

## Re: tracking admin commands

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-10/msg00189.html>

---

- *From:* "M. Burnett [MVP]" <[mb@xxxxxxxx](mailto:mb@xxxxxxxx)>
  - *Date:* Wed, 25 Oct 2006 15:50:26 +0000
- 

You can audit all executables and know when someone runs them, but you wouldn't know the actual parameters used on the command line.

But yeah, Roger is right, there's not much more you can do other than install a keylogger or a good host monitoring application.

As a side note about the effects of commands, I do have several tightly-controlled servers where I need to know EVERYTHING that happens on them. I have a log parser script that e-mails me a report every 24 hours. That report includes all new logins, all executables run, all Windows firewall events that involve new opened ports, a list of all objects that were accessed (excluding a few high activity dirs), Windows Defender events, all failed audits, and a few other misc events. It also lists any errors or warnings that appear in the event logs (filtering out some non-important events that often show up).

The reports are shorter than you'd think and it just take a moment to scan for irregularities. It is highly unlikely that anything would happen on those servers without me knowing. This is a good example of monitoring the effects of commands. I don't know exactly what someone did at first, but it alerts me that something has happened.

This is particularly effective for monitoring outside attacks because no matter what methods they use, their targets will always be the same.

Mark Burnett

"Roger Abell [MVP]" <[mvpNoSpam@xxxxxxxx](mailto:mvpNoSpam@xxxxxxxx)> wrote in message [news:#ih9sVE#GHA.4472@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:#ih9sVE#GHA.4472@xxxxxxxxxxxxxxxxxxxxxxxx):

"Rodo" <[ralvarado@xxxxxxxxxxxx](mailto:ralvarado@xxxxxxxxxxxx)> wrote in message [news:ezbPRiD%23GHA.4404@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ezbPRiD%23GHA.4404@xxxxxxxxxxxxxxxxxxxxxxxx)

>A trace of commands. From what you said in your previous post, I assume

Re: tracking admin commands

>results of command would show through auditing objects.  
>

"results" only indirectly

For example, as admin if I issue

xcacls c:\temp /e /g users:f

the results are changes in NTFS permissions on c:\temp  
and that acted-on object would have to be audited to see  
the results.

I am aware of no way, short of putting keyloggers on all  
admin usable workstations/servers, that you can get an  
record of all commands issues by admins (not to mention  
that some UI tools do not really issue commands underneath  
whereas others do).

> "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message  
> [news:OyxyOO\\$9GHA.4708@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OyxyOO$9GHA.4708@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

>> So you want to have a trace of the commands, or of the  
>> effects resulting from the commands ?

>>

>> "Rodo" <ralvarado@xxxxxxxxxxx> wrote in message

>> [news:OYCJ8S49GHA.3392@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OYCJ8S49GHA.3392@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Windows server hardening

>>> Are system administrator commands traceable back to an individual  
user

>>> ID?

>>>

>>>

>>

>>

>

>