

## Re: unsuspected shutdown. TCP attack?

**Source:**

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2004-02/2285.html>

---

**From:** Dave (*noone\_at\_nowhere.com*)

**Date:** 02/25/04

Date: Wed, 25 Feb 2004 12:20:32 -0000

ok, if it is your application you should be able to load the program in the original debugging environment and see what is causing that problem. it may be your program has a bug that is bringing down the tcp/ip stack and causing other services to malfunction.

there are various tools to let you monitor the tcp/ip statistics, capture network traffic, and other details of the system operation. netstat and the task manager are the simple built in ones, others are available either free or for mega\$\$\$ depending on the complexity of the problem.

i would start by back tracking and see what you changed before the problem started. if you did that service pack just before the problem started, try undoing it or preferably building a clean system without it and running that for a while, then adding the sp and see if the problem repeats.

"Peter Slam" <pslm@hotmail.com> wrote in message  
news:eVeRGr3%23DHA.3232@TK2MSFTNGP10.phx.gbl...

> *Charlie,*  
>  
> *Thank you very much for your answer.*  
>  
> *I tried 3 diferent computer with 3 diferent network cards.*  
> *Event log is in "Overwrite when necessary" mode, but is not full.*  
> *I will check again drivers and Local policies, but every time, a few*  
> *minutes*  
> *before system shutdown or restart, every connection to comuter fails (RCP,*  
> *my application, ...etc).*  
> *I changed switch, cable, power line and source, computer, network*  
> *card....all!*  
> *The only think that is the same is ... IP address.*  
> *And my aplication reports "Failed to call socket() function. ret*  
> *value:INVALID\_SOCKET" a few minutes before shutdown or restart (this*  
> *application was working fine for 6 months until now).*  
>  
> *There is a debug tool to show buffers or other internal values of TCP/IP*  
> *stack?*  
>

microsoft.public.win2000.networking: Re: unsuspected shutdown. TCP attack?

> Thank you.  
>  
> Pet.  
>  
> "Charles Otstot" <saries@notmyreal.address.com> wrote in message  
> news:uLKhWgw%23DHA.3500@TK2MSFTNGP10.phx.gbl...  
> > Peter,  
> >  
> > Having just stumbled across your thread I'm shooting in the dark, but  
I'll  
> > hit one thing you've probably checked...your NIC drivers.  
> > I'm guessing you have recently installed Windows 2000 Service Pack 4  
(this  
> > would explain all the empty logs...  
> >  
>  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;829246&Product=win2000>).  
> > If your NIC drivers were originally OEM (manufacturer-labeled, for  
> example,  
> > Dell branded drivers for embedded 3COM cards), the Service Pack  
> installation  
> > could have overwritten those drivers with Microsoft native-Windows 2000  
> > drivers. This could account for your noted blue-screen event.  
> >  
> > I'll also hit one thing you may not have checked, in your local security  
> > policy...  
> > Do you have "Shut down system immediately if unable to log security  
> audits"  
> > enabled (this is found in Local policies...Security Options)? If you are  
> > auditing improperly (generating enough events to exceed the max size of  
> your  
> > security log and not allowing those events to be overwritten), your  
> Security  
> > Log could be filling up and shutting down your system. The  
aforementioned  
> > Service Pack 4 installation could be causing this issue...assuming you  
> > installed SP 4, your event logs may (likely are) being corrupted and  
while  
> > appearing empty, one or more are actually full. The corruption could be  
> > preventing entries from being written and the above mentioned security  
> > setting could be shutting you down when you reach an event logging  
> > threshold.  
> >  
> > I realize this may be a bit esoteric, but it sounds like you are looking  
> for  
> > unusual explanations at this point. I will say that I've never heard of  
> > anyone attacking a system in the fashion your describing, so I would  
think  
> > something malicious would still be far down the list of suspects (almost  
> to  
> > the point of only if it is the only answer left).

Re: unsuspected shutdown. TCP attack?

microsoft.public.win2000.networking: Re: unsuspected shutdown. TCP attack?

>>  
>> *Charlie*  
>>  
>>  
>> *"Peter Slam" <pslm@hotmail.com> wrote in message*  
>> *news:ezBCTRt%23DHA.712@tk2msftngp13.phx.gbl...*  
>>> *Marc,*  
>>>  
>>> *System, Application and Security event logs are EMPTY!*  
>>> *In one of the machines tested, one time is see a "bluescreen" with*  
*NDIS*  
>>> *error before restart.*  
>>>  
>>> *There is a patch to make more secure TCP/IP stack? (even if this is*  
>>> *expeerimental or in beta stage, i will try it!)*  
>>>  
>>> *Thanks,*  
>>>  
>>> *Pet.*  
>>>  
>>>  
>>> *"Marc Reynolds [MSFT]" <marcrey@online.microsoft.com> wrote in message*  
>>> *news:edGWEEt%23DHA.2808@TK2MSFTNGP10.phx.gbl...*  
>>>> *It is possible, but only one possiblity. Before you start goijng*  
*down*  
>> *the*  
>>>> *network attack path, check your System, Application and Security*  
*event*  
>>> *logs*  
>>>> *for ANY recent event errors that may give you some type of a clue to*  
>> *what*  
>>>> *may have caused the shutdown.*  
>>>>  
>>>> *--*  
>>>>  
>>>> *Thanks,*  
>>>> *Marc Reynolds*  
>>>> *Microsoft Technical Support*  
>>>>  
>>>> *This posting is provided "AS IS" with no warranties, and confers no*  
>>> *rights.*  
>>>>  
>>>>  
>>>> *"Peter Slam" <pslm@hotmail.com> wrote in message*  
>>>> *news:uPKX#Ir#DHA.4012@tk2msftngp13.phx.gbl...*  
>>>>> *Hi!*  
>>>>>  
>>>>> *My server shut downs unexpected randomly. Evend log only shows*  
*"Last*  
>>>>> *shutdown was unsuspected".*  
>>>>> *I checked everythink, and i changed switch, cable and ...*

Re: unsuspected shutdown. TCP attack?

computer!

> I

>>>> *changed computer 2 times, and network card! I applied registry*

>>>> *recomendations of microsoft to improve TCP security.And the*

problem

>>>> *persist!*

>>>> *Theres is a expert people here (MCP, MVP) without answer for this*

>>>> *question.*

>>>>

>>>> *My computer has a public IP, but is behind a firewall, and only*

with

>>> *open*

>>>> *TCP ports to a custom application. (this application was working*

> *fine*

>>> *for*

>>>> *6*

>>>> *months).*

>>>>

>>>> *The question is this: IS POSSIBLE TO HANG A WIN200 COMPUTER WITH A*

>>>> *MALFORMED*

>>>> *OR SOME KIND OF TCP PACKETS?*

>>>>

>>>> *Thank you in advance!!!!*

>>>>

>>>> *Pet.*

>>>> *to msoft people: if you think that this can be a bug of tcp/ip*

> *stack,*

>>> *and*

>>>> *do*

>>>> *you want to analyze it, i can offer to you to take full control*

over

>>> *this*

>>>> *server.*

>>>>

>>>>

>>>>

>>>>

>>>>

>>>

>>>

>>

>>

>

>