

RE: Hacked Server

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-11/msg03215.html>

- *From:* Colin <Colin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 21 Nov 2007 01:04:03 -0800
-

Hi Geoff,

What do your logs say ? Failed logons is proof that Mr Hacker didn't logon. Also, I doubt any hacker worth his salt would only shut down the server when he could so easily destroy data etc. Have you got a UPS installed and is the sensitivity set to high (I had this same problem – my server shut down every morning at around 0600 because the power fluctuates at that time and the UPS did it's job thinking the power was about to go down). ? The logs should tell you what time the server is shutting down. If it's the same time you could have a similar problem to me or it could be a service that is running and causing the shut down. Is WSUS set to install updates on the server automatically for example ?

Regards Colin.

"Geoff" wrote:

Hello All,

We run a SBS 2003 Box with 2 NIC connected to the net via a fairly std ADSL Router. Two days ago I saw a lot of failed logon attempts in the logs. Yesterday when I came in the server had been shut down.

I renamed the admin account and changed the password, closed all router ports apart from VPN, and RWW ran full scans for viruses trojans etc disabled all remote access permissions for all other accounts.

This morning its happened again? I have to assume that whoever did this the first time left some back door that I did not find so they could do it again.

Can anyone point me in the right direction?

Thanks

Geoff