

# Re: security problems

---

*Source:*

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2007-03/msg00014.html>

---

- *From:* Jim Howes <[sewoh.mij@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:sewoh.mij@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 01 Mar 2007 11:26:04 +0000
- 

Marc wrote:

Hi,

I have installed a windows 2000 server sp4 with all updates, it's a member server.

I can't copy files to eg c:\windows\system32; but can create new files ?!

I can't stop some services eg McAfee services.

I tried this as the local administrator and the domain administrator

Can someone help me ?

You can get access to the system as SYSTEM, which has more clout than a normal administrator (For instance, SYSTEM can look in C:\System Volume Information, although I have no idea why you might want to do anything in there)

Perhaps that will allow you fix things, providing you can do so from the command line:

How to become NT AUTHORITY\SYSTEM:

1. Start a command prompt as any local administrator
2. Look at the clock, assume for instance, it is 12:34
3. Type

at 12:35 /interactive cmd.exe

(i.e. at 'one minute from now' You may want to make that two minutes if the clock ticks over to 12:35 while you are typing slowly)

4. Wait; you can close the original command window if you like.

At 12:35, a command prompt will open, this is running as SYSTEM, and not as a potentially crippled local administrator.

5. Type carefully.

You probably want to look at the 'cacls' command, and perhaps install subinacl

## Re: security problems

from the resource kit.

You are probably looking at a situation where the GUID for the 'Administrators' group has changed, or bad permissions on some directories.

'compmgmt.msc' is what you get if you right-click on 'My computer' and select 'manage'. Running from the system command line may get you into places that you currently can't get to.

However, the stuff you want to run depends on exactly what the problem actually is, but being logged in as the local system account can help you see what is really there.

.