



jornadas de reflexión

en el marco del congreso nacional de software libre

2022



invitado especial
richard stallman
líder del proyecto GNU

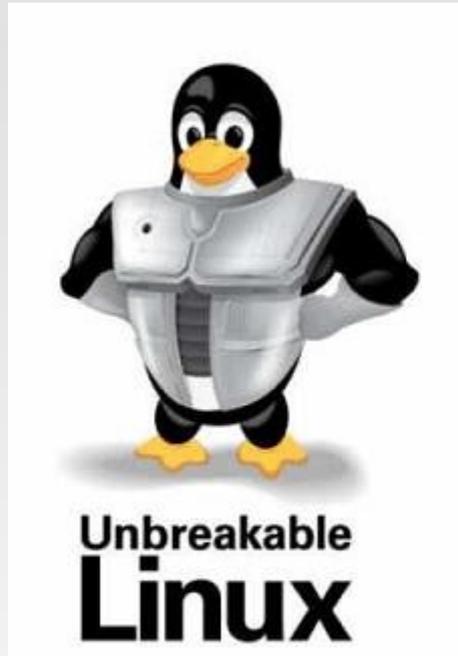
SEGURIDAD EN SISTEMAS GNU/LINUX

Ronald Escalona

AGENDA

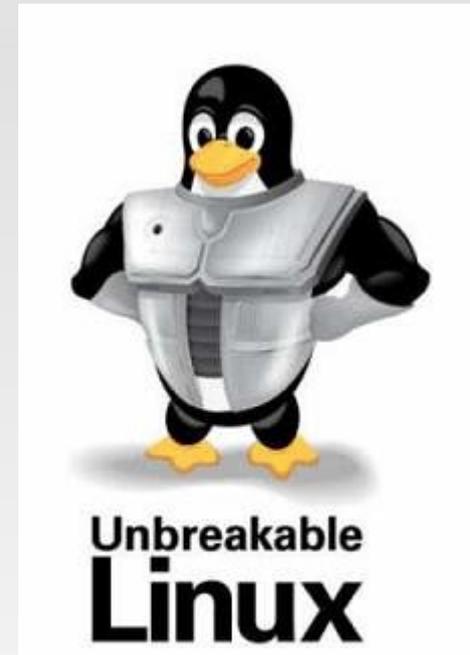
- Introducción
- Hardening Linux
 - Sistema - Usuario Final
 - Sistema - Usuario avanzado
- Infraestructuras de Seguridad FOSS

Introducción



Introducción

- Mitos acerca de la seguridad en GNU/Linux
 - Es GNU/Linux más seguro que otros S.O.?
 - Es GNU/Linux un S.O. Libre de Virus?



Hardening Linux – Usuario final

- Protección contra el *malware*
 - *malicious software*
 - *Escritos para GNU/Linux*
 - *Escritos para otros Sistemas Operativos*
 - *Escaneo activo previene la PANDEMIA*
 - *Medios de almacenamiento extraíbles*
 - *Transferencias de archivos por red, etc.*
 - *Cross-Platform Malware*
 - *OpenOffice.org*
 - *Perl, Php, Gtk, etc.*
 - *Firefox*
 - *Rootkits, el talón de Aquiles...*

Hardening Linux – Usuario final

- Instalando el AntiVirus – ClamAv
 - `sudo aptitude install clamav-daemon`
- Actualizando...
 - `sudo freshclam`
- Seek & Destroy!
 - `clamscan`
 - `Clamdsca`
 - `User ClamAv`

amavisd-new	1:2.6.2-2ubuntu2	Interfaz entre MTA y escá
amavisd-new-milter	1:2.6.2-2ubuntu2	Interfaz entre sendmail-n
clamassassin	1.2.4-1	email virus filter wrapper
clamav-base	0.95.1+dfsg-1ubun	anti-virus utility for Unix
clamav-daemon	0.95.1+dfsg-1ubun	anti-virus utility for Unix
clamav-data		
clamav-dbg		
clamav-docs		
clamav-freshclam		

AntiVirus utility for Unix - s

Antivirus is an anti-virus tool software is the integration with (mail filtering). The package provides a multi-threaded daemon in the clamd daemon in the clamav package, an internet in the clamav-freshclam package.

clamav6, which can be used

¿Marcar los cambios adicionales requeridos?

La acción elegida afecta a otros paquetes. Los cambios siguientes se requieren para proceder.

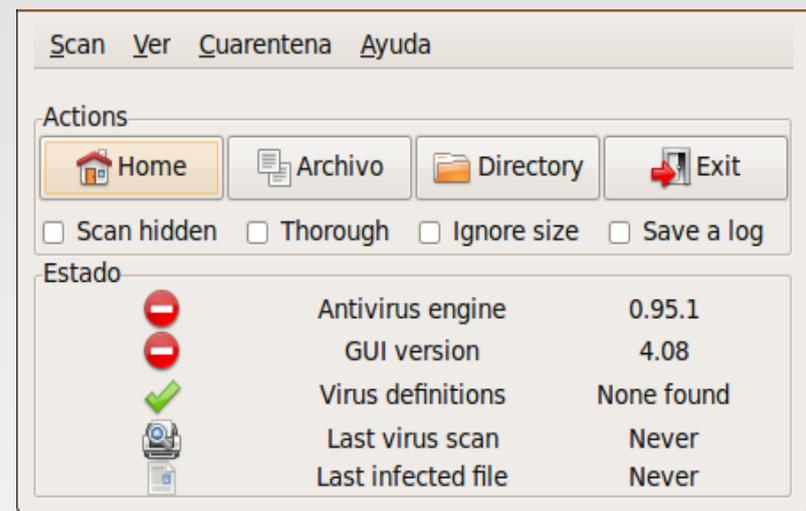
Para ser instalado

- clamav
- clamav-base
- clamav-freshclam
- libclamav6
- libtommath0

Cancelar Marcar

Hardening Linux – Usuario final

- Interfaz gráfica a ClamAv



```
ronald@dolly:~$ sudo freshclam
ClamAV update process started at Thu Jul 23 07:24:39 200
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.95.1 Recommended version: 0.95
DON'T PANIC! Read http://www.clamav.net/support/faq
main.cld is up to date (version: 51, sigs: 545035, f-lev
daily.cvd is up to date (version: 9608, sigs: 57371, f-l
ronald@dolly:~$
```

Hardening Linux – Usuario final

- Protección contra Rootkits!
 - sudo aptitude install rkhunter
 - --update
 - --check
 - sudo aptitude install unhide
 - proc | sys | brute
 - sudo aptitude install chkrootkit

Obtener captura de pantalla

Rootkit Hunter scans systems for known and unknown rootkits, backdoors, sniffers and exploits.

It checks for:

- MD5 hash changes;
 - files commonly created by rootkits;
 - executables with anomalous file permissions;
 - suspicious strings in kernel modules;
 - hidden files in system directories;
- and can optionally scan within files.

Unhide is a forensic tool to find processes and TCP/UDP ports hidden by rootkits, Linux kernel modules or by other techniques. It includes two utilities: unhide and unhide-tcp.

unhide detects hidden processes using three techniques:

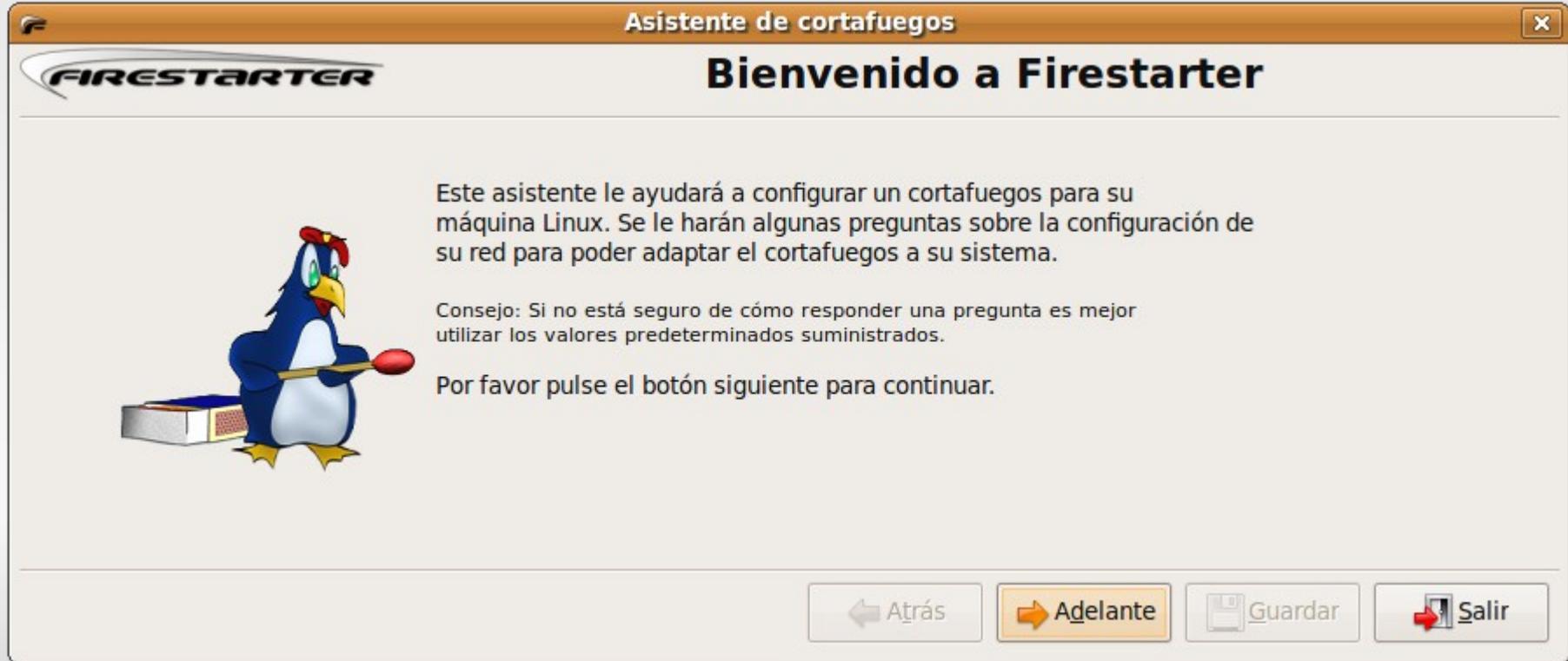
- comparing the output of /proc and /bin/ps
- comparing the information gathered from /bin/ps with the one gathered from system calls (syscall scanning)
- full scan of the process ID space (PIDs bruteforcing)

unhide-tcp identifies TCP/UDP ports that are listening but are not listed in /bin/netstat through brute forcing of all TCP/UDP ports available.

This package can be used by rkhunter in its daily scans.

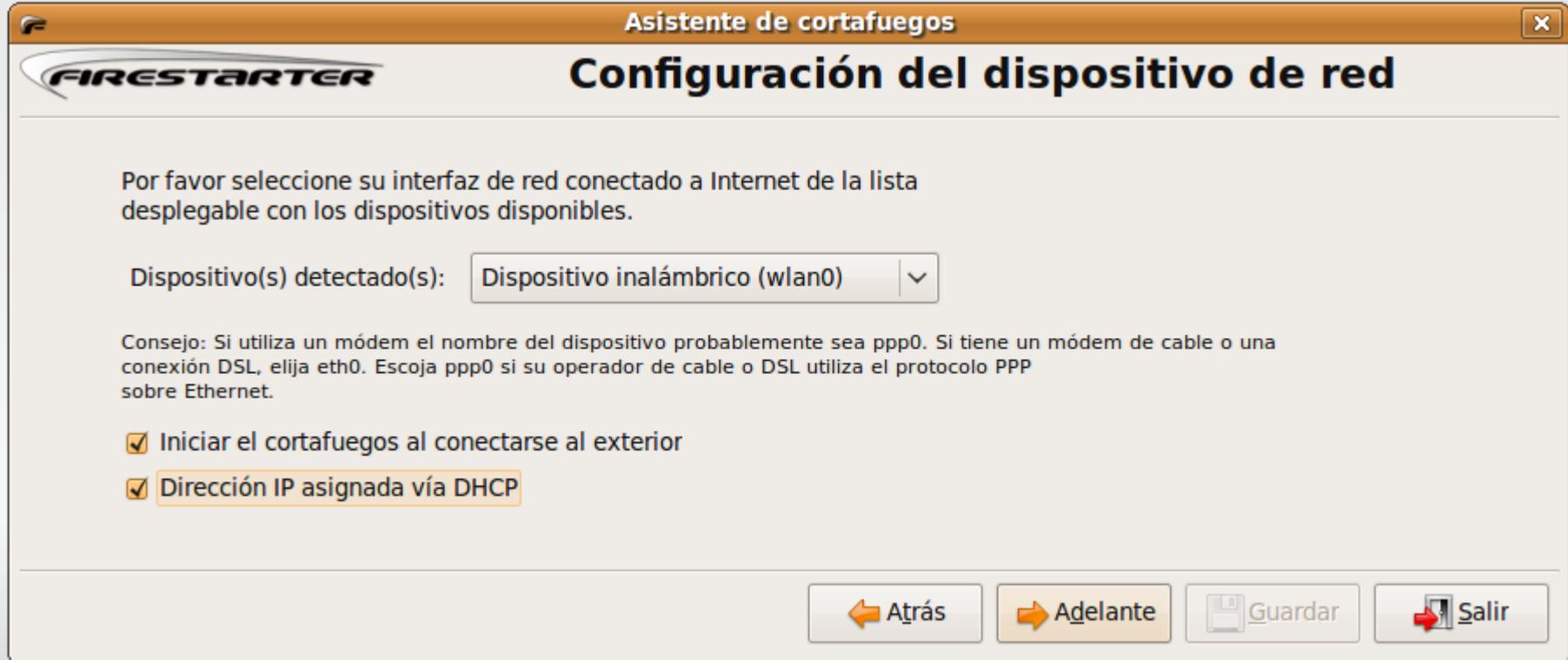
Hardening Linux – Usuario final

- El Cortafuegos...
 - sudo aptitude install firestarter
 - Asistente de configuración



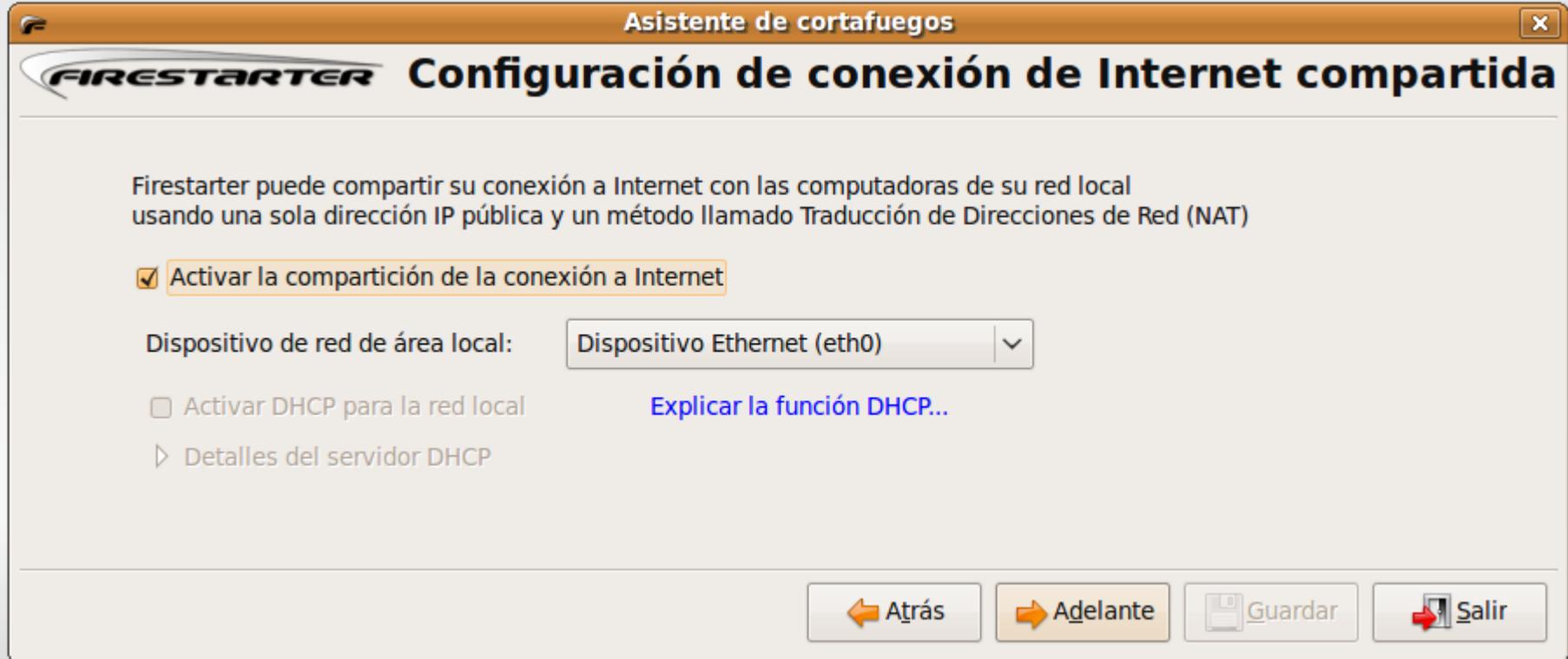
Hardening Linux – Usuario final

- El Cortafuegos...
 - sudo aptitude install firestarter
 - Asistente de configuración



Hardening Linux – Usuario final

- El Cortafuegos...
 - sudo aptitude install firestarter
 - Compartir Internet



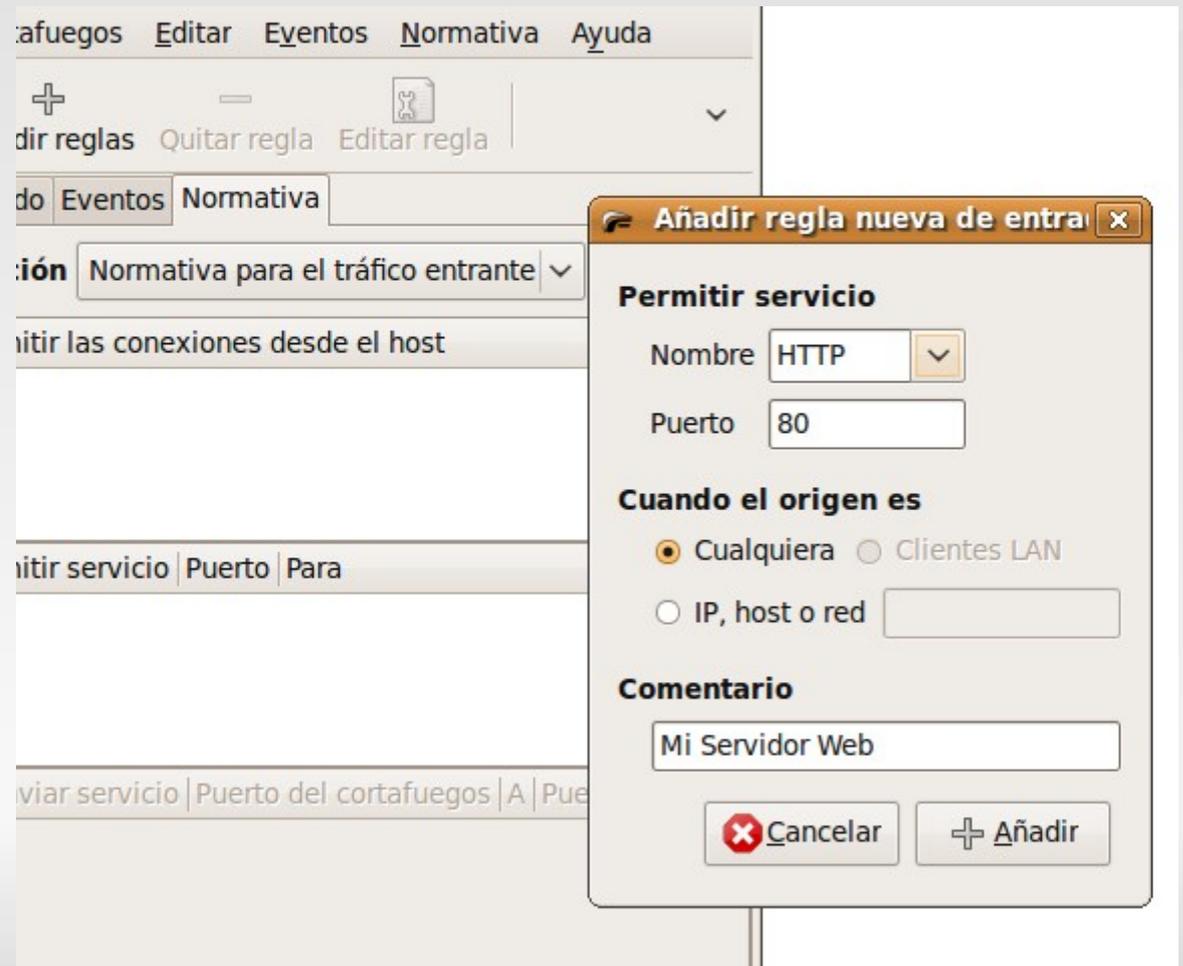
Hardening Linux – Usuario final

- El Cortafuegos...



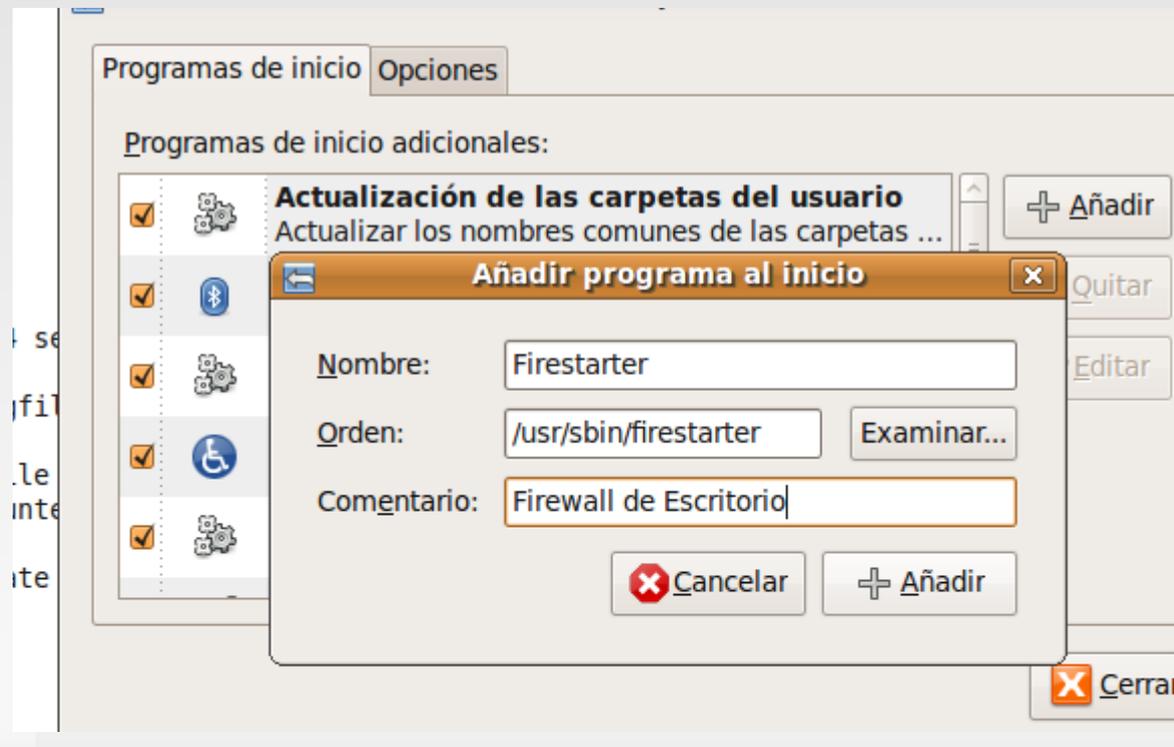
Hardening Linux – Usuario final

- El Cortafuegos...
 - Edición de reglas



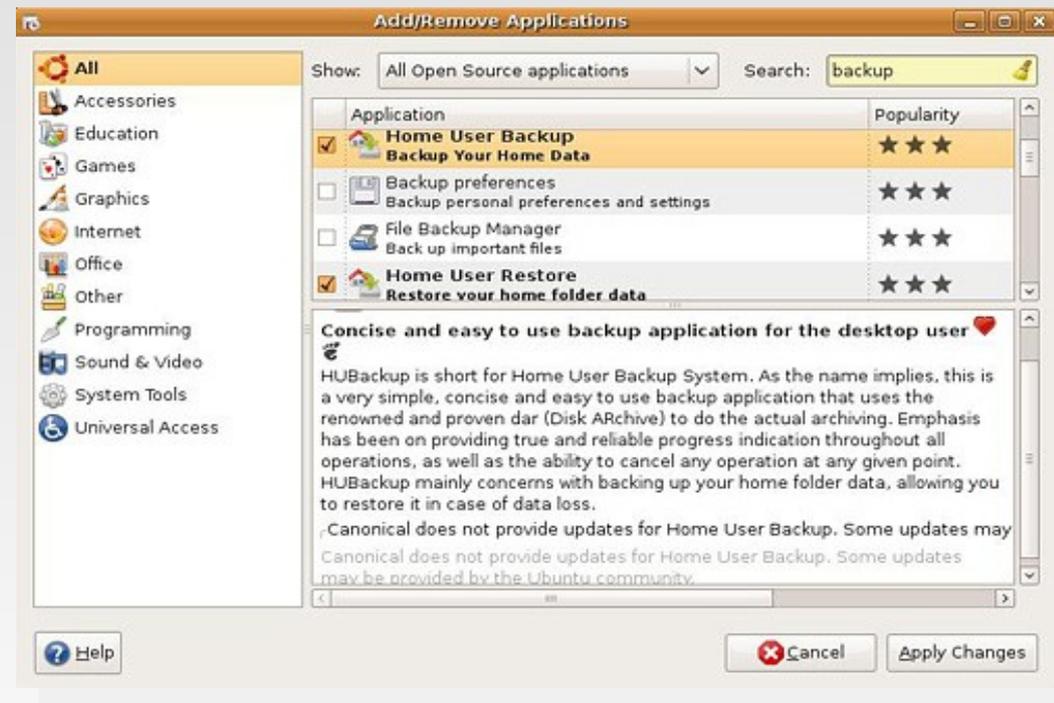
Hardening Linux – Usuario final

- El Cortafuegos...
 - Ejecutar al inicio de sesión



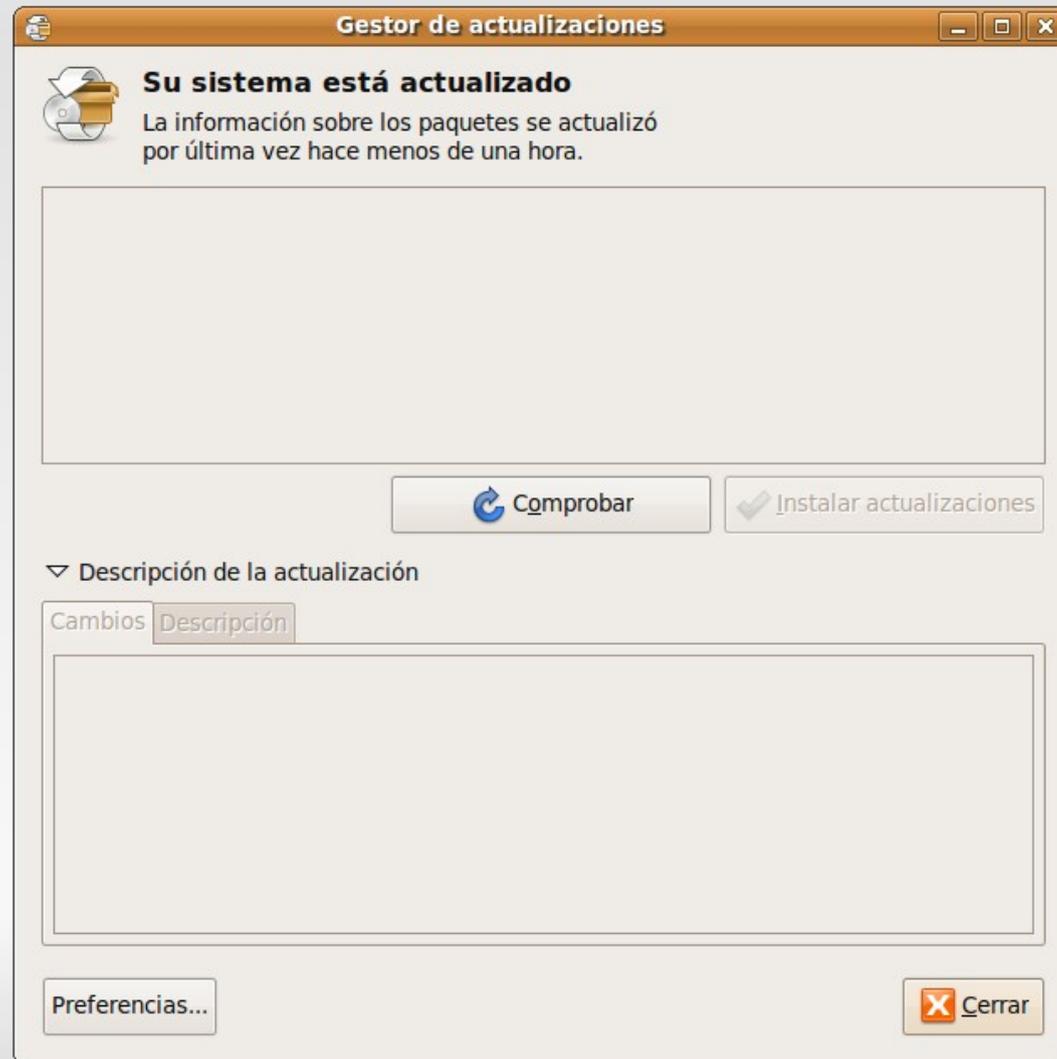
Hardening Linux – Usuario final

- Respalda y Restaurar los datos... 'dar'
 - sudo aptitude install dar
 - Archivador lleno de características que permite copias de seguridad diferenciales, troceado, compresión y admite ATTR/ACL. DAR también admite tuberías para operaciones remotas, incluyendo ssh.



Hardening Linux – Usuario final

- Crear hábito de actualización del Sistema!



Hardening Linux – Avanzado

- Proteger el bios y el bootloader
 - `sudo cp /boot/grub/menu.lst /boot/grub/menu.lst-backup`
 - `grub-md5-crypt`

```
ronald@Dolly:~$ grub-md5-crypt
Password:
Retype password:
$1$NtRC8/$xEo9CglrvVAfLf3qA6VHR0
```

```
## password ['--md5'] passwd
# If used in the first section of the menu file, disable all
interactive editing
# control (menu entry editor and command-line) and entries protected
by the
# command 'lock'
# e.g. password topsecret
#      password --md5 $1$jLhUO/$aW78kHK1QfV3P2b2znUoe/
# password topsecret
password --md5 $1$NtRC8/$xEo9CglrvVAfLf3qA6VHR0
```

Hardening Linux – Avanzado

- Recomendaciones:
 - Asegurar el proceso de inicio (boot process)
 - Asegurar servicios y demonios
 - Asegurar el Sistema de Archivos
 - Cifrado: LUKS, cryptomount, etc.
 - Forzar el uso de Cuotas y Límites en el sistema
 - Habilitar Control de Acceso Obligatorio (MAC)
 - SELinux
 - AppArmor
 - SMACK
 - Políticas de Actualización e instalación de patches

Hardening Linux – Avanzado

- Recomendaciones:
 - Gestión de configuración centralizada
 - Puppet
 - RCS
 - CFEngine
 - Sistemas de Detección de Intrusos
 - HIDS / HIPS
 - OSSEC
 - Osiris
 - SNARE
 - NIDS / IPS
 - Snort, ¿algún otro? ;^)

Hardening Linux – Avanzado

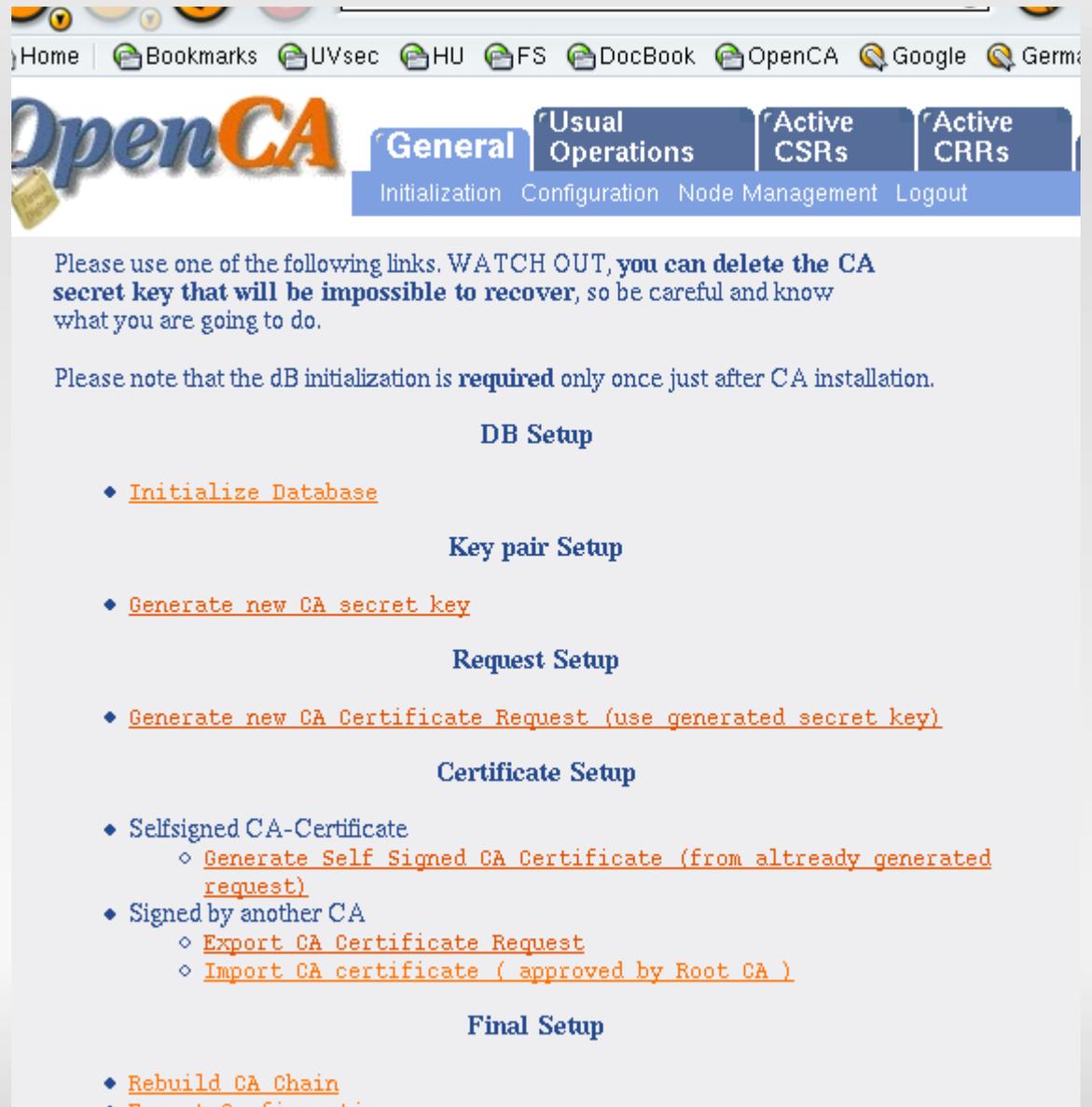
- Recomendaciones:
 - Revisión de Vulnerabilidades
 - OpenVAS
 - Nessus
 - Monitorización
 - Nagios
 - Ntop
 - Zabbix, Zenoss, OpenNMS, etc.
 - Generación de políticas de seguridad!

Infraestructuras de Seguridad

- Infraestructuras de clave pública (PKI)
 - OpenCA
 - Auto-gestionada
 - Certificada por una TTP

Hardening Linux – Avanzado

- OpenCA-LiveCD



The screenshot shows the OpenCA web interface. At the top, there is a navigation bar with the OpenCA logo and several tabs: 'General', 'Usual Operations', 'Active CSRs', and 'Active CRRs'. Below the tabs, there are links for 'Initialization', 'Configuration', 'Node Management', and 'Logout'. The main content area contains a warning message: 'Please use one of the following links. WATCH OUT, you can delete the CA secret key that will be impossible to recover, so be careful and know what you are going to do.' Below this, there is a note: 'Please note that the dB initialization is required only once just after CA installation.' The interface is organized into several sections, each with a title and a list of links:

- DB Setup**
 - ◆ [Initialize Database](#)
- Key pair Setup**
 - ◆ [Generate new CA secret key](#)
- Request Setup**
 - ◆ [Generate new CA Certificate Request \(use generated secret key\)](#)
- Certificate Setup**
 - ◆ Selfsigned CA-Certificate
 - ◇ [Generate Self Signed CA Certificate \(from already generated request\)](#)
 - ◆ Signed by another CA
 - ◇ [Export CA Certificate Request](#)
 - ◇ [Import CA certificate \(approved by Root CA \)](#)
- Final Setup**
 - ◆ [Rebuild CA Chain](#)
 - ◆ [Export Configuration](#)

Infraestructuras de Seguridad

- Open Source Security Information Management
 - OSSIM es una distribución de productos open source integrados para construir una infraestructura de monitorización de seguridad.
 - Su objetivo es ofrecer un marco para centralizar, organizar y mejorar las capacidades de detección y visibilidad en la monitorización de eventos de seguridad de la organización.

Infraestructuras de Seguridad

- Open Source Security Information Management
 - Arpwatch
 - P0f
 - Pads
 - Nessus
 - Snort
 - Spade
 - Tcptrack
 - Ntop
 - Nagios
 - Osiris
 - OCS-NG
 - OSSEC
 - integrity, rootkit, registry detection and more

Infraestructuras de Seguridad



[DASHBOARD](#) | [Incidents](#) | [Events](#) | [Monitors](#) | [Reports](#) | [Policy](#) | [Correlation](#) | [Configuration](#) | [Tools](#) | [Logout \[admin\]](#)

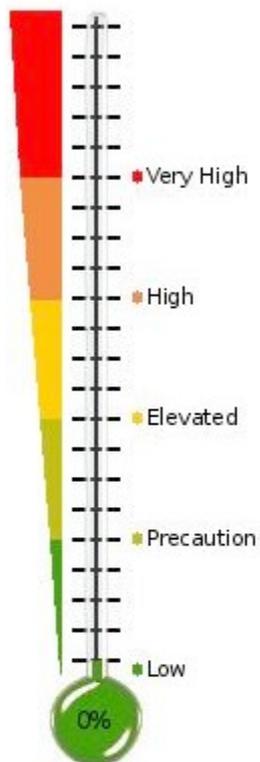
EXECUTIVE PANEL | [Aggregated Risk](#) | [Alarms](#) | [Help](#)

[\[Main | Incidents | Security | Network | Inventory | Vulnerabilities \]](#)

[\[Edit\]](#) [\[Edit Tabs\]](#) [\[Fullscreen\]](#)

Service Level

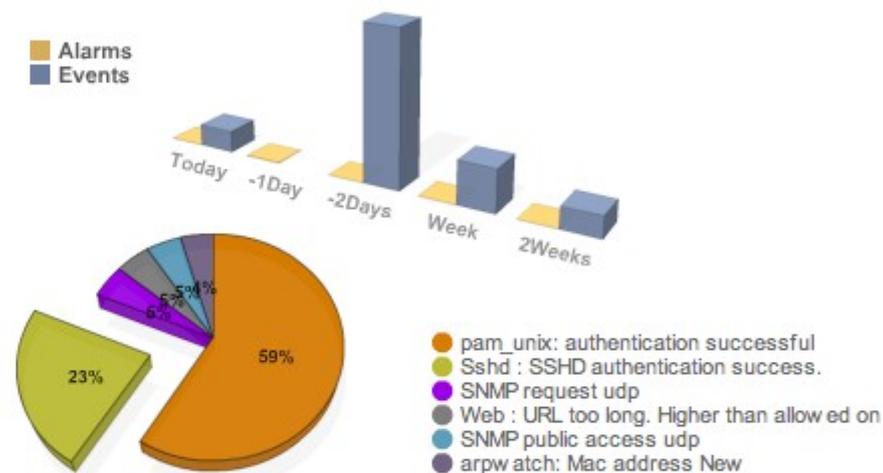
[\[help\]](#)



- Events / Day
- Alarms / Day

Alarms / Events

[\[help\]](#)



Events by Sensor/Plugin

Availability

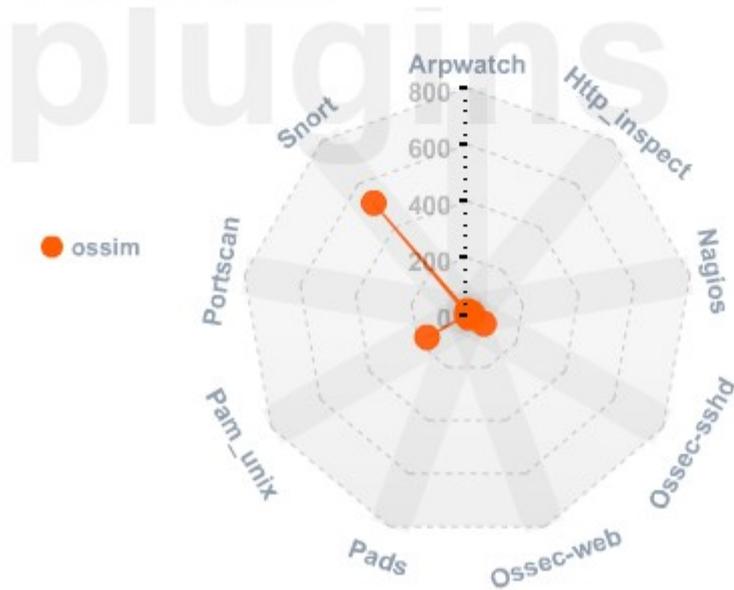
[\[help\]](#)

*Note: Please, configure Nagios and update this panel to view a snapshot of your network.

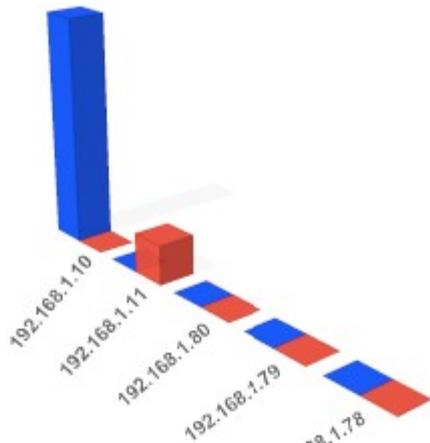
Infraestructuras de Seguridad



Events by Sensor/Plugin

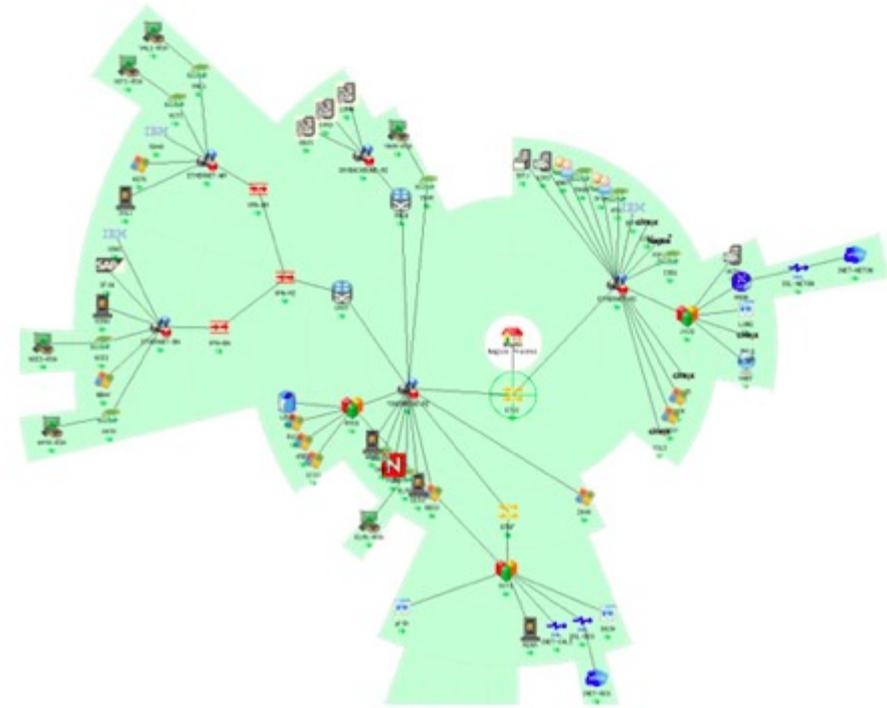


Top 10 hosts risk



Availability

*Note: Please, configure Nagios and update this panel to view a snapshot of your network.

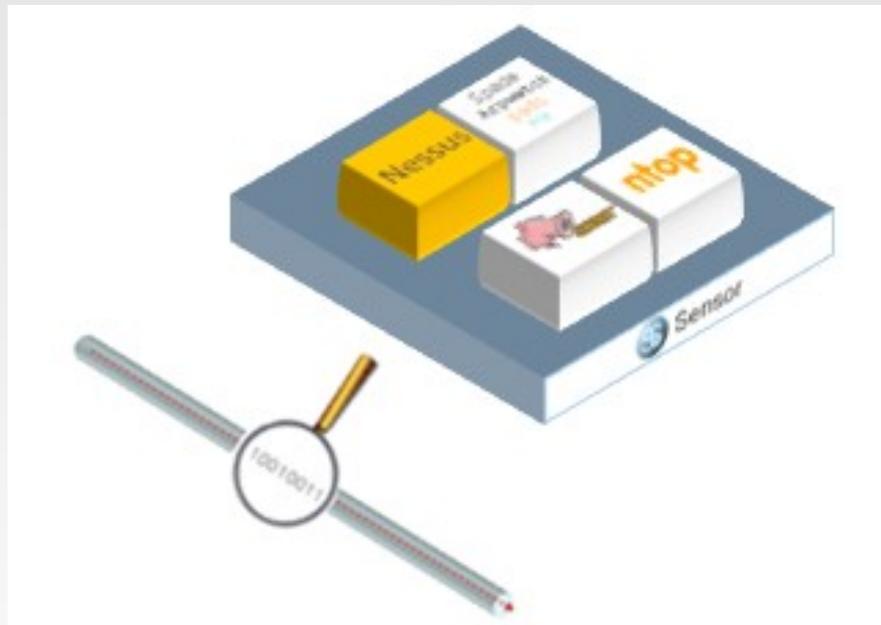


Throughput



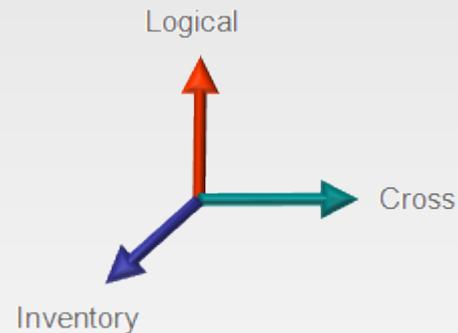
Infraestructuras de Seguridad

- Open Source Security Information Management
 - Detecta



Infraestructuras de Seguridad

- Open Source Security Information Management
 - Correlaciona



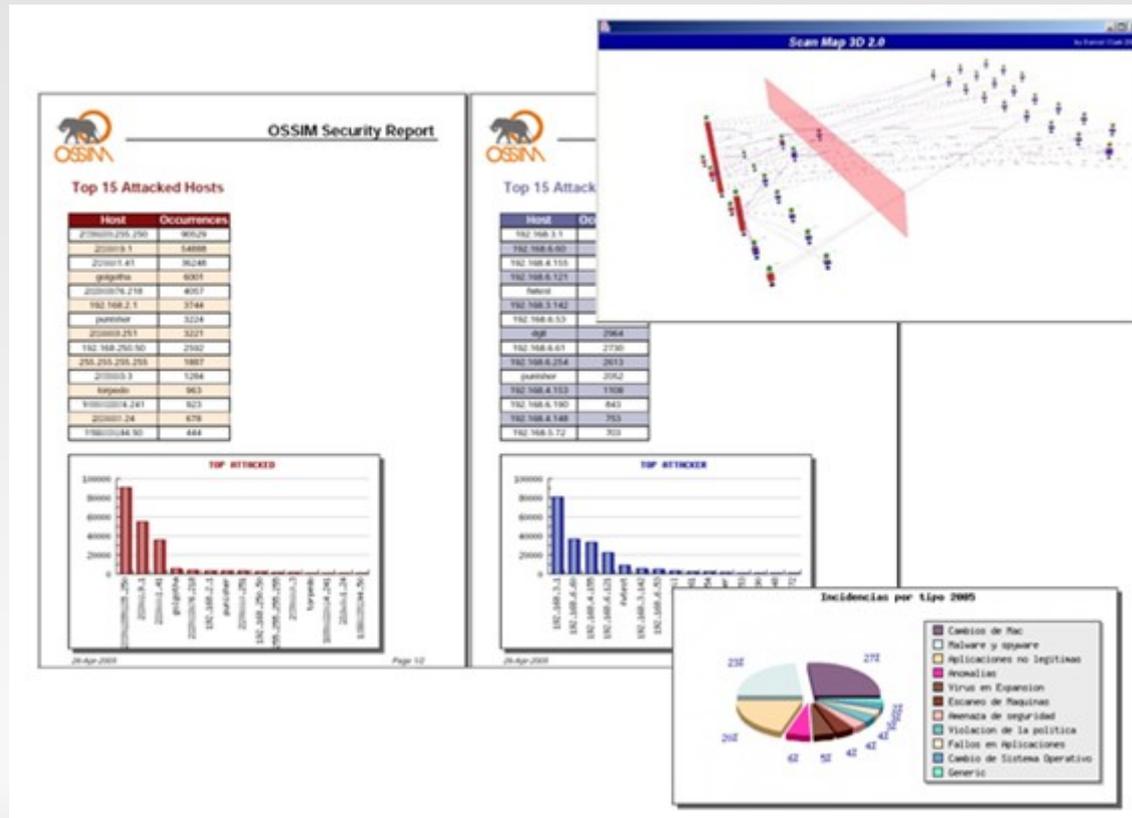
Infraestructuras de Seguridad

- Open Source Security Information Management
 - Reporta



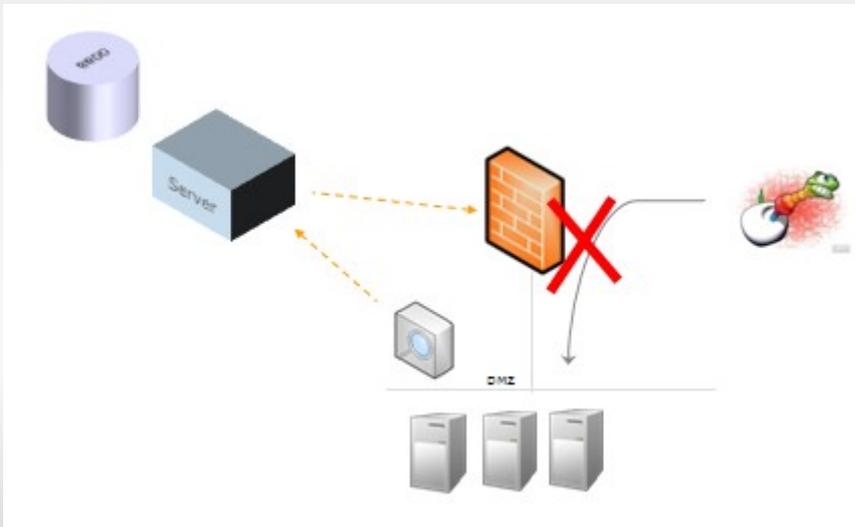
Infraestructuras de Seguridad

- Open Source Security Information Management
 - Reporta



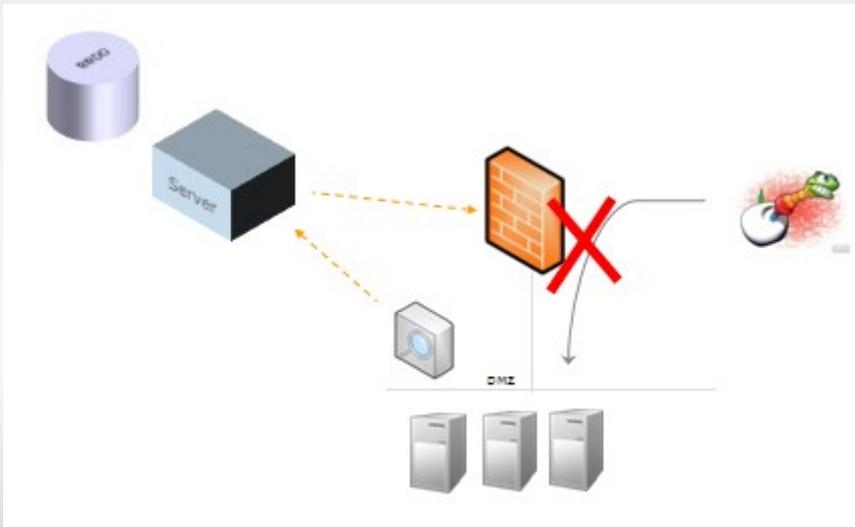
Infraestructuras de Seguridad

- Open Source Security Information Management
 - Gestiona (Risk Analysis)



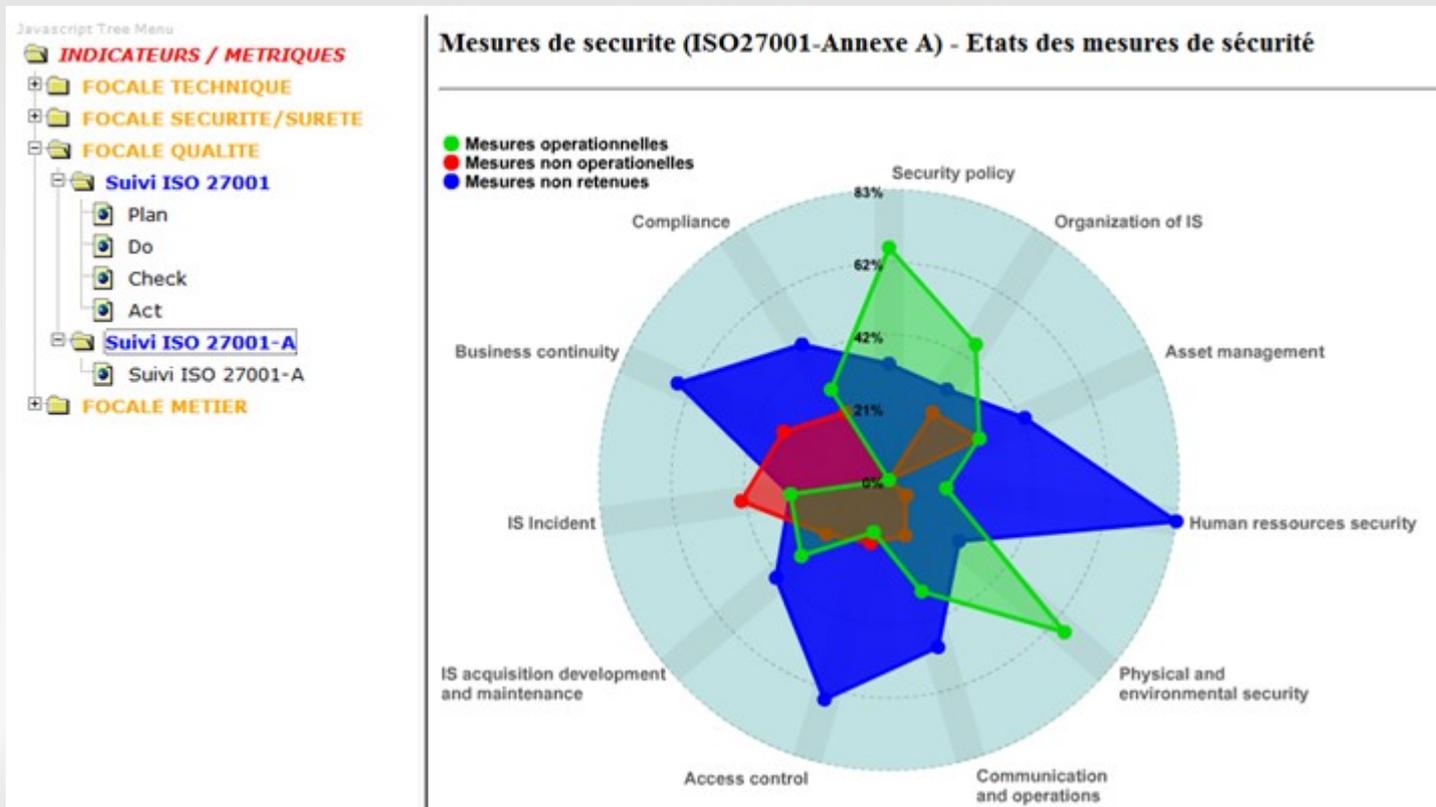
Infraestructuras de Seguridad

- Open Source Security Information Management
 - Gestiona (Risk Analysis)

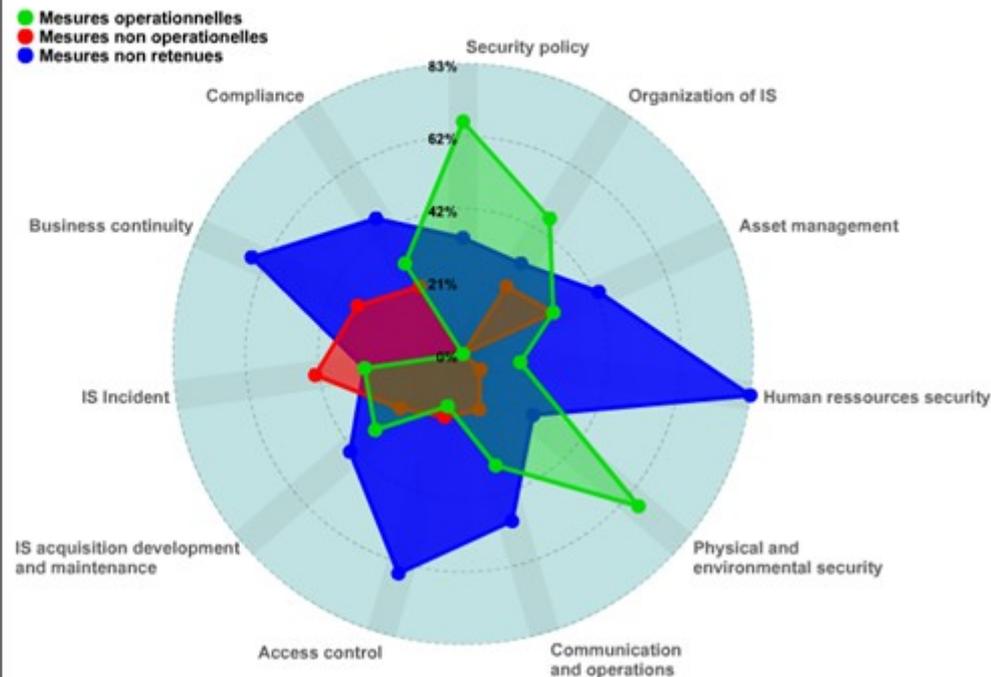


Infraestructuras de Seguridad

- Open Source Security Information Management
 - Compatible, normas internacionales - Fondonorma

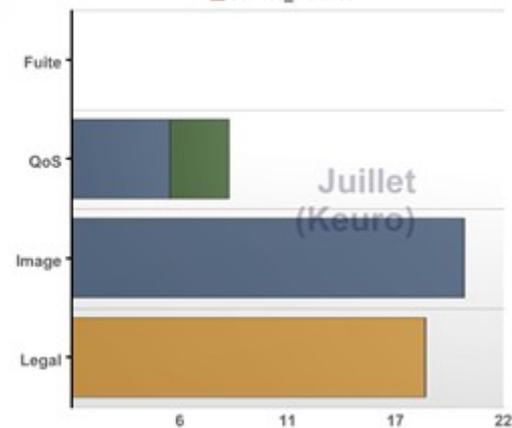
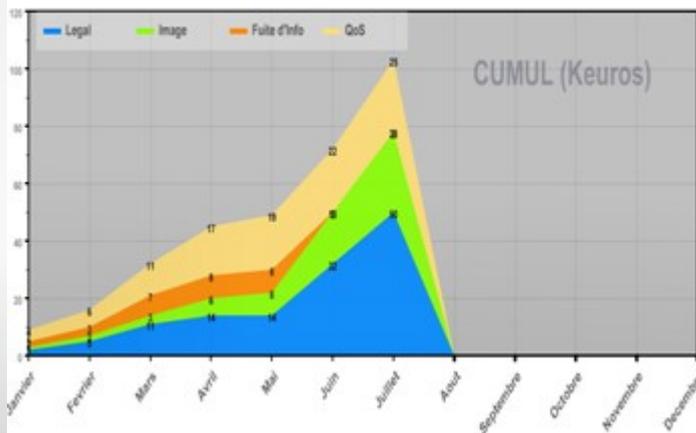
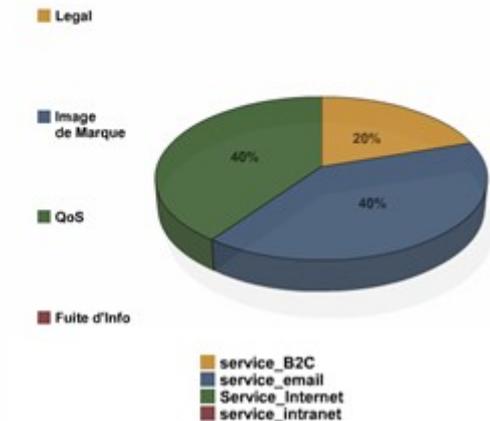
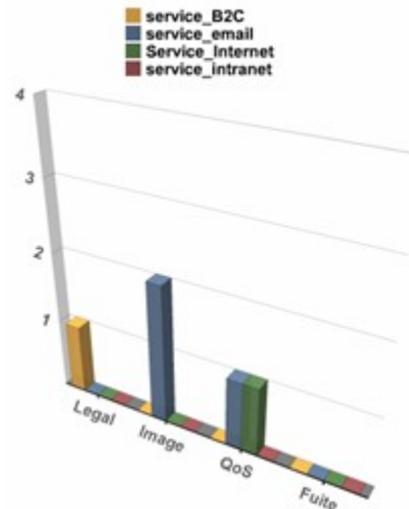
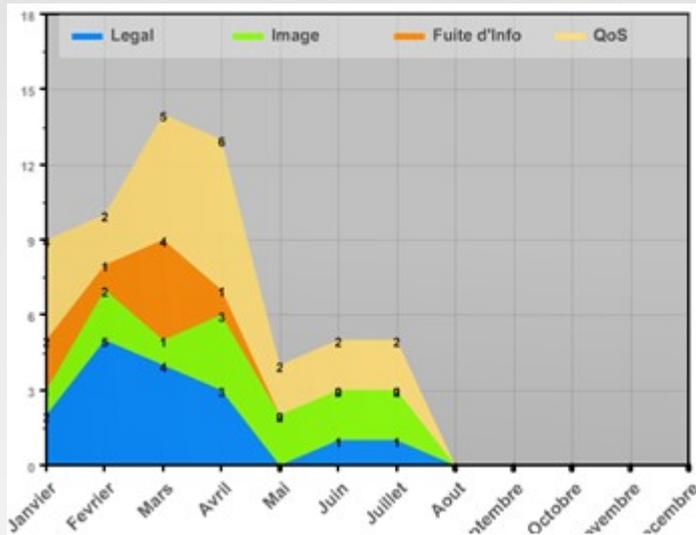


Mesures de securite (ISO27001-Annexe A) - Etats des mesures de securité



Infraestructuras de Seguridad

- Open Source Security Information Management
 - Compatible, normas internacionales - Fondonorma



Seguridad en Linux

Gracias por su atención...