

microsoft.public.win2000.security: Re: tracking what programs are launched?

Re: tracking what programs are launched?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-10/0492.html>

From: Steven L Umbach (n9rou_at_n0-spam-for-me-comcast.net)

Date: 10/13/04

Date: Wed, 13 Oct 2004 17:33:56 GMT

OK! Good luck on your exams. Since you are pursuing security elective I also highly recommend that you buy [and read] the Windows Security Resource Kit. Note that you may be able to but it used on Amazon for a very reasonable price [\$10 or so]. I have had good luck buying used books from Amazon's used book vendors that are available from the page where you find a book. Often the books are in like new condition with a minor bent corner on the front cover or such and can not be sold as new. --- Steve

<http://www.amazon.com/exec/obidos/ASIN/0735618682/qid%3D1030669239/sr%3D11-1/ref%3Dsr%5F11%5F104>
http://www.amazon.com/gp/product/offer-listing/0735618682/ref=dp_pb_a//104-7266434-6041566?condition=all
--- same book, used vendors.

"djc" <noone@nowhere.com> wrote in message
news:%231OXxNUeEHA.820@TK2MSFTNGP12.phx.gbl...

> *oh ya! I should have thought of that considering I am currently preparing
> for the Security elective test as part of the MCSA 2000: Security Cert!
> Shame on me.*

>

> *Thanks Steve.*

> *-djc*

>

> *"Steven L Umbach" <n9rou@n0-spam-for-me-comcast.net> wrote in message
> news:QLcbd.251005\$313.77955@attbi_s03...*

>> *You can enable auditing of object access on a computer and then audit an
>> executable for the execute permission. Of course that will not work for
> user*

>> *installed executables. Another built in method would be to enable*

>> *auditing*

>> *of process tracking. Yeah there will be a lot to sift through but the*

>> *info*

>> *will probably be there. Try it out on a test computer to see if it does*

> *what*

>> *you want. The problem with process tracking is that is can not be enabled*

> *on*

>> *a user/group basis. EventComb is free from Microsoft and can help a lot*

>> *in*

>> *searching multiple computers for specific events and text strings. ---*

>> *Steve*

Re: tracking what programs are launched?

microsoft.public.win2000.security: Re: tracking what programs are launched?

>>
>>
>> "djc" <noone@nowhere.com> wrote in message
>> news:eYMeqHSsEHA.3200@TK2MSFTNGP14.phx.gbl...
>> >I need to be able to see 'who' is running certian programs and when...
> lets
>> > say Solitaire for example.
>> >
>> > Now I know of course if Solitaire should not be run it just shouldn't
>> > be
>> > on
>> > the machine... so, moving past that, what options do I have to log when
>> > the
>> > program is run?
>> >
>> > I am hoping to find a simple, already there, kind of solution... like
>> > turning on some kind of logging which I can just search through with a
>> > batch
>> > or script file as opposed to some full blown 'monitoring' software
>> > suite
>> > that would need to be installed on the target machines. The least
>> > amount
>> > of
>> > effort is the goal since I will in fact just be removing these
>> > programs.
>> > But
>> > I have been asked to find out the whos and whens first.
>> >
>> > note:
>> > – I know there are several ways to prevent programs from being run such
> as
>> > using a GPO to create an Allow list of programs. Right now, the object
> is
>> > not to prevent it but to so who is running it and when.
>> >
>> > any info would be greatly appreciated.
>> >
>> >
>>
>>
>
>