

Re: Possible hack?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-01/2406.html

From: Bigbruva (*Richardh_at_dontusetthis.ws*)

Date: 01/29/05

Date: Fri, 28 Jan 2005 16:07:46 -0800

Okay so this log was not deleted, it looks more like the Event log service has been stopped (which an Admin can do)

If this service is not running no event logs will be generated so nothing needs to be deleted. The problem you have is that you have given this user full admin rights so you will find it very difficult to track him.

I am not sure what you think he has "hacked" but turning off the event log service does not constitute "hacking"

If this person has stolen data find it and use that as proof, if they have installed some kind of rootkit or illegal software on the machine you may have a case but without these things you will have trouble proving anything.

You could try simply making this person aware that you have detected unusual behavior on their computer and have to reformat and rebuild the system (to remove any possible rootkit programs), this time, not giving them admin rights (for their own security).

I don't know if this helps (let us know if it does) but other than this it sounds like you might have an HR situation to deal with which no one on this newsgroup is going to be able to help you with.

Good luck

BB

"John" <John@discussions.microsoft.com> wrote in message news:41C370E1-A3A5-44B3-A2CC-7383BC5D7F35@microsoft.com...
> *HMMM...*
> *This is an XP Pro box-log file created 5/24/03 and shows events thru*
> *5/14/04. It then jumps to 1/25/05 with NO reference to deletion by admin.*
> *The*
> *properties of the file show it was created on 5/24/03 and both modified*
> *and*
> *accessed show the same date of 1/21/05. The event log reads as follows:*
>

microsoft.public.windowsxp.security_admin: Re: Possible hack?

> *Information 1/25/2005 12:16:40PM Eventlog None*
> *6009 N/A*
> *Information 5/14/2004 7:08:49PM Application Popup None*
> *26 N/A*
>
>
> *This is what caught my eye--the jump in dates--We suspect he deleted the*
> *entries for this timeframe to cover up some things. We are 99.99% sure he*
> *changed the admin password and did what he wanted between the dates*
> *missing,*
> *but the other log files are either missing entirely or similar dates are*
> *missing from the log files.*
>
> *Logging is ok for the way we want to track it and its not an issue of*
> *being*
> *overwritten.*
>
> *Any ideas?*
> *Thanks!!*
>
>
>
> *"Bigbruva" wrote:*
>
>> *If an administrator deletes the event log entries the first entry in the*
>> *new*
>> *log will tell you that the Administrator has deleted the logs.*
>> *If you can find this entry, you have the date and time this was done. If*
>> *no*
>> *genuine admin did this your have grounds for concern.*
>>
>> *However depending on the setup of your logging, the system can over write*
>> *its own log files if the required logging time has been exceeded or if*
>> *the*
>> *log files have reached a certain size (as defined in the local policy for*
>> *that system).*
>>
>> *Check the settings for the event log on this system and see if that is*
>> *the*
>> *cause before you take it any further down the hacking road. If you need*
>> *more*
>> *help we will need to know what the system is your are talking about*
>> *Windows*
>> *2000, Windows Server 2003, or what?*
>>
>> *Hope that helps*
>>
>> **BB**
>>
>> *"John" <John@discussions.microsoft.com> wrote in message*
>> *news:3FA22975-ECB0-4A01-905D-1B3EDEE6909F@microsoft.com...*

Re: Possible hack?

microsoft.public.windowsxp.security_admin: Re: Possible hack?

>> > *We have a computer on a domain that the system event log is showing
>> > some
>> > wierd entries. It skips about 8 months of logging. When you right click
>> > system log under event viewer and select properties it shows the
>> > correct
>> > creation date, but the modified and accessed dates are both the same—a
>> > week
>> > ago. This is troubeling since the log shows events from the modified
>> > date
>> > up
>> > through today. There is just the 8 months of data missing. There is
>> > concern
>> > this system has been hacked by an employee known to do this type of
>> > stuff.
>> > Management needs proof it was hacked in order to do anything to this
>> > individual. We feel he did this to cover his track on some other stuff,
>> > since
>> > a bunch of older logs are missing data or are gone altogether. Any
>> > ideas?
>> >
>>
>>
>>
>>*