



# Cancerbero

El perro guardian  
de los puertos



<http://cancerbero.sourceforge.net>

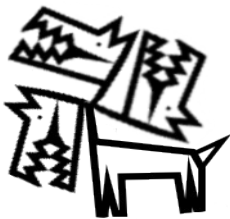
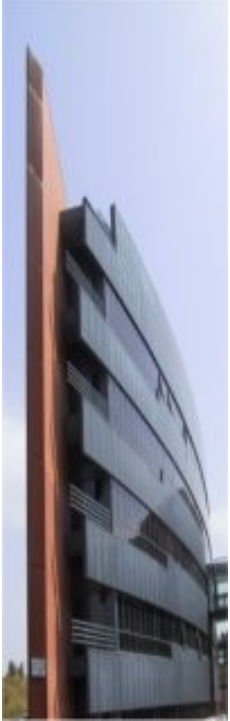
**Víctor Barahona** <[victor.barahona@uam.es](mailto:victor.barahona@uam.es)>

**Carlos ramirez** <[carlos.ramirez@uam.es](mailto:carlos.ramirez@uam.es)>

# Agenda

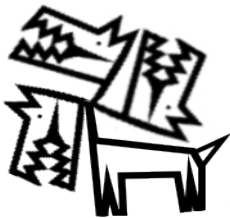
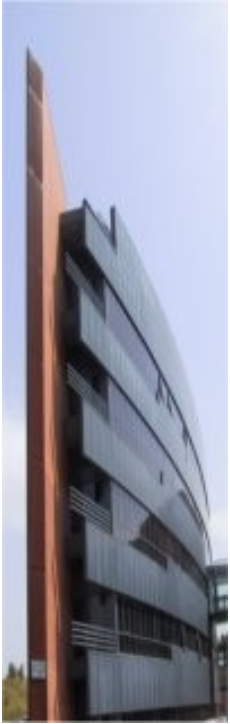
---

- ¿Quién?
- ¿Qué?
- ¿Por qué?
- ¿Cómo?
- ¿Cuándo?
- Arquitectura.
- Funcionalidades.
- Demo.
- Futuro.



## ¿Quién es cancerbero?

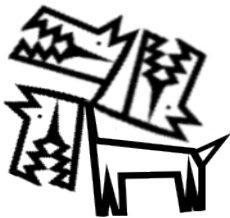
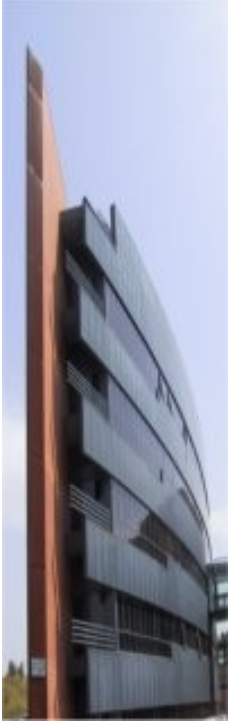
- Mitología griega
- Can Cerbero
- Tiene tres cabezas
- Vigilaba las puertas de Hades
- No permitía entrar a los “vivos”



## ¿Que es cancerbero?

---

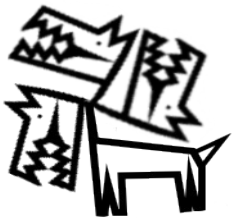
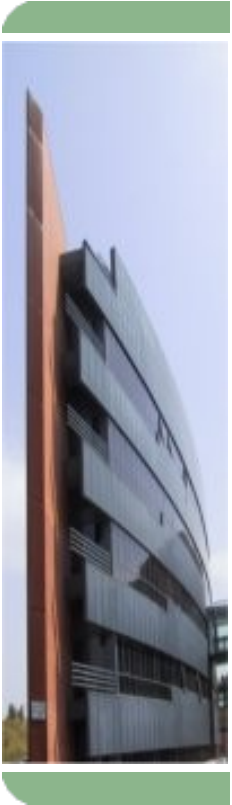
- Sistema de gestión de escanos periodicos.
- Escanea los 65535 puertos tcp.
- Fingerprinting de OS y servicio.
- Mantiene un historico de cada host.
- Genera alarmas ante cambios.



## ¿Por qué desarrollar cancerbero?

---

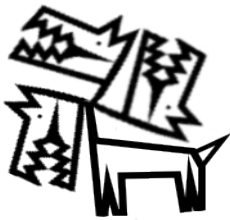
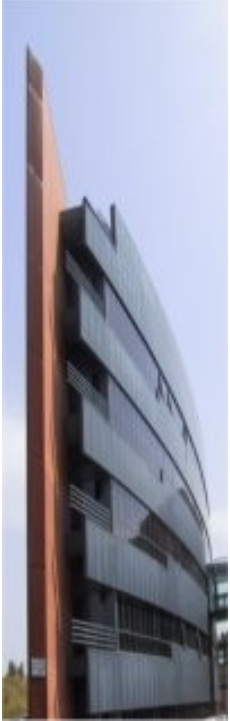
- Poco control sobre los usuarios.
- Ante sospecha escaneo con nmap.
- Service Fingerprinting (-sV)
- ¿Cómo saber qué es normal y qué no lo es?
- Necesitabamos una “foto” previa y actualizada.



## ¿Cómo se hace cancerbero?

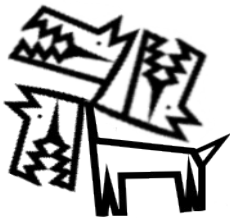
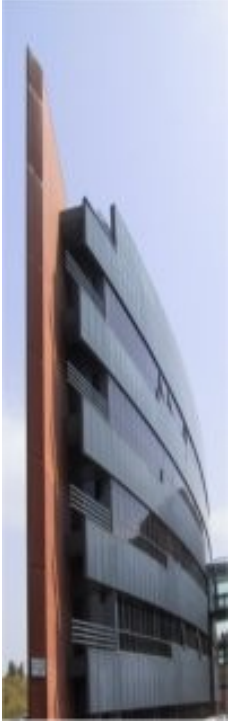
---

- Al principio 2 scripts.
- Se monta un proyecto.
- Licencia GPL
- Basado en herramientas OpenSource:
  - Perl
  - PHP
  - Nmap
  - MySQL



## ¿Cuándo se desarrolla cancerbero?

- Inicio Agosto 2005
- Primera version pública (0.4) en Marzo del 2006
- Replanteo de cancerbero (0.5) en Octubre 2006
- Utilidad y madurez (0.6) en Junio 2007
- Mas por venir (0.7) ¿Diciembre?



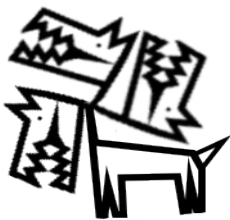
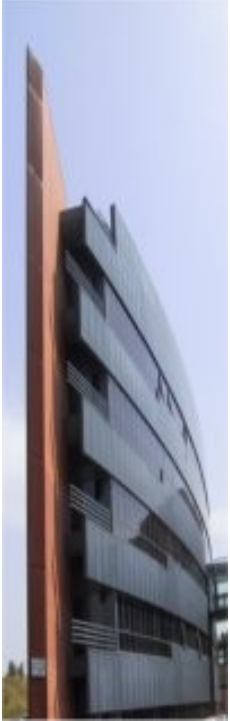
# Elementos de cancerbero

---

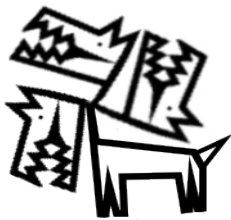
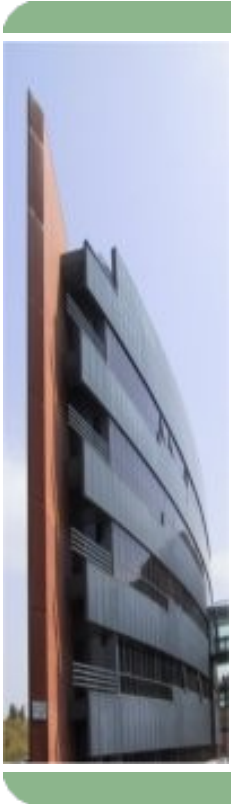
 Base de datos: CancerberoDB

 Cancerbero-sensor: cancerbero

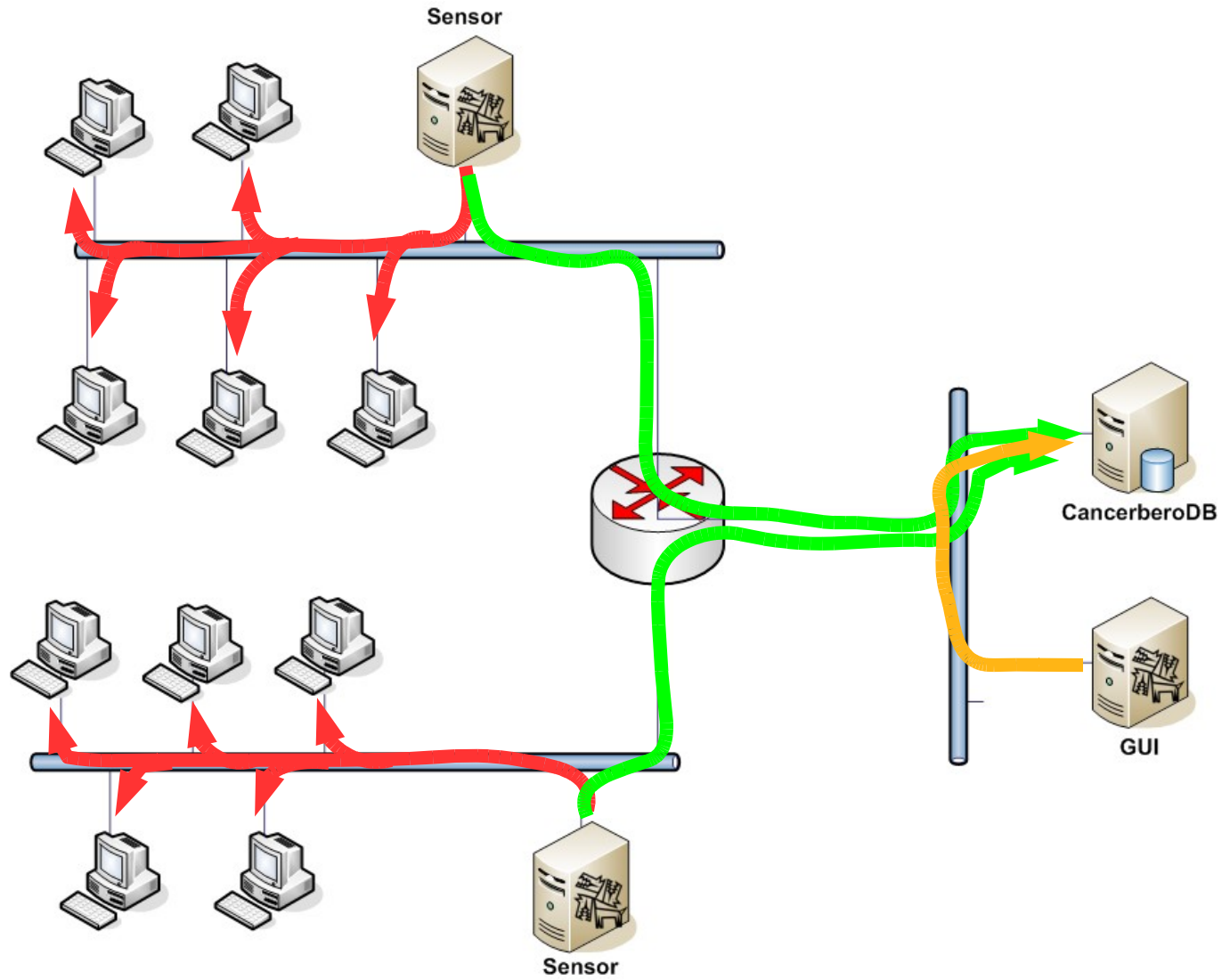
 Consola grafica: cancerbero-GUI



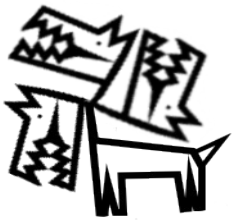
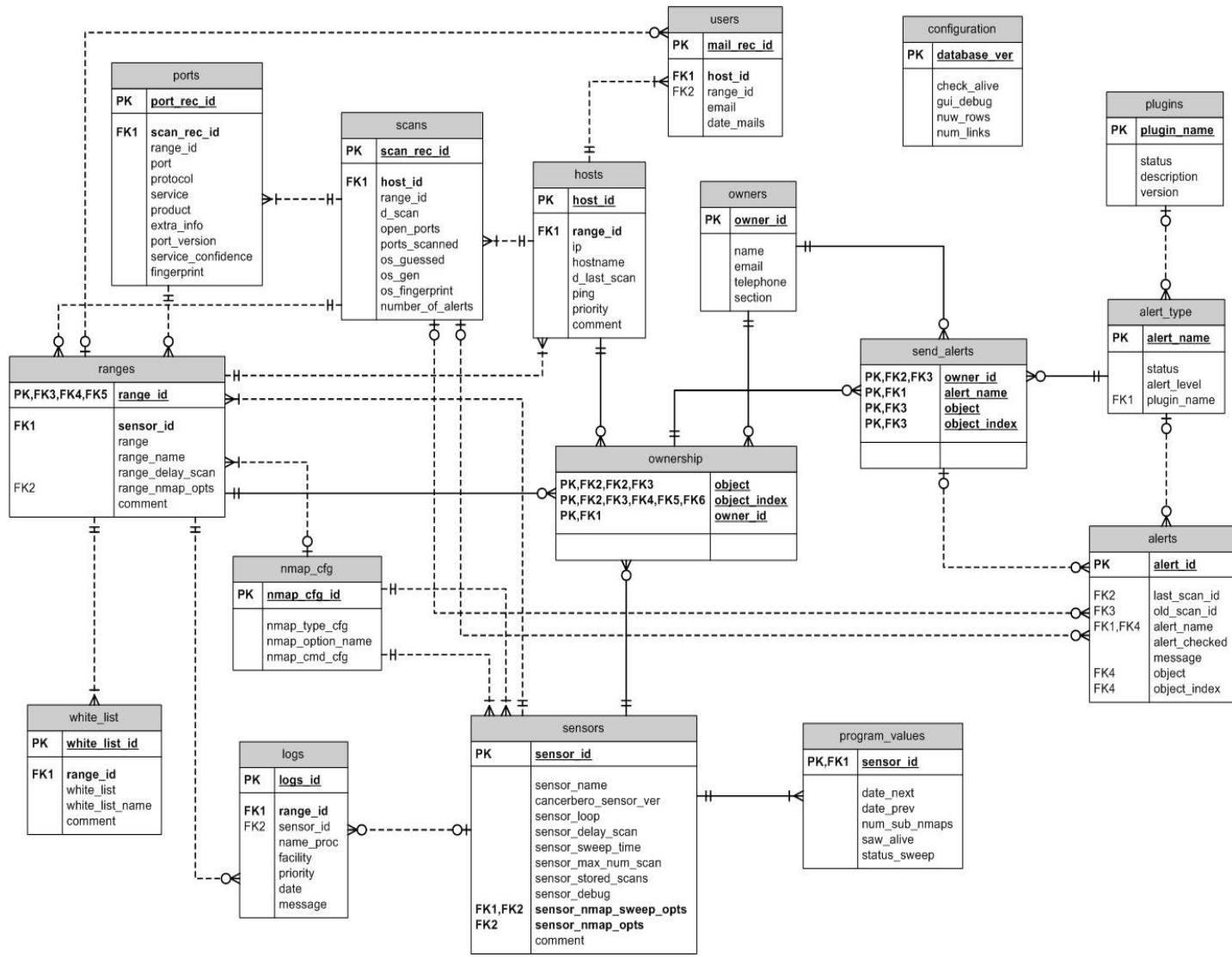
# Arquitectura cancerbero



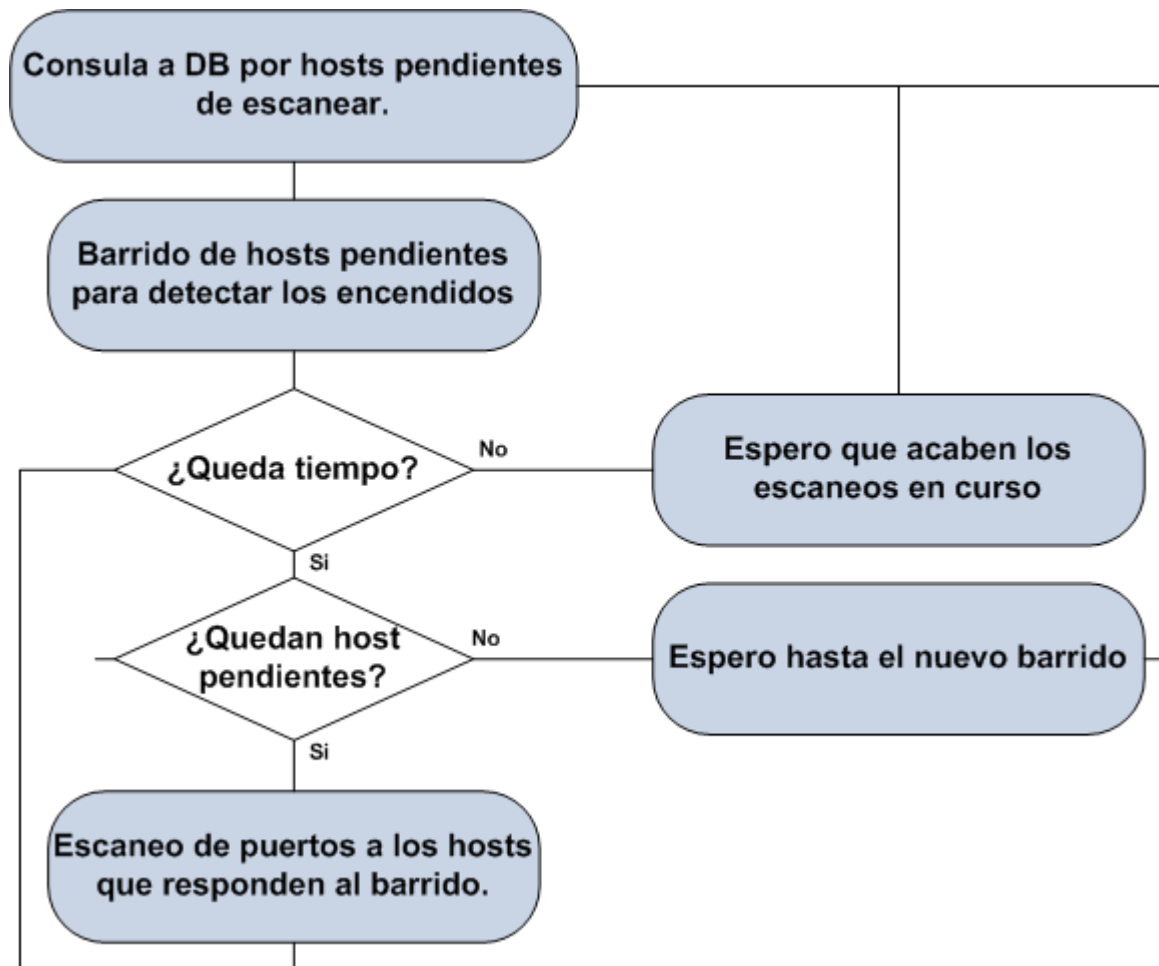
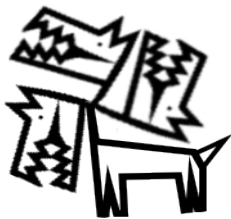
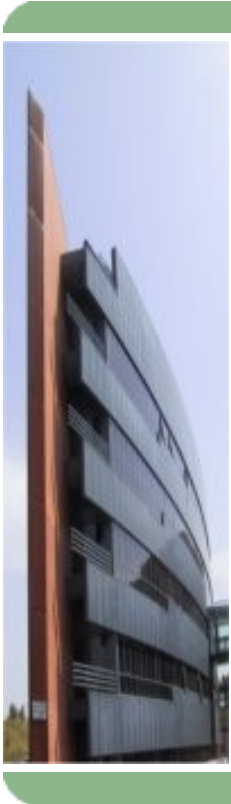
29/06/07



# CancerberoDB



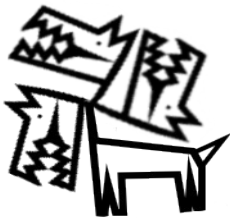
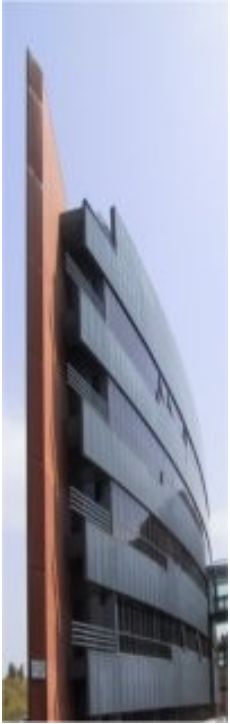
# Cancerbero-sensor



## Funcionalidades avanzadas

---

- Gestion y configuración grafica
- Multiples rangos.
- Multiples sensores.
- Lista blanca.
- Configuración personalizada Nmap
- Plugins.
- Alertas.
- Owners.



# Instalación

- Dependencias:

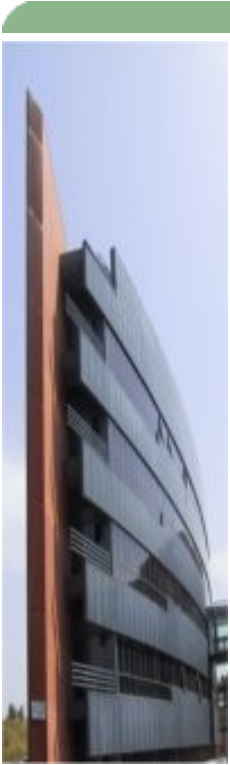
```
# apt-get install fping libapache2-mod-php5 php5-mysql  
php5-cli apache2 mysql-server ucf nmap libdbi-perl  
libnmap-parser-perl
```

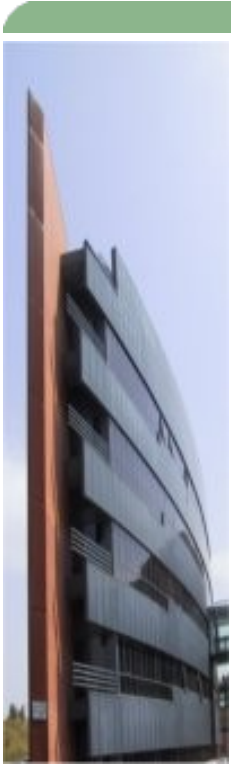
- Tres tipos de instalación:

- Paquetes Debian.
- Inst. guiada.
- Inst. manual.

- Testeado en Debian(Ubuntu) y Fedora.

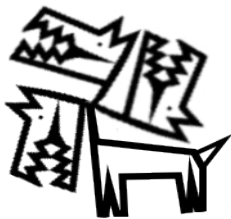
- En breve paquetes RPM.





# DEMO

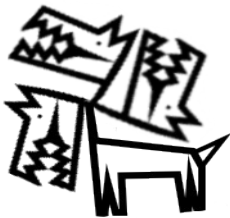
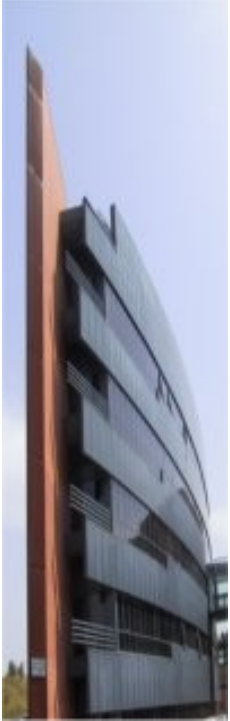
<http://cancerbero.sf.net/site>



## Reflexiones y limitaciones

---

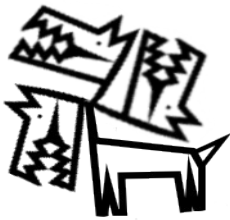
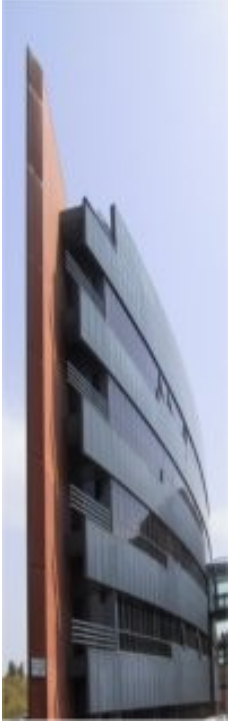
- Host con firewall.
- Impacto en Fws de red.
- Ojo con las impresoras.
- Detección de OS en windows.
- ¿Son lícitos los escaneos?
- ¿Pueden afectar a los hosts?
- ¿Se quejan los usuarios?



## Futuro

---

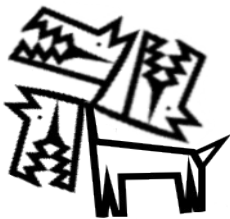
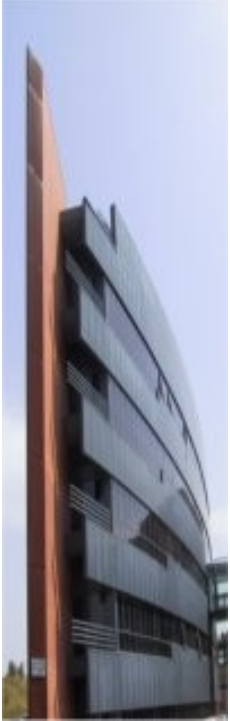
- Paquetes RPM.
- Borrado de alertas.
- Comparación de escaneos en GUI.
- Tratamiento de servicios RPC.
- Plugin: alertas a Descon2
- Plugin: servicios en puertos no estandar.
- Mejora de mensajes de alarmas.
- Guardar banners servicios desconocidos.
- Nuevo sistema de estadísticas (rrdtool)
- ¿Nessus?

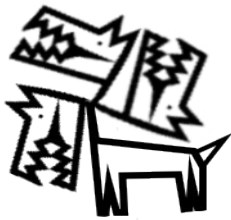
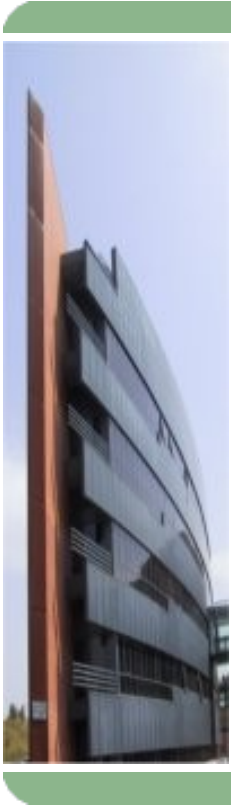


## Links

---

- Pagina oficial:  
<http://cancerbero.sourceforge.net>
- Proyecto:  
<http://sourceforge.net/projects/cancerbero/>
- On-line Demo:  
<http://cancerbero.sourceforge.net/site/>
- Cancerbero 0.4 en Linux Magazine:  
[http://www.linux-magazine.com/issue/67/Charly\\_Column.pdf](http://www.linux-magazine.com/issue/67/Charly_Column.pdf)
- Nmap:  
<http://insecure.org/nmap/>
- Nmapparser:  
<http://nmapparser.wordpress.com/>





# Muchas gracias

## ¿Preguntas?