

Re: [fw-wiz] RE: IDS (was: FW appliance comparison)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-01/msg00157.html>

- *From:* "Marcus J. Ranum" <mjr@xxxxxxxxxx>
 - *Date:* Wed, 25 Jan 2006 23:06:18 -0500
-

Brian Loe wrote:

>Where I work, I'm not sure how we could do it. We're a transactions
>company, and do thousands and thousands (and more at times) a second.

Would you like to think about that for maybe a second?? Logging an event is, what, thousands of times less CPU and I/O intensive than executing a transaction?? So how can you say that you're not sure how to do something that's *_easier_* than what you are already doing??

>Debugging from ONE of our firewalls puts us into the gigabyte-per-hour
>realm.

Let's see – how exciting is that? 1024 megs in 3600 seconds is.. whoah!!! Holy moly – not very impressive, really. My *_ipod_* can move data faster than that; have you considered using one of those? 24 gigs per day? With compression, you might fit as much as a month's worth of logs on a \$750 LaCie "bigger disk" firewire drive. Logs compress really well, which further reduces your I/O requirements.

Sure, it's not something you'd want to handle with lightweight tools or slow interpreted programming languages, but you are not talking about spine-crushing data rates.

> I tried turning up a syslogging system here once... it died
>three hours later. Maybe I wasn't using the greatest hardware,
>database and reporting software – but where do you find that sort of
>thing?

Syslog definitely has problems with high rates of input. See: <http://lists.jammed.com/loganalysis/2002/01/0054.html> but it's mostly due to UDP output queue overruns.

It's not a hardware problem... But – wait – you said "database"? Please tell me you weren't trying to stick that much data into a SQL database with indexes on your tables and an interpreted query/optimizer engine on top of all that? If so, I'm not surprised

Re: [fw-wiz] RE: IDS (was: FW appliance comparison)

it didn't work --- but that's not a "logging is hard" problem that is a "using a relational database for a write-heavy application is the wrong tool" problem.

> With that much data, and 98% of it being useless, you kind have
>to ask yourself, "what's the point?"

I don't ask myself that. Because I don't agree that 98% of it is useless. It's probably closer to 99.99999% of it is useless. Except for the one or two lines that you might someday really, really need.

> IF we catch something it'll
>probably still be too late - our IDS will have already been updated
>with the new "something".

That's the problem, then. You're assuming that your IDS is going to know how to detect some site-specific hack that only works against you. That's what the logging is for. It's for figuring out what happened after it's too late. Sometimes being able to determine if the customer database got out because of a SQL injection attack through log examination can be quite useful if management is otherwise convinced the problem is an insider.. I once spent a few happy weeks poring through 40 gigs of transaction log data (yeah, 3 days' worth...) trying to identify traces of a hithertofore unknown DOS attack. At stake were a bunch of sysadmins' jobs. It was a very intellectually stimulating mission.

> I don't want to have to go to my manager and
>say, "well, we spent 250k on a machine that would log every
>transaction - no, sorry, PACKET

Well, see, what you'd normally do is actually think about the problem a little bit - not just jump into it half-assed. Most of the commercial logging tools are aimed at attempting to "do everything" but you pay a lot for that - if you actually know what you want to do, you can do it for not a whole lot.

> - we ever passed and we still got
>hacked because we didn't hire a new engineer to review the data
>streaming out of the system and therefore see the new exploit in time
>to shut it down.

If you are stupid about how you deploy technology, you will usually get stupid results. Try explaining that to your boss. No - wait - don't.

mjr.

Re: [fw-wiz] RE: IDS (was: FW appliance comparison)

Re: [fw-wiz] RE: IDS (was: FW appliance comparison)

firewall-wizards mailing list

firewall-wizards@xxxxxxxxxxxxxxxxxxxxxx

<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

• **References:**

- ◆ **Re: [fw-wiz] RE: IDS (was: FW appliance comparison)**
◇ From: Marcus J. Ranum
- ◆ **Re: [fw-wiz] RE: IDS (was: FW appliance comparison)**
◇ From: Paul D. Robertson
- ◆ **Re: [fw-wiz] RE: IDS (was: FW appliance comparison)**
◇ From: Brian Loe

- Prev by Date: **Re: [fw-wiz] FW appliance comparison – Seeking input for the forum**
- Next by Date: **Re: [fw-wiz] FW appliance comparison – Seeking input for the forum**
- Previous by thread: **Re: [fw-wiz] RE: IDS (was: FW appliance comparison)**
- Next by thread: **Re: [fw-wiz] RE: IDS (was: FW appliance comparison)**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**