

Re: windows services question

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-12/msg00466.htm>

- *From:* "Larry Smith" <no_spam@xxxxxxxxxxxx>
 - *Date:* Mon, 18 Dec 2006 21:10:19 -0500
-

Well, they would be unable to kill a service process from the Task Manager, because services run under the LocalSystem account, so that other users cannot open a handle with "terminate" access to it. Task Manager does not seem to do anything in order to assign itself the token of a system account even if it runs under the account with Admin rights, so that users would be unable to terminate a process via it.

You can terminate a service as an administrator or anyone else for that matter. You simply need the "SeDebugPrivilege" in your token which only administrators have by default (system account is also an administrator BTW). The trick is to enable it first since most privileges are disabled by default even for administrators. This is the reason why administrators can't terminate a service from the task manager normally. The privilege exists in their token but they simply have to enable it first (which is very simple to do in code).