

Re: IIS 5.0 Windows Authenticion/NT Challenge Response

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-03/0614.html>

anonymous_at_discussions.microsoft.com

Date: 03/24/04

Date: Wed, 24 Mar 2004 11:12:50 -0800

Hi David,

I downloaded the WFETCH tool and ran the tool and this is the result I got out of it shown below. This is running in Anonymous mode. I don't see it returning any errors but am not sure, probably am not reading it properly.

Do you see anything that is causing it to login anonymously? The website URL and IP Address are just examples since, I removed the original one.

Thanks

John

```
resolve hostname "abc.xyz.com"WWWConnect::Connect
("123.123.123.123", "80")\nsource port: 3356\r\n
REQUEST: *****\nGET
xyz/xyz/xyz/embedded.taf HTTP/1.1\r\n
Host: abc.xyz.com\r\n
Accept: */*\r\n
Connection: Keep-Alive\r\n
\r\n
RESPONSE: *****\nHTTP/1.1 400 Bad Request\r\n
Server: Microsoft-IIS/5.0\r\n
Date: Wed, 24 Mar 2004 19:09:07 GMT\r\n
Connection: close\r\n
Content-Type: text/html\r\n
Content-Length: 87\r\n
\r\n
<html><head><title>Error</title></head><body>The parameter
is incorrect. </body></html>WWWConnect::Close
("123.123.123.123", "80")\nclosed source port: 3356\r\n
```

>-----Original Message-----

>It looks like the Web Browser machine happens to have sufficient credentials

>to auto-login to the web server, which does not have
Anonymous enabled. It
>only LOOKS like anonymous is allowed access, but that is
NOT the case. If
>what you say is true, it would be a huge security hole in
IIS; but I'm 100%
>what you say isn't true, so you just need an explanation.
>
>The easiest way to prove this is to take a Network trace
of all traffic
>coming into the web server, and you will see whether an
anonymous request
>succeeds or not. I'm sure you'll see 401.2 being
returned for the anonymous
>requests (which is good -- anonymous requests are all
rejected, as it
>should), and then you will see the web browser attempt to
auto-login with
>NTLM a bunch of times (sequence of 401.2 and 401.