

Re: way to duplicate logs?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-12/0024.html>

From: Nielsen (nielsen_at_memberwebs.com)

Date: 12/11/04

Date: Sat, 11 Dec 2004 01:25:58 +0000 (GMT)

Bob Ababurko wrote:

> Also, is there a way to make more than one copy of these logs?...I am
> not sure how this is set up and but I would like to possibly have
> another set of logs in place so if someone is editing them, I can catch
> it. I know there is a chance that I may be overreacting., but just in
> case I want to know.

You can forward them to another machine. Add a line like this to your syslog.conf:

```
*.* @hostname
```

And then on the other machine change syslogd to accept (udp log packets) connections from other machines by removing the '-s' flags.

Of course if someone is really messing around they'll be able to send bogus logs to your other logging machine too.

Cheers,
Nate

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"