

## Re: logfiles

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2004-07/0301.html>

---

**From:** Jeff Cochran ([jeff.nospam\\_at\\_zina.com](mailto:jeff.nospam_at_zina.com))

**Date:** 07/10/04

Date: Sat, 10 Jul 2004 20:59:31 GMT

On Sat, 10 Jul 2004 10:46:22 -0700, "Joel Eusebio" <[joele@telus.net](mailto:joele@telus.net)> wrote:

>Thanks.....but if auditing was not enabled it's really hard to look for  
>evidence.

Yep. In the event logs at least. But your firewall log should trap everything. Um, assuming you enabled that as well.

Pretty much, if you're not logging anything and aren't configured to track access, then you aren't going to be able to track access very well.

Jeff

>"Jeff Cochran" <[jeff.nospam@zina.com](mailto:jeff.nospam@zina.com)> wrote in message

>news:41017733.147550626@msnews.microsoft.com...

>> On Fri, 09 Jul 2004 17:01:27 -0700, Joel Eusebio <[joele@telus.net](mailto:joele@telus.net)>

>> wrote:

>>

>> >I am investigating a possible compromise on one of our Windows 2003

>> >servers. Where do I start looking for evidence of a file that was

>> >downloaded to the box?. My suspicion was a trojan was downloaded to the

>> >box and opened up backdoor ports. Thanks.

>>

>> FTP logs, IIS logs, Firewall logs, security log in Event Viewer if you

>> enabled auditing on the particular events before they happened, etc.

>>

>> Jeff

>