Mail Flow Tester

Developed by Andrew Stobart

Description

This application is used to send test messages via SMTP. Sending test messages through Telnet can be tedious and slow, and this application can replace the manual typing of SMTP commands.

This application also contains quick options like sending a Gtube string or an EICAR attachment.

Where to get

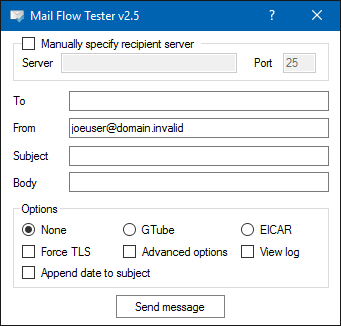
https://github.com/SeriousSneak/Mail-Flow-Tester

Where you would use it

* You need to spoof a sender
* You need to send a message directly to an end point and do not want to perform an MX lookup on the recipient domain
* You need to quickly send a Gtube String, EICAR attachment, or Force TLS

Usage

Compact (default) view:



Manually specify receiving server

Checking off "Manually specify receiving server"

* This is useful if you do not want to send a message to the MX value listed for the recipient domain (ie. You want to test mail through O365, but the customer has not yet changed their MX record.

Not checking off "Manually specify receiving server"

* The application will attempt an MX lookup on the recipient domain. If the lookup is successful, the message will be sent to the address listed in the MX for the domain. This address will appear in the Server test box and in the popup success window.

Machine generated alternative text:
Manually specify receiving server 
Server mx2hotmaiI com 

Machine generated alternative text:
Sweet! 
The message was sent to mx2.hotmaiI.com. 

Options

Gtube

* Selecting this will automatically enter the Gtube string (XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL\*C.34X) for the body of the message

C:\Users\astobart\AppData\Local\Temp\msohtmlclip1\02\clip_image004.png

* GTUBE (Generic Test for Unsolicited Bulk Email) is a string which will cause most anti-spam systems to mark the message as spam. EOP will mark messages with this string as High Confidence Spam and stamp SCL:9 in the header. See <https://en.wikipedia.org/wiki/GTUBE>.

EICAR

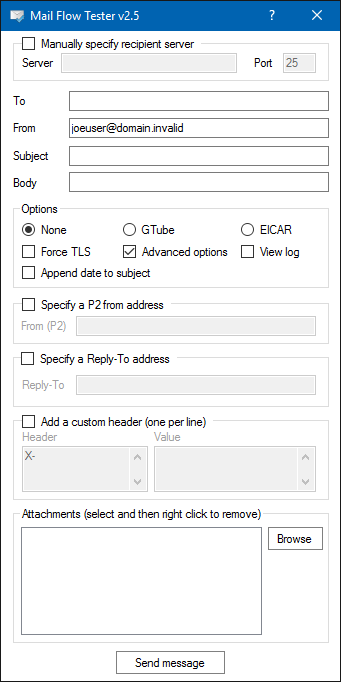
* Selecting this option will cause an attachment, eicar.txt, to be attached to the sent message. This TXT file will contain the EICAR string
* This test file will cause most malware systems to detect malware, this includes the malware systems used by EOP. This is meant to test antimalware systems

Force TLS

* When selected, the application will force TLS on the sent message
* If not selected, a message will be sent in the clear. A network trace will show you all the SMTP commands.
  + Machine generated alternative text:
    Stream Content 
    220 COL004-Mc1F38. hotmail.com sending unsolicited commercial or bulk e-mail to 
    Microsoft's computer network is prohi bited. other restrictions are found at http. 
    privacy. mi crosoft. com/en-us/anti-spam. mspx. Thu, 27 Aug 2015 07 : 17 :45 -0700 
    EHLO Dr evzenbook 
    250-COL004-MCIF38. hotmail.com (3. 21.0. 208) Hello L167.220. 24. 221 J 
    250-SIZE 36909875 
    250-PIPELINING 
    8bitmi me 
    250- 
    250-BINARWIME 
    250-CHUNKING 
    250-STARTTLS 
    250-AUTH LOGIN 
    2 SO-AUTH—LOGIN 
    250 0K 
    MAIL FROM invalid:- 
    250 joeuseradomain. invalid. 
    . sender 0K 
    •aoutlook. com:- 
    RCPT TO: 
    look. com 
    250 
    DATA 
    354 start mail input; end with .:CRLF:-. -zCRLF:- 
    Message-ID: e:f6f5791a-a420-4831-a518-1bd5f866d53bamft. local:- 
    MIME-version: 1.0 
    From: joeuseradomain. invalid 
    To: andr ew. stobartaoutlook. com 
    Date: 27 Aug 2015 -0500 
    subject: Not using TLS 
    content-Type: text/plain; charset—us-ascii 
    content-Transfer-Encoding: quoted-pri ntable 
    This message was sent not using TLS. 

Advanced Options

* This will cause more options to be revealed. The application will look as follows when this has been selected.



* Specify a different P2 header
  + This is the 5322.From header and is what will show up in Outlook. The 5321.MailFrom header is what is specified at the top of the application in the From field.
  + For more information on 5322.From and 5321.MailFrom, see <http://blogs.technet.com/b/eopfieldnotes/archive/2015/02/26/using-dmarc-to-prevent-spoofing.aspx>.

* Specify a Reply-To address
  + If set, when the recipient replies to the message, the reply will be sent to the address specified in the Reply-To header.

* Add a custom header (one per line)
  + Allows you to stamp your own X headers in the sent message. This is great for testing TransportRules that trigger on an email header
* Attachments
  + You can attach files to the sent message

View Log

* This is a log of all messages that have been sent from the application since it was launched

Machine generated alternative text:
Mail Flow Tester v2.3 
Manually specify receiving server 
Server mxl mm ail com 
Date 
9/1/2015 15:43 
9/1/2015 15:43 14 
Subject 
Test 
Test 
Test 
Options 
Result 
Success 
Success 
Success 
mx2 hotmail 
mx2 hotmail 
mxl hotmail 
From 
utlook com 
Oeuser@dom ain win valid 
joeuser@domainwinvalid 
joeuser@domainwinvalid 
joeuser@domainwinvalid 
com 
com 
C) G Tube 
@ EICAR 
C) None 
n Force TLS 
Advanced options View log 
Send message 

* This view also allows you to see the MessageID for the sent message

Machine generated alternative text:
Subject 
Options 
Resutt 
Success 
Success 
Success 
mx2 hotmail com 
mx2 hotmail com 
mxl hotmail com 
Message-I D 
G3371e5b-73S5-4c3e-S1b8-70Ed72bab7d4@mft10cab 

* Using the button "Export log," the entries can be exported to a .CSV file
* You can use the "Clear log" button to clear the full log, or by right clicking you can clear a single line or copy a single cell

Machine generated alternative text:
mx3 hotmail com 
Message-ID 
Copy cell 
Delete rcw 