

Re: Am I hacked?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-08/8807.html>

From: John (john_at_nospam.infovis.co.uk)

Date: 08/27/04

Date: Fri, 27 Aug 2004 03:18:47 +0100

I need to run this server for one more day. There is only one server in the network and the organisation has to get by on the Friday. Any tasks that look suspicious?

Thanks

Regards

"Marina Roos [SBS-MVP]" <marina@roos.nodontwantspam.nl.com> wrote in message news:etxc8k9iEHA.3016@tk2msftngp13.phx.gbl...

> John,

>

> *Disconnect that server from the internet NOW!*

>

> --

> *Regards,*

>

> *Marina*

> *Microsoft SBS-MVP*

>

> *"John" <john@nospam.infovis.co.uk> schreef in bericht*

> *news:eckhch9iEHA.356@tk2msftngp13.phx.gbl...*

>> *Here is the list of tasks running on the server;*

>> *<http://www.infovis.biz/bad%20task.jpg>. While I am preparing to flatten the*

>> *server, anything I can/should get rid of?*

>>

>> *Thanks*

>>

>> *Regards*

>>

>>

>> *"Susan Bradley, CPA aka Ebitz - SBS Rocks [MVP]" <sbradcpa@pacbell.net>*

>> *wrote in message news:uuziaq8iEHA.3564@TK2MSFTNGP10.phx.gbl...*

>>> *You could have a Rootkit installed.*

>>>

>>> *You can't assure yourself that all has been cleaned off*

Re: Am I hacked?

> > >
> > > *Help: I Got Hacked. Now What Do I Do? – Microsoft TechNet: Security*
> > > *Management Column:*
> > > <http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx>
> > >
> > > *So, you didn't patch the system and it got hacked. What to do? Well,*
> > > *let's see:*
> > >
> > > *. You can't clean a compromised system by patching it. Patching only*
> > > *removes the vulnerability. Upon getting into your system, the attacker*
> > > *probably ensured that there were several other ways to get back in.*
> > >
> > > *. You can't clean a compromised system by removing the back doors. You*
> > > *can never guarantee that you found all the back doors the attacker put*
> > > *in. The fact that you can't find any more may only mean you don't know*
> > > *where to look, or that the system is so compromised that what you are*
> > > *seeing is not actually what is there.*
> > >
> > > *. You can't clean a compromised system by using some "vulnerability*
> > > *remover." Let's say you had a system hit by Blaster. A number of*
vendors
> > > *(including Microsoft) published vulnerability removers for Blaster.*
Can
> > > *you trust a system that had Blaster after the tool is run? I wouldn't.*
> > > *If the system was vulnerable to Blaster, it was also vulnerable to a*
> > > *number of other attacks. Can you guarantee that none of those have*
been
> > > *run against it? I didn't think so.*
> > >
> > > *. You can't clean a compromised system by using a virus scanner. To*
tell
> > > *you the truth, a fully compromised system can't be trusted. Even virus*
> > > *scanners must at some level rely on the system to not lie to them. If*
> > > *they ask whether a particular file is present, the attacker may simply*
> > > *have a tool in place that lies about it. Note that if you can*
guarantee
> > > *that the only thing that compromised the system was a particular virus*
> > > *or worm and you know that this virus has no back doors associated with*
> > > *it, and the vulnerability used by the virus was not available*
remotely,
> > > *then a virus scanner can be used to clean the system. For example, the*
> > > *vast majority of e-mail worms rely on a user opening an attachment. In*
> > > *this particular case, it is possible that the only infection on the*
> > > *system is the one that came from the attachment containing the worm.*
> > > *However, if the vulnerability used by the worm was available remotely*
> > > *without user action, then you can't guarantee that the worm was the*
only
> > > *thing that used that vulnerability. It is entirely possible that*
> > > *something else used the same vulnerability. In this case, you can't*
just
> > > *patch the system.*

> > >
> > > . *You can't clean a compromised system by reinstalling the operating
> > > system over the existing installation. Again, the attacker may very
well
> > > have tools in place that tell the installer lies. If that happens, the
> > > installer may not actually remove the compromised files. In addition,
> > > the attacker may also have put back doors in non-operating system
> > > components.*
> > >
> > > . *You can't trust any data copied from a compromised system. Once an
> > > attacker gets into a system, all the data on it may be modified. In
the
> > > best-case scenario, copying data off a compromised system and putting
it
> > > on a clean system will give you potentially untrustworthy data. In the
> > > worst-case scenario, you may actually have copied a back door hidden
in
> > > the data.*
> > >
> > > . *You can't trust the event logs on a compromised system. Upon gaining
> > > full access to a system, it is simple for an attacker to modify the
> > > event logs on that system to cover any tracks. If you rely on the
event
> > > logs to tell you what has been done to your system, you may just be
> > > reading what the attacker wants you to read.*
> > >
> > > . *You may not be able to trust your latest backup. How can you tell
when
> > > the original attack took place? The event logs cannot be trusted to
tell
> > > you. Without that knowledge, your latest backup is useless. It may be
a
> > > backup that includes all the back doors currently on the system.*
> > >
> > > . *The only way to clean a compromised system is to flatten and
rebuild.*
> > > *That's right. If you have a system that has been completely
compromised,
> > > the only thing you can do is to flatten the system (reformat the
system
> > > disk) and rebuild it from scratch (reinstall Windows and your
> > > applications). Alternatively, you could of course work on your resume
> > > instead, but I don't want to see you doing that.*
> > >
> > >
> > > *This list makes patching look not so bad, yes? We may hate patches,
but
> > > the alternative is decidedly worse.*
> > >
> > > *The topic for the next article is still up to debate. If you have
ideas,*

> > > *comments or feedback of any kind, as always you may click the "Contact
> > > Us" link below and tell me.*
> > >
> > >
> > >
> > > *Marina Roos [SBS-MVP] wrote:*
> > > > *Hi John,*
> > > >
> > > > *Forget it. Your data can't be trusted anyway. You first of all close
> > > that*
> > > > *ftp server and close port 20 and 21 inbound right now! You should
have*
> > *done*
> > > > *that already.*
> > > > *You won't be able to find out what has been installed. Start from
> > scratch,*
> > > > *you can't trust that box anymore.*
> > > >
> > >
> > > --
> > > <http://www.sbslinks.com/really.htm>
> > >
> >
> >
>
>