

Semana de Ingeniería ELÉCTRICA Y ELECTRÓNICA 2002

11 abril 2002

Panorama de la Seguridad en Redes

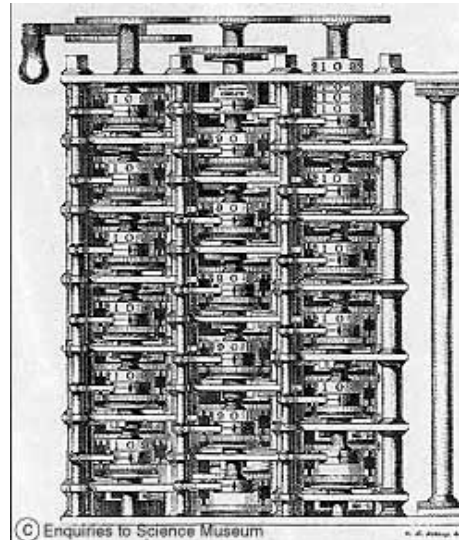
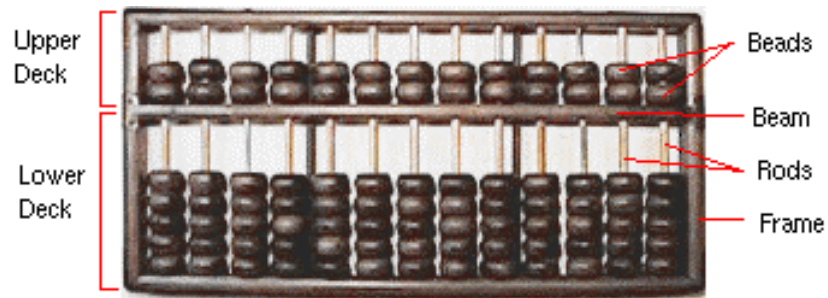
Roberto Gómez Cárdenas

rogomez@campus.cem.itesm.mx

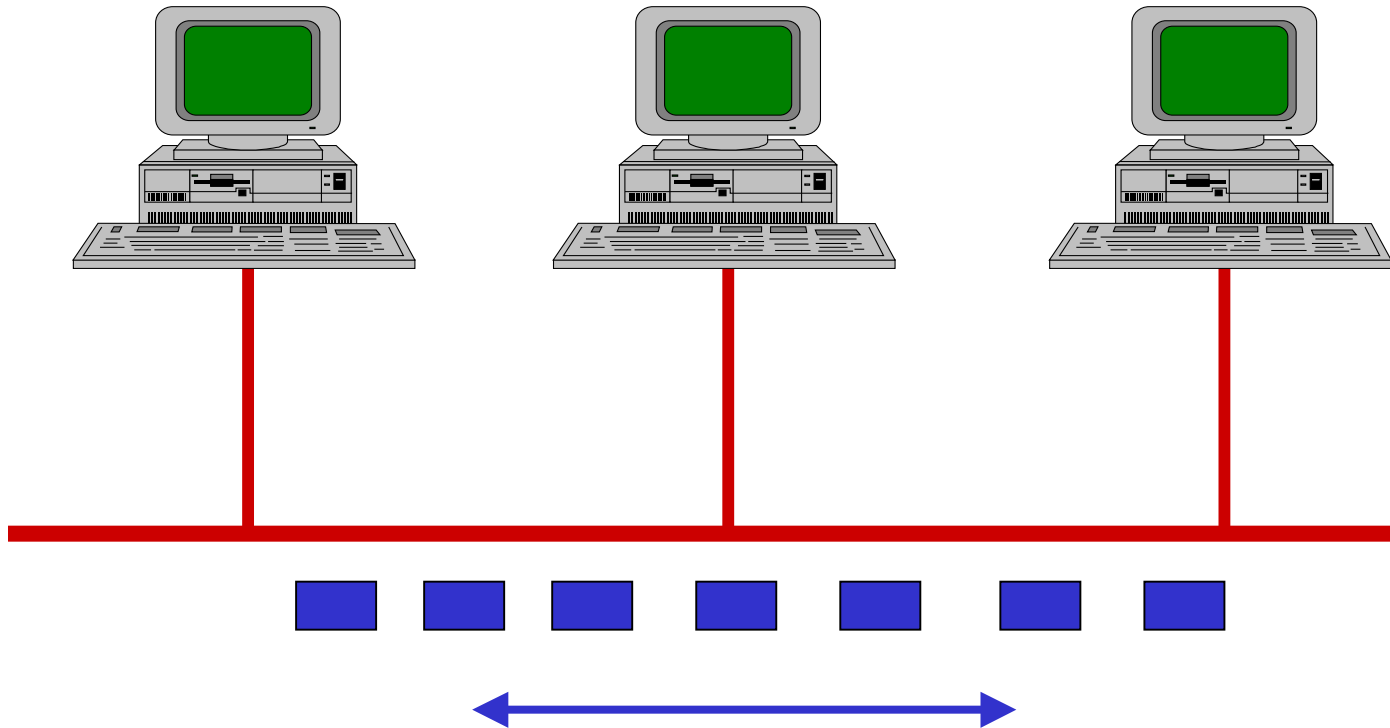
<http://webdia.cem.itesm.mx/dia/ac/rogomez>



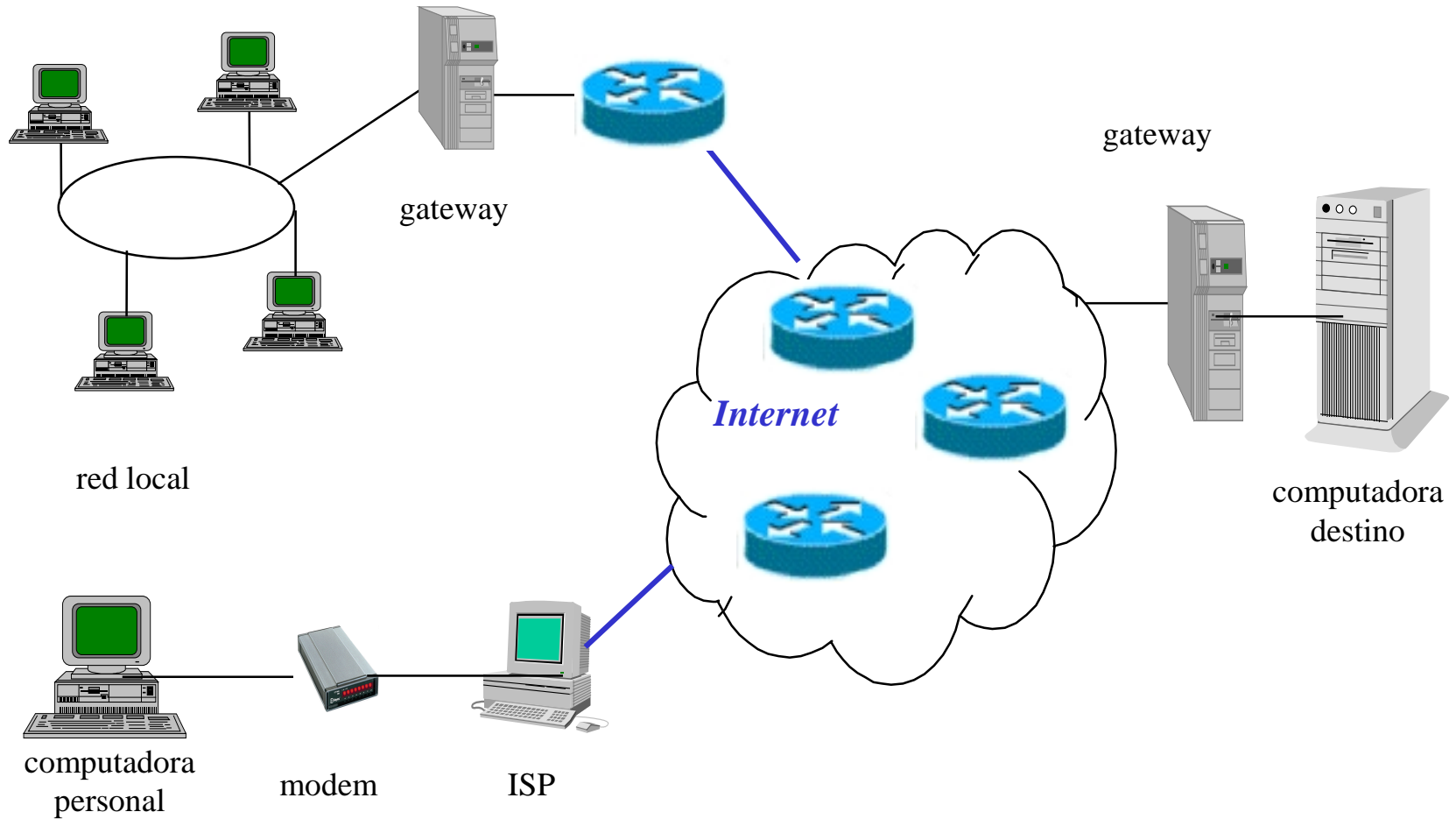
Primeras computadoras



¿Y después?

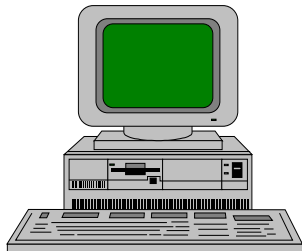


Expandiendo las redes

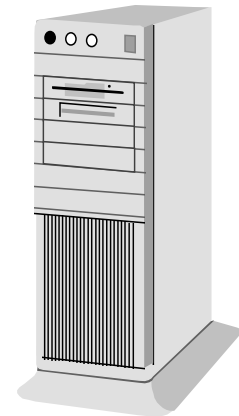


El esquema cliente/servidor

cliente



servidor



petición



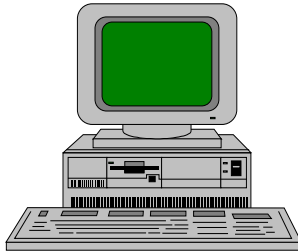
procesamiento

respuesta



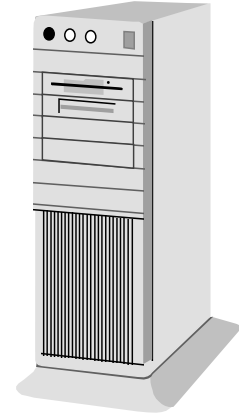
¿Y donde estan los malos?

cliente



¡de los dos lados!

servidor



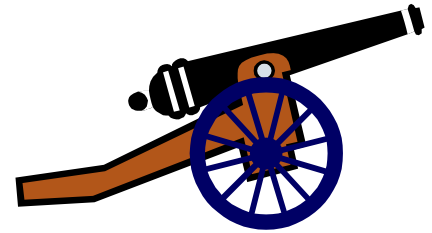
Haciendo cuentas ...

- Computación electrónica 50 años !
- Redes sólo tienen 30 años de vida !
- Seguridad 23 años !
- Internet 15 años !
- Web 6 años !
- Intranets 3 años...
- Extranets 2 años...

¿Seguridad?



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



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.

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.



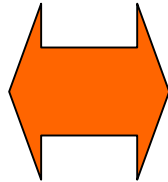
Un sistema posee la propiedad de *disponibilidad* si, la información es accesible (está disponible) en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.



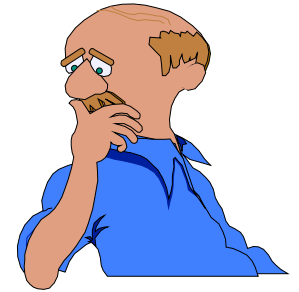
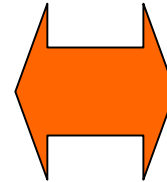
¿Quien contra quien?



**Amenazas
Vulnerabilidades
Ataques**



**Mecanismos
y
Políticas**



**Confidencialidad
Integridad
Disponibilidad**

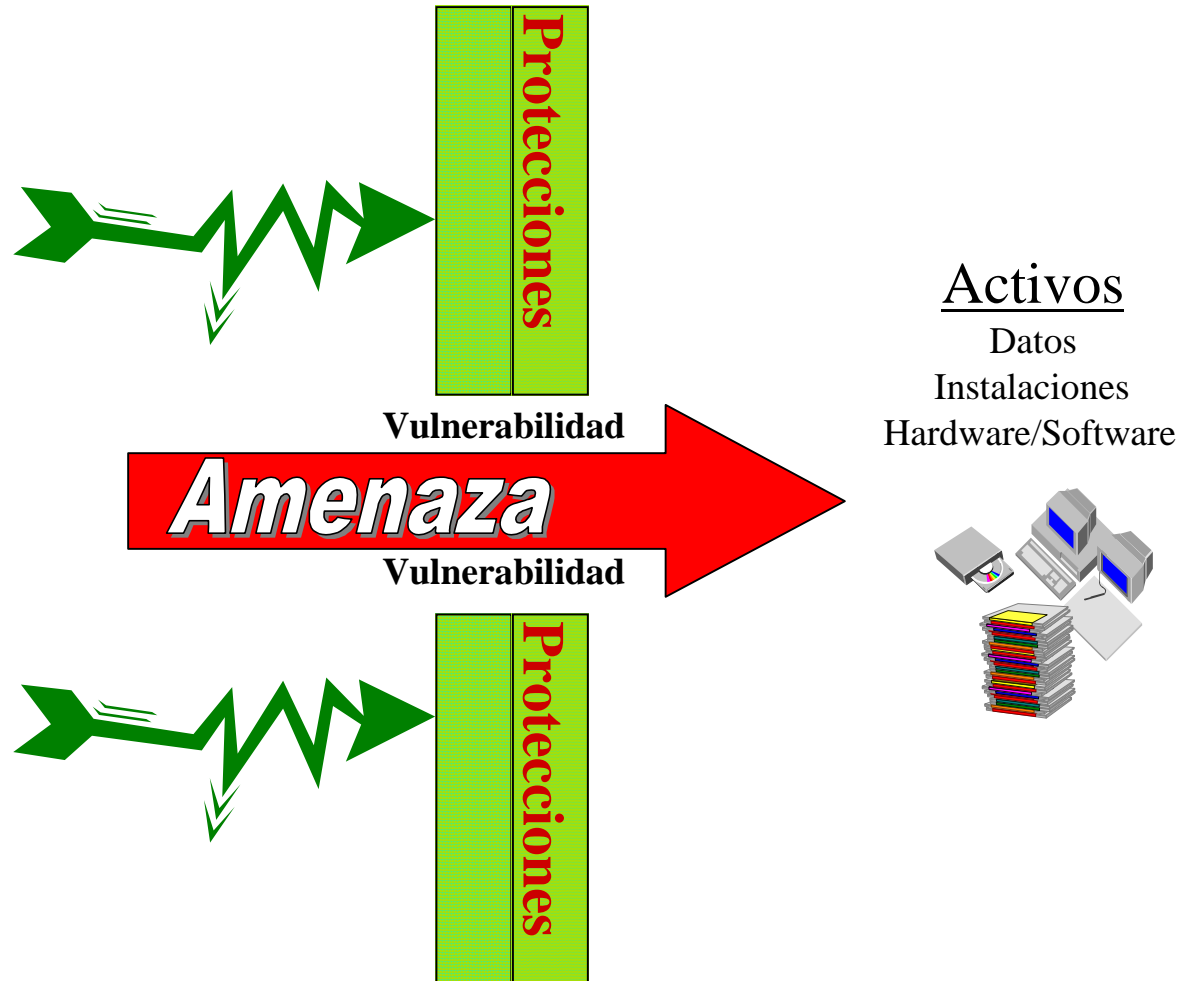
Amenaza



- Circunstancia o evento que puede causar daño violando la confidencialidad, integridad o disponibilidad
- Frecuentemente aprovecha una 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*.

Vulnerabilidad vs amenaza



¿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.
- El hecho de que se haga un ataque no necesariamente significa que tendrá éxito.
- Esto incluye cualquier acción que causa la destrucción, modificación o retraso del servicio no autorizado.

- Es una técnica o método que implementa uno o más servicios de seguridad.
- Un servicio garantiza la seguridad de los datos que residen en un host o que circulan en una red.
- La mayoría de los mecanismos actuales se basan en la criptografía.

- Definición del conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Depende de los objetivos y metas de la organización.
- Generalmente es expresada en un lenguaje o idioma.

- *Paranoico*: Nada está permitido.
- *Prudente*: Lo que no está expresamente permitido, está prohibido.
- *Permisivo*: Lo que no está expresamente prohibido, está permitido.
- *Promiscuo*: Todo está permitido.

Ejemplo de Política (en lenguaje natural)



- Sólo se permitirá el intercambio de correo electrónico con redes de confianza.
- Toda adquisición de software a través de la red debe ser autorizada por el administrador de seguridad.
- Debe impedirse la inicialización de los equipos mediante disco.

¿De quien me debo cuidar?

- Los hackers
- Los crackers
- Los scripters



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.



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”.

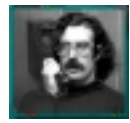
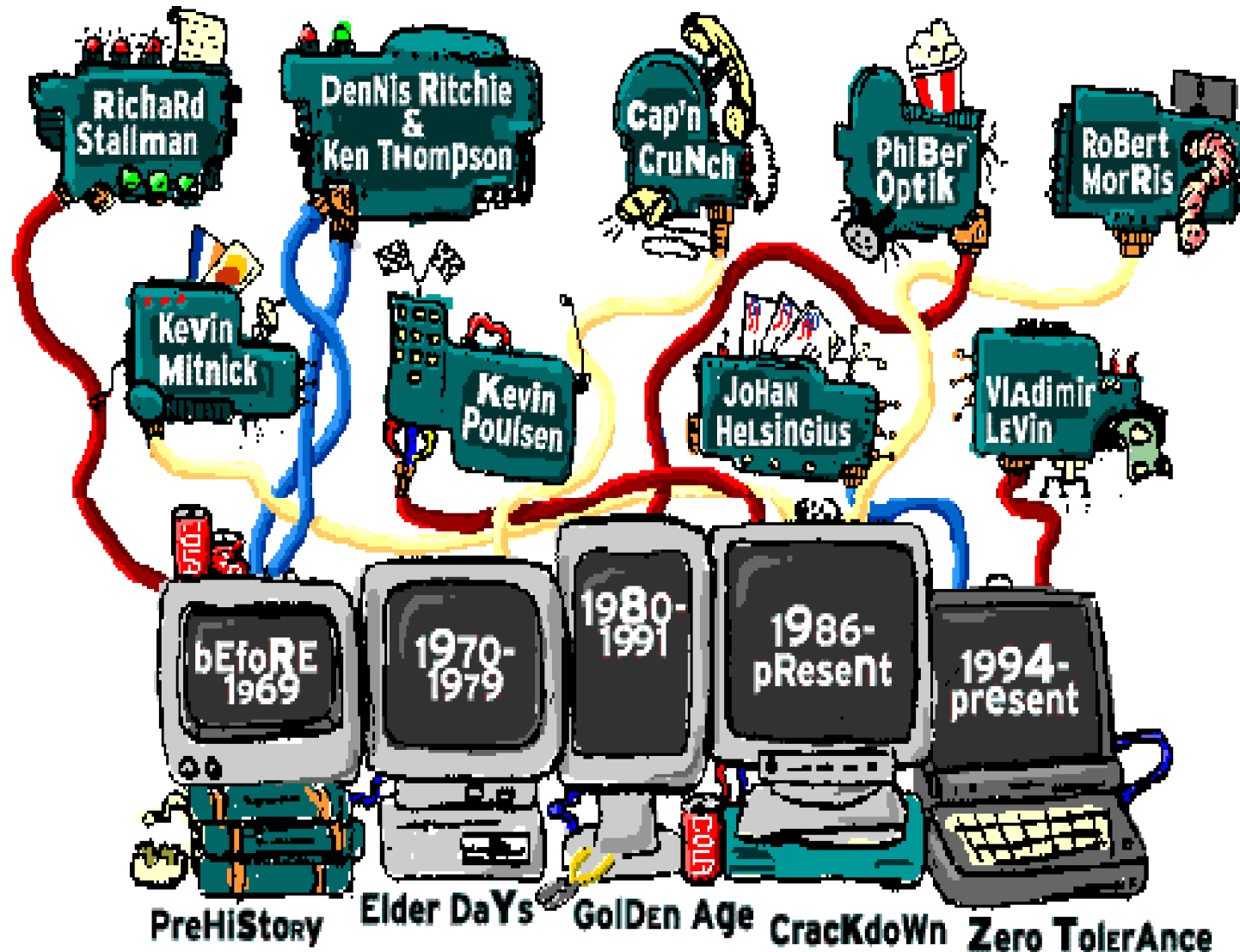


El Hacker: La Visión del Resto de los Usuarios



- ¿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.

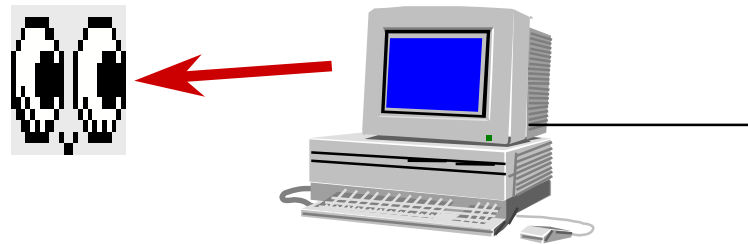
El hall de la fama de los hackers



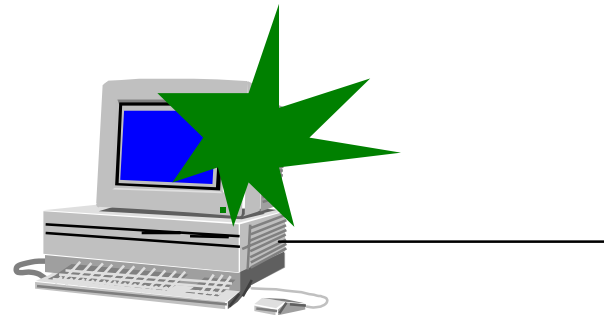
El hacker Kevin Mitnick



Ataques Pasivos.



Ataques Activos.

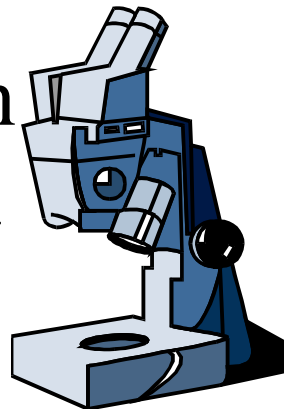


Principales Ataques

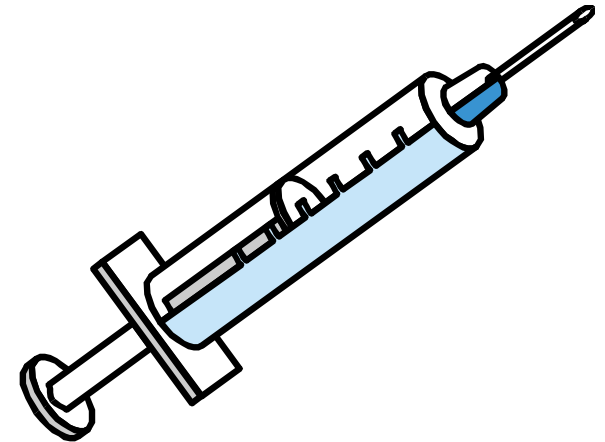


- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Stack overflow
- Pepena
- Bombas lógicas
- Secuestro sesiones
- Dedos inexpertos
- Falsificación
- Usurpación
- Sniffers
- Spoofing
- Spam
- Grafiti
- Ingeniería Social
- Negación de servicio

- 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..



- 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.



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

Variantes relacionadas con virus

- En ocasiones se habla de estas variantes como si se tratara de virus , 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 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	Status
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: CompMovilVirtual.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

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 nez C.



The screenshot shows the Outlook Express interface. The title bar reads "[Fwd: Cuidado!!!!] - Netscape Folder". The menu bar includes File, Edit, View, Go, Message, Communicator, and Help. The left pane shows the "Local Mail" folder tree with subfolders: Inbox, Uns...ages, Drafts, Templates, Sent, Trash, alain, roberto, and news. The top right pane displays a list of messages. The main pane shows the content of the selected message.

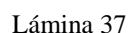
Name	Subject	Sender	Date	Priority	Stat...
	TIE3 00489381	• Toney Roa	09/04/2000 8:50 ...		• read
	TIE3 451838	• Aldo Martinez	09/04/2000 8:57 ...		• read
	Undeliverable: AYUDA S...	• System Administrator	09/04/2000 9:08 ...		• read
	las viejas de la semana	• Toño Durán	09/07/2000 5:31 ...		• read
	importante	• Toño Durán	09/07/2000 6:02 ...		• read
	Re: Del Instituto de Ingen...	• Abigail Zamora Hernández	09/07/2000 7:04 ...		• read
	RV: Pleito de Vecindad	• Adolfo Márquez Matus	09/07/2000 9:03 ...		• read
	SIGOPS-ANNOUNCE mo...	• Mike Dahlin	09/07/2000 9:12 ...		• read
	FW: free software company	• Allan Baker Ortégón	09/08/2000 1:48 ...		• read
	Re: [linuxcm] Re:Ayuda L...	• Allan Baker Ortégón	09/08/2000 1:48 ...		• read
	RV: Ericsson	• Ramiro Sanchez Rabling	09/08/2000 8:56 ...		• read

Subject: Cuidado!!!!
Date: Wed, 15 Nov 2000 22:26:36 -0600
From: "Salvador G. Medina" <adan@servidor.unam.mx>
To: [Shafia Sucar <shafia@quijote.ugto.mx>](mailto:shafia@quijote.ugto.mx), francia-mexico@casadefrancia.org.mx

Hola,
 Desgraciadamente el virus del que nos hablo Ofelia ya circulo en esta lista, en mensajes aparentemente enviados por Shafia (con fecha de mañana 16), no abran los attachment (Navidad18 y Navidad22) y limpien su maquina con Norton 2000, antes de enviar mensajes. Usuarios de Mac solo borren los attachment.
 Saludos, Salvador.

At 09:51 -0600 16/11/00, Shafia Sucar wrote:
 >>Annie,
 >>

Total messages: 113 Unread messages: 0



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

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	

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 <lula.frye@hq.acm.org>](mailto:lula.frye@hq.acm.org)
To: [Roberto Gomez Cardenas' <rogomez@campus.cem.itesm.mx>](mailto:rogomez@campus.cem.itesm.mx)

BUOUOEJIPU

[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?



```
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

Browse...

Find Now

Stop

New Search

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
FLINCS	C:\WINDOWS\OPTIONS\CABS\CONTENT\WS.I	13KB	VBScript Script File	01/10/2001 7:04 PM

542 file(s) found

Monitoring New Items

Precauciones a tomar con correos electrónicos



- Usar un antivirus
- 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

Antivirus y vacunas

- Programa encargado de la detección de virus.
- Algunos intentan parar el virus en el momento en que se produce el ataque (sistemas de prevención)
 - la mayoría vigilan la entrada desde disco pero no desde internet
- Otros comprueban el código del programa antes de que se ejecute.
 - usuario puede ser avisado de los posibles peligros del programa que va a ejecutarse
 - el proceso se conoce vulgarmente como “escaneado”
- Una vacuna esta diseñada para limpiar un virus en concreto, solamente un virus



- Mantener al día el antivirus
 - algunos lo hacen de forma automática
- Nunca instalar y ejecutar más de un antivirus
- Usar sentido común
 - ¿vale la pena examinar lo que me llegó por correo electrónico?
 - verificar el origen del correo
 - ¿conozco a la persona que lo envió?
 - ¿en realidad necesito el archivo que viene con el correo?
 - ¿acaso yo pedí dicho archivo?

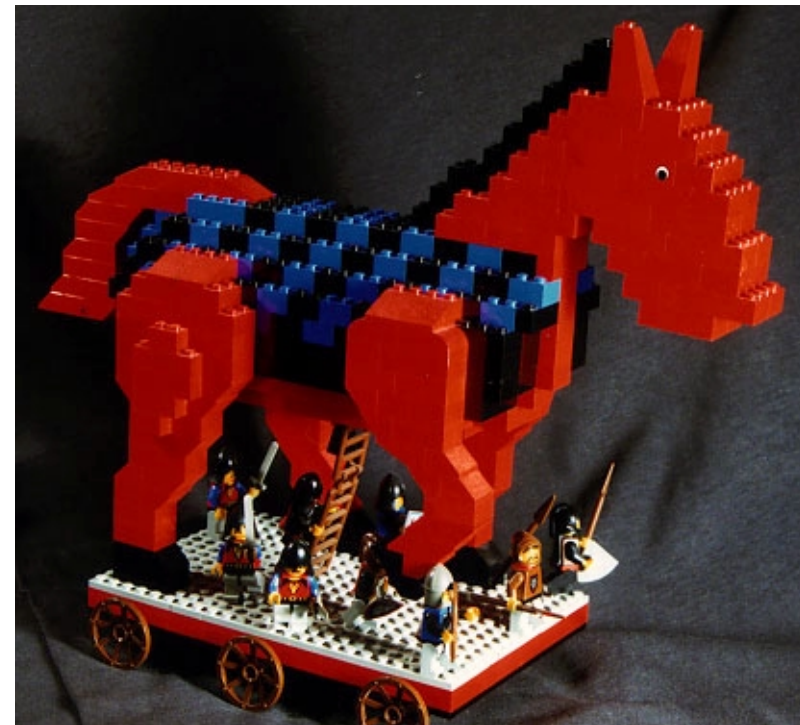
- Distribución de SW por Internet
- Plug-ins desarrollados por terceros diferentes a los creadores de los browsers, que toman el control de la máquina
- Ofrecen soporte de nuevos formatos de archivos y aplicaciones
 - acroread, real player, etc
 - fondos de pantalla
 - protectores de pantalla

- Afectan configuraciones de otros productos ya instalados.
- Posibilidad de que el software realice más actividades que las originales.
 - caballos de troya
 - puertas traseras (backdoors, trapdoors)

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.



Un 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.

Trapdoors, backdoors o puertas traseras



- 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.

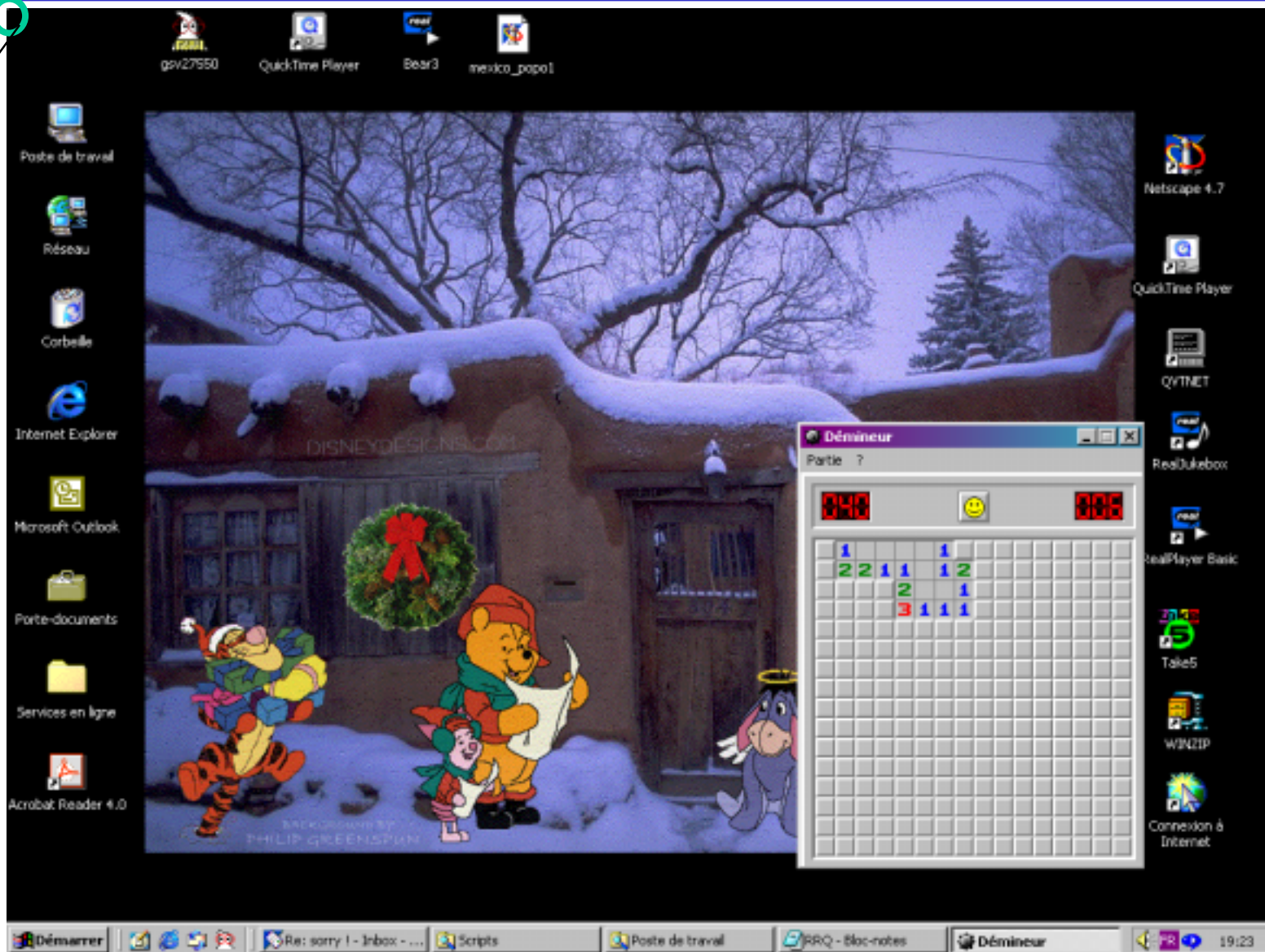
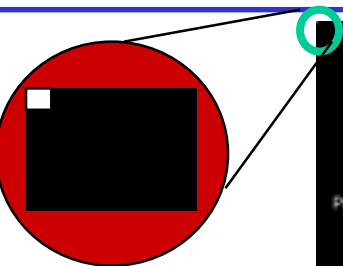


Ejemplo puerta trasera



- 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

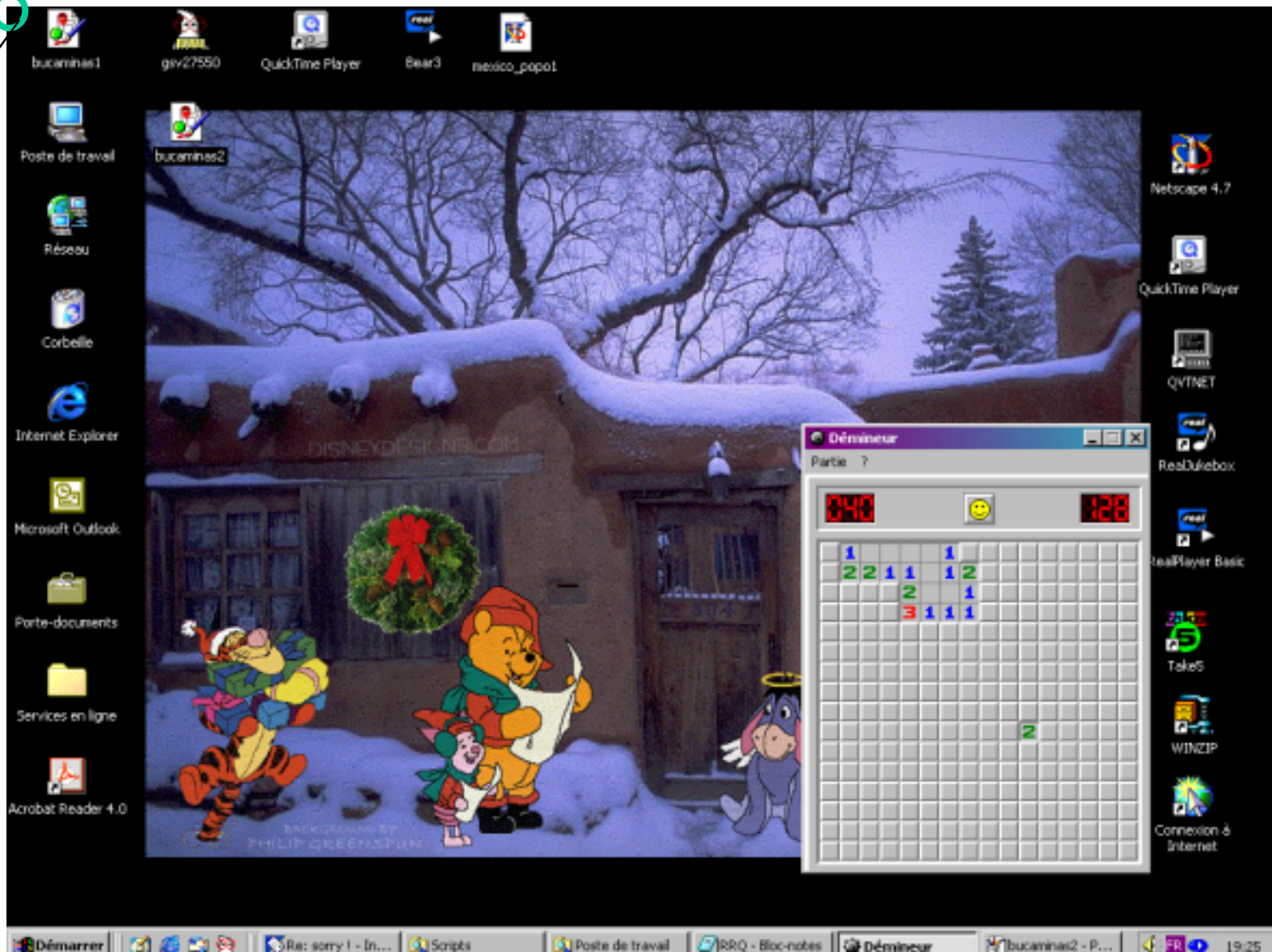
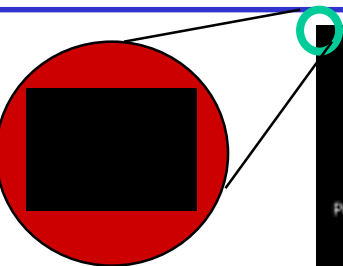
Puerta trasera en buscaminas (1)



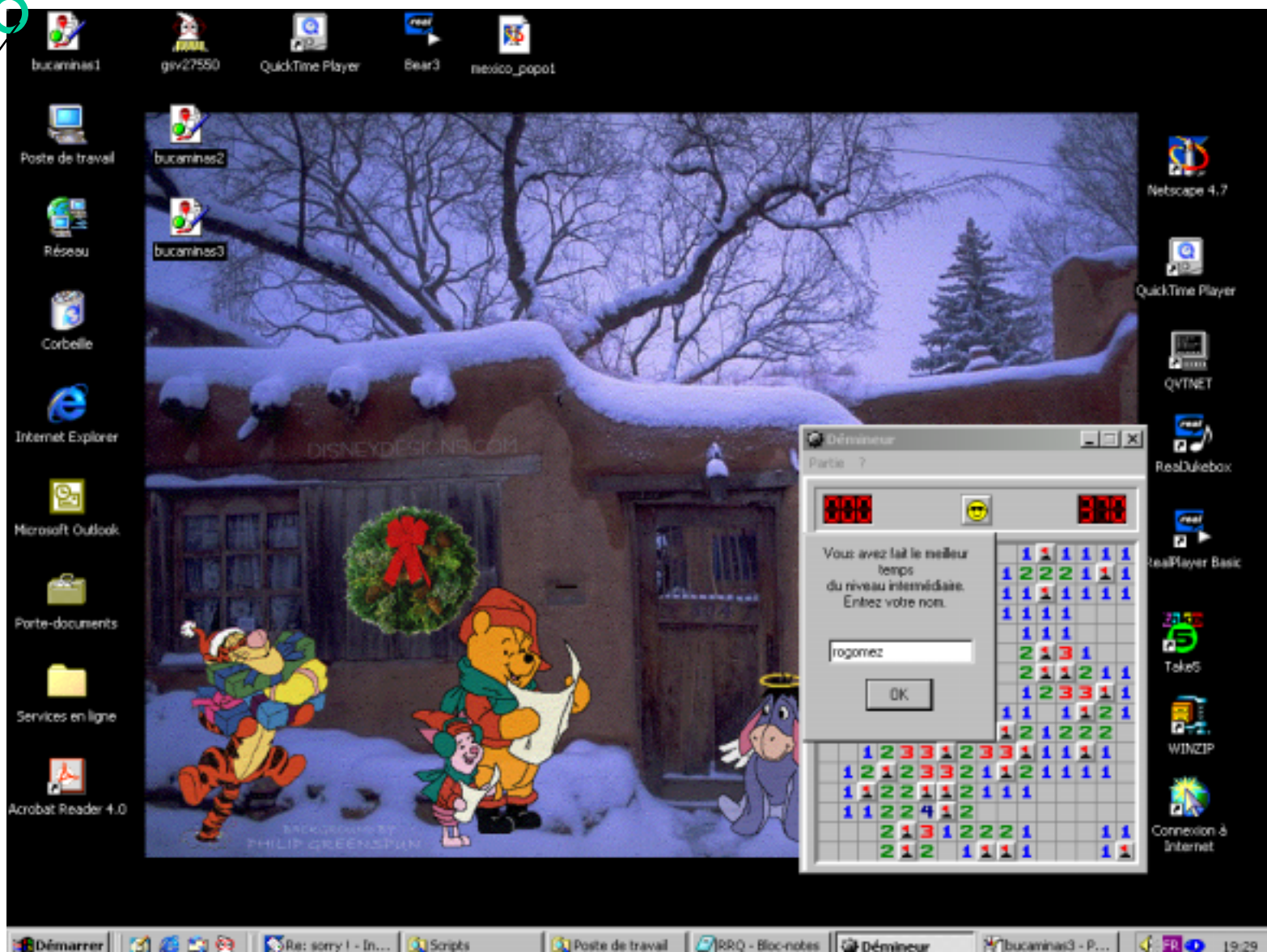
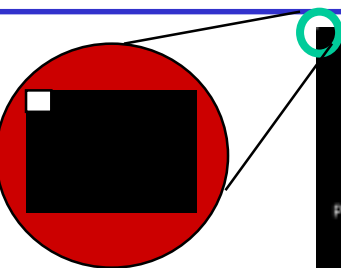
Puerta trasera en buscaminas (2)



Puerta trasera en buscaminas (3)



Puerta trasera en buscaminas (4)



Precauciones a tomar en cuenta



- Estar seguros de que en realidad se necesita el software
- No pueden proporcionarmelo en el área de sistemas.
- Preguntar si alguien más lo ha usado y si ha tenido problemas.
- De preferencia que se software recomendado por la misma marca del browser.

Hoax (engaño, burla, petardo)



- Tipicamente son alertas de peligro, o peticiones de ayuda, empezadas por gente maliciosa - y divulgadas por usuarios inocentes que piensan que estan 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:

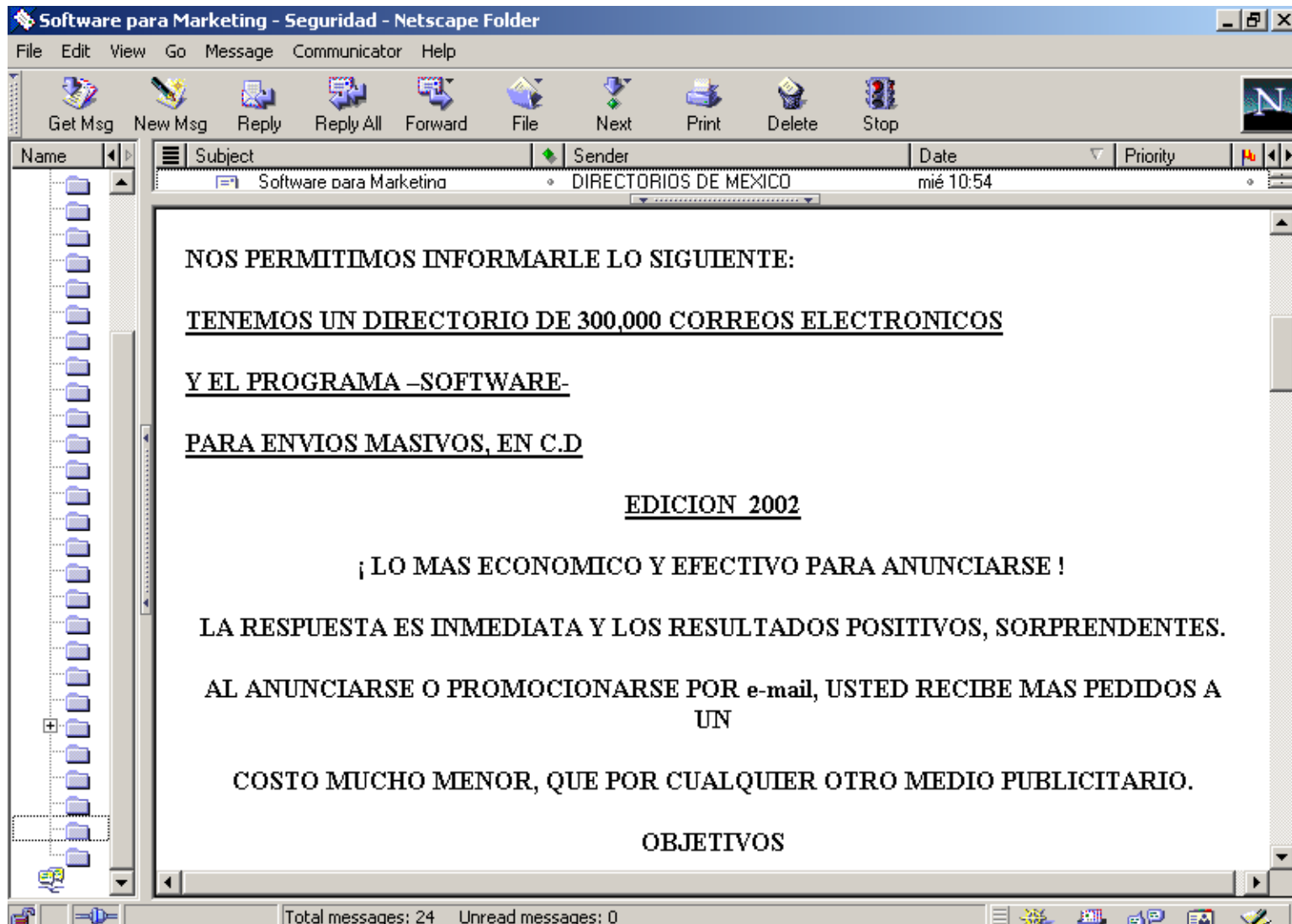
Primero: dirija este e-mail a ACS@aol.com

Segundo: en la parte donde dice CC agregue los e-mails de todos los amigos y colegas que conozca

Saludos cordiales,

Alfonso

¿Y para que quiere alguien direcciones electrónicas?



¿Y eso es negocio?



Software para Marketing - Seguridad - 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

Software para Marketing DIRECTORIOS DE MEXICO mié 10:54

PUBLICITAR NUEVOS PRODUCTOS

COBERTURA

D.F. y Zona Conurbada: 230,000 Direcciones Electrónicas

Provincia: 70,000 Direcciones Electrónicas

Empresas 84% Universidades 11% Particulares 5%

PRECIO: \$ 19,950.00 más I.V.A.

SOLAMENTE SE LE VENDERÁ A 10 COMPRADORES PARA QUE REALMENTE LES SEA MUY PRODUCTIVO.

INFORMACION COMPLEMENTARIA DEL DIRECTORIO DE 300,000 CORREOS ELECTRONICOS

ZONIFICACION	Cantidad
ZONA NORTE (D.F. y AREA METROPOLITANA)	118,000
ZONA SUR (D.F. y AREA METROPOLITANA)	112,000

Total messages: 24 Unread messages: 0

2do. ejemplo hoax

Este reenvío 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..

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



Ejemplo spam



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...

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
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

 **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 traves 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 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

¿Qué hacer con los hoaxes/spams?



- 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



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 (usenames y passwords) necesaria para acceder a un sistema.
- Se basa en ataques como: usurpación de identidad, pepena, inocencia de la gente, relaciones humanas, etc.





"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.

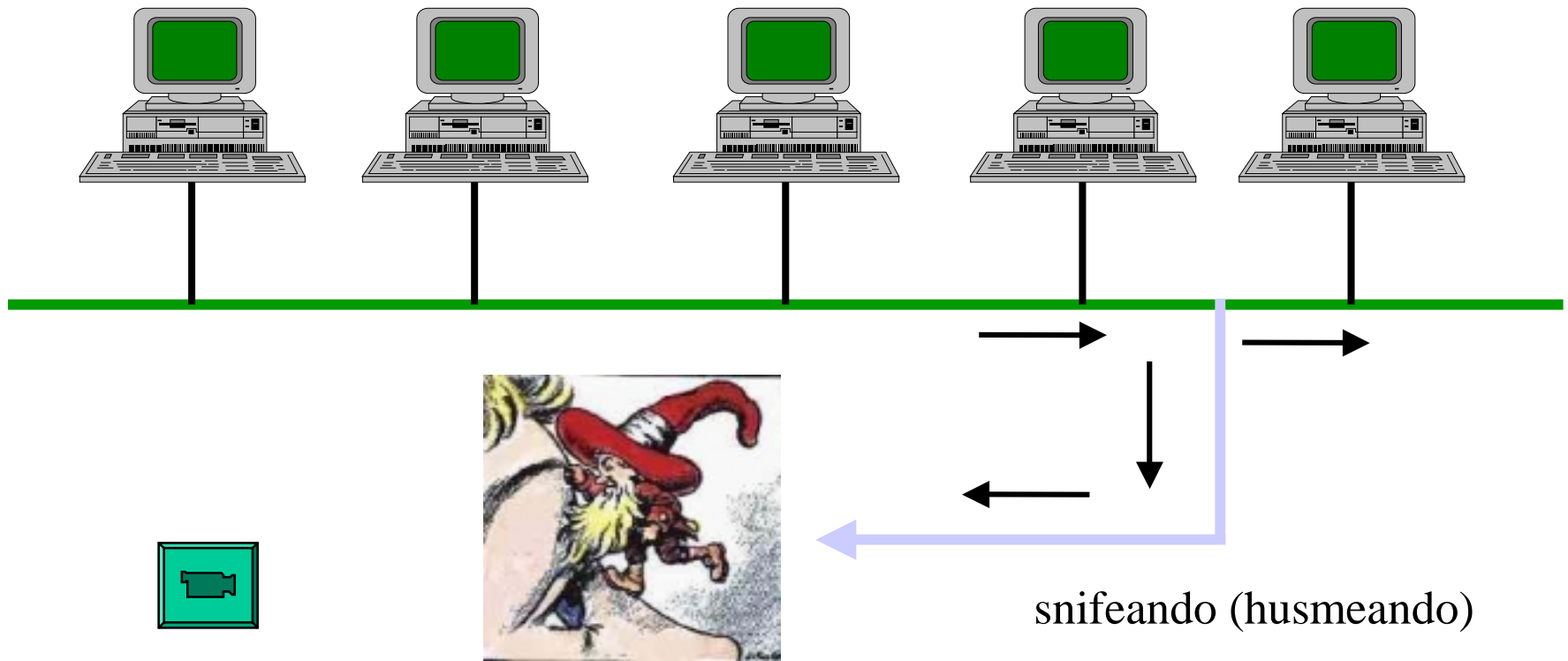
Oh Great!!!!!! My password is rover. I can't wait to see that new screen saver!!!!!"

Medidas a tomar




- Verificar la identidad de la persona con la que estamos conversando.
- Verificar la información transmitida con las fuentes
- Reportar cualquier anomalía

¿Cómo se comunican dos computadoras en una red local?



computadora en
modo promiscuo

Protocolos transmisión encriptados



The screenshot shows a Netscape browser window displaying the Amazon.com product page for the book "Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edit" by Bruce Schneier. The browser's address bar shows the URL: amazon.com/exec/obidos/ASIN/0471117099/o/qid=971146521/st=2-2/102-5972864-6451304. The Amazon.com header includes navigation links like "WELCOME", "DIRECTORY", "BOOKS", and "SEARCH". The product page features a search bar, a "GO!" button, and a "BOOK INFORMATION" section. The book's cover is displayed, along with pricing information: List Price: \$54.95, Our Price: \$43.96, and a savings of \$10.99 (20%). The availability is noted as "Usually ships within 24 hours." The page also includes a "READY TO BUY?" section with buttons for "Add to Shopping Cart" and "Add to Wish List". The bottom of the browser window shows the Windows taskbar with the Start button and several open applications.

Amazon.com: buying info: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edit - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: amazon.com/exec/obidos/ASIN/0471117099/o/qid=971146521/st=2-2/102-5972864-6451304 What's Related

Members WebMail Connections BizJournal SmartUpdate Mktplace RealPlayer

amazon.com. YOUR ACCOUNT HELP

WELCOME DIRECTORY BOOKS

SEARCH BROWSE SUBJECTS BESTSELLERS NEW & FUTURE RELEASES BARGAIN BOOKS AWARDS SPANISH LANGUAGE

TODAY'S FEATURED STORES BOOKS ELECTRONICS DVD SOFTWARE CAMERA & PHOTO

SEARCH

Books GO!

BOOK INFORMATION

Explore this book

buying info

table of contents

Amazon.com

articles

editorial reviews

customer reviews

See more by this

Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition

by Bruce Schneier

List Price: \$54.95

Our Price: \$43.96

You Save: \$10.99 (20%)

Availability: Usually ships within 24 hours.

See larger photo

Paperback - 784 pages 2 edition (October 18, 1995)

John Wiley & Sons; ISBN: 0471117099 ; Dimensions (in inches): 1.87 x 9.20 x 7.54

Other Editions: Hardcover

READY TO BUY?

Add to Shopping Cart (you can always remove it later)

Shopping with us is 100% safe. Guaranteed.

Add to Wish List

(We'll set one up for you)

View my Wish List

Start Exploring... Microsoft... Amazon...

9:56 PM

Protocolos transmisión encriptados



Amazon.com Checkout: Sign In - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: <https://www.amazon.com/exec/obidos/checkout-sign-in/103-4769853-4624626> What's Related

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels

amazon.com

WELCOME ADDRESS ITEMS WRAP SHIP PAY CONFIRM

*** Please fix the areas indicated below. ***

*** You didn't provide an e-mail address. We'll need it to communicate with you about the status of your orders. And, when you visit us again, you'll use it to access your account. ***

Ordering online is easy.
We'll walk you through the process, step by step.

Enter your e-mail address:

☐ I am a new customer.
(You'll create a password later.)

☐ I am a returning customer,
and my password is:

[Forgot your password?](#)

[Sign in using our secure server](#)

Amazon.com Safe Shopping Guarantee

We guarantee that every transaction you make at Amazon.com will be 100% safe. This means you pay nothing if unauthorized charges are made to your credit card as a result of shopping at Amazon.com.

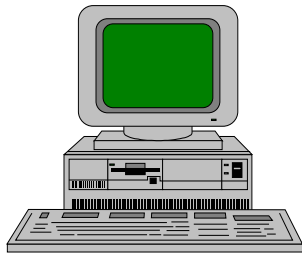
[Learn More](#)

Document: Done

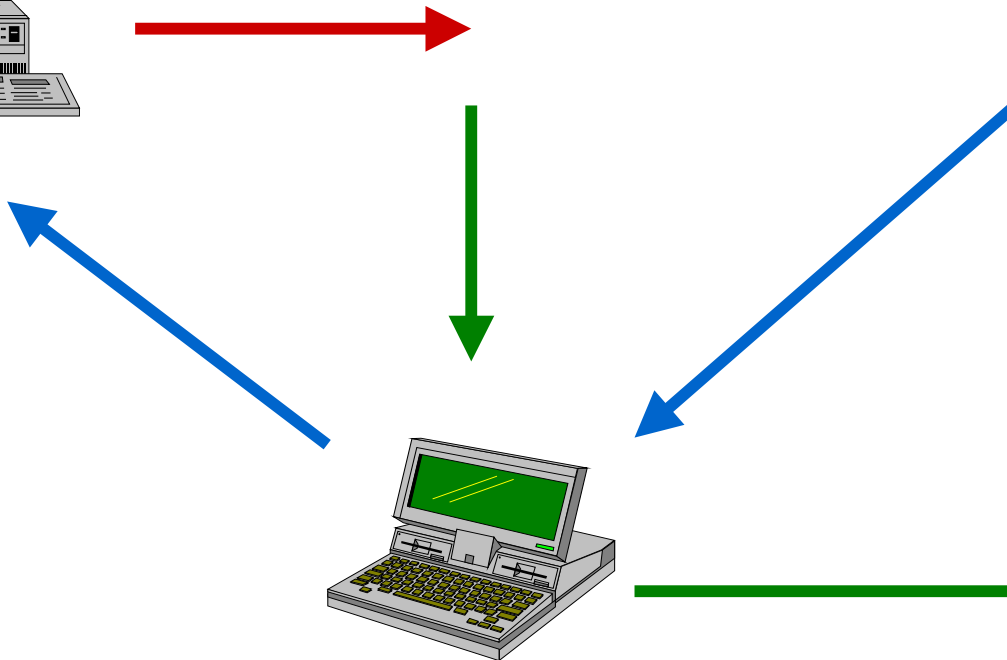
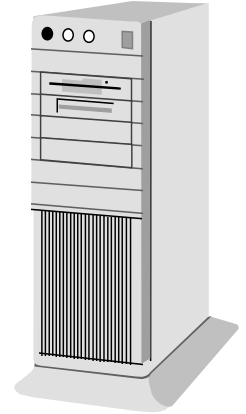
Spoofing



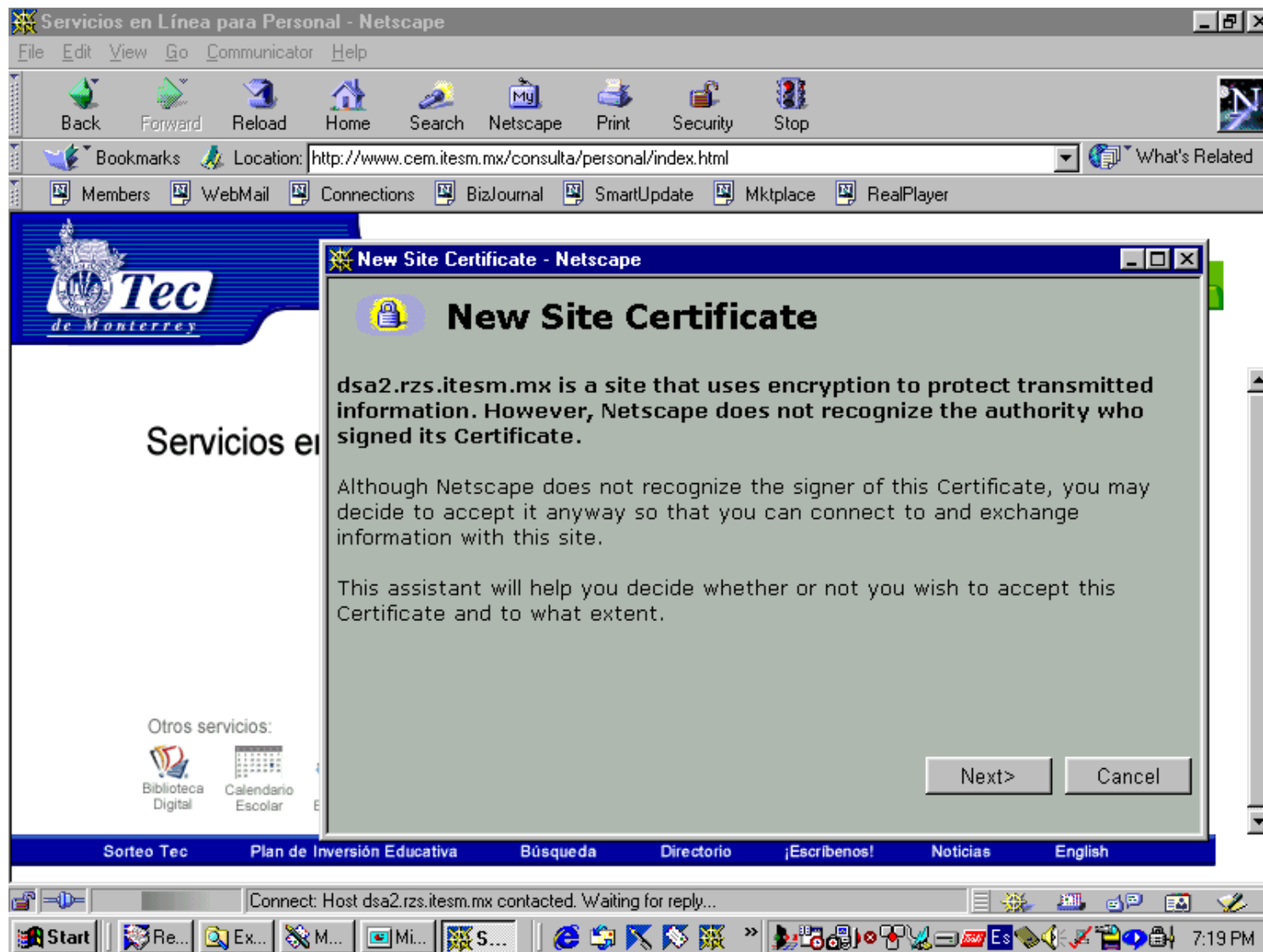
cliente



servidor

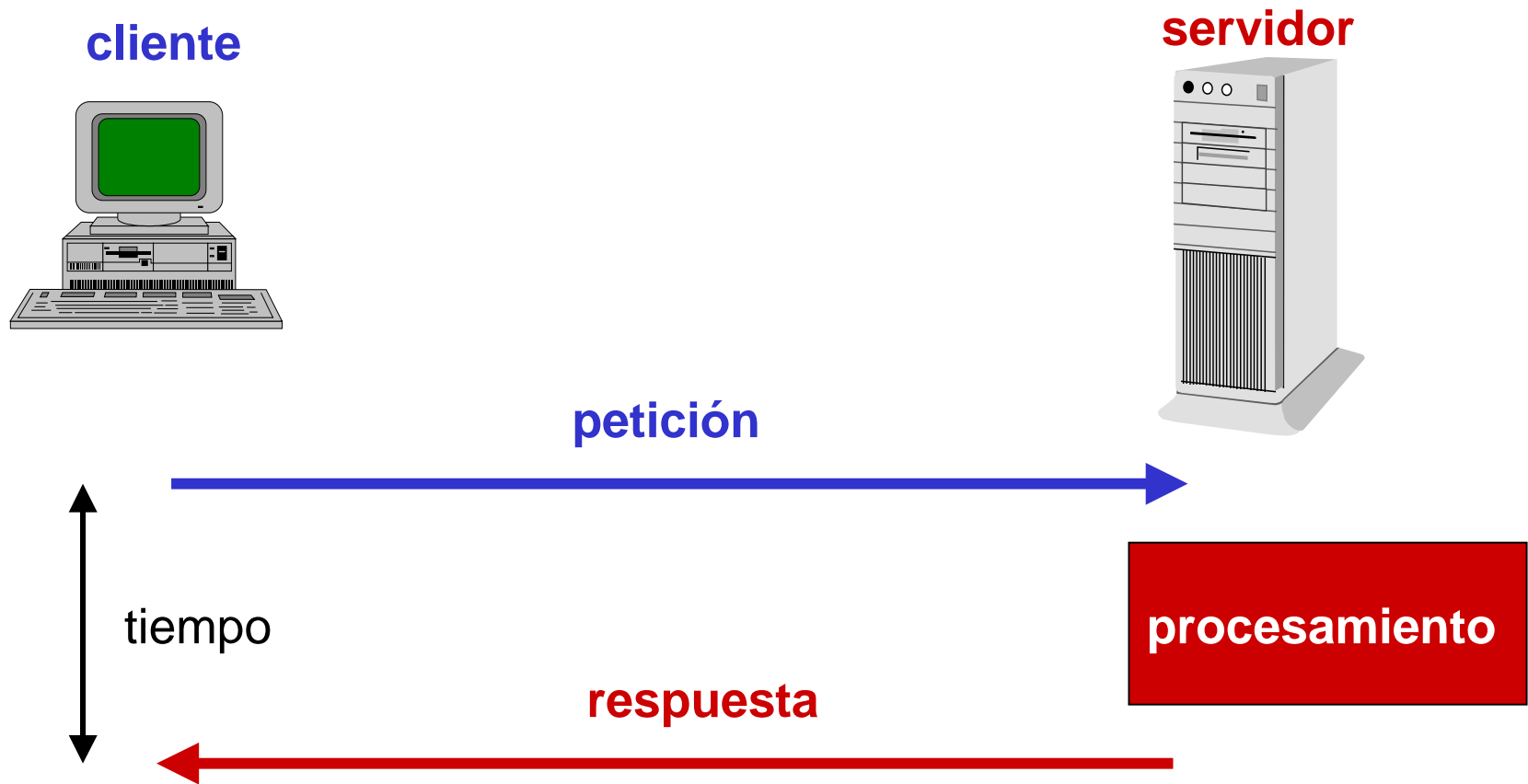


Los certificados



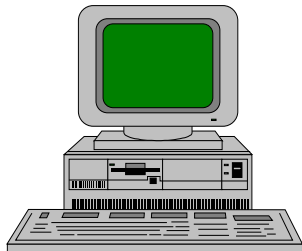
- Los *browsers* son la herramienta que usan los usuarios para navegar por internet.
- Dos elementos fundamentales en internet:
 - cliente: el que realiza la búsqueda de información
 - servidor: el que coloca la información en algun servidor
- Cuando la aplicación en el servidor es muy pesada
 - preferible realizar el trabajo en el cliente
 - desempeño (tiempo respuesta) mejora bastante
- Dos tecnologías:
 - active x
 - los applets de java

El esquema cliente/servidor

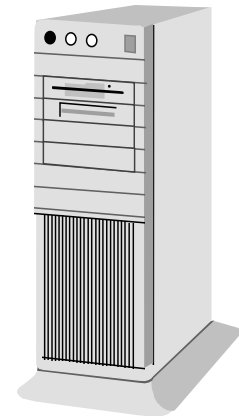


¿Y si el procesamiento es grande?

cliente



servidor



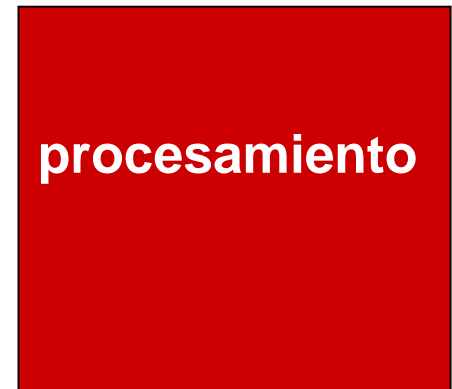
petición



tiempo



procesamiento

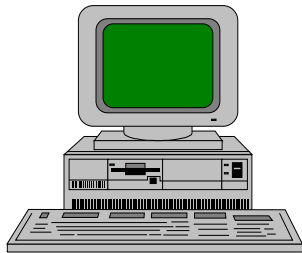


respuesta

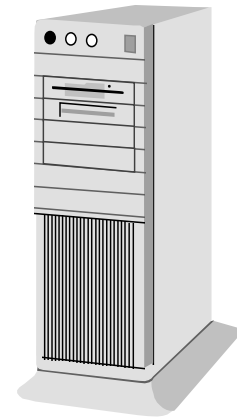


Prefiero que se haga en el cliente

cliente



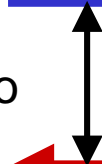
servidor



petición



tiempo



respuesta (programa a ejecutar)

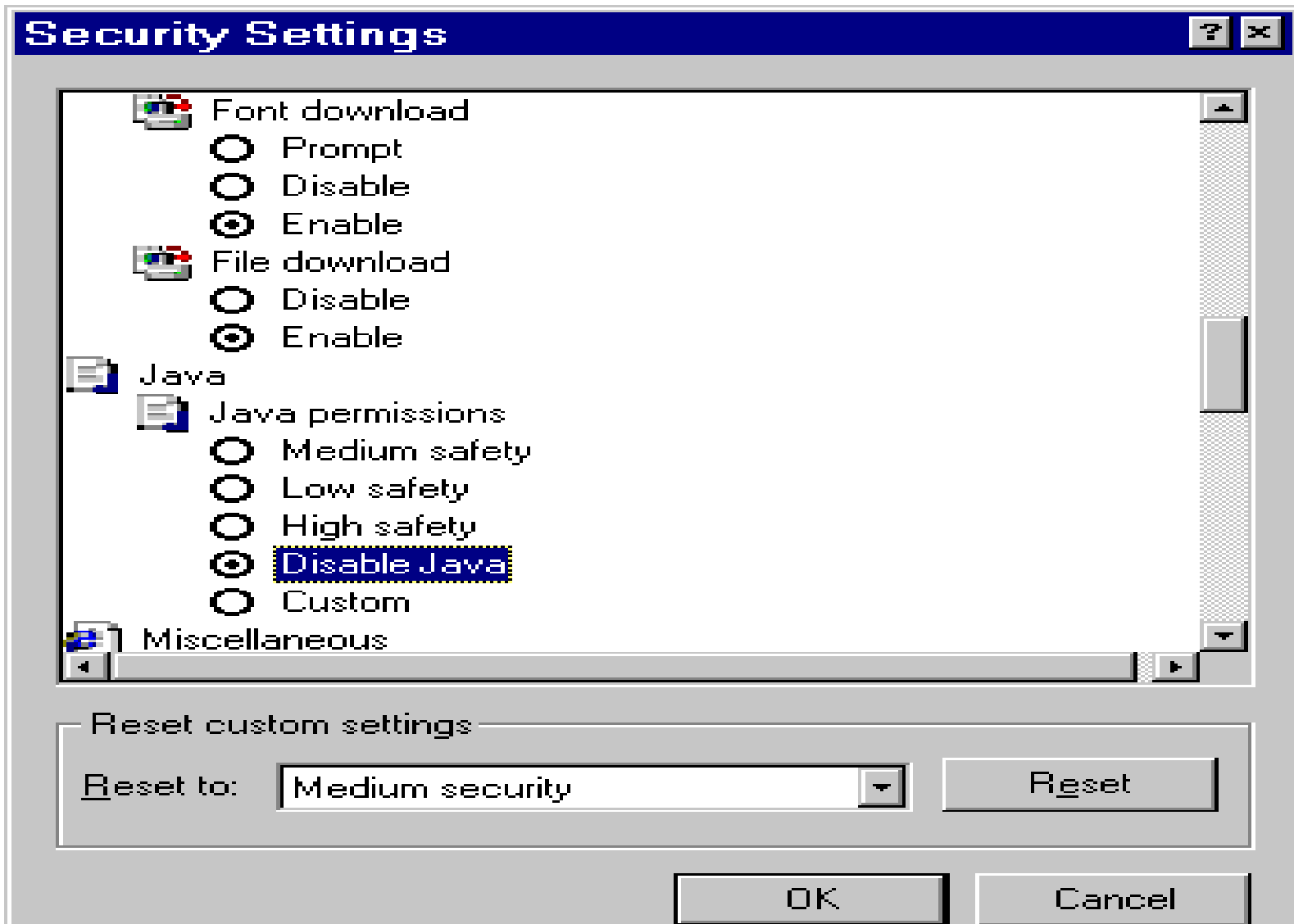


procesamiento

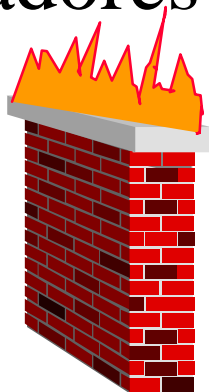
¿Qué pueden llegar a hacer?

- 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

- 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



- Firewalls
- Proxies
- IDS
- Biométricos
- Tarjetas Inteligentes
- Analizadores de Vulnerabilidades



- *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

- *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.securityfocus.com>
- <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

Más conclusiones



- La seguridad nunca es negra o blanca y el contexto cuenta más que la tecnología.
- No porque un sistema operativo no protega 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.

¡Gracias por su atención!



Panorama de la Seguridad en Redes

Roberto Gómez Cárdenas

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”