

Re: BYPASS privilege !!

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2007-06/msg00947.html>

- *From:* BaxterD@xxxxxxxxxxx
 - *Date:* Mon, 11 Jun 2007 17:05:49 -0700
-

First of all, I would like to say that this discussion came about during a meeting on SOX requirements, which morphed into a discussion about how it would be possible to "trick" our application if the villain had certain knowledge, programming skills and system privileges. We managed to come up with a surprising number of ways to work mischief, that would be difficult to detect immediately, and possibly even more difficult to figure out.

Thanks to you all for your responses, and I want to start by saying that we agree with all of you. Whether BYPASS is freely given to the SYSTEM account or not, there is really no way of stopping a malicious admin from reeking havoc with your system, should he choose to.

We were looking at it more from the point of auditability (?). A fundamental requirement of SOX is that there should be a clear demarkation between OS Admins and App Admins, and while it is usually relatively simple to restrict App Admins access to the OS, it is much less simple to stop a Sys Admin from messing with the App (again, should he choose to). In particular, it is usually the Sys Admin who sets up all of the security on your Application Data Files and Executables/Scripts, and as such he/they have all the power to work under/over/around/through the same security.

To repeat what I said in para 1, it must be accepted that at some level, it is impossible to stop a malicious admin from doing whatever they have in mind to do.

This being the case, then there are really only three objectives which we can aim for;

1. Lock down your executables, scripts and data as securely as possible.
however if someone still manages to cause malicious damage, then;
2. be able to determine, after the fact, exactly what was done to your App, or Data, and be able to recover from it.
and,
3. To be able to determine, again after the fact, exactly who did it.

Re: BYPASS privilege !!

As far as SOX is concerned, they are primarily interested in objective #2. However objective #3 is still important if you want to avoid it happening again.

Recovery after damage can be done (in our case) using the capabilities of RMS journaling, however the ability to achieve objective #3 depends on how you implement Objective #1.

Obviously, Identifiers and ACL's provide a way to lock down the files and directories which make up the application, and the UAF provides the means to control the app users.

Equally obvious, to a user with BYPASS privilege, it matters not how well you lock down the security on your app, since BYPASS by definition, will bypass all system security. Once the app is properly secured, then the only way for a non-application, privileged username to access the application directories or files is either to grant themselves the necessary identifiers, or use BYPASS to bulldoze their way in. Both of these actions, (and most other discrete attempts) can be recorded in the Security Audit Journal.

However, If there happen to be multiple Administrators, all using the SYSTEM account for their admin duties. How do you determine who did what?

I know this sounds fairly paranoid, and for people running 2- and 3-tier apps, this all sounds a bit weird, but we are just running through (a few of the endless number of) options.

1. Give each admin a personalized admin account with no BYPASS (and maybe other privs also)
2. Lock down the SYSTEM account for use only when carrying out Maint, Upgrades or Patching.
3. Enable auditing of Privilege use and UAF modification.

Final comment, I could present an endless number of scenarios which represent risk, and for each one, someone would come up with a solution. However the solution always comes after the solution. We are not asking for solutions, we are merely asking if anyone knows the answers to the two simple questions,

1. Does anyone know of any function, particularly during system startup, which "absolutely" requires BYPASS" privilege.
2. Does anyone know of any Admin function which "absolutely" requires the SYSTEM account.

thanks.

Dave.

Re: BYPASS privilege !!

Re: BYPASS privilege !!

On Jun 11, 5:00 pm, "Richard B. Gilbert" <rgilber...@xxxxxxxxxxxx>
wrote:

JF Mezei wrote:

In the end, isn't it still true that for a functional system, you still
need to trust at least one system manager who could still wreak havok on
your system if he truly wanted to ?

Or can a system truly be locked down to a point where the system manager
cannot do his job without supervision from the security folks ?

Yes, it can! It may take me days to remember exactly what it's called
but there is a secondary password that can be required to log in to an
account; IOW two passwords, only one of which is known to the system
manager. I've never known a site that actually used this feature but
it's there!

Re: BYPASS privilege !!