

Re: weird server activity

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2002-01/7744.html>

From: James Jeffrey (james@jgj.org.uk)

Date: 01/26/02

Date: Sat, 26 Jan 2002 17:23:35 +0000
From: James Jeffrey <james@jgj.org.uk>
To: freebsd-security@freebsd.org

Hi,

As a very low grade FreeBSD'ian I'm ready to get shot down in flames here but...

I think the logs are a red herring, its just various attempts to exploit IIS which wont effect you, I get them all the time. This dosen't really sound like a security problem as such, I suppose it could be some kind of DoS, but from my limited experience it is more likely to be leaky software and your running out of memory or something. Does your website have any active content? Any cgi–scripts or the like that could be generating problems?

I have seen similar symptoms on Solaris webserveres that were caused by badly written web–backend software exhausting the virtual memory, and I once wrote a cgi–script which did much the same to a FreeBSD box..... :(

regards,

James Jeffrey (CCSA, CCSE)

james@jgj.org.uk

On Saturday, January 26, 2002, at 05:13 , William J. Borskey wrote:

> *I am running FreeBSD 4.4. I use Apache–fp and openssh. About a week ago
> my system went down and I wasnt
> able to log in or look at any web pages. I could connect, but it woud
> not spawn a process to log me in, or serve me a
> web document. I got someone to reboot the machine from the console, I
> was then able to log into the machine.
> Starting processes was slow but top reports normal system loads. Then
> after about an hour the machine would no
> longer run any processes and quickly shut me out by killing the sshd i
> was connected with. I did get a chance to
> look at some of my logs, not all unfortunatly. The httpd–access file
> had some weird sequences of windows*

FreeBSD–Security: Re: weird server activity

> *sounding paths, but it wasnt code red or anything like code red:*
> 147.46.54.38 – – [19/Jan/2002:15:12:57 –0600] "GET
> /scripts/root.exe?/c+dir HTTP/1.0" 404 200
> 147.46.54.38 – – [19/Jan/2002:15:12:57 –0600] "GET
> /scripts/root.exe?/c+dir HTTP/1.0" 404 200 "-" "-"
>

<SNIP>

> 147.46.54.38 – – [19/Jan/2002:15:12:57 –0600] "GET
> /MSADC/root.exe?/c+dir
> 147.46.54.38 – – [19/Jan/2002:15:12:58 –0600] "GET
>
> /scripts/..%25f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404
> 200 "-" "-"
> *i havnt been able to look at any other logs and i doubt that that has
> anything to do with it.*

>
> *William Borskey*

>
>

> *Get your FREE download of MSN Explorer at*
> <http://explorer.msn.com/intl.asp>.

>
>
> *To Unsubscribe: send mail to majordomo@FreeBSD.org*
> *with "unsubscribe freebsd–security" in the body of the message*

>

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd–security" in the body of the message