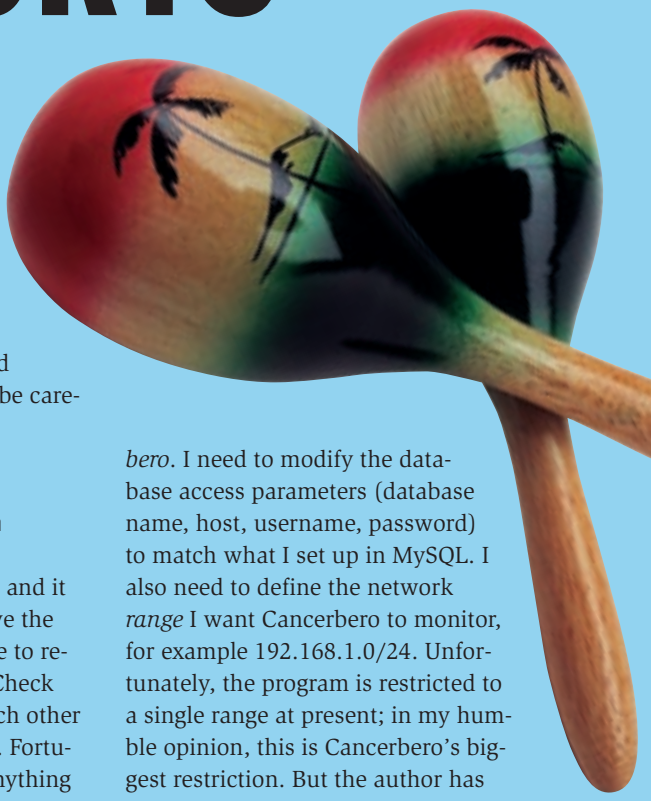
The Sysadmin's Daily Grind: Cancerbero

RATTLING PORTS

When ports on a host start opening and closing like window shutters in a gale, it's time for admins to pay attention.

BY CHARLY KÜHNAST



Last month, I took a look at some features of the new Nmap 4.00. This topic is far too interesting for just one month, however, so this month, I'll describe Cancerbero [1], a server monitoring tool based on Nmap.

The tool, which was written in Perl, leverages the power of Nmap to port scan your network devices. Cancerbero logs the results in a database and uses a small-footprint PHP front-end to make the results more readable. The benefits are obvious: I get an at-a-glance overview of open ports, and I can easily see which ports are open or closed.

A tarball archive and a Debian package of the program are available. The latter option is not open to me, as my lab machine runs an RPM-based distribution. However, this might be a good opportunity to try out Alien, the tool with

Figure 1: Cancerbero's detail view after completing a scan. The PHP front-end lists the open ports and the operating systems of the servers.

the extraterrestrial name that converts package formats to RPM. If it doesn't work, I can always fight my way through the tarball. Nothing ventured, nothing gained:

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

An alien just gave me a file called *cancerbero-0.4-2.i386.rpm*. Let's be careful with the first installation test:

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

All is quiet on the Western front, and it stays that way even after I remove the *--test* parameter. Of course, I have to resolve the dependencies myself. Check out the list at [2] to find out which other components Cancerbero expects. Fortunately, the list doesn't contain anything really obscure, and if you dabble with Perl, you probably have most of these components installed anyway.

Creating a Database Table

As Cancerbero wants to store the data it collects in a MySQL database, I have to create a database first – there is an excellent step-by-step guide at [2]. Cancerbero gives you a sample table to explain the structure, and you can enter

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

to use this. When you install the package (or untar the tarball), a directory named */site* is revealed. I need to move this directory to a path where the web server can see it.

The central configuration file, *cancerbero.conf*, is stored below */etc/cancerbero*. I need to modify the database access parameters (database name, host, username, password) to match what I set up in MySQL. I also need to define the network *range* I want Cancerbero to monitor, for example 192.168.1.0/24. Unfortunately, the program is restricted to a single range at present; in my humble opinion, this is Cancerbero's biggest restriction. But the author has promised to improve this, and the program has only just reached version 0.4.

The *white_list* lets me define a comma-separated list of networks and hosts that Cancerbero should never scan. This is really useful if you have printers on your network. Finally, I need to pass the database parameters that I have already passed to Cancerbero to the PHP front-end. To do so, I just need to enter the data in */include/dbconnect.php*. Finished! Now I can just click to scan in my browser. ■

SYSADMIN

Samba 4 60
Learn what's new in the next release of the Samba file and print server suite.

INFO

[1] Cancerbero: *http://cancerbero.sourceforge.net*

[2] Installation: *http://cancerbero.sourceforge.net/install.html*

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data-center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).