

Re: I was hacked

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-08/0101.html>

From: DvDmanDT (dvdmandt_at_telia.com)

Date: 08/04/03

Date: Mon, 4 Aug 2003 04:45:40 +0200

Only me noticing that the requests seemed to come from a LAN? Or was that the firewall?

Search all your filesystem for the file "A~NSISu_.exe" and search google for it as well...

To secure IIS somewhat, remove all the virtual directories even if they are used and figure a better way to write your scripts or something... I'm on Apache and I've only been hacked thru my own script... Therefore, I nowadays use Apache to proxypass all requests to IIS and that way I can have some script to check if the url is valid and if so execute the script... Otherwise block IP...

```
--  
// DvDmanDT  
MSN: dvdmandt@hotmail.com  
Mail: dvdmandt@telia.com  
"Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> skrev i meddelandet  
news:ejIyw8iWDHA.2352@TK2MSFTNGP12.phx.gbl...  
> Hi,  
>  
> The entire set of weblogs shows HTTP 404 (not found), or 403 (Access  
Denied)  
> etc type status codes. So, none of those attacks was succesful.  
>  
> That said, if the remote attacker was able to use a buffer overflow  
attack,  
> then there'd be nothing in your IIS weblogs, since the exploit happens  
> before the request can be logged by IIS.  
>  
> Do you have some kind of application level firewall on this machine? If  
so,  
> you could see if the process is attempting to conect to anywhere remotely.  
>  
> Additionally, seaching for the .exe in particular seems to indicate it may  
> be associated with some kind of spyware - have you installed anything of  
the  
> sort? (downloaded something from the 'net, installed a file-sharing app or  
> similar?). Maybe you should run adAware (http://www.lavasoftusa.com/)  
>  
> Cheers  
> Ken  
>
```

microsoft.public.inetserver.iis.security: Re: I was hacked

```
>
> "Frank" <frank@nosppamplease.com> wrote in message
> news:VUZWa.36782$Vt6.14734@rwrnsc52.ops.asp.att.net...
> : I have a Windows 2000 server that is current w/ the latest patches from
> MS.
> : It is running an IIS server that is configured w/ Microsoft's URLScan
> tool.
> : It is also running Terminal Services w/ 128 bit encryption turned on. I
> : have a firewall configured to allow only inbound/outbound HTTP traffic
on
> : port 80 and Terminal Services. I'm also running Snort as an IDS, a
virus
> : scanner that updates/scans nightly. I have Windows security auditing
> turned
> : on. I've also hardened the system by turning off all unnecessary
service
> : and making all the appropriate registry changes to restrict a access
(e.g.
> : disabling anonymous access).
> :
> : Sounds somewhat secure, right?
> :
> : Last night I was hacked. I'm still trying to sort out what happened. I
> saw
> : a series of attempts to attack IIS that the IIS log claimed were coming
> from
> : itself. Unfortunately, my firewall was not logging HTTP traffic -
> although
> : I think I have the source ip via Snort. All these attacks failed.
Next,
> I
> : saw a series of logon failures using Terminal Services. Again, all of
> these
> : failed. Then, a few minutes later, I mysteriously see a process called
> : A~NSISu_.exe. This seems to come out of nowhere. Prior to this I did
not
> : see any cmd sessions or anything else that suggests the attacker
> : successfully breached my server
> :
> : Below is the web log followed by the event in the event viewer that
showed
> : the first visible process of the attack. Following this, I saw a series
> of
> : processes start (cmd.exe, nbstat, route).
> :
> : I can take care of reinstalling and hardening my system. I have one
> primary
> : concern at this stage: understanding how they cracked my server. If you
> : have advice or suggestions, it would be appreciated.
> :
> :
> :
> :
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/*.*.idc 404 4184 21 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /iisadmin/ - 404 4184 25 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan>
> :
> :
```

Re: I was hacked

microsoft.public.inetserver.iis.security: Re: I was hacked

```
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/qfullhit.htw 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/qsumrhit.htw 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/abczxv.htw 404 4184 26 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/author.idq 404 4184 49
> 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/filesize.idq 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/filetime.idq 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/query.idq 404 4184 48
> 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/queryhit.idq 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/simple.idq 404 4184 49
> 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/webhits.exe 404 4184 50
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cfcache.map - 404 4184 27 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /_vti_pvt/administrators.pwd - 403 4358 43 344 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /_vti_pvt/authors.pwd - 403 4358 36 16 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /_vti_pvt/users.pwd - 403 4358 34 16 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /_vti_pvt/service.pwd - 403 4358 36 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 POST
> : /_vti_bin/shtml.dll/_vti_rpc - 405 4230 368 15 10.2.2.50 MSFrontPage/4.0
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/ - 404 4184 24 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /scripts/ - 401 4572 48 47 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/sh - 404 4184 26 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/csh - 404 4184 27 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/ksh - 404 4184 27 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/cmd.exe 404 4184 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/cmd.exe 404 4184 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/cmd32.exe 404 4184 33 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/cmd32.exe 404 4184 33 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/perl.exe 404 4184 35 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/perl.exe 404 4184 35 0 - -
```

Re: I was hacked

microsoft.public.inetserver.iis.security: Re: I was hacked

```
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/tools/newdsn.exe 404 4184 40 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/_vti_bin/fpcount.exe 404 4184 71 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/rightfax/fuwww.dll/ 404 4184 36 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /iissamples/issamples/query.asp - 403 4270 46 78 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /samples/search/queryhit.htm - 404 4184 43 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /scripts/*.pl - 401 4572 62 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /iissamples/exair/search/advsearch.asp - 403 4270 53 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/iisadmpwd/aexp3.htr 404 4184 35 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /scripts/repast.asp - 403 4270 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/ 404 4184 20 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/users/ 404 4184 26 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/ 404 4184 28 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/ 404 4184 28 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /iissamples/exair/howitworks/codebrws.asp - 403 4270 56 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /msadc/samples/selector/showcode.asp - 403 4270 51 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /index.htm PageServices 200 0 29 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /search - 404 4184 23 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /index.html+ - 404 4184 29 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/rguest.exe 404 4184 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/rguest.exe 404 4184 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/wguest.exe 404 4184 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/wguest.exe 404 4184 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/get32.exe 404 4184 33 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/alibaba.pl - 404 4184 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/tst.bat 404 4184 31 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-win/uploader.exe 404 4184 36 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/FormHandler.cgi - 404 4184 39 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/testcgi - 404 4184 31 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/test-cgi/* * 404 4184 36 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/test.cgi - 404 4184 32 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/enivron.pl - 404 4184 34 0 - -
```

microsoft.public.inetserver.iis.security: Re: I was hacked

```
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /scripts/environ.pl - 401 4572 68 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /server-info - 404 4184 27 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /server-status - 404 4184 29 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/tcsh - 404 4184 28 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/cgitest.exe 404 4184 35 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /~root - 404 4184 21 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> /~ftp -
> : 404 4184 20 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/phf Qalias=&Qname=haqr&Qemail=&Qnickname=&Qoffice_phone= 404
4184
> : 80 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/count.cgi - 404 4184 33 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/nph-test.cgi - 404 4184 36 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/webdist.cgi - 404 4184 35 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/aglimpse.cgi - 404 4184 36 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/campas %0acat%0a/etc/passwd%0a 404 4184 54 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/jj - 404 4184 26 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/formmail - 404 4184 32 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/formmail.pl - 404 4184 35 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/faxsurvey /bin/cat%20/etc/passwd 404 4184 56 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/view-source ../../../../../../etc/passwd 404 4184 67 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/srchadm/webhits.exe 404 4184 43 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/tools/mkilog.exe 404 4184 40 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/tools/mkplog.exe 404 4184 40 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/query mss=../../../../../../../../etc/passwd 404 4184 65 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/htimage.exe 404 4184 39 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/htimage.exe 404 4184 39 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/author.idq 404 4184 49
> 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/filesize.idq 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/filetime.idq 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/query.idq 404 4184 48
```

Re: I was hacked

microsoft.public.inetserver.iis.security: Re: I was hacked

```
> 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/queryhit.idq 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/simple.idq 404 4184 49
> 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/qfullhit.htw 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/qsumrhit.htw 404 4184 51
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/scripts/samples/search/webhits.exe 404 4184 50
> : 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /robots.txt - 404 4184 26 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/echo.bat 404 4184 41 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/hello.bat 404 4184 42 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/htsearch exclude=%60/etc/passwd%60 404 4184 58 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/ezshopper/loadpage.cgi user_id=1&file=|cat%20/etc/passwd| 404
> 4184
> : 81 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/ezshopper/search.cgi
> :
>
user_id=id&database=dbasel.exm&template=../../../../../../../../etc/passwd&dist
> : inct=1 404 4184 127 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/names.nsf/ 404 4184 31 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/catalog.nsf/ 404 4184 33 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/log.nsf/ 404 4184 29 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/domlog.nsf/ 404 4184 32 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/domcfg.nsf/ 404 4184 32 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/sojourn.cgi cat=../../../../../../../../etc/passwd 404 4184 71
0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/ows-bin/perlidl.c.bat 404 4184 41 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-bin/windmail.exe 404 4184 36 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /_vti_bin/shtml.dll - 403 4358 34 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /.htaccess - 404 4184 25 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /_vti_pvt/doctodep.btr - 403 4358 37 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /carbo.dll icatcommand=..\..\..\boot.ini&catalogname=catalog 404 4184
> 78
> : 16 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
```

Re: I was hacked

microsoft.public.inetserver.iis.security: Re: I was hacked

```
> : /cfdocs/expeval/ExprCalc.cfm OpenFilePath=c:\boot.ini 404 4184 68 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cfdocs/expeval/openfile.cfm - 404 4184 43 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/pfdispaly.cgi '%0A/bin/uname%20-a|' 404 4184 59 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/MachineInfo - 404 4184 35 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /mylog.phtml screen=/etc/passwd 404 4184 46 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /mlog.phtml screen=/etc/passwd 404 4184 45 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /cgi-bin/wrap - 404 4184 28 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/ows-bin/oasnetconf.exe 404 4184 72 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/ows-bin/oaskill.exe 404 4184 45 0 - -
> : 2003-08-02 05:54:56 192.168.0.1 - W3SVC1 MYSERVER 192.168.0.1 80 GET
> : /<Rejected-By-UrlScan> ~/cgi-shl/win-c-sample.exe 404 4184 40 0 - -
> :
> :
> :
> :
> : Event Type: Success Audit
> : Event Source: Security
> : Event Category: Detailed Tracking
> : Event ID: 592
> : Date: 8/2/2003
> : Time: 2:50:28 AM
> : User: MYSERVER\MyAdmin
> : Computer: MYSERVER
> : Description:
> : A new process has been created:
> : New Process ID: 1764
> : Image File Name: \DOCUME~1\ADMINI~1\LOCALS~1\Temp\A~NSISu_.exe
> : Creator Process ID: 1916
> : User Name: MyAdmin
> : Domain: MYSERVER
> : Logon ID: (0x0,0xDE65)
> :
> :
> :
> :
> :
> :
> :
```