

Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-11/5927.html>

From: Karl Westerholm [MS] (karlwestonline@microsoft.com)

Date: 11/15/02

From: karlwestonline@microsoft.com (Karl Westerholm [MS])

Date: Fri, 15 Nov 2002 01:20:36 GMT

Based on the configuration we are using for this dir, (Basic authentication selected, anonymous & windows integrated *not* selected) there should be no access by the IUSR at all on the 'testing' VDIR.

Now, it is possible that you are first hitting the root of the website just before browsing to the testing VDIR, and the root itself may have anonymous access enabled. If that was what was happening then we could maybe explain why we see the IUSR account in use.

Can you reconfirm that the testing VDIR has *only* the Basic authentication option selected? Regardless of what else may be happening on the website, we have to first 100% confirm that there are no problems browsing to this VDIR as the local administrator account via Basic-only auth.

As far as the router/firewall, as long as port 80 is opened we should be in good shape. The exchange of information that takes place between your browser & IIS to allow Basic to function takes place only over that port.

-->Karl

“Please do not send email directly to this alias. This is our online account name for newsgroup participation only.”

This posting is provided “AS IS” with no warranties, and confers no rights. You assume all risk for your use. © 2001 Microsoft Corporation. All rights reserved.

| From: trinetgrinch@yahoo.com (Vincent Polite)

| Newsgroups: microsoft.public.inetserver.iis.security

| Subject: Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

| Date: 14 Nov 2002 11:05:50 -0800

microsoft.public.inetserver.iis.security: Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

| Organization: <http://groups.google.com/>

| Lines: 412

| Well, here's something wierder. I turned on Failure auditing for all
| the events that you suggested, and I'm not getting any messages coming
| into the Security Log for ANY of my login attempts via web browser or
| Frontpage.

| Oh... waitaminute. I need to turn on auditing on the folder, too.

| Hold on.

| OK. Everytime I attempt to login under Basic Authentication, no
| matter what username I use, the Event Log registers: Event 560:
| IUSR_blah account. Interestingly enough, in the log file there is a
| single reference as <DOMAIN NAME>\IUSR_blah, but everywhere else in
| the event log it is listed like a local user.

| In any case, the anonymous user impersonated by the IIS Server is the
| one that seems to trigger all the entries. I don't know if this is
| considered normal when you fail to authenticate, but I'm not getting
| any specific reference to any of the accounts that I specifically used
| to log in.

| Could my router (NAT/Firewall) somehow cause this? Does Basic Auth.
| go over a different port than port 80? But I get this whether I use
| the NETBIOS name of the box or the name based on DNS. This local box
| is also the DNS server and has a correct local IP address entry for
| the server...

| so... what would be the next step here?

| VP

| karlwestonline@microsoft.com (Karl Westerholm [MS]) wrote in message
| news:<bb6fhN2iCHA.1880@cpmsftngxa08>...

| > Hmm...some odd results. So with the Basic-only auth, we are unable
| to

| > get the local administrator account to logon/browse the simple ASP page

| > through IIS? (local to the IIS box, that is?) The main test I wanted

| to

| > confirm with this is that -- in the context of the IIS5 machine's local

| > administrator account -- we should have no problems at least browsing

| to

| > the content.

| >

| > If this is possible, then our next step is to introduce the added

| > complexity of attempting to physically connect & publish via FrontPage.

| > But, if I am understanding your results, this does not seem to be
| taking

Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

|> place except when you enable Integrated auth?
|>
|> Are you sure that when you hit the IIS5 box and are prompted w/Basic
|> auth that you are using the actual administrator account from the IIS5
|> server? (and not, say, a domain administrator account?)
|>
|> Regardless, I would next say lets enable failure auditing for all
|> events. To do this, go into the IIS server's administrative
tools/local
|> security policy MMC.
|>
|> Drill down in this MMC past 'security settings', 'local policy', &
then
|> into 'audit policy'. Double-click each entry you see there & then
click
|> the 'failure' checkbox. Once these are all set, go back to the
top-level
|> 'security settings' and right-click the icon you'll see there. (its a
grey
|> computer with a yellow padlock on it) From this menu, you should be
able
|> to select 'reload' to insure that these new auditing settings are
actually
|> enabled.
|>
|> Now, drill back down into the audit policy section: take note of
the
|> 'effective setting' vs. the 'local settings' column. If the effective
|> setting is configured differently then the local settings column is,
then
|> this machine is a domain member & the audit policy we want to change is
|> being set at the DC level & will need to be overridden on the DC.
|>
|> In any case, once this auditing is set then attempt to connect once
more
|> via Basic-only auth to our testing VDIR (also by windows machinename)
and
|> attempt to logon as local machine's 'administrator' account. If you
still
|> fail, you could try using 'IISmachinename\administrator', but the main
|> purpose of this test is to see whay (if anything) we might turn up in
the
|> Event Viewer Security log.
|>
|> In the event of failed logins, we should see *some* failed event in
|> security log (look for events with a 'lock' icon) that will help
explain
|> why our admin account is not working.
|>
|> Once we can get the admin account to successfully authenticate &
browse

microsoft.public.inetserver.iis.security: Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

|> then we can move on and add the FP connectivity/authentication tests to
the

|> mix for the admin user. Ultimately, assuming we can get that to work,
we

|> finally start using the actual garden-variety local users, (and/or
domain

|> user accounts) insure they have the appropriate NTFS & user rights to

|> access content & logon locally, and (hopefully) finally get *them*

happy as

|> well.

|>

|> Note that if this IIS5 machine is a member of a domain, we may as
well

|> enable the same kind of auditing on the DC as we are doing on the IIS5

|> server. At some point we *should* start seeing security log failure
events

|> either on the local machine or on the DC that can 100% be synchronized
with

|> our failed attempts to either logon & browse, and/or connect via
FrontPage.

|>

|> --->Karl

|>

|>

|>

|>

|> "Please do not send email directly to this alias. This is our online

|> account name for newsgroup participation only."

|>

|> This posting is provided "AS IS" with no warranties, and confers no
rights.

|> You assume all risk for your use. © 2001 Microsoft Corporation. All
rights

|> reserved.

|>

|> _____

|> | From: trinetgrinch@yahoo.com (Vincent Polite)

|> | Newsgroups: microsoft.public.inetserver.iis.security

|> | Subject: Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage
2002

|> = failure?

|> | Date: 13 Nov 2002 10:16:09 -0800

|> | Organization: <http://groups.google.com/>

|> |

|> | Karl,

|> |

|> | Thanks for laying out some basic testing strategy. I appreciate it,

|> | as I lost my discipline through frustration.

|> |

|> | That said, I wanted to post the results of my first test.

|> |

Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

> | I created a folder on my E: drive called E:\testing. In it I included
> | a default.asp page with a basic Response.Write("Hello World") type of
> | message.
> | I locked down the default.asp file and the E:\testing folder with NTFS
> | permissions only corresponding to the Administrator account and the
> | SYSTEM account.
> |
> | In IIS I took the virtual server that I was testing, and adding the
> | testing directory as a virtual directory, protected under the Basic
> | Authentication premise.
> |
> | Browsing to the web, under my current configuration, I am currently
> | forced to use a fully qualified domain name because of my use of host
> | headers. In browsing to the page, I am challenged by the Basic
> | authentication dialog box.
> |
> | Under Windows XP (remote test client), I am prompted for a
> | username/password. Under Win2K Server (local test client), I am
> | prompted for a username/password, and the dialog box notifies me that
> | the "Realm" being authenticated against is the name of my virtual
> | server.
> |
> | I attempted to login using the following combinations.
> |
> | <administrator accountname>
> | <domainname>\<administrator accountname>
> | <administrator accountname>@domainname
> | <administrator accountname>@domainname.com
> |
> | None of the username/password combinations were accepted.
> |
> | When I add the Integrated Windows Authentication tab, my internal
> | client validates, while my external client (behind the proxy server)
> | gives me the expected message that NT Challenge/Response is not
> | supported by this proxy.
> |
> | Turning everything back to Basic Authentication gives me the same
> | issues (no username/password combination is accepted)
> |
> | This time, I turn off ALL of my other virtual web servers and
> | host-header enabled sites, so the only thing that is on is the server
> | I am testing. This also allows me to surf to the site using the
> | NetBios name of the server.
> |
> | I attempt to access the protected directory using the following
> | conventions:
> |
> | <http://>/testing>
> | <http://>/testing>
> |
> | Both methods give me the same Basic Authentication dialog that I

|> | cannot seem to bypass.

|> |

|> | Switching the server to accept Integrated Windows Authentication, and

|> | everything works as expected.

|> |

|> | Hmmmmm.

|> |

|> | Vincent Polite

|> | Not tearing his hair out because he's had his Mountain Dew this

|> | morning. :)

|> |

|> | Any ideas?

|> |

|> | P.S. The event log under System, Application, or Security doesn't

|> | show any events that show my failed attempts that I have been trying

|> | to log into the server.

|> |

|> |

|> |

|> |

|> |

|> | karlwestonline@microsoft.com (Karl Westerholm [MS]) wrote in message

|> news:<pOD2\$griCHA.2368@cpmsftngxa09>...

|> |> I've been where you are, and I can certainly sympathize! With every

|> |> extra bit added to the configuration of this puzzle, the problem seems

|> |> to

|> |> become almost unsolvable. But, as someone once said, 'the truth is out

|> |> there'! :)

|> |>

|> |>

|> |> I would try to start with the simplest possible configuration and

|> |> work

|> |> upward:

|> |>

|> |> 1.) Create a brand-new test physical directory (called, say,

|> |> c:\testing)

|> |> local to your IIS5 server, and be careful to keep this physical

|> |> directory

|> |> outside of any other web content directories you have currently.

|> |>

|> |> 2.) Place a single *simple* HTML or ASP file in that dir

|> |> (something

|> |> like

|> |> '<% response.write time %>', in other words) and Assign NTFS

|> |> permissions on

|> |> the file + dir to be 'administrator' & 'system' full control...no

|> |> other

|> |> NTFS perms.

|> |>

|> |> 3.) Map this physical dir to a virtual directory (called, say,

|> 'testing'

|> |> :) under the website in question, enabling only Basic authentication.

|> |>

|> |> 4.) Prove that you can at least browse to this file in IE, are

|> prompted to

|> |> authenticate, and can use the local administrator account to

|> successfully

|> |> authenticate to it.

|> |>

|> |>

|> |> Gotchas to be aware of:

|> |>

|> |> - Always have 'show friendly HTTP error messages' turned off in your

|> test

|> |> copy of IE. (IE's tools/internet options/advanced tab) If this option

|> is

|> |> checked on your test IE client, it may mask additional error messages

|> you

|> |> may be getting that are very significant.

|> |>

|> |>

|> |> - When testing with IE or FrontPage local to the webserver for a baseline

|> |> 'is this working yet?' reference, be sure to connect via

|> |> windowmachinename

|> |> rather than IP or FQDN. That is to say, use 'http://machinename' to

|> |> connect rather than 'http://1.2.3.4'.

|> |>

|> |> IE (and FrontPage too, if I am not mistaken) will interperate the

|> |> presence of periods in the address as indicating the request *may* be

|> |> Internet, and not Intranet. This may have the effect of remoting your

|> |> request out through a configured Proxy even when you do not wish to do

|> so.

|> |>

|> |>

|> |> - Be careful to cycle the IISAdmin service whenever you are making security

|> |> tweaks & NTFS-type permissions modifications. IIS5 will cache the

|> |> credentials of a given user account for a period of time (15

minutes. I

|> |> believe) so if you do not cycle the IISAdmin service, or wait until the

|> |> credentials are no longer cached, you may have made a tweak that |> actually

|> |> fixed the problem but just do not realize it has worked.

|> |>

|> |> You can cycle IISAdmin from control panel/services, but I generally

|> like

|> |> to use the command-line:

|> |>

|> |> net stop iisadmin

|> |> (followed by)

|> |> net start w3svc

|> |>

|> |> Of course, this *also* has the effect of stopping all your websites

|> on

|> |> that box until the w3svc service is restarted. You can adjust the

|> caching

|> |> of credentials in IIS upward or downward, but setting it to too small a

|> |> time can have implications to poor performance. See also:

|> |> <http://support.microsoft.com/default.aspx?scid=KB;en-us:152526&>

|> |>

|> |>

|> |> Now that I have some of those gotchas out of the way, lets get back

|> to

|> |> our testing VDIR. I am presuming that at this point browsing locally,

|> |> authenticating as the admin user, and displaying simple content is

|> working

|> |> perfectly.

|> |>

|> |> Next, lets configure the server extensions on this

VDIR....select

|> the

|> |> defaults.

|> |>

|> |> Once you have the extensions configured, attempt to connect to via

|> |> FrontPage from the local machine. Can you connect? Does it prompt you

|> for

|> |> authentication? Do the admin user credentials that worked for browse

|> allow

|> |> you to connect fully w/FP as well?

|> |>

microsoft.public.inetserver.iis.security: Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

|>|> If not, keep careful track of any errors you get in the process
and
|> post
|>|> them back here. Also, immediately after whatever FP-failure you
|>|> experience, track down the IIS5 server's System & Application event
|> viewer
|>|> logs. Look for any red (stop) or yellow (warning) error messages
that
|> seem
|>|> to be synced up with the failure....and post them as well! :)
|>|>
|>|> Regards.
|>|> -->Karl
|>|>
|>|>
|>|>
|>|> "Please do not send email directly to this alias. This is our
online
|>|> account name for newsgroup participation only."
|>|>
|>|> This posting is provided "AS IS" with no warranties, and confers no
|> rights.
|>|> You assume all risk for your use. © 2001 Microsoft Corporation. All
|> rights
|>|> reserved.
|>|>
|>|> -----
|>|> | From: trinetgrinch@yahoo.com (Vincent Polite)
|>|> | Newsgroups: microsoft.public.inetserver.iis.security
|>|> | Subject: Basic Authentication + IIS 5 + Windows 2000 + Frontpage
2002
|>≡
|> failure?
|>|> | Date: 12 Nov 2002 16:17:27 -0800
|>|> | Organization: http://groups.google.com/
|>|> |
|>|> | I have seen threads about this topic all over UseNet, so I wanted
to
|>|> | state my problem which may or may not have a unique twist.
|>|> |
|>|> | The setup:
|>|> |
|>|> | My web server is a Windows 2000 Server. It houses Exchange 2000
and
|>|> | runs IIS5 Web Services and FTP Service. From a website
perspective, I
|>|> | host (for personal reasons) about 30 different websites. These
|>|> | websites are differentiated using host-headers, configured
through the
|>|> | Internet Services Manager.

Re: Basic Authentication + IIS 5 + Windows 2000 + Frontpage 2002 = failure?

|>|>|

|>|>| The websites are divided into 4 domains.

|>|>|

|>|>| *.domain1.com (20)

|>|>| *.domain2.com (2)

|>|>| hostname1.domain3.com

|>|>| hostname2.domain4.com

|>|>|

|>|>| The last two entries are websites that I planned on hosting for some

|>|>| friends. However, to avoid having all their network traffic getting

|>|>| sent to my machine before the site was ready, I set up special

|>|>| instances on the server.

|>|>|

|>|>| The web server itself is behind a Netgear Home Protection System on

|>|>| the tail end of an ADSL Line. I have set up port forwarding for ports

|>|>| 80 (HTTP), 443 (HTTPS on IIS), 25(SMTP), and the ports for my remote

|>|>| control program. (I'm pretty sure FTP is set up as well)

|>|>|

|>|>| On all of the sites I have set up the Frontpage Server Extensions

|>|>| circa 2002. On the majority of the sites, I have set up

Sharepoint

|>|>| Team Services.

|>|>|

|>|>| When I was using NTLM, I was able to connect to my sites and

|>|>| authenticate with any password protected sites no problem. All the

|>|>| sites worked perfectly, and I had nary a problem.

|>|>|

|>|>|

|>|>| The problem:

|>|>|

|>|>| I wanted to work on a friends' site using the facilities/software

I

|>|>| had available at the office. I was going to use Frontpage 2002 to

|>|>| edit this website, but my company's proxy server will not allow NT

|>|>| Challenge/Response w/untrusted domains.

|>|>|

|>|>| Because I cannot convince the powers that be at my office to let me

|>|>| use NT Challenge/Response against my web server, I felt a reasonable

|>|>| alternative would be to change the authentication on the website to

|>|>| "Basic Authentication."

|>|>|

|>|>| Once I made this change through the Internet Services Manager, I

was

|>|>| unable to use Frontpage to edit the site. The problem went beyond

|>|>| Frontpage, as well. In order to make sure it wasn't my company's

|>|>| proxy server, I tried to edit the site running Frontpage locally

on

|>|>| the server itself, and I couldn't validate any of my accounts.

|>|>|

|>|>| After perusing this newsgroup for about a week, i ran across the

|>|>| following notions:

|>|>|

|>|>| 1) Make sure the accounts can log on locally to the server.

|>|>| 2) Make sure that when logging on, use the servername\username

format

|>|>| for the username password prompt.

|>|>| 3) Set a default domain equal to the domain of the account you are

|>|>| using.

|>|>| 4) Set a default domain equal to '\' which signifies all trusted

|>|>| domains.

|>|>|

|>|>| Nothing works. At this point my brain is too numb to orchestrate

the

|>|>| test of just checking basic authentication against a protected

page in

|>|>| the website, but I'm pretty sure I can't get that to work as

well.

|>|>| Meaning, go into Explorer, remove permissions for a specific page

|>|>| except for a specific user, and then try to browse to that page

using

|>|>| a web browser under basic authentication.

|>|>|

|>|>| Any ideas as to how I can approach this problem at this point?

|>|>| Clearly I haven't tried everything, but I feel like I've exhausted

|>|>| quite a few possibilities.

|>|>|

|>|>| Thanks.

|>|>|

|>|>| Vincent Polite

|>|>| Internet Application Specialist about to rescind his title

|>|>|

|>|

|