

Re: Monitoring a file?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2003-11/2554.html>

From: Cordula's Web (*cpghost_at_cordula.ws*)

Date: 11/24/03

Date: Mon, 24 Nov 2003 00:53:38 +0100 (CET)

To: freebsd-questions@freebsd.org

> > *I've finally found the culprit with a traditional method:*
> > ** md5 (binary from an uncompromised machine) on all files*
> > ** reinstalling from scratch (not buildworld, but really*
> > *installing from FTP)*
> > ** md5 again and diff.*
>
> *[snip]*
>
> > *Ugh... system clean again at last. :)*
>
> *You can't be sure. The attacker probably put an suid binary somewhere*
> *besides the normal system binaries, in which case it's still there and*
> *you may still be vulnerable. When you know you've been hacked, you*
> *need to wipe the disk and *really* reinstall from scratch. And be*
> *very careful about what you restore from backups, too.*

I've inherited a set of 280 1U rack mount boxes, and I am in the process of reinstalling from scratch every single server. Started with infrastructure (DNS and firewalls), then working down to every server with a fresh FTP install from the first recovered box. Yes, newfs everything, and recompiling `_all_` binaries from scratch. I even reconfigured VLANs on the switches to avoid man-in-the-middle attacks like tcp hijacking, while ftp installing, and locked the subnets to these racks until everything's restored.

The only backups were databases in SQL and LDIF format and lots of text data. No binaries and no compromised sources to recover from. Of course, the data could've been hacked too, but that would take more time to fix. I've only checked (and cleaned!) authorization and authentication data so far.

Sometimes, small incidents trigger major reconfigurations. Good that this happened before monday! ;)

Thank you.

--

Re: Monitoring a file?

freebsd-questions: Re: Monitoring a file?

Cordula's Web. <http://www.cordula.ws/>

freebsd-questions@freebsd.org mailing list

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

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