

Re: possible compromise or just misreading logs

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-12/0021.html>

jan.muenther_at_nrns.com

Date: 12/08/03

Date: Mon, 8 Dec 2003 17:48:04 +0100
To: Roger Marquis <marquis@roble.com>

> *Sure, unless you're running an Orange book A level system it's
> impossible to secure anything. But that's a rhetorical argument.*

I guess you misunderstood me here. I wasn't arguing that any system can be broken into – true, but not the point here – but that it's possible to do it without getting noticed, even if you run Tripwire or a similar product.

> *We're talking about filesystems here.*

Well, okay – if we focus on that point alone, Tripwire surely does a good job. I was just opposing the apodictic statement that it's impossible to break into a system without Tripwire triggering an alert. I wasn't saying that it's superfluous to run, just that you shouldn't neglect all other possible and necessary security measures around it.

Again, don't get wrong, I'm not one of the bigots who likes to slag off any security safeguard by saying it can be circumvented. All I was stating is that even when you have all that in place, you should still stick to best practices in every other regard.

> > *Apart from that, there are even tools (LKM based) which spoof MD5 checksums.
> Wouldn't effect tripwire. In addition to MD5 you'd need to spoof
> snefru, crc32, crc16, md4, md2, sha, and haval, and you'd have to
> spoof them for, at a minimum, the tripwire binary and its database
> file(s).*

Guess that depends on the Tripwire version, too... see
<http://www.phrack.com/show.php?p=43&a=14>

Cheers, J.

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"