jornadas de reflexión

en el marco del congreso nacional de software libre

julio 2023

software libre

invitado especial

richard stallman

líder del proyecto GNU

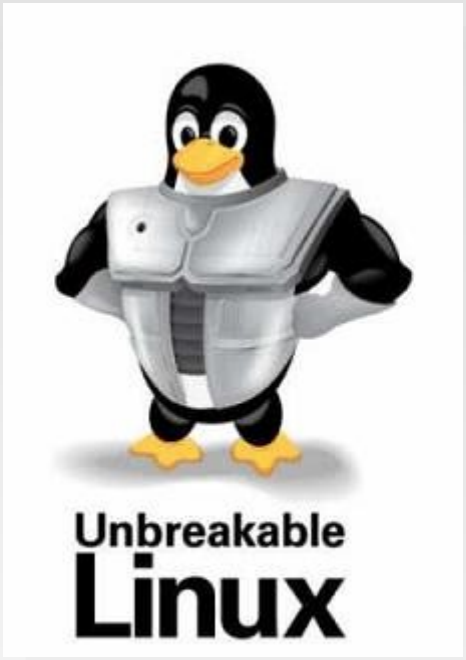
SEGURIDAD EN SISTEMAS GNU/LINUX

Ronald Escalona

AGENDA

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

Introducción

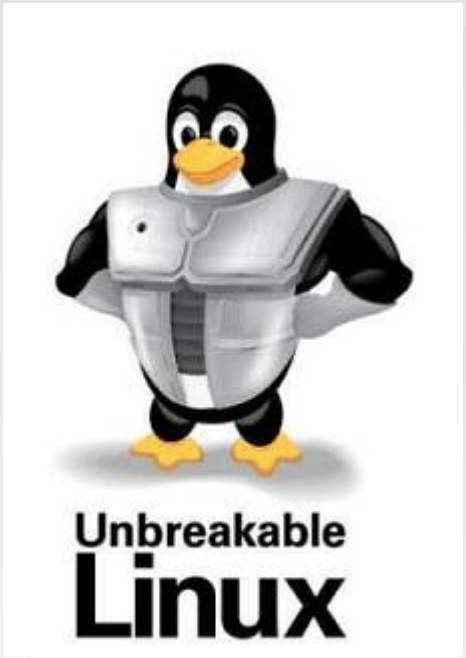
¿ 

?

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?

¿



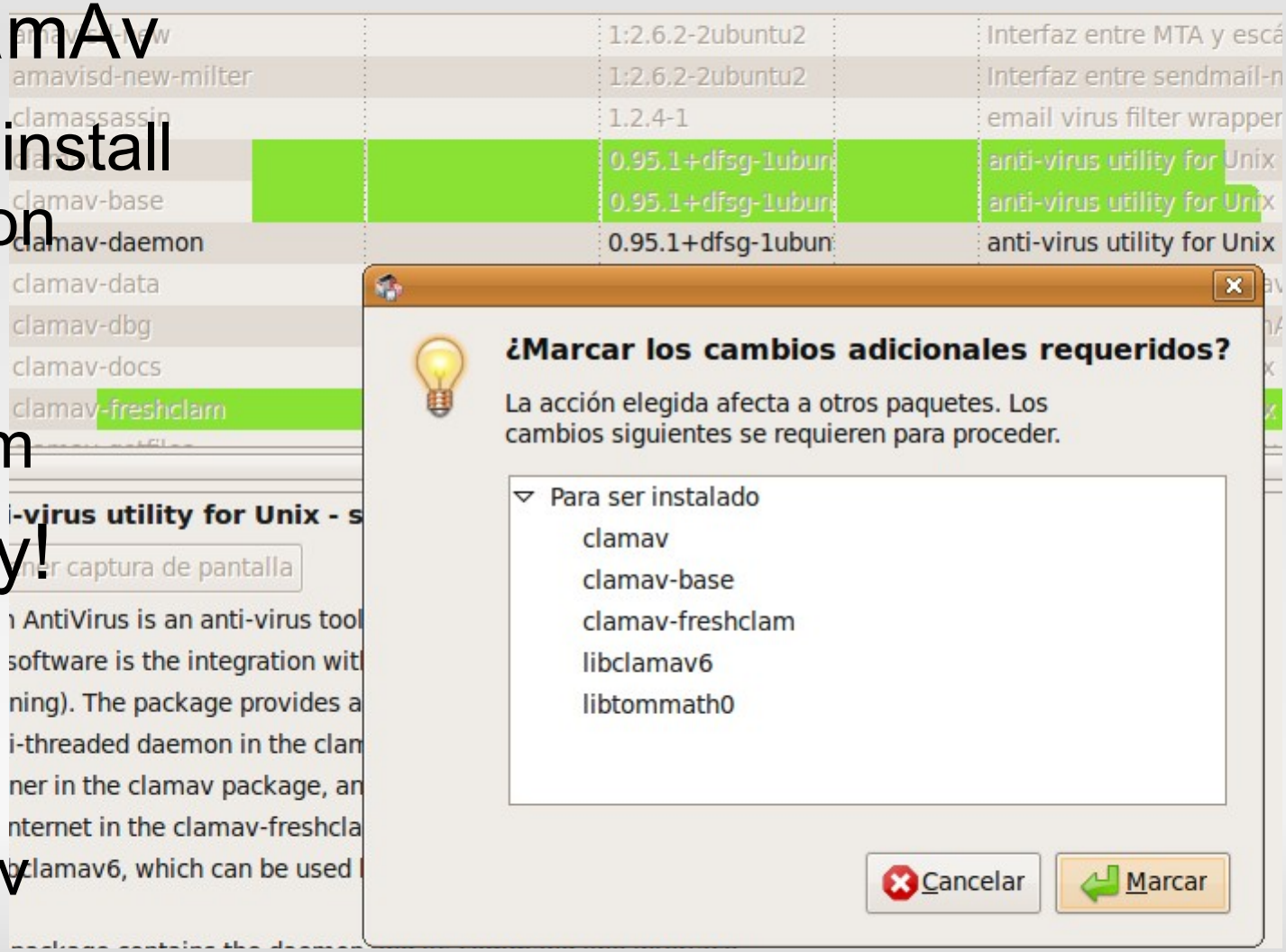
?

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...*

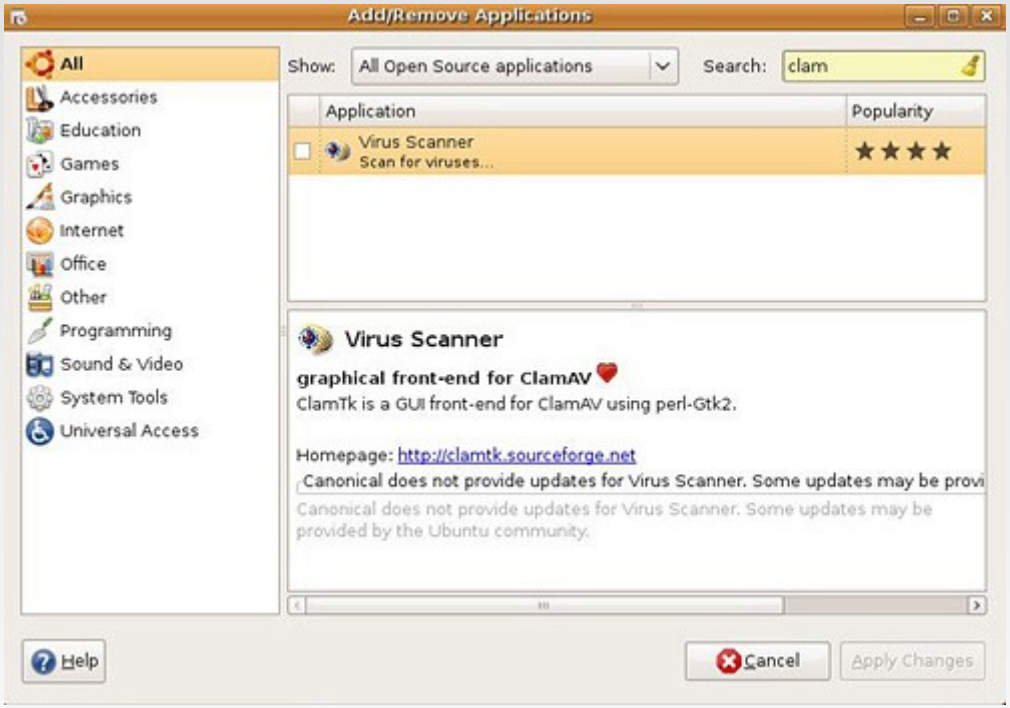
Hardening Linux – Usuario final

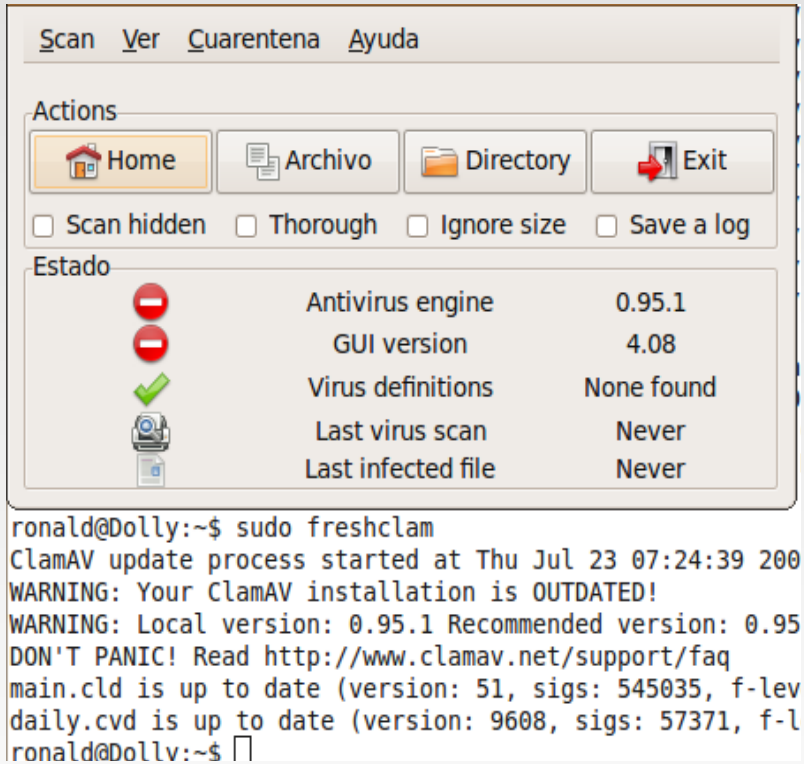
- Instalando el AntiVirus – ClamAv
  - sudo aptitude install clamav-daemon
- Actualizando...
  - sudo freshclam
- Seek & Destroy!
  - clamscan
  - Clamdscan
  - User ClamAv



Hardening Linux – Usuario final

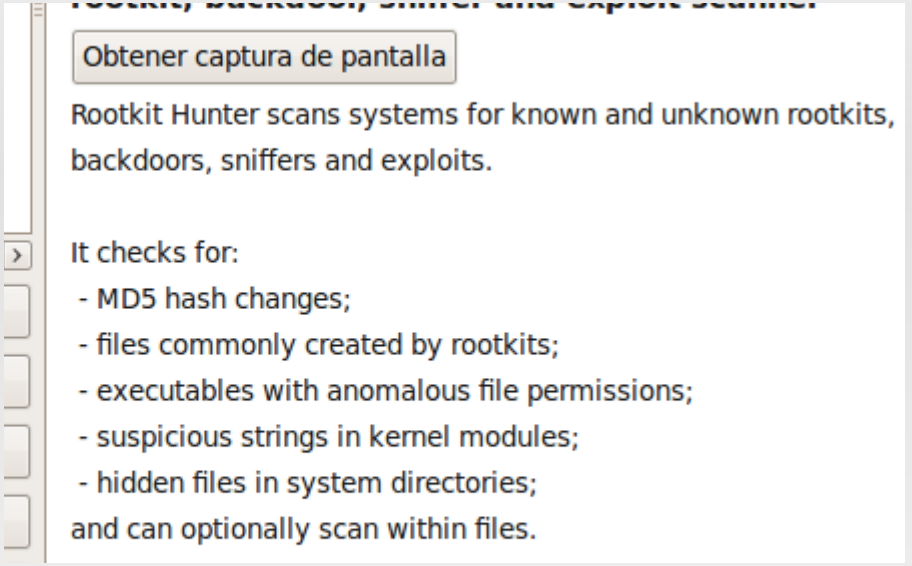
- Interfaz gráfica a ClamAv

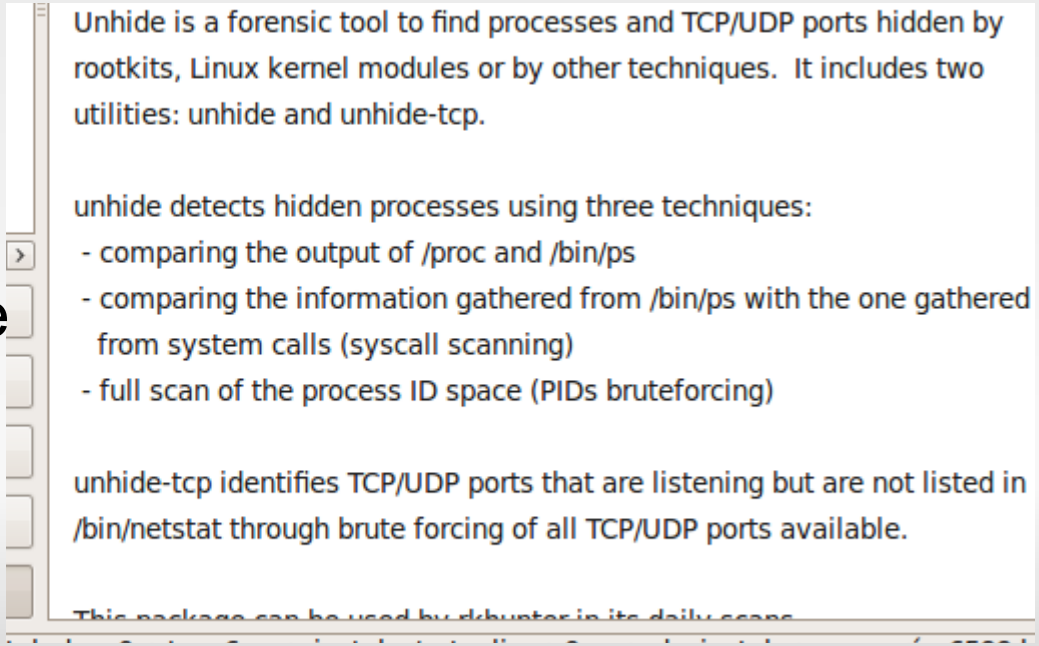




Hardening Linux – Usuario final

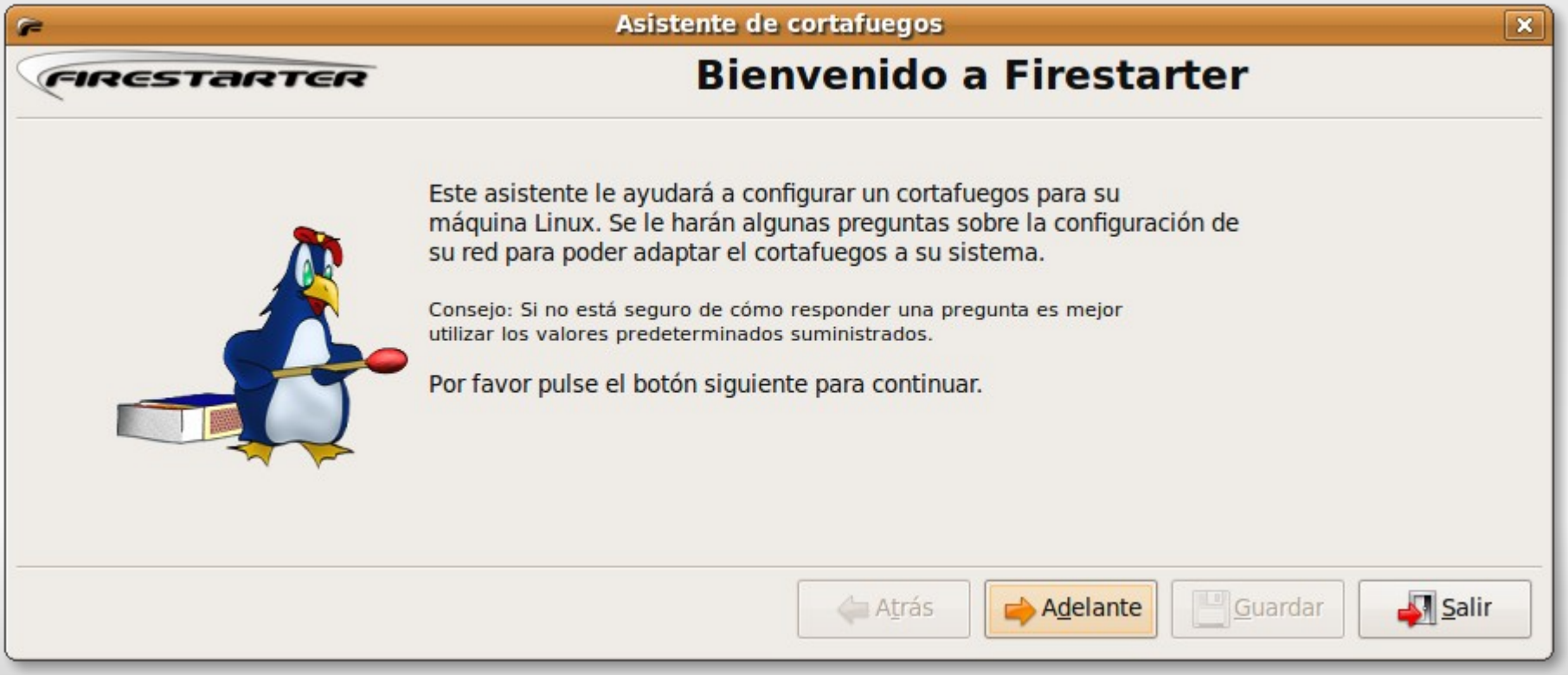
- Protección contra Rootkits!
  - sudo aptitude install rkhunter
    - --update
    - --check
  - sudo aptitude install unhide
    - proc | sys | brute
  - sudo aptitude install chkrootkit





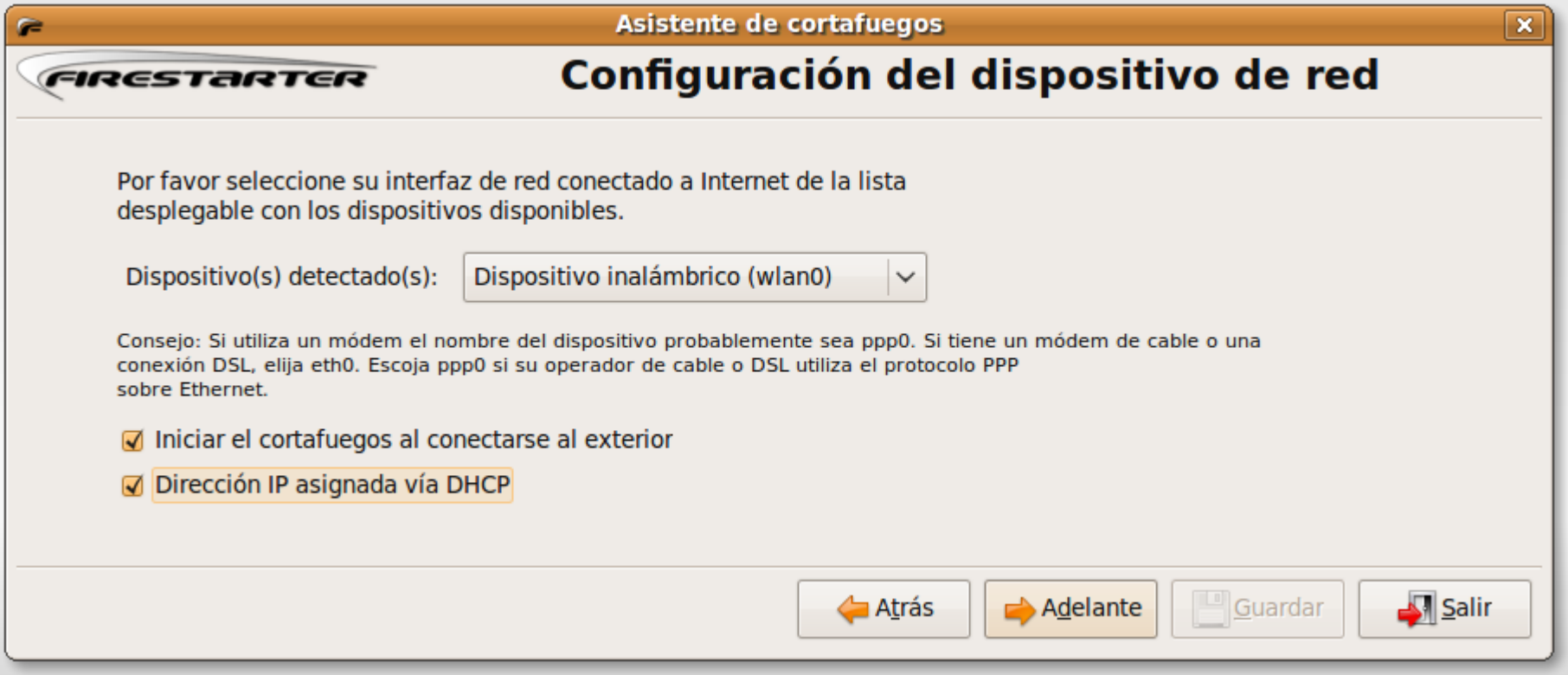
Hardening Linux – Usuario final

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



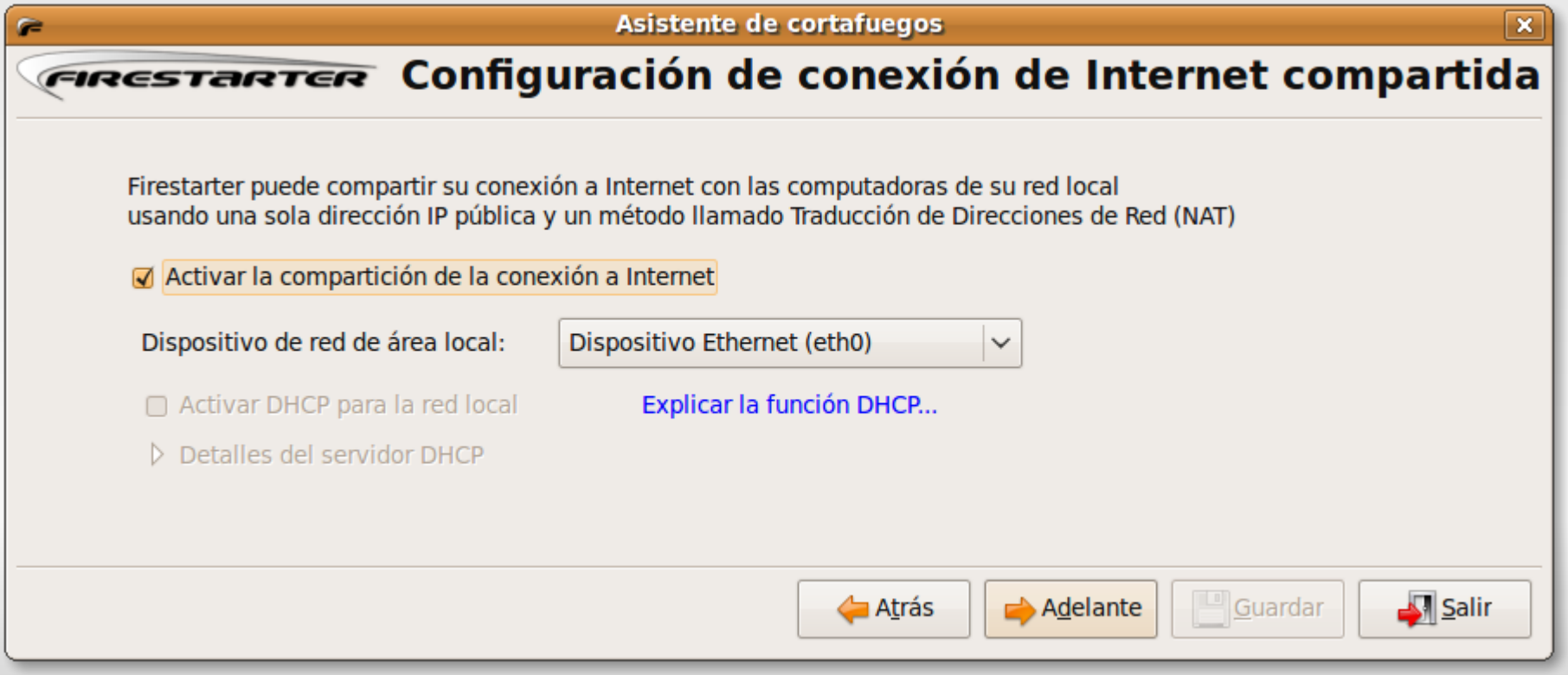
Hardening Linux – Usuario final

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



Hardening Linux – Usuario final

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

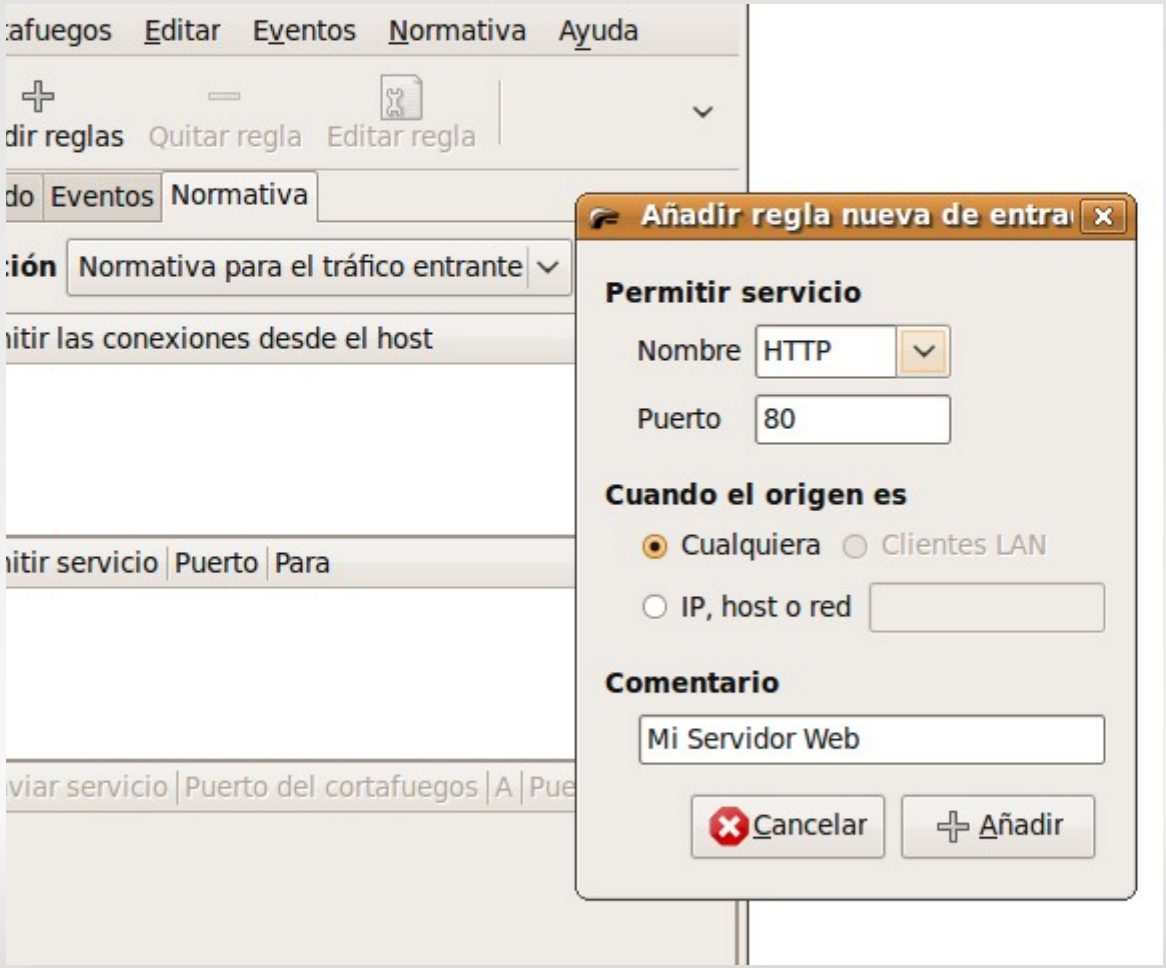


Hardening Linux – Usuario final

- El Cortafuegos...

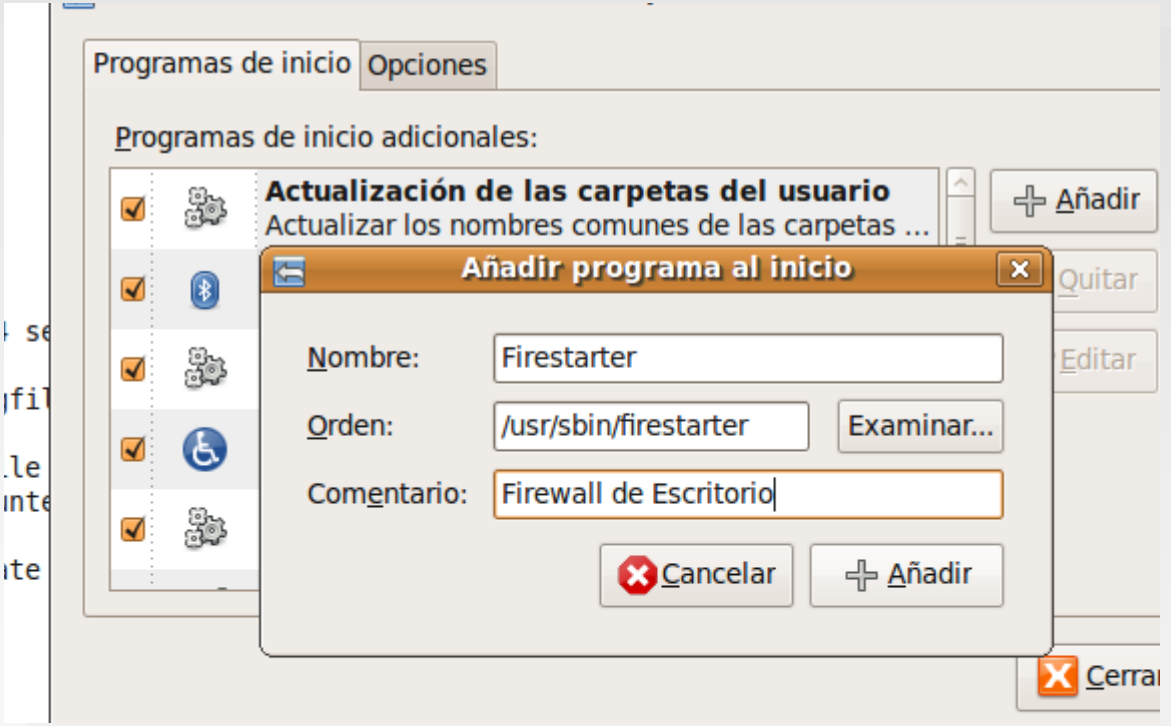
Hardening Linux – Usuario final

- El Cortafuegos...
  - Edición de reglas



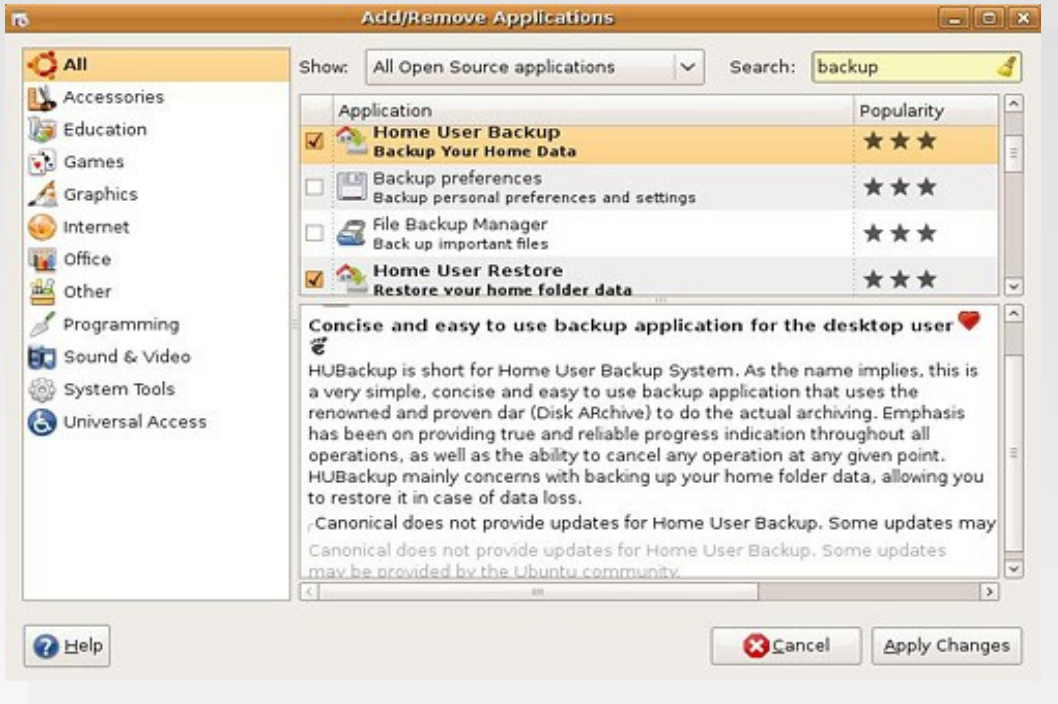
Hardening Linux – Usuario final

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



Hardening Linux – Usuario final

- Respaldar 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

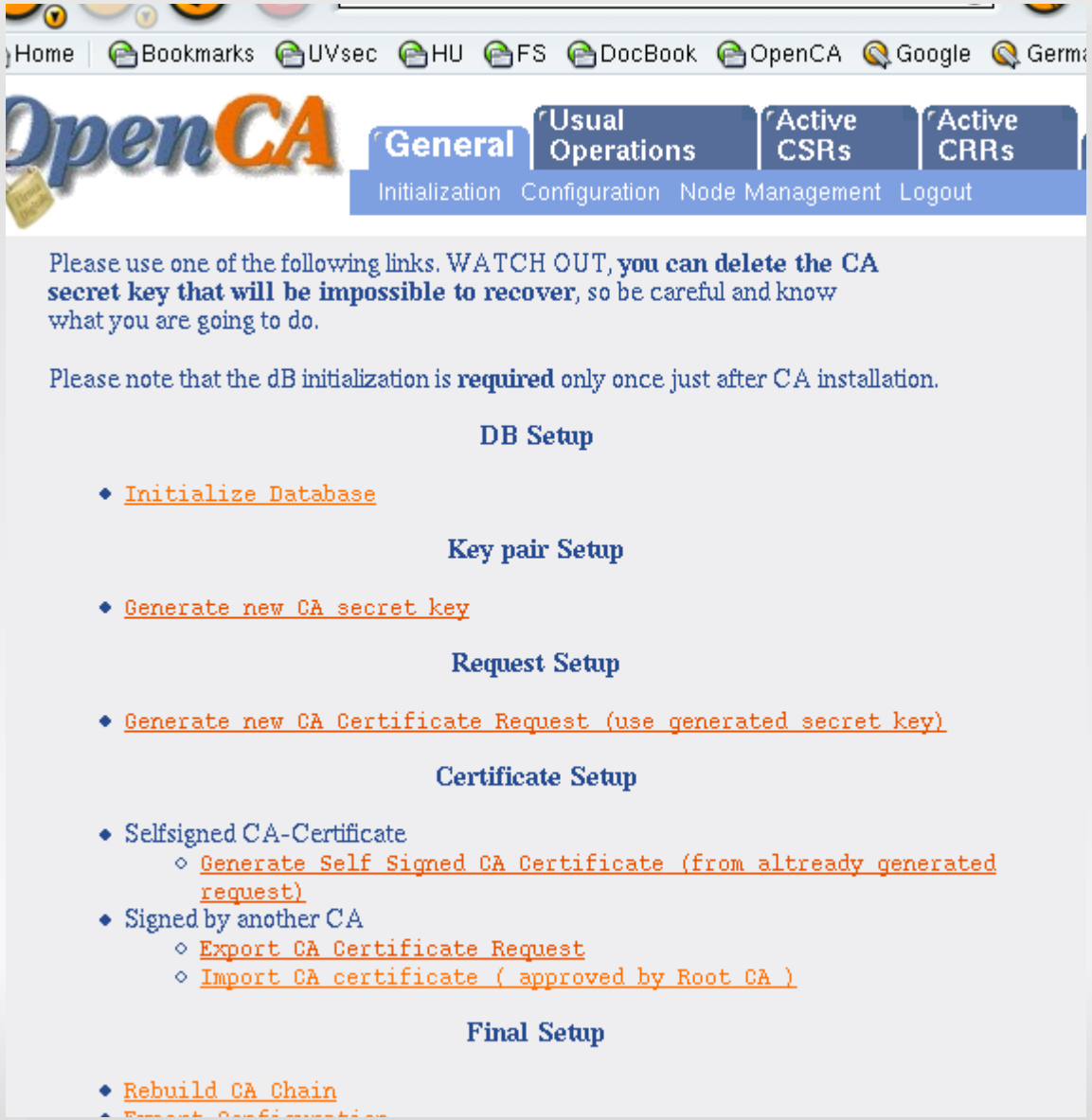
- Recomendaciones:
  - Revisión de Vulnerabilidades
    - OpenVAS
    - Nessus
  - Monitorización
    - Nagios
    - Ntop
    - Zabbix, Zenoss, OpenNMS, etc.
  - Generación de políticas de seguridad!

Infraestructuras de Seguridad

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

Hardening Linux – Avanzado

- OpenCA-LiveCD



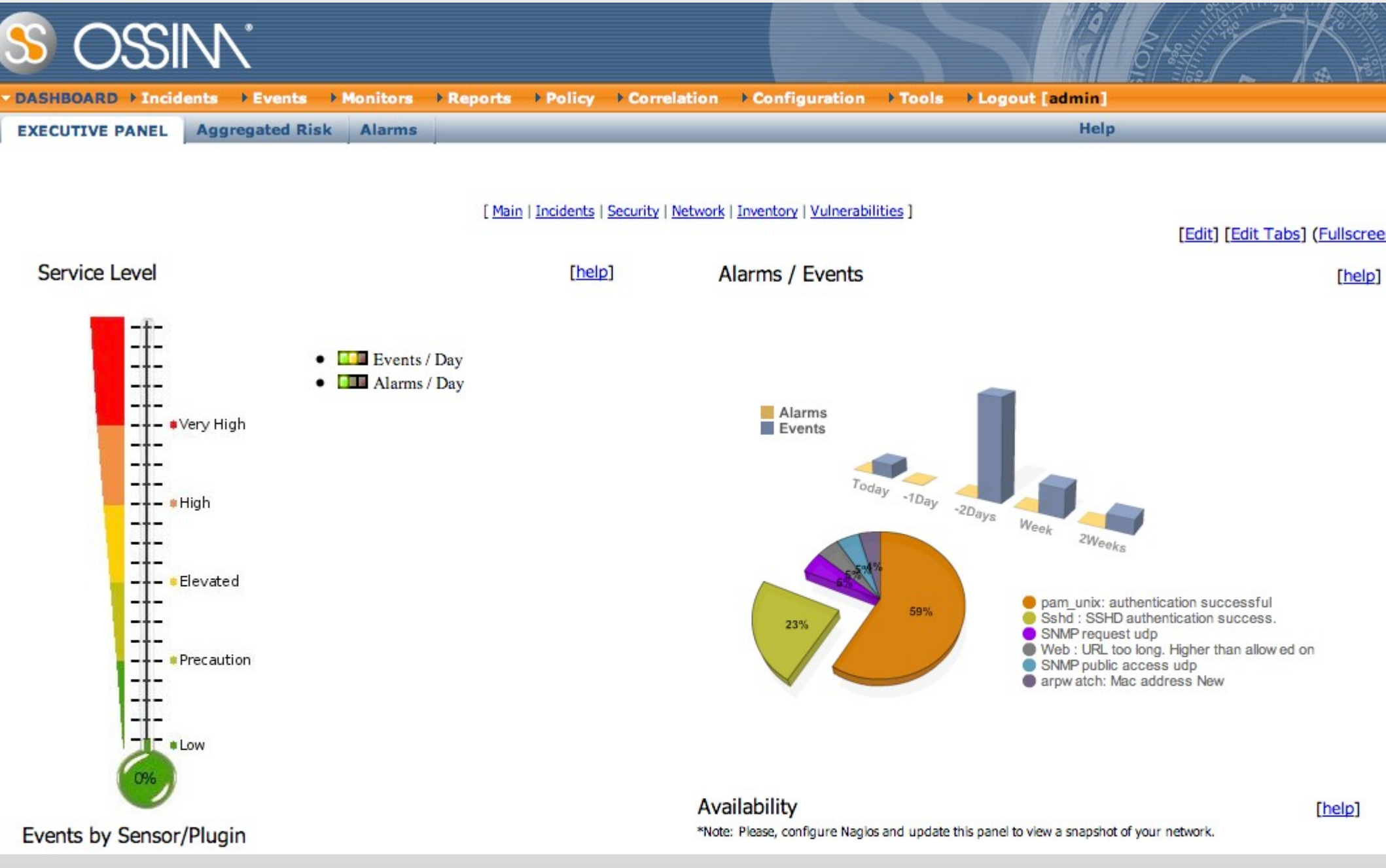
Infraestructuras de Seguridad

- 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

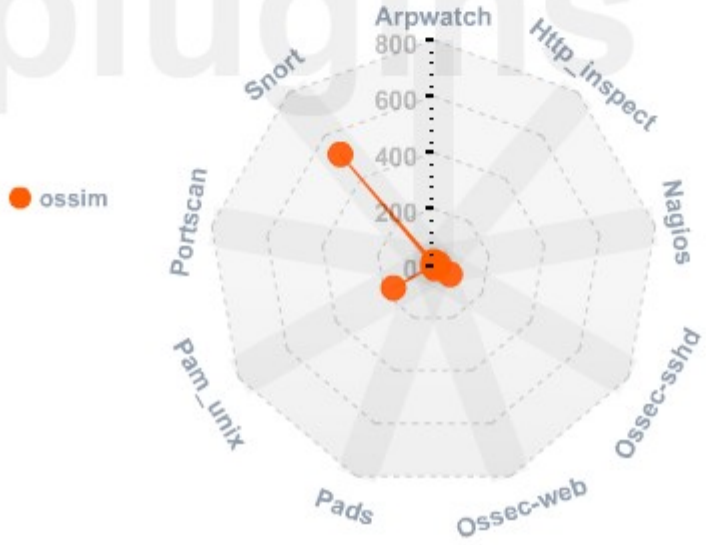
- Open Source Security Information Management
  - Arpwatch
  - P0f
  - Pads
  - Nessus
  - Snort
  - Spade
  - Tcptrack
  - Ntop
  - Nagios
  - Osiris
  - OCS-NG
  - OSSEC
    - integrity, rootkit, registry detection and more

Infraestructuras de Seguridad



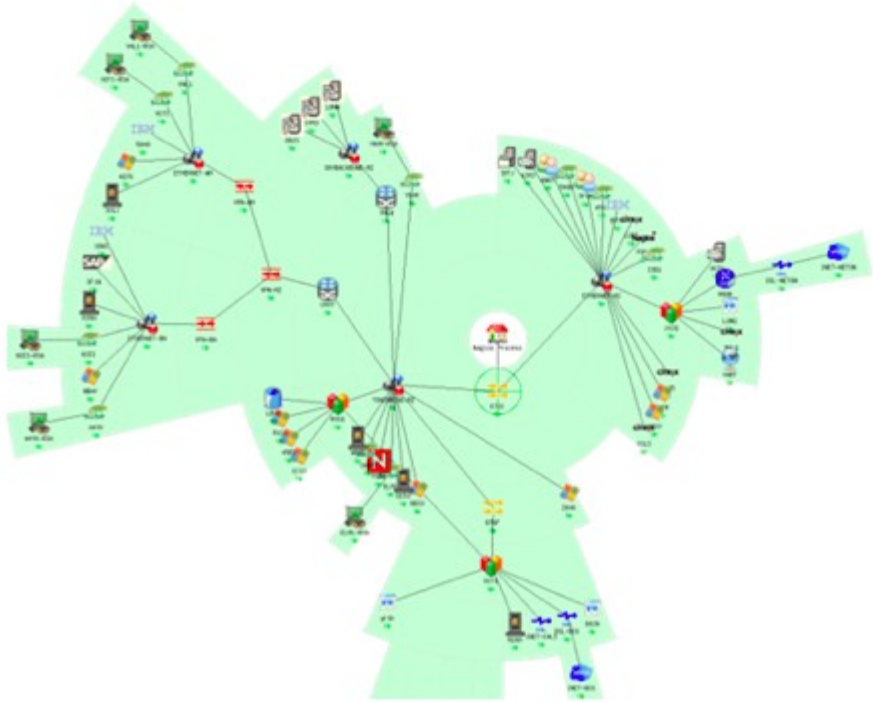
Infraestructuras de Seguridad

Events by Sensor/Plugin

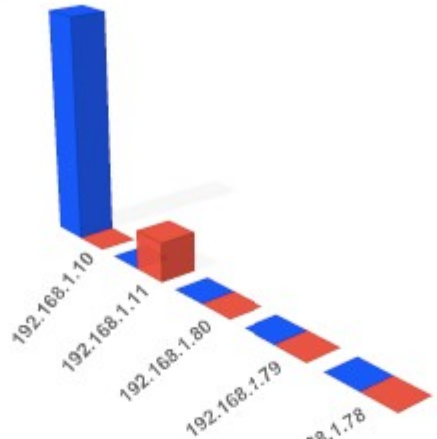


Availability

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



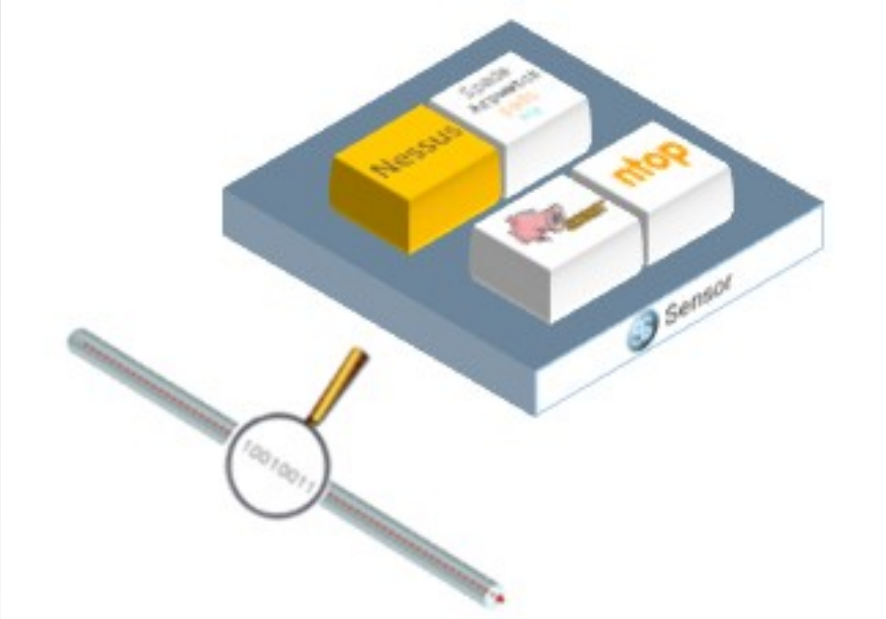
Top 10 hosts risk



Throughput

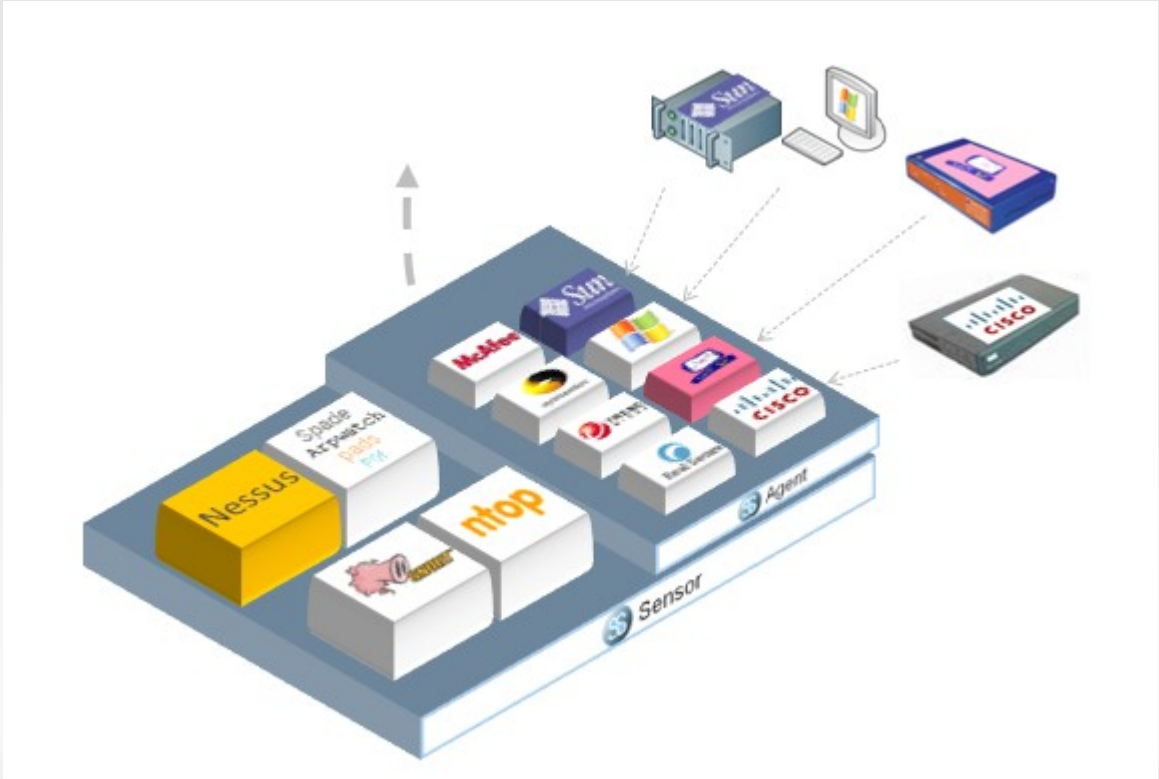
Infraestructuras de Seguridad

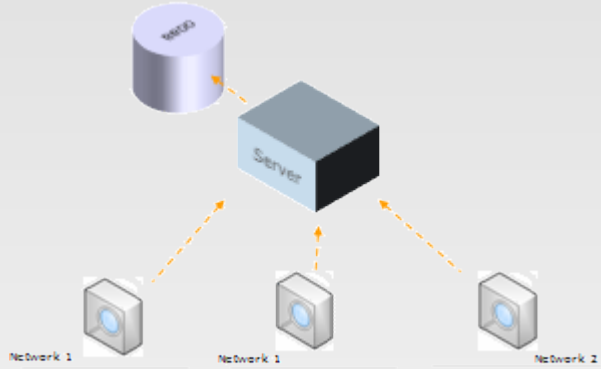
- Open Source Security Information Management
  - Detecta



Infraestructuras de Seguridad

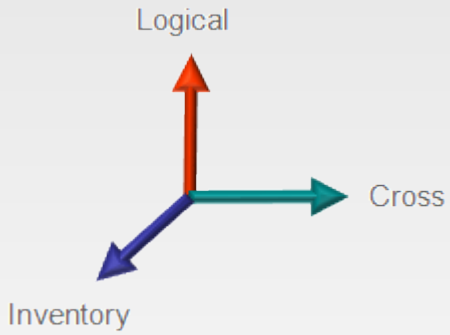
- Open Source Security Information Management
  - Colecta





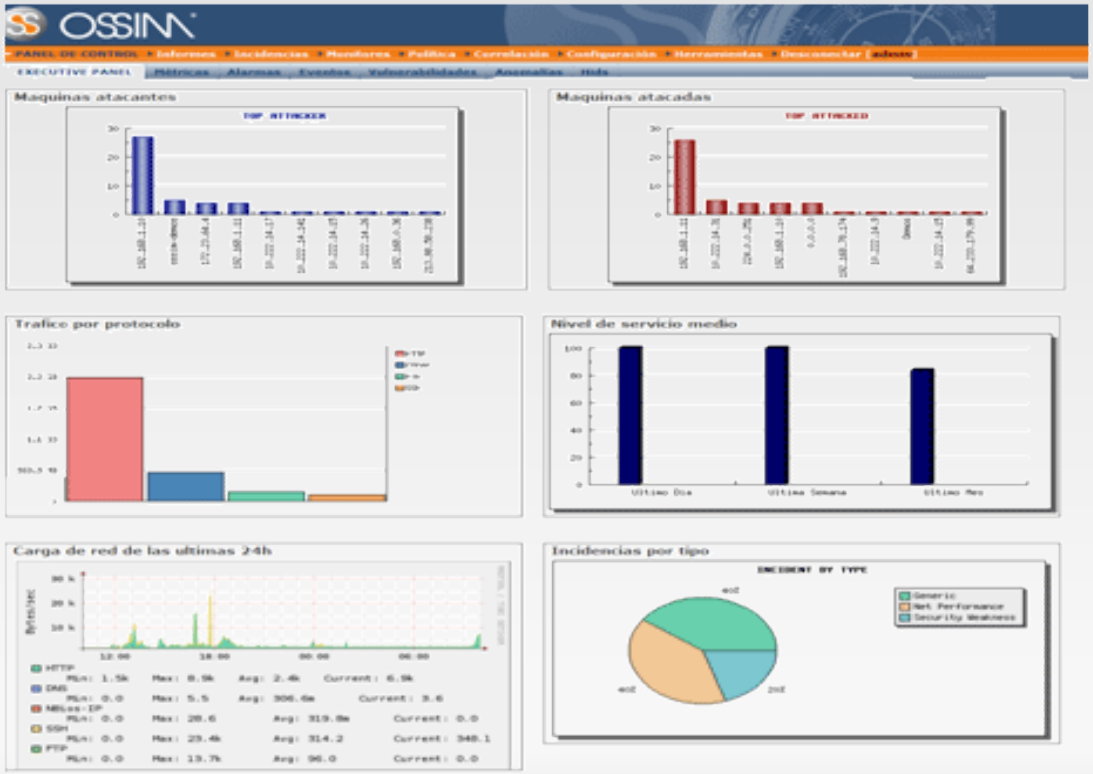
Infraestructuras de Seguridad

- Open Source Security Information Management
  - Correlaciona



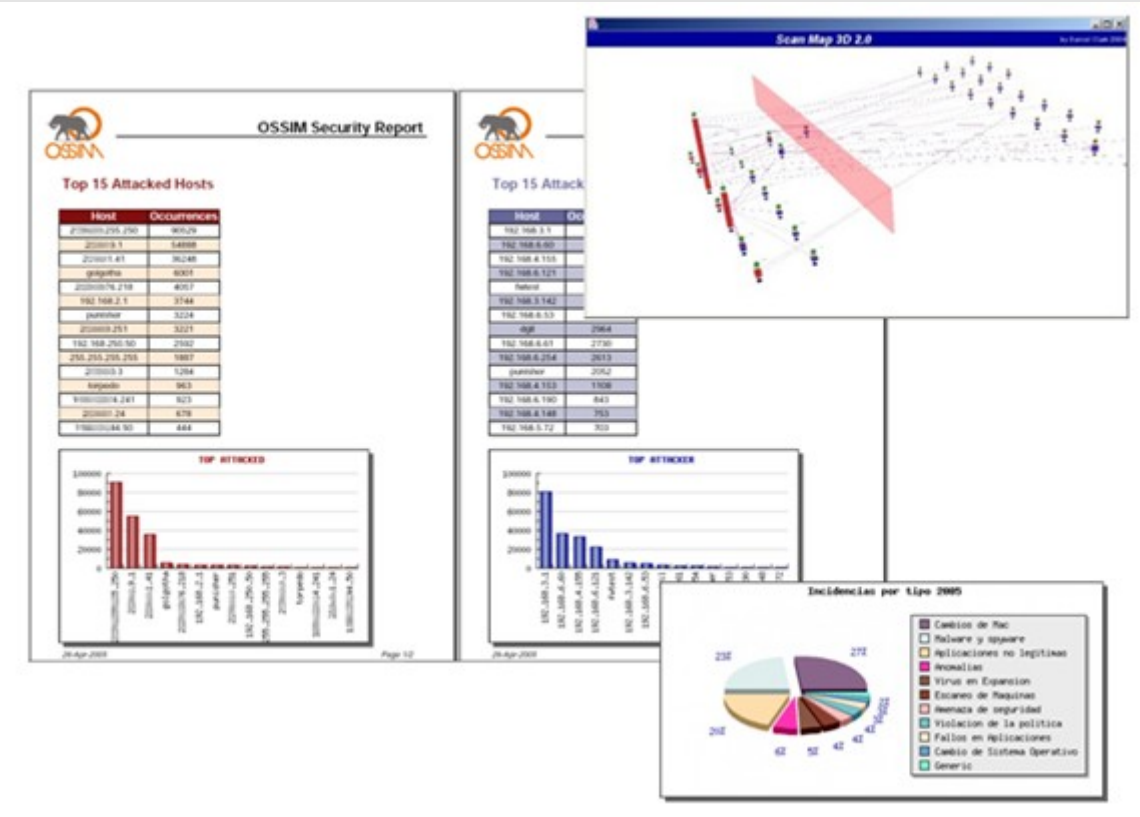
Infraestructuras de Seguridad

- Open Source Security Information Management
  - Reporta



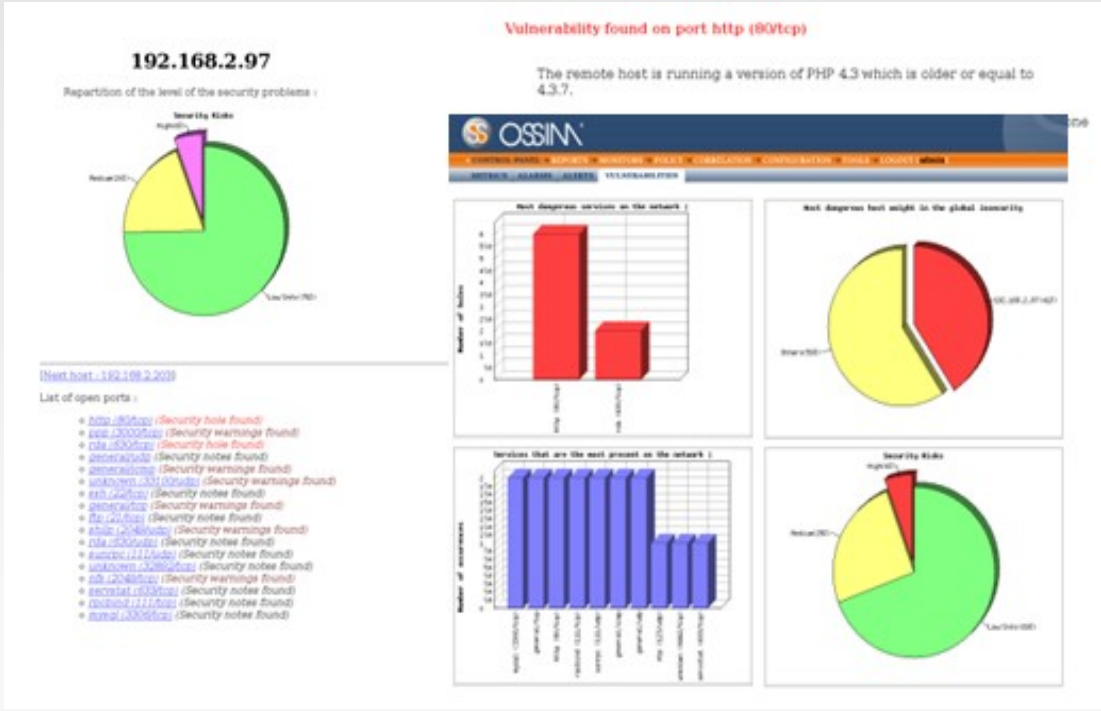
Infraestructuras de Seguridad

- Open Source Security Information Management
  - Reporta



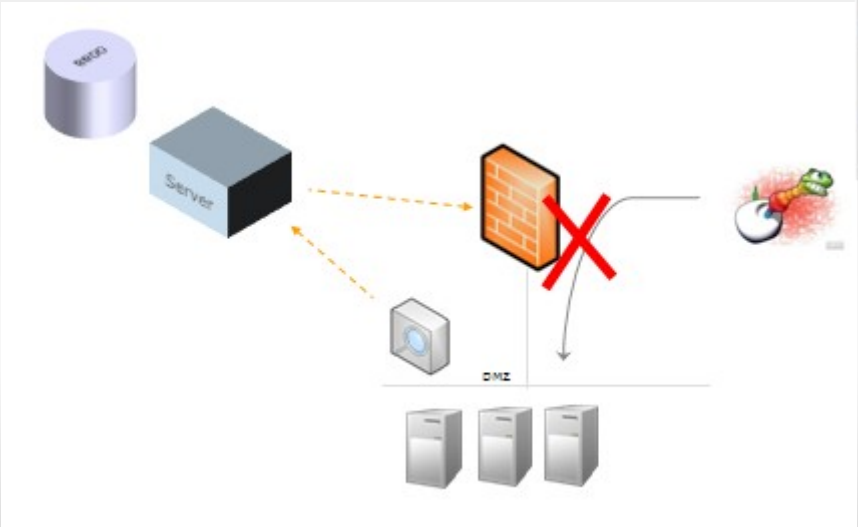
Infraestructuras de Seguridad

- Open Source Security Information Management
  - Reporta



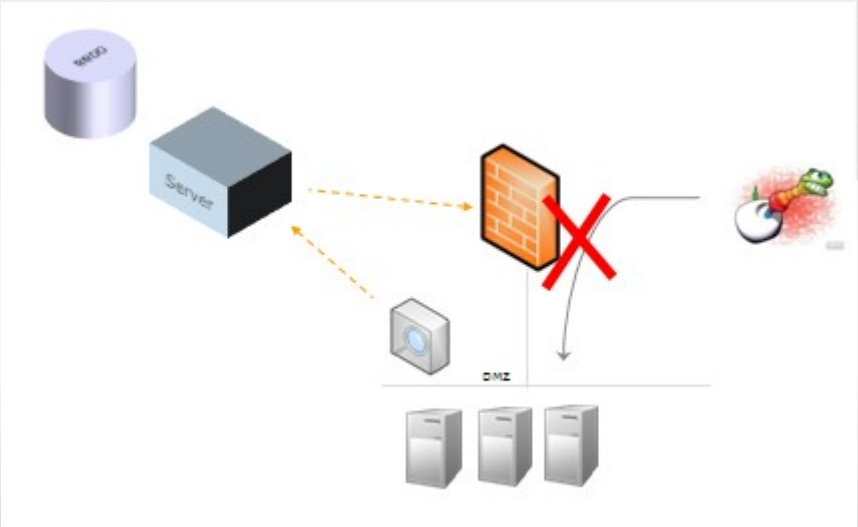
Infraestructuras de Seguridad

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



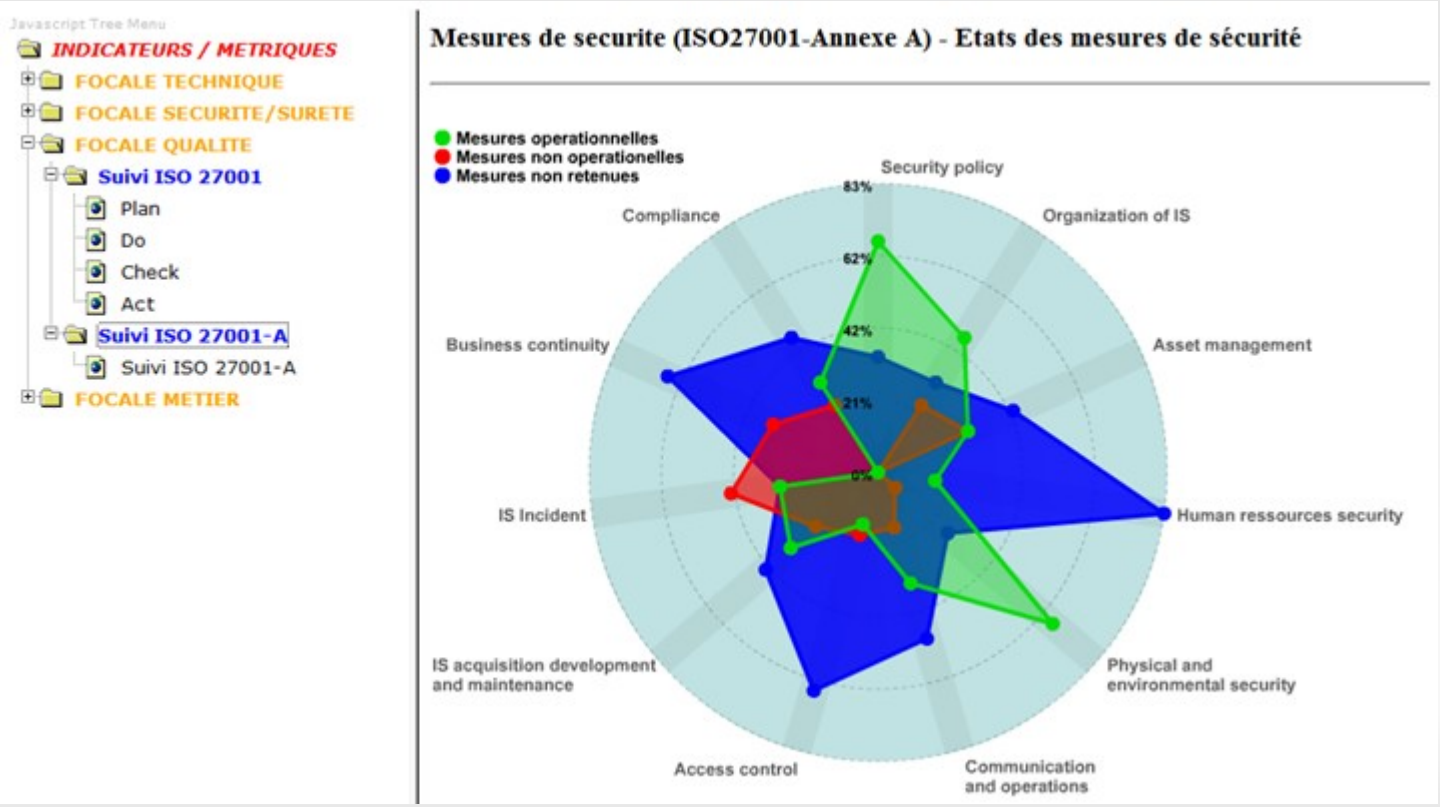
Infraestructuras de Seguridad

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



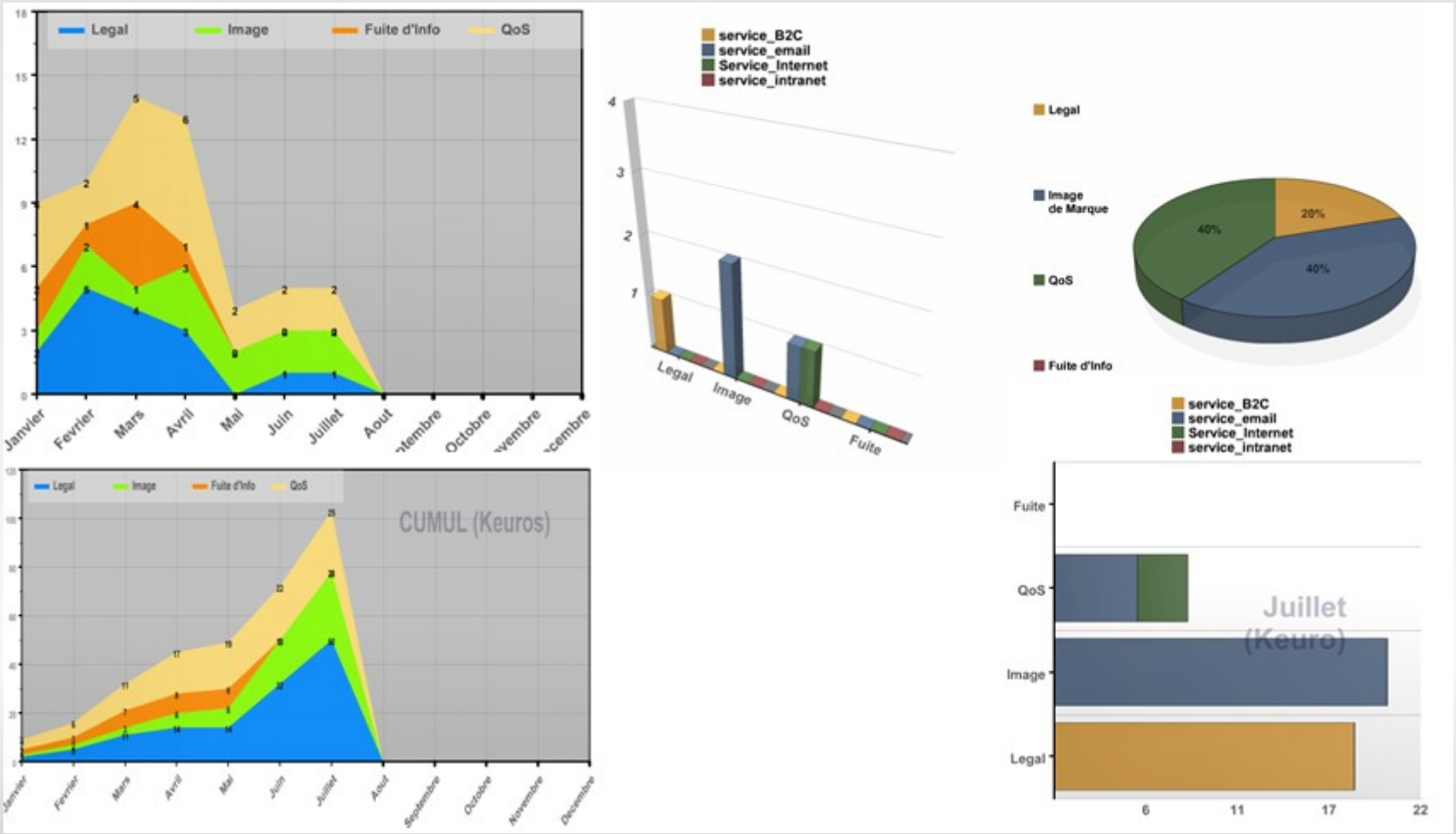
Infraestructuras de Seguridad

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



Infraestructuras de Seguridad

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



Seguridad en Linux

Gracias por su atención...

Ronald Escalona