

Re: User Rights Assignment – not available – Resolved

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-02/msg00936.html

- *From:* "Tim Munro" <Excelsior@xxxxxxxxxxxx>
 - *Date:* Mon, 27 Feb 2006 13:21:54 -0500
-

I made a statement that "Clearly I had been hacked". Now I'm not so sure. I'm wondering if this could have been a vestage of a failed SID change on my computer.

--
Tim

"Tim Munro" <Excelsior@xxxxxxxxxxxx> wrote in message <news:utvyRy7OGHA.3460@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I used the DumpSec tool Steve pointed me to and obtained an error from it:

```
rc=3221225524 LsaEnumerateAccountsWithUserRight
```

Translating this to Hex I got C0000034. Googling this I found article: <http://support.microsoft.com/default.aspx?scid=kb:en-us:199071> . Although all my "secrets" were Ok, I poked around for a bit. I went into the "Accounts" key, and noted some SIDs I could not explain. Armed with the base sids of our domains, and my local machine, I removed all sid entries I could not resolve. Low and behold my "User Rights Assignment" came back. No reboot nothin'. Clearly I had been hacked.

Situation resolved for now. I have since done a full sweep of my machine and all looks well.

Thanks Steve for your effort to help me here. Pointing me to DumpSec lead me down the right path.

--
Tim

"Tim Munro" <Excelsior@xxxxxxxxxxxx> wrote in message <news:%23knYXN6OGHA.1832@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

OK Thanks Steve, I'll see what I come up with.

Re: User Rights Assignment – not available – Resolved

Tim

"Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

news:vomdnYRpK7rvOpzZRVn-vw@xxxxxxxxxxxxxx

Hmm. I have never seen that happen. A couple things you could try. Go to the \windows\system32\config folder and rename the security file to something else. Then copy the security file from the \windows\repair folder. You can not do that however in normal operating system state but might be able to do it while booted into Recovery Console.

<http://support.microsoft.com/?kbid=307654> --- XP Recovery Console.

Another thing to try is to run the Security Configuration and Analysis mmc snapin and analyze and then configure with the setup security.inf security template to see if that helps or not. Beyond that if it was me I would try to restore a backup of the System State [if you have any] or you could try a system restore to an earlier point which is what to try first. If none of that works I would try an upgrade/repair install before resorting to a pristine install. An upgrade/repair install however will require that you first install your service pack [if not slipstreamed into install media] and then all critical updates at Windows Updates. Another possibility is to live with it the way it is. You could try using the free utility dumpsec from Somarsoft to see if it shows user rights and use the Resource Kit command line tool NTrights to change user rights when needed. --- Steve

http://www.microsoft.com/windowsxp/using/helpandsupport/getstarted/ballew_03may19.mspx

--- XP System Restore

<http://www.somarsoft.com/> ---- Dumpsec

<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ntbackup>

--- System State backup

"Tim Munro" <Excelsior@xxxxxxxxxxxx> wrote in message

Re: User Rights Assignment – not available – Resolved

news:eOK0p0uOGHA.3924@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

No go.

Here's the top of the log file created:

Sunday, February 26, 2006 10:47:44

----Configuration engine was initialized
successfully.-----

----Reading Configuration Template info...
Event audit settings are turned off.

----Configure User Rights...

Warning 2: The system cannot find the file
specified. <---- what file?

Error enumerating info for Accounts from
LSA. <----- this bothers
me.

Configure S-1-5-20.

Configure S-1-5-19.

Configure S-1-5-32-551.

Configure S-1-5-32-544.

Configure S-1-1-0.

Configure S-1-5-32-545.

Configure S-1-5-32-547.

Configure

S-1-5-21-1060284298-329068152-839522115-501.

Configure S-1-5-32-555.

User Rights configuration was completed
successfully.

"Steven L Umbach"

<n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:KuOdnOwyzqHHFJ3ZRVn-vg@xxxxxxxxxxxxxx

Weird. There are free tools
from SysInternals called
filemon and
regmon that if you start
them just before you try to
run something and
then stop them from logging
when the action fails you
may find helpful
information in the log for
access denied entries that

Re: User Rights Assignment – not available – Resolved

would indicate something you do not have necessary permissions for. I use them quite a bit and find it is helpful to add access denied to filter view to highlight as there could be thousands of entries in the log. The link below is to regmon and filemon.

<http://www.sysinternals.com/Utilities/Filemon.html>
<http://www.sysinternals.com/Utilities/Regmon.html>

Another thing you could try is to use the secdit command to try and restore security settings to default defined levels which may help per the link below. You can simply copy and paste the command to run as it is. --- Steve

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:313222>

"Tim Munro"
<Excelsior@xxxxxxxxxxxx>
wrote in message
<news:OPXQhEiOGHA.2064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I went through both the integrity check and did a repair anyway. Result is the same. I'm guessing here that this may be a permissions problem. Everything

Re: User Rights Assignment – not available – Resolved

else on the
"Local
Policy"
mmc is
accessible
and
changeable.
It's just the
"User
Rights
Assignment"
that is bad.

When I
went to
rebuild
(copying
and
renaming as
the article
suggests) I
did get the
access
denied.
Unfortunately
"Import
Template"
was greyed
out when I
used the
filename
secedit.sdb.
Any
other name
and it was
fine.

Is there
somewhere
in the
registry I
can check
for
permissions
that might
be causing
this
behaviour?

Thanks

--

Re: User Rights Assignment – not available – Resolved

Tim

"Steven L
Umbach"

<n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in
message

news:8OidnU6airjcPGLenZ2dnUVZ_vudnZ2d@xxxxxxxxxxxxxxxxxx

Hmm.
It
sounds
like
you
may
have
a
corrupt
secedit.sdb
file.
See
the
link
below
for
two
possibilities
of
which
one
is
to
attempt
a
repair
with
esentutl
and
the
other
is
a
rebuild.

Steve

<http://support.microsoft.com/?kbid=894351>

To
resolve
this

Re: User Rights Assignment – not available – Resolved

issue,
first
run
the
Esentutl.exe
tool
to
examine
the
integrity
of
the
Secedit.sdb
database.
To
do
this,
follow
these
steps:
1.
Click
Start,
click
Run,
type
cmd,
and
then
click
OK.
2.
At
the
command
prompt,
type
the
following
command,
and
then
press
ENTER:
esentutl
/g
Drive:\WinDir\security\database\secedit.sdb
Note
In
this
command,

Re: User Rights Assignment – not available – Resolved

Drive
is
the
hard
disk
drive
where
Windows
XP
Professional
is
installed,
and
WinDir
is
the
folder
where
Windows
XP
Professional
is
installed.
After
the
Esentutl.exe
tool
finishes,
use
one
of
the
following
methods
to
resolve
the
issue,
depending
on
the
message
that
the
Esentutl.exe
tool
returns:
.
If
the
Esentutl.exe

tool
returns
the
following
message,
use
Method
1
to
resolve
the
issue:
This
operation
may
find
that
this
database
is
corrupt
.
If
the
Esentutl.exe
tool
returns
information
that
is
similar
to
the
following
message,
use
Method
2
to
resolve
the
issue:

Microsoft(R)
Windows(R)
Database
Utilities
Version
5.2
Copyright
(C)

Re: User Rights Assignment – not available – Resolved

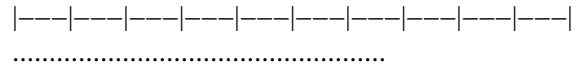
Microsoft
Corporation.
All
Rights
Reserved.

Initiating
INTEGRITY
mode...
Database:
L:\WINDOWS\security\database\secedit.sdb
Temp.
Database:
TEMPINTEG2680.EDB

Checking
database
integrity.

Scanning
Status
(%
complete)

0
10
20
30
40
50
60
70
80
90
100



Integrity
check
successful.

Operation
completed
successfully
in
0.841
seconds.
Note
When
you
run

the
Esentutl.exe
tool,
your
computer
is
returned
to
the
original
installation
state
where
the
Local
Security
Policy
is
not
defined.
You
may
have
to
start
your
computer
in
Safe
Mode
to
rename
files
or
to
move
files.
To
start
your
computer
in
Safe
Mode,
press
the
F8
key
while
Windows
XP

Re: User Rights Assignment – not available – Resolved

Professional
is
starting,
type
1
to
choose
Safe
Mode
from
the
startup
options,
and
then
press
ENTER.

"Tim
Munro"
<Excelsior@xxxxxxxxxxxx>
wrote
in
message
news:uOKPnsWOGHA.2124@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello
all,

On
my
local
PC
(Windows
XP
SP2),
in
"Local
Security
Settings>Local
Policies>User
Rights
Assignments"
I
get
"Windows
cannot
read
template
information".
Any

Re: User Rights Assignment – not available – Resolved

idea
what
happened
and/or
how
to
get
this
back?

--
Tim.