The Sysadmin's Daily Grind: Fwlogwatch

The Beast

The Fwlogwatch tool extracts interesting lines from Firewall logfiles, and can become useful in automatically reporting, if the admin so desires. Something efficient and powerful is an added bonus to our amory of tools

BY CHARLY KÜHNAST

Iptables logfiles can contain so much information that admins attempting to evaluate them can no longer see the wood for the trees. The GPL tool Fwlogwatch [1] can help. The tool is available as a RPM package for Red Hat or as a rather large 90 Kbyte tarball that can be installed using *make && make_install*.

I tend to keep Fwlogwatch on a diet of iptables logfiles, but the tool will happily consume output from ipchains, BSD ipfilters, Cisco IOS and Pix, Elsa Lancom routers, and Snort. The following lines show some typical syntax for the program:

```
fwlogwatch -w -o out.html➥
-n -p -s -d -y /var/log/fwlog
```

This tells Fwlogwatch to evaluate critical iptables entries, and write them to the file *out.html*. If you are only interested in viewing entries with multiple occurrences, you can add the *-m X* parameter to filter any lines that occur less than X times in brief succession (see Figure 1).

One practical aspect is the fact that you do not need to parse a complete logfile. The *-l 1h* parameter only looks at data in the past hour, for example. Fwlogwatch also offers a Realtime Response Mode where the logfile is monitored in realtime, allowing prompt incident response. The syntax is as follows:

```
fwlogwatch -R -a 5 -l 8h -A➥
notify.pl -B block.pl
```

This turns Fwlogwatch into a clever daemon that lurks in the background watching for incoming connections. An alert threshold of five occurrences in the logfile is specified by the *-a 5* flag. If this threshold is exceeded, the daemon calls two scripts, as specified in the sample syntax earlier: *notify.pl*, the name should be self-explanatory, and a response action script called *block.pl*. You will have to write both of these yourself, as they do not come with the Fwlogwatch package.

Alert and Response Scripts

The *block.pl* script can be designed to apply a *REJECT* rule to connections for IP addresses that make a nuisance of themselves by launching continual portscans.

Of course, this is just an example, portscans need not be malevolent but people who scan my servers for hours and fill the logfiles with reams of garbage data, are looking to get their fingers rapped!

#	interval	proto	source	port	destination	port
5	00:00:00:45	tcp	194.77.253.244	34310	10.254.35.148	888
4	00:00:00:30	udp	10.254.20.1	35042	10.254.35.148	161
2	00:00:00:03	tcp	10.254.35.10	29872	10.254.35.148	23
2	00:00:00:03	tcp	10.254.35.10	29875	10.254.35.148	161
1	-	tcp	10.254.35.10	29876	10.254.35.148	3128

Figure 1: Multiple occurrences are easily filtered

A rule of this kind is ephemeral and will disappear after the interval specified by the *-l 8h* flag, that is eight hours in our example. The default is 24 hours.

Talking about daemons, the tool provides a useful function for admins who want to report misdemeanors by other Internet residents to the powers that be. If you add appropriate scripts, the tool can parse the logfile to create perfectly worded complaint messages. ■

INFO

[1] Fwlogwatch: *http://cert.uni-stuttgart.de/projects/fwlogwatch*

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). Although Charly started out on IBM mainframes, he has been working almost exclusively with Linux since 1995.