

Re: Firewall log analysis

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-06/0775.html>

From: David Qunt (davidqunt_at_hotmail.com)

Date: 06/16/04

Date: Wed, 16 Jun 2004 20:03:50 GMT

Lars M. Hansen <badnews@hansenonline.net> squirted these wordjisms deep inside the bumtube of the newstwat in news:7j31d01cc3njjqj3j084bsbrltm8rm9fda@4ax.com:

> *On Wed, 16 Jun 2004 18:23:25 GMT, David Qunt spoketh*
>
>>
>>*Encouraging me?*
>>
>>*Hmmmm, your first response to the OP was*
>>
>>*"I doubt such a program exists. "*
>>
>
> *And I still think you'll have a hard time finding a program that'll*
> *take the Sonicwall logs (syslog or otherwise), look up who the ISP is*
> *(accurately), find the abuse e-mail address and list it all nicely.*
> *However, half the context is missing there, because the next few lines*
> *says what a number of firewall log analyzers do, and it's not what the*
> *OP describes.*
>
>>

What you fail to understand is that I won't have a hard time finding it, because I am not the one looking. The OP was.

>>*Did you google to check that first? After my post pointing out one did*
>>*exist for ZoneAlam, Duane responded by highlighting kiwisyslog.com for*
>>*several brands of FW and routers.*
>>
>
> *Oddly, so did I in the second paragraph.*

After making a pointless snipe at me.

>
>>
>>*However, instead of responding as Duane did when he replied to my*

>>post, you simply sniped this at me:
>>
>>"ZoneAlarm is a toy for desktops, Sonicwall is a professional grade
>>network firewall. Hardly a comparison..."
>>
>>Encouragement was not what you were doing there, Lars, despite what
>>you now claim. What you did there was cricically lecture me for not
>>much more than passing comment.
>>
>
> Yeah, it was a snide remark. You made the same statement twice with
> regards to what is available for a desktop security package which has
> little relevance to original question, despite it being stated already
> by myself and others that the OPs list of requirements for the
> software was probably unrealistic.

Yes, but that was because I didn't fully appreciate the nature of Sonicwall. I have already admitted that I posted within the limitations of my knowledge in an attempt to be as helpful as I could. My knowledge may not be all it should be, just as it is obvious that there is room for improvement in your bedside manner. I was trying to be constructive, and your motivation as far as your continuing attitude towards me is something different entirely.

>
>>
>>Your suggestion of googling may be valid to a certain extent. But if
>>you take that to its logical conclusion, any time someone asks a
>>question online, or tries to answer one or help out, he or she will be
>>pointed at google and told to piss off and look there. But never mind.
>>
>
> I've never suggested "google or piss off", nor do I recall having seen
> anyone else taking the "google is your friend" to any such extremes.
>

Read back the part of my post which you quoted, and you'll see that I didn't quote you as saying that at all. Note the important words, 'if you take that to its logical conclusion' It should be fairly obvious that what I meant is that if everybody did what you did, you would simply have lots of people all pointing other people towards google.

>>
>>In any event, I would point out that what you said applies equally to
>>the OP. And you, for that matter. I would suggest that your advice for
>>me to google might be better directed at the OP. He is, after all, the
>>one with the Sonicwall firewall, and the log he wants to interpret,
>>and the other things he wants to do with it. He is therefore the one
>>who was looking for help, which is why I am slightly puzzled why you
>>had a go at me.
>>

>>*I am merely a passer-by, lurking in here for any useful information,
>>and chipping in occasionally. I will probably be doing that less
>>frequently in future, despite your sudden change from lecturing to to
>>encouragement, if this kind of exchange is the usual result.*
>>
>>*If it's any consolation to you, there is no need to encourage me
>>towards google. When I am looking for an answer myself, I usually
>>consult google as my first port of all. That is probably why you will
>>not find many posts from me asking questions which have already been
>>answered elsewhere. I don't use google to research everything I am
>>about to post, and I suspect you don't either, as it is simply not
>>practical.*
>>
>>*I still stand by my post insofar as it was intended to be
>>constructive, unlike yours – even if what I said was not technically
>>correct, it led immediately to Duane pointing out a possible
>>alternative that may do what the OP requires. Which is more than you
>>did, preferring to say instead that you doubt such a program exists.*
>>
>
> *My posts regarding this subject have been constructive, with the
> exception of this pissing contest with you because you were offended
> by me calling ZoneAlarm a toy...*

Show me where I asaid I was offended at your comments towards ZoneAlarm. I never said I was bothered about that, and I don't particularly care what you say about that product at all. I'm not here to defend ZoneAlarm in the face of your clearly expressed opinion about its merits or otherwise. I've been quite clear that I am 'puzzled' – not offended – by your attitude in sniping at me, instead of concentrating on helping the OP.

You do like to presume rather a lot. You were the one starting a pissing contest, when you made a comparison between ZoneAlarm and Sonicwall – something that I did not do, and yet you accused me of.

>
>>
>>*Still, I shall apologise for my utterly miserable failure to be 100%
>>sure of my facts all of the time when discussing matters online,
>>especially since it's a characteristic shared by about 100% of people
>>at least some of the time. I shall think twice about trying to help
>>from now on, so that I can avoid stealing 3k of your bandwidth and
>>ruining your utopian ideal of how you would like this newsgroup to be
>>run if it were yours to control.*
>>
>>*Best regards*
>
> *whatever.*

You just can't help yourself with the rudeness and snipes, can you? Feel free if it makes you feel any better about your behaviour.

```
--  
*****  
> David Qunt  
>  
*****
```