

Re: Network Cable Disconnection and Elevated Access

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-09/msg00119.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Wed, 6 Sep 2006 07:52:19 -0700
-

Well, you appear to have a number of issues . . .

First, if they are logging on as only plain users then they should not have been allowed changes to SysVol content or permissions. You may want to look at <http://support.microsoft.com/kb/812538> but notice that this is about share level permissions only, that is, the NTFS level permissions should have controlled more tightly.

Next, if all is in health then group policy should be applying even if the network is disconnected during the login. Are you perhaps doing your main control in a login script that however is not being executed during the disconnected login??

There is a group policy setting that can be used to prevent login using asynchronous group policy application, or you could set the number of cached logins to zero.

Those however assume that they are logging in with a domain account. Since you asked in your question 1 about as who/what they have authenticated, I guess it is not safe to assume that they are using domain login (although if not they really would not need to disconnect the machine from the network).

As to your question 1 directly . . .

We have no way of knowing as what account they have logged in. There is no "fall back" or "default" account. They logged in as who they indicated at the login prompting. Look in your event logs.

As for your 2 and 3, if you are willing to have the environment become unusable if the network is down or domain control cannot be contacted otherwise, then consider use of the policy/policies "Always wait for the network at computer startup and logon" in computer\adm templates\system\logon or, if it is only an issue with control not happening due to logon scripts not executing (sound likely in your scenario) "Run logon scripts synchronously" in computer\adm templates\system\scripts or, perhaps better, in user\adm templates\system\scripts and / or

Re: Network Cable Disconnection and Elevated Access

"number of previous logons to cache" set to 0 in
computer\windows\security\local\sec options

"Lokiarmos" <2198234981234810834@Localhost> wrote in message
news:4F0D4037-3FBA-4D22-899F-6FFB7BD52E9A@xxxxxxxxxxxxxxxx

We have discovered in my workplace (A School) that they students are unplugging the network cables as the students log on, this prevents the GP from been applied.

This then allows them the browse the network, although they can only see visable shares which are not many but what did surprise me was that they could get access to the sysvol and where able not only to write to it but change permissions.

This in turned stuffed up sysvol and forced me to do a authorative restore on it.

Now the questions i have are

1. Whom or to what level are they been authenticated as
2. How can i prevent them from logging on if the GPOs are not applied.
3. And how do i do it in the way that won't affect the other users (teachers) who use the machine.