

Forum:[Hack Forums](#)

Thread: [Access Deny with Admin Account](#)

Jdutchman121 - August 18, 2018, 11:37 am

can anyone help

got a rdp getting this even when i try running exe from cmd with RUN AS ADMINISTRATOR

OS: Windows Server 2008

Language: Chinese

ps: lmk if im in wrong section

f1re_w1re - August 18, 2018, 9:39 pm

It's very difficult to understand your English..

When you RDP to a computer, you need to make sure that you are allowed remote access. So you need to check the remote device and see what you have going on. Also, when you RDP, are you part of a domain or are you just using your local account?

CyberStrike - August 18, 2018, 10:26 pm

Have you checked that you are in fact in the administrators group on that account (local)? if he is part of local admin group he should still be able to run administrative functions on that machine, not others within the domain. If you are a regular user time to privesc, going from user to a more privileged user either Administrator or SYSTEM then if so desired go for domain or enterprise admin. Something else what security measures are in play? IIRC there are GPO's to prevent regular users from installing software.

Jdutchman121 - August 19, 2018, 3:32 am

issue is fixed file was being detected by Windows Defender

I N C R E D I B L E - August 19, 2018, 3:44 am

(Aug 19, 2018 03:32 AM)Jdutchman121 Wrote: [\[CITE\]](#) issue is fixed file was being detected by Windows Defender

That was indeed a foresing workaround. because if you're already running administrator account. that's highly unlikely.

good to see the issue resolved though. ?

Terry A. Davis - August 21, 2018, 2:09 am

(Aug 18, 2018 10:26 PM)SilentWatch Wrote: [\[CITE\]](#) Have you checked that you are in fact in the administrators group on that account (local)? if he is part of local admin group he should still be able to run administrative functions on that machine, not others within the domain. If you are a regular user time to privesc, going from user to a more privileged user either Administrator or SYSTEM then if so desired go for domain or enterprise admin. Something else what security measures are in play? IIRC there are GPO's to prevent regular users from installing software.

It's not usually Group Policy that handles it, that's normal ACL permissions.

Chrome for example lets you install even if you're not an Admin, just say no to the UAC prompt and it plops itself in %AppData% (Roaming AppData).

You can specify in GP what stuff is allowed to run, but as for installing usually that should be left up

to simple Windows rules. Non-Admins can't install to Program Files.

CyberStrike - August 22, 2018, 10:02 pm

(Aug 21, 2018 02:09 AM)Endless Night Wrote: [\[CITE\]](#) It's not usually Group Policy that handles it, that's normal ACL permissions.

Chrome for example lets you install even if you're not an Admin, just say no to the UAC prompt and it plops itself in %AppData% (Roaming AppData).

You can specify in GP what stuff is allowed to run, but as for installing usually that should be left up to simple Windows rules. Non-Admins can't install to Program Files.

I was referring to the following:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc783635\(v=ws.10\)#enabling-users-to-install-applications-and-features-on-demand](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc783635(v=ws.10)#enabling-users-to-install-applications-and-features-on-demand)

(I have seen this employed in a few corporate networks)