


Universidad Nacional Autónoma de Bucaramanga


## Panorama general de los principales ataques y defensas de un sistema informático

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

Lámina 1

Dr. Roberto Gómez C.





## Primeras computadoras

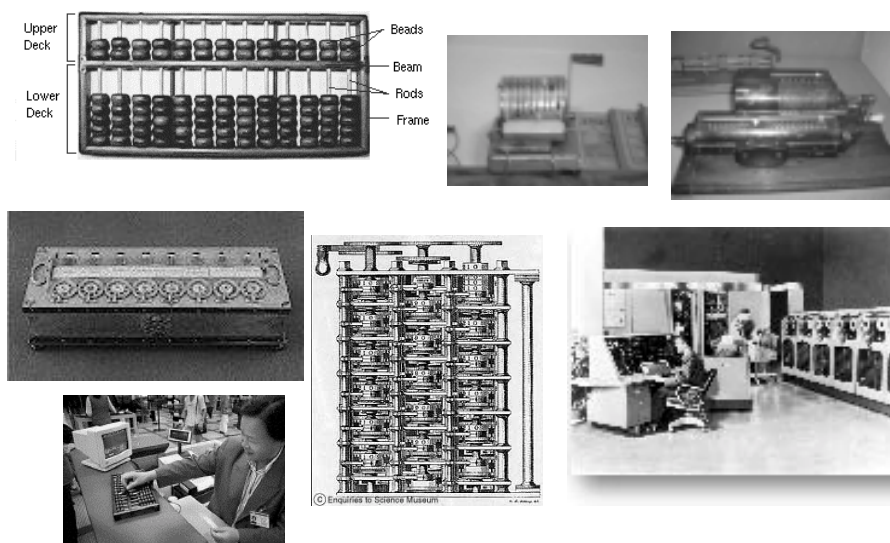
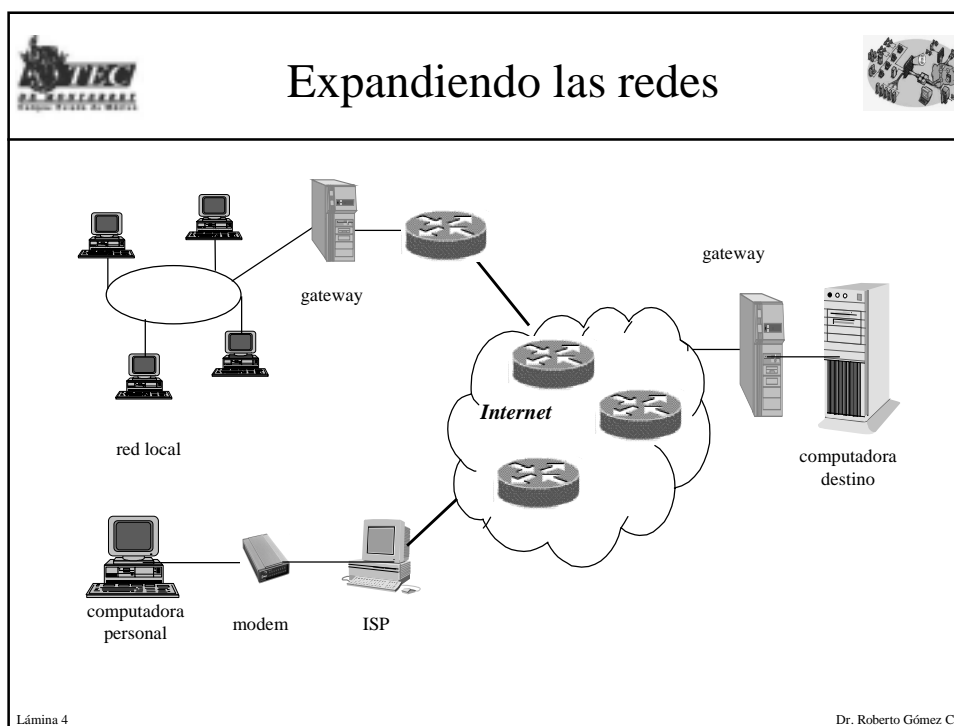
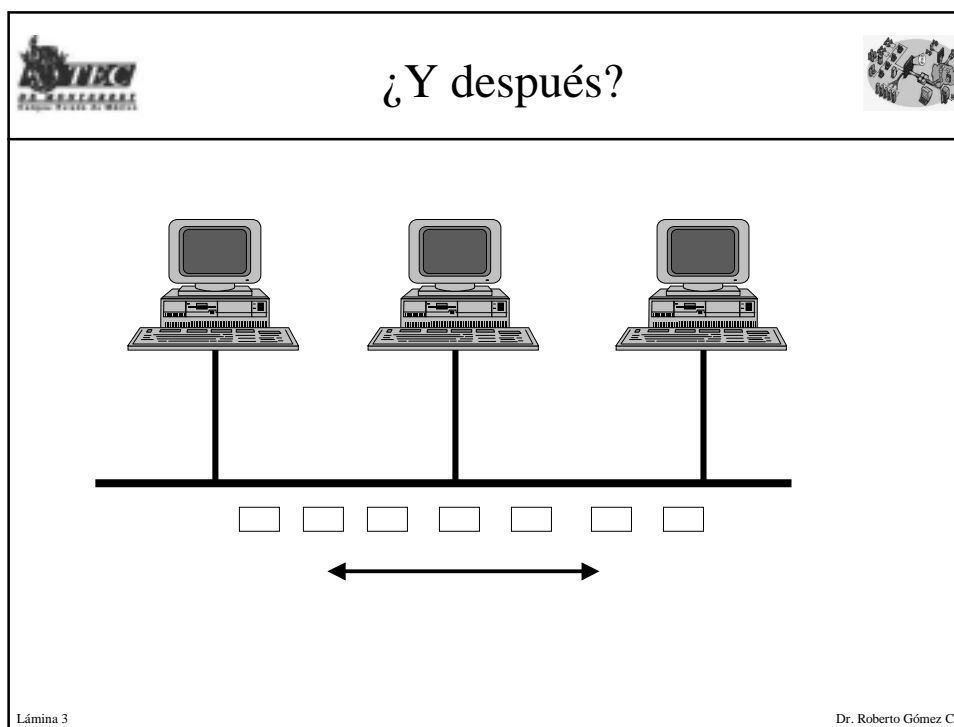
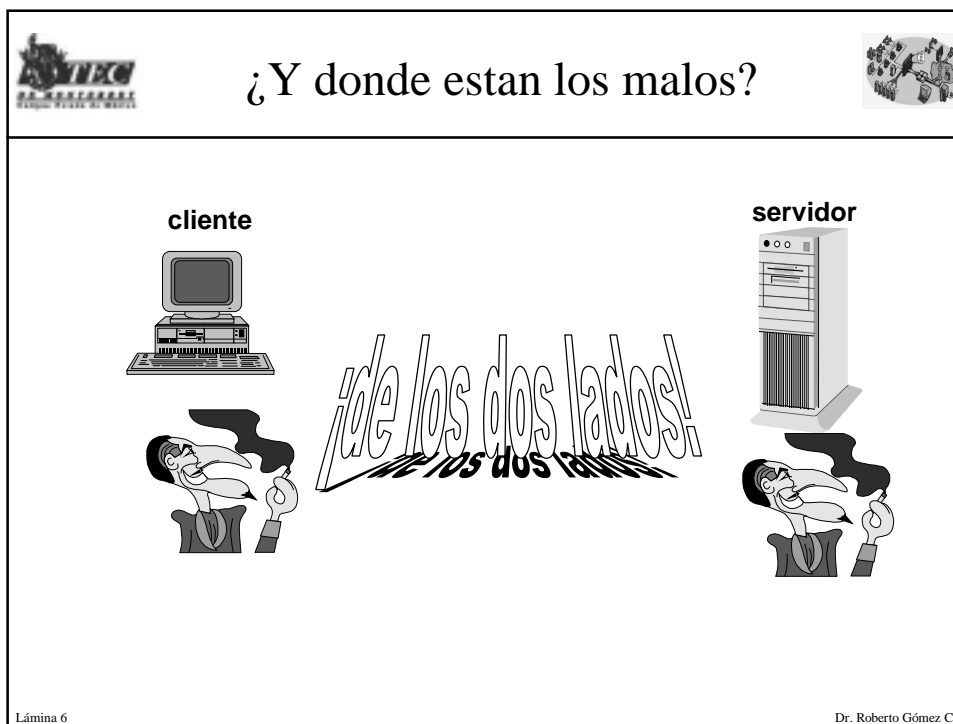
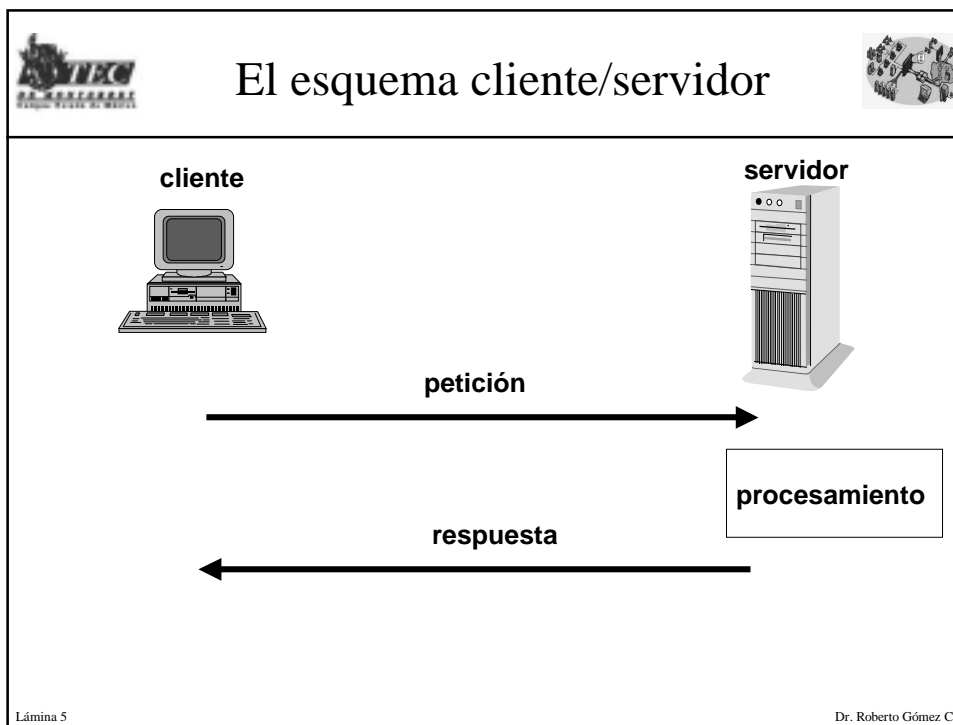


Lámina 2

Dr. Roberto Gómez C.







## ¿Y quienes son los malos?



- Los hackers
- Los crackers
- Los script kiddies



```


Last login: Mar 12 07:03:29 on console
Welcome to os4!
> telnet -a -b ABSOLUT 192.168.100.1:8080
> enter login: #####
> enter passw: #####
> invalid passw ERROR (retype)
> retype passw #####
> OK you are SUCCESSFULLY logged in
> cd /usr/.ABSOLUT/SECRETS
> ls -l -a BACKDOORVIRUSES
-rwxr-xr-- TROJANHORSE#BF1 - 306 Mar 7 20:55
-r-xr-xr-- TROJANHORSE#CA0 - 1026 Mar 11 00:13
-r-xr-xr-- TROJANHORSE#CB9 - 716 Mar 5 14:15
-rwxrw-r-- TROJANHORSE#CFF - 4865 Feb 9 22:06
-r-xr-xr-- TROJANHORSE#D2C - 48 Jan 28 17:24
-r-xr-xr-- TROJANHORSE#D8A - 512 Mar 2 02:22
-r-xr-xr-x TROJANHORSE#DA6 - 512 Mar 7 04:46
-r-xr-xr-- TROJANHORSE#DD7 - 642 Feb 13 01:58
-r-xr-xr-- TROJANHORSE#DF2 - 1784 Dec 31 11:33
-rwxr-xr-- TROJANHORSE#EA3 - 1256 Mar 4 14:56
-rwxrw-r-- TROJANHORSE#EB4 - 2873 Mar 5 08:17
-r-xr-xr-- TROJANHORSE#ED8 - 255 Feb 17 10:45
-r-xr-xr-- TROJANHORSE#FA3 - 207 Feb 17 10:57
> sudo -sp TROJANHORSE#D2C
System is about to reboot
Killing all processes .....

```


ABSOLUT HACKER.

ABSOLUT COUNTRY OF SWEDEN VODKA & LOGO, ABSOLUT, ABSOLUT BOTTLE DESIGN AND ABSOLUT CALLIGRAPHY ARE TRADEMARKS OWNED BY V&S VIN & SPRIT AB. THOSE WHO APPRECIATE QUALITY ENJOY IT RESPONSIBLY. THIS AD WAS MADE BY PRY 2000.

Lámina 7
Dr. Roberto Gómez C.



## 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.


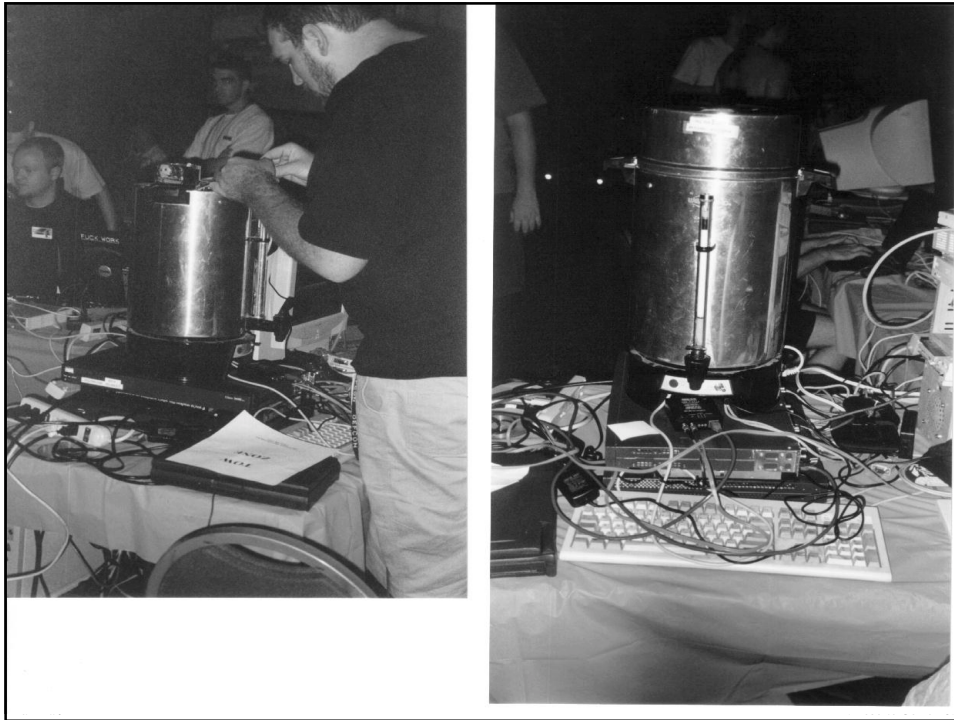


Lámina 8
Dr. Roberto Gómez C.




## 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.

Lámina 10

Dr. Roberto Gómez C.



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".






Lámina 11

Dr. Roberto Gómez C.



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.

Lámina 12

Dr. Roberto Gómez C.

# El hall de la fama de los hackers

Richard Stallman

Dennis Ritchie & Ken Thompson

Cap'n Crunch

PhiBer Optik

Robert MorRis

Kevin Mitnick

Kevin Poulsen

Johan Helsingius

Vladimir Levin

bEfoRE 1969

1970-1979

1980-1991

1986-pResent

1994-present

PreHiStory Elder DaYs Golden Age CrackDoWn Zero TolerAnce


[www.discovery.com/area/technology/hackers/hackers.html](http://www.discovery.com/area/technology/hackers/hackers.html)

Dr. Roberto Gómez





# El hacker Kevin Mitnick






## Algunos términos y personajes relacionados




- Geeks
- Lammer
- Wracker
  - programas shareware o freeware
- Newbie
- Rider
- Sneaker
  - espía informático por excelencia
- Carding 

EsTo TiPo De TiPoGrAfla Ya No EsTa De MoDa Y yA nO sE uSa  
3ST0 S3RI4 UN 3J3MPLO D3 DICH0 L3NGU4J3




**Una madrecita  
Aprendiendo a  
“Hackear”.**

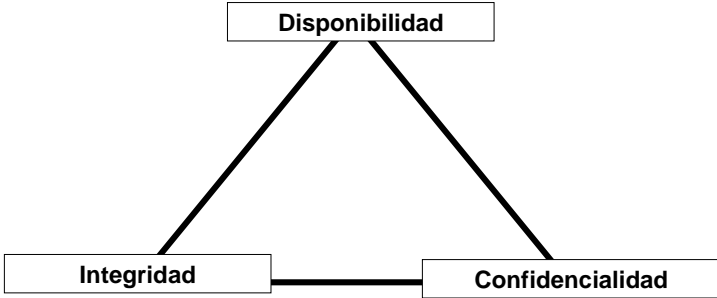
Lámina 15
Dr. Roberto Gómez C.



## Seguridad Computacional



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



```

graph TD
    A[Disponibilidad] --- B[Integridad]
    A --- C[Confidencialidad]
    B --- C
    
```

Lámina 16
Dr. Roberto Gómez C.



## El principio básico

Lámina 17

Dr. Roberto Gómez C.

## La estrategia es un ciclo

Lámina 18

Dr. Roberto Gómez C.

Asegurando el sistema

- **Objetivo**
  - minimizar los riesgos potenciales de seguridad
- **Análisis de riesgos**
  - análisis amenazas potenciales que se pueden sufrir,
  - las pérdidas que se pueden generar
  - y la probabilidad de su ocurrencia
- **Diseño política de seguridad**
  - definir responsabilidades y reglas a seguir para evitar tales amenazas o
  - minimizar sus efectos en caso de que se produzcan
- **Implementación**
  - usar mecanismos de seguridad para implementar lo anterior

Lámina 19

Dr. Roberto Gómez C.

Pasos en un análisis de riesgos

**1. Identificación costo posibles pérdidas (L)**  
  
Identificar amenazas

**3. Identificar posibles acciones (gasto) y sus implicaciones. (B)**  
Seleccionar acciones a implementar.


**2. Determinar susceptibilidad.**  
La probabilidad de pérdida (P)

**¿  $B \leq P * L$  ?**


Se cierra el ciclo

Lámina 20

Dr. Roberto Gómez C.




Política de Seguridad




- Especifica las características de seguridad que un sistema debe observar y proveer
  - conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Especifica las amenazas contra las que la organización debe protegerse y cómo debe protegerse
- Depende de los objetivos y metas de la organización.
- Generalmente es expresada en un lenguaje o idioma.

Lámina 21

Dr. Roberto Gómez C.




Paradigmas




- *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.

Lámina 22

Dr. Roberto Gómez C.




### 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.

Lámina 23

Dr. Roberto Gómez C.



### ¿Que es un ataque?



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

Lámina 24

Dr. Roberto Gómez C.

## 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.

Lámina 25

Dr. Roberto Gómez C.

## Tipos de Ataques

### Ataques Pasivos.

### Ataques Activos.

Lámina 26

Dr. Roberto Gómez C.




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

Lámina 27

Dr. Roberto Gómez C.



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..






Lámina 28

Dr. Roberto Gómez C.





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

Lámina 29

Dr. Roberto Gómez C.




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

Lámina 30

Dr. Roberto Gómez C.



## 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.




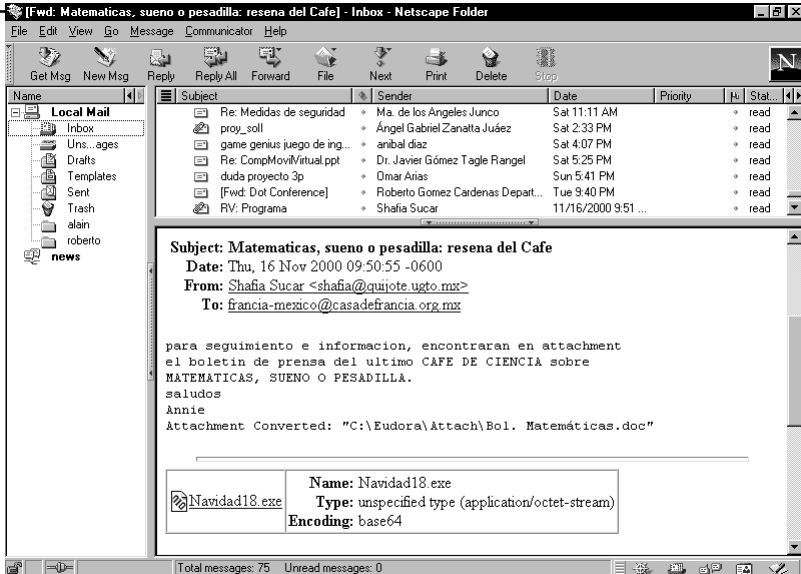


Lámina 31



## El gusano navidad.exe (1)







The screenshot shows a Netscape Messenger window titled "[Fwd: Matematicas, sueño o pesadilla: resena del Cafe] - Inbox - Netscape Folder". The email list shows a message from "Shafia Sucar" dated "11/16/2000 9:51 ...". The email content includes the subject "Matematicas, sueño o pesadilla: resena del Cafe", the date "Thu, 16 Nov 2000 09:50:55 -0600", and the sender "Shafia Sucar <shafia@quiote.upto.mx>". The email body mentions a bulletin from CAFE DE CIENCIA and includes an attachment "Navidad18.exe" which is described as "Type: unspecified type (application/octet-stream)" and "Encoding: base64".

Lámina 32





## El gusano navidad.exe (2)



Local Mail

Inbox

Uns...ages

Drafts

Templates

Sent

Trash

alain

roberto

news

Name	Subject	Sender	Date	Priority	Stat...
TIE3 00489381		Toney Roa	09/04/2000 8:50...		read
TIE3 451838		Aldo Martínez	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: Pleto 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 Ortegón	09/08/2000 1:48...		read
Re: [linuxem] Re: Ayuda L...		Allan Baker Ortegón	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>, 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

Start


Triv...

2:44 PM

to Gómez C.



## El gusano navidad.exe (3)



Local Mail

Inbox

Uns...ages

Drafts

Templates

Sent

Trash

alain

roberto

news

Name	Subject	Sender	Date	Priority	Stat...
INVITACIONMININOVIE...		enesa@conectate.com.uy	11/19/2000 5:25...		read
Buenas Noches !!		Enika Mata Sanchez	11/20/2000 1:55...		replied
Il y a si longtemps que je ...		Eri	11/20/2000 10:29...		read
Saludos		Igor Sánchez	11/20/2000 11:55...		read
Re: emails		Dalia Mata Sánchez	11/20/2000 11:55...		read
Re: Buenas Noches !!		Enika Mata Sanchez	11/20/2000 1:13...		read

Subject: Re: Cuidado!!!!

Date: Fri, 17 Nov 2000 00:44:06 -0600

From: Shafia Sucar <shafia@quijote.ugto.mx>

To: "Salvador G. Medina" <adan@servidor.unam.mx>

CC: francia-mexico@casadefrancia.org.mx

References: 1

Estimados Lectores,

Lamento mucho haber sido la culpable de que mensajes que yo No envíe, 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


Triv...

2:38 PM

to Gómez C.




## 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

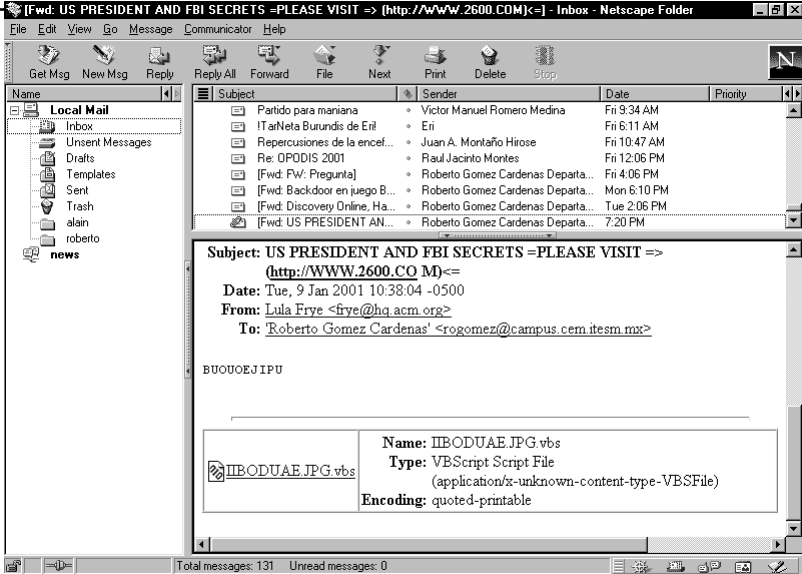
Lámina 35
Dr. Roberto Gómez C.



## Otro ejemplo virus/gusano




---




The screenshot shows an email client interface with a list of messages on the left and a detailed view of a selected message on the right. The selected message has the subject 'Fwd: US PRESIDENT AND FBI SECRETS =PLEASE VISIT => (http://WWW.2600.COM)<=' and contains a VBScript file named 'IIBODUAE.JPG.vbs'. The email header shows it was sent by 'Lula Frye' to 'Roberto Gomez Cardenas' on January 9, 2001.

Lámina 36
Dr. Roberto Gómez C.



## Viendo las consecuencias ...



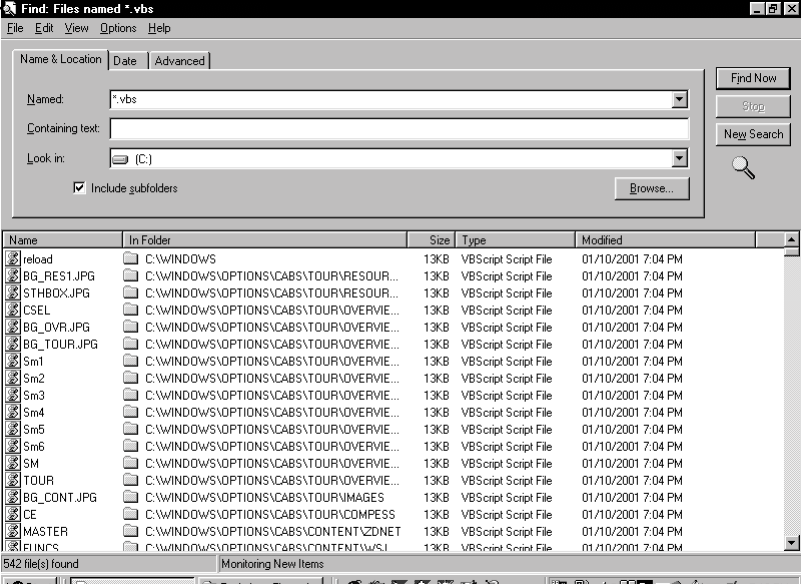




Lámina 37




## 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

Lámina 38

Dr. Roberto Gómez C.





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

Lámina 39

Dr. Roberto Gómez C.




Por último, pero no menos importante


- 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 llego por correo electrónico?
  - verificar el origen del correo
  - ¿conozco a la persona que lo envio?
  - ¿en realidad necesito el archivo que viene con el correo?
  - ¿acaso yo pedi dicho archivo?

Lámina 40

Dr. Roberto Gómez C.




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
  - acroread, real player, etc
  - fondos de pantalla
  - protectores de pantalla

Lámina 41

Dr. Roberto Gómez C.




Riesgos plugins




- 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)

Lámina 42

Dr. Roberto Gómez C.



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.

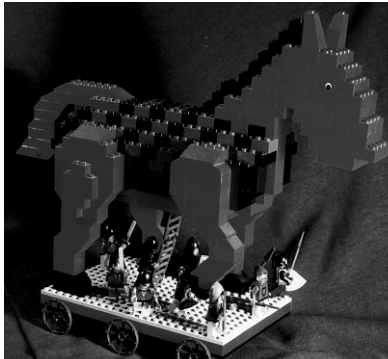




Lámina 43



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

Lámina 44

Dr. Roberto Gómez C.




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.

Lámina 45

Dr. Roberto Gómez C.



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.






Lámina 46

Dr. Roberto Gómez C.





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

Lámina 47

Dr. Roberto Gómez C.




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.


Lámina 48

Dr. Roberto Gómez C.






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.

Lámina 49

Dr. Roberto Gómez C.




Algunos ejemplos de hoax




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

Lámina 50

Dr. Roberto Gómez C.



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 ENFERMEDAD 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.

Lámina 51

Dr. Roberto Gómez C.



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

Lámina 52

Dr. Roberto Gómez C.



# ¿Y para que quiere alguien direcciones electrónicas?



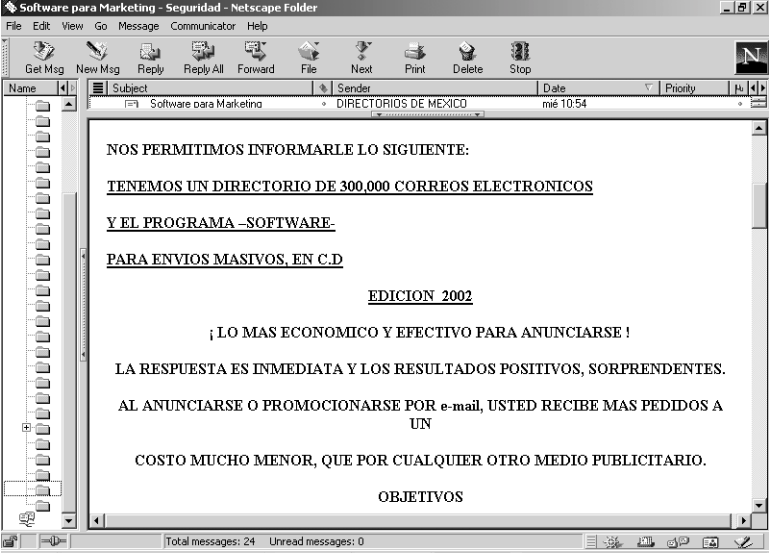




Lámina 53

19:18 Roberto Gómez C.



# ¿Y es negocio?



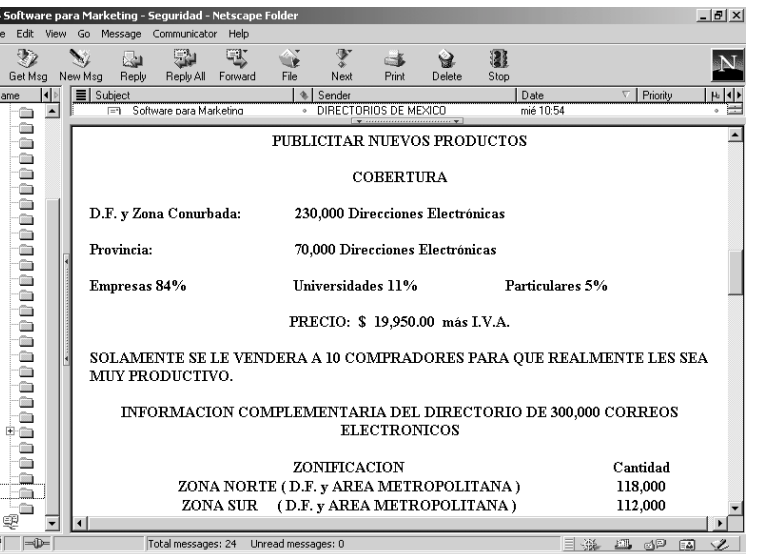




Lámina 54

19:19 Roberto Gómez C.



## 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..

Lámina 55Dr. Roberto Gómez C.



## Spam



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






Lámina 56



## Ejemplo SPAM



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

File Edit View Go Message Communicator Help

Name	Subject	Sender	Date	Priority	Is	Status
Bonjour II		Enka Mala 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.itemc.mx>

*Estimado amigo:*

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



Escribanos a: [clasificadorrural@ciudad.com.ar](mailto:clasificadorrural@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 profesión a esta trascendente actividad. A través de <http://www.clasificadorrural.com> Ud. podrá en forma sencilla, amigable y eficiente ofrecer sus productos y servicios y consultar la mejor oferta en el país para sus negocios y necesidades.


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

Total messages: 113    Unread messages: 0

Lámina 57 Dr. Roberto Gómez C.




## ¿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

Lámina 58 Dr. Roberto Gómez C.




## 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, pena, inocencia de la gente, relaciones humanas, etc.



Dr. Roberto G

Lámina 59



## Ejemplos Ingeniería Social





### Cuídate de los hackers con piel de oveia

Empleados de importantes empresas mexicanas revelan sin objeción sus passwords, arriesgando la integridad de los sistemas de las compañías

- “No sé si usted me pueda ayudar, es que soy de sistemas y estamos teniendo problemas con la red, ¿no la ha notado un poco lenta?”
- “Pues sí, algo, si se siente lenta”.
- “Es que tenemos un problema con un servidor, estamos chequeando todos los usuarios, ¿cuál es tu nombre de usuario?”
- “Gracias... no, no aparece, ¿me puedes dar tu clave?”
- “No, ¿para qué?”.
- “Nada más para ver si te puedo dar de alta po, no te apures, si quieres luego la cambiamos, es que si no arreglo esto rápido me van a echar una bronca”.
- “Órale, gracias... pa quedó”.

#### Cambio de password

“¿Hola? ¿Sistemas? Soy Juan Pérez, de contabilidad. Oye, perdí mi password, ¿me podrías cambiarlo? Gracias! Sí, que el password nuevo sea...”.

#### IRC y mensajería instantánea

ATENCIÓN: Has sido infectado con un virus que permite que los hackers se metan en tu máquina y lean tus archivos, etc. Te sugiero que bajes este archivo y limpies tu máquina. El archivo está en...

#### Por teléfono

¿Juan Pérez? Hola, soy Pedro López, de sistemas; tuvimos un problema con tu cuenta, parece que se corrompió el archivo de passwords. ¿Te pudiste conectar bien hoy? Ajá, perfecto. A ver, tu nombre de usuario es ¿perez, verdad? ¿Y tu password es perez01? ¿No? Ah, ese es el problema, ¿me puedes decir tu password?

#### Correo electrónico


De: soporte@correo.com  
Para: jperez@correo.com

Estimado señor Pérez:


Lamentamos informarle que su cuenta de correo presenta un problema. Para realizar una revisión, requerimos que nos responda a este mensaje, enviando su nombre de usuario y su password. La revisión es gratuita, y en menos de 24 horas podremos arreglar el problema. Agradecemos la atención prestada a la presente”.

#### Activación

Los nombres de usuario y passwords obtenidos vía telefónica no se escribieron en ninguna parte, por lo que Grupo Reforma no guarda registro de ellos.




Medidas a tomar




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

Lámina 61

Dr. Roberto Gómez C.



Graffiti

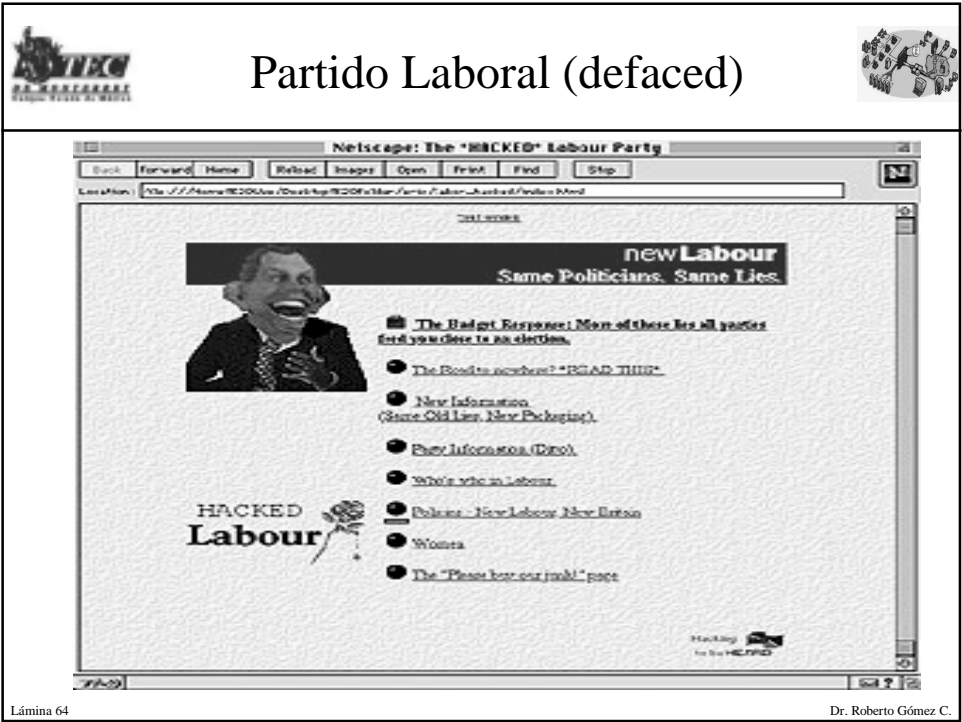
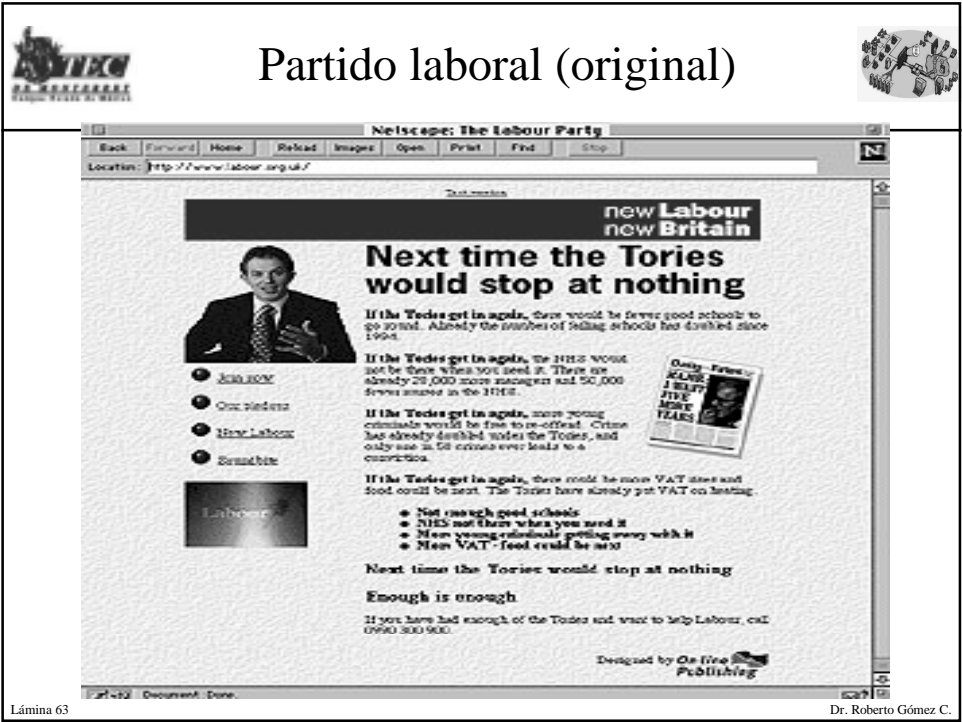


- Consiste en susbtituir páginas de un organismo por otras.
- El objetivo es dañar la reputación de la empresa
- Este tipo de ataques no tiene un periodo de duración grande

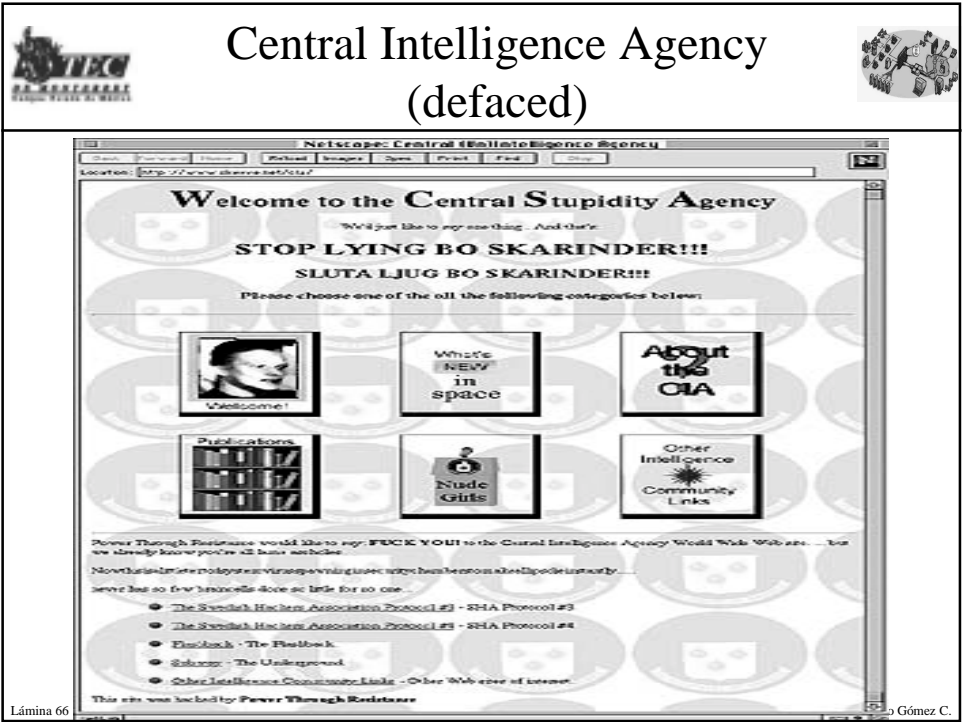
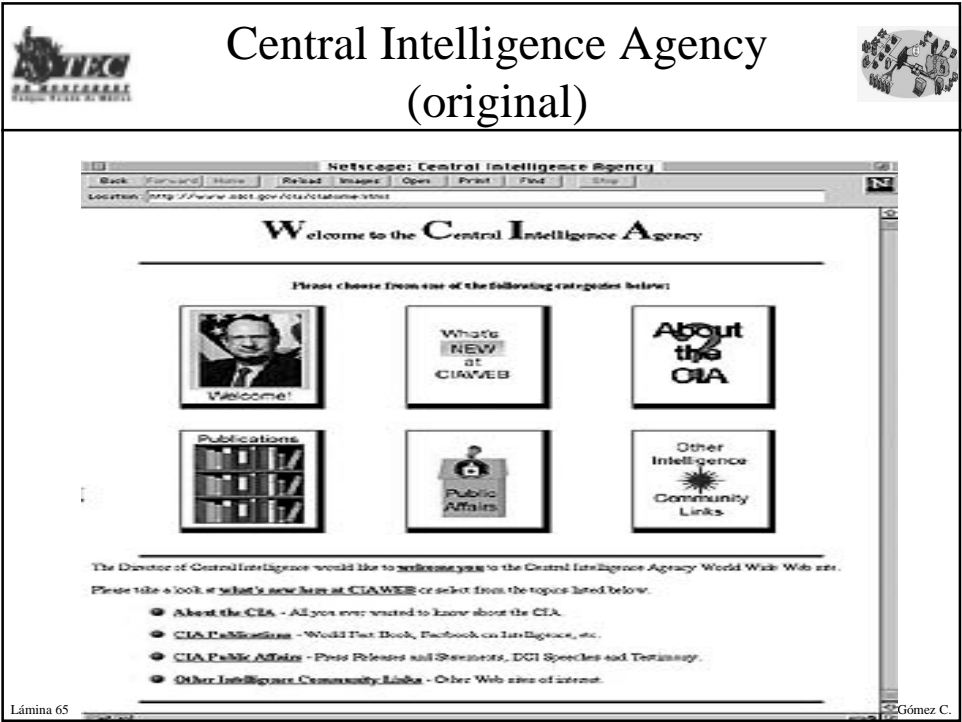
Lámina 62

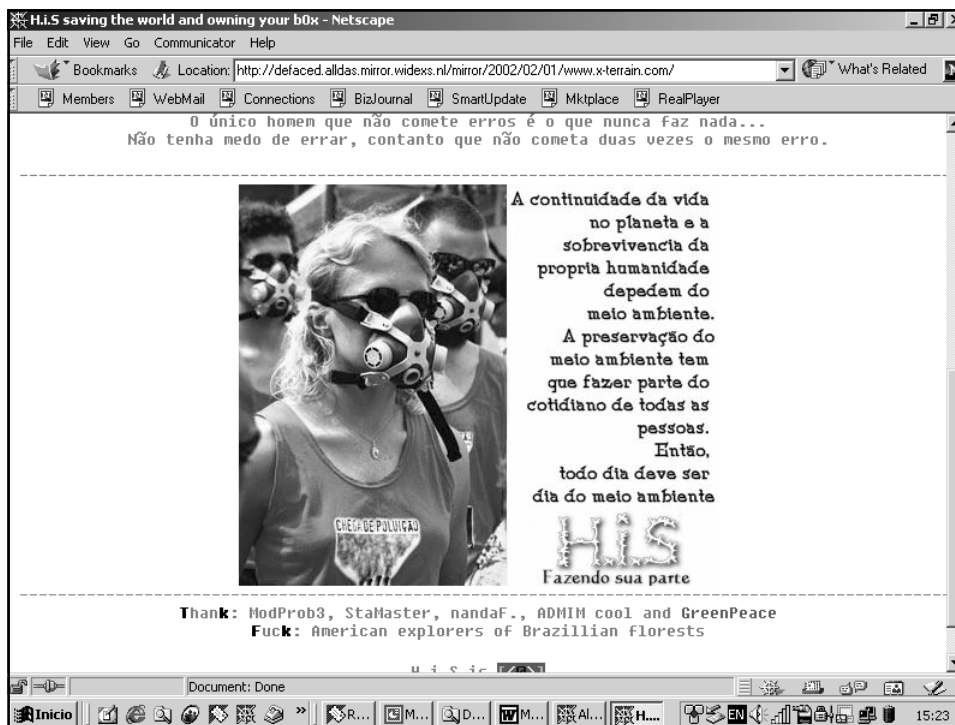
Dr. Roberto Gómez C.















## Defaced pages



- Primero fue attrition
  - <http://www.attrition.org>
- Después fue alldas
  - <http://defaced.alldas.de/>
- Ahora es:
  - <http://www.zone-h.org/defacements/onhold>

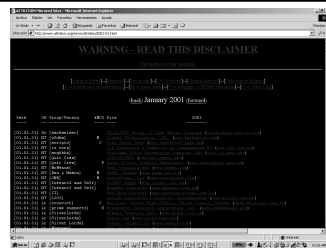
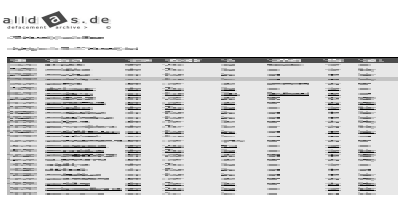
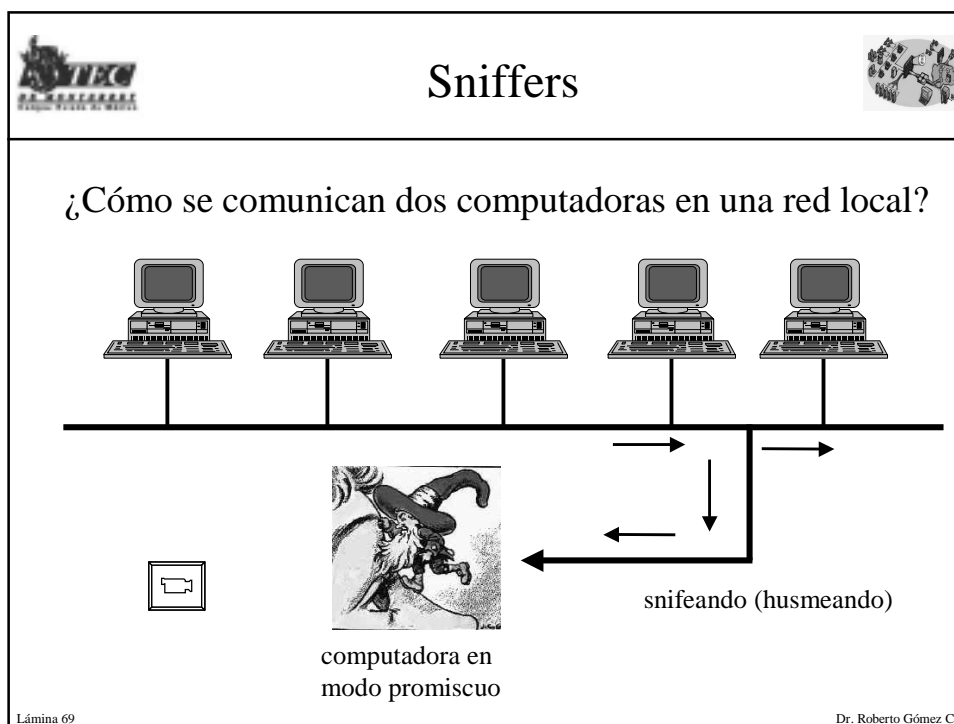






Lámina 68
Dr. Roberto Gómez C.




 **¿Y como me protejo de los sniffers?** 

- Programas de detección sniffers
  - detección muy pobre
- Redes switcheadas
  - sniffers activos
- Encriptación
  - IPSec
  - SSL
  - SSH

Lámina 70 Dr. Roberto Gómez C.

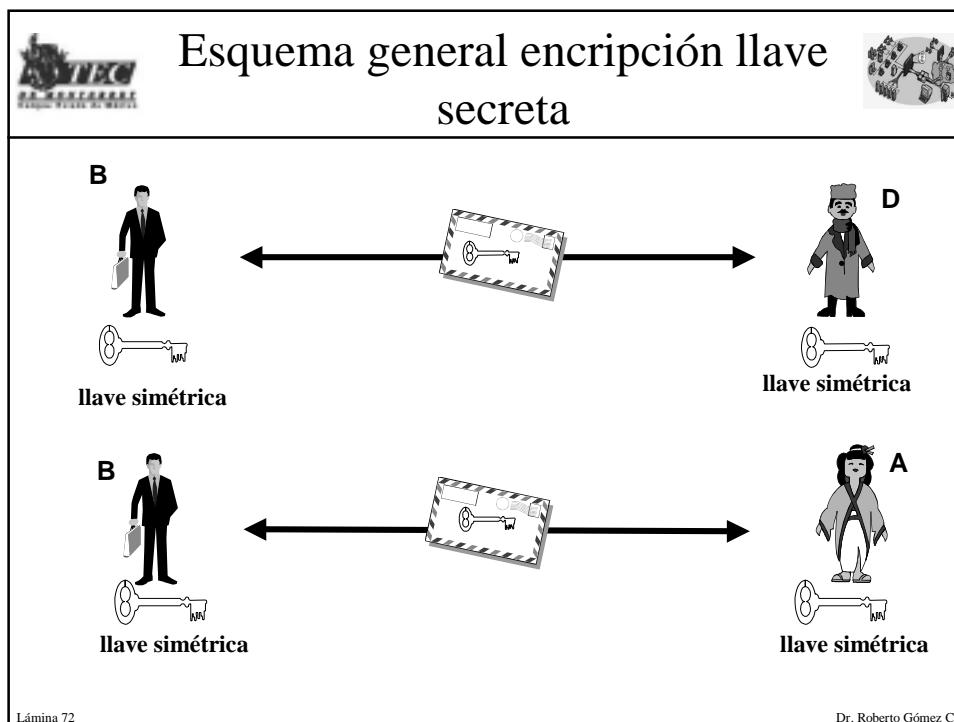


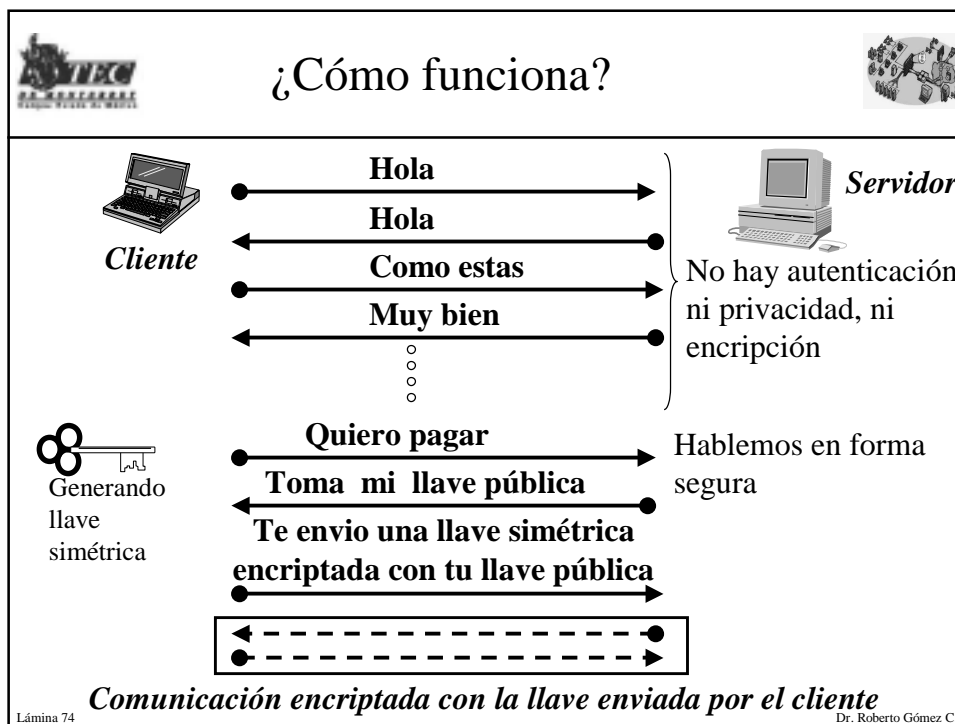
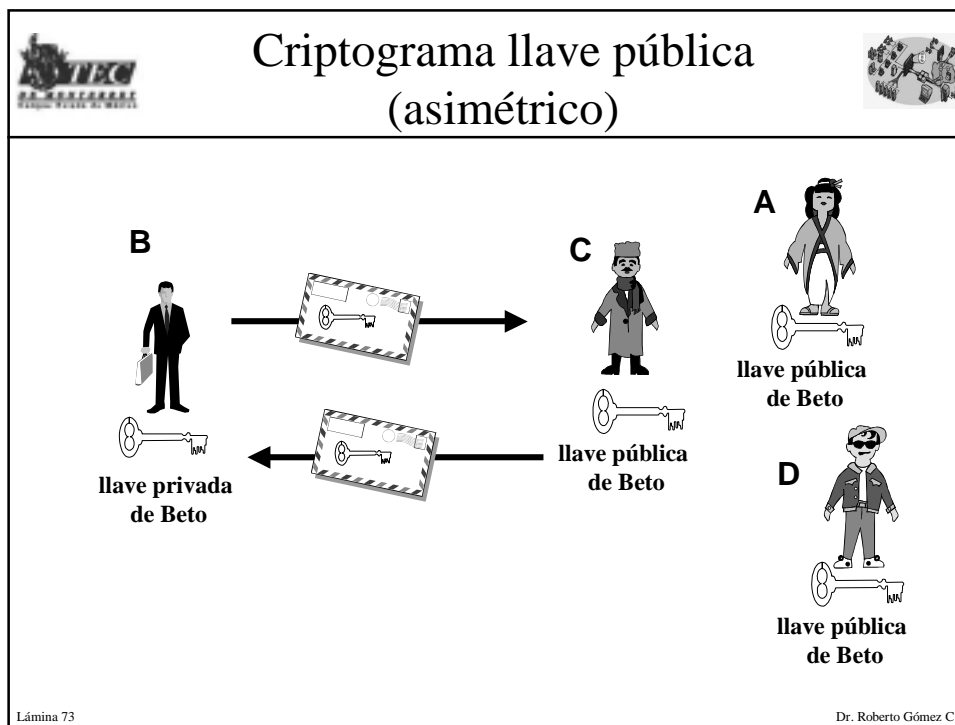
Métodos Criptográficos

- Métodos simétricos
  - llave encriptado coincide con la de descifrado
  - la llave tiene que permanecer secreta
  - emisor y receptor se han puesto de acuerdo previamente o existe un centro de distribución de llaves
  - son propios de la criptografía clásica o criptografía de llave secreta
- Métodos asimétrico
  - llave encriptado es diferente a la de descifrado
  - corresponden a la criptografía de la llave pública, introducida por Diffie y Hellman en 1976

Lámina 71

Dr. Roberto Gómez C.





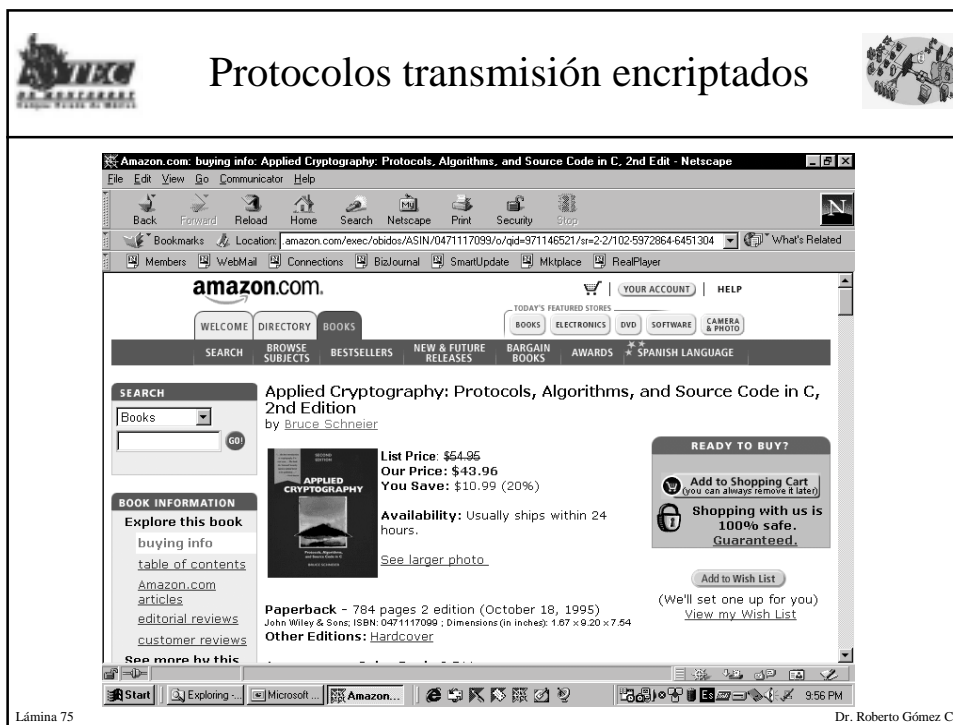


Lámina 75

Dr. Roberto Gómez C.

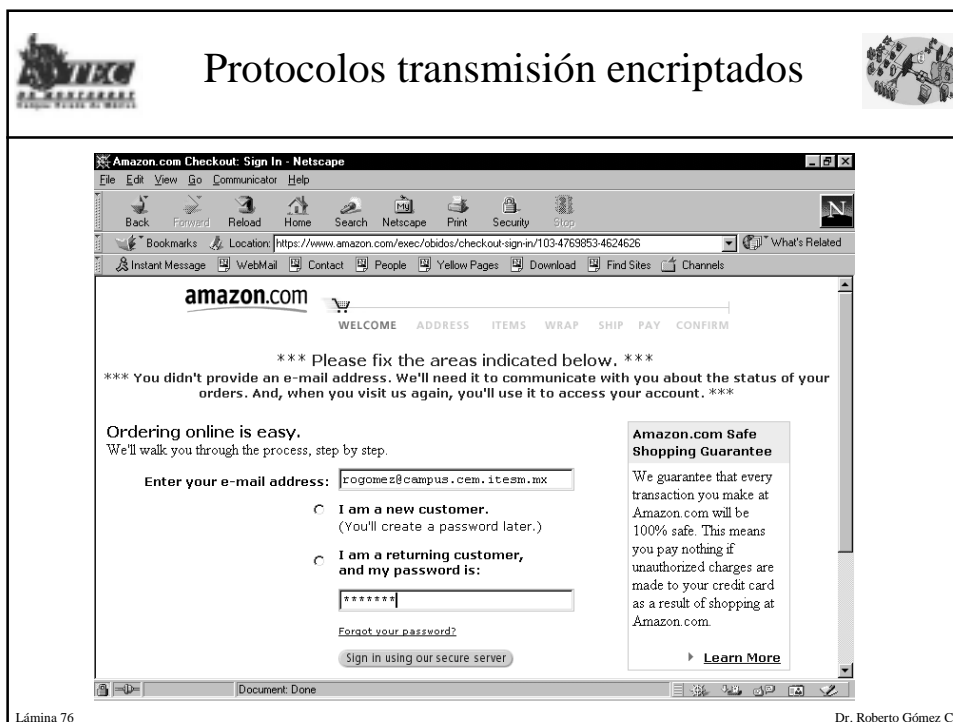

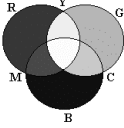


Lámina 76

Dr. Roberto Gómez C.



Esteganografía??



- Area similar a la de criptología.
- Viene del griego stegos (ocultar).
- Conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos.
- La información puede esconderse de cualquier forma
  - esconder documentos electrónicos dentro de imagenes.
  - aprovechar campos no usados de los paquetes de protocolos de redes.

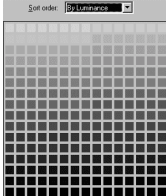


Lámina 77

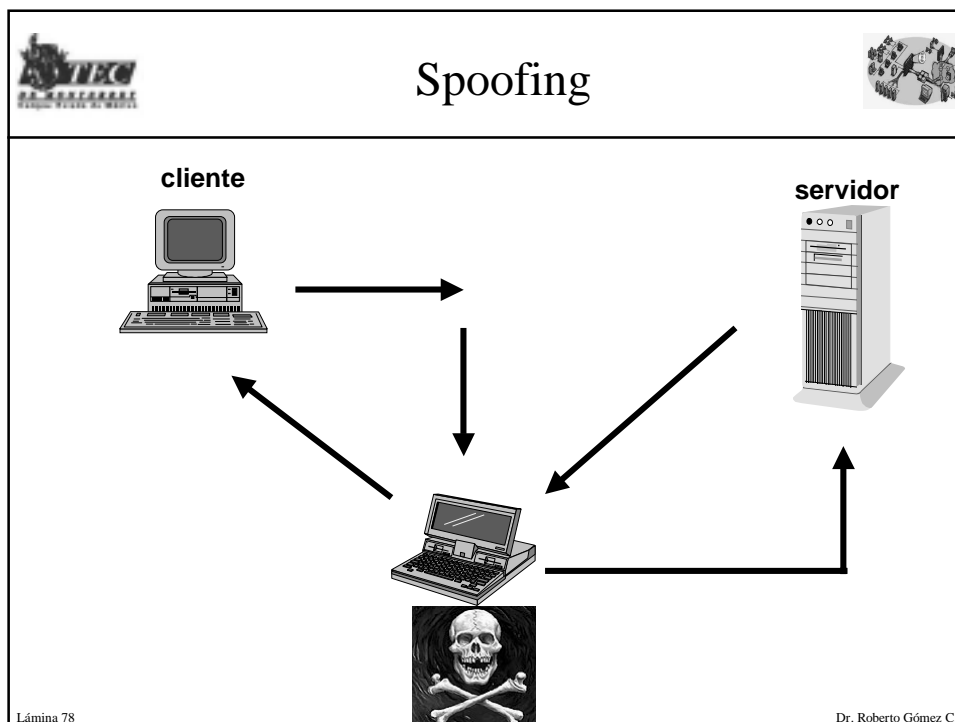




Lámina 79

Dr. Roberto Gómez C.

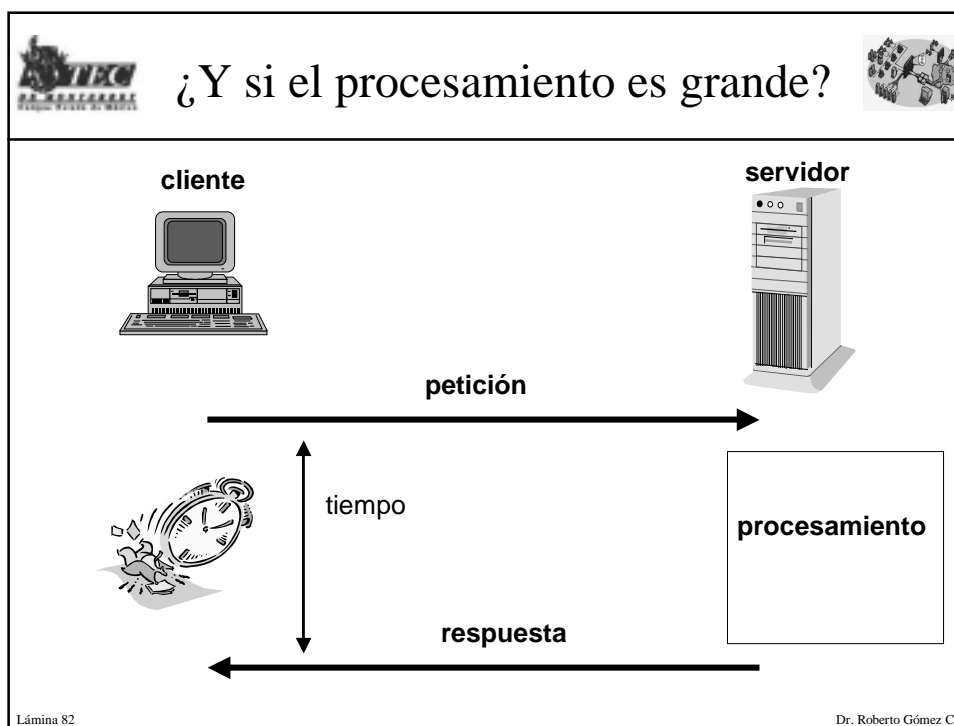
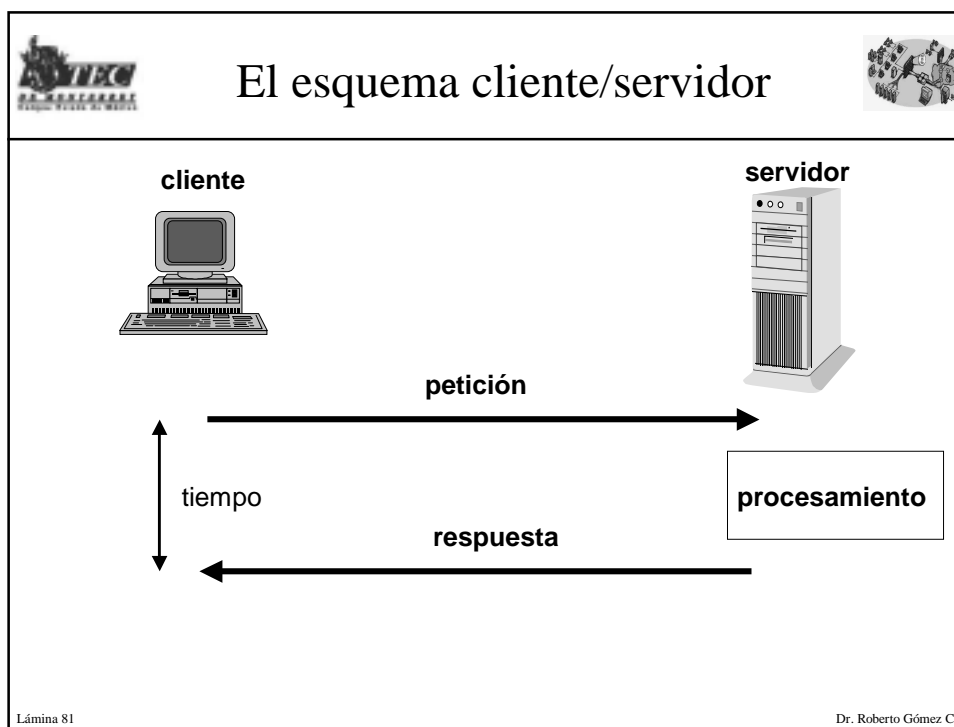
## El código móvil

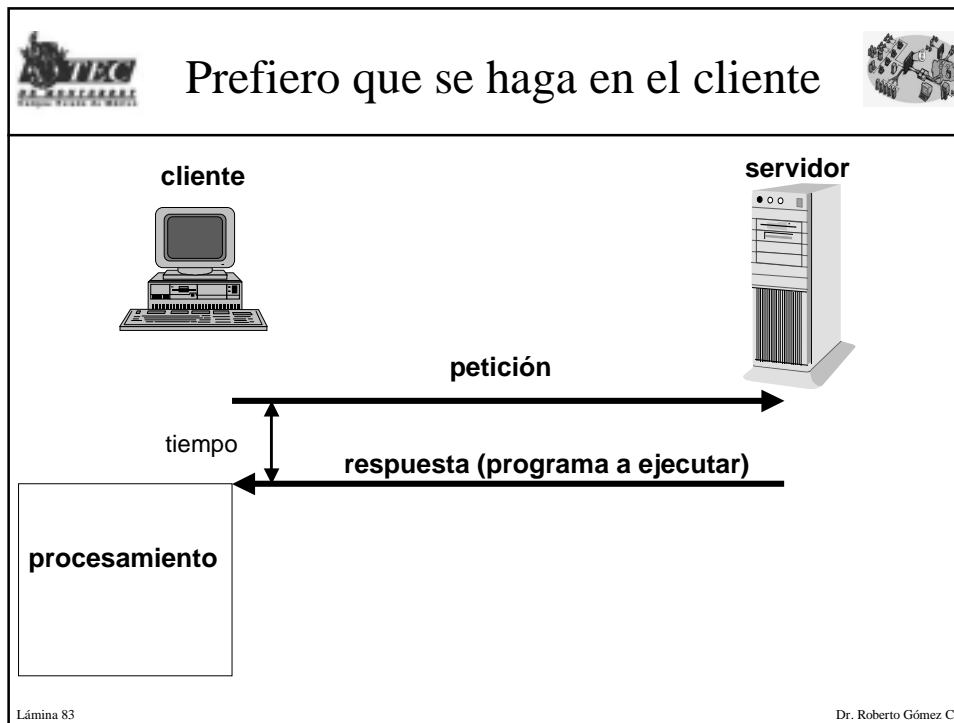
- Los *browsers* son la herramienta que usan los usuarios para navegar por internet.
- Dos elementos fundamentales en internet:
  - cliente: el que realiza la búsqueda de información
  - servidor: el que coloca la información en algún servidor
- Cuando la aplicación en el servidor es muy pesada
  - preferible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

Lámina 80

Dr. Roberto Gómez C.








¿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

Lámina 84

Dr. Roberto Gómez C.



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

Lámina 85

Dr. Roberto Gómez C.




Configuración Microsoft Internet Explorer






Lámina 86

Dr. Roberto Gómez C.




## Protegiendo el perímetro




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

Lámina 87 Dr. Roberto Gómez C.



## Autenticación



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

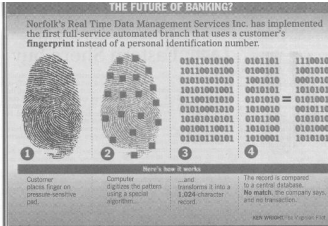
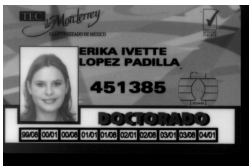



Lámina 88 Dr. Roberto Gómez C.

Control de acceso

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

Lámina 89


Roberto Gómez C.

Filtrando la información


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

Lámina 90

Dr. Roberto Gómez C.



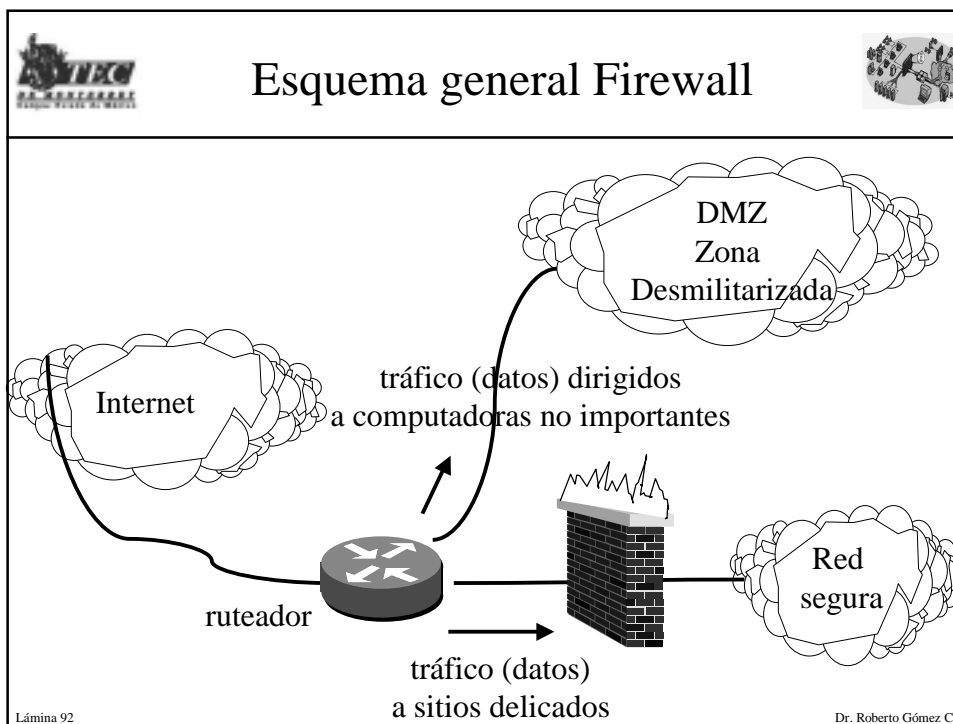
¿Qué es un firewall?




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


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

Lámina 91 Dr. Roberto Gómez C.





## Ejemplo reglas de acceso



**Demonstration - FireWall-1 Security Policy**

File Edit View Manage Policy Window Help


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

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


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

MAIN MENU EXIT

Lámina 93 Gómez C.

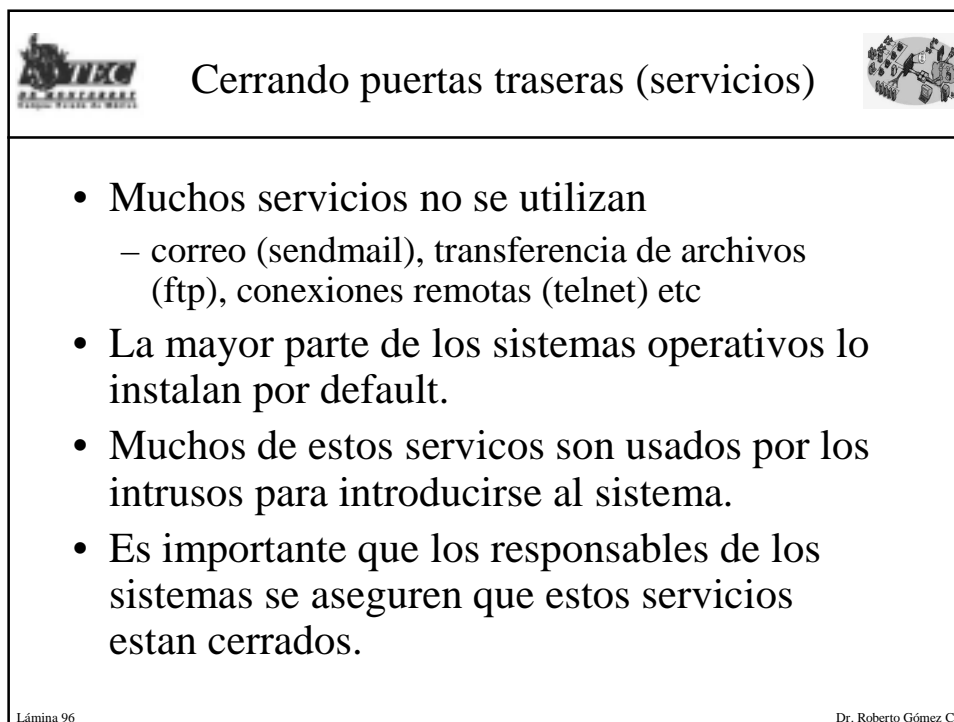
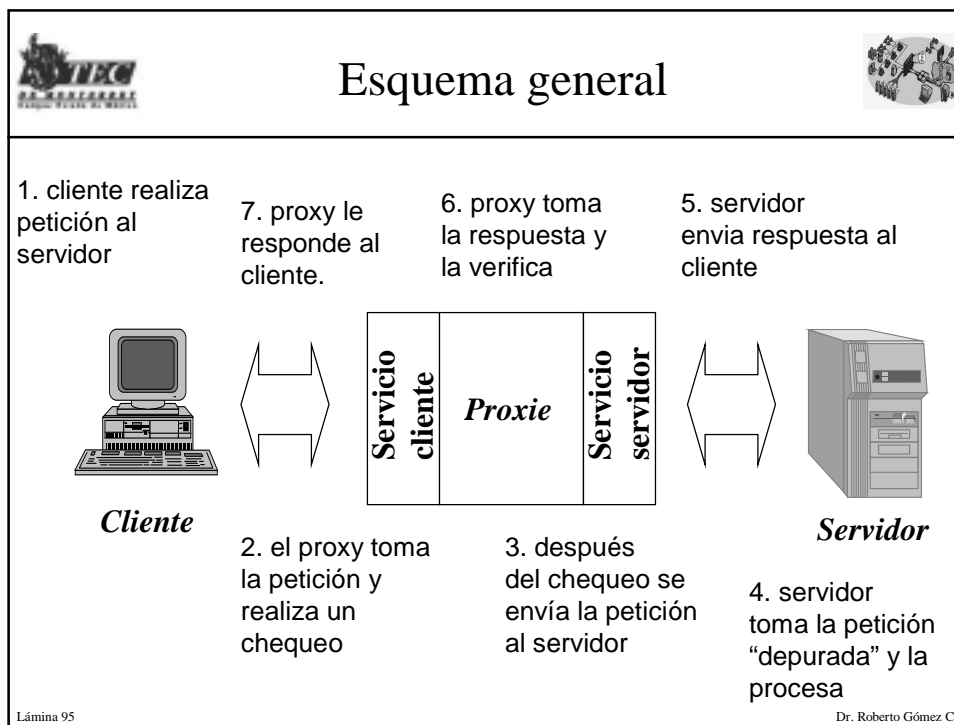


## ¿Qué quiere hacer adentro: proxies?




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


Lámina 94 Dr. Roberto Gómez C.







Cerrando puertas traseras (conexiones)



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






Lámina 97

Dr. Roberto Gómez C.



¿Y si contratamos vigilantes?



# IDS



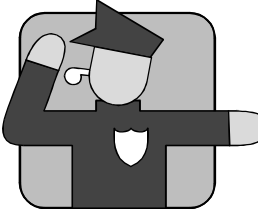




Lámina 98

Dr. Roberto Gómez C.

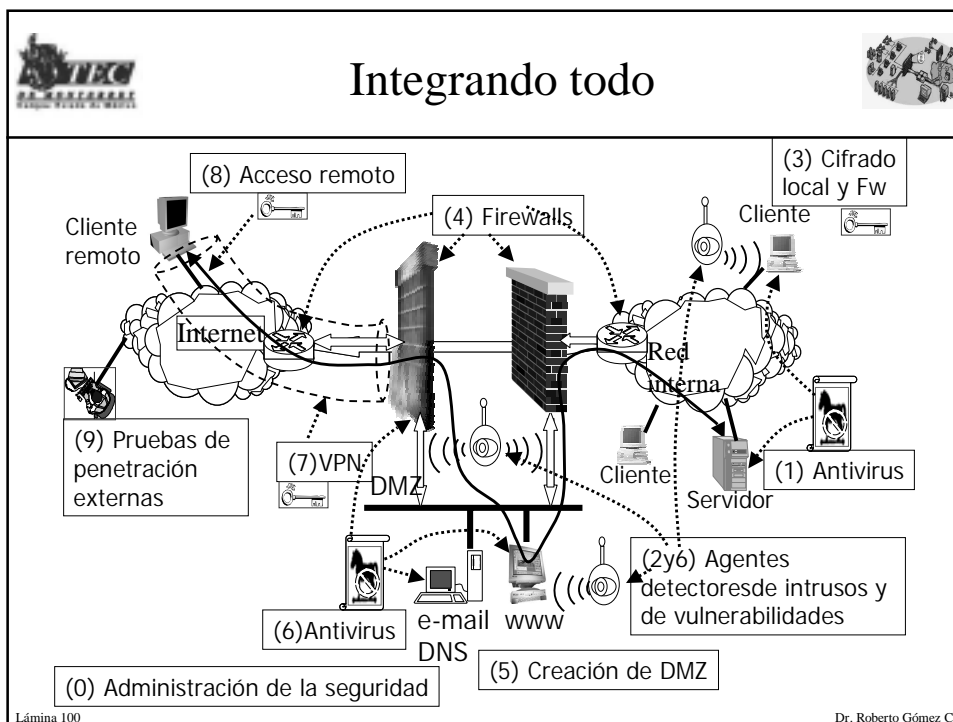


## IDS



- Intrusion Detection Systems.
- Software específicamente diseñado para reconocer los patrones de un comportamiento no deseado.
- Pueden proporcionar un medio para registrar intentos, detener intentos en progreso y cerrar hoyos que coincidan con algunos patrones de ataques, bloqueando la secuencia para que ya no ocurra.
- Busca automatizar la detección y eliminación de intrusos.

Lámina 99
Dr. Roberto Gómez C.



¿Y las redes inalámbricas?

- El medio de transmisión más utilizado es el cable, pero para el caso de una red inalámbrica ese medio físico es el aire.
- WLAN: Siglas en inglés de Wireless Local Area Network.

Lámina 101


Dr. Roberto Gómez C.


Riesgos de una WLAN

- Monitoreo de tráfico inalámbrico
  - datos de usuarios
  - localización de usuarios
  - identidad de usuarios
  - análisis de tráfico
- Acceso no autorizado a una red a través de un enlace inalámbrico
  - persona pasaendose en una bicicleta
- Corrupción de servicios inalámbricos
- Descubrimiento
  - wardriving

Lámina 102

Dr. Roberto Gómez C.



Consejos

- Habilitar WAP
  - si no es posible habilitar WEP con llave de 104 bits (128 bits)
- Conectar los Access Points en una zona de seguridad “pública” (ó de bajo riesgo) posiblemente en una DMZ, jamás conectar la red inalámbrica a la red alámbrica de manera transparente.
- Implementar un segundo nivel de seguridad:
  - VPN
  - IPSEC
  - SSL
  - SSH

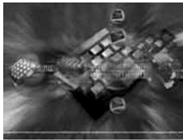




Lámina 103

Dr. Roberto Gómez C.





Conclusiones y Recomendaciones

- 100% de seguridad **no existe!!!!**
- Seguridad a través de educación.
- Programas de seguridad integral.
- Contar con una caja de herramientas
- Creación de departamentos o divisiones especializados en seguridad computacional.
- Leer, leer, leer...
- Estar al segundo en cuestiones de seguridad.
- Los ataques tienen estructura, por lo tanto se pueden detectar en su mayoría.

Lámina 104



Dr. Roberto Gómez C.



## Páginas para mayor información

- Security Focus: [www.securityfocus.com](http://www.securityfocus.com)
- CERT : [www.cert.org](http://www.cert.org)
- SANS: [www.sans.org](http://www.sans.org)
- Securiteam: [www.securiteam.com](http://www.securiteam.com)
- Snort: [www.snort.com](http://www.snort.com)
- ISS: [www.iss.net](http://www.iss.net)
- Página seguridad RSA: [www.rsasecurity.com](http://www.rsasecurity.com)
- Cypherpunks: [www.vnunet.com](http://www.vnunet.com)
- Bruce Schneider: [www.counterpane.com](http://www.counterpane.com)
- Security Space: [www.securityspace.com](http://www.securityspace.com)
- Ernst&Young: [www.esecurityonline.com](http://www.esecurityonline.com)

Lámina 105 Dr. Roberto Gómez C.



# Gracias por su atención

## Panorama general de los principales ataques y defensas de un sistema informático

Roberto Gómez  
[rogomez@itesm.mx](mailto:rogomez@itesm.mx)  
<http://webdia.cem.itesm.mx/ac/rogomez>

Lámina 106 Dr. Roberto Gómez C.