

IIS Auth Error – Kerberos/NTLM not accepting credentials

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2005-01/0080.html>

From: Colin Bower (colinbowern_at_nospam.indimensions.com)

Date: 01/12/05

Date: Wed, 12 Jan 2005 16:57:11 -0500

I've got a Windows Server 2003 / IIS 6 machine running Windows SharePoint Services that users are having problems authenticating against. When someone tries to connect they are prompted for credentials.

— The Windows XP SP2 client computers have the domain added to the local intranet zone ("*.mydomain.com").

— The IIS 6 virtual server is set to use host header names (dev, dev.mydomain.com) which is different from the machine name (frink, frink.mydomain.com).

— IIS has been configured to use both Kerberos and NTLM (as per <http://support.microsoft.com/?id=832769>)

— The application pool identity is a domain user account which belongs to IIS_WPG, STS_WPG. SPNs have been set up as follows (to cover all the bases):

```
setspn -A HTTP/frink MYDOMAIN\sharepoint
```

```
setspn -A HTTP/dev MYDOMAIN\sharepoint
```

```
setspn -A HTTP/dev.mydomain.com MYDOMAIN\sharepoint
```

— The application pool identity domain user account has been set to "Trust this user for delegation to any service (Kerberos only)".

There is one particular computer which seems to be causing the most problems. This user is setup like every other user in terms of permissions, group access, etc. On their Windows XP SP2 laptop they attempt to login and get prompted for credentials. If they enter it correctly they get through. Another sharepoint instance is installed on a domain controller and the user is able to access that one without being prompted for credentials.

Looking at the headers being passed by ieHTTPHeaders the negotiate header is getting sent along with the credential blob. On the server end it's showing:

Event Type: Failure Audit

microsoft.public.inetserver.iis.security: IIS Auth Error – Kerberos/NTLM not accepting credentials

Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 1/12/2005
Time: 4:47:12 PM
User: NT AUTHORITY\SYSTEM
Computer: FRINK
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: problem.user
Domain: dev.mydomain.com
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: USER-LAPTOP
Caller User Name: –
Caller Domain: –
Caller Logon ID: –
Caller Process ID: –
Transited Services: –
Source Network Address: 192.168.1.111
Source Port: 1446

The interesting bits here is that the domain is not the domain of the network but the name of the machine. Also, even though the browser is IE 6, the machine has logged on successfully to the network, and the headers show negotiate the audit log entry is showing NTLM as the auth package.

Any thoughts on what to do next would be great!

Thanks!

Colin

PS – I've been over the following resources already with no luck:

<http://www.choam.org/tbp/weblog/2003/08/02/000072>

http://groups-beta.google.com/group/microsoft.public.inetserver.iis/browse_thread/thread/f7250b172eaf948f#14d0295