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 <u>article</u> about Telnet and Exchange 2003.

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

🖙 Telnet kondom.nwtrøders.mskt 220 Londom.nwtrøders.msft Microsoft ESMIP MAIL Service, Version: 6.0.3790.1830 ready at Thu, 5 Jan 2006 19:51:45 +0100 🖬

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.

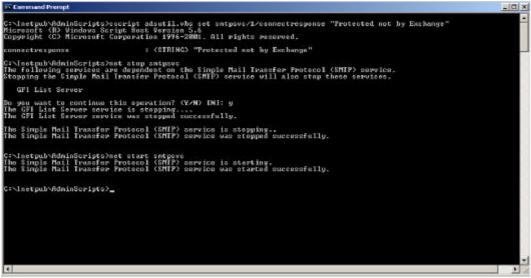


Figure 2: Executing ADSUTIL.VBS

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

```
🖎 Telnet london.nwtraders.msft
220 London.nwtraders.msft Protected not by Exchange Thu, 5 Jan 2006 20:42:21 +0100
```

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.

Exchange System Manager Be Action Ver Window Help $ \Rightarrow \Rightarrow \mathbf{e} = \mathbf{e}^{\mathbf{e}} \mathbf$			
Auchivend Traders (Exchange) Gobal Settings Gobal Settings Administrative Science Administrative Science Setting	Default SMTP Vetual Server Name Default SMTP Vetual Server General Access Messages Defivery Outcound First retry interval (minutes) Segnd retry interval (minutes) Sybsequent retry interval (minutes) Delay notifications Expiration timeout Delay golfications Expiration timeout Outpound Security Outbound gen	Maximum hop count 10 10 10 10 10 10 10 10 10 10 10 11 12 2 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 13 14 15 15 16 17 18 19 19 10 10 11 12 12 12 12 12 12 12 13 14 15 15 16 17 18 19 19 10 10 10 11 12 13	×

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.

🚾 Telnet london.n	wtraders.ms	ìt 🛛			_				_ 0	×
+OK Microsoft	Exchange	Server	2003	POP3	server	version	6.5.7623.0	(London.nwtraders.msft)	ready.	-

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 <u>here</u>. 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.

LONDON (local)	ID	Name	Data Type	Data		Attributes	Bytes	
🖕 🎻 LM	1002	КеуТуре	String	IIsPop3Server		none	26	
🗄 🤭 DS2MB	1013	Connectio	DWORD	600		none	4	
🗄 🍝 EventManager	1014	MaxConn	DWORD	200000000		none	4	
	1015	ServerCo	String	Default POP3 Virtual Ser	/er	IABLE	54	
	1016	ServerState	DWORD	2		none	4	
🗉 🧽 IMAP4SVC	1017	ServerAut	DWORD	1		IABLE	4	
🗄 🤭 Logging	1023	ServerBin	MultiString	:110:		IABLE	10	
🦳 🤭 MimeMap	1025	ClusterEn	DWORD	0		none	4	
🗄 🧒 NNTPSVC	1099	Win32Error	DWORD	0		none	4	
🖻 🍝 POP3SVC	2021	SecureBin	MultiString	:995:		IABLE	10	
Ū Ū 🏷 1	4000	LogType	DWORD	0		none	4	
Sessions	49862		DWORD	0		none	4	
	49870		DWORD	0	2232	none	4	
Info New R	ecord			>	<	none	20	
🗄 🌍 lesvc				and the second		none	2	
🕀 🤭 SmtpSvc 🛛 🛛 🗠	ner Key:			<u>o</u> k		none	4	
🛱 🐔 1/291/C	· · · · · ·					none	44	
E resvc	M/POP3SVC/1/					IABLE	4	
🖶 🐔 Schema				Cancel		IABLE	4	
Re	cord <u>N</u> ame or Ider	ntifier:	<u>I</u> dentifier	:		IABLE,S,R	468	
41	661	1	41661			none	4	
41	ooll		41661			none	8	
					5-8C582C270FC3}	none	76	
Da	ta <u>T</u> ype					none	4	
Str	ing		-					

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.

🔋 • 🚨 🐚 🛍 🧐 🛅 • 🗙	2 🛠							
🗉 🧾 LONDON (local)	ID	Name	Data Type	Data		Attributes	Bytes	U
🗄 🤭 LM	1002	KeyType	String	IIsImapServer		none	26	S
🗄 🦔 DS2MB	1013	Connectio	DWORD	1800		none	4	S
🗄 🍝 EventManager	1014	MaxConn	DWORD	200000000		none	4	S
	1015	ServerCo	String	Default IMAP4 Virtual Ser	ver	IABLE	56	S
🗄 🥌 IISADMIN	1016	ServerState	DWORD	2		none	4	S S S
E 🤝 IMAP4SVC	1017	ServerAut	DWORD	1		IABLE	4	S
🗎 🖗 🏷 🔟	1023	ServerBin	MultiString	:143:		IABLE	10	S
📃 🚽 🥌 Sessions	1025	ClusterEn	DWORD	0		none	4	S S S
Info	1099	Win32Error	DWORD	0		none	4	S
🗄 🤭 Logging	2021	SecureBin	MultiString	:993:		IABLE	10	S
MimeMap	4000	LogType	DWORD	0		none	4	S
	ecord			×		none	4	S S S
	ccord			<u>_</u>		none	4	S
POP3SVC	iner Key:				1	none	4	
				<u> </u>	-	none	4	S
	M/IMAP4SVC/1/					none	20	S
🗄 🧒 W3SVC				<u>C</u> ancel		none	4	S S S
🗄 🤭 resvc 🛛 🛛 🗛	ecord Name or Iden	tifier:	Identifier:			none	2	S
	-	1000	1		-	none	4	S
45	1884	-	49884		e	none	44	S
					1	IABLE	4	S S F
Da	ata <u>T</u> ype				1	IABLE	4	F
S	ring	•	1			IABLE,S,R	468	S S S S
10	10					none	4	S
						none	8	S
					E7-28F5ED2D12F8	none	76	S
						none	4	S

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.

kun Gemeral		
deres de la		
∑akue Datus		
Secure IMAP4		
E Esperido III	na -	

Figure 11: Enter A IMAP4 connection response string

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

••• Telnet london.nwtraders.msft * OK Secure IMAP4

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-4c73b628-ade629c89499&DisplayLang=en