

Re: More on user permissions in a 2K AD domain

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-11/0877.html

From: Eric H. Vela (*nocontact_at_here.com*)

Date: 11/15/04

Date: Mon, 15 Nov 2004 13:41:43 -0600

TS in admin mode is what I was referring to. I'm not sure I particularly like the idea. But it WOULD make certain aspects of management easier since the target server is offsite.

The target DC and Domain are in a situation of being only one server in the domain serving as DC, User, File, DNS and SQL servers. I know this is not the recommended set up, but my hands are tied on that front so I am setting up a test situation identical to that and wish to lock down the server tighter than Ft. Knox with the intention of applying the same to the server/domain in production. Though I'm out in the middle of nowhere, it seems this area is a target for server hacking --- either that or the average sys admin isn't knowledgeable enough to protect their systems around these parts. The current state of the target domain is poor on the security scale and I intend to fix that as best as I can. Access to knowledgeable personnel locally is limited so I'm pretty much on my own on this one.

As always, the weakest link in the target domain is the users. My hands are also tied on the local access of the workstations, but I can set the server to any privilege I desire. Still formerly, the sys admin had used the primary Domain Admin (was still named Administrator) for all administration things on the workstations, and I'm aware that Windows 2K caches login information locally on the workstations, and this information may be hacked giving information about how to attack the server more easily with higher access. However, if the Domain Admin logins never happen on the workstation, the cached information is not created. Right? So my aim is to keep as much information about the domain and its admins off of the workstations as possible. The situation may arise where one of the above mentioned, unrestricted, workstation users will want to add another computer to the domain themselves. (Again, not my recommendation, but my hands are tied.)

So essentially, it's a bad situation that I'm trying to make the best of. I want to protect the server as best as possible if (or rather, when) a workstation gets hacked. It is the heart of their entire operation.

Eric

microsoft.public.win2000.active_directory: Re: More on user permissions in a 2K AD domain

"Lanwench [MVP – Exchange]"

<lanwench@heybuddy.donotsendme.unsolicitedmail.atyahoo.com> wrote in message news:uB059UzyEHA.1564@TK2MSFTNGP09.phx.gbl...

> Eric H. Vela wrote:

>> *First, I would like to thank Gautam Anand, Oli Restorick, and Marco for their feedback that has led to the following hypothesis.*

>>

>> *Before I go off and attempt this and end up in a wild goose chase, is it possible to create a user that has no login privileges, no resource*

>> *access and whatnot but can add computers to a domain? What I am*

>> *wanting is to keep the Domain Admins off of any workstation. I made*

>> *the realization that the computer only needs to be able to join a*

>> *domain and then a *local* RunAs Admin privilege combined with normal*

>> *Domain User permissions is all that is needed from then on for the*

>> *remainder of the setup.*

>>

>> *... or am I WAY off base?*

>

> *Actually, I may be a little confused as to what you're trying to do, but*

> *users themselves by default can join up to 10 computers to the domain.*

> *What's your desired end goal here? You can delegate pretty much anything*

> *you*

> *want to an account, but I'm not sure what you're trying to do.*

>

>>

>> *And while I'm here, what are your feelings about Terminal Services*

>> *running on the DC? I'm thinking of not using TS on the DC at all and*

>> *have only local console access. (You might have guess by now that I'm*

>> *one of those "abstinence is the only sure protection" kind of people.)*

>

> *TS in admin mode is fine – if you mean in application mode, no, don't do*

> *it.*

>

>>

>> *Thanks again in advance.*

>> *Eric*

>> *(cross-posted in: microsoft.public.win2000.active_directory and*

>> *microsoft.public.win2000.security due to relevancy.)*

>

>