

Re: Windows Credentialing Security Problem

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-04/2392.html>

From: Joseph Geretz (jgeretz_at_nospam.com)

Date: 04/23/04

Date: Thu, 22 Apr 2004 22:46:57 -0400

Thanks Ken,

- > *I suspect (very strongly) that this is a double-hop authentication problem.*
- > *You can confirm this by disabling IWA, and enabling Basic Auth. If all your*
- > *problems go away, then it is the double-hop auth problem.*

Your suggestion is right on target. So this is a delegation issue. Thanks for clearing that up. You've given me quite a list of suggestions and references which I'll start to work through. If I have specific questions on any of these points I'll post back.

Thanks,

Joe Geretz

"Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message news:uclBZsCKEHA.2784@TK2MSFTNGP10.phx.gbl...

- > *I suspect (very strongly) that this is a double-hop authentication problem.*
- > *You can confirm this by disabling IWA, and enabling Basic Auth. If all your*
- > *problems go away, then it is the double-hop auth problem.*
- >
- > *With Basic Auth, the webserver has your username and password, so it can*
- > *directly impersonate you when authenticating to the remote resource.*
- >
- > *With Digest or IWA auth, IIS only has a token that doesn't have access to*
- > *remote resources. To get around this you can configure Delegation.*
- >
- > *a) Both the user account(s) and the server's computer account must be*
- > *trusted for delegation in the directory. See*
- > *<http://support.microsoft.com/default.aspx?kbid=325894>*
- > *HOW TO: Configure Computer Accounts and User Accounts So That They Are*
- > *Trusted for Delegation in Windows Server 2003 Enterprise Edition (also*
- > *includes Windows 2000 instructions)*

microsoft.public.inetserver.iis: Re: Windows Credentialing Security Problem

- >
- > *b) The SPN (Service Principal Name) needs to be registered, if it isn't*
- > *already (e.g. you are using a FQDN rather than the NetBIOS name of the*
- > *service). Use the SetSPN.exe tool to do this. For more information on*
- > *SetSPN.exe*
- > *Authentication May Fail with "401.3" Error If Web Site's "Host Header"*
- > *Differs from Server's NetBIOS*
- > *see: <http://support.microsoft.com/?id=294382>*
- >
- > *c) The client browser and IIS server must authenticate using Kerberos not*
- > *NTLM v2 (Not required in a windows 2003 Domain – see below) This means*
- > *that:*
- > *– Use Integrated Windows Authentication (requires restart) is checked in*
- > *I.E.*
- > *– IIS is sending "Negotiate" WWW-Authenticate headers*
- > *– The client-browser can contact the KDC (the Windows Domain Controllers)*
- > *to*
- > *get an appropriate Kerberos ticket*
- >
- > *If you are using a Windows 2003 Domain, you can take advantage of Protocol*
- > *Transition. This allows the user to authenticate using any protocol to*
- > *IIS,*
- > *and IIS can still get a Kerberos ticket to access the remote SQL Server.*
- > *There is information on setting up constrained delegation (using all*
- > *protocols) here:*
- >
- >
- > http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/proddocs/en-us/se_con_del_computer.asp
- > *Configuring Users and Computers for delegation (there's a couple of*
- > *pages –*
- > *use the links in the nav bar to get to them). Following the instructions*
- > *on*
- > *constrained delegation.*
- >
- > *there is more information on Protocol Transition here:*
- > *Windows 2003 Protocol Transition*
- >
- > <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/constdel.mspx>
- >
- > *This article may also help:*
- > <http://support.microsoft.com/default.aspx?scid=kb:en-us:810572>
- > *HOW TO: Configure an ASP.NET Application for a Delegation Scenario*
- >
- > *Hope this all helps!*
- >
- > *Cheers*
- > *Ken*
- >
- >
- >

microsoft.public.inetserver.iis: Re: Windows Credentialing Security Problem

> "Joseph Geretz" <jgeretz@nospam.com> wrote in message
> news:utBJmkCKEHA.3428@TK2MSFTNGP09.phx.gbl...
> : I'm having a credentialing problem in my web application. Actually, I
> don't
> : think this is an IIS security issue, since I'm able to access the page
I'm
> : requesting. However, the executing page itself is not able to access a
> : specific network resource and I just can't figure out why. First of all,
> let
> : me say this worked fine with IIS running on Win2000 Server. This has not
> : worked since I upgraded to Windows Server 2003.
> :
> : My Platform: Windows Server 2003 / IIS6 / .Net Framework v1.1.4322
> :
> : My web site has a virtual directory named FPSNowAuth. This virtual
> directory
> : disallows anonymous access and is set to use Windows Integrated
security.
> : Thus every page access from this virtual directory must either be
> : authenticated or fail.
> :
> : Here are the relevant blocks from the Web.config file:
> :
> : <authentication mode="Windows" />
> : <identity impersonate="true" userName="" password="" />
> :
> : Thus, code executing in the context of a page request should be
executing
> in
> : the security context of the authenticated user. Here's a snippet from
the
> : log file:
> :
> : 2004-04-22 04:28:34 192.168.1.3 GET /FPSNowAuth/browser.aspx
> : dir=ftp/Dimension 81 INTDOM\Boss 192.168.1.1
> : Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0;+.NET+CLR+1.0.3705)
200
> :
> : As you can see, I accessed the page '/FPSNowAuth/browser.aspx' with the
> : querystring 'dir=ftp/Dimension' appended to the URL. I authenticated as
> : INTDOM\Boss, the Domain Administrator. HTTP Status was 200. The page
> request
> : succeeded. However...
> :
> : browser.aspx is a .NET page which returns a directory listing of the
> : directory identified by the dir querystring parameter, in this case
> : ftp/Dimension. (For a practical example of this, you may check out
> : www.fpsnow.com/browser.aspx?dir=ftp/download. This is the public area of
> my
> : site.) FPSNowAuth/ftp/Dimension is mapped to a network fileshare
> : \\Dimension\User. Here we get to the heart of the problem.

> :
> : *When I'm on the server, browsing the virtual directory in the IIS console,*
> *I*
> : *can see all the folders and files subordinate to \\Dimension\User. When I*
> : *hit this page from a browser on the server, I get a nicely formatted*
> *listing*
> : *of these folders and files, generated by browser.aspx. However, when I*
> *hit*
> : *this page from a browser on any other workstation, I get the following*
> : *runtime error during the course of the page execution:*
> :
> : *Access to path \\Dimension\User is denied.*
> :
> : *This despite the fact that I have authenticated as INTDOM\Boss, as shown*
> *in*
> : *the log file snippet. So running under the identity of INTDOM\Boss, why*
> *the*
> : *heck am I denied access to a network resource?*
> :
> : *For the .NET developers among us, here's the line of code which throws*
> *the*
> : *exception:*
> :
> : *DirectoryInfo[] Dirs = DirectoryInfo.GetDirectories();*
> :
> : *The directory indicated by DirectoryInfo is \\Dimension\User\. Prior to*
> *executing*
> : *this line, I've already checked to ensure that Request.IsAuthenticated*
> *==*
> : *true. I've stepped through this in debug mode and confirmed that it is*
> : *indeed true (as the log file entry indicates).*
> :
> : *So, I'm baffled. The page is executing under the identity of the domain*
> : *admin, yet I get an access denied when attempting to access a network*
> : *resource. Any ideas?*
> :
> : *Thank for any assistance which you can offer.*
> :
> : *– Joe Geretz –*
> :
> :
>
>