Global Information Assurance Certification Paper

SANS GSEC Certification
Level 1 GSEC
SANS Security Essentials

MIMEsweeper: Increase your Lotus Notes email security

GSEC Practical Assignment Version 1.2b

Christopher T. Lauer
April 17th, 2001

Introduction

Lotus Notes is a database groupware product that also provides email functionality. It has been in existence for a little over a decade now. Lotus Notes provides authentication, access control lists, and can even use message encryption in order to help provide a secure email-messaging environment. However, there is a significant security threat that exists outside the realm of these built in security measures.

The threat is the email virus. Email viruses are on the rise and come in the form of message attachments. The attachment is usually given a name that will gain the user's curiosity. If the user launches the attachment, the virus may load and negative consequences can result. The extent of these consequences can vary from annoyance, to your computer being rendered useless. Some examples of these are the Melissa virus, Lovebug virus, and recently the W32.Matcher virus. Of course, a vulnerability exists due to the presence these types of threats. Now that we've identified the threats, lets find out how to guard against them.

Recommendation

MIMEsweeper is a software package that can help protect your Notes environment from the threat of email viruses. It is a product of Content Technologies and has been in existence for almost six years now. It offers a policy-based solution that protects your email application against undesirable attachments. It can be configured to block the attachment types that you don't want circulated, or that you want to manually verify before the message is delivered. Spam blocking, message size management, the addition of legal disclaimers to messages, keyword search, and email sender controls are other features that are provided by MIMEsweeper. However, the focus of this paper will be on its virus protection capabilities.

Email scanning: How does it work?

MIMEsweeper for Lotus Notes provides scanning protection for both inbound, and outbound, email. This scanning, and analysis, is completed through four stages. These are "Policy Identification", "Content Disassembly", "Content Analysis", and "Classification". Below is a brief description of each stage.

Policy Identification

Developing a policy is an essential part of utilizing MIMEsweeper. This sounds complicated, and may be undesirable to many system administrators. The tendency for many is to immediately install the software and start playing with the configuration parameters. Don't go this route! Take the time in the beginning to develop, and document, a policy. There is an "easy to follow" guide at the MIMEsweeper web site. This is an excellent way to develop, and document, your policy. It addresses detecting attachment types, legal disclaimers, virus scanning, text analysis, and many more aspects of protecting your email environment. The guide is a "check list" type document. It can be found at:
http://www.MIMEsweeper.com/products/collateral/pdfs/whitepapers/policyguide.pdf

Your policy "rules" will be applied to each email message. The policy actions can vary depending on the message sender, and the message recipient. In the end, you will have a much greater comprehension of the product by investing the time to generate a good policy.

Content Disassembly

The next stage in email scanning is content disassembly and identification. Each email message is broken down into its component parts. This is accomplished through a recursive algorithm. The recursive disassembly ensures that all the data is validated, even if the information is compressed, encoded, nested, or incorporates a variety of these techniques. MIMEsweeper extracts, and processes, each file until it is recognized as a raw data type. Some of these raw data are text files, bitmaps, binary files and application executables. MIMEsweeper also detects custom file formats by using a flexible binary pattern-matching algorithm.

Content Analysis

Analysis of the email messages is next. This stage applies the established policy "rules" to various actions that are taken against messages. The "content analysis" stage takes care of detecting malicious code, cleaning infected messages, detection of spam, management of messages based on attachment type, management of messages based on size, message text analysis, and attaching legal disclaimers to email messages. Mimeweeper uses plug-in validators to check the content of each data component generated during the "content analysis" stage. The validators currently used are `VALEXE`, `VALATTR`, `VALLEX`, and `VALHTML`. The `VALEXE` validator provides a link to third party applications, such as anti-virus tools. MIMEsweeper supports a variety of anti-virus tools. Both Norton anti-virus and McAfee anti-virus software work well with MIMEsweeper. `VALATTR` is an attribute validator used to determine the data type of a message component. The `VALLEX` validator performs lexical analysis to scan, or search, the data component for keywords or phrases. `VALHTML` is an HTML validator. It is used to search HTML formatted message for threats. These threats can exist within the email message itself, or in the form of an HTML attachment.

A validator response is generated after each message component is checked. This response will determine the message classification for Minesweeper. As you can see, the "content analysis" stage is responsible for much of what MAILsweeper does to protect, and manage, Lotus Notes email.

Classification

The final stage is "Classification". This stage is responsible for selecting the disposal path for each message. This selection is based on the validator response that is generated in the "content analysis" stage. Each disposal path is made up of disposal actions. The following is a list of the disposal actions:

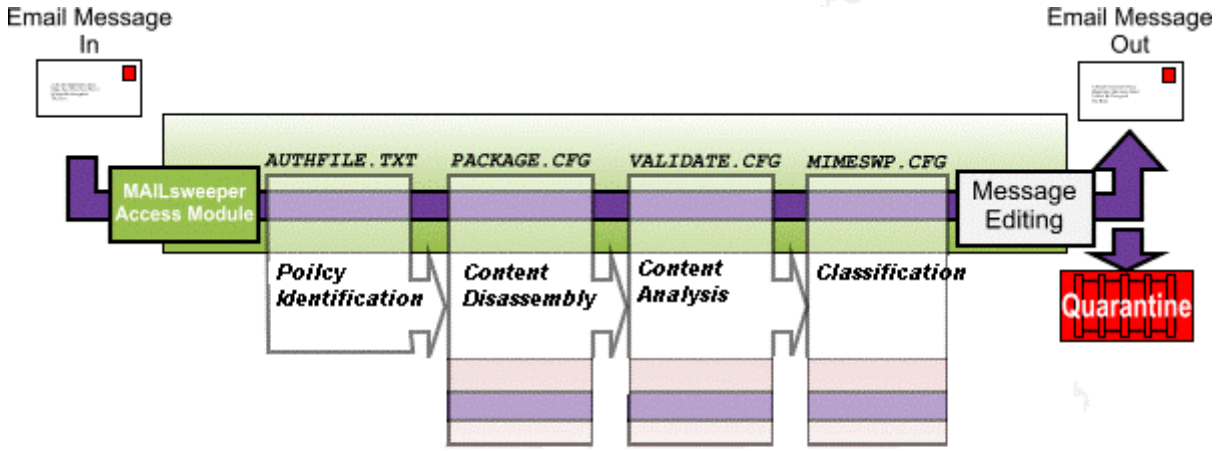
Deliver – The message is delivered to the designated recipient.

Quarantine – The message not delivered, but is placed in the appropriate quarantine area. This is done so that the MIMEsweeper administrator can examine it and determine what further appropriate action should be taken.

Inform – A message is generated and sent to a user(s) to make them aware of quarantined message. This message informs the user why an email message has been quarantined. The user is usually the MIMEsweeper administrator, but can also be the sender and/or the recipient.
Edit – The email message is held temporarily. Text is inserted, such as a disclaimer, and the message is then delivered to the intended recipient.
Save – This action saves a copy of the email message for review.
Event – Allows an entry to added to the Windows NT event log.
Trap – Generates, and sends, a SNMP trap message to the SNMP administrator.

Summary of Email scanning

By now, it should be clear how the four stages take care of the MIMEsweeper scanning process. The below graphic shows this process, and the files associated each stage.



Each stage is necessary, and basically flows in the order that they were discussed. Also, you can now see the necessity of developing a well-documented policy. It is the foundation on which MIMEsweeper operates. Now that we know it works, lets look at implementing MIMEsweeper.

Implementing MIMEsweeper

This section will cover implementing MIMEsweeper. First lets look as the hardware, and software, requirements to complete this task.

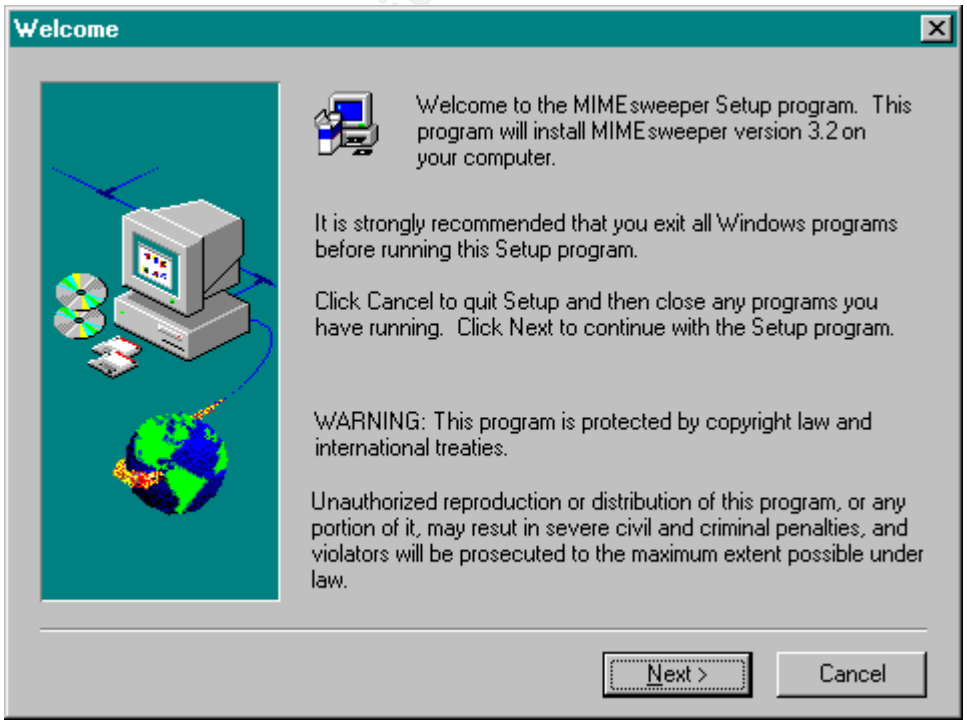
MIMEsweeper must reside on the Lotus Notes server. The server should meet all of the hardware requirements that are recommended by Lotus. This information can be found at: http://www.lotus.com/home.nsf/welcome/dominomailserver. This paper will assume that you already have a Lotus Notes server, and that it meets the Lotus hardware requirements. In addition, MIMEsweeper will need 500 MB of hard disk space.

Now lets look at the software requirements. The Notes mail server must be running Domino version R5 (5.02b), or Domino version R4 (4.51 to 4.6). The operating system must be Microsoft Windows NT Workstation, or NT Server, version 4.0 with service pack 5. The TCP/IP protocol must be configured, and the RPC service available. You will also need a third party anti-virus software tool. McAfee virusscan is used in my organization, and it has worked well. MIMEsweeper supports several major anti-virus tools. A complete list can be found in the MIMEsweeper administrator's guide. Command line anti-virus tools should be installed before MIMEsweeper is installed. DLL based anti-virus tools are installed after the MIMEsweeper installation.

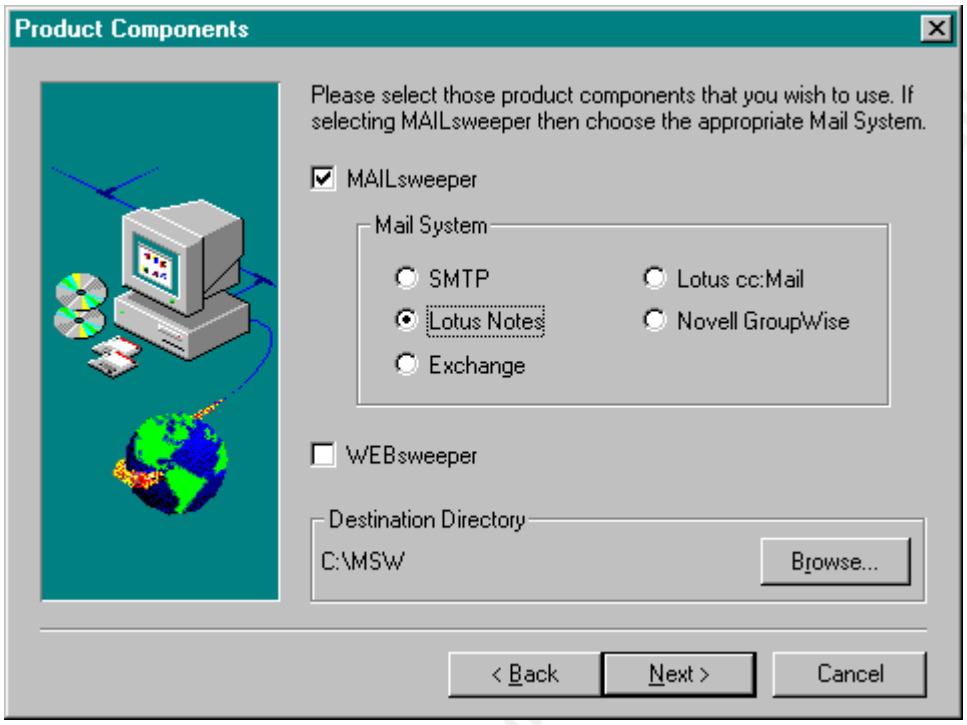
There are a few things that need to be done before you install MIMEsweeper. First, you need to identify the Lotus Notes users that will be receiving the MIMEsweeper notification messages. Now the Lotus Notes administrator will need to create a group called GROUP_TOOLS_ADMIN in the address book on the server. The previously identified users now should added to this group. Next, the Notes administrator needs to create a new Notes user. The user should be named MAILsweeper. Some MIMEsweeper notifications will appear to come from this new user. Finally, you should make backup copies of the LOG.NTF, and MAILBOX.NTF files. MIMEsweeper updates these design template files with new designs for its own use. These files should be located in the Notes/Data folder on your Notes server. This step is taken as precautionary measure.

Now, we can install the MIMEsweeper software. A Windows NT user that has write access to the registry should install the software. Preferably a user that is in the Administrator's group. First, you will need to stop the Lotus Notes server and client processes. Also, exit any other programs that are running. Put the MIMEsweeper installation CD-ROM into the CD tray. Run the program called SETUP.EXE located on the CD-ROM.

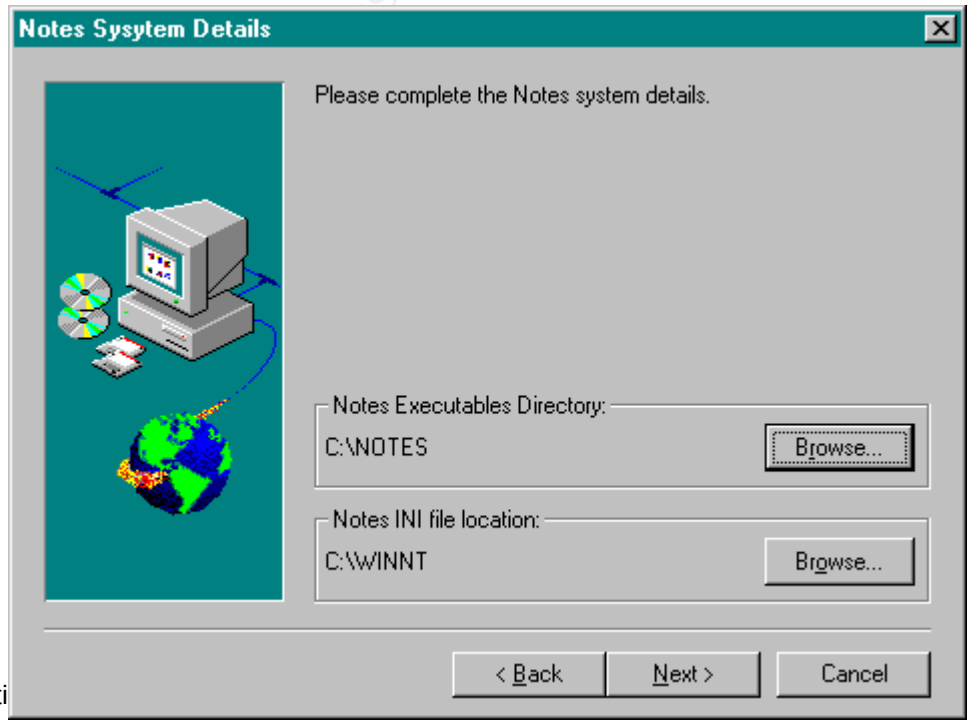
The first dialog popup window is will be the "Welcome" box. Read this and click on the "Next" button.



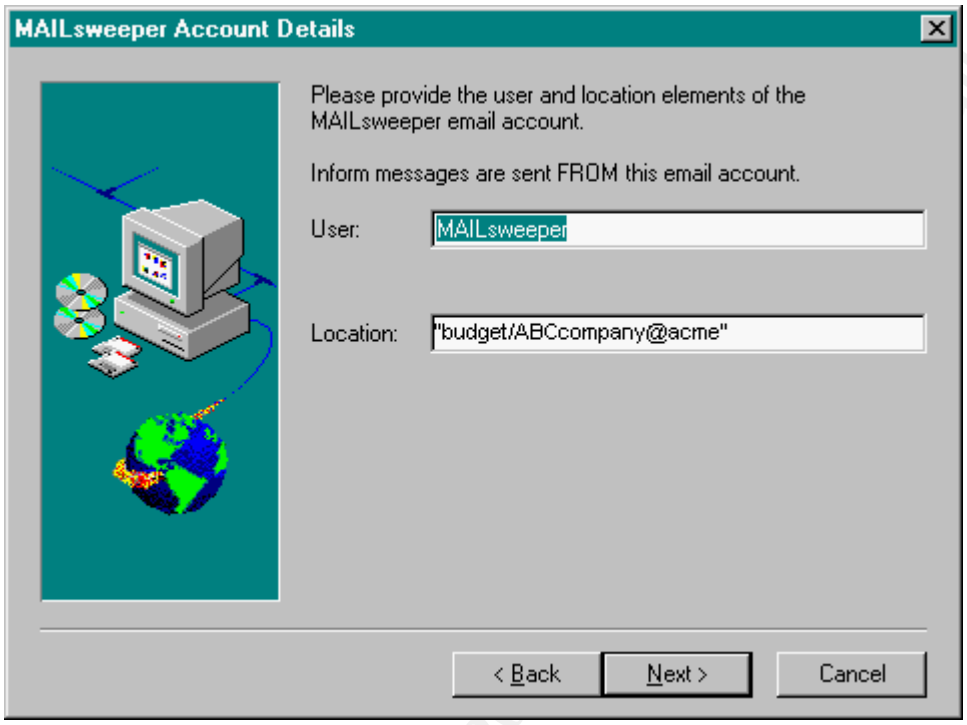
The next screen will display the "Product Components" popup. Select the "MAILsweeper" option, and then the "Lotus Notes" option. The destination directory is also selected here. I recommend that you install the software on a different disk partition then the Windows NT operating system has been installed. Now click on the "Next" button.



The next popup will ask you to specify the location of the Lotus Notes executables directory and the location of the Notes.ini file. Do this and then click on "Next".

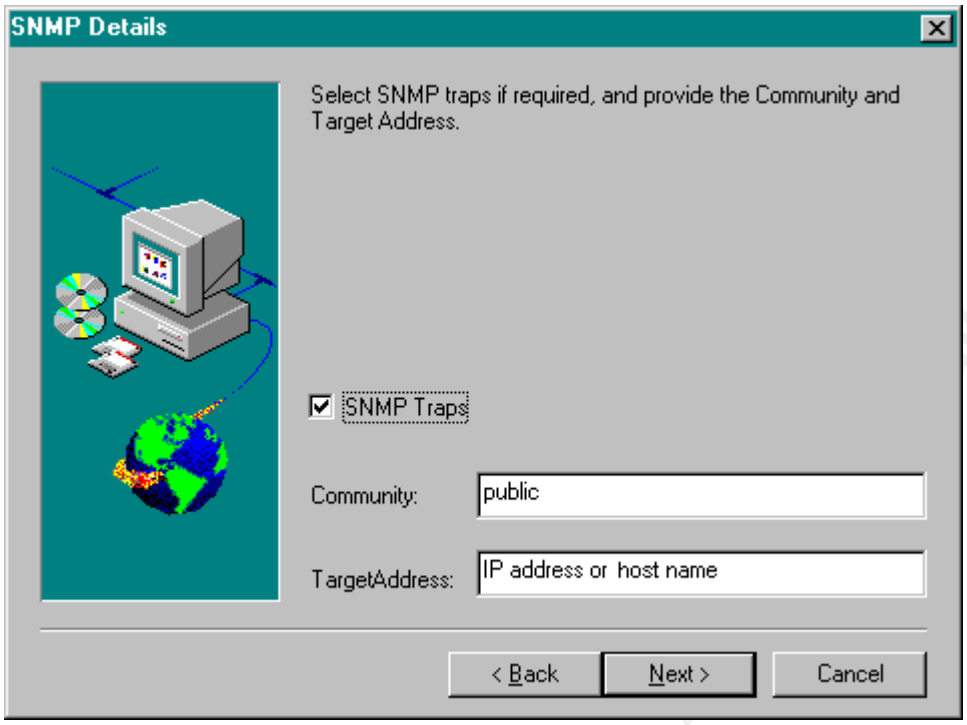


You will now be prompted for MAILsweeper email account information. This specifies where inform messages are sent from. Please keep in mind that this user account must already exist. Enter the user name "MAILsweeper" in the user field. Now enter the "Location" information in the location field. This value should be in the format "OrganizationUnit/Organization@Domain". For example, "budget/ABCcompany@acme". Click on "Next".

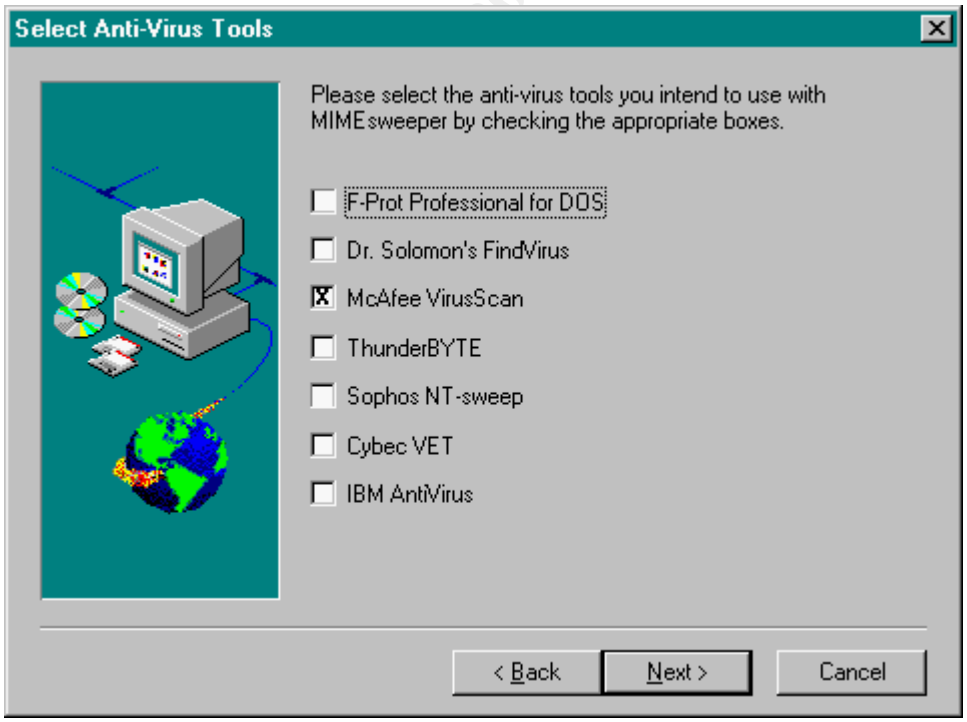


Similarly, you are now prompted for the MAILsweeper administrator email account information. This specifies where inform messages are sent to. Enter the group name GROUP_TOOLS_ADMIN in the user field. This group must also already exist. Enter the location information for the group as described in the previous step for the MAILsweeper account information. Click on the "Next" button.

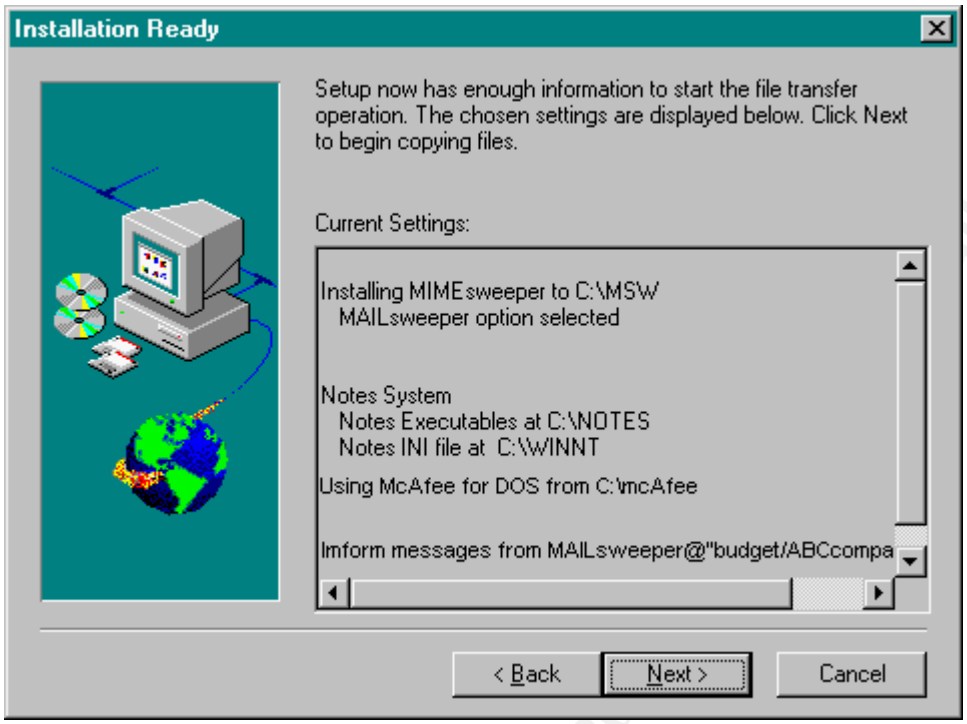
The SNMP details screen is next. MAILsweeper is capable of generating SNMP traps at startup and shutdown. If SNMP traps are required you can enable them here by checking the "SNMP Traps" option. Now enter the SNMP community name as used by the SNMP manager. The default value for this field is "public". Next, the target address must be entered. This is the IP address, or host name, of the SNMP manager. Click on "Next".



You will now see the "Select Anti-Virus Tools" box. Select the anti-virus tool that you wish to use with MAILsweeper. Next, you will be prompted to enter the location of the directory for the anti-virus tool. You may also be prompted for the version type. For example, Windows NT or DOS. Click on the "Next" button.



The "Installation Ready" box will now appear.



The information, and options, that you entered is displayed in the popup. Please review the information and ensure that is correct. Use the "Back" button to make any necessary changes. You can click on "Next" once you have finished verifying this information. Files will be now be transferred from the CD-ROM and a program group is created. The license key may be entered at the completion of this process by checking the "set MIMEsweeper license key" box. This must be done before clicking the "Finish" button. You have now completed the installation and can restart the server. This will start the MAILsweeper service that has been added to Windows NT.

MIMEsweepers configuration

MIMEsweeper is now installed and running with a default configuration. This will provide extensive protection from viruses. The program can be run without any further configuration. However, you should tailor it to meet the needs of your specific security policy. The policy guide, mentioned previously, is a great tool in helping to accomplish this task. Specific instructions for changing the configuration can be found in the MIMEsweeper Administrator's Guide. The following are some of the areas, and features, that can be configured within MIMEsweeper.

Email access
Post office locations.
Preventing spam and spoofed mail.

User Authorization
Configuring AMUchecks to control user and location access rights. Creating attributes that can subsequently be used during processing. For example, an attribute to give the message a sense of direction.

Content Disassembly
Adding new container handlers, as they become available.

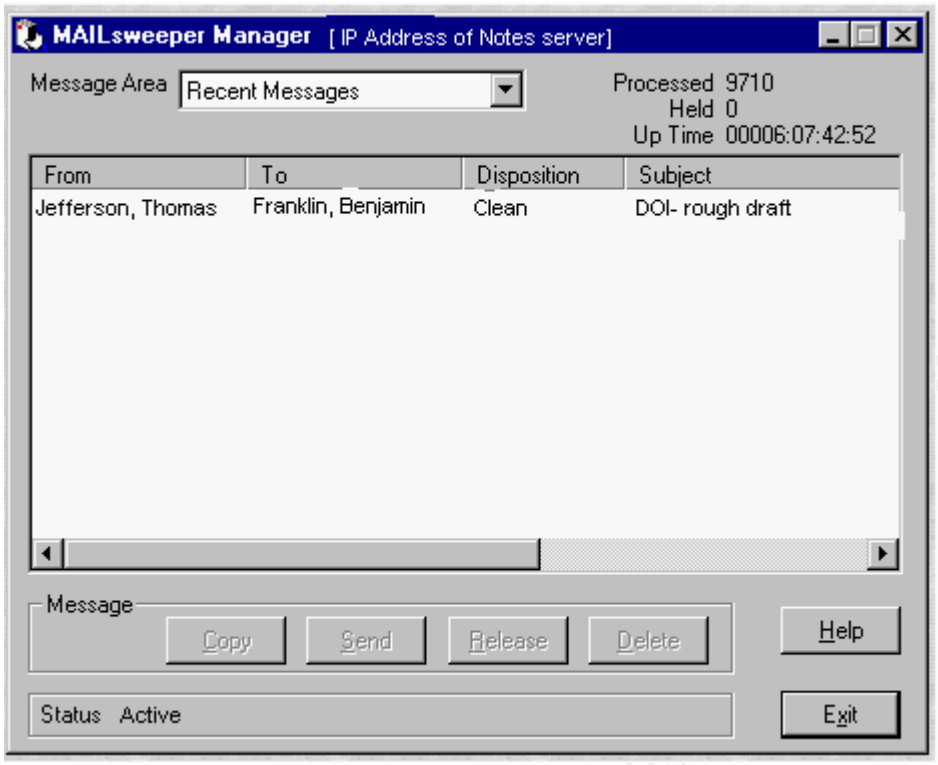
Content Analysis
Adding third party validator instances, for example, anti-virus tools.
Using or creating attributes to control the validation process.
Configuring of lexical analysis (LEX) to check for keywords or phrases.
Blocking unsafe HTML and Java applets.

Classification
Creating new disposal routes for messages.
Determining priorities for validation results.
Setting inform lists for notifications on actions taken.
Setting quarantine areas (up to 10), classifications and comments.
Configuring automated message editing (AME). For example, to add legal disclaimers to messages.

Miscellaneous
Setting logging levels for messages.
Saving message logs for all messages.

Using MIMEsweeper

The MIMEsweeper interface is fairly easy to use and can be installed remotely from the server. The MAILsweeper manager is a graphical interface shown below, that gives the following information:



MIMEsweeper Status – Active or Inactive.
The IP address of the Lotus Notes server.
The number of messages processed since MAILsweeper was started.
The number of messages quarantined since MAILsweeper was started.
The amount of time the MAILsweeper process has been up.
Displays the messages in each of the message quarantine areas.
Message sender
Message recipient
Message disposition
Message subject
Online help

The interface allows you to copy, send, release, or delete messages from the quarantine areas. These actions are taken after the administrator has examined the quarantined message.

The administrator will also received "inform" email messages from MAILsweeper in their Lotus Notes account. The inform messages will tell the administrator when, and where, messages have been quarantined. This will prompt the administrator to investigate the incident, and take the appropriate action via the MAILsweeper interface.

Summary

MIMEsweeper is a good security tool that is used in conjunction with Lotus Notes. It is fairly easy to install, configure, and manage. Please keep in mind that you need to update your third party anti-virus files as they are released. Also, you should periodically check the support section the MIMEsweeper web page for technical news, and updates. You can also subscribe to their free newsletters via email. I'm sure you will appreciate the protection that MIMEsweeper provides, and find it invaluable as part of your organization's security plan.

References:

Symantec Corporation. "The Symantec Anti-Virus Research Center's Online Encyclopedia".

URL: http://www.symantec.com/avcenter/vinfodb.html (May 9, 2001).

Florio, Susan. Lotus Development Corporation. "The History of Notes and Domino".

URL: http://www.notes.net/history.nsf/ (May 9, 2001).

Baltimore Technologies Corporation. "MIMEsweeper Policy Guide". November 2000.

URL: http://www.MIMEsweeper.com/products/collateral/pdfs/whitepapers/policyguide.pdf (May 9, 2001)

Baltimore Technologies Corporation. "MIMEsweeper for Domino".

URL: http://www.MIMEsweeper.com/products/dominoR5/default.asp (May 9, 2001).

Baltimore Technologies Corporation. "MIMEsweeper Technical Information".

URL: http://www.MIMEsweeper.com/products/dominoR5/techspec.asp (May 9, 2001).

Baltimore Technologies Corporation. "MIMEsweeper Support".

URL: http://www.MIMEsweeper.com/support/ (May 9, 2001).

Lotus Notes Administrator's Guide. Cambridge: Lotus Development Corporation, 1996.

MIMEsweeper Administrator's Guide. Content Technologies Limited, 1998.