

microsoft.public.windowsxp.security\_admin: Re: Our server hacked and tagged. MS doc's suck!

## Re: Our server hacked and tagged. MS doc's suck!

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2003-05/3805.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-05/3805.html)

---

**From:** Mike Brannigan [MSFT] ([mikebran\\_at\\_online.microsoft.com](mailto:mikebran_at_online.microsoft.com))

**Date:** 05/31/03

Date: Sat, 31 May 2003 12:27:24 +0100

Tom,

Have a look at the FSUTIL command and see if the folders you are dealing with are hard linked anywhere.

Try taking ownership of the individual folders.

Ultimately you may be forced to visit the server and bring it up in single either recovery console or repair mode and try it that way.

As regards this all being our fault due to a "vulnerability in our OS", I believe in your original pots you admitted that it was due to someone giving anonymous FTP RW access. This is a security configuration issue and not an OS vulnerability. Remember – leave the front door to you house open and you may just get robbed.

We could never release a tool that would circumvent he built in security protection, you can obviously see the inherent danger in that. In most cases the inbuilt tools are sufficient coupled with the other systems of ownership and the take ownership rights etc.

--

Regards,

Mike

--

Mike Brannigan [Microsoft]

This posting is provided "AS IS" with no warranties, and confers no rights

Please note I cannot respond to e-mailed questions.

Please use these newsgroups

"Tom Valenzuela" <[tomvalenz@sympatico.ca](mailto:tomvalenz@sympatico.ca)> wrote in message news:038e01c32704\$3cdc2a40\$a601280a@phx.gbl...

> Well this helped. I turned off IIS, ensure administrator  
> had the rights and began removing directories, all that  
> remain now that don't delete are the following... As you  
> will see they are not owned by BUILTIN

>

> 04/22/2003 05:09p <DIR> 00TAGG~1 ---

> 00tagged

> 05/11/2003 09:43p <DIR> ^33945~1 ---

> ^ 33945

Re: Our server hacked and tagged. MS doc's suck!

microsoft.public.windowsxp.security\_admin: Re: Our server hacked and tagged. MS doc's suck!

```
>
> Any ideas??? Tried all commands, Access Denied and there
> is no Security tab when you right click the folder...
> unlike the other ones I was able to delete... Interesting
> to say the least.
>
> In the end, Microsoft, you should have a tool to remove
> such things. It's a shame your OS has such vulnerability
> and very little tools to fix them.
>
> Regards,
> Tom
>
>
> Tom
> >-----Original Message-----
> >If you are getting issues with deleting folders even
> though you have
> >permissions then you may be forced to stop any service
> that might be holding
> >a lock on those folders - such as a web or FTP service.
> >
> >
> >--
> >Regards,
> >
> >Mike
> >--
> >Mike Brannigan [Microsoft]
> >
> >This posting is provided "AS IS" with no warranties, and
> confers no
> >rights
> >
> >Please note I cannot respond to e-mailed questions.
> >Please use these newsgroups
> >
> >"Tom Valenzuela" <tomvalenz@sympatico.ca> wrote in
> message
> >news:624301c326ba$4068d310$a301280a@phx.gbl...
> >> Ya we did that and 'permission denied' still, somewhere
> >> down the tree of the folder it experiences a
> >permissions
> >> error..Unfortunately we are unable to go down the tree
> >of
> >> the directory but I will look closer at the permissions
> >> and owner. Right now it's all administrator as far as I
> >> can see and I made sure to use the checkbox to ensure
> >it
> >> goes down to the childnodes and sub directories.
> >>
> >> I will look at it more and see. I was thinking these
> >> directories might have some kind of root somewhere
> >that we
> >> could delete and get rid of them, but as you said, I
> >will
> >> look at it as simply files and folders.
> >>
> >> I wish there was a utility out there that could easily
> >do
> >> this for us and just simply nuke the directory..
> >> unfortunately haven't found any.
```

Re: Our server hacked and tagged. MS doc's suck!

microsoft.public.windowsxp.security\_admin: Re: Our server hacked and tagged. MS doc's suck!

```
> >>
> >> thanks for your help! I will post again if I meet any
> >> problems, hope you can check on here once in a while
> for
> >> next day or so...hehehehehe!
> >>
> >> Tom
> >>
> >>
> >> >-----Original Message-----
> >> >"Tom Valenzuela" <tomvalenz@sympatico.ca> wrote in
> message
> >> >news:61ae01c326b5$edd3e990$a301280a@phx.gbl...
> >> >> ok, questions. Map a drive to root of what?
> >> >
> >> >The Physical disk on the remote server that holds the
> >> offending folders.
> >> >
> >> >Forget about the homepage, FTP or Web side of things -
> >> just deal at the
> >> >simplest level of the disk folders themselves.
> >> >
> >> >Ok - so you have a remote desktop session to the
> server.
> >> The you do not need
> >> >to do any mapping.
> >> >Just logon to the remote desktop as the server
> >> Administrator and then take
> >> >ownership of the folders and then reset the
> permissions
> >> and delete.
> >> >
> >> >--
> >> >Regards,
> >> >
> >> >Mike
> >> >--
> >> >Mike Brannigan [Microsoft]
> >> >
> >> >This posting is provided "AS IS" with no warranties,
> and
> >> confers no
> >> >rights
> >> >
> >> >Please note I cannot respond to e-mailed questions.
> >> >Please use these newsgroups
> >> >
> >> >"Tom Valenzuela" <tomvalenz@sympatico.ca> wrote in
> message
> >> >news:61ae01c326b5$edd3e990$a301280a@phx.gbl...
> >> >> ok, questions. Map a drive to root of what? the
> >> homepage?
> >> >> or to the c:\. i have accessed the folder and
> changed
> >> >> permission and stuff on it all way down the tree
> using
> >> the
> >> >> bullets and stuff but still says permission denied,
> is
> >> >> this because i didn't map a drive? I assume you
> meant to
> >> >> c:\
```

Re: Our server hacked and tagged. MS doc's suck!

microsoft.public.windowsxp.security\_admin: Re: Our server hacked and tagged. MS doc's suck!

```
> >> >>
> >> >> The directory i am trying to delete in the root of
> our
> >> >> homepage is \ \, like that... and in the logs for
> it
> >> this
> >> >> directory is seen created as \++\.. Even after
> changing
> >> >> owner and stuff says permission denied or it craps
> out
> >> >> while trying to change the permission somewhere
> down the
> >> >> hierarchy of this folder.
> >> >>
> >> >> I am doing this via remote desktop...
> >> >>
> >> >> Thanks for your fast response.
> >> >> Tom
> >> >>
> >> >> >-----Original Message-----
> >> >> >Tom,
> >> >> >
> >> >> >This has nothing to do with POSIX commands.
> >> >> >
> >> >> >All you need do is take ownership of the
> folders/files
> >> >> >and then reset the
> >> >> >permissions on them (which you can now do as you
> re the
> >> >> >owner even though
> >> >> >you may not have permissions to begin with).
> >> >> >Give your self Full Control and ensure that they
> are
> >> >> >propagated to all child
> >> >> >files and folders (you will be asked if this is
> what
> >> >> >you
> >> >> >want to do).
> >> >> >Then just delete them.
> >> >> >
> >> >> >You can do this by mapping a drive to the root of
> the
> >> >> >disk volume which by
> >> >> >default exists as the admin share <drive letter>$
> >> >> >e.g. F$
> >> >> >
> >> >> >You should do all of the is under an administrative
> >> >> >account.
> >> >> >
> >> >> >Taking ownership and resetting file permissions are
> >> >> >covered in the online
> >> >> >help for your OS.
> >> >> >
> >> >> >--
> >> >> >Regards,
> >> >> >
> >> >> >Mike
> >> >> >--
> >> >> >Mike Brannigan [Microsoft]
> >> >> >
> >> >> >This posting is provided "AS IS" with no
> warranties,
```

Re: Our server hacked and tagged. MS doc's suck!

microsoft.public.windowsxp.security\_admin: Re: Our server hacked and tagged. MS doc's suck!

```
> >> and
> >> >> confers no
> >> >> >rights
> >> >> >
> >> >> >Please note I cannot respond to e-mailed questions.
> >> >> >Please use these newsgroups
> >> >> >
> >> >> >"Tom" <tomvalenz@sympatico.ca> wrote in message
> >> >> >news:050401c326a6$ce9ae470$a001280a@phx.gbl...
> >> >> >> I got directories someone created after someone
> gave
> >> R/W
> >> >> >> to anonymous FTP, doh. Fixed that issue but i
> have
> >> >> >> directories I can't delete and give me permission
> >> denied
> >> >> >> or an error if I try and access them. I've read
> KB
> >> >> article
> >> >> >> on MS about Posix commands. They don't work.
> Can't
> >> find
> >> >> >> process or returns a 'failed' message. I'm doing
> this
> >> >> all
> >> >> >> via Remote Desktop as server is over 1 hour away.
> >> >> Someone
> >> >> >> else said environment variables have to be set..
> Hmm,
> >> >> gee
> >> >> >> where is that documented as I looked in the Posix
> >> >> >> manual... I'd really appreciate it if someone can
> >> tell
> >> >> me
> >> >> >> how to get rid of these directories. We closed
> our
> >> FTP
> >> >> and
> >> >> >> I have checked user rights/groups and stuff,
> nothing
> >> out
> >> >> >> of the ordinary. But as Administrator you think
> I'd
> >> just
> >> >> >> click on em and delete em...but no.
> >> >> >>
> >> >> >> We are pursuing the hacker in GERMANY. Whoever
> it is,
> >> >> >> trust me, you hacked the wrong site. You're good,
> >> but I
> >> >> >> have 3 layers of logging on.. I got you tracked
> >> biatch!
> >> >> >>
> >> >> >> I'm looking for a utility that can go and delete
> >> these
> >> >> >> directories or someone who really actually knows
> how
> >> to
> >> >> >> use the posix commands to remove the directories.
> >> >> >
> >> >> >
> >> >> >.
```

Re: Our server hacked and tagged. MS doc's suck!

microsoft.public.windowsxp.security\_admin: Re: Our server hacked and tagged. MS doc's suck!

> >> >> >  
> >> >  
> >> >  
> >> >  
> >> >.  
> >> >  
> >  
> >  
> >.  
> >