

Re: Anti-Rootkit app

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2008-01/msg00017.html>

- *From:* "Michael W. Lucas" <mwlucas@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 14 Jan 2008 16:24:11 -0500
-

On Sun, Jan 13, 2008 at 10:38:37PM +0100, Jordi Espasa Clofent wrote:

Hi all,

I need to install an anti-rootkid in a lot of servers. I know that there're several options: tripwire, aide, chkrootkit...

?What do you prefer?

Obviously, I have to define my needs:

- easy setup and configuration
- actively developed

These needs are nice, but what effects do you want to achieve?

If you want to verify that nobody's loaded a rootkit, you can use chkrootkit. Note that detecting a running rootkit is actively hard, and is prone to failure.

If you want to verify that nobody has changed files on your system, you can use a tripwire-like system. Mtree(1) actually includes tripwire-like functionality, which I've used quite successfully in the past.

I think that the latter is more realistic, but that's just my humble opinion.

==ml

--

Michael W. Lucas mwlucas@xxxxxxxxxxxxxxxxxxxxxxxx, mwlucas@xxxxxxxxxxxx
<http://www.BlackHelicopters.org/~mwlucas/>
Now Shipping: "Absolute FreeBSD" -- <http://www.AbsoluteFreeBSD.com>
On 5/4/2007, the TSA kept 3 pairs of my soiled undies "for security reasons."

freebsd-security@xxxxxxxxxxxx mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

Re: Anti-Rootkit app

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