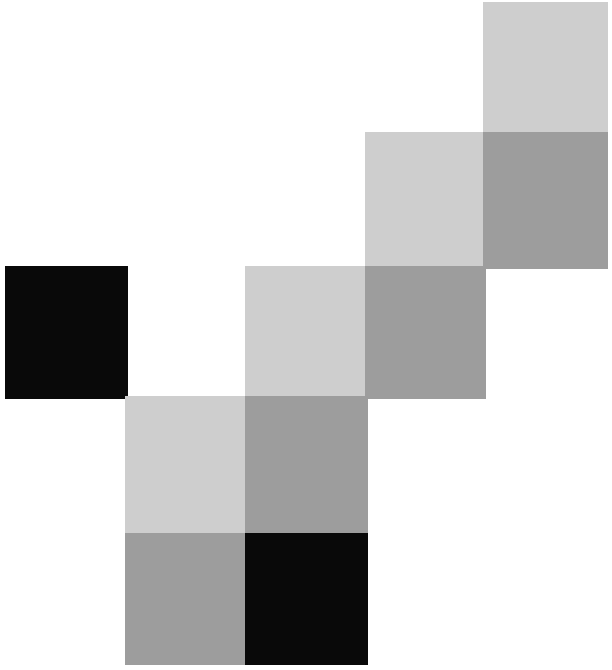


Introducción a la Seguridad de la Información

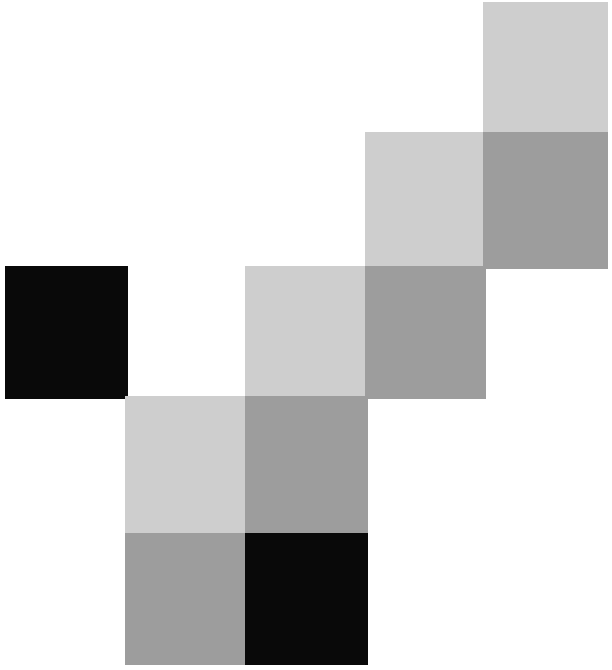
Juan Carlos Oré
juancarlosore@yahoo.com
Junio 2006

Contenido

1. Situación actual de la Seguridad
   a. Panorama
   b. Casos
   c. Mitos
2. Elementos de la Seguridad
   a. Pilares
   b. Tipos de atacantes
   c. Tipos de ataques

Contenido (cont.)

3. Defensa
   a. Firewalls
   b. IDS
   c. Criptografía
   d. VPN
4. Recomendaciones

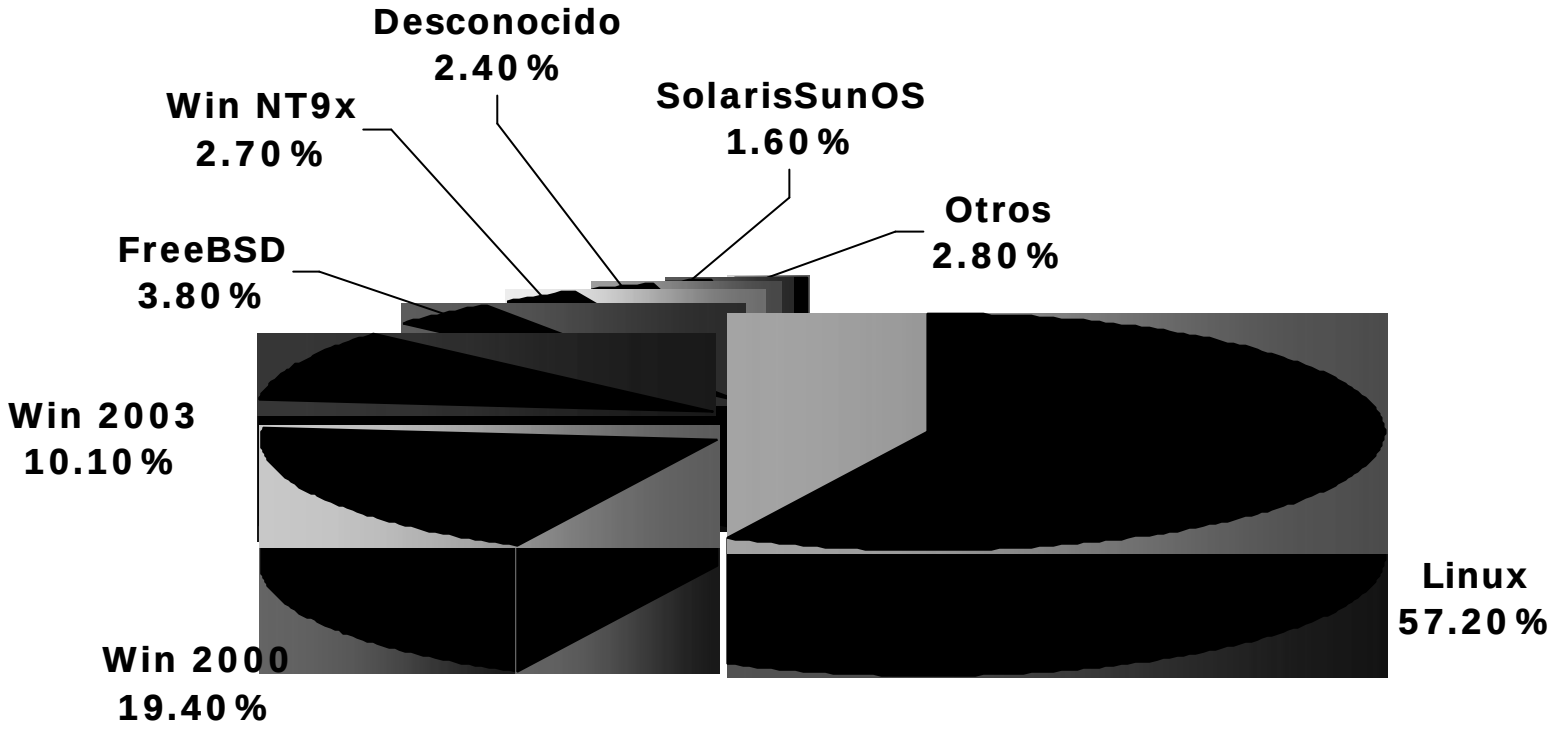


Situación actual de la Seguridad

Contenido

1. Situación actual de la Seguridad
   a. **Panorama**
   b. Casos
   c. Mitos
2. Elementos de la Seguridad
   a. Pilares
   b. Tipos de atacantes
   c. Tipos de ataques

Ataques registrados en Zone-H por S.O.



Fuente: www.zone-h.org

Ejemplos Ataques

ANTES

London Real Estate and Loan :: Contra Costa, Alameda, and East Bay Premiere Realtor - Microsoft Internet Explorer

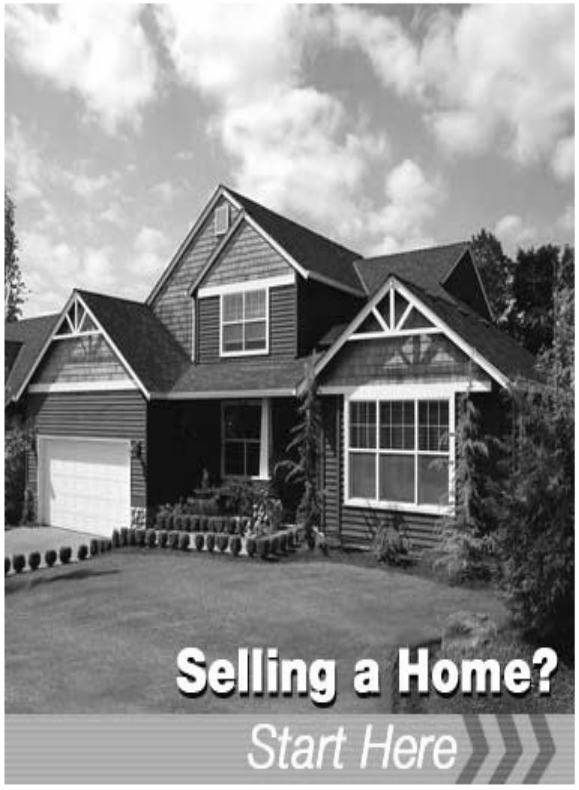
File Edit View Favorites Tools Help

Back Search Favorites

Address http://web.archive.org/web/20040927170921/http://lreal.com/ Go Links Norton Internet Security

LONDON
Real Estate & Loan

LOAN PROGRAMS | ABOUT LONDON | CONTACT | SEARCH FOR HOMES > >



Internet

Ejemplos Ataques

DESPUÉS

Ejemplos Ataques

ANTES

Absolute Career Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://web.archive.org/web/20050305092436/http://www.absolutecareer.com/ Go Links Norton Internet Security

Absolute Career Services

Kickstart Your Career! Call 312-222-9966

Home | Topics | FAQ | Services | Success Stories | Testimonials | Products | Contact Us

: Home

? OUR MISSION ?

MAKE YOUR JOB SEARCH VICTORIOUS!

Finding employment at a salary worth your value is like waging war. Job-search success is based on the quality of your weapons. For 15 years we've built a reputation as resume writers who craft quality weapons that win the employment war! It's worth noting, that though we are based in Chicago and Oak Park, Illinois, we often serve clients via email and fax across the U.S.

Main Menu

- Home
- FAQ
- Recommend Us
- Web Links
- Your Account
- Contact Us

Who's Online

There are currently, 3 guest(s) and 0 member(s) that are online.

You are Anonymous user. You can register for free by clicking here

Done Internet

Ejemplos Ataques

DESPUÉS

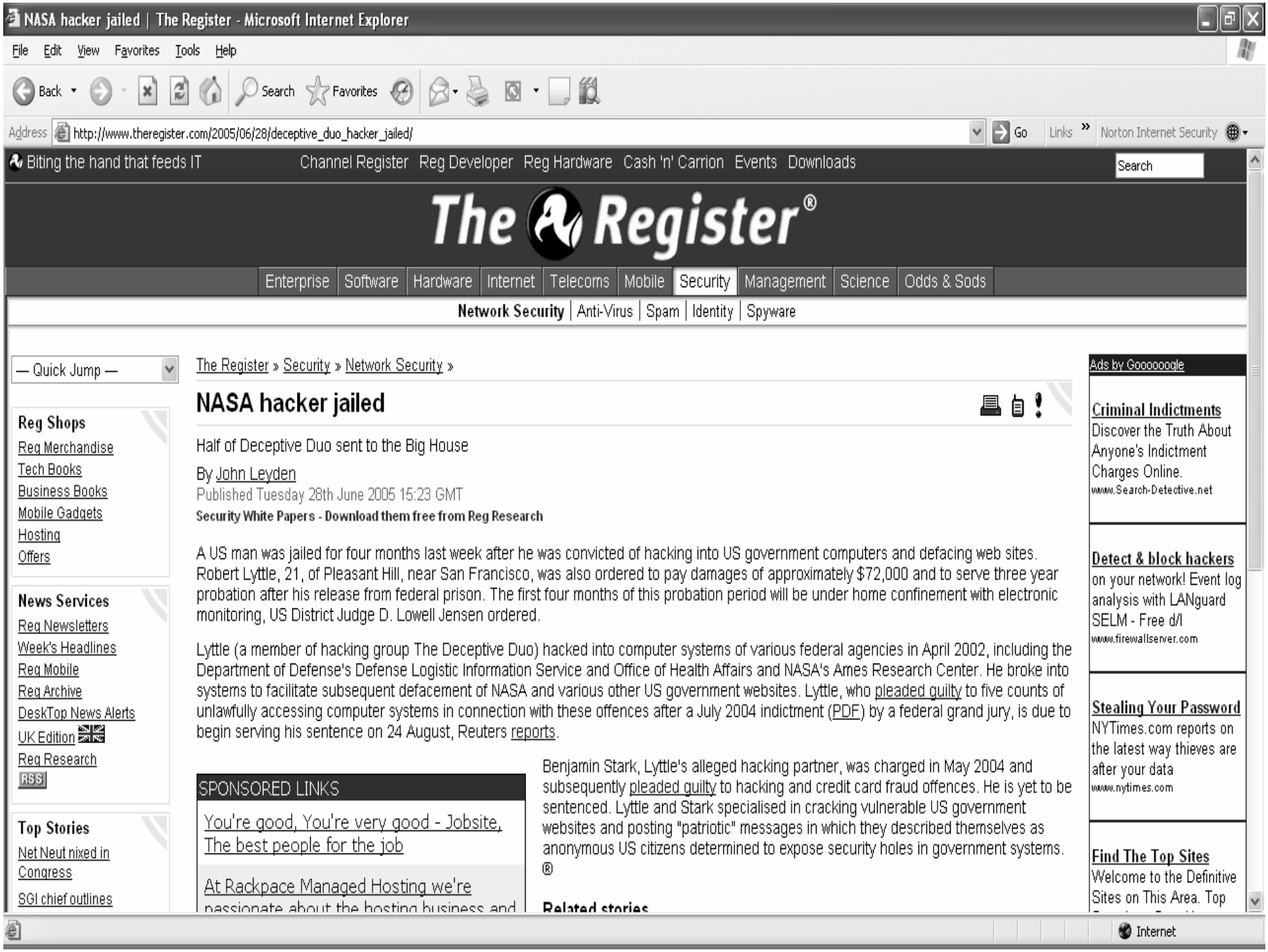
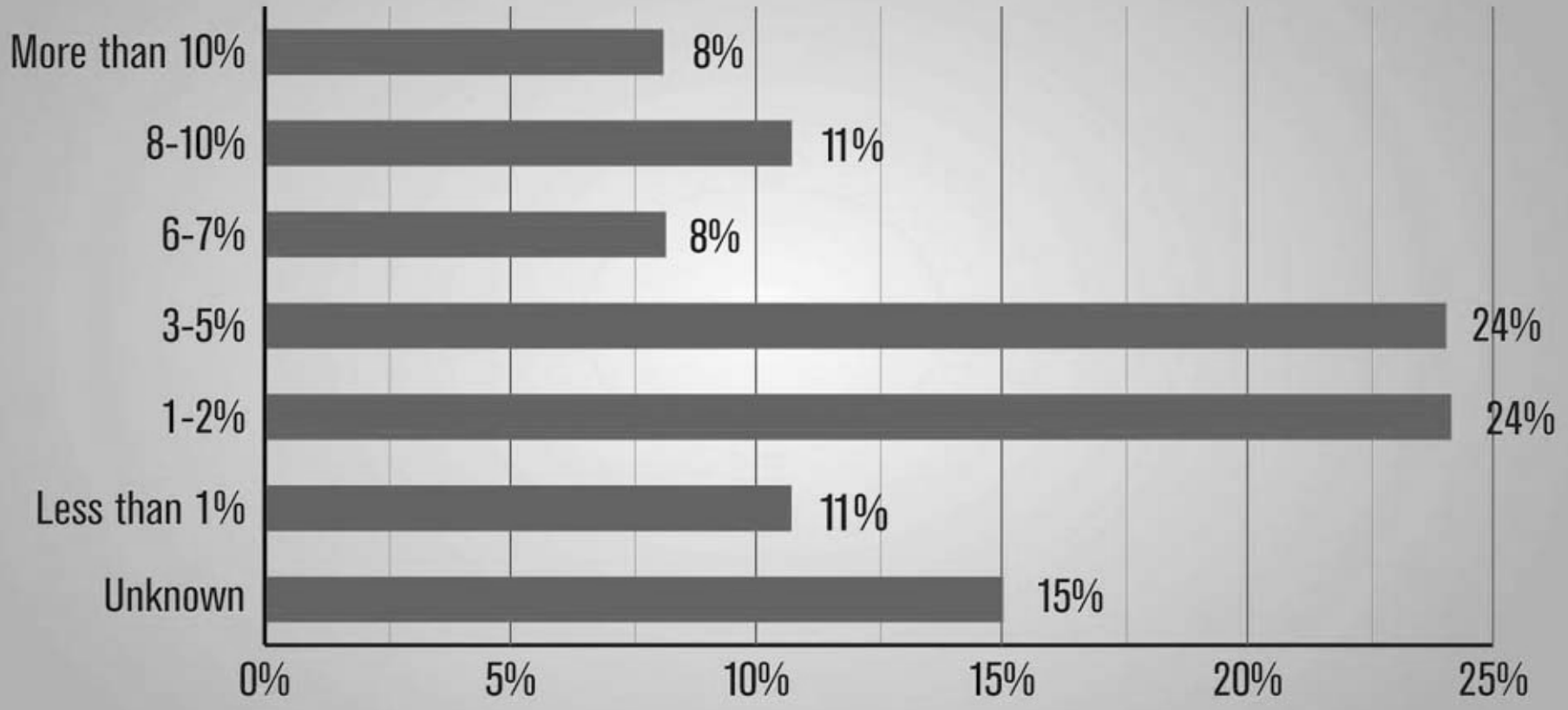

NASA hacker jailed | The Register - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.theregister.com/2005/06/28/deceptive_duo_hacker_jailed/
Go Links Norton Internet Security
Biting the hand that feeds IT
Channel Register Reg Developer Reg Hardware Cash 'n' Carrion Events Downloads
Search
The Register®
Enterprise Software Hardware Internet Telecoms Mobile Security Management Science Odds & Sods
Network Security | Anti-Virus | Spam | Identity | Spyware
— Quick Jump —
Reg Shops
Reg Merchandise
Tech Books
Business Books
Mobile Gadgets
Hosting
Offers
News Services
Reg Newsletters
Week's Headlines
Reg Mobile
Reg Archive
DeskTop News Alerts
UK Edition
Reg Research
RSS
Top Stories
Net Neut nixed in Congress
SGI chief outlines
The Register » Security » Network Security »
NASA hacker jailed
Half of Deceptive Duo sent to the Big House
By John Leyden
Published Tuesday 28th June 2005 15:23 GMT
Security White Papers - Download them free from Reg Research
A US man was jailed for four months last week after he was convicted of hacking into US government computers and defacing web sites. Robert Lyttle, 21, of Pleasant Hill, near San Francisco, was also ordered to pay damages of approximately $72,000 and to serve three year probation after his release from federal prison. The first four months of this probation period will be under home confinement with electronic monitoring, US District Judge D. Lowell Jensen ordered.
Lyttle (a member of hacking group The Deceptive Duo) hacked into computer systems of various federal agencies in April 2002, including the Department of Defense's Defense Logistic Information Service and Office of Health Affairs and NASA's Ames Research Center. He broke into systems to facilitate subsequent defacement of NASA and various other US government websites. Lyttle, who pleaded guilty to five counts of unlawfully accessing computer systems in connection with these offences after a July 2004 indictment (PDF) by a federal grand jury, is due to begin serving his sentence on 24 August, Reuters reports.
SPONSORED LINKS
You're good, You're very good - Jobsite, The best people for the job
At Rackpace Managed Hosting we're
Benjamin Stark, Lyttle's alleged hacking partner, was charged in May 2004 and subsequently pleaded guilty to hacking and credit card fraud offences. He is yet to be sentenced. Lyttle and Stark specialised in cracking vulnerable US government websites and posting "patriotic" messages in which they described themselves as anonymous US citizens determined to expose security holes in government systems. ®
Related stories
Ads by Goooooogle
Criminal Indictments
Discover the Truth About Anyone's Indictment Charges Online.
www.Search-Detective.net
Detect & block hackers
on your network! Event log analysis with LANguard SELM - Free d/l
www.firewallserver.com
Stealing Your Password
NYTimes.com reports on the latest way thieves are after your data
www.nytimes.com
Find The Top Sites
Welcome to the Definitive Sites on This Area. Top
Internet

Figure 5. Percentage of IT Budget Spent on Security

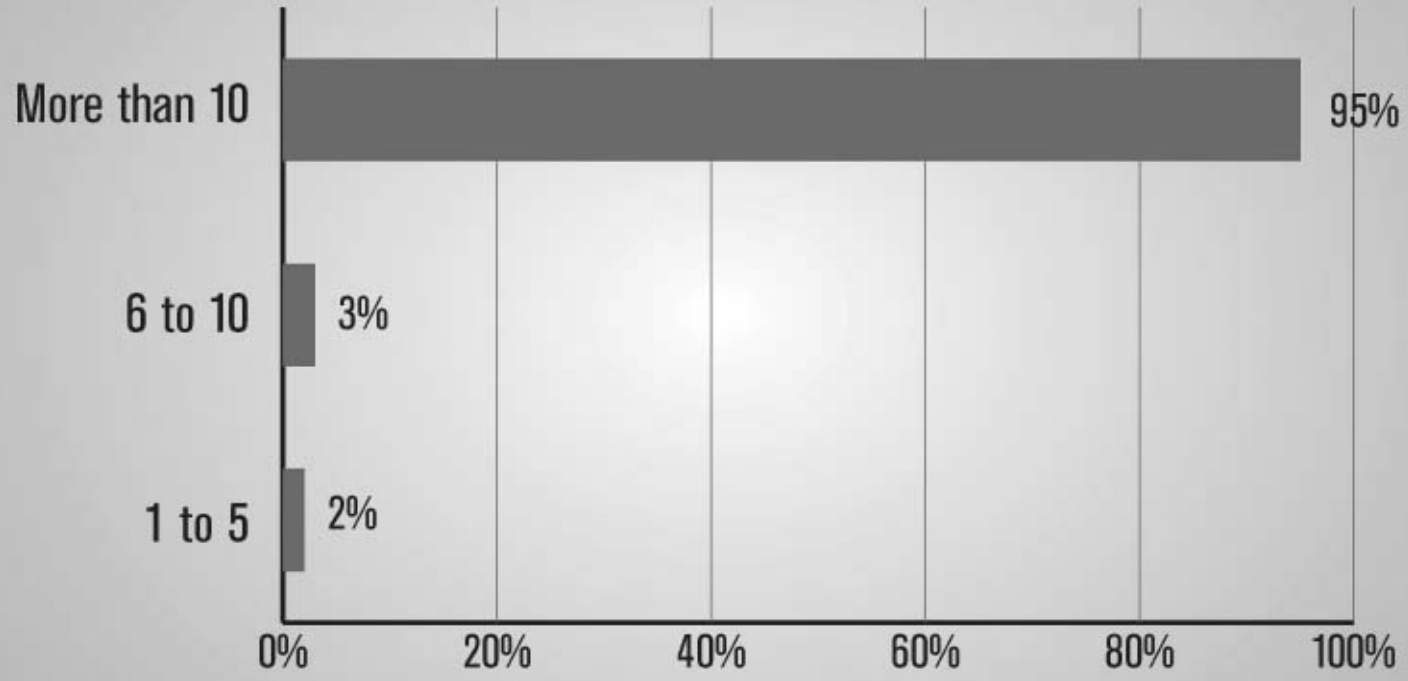
(Numbers do not total 100% due to rounding.)



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 690 Respondents

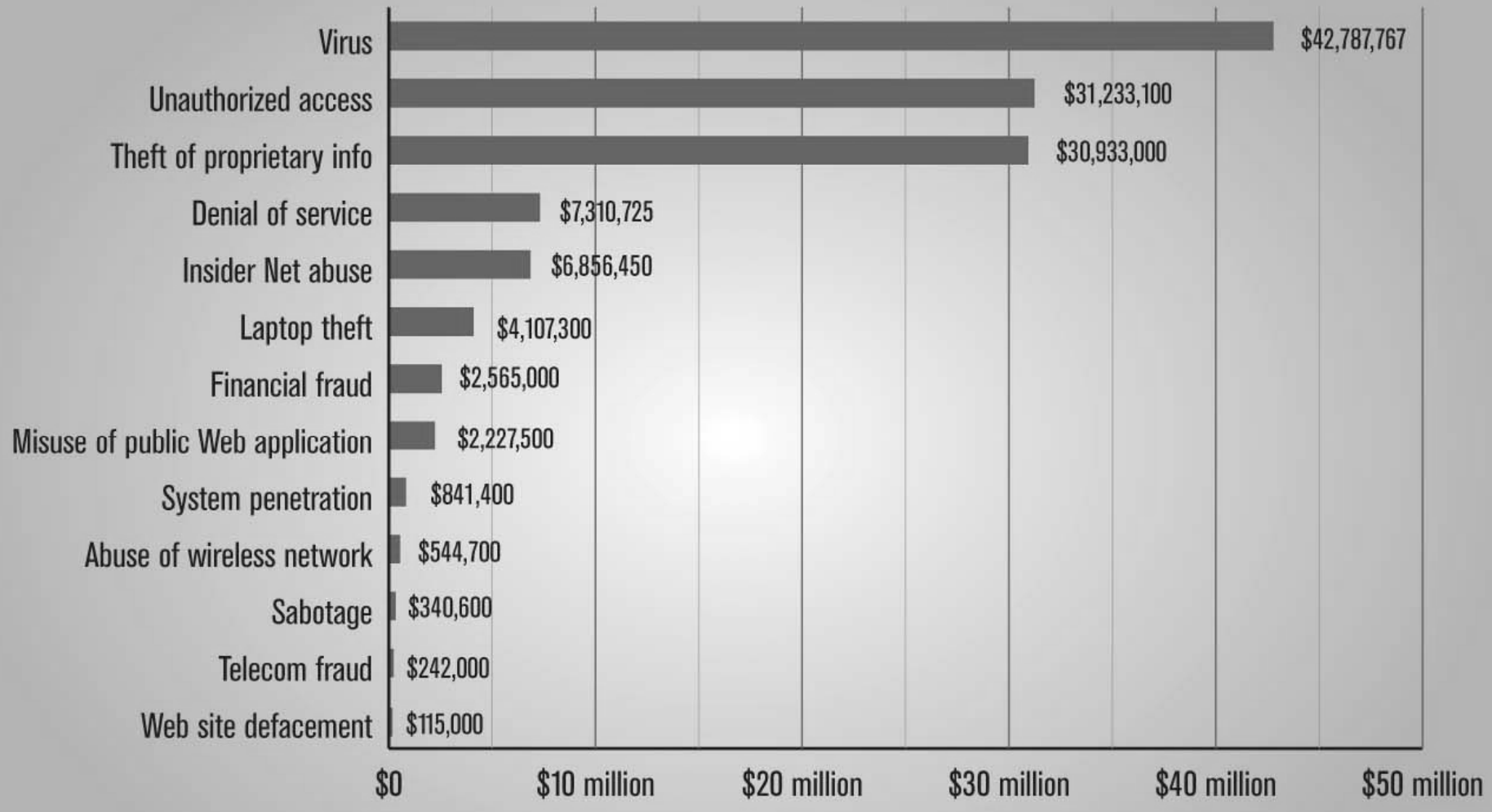
Figure 15. Percentage Experiencing Web Site Incidents



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 258 Respondents

Figure 16. Dollar Amount Losses by Type



Total Losses for 2005 were $130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 639 Respondents

Contenido

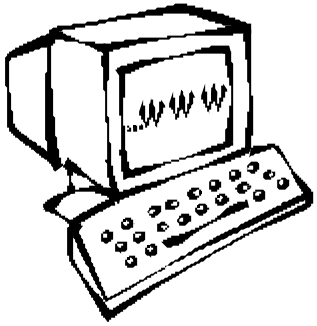
1. Situación actual de la Seguridad
   a. Panorama
   b. Casos
   c. Mitos
2. Elementos de la Seguridad
   a. Pilares
   b. Tipos de atacantes
   c. Tipos de ataques

Caso Banco Central Chile

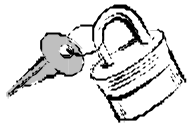
- Descripción
- Medidas
- Carta

Caso Serpost

Uso de los recursos de la empresa (pornografía) y facultad de empresa a revisar correos electrónicos:



Ejemplos a seguir

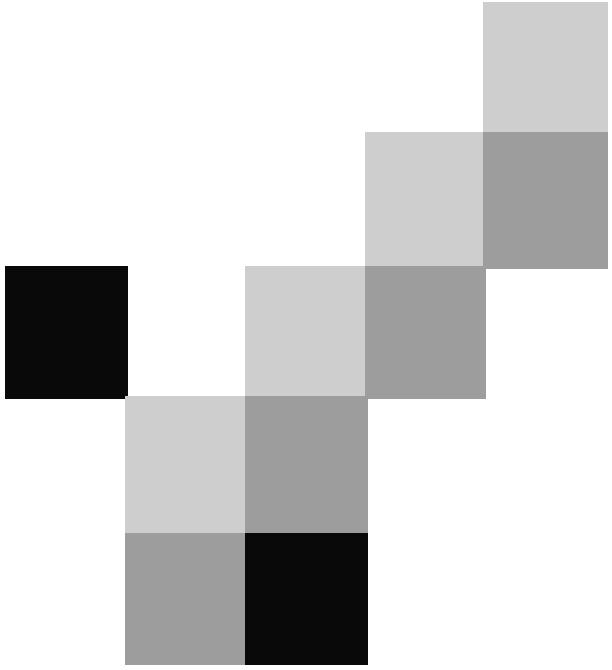
- INEI 
- PCM – CCISI 

Contenido

1. Situación actual de la Seguridad
   a. Panorama
   b. Casos
   c. **Mitos**
2. Elementos de la Seguridad
   a. Pilares
   b. Tipos de atacantes
   c. Tipos de ataques

Mitos de Seguridad

- El sistema puede llegar al 100% de seguridad.
- Mi red no es lo suficientemente atractiva para ser tomada en cuenta.
- Nadie pensará que mi clave de acceso es sencilla
- Linux es más seguro que Windows.
- Si mi servidor de correos tiene AV, mi estación no lo necesita.

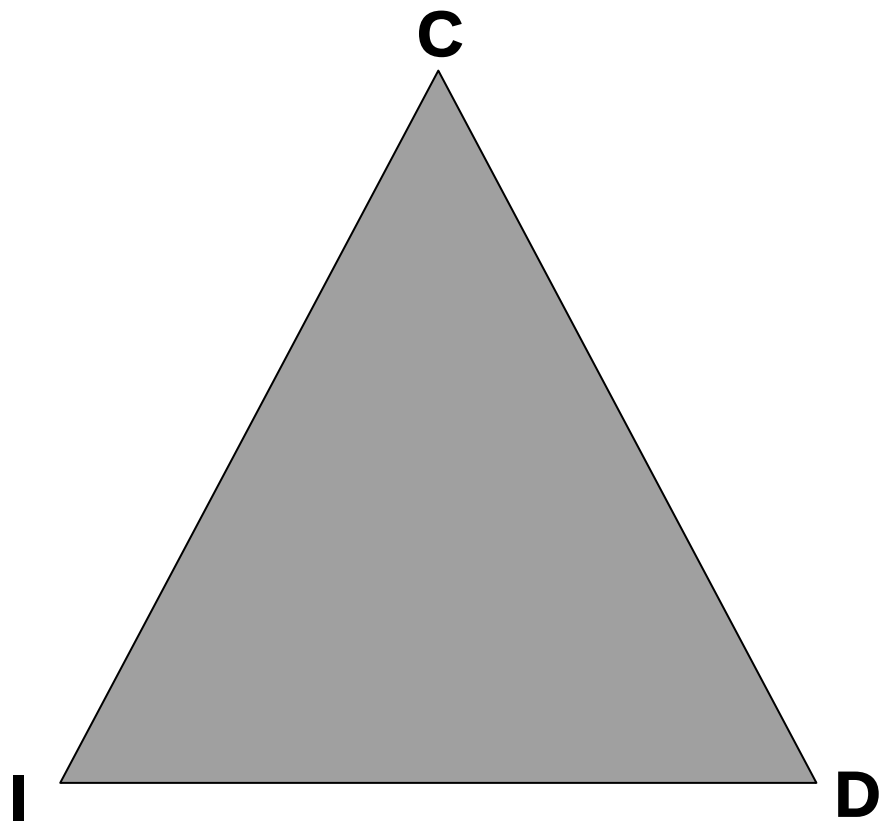


Elementos de Seguridad

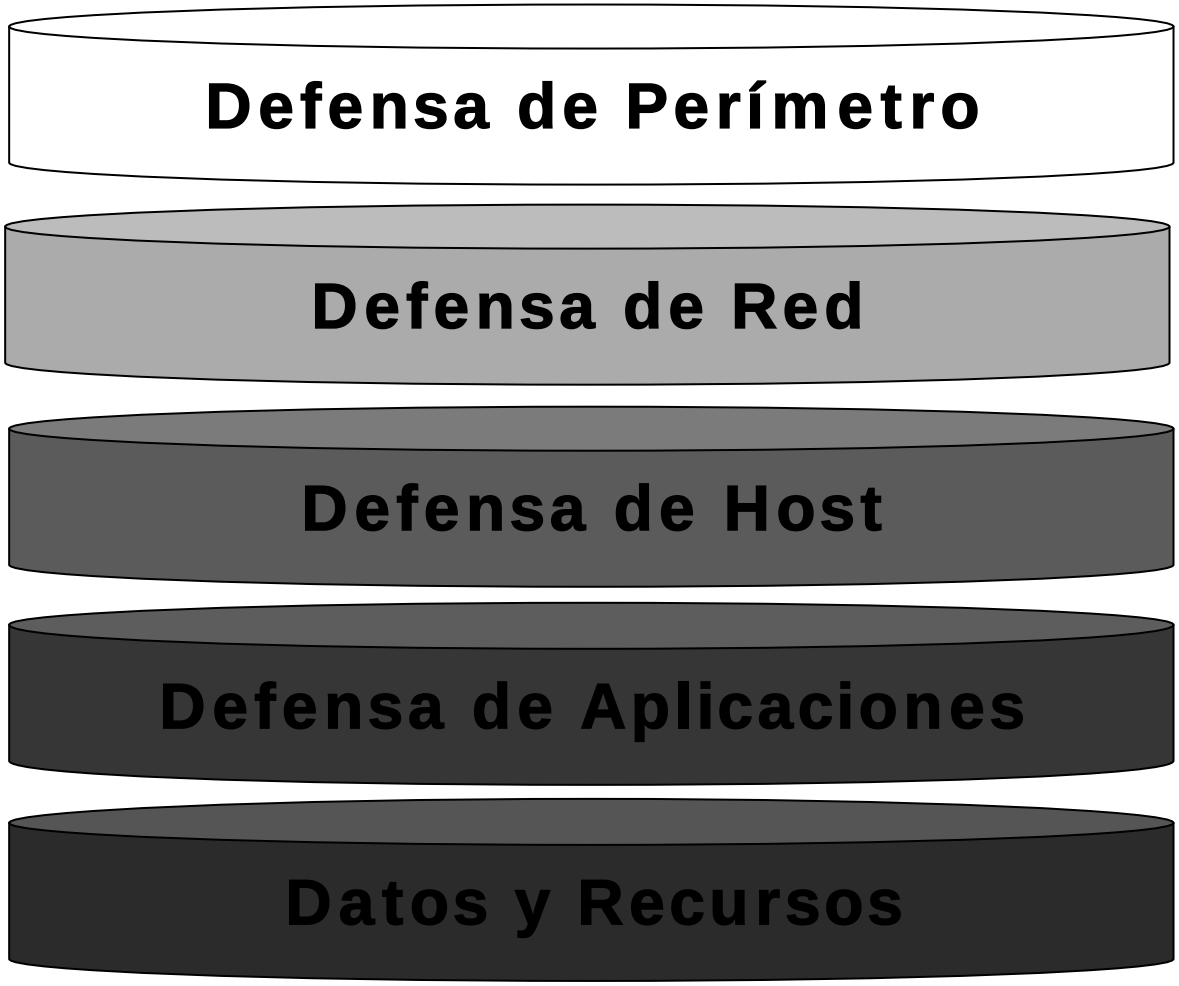
Contenido

1. Situación actual de la Seguridad
   a. Panorama
   b. Casos
   c. Mitos
2. Elementos de la Seguridad
   a. **Pilares**
   b. Tipos de atacantes
   c. Tipos de ataques

Pilares de la Seguridad



Seguridad Multicapa



Contenido

1. Situación actual de la Seguridad
   a. Panorama
   b. Casos
   c. Mitos
2. Elementos de la Seguridad
   a. Pilares
   b. Tipos de atacantes
   c. Tipos de ataques

Tipos de atacantes

- **Script kiddies:** No saben nada acerca de redes y/o protocolos pero saben manejar herramientas de ataque creadas por otros. Por lo general no siguen una estraegia muy silenciosa de ataques.
- **Hackers medium:** Personas que saben acerca de redes, protocolos, S.O. y aplicaciones pero que no crean sus propias herramientas, sino que utilizan las desarrolladas por otros.
- **Hackers:** Personas que además de conocer de redes, protocolos, S.O. y aplicaciones, desarrollan sus propias herramientas.

Contenido

1. Situación actual de la Seguridad
   a. Panorama
   b. Casos
   c. Mitos
2. Elementos de la Seguridad
   a. Pilares
   b. Tipos de atacantes
   c. **Tipos de ataques**

Tipos de ataques

- **Fuerza bruta**: Ataque que logra obtener acceso a recursos mediante el rompimiento de la clave de acceso a través del ensayo prueba y error.

  La forma de protección es establecer límites en el ingreso de claves a las cuentas habilitadas con monitoreo y registro de actividades.

Tipos de ataques

- **Denial of Service (DoS):** Anulación de un servicio o acceso a éste mediante técnicas de inundación de paquetes o aprovechamiento de debilidades en las aplicaciones y protocolos. Ejem: Ping of Death.

Tipos de ataques

- **Spoofing:** Falseamiento de la dirección origen en una sesión: Ips, Mac Address.

Tipos de ataques

- **Man-in-the-middle:** Ubicación de un usuario o programa en medio de una sesión tomando control de ésta y haciéndoles creer a los usuarios que ellos están conectados directamente con los recursos y/o servicios.

Tipos de ataques

- **Keyloggers:** Aplicaciones que registran el tecleado efectuado por un usuario.
- **Virus:** Aplicación diseñada para propagarse de un sistema a otro.

Tipos de ataques

- **Gusanos:** Aplicación de características similares a un virus con la particularidad de que es capaz de propagarse por sí mismo.
- **Troyanos:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Tipos de ataques

- **Sniffers:** Proceso de escucha y captura de tráfico de un segmento de red en manera no autorizada.
- **Spamming:** Bombardeo indiscriminado de e-mails hacia un objetivo desde un servidor de correos que no realiza autenticación de usuarios antes de aceptar el envío de los mismos.

Tipos de ataques

- **SQL Injection:** Técnica para explotar aplicaciones Web que no validan la información suministrada por el cliente para generar consultas SQL maliciosas.

  Algunos comandos ejemplo:

  - ; para ejecutar múltiples querys
  - -- para comentar el final del query
  - construcciones del tipo ’ or ’’=’
  - construcciones del tipo 1=1
  - usar UNION
  - xp_cmdshell() en MS SQL Server

Tipos de ataques

- **Ingeniería Social:** Proceso de vulnerar la confianza y buena fe de las personas para obtener información de ellas por medio de la persuasión y obtención amigable de información.
- **Errores de código:** Aprovechamiento de errores de los programadores. Ejem: Buffer Overflow

Ejemplos de Ataques

- SQL Injection

SQL Injection

Supongamos que se ha desarrollado una tienda virtual y se ha publicado en Internet. Dicha tienda se ha desarrollado mediante las tradicionales páginas ASP y el motor de base de datos SQL Server.

SQL Injection

Se han situado unas casillas para que los usuarios puedan introducir su "login" y contraseña con el fin de autenticarse en el sistema y que por ejemplo se le puedan aplicar unos descuentos concretos.

SQL Injection

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML
4.01 Transitional//EN">
<html>
<head><title>SQL Injection</title></head>
<body>
<form action="login.asp" method="get">
Login: <input type="text" name="strlogin"
size="15" maxlength="100" /><br />
Password: <input type="text"
name="strpassword" size="15"
maxlength="100" /><br />
<br />
<input type="submit" name="enviar"
value="enviar" />
</form>
</body>
</html>
```

```
<%
    Option Explicit
    Dim strLogin, strPassword, strSQL
    Dim connection, rs

    strLogin = Request("strLogin")
    strPassword = Request("strPassword")
    strSQL = "SELECT * FROM users WHERE strlogin='" &
strLogin & "' AND " & " strpassword='" & strPassword &
"'"

    Set connection =
Server.CreateObject("ADODB.Connection")
    connection.Open("Provider=SQLOLEDB; Data
Source=(local); Initial Catalog=tienda; User Id=sa; Password=
")

    Set rs = connection.Execute(strSQL)
    If( Not rs.EOF ) Then
        Response.Write("Indentificacion correcta")
    else
        Response.Write("Indentificacion INCORRECTA")
    End If
    rs.Close
    connection.Close

    Set rs = Nothing
    Set connection = Nothing
%>
```

SQL Injection

Supongamos que el usuario llega a su formulario de identificación, e inserta los datos "oscar" como identificación y "abcdef" como contraseña.

SQL Injection

```
SELECT user_id FROM users
WHERE strlogin='oscar' AND
strpassword='abcdef'
```

SQL Injection

'or 1=1 --

```
SELECT user_id FROM users
WHERE strlogin='bob' or 1=1 -- ' AND
strpassword='abcdef'
```

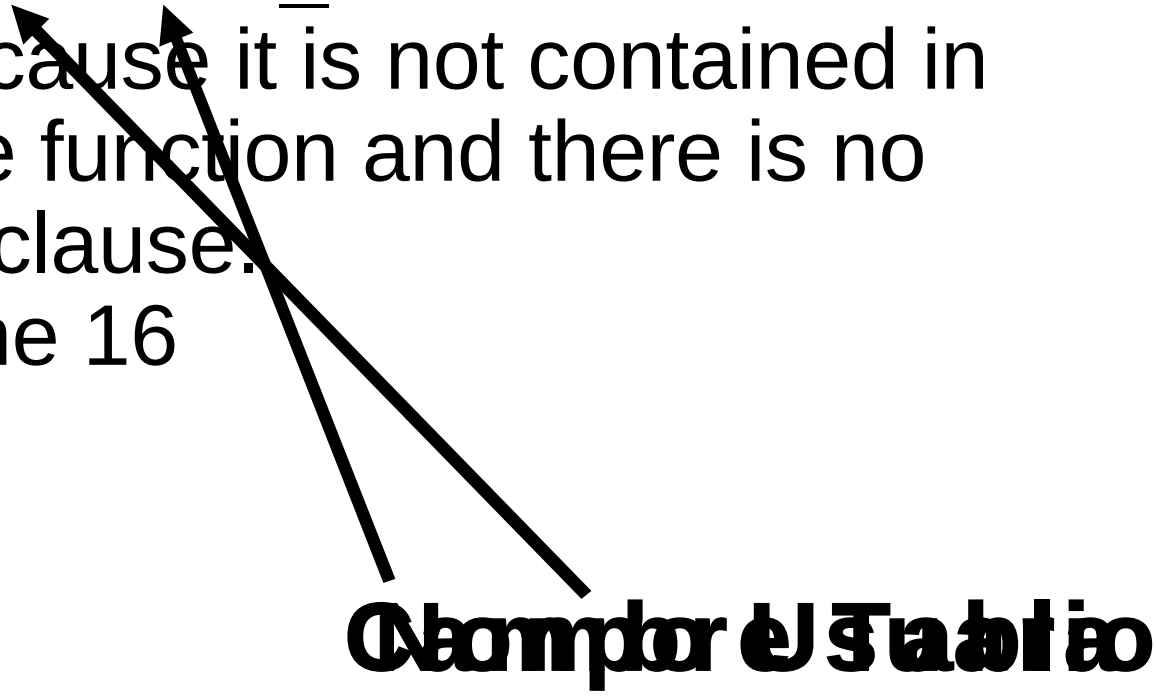
SQL Injection

'having 1=1 --

```
SELECT user_id FROM users
WHERE strlogin = 'dsaving 1=1 --'
AND strPass = 'abcdef'
```

SQL Injection

Microsoft OLE DB Provider for SQL Server error '80040e14'
Column '**users.user_id**' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
/login.asp, line 16



SQL Injection

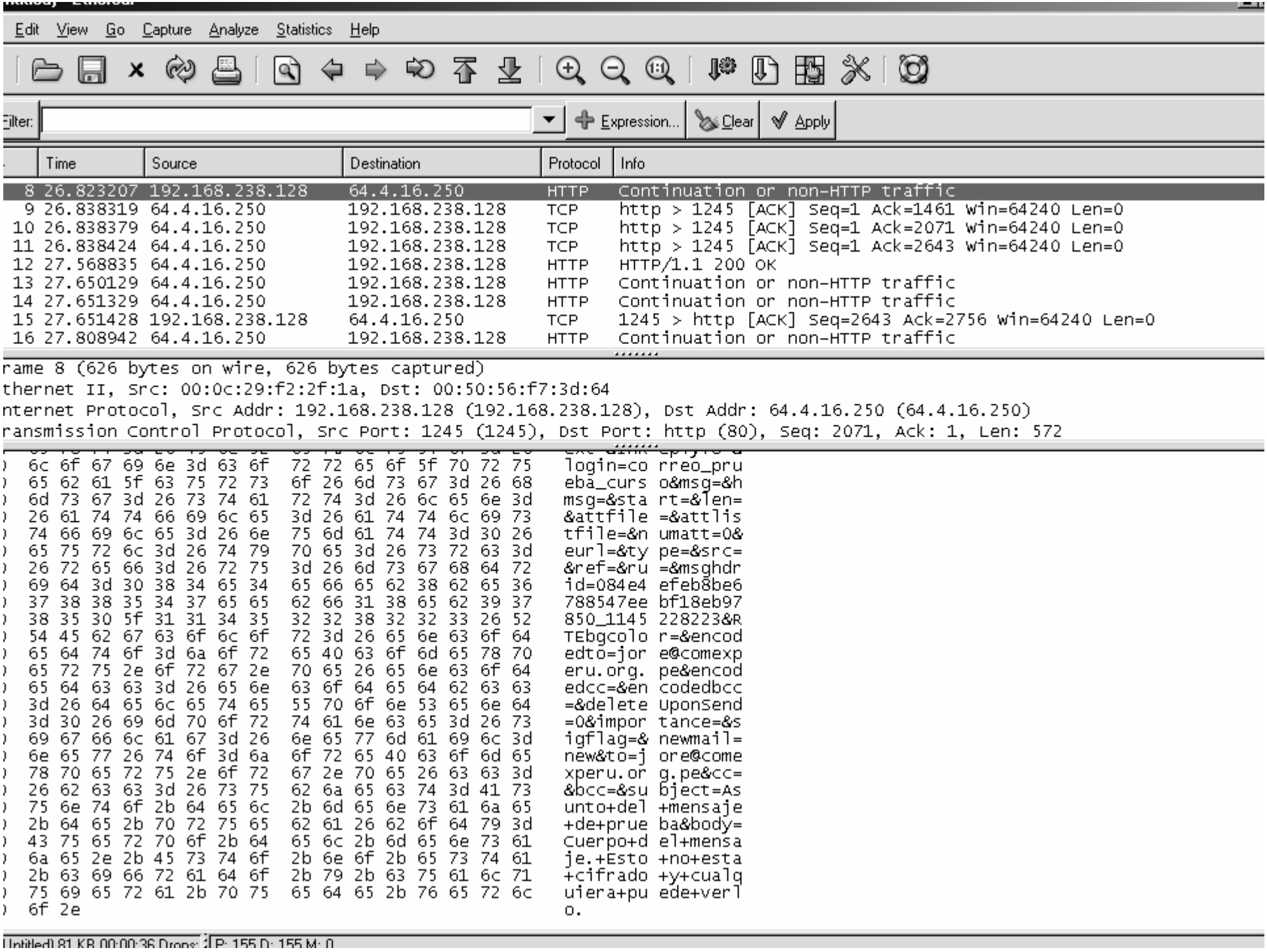
'or 1=1; drop table users; --

SELECT user_id FROM users
WHERE strlogin='bsmith' **or 1=1; drop table users; --**
AND strpassword='abcdef'

SELECT user_id FROM users
WHERE strlogin='bsmith' **or 1=1; drop table users; --**
AND strpassword=''

Ejemplos de Ataques

- Uso de Sniffer: Ethereal


Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Time Source Destination Protocol Info
8 26.823207 192.168.238.128 64.4.16.250 HTTP Continuation or non-HTTP traffic
9 26.838319 64.4.16.250 192.168.238.128 TCP http > 1245 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
10 26.838379 64.4.16.250 192.168.238.128 TCP http > 1245 [ACK] Seq=1 Ack=2071 Win=64240 Len=0
11 26.838424 64.4.16.250 192.168.238.128 TCP http > 1245 [ACK] Seq=1 Ack=2643 Win=64240 Len=0
12 27.568835 64.4.16.250 192.168.238.128 HTTP HTTP/1.1 200 OK
13 27.650129 64.4.16.250 192.168.238.128 HTTP Continuation or non-HTTP traffic
14 27.651329 64.4.16.250 192.168.238.128 HTTP Continuation or non-HTTP traffic
15 27.651428 192.168.238.128 64.4.16.250 TCP 1245 > http [ACK] Seq=2643 Ack=2756 Win=64240 Len=0
16 27.808942 64.4.16.250 192.168.238.128 HTTP Continuation or non-HTTP traffic
rame 8 (626 bytes on wire, 626 bytes captured)
thernet II, Src: 00:0c:29:f2:2f:1a, Dst: 00:50:56:f7:3d:64
nternet Protocol, Src Addr: 192.168.238.128 (192.168.238.128), Dst Addr: 64.4.16.250 (64.4.16.250)
ransmission Control Protocol, Src Port: 1245 (1245), Dst Port: http (80), Seq: 2071, Ack: 1, Len: 572
6c 6f 67 69 6e 3d 63 6f 72 72 65 6f 5f 70 72 75 login=co rreo_pru
65 62 61 5f 63 75 72 73 6f 26 6d 73 67 3d 26 68 eba_curs o&msg=&h
6d 73 67 3d 26 73 74 61 72 74 3d 26 6c 65 6e 3d msg=&sta rt=&len=
26 61 74 74 66 69 6c 65 3d 26 61 74 74 6c 69 73 &attfile =&attlis
74 66 69 6c 65 3d 26 6e 75 6d 61 74 74 3d 30 26 tfile=&n umatt=0&
65 75 72 6c 3d 26 74 79 70 65 3d 26 73 72 63 3d eurl=&ty pe=&src=
26 72 65 66 3d 26 72 75 3d 26 6d 73 67 68 64 72 &ref=&ru =&msghdr
69 64 3d 30 38 34 65 34 65 66 65 62 38 62 65 36 id=084e4 efeb8be6
37 38 38 35 34 37 65 65 62 66 31 38 65 62 39 37 788547ee bf18eb97
38 35 30 5f 31 31 34 35 32 32 38 32 32 33 26 52 850_1145 228223&R
54 45 62 67 63 6f 6c 6f 72 3d 26 65 6e 63 6f 64 TEbgcolo r=&encod
65 64 74 6f 3d 6a 6f 72 65 40 63 6f 6d 65 78 70 edto=jor e@comexp
65 72 75 2e 6f 72 67 2e 70 65 26 65 6e 63 6f 64 eru.org. pe&encod
65 64 63 63 3d 26 65 6e 63 6f 64 65 64 62 63 63 edcc=&en codedbcc
3d 26 64 65 6c 65 74 65 55 70 6f 6e 53 65 6e 64 =&delete UponSend
3d 30 26 69 6d 70 6f 72 74 61 6e 63 65 3d 26 73 =0&impor tance=&s
69 67 66 6c 61 67 3d 26 6e 65 77 6d 61 69 6c 3d igflag=& newmail=
6e 65 77 26 74 6f 3d 6a 6f 72 65 40 63 6f 6d 65 new&to=j ore@come
78 70 65 72 75 2e 6f 72 67 2e 70 65 26 63 63 3d xperu.or g.pe&cc=
26 62 63 63 3d 26 73 75 62 6a 65 63 74 3d 41 73 &bcc=&su bject=As
75 6e 74 6f 2b 64 65 6c 2b 6d 65 6e 73 61 6a 65 unto+del +mensaje
2b 64 65 2b 70 72 75 65 62 61 26 62 6f 64 79 3d +de+prue ba&body=
43 75 65 72 70 6f 2b 64 65 6c 2b 6d 65 6e 73 61 Cuerpo+d el+mensa
6a 65 2e 2b 45 73 74 6f 2b 6e 6f 2b 65 73 74 61 je.+Esto +no+esta
2b 63 69 66 72 61 64 6f 2b 79 2b 63 75 61 6c 71 +cifrado +y+cualq
75 69 65 72 61 2b 70 75 65 64 65 2b 76 65 72 6c uiera+pu ede+verl
6f 2e o.
Untitled) 81 KB 00:00:36 Drops: P: 155 D: 155 M: 0

Ejemplos de Ataques
MAC Address Flooding Storms

- Objetivo: Anular la principal funcionalidad del switch: la segmentación.
- Gracias a herramientas de software (Ejem: Macof) se inunda de tramas al switch a nivel de direcciones MAC.
- Cuando la tabla MAC del switch se llena, dejará de actuar como tal y se convertirá en un hub.

Ejemplos de Ataques
MAC Address Flooding Storms

- La mejor forma de detener este tipo de ataques es limitar el número de direcciones MAC por puerto del switch.

Ejemplos de Ataques
ARP Poisoning Attack

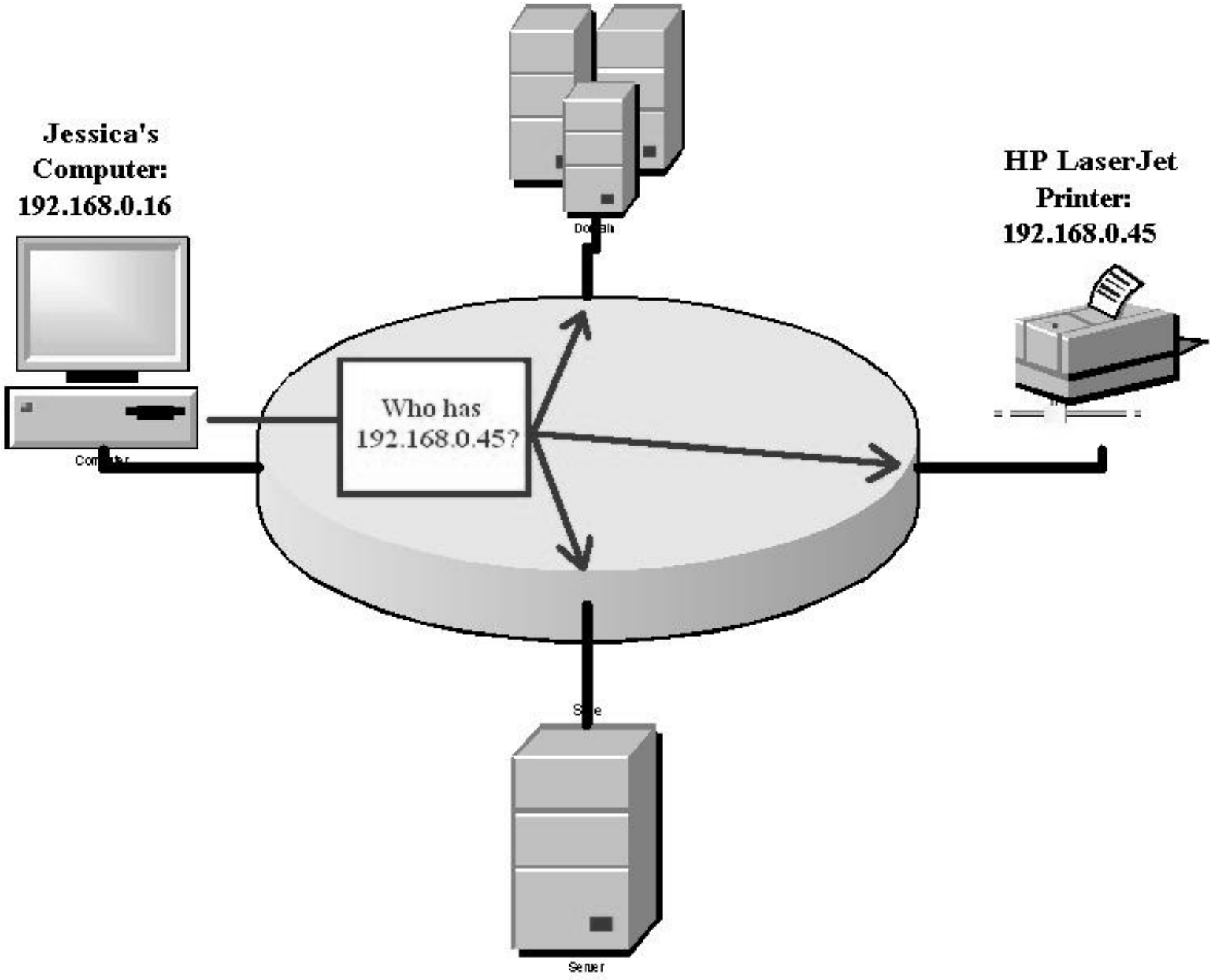
- Address Resolution Protocol (ARP)
- ARP permite a un host descubrir dinámicamente la dirección MAC correspondiente a una dirección IP en particular.

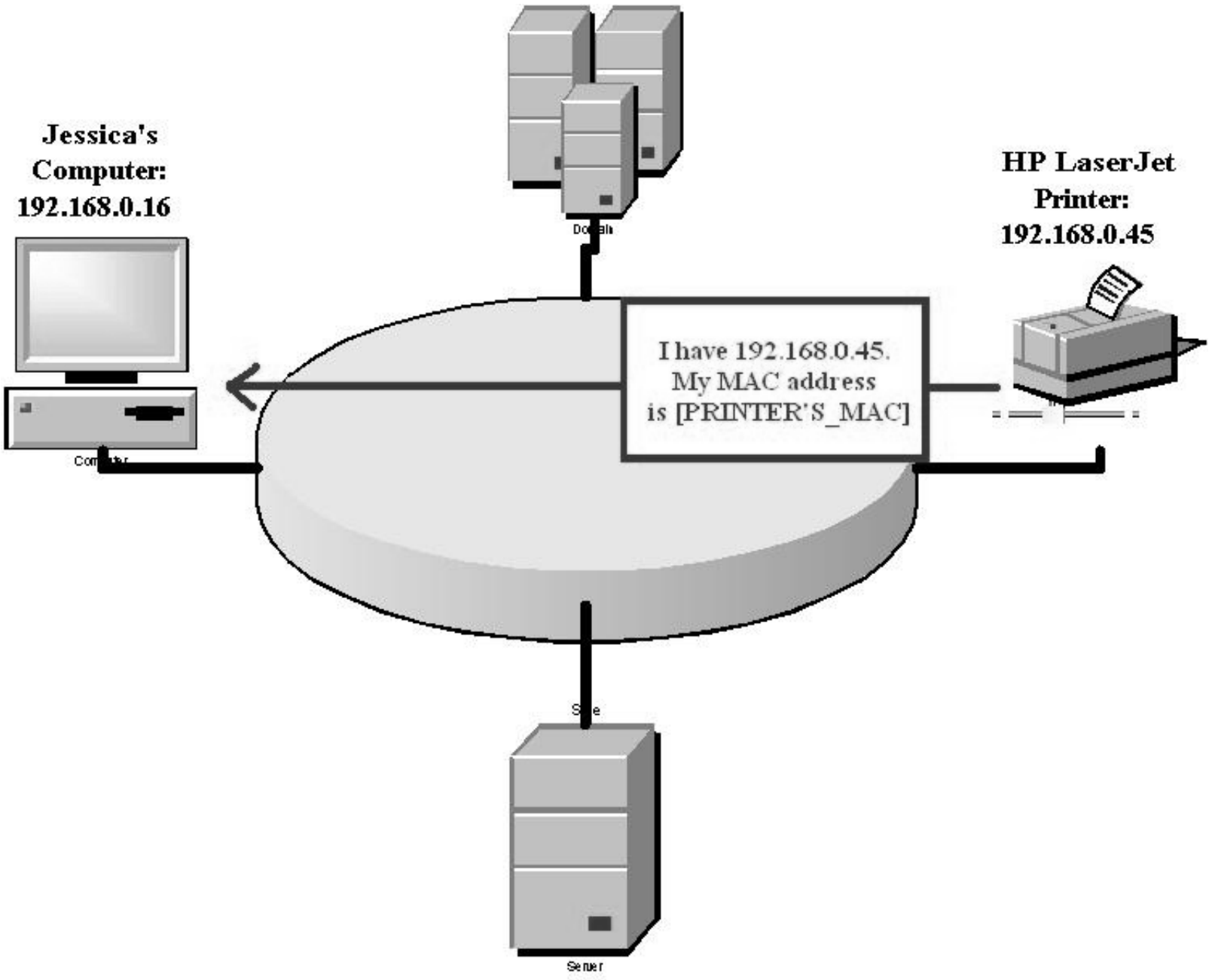
Ejemplos de Ataques
ARP Poisoning Attack

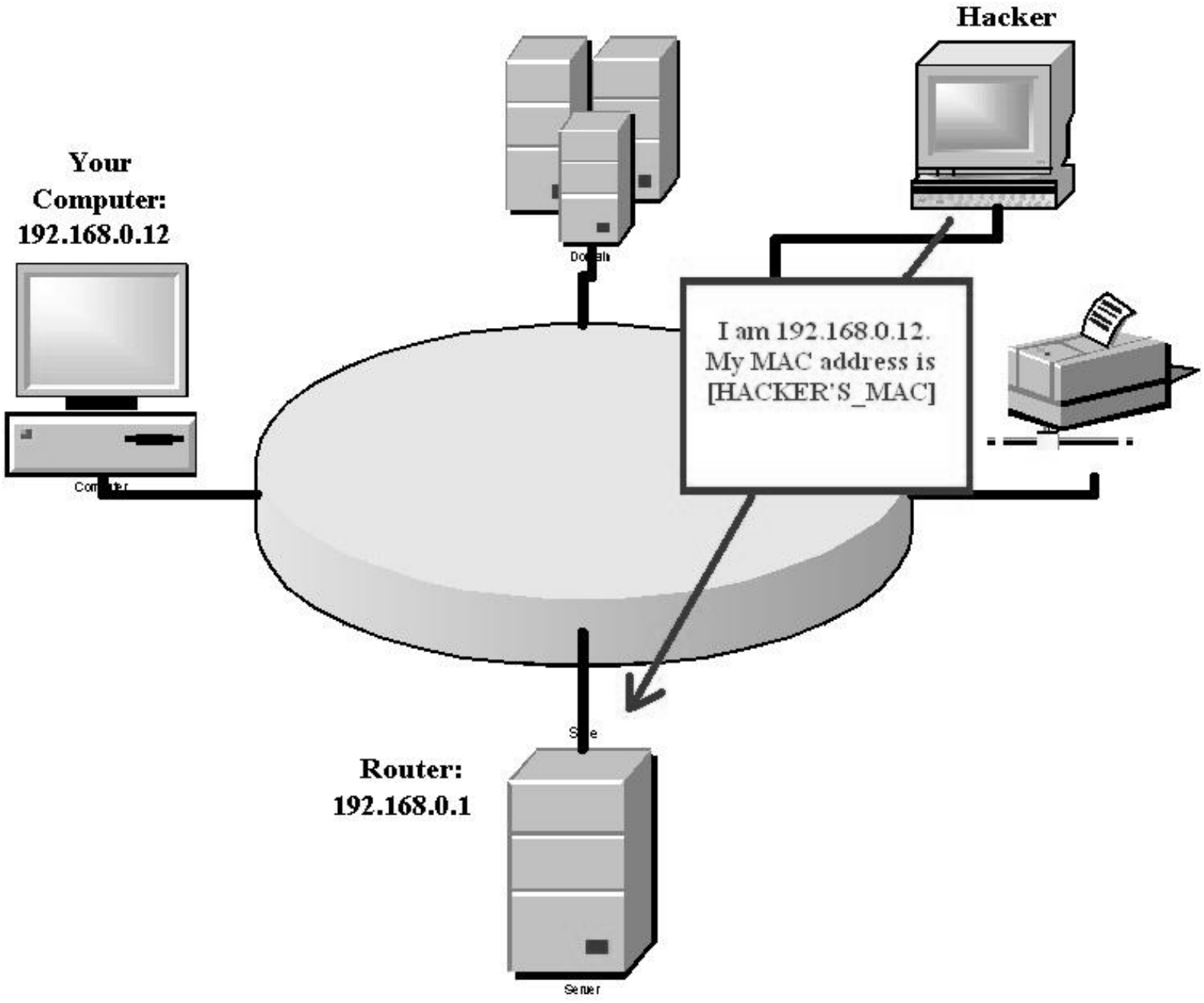
- Paso 1: La estación con dirección 192.168.1.1 y dirección MAC 0002.4534.AC12 desea transferir datos a la estación 2 con dirección IP 192.168.1.2 y envía un paquete ARP Request a todas las estaciones de la red (broadcast)

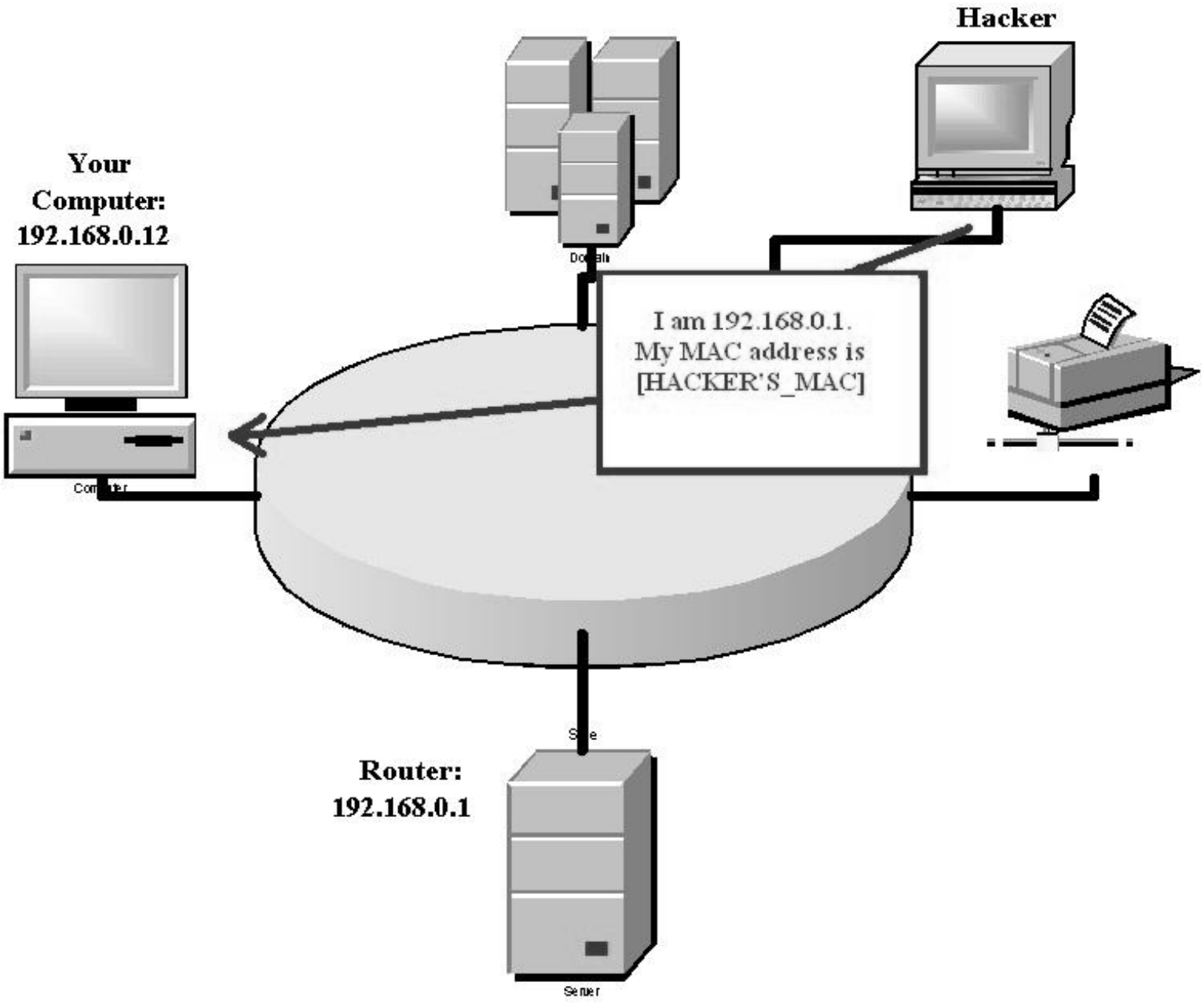
Ejemplos de Ataques
ARP Poisoning Attack

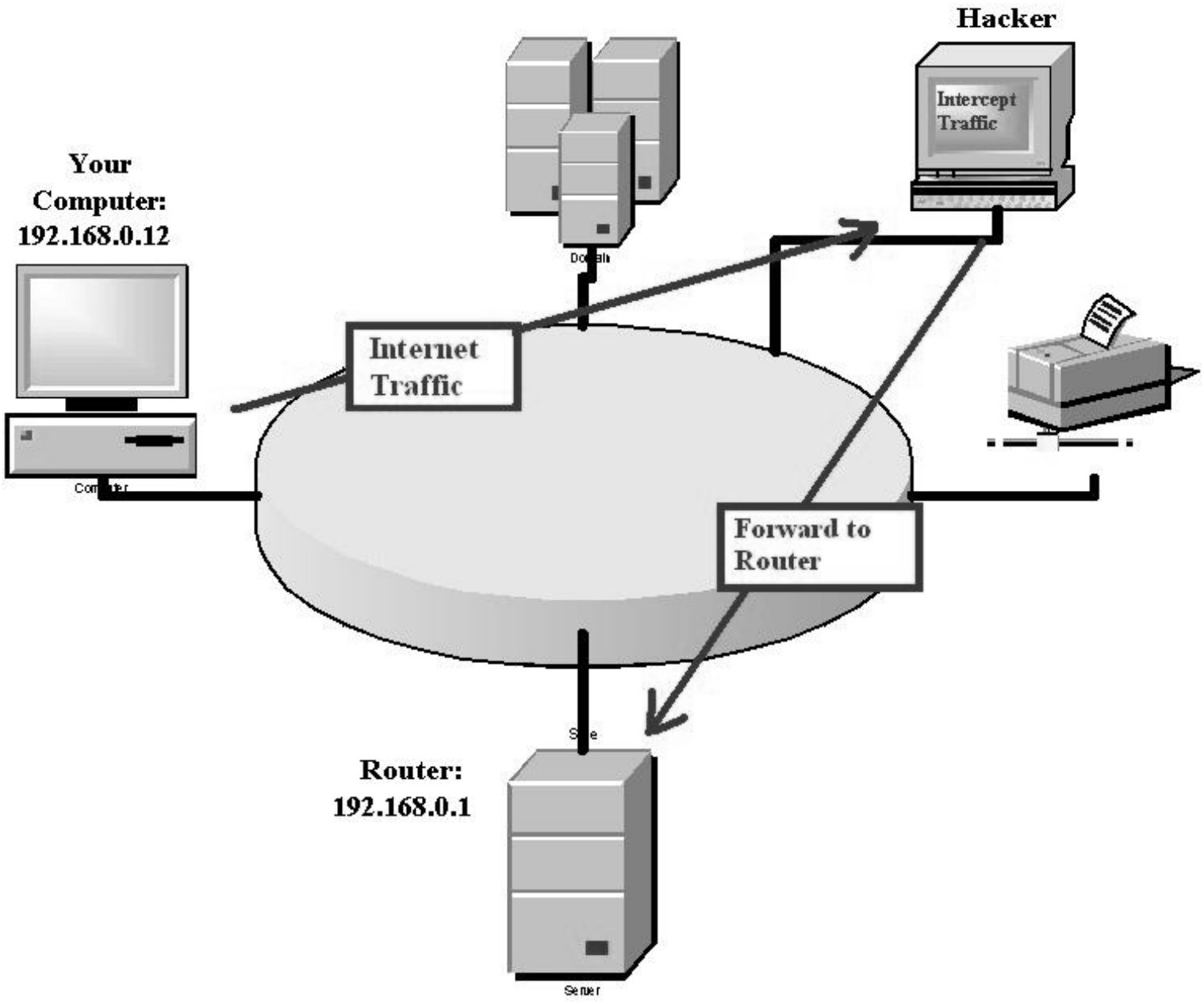
- Paso 2: Solamente la estación destino reconocerá ese paquete, por la dirección IP, y responderá con un paquete ARP Reply el cual contendrá su dirección MAC.


Jessica's
Computer:
192.168.0.16
HP LaserJet
Printer:
192.168.0.45
Who has
192.168.0.45?
Server


Jessica's
Computer:
192.168.0.16
HP LaserJet
Printer:
192.168.0.45
I have 192.168.0.45.
My MAC address
is [PRINTER'S_MAC]
Server


Hacker
Your
Computer:
192.168.0.12
I am 192.168.0.12.
My MAC address is
[HACKER'S_MAC]
Router:
192.168.0.1


Hacker
Your
Computer:
192.168.0.12
I am 192.168.0.1.
My MAC address is
[HACKER'S_MAC]
Router:
192.168.0.1


Hacker
Intercept Traffic
Your Computer: 192.168.0.12
Internet Traffic
Forward to Router
Router: 192.168.0.1

Ejemplos de Ataques
ARP Poisoning Attack

- Herramientas:
  - Caín y Abel
  - WinARPSpoofer
- Solución
  - No tiene
- Prevención
  - WinARPWatch

Ejemplos de Ataques Source Routing

- Enrutamiento normal es por IP destino.
- Con fines administrativos y para verificar conectividad el Source Routing uso enrutamiento por la IP fuente.

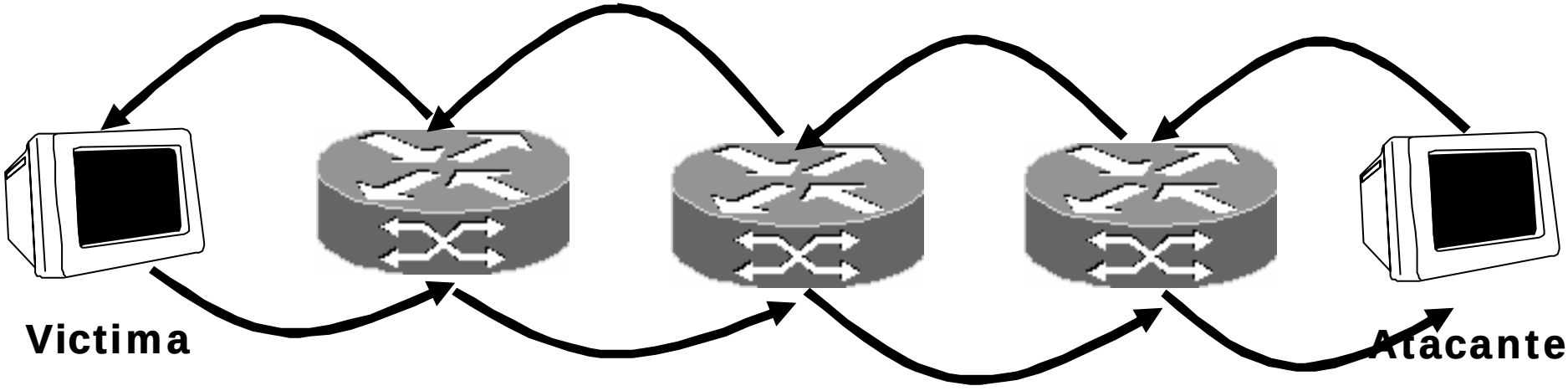
Ejemplos de Ataques Source Routing

- **Strict Source Routing:** Permite al administrador especificar el camino a través de todos los ruteadores al destino. La respuesta de retorno utiliza el mismo trayecto.
- **Loose Source Routing:** Permite a los administradores especificar una dirección que el paquete debe pasar en su camino hacia su destino.

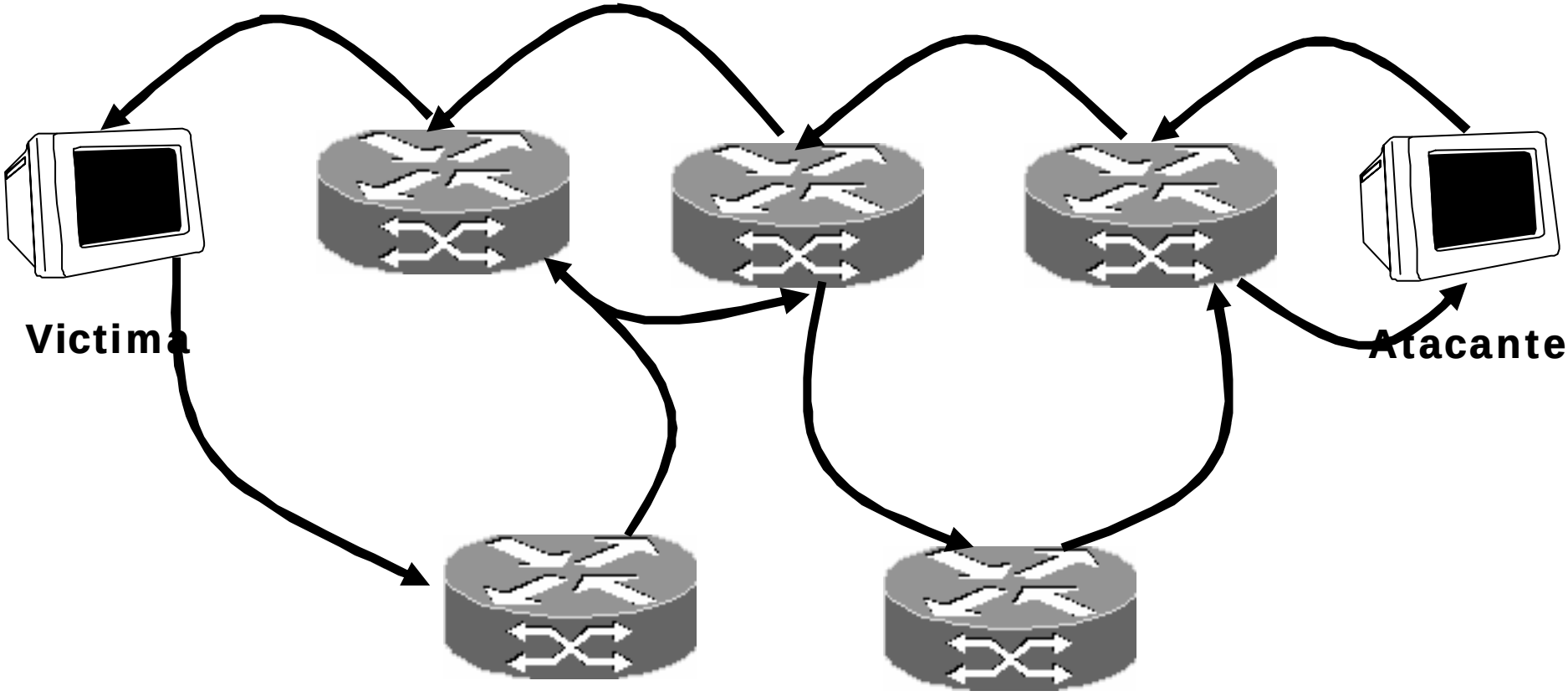
Ejemplos de Ataques Source Routing

- La defensa contra ataques LSR es simplemente no permitir que estos paquetes ingreses o dejen la red. Esto se puede realizar bloqueando estos paquetes en el firewall o en el ruteador.

Ejemplos de Ataques
Strict Source Routing



Ejemplos de Ataques
Loose Source Routing



Contenido (cont.)

3. Defensa
   a. **Firewalls**
   b. IDS
   c. Criptografía
   d. VPN
4. Recomendaciones

Firewalls

- Dispositivos que controlan el tráfico.
- Al inicio, el ruteador aislaba las redes y controlaba el tráfico de las organizaciones.
- Al incrementarse el tráfico, el ruteador dejó de ser eficiente en esta función y se prefirió dejarla a otro equipo: Firewall.

Firewalls

- Tipos de Firewalls:

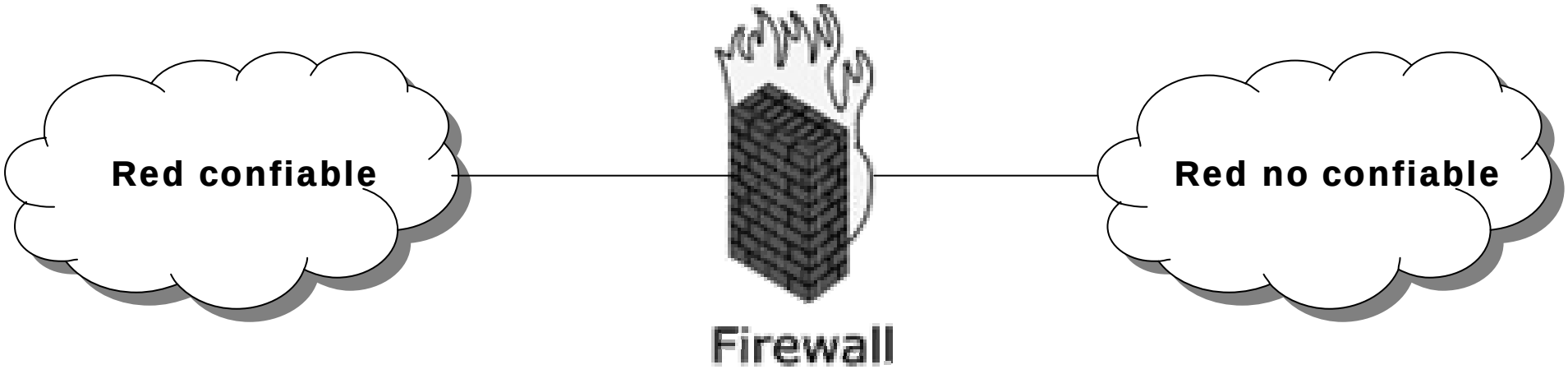
1. Packet Filtering

- Primero que apareció en el mercado y es conocido también como screening router. Trabaja principalmente en la capa 3 de OSI (Red) y en menor grado en la capa 4 (Transporte).

Firewalls

- Filtra paquetes basado en la dirección IP fuente y dirección IP destino de los paquetes entrantes no realizando análisis de contenido ni seguimiento de la conexión.
- Son implementados dentro del ruteador y trabajan con listas de control de acceso (Access Control Lists).

Firewalls



Firewalls

- Tipos de Firewalls:
2. Application level Firewalls
- Firewall que utiliza un software proxy.
- Transfiere una copia de cada paquete de datos aceptado en la red a otra enmascarando el origen del dato.
- Esto permite controlar que servicios son utilizados por las estaciones de trabajo y protege además a la red de usuarios externos que traten de obtener información.

Firewalls

- Tipos de Firewalls:

3. Stateful Inspection Firewalls

- Paquetes son capturados por un motor de inspección que está operando a la velocidad de la red.
- Paquetes son encolados y analizados en todos los niveles OSI.
- Conocido como Firewall de 3ra generación.

Firewalls

- Tipos de Firewalls:

4. Dynamic packet filtering Firewalls

- Tecnología de 4ta generación que habilita la modificación de las reglas del firewall.

Firewalls

- Tipos de Firewalls:

5. Kernel proxy

- Tecnología de 5ta generación que provee evaluación de sesiones multicapa de manera modular basada en kernel.

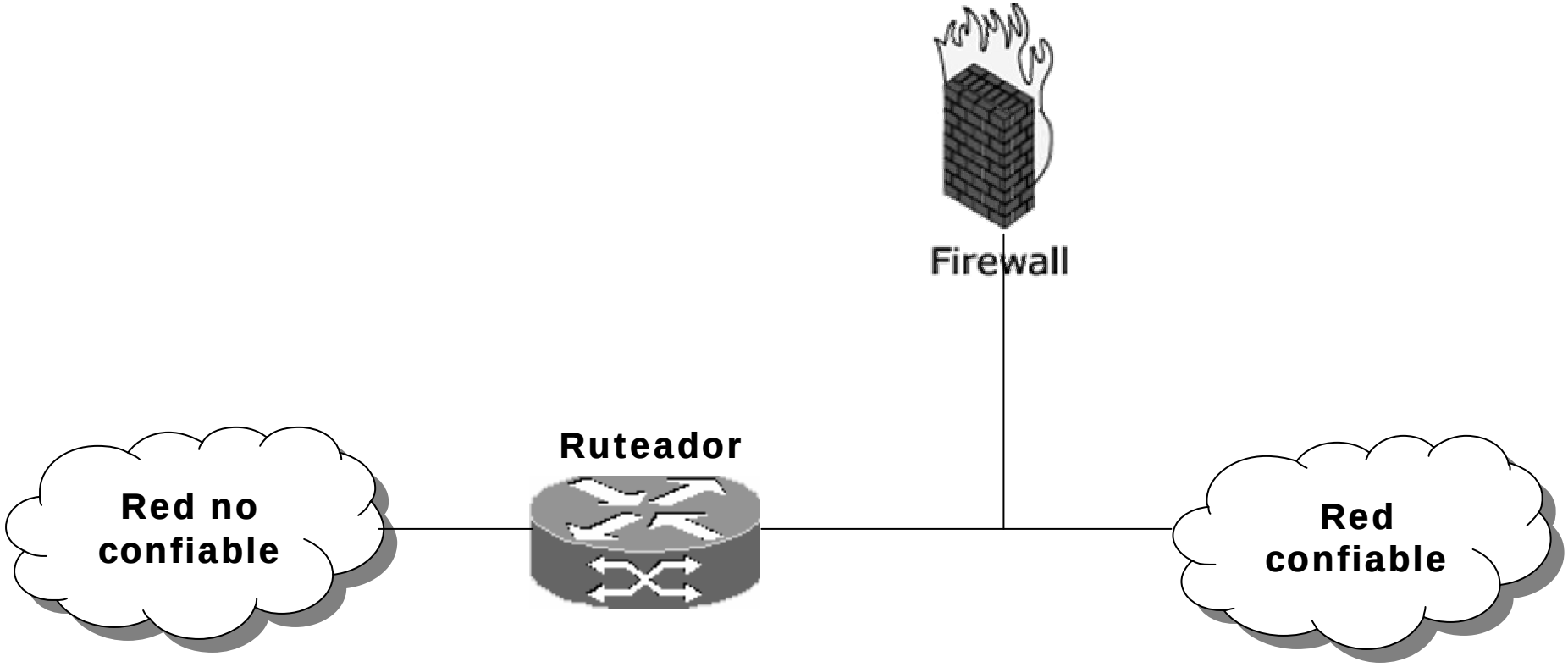
Firewalls

- Arquitectura de Firewalls:

1. Packet filtering routers

Firewalls

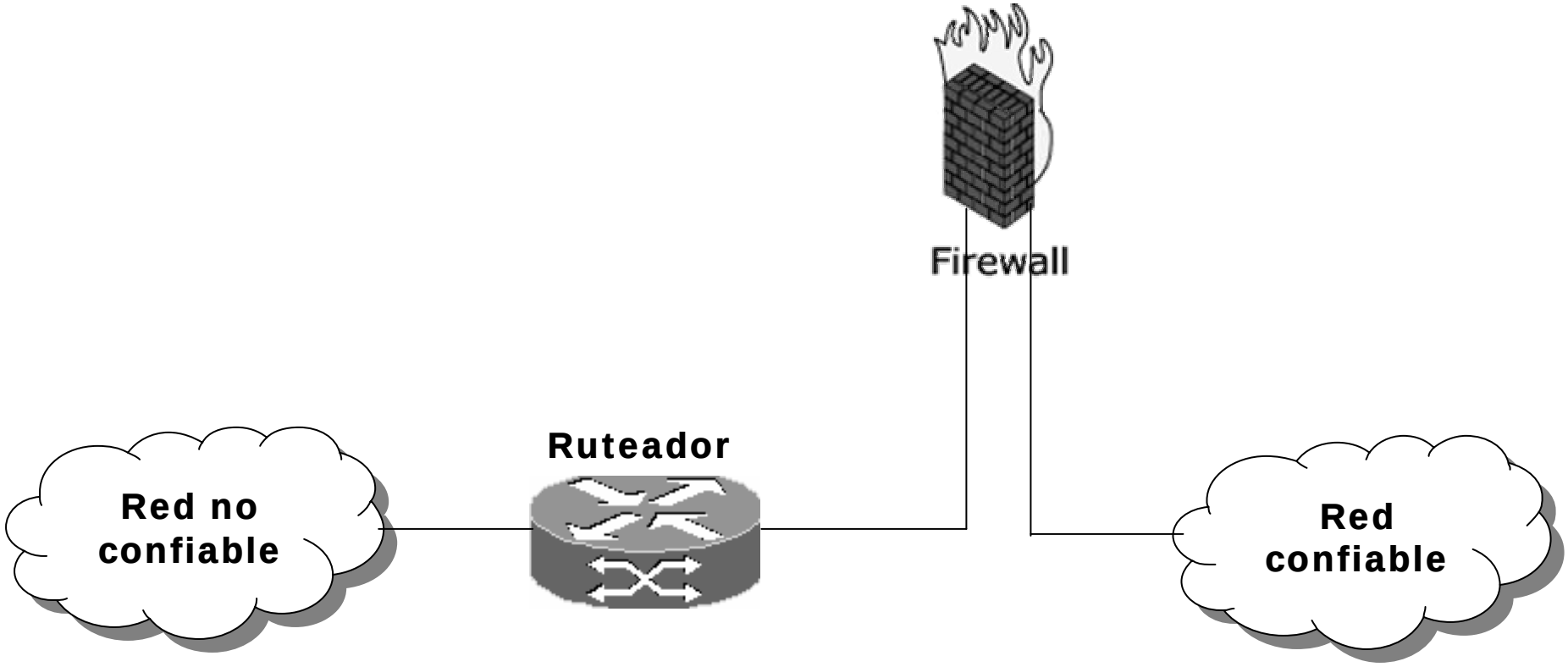
- Arquitectura de Firewalls:
2. Screened-Host Firewall Systems



Firewalls

- Arquitectura de Firewalls:

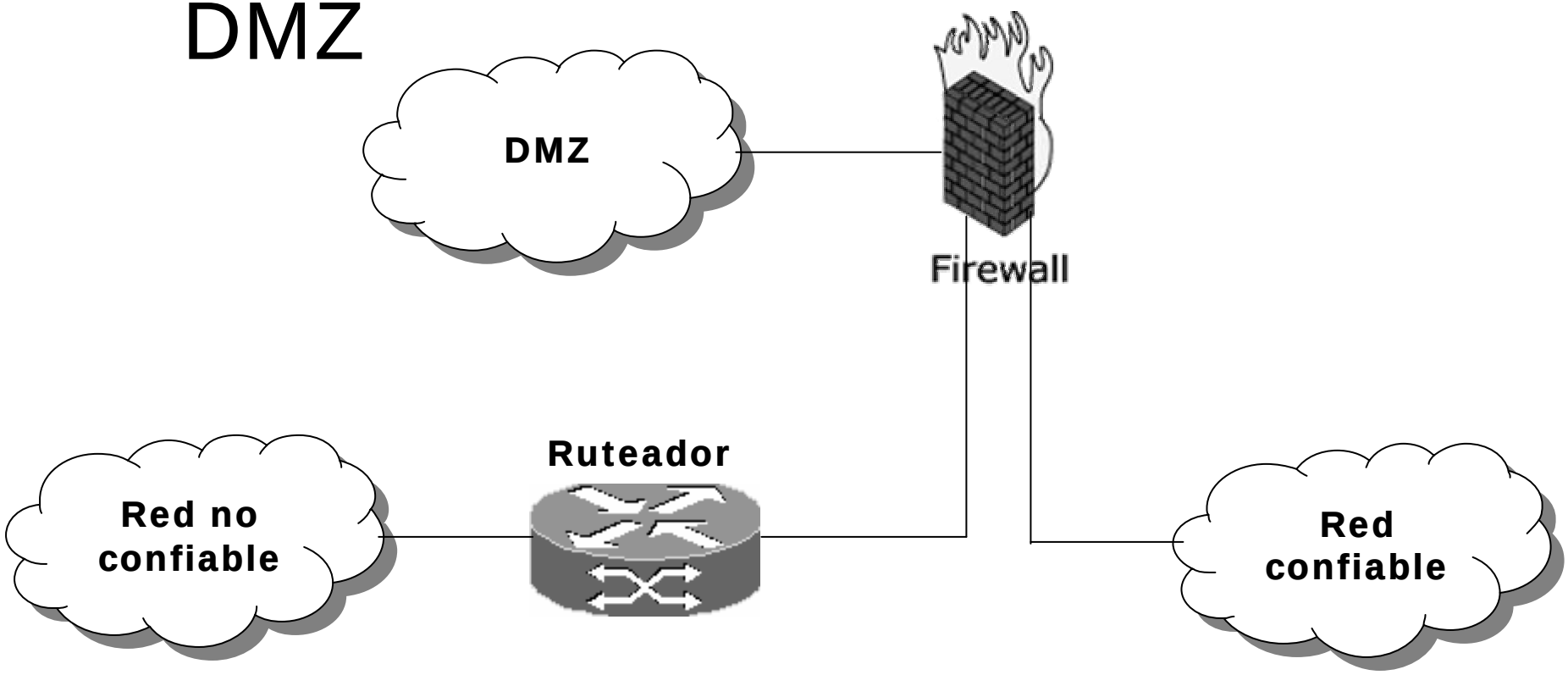
3. Dual-homed host Firewalls



Firewalls

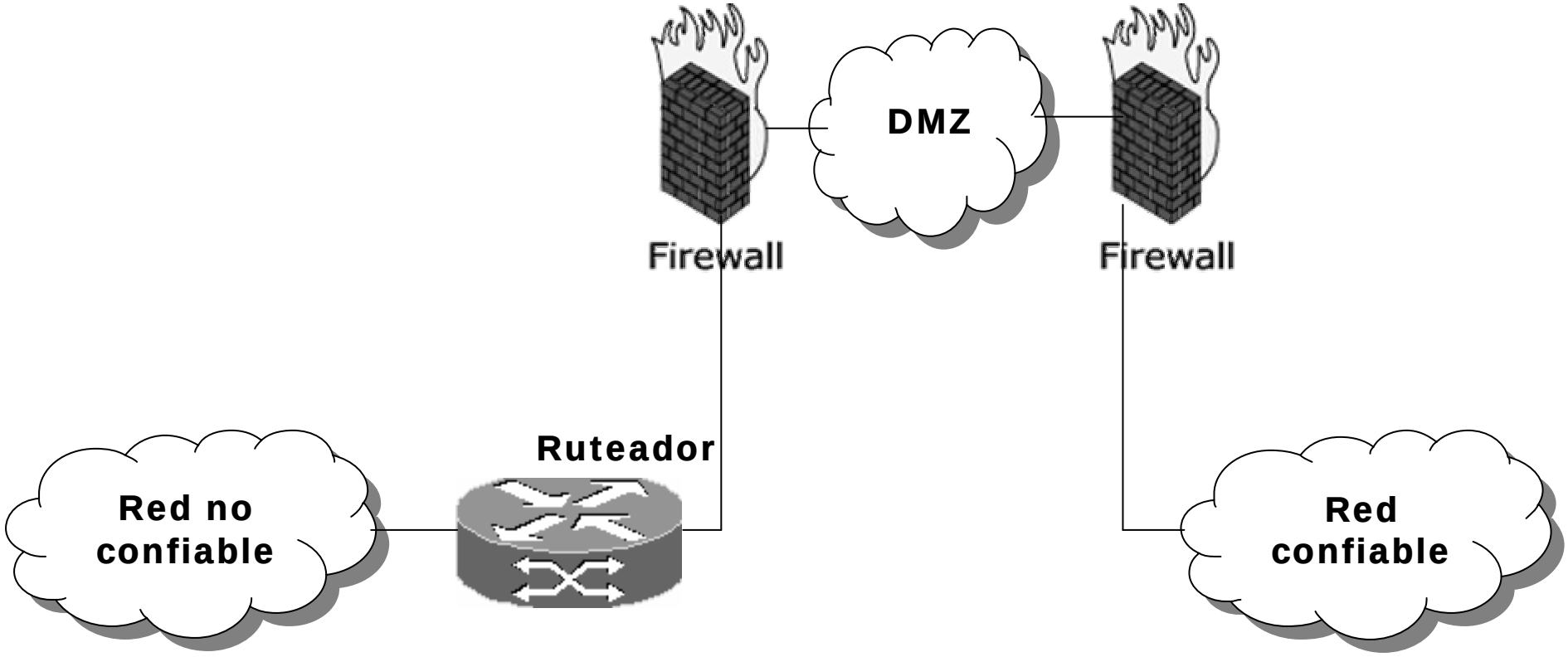
- Arquitectura de Firewalls:

4. Screened-subnet Firewall con DMZ



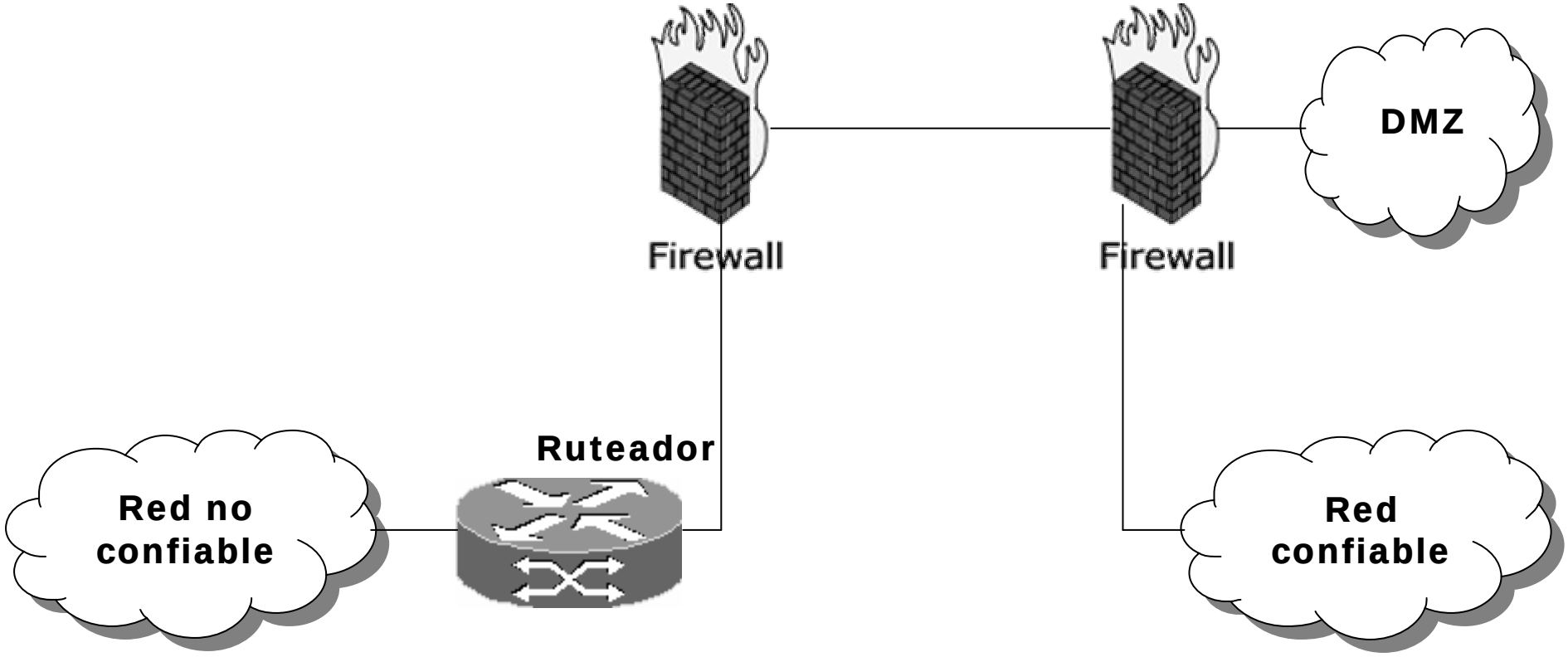
Firewalls

- Arquitectura de Firewalls:



Firewalls

- Arquitectura de Firewalls:



Contenido (cont.)

3. Defensa
   a. Firewalls
   b. **IDS**
   c. Criptografía
   d. VPN
4. Recomendaciones

IDS

- La detección de intrusos es una de las actividades claves del especialista de seguridad.
- A través de ella se puede determinar si existen actividades hostiles o no en la organización.
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- IDP: Intrusion Detection & Prevention

IDS

- El IDS es como un sniffer, escucha y envía alertas de acuerdo a lo configurado.
- El IPS en cambio detecta algo actividad anómala y la bloquea.
- Tipos de IDS:

1. Network-Based IDS (Nids)

- Monitorean el tráfico del segmento de red donde son instalados

IDS

- Pros
  - No afecta la performance de la red.
  - Invisibles a los atacantes: La NIC de monitoreo no tiene dirección lógica.
  - Reconocen ataques de fragmentación y escaneos.
- Contras
  - Pueden perder paquetes por sobrecarga.
  - Pueden reensamblar mal los paquetes.
  - No informan si un ataque ha sido exitoso o no.
  - No monitorean datos encriptados.

IDS

- Tipos de IDS:
2. Host-Based IDS (Hids)
- Programas que se instalan en el servidor o host y monitorean al sistema operativo constantemente.

IDS

- Pros
  - Monitorean eventos locales.
  - Pueden trabajar con tráfico de red encriptado.
  - No afectado por la red.
- Contras
  - Captura específica al sistema monitoreado.
  - Susceptibles a ataques de DoS.
  - Afecta performance del host donde está instalado.

Contenido (cont.)

3. Defensa
   a. Firewalls
   b. IDS
   c. **Criptografía**
   d. VPN
4. Recomendaciones

Criptografía

- Existen dos tipos de llaves:

1. Llave privada (simétrica)

- Tanto el emisor como el receptor comparten una llave secreta que es utilizada para encriptar y desencriptar los mensajes.
- La ventaja es que son rápidas de utilizar y son utilizadas para encriptar grandes volúmenes de información.

Criptografía

- Existen dos tipos de llaves:
2. Llave pública (asimétrica)
- Se utilizan 2 llaves: una pública y una privada.
- La llave pública está disponible para que cualquiera la pueda utilizar para encriptar mensajes y enviarlos al propietario, el cual desencriptará con la llave privada que solo él conoce.

Criptografía

- Solución de criptografía:

1. La llave pública del receptor es obtenida.
2. Los datos son encriptados con una llave simétrica.
3. La llave simétrica es encriptada con la llave pública del receptor.
4. La llave simétrica encriptada y los datos encriptados son enviados al receptor.
5. El receptor desencripta la llave simétricas con su llave privada.
6. Los datos son desencriptados con la llave simétrica.

Contenido (cont.)

3. Defensa
   a. Firewalls
   b. IDS
   c. Criptografía
   d. VPN
4. Recomendaciones

VPN

- Son sesiones en un canal de comunicaciones autenticado y encriptado en una red pública.
- 3 tipos de túneles:
  1. Lan to Lan: Los ruteadores encriptan.
  2. Host to Lan
  3. Host to Host
- IPSEC es un estándar que provee encriptación a nivel de paquete, autenticación e integridad de mensajes sobre IP.
- Video

Contenido (cont.)

3. Defensa
   a. Firewalls
   b. IDS
   c. Criptografía
   d. VPN
4. **Recomendaciones**

Recomendaciones

- Contar con una política de seguridad.
- Involucrar a la alta gerencia.
- No publicar servicios innecesarios.
- Webs:
  - www.whois.sc
  - www.hackerhighschool.org
  - www.isecom.org
  - www.insecure.org
  - www.eccouncil.org
  - www.sans.org

MUCHAS GRACIAS