

Re: Theory Question

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-04/2134.html>

From: John Howie (JHowie@msn.com)

Date: 04/08/01

From: "John Howie" <JHowie@msn.com>
To: "jal" <jal@abulafia.com>, <freebsd-security@freebsd.org>
Date: Sun, 8 Apr 2001 02:30:11 -0700

jal,

You hit the nail on the head. You mitigate the risks you can, and insure against the rest.

john...

----- Original Message -----

From: "jal" <jal@abulafia.com>
To: <freebsd-security@FreeBSD.ORG>
Sent: Sunday, April 08, 2001 12:58 AM
Subject: Re: Theory Question

> *On Sat, Apr 07, 2001 at 04:16:55PM -0700, John Howie wrote:*
> >
> > *[...] If I force would-be*
> > *intruders to have to defeat/circumvent individual measures such as*
> > *firewalls/NAT boxes just to determine my topologies before they can even*
> > *make an attempt at an attack on servers, then most will give up and go*
> *away.*
>
> *Without (dis)agreeing with John or anyone else, I feel like*
> *this is the time to point out that security is a cost, to*
> *be evaluated like any other. At a certain point, the average*
> *business needs to ask itself whether paranoia[1] makes any sense*
> *in spent resources, compared with the measures taken to secure*
> *weaker links, not to mention the cost of losing whatever is being*
> *protected in the first place.*
>
> *So you have the most kick ass network of IDS boxes watching your*
> *heirarchical firewalls, and have deployed the right protocols,*
> *LLE, etc. in all the right places. How's your phone system?*
> *How hard is it to trick someone's assistant, or the Extremely*
> *Important Person themself? What does it mean if that works? If you*
> *reply that that isn't a techincal problem, you don't get security,*
> *which is only ever approaches being half technical in nature.*

FreeBSD–Security: Re: Theory Question

- >
- > *WRT the original problem, my suggestion is to ideally treat the IDS*
- > *as an island, cut the TX pair, assume it can be flooded/compromised,*
- > *and write logs in a way that makes it difficult to alter them without*
- > *being noticed. If the box has to transmit data, you begin making*
- > *different trade–offs involving the network security of your security*
- > *network. Look at those closely, but keep an eye on the value*
- > *of what you're protecting. In general, I'd say that if you have*
- > *legitimate reason to be paranoid enough to build this sort of thing, you*
- > *have legitimate reason to not trust private networks, etc. to hide*
- > *you. Again, policy matters a lot – did some random admin leave a*
- > *laptop connected to the "secure" network when they ran off to fix some*
- > *email problem? If you worry about things on this level, the network*
- > *structure is not your biggest problem.*
- >
- > –j
- >
- > *[1] Intel "only the paranoid survive" Corp. was given a nice*
- > *demonstration of internal security issues by Randall Schwartz.*
- > *Leaving aside your view of what he did, it makes a nice object*
- > *lesson on the limitations of a mostly technical (followed by*
- > *legal, unfortunately) approach to security problems, some of which*
- > *they apparently didn't know they had.*
- >
- >
- > *To Unsubscribe: send mail to majordomo@FreeBSD.org*
- > *with "unsubscribe freebsd–security" in the body of the message*

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