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

Indice

1. Parte 1. Introduccion
2. Parte 2. Políticas de Seguridad
    a) Analisis
    b) Diseño
3. 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)

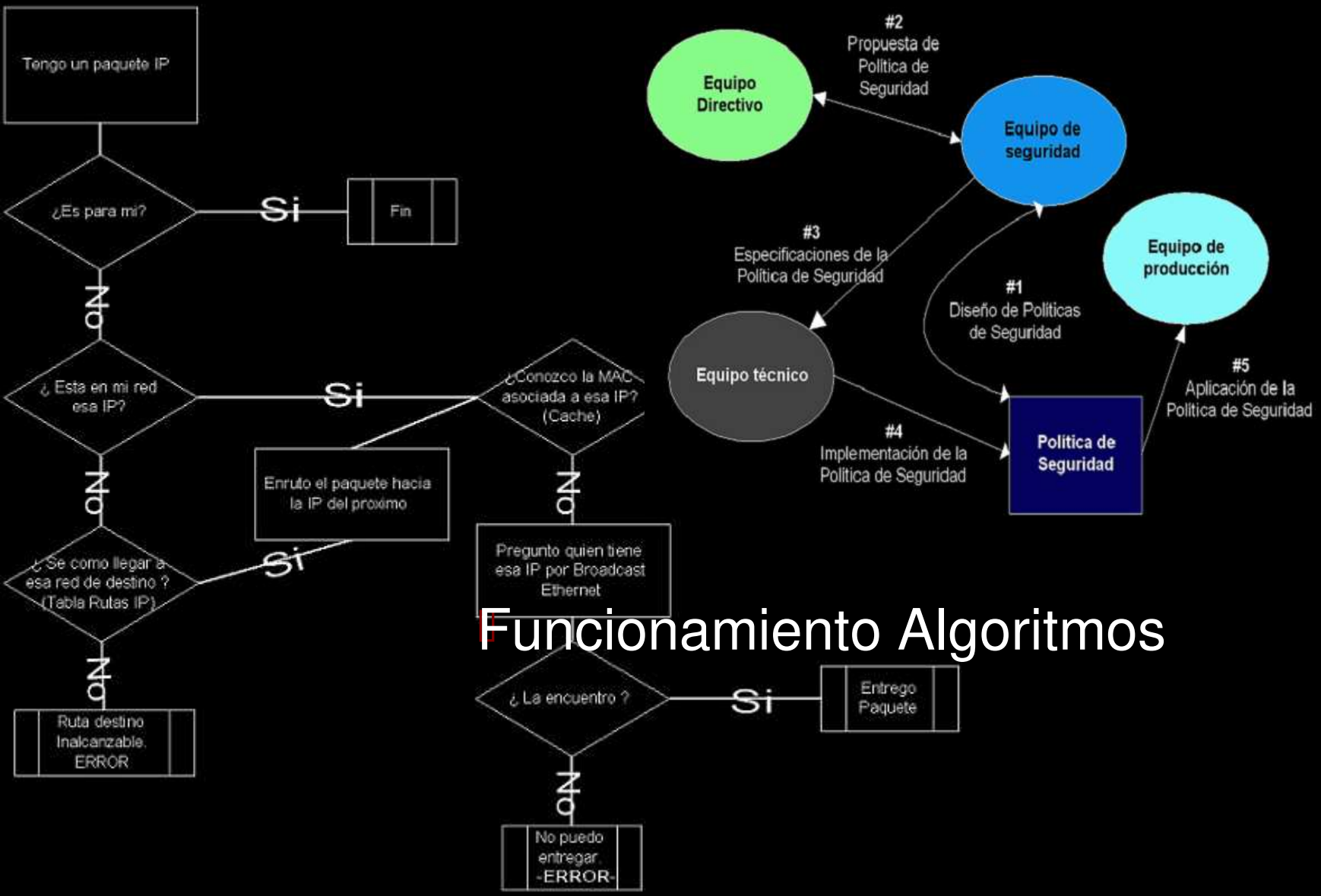
- B) Seguridad Perimetral (continuacion)
  - 2) IDS. Snort
    - Arquitectura
    - Respuestas
    - Integracion de resultados
  - 3) Securización
- C) Gestion y monitorizacion
  - MRTG
  - NTOP
  - Iptraf

Parte IV. Auditorias de Seguridad.

Parte V. Recursos de seguridad.

Avance

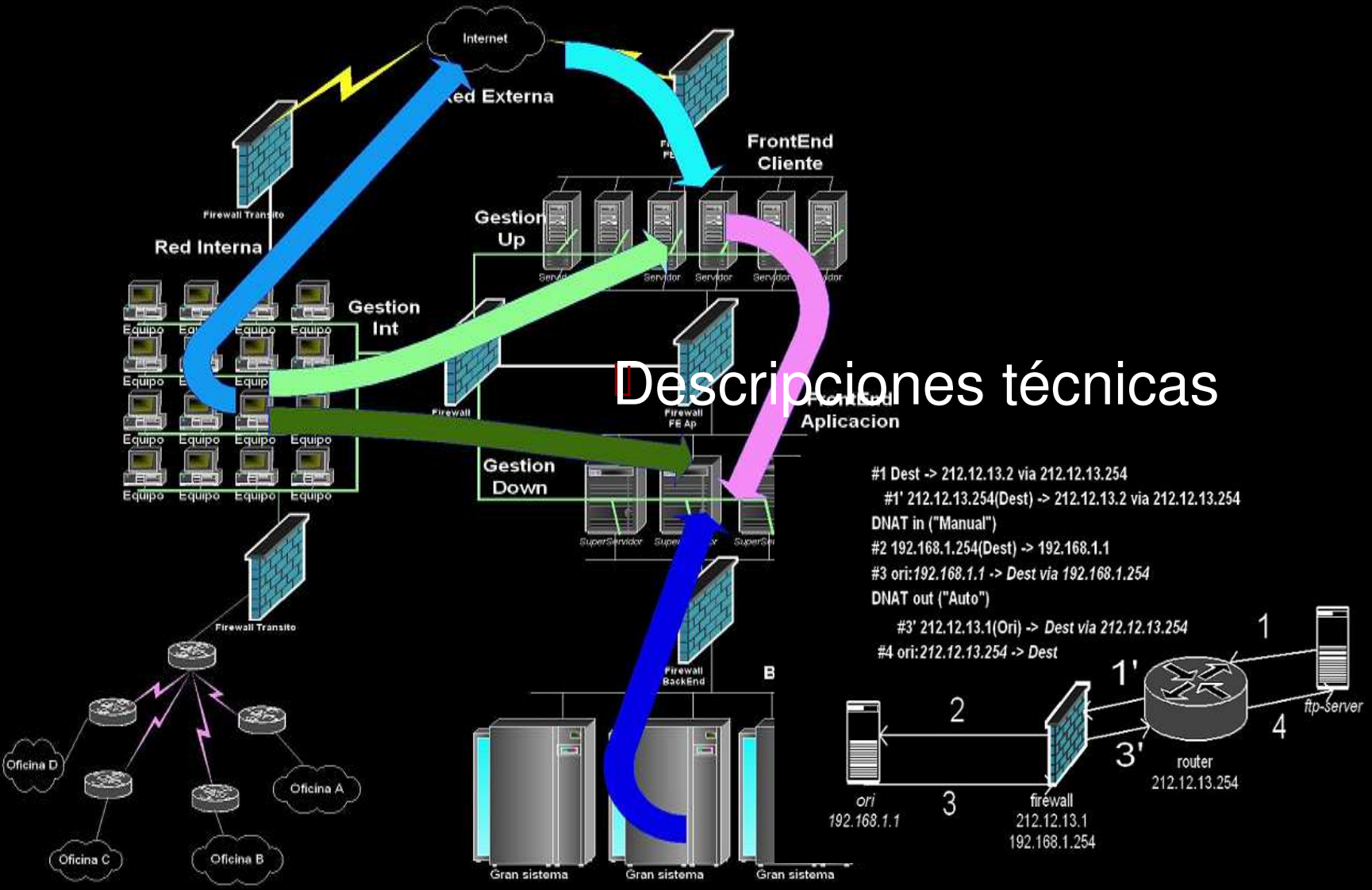
- Teoría organizativa



- Funcionamiento Algoritmos

Avance

- Arquitectura real de redes

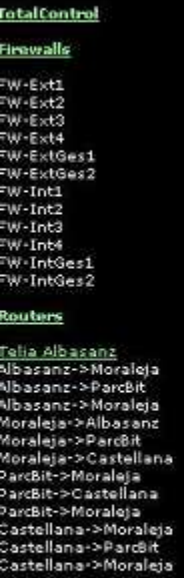


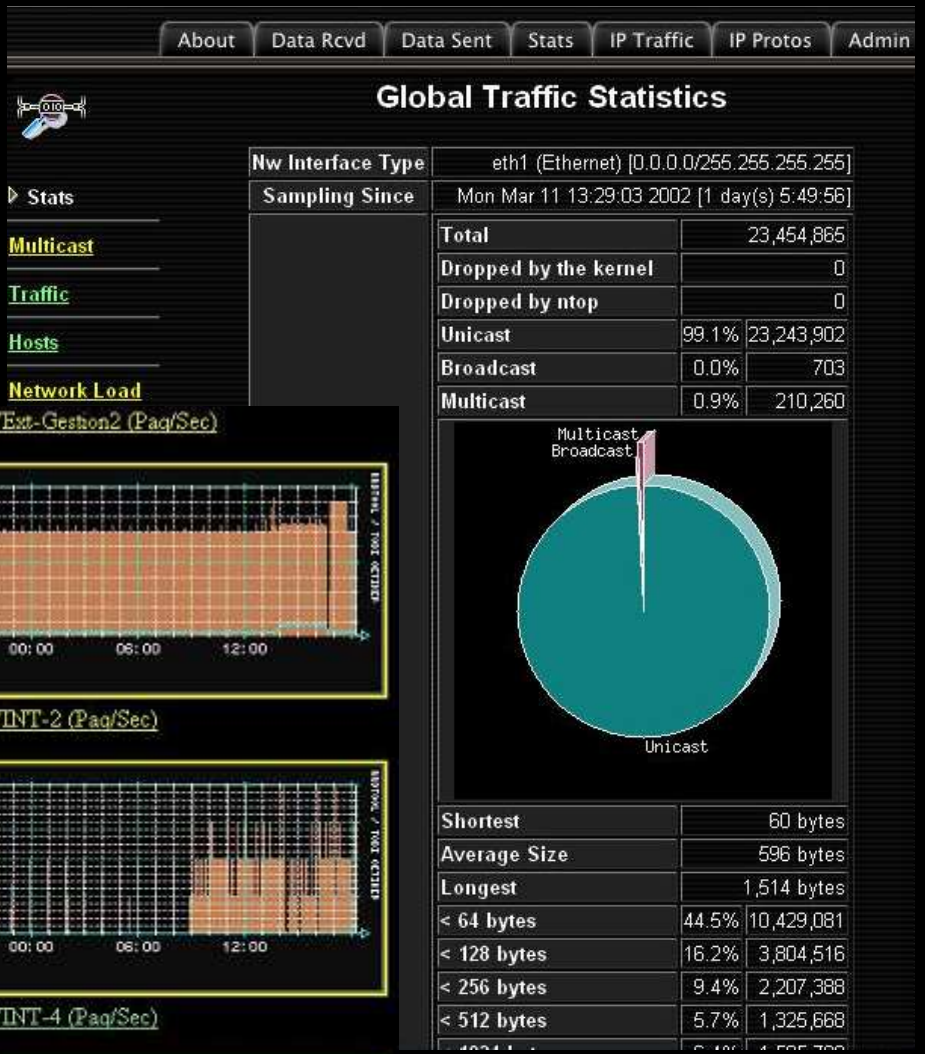
- Descripciones técnicas

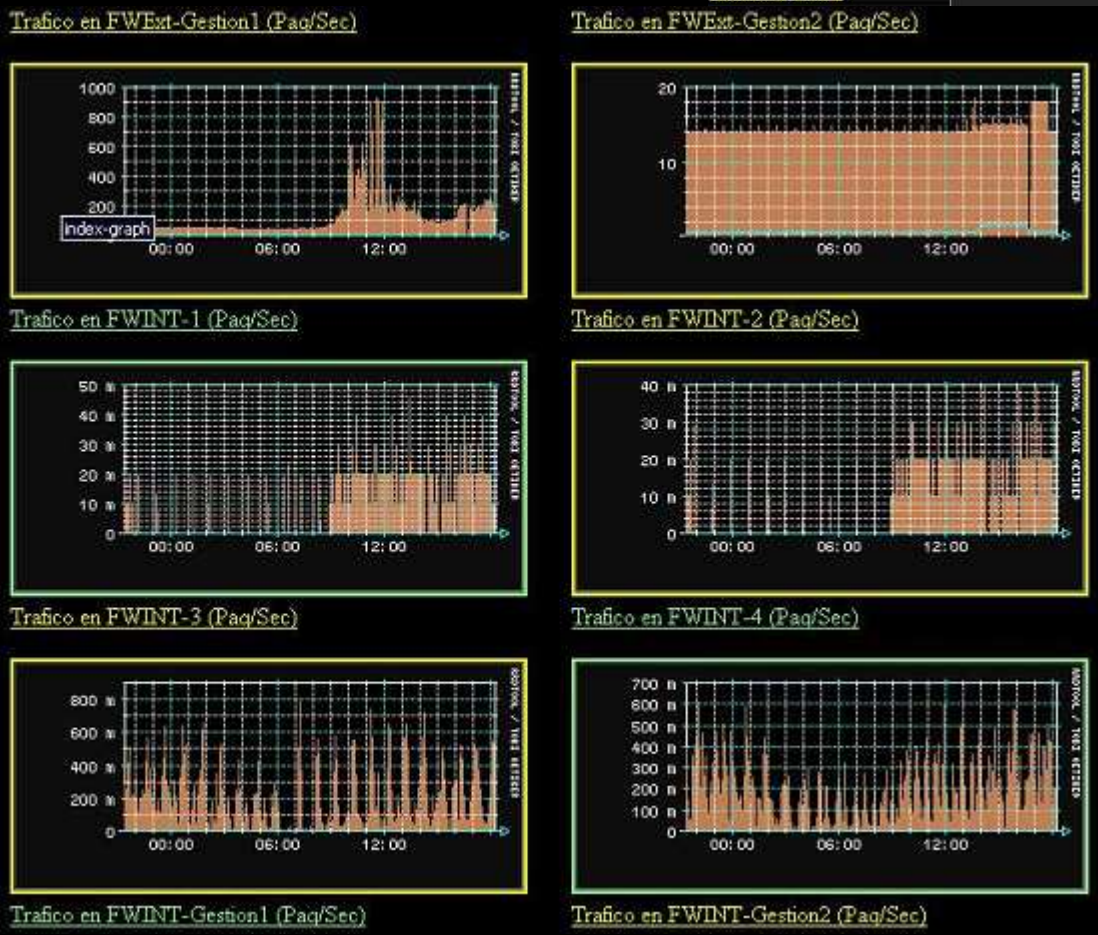
#1 Dest -> 212.12.13.2 via 212.12.13.254
#1' 212.12.13.254(Dest) -> 212.12.13.2 via 212.12.13.254
DNAT in ("Manual")
#2 192.168.1.254(Dest) -> 192.168.1.1
#3 ori:*192.168.1.1 -> Dest via 192.168.1.254*
DNAT out ("Auto")
#3' 212.12.13.1(Ori) -> *Dest via 212.12.13.254*
#4 ori:*212.12.13.254 -> Dest*

Avance

Gestion y control

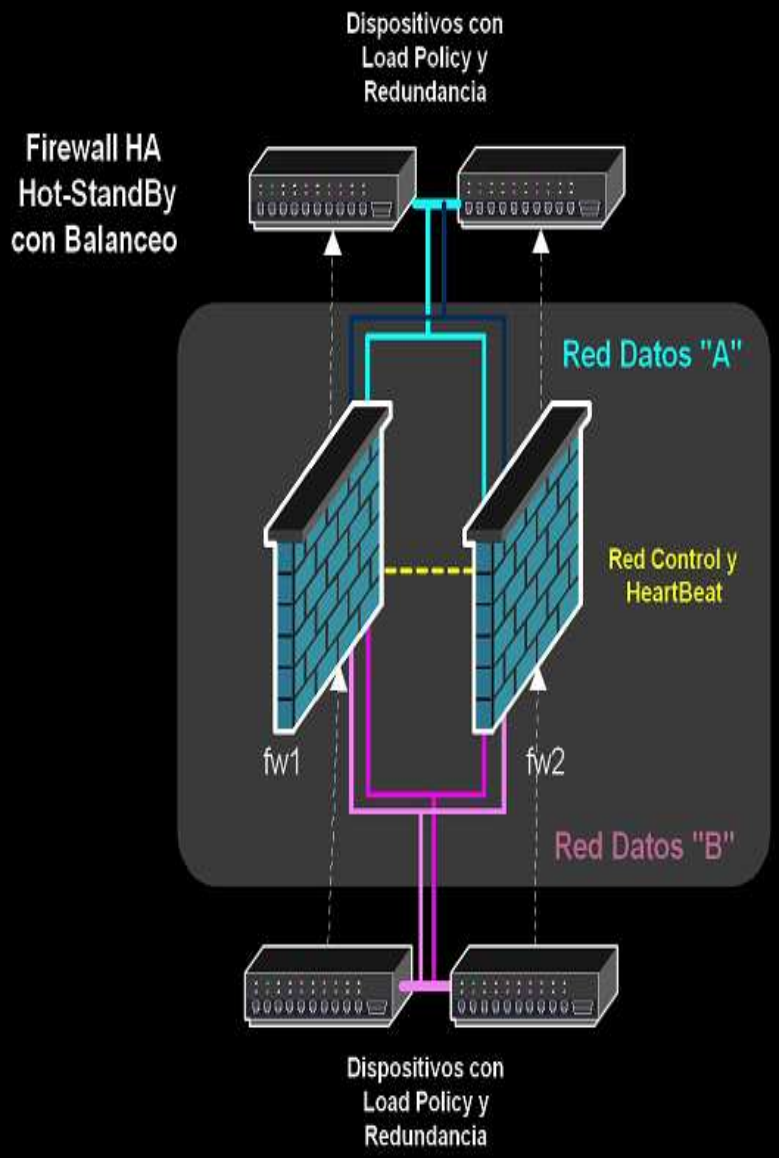






Avance

Teoría



.. y práctica

```
#!/bin/bash
# Checking conectivity 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=$1             # IP de comprobacion, pasada como 1# parametro
COMANDO="`ping -c 1 "$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

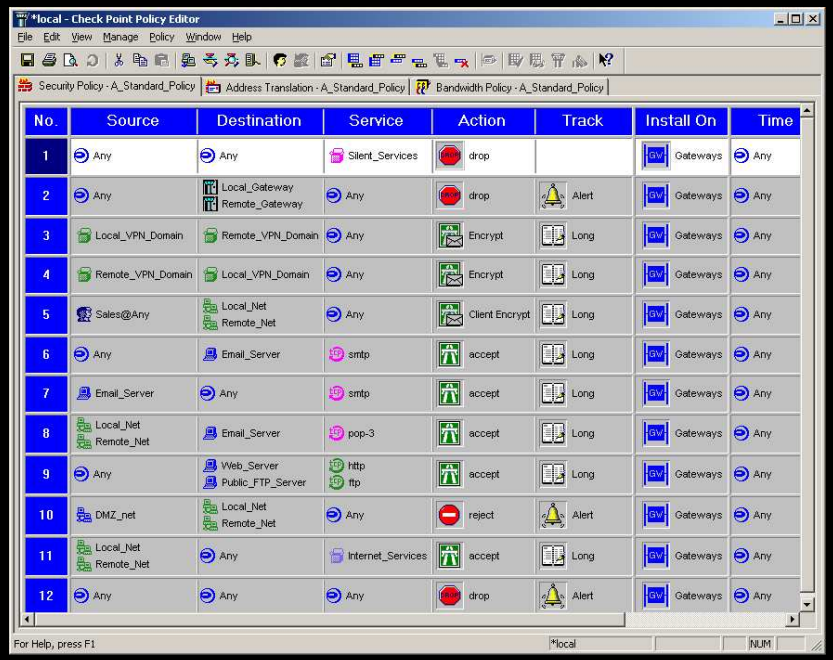
GNU y Seguridad

- ¿ 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




```
# 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

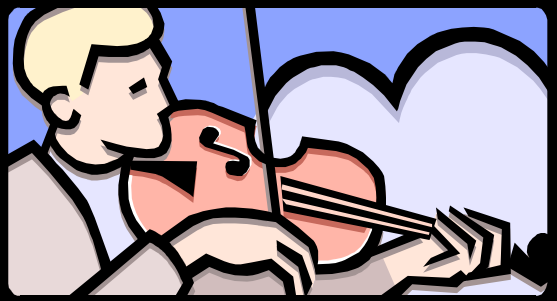
GNU y Seguridad III

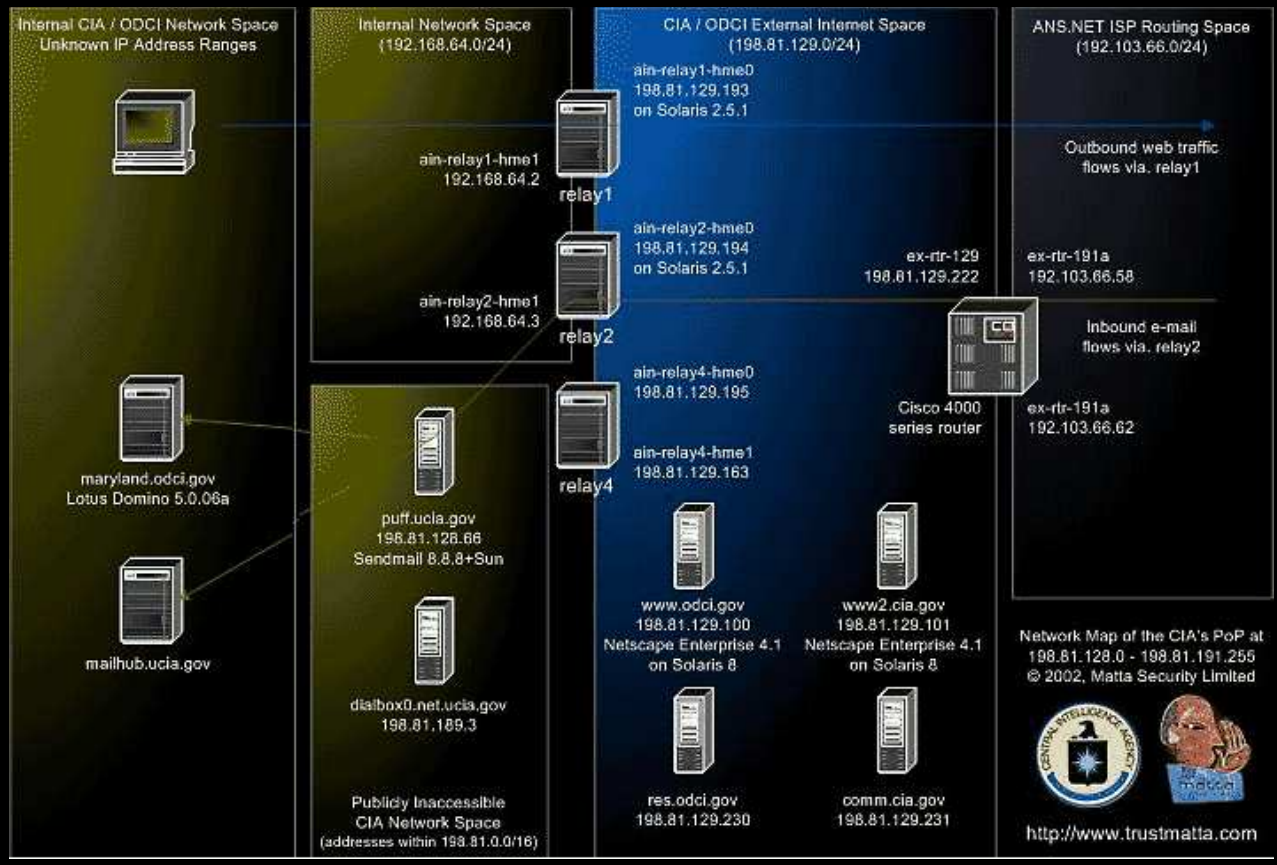
- Teoría vs Práctica en la seguridad
  - Falta de conocimientos
  - Prisas y falta de profesionalidad
  - GUI's
  - Capacidad de Organización y de escalabilidad.

- ¿ Es GNU Seguro ?
  - Código Abierto
  - Documentación

Un poco de miedo I

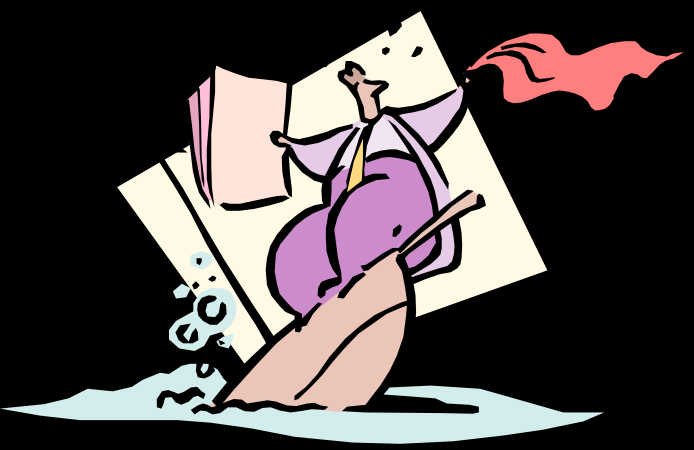
Un buen día....

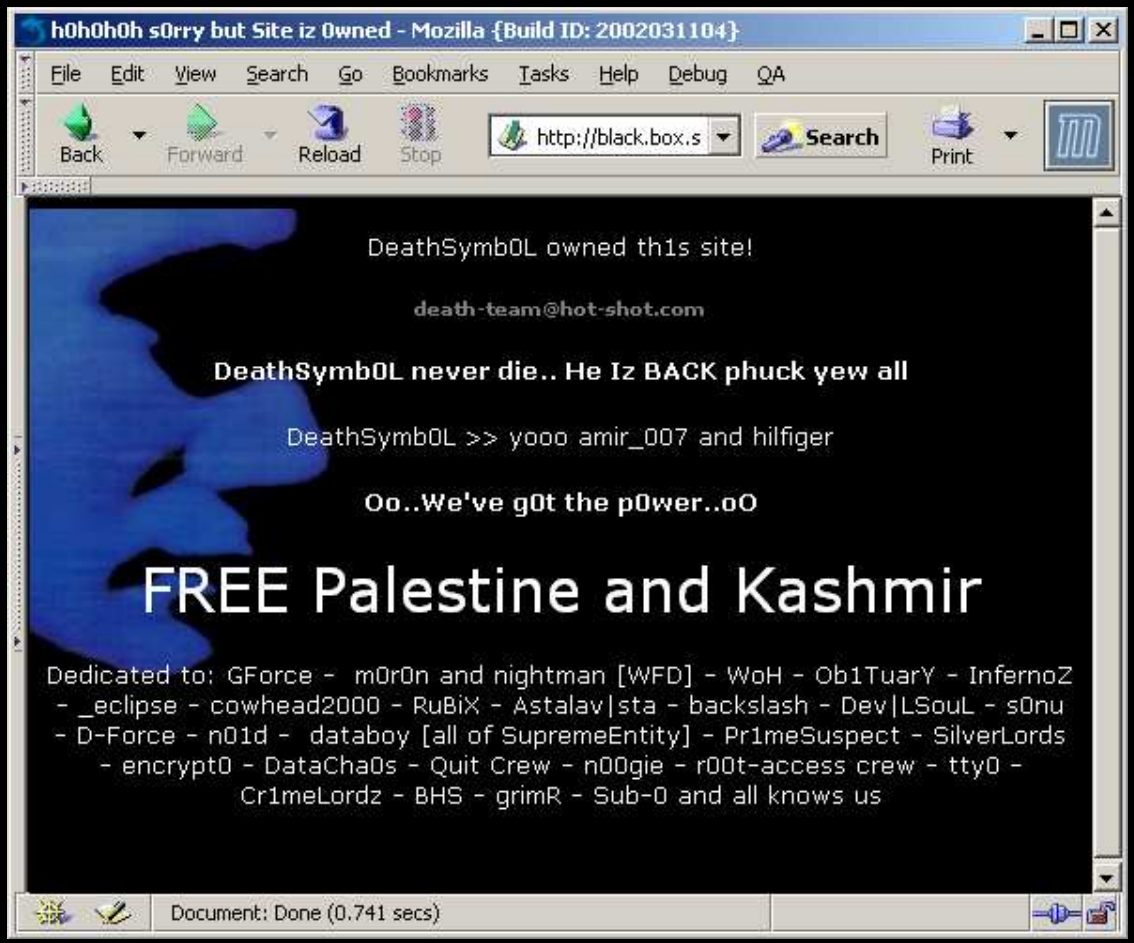




Un poco de miedo II

www.kenwood.cd



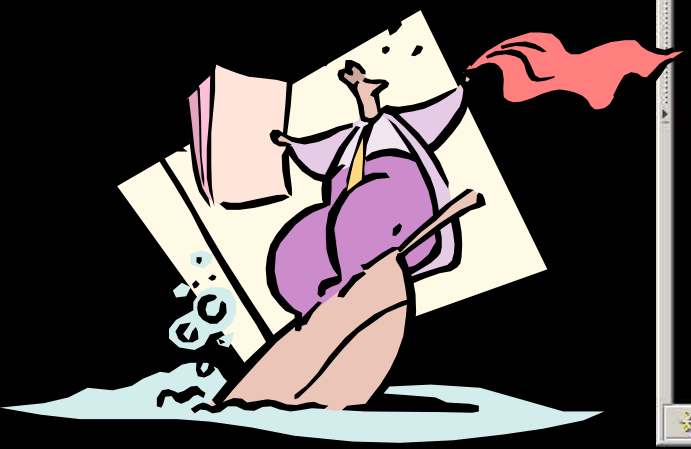


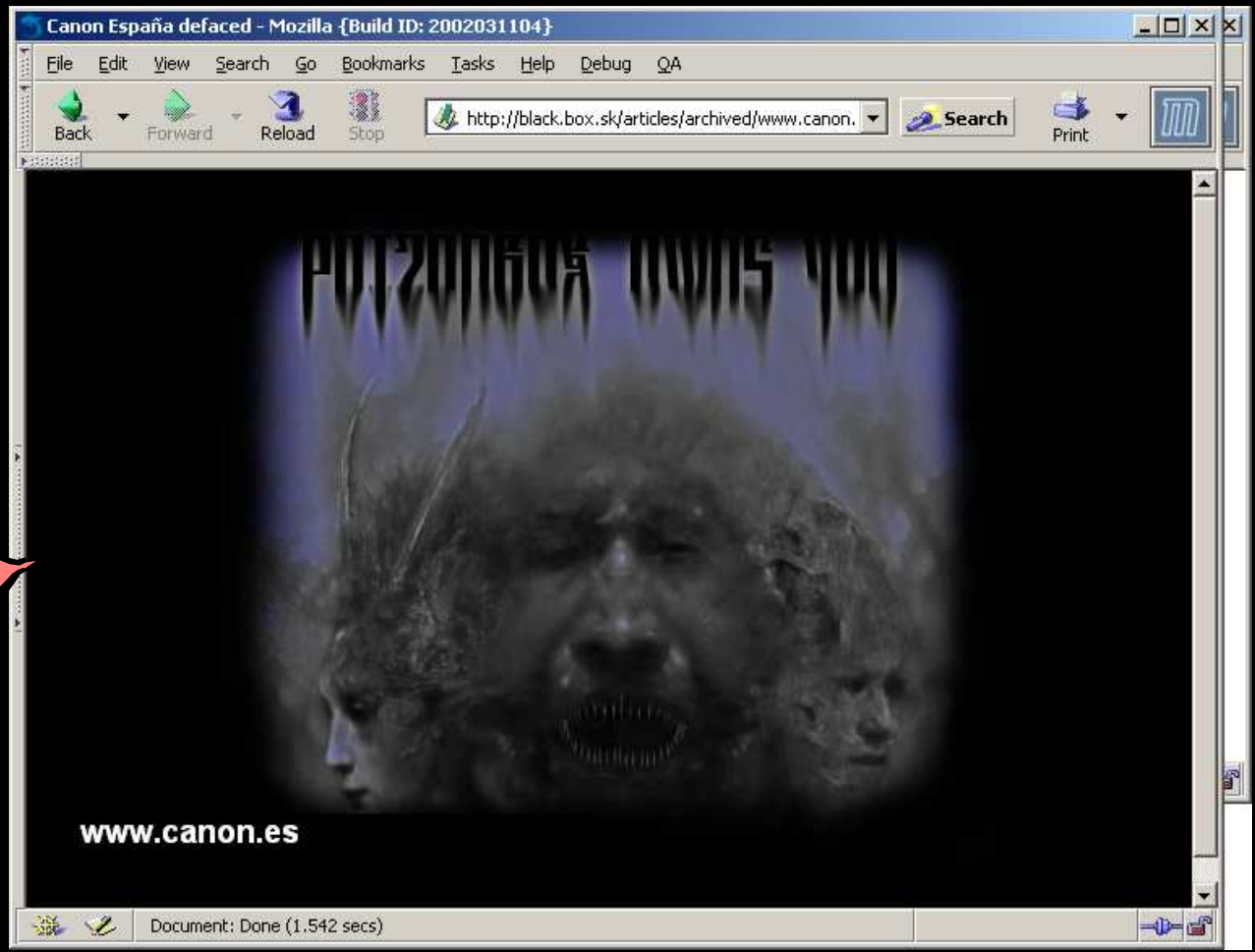
Un poco de miedo III

- www.securitybase.com

Un poco de miedo IV

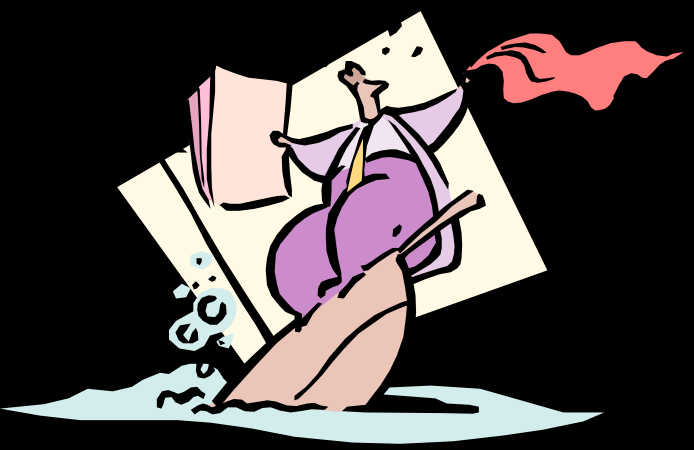
- www.canon.es

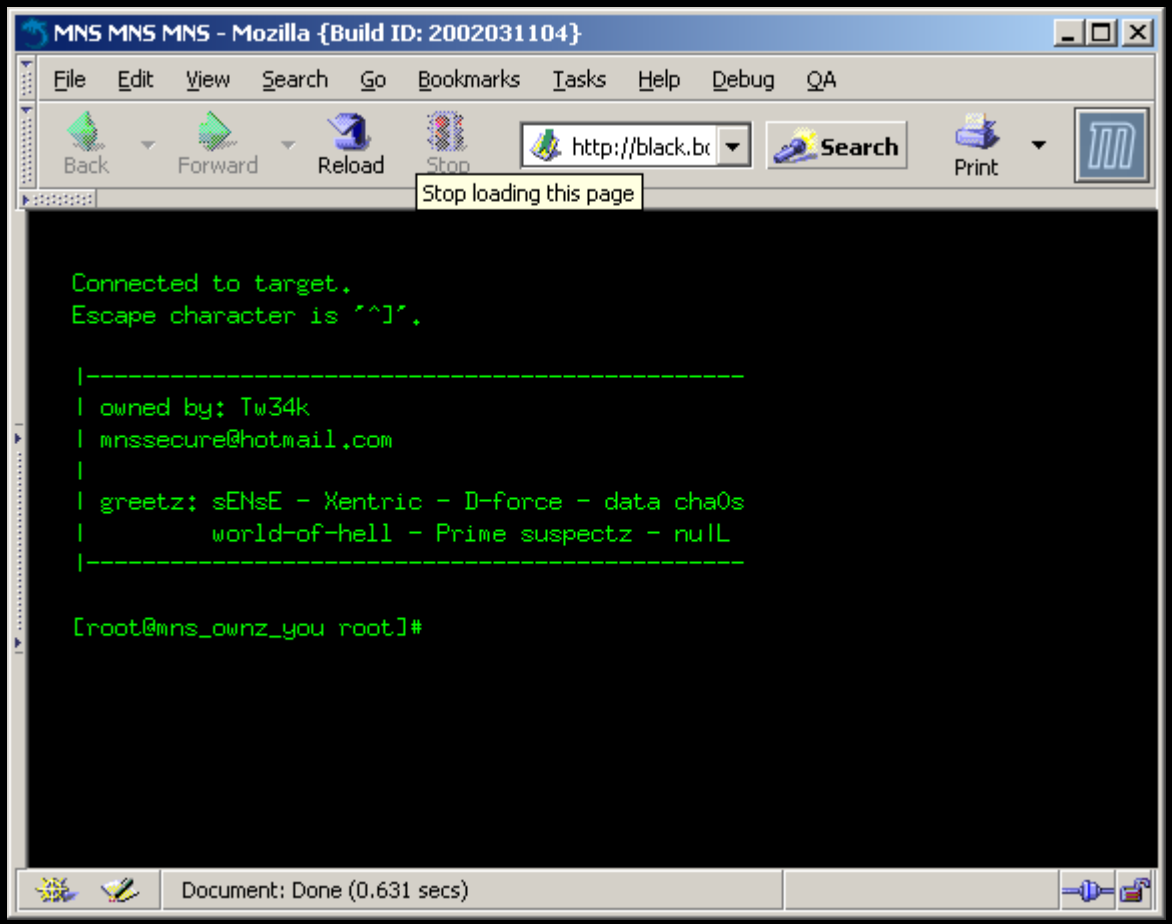




Un poco de miedo V

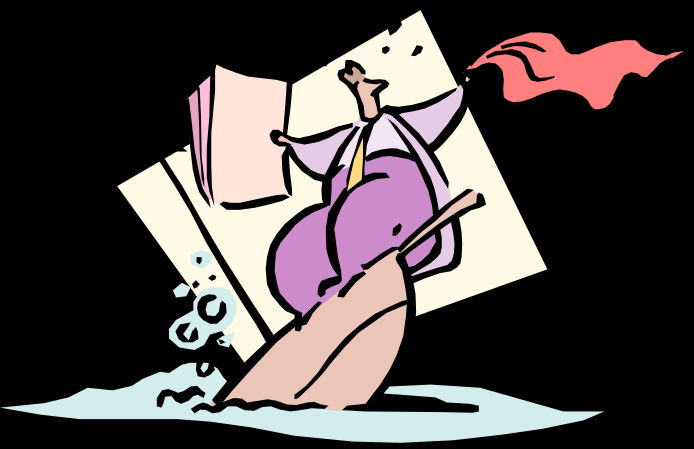
www.securecreditcard.net

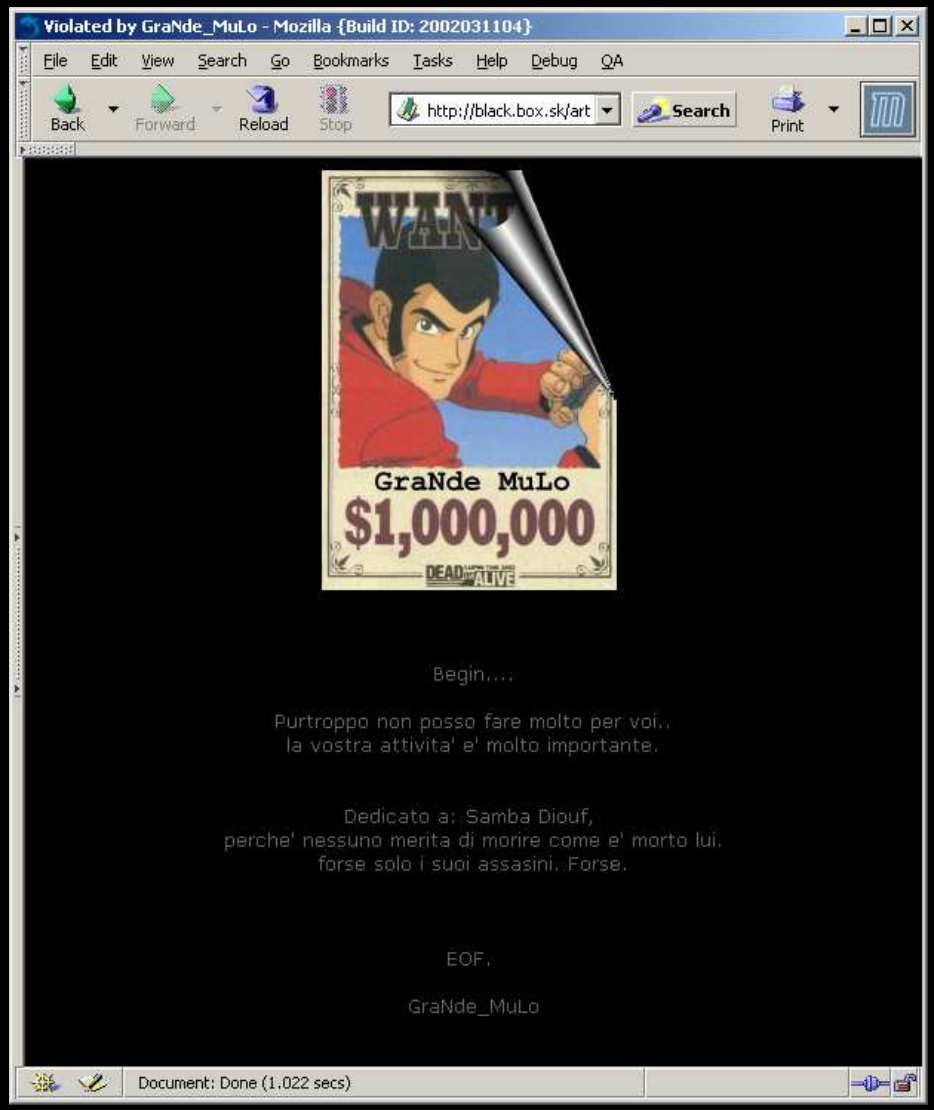




Un poco de miedo VI

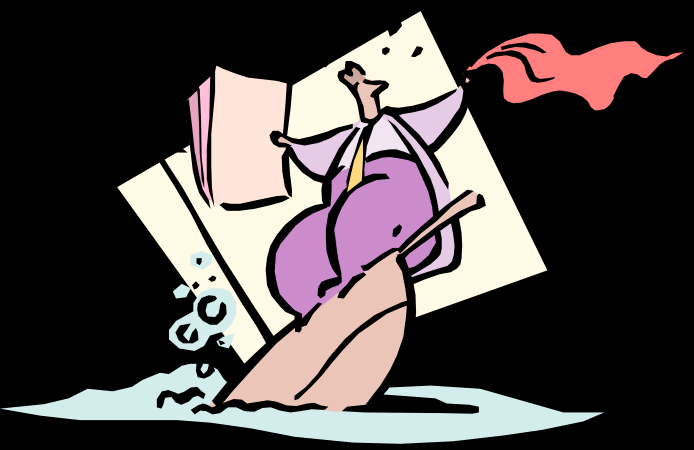
www.exodus.it

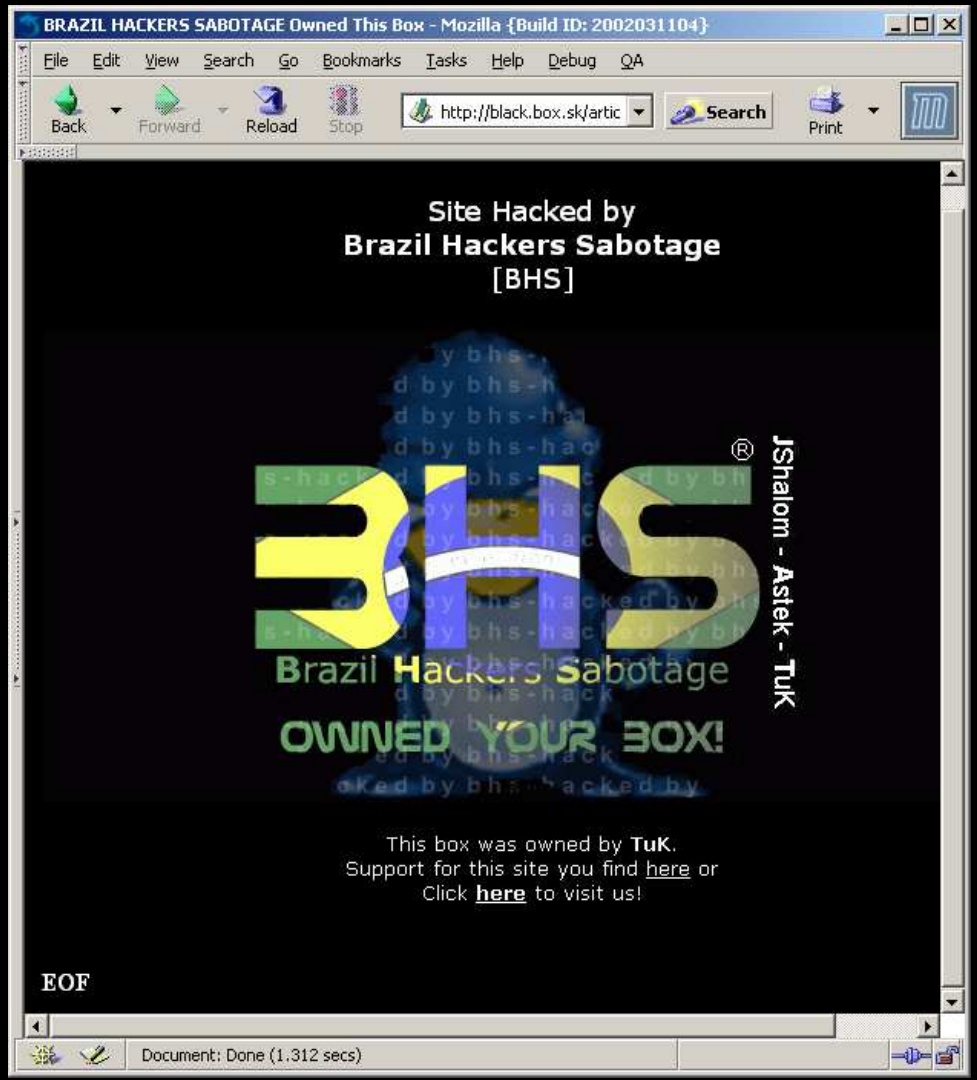




Un poco de miedo VII

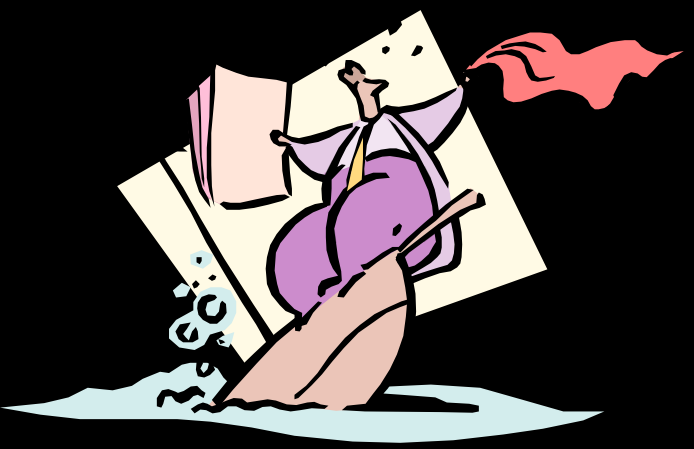
www.comntel.com

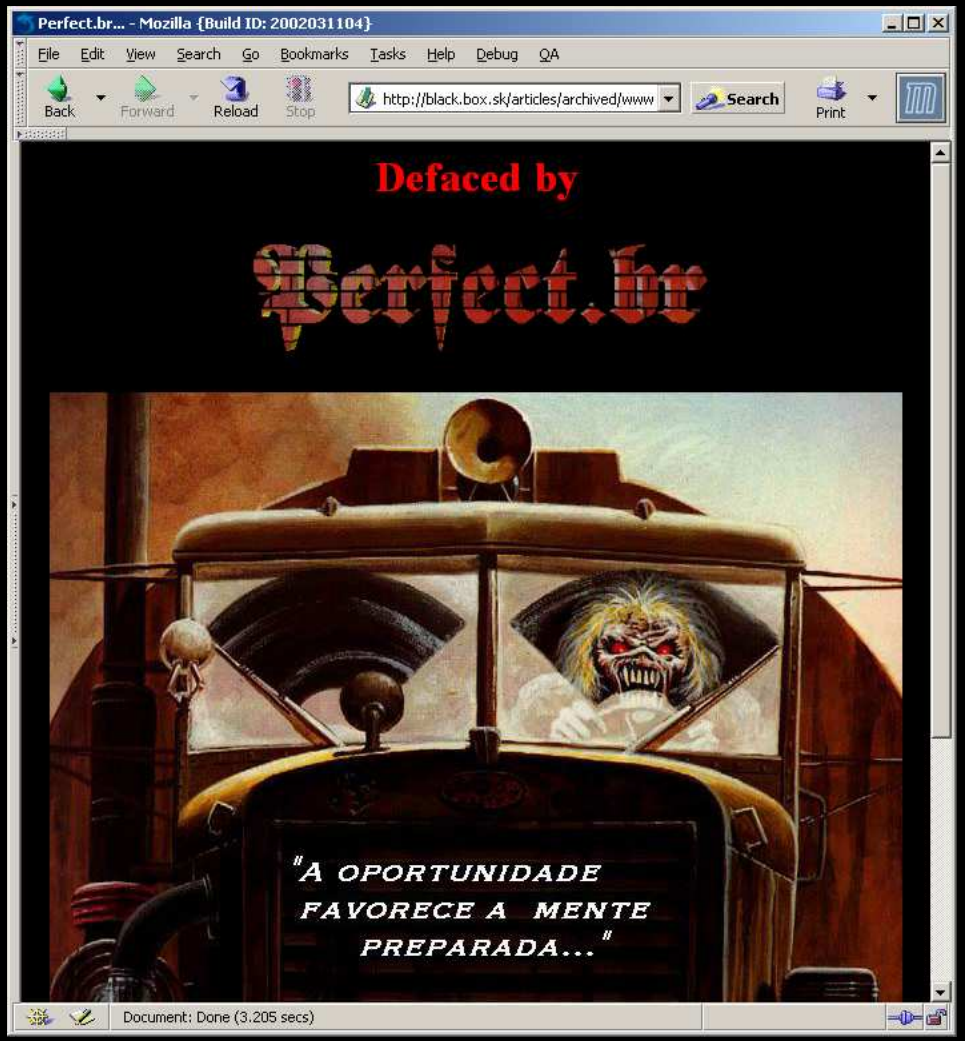




Un poco de miedo VIII

www.fox.dk





Un poco de miedo IX

Algunas noticias sobre seguridad

(neworder.box.sk)

game
@ SMS Mar 14 2002 - 01:26 EST

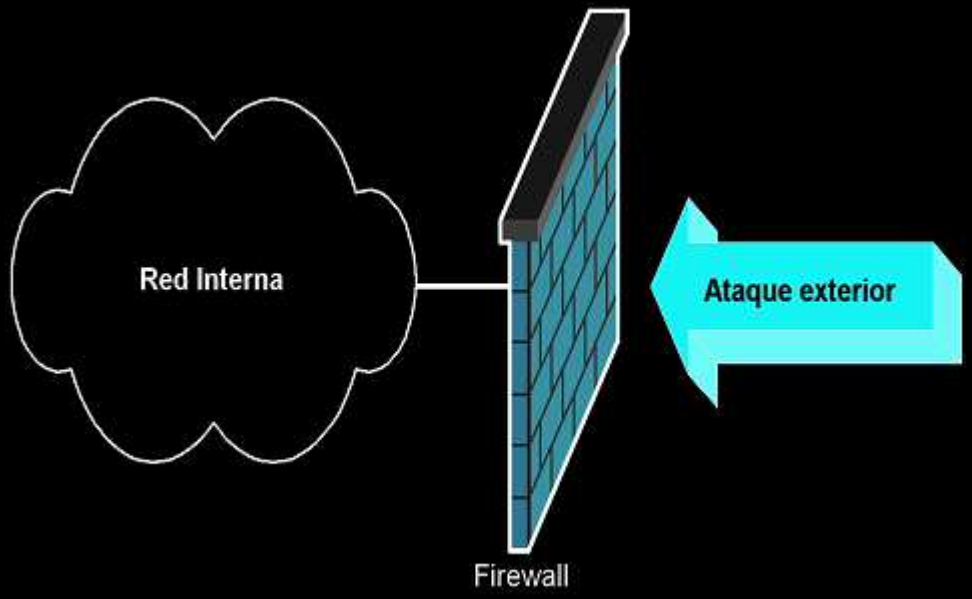
The_MadMan writes: Corporate security and IT professionals got a chance last week to think like hackers so they could learn how to better prevent unauthorized users from gaining access to their networks.

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*).