

Re: Hack Attempt on Windows 2003 AD Native

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-11/1637.html

From: Andrei Ungureanu (*andreix.nospam_at_msn.com*)

Date: 11/25/04

Date: Thu, 25 Nov 2004 23:33:29 +0200

Have you tried to implement an account lockout policy? I think it will help you in this case. Be very careful if you want to disable the Administrator account as this account has a special property; you can log on with him from a domain controller even if the account is locked out. If you create another admin account and somebody else will find it, he can pretty easy lock it out.

Get a firewall quickly ... and get rid of the public ip address from the DC. If you are using the DC for some sort of NAT server ... then change it with a XP workstation (until you'll get a firewall)... it's better than exposing your AD to public internet.

HTH

--

Andrei Ungureanu

www.eventid.net

Free Windows event logs reports

<http://www.altairtech.ca/evlog/>

"Ryan Hanisco" <rhansico@flagshipis.com> wrote in message

news:u2TRX3l0EHA.1392@TK2MSFTNGP14.phx.gbl...

> Herb,

>

> You can disable the Administrator account through the ADU&C in Server 2003

> just as you would a normal account. In my opinion, this should be done as

> part of the standard build on any server or domain -- just make sure you

> have a surrogate with all permissions before you disable it.

>

> You can also use the following article to get back into your Administrator

> account once it has been disabled:

> <http://support.microsoft.com/default.aspx?scid=kb;en-us;814777>

>

>

> --

> Ryan Hanisco

> MCSE, MCDBA

> Flagship Integration Services

>

>

>

> "Herb Martin" <news@LearnQuick.com> wrote in message

> news:uSdTHS10EHA.2976@TK2MSFTNGP12.phx.gbl...

>> "Ryan Hanisco" <rhansico@flagshipis.com> wrote in message

Re: Hack Attempt on Windows 2003 AD Native

microsoft.public.windows.server.active_directory: Re: Hack Attempt on Windows 2003 AD Native

```
>> news:#tF0#2k0EHA.1152@TK2MSFTNGP14.phx.gbl...
>> > JJ,
>> >
>> > Instead of renaming the Administrator account, you may consider
>> > creating
>> > other Admin accounts and disabling the Administrator account. This
>> > will
>>
>> How do you disable the built-in Administrator account?
>>
>>
>
>
```