

Re: Is it really true that NTFS is secure?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-12/9148.html>

From: George Hester (hesterloli@hotmail.com)

Date: 12/14/02

From: "George Hester" <hesterloli@hotmail.com>

Date: Sat, 14 Dec 2002 13:22:44 -0500

Thanks Karl. New update.

I had done logon Success\Failure. All my Successes were Administrator caused. It WAS the Administrator account that was being used to reenable the Users Guest account and it was the Administrator account that was putting the Administrator account in the Group Guest account.

Now I have fixed this damn issue and I don't believe it has anything to do with a malicious machine from outside doing this. There is something wrong with Windows 2000 it looks to me.

This is what I did. I removed the Users Guest account from the Groups Guest account. The Groups Guest account is at this moment empty. I then changed the Users IUSR_MachineName account to be a member of the Groups Users account. I then disabled the Users Guest account.

And that's the end of that story. It seems to me my machine was doing this on its own. I (the Administrator) was NOT enabling the Users Group account. In fact I was disabling it everytime I would find it enabled. And it would go back to enabled about 1 or 2 hours AFTER I had disabled it. And the Administrator account was doing this.

The junk I sent you earlier this always happens. I really don't think it is specifically directed at me. I really do not know why this crap happens but I can assure you it had nothing to do with my complaint in this matter. Looks to me this is a flaw with Windows 2000 Professional then anything else.

Thanks for everyone's suggestions.

--

George Hester

"Karl Levinson [x y] mvp" <jamescagney90210@excite.com> wrote in message news:#5NHilL3oCHA.392@TK2
> Enable failure auditing for everything listed in the auditing section in
> Group Policy, but more importantly I would think you'd enable both success
> and failure auditing starting with "Audit Account Management," and also try
> enabling both success and failure auditing for "privilege use," though you
> might have to remove success auditing on this or other items if this
> generates too many events. Might as well audit success and failure for
> "policy change" as well, just in case.
>
> If you haven't already, look up the trojans found at the web site for the
> software that found them [or www.sarc.com if necessary] to try to find out
> how they work and whether they cause anything like this.
>
>

microsoft.public.security: Re: Is it really true that NTFS is secure?

```
> "George Hester" <hesterloli@hotmail.com> wrote in message
> news:eGc4B4woCHA.1888@TK2MSFTNGP09...
> Update.
>
> The account Group got put back in the Administrator group again. I had
> audits going and here is the time\status in which this occurred:
>
> Event Source: Security
> Event Category: Account Logon
> Event ID: 681
> Date: 12/13/2002
> Time: 5:56:46 PM
> User: NT AUTHORITY\SYSTEM
> Computer: MyMachineName
> Description:
> The logon to account: Administrator
> by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
> from workstation: HAMID-MSLR91LJD
> failed. The error code was: 3221225578
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Logon/Logoff
> Event ID: 529
> Date: 12/13/2002
> Time: 5:56:46 PM
> User: NT AUTHORITY\SYSTEM
> Computer: MyMachineName
> Description:
> Logon Failure:
> Reason: Unknown user name or bad password
> User Name: Administrator
> Domain: HAMID-MSLR91LJD
> Logon Type: 3
> Logon Process: NtLmSsp
> Authentication Package: NTLM
> Workstation Name: HAMID-MSLR91LJD
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Account Logon
> Event ID: 681
> Date: 12/13/2002
> Time: 5:56:46 PM
> User: NT AUTHORITY\SYSTEM
> Computer: MyMachineName
> Description:
> The logon to account: Administrator
> by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
> from workstation: HAMID-MSLR91LJD
> failed. The error code was: 3221225578
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Account Logon
> Event ID: 681
> Date: 12/13/2002
> Time: 7:41:52 PM
> User: NT AUTHORITY\SYSTEM
> Computer: MyMachineName
> Description:
> The logon to account: Administrator
```

microsoft.public.security: Re: Is it really true that NTFS is secure?

```
> by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
> from workstation: SAVVYEM
> failed. The error code was: 3221225578
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Logon/Logoff
> Event ID: 529
> Date: 12/13/2002
> Time: 7:41:52 PM
> User: NT AUTHORITY\SYSTEM
> Computer: MyMachineName
> Description:
> Logon Failure:
> Reason: Unknown user name or bad password
> User Name: Administrator
> Domain: SAVVYEM
> Logon Type: 3
> Logon Process: NtLmSsp
> Authentication Package: NTLM
> Workstation Name: SAVVYEM
>
> This last tried to sign on with user name root, admin, test, administrator
> and then finally gave up. But my Guest User account is still changing to
> enabled and putting itself in the Administrator Group. That action I am not
> seeing in the Event Viewer anywhere. What can I do to catch that event? I
> believe I need the Guest group for IIS as IUSER_MachieName is in there.
> Please be detailed as I looked in Group Policy and cannot seem to find what
> is necessary so I can see when that event occurs and what\who is
> responsible. Thanks
>
> --
> George Hester
>
> _____
> "Karl Levinson [x y] mvp" <levinson\_k@excite.com> wrote in message
> news:#c7LZ5soCHA.2384@TK2MSFTNGP11...
> > You can enable auditing to watch for things like this:
> >
> > http://securityadmin.info/faq.htm#auditing
> >
> > Checking your IIS web logs is another common place to check. Look for
> > anything that mentions .EXE or % and that also has a code 200 or 502 in
> > that
> > line. URLScan is a free IIS tool that comes with IISLockdown from
> > www.microsoft.com/technet/security that will block all this stuff, if
> > that's
> > what this is. Most firewalls won't detect or block this stuff.
> >
> > Be sure you have a firewall, as this will log all traffic to and from your
> > server. The firewall should also block NetBIOS traffic on TCP and UDP
> > ports
> > 135-139 and 445 from the internet, as this is another way people could be
> > accessing your guest account.
> >
> > Intrusion detection such as Black Ice or Snort [free] might be worth a
> > try,
> > though getting Snort to alert just on interesting events on a Windows
> > server
> > takes some knowledge.
> >
> > The free file change checker from www.gfi.com can also help you monitor
> > your
```

microsoft.public.security: Re: Is it really true that NTFS is secure?

> > system for intrusions not caught by antivirus, trojan scanners or
> firewalls.
> >
> > Other things to do to look for the source of the hacking and secure your
> > servers and computers are listed at:
> >
> > <http://securityadmin.info/faq.htm#hacked> [first]
> > <http://securityadmin.info/faq.htm#harden> [second]
> >
> >
> > "George Hester" <hesterloli@hotmail.com> wrote in message
> > news:ufXDRfmoCHA.2424@TK2MSFTNGP12...
> > Please understand that my machine comes up empty handed on all AV scans
> > and
> > trojans. I need to find some way of watching when this Group Policy
> > change
> > happens. Like a log. That tells me the time that it happend or the
> > responsible party. It doesn't show in Event Viewer.
> >
> > You know I ran a server W2K prior to this and never had this issue.
> > Started
> > on Prof full time now and I am battling security it seems every hour.
> >
> > --
> > George Hester
> >
> > "George Hester" <hesterloli@hotmail.com> wrote in message
> > news:OwrkSZmoCHA.2424@TK2MSFTNGP12...
> > Yes you may be able to help me with something. My Guerst user keeps
> > getting
> > enabled and put in the Administrator group. How?
> >
> > --
> > George Hester
> >
> > "Karl Levinson [x y] mvp" <levinson_k@excite.com> wrote in message
> > news:eleuHGkoCHA.1628@TK2MSFTNGP12...
> > > Do you have a problem we could help you with? Are there more details?
> > >
> > > What does this code have to do with NTFS? I'm sorry if your machine was
> > > exploited, though I'm not sure this has to do with NTFS.
> > >
> > > NTFS file permissions are plenty secure against remote exploits. If you
> > > have other security vulnerabilities that permit running commands as an
> > > account that has permissions in the NTFS ACLs, that's not exactly an
> > > NTFS
> > > failing.
> > >
> > > Windows 2000 configured correctly is as secure as most other operating
> > > systems configured correctly. Windows 2000 in the default install is
> > > about
> > > as un-secure as Linux in the default install, especially if you go back
> > > to
> > > Linux from the year 2000. Securing Windows 2000 is about as complex and
> > > time consuming as securing Linux, maybe even easier.
> > >
> > > More information on ways to determine how you were hacked and how to
> > > secure
> > > your computer:
> > >
> > > <http://securityadmin.info/faq.htm#hacked>
> > > <http://securityadmin.info/faq.htm#re-secure>

Re: Is it really true that NTFS is secure?

