

## Re: Security Breach in AD! Help!

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-02/0237.html>

---

**From:** Roger Abell [MVP] (*mvpNoSpam\_at\_asu.edu*)

**Date:** 02/09/05

Date: Tue, 8 Feb 2005 22:12:52 -0700

see reply in your new thread . . .  
it is computer policy

--

Roger

"Todd" <Todd@discussions.microsoft.com> wrote in message  
news:A03DD4A7-7D54-498E-B15E-0751895BD7DE@microsoft.com...

>I have a question regarding Restricted Groups...

>

> I am trying to make the changes that I've set for Restricted Groups to be  
> as

> close to real time as possible. We had another user created today and in  
> about 5 minutes the user was removed from the built in admin group. I  
> have

> changed the default domain policy, the default domain controller policy,  
> and

> the local machine policy all to reflect the following changes trying to  
> make

> this a real time restriction:

> I have enabled the... refresh interval for computers to 0, refresh  
> interval

> for domain controllers to 0 for the computer policies

> as well as the refresh interval for users to 0 for the user policies.

> I obviously do not know what I am doing since I don't know what Group  
> policy

> to apply and on what interface to get my desired results.

>

> Please help!

>

> thanks

>

> Todd

>

>

> "Steven L Umbach" wrote:

>

>> For the domain check the membership of the administrators group, the  
>> domain

>> admins, and enterprise admins groups. Make sure it is what it is supposed  
>> to

>> be and if there are any non default groups as members of these groups

>> evaluate why they are there and check their memberships. Reset the

>> passwords

>> on every user account [ including yours and your bosses] in any of those  
>> groups. Make sure you are using hard to guess passwords. Also enable

>> auditing of account logon for success and failure and account management

## microsoft.public.win2000.security: Re: Security Breach in AD! Help!

```
>> for
>> success and failure in Domain Controller Security Policy. Auditing of
>> account management will tell you if group membership has been changed [by
>> normal means] and by who. You can also look and see when any user has
>> logged
>> onto the domain and from what computer. Be sure to increase the size of
>> your
>> security logs quite a bit to sat at least 10mb. You can use the filter
>> view
>> in Event Viewer or Event Comb to narrow searches.
>>
>> Check all of your GPO's at the domain and domain controller level to see
>> if
>> "restricted groups" is configured in a way that could cause such a
>> problem
>> and also check for any GPO that can apply to domain controllers and Local
>> Security Policy of each for any startup scripts that may be used to add
>> accounts to admins/domain admins admins group. Gpresult /v on the domain
>> controllers can help you do such. Also check Scheduled Tasks and the AT
>> command on each domain controller for anything unusual. If you are using
>> a
>> domain account that is in the administrators/domain admins group for any
>> service authentication in the domain, that accounts passwords is easily
>> recovered from any domain computer using that account, so check out that
>> as
>> a possibility.
>>
>> Your domain controller must be physically secured to some degree or
>> someone
>> could obtain passwords from them. If nothing else a sturdy locking case
>> that
>> blocks access to the drives must be used. Configure the cmos of your
>> domain
>> controllers to boot only from the system drive and password protect the
>> cmos
>> settings. Also disable USB on the domain controllers in cmos if not
>> needed.
>> Another possibility is that your passwords are being captured by keyboard
>> loggers installed on computers that you use. These can be hardware
>> plugged
>> into the back of the computer keyboard port or in the keyboard cable, or
>> installed as software. Some programs such as Pest Patrol do a pretty good
>> job of checking for software keyboard loggers. The Microsoft Spyware
>> program
>> will check for many also. Be VERY careful on what computers you use
>> domain
>> admin credentials on. Spy cameras are another way to try and capture user
>> credentials. Note that telnet connections may be in clear text and ftp
>> connections will be in clear text so be careful when you use admin
>> credentials.
>>
>> I would also examine the domain controllers very carefully and do full
>> malware scans with at least two different products. Trend Micro has the
>> free
>> Sysclean package which I would use also along with it's matching pattern
>> file. Use the free tools from SysInternals - TCPView, Autoruns, and
>> Process
>> Explorer to examine port usage and process usage on your domain
>> controllers.
>> Be extremely suspicious of any remote control software, processes that
>> map
>> to an executable that does not have a publisher name associated with it,
```

## microsoft.public.win2000.security: Re: Security Breach in AD! Help!

```
>> and
>> any process that is not related to anything that should be running on the
>> domain controller [which can be hard to do if you do not have a known
>> clean
>> like install to compare to]. Check for root kits by using Plist from
>> SysInternals to compare the processes running locally to those when you
>> check processes running from a remote computer. Also run the Microsoft
>> Baseline Security Analyzer on your domain controllers to check for basic
>> vulnerabilities including unneeded services and missing critical updates.
>> That should give you a start. The links below should help. --- Steve
>>
>> http://www.sysinternals.com/ntw2k/freeware/procexp.shtml -- Link to
>> SysInternals Process Explorer and other utilities.
>> http://www.trendmicro.com/download/dcs.asp
>> http://www.trendmicro.com/download/pattern.asp
>> http://www.microsoft.com/technet/security/tools/mbsahome.mspx
>> http://www.microsoft.com/athome/security/spyware/software/default.mspx
>> http://www.microsoft.com/technet/security/bestprac/bpent/sec3/monito.mspx
>>
>> "Todd" <Todd@discussions.microsoft.com> wrote in message
>> news:10C4CF0D-C6FB-4678-AFBC-D8DBDEB97003@microsoft.com...
>> > Hello, my name is Todd and I am an MCP (almost an MCSA-2003) working
>> > for a
>> > Computer Consulting business. One of our clients (our biggest one) has
>> > AD
>> > running and we have had a heck of a time figuring out this problem:
>> > The only 2 people with administrative permissions on the entire
>> > domain
>> > is
>> > my boss (owner of company) and myself. However, we keep finding new
>> > users
>> > that are being created and are being assigned to the built in
>> > administrators
>> > group, giving them admin permissions. There appears to be no way to
>> > stop
>> > them. We have changed our Administrator account psw (although I don't
>> > think
>> > this would have helped anyway as the accounts that are being created
>> > have
>> > admin rights...they don't need our account). We have removed all
>> > spyware
>> > /
>> > adware and have run virus scans galore (although we periodically still
>> > have
>> > to remove them from the system...even in the past couple of weeks).
>> > The
>> > only
>> > ports open are those we are using...it seems to be a secure environment
>> > with
>> > the exception of the ghost administrator running around. We have tried
>> > deleting the accounts from the default admin group and have disabled
>> > the
>> > accounts. They either reappear after being deleted in a few days or
>> > when
>> > we
>> > disable the accounts they return with different names like "1" "2"
>> > "skip0"
>> > and "dick".
>> >
>> > Has anyone ever heard of a similar problem or hack that we could look
>> > for
>> > that would allow someone without admin rights (or by using a system
```

