The sys admin's daily grind: login mail

Spyglass

Charly often gets suggestions and ideas for his column at community get-togethers. Last week, he picked up a tip for an early warning system that quickly secures login attempts.

By Charly Kühnast

Some servers I don't log in to for weeks on end. On machines like this, the danger of intruders being able to log in without my noticing is fairly high. And if attackers do manage to crack open a victim's computer, they will do everything they can to cover their tracks. This includes removing all traces of the login from the logs, which makes it more or less impossible to ascertain the exact time of the attack and – what's more important – the attacker's IP.

Enter Markus's script. Markus? Well, just recently there was a meeting of system and network administrators at a training center in Essen, Germany – yours truly being just one of them – to discuss establishing a complex OpenVPN structure with some hands-on stuff to follow. The Master of Ceremonies at this event was none other than OpenVPN expert Markus Feilner (who also happens to be on the editorial staff of one of our sister magazines). Of course, we took some time to chat during breaks, especially about my penchant for trying to solve problems with incredibly long one-liners. Markus said he had a beast of a similar feather for me to look at, an intrusion detector. The functional principle of this one-liner is just as simple as it is effective.

Gone is Gone

The one-liner starts when the shell is opened and immediately sends mail to the admin containing the output from a `who` command. This happens so quickly that the attacker doesn't stand a chance of stopping the mail from going out. The one-liner resides in the system global `bashrc`:

```
echo 'Login on' `hostname` `date` \
   `who`| mail -s "Login on `hostname` \
   `who | awk '{print $5}'`" \
   charly@kuehnast.com
```

The part up to the first pipe character (|) generates the content of the mail. The `date` command provides a precise timestamp, and `who` contributes a list of logged in users. Output from `who` can look like this:

```
root pts/0 2010-05-02 13:21
   (islay.kuehnast.com)
```

Here, I'm logged in as root. The hostname in parentheses tells you where the login originated. This information is decisive if you want to catch an intruder.

The second part of the one-liner triggers the `mail` command and, thanks to the `-s` option, generates the subject line. Awk extracts the hostname of the IP of the sender in a targeted way from the `who` output. This means I don't even need to open the message, just check the subject line to see if the login came from a known and trustworthy source or not, in which case, I would need to take a closer look at the system.

Talk about taking a closer look: I'm heading off to LUG Camp. I wonder who will give me an idea for the next column. Come back next month to find out. ■■■

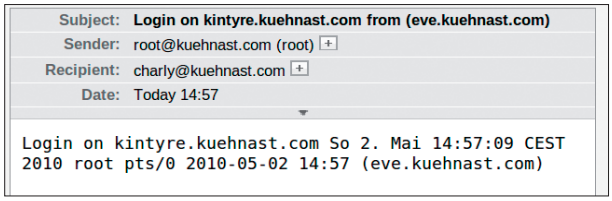

Figure 1: You've probably seen more exciting messages, but information is priceless if you're hunting down an intruder.

CHARLY KÜHNAST

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.