

Re: Security Question

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-11/msg01913.html>

- *From:* "Gregg Hill" <bogus@xxxxxxxxxxxxx>
 - *Date:* Fri, 10 Nov 2006 19:07:10 -0800
-

This may not apply, but are there any ex-employees who knew the name? Or perhaps an owner who bragged to a friend that no one could hack him?

Gregg Hill

"cjobs" <cjobs@xxxxxxxxxxxxx> wrote in message
[news:ej\\$JS\\$PBHHA.3560@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:ejJSPBHHA.3560@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

kj,

Thanks for the additional comments. This client Trend SCM running. It's very unlikely that there is software on one of the user stations that would do that. This has come from the outside. They also haven't gotten in because the password is quite complex. But given that this was the first time I came across this I was curious how they got the username in the first place.

--

Claus

"kj" <kj@xxxxxxxxxxxxx> wrote in message
<news:%23msZdRPBHHA.204@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

A simple ldap query will return the administrator account, but in Windows 2003 AD "anonymous" ldap queries aren't allowed. However, a logged in user with no other special privileges can easily determine the name of the Administrator account. While a typical user isn't going to know how to do this (or care probably), spyware/malware or such could easily do this under the user credentials. As Les said this "obscurity" measure isn't a significant security layer for a determined intruder.

That said, I'm not aware of any spyware that has been found to do this, but it is certainly possible.

--

/kj

"Les Connor [SBS Community Member - SBS MVP]"

Re: Security Question

<les.connor@xxxxxxxxxxxx>
wrote in message
news:%23hIktUOBHHA.3928@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

SMTP tar pit feature for Microsoft Windows Server 2003

<http://support.microsoft.com/kb/842851>

Getting a valid email address is one thing; the planets would have to be aligned with the stars for someone to get a valid username from an AD harvest, but if the email address is <name>@domain.com and the user account is <name>, then it's a no brainer.

I see quite a few installs like this – I don't really like it but it's because of defaults. Customizing user account and email address generation is an obscurity measure, not effective against a black hat but keeps the dabblers moving on.

--
Les Connor [SBS Community Member – SBS MVP]

SBS Rocks !

"Tell me and I'll forget. Show me and I'll remember. Involve me and I'll understand." – Confucius

"cjobs" <cjobs@xxxxxxxxxxxx> wrote in message
news:uEgA%23KJBHHA.1196@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Les,

Can you elaborate a bit more on this?

--
Claus
"Les Connor [SBS Community Member – SBS MVP]" <les.connor@xxxxxxxxxxxx>
wrote in message
news:eMtbFTIBHHA.1220@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

From an AD harvest? If AD filter is on, this is one of the caveats –

Re: Security Question

hence the use of tarpitting
for mitigation.

--

Les Connor [SBS
Community Member – SBS
MVP]

SBS Rocks !

"Tell me and I'll forget.
Show me and I'll remember.
Involve me and
I'll understand." – Confucius

"cjobs"
<cjobs@xxxxxxxxxxxxxx>
wrote in message
news:%23I2IDv0AHHA.144@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi all,

A first for
me, so I
would like
to get some
feedback
from other
admins.

As a
standard,
we always
change the
Administrator
account
name to
something
else. For the
first time
we had a
breakin
attempt at
one of
our clients
(SBS2003/ISA2004)
that was
using the
correct
renamed

Re: Security Question

admin
account
name. Now,
the
password is
pretty
complex but
I still
don't like
the fact that
50% of the
safeguard is
out there.
Does
anybody
have an idea
how an
outside
hacker
would be
able to
obtain
that
username?

--

Claus