

El Día a Día del Administrador de Sistemas: Cancerbero

PUERTOS MOVIDITOS

Cuando los puertos de un equipo empiezan a abrirse y cerrarse como ventanas lanzadas al viento, es hora de que los administradores presten atención. **POR CHARLY**

KÜHNAST

El mes pasado, le eché un vistazo a algunas de las nuevas características de Nmap 4.00. Este tema fue muy interesante entonces, sin embargo, éste describiré a Cancerbero [1], una herramienta para monitorizar un servidor basado en Nmap. La herramienta, que está escrita en Perl, hace uso de la potencia de Nmap para escanear los puertos de los dispositivos de red. Cancerbero registra los resultados en una base de datos y utiliza una pequeña interfaz PHP para poder ver mejor los resultados. Los beneficios son obvios: Echemos un vistazo rápido a los puertos y fácilmente podremos saber qué puertos están abiertos o cerrados. Se

distribución basada en RPM. Sin embargo, esto puede ser una buena oportunidad para sacar Alien, la herramienta con nombre extraterrestre que convierte paquetes formateados a RPM. Si no funciona, también puedo pelearme con el fichero tar. Quien no arriesga no gana:

```
alien -r cancerbero_
0.4-1_i386.deb
```

Alien me dio un fichero llamado *cancerbero-0.4-2.i386.rpm*. Vamos a tener cuidado con la primera instalación:

```
rpm -Uvh --test
cancerbero-0.4-2.i386.rpm
```

```
mysql -D database-name
-u SQL-username -p
< cancerbero.sql
```

Cuando instalé el paquete (o desempaqueté el fichero tar), se creó un directorio denominado */site*. Necesito mover este directorio a la ruta donde el servidor web pueda verlo. El fichero de configuración principal, *cancerbero.conf*, se almacena bajo */etc/cancerbero*. Tengo que modificar los parámetros de acceso a la base de datos (nombre de la base de datos, host, nombre de usuario, contraseña) para que coincida con la configuración de MySQL. También necesito definir el *rango* de la red que Cancerbero va a monitorizar, por ejemplo 192.168.1.0/24. Desafortunadamente, el programa está restringido a un solo rango actualmente; en mi humilde opinión, esta es la mayor restricción de Cancerbero. Pero el autor ha prometido arreglarlo y el programa sólo va por la versión 0.4. La *lista-blanca* me permite definir una lista separada por comas de redes y equipos que esta herramienta nunca debería escanear. Esto es realmente útil si se tienen impresoras en la red. Finalmente, necesito pasar los parámetros de la base de datos que ya le he pasado a Cancerbero en su interfaz PHP. Para hacerlo, sólo necesito introducir los datos en */include/dbconnect.php*. ¡Terminado! Ahora sólo tengo que hacer clic para escanear con mi navegador.

host_id	Date	Time	Hostname	Ip	Ports	OS	Ping
31500	2006-02-22	14:20:25	Edit NO DNS	64.88	0	IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS*	✓
20289	2006-02-22	14:20:24	Edit batisselles	251.99	1	Motorola SurfBoard SB4100E Cable Modem	✓
29767	2006-02-22	14:20:25	Edit mauintanillo1	251.108	6	Microsoft Windows XP SP2	✗
45558	2006-02-22	14:20:26	Edit liduran	3.50	1	Microsoft Windows XP Pro SP1/SP2 or 2000	✗
53106	2006-02-22	14:20:27	Edit NO DNS	66.6	0	Microsoft Windows SP4	✗
38825	2006-02-22	14:20:26	Edit salapas5	6.157	10	Microsoft Windows 98SE 4.10.2222	✓
63351	2006-02-22	14:20:56	Edit carial	41.11	4		✓

Figura 1: Salida detallada de Cancerbero tras completar un escaneo. La interfaz en PHP muestra un listado de los puertos abiertos y los sistemas operativos de los servidores.

encuentran disponibles un archivo tar y un paquete Debian del programa. En mi caso, la última opción no lo está, ya que mis equipos de laboratorio ejecutan una

componentes que necesita Cancerbero. Afortunadamente, la lista no contiene nada que sea realmente raro y si está acostumbrado a tratar con Perl, probablemente ya tenga estos componentes instalados en el sistema.

Crear una Tabla en la Base de Datos

Como Cancerbero quiere almacenar los datos en una base de datos MySQL, tendré que crearla primero (hay una excelente guía paso a paso en [2]). Cancerbero le proporciona una tabla para explicar la estructura, y para usarla puede introducir:

SYSADMIN

Samba 460

Aprende lo nuevo de la próxima versión del servidor de ficheros y de impresión Samba.

Privilegios root con OP64

La versátil utilidad Op es una herramienta sencilla para la gestión de los privilegios de los usuarios.

RECURSOS

[1] Cancerbero: <http://cancerbero.sourceforge.net>

[2] Instalación: <http://cancerbero.sourceforge.net/install.html>