

Re: Changes in IDS Companies?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2002-11/0029.html>

From: Gary Golomb (gee_two@yahoo.com)

Date: 11/13/02

Date: Tue, 12 Nov 2002 18:03:29 -0800 (PST)

From: Gary Golomb <gee_two@yahoo.com>

To: focus-ids@securityfocus.com

For a smart-ass response, see below....

> -----Original Message-----

> From: Dominique Brezinski [<mailto:dom@decru.com>]

> Sent: Tuesday, November 12, 2002 5:29 PM

> To: detmar.liesen@lds.nrw.de; focus-ids@securityfocus.com

> Subject: Re: Changes in IDS Companies?

>

> For a smart-ass response, see below....

>

> ----- Original Message -----

>>From: <detmar.liesen@lds.nrw.de>

>>To: <focus-ids@securityfocus.com>

>>Sent: Monday, November 11, 2002 11:40 PM

>>Subject: AW: Changes in IDS Companies?

>

>

> <snip>

> >I don't have enough practical experience to tell if the following idea is

> good,

> >but I suggest using a GIDS as a protecting device with just the most

> important

> >signatures that are knownt to reliably detect/block those attacks we fear

> most:

> >-worms

> >-trojans/backdoors

> >-well-known exploits

>

> I hate to state the obvious, but if we know enough about these threats to

> write a signature to detect them, then we know enough to re-configure our

> systems to be immune to them. Having a GIDS protect against such things

> just leads to a false sense of security.

>

> >Additionally, NIPS vendors should always maintain a list of those most

> common

> >and most dangerous attacks that also gives information about known

Re: Changes in IDS Companies?

SecurityFocus IDS: Re: Changes in IDS Companies?

- > *>false-positives for these signatures.*
- >
- > *Yeah, so we can patch or re-configure or systems to be immune to*
- > *vulnerabilities and not use their products ;>*
- >
- > *On a good day signature-based NIDS cost organizations money to run for no*
- > *actionable return....On a bad day they leave the organization feeling*
- > *secure*
- > *when they are not.*
- >

I hate to state the obvious, but patching and reconfiguring every system at the whim the worm/exploit/vulnerability d'jour in a multi-thousand node environment is not really THAT easy. Heck, I'd challenge the idea that it's even possible in the first place. In fact, let's not kid ourselves; this is not just a problem for multi-thousand node environments...

So on a good day, signature-based (or methodology-"X" based) IDSs give us the visibility into activity that we really don't have a better way to identify – that is, things that are not "good," "bad," "true," or "false"... It's visibility into things that are "suspicious."

Should that make anyone feel "secure?" I don't think so. I think "aware" is a better choice of words, but this isn't a discussion about semantics... It's the whole point of IDS that people seem to be forgetting, or like me just getting confused as hell by all the propaganda from the marketing machines of the security industry. The point of IDS is not to replace firewalls or integrate/morph into "application based proxy router 5 speed blenders." They sit out-of-band and just watch all the network activity they can, and in doing so you are afforded a luxury that no other security technology can provide (ie: the ones that actually "secure" you network). They give you the flexibility to say "this *might* not be legitimate activity. If it is, that's ok because we're out-of-band and simply triggering an alert is not going to break anything. If it isn't, well, here is more information for dealing with the event." It's a passive tool used for automated log parsing and auditing existing protective security mechanisms because when you're out-of-band like that, you're allowed to take liberties those other in-line methods cannot – nothing more.

Can you integrate methodologies born from ID research into other products? Of course, which if I was paying attention correctly were the early points of this thread.

And are fully patched and perfectly configured networks a better solution? Sure. I think you were privy to situations recently where fully patched and up-to-date "secure" systems weren't immune to being remotely compromised because – specifically – of the "secure" encryption services running on them. Of course, in this case having a [signature-based (or methodology-"X" based)] IDS that could alert you to a "no job control" error on the wire in presumably encrypted traffic would have been decent. At least, it worked in the cases I saw, but it could just be perspective. IDS is what you make of it.

Do you Yahoo!?

U2 on LAUNCH – Exclusive greatest hits videos

<http://launch.yahoo.com/u2>

• *Previous message:* [Kohlenberg, Toby: "RE: Changes in IDS Companies?"](#)

SecurityFocus IDS: Re: Changes in IDS Companies?

- *Maybe in reply to:* Andrew Plato: "Re: Changes in IDS Companies?"
- *Next in thread:* Dominique Brezinski: "Re: Changes in IDS Companies?"
- *Next in thread:* Proxy Administrator: "Re: Re: Changes in IDS Companies?"
- *Maybe reply:* Proxy Administrator: "Re: Re: Changes in IDS Companies?"
- *Maybe reply:* Proxy Administrator: "Re: Re: Changes in IDS Companies?"
- *Reply:* Dominique Brezinski: "Re: Changes in IDS Companies?"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]