

# Políticas de Seguridad en entornos GNU

---

Sancho Lerena  
slerena@gnusec.com



"Software Libre" es cuestión de libertad, no de precio. "Free" en "free software" es una palabra que debe ser traducida como "libre" tal como en "libertad de expresión" ("Free speech"); no como "Gratis" como en "cerveza gratuita" ("Free beer").

[www.gnu.org](http://www.gnu.org)

# Indice

Parte 1. Introduccion

Parte 2. Políticas de Seguridad

a) Analisis

b) Diseño

Parte 3. Implementacion

a) Arquitectura de redes seguras

B) Seguridad Perimetral

1) Firewall. Netfilter

- Inspeccion de estados
- NAT
- Filtrado
- Cadenas
- Scripting
- Modulos
- HA con VRRP

# Indice (continuación)

## B) Seguridad Perimetral (continuacion)

### 2) IDS. Snort

- Arquitectura
- Respuestas
- Integracion de resultados

### 3) Securización

## C) Gestion y monitorizacion

MRTG

NTOP

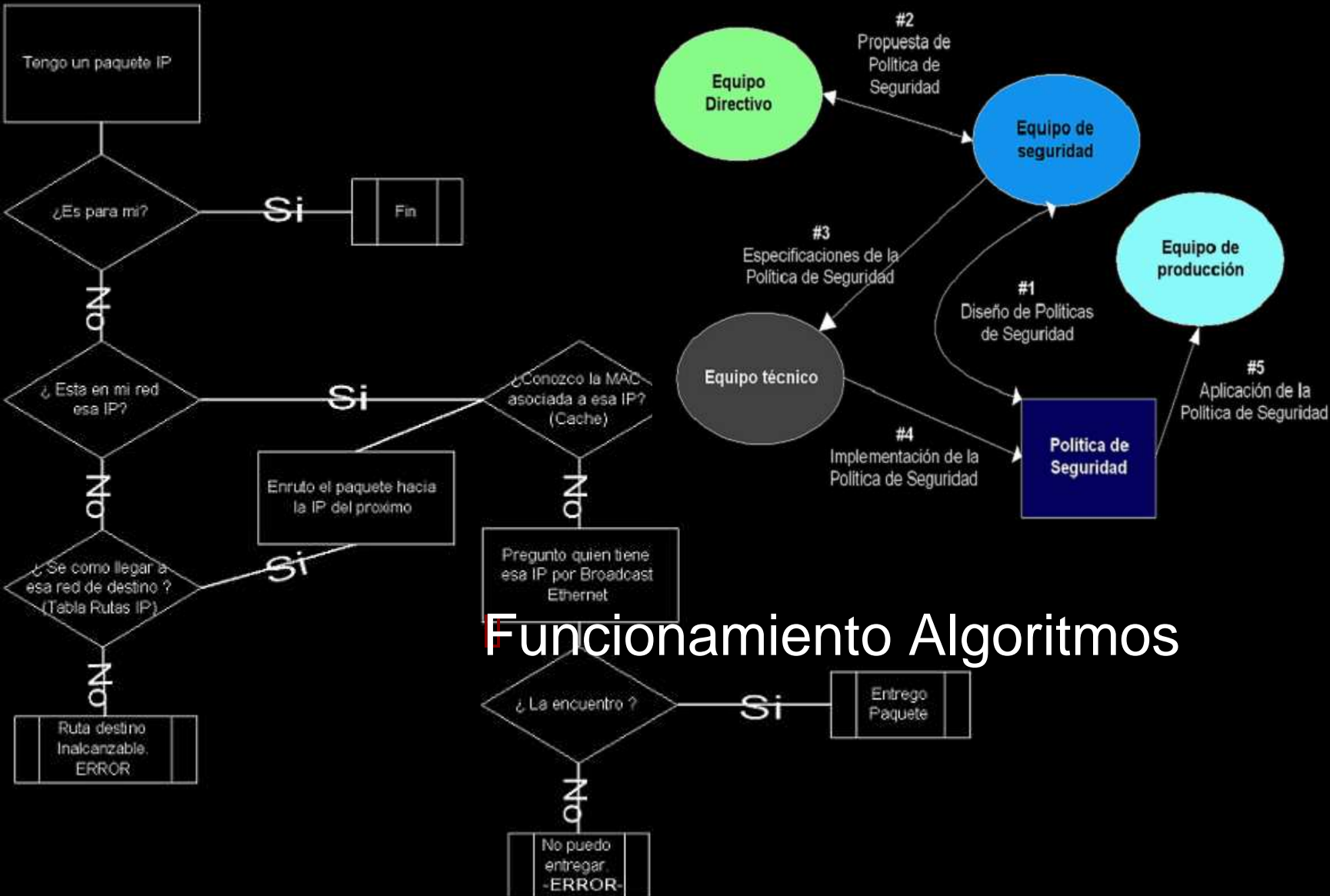
Iptraf

Parte IV. Auditorias de Seguridad.

Parte V. Recursos de seguridad.

# Avance

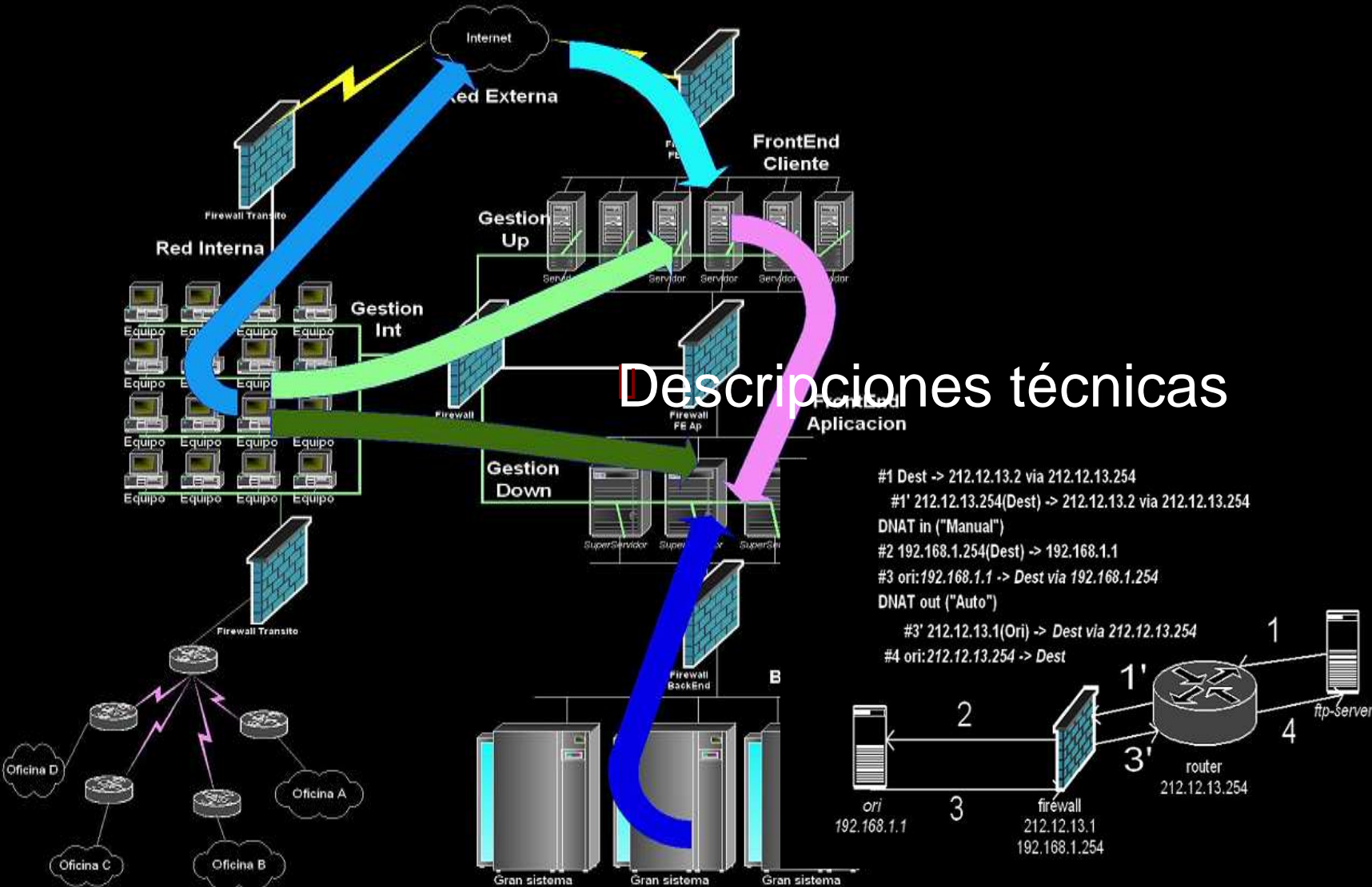
## Teoría organizativa



## Funcionamiento Algoritmos

# Avance

## Arquitectura real de redes



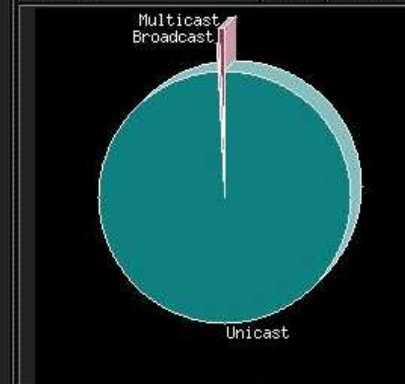
# Avance

## Gestion y control

About Data Rcvd Data Sent Stats IP Traffic IP Protos Admin

### Global Traffic Statistics

Nw Interface Type	eth1 (Ethernet) [0.0.0.0/255.255.255.255]	
Sampling Since	Mon Mar 11 13:29:03 2002 [1 day(s) 5:49:56]	
<b>Total</b>	23,454,865	
Dropped by the kernel	0	
Dropped by ntop	0	
Unicast	99.1%	23,243,902
Broadcast	0.0%	703
Multicast	0.9%	210,260



Shortest	60 bytes	
Average Size	596 bytes	
Longest	1,514 bytes	
< 64 bytes	44.5%	10,429,081
< 128 bytes	16.2%	3,804,516
< 256 bytes	9.4%	2,207,388
< 512 bytes	5.7%	1,325,668



Stats

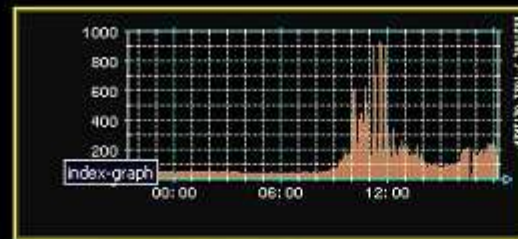
Multicast

Traffic

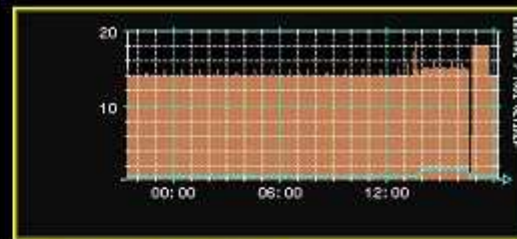
Hosts

Network Load

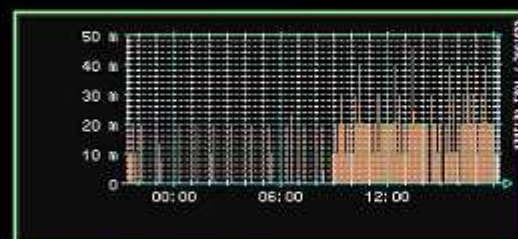
Trafico en FWExt-Gestion1 (Pag/Sec)



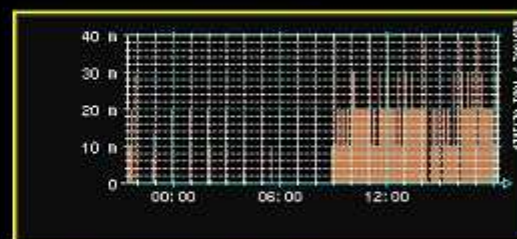
Trafico en FWExt-Gestion2 (Pag/Sec)



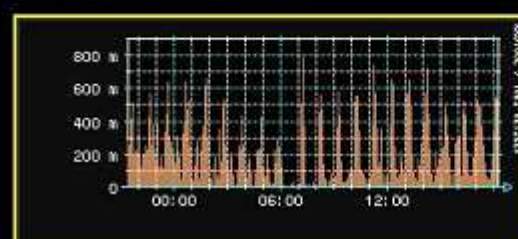
Trafico en FWINT-1 (Pag/Sec)



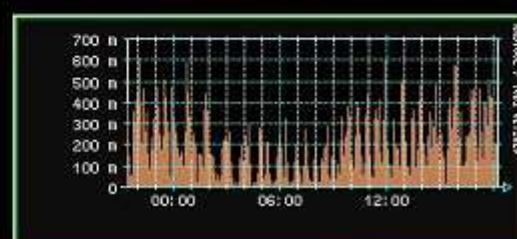
Trafico en FWINT-2 (Pag/Sec)



Trafico en FWINT-3 (Pag/Sec)



Trafico en FWINT-4 (Pag/Sec)



Trafico en FWINT-Gestion1 (Pag/Sec)

Trafico en FWINT-Gestion2 (Pag/Sec)

#### Total Control

#### Firewalls

- FW-Ext1
- FW-Ext2
- FW-Ext3
- FW-Ext4
- FW-ExtGes1
- FW-ExtGes2
- FW-Int1
- FW-Int2
- FW-Int3
- FW-Int4
- FW-IntGes1
- FW-IntGes2

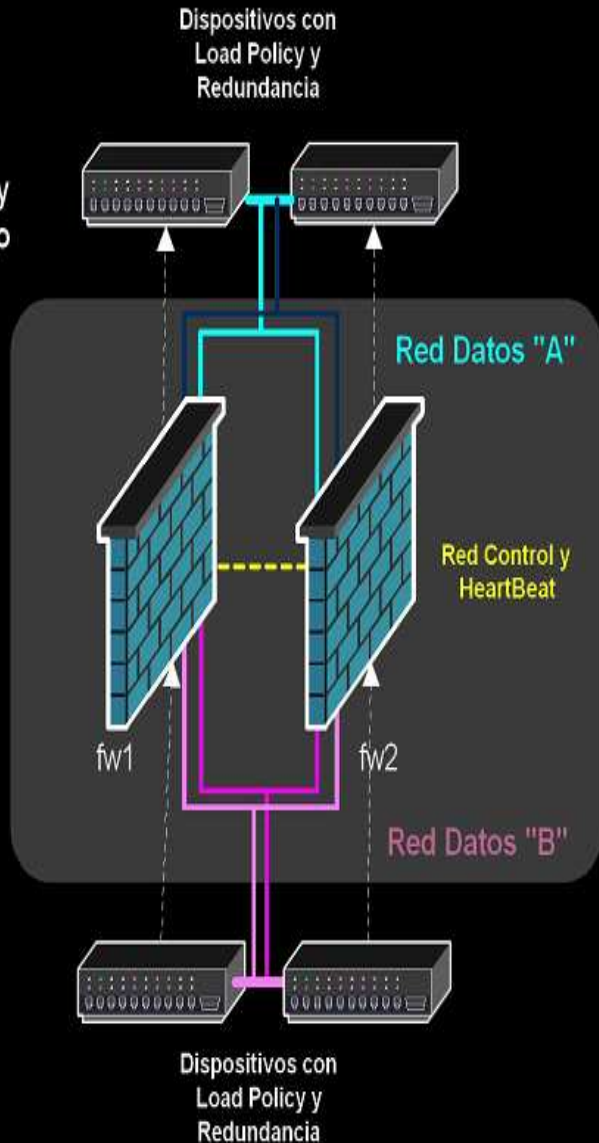
#### Routers

- Talia Albasanz
- Albasanz->Moraleja
- Albasanz->ParcBit
- Albasanz->Moraleja
- Moraleja->Albasanz
- Moraleja->ParcBit
- Moraleja->Castellana
- ParcBit->Moraleja
- ParcBit->Castellana
- ParcBit->Moraleja
- Castellana->Moraleja
- Castellana->ParcBit
- Castellana->Moraleja

# Avance

## Teoría

Firewall HA  
Hot-StandBy  
con Balanceo



## ... y práctica

```
#!/bin/bash
# Checking connectivity with ICMP Ping, VRRPD Companion Script
VER="11/03/2002 - v1.0"
SLEEP_TIME=$2          # Tiempo de parada entre checks, en segundos
if [ -z $2 ]
then
    SLEEP_TIME=5       # Si no se especifica, el check es cada 5 segundos
fi;
# Obtener el PID de los procesos de VRRPD en memoria
LISTA_PROCESOS=`ps -A | grep "vrrpd" | tr -s " " | cut -d " " -f 2`
if [ -z "$LISTA_PROCESOS" ]
then
    echo " No VRRP Daemon running, aborting. "
    exit
fi;
IP_DESTINO=$1          # IP de comprobacion, pasada como 1º parametro
COMANDO="`ping -c 1 "$IP_DESTINO" | grep '100% packet loss'`"
RES=0
while [ "$RES" -eq 0 ];do
    if [ ! -z "$COMANDO" ] ;then
        echo " Ping fail "
        echo " Shutting down VRRP daemons "
        kill -s 9 $LISTA_PROCESOS
        RES=1;else
            echo " Debug: Ping ok"
            sleep $SLEEP_TIME
        fi;done;
```

# Parte I. Introduccion a la seguridad





# GNU y Seguridad

¿ Que es la Seguridad ?.

┆ Lógica

┆ Física

┆ Redes

    Firewalls

    IDS

┆ Hosts/Aplicaciones

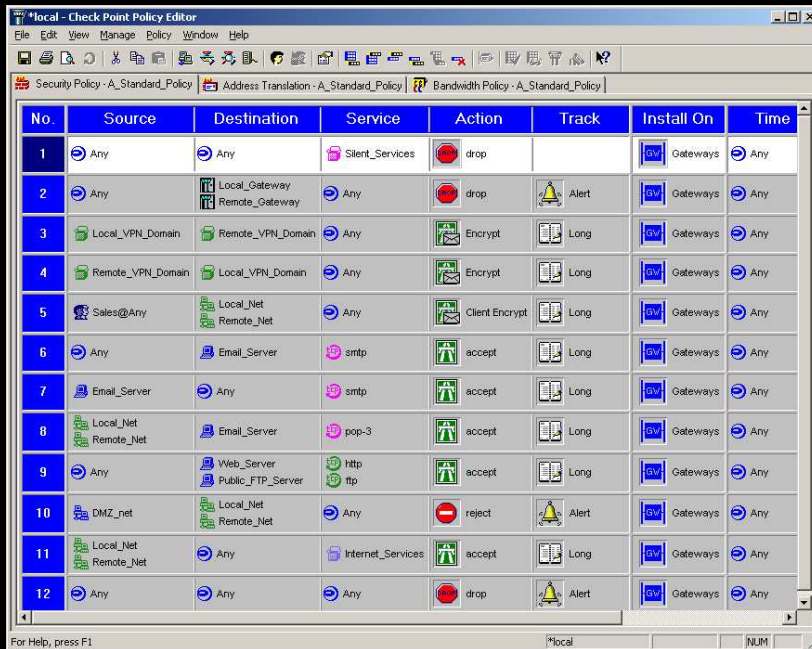


Software Abierto vs Software Cerrado

┆ Soporte y otros “problemas”

# GNU y Seguridad I

## Software Abierto vs Software Cerrado



The screenshot shows the Check Point Policy Editor interface. The main window displays a table with 12 rows of security policies. The columns are: No., Source, Destination, Service, Action, Track, Install On, and Time. The policies are numbered 1 through 12.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	Any	Silent_Services	drop		Gateways	Any
2	Any	Local_Gateway Remote_Gateway	Any	drop	Alert	Gateways	Any
3	Local_VPN_Domain	Remote_VPN_Domain	Any	Encrypt	Long	Gateways	Any
4	Remote_VPN_Domain	Local_VPN_Domain	Any	Encrypt	Long	Gateways	Any
5	Sales@Any	Local_Net Remote_Net	Any	Client Encrypt	Long	Gateways	Any
6	Any	Email_Server	smtp	accept	Long	Gateways	Any
7	Email_Server	Any	smtp	accept	Long	Gateways	Any
8	Local_Net Remote_Net	Email_Server	pop-3	accept	Long	Gateways	Any
9	Any	Web_Server Public_FTP_Server	http ftp	accept	Long	Gateways	Any
10	DMZ_net	Local_Net Remote_Net	Any	reject	Alert	Gateways	Any
11	Local_Net Remote_Net	Any	Internet_Services	accept	Long	Gateways	Any
12	Any	Any	Any	drop	Alert	Gateways	Any

```
# Filtrado: FORWARDING
# =====

echo "Activamos filtrado de forward (FORWARD)..."
echo "Dejamos pasar las conexiones ESTABLECIDAS o RELATIVAS a las establecidas..."
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

echo "Las conexiones bidireccionales..."
iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT # ping
iptables -A FORWARD -p icmp --icmp-type echo-request -j ACCEPT # ping
iptables -A FORWARD -p udp --dport 53 -j ACCEPT # DNS
iptables -A FORWARD -p udp --sport 53 -j ACCEPT # DNS
iptables -A FORWARD -s #LOCALNET -p udp --dport 161:162 -j ACCEPT # SNMP

echo "Las conexiones entrantes hacia " #IRIS
iptables -A FORWARD -d #IRIS -p tcp --dport 21 -j ACCEPT # FTP en ARES
iptables -A FORWARD -d #IRIS -p tcp --dport 22 -j ACCEPT # SSH
iptables -A FORWARD -d #IRIS -p tcp --dport 23 -j ACCEPT # Telnet
iptables -A FORWARD -d #IRIS -p tcp --dport 80 -j ACCEPT # HTTP Apache puerto 80
#iptables -A FORWARD -d #IRIS -p tcp --dport 8080 -j ACCEPT # HTTP Proxy SQUID
iptables -A FORWARD -d #IRIS -p tcp --dport 25 -j ACCEPT # SMTP
iptables -A FORWARD -d #IRIS -p tcp --dport 110 -j ACCEPT # POP
iptables -A FORWARD -d #IRIS -p tcp --dport 443 -j ACCEPT # HTTPS
iptables -A FORWARD -d #IRIS -p tcp --dport 6346 -j ACCEPT # Gnutella

echo "Las conexiones entrantes hacia " #HERCULES
iptables -A FORWARD -d #HERCULES -p tcp --dport 261 -j ACCEPT # Pruebas CURRO ***** (Auth
FW-1)
iptables -A FORWARD -d #HERCULES -p tcp --dport 5900 -j ACCEPT # VNC
iptables -A FORWARD -d #HERCULES -p tcp --dport 21 -j ACCEPT # FTP en Hercules
iptables -A FORWARD -d #HERCULES -p tcp --dport 4661 -j ACCEPT # eDonkey2000

iptables -A FORWARD -d #HERCULES -p tcp --dport 5631 -j ACCEPT # PCAnyWhere

echo "Las conexiones entrantes hacia " #ARES
iptables -A FORWARD -d #ARES -p tcp --dport 5901 -j ACCEPT # VNC
iptables -A FORWARD -d #ARES -p tcp --dport 23 -j ACCEPT # SSH
```

# GNU y Seguridad II

## GNU y Empresa

- ▣ Diferentes tecnologías

  - ▣ Contraste

  - ▣ Seguridad

  - ▣ Variedad

- ▣ Aplicaciones fuera de entornos críticos

- ▣ Alternativas de bajo coste

- ▣ Funcionalidades más flexibles



# GNU y Seguridad III

## Teoría vs Práctica en la seguridad

- Falta de conocimientos

- Prisas y falta de profesionalidad

- GUI's

- Capacidad de Organización y de escalabilidad.



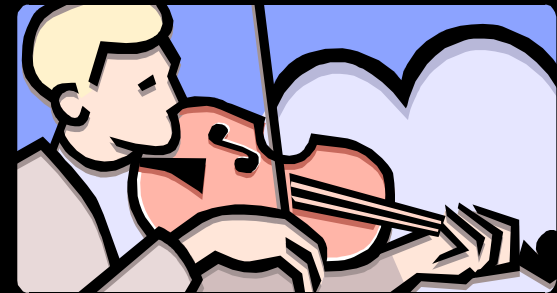
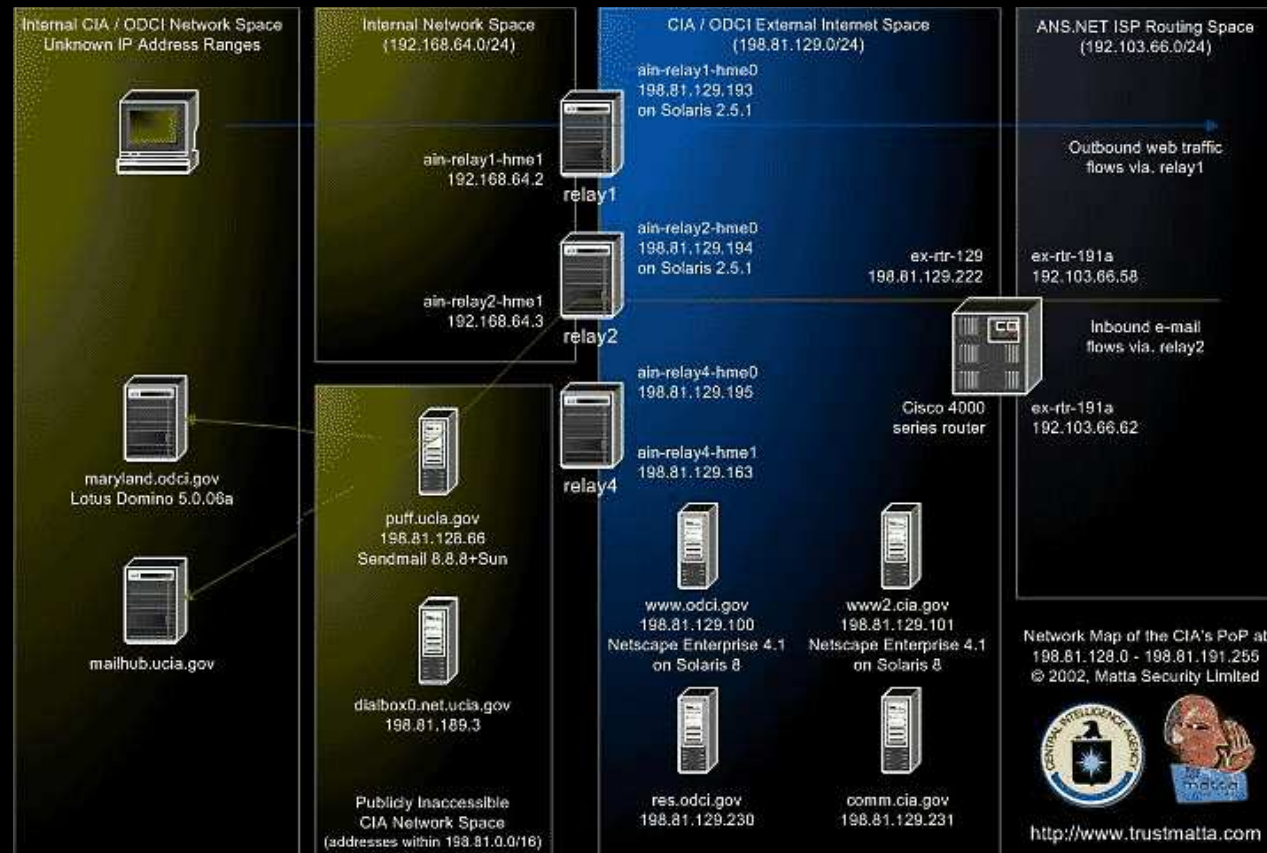
## ¿ Es GNU Seguro ?

- Código Abierto

- Documentación

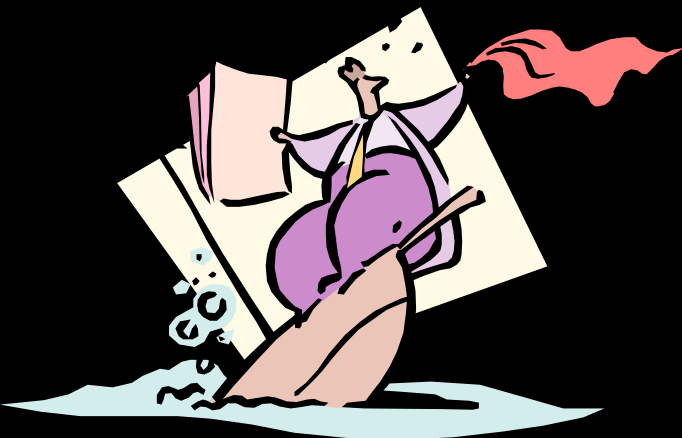
# Un poco de miedo I

Un buen día....



# Un poco de miedo II

www.kenwood.cd



h0h0h0 sorry but Site iz Owned - Mozilla {Build ID: 2002031104}

File Edit View Search Go Bookmarks Tasks Help Debug QA

Back Forward Reload Stop <http://black.box.s> Search Print

DeathSymb0L owned this site!

death-team@hotmail.com

**DeathSymb0L never die.. He Iz BACK phuck yew all**

DeathSymb0L >> yooo amir\_007 and hilfiger

Oo..We've g0t the p0wer..o0

**FREE Palestine and Kashmir**

Dedicated to: GForce - m0r0n and nightman [WFD] - WoH - Ob1TuarY - InfernoZ  
- \_eclipse - cowhead2000 - RuBiX - Astalav|sta - backslash - Dev|LSouL - s0nu  
- D-Force - n01d - databoy [all of SupremeEntity] - PrimeSuspect - SilverLords  
- encrypt0 - DataCha0s - Quit Crew - n00gie - r00t-access crew - tty0 -  
Cr1meLordz - BHS - grimR - Sub-0 and all knows us

Document: Done (0.741 secs)

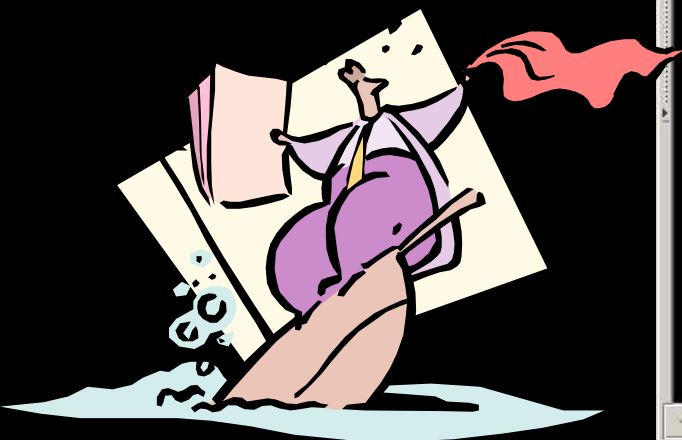
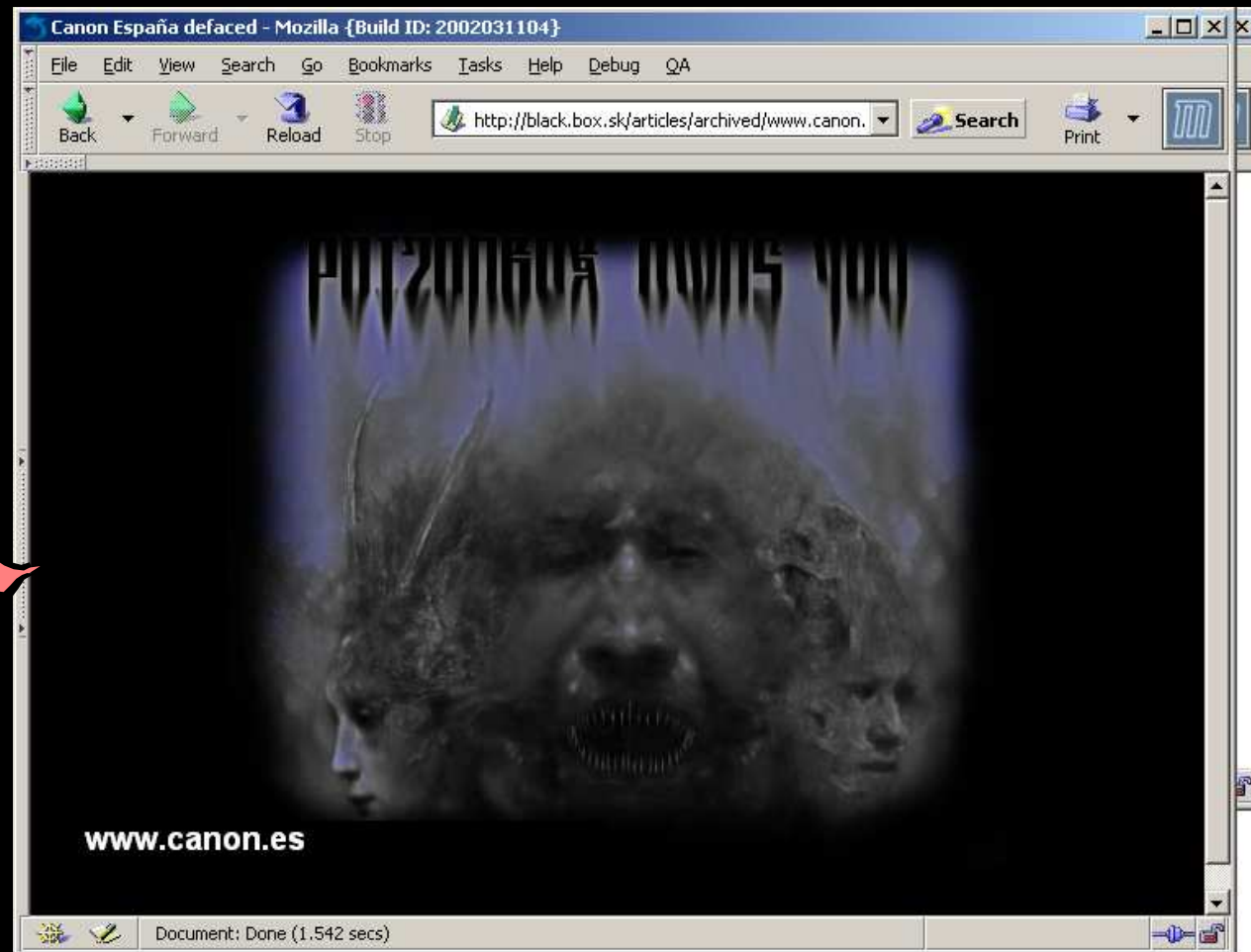
# Un poco de miedo III

[www.securitybase.com](http://www.securitybase.com)



# Un poco de miedo IV

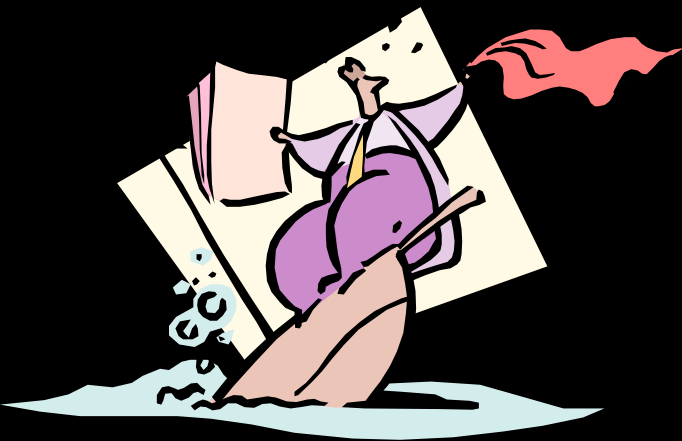
[www.canon.es](http://www.canon.es)





# Un poco de miedo V

[www.securecreditcard.net](http://www.securecreditcard.net)



```
MNS MNS MNS - Mozilla {Build ID: 2002031104}
File Edit View Search Go Bookmarks Tasks Help Debug QA
Back Forward Reload Stop http://black.br Search Print
Stop loading this page

Connected to target.
Escape character is '^]'.

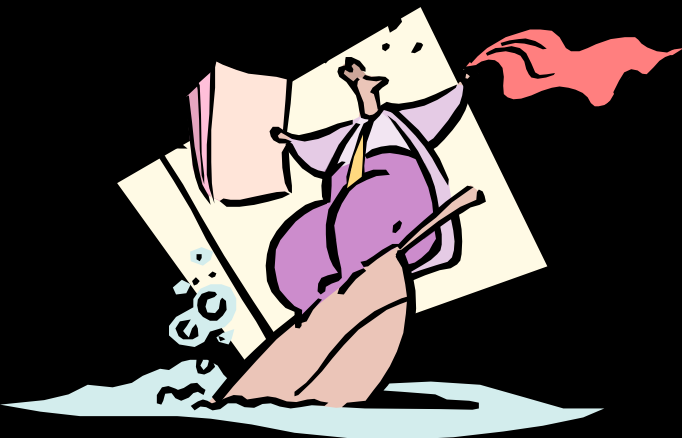
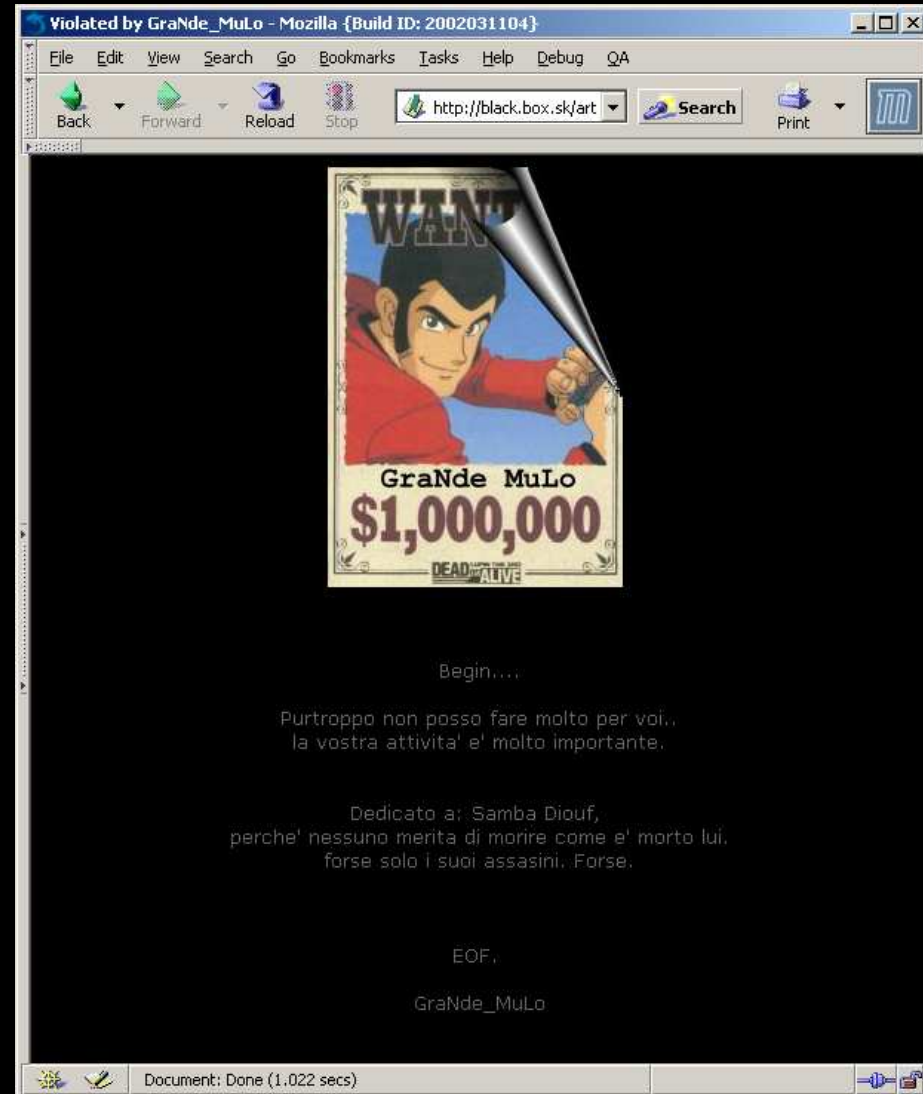
-----
| owned by: Tw34k
| mnssecure@hotmail.com
|
| greetz: sENsE - Xentric - D-force - data cha0s
|         world-of-hell - Prime suspectz - null
|
-----

[root@mns_ownz_you root]#
```

Document: Done (0.631 secs)

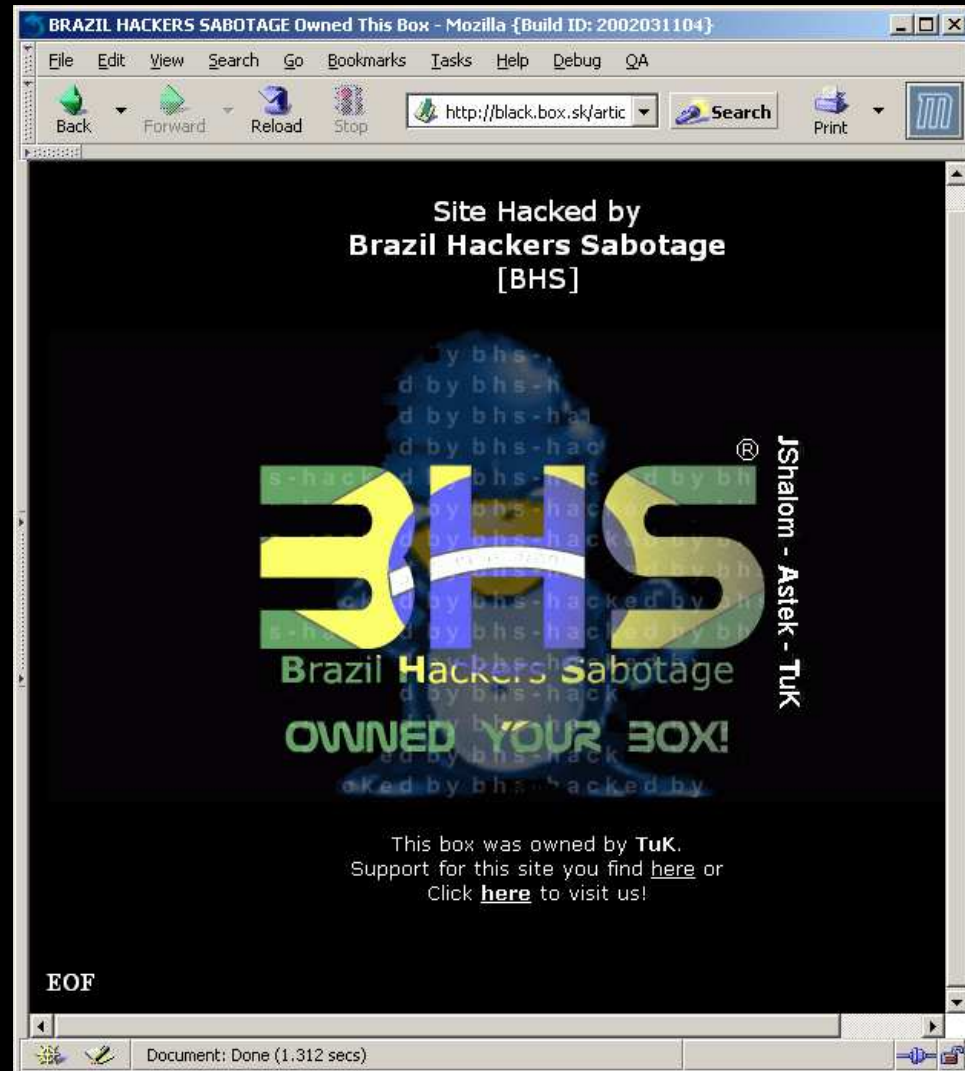
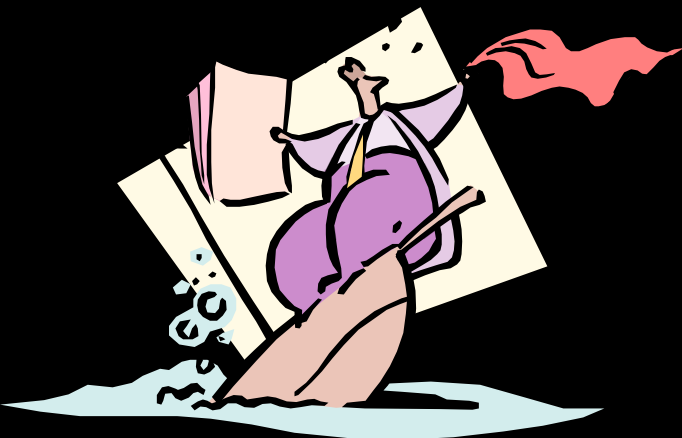
# Un poco de miedo VI

[www.exodus.it](http://www.exodus.it)



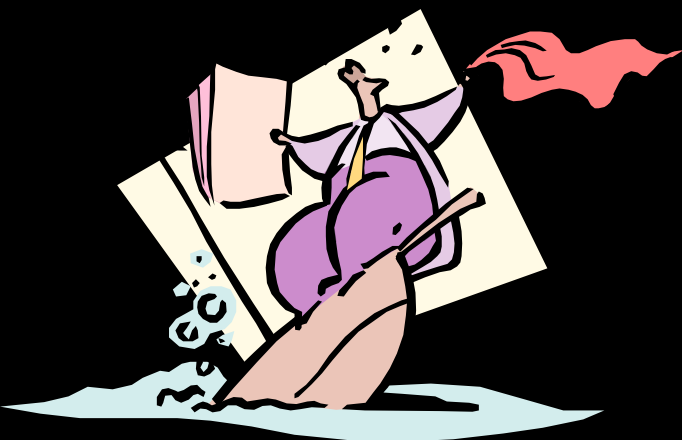
# Un poco de miedo VII

www.comntel.com



# Un poco de miedo VIII

[www.fox.dk](http://www.fox.dk)



# Un poco de miedo IX

## Algunas noticias sobre seguridad

(neworder.box.sk)

**The MadMan** writes: Corporate security and IT professionals got a **game** chance last week to think like hackers so they could learn how to better prevent unauthorized users from gaining access to their networks.

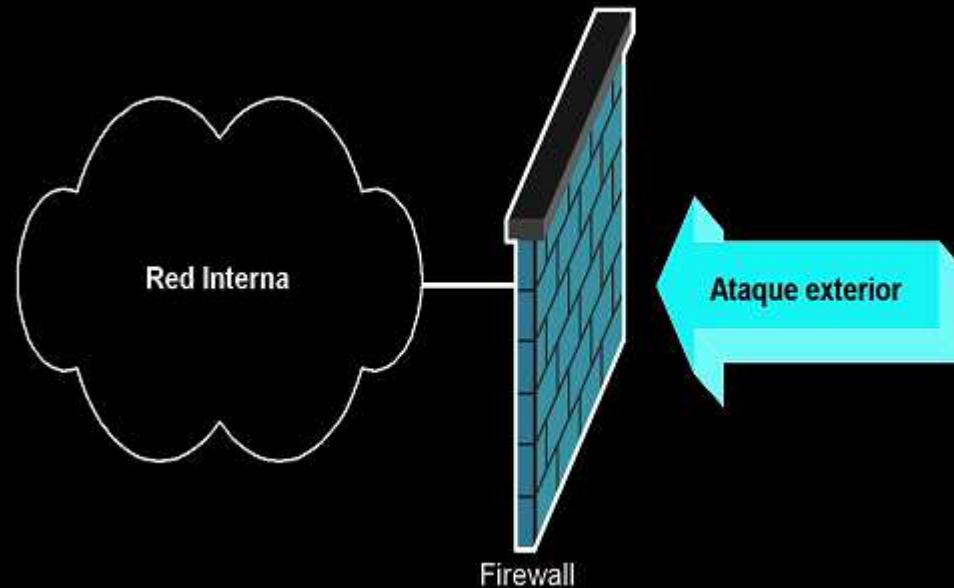
More than a dozen computer specialists from across the country took part in an intensive five-day "boot camp" offered by New York-based Ernst & Young LLP on the defense of enterprise networks. They paid

**\$5,000** apiece for the training here.

[Read More](#)  
[read comments \(0\)](#) | [write comment](#)



# La seguridad no es...



Ni un firewall “tonto” (*Filtrado Simple*)

Ni tampoco un Firewall “listo” (*Filtrado de estados*).