How to change the POP3/IMAP4 and SMTP banner in Exchange 2003 for Security reasons

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will show you how to change the banner for the POP3/IMAP4 and SMTP service in Exchange 2003. Changing the banner for these Exchange services enhance the security a little bit if an attacker and legitimate users doesn't know on the first try which server is communicating with them. Please keep in mind that this is only one (and a small) of several methods to secure our Exchange environment.

Let's begin

First of all let us discuss about the necessity to modify the Banner of the SMTP/IMAP4 and POP3 banner. What do you see if you connect via Telnet to your Exchange Server for SMTP/IMAP4 and POP3? You will see the Version number of Exchange, the installed Windows Version and the Service Pack version. This information is great for and intruder or hacker that now knows the Windows and Exchange Version and the possible weaknesses of these products. An intruder can now use this information use some exploits to gain access to the system.

First I will show you what you will see when you try to Telnet your Exchange Server for POP3/IMAP4 and SMTP without modifying the banner. If you don't know how to connect via Telnet to Exchange, read my article about Telnet and Exchange 2003.

The SMTP Message will look like this. Nice: The Server is using Windows 2003 (3790) and Service Pack1 (1830).

Figure 1: SMTP before Banner modifying

Now we can use the script ADSUTIL.VBS to modify the SMTP banner. You can find ADSUTIL.VBS in the Inetpub\AdminScripts directory on the IIS Server (Exchange Server). Execute the script as follow:

CSCRIPT ADSUTIL.VBS set smtpsvc/x/connectresponse "Text that the SMTP service should display"

The x stands for the number of the Virtual SMTP server. After changing the Banner, stop and start the SMTP service by using the Services console or by issuing the NET STOP SMTPSVC and NET START SMTPSVC command.

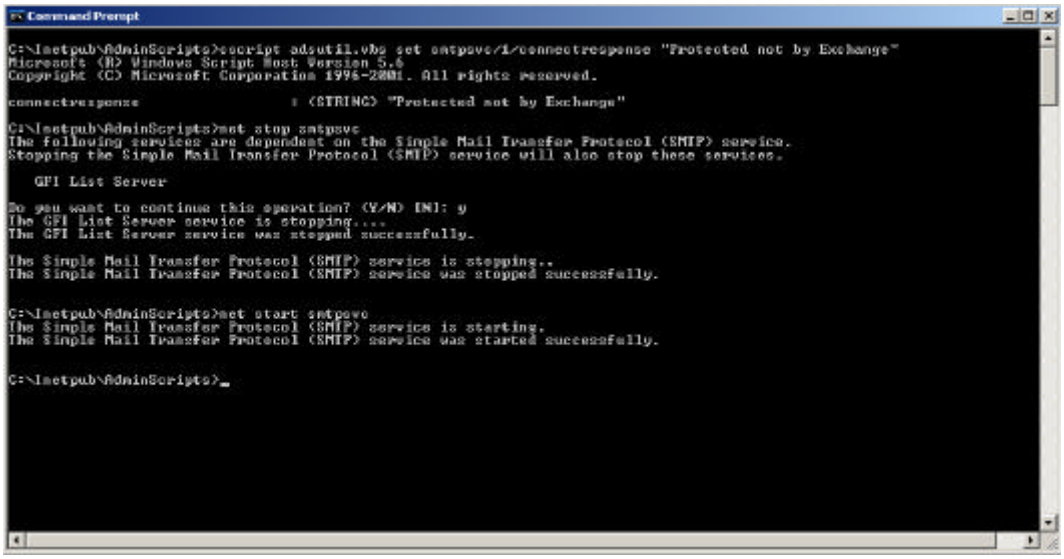
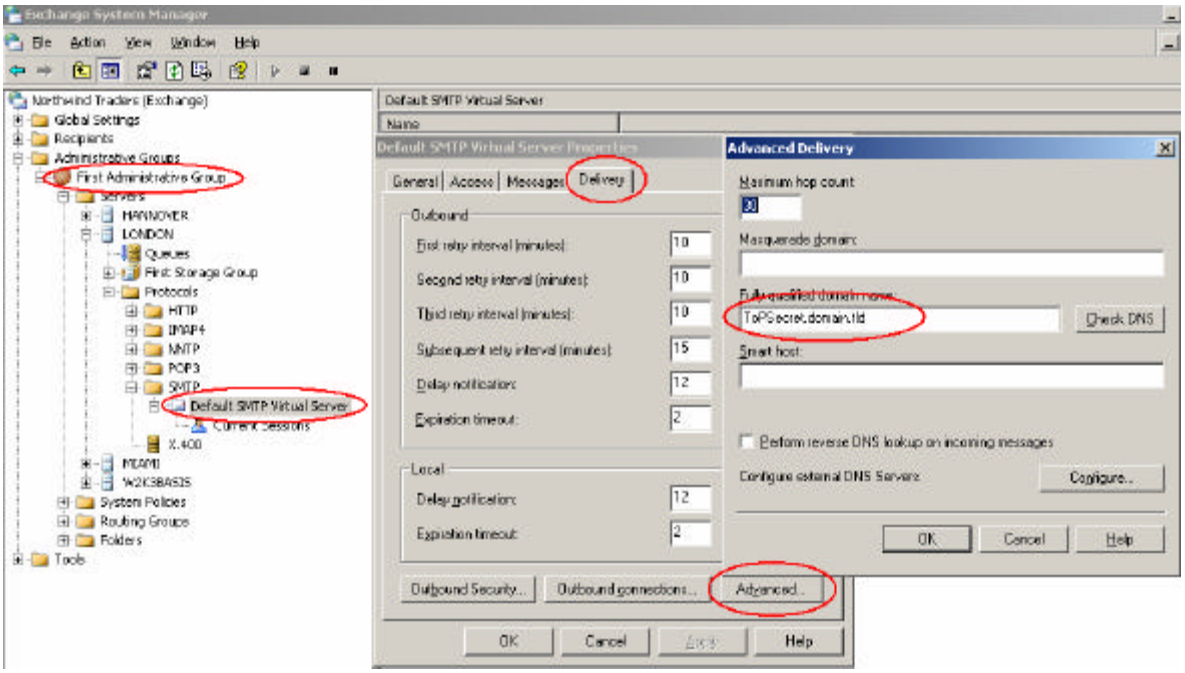


Figure 2: Executing ADSUTIL.VBS

Now it is time to connect via Telnet after Banner modifying and you will see the following connection response.

Figure 3: SMTP after Banner modifying

Is this enough? If not, it is possible to fake the connection response after 220 – with a name that you want. You can change the connection response by using the Exchange System Manager in the delivery properties of the Exchange Virtual SMTP Server like in the following picture.



If you want to disable some SMTP verbs, read the following article.

Now let's go to Telnet to the Exchange 2003 POP server. Open a command prompt and enter TELNET ExchangeServerName 110 and press Enter and you will see a picture like the following.

Figure 5: POP3 Banner before modifying

As you can see, we are using Exchange 2003 (6.5) with Service Pack 2 (7623.0).

Please note: For security purposes the Microsoft POP3 service is disabled by default after Exchange 2003 installation.

You can change these settings by using a tool called SMTPMD which is not available for download. You must open a request to Microsoft PSS to get this handy tool.
One other way is to use the IIS Metabase Explore. The IIS Metabase Explorer is part of the IIS6 Resource Kit which you can download here. After installing the IIS Resource Kit, open the IIS Metabase Explorer and navigate to the POP3SVC key and than to 1 (usually) and create a new Record with the settings shown in the following picture.

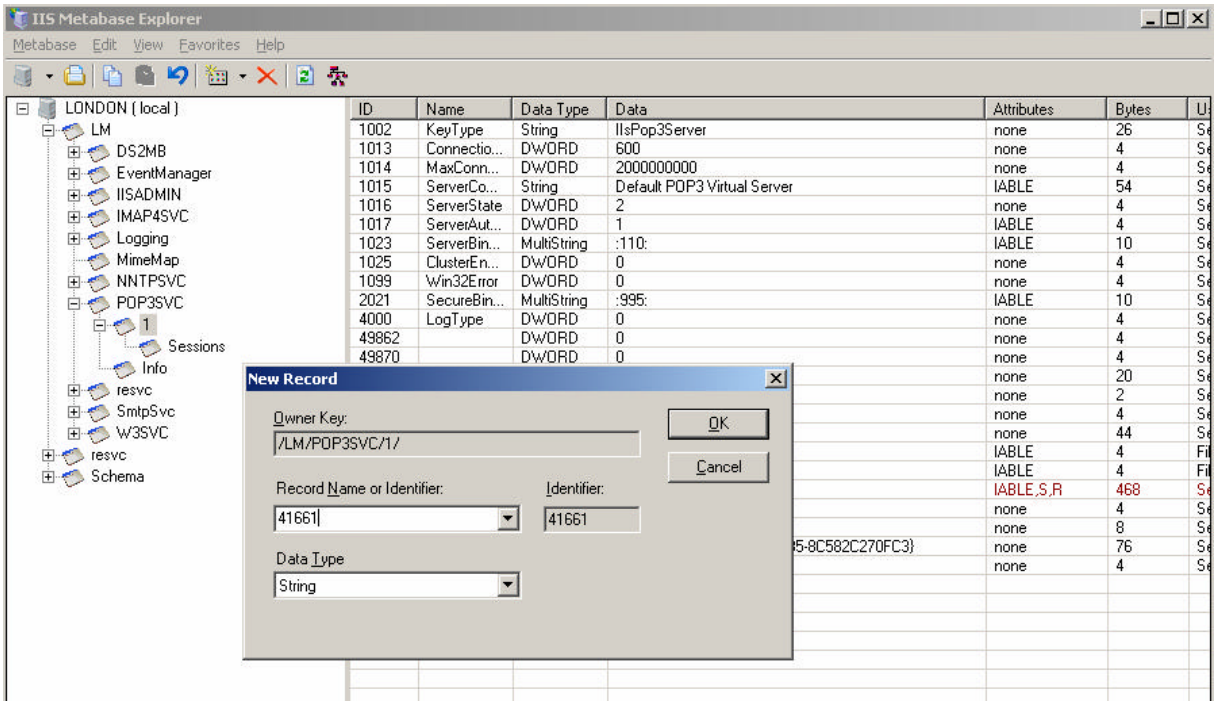


Figure 6: Use IIS Metabase Explorer to create a new POP3 String

Please note:

In Exchange 2000, this modification is applied to all the virtual servers on the Exchange server but in Exchange Server 2003, the modification is applied only to the virtual server that you modify (for example 1 for the first Virtual Server) If a banner is deleted from any one of the Virtual Server, the Virtual Server will use the default banner.

Insert any value that you want.

Figure 7: Enter A POP3 connection response string

Now Telnet again to the POP3 service and you will see a connection response like that.

Figure 8: Telnet to POP3 after Banner modifying

As a last step let us connect via Telnet to the Exchange 2003 IMAP4 service and you will see the following connection response.

Figure 9: Telnet to IMAP4 before Banner modifying

Please note: For security purposes the Microsoft IMAP4 service is disabled by default after Exchange 2003 installation.

For IMAP4 banner modifying we are using the IIS Metabase Explorer a second time. Navigate to the IMAP4 key and than 1 (usually) and create a new record with the details from the following picture.

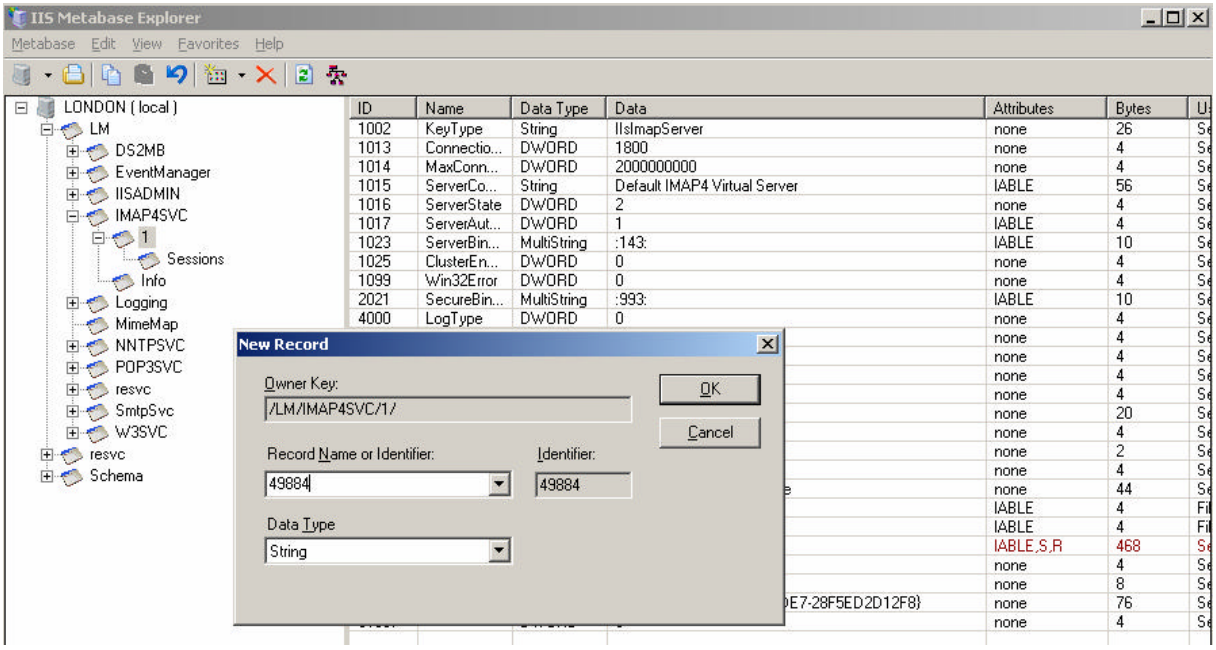


Figure 10: Use IIS Metabase Explorer to create a new IMAP4 String

Please note:

In Exchange 2000, this modification is applied to all the virtual servers on the Exchange server but in Exchange Server 2003, the modification is applied only to the virtual server that you modify (for example 1 for the first Virtual Server) If a banner is deleted from any one of the Virtual Server, the Virtual Server will use the default banner.

Insert any value that you want.

Figure 11: Enter A IMAP4 connection response string

Now Telnet again to the IMAP4 service and you will see a connection response like that.

Figure 12: Telnet to IMAP4 service after Banner modifying

Conclusion

In this article I have shown you how to change the banner for the POP3/IMAP4 and SMTP service in Exchange 2003. Changing the banner for these Exchange services enhance the security a little bit if an attacker and legitimate users doesn't know on the first try which server is communicating with them.

Related Links

How to modify the POP or IMAP banner
http://support.microsoft.com/kb/303513/en-us
How to change the default connection response that you receive after you connect to the SMTP port in Exchange 2003
http://support.microsoft.com/kb/836564/en-us
XCON: How to Modify the SMTP Banner
http://support.microsoft.com/kb/281224/en-us
IIS6 Resource Kit
http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLang=en