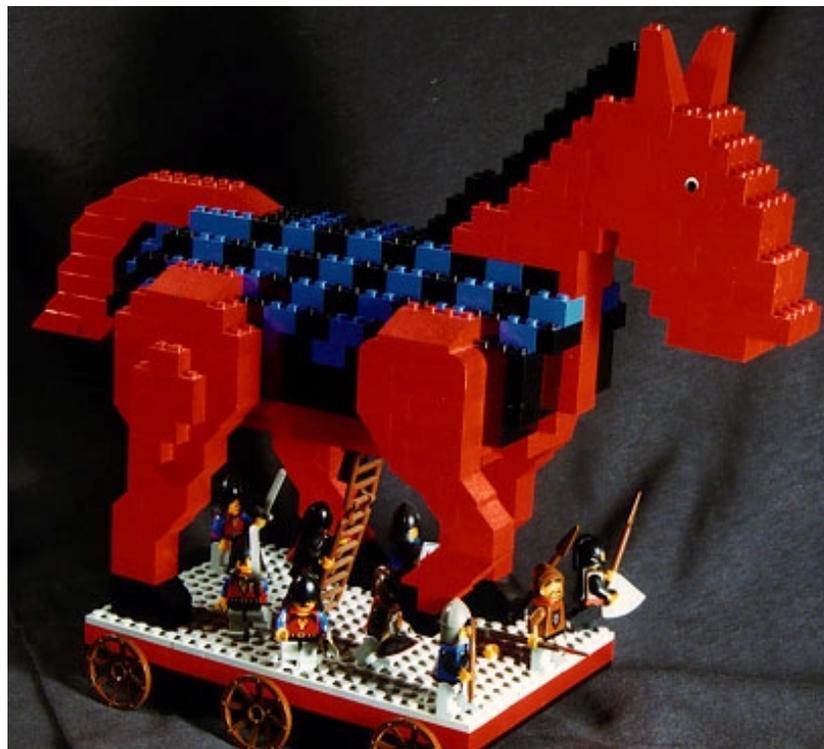
Total messages: 14 Unread messages: 0

Start | Ex... | ej... | Mi... | Ne... | 7:56 PM



# 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.





# Ejemplo de Caballo de Troya

- El Caballo de Troya por login es uno de los más comunes.
- En este ataque, el usuario encuentra su estación de trabajo con una pantalla solicitándole su login.
- El usuario inadvertido teclea su login y su password como de costumbre; esta vez recibiendo un mensaje de error:

login: mbui

Password:

Login incorrect



## Continuación del ejemplo

- En el segundo intento, el usuario logrará acceder al sistema.
- El no sabe que su password fue almacenado en algún archivo donde, más tarde, el creador del Caballo de Troya lo recuperará.
- El falso programa de login, después de almacenar el password robado, invoca el verdadero programa de login, dejando al usuario actuar con una nueva sesión de login.



# Otros ejemplos caballos troya

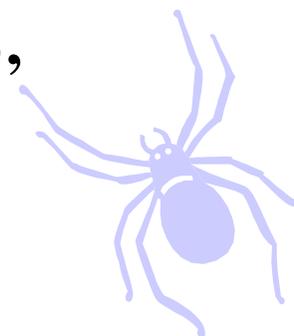
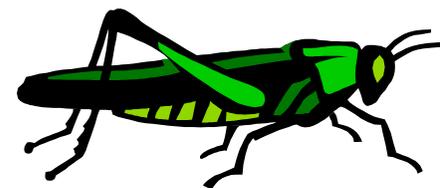
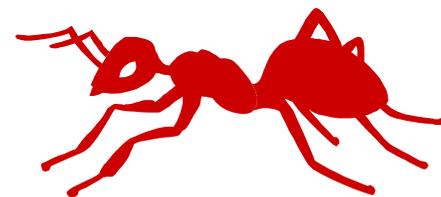
- Whack-A-Mole
  - se capturan datos a través de un juego llamado whackamole.exe.
- BoSniffer
  - utilidad que infecta, se hace pasar como un anti-Back Orifice para borrar trapdoors.
- eLiteWrap
  - programa empaqueta varios archivos en un ejecutable y desempaca estos o los ejecuta en un sistema remoto.





# 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.

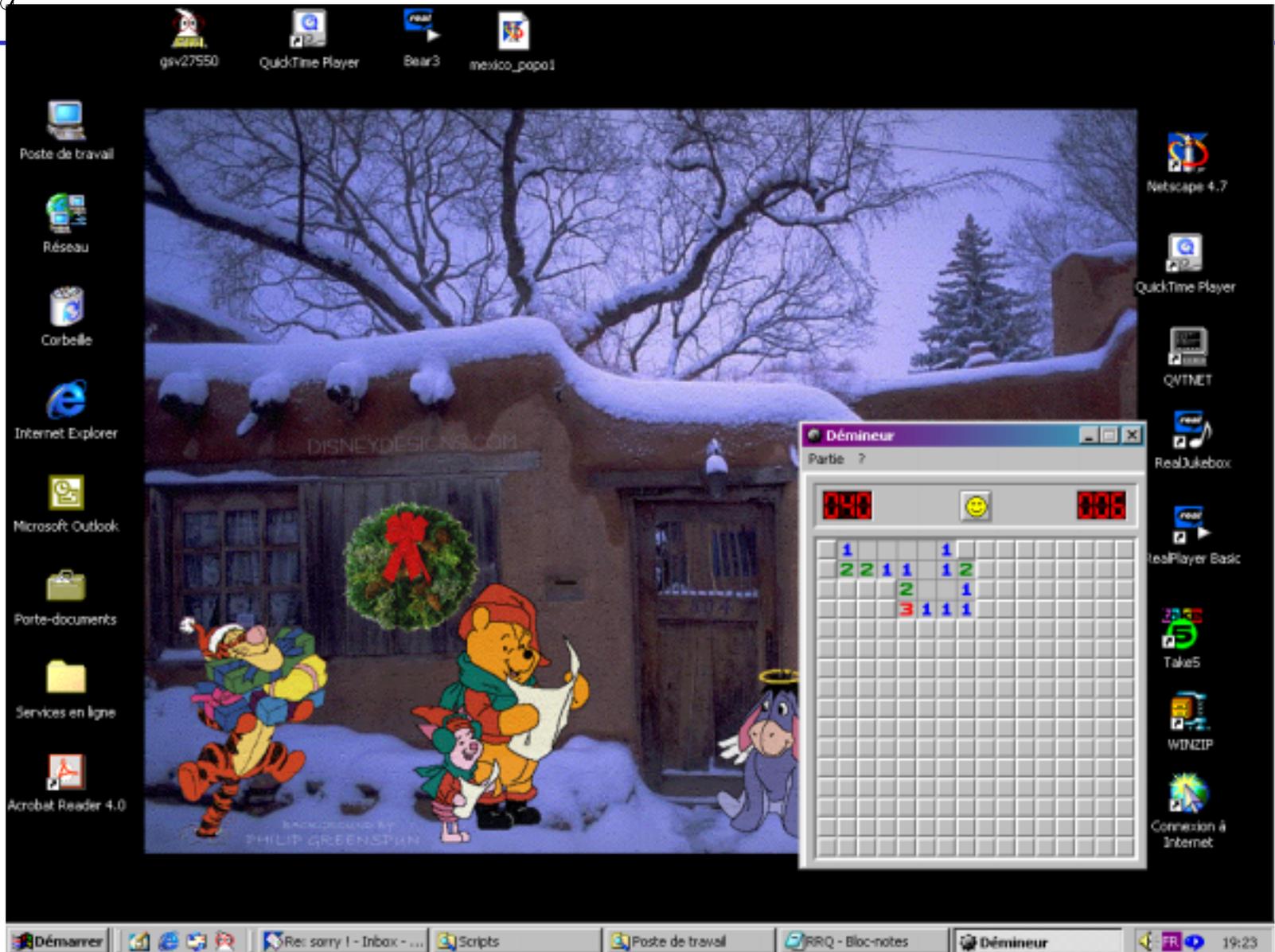




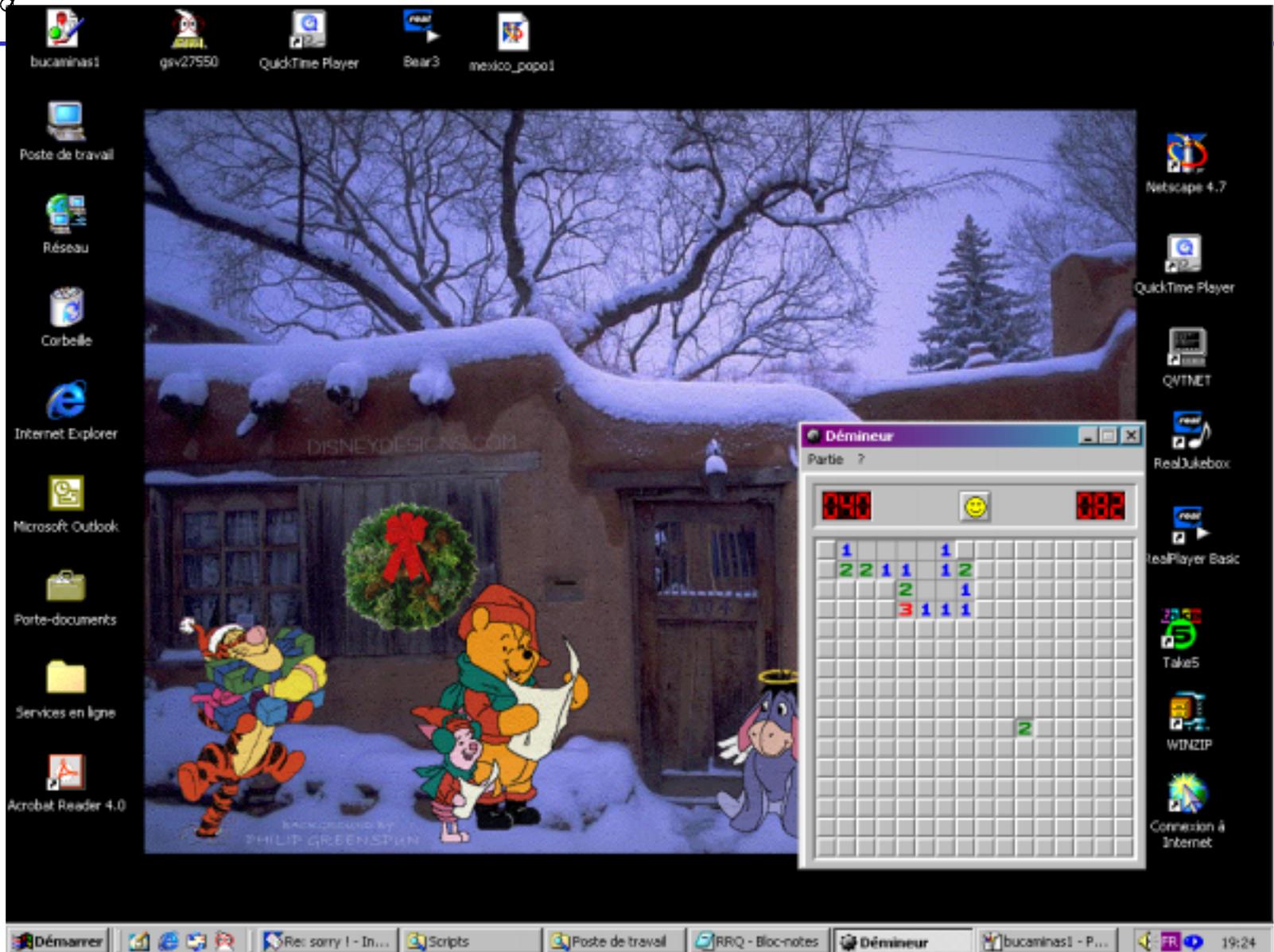
# Ejemplo Backdoor

- Programa buscaminas de Windows 2000
- Correr Minesweeper, teclear “xyzzzy” 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

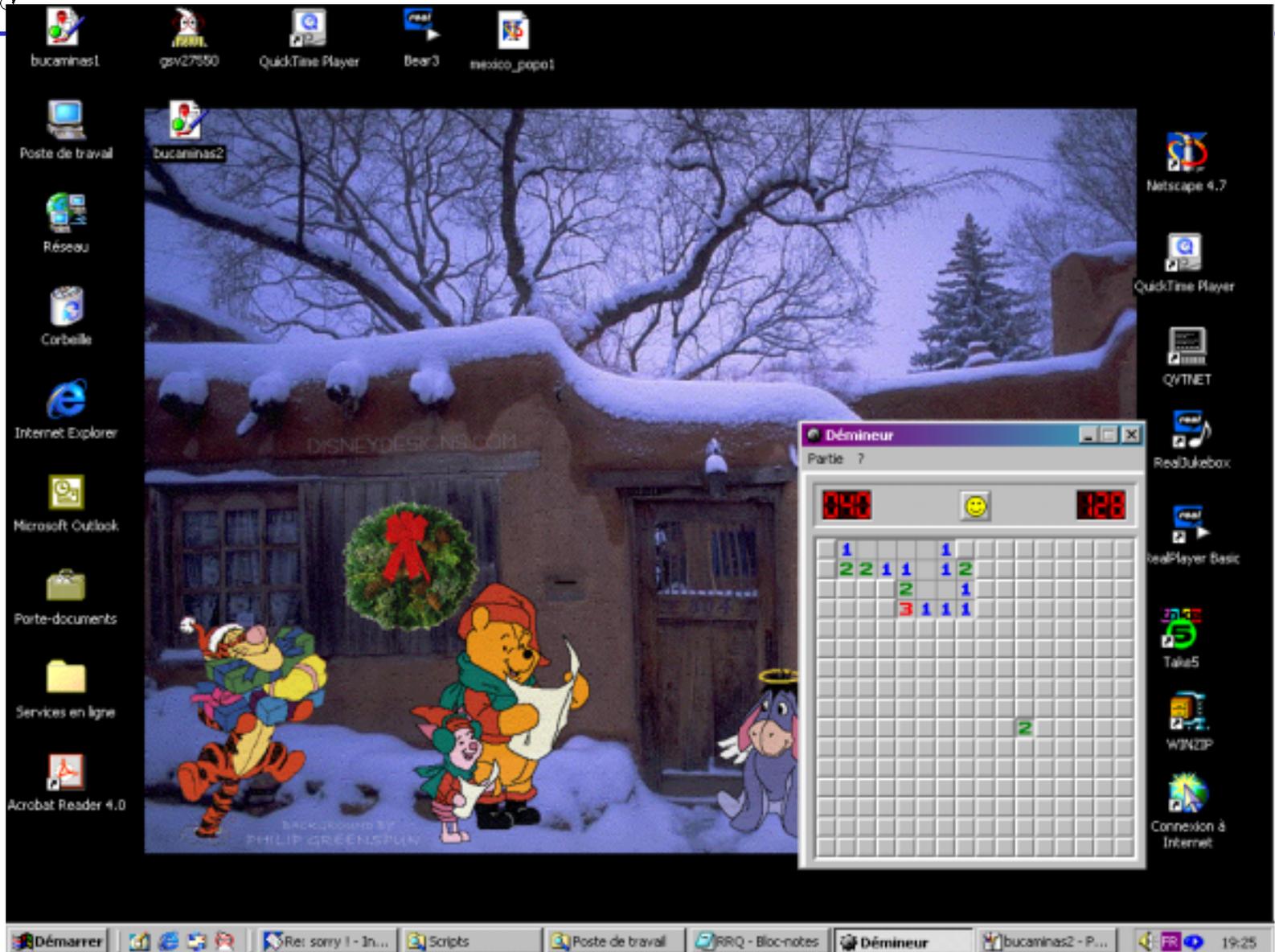
# Trapdoor en buscaminas (1)



# Trapdoor en buscaminas (2)



# Trapdoor en buscaminas (3)



# Trapdoor en buscaminas (4)





# Hoax

(engaño, burla, petardo)

- Típicamente son alertas de peligro, o peticiones de ayuda, empezadas por gente maliciosa - y divulgadas por usuarios inocentes que piensan que están ayudando a la comunidad al espacir la advertencia.
- El incremento de virus y programas troyanos muchos usuarios han usado Internet como un medio para alertar a amigos y colegas de trabajo acerca de estos menesteres.



## Algunos ejemplos de hoax

- A Virtual Card For You
- A.I.D.S. Virus Hoax
- ANTHRAX Virus Hoax
- Anticristo Virus Hoax
- AOL4FREE
- ASPARTAME HOAX
- Big Brother Hoax
- BLOAT VIRUS HOAX
- BUDSAVER.EXE
- SULFNBK Hoax
- Win A Holiday
- Celulares Hoax
- D@fit Hoax
- Dangerous HIV Hoax
- Death Ray
- Deeyenda Virus Hoax
- NEW YORK BIG DIRT HOAX
- Perrin Hoax
- PIKACHUS BALL HOAX
- PKZ300 Warning



## 1er. ejemplo Hoax

Mr. Xxxxx 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.

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 CADA PERSONA QUE ENVIE ESTE MENSAJE. POR FAVOR, DENLE A JESSICA Y A TODAS LAS VICTIMAS DEL CANCER UNA OPORTUNIDAD.



## 1er. ejemplo Hoax (cont)

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](mailto: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



## 2do. ejemplo de Hoax

Netscape and AOL have recently merged to form the largest internet company in the world. In an effort to remain at pace with this giant, Microsoft has introduced a new email tracking system as a way to keep Internet Explorer as the most popular browser on the market. This email is a beta test of the new software and Microsoft has generously offered to compensate those who participate in the testing process.

For each person you send this email to, you will be given \$5. For every person they give it to, you will be given an additional \$3. For every person they send it to you will receive \$1. Microsoft will tally all the emails produced under your name over a two week period and then email you with more instructions. This beta test is only for Microsoft Windows users because the email tracking device that contacts Microsoft is embedded into the code of Windows 95 and 98.



## 3er. ejemplo hoax

Este reenvio lo recibí de un amigo hoy y es verdad lo busqué con estas instrucciones y lo encontré, lo tenía sin saberlo. No lo detecta el Norton 2001 ni McAfee, los tengo instalado y pasó igual. Un virus está llegando a través de los mails de modo oculto. Gracias a un aviso pude detectarlo (lo tenía sin saberlo) y eliminarlo. Buscarlo del siguiente modo:

1. Ir a Inicio
2. Luego: Buscar
3. Archivo o carpeta
4. Típear el archivo: sulfnbk.exe
5. Eliminar (NO ABRIRLO)
6. Eliminar de la papelera de reciclaje

Gracias a estas instrucciones lo eliminé.. suerte..



# ¿Qué hacer?

- No redireccionar mensajes de este tipo.
  - sistema correo puede colapsar debido al redireccionamiento de este tipo de mensajes
- Los corporativos pueden confrontar este tipo de problemas, con un políticas del estilo:
  - usuarios finales no deben difundir alertas de viurs
  - cualquier informe de virus se debe enviar al departamento de sistemas de información



# Precauciones a tomar con correos electrónicos

- Si recibe un correo, con un archivo en attach, de una fuente desconocida simplemente borrelo.
- Los virus y programas troyanos contienen código que es necesario ejecutar para poder infectar
  - si hace doble-click sobre un archivo que viene en forma de attach dentro de un correo, esta ejecutando código y puede infectar su máquina
  - ningún antivirus es capaz de “scanear” estos archivos antes de abrirse



# Spam

- Intento de entregar un mensaje, a través de Internet, a una persona que de otra forma no hubiera elegido recibirlo.
- Cada vez recibimos más correos no deseados:
  - Ventas.
  - Insultos.
  - Bombardeos.
  - Pornografía
  - Hoax





# Spam ...

- Todas las plataformas aceptan correo de Internet.
- Se consiguen listas de varios sitios de internet y después se envían información que en su mayoría es publicidad comercial.
- Consecuencias:
  - pérdida productividad del usuario reducción de disponibilidad de recursos



# Ejemplo spam

Read Minds - Trash - Netscape Folder

File Edit View Go Message Communicator Help

Subject	Sender	Date
Read Minds	gp@sina.com	Tue 12:06 PM

**Subject:** Read Minds  
**Date:** 14 Aug 01 12:06:17 PM  
**From:** [gp@sina.com](mailto:gp@sina.com)  
**Reply-To:** [alengk@china.com](mailto:alengk@china.com)  
**To:** [suzl@soho.net](mailto:suzl@soho.net)

Lottery Winnings

Get free help with horoscopes and lucky numbers. Increase your odds of winning the lottery. We have helped thousands win big \$. Go <http://www.onlinepsychic.com/indexmnr.html>

Are you being cheated on?

Odds are you might be. Over 50% of all relationships involve spouses who cheat. We can tell you if your spouse is cheating. Free readings online at <http://www.onlinepsychic.com/indexmnr.html>

You are in luck

You are entitled to one free psychic reading from the nation's leading internet psychic. Visit <http://www.onlinepsychic.com/indexmnr.html> today for your free reading.

100% Accurate

Our master psychics can predict your future and unlock hidden secrets to make you money, find you love and romance, and secure your happiness. You get one free reading anytime, so visit <http://www.onlinepsychic.com/indexmnr.html> today for your free reading.

Document: Done

Start | E.. | D.. | R.. | W M.. | M.. | 4:44 PM

# Aclaración sobre SPAM



[Fwd: INVITACION ESPECIAL A ClasificadoRural - Sus ANUNCIOS] - Inbox - Netscape Folder

File Edit View Go Message Communicator Help

Name	Subject	Sender	Date	Priority	Stat...
Local Mail	Bonjour !!	Erika Mata Sanchez	11/17/2000 9:34 ...		read

**Subject:** INVITACION ESPECIAL A ClasificadoRural - Sus ANUNCIOS  
**Date:** Fri, 29 Sep 2000 11:17:14 -0400  
**From:** [Avisos@ClasificadoRural.com](mailto:Avisos@ClasificadoRural.com)  
**To:** <[Anuncio@cem.itesm.mx](mailto:Anuncio@cem.itesm.mx)>

*Estimado amigo:*

Tenemos el agrado de anunciarle la disponibilidad de su sitio en Internet, <http://www.clasificadorural.com>  
Agradeciendole anticipadamente su visita al mismo.

Escribanos a: [clasificadorural@ciudad.com.ar](mailto:clasificadorural@ciudad.com.ar)

 **ClasificadoRural.com**   
LA HERRAMIENTA DEL CAMPO

Nuestro objetivo es convertirnos en la herramienta para el hombre de campo y para quienes dedican su vida y su profesion a esta trascendente actividad. A través de <http://www.clasificadorural.com> Ud. podrá en forma sencilla, amigable y eficiente ofrecer sus productos y servicios y encontrar la mejor oportunidad para sus negocios y necesidades.

**Aclaración sobre SPAM: Bajo decreto S1618 titulo 3ro. Aprobado por el 105 congreso de estandarización de normativas internacionales este E-mail no podrá se considerado SPAM mientras incluya una forma de ser removido. Si no desea recibir este mensaje por favor re-envie este e-mail a [clasificadorural@ciudad.com.ar](mailto:clasificadorural@ciudad.com.ar) colocando en asunto eliminar y será automáticamente removido de nuestra base de datos**

Total messages: 113 Unread messages: 0

Start Tivol... E... M... M... h... L... 2:16 PM



# Ingeniería Social.



- Es una de las formas más comunes para penetrar sistemas de “alta seguridad”.
- Uso de trucos psicologicos, por parte de un atacante externo, sobre usuarios legitimos de un sistema para obtener información (usernames y passwords) necesaria para acceder a un sistema.
- Se basa en ataques como: usurpación de identidad, pepena, inocencia de la gente, relaciones humanas, etc.





# Ejemplo ingeniería social

"Hi Bev, this is Sam from the IS Department. We just got in a new corporate screensaver and since you're the VP's secretary you will get it first. It's really cool wait 'till you see it. All I need is your password so I can log on to your PC from the computer center and install it.

Oh Great!!!!!! My password is rover. I can't wait to see that new screen saver!!!!!!"



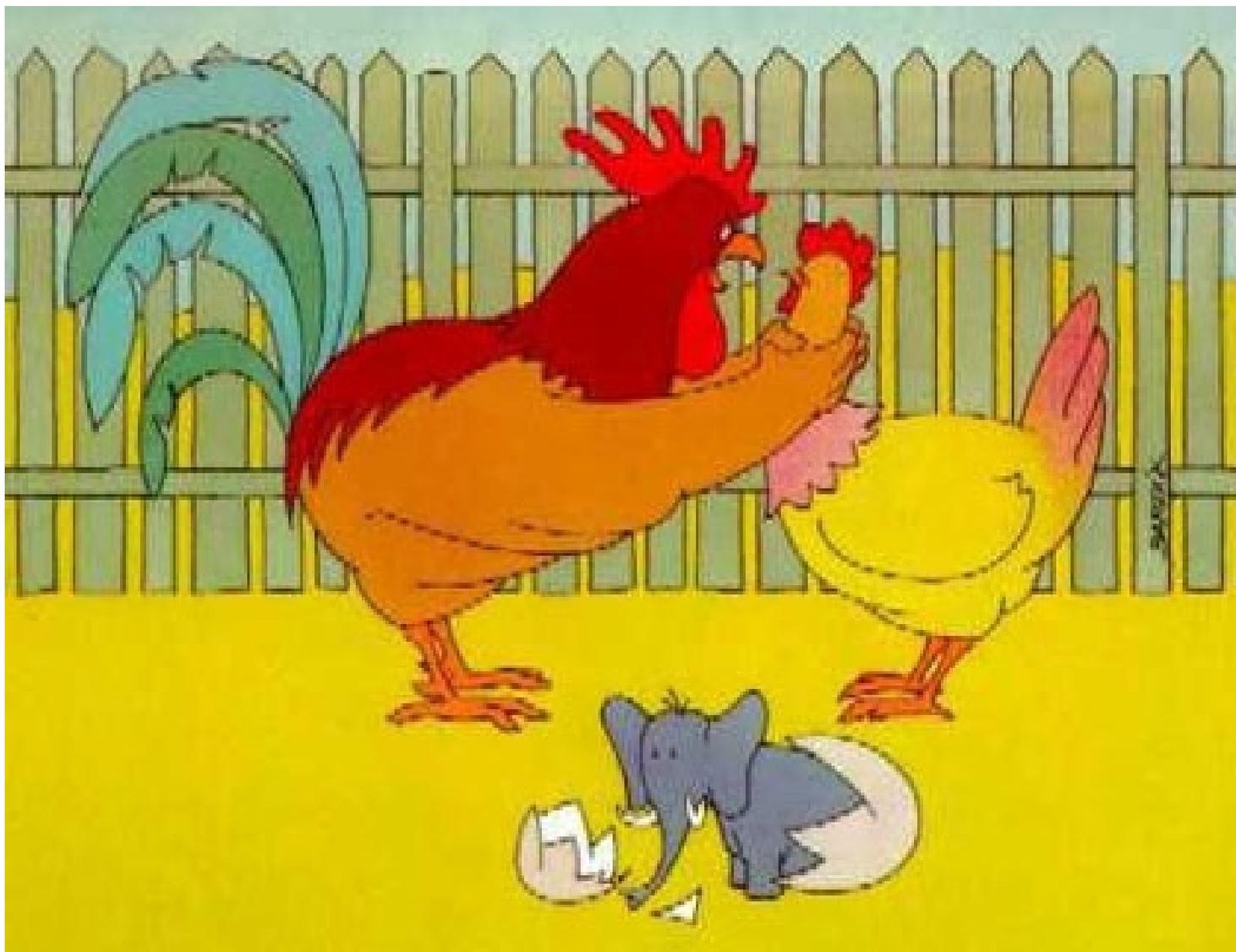
# Falsificación

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



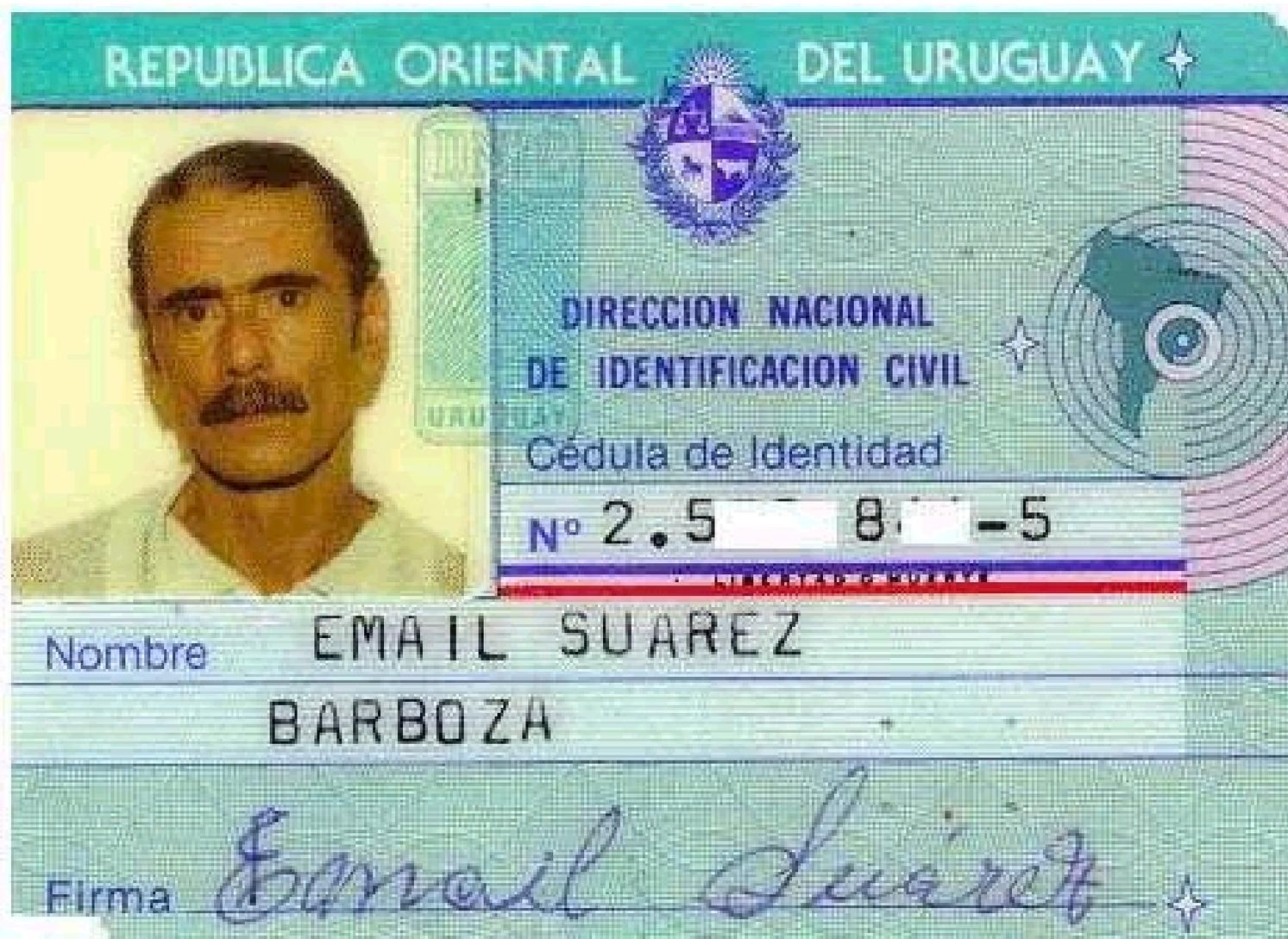


# Usurpación



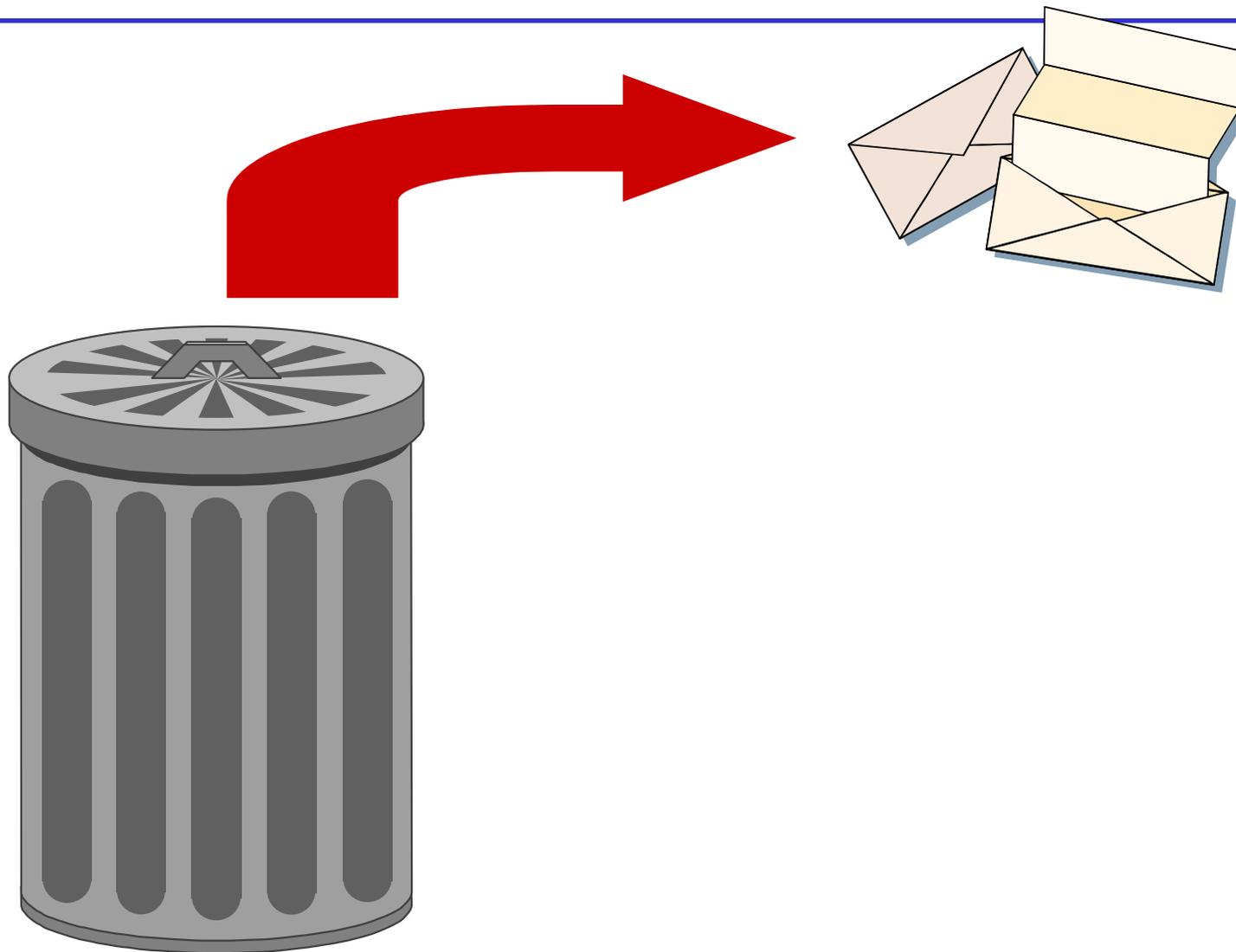


# ¿Quién es e-mail?





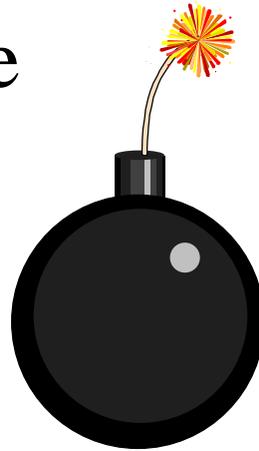
# Pepeña





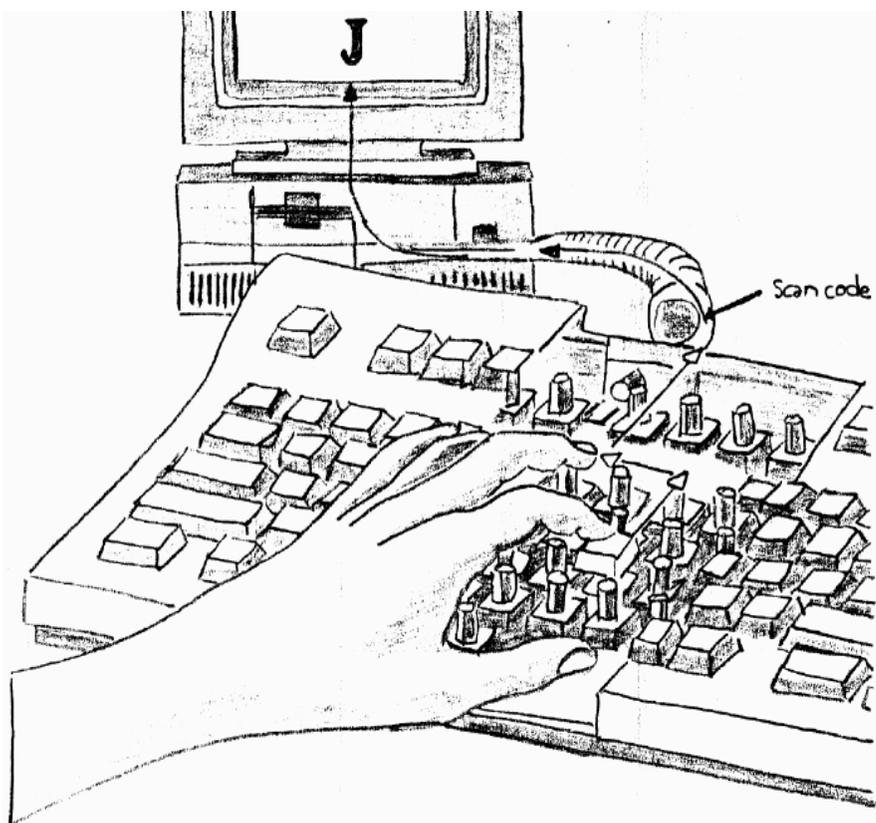
# Bomba lógica

- 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





# Grafitti

- Consiste en sustituir 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)

Newscape: The Labour Party

Back Forward Home Reload Images Open Print Find Stop

Location: <http://www.labour.org.uk/>

Labour

**new Labour  
new Britain**



## Next time the Tories would stop at nothing

If the Tories get in again, there would be fewer good schools to go to. Already the number of failing schools has doubled since 1994.

If the Tories get in again, the NHS would not be there when you need it. There are already 28,000 more managers and 50,000 fewer nurses in the NHS.

If the Tories get in again, more young criminals would be free to re-offend. Crime has already doubled under the Tories, and only one in 50 crimes ever leads to a conviction.

If the Tories get in again, there would be more VAT on food and fuel. The Tories have already put VAT on heating.



- Not enough good schools
- NHS not there when you need it
- More young criminals getting away with it
- More VAT - food could be more

### Next time the Tories would stop at nothing

### Enough is enough

If you have had enough of the Tories and want to help Labour, call 0990 300 900.

Designed by **The Fine Publishing**





# Agencia Central de Inteligencia (original)





# Agencia Central de Inteligencia (hackeada)

NetScape: Central Intelligence Agency

Location: <http://www.cia.gov/>

## Welcome to the Central Stupidity Agency

We'd just like to say one thing... And that's...

### STOP LYING BO SKARINDER!!!

### SLUTA LJUG BO SKARINDER!!!

Please choose one of the all the following categories below:

 Welcome!	What's <b>NEW</b> in space	About the <b>OIA</b>
 Publications	 Nude Girls	Other Intelligence  Community Links

Power Through Resistance would like to say: FUCK YOU to the Central Intelligence Agency World Wide Web site... but we already know you're all busy suckles.

Now that's all the politics we've got going on here, sorry but we know it's all politics anyway...

seems but so few suckles here so little for so one...

- [The Swedish Hackers Association Protocol #3](#) - SHIA Protocol #3
- [The Swedish Hackers Association Protocol #4](#) - SHIA Protocol #4
- [Feedback](#) - The Feedback
- [Science](#) - The Underground
- [Other Intelligence Community Links](#) - Other Web sites of interest

This site was hacked by Power Through Resistance

<http://www.sans.org>



Address <http://www.sans.org/newlook/home.htm>

Go Links



# Fluffi Bunni OWNZ YOU.

A BamBam here a dot slash there  
here a dot there a slash  
everywhere a dot slash

look mommy im on sans !



# Ataque de Fuerza Bruta

- También Llamado Exhaustive Attack.
- “Consiste en Descubrir Datos Secretos al Tratar Todas las Posibilidades y Checar para Corregir”
- Para una Contraseña de Cuatro Dígitos
  - uno puede iniciar con 0000 y moverse al 0001, 0002 hasta 9999.



## Basado en diccionario

- También conocido como “Spelling Dictionary”
- Todas las contraseñas deben ser encriptadas, una vez que los usuarios las introducen en forma de texto claro.
- Existen diccionarios de escritura correcta (spelling dictionary) encriptadas o listas de contraseñas comunes que se usan para intentar penetraciones a los sistemas
- Copiado de una tabla cifrada de contraseñas y se intenta el acceso usando los resultados en lugar de un diccionario.



## 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.

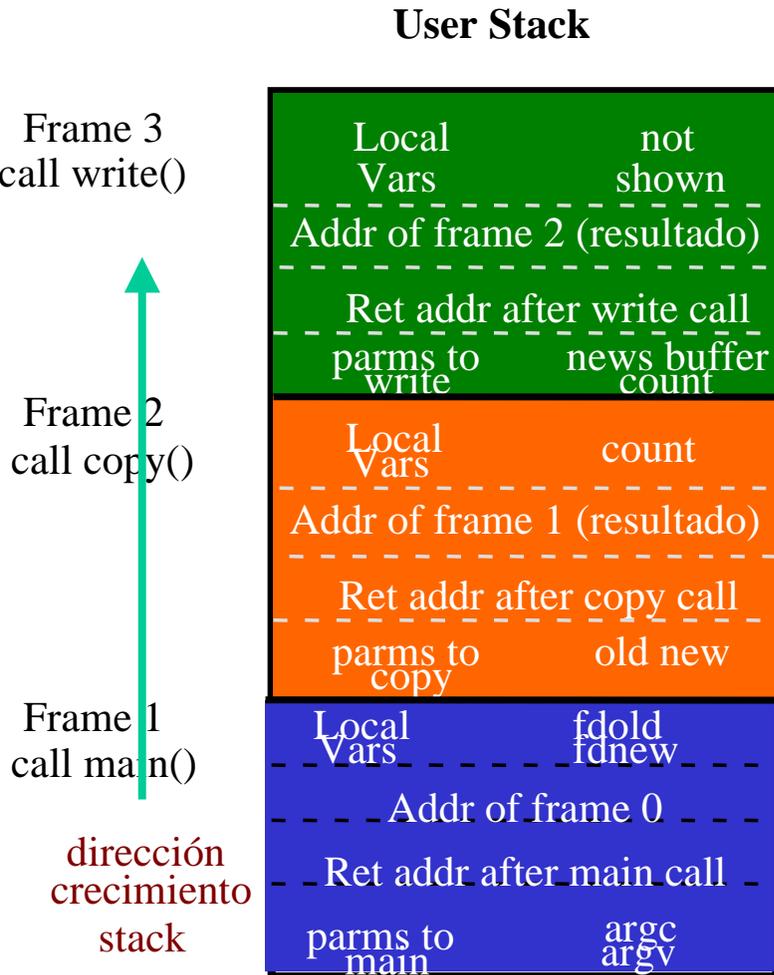


## El stack o buffer overflow

- 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.



# ¿Para que sirve el stack?



```
copy (int old, int new)
```

```
{  
    int count;  
    while ( (count = read(old, buffer, sizeof(buffer))) > 0 )  
        write(new, buffer, count);  
}
```

```
main(argc, argv)
```

```
{  
    int fdold, fdnew;  
    fdold = open(argv[1], O_RDONLY);  
    fdnew = open(argv[2], 0666);  
    copy (fdold, fdnew);  
    exit(0);  
}
```



# Un primer ejemplo

**toto@cachafas:1> cat prog1**

```
int main(int argv,char **argc) {  
    char buf[25];  
  
    strcpy(buf,argc[1]);  
}
```

**toto@cachafas:2> gcc prog1.c -o prog1**

**toto@cachafas:3> prog1 'esto es una prueba de un buffer overflow'**

????????????????????????????????

¿¿que pasa si en lugar de strcpy() se usa strncpy()??



# Un segundo ejemplo

```
void function(int a, int b, int c)
{
    char buffer1[5];
    char buffer2[10];
    int *ret;
    ret = buffer1 + 12;
    (*ret) += 8;
}
```

```
void main( ) {
    int x;
    x = 0;
    function(1,2,3);
    x = 1;
    printf("%d\n",x);
}
```

```
toto@cachafas:4> gcc prog2.c -o prog2
```

```
toto@cachafas:5> prog2
```

```
0
```

```
toto@cachafas:6>
```



# 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



# DoDS: Negación Servicio Distribuido

- En febrero/marzo del 2000, varias empresas que apoyan su estrategia en Internet fueron atacadas.
- Entre ellas destacan:
  - CNN (Agencia Noticiosa)
  - Amazon (Venta de libros, discos, etc.)
  - e-Bay (Venta de artículos en remate)
  - e-Trade (compra y venta de acciones)
  - Yahoo (Correo gratuito)



# Características

- **Tipo** : *Negación de servicio desde cientos de máquinas*
- **Duración** : *Dos horas aprox.*
- **Conocimientos del intruso** : *Básicos*
- **Primeros ataques registrados** : *Más de cuatro meses*
- **Localización del culpable**: *Casi nula*
- **Solución total** : *No existe*
- **Solución aproximada** : *Reforzamiento de seguridad y detección de intrusión*

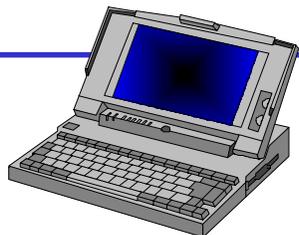


# Consecuencias

- El presidente de Estados Unidos, Bill Clinton, solicitó 2 mil millones de dólares para combatir los terroristas cibernéticos.
- Creación de un centro nacional de seguridad cibernética.
- El gobierno Japonés solicita apoyo a Estados Unidos ante insistentes ataques de hackers.
- Falsificación de tarjetas inteligentes
- Negación de Servicio en Yahoo, e-Bay, Amazon, CNN, entre otras



# Descripción ataque sufrido



**Hacker**



**Máquina  
inocente**



**Máquina  
inocente**

**1. Ambiente normal**



**Usuario**



**Víctima**



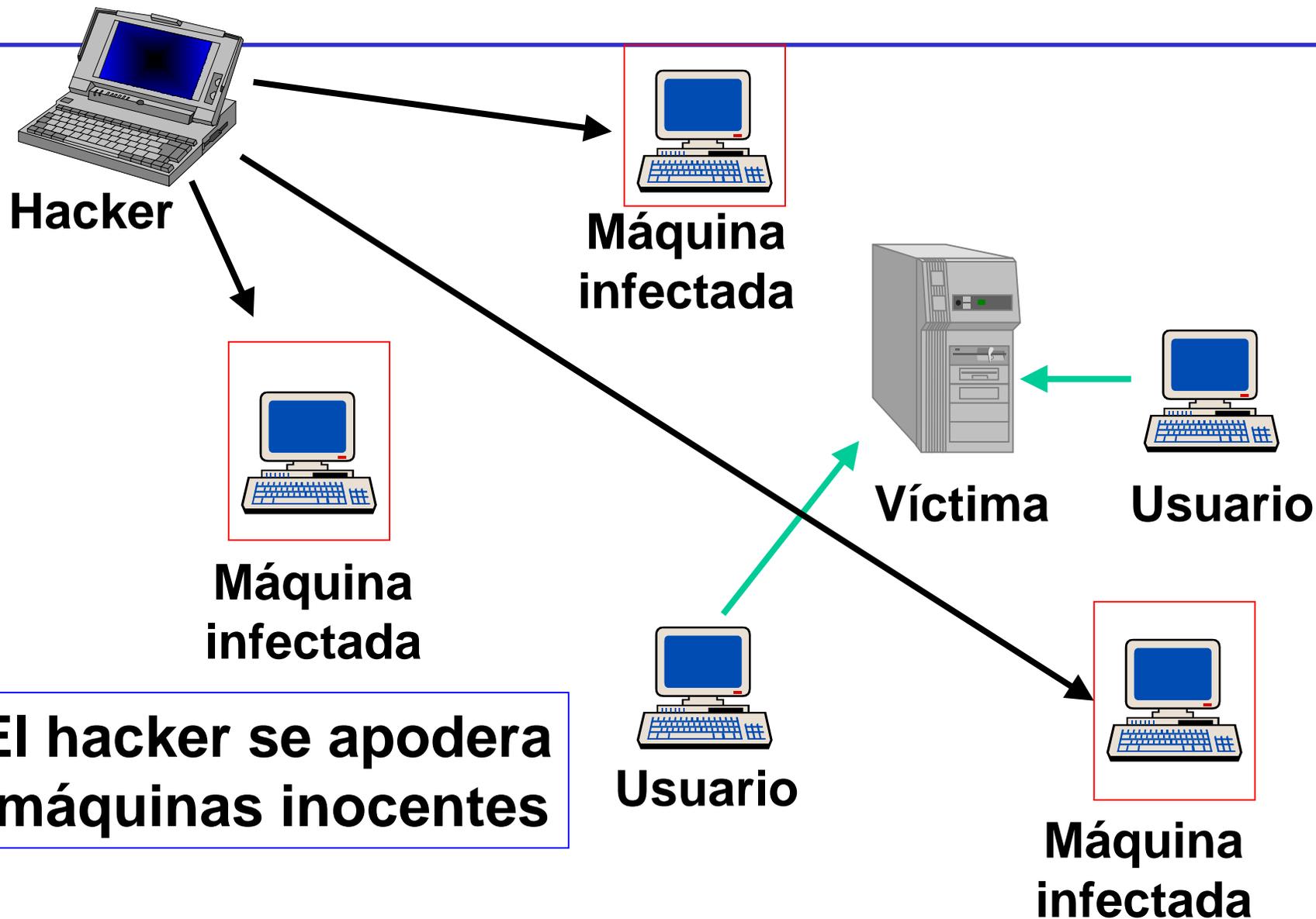
**Usuario**



**Máquina  
inocente**



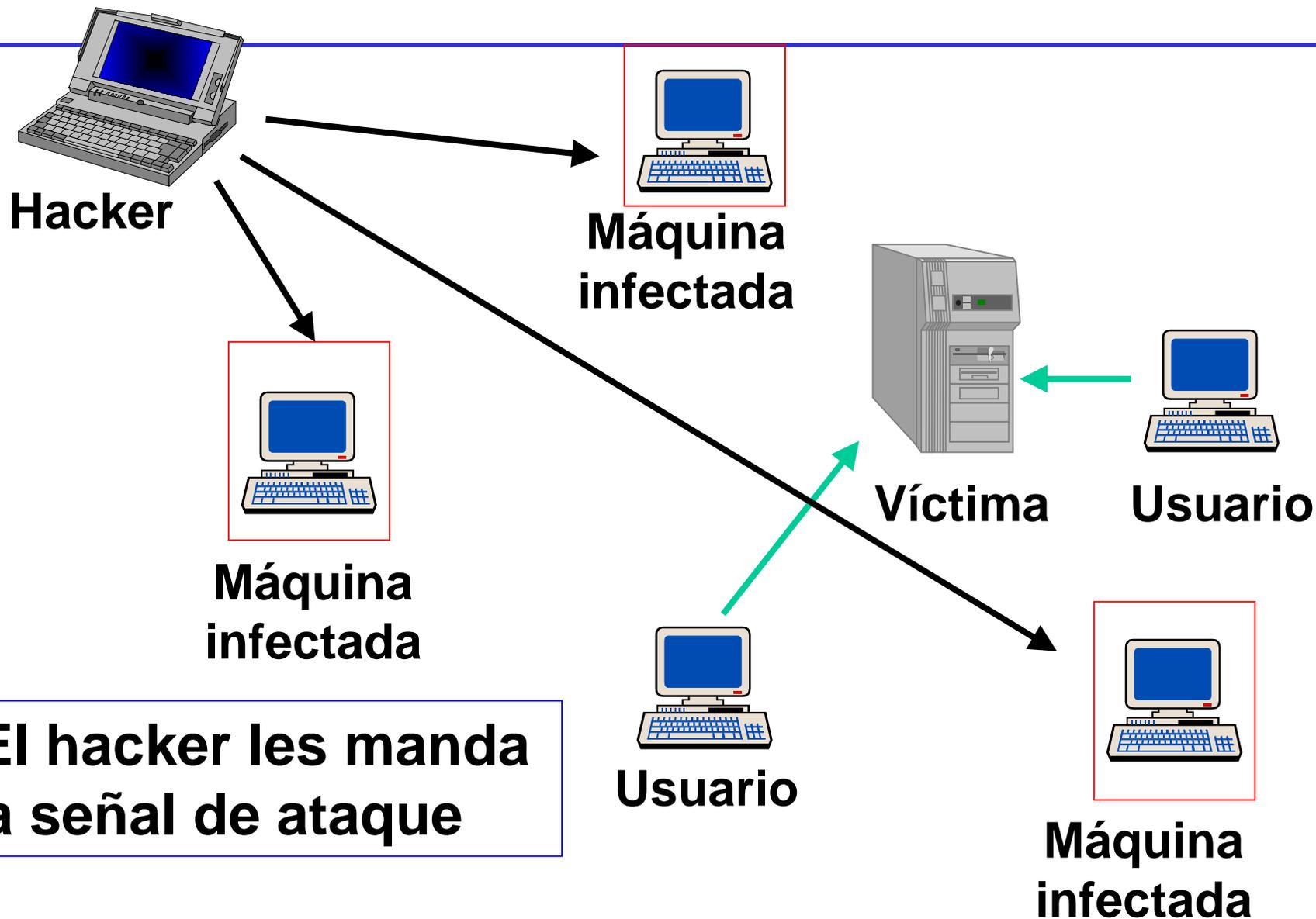
# Descripción ataque sufrido



**2. El hacker se apodera de máquinas inocentes**



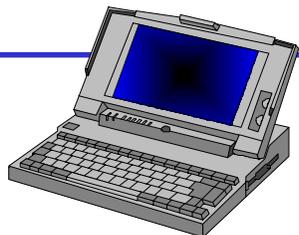
# Descripción ataque sufrido



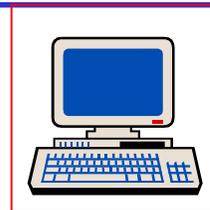
**3. El hacker les manda una señal de ataque**



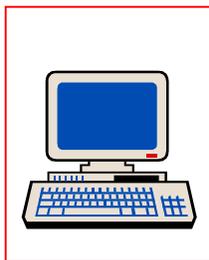
# Descripción ataque sufrido



**Hacker  
sólo observa**

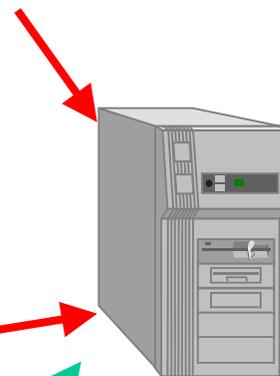


**Máquina  
infectada**



**Máquina  
infectada**

**4. Las máquinas  
infectadas  
atacan a la víctima**



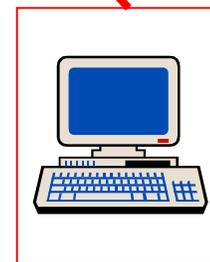
**Víctima**



**Usuario**



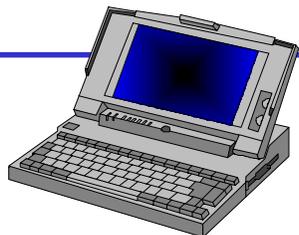
**Usuario**



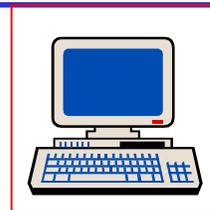
**Máquina  
infectada**



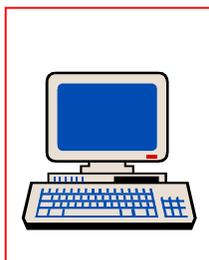
# Descripción ataque sufrido



**Hacker  
sólo observa**

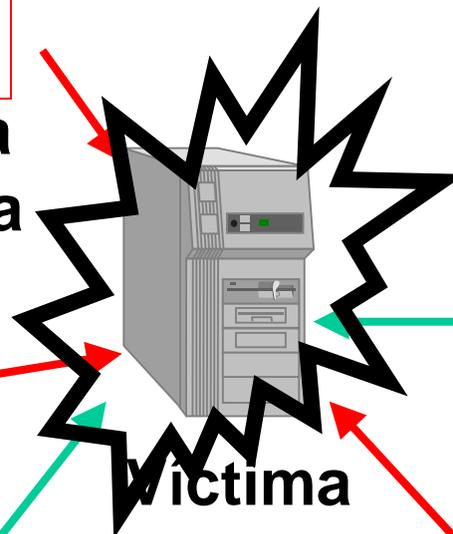


**Máquina  
infectada**



**Máquina  
infectada**

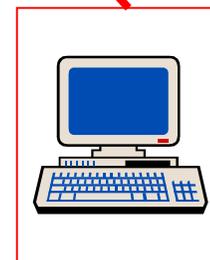
**5. La máquina víctima  
no puede dar servicio**



**Usuario**



**Usuario**



**Máquina  
infectada**

# Mission: Total Overload

Investigators and computer-security experts aren't certain how the attacks were carried out, but the hackers likely used a so-called 'smurf' assault like this:

- Hacker program
- 'Ping' or query
- Response
- Failure to connect

**1** The hacker scans the Internet for vulnerable 'server' or 'host' computers operated by businesses and universities

**2** The hacker then breaks into the weak computers and secretly stashes a 'slave' software program that will await his instructions to begin the attack

'Are you alive?'  
(sent to network PCs)

'Are you alive?'  
(sent to network PCs)

**3** He issues the signal and the slaves begin to broadcast a 'ping' request to their locally connected computers, asking whether they are 'alive,' that is, online and working

**3** He issues the signal and the slaves begin to broadcast a 'ping' request to their locally connected computers, asking whether they are 'alive,' that is, online and working

Last week's cyberattacks will be difficult to trace. They could have originated from anywhere in the world, they used multiple computers belonging to others to cover their in-



'I'm here'  
(overwhelms target site)

**4** Amazon.com is so flooded with bogus replies from hundreds, if not thousands, of machines that legitimate attempts to get through never make it to the victimized site

**4** Their reply directed back instead, the hacker forces the return address to victim, in this case Amazon.com

a computer at the University of Santa Barbara. Stanford and confirmed that their computers were the attacks. By the end of the year, the FBI was seeking subpoenas to subpoena records from servers in California and Oregon. The FBI probably won't get the authorities to go after the real culprits, who are likely to leave valid return addresses. The FBI's strategy is that by painstakingly examining the logs of the routers that direct Internet traffic, investigators might discover clues about the origin of the attack. Another approach is to examine the "magic packets" directed at the target computers, in hopes of identifying snippets of text or code that identify the perpetrators. "It's a snow-drift of a hunt," says a law-enforcement source. "These investigations are time-consuming and immense." The FBI is currently overloaded with Internet infrastructure (a situation made worse by the lucrative private sector), so it often relies on outside consultants, who have moved operations to the Pennsylvania Avenue headquarters of the FBI. The consultants have specialized software to speed the technical search.

The FBI was extremely careful, and its "forensics" approach won't be the FBI would have to rely on traditional detective work to nab the culprits. "They are probably using anonymous informants through the underground to try to gain intelligence on who might be behind these attacks," says former hacker Kevin Mitnick, who was recently released from prison. "Their motive is bringing rights, and their tale will be told to an investigator who's the FBI's best chance at finding out who's behind this."

The FBI was found at the end of the year. "If caught, the perpetrators could face years in prison with a fine of up to \$250,000 (each). Mitnick admitted that he only doesn't know who they are, but is unsure of their motives. Some investigators, including digital rubberneckers, have ventured several theories on what's behind it:

**1. Hackers.** Launching an assault on a computer or Web site for financial gain is a hallmark of many hackers, who get their chips on a crummy laptop machine to compete with e-commerce moguls like

Jeff Bezos. (These are the guys with the "white hat" over to work for someone else.) These could be teenage geeks ("Aardvark" "Not now, Mom, I'm to its knees!") or a techno-vandal, the kind who fires digital bullets from a cybercafé in San Francisco. Since then, the FBI has been looking for the culprits.

do...  
tively...  
or "script...  
hind one or...  
Web meltdown...  
walk down the street...  
nas and tires," says A...  
sometimes they take o...  
**Profiteers.** On the...  
there is a financial co...  
NEWSWEEK has learn...  
been alerted to the p...  
attacks might have been...  
price of computer-se...  
leapt skyward this w...  
near panic about the f...  
"You don't do this...  
involved," says one so...  
investigation...  
but seven times...  
no evidence...  
panies are the...  
lent of hock...  
In fact, they're...  
ting hit the...  
ried all week...  
ried," says Z...

Network Associates...  
**Net purists.** Not too...  
was the last, best hop...  
aisance of personal ex...  
speech, embracing the...  
man experience. Now...  
mega shopping mall...  
hours, Brimfields and...  
gift of instant billionai...  
ways comparable to w...  
tle at the WTO (anti...  
says Kalle Lasn, edito...  
hased magazine Adbu...  
the DOS was launch...  
rouse the credit-card...  
calls "a consumer tr...  
who has helped orga...  
the Web-activist grou...  
"These DOS attacks...  
our tactics, but we alw...  
sage," he says. Still, i...  
that while Yahoo's



# Consecuencias

- Económicas
  - ✘ El criterio de los inversionistas se vio afectado directamente (ej. acciones a la baja)
  - ✘ Yahoo! estima pérdidas por US\$500,000 dls por dejar de dar servicio durante 3 horas
  - ✘ Incitación hacia la competencia ilícita
- Legales
  - ✓ El FBI investigará el origen de los ataques y se sancionará severamente a los que resulten responsables

No me van a creer, pero acabo de recibir por parte de mi esposa un ATAQUE DE NEGACIÓN DE SERVICIO.



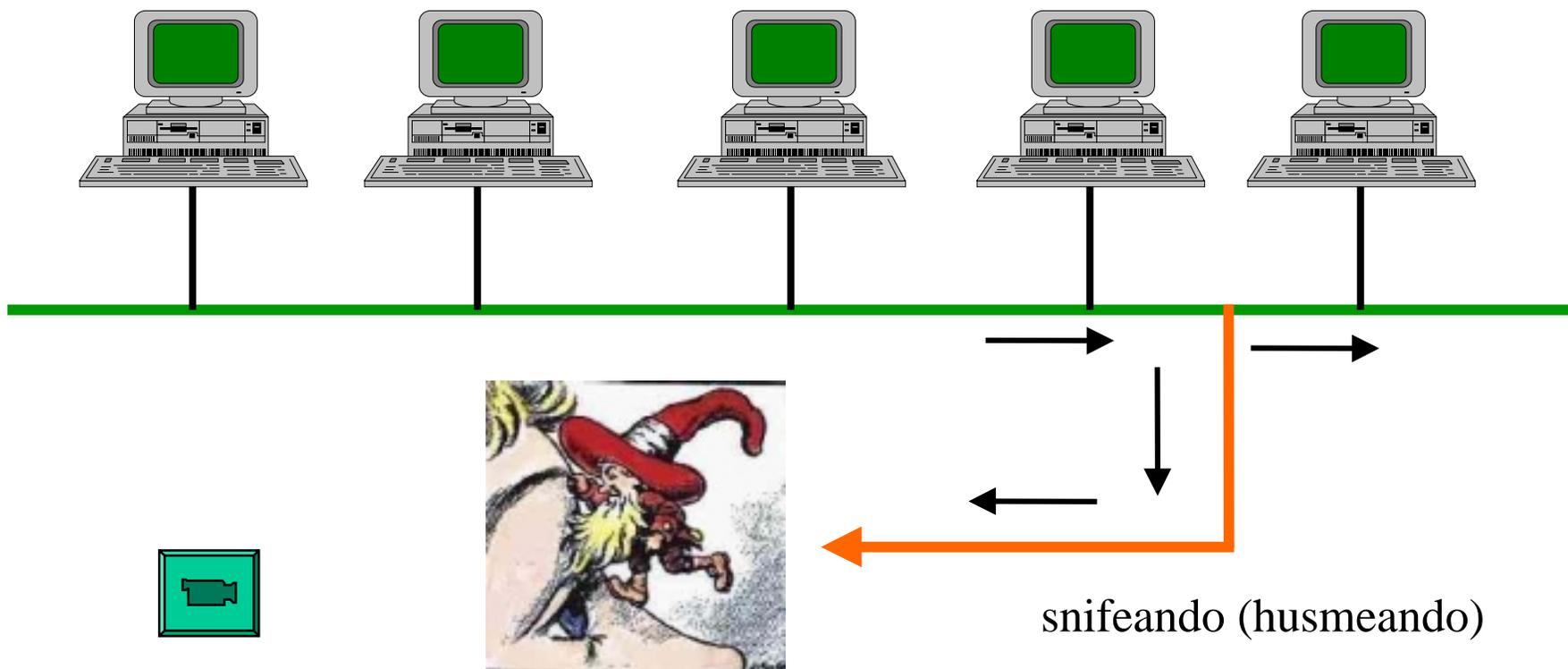
**A la moda...**

por jamaya



# Sniffers

¿Cómo se comunican dos computadoras en una red local?



snifeando (husmeando)

computadora en  
modo promiscuo



# Análisis de tráfico

- Termino en inglés: Traffic Analysis
- El análisis de tráfico es una técnica complicada para inferir posibles sucesos a partir de la cantidad de información que circula en uno o varios segmentos de red.
- No es necesario que la información circule “en claro”.
- Usada por los americanos durante el inicio de la segunda guerra mundial

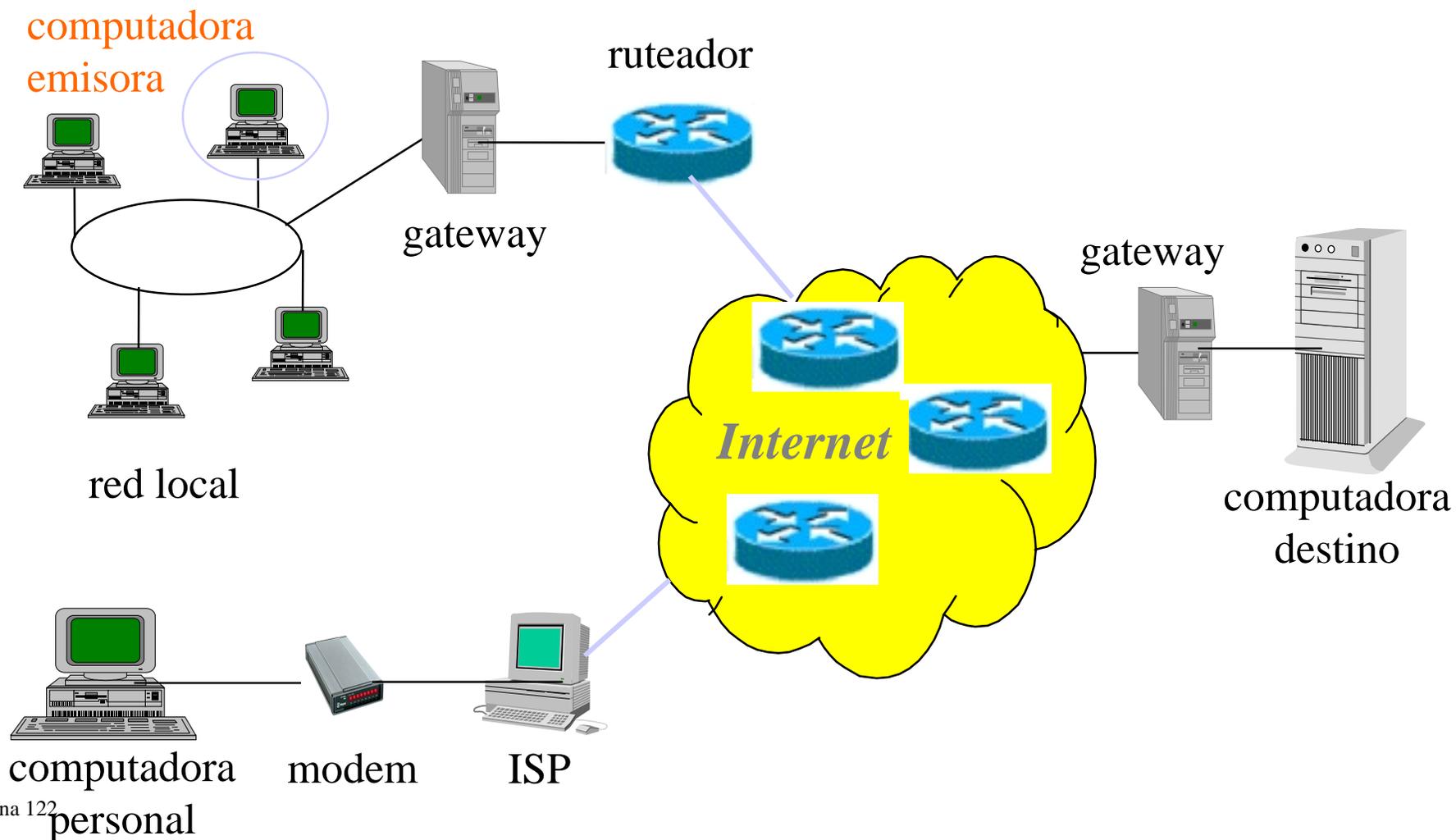


# Spoofting

- Spoofting es la creaci3n de paquetes de comunicaci3n TCP/IP usando una direcci3n IP de alguien m1s.
- Lo anterior permite entrar en un sistema haci3ndose pasar por un usuario autorizado.
- Una vez dentro del sistema, el atacante puede servirse de 3ste como plataforma para introducirse en otro y as3 sucesivamente.



# ¿Cómo se comunica una computadora con otra?





# Un ejemplo de Spoofing

- Un ejemplo es hacer un telnet al puerto 25 y enviar correos a nombre de otra persona.
  - una variante es modificar los parametros del manejador de correos.
- Además, cualquiera, con un poco más de conocimientos, puede escoger cualquier dirección IP.



# Otros ejemplos de Spoofing

- **Man-in-the-Middle**
  - los paquetes pretenden ser un extremo de la comunicación.
  - el atacante intercepta los paquetes y puede responder haciéndose pasar por otra máquina
- **Routing Redirect**
  - redirecciona el ruteo de la información del host original al host del atacante (variante método anterior).
- **Source Routing**
  - redirecciona paquetes individuales por el host atacante



# Otros ejemplos de Spoofing

- Blind Spoofing
  - redirecciona la respuesta de un host, permitiendo mandar comandos, pero no puede obtener respuesta inmediata.
- Flooding
  - envía mensajes a varias máquinas aleatorias.
  - estos mensajes llenan la cola de recepción de direcciones de origen con la dirección de la máquina víctima
  - esto provoca que las máquinas le envíen mensajes de respuesta a la víctima, provocando que esta última se sature

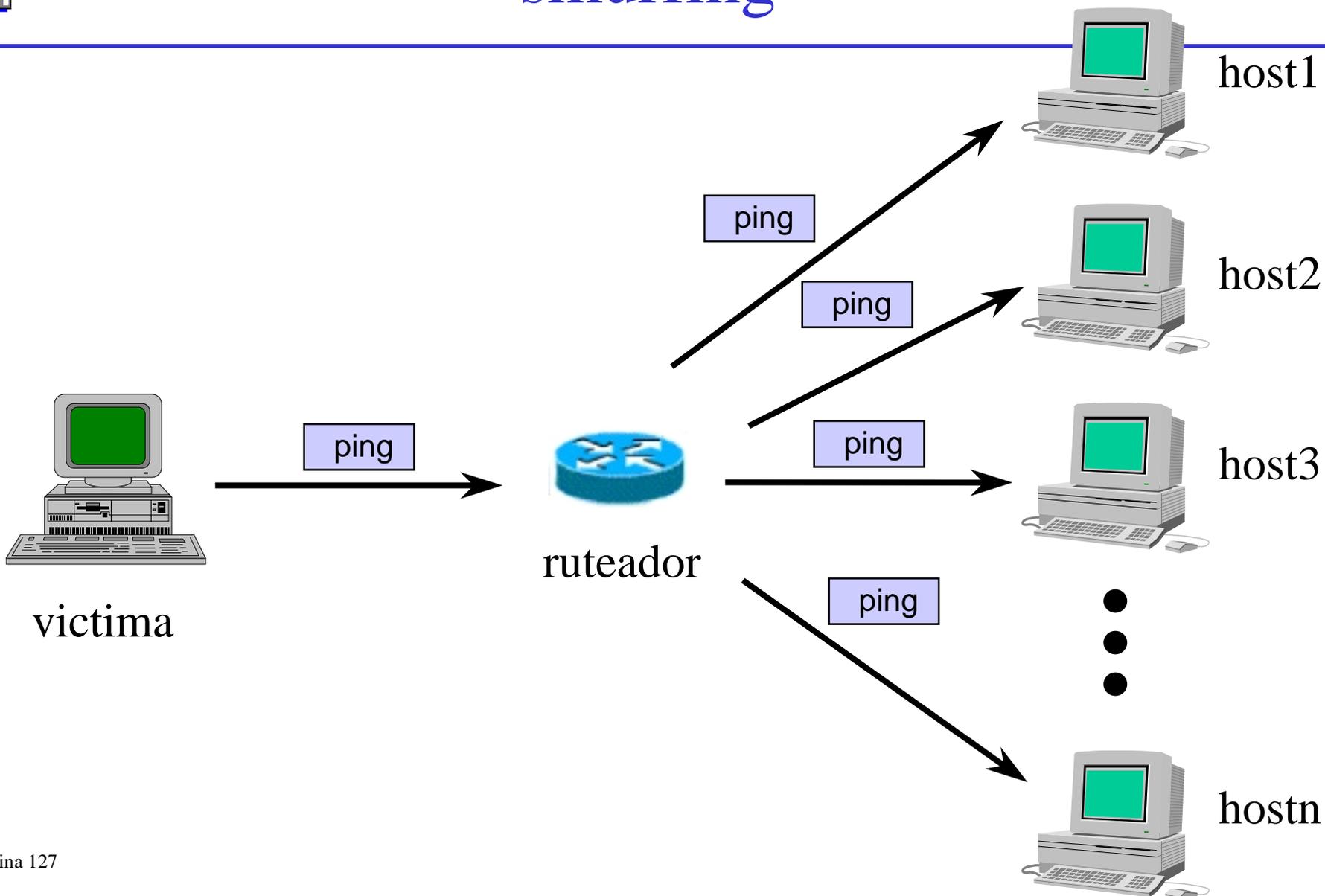


# Smurfing

- Ataque que afecta, principalmente, a la disponibilidad de los equipos.
- Se lleva a cabo principalmente en ruteadores Cisco y probablemente en otras marcas.
- Consiste en pedir una respuesta a varias máquinas y haciendo pasar por otra computadora.
  - de esta forma todas las respuestas llegaran a la víctima

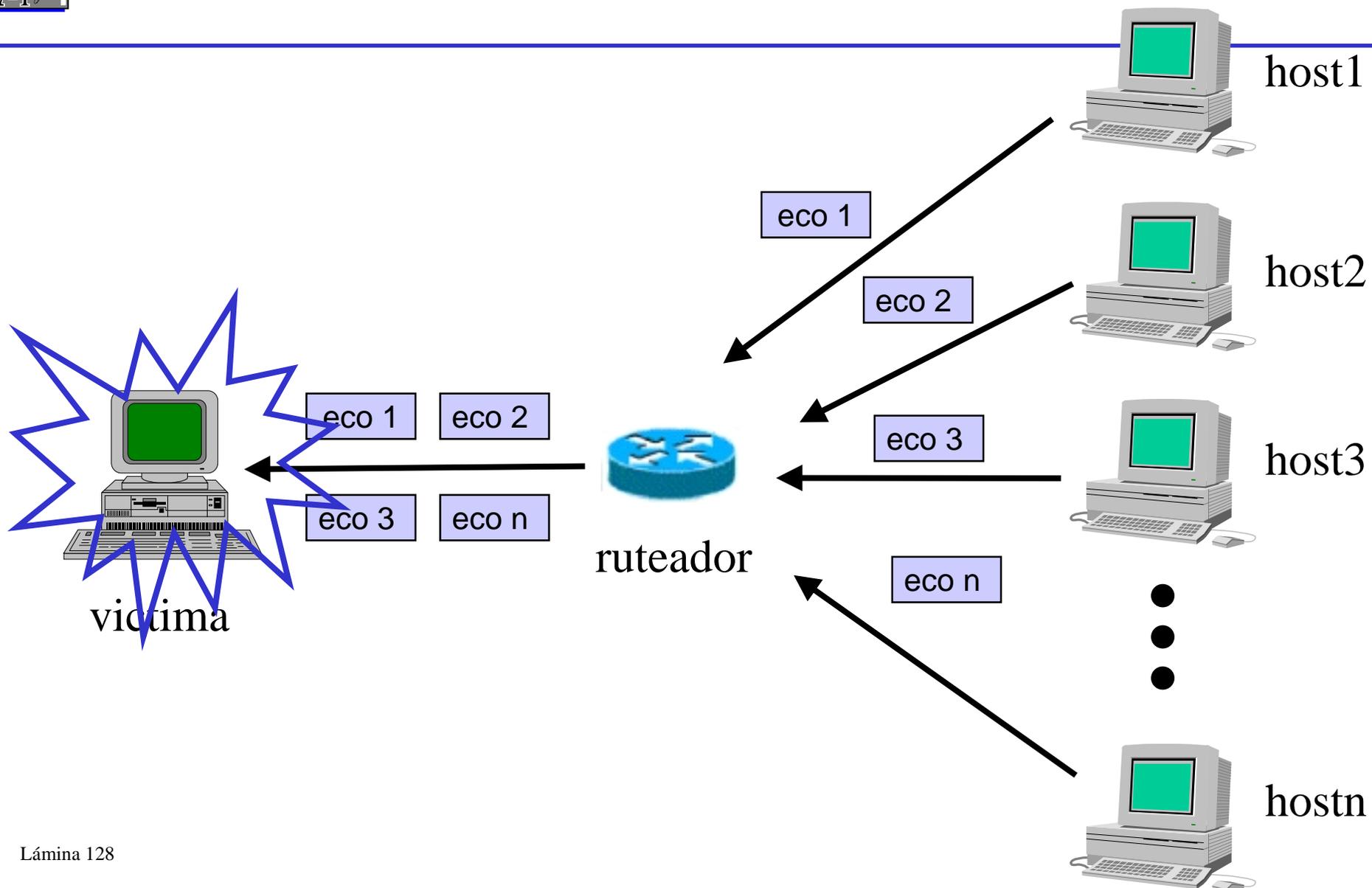


# Ejemplo negación servicio: smurfing





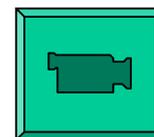
# El smurfing





# 1er ejemplo spoofing: ataque ARP

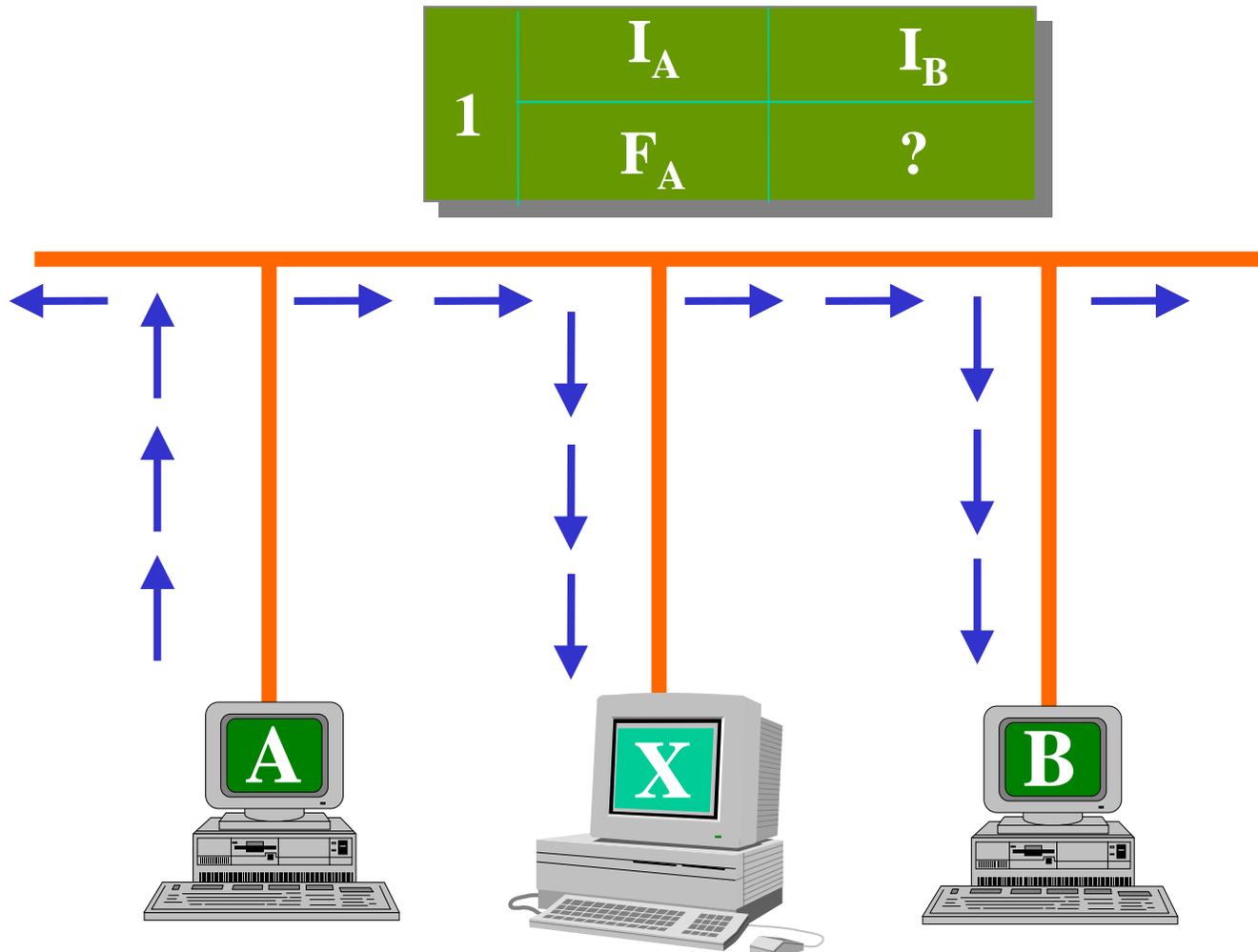
- Consiste en hacerse pasar por una persona que no se es.
- Aprovecha el principio de funcionamiento del protocolo ARP.
- Sólo es útil es redes/máquinas que utilizan este protocolo (locales).





# Protocolo ARP

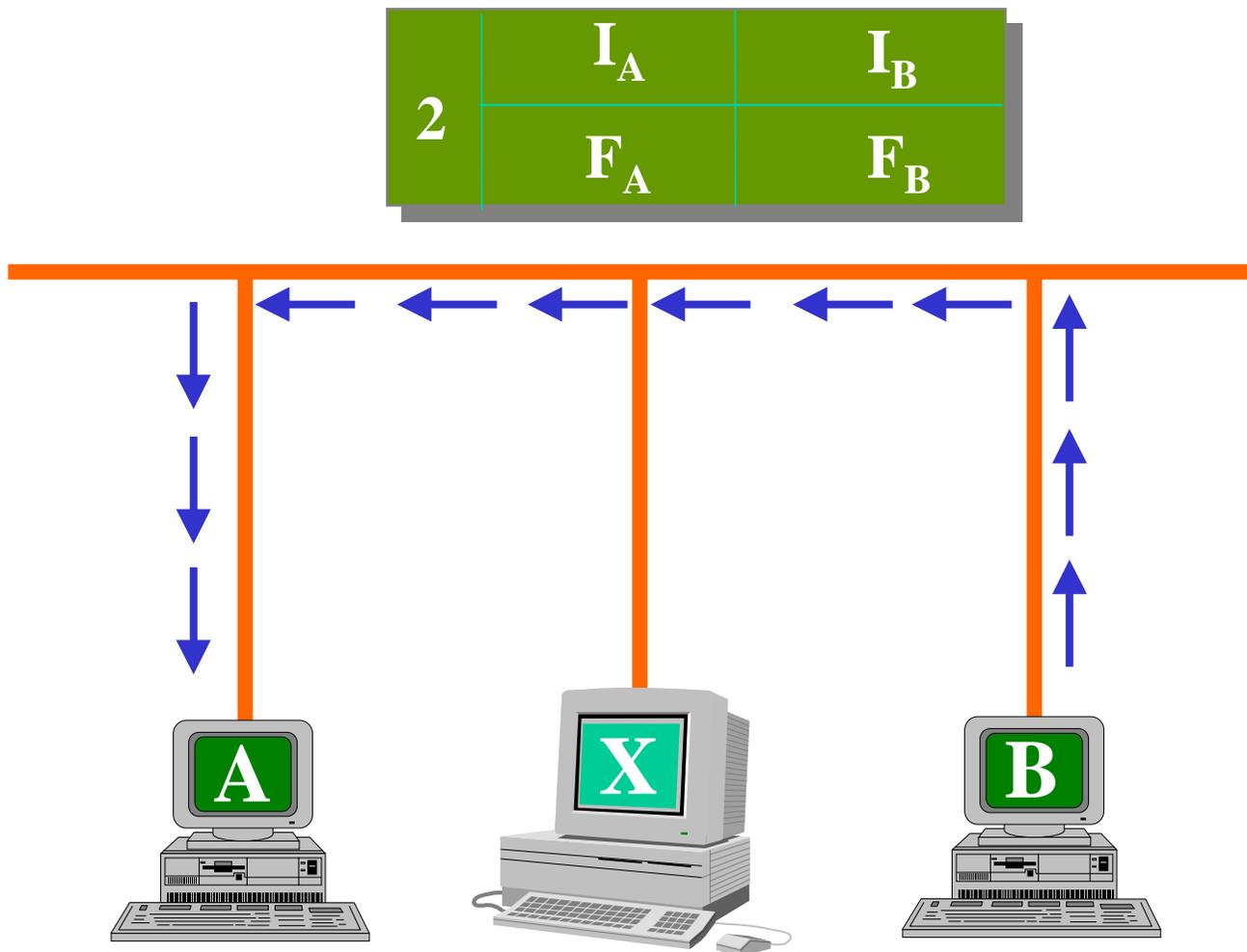
(funcionamiento normal)





# Protocolo ARP

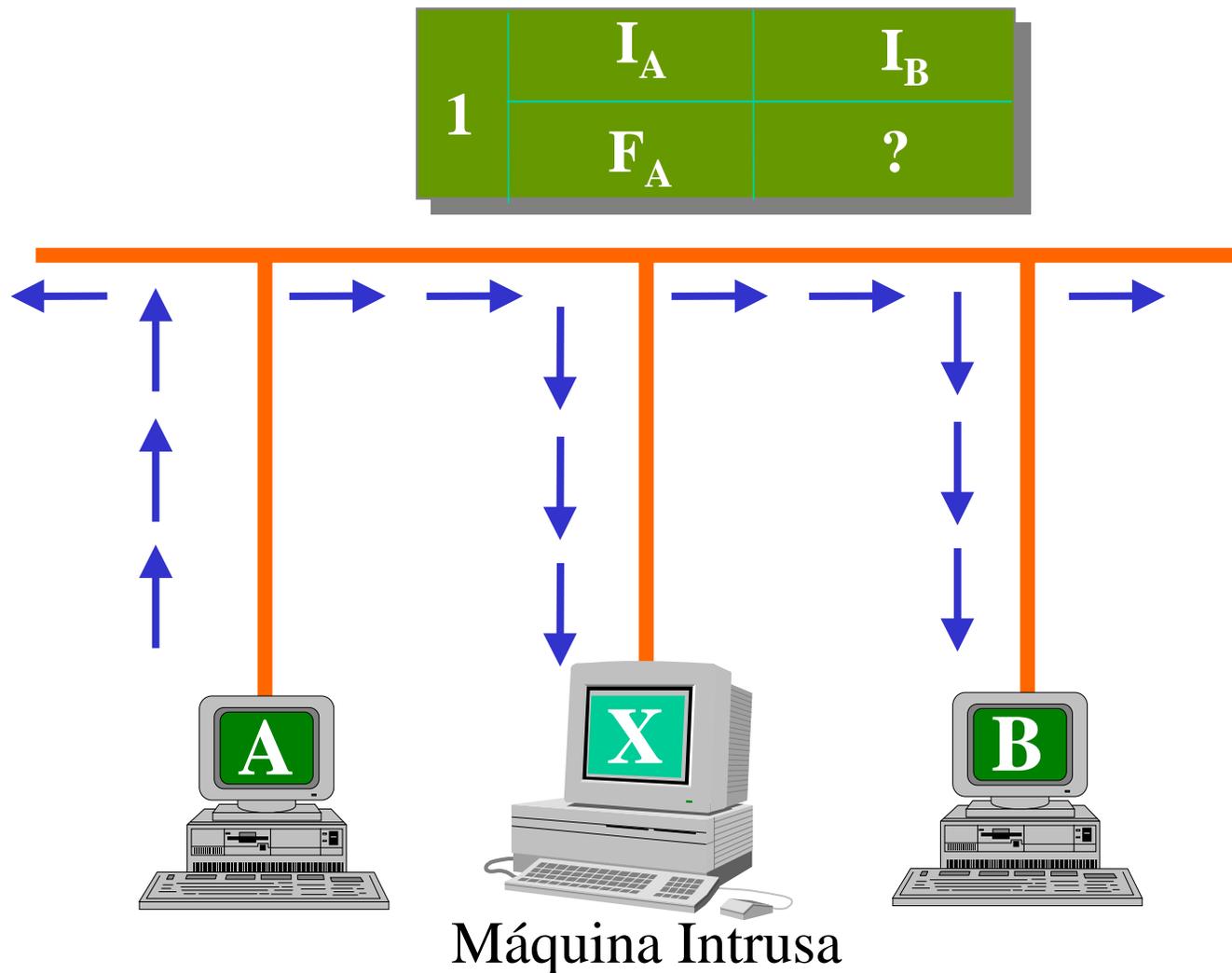
(funcionamiento normal)





# Ataque ARP

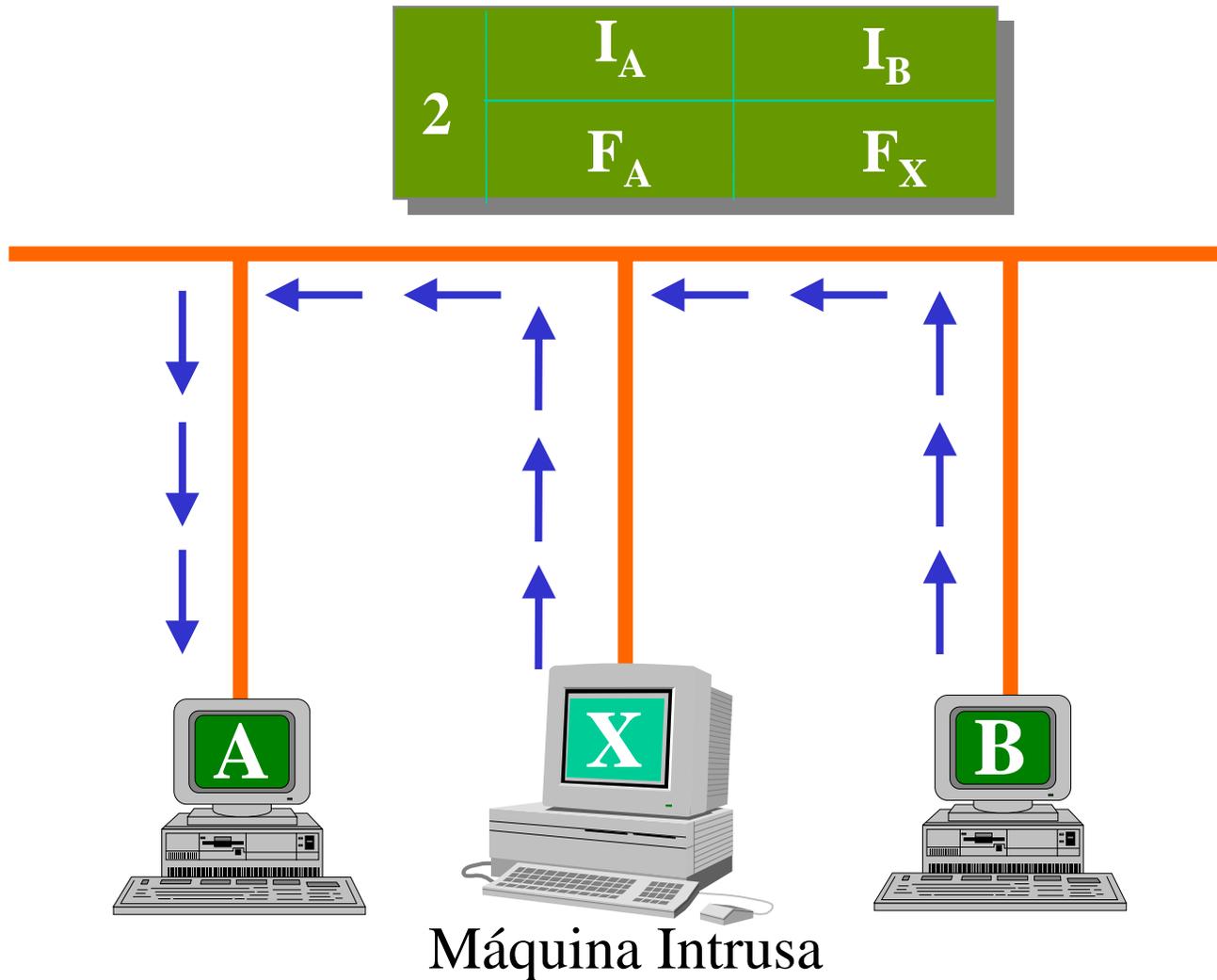
(máquina A solicita dirección de B)





# Ataque ARP

(máquina X responde con su dirección)





# Las tablas ARP de las máquinas

A

Tabla ARP

$I_B$	$F_x$
-------	-------

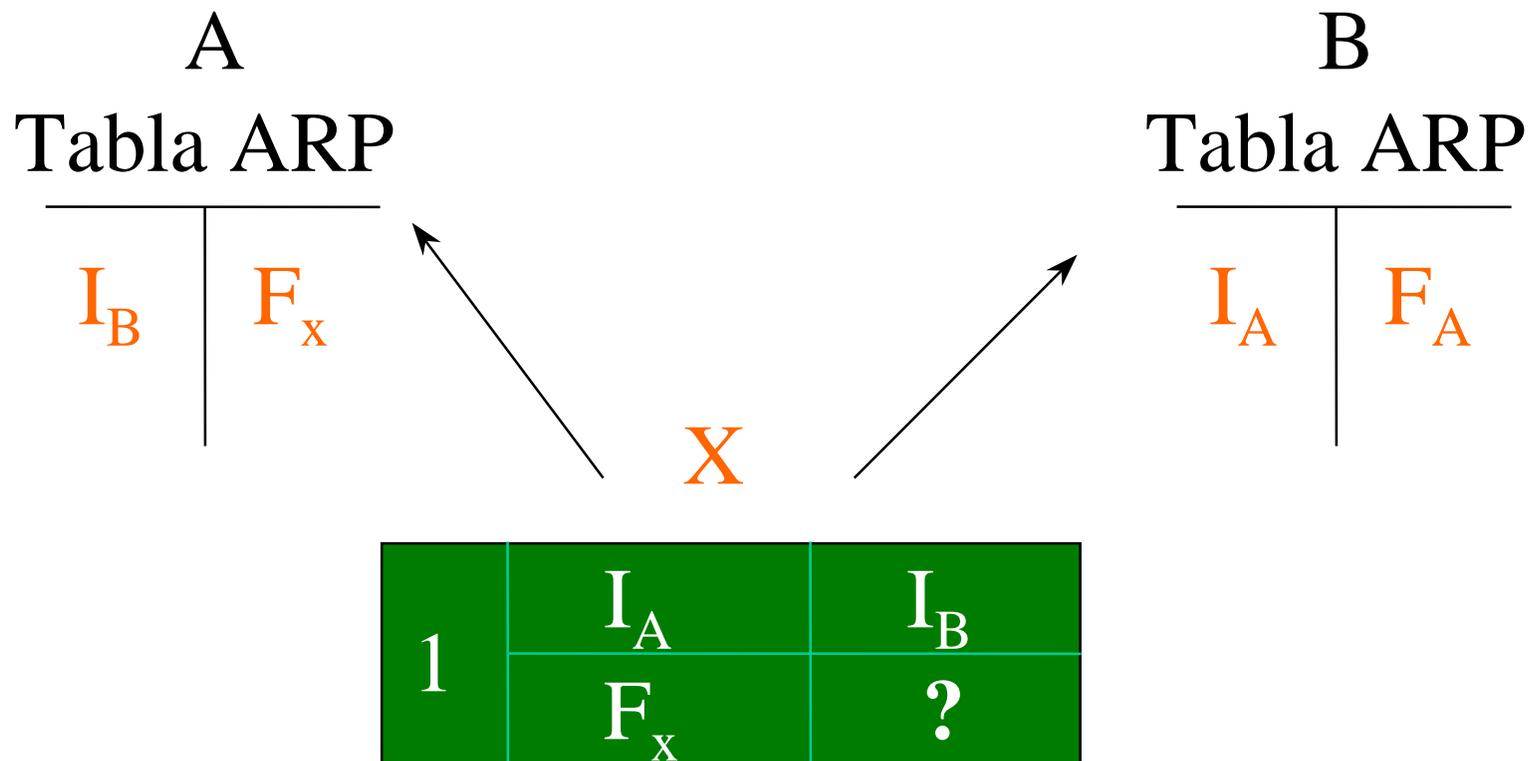
B

Tabla ARP

$I_A$	$F_A$
-------	-------



# Para completar el ataque (x notifica a B que el es A)





# Para completar el ataque (B actualiza su tabla)

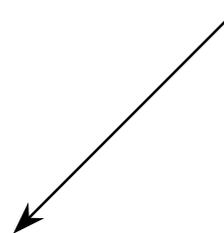
A  
Tabla ARP

$I_B$	$F_x$
-------	-------

B  
Tabla ARP

<del><math>I_A</math></del>	<del><math>F_A</math></del>
$I_A$	$F_x$

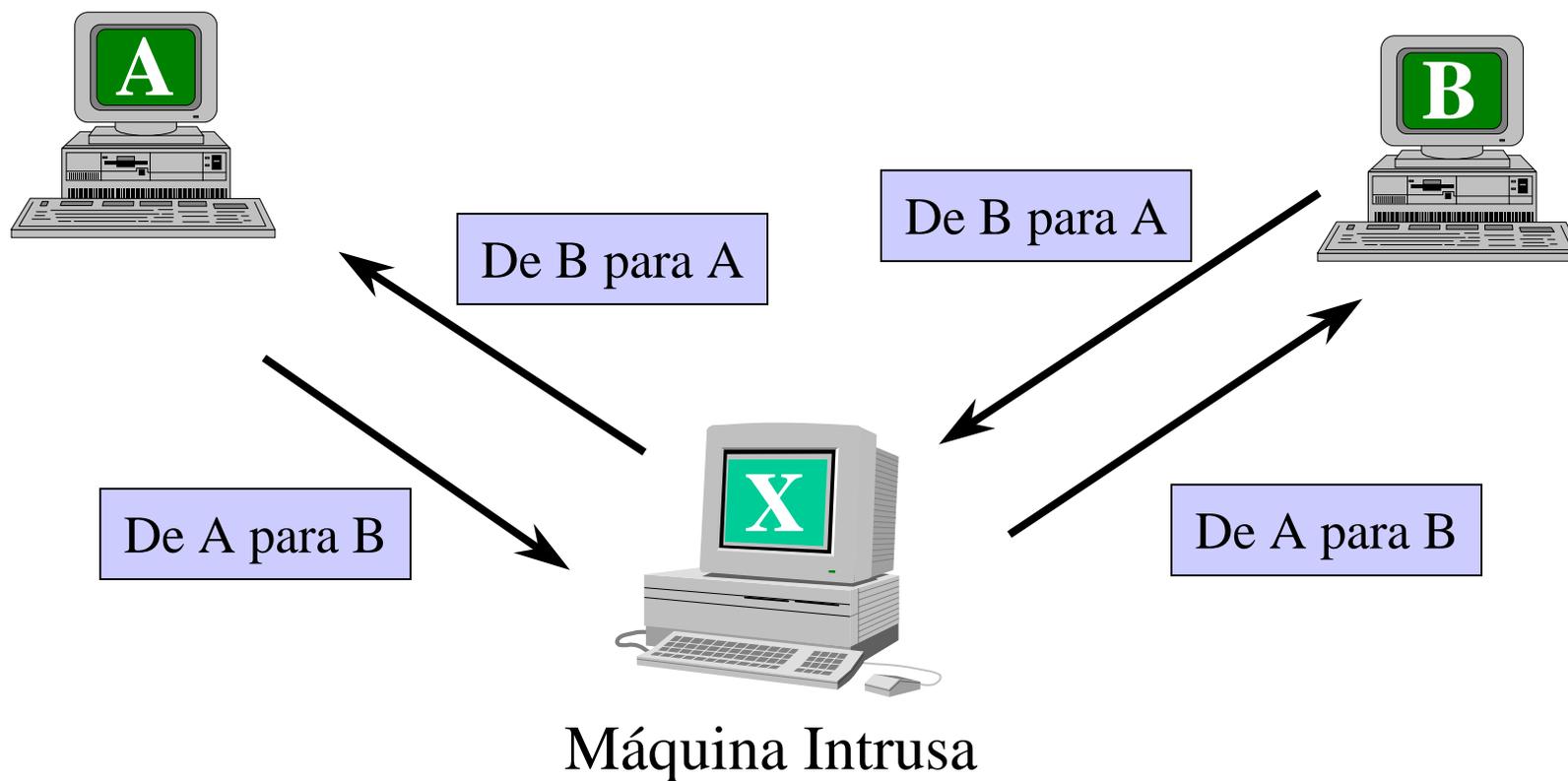
X



2	$I_A$	$I_B$
	$F_x$	$F_B$



# Finalmente





# Protocolo ICMP

## (Internet Control Message Protocol)

- Permite a ruteadores y servidores reportar errores o información de control sobre la red.
- Reporta errores como:
  - Expiración del TTL
  - Congestión
  - Dirección IP destino no alcanzable, etc.
- Viaja encapsulado en el área de datos de un datagrama IP.



# Mensajes ICMP más comunes

Tipo	Descripción
0	Echo reply
3	Destination Unreachable
4	Source Quench
5	<b>Redirect (Cambio de Ruta)</b>
8	Echo request
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply



# Mensaje ICMP Cambio de Ruta

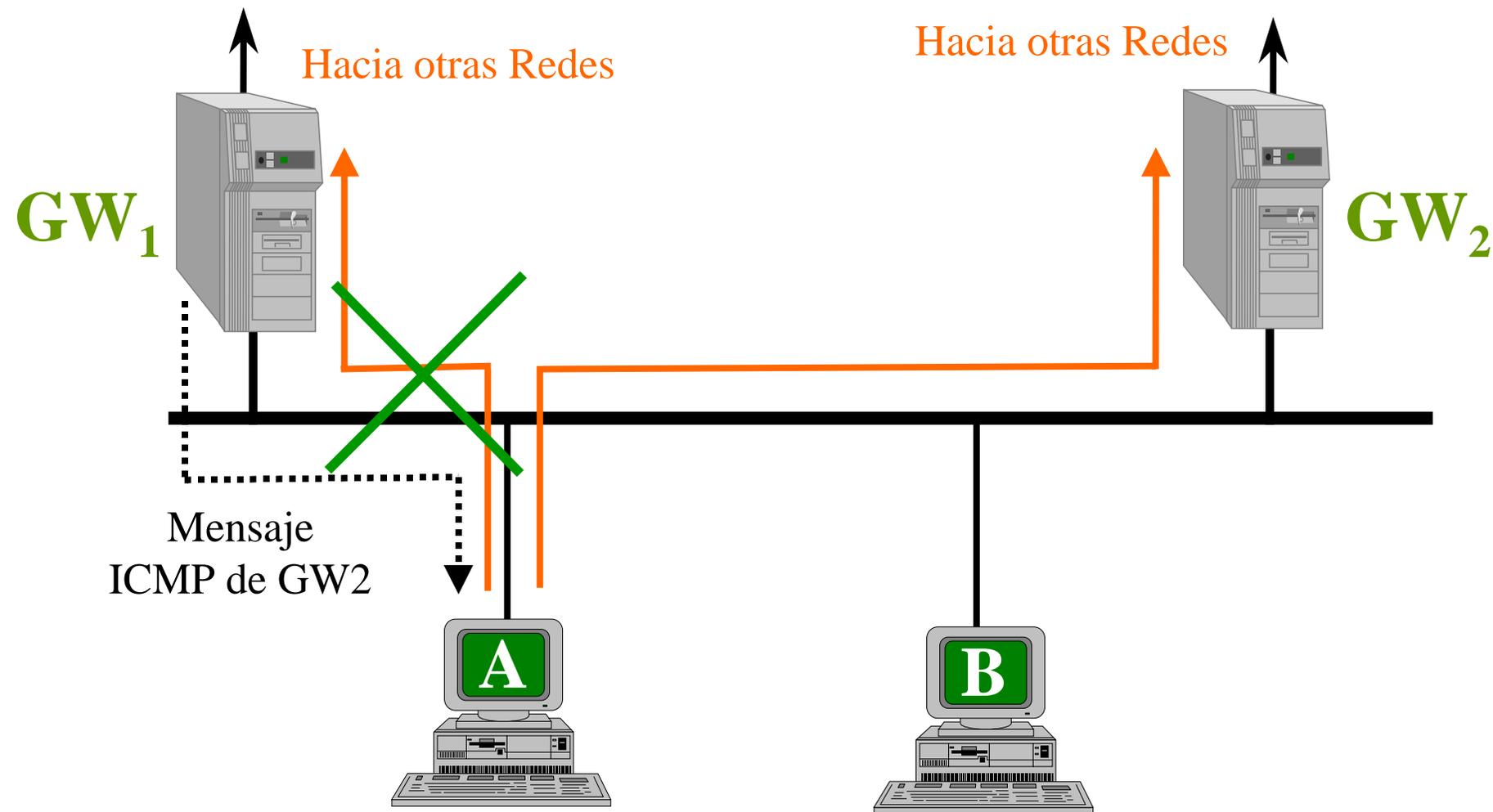
---

Utilizado por un ruteador para indicarle a una máquina en su segmento que utilice una nueva ruta para determinados destinos.



# Mensaje ICMP Cambio de Ruta

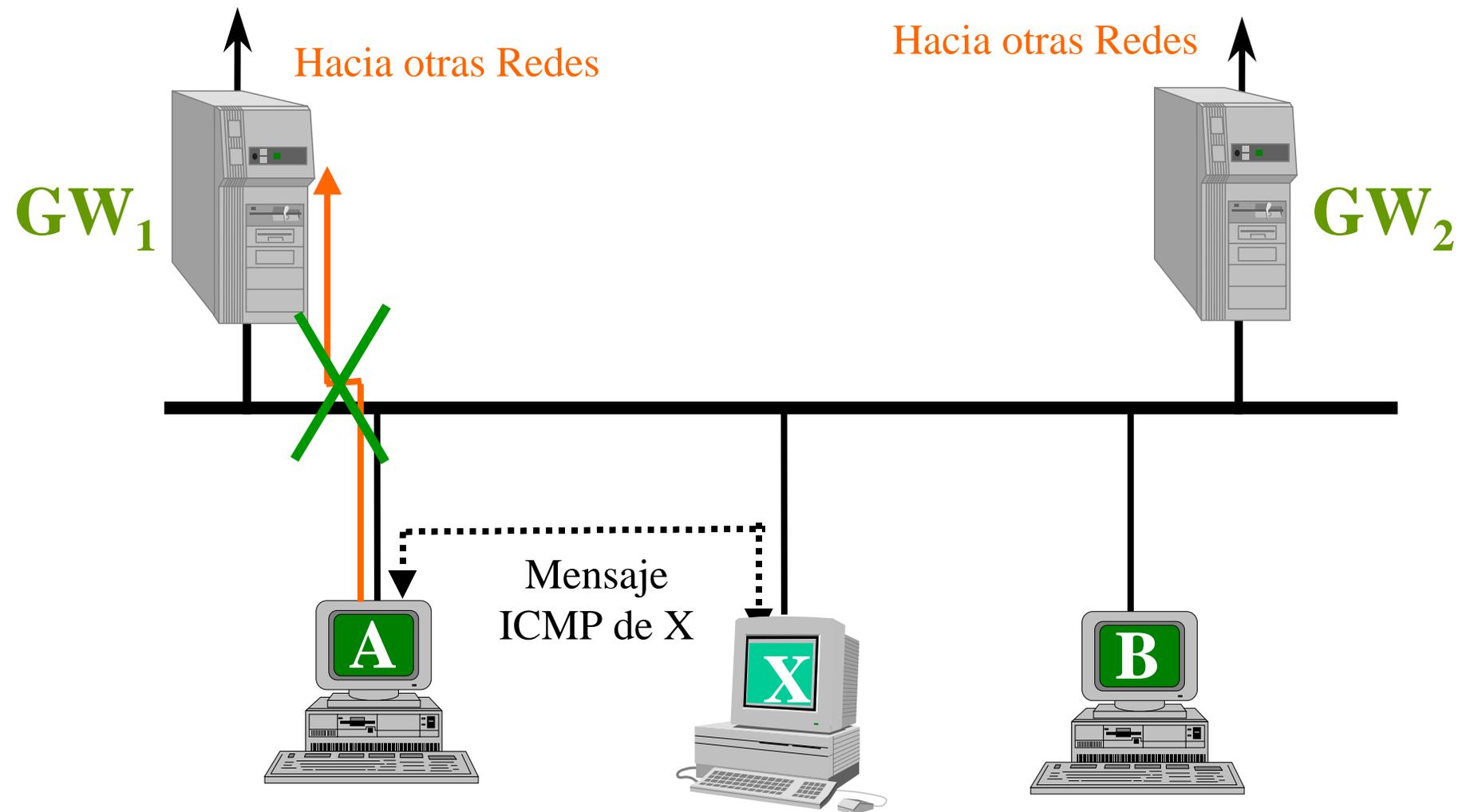
(funcionamiento normal)





# Ataque ICMP

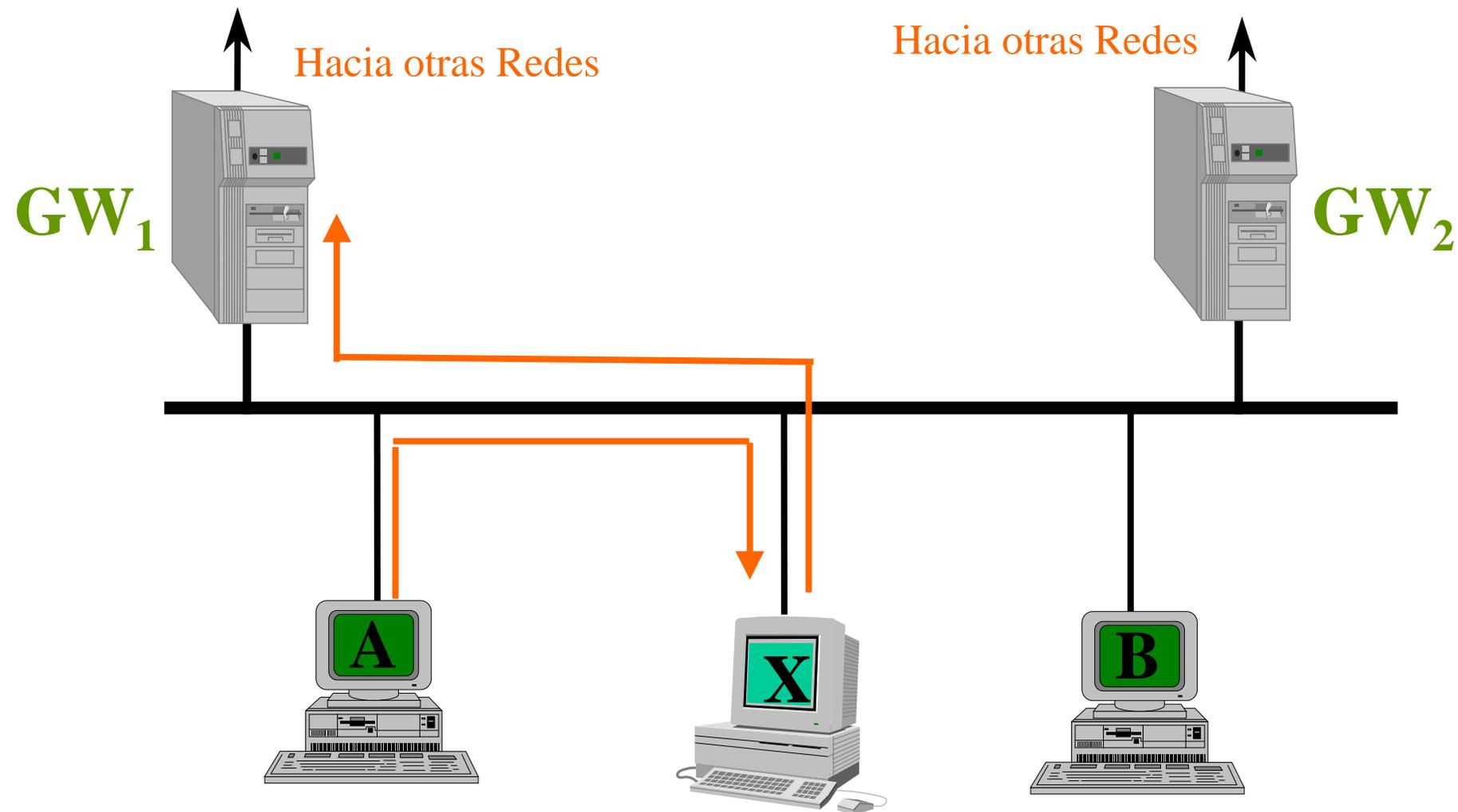
(Mensaje cambio de ruta)





# Ataque ICMP

(Mensaje cambio de ruta)





# TEMPEST

- TEMPEST nombre corto no clasificado que se refiere a la investigación y estudios de emanaciones comprometedoras.
- Basado en la captura de emanaciones electronicas.
  - una vez atrapadas y analizadas se pueden recrear sesiones de trabajo



# Pseudo flaw and Interrupts

- Este tipo de ataque se basa en las debilidades que existen en los sistemas operativos así como los diferentes programas que son usados en ellos.
- La diferencia entre las pseudo fallas y las interrupciones está en que las primeras son debilidades o agujeros de seguridad que existen en los programas y se deben a fallas de programación que permiten explotar una serie de entradas desconocidas para los usuarios comunes pero no para los hackers.



# Pseudo flaw and Interrupts

- Las segundas, las interrupciones, representan problemas de programación pero a un nivel diferente, donde, es posible hacer que un programa termine su ejecución de forma anormal y así dejando al hacker en posibilidad de ejecutar otros programas con autoridad de administrador o root.
- La única forma de preveer este tipo de ataques es aplicando todos los parches de seguridad que los creadores de los sistemas operativos y programas ponen a disposición de la gente.



# Browsing and Inference

- ***Browsing***: el acto de buscar en una entidad de almacenamiento para ubicar o adquirir información sin necesariamente conocer la existencia o el formato de la información que se busca.
- ***Inference***: ataque que consiste en unir fragmentos de de información accesible para obtener información que se supone secreta. Dicho descubrimiento de información depende del conocimiento suplementario que el atacante tenga.



# Cramming

- Nombre que se otorga a un tipo de incidente que proviene de las personas conocidas como PHREAKERS, que son los hackers del mundo telefonico.
- Un PHREAKER puede realizar llamadas de larga distancia gratis y demas situaciones, sin que sean cargadas a su numero telefonico,
- Esos cargos deben de ser destinados a alguien ya que los sistemas contables de las compañías telefónicas no son burladas, solo dirigidos a un lugar incorrecto.



# Cramming

- Este cierto lugar incorrecto puede ser el recibo o telefónico de alguien que no sospecha nada y que no sabe de la existencia de PHREAKERS.
- Cuando este pobre incauto ve su recibo telefonico y ve los cargos, se dice que lo que le hicieron fue un CRAMMING.



# Time of check/Time of use (TOC/TOU)

- Ataque asíncrono que consiste en cambiar alguna información de control o el contenido de un archivo en el momento en que las funciones de seguridad de un sistema revisa el contenido de variables (o los permisos de acceso a archivos), y el momento en que las variables son utilizadas.



# Cliente/Servidor

- Java
- Active X
- Los applets
- Browsers y URLs
- Plugins
- Las cookies
- Los CGI



# Java

- Lenguaje de programación desarrollado por Sun Microsystems.
- Independiente de plataforma.
- Es más ampliamente empleado para desarrollo de páginas WEB.
- Principal elemento seguridad: Javabox y Security Manager.
- Lugar “ virtual “ donde un applet de Java puede ejecutarse pero no salirse de él.



# Disponibilidad y Java

- Java puede crear ciclos recursivos
- Con dichos ciclos se pueden agotar los recursos de un sistema y de esta forma, evitar que otros procesos que se encuentran ejecutándose puedan continuar con sus procesos normales ya que no tendrán recursos para hacerlo.
- Un caso común para esto son los scripts de Java que crean ventanas chicas que se duplican rápidamente hasta agotar los recursos de cualquier sistema no importando la plataforma operativa.



# Ataques incómodos

- Son los más comunes
- Utilizan Java para realizar programas que bajen imágenes y sonido de Internet durante un determinado tiempo.
  - desgraciadamente la información que se baja de Internet no puede ser monitoreada
  - por esto mismo, es posible bajar información no apta o sensible para algunas personas sin que ellas lo hayan solicitado.



# Active X

- ActiveX, tecnología desarrollada por Microsoft.
- Básicamente usados para distribución de SW por Internet.
- Se presenta como ícono en Páginas WEB, restringido al ambiente Microsoft.
- Se distribuyen como archivos ejecutables (ActiveX control ).
- Toman el control del disco duro.
- Deben traer una firma de quien lo creo a través de “Autenticode”.



# Los applets

- Programa diseñado para ser ejecutado dentro de otra aplicación.
- Los applets no pueden ser ejecutados directamente por el sistema operativo.
- Un applet bien diseñado puede ser invocado desde diferentes aplicaciones.
- Web browsers puede interpretar applets de Web servers.
- Debido a su tamaño son ideales para aplicaciones pequeñas de Internet.



## ¿Qué pueden llegar a hacer?

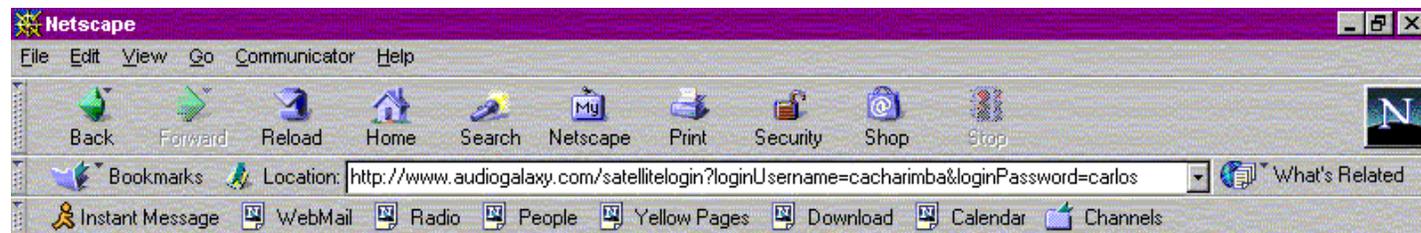
- Pueden leer o escribir en el sistema de archivos del cliente.
- Pueden realizar conexiones a red del host original.
- Pueden iniciar programas en el cliente.
- Pueden realizar llamadas a métodos definidos en el cliente.
- Recomendación: configuración del browser



# URLs



- Dirección de Web ( Uniform Resource Locator ).
- No solamente apunta a direcciones análogas a archivos en cualquier máquina dentro de la red, sino que puede referenciar a queries, documentos almacenados en bases de datos, e inclusive comandos ejecutables.
- Para el año 2001 se estima que habrá más de 15 millones de URL´s dando servicio en Internet.





# Ataques con Robots

- Este tipo de ataques se deriva del uso de “robots inteligentes” que se encargan de navegar Internet en busca de información y realizando acciones específicas
- Por ejemplo, dentro de un grupo de servidores de noticias, un robot puede buscar información que alguien solicita



# Las cookies

- Es información que un sitio Web escribe en el disco duro, de tal forma que pueda recordar algo acerca del usuario tiempo después.
- Tecnicamente:
  - información para uso futuro almacenada por el servidor en el cliente
- Su ubicación depende del browser.
- Permite al servidor almacenar información acerca del usuario en su propia máquina.
- Principal problema: privacidad



# Los plugins

- Distribución de SW por Internet
- Plug-ins desarrollados por terceros diferentes a los creadores de los browsers, que toman el control de la máquina
- Ofrecen soporte de nuevos formatos de archivos y aplicaciones
- Afectan configuraciones de otros productos ya instalados.



# Los CGI's

- Un cliente remoto pueda ejecutar comandos o instrucciones del sistema sin que el servidor pueda hacer nada para evitarlo, entre otras actividades :
  - Leer, remplazar, modificar o borrar archivos
  - Enviar archivos de regreso vía Internet
  - Ejecutar programas bajándolos en el servidor, tales como sniffers de passwords, o programas que permitan accesos remotos como Telnet
  - Enviar ataques que originen negación de servicios, etc



# Ataques criptográficos

- Ciphertext only Attack
  - el atacante solo tiene conocimiento del texto encriptado y a partir de él trata de encontrar la llave secreta con la que se encriptó dicho texto
  - criptosistemas vulnerables a este tipo de ataques son absolutamente inseguros
  - ejemplos son los ataques a criptosistemas clásicos mediante análisis estadístico de frecuencias de los símbolos



# Ataques criptográficos

- Chosen plaintext Attack
  - el atacante puede elegir un texto en claro y obtener su correspondiente criptograma
  - una forma de obtener el par texto claro/criptograma es insertar elementos en un base de datos, y después observar los cambios en el criptograma almacenado
- Kown-Plaintext Attack
  - criptoanalista conocer algunos pares texto-claro/criptogramas
  - si el criptograma representa un programa, se puede esperar que se repitan palabras como begin, end, do, while, etc



# Ataques criptográficos

- Chosen-Ciphertext Attack
  - el atacante elige un criptograma y obtiene el correspondiente texto en claro, es decir, el atacante tiene acceso al criptosistema, pero no a la llave
  - con sistemas de llave pública, el inverso del ataque de chosen-plaintext es factible
  - el analista puede deducir la llave secreta
- Ataque con llave conocida
  - el oponente obtiene algunas llaves utilizadas durante previas encrypciones e intenta determinar nuevas llaves



# Ataques criptográficos

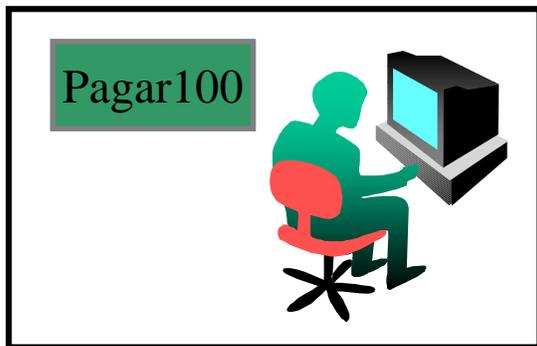
- Reutilización del protocolo
  - el oponente realiza el ataque registrando una de las comunicaciones, o parte de ella, e intenta utilizarla insertándolas en una comunicación posterior



# Solicitando una llave pública

**Alicia**

Alicia va a pagarle  
100 pesos a Beto



“Solicita la Llave  
Pública de Beto”

Entregando llave  
pública de Beto  
Llave=3, 5555

**Beto**

Llave Pública de Beto  
Llave=3, 5555





# El ataque “Man in the Middle” (MIM)

**Alicia**

Alicia va a pagarle  
100 pesos a Beto



“Solicita la Llave  
Pública de Beto”

Llave=3, FFFF

Cambiando  
Llave=3, FFFF por  
Llave=3, 5555



Jorge  
“El Cambiador”

“Solicita la Llave  
Pública de Beto”

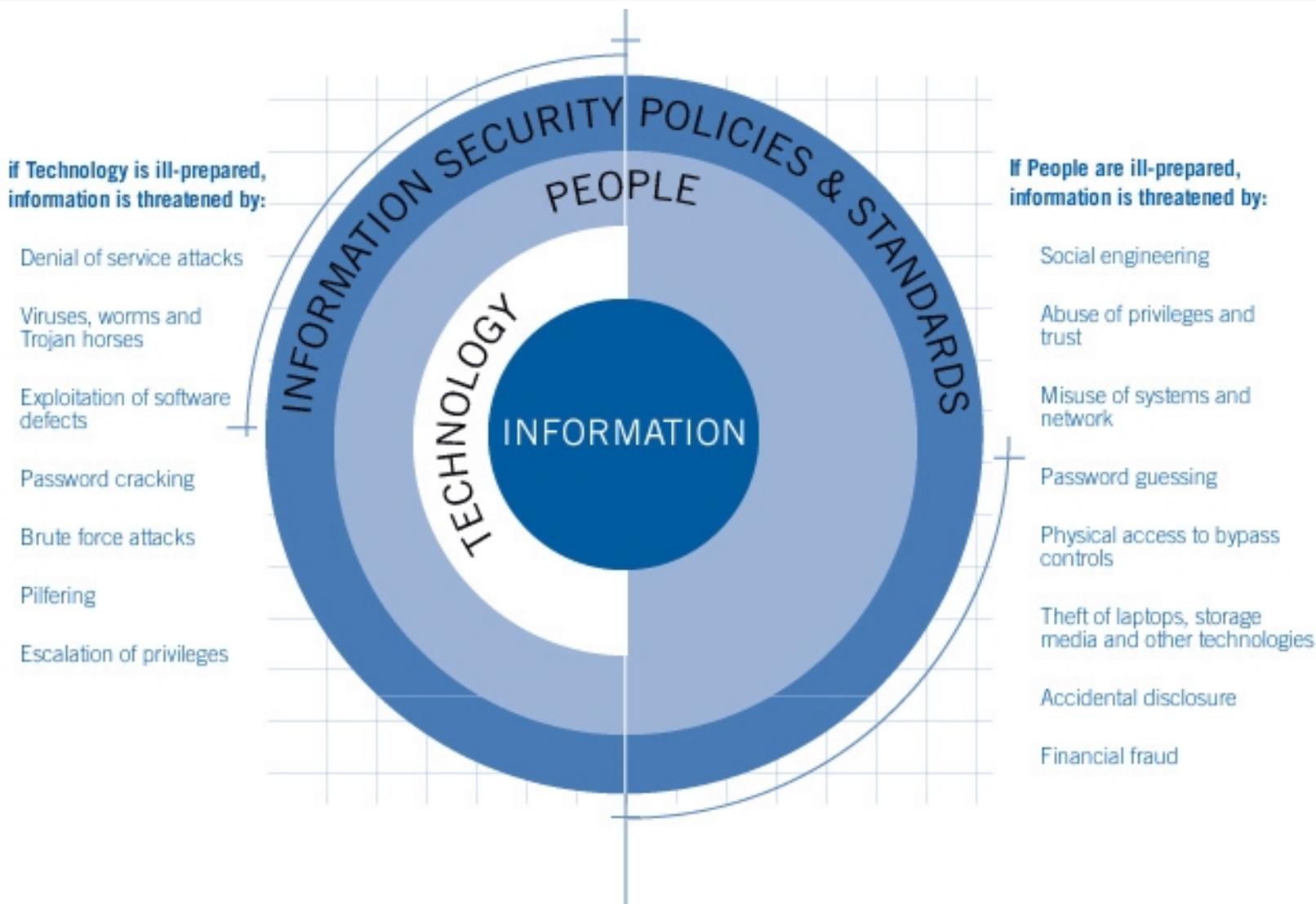
Llave=3, 5555

**Beto**





# ¿Y el factor humano?





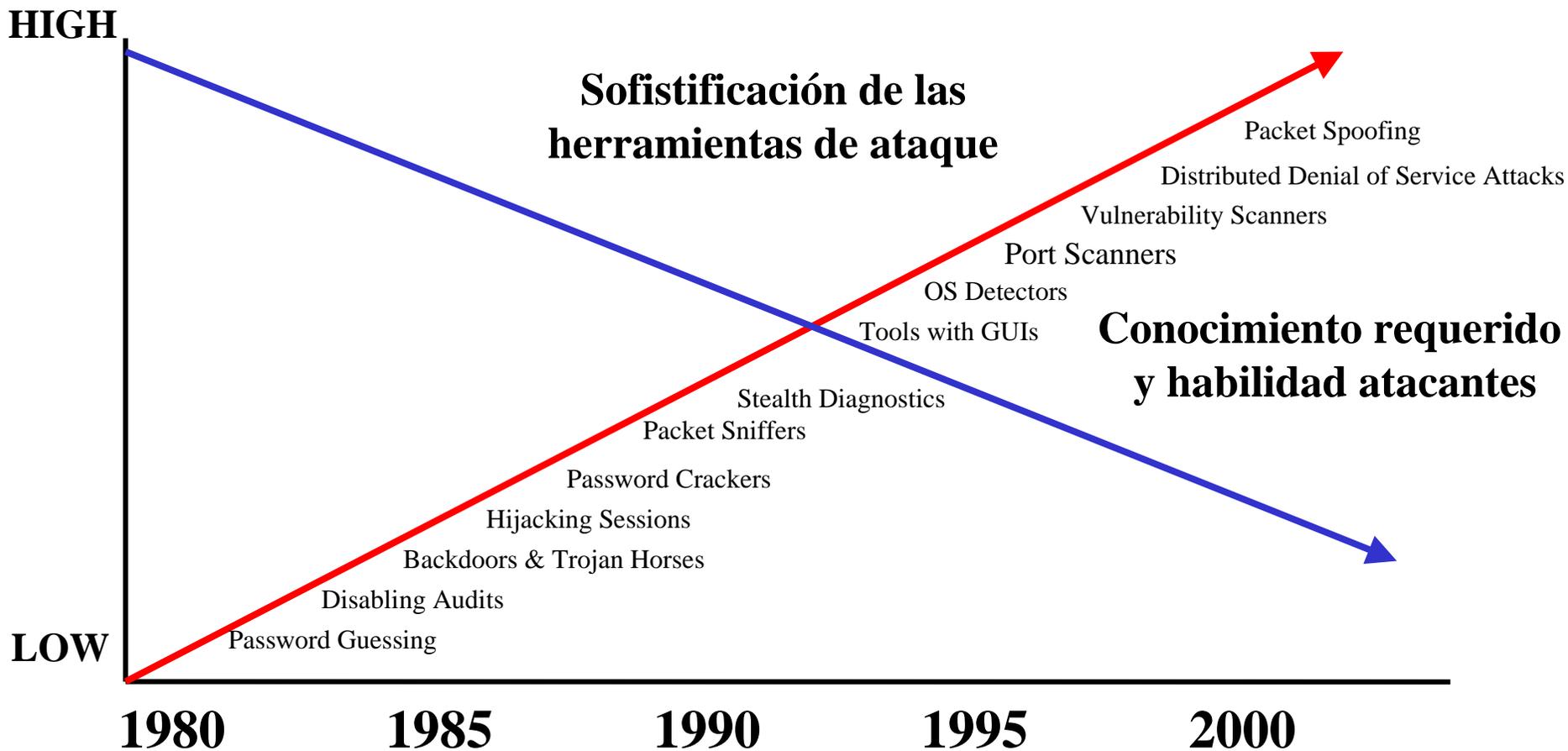
---

# Algunos comentarios ...

## y estadísticas



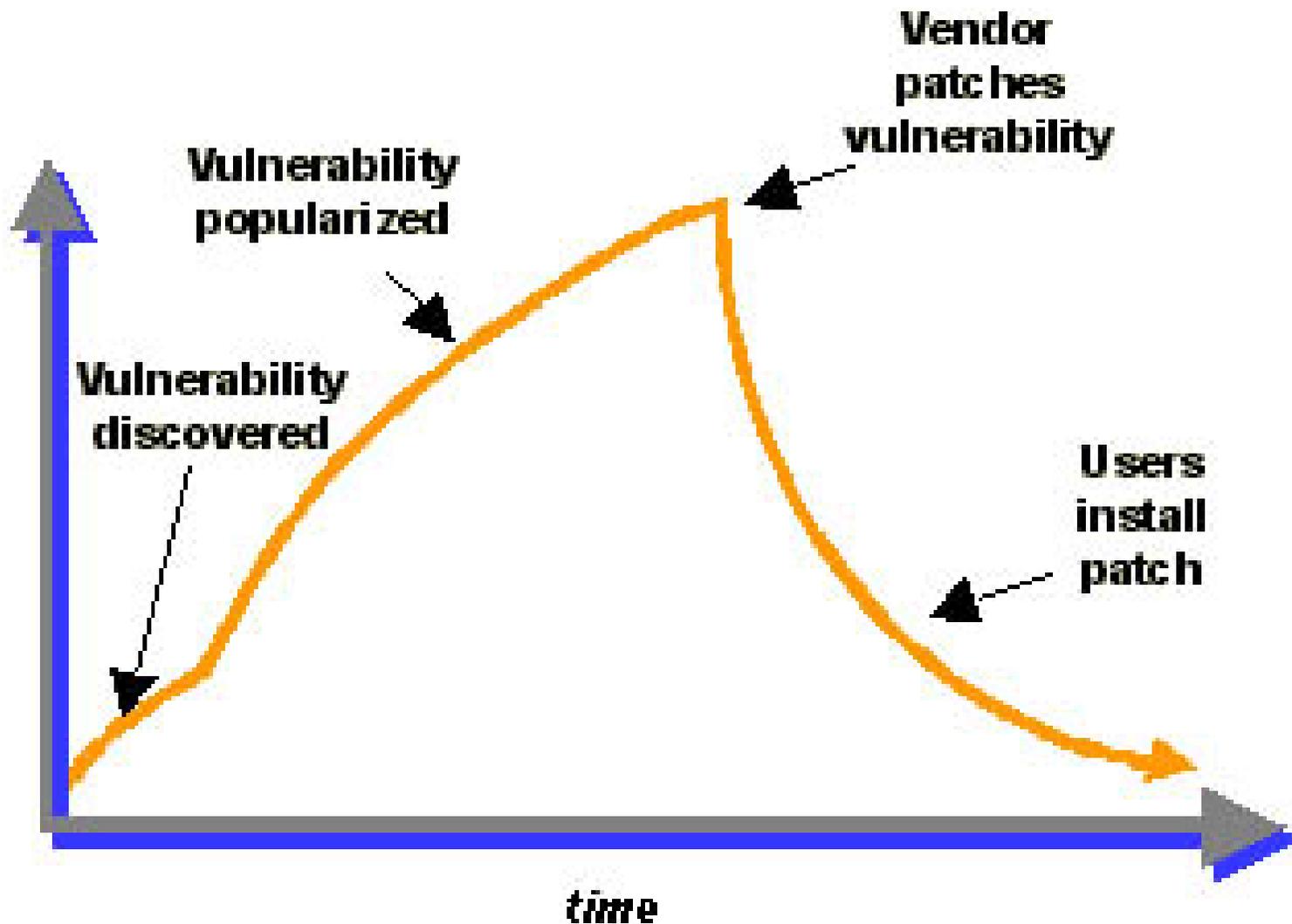
# External Threats: Hacker Tool Explosion



Busqueda reciente en internet de "Hacker Tools" regresan cerca de 2100 hits



# Tiempo vida vulnerabilidad



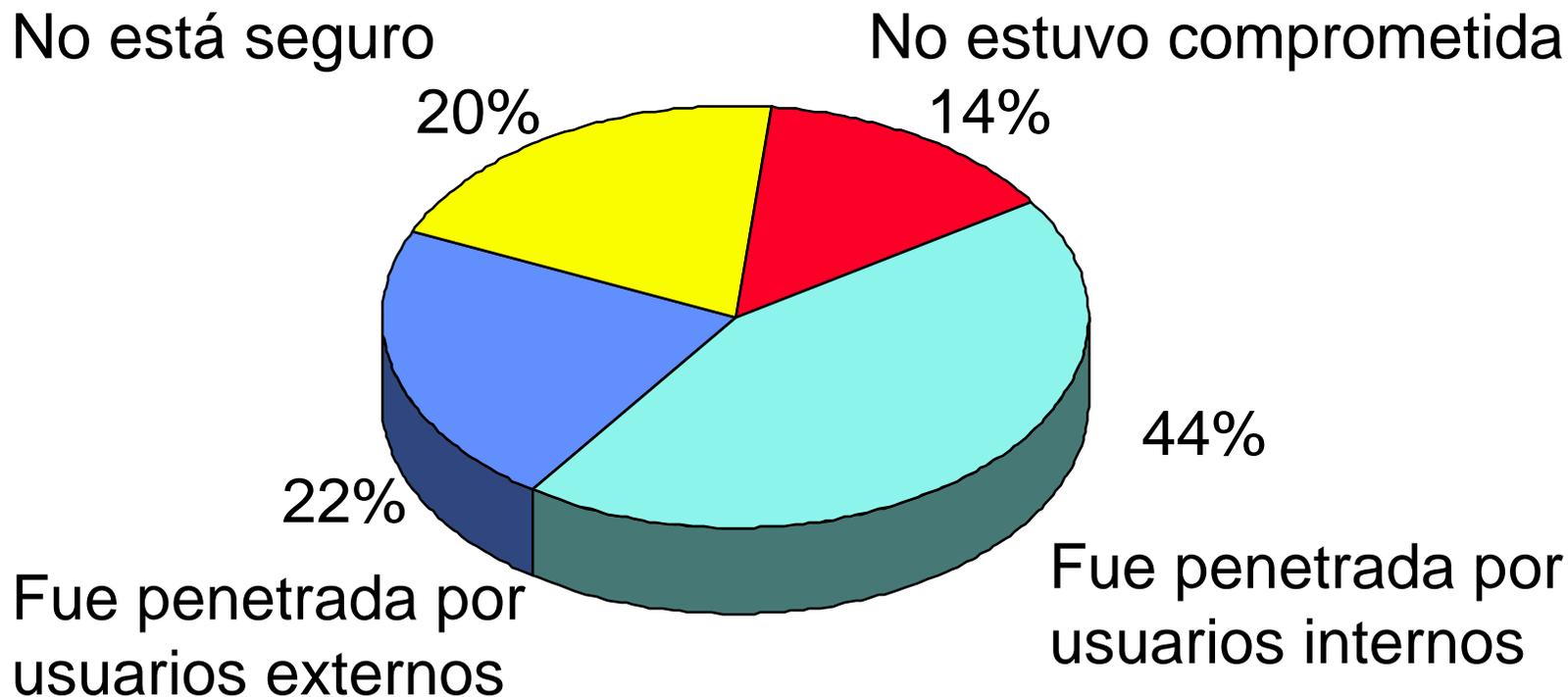


# Publicación vulnerabilidades

- Personas a favor
  - publicar vulnerabilidades para prevenir ataques
  
- Personas en contra
  - otorgar herramientas de posibles ataques a personas que no se informan a tiempo



# Estadísticas





# ¿Quién ataca?

- Crackers.
- Hackers.
- Enemigos.
- Espías.
- Competidores.
- Curiosos.
- Proveedores de software.
- Programadores

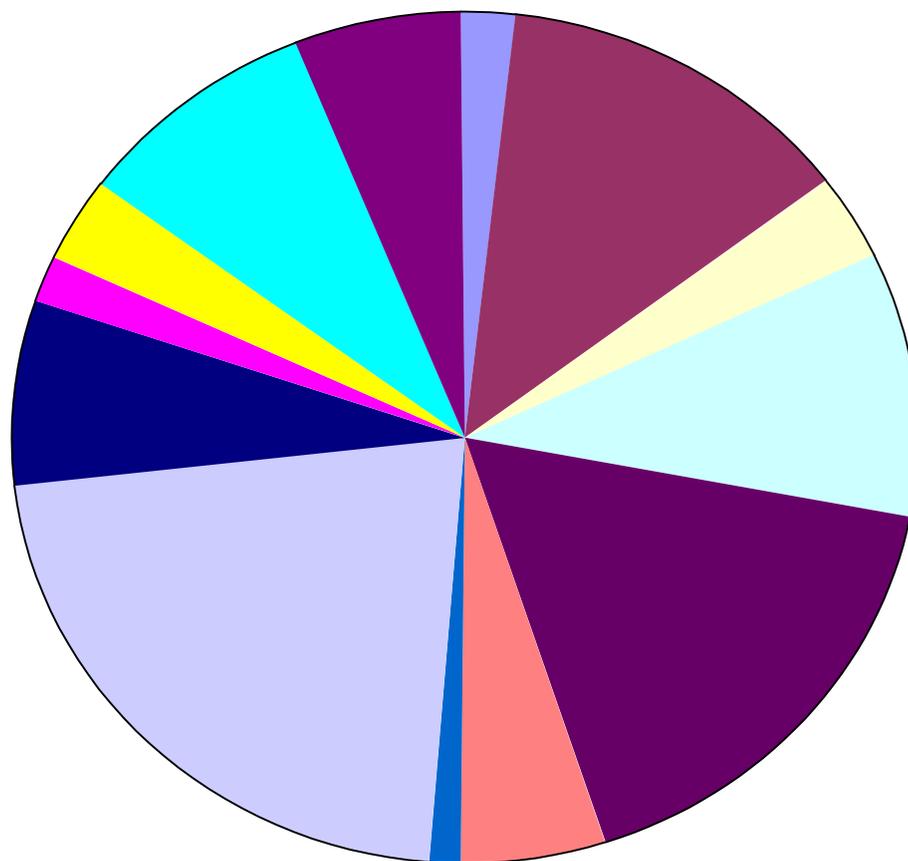
Externos (20%)

Internos (80%)



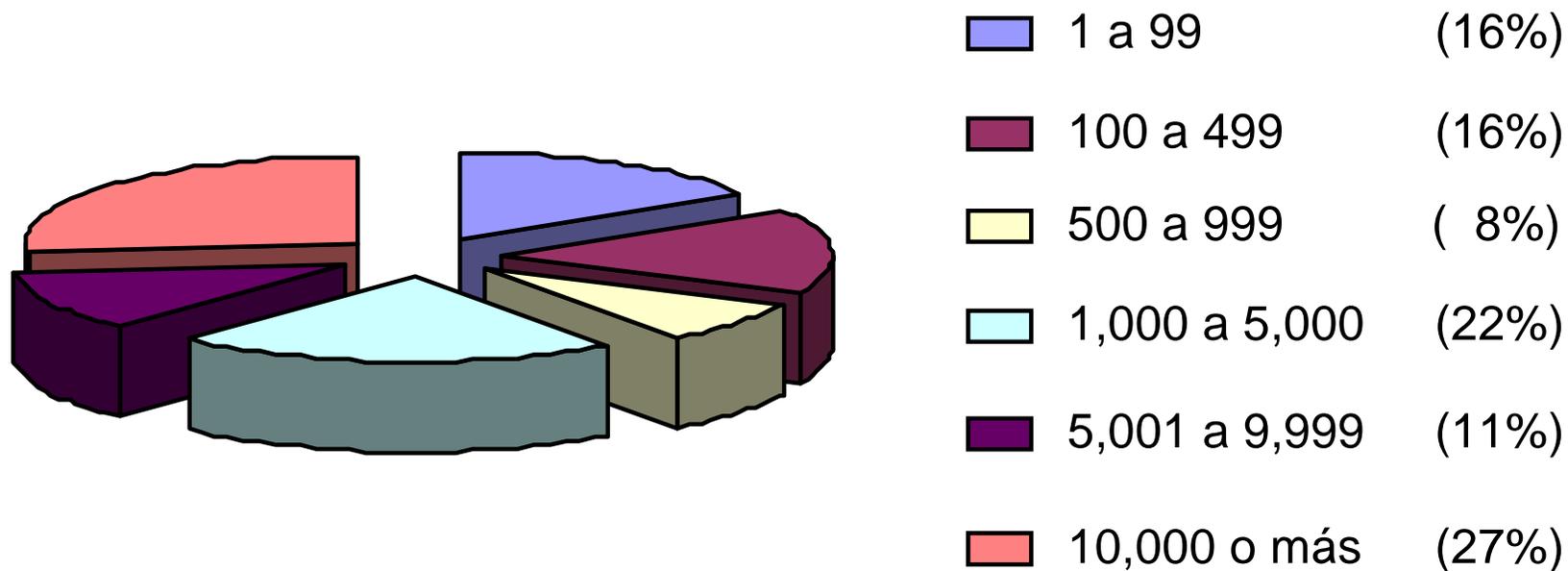
# Respuestas del Sector Industrial

	Gob. Local	(2%)
	Otros	(13%)
	Servicio Público	(3%)
	Manufactura	(10%)
	Financias	(17%)
	Telecomunicaciones	(5%)
	Transporte	(1%)
	Alta Tecnología	(22%)
	Médico	(7%)
	Mercado Minorista	(2%)
	Educación	(3%)
	Gob. Federa	(9%)
	Gob. Estata	(6%)



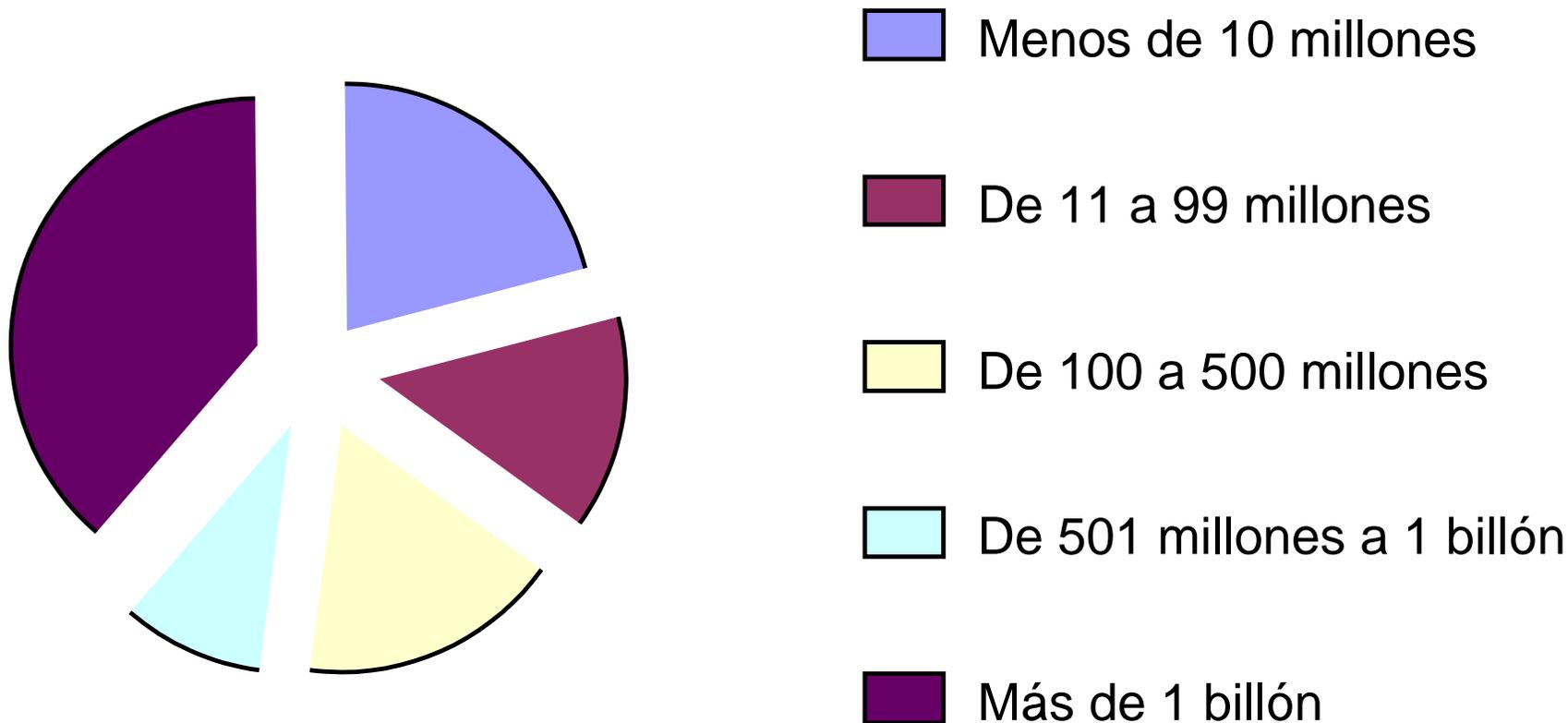


# Respuestas por número empleados



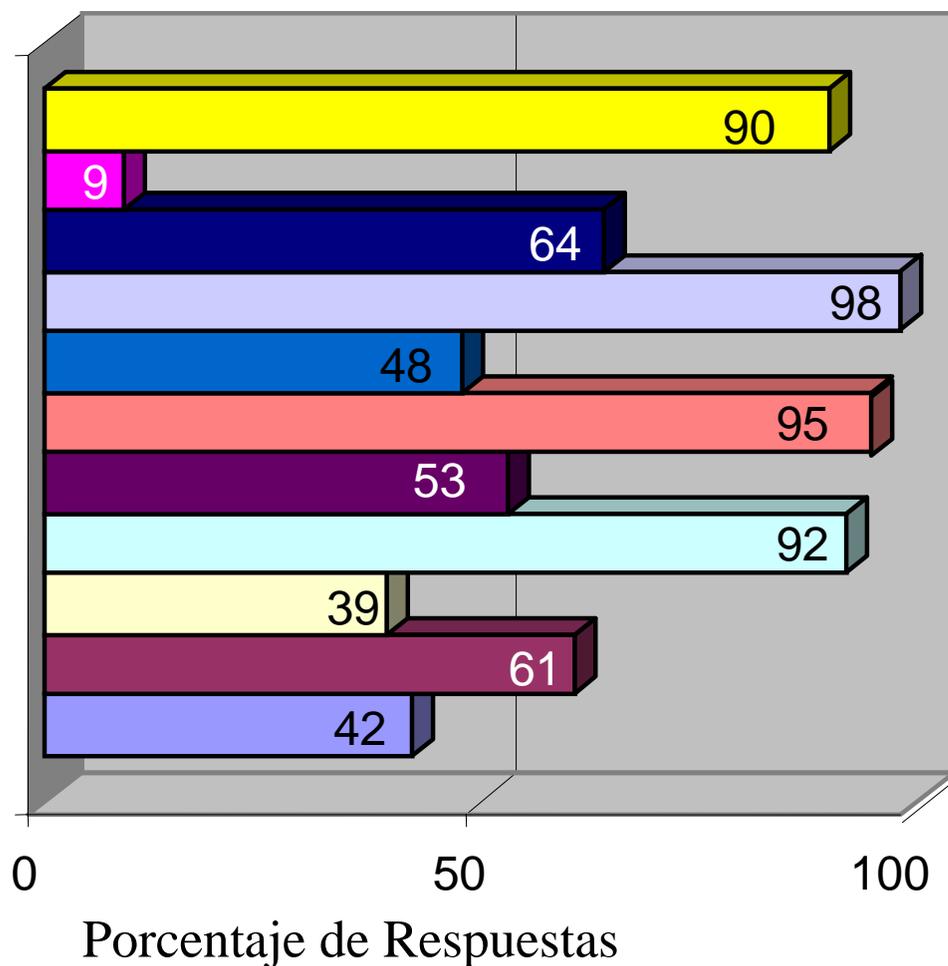


# Respuestas por ingresos





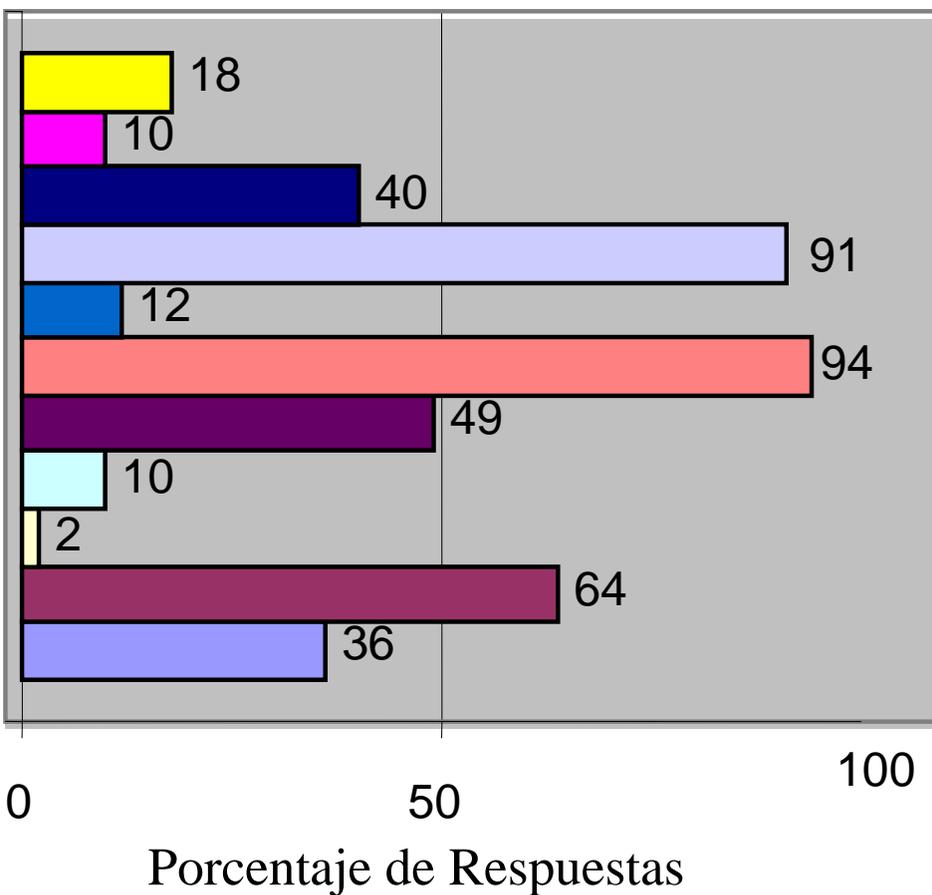
# Tecnologías seguridad usadas



- Control de acceso
- Biometricos
- Archivos encriptados
- Software Anti-virus
- Passwords reusables
- Firewalls
- Login encriptado
- Seguridad Física
- PCMCIA
- Detección de intrusos
- Digital IDS



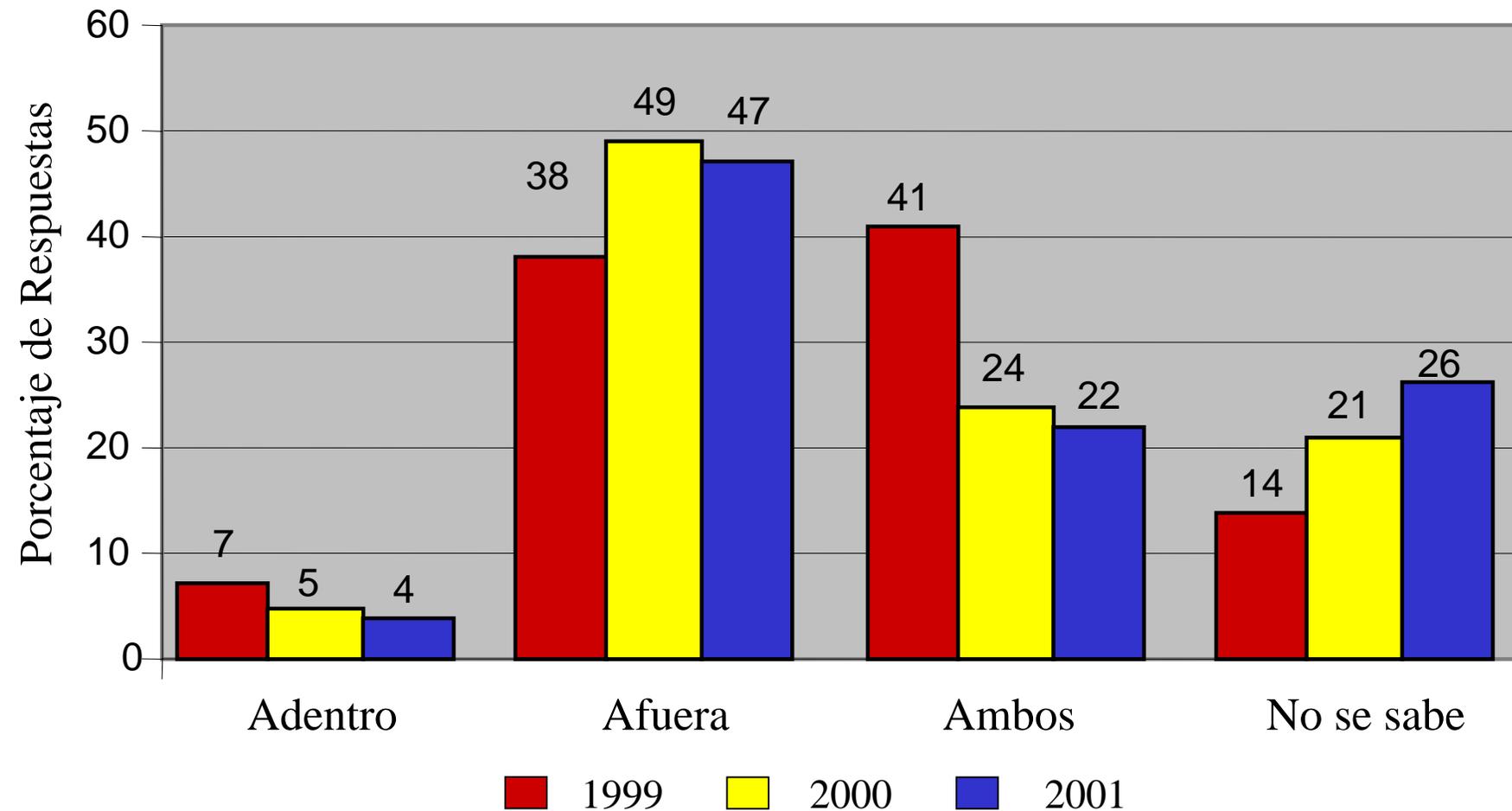
# Tipos de ataques



- Saboteo
- Fisgoneo Telecomunicaciones
- Penetración sistema
- Abuso interno
- Fraude Financiero
- Virus
- Acceso no autorizado de internos
- Fraude Telecomunicaciones
- Active Wiretrap
- Laptop
- Negacion Servicios

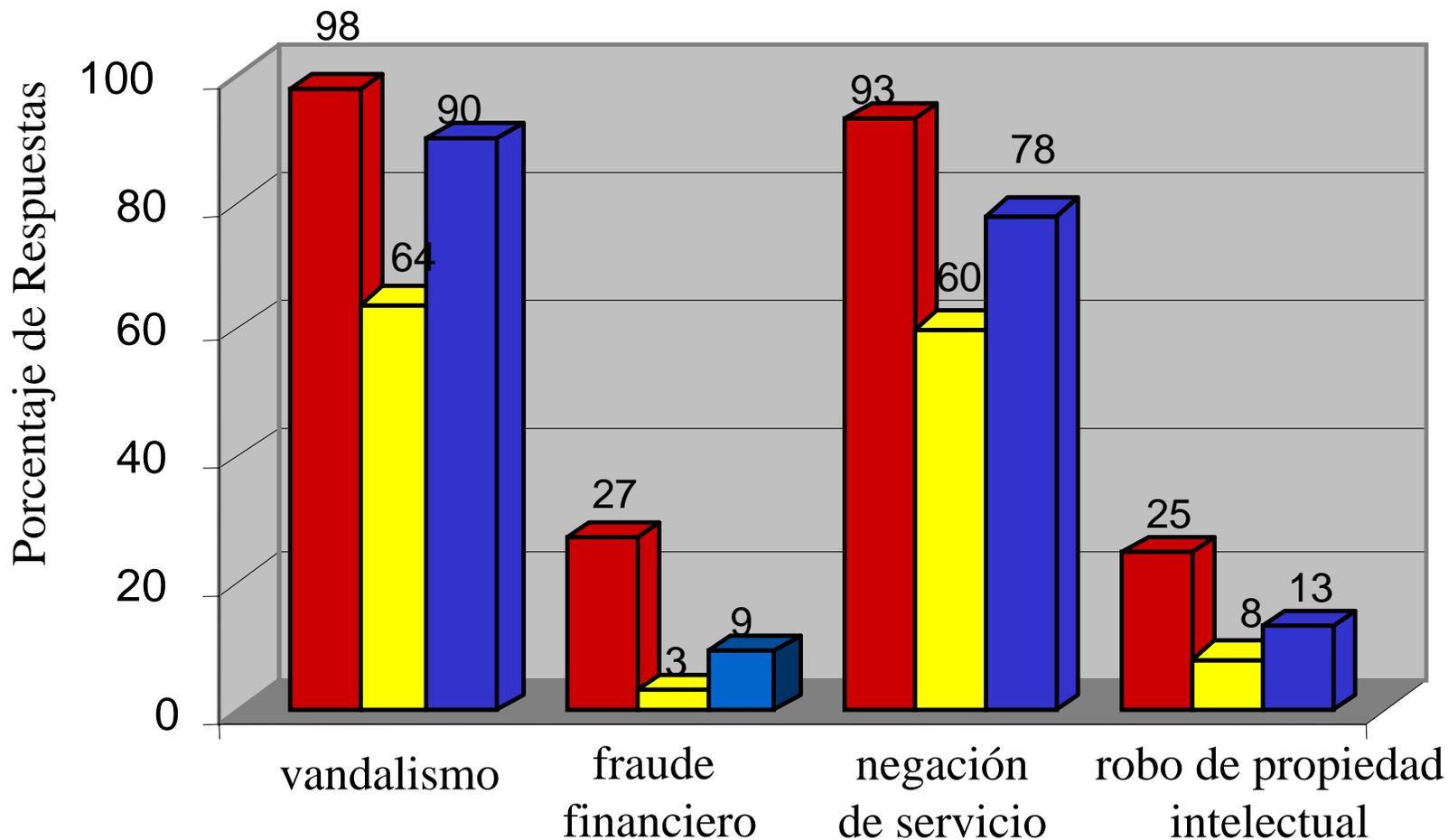


# Incidentes Sitios WWW: ataques vieron de fuera o de dentro





# Incidentes Sitios WWW: que tipo de acceso no autorizado o maluso





# Algunas conclusiones

- La seguridad nunca es negra o blanca y el contexto cuenta más que la tecnología.
- No porque un sistema operativo no proteja contra granadas de mano, este no sirve
  - solo implica que no podemos deshacernos de nuestras paredes, ventanas y puertas
- Diferentes tecnologías de seguridad tienen lugares importantes en una solución general de seguridad.



# Más conclusiones

- El termino seguridad no tiene sentido fuera de contexto.
  - un sistema puede ser seguro mientras ciertos avances matemáticos no ocurran, o por un periodo de tiempo, o contra ciertos tipos de ataques.
  - un sistema puede ser seguro contra el criminal promedio, o contra cierto tipo de espionaje industrial, o contra una agencia nacional de inteligencia con un cierto conjunto de habilidades.