

Re: domain admin account impersonating

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-11/msg00067.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Tue, 7 Nov 2006 21:33:28 -0700
-

No problem Pedro. Glad things may have become more clear. I have seen people intentionally isolate some things from their "more carefully protected" corporate domain, doing this isolating by making those other things set up on stand-alone workstations. OK, so far, that can be a valid approach for protecting the jewels. But, then in order to make backup, or administration, or monitoring, etc. more convenient they define matching accounts (same name and password) that span the stand-alones and the corp domain, with admin access in them all. That pretty near totally defeats any gain that could happen from having separated those things out from the domain in the first place. Oh well . . .

Roger

"Pedro Leite" <aa> wrote in message
news:ulH4G0oAHHA.4328@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

hi

thank you for your input. your reply was ver enlightning on this matter. what i have learnt is that the domain account should be unique in a network environment, domain oriented or not. period. of course that a domain is much more than user authentication. i kinda exxxagerated by saying breaking, but the point was that on a machine out of the domain, i was acting as domain admin. tiny little issue that in my opinion, but just shouldn't happen but as a ms workstation and server user, i must beleive that it happens for a reason and a good one. if i'm not happy with it, file a report at microsoft and if the management at my company simply see this as a major security issue (which i don't), well, there are other options.

i gueses that the bottom line is that the domain admin account can be impersonated, with the same username and password. a somewhat esoteric

Re: domain admin account impersonating

scenario but that's just it.

i appreciate your info on the security settings on ie (actually we are on firefox) but thank you the same.
thank you once again.

PLeite

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> escreveu na mensagem
news:%23VJaPYnAHHA.5060@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Yes, I do believe it is "by design".

Starting with Windows XP this became less simple, whereby the accessing XP system will be seen to send, not "username" and its password response which the accessed system will, in absence of a qualified domain\username take as "username" as defined on it (the accessed system), but instead the accessing XP will be seen to send XPhost.domain.tld\username (qualified with the DNS domain of the XP) which of course will fail. One then sees XPhost.domain.tld\username in a prompt asking for password and thinks it tries this instead of sending just "username", but this one with the DNS domain is done as a retry action as is shown as it was the last attempted.

There is no test as to what groups the account is member in before attempting behind the scenes authentication.

I do not see how it breaks the domain concept. I mean, if someone knows the username and password for an account in the domain so that they can do this then they really do not need to do this.

You may want to pay attention to the IE Options setting under Advanced in Security section that enables Windows Integrated Authentication and also to the ability by XP and later Windows to cache Windows network credentials (i.e. start/run keymgr.dll).

Roger

"Pedro Leite" <aa> wrote in message
news:OzmcYPIAHHA.4496@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

good morning

thank you for the information.
so, can we say that is " by design " ?? it happens because it does. (

not

Re: domain admin account impersonating

flaming, just trying to make things clear)
does this happens only on admin accounts ? can i create an
user on the

off

domain pc and logo to the shares with the user's domain
password ??
this
kind of breaks the concept of windows domains doesn't it ??

apart from the obvious of having the domain admin account "
on the
loose
",
are there any other security issues that i should be on the
lookout for

??

and before someone says it, i fully agree that having the local
admin

user

equal to the domain admin is a cumbersome error. a
malpractice that i

must

correct.

thank you
PLeite

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> escreveu
na mensagem
news:%23cqF1faAHHA.4592@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Windows has done this for a very long time.
If you have two accounts, in separate
authentication realms, and those
accounts have the same name and password,
then while using one of
them it is possible to access resources in the
other realm by means of
the other account. This happens
"transparently" with a login behind
the scenes when an access attempt is made.
It is not a matter of the
accounts having the same SID (which they

Re: domain admin account impersonating

do not) but that one can
log in as the other by presenting its own
credentials since they
match.

"Pedro Leite" <aa> wrote in message
news:%23eBIMYaAHHA.4592@xx

good afternoon

can anyone explain this
behaviour ?? as described
setup is sbs 2k3

recently added a new pc to
the network and to the
domain for updates
and
application deployment.
so, i named the pc admin
account the same as the
domain admin
account

and

gave it the same password.
now, the new pc is off the
domain but the admin
account is still the

same

with the same domain
admin password.

whenever i log to the pc
with the admin account, i
have full control

over

the domain machines, c\$
share, all users document
folders, all

shares,

direct internet acces through
the firewall...

Re: domain admin account impersonating

Re: domain admin account impersonating

questions, is the domain
admin sid the same as a
local admin sid's

account

?? the authentication being
made with a blend of
username and

password,

all
mixed up, hashed whatever
and then sent to validation
??

isn't the domain admin
account user equal to
domainname\admin and
the
local
admin, machinename\admin
??

for my knowledge please
comment on the above

thank you

Pedro Leite

Re: domain admin account impersonating