

Re: preventing tampering with tripwire

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-06/9804.html>

From: Maxlor (mail@maxlor.com)

Date: 06/19/02

Date: Wed, 19 Jun 2002 02:12:33 +0200
From: Maxlor <mail@maxlor.com>
To: Baldur Gislason <baldur@foo.is>

As I read that, I thought "Doh". Thats really pretty much the ideal solution...

And if an attacker has physical access to my machine, well, he can do pretty much anything he wants anyway.

Thanks!

—On Dienstag, 18. Juni 2002 23:40 +0000 Baldur Gislason <baldur@foo.is> wrote:

> *use kern.securelevel 1 or higher and man chflags, set the tripwire binary*
> *schg so it cannot be tampered with. Of course there's no such thing as*
> *absolute security, but this moves you just a step closer. Unless the*
> *intruder performs a reboot and makes his changes before the kernel*
> *securelevel is raised on boot.*
>
> *Baldur*

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message