Securing Exchange Server and Outlook Web Access

By Jim McBee

Excerpted from the forthcoming book "Special Ops", by Erik Pace Birkholz, Foundstone

Copyright 2003 by Syngress Publishing, all rights reserved

INTRODUCTION	
INTRODUCING EXCHANGE 2000	
Windows 2000 Dependencies Exchange 2000 Components	5 6
UNDERSTANDING THE BASIC SECURITY RISKS ASSOCIATED WITH EXCHAN	GE 2000 7
GUESS MY ACCOUNT AND UPN NAME! EXCHANGE 2000, WINDOWS 2000, AND ACTIVE DIRECTORY EXCHANGE 2000 ADMINISTRATIVE RIGHTS MAILBOX RIGHTS DENIAL OF SERVICE AND EXCHANGE Boundless E-Mail Storage The E-Mail-Based Virus Types of FILE VULNERABILITIES Information Store File Vulnerabilities Message Tracking Logs VULNERABILITY OF TRANSMITTED DATA MESSAGE AUTHENTICITY EVENT SERVICE AND EVENT SINKS	
PREVENTING EXCHANGE SECURITY PROBLEMS	
THE W2K/IIS PLATFORM MUST BE SOLID DEDICATE SERVERS TO SPECIFIC FUNCTIONS DISABLE UNNECESSARY SERVICES Unnecessary Exchange 2000 Back-End Server Services Unnecessary Exchange 2000 Front-End Server Services TIGHTENING MAILBOX SECURITY	
ENABLING SSL FOR INTERNET OR REMOTE CLIENTS	

Enabling SSL for POP3, IMAP4, or NNTP Clients	26
Enabling SSL for Outlook Web Access Clients	28
LOCKING DOWN AN IIS/OWA SERVER	30
IMPOSING LIMITS	31
Mailbox Size Limits	31
Size and Recipients Limits	32
SMTP Virtual Server Limits	33
PROTECTING CRITICAL FILES	34
NETWORK ANALYSIS RISK REDUCTION	35
DENYING CLIENT ACCESS	37
Restricting Internet Clients	37
Restricting MAPI Client Versions	38
STOPPING VIRUSES	39
Choosing the Correct Anti-Virus Solution	39
SMTP Virus Scanners and Content Inspection	39
Virus Scanning at the Desktop	40
Blocking File Attachments	40
Exchange 2000 and Firewalls	42
MAPI Clients and Firewalls	43
Accessing the Exchange 2000 Directory Service	44
Accessing the Information Store	44
Where Are My New Mail Notifications?	45
POP3, IMAP4, NNTP, and HTTP Clients	45
SMTP SECURITY	46
Restricting SMTP Relay	46
Just the Bugs, Ma'am	47
Providing Encrypted Data Streams of SMTP Traffic	48
Changing the SMTP Banner	49
Giving Away the Store	49
AUDITING FOR POSSIBLE SECURITY BREACHES	50
WINDOWS 2000 EVENT AUDITING	50
EVCHANCE 2000 EVENT AUDITING	52
LACIANCE 2000 EVENT ADDITING	52
SMTP Logaina	56
HTTP Logging	56
SECURING MAPI CULENTS	58
Message Content Vulnerabilities	58
Protecting Against Message-Based Viruses at the Client	58
ENABLING MESSAGE ENCRYPTION (S/MIME)	59
	<i></i>
FOLLOWING BEST PRACTICES	60
SECURITY CHECKLIST	61
Before Starting Exchange Review	61
Standard Exchange 2000	61
Front-End/Back-End Server Considerations	62
High Security Exchange 2000	62
Alternative Controls.	63

SUMMARY	
SOLUTIONS FAST TRACK	
Introducing Exchange 2000 Understanding the Basic Security Risks Associated with Exchange 2000	63 64
Preventing Exchange Security Problems	
Auditing for Possible Security Breaches Following Best Practices	64 64
LINKS TO SITES	
MAILING LISTS	
OTHER BOOKS OF INTEREST	65
FREQUENTLY ASKED QUESTIONS	66

Introduction

Even as recently as five years ago, many computer industry experts would never have guessed how pervasive and "business critical" electronic messaging would eventually become. The degree to which some information technology professionals are surprised by the pervasive nature of today's electronic mails systems is merely amusing to those of us that have had an e-mail address for more than 20 years.

I have been using electronic mail of one type or another since 1980 and have specialized in messaging systems since 1988, so it comes as no surprise to me the current dependency that businesses and government entities have on e-mail. However, this dependency has introduced a number of issues surrounding usage, administration, and security of e-mail.

I began working with Exchange 4.0 during the beta period in 1995; for me it was love at first sight since it introduced many features that were sorely missing from LAN-based electronic mail systems of the day. However, I suspect that for each of these new features, I have found an equal number of new headaches; yet Exchange remains my favorite Microsoft product. To this day, the product remains fairly stable and secure; there have been few bugs or security problems directly attributed to the Exchange product. Most security problems related to Exchange end up being related to the underlying operating system and services.

However, any administrator that does not understand the ramifications of certain configurations of Exchange 2000 is going to introduce potential security problems. Even experienced system administrators often overlook e-mail security issues or neglect best practices. Some administrators even procrastinate on securing their organizations because they believe in "security through obscurity." Administrators must also realize that external "hackers" are not the only source of attacks and data compromise; the 2002 "Computer Crime and Security Survey" conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad estimates that approximately 60% of security breaches occur from within an organization's network.

Security through obscurity or neglecting good security practices is no longer an option with today's email systems. Most businesses' e-mail systems contain sensitive and business critical information that must remain available and must be protected. Throughout this chapter, I am going to make a couple of assumptions with respect to the environment in which you are working. This is so that I don't address bugs and security issues that have been fixed in earlier versions of service packs. These assumptions are as follows:

Base operating system configuration is Windows 2000 Service Pack 3

Minimum Exchange configuration is Exchange 2000 Service Pack 3

Internet Explorer version is either Internet Explorer 5.5 Service Pack 2 or Internet Explorer 6.0

Your network has a firewall, and you are blocking server message block (SMB), Common Internet File System (CIFS), and NetBIOS and Windows 2000 Terminal Services ports inbound from the Internet

You have read Chapters 5 (Windows 2000 Operating System), 6 (Windows Active Directory), and 10 (Microsoft IIS) and have taken reasonable measures to secure the Windows 2000 operating system, Active Directory, and Internet Information Server. You understand that the nature of security holes is ever changing and that there may be more recent updates to the operating system, Exchange 2000, and Internet Explorer that you may need to update to fix recently discovered vulnerabilities.

This ebook includes a brief introduction to Exchange 2000, identifies some of the potential security risks associated with Exchange 2000, covers how to solve these security problems, discusses the need for auditing procedures, and wraps up with some best practices for running a secure Exchange 2000 organization. We'll focus on understanding Exchange 2000 and its dependency on the underlying operating system, Active Directory, and Internet Information Server.

Introducing Exchange 2000

Exchange 2000 is the latest iteration of Microsoft's enterprise messaging platform. However, the Exchange 2000 release contains significant changes from previous versions. Exchange 2000 is dependent on several components of Windows 2000, including Active Directory and Internet Information Services. In addition, several changes had to be included with Exchange 2000 in order to make it backwards-compatible with previous versions. Figure 1 shows a simplified view of the Exchange 2000 components and some of the Windows 2000 services that are required to run Exchange 2000.

Figure 1 Major Components of Exchange 2000 and Windows 2000 Dependencies



Windows 2000 Dependencies

Exchange 2000 is completely dependent on several components of Windows 2000. A list of services (provided here) must be running prior to the Exchange 2000 System Attendant starting.

The first of these dependencies is the Windows 2000 Active Directory. Previous versions of Exchange included a fairly sophisticated directory service; this directory service was touted by many as the crown jewel of the Exchange platform. This directory contained information about each mailbox such as the home Exchange server name, message size restrictions and storage restrictions as well as mailbox owner "white pages" information such as address, city, state and telephone number. A sometimes complex process to keep the directories between Exchange 4.0 and 5.*x* servers had to be maintained. Since Active Directory is capable of providing sophisticated directory services, the need for a separate directory is not necessary, thus Exchange 2000 uses the Windows 2000 Active Directory to store configuration information as well as information about all mailboxes and other mail-enabled objects. The Active Directory bares many resemblances to the earlier versions of the Exchange directory due in part to the fact that many of the developers were transferred to the Active Directory team. Exchange 2000 servers must maintain communication with at least one Windows 2000 domain controller and global catalog server at all times.

WARNING

Exchange 2000 will not function if it loses communication with either a domain controller and/or global catalog server. Communications with these servers must be guaranteed in order for message flow to continue.

Prior to Exchange 2000 installation, the Windows 2000 server must have the Internet Information Services (IIS) HTTP, SMTP, and NNTP components installed and running. Once Exchange 2000 is installed, these services do not necessarily need to remain running, but some services (such as Web services or message transport) will not function if they are disabled.

During Exchange 2000 installation, the SMTP and NNTP components are extended to provide additional functionality required by Exchange. Virtual HTTP directories are created to provide access to Outlook Web Access (OWA) supporting files, mailboxes, and public folders. The Exchange 2000 installation process also installs POP3 and IMAP4 services that function as part of IIS.

The IIS SMTP service is extended during the installation of Exchange 2000 to allow the service to expand distribution lists, query the Active Directory for mailbox properties, use the routing engine, and to provide Exchange-to-Exchange communication. All Exchange 2000–to–Exchange 2000 communication is handled via the SMTP engine. One of the components is called the Advanced Queuing Engine; this component processes every message that is sent on the Exchange server.

Exchange 2000 Components

Exchange Server is not a single, large program, but rather it is a number of small programs that each carry out specialized services. The Exchange installation process not only installs new services, but it extends a number of existing Windows 2000 services. Table 1 has a list of the common Exchange 2000 services, that service's executable service, and the Windows 2000 service on which this service depends.

Table 1 Exchange 2000 Services and Dependencies

Exchange 2000 Service	Windows 2000 Service Dependencies
Microsoft Exchange System Attendant	Remote Procedure Call (RPC)
(mad.exe)	Remote Procedure Call (RPC Locator)
(Mailer Administrative Daemon, in case you were	NT LM Security Support Provider
wondering)	Event Log
	Server
	Workstation
Microsoft Exchange Information Store	IIS Admin Service
(store.exe) (This service usually consumes most of the	Microsoft Exchange System Attendant
RAM in an Exchange server. This is normal.)	
Simple Mail Transport Protocol (SMTP)	IIS Admin Service
(process of inetinfo.exe, installed with Windows 2000)	
Microsoft Exchange Routing Engine	IIS Admin Service
(process of inetinfo.exe)	
Microsoft Exchange IMAP4	IIS Admin Service
(process of inetinfo.exe)	Microsoft Exchange Information Store
Microsoft Exchange POP3	IIS Admin Service
(process of inetinfo.exe)	Microsoft Exchange Information Store
Microsoft Exchange MTA Stacks	IIS Admin Service
(emsmta.exe)	Microsoft Exchange System Attendant
Network New Transport Protocol (NNTP)	IIS Admin Service
(process of inetinfo.exe, installed with Windows 2000)	
Microsoft Search	NT LM Security Support Provider
(mssearch.exe)	Remote Procedure Call (RPC)

The first Exchange 2000–specific component that starts is the *Microsoft Exchange system attendant*. The system attendant service runs a number of different processes. One of these processes is the DSAccess cache; this cache keeps information that has been recently queried from Active Directory. The default cache lifetime is five minutes. As a general rule, components such as the information store and IIS use the DSAccess cache rather than querying Active Directory over and over again; the exception to this is the SMTP Advanced Queuing Engine (AQE); the AQE queries an Active Directory global catalog server each time it processes a message. Another process is the DSProxy process; this process handles querying the Active Directory for address list information that is queried by older MAPI clients (Outlook 97 and 98). This service essentially emulates the MAPI functions that the Exchange 5.*x* directory service handled. For Outlook 2000 and later MAPI clients, the system attendant runs a

process called the NSPI (Name Service Provider Interface) or the DS Referral interface that refers the client to a global catalog server.

A third process is the Directory Service to Metabase (DS2MB) process, which is responsible for querying the Internet protocol configuration data located in the Active Directory and updating the IIS Metabase with any updated configuration information. The system attendant also runs a process called the RUS (Recipient Update Service). This process is responsible for updating Exchange properties on objects (servers, public folders, user accounts, groups, contacts) found in the Active Directory. This information includes e-mail addresses and address list membership.

WARNING

One of the more common problems with Exchange 2000 occurs when an administrator attempts to tighten security on Active Directory objects. The administrator blocks inheritance on an OU or removes the Domain Local group Exchange Enterprise Servers from the Security list.

The crown jewel of Exchange 2000 is now the *information store*. The information store service provides access to the mailbox and public folder stores for all types of clients. MAPI clients access the information store directly whereas standard Internet clients (POP3, IMAP4, NNTP) access the store through Internet Information Service (IIS). The information store service uses the ESE98 (Extensible Storage Engine) database engine to handle database file access and management of transaction logs.

Exchange 2000 includes a kernel-mode device driver called the Exchange Installable File System (ExIFS) driver. This allows properly authorized users to access messages and files in their mailbox as well as public folders via the file system.

A shared memory component called the Exchange Inter-Process Communication (ExIPC) layer provides high-speed communication and queuing between the information store and components such as SMTP, HTTP, and POP3 that operate under the Inetinfo process. The developers called the ExIPC process DLL EPOXY because it is the glue that holds the information store and IIS together.

An additional component of the information store is called the Exchange Object Linking and Embedding Database layer (ExOLEDB). This component is a server-side component that allows developers to use ADO (Active Data Objects) or CDO (Collaborative Data Objects) to access public folder and mailbox data programmatically through OLE DB. By default, ExOLEDB is only accessible locally by programs running on a specific Exchange server, however, the functionality could be wrapped into a Component Object Model (COM) component and used remotely by ASP pages or other Web applications.

Exchange 2000 still provides an X.400-compliant MTA (message transfer agent), but this component is used only if the server is communicating with X.400 messaging services or if the Exchange server is communicating with non–Exchange 2000 servers.

Νοτε

If you are interested in further reading about the Exchange 2000 architecture, consult Chapter 26 of the *Exchange 2000 Resource Kit* from Microsoft Press.

Understanding the Basic Security Risks Associated with Exchange 2000

In order to successfully harden Exchange 2000 servers against attacks on the server, it is important that you understand the potential security risks that the Exchange server may face. This includes vulnerabilities that may be exploited by an unscrupulous administrator, a member of your user community, or an external hacker. This includes threats to information that may be discerned through Active Directory, someone accessing critical database or log files, network sniffing, message forgeries,

or malicious code being installed on the Exchange 2000 server. This section of this ebook covers some of the vulnerabilities that may be found in Exchange 2000; the following section addresses how to make sure these and other weaknesses are fixed.

Perhaps one of the biggest threats to an organization's messaging infrastructure is widespread, mailbased viruses. Certainly since 1999, viruses have been the cause of most of the loss of productivity that I have seen on e-mail systems.

A seemingly benign threat to your information security is that amount of information on your network that is available to the average user. This may include log files and information in Active Directory. For example, under some circumstances, an end user can see the message tracking logs, which may include messages' subject information as well as the senders and recipients. Although this information may *seem* harmless, in the wrong hands it might be damaging. Anyone that knows anything about corporate or government espionage will tell you that you usually don't stumble across the secret plans to invade Canada, but rather you stumble across a lot of pieces to a puzzle that eventually points to the big picture. Of course, if a user stumbles across a log that indicates the CEO sent a message to the CFO with a subject of "Eyes Only: Plans for acquisition of YYY Corporation", then the subject alone is damaging.

Guess My Account and UPN Name!

Yes, that's right Chuck, it is time to play another round of "Guess that user's login name!" And the prize today is a starting point for your friendly neighborhood intruder!

All kidding aside, one of my beefs with many organizations is that they assign the user's SMTP alias to be the exact same as their Active Directory logon account name. Do you give out your social security number to strangers on the street? Why not? Because they might use that knowledge of you against you; the same can be said of an SMTP address. An e-mail address of JimM@somorita.com would tell you that my login name is probably JimM. Worse still, many organizations that are using the Active Directory User Principal Name (UPN) name are assigning the user a UPN name and SMTP address that is exactly the same. If this is the case, then you are giving the user half of the hacking equation: the user's name. I certainly hope this is the easy half of the equation, but nonetheless it is a starting point.

I strongly recommend enforcing an organizational policy that requires an Active Directory login name that does not match the SMTP address. Even better, pick something that not many people are going to know, such as the user's employee number or some other unique identifier. Never give an intruder one piece of information they could use against you.

Exchange 2000, Windows 2000, and Active Directory

I had previously mentioned in this book that Exchange 2000 is completely dependent on Active Directory. A thorough discussion of the details of Exchange 2000 and Active Directory integration could easily consume 200+ pages of this book, and that discussion would probably take you away from the reason you are reading this book, which is focusing on security and data protection. This ebook is focused entirely on security and protecting your resources, so we can avoid many of the onerous details of Windows 2000 and Active Directory integration. However, this does not relieve you of the necessity to learn as much as you can about Active Directory and how Exchange 2000 interacts with it.

One of the most important things to keep in mind is how permissions are assigned for administration of Exchange 2000 components. All permissions are assigned directly to Active Directory user accounts. This includes permissions assigned to the configuration partition of Active Directory, mailboxes, public folders, and all mail-enabled Active Directory objects (user accounts, contact objects, and groups).

One potential security hole that you should check for is a group called the "Pre-Windows 2000 Compatible Access" group found in the Active Directory Users and Computers' Builtin container. If this

group exists, it may allow anonymous users to query information about users in Active Directory, and it will allow authenticated users to query any Active Directory information about mailboxes and user accounts. Once you are sure this group is not necessary, you should remove the Everyone group from its membership list.

Exchange 2000 Administrative Rights

A fairly common vulnerability in all computer systems occurs when a junior level administrator (or even end users or the guest) is given excessive permissions. The permissions necessary for administrators to perform their daily jobs is commonly misunderstood and often configure d incorrectly. When these permissions are applied incorrectly, nearly disastrous results can occur.

Further, any of the Enterprise Admins group can alter the Exchange 2000 permissions regardless of who is actually the Exchange 2000 administrator. This is due to the default permissions that are assigned to the Active Directory configuration container that holds the Exchange 2000 configuration. Almost all of the Exchange 2000 configuration information is stored in the Active Directory database's Configuration partition. The Configuration partition (like the Schema partition) is found on *each* domain controller in the entire forest. The Configuration partition can be viewed using the ADSIEdit utility. Figure 2 shows the Microsoft Exchange container within the Services container. This is the location of almost all the configuration data for each Exchange 2000 server in the entire forest.

📮 Jim's Active Directory Config Console - [Console Root\ADSI Edit\Configuration Container [hnlex01.... 💶 🔲 🗙 强 Console 🗅 🖻 🖪 🔲 _ 8 × Window Help 🗈 🔃 🗙 😭 🕼 😫 Action View **Eavorites** 수 🔿 Tree Favorites Name Class CN=Active Directory Connecti... container 🗄 🍕 ADSI Edit ٠ CN=Somorita Surfboards Ltd. msExchOrga 🖆 📲 Configuration Container [hnlex01.somorita_hnl.com] 🗄 💼 CN=Configuration,DC=somorita hnl,DC=com 🗄 🔲 CN=DisplaySpecifiers 🗄 🧰 CN=Extended-Rights 🗄 🔲 CN=LostAndFoundConfig 🕂 🧰 CN=Partitions 🗄 🔲 CN=Physical Locations 🗄 🛄 CN=Services 🖃 🧰 CN=Microsoft Exchange 🗄 🛄 CN=Active Directory Connections Ė 🧰 CN=Somorita Surfboards Ltd 🗄 🚞 CN=Address Lists Container 🗄 🛄 CN=Addressing 🕂 🧰 CN=Administrative Groups 🖻 🔲 CN=Honolulu 🗄 🧰 CN=Advanced Security 🗄 🚞 CN=Directory Replication 🗄 🧰 CN=Folder Hierarchies 🕂 🦲 CN=Policies 🗄 🛄 CN=Routing Groups 🕂 🧰 CN=Servers 🗄 🧰 CN=San Francisco 🗄 🛄 CN=Connections 🖻 🛄 CN=Global Settings 🕂 🧰 CN=Instant Messaging • **•**| ۲

Figure 2 ADSIEdit Shows the Exchange 2000 Configuration Information in the Configuration Partition

During the first Exchange 2000 server installation or the Exchange 2000 schema preparation process, the container *CN=Services,CN=Microsoft Exchange* is created and default permissions are assigned to this container. All containers under *CN=Microsoft Exchange* will automatically inherit the permission assigned at this container or from the *CN=Services* container. A summary of these default permissions at the *CN=Microsoft Exchange* container are listed in Table 2. These permissions are inherited by the Exchange organization container and the Active Directory Connections container. During the forestprep process, the installer is prompted for a user or group to which they should assign Exchange administrator permissions. The default is the domain Administrator account.

Table 2 Default Permissions at the CN=Services, CN=Microsoft Exchange Container

Account/Group	Permissions
Administrator (the forest root domain administrator)	Full Control
Authenticated Users (only to the Exchange org object)	List Contents and Read All Properties
Domain Admins (from the forest root domain)	All permissions except Full Control and Delete All Child
	Objects
Enterprise Admins	Full Control
Exchange Domain Servers	Read

At the Exchange container level, some of the permissions that are inherited from the *CN=Microsoft Exchange* container are extended, and some new permissions are also found that are specific to Exchange 2000. Figure 3 shows the ADSIEdit Security property page for the Exchange organization; in this case, the Exchange organization is Somorita Surfboards Ltd.

Figure 3 Security on the Exchange Organization Container as Seen from ADSIEdit

CN=Somorita Surfboards Ltd Properties		<u>?</u> ×
Attributes Security		
Name Image: Administrator (SOMORITA_HNL\Administrator) Image: Administrator (SOMORITA_HNL\Administrator) Image: Administrator (SOMORITA_HNL\Domain A Image: Administrator (SOMORITA_HNL\Enterprister)		Add Remove
Permissions:	Allow	Deny
Modify public folder replica list Open mail send queue Read metabase properties Receive As Send As View information store status	\mathbf{X}	
Advanced Allow inheritable permissions from parent to propa object	agate to t	his
ОК Са	ancel	Apply

One of the things you should notice from Figure 3 is that the there are two permissions that have been explicitly denied. These are the Receive As and Send As permissions. If an administrator or user inherits these permissions, this will allow the administrator or user to open any mailbox within the organization or to send mail as any user in the organization. Therefore, these permissions are automatically blocked at the Exchange organization level, but it is possible to remove the Deny permissions. In one situation that I am aware of, an administrator accidentally gave the entire helpdesk permissions to open anyone's mailbox. Great care must be taken to ensure that these rights are not accidentally granted.

Table 3 shows the list of permissions that are either inherited or assigned by default at the Exchange organization level (e.g., *CN=Services,CN=Microsoft Exchange,CN=Somorita Surfboards Ltd*).

Table 3 Default Permissions at the Exchange Organization Container

Account/Group	Permissions
Administrator (forest root domain)	Full Control; Receive As and Send As explicitly denied
Authenticated Users	Read All Properties to the Organization object only
Domain Admins	All permissions except Full Control and Delete All Child
	Objects; Receive As and Send As explicitly blocked
Enterprise Admins	Full Control; Receive As and Send As explicitly blocked
Everyone	Create named properties in the information store,
	Create public folder
	Create top level public folder
Exchange Domain Servers	All permissions except Full Control, Write, and Delete
	All Child Objects. Receive As and Send As are allowed
	for this group.

As you can see from these permissions, members of the Enterprise Admins group can perform just about any action that they want. Since the Enterprise Admins permissions include the capability to change permissions, anyone in this group could give themselves permissions to every mailbox in the entire organization. Exchange 2000 administrators must place a lot of trust in members of the Enterprise Admins group.

Use the Delegate Control wizard on the context menu of Exchange System Manager rather than assigning the permissions manually. This ensures that the Receive As and Send As permissions are explicitly blocked, even for Exchange Administrators.

Mailbox Rights

The actual rights to access a mailbox are a little different than the rights for Active Directory objects and the Configuration container data. These rights are assigned to Active Directory security principals (user accounts and security groups), but they are actually saved to the information store where the mailbox is located. The mailbox rights can be viewed through Active Directory Users and Computers, but you must enable advanced features through the View | Advanced Features menu. Figure 4 shows the mailbox rights for a mail-enabled user account. You cannot access the mailbox rights information unless the user's information store is mounted and accessible.

Figure 4 Mailbox Rights Assigned and Inherited

Permissions for Hutchinson, Becky - Research TYS	×
Name Add	
Permissions: Allow Deny Delete mailbox storage	
OK Cancel Apply	

Notice that the rights are inherited from the Administrative group or the Exchange organization container. Also note the name SELF in the list of users assigned to the mailbox; this is the Active Directory user account. If you view the mailbox rights list and do not see anyone but the SELF account, this means that the mailbox has not yet been accessed. Once the mailbox has been accessed for the first time, the Active Directory permissions will be inherited.

Denial of Service and Exchange

Due to the fact that Exchange 2000 is completely dependent on Windows 2000 and the Active Directory, it goes without saying (yet I'm saying it anyway) that a denial of service attack that causes clients to be denied access to Windows 2000 machines or denies access to the Active Directory will negatively affect Exchange 2000. Once an Exchange 2000 server loses contact with all domain controllers and global catalog servers, it will no longer be able to route messages nor authenticate new users.

However, the biggest denials of service that I actually see in production Exchange systems come either from viruses or administrators not adequately enforcing message storage limits. Message looping or many large messages sent to a single mailbox can actually cause the Exchange server to run out of disk space and shut down.

Boundless E-Mail Storage

A number of Exchange systems becoming unresponsive or not available that I have observed over the past few years have been a result of message queues filling up with large messages, wide area network bandwidth being clogged as result of large e-mail messages, and information stores filling up their disk capacity.

This is because Exchange information stores and mail-enable users often do not have any limits on the amount of storage that they can use or the maximum messages sizes they can send and receive. This causes both transaction logs and mailbox store disks to fill to their capacity, and of course, the mailbox stores dismount and become unavailable. And this problem is not always quickly and easily solved by

the administrator since it may be difficult to free up enough space to get the mailbox store remounted and continue operation.

The E-Mail-Based Virus

Since early 1999, a category of viruses known as the e-mail-based virus has made a major nuisance of themselves. Viruses such as Melissa, ILOVEYOU, Anna Kournikova, and more have made mail administrator's lives miserable. These viruses act like worms; a user opens a message containing a script or executable , the worm examines the user's address book and the Exchange Global Address List, and sends a copy to everyone in the list. The virus could be contained in the message in the form of an attachment or embedded in an HTML formatted message.

Over the past three years, I have seen numerous enterprise-wide messaging systems that had to be shut down for days at a time. The problem becomes exponentially worse with each additional message that is opened. One environment in which I worked had a Global Address List of nearly 75,000 mailboxes. Each time one of those users opened an infected message (or opened an infected attachment), an additional 75,000 messages were sent out.

Even if only five percent of these users were unknowingly opening one of these messages, over 280,000,000 messages could be generated. This will clog up SMTP queues, gobble up WAN bandwidth, take up inbound queue disk space, generate gigabytes worth of transaction logs, and overwhelm global catalog servers. If an organization has mail-enabled contacts from customers, vendors, or other external organizations, these e-mail-based viruses will be sent to those users as well.

In my largest customers, e-mail viruses contribute to loss of service far more than server crashes, database corruption, or other hardware failures.

Types of File Vulnerabilities

Exchange 2000 has a couple of sneaky vulnerabilities that most administrators never realize: information store file vulnerabilities and message tracking logs. Both require access to either the Exchange server, the network, or to the server's backup in order to exploit. These are files in which the data can be easily viewed and possibly used to some nefarious purpose.

Information Store File Vulnerabilities

An exploit of the information store files requires physical access to the backup tapes or the server console. Exchange information stores are broken up into two separate data files. The first of these is called the MAPI store (a.k.a. the rich text store). All messages received have their message header information stored in this file; messages from MAPI have their message bodies and attachments stored in this file as well. The format of the message is called Message Database Encoding Format (MDBEF); the information is encoded and not easily readable, but not impossible to read. A creative intruder with a hex editor or database tools may able to view the data in the EDB file.

The real vulnerability is the other database file; this file is known as the streaming file or the native content store. When messages are received from SMTP clients, HTTP clients, NNTP clients, or through the file system (ExIFS), the message body and attachment is stored in this file in the exact format in which it was transmitted. This reduces the Exchange server's overhead by only converting data as necessary. This file can be retrieved into Notepad or any other text viewing program, and the entire contents can be viewed.

Message Tracking Logs

The message tracking facility allows an administrator to view which components and which servers have touched an internal e-mail message. This can be useful in locating a stalled message or determining the path that a message took to go from one Exchange server to another Exchange server in the same organization. Message tracking must be enabled for each server or via an Exchange system policy. The options on the server properties (shown in Figure 5) includes the capability to configure how long the message tracking logs are retained and whether or not the subject is included in the logs. (Enabling subject logging also allows message subjects to visible in the SMTP Queue Viewer.)

Figure 5 Configuring the Server Properties to Handle Message Tracking

HNLEX02 Properties	×
Directory Access Policies Security Monitoring Full-Text Indexing General Locales Mailbox Management Diagnostics Logging Details	
HNLEX02	
Version 6.0 (Build 6249.4: Service Pack 3)	
Enable subject logging and display	
Enable message tracking	
Log file maintenance	
Remove log files	
Remove files older than (days):	
This is a front-end server	
Clients connect here, and commands are relayed to a back-end server.	
Automatically send fatal service error information to Microsoft.	
OK Cancel Apply Help	

Although this may not seem like a big security breach, you should consider what is found in this file. First of all, the files are tab-delimited ASCII text files and are easily readable by any text editor. Second, the fields in these files includes the sender's Exchange legacy distinguished name (*/o=Somorita Surfboards/ou=Honolulu/cn=Recipients/cn=SuriyaS*), the recipient's address (SMTP, X.400, or legacy Exchange distinguished name), and, if enabled, the subject of the message. A clever person may be able to deduce a lot of information about an organization merely based on who is sending whom e-mail messages and the subjects of those messages.

NOTE

For more information on the message tracking log format and the fields found in these logs, see Microsoft Knowledge Base article Q246965.

Although there are known vulnerabilities with these log files, I still recommend that administrators turn this type of logging on. The diagnostic, historical, and usage information found in these logs can prove to be invaluable.

Vulnerability of Transmitted Data

All message systems are vulnerable to information being intercepted on the network through the use of a sniffer-type device, and Exchange 2000 is no exception. The degree of difficulty that an intruder may encounter when analyzing e-mail traffic will depend on the type of client being used. Outlook clients using MAPI over RPC transmit data in an encoded format, but (by default) not encrypted. The recipient and sender's names may be in clear text, but the message body and attachments are encoded. Only the more elite intruders would be able to make use of this encoded information.

However, Internet clients, such as POP3, IMAP4, SMTP, and NNTP, are astoundingly easy to intercept, and it is also easy to view the data. Figure 6 shows the message text from a POP3 session; the message data is clearly readable. If the message is MIME encoded, the message text is easily decoded using a Base64 encoding/decoding program. The POP3 username and password is transmitted in clear text and equally easy to read.

Micros	oft Netwo	ork N	1onil	or -	[Cap	oture	: 4 (I	lex)]													
🐺 File E	Edit Displa	ау Г	Tools	Ор	otions	Wir	ndow	He	lp													_ 8 ×
é 🔒	X	Ē	8		= -	-	<u>_</u>		ب ٠	t	Ŷ	0		14	191 (191		?					
Frame	Time		Src	MAG	C Ad	ldr	Dst	MA	C Ac	ldr	Pr	oto	col	1 I	escrip	tion						Src Otl 🔺
27	29.9627	86	PUU	00			FOCT	AL			TC	P			AP,	len:	8,	seq	: 37943287	97-379	9432880	 192.168
28	29.9728	00	LOC.	AL			PUU	00			TC	P			.A,	len:	1460,	seq	:31165697	62-311	L657122	 HNLEX02
29	29.9728	00	LOC.	AL			PUU	00			TC	P			AP,	len:	318,	seq	:31165712	22-311	1657154	 HNLEX02 -1
21		~~		~~			100	• •			-				•	•	~		000 40000	or or		الشروع ممد
												_										
⇔ Frame:	Base fi	rame	pr	oper	rtie	s																
+ETHERN:	ET: ETYI	PE =	• 0 x I	0800	D :	Prot	ocol	L =	IP:	D	OD	Int	ern	let	Protoc	ol						
♣IP: ID	= 0x45I	3;	Prot	- o	= TC	P; L	en:	150	0													
ф <u>тср:</u>	A, 1	len:	14	50,	seq	:311	6569	9762	-31	.165	712	22,	. ac	:k:3	3794328	BO5, '	win:64.	189,	src: 11	0 dst	: 1635	
1																						-
000002D0	54 6F	3A	20	22	52 7	25 73	3 73	65	6C	6C	20	45	62	72	To:	"Russ	ell Eb	r				<u> </u>
00000280	61 68	69	6D	69 :	ZZ Z	:0 30	; 5Z	45	6Z	72	61 67	68	69	6D	ahim	1" <p< td=""><td>Kbrahi ~</td><td>m</td><td></td><td></td><td></td><td></td></p<>	Kbrahi ~	m				
00000280	69 40	48	Б¥ ГО	<u>ьк</u> (68 6 72 6	50 78 20 00) 6C	75	28	53	Б.¥ ПО	6D 4C	БF П4	72	10H0	noiui	u.somo	r				
00000300	07/4	61	53 615	75 28 -	72 0 20 0	00 02	. or . no	22	52	75	73	4U 20	74	64	itas	ur ibo	"Consider	a 				
00000310	26 63	75	70	61 '	20 0 74 6	1 61	1 61	72	61	6B	75	60	22	20	Sun	ot on o	ourry.	a				
00000330	30 53	75	72	69 '	79 6	1 53	3 40	48	6F	6E	6F	6C	75	60	<sur< td=""><td>ivaSØ</td><td>Honolu</td><td>1</td><td></td><td></td><td></td><td></td></sur<>	ivaSØ	Honolu	1				
00000340	75 2E	53	6F	6D (6F 7	2 69	74	61	53	75	72	66	62	6F	u.So	morit	aSur fb	0				
00000350	61 72	64	73	4C '	74 6	54 2H	63	6F	6D	ЗE	2C	OD	0A	09	ards	Ltd.c	om>,					
00000360	22 52	65	69	64 :	20 5	53 68	69	67	65	6F	6B	61	20	2D	"Rei	d Shi	geoka	-				
00000370	20 48	4 E	4C	22 :	20 3	C 52	65	69	64	53	40	48	6F	6E	HNL	" ≤Re	idS@Ho	n				
00000380	6F 6C	75	6C	75 ;	2 E 5	3 6I	6D	6F	72	69	74	61	53	75	olul	u. Som	oritaS	u				
00000390	72 66	62	6F	61 '	72 6	54 73	8 4C	74	64	2 E	63	6F	6D	ЗE	rfbo	ardsL	td.com	.>				
00000340	OD OA	58	2D	4D (69 6	5D 65	5 4F	4C	45	ЗA	20	50	72	6F	X-	MimeO	LE: Pr	0				
000003B0	64 75	63	65	64 ;	20 4	2 79	20	4D	69	63	72	6F	73	6F	duce	d By	Micros	0				
00000300	66 74	20	45	78 (63 6	8 61	. 6E	67	65	20	56	36	2 E	30	ft E	xchan	ige V6.	0				
00000300	1 213 36	32	34	39 :	2K 3	10 UI	AU (43	63	3A AF	20	ZZ	4Z	65	.624	9.0 Name	Uc: "B	e				
00000380	68 20	53	63	68 (90	ыр 7 42 с	12 72 15 61	20	2D 40	20	45	6K 67	67	20	48	n Sc	norr	- Eng	н				_
00000380	948 4C	22	20	36 4	42 6	05 61	1 33	40	48	ъF	ьк	ъř	<i>ъ</i> С	75	ИΓ	<вens	GHONOI	u				
												TCP	pro	toco	l summary			F#: 28	3/39	Off: 3	34 (x22)	L: 20 (x14)

Figure 6 Message Text Intercepted from a POP3 Session

When using Outlook Web Access, the type of browser client you are using may even allow the username and password to be intercepted. Non–Internet Explorer clients do not support NTLM or Kerberos authentication and thus usernames and passwords are *always* exposed. However, you must use a minimum of Internet Explorer 3.01 to support NTLM authentication or a minimum of Internet Explorer 5 to support Kerberos authentication.

To avoid problems with using the OWA interface as well as to use NTLM authentication, I generally recommend the browser client be Internet Explorer 5.5 SP2 or later. Part of that recommendation is just

my Borg implants doing their job, but part of it is practical since you can use the NTLM challenge response password authentication method and you get more Outlook Web Access features.

Νοτε

Supporting non–Internet Explorer clients and older Internet Explorer clients can be a pain. Many problems are fixed by installing the latest version of the browser and applying the security updates. I recommend that browser clients be upgraded to Internet Explorer 5.5 SP2 (plus fixes) or Internet Explorer 6.0 (plus fixes) before doing any additional OWA troubleshooting.

If you are supporting non-IE clients or if your Outlook Web Access clients are connecting to an Exchange 2000 front-end server, the only method of authentication available is Basic. Although the password is not sent across the network in clear text, it is nearly so. Anyone with a network analyzer sitting in the path of that authentication packet can intercept the Base64 encoded username/password. Figure 7 shows the Microsoft Network Monitor program with the HTTP authorization header from a Basic authentication client.

Figure 7 HTTP Basic Authorization Information Encoded Using Base64 Encoding

🤗 Micros	soft Network	Monitor - [Captur	e: 3 (Detail)]				_ 8 ×
🐺 File	Edit Display	Tools Options W	/indow Help				_ 8 ×
ĉ 🛛	x 🖻 🛱		<u> </u>	9 🔗 M	1 991 991 🔲 ?		
Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description		Src Otł 🔺
19	18.376241	PUUOO	LOCAL	TCP	S., len: 0, seq:35764986	79-357649867	192.168
20	18.376241	LOCAL	PUUOO	TCP	.AS., len: 0, seq:28902971	48-289029714	HNLEX02
21	18.376241	PUUOO	LOCAL	TCP	.A, len: 0, seq:35764986	80-357649868	192.168
22	18.376241	PUUOO	LOCAL	HTTP	GET Request (from client using	port 1580)	192.168
23	18.396269	LOCAL	PUUOO	HTTP	Response (to client using port	1580)	HNLEX02
24	18.396269	PUUOO	LOCAL	HTTP	GET Request (from client using	port 1580)	192.168 🗸
•							▶
HTTP HTTP HTTP	: Request M : Uniform H : Protocol	lethod = GET lesource Ident: Version = HTT	ifier = /exchar P/1 1	nge/GRenzi			<u> </u>
HTTP	: Accept =	image/gif,	age/x-xbitmap,	image/jpec	, image/pjpeg, application/vnd.		
HTTP	: Accept-La	inguage = en-u:	5	5.51			
HTTP	: Accept-Er	coding = gzip	, deflate				
HTTP	: User-Ager	nt = Mozilla/4	.0 (compatible;	: MSIE 6.0;	Windows NT 5.1; Q312461; .NET		
HTTP	: Host = hr	lex02					
HTTP	: Connectio	n = Keep-Aliv					
arry	: Authoriza	cion = Basic (сиятралрантан	ostzayzwses	TORI3VSBGISdWx6Mg==		
•							
00000144	0 00 40 50	40 45 30 36 4	28 00 00 00 FR	CO. CR. CA. (P NOTE C.O. Ninda		
00000140	0 20 40 83	49 45 20 36 2 1 47 54 20 35 2	28 30 38 20 57	22 21 22 2	F MSIE 6.0; Windo		<u> </u>
00000160	0 36 31 38	20 28 48 45 4	54 20 43 4C 52	20 31 28 3	0 61: NET CLB 1 0		
00000170	0 216 33 37	30 35 29 0D 0	DA 48 6F 73 74	3A 20 68 6	E .3705)Host: hn		
00000180	0 6C 65 78	30 32 OD OA 4	13 6F 6E 6E 65	63 74 69 6	F lex02Connectio		
00000190	0 6E 3A 20	4B 65 65 70 2	2D 41 6C 69 76	65 OD OA 4	l n: Keep-AliveA		
000001A0	0 75 74 68	6F 72 69 7A 6	51 74 69 6F 6E	3A 20 42 6	l uthorization: Ba		
000001B	0 73 69 63	20 63 32 39 1	74 62 33 4A 70	64 47 46 6	6 sic c29tb3JpdGFf		
00000100	0 61 47 35	73 40 32 64 7	79 5A 57 35 36	61 54 6F 6	B aG5sL2dyZW56aTok		
000001D0	0 59 33 56	73 62 47 60 5	53 64 57 78 36	4D 67 3D 3	D Y3VsbG1SdWx6Mg==		
000001E0	O OD OA OD	OA					
							<u> </u>
				Identifies	the user requesting a URI (F#: 22/97	Off: 430 (x1AE)	L: 50 (x32)

It is a simple matter to take the authorization string, save it to a text file, and then run one of the many Base64 encoding/decoding programs on this file to decode the username and password. In this instance, the Base64 authorization string is *c29tb3JpdGFfaG5sL2dyZW56aTokY3VsbGlSdWx6Mg==*, this decodes to be *somorita_hnl/grenzi:\$culliRulz2*. User *GRenzi's* domain is *Somorita_HNL*, and his password is *\$culliRulz2*. A perfectly good password has been compromised.

Message Authenticity

When you receive an e-mail message from anyone, whether he is on your own network or otherwise, how do you know if your friend or co-worker was really the originator? If you received a message from your boss telling you to take the rest of the year off with pay plus a bonus, you might quickly question

the authenticity of the message. However, a simple request from your boss instructing you to e-mail an important document or file to an external address might not even raise Mr. Spock's eyebrow.

One of the problems with any SMTP-based e-mail system is that messages are fairly easily spoofed. With almost no effort, I could send a message from the boss to users in most any company in the world and tell them to take Friday off. Of course, I still need to know the names of the people to which I want to send the message.

Another one of the problems with SMTP systems is that the message is transmitted in either clear text format or as a MIME message and therefore using simple Base64 encoding. Thus, if someone with the proper software is sitting in the path of the IP datagram, she could intercept a message, modify it for her own purposes, and then forward it on to the intended recipient.

Event Service and Event Sinks

A feature that was first introduced in Exchange 5.5 was the Exchange Event Service. This service allows an administrator to run a script each time a message arrives, is deleted, or is modified, in a specified mailbox. The script can also run on a schedule. This capability allows the automation of message processing for applications such as workflow applications.

Exchange 2000 introduced additional event capabilities with store events, SMTP protocol events, and NNTP protocol events. These events allow an Exchange administrator to customize the behavior of how messages are processed in the information store and to customize how messages are handled by the Advanced Queuing Engine. You can even change the behavior of the SMTP/NNTP protocols. Although these are powerful features, they can be used for nefarious purposes. If a malicious user could get physical access to your Exchange servers even for just a few minutes, an event sink could be registered that could forward to the intruder a copy of every message sent or received by your CEO.

Message Relay via SMTP

A feature of SMTP that is both a blessing and a curse is the SMTP relay feature. Relay simply means that any SMTP message that is accepted by one SMTP server will automatically be forwarded on its destination domain by that server. Often, an organization will configure a single SMTP host (such as a firewall) to relay all inbound and outbound mail for an organization.

This feature must be carefully configure d and tightly controlled, otherwise your SMTP server may find itself forwarding mail for another organization. This happens dozens of times every day. The Exchange 5.5 Internet Mail Service, tragically, was automatically configure d as an open relay.

The Exchange 2000 SMTP Virtual Server relaying is automatically configure d as closed, but often an administrator "thinks" they need an open relay and they open the SMTP Virtual Server to the world. The only domains that any SMTP Virtual Server will accept a connection for inbound are the domains found in the Recipients Policies container. Figure 8 shows the Default Policy for an organization that accepts inbound mail for two domains: Honolulu.SomoritaSurfboardsLtd.com and Somorita.com. Additional domains can be configure d with additional recipient policies; the recipient policies are also used to determine which SMTP addresses the user community has.

Figure 8 Recipient Policies Control Which Domains Are Accepted as Inbound

Default Policy Proper	rties
Mailbox Manager General	Settings (Policy) Details Security E-Mail Addresses (Policy)
Generation rules:	
Туре	Address
I MS I smtp I SMTP I X400	SOMORITASU/HONOLULU @Honolulu.SomoritaSurfboardsLtd.com @somorita.com c=US;a= ;p=Somorita Surfboa;o=Honolulu;
New	Edit Remove Set as Primary
0K	Cancel Apply Help

Notes from the Underground...

In Search of Open Relays

Do you think you need an open SMTP relay? A surprising number of network managers think that they do due to the fact that they have POP3 or IMAP4 clients. Or perhaps another SMTP host in the organization is using that host as an SMTP relay. However, SMTP can be configure d to relay *only* for the required clients and no one else. There is *never* a valid reason to have an SMTP relay that is open to the Internet.

Right now, as you are reading this, some spammer's "bot" is scanning through all IP addresses in an IP address subnet block looking for hosts that support SMTP relay. Once they find one, they will use that SMTP host as a relay point for hundreds, thousands, or maybe even millions of spam or UCE (unsolicited commercial e-mail) messages. (For more information about spam, see www.cauce.org.)

Unfortunately, if your SMTP open relay is ever discovered, and it will be, the source IP address of those millions of spam messages is going to originate from your server. This will use your bandwidth and your server resources to deliver these messages.

An enterprising user or e-mail administrator is going to report your IP address to one or more blackhole lists. There are a number of software packages on the market that can query these black-hole lists to see if your server is on one of those lists. If your server's IP address is on that list, their server will reject inbound mail from you. This happens far too often. As a matter of fact, this is one of the top Exchange 5.5 IMS (Internet Mail Service) support issues for Microsoft PSS (Product Support Services).

For more information on black hole lists, see www.ordb.org, http://relays.osirusoft.com, and www.mail-abuse.org.

Preventing Exchange Security Problems

At long last, the moment you have been waiting for. This section includes information on how to "harden" Exchange 2000 to prevent security problems previously mentioned as well as other vulnerabilities. Most of the recommendations in this ebook should be followed completely. However, a few of the recommendations are for organizations that are concerned with extremely tight security.

Applying new security settings in a configuration for which you have not previously used them can cause you more problems. Apply new security settings incrementally and test the server's functionality before you apply additional security settings.

Larger organizations will probably want to apply security policies to servers using Active Directory Group Policy Objects rather than configuring each server's local security policy individually. I recommend creating an OU called Servers and under this OU creating a category for each type of Windows 2000 server you are managing. I create two OUs for Exchange servers (shown in Figure 9): Exchange 2000 Front-end Servers and Exchange 2000 Back-end Servers. Once these OUs are created, I can apply the policies necessary to secure these servers properly and to do it only once.

Jim's Active Directory Config Console - [Console Root\Active Directory Users and Computers [hnlex01... _ 🗆 🗡 🐕 <u>C</u>onsole 🗋 🗃 🔚 💷 _ 8 × Window Help Eavorites 🖻 📧 🗙 😭 🚺 R 🍖 🖗 🕲 🖉 🍕 🗿 Action View 수 🔿 Tree Favorites Name Excha Туре 🖳 HNLEX001 Computer 📄 Console Root HNLEX002 🚊 🐗 Active Directory Users and Computers [hnlex01.somorita] Computer HNLEX003 Computer 🖻 🚮 somorita_hnl.com SINEX001 🗄 💼 Builtin Computer 🗄 🖳 Computers SFOEX001 Computer 🗄 🧭 DLs and Local CRs SFOEX002 Computer 🧭 Domain Controllers LAXEX001 Computer 🙆 Engineering NYCEX001 Computer Empirical ForeignSecurityPrincipals NYCEX002 Computer 🗄 🕘 LostAndFound 🙆 Marketing Microsoft Exchange System Objects 🗄 🧭 Remote Mailboxes 🗄 🧭 Sales 🗄 💼 System 💼 Users 🖻 🧭 Servers 🗄 🧭 Exchange Front-End Servers 🙆 Exchange 2000 Back-End Servers 🗄 🧭 SQL and Database Servers 🗄 🙆 File and Print Servers 🗄 🧭 Web Servers 🗄 🐼 Software Distribution Servers 🗄 🧭 Home Directory and Profile Servers Þ ۲

Figure 9 Organization Exchange Servers Using Active Directory OUs

The W2K/IIS Platform Must Be Solid

As I discussed previously, Exchange 2000 is dependent on the Windows 2000 operating system, Internet Information Server, and Active Directory. Consequently, Exchange is only as secure as the platform on which it is running. This means that you must harden the Windows 2000 and Internet Information Server environment.

First and foremost on the agenda for hardening Exchange 2000 is to make sure that all Windows 2000, Internet Information Server, and Internet Explorer service packs and security hot fixes are applied.

Next, consider locking down some potentially unnecessary services and ports. This means removing any services that are not absolutely necessary for the operation of Exchange 2000. Remove unnecessary protocols and network drivers (such as the Network Monitor Driver) if installed. On the TCP/IP properties of each network adapter, disable NetBIOS over TCP/IP (as shown in Figure 10). There is no reason for file and print services clients to be connecting to the Exchange server using NetBIOS.

Figure 10 Disable NetBIOS over TCP/IP for All Exchange Server Network Adapters

Advanced TCP/IP Settings	<u>? ×</u>
IP Settings DNS WINS Options	
WINS addresses, in order of use:	
192.168.254.55 192.168.240.23	Ŷ
	Ŷ
Add Edit	Remove
	·
If LMHOSTS lookup is enabled, it applies to a TCP/IP is enabled	Il connections for which
Enable LMHOSTS lookup	Import LMHOSTS
C Enable NetBIOS over TCP/IP	
Disable NetBIOS over TCP/IP	
O Use NetBIOS setting from the DHCP server	er
	OK Cancel

Next, get the Exchange Server up to the very latest patches and security fixes. Although there are usually not many security fixes for Exchange 2000, when one is released it is usually patching a known vulnerability. You can bet that many potential intruders know about the vulnerability before Microsoft does.

Tools & Traps...

The Human Touch

Many of the problems I see with e-mail-related security systems have nothing to do with how well secured the system actually is, but they are symptoms of a poorly trained user community. Anyone that has worked in a military environment can tell you how much hassle is involved when a user accidentally transmits a piece of classified material over an unclassified network. This regularly happens with unclassified e-mail systems.

Another common problem with e-mail systems is that users accidentally send sensitive messages outside of the organization or to internal users that should not see that information. Even implementing content inspection systems such as Clearswift's MailSweeper (www.mimesweeper.com) or GFI's MailSecurity for Exchange/SMTP (www.gfi.com) cannot consistently prevent sensitive information from leaving an organization.

Since the some of the security problems lay with what some call Layer 8 (the Bozone layer), good user education programs and policies should always be in place.

Dedicate Servers to Specific Functions

Whenever possible, dedicate servers to a specific task. This is not always possible in smaller organizations, but in a larger organization, I recommend breaking up servers into specific types of servers. This allows you to enable the maximum possible security configuration for that particular server role without worrying about breaking another service that may require a slightly less secure configuration. Some of the roles that I recommend include the following:

Mailbox servers (back-end)

Public folder servers (back-end)

OWA, POP3, and IMAP4 servers (front-end)

Communications/bridgehead servers, such as SMTP Connectors, faxing, pager gateways (front-end)

Disable Unnecessary Services

Disabling unnecessary services may seem like an obvious recommendation, but it is nonetheless often overlooked. And often Exchange administrators do not realize when they can disable a specific service. Windows 2000 and Exchange 2000 install a number of services that may not be necessary in your environment. Although most of these services are fairly innocuous, I still think it is a good practice to disable these if they are not necessary. I have broken this up into two types of Exchange servers: front-end servers and back-end servers.

For both of these types of servers, using the Services management console, disable the service rather than simply setting the service to Manual since another service may try to start this service.

If the Exchange 2000 server is running in a native Exchange 2000 organization (no Exchange 5.5 servers), you should switch the organization to "native" mode. This is done on the properties of the Exchange organization using Exchange System Manager. Before you can switch the organization to native mode, you should disable the Microsoft Exchange Site Replication Service and the Active Directory Connector. Any configure d Site Replication Services should be deleted from Tools | Site Replication Services container in Exchange System Manager.

Unnecessary Exchange 2000 Back-End Server Services

Exchange 2000 back-end servers are servers on which mailboxes and public folders resides. By default, Exchange 2000 servers are back-end servers unless a server is reconfigure d as a front-end

server. Mailboxes stored on front-end servers are not accessible. Table 4 shows a list of services that you may be able to disable on Exchange 2000 back-end servers.

Table 4 Windows and Exchange 2000 Services That Might Not Be Necessary on Back-End Servers

Service	Conditions under which it can be disabled
Computer Browser	Disable if you do not want this computer to participate in browsing
	functions or appear in the Network Neighborhood.
Distributed File System	Disable if this server does not have any DFS shared resources.
Indexing Service	Disable if this server does not need a service to provide full-text
	indexing of Web page content.
Microsoft Exchange Event	Disable if there are no Exchange 5.5–compatible event scripts
	that must be executed. If you have no Exchange 5.5 event
	scripts, you are better off removing this service.
Microsoft Exchange IMAP4	Disable if you have no IMAP4 clients.
Microsoft Exchange MTA Stacks	Disable if you have no Exchange 5.5 servers and/or X.400
	Connectors using this server as a bridgehead.
Microsoft Exchange POP3	Disable if you have no POP3 clients.
Microsoft Exchange Site Replication Service	Disable if you have no Exchange 5.5 servers in your organization.
Microsoft Search	Disable if you do not wish to do full-text indexing of mailbox and
	public folder stores.
Network News Transport Protocol (NNTP)	Disable if you have no NNTP clients or NNTP news feeds
	connected to this server.
Telnet	This service should always be disabled. Use SSH or Terminal
	Services if you need remote administration abilities.
World Wide Web Publishing Service	Disable only if you do not want to provide access to this server
	via OWA and you do not want to manage public folders on this
	server.

This is not an "all inclusive" list, but it serves as a good guideline. If the service is not installed as part of a Windows 2000 default installation, it does not need to be installed to run Exchange 2000. The exception to this rule is the NNTP Service; however during the installation of NNTP, administrators often install the FTP Publishing Service. FTP is not required on Exchange 2000 servers; it should be removed. I also did not include in the above list the Exchange 2000 foreign mail system connectors such as Microsoft Mail, cc:Mail, and Notes/Domino. If you are not connecting to these systems, remove these connectors.

Unnecessary Exchange 2000 Front-End Server Services

Exchange 2000 front-end servers were introduced with Exchange 2000. The front-end server allows you to place an Exchange 2000 server in a DMZ, or even (gasp!) outside a firewall, and direct OWA, HTTP, POP3, IMAP4, NNTP, and SMTP clients to this server. For mail and news clients, the front-end server will connect to the back-end server on behalf of the client and retrieve their mail or news. However, MAPI clients are not able to connect to a front-end server.

Once the server is configure d as a front-end server, it is no longer necessary to run many of the services that a back-end server requires. This usually includes the information store. The exception to this is when the front-end server is also routing inbound or outbound SMTP mail, in which case the default mailbox store must remain mounted. Table 5 includes a list of services that you may be able to disable on front-end servers.

Table 5 Windows and Exchange 2000 Services That Might Not Be Necessary on Front-End Servers

Service

Conditions under which it can be disabled

Computer Browser	Disable if you do not want this computer to participate in browsing functions or appear in the Network
	Neighborhood.
Distributed File System	Disable if this server does not have any DFS shared
	resources.
Indexing Service	Disable if this server does not need a service to provide
	full-text indexing of Web page content.
Microsoft Exchange Event	Disable.
Microsoft Exchange IMAP4	Disable if you have no IMAP4 clients.
Microsoft Exchange Information Store	Disable if this server is not hosting inbound or outbound SMTP or X.400 connections. The default mailbox store must remain mounted if this server is hosting SMTP virtual servers or X.400 connectors.
Microsoft Exchange Management	Disable if this server is not hosting inbound or outbound SMTP or X.400 connections. This disables remote query of message tracking logs.
Microsoft Exchange MTA Stacks	Disable if this server is hosting no X.400 connectors.
Microsoft Exchange POP3	Disable if you have no POP3 clients.
Microsoft Exchange Routing Engine	Disable if this server does not support SMTP virtual servers.
Microsoft Exchange Site Replication Service	Disable.
Microsoft Exchange System Attendant	Disable if you do not want to make any configuration changes to this server. It will need to be re-enabled anytime a virtual server configuration change is made that affects this server. You cannot disable this service if the information store is enabled.
Microsoft Search	Disable.
Network News Transport Protocol (NNTP)	Disable if you have no NNTP clients or NNTP news feeds connected to this server.
Simple Mail Transport Protocol (SMTP)	Disable if this front-end server does not host SMTP virtual servers.
Telnet	This service should always be disabled. Use SSH or Terminal Services if you need remote administration abilities.
World Wide Web Publishing Service	Disable only if you do not want to provide access to this server via OWA.

Tightening Mailbox Security

I discussed earlier in this ebook the permissions that are delegated to administrators on the Exchange organization container. The Enterprise Admins group has full control to the entire organization, and the Domain Admins group has almost Full Control to the entire organization. However, these groups are explicitly denied the Receive As and Send As permissions. Figure 11 shows the Security property page of the Exchange organization object in Exchange System Manager.

Figure 11 Security at the Exchange Organization Level

Somorita Surfboards Ltd Properties	<u>?</u> ×
General Details Security	
Name	Add
Image: Second strate and the second strate and th	Remove
Domain Admins (SOMORITA_HNL\Domain A	
Enterprise Admins (SOMORITA_HNL\Enterpri	
Everyone	
Permissions: Allow	Deny
Read metabase properties Image: Comparison of the store Administer information store Image: Comparison of the store	
Create named properties in the information store	
Receive As	
Send As	
Advanced Allow inheritable permissions from parent to propagate to thi object	is
OK Cancel Apply	Help

One of the reasons it is important to understand this is that a member of Domain Admins or Enterprise Admins can revoke these two Deny permissions. Or a user or group can be added to this list of permissions and given the Receive As and Send As permissions. These permissions will inherit from the organization or administrative group object all the way down to each mailbox. It is a very good practice to regularly confirm that these permissions have not been accidentally assigned or that the default permissions have not been removed. Check at both the Exchange organization object level as well as the administrative group.

NOTE

Don't see the Security property page in Exchange System Manager? It is intentionally hidden and must be enabled using a Registry key. Open the HKEY_CURRENT_USER sub tree of the Registry and navigate to \Software\Microsoft\Exchange\EXAdmin. Create a value called *ShowSecurityPage* of type *REG_DWORD* and set the data to *0x1*. Next time you load Exchange System Manager, the Security property page will be available on the Organization and Administrative Group containers.

Enabling SSL for Internet or Remote Clients

If you have remote clients using Outlook Web Access (OWA) or that are POP3, IMAP4, or NNTP clients, you must implement SSL. As I demonstrated earlier in this chapter, intercepting e-mail data and passwords is trivial provided you can get a network analyzer in the path of the IP datagrams traveling between the client and the Exchange server.

WARNING

If you have Exchange 2000 front-end servers, implement and require SSL only on the front-end servers, not the back-end servers. Communication between the front-end and back-end servers is over standard POP3, IMAP4, NNTP, or HTTP ports, not SSL ports. If you wish to encrypt data transmission between front-end and back-end servers, implement IPSec.

Implementing SSL requires that you get a X.509 certificate from a certificate authority (CA). The first decision you need to make is whether you are going to issue your own certificates using a product such as Microsoft's Certificate Server or whether you are going to pay for certificates from a trusted certificate authority. Trusted certificate authorities are determined initially by whoever distributed your operating system or Web browser. To see a list of trusted root authorities in Internet Explorer 6.0, choose **Tools** | **Internet Options**, click the **Content** tab, click the **Certificates** button, and click the **Trusted Root Certification Authorities**.

The downside to "rolling your own" certificates is that these certificates are not trusted by clients. When a Web browser client connects to a server using SSL and that server's certificate was not issued by a known authority, the client receives an error message similar to the one shown in Figure 12. This error indicates that the server's certificate was issued by an unknown certificate authority. The user can always click Yes to proceed, and SSL will work normally, but this message may cause users to call your help desk. The downside to getting certificates from a known and trusted authority is that each certificate can cost \$200 or more per server.

Figure 12 Security Alert Indicating That a Certificate Was Issued by an Unknown Authority

Security	Aler	:	
£	Infor char secu	Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.	
	⚠	The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.	
	0	The security certificate date is valid.	
	0	The security certificate matches the name of the page you are trying to view.	
	Doy	ou want to proceed?	
		Yes <u>No</u> Yiew Certificate	

WARNING

When requesting a certificate, when you specify the CN (common name) make sure you use the FQDN that the clients will use when they access the server.

Enabling SSL for POP3, IMAP4, or NNTP Clients

Once you have decided what you want to do about a certificate authority, you can use the Exchange System Manager to issue certificates to all Exchange IMAP4, POP3, and NNTP virtual servers on which you require secure communications. To issue a certificate, you must have the FQDN that your clients will be using when they connect to that particular server. For example, if you are configuring an Exchange 2000 front-end server that will be used by POP3 clients, you would configure the POP3

virtual server on the front-end server to use SSL. You would need to assign a FQDN to that front-end server. In this example, I use mail.somorita.com. I would need to follow these steps to assign a certificate to the front-end POP3 virtual server.

- 1. Using Exchange System Manager, open up the front-end server's Protocols container and the POP3 container. Right-click on the **POP3 virtual server** and choose **Properties**.
- 2. Click the **Access** property page and then the **Certificate** button. When the wizard starts, click **Next**.
- 3. If you have already got the certificate on the server for another protocol, click **Assign an** existing certificate, or if you have a backup of a certificate click **Import a certificate from** a Key Manager backup file. Since this is probably the first time you have configure d SSL, click Create a new certificate and click Next.
- 4. If you are going to send the request to another certificate authority, click **Prepare the request now, but send it later**. (This option will create a certificate request file that you can send on to certificate authority.) If you have installed the Windows 2000 certificate server as an "Enterprise" certificate server, you can click **Send the request immediately to an online certification authority**. Then click **Next**.
- 5. Specify a name for the certificate and a key length. 1024 bits is probably more than adequate. Once you have entered this data, click **Next**.
- 6. Provide an organization name and organization unit for this server, then click **Next**
- 7. On the next screen, you must provide the Common name of your server. This is the FQDN of the server. This must be the same name that the users use. In this example, the server might be called HNLEX02, but if the users are going to access it via POP3, I would use the alias the users will use, such as MAIL.SOMORITA.COM. When you have typed in a FQDN, click **Next**.
- 8. Provide the country, state, and city information, then click **Next**.
- 9. If you selected Send the request immediately to an online certification authority, you will then be prompted for a list of Enterprise certificate authorities. Select one of the authorities and click Next. Review the screen of information and click Next again. If you selected Prepare the request now, but send it later, you will be prompted for the name of the certificate request file. This file can be sent to a trusted authority, and they will generate a certificate for you to load later. Click Next twice.
- 10. Once this is complete, click **Finish**.

The certificate is now installed and SSL can be used. In order to enforce SSL, you should then click on the virtual server's **Access** tab and click the **Communication** button. To require SSL of all clients of this virtual server, click the **Require secure channel** check box shown in Figure 13. If you click the **Require 128-bit encryption** check box, all clients must support 128-bit encryption.

Figure 13 Requiring SSL of All Clients Connecting to This Virtual Server

Security
Once a valid key certificate is installed, you can require that access take place on a secure channel.
Require secure channel
Access can also be limited by the strength of the encryption. Select this option only if 128-bit encryption is supported on this computer.
Require 128-bit encryption
OK Cancel Help

WARNING

If you require 128-bit encryption, all clients must support 128-bit encryption. For Microsoft clients, this means they must have downloaded the 128-bit encryption pack for their operating systems, or they must be using Windows 2000 SP2 or later. If they do not support 128-bit encryption, they will not be able to connect to the server.

Enabling SSL for Outlook Web Access Clients

Configuring SSL for Outlook Web Access (OWA) is almost the exact same process as for POP3, IMAP4, or NNTP, but you use the Internet Services Manager to configure SSL instead of Exchange System Manager. Select the properties of the virtual Web server, then click the **Directory Security** property page and then click the **Server Certificate** button. That launches the same wizard that you may have used to configure SSL for a POP3, IMAP4, or NNTP client.

Once you have configure d the HTTP server with SSL, you can also configure IIS to require SSL. This is done on the Directory Security property page of the virtual Web server; click the **Edit** button and in the Secure Communications dialog box (shown in Figure 14) check **Require secure channel (SSL)**. You can also require 128-bit encryption through this dialog box, but make sure that all of your clients support it.

Figure 14 Requiring SSL on the Properties of an HTTP Virtual Server

Secure Communications
Require secure channel (SSL)
Require 128-bit encryption
Client certificates
Ignore client certificates
Accept client certificates
Require client certificates
Enable client certificate mapping Client certificates can be mapped to Windows user
accounts. This allows access control to resources Edit
Enable certificate trust list
Current CTL:
New Edit
OK Cancel Help

You may find that your user community has problems typing **https** to connect to a SSL-enabled Web server. Users are so accustomed to simply typing **http** (or even leaving that out) that they have a hard time remembering to type **https**. The network dictator in me wants to say "Tough turkey!" but we can't always take that attitude with our users. So, if you are willing to leave port 80 open through your firewall to the OWA servers, I will present to you a couple of options. For each of these examples, I am using an OWA server whose FQDN is owa.somorita.com.

The first way is simple redirection. On a server that is requiring SSL, notice that if you simply type **http** to connect to that server you will get an HTTP 403.4 error message stating that SSL is required. This page is generated by an HTML file (c:\winnt\help\ishelp\common\403-4.htm). You can either create your own page or edit that page to remind the user that he should be using HTTPS and then possibly even automatically redirect him to https://owa.somorita.com/exchange.

The following ASP code will allow you to redirect a user to another Web page (in this example, owa.somorita.com/exchange). However, if you ran the IIS Lockdown tool and took the defaults, ASP pages are disabled automatically.

<html><head>

<meta http-equiv="refresh" content="0; url=https://owa.somorita

.com/exchange">

</head></html>

Another way requires that you direct users initially to a page such as http://owa.somorita.com. On this page, you provide a "Welcome to the e-mail system. Authorized users only!" Web page and then provide them a link that directs them onwards to https://owa.somorita.com/exchange. However, this method requires that port 80 be left open and that the Web server does not require SSL. Unless of course, you are using two different virtual servers.

Locking Down an IIS/OWA Server

I highly recommend that you run both of these tools on your Exchange 2000 servers that are providing public OWA access. Simply run the IIS Lockdown tool, and it will ask you what role the server is functioning as. Figure 15 shows you the Select Server Template dialog box of IIS Lockdown. Choose the **Exchange Server 2000 (OWA, PF Management, IM, SMTP, NNTP)**. IIS Lockdown will automatically install URLScan for you.

Figure 15 URLScan's Select Server Template Dialog Box

🐐 Internet Information Services Lockdown Wizard	×
Select Server Template You can easily configure this server by selecting the template that most closely matches its role.	?
Select the template that most closely matches the role of this server. To view the settings for this template, select the View template settings check box, and then click Next. Server templates:	
Small Business Server 2000 Exchange Server 5.5 (Dutlook Web Access) Exchange Server 2000 (DWA, PF Management, IM, SMTP, NNTP) SharePoint Portal Server FrontPage Server Extensions SharePoint Team Services BizTalk Server 2000 Commerce Server 2000 Proxy Server Static Web server Dynamic Web server (ASP enabled) Other (Server that does not match any of the listed roles) Server that does not require IIS	
< Back Next > Cancel Hel	p

I will offer you a couple of pieces of advice regarding the use of IIS Lockdown and URLScan. These include the following:

Make absolutely sure that you have a recent release. Any version released on or after 11/14/2001 should be fine.

Always choose the right server role when you run IIS Lockdown.

Be very careful installing this tool if the HTTP server is providing multiple functions, such as OWA, IP Printing, Active Server Pages, etc.

Examine the URLScan log periodically.

You can undo anything the IIS Lockdown tool has done by simply running the tool again.

NOTE

For additional information on IIS Lockdown, URLScan, and Exchange, see Microsoft KB Q309508.

Imposing Limits

Impose mailbox and message size limits on a user community that has never had such limits before, and you are likely to find yourself being burned in effigy in the company parking lot. Or you may walk down the stately corridors of your organization only to find users with Exchange Administrator voodoo dolls. Limits are not something that a mature messaging user community deals with easily.

For this reason, you need to strike a delicate balance between functionality and available resources. I'll be the first to hit the boss's office if I think we do not have enough disk capacity to allow the user community to effectively do their jobs. If there is a business case for getting more disks, I'll buy as much disk capacity as I can possibly get online. Just remember, with large mailbox and public folder stores comes increased backup and (yikes!) restoration times. If your organization must meet specific service level agreements for restoration of messaging services, you should be very careful to calculate the maximum store sizes and how much time it will take to restore those mailbox/public folder stores. But, I digress.

Mailbox Size Limits

First, let's consider mailbox storage limits. These can be configure d in one of several ways. First, they can be configure d on the properties of each mailbox store. Figure 16 shows the Limits property page of a mailbox store; this figure shows the limits I recommend for a typical Exchange 2000 server (I am occasionally accused of being rather generous). I strongly believe that if there is a "business" reason for keeping 75MB of data in one's mailbox, the user should be able to do so. However, e-mail storage requirements will vary from business to business and also from user to user. Carefully plan your storage limits and make sure that you have the disk space necessary to support those limits.

Figure 16 Setting Mailbox Storage Limits on the Limits Property Page of the Mailbox Store

Mailbox Store (HNLEX02) Properties	<u>? ×</u>	
Details Policies	Security	
General Database Limits	Full-Lext Indexing	
Storage limits		
✓ Issue warning at (KB):	75000	
Prohibit send at (KB):	85000	
Prohibit send and receive at (KB):	150000	
Warning message interval:		
Run daily at Midnight	Customize	
Deletion settings		
Keep deleted items for (days):	15	
Keep deleted mailboxes for (days): 30		
Do not permanently delete mailboxes and ite been backed up	ms until the store has	
OK Cancel	Apply Help	

The other way that you can apply mailbox limits en masse is to apply a mailbox store policy to multiple mailbox stores using an Exchange 2000 system policy. This allows you to configure many mailbox stores that are affected by a single policy.

Of course, any limit that is applied to a mailbox store can be overridden on a per-user basis by editing that user's properties in the Active Directory Users and Computers console. Locate the **Exchange General** property page and click the **Storage Limits** button to override an individual user's mailbox limits. This gives you the ability to give your VIPs more e-mail storage than the typical user or to restrict the maximum amount of storage that low-end users can consume.

Size and Recipients Limits

Another place that I think it is important to apply mail limits are for the maximum inbound (receiving) and outbound (sending) message size. There are a couple of places that you can apply limits for inbound and outbound messages; these include the following:

Applying them globally for the entire organization on the Message Delivery properties Applying them individually for each user account on the Exchange General property page and through the Delivery Restrictions button

Applying them at each SMTP virtual server

Applying them on the Content Restrictions property page for the SMTP Connector, Routing Group Connector, or X.400 Connector

Regarding message size, I think it is a very good practice to apply maximum messages size limits globally. You do this using the properties of the Message Delivery object found in the Global Settings container in Exchange System Manager. Figure 17 shows the Defaults property page of the Message Delivery property page. Configure these global limits to be the maximum default amount for any user. Although I recommend a maximum default of 5MB (5,120KB) for sending and receiving message sizes, you should adjust this to meet the needs of your average user. I also recommend changing the recipients limits to a maximum of 100 recipients per message; this will limit the maximum number of recipients in the To:, Cc:, and Bcc: fields for all MAPI and OWA clients (including total distribution list membership). IMAP4 and POP3 clients may be able to get around this limit when they use SMTP to deliver messages.

Figure 17 Global Default Incoming and Outgoing Message Sizes and the Maximum Recipients per Message

Message Delivery P	roperties	<u>? ×</u>
General Defaults	Filtering Details Security	
Select the default of organization.	elivery restrictions and options for reci	pients in this
- Sending message	size	
🔿 No limit	Maximum (KB):	5120
Receiving messa	ge size	
⊂ No limit	Maximum (KB):	5120
Recipient limits-		
O No limit	 Maximum (recipients): 	100
0	Cancel Apply	Help

If you set the limits shown in Figure 17 globally, you can still override these limits for each individual user through Active Directory Users and Computers. For each user that you want to override sending and receiving message size limits, choose the **Exchange General** property page and click the **Delivery Restrictions** button. To override the maximum recipients limit, choose the **Exchange General** properties page and click the **Delivery Options** button.

SMTP Virtual Server Limits

One final place that I recommend setting SMTP virtual server limits is on any publicly exposed SMTP virtual server. The default for SMTP virtual servers for a basic Windows 2000/IIS installation is 4,096KB, however, when Exchange 2000 is installed, the installation program removes this limit.

Setting this limit will allow you to restrict the maximum size of a message entering your organization from outside.

I recommend creating separate SMTP virtual servers to be used for inbound SMTP mail (the ones to which the MX records or inbound SMTP relay hosts point) or outbound SMTP mail (the SMTP virtual servers used as bridgeheads by the SMTP Connector). For these publicly exposed SMTP virtual servers, set the maximum message size limit to the largest message size you would expect to send or receive. This may be quite a bit larger than the default global message size limits for your users. Figure 18 shows a SMTP virtual server's Messages property page with the message size limit configure d to 25MB (25,600KB).

Figure 18 SMTP Virtual Server's Message Size Limit

Default SMTP Virtual Server Properties	<u>?×</u>	
General Access Messages Delivery		
Specify the following messaging information.		
Limit message size to (KB):	25600	
Limit session size to (KB):	10240	
Limit number of messages per connection to:	20	
Limit number of recipients per message to:	64000	
Send copy of Non-Delivery Report to:		
NDR-Mailbox@somorita.com		
Badmail directory:		
c:\SMTP\VSI-1\BADMAIL	Browse	
, Forward all mail with unresolved recipients to host:		
,		
OK Cancel Apply	Help	

Protecting Critical Files

No client should ever have to have access to the Exchange server's file system. A combination of appropriate shared folder permissions and restricted physical access should ensure that end users never access the Exchange server's file system.

When Exchange 2000 is installed, a couple of shared folders are created. These shared folders, their default location on the file system, and their intended purpose are shown in Table 6.

Table 6 Shared Folders Created by Exchange 2000 Installation

Share name	Default file system location	Usage
Address	\program files\exchsrvr\address	This folder holds the DLLs that are used by the
		System Attendant's Recipient Update Server to

		generate a proxy address (such as SMTP, X.400, Notes, cc:Mail, etc.).
servername.LOG	\program files\exchsrvr\servername.log	Stores message tracking log files.
Resource\$	\program files\exchsrvr\res	Contains the DLLs that are used by event viewer to properly display events generated by Exchange 2000 components.

To each of these shared folders, the Administrators local group and the local computer account are given Full Control permissions. Unfortunately, the Everyone group is given Read permission to the shared folder also. This should be removed and replaced with the Exchange Admins group instead. Users should never need access to these folders, and they certainly should never have access to the message tracking data.

I used to be an advocate of using NTFS permissions to further secure an Exchange server. However, each Exchange server type is slightly different, and the permissions required are usually unique to the specific role in which the Exchange server functioned. If permissions are applied incorrectly to a specific data directory, Exchange server or one of its connectors will not function.

As a general rule, I strongly believe that if an untrusted administrator or user is able to log on to the console of your Exchange server or if they can access a shared folder on your Exchange server, then you have bigger problems than default NTFS permissions. So rather than focusing on delicately securing each folder with the proper NTFS permissions for the specific Exchange server role, I prefer to focus on improved physical security, giving access only to trusted administrators, and locking down the shared folder permissions.

The only exception to this rule is for Exchange servers that are used as front-end servers. Front-end servers should have their command-line utilities secured so that they cannot be accessed by non-Administrators. The critical command-line tools are secured by the IIS Lockdown tool.

Νοτε

Physical security for Exchange servers must be a high priority when configuring and placing Exchange servers.

Notes from the Underground...

Problems with Locking Down Security Too Tightly

I was recently called in to help fix a problem with a server that was not allowing any OWA users except administrator equivalent users to login. The problem was caused when an overenthusiastic network administrator decided to lock down the server as tightly as possible. He completely removed the Everyone group's NTFS permissions to the entire file system, and he used the HISECDC.INF security template to lock down the machine.

Unfortunately, this locked down the machine a little too tightly. Finding the root problem for inability for OWA to log in was like handling a Russian nesting doll; each time we opened up one, we found another one inside. And the administrator had not documented exactly what he had done. After a few dozen Knowledge Base articles and a couple of calls to Microsoft PSS, we finally unraveled all of the places that too much security had been applied.

This experience re-emphasizes the need to properly document all steps involved in tightening security, making sure that changes are made incrementally, and knowing exactly what steps (and the results of those steps) should be taken ahead of time.

Network Analysis Risk Reduction

When I teach networking and Exchange classes, one of my favorite side-topics is network monitoring. At many points throughout an Exchange class, I will fire up the Microsoft Network Monitor and demonstrate how easy it is to intercept data if you have Network Monitor running and you are sitting in

the path of the user's IP datagrams. Protecting the network from a physical layer assault is extremely important, and the following is a list of things that you should consider to improve security of messaging data traveling on your network:

Move all servers to switched networks to reduce the ease of which a rogue individual can perform network monitoring.

Enable and require SSL for all standard Internet such as OWA, POP3, IMAP4, and NNTP.

Enable IPSec between all Exchange 2000 servers including those configure d as front-end and back-end servers. However, note that you cannot use IPSec on Windows 2000 clustered nodes.

Enable IPSec between Exchange 2000 and domain controllers/global catalog servers to protect LDAP queries.

Deploy X.509v3 certificates for users and instruct them to use S/MIME clients to encrypt message data and/or use digital signatures.

Enable encryption for MAPI clients.

The last point, enabling encryption for MAPI clients, is a point that many administrators don't even realize exists. Although MAPI messages are difficult to decode, it is not impossible. Outlook MAPI clients use RPCs to communicate with the Exchange information store and the Active Directory (or Exchange 2000 System Attendant). RPCs include the capability to provide encryption of the RPC data stream using RSA RC-2 streaming encryption (either 40-bit encryption for Windows 95/98/Me or 128-bit encryption for Windows NT/2000/XP clients with the appropriate service packs.)

Enabling MAPI over RPC client encryption is simple, but it must be configure d for a messaging profile rather than at the server. Display the properties of the user's messaging profile and click **Properties** for the **Microsoft Exchange Server** service, then choose the **Advanced** property page (shown in Figure 19). On the Exchange service's Advanced property page, check **When using the network** and/or **When using dial-up networking** to encrypt MAPI over RPC data crossing the network.

Figure 19 Enabling Encryption for Outlook MAPI over RPC Clients

Microsoft	Exchange 9	5erve	r				x
General	Advanced	Dial-U	Jp Netw	orking	Remo	ote Mail	
- Mailbo Open	ixes these additio	nal mai	ilboxes:				1
					Ad	ld	
					Rer	nove	
Encrypt information							
Logon network security:							
NT Password Authentication							
Enable offline use Offline Folder File Settings							
01		Cancel		Apply	y	He	elp

Denying Client Access

You may run a very tight ship on your network. So tight, in fact, that you may let only certain clients or even certain versions of clients access your Exchange server. If this is the case, I should introduce you to a couple of features of Exchange that let you limit the types of Internet clients or even the MAPI version of the MAPI clients.

Restricting Internet Clients

A couple of options are available when restricting Internet clients such as POP3, IMAP4, NNTP, and HTTP (OWA) clients. These options include the following:

Disabling an entire service (POP3, IMAP4, and NNTP)

Restricting the IP addresses from which a client can access POP3, IMAP4, NNTP, or HTTP services

Restricting which users can access the server via POP3, IMAP4, NNTP, or HTTP

On each Exchange 2000 server, you can easily disable the POP3, IMAP4, and NNTP services; there are no dependencies or issues that would prevent you from disabling these protocols. However, disable the HTTP protocol only if you are willing to compromise the ability to manage public folders on that Exchange server. If you wish to disable HTTP, I recommend restricting the IP addresses from which it can be accessed on a particular Exchange server. That way you can still manage public folders from administrative workstations, but outsiders cannot access HTTP functions on that server.

Using Exchange System Manager, for POP3, IMAP4, and NNTP virtual servers, click the **Access** property page, then click the **Connection** button. From the Connection dialog box shown in Figure 20, you can specify the IP addresses that are either allowed to access the virtual server or that are not allowed to access the virtual server.

Figure 20 Restricting Which Clients Can Access the Virtual Server

Connection	×
Select which comp Only the list	uters may access this virtual server: below
C All except th	e list below
Computers:	
Access	IP Address (Mask) / Domain Name
of Granted	192.168.0.0 (255.255.255.0)
of Granted	somorita.com
Add	Remove OK Cancel Help

You can restrict/allow based on an individual IP address, network ID, or domain name. The process of restricting based on a domain name adds additional overhead to the server because for each connection, the server must perform an inverse DNS query to confirm that the client has a PTR record in one of the allowed or denied domain names.

Configuring the HTTP virtual servers to restrict based on IP address or domain name is performed through Internet Services Manager on the Directory Security property page. The dialog box you see in Exchange System Manager is identical to the one shown in Figure 20.

Νοτε

To increase security on back-end servers, you can restrict the clients that can access the back-end servers via HTTP, POP3, IMAP4, or NNTP to only the IP addresses of the front-end servers.

Another way to restrict clients to accessing the server via the standard Internet protocols is to restrict them based on their username. This is done through Active Directory Users and Computers, but you must first enable the advanced view (**View** | **Advanced Features**). Display the user's properties that you wish to disable and click the **Exchange Advanced** property page; then click the **Protocol Settings** button. From this screen, you can disable the user from accessing POP3, IMAP4, or HTTP services. You can also do this in bulk by exporting the *protocolSettings* attribute from Active Directory using LDIFDE, changing the attribute, and then re-importing for all users. If you choose to manipulate this using LDIFDE, be careful because the data is exported from the directory in Base64 encoding so you might want to re-import the data by cutting and pasting from a user that already has the protocol disabled.

Restricting MAPI Client Versions

Microsoft introduced a spiffy new feature into Exchange 2000 SP1 that allows you to restrict access to the server to only certain MAPI clients. This is very useful if you have tested and deployed a specific version of the Outlook client to desktops, and you want to make sure that all of your users are up to a minimum level. However, be warned, that each Office service pack and security fix will probably update the MAPI version number, so keep that in mind when you deploy Outlook updates and service packs to the client desktop.

First, you may ask how you can determine the MAPI version of a specific client. It is not quite as easy as it would seem. I use the Logons container of the mailbox or public folder stores to determine this. The information is displayed as a number that looks like w.x.y.z; we are interested in three of these four (w.y.z). So for example, if the version is 10.0.0.2627, we are only interested in 10.0.2627. This will not necessarily be the same as the Outlook version you see in Outlook's Help | About screen; so do not use that number. Table 7 shows some of the common clients and the MAPI versions; for your specific Office service release, you will need to determine the correct version.

Client	MAPI Version	Required for Registry
Exchange 4.0 Inbox client	4.0.993.3	4.993.3
Exchange 5.0 Inbox client	5.0.1457.3	5.1456.3
Outlook 97 8.03	5.0.1960.0	5.1960.0
Outlook 98	5.0.2178.0	5.2178.0
Outlook 2000 SR-1	5.0.3121.0	5.3121.0
Outlook 2002	10.0.2627	10.0.2627
Exchange 2000 SP3	6.0.6249.0	6.6249.0

Table 7 Some Common MAPI Client Versions and the Number Necessary for the Registry

In order to enable this feature, you must create a new value in the

HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem key called *Disable MAPI Clients* of type *REG_SZ*. You are going to put into this value the versions of the MAPI clients that you want *disabled*; it is permissible to put in a range of client versions as well. But you must make sure that you do not disable versions 6.0.0 through0.0 because this will prevent the Exchange server MAPI components from accessing mailboxes on the server. Separate multiple entries with a comma. If you wanted to disable all MAPI clients except the Exchange 2000 components, you would enter - **6.0.0,0.0**. If you wanted to disable all clients except for Outlook 2002, the Registry entry would contain - **6.0.0,7.0.0-10.0.2627**.

Stopping Viruses

The e-mail-based virus has become the scourge of the IT world. All of the Exchange systems that I have anything at all to do with have been overcome by at least one e-mail-based virus since these viruses first began to spread in 1999. Most of these sites have been hit again and again due to carelessness or shortsightedness on the part administrators and consultants (myself included). Guessing that someone might use an EXE file or a script embedded in an HTML message to propagate a virus does not take a rocket scientist. But who would have dreamed that someone would embed an e-mail virus in an SCR file?

For this reason, viruses continued to sneak by even the most savvy e-mail administrators well into 2001 and 2002. And for this reason, continued vigilance and even what may seem to be extreme restrictions on the e-mail system must be maintained.

WARNING

No anti-virus solution will be effective if its signatures and scanning engine are out of date. The software should be configure d to check for virus signature updates at least once per day. And the minute you hear of a new e-mail-based virus, force a signature update immediately to see if new signatures have been released. If not, check again in an hour or two.

Choosing the Correct Anti-Virus Solution

The first step toward a virus-free utopia is to make sure that you have chosen the correct anti-virus software to work on the Exchange 2000 server. This software *must* be Microsoft Anti-Virus API (AVAPI) 2.0–aware. Most major anti-virus vendors on the market today provide AVAPI 2.0–aware solutions for Microsoft Exchange. But you must make absolutely sure that the product is designed to work with and on the Exchange server.

AVAPI 2.0 aware products are capable of scanning the e-mail after it arrives on the Exchange server, but before the user is notified that the message is in their mailbox. Some MAPI-only-based solutions may actually allow a message to arrive in the user's mailbox before the message gets scanned.

WARNING

Should you use a file-based scanner on the Exchange 2000 server? File-based virus scanners can cause dreadful (and fatal) problems for Exchange server due to the fact that these scanners may actually find a virus in an Exchange log or database file and remove the virus. Since file-based virus scanners (such as Norton Anti-Virus Corporate Edition) do not have a clue about ESE database checksums, they *will* corrupt the file. I have configure d both Norton Anti-Virus for Microsoft Exchange and Norton Anti-Virus Corporate Edition on the same machine, but you *must* configure the file-based scanner to ignore the Exchange data, log file, and queue directories.

SMTP Virus Scanners and Content Inspection

There is a wide variety of SMTP mail scanners on the market today. These scanners do not depend on any single e-mail vendor or platform (Windows or Unix), but rather perform the scanning and content inspection on messages prior to the message being delivered to the mail server. In most cases, the

DNS MX records point to these SMTP scanners rather than to your Exchange server; the SMTP scanner inspects the message and forwards on to an Exchange server.

I have implemented a number of these systems with great success, but I recommend using a different vendor for your SMTP scanner than you use for your Exchange server. For example, if you use Norton Anti-Virus for Exchange on your Exchange 2000 servers, use Trend's VirusWall product as an SMTP scanner. This ensures that you have two different vendors inspecting your e-mail, which greatly improves the chances for catching viruses before they arrive at the user's desktop.

Νοτε

Many organizations implement anti-virus systems from different vendors not only at the SMTP scanner, but also for the client and Exchange server.

Many firewall products today will also perform virus and content inspection as SMTP traffic comes through the firewall. Depending on the size of your organization and how overburdened your firewall is, this may be a good place or a bad place to implement SMTP mail scanning. If the firewall is heavily burdened, scanning SMTP traffic will only make matters worse.

Some of these SMTP scanners are more than simple virus scanners, such as Clearswift's Mail Sweeper (formerly MIMESweeper) or GFI's Mail Se, can actually scan through a message looking not only for viruses, but also things that might indicate that the message is spam or that the message contains sensitive or objectionable material.

If you are implementing a content inspection system, you may want to use it not only to inspect inbound e-mail, but also direct outbound mail through this system as well. Most content inspection systems allow you to configure key phrases and words that perhaps should not be contained in e-mail leaving the organization.

Virus Scanning at the Desktop

Some administrators reach an early state of comfort when they deploy anti-virus software to the Exchange server; since the Exchange server is protected, they must be protected from viruses. I can tell you from experience that newly released viruses can sneak by. Users often have a tendency to bring files in from home on floppy disks and they check their Yahoo mail or POP3 mail at their ISP from work. This can easily and quickly introduce a virus to your mail system.

For this reason, in order for you to be more completely protected you must make sure that all of your desktop clients have a file based anti-virus scanning software that is capable of scanning Outlook or other mail systems. Some administrators go so far as to make sure that they use a different version of their anti-virus software at the desktop than they do for the Exchange-based solutions.

Blocking File Attachments

Just like increased airport security has increased wait times at metal detectors, blocking certain types of files has become a necessary evil for e-mail administrators. This is another one of those actions that the e-mail administrator can perform and then find himself being burned in effigy in the cafeteria. Choosing a list of file types to block is difficult. Table 8 is a list of critical files that I recommend blocking on all e-mail systems.

Table 8 Critical Files to Be Blocked on All E-Mail Systems

File type	File Type Description
.bat	Batch file (DOS or Windows)
.chm	Windows help files
.cmd	Batch command (Windows and OS/2)
.com	DOS-based application

.eml	E-Mail extensions (registered to Outlook Express)
.exe	Executable files
.js	JavaScript files
.pif	Program information files
.pl	PERL script
.reg	Registry files (registered to Regedit)
.scr	Screen saver files
.sh	Shell script
.shs	Scrap file extension
.vb	Visual basic files
.vbs	Visual basic script extension
.WS	Windows scripting host
.WSC	Windows scripting components
.wsf	Windows scripting host
.wsh	Windows scripting host

If you are extra cautious, you might also consider blocking this list that is published on the Exchange 2000 administrator's mailing list FAQ (see Table 9).

Table 9 Additional File Types to Be Blocked on E-Mail Systems

File type	File Type Description
.hlp	Help data file
.oft	Outlook template
.adp	AOL server dynamic pages
.asx	Windows media shortcut
.bas	Basic program extension
.bin	Binary file
.cpl	Control panel applet
.crt	Security certificate file
.dll	Dynamic link library
.hiv	Registry hive file used during Windows installation
.hta	HTML application
.inf	Setup information text file
.isp	Internet communications settings
.msi	Program setup file (used by Microsoft Installer)
.mst	Program setup script (used by the MSI)
.OCX	OLE control extension
.ovl	Program overlay file
.sct	Script tools
.sys	Device driver file
.VSS	Visual Source Safe file
.vxd	Virtual device driver

I usually try to block forbidden attachments at the SMTP scanning system rather than on the Exchange server, but you will probably also want to block your forbidden file attachments list internally as well just in case a virus sneaks in through another path. If possible, you should configure the SMTP scanner to send a message back to the originator of the message indicating the types of files that are forbidden and instructing them that they should Zip or rename the file and send it again.

Tools & Traps...

Case Study: Multiple Layers of Virus Protection

Through 1999 and 2000, VVV Corporation had their share of e-mail-based viruses. With just over 25,000 entries in their Exchange 5.5 global address list, viruses spread quickly. Nearly 2,000 of the entries in the global address list were actually custom recipients for customers and vendors. During the Anna Kournikova outbreak, the company had to pull the plug on its Internet connection and shut down

its Exchange servers due to nearly 100,000 messages in the Internet Mail Service queues. Most of the Exchange servers' message transfer agents were performing extremely slowly to not at all due to the congestion on each server. The administrators had to remove the virus from each mailbox using the ExMerge program. During several of the virus outbreaks, including Anna Kournikova, the company lost some goodwill with its customers and vendors; the IT department lost a lot of credibility with its user community due to loss of service.

One of the criteria for deployment of Exchange 2000 was that it *must* be more tolerant of e-mailbased viruses. Well, Exchange 2000 is not really much more tolerant than Exchange 5.5 was except that you can select only a small number of users from the global address list at a time and the administrator can restrict the maximum number of recipients in a single message.

To further fight virus outbreaks, the company moved to a single anti-virus client. They chose Norton Anti-Virus Corporate Edition on the desktop with the signatures managed automatically via the Symantec System Center and Norton Anti-Virus Server. On the Exchange servers, the company used Sybari's Antigen. Finally, all SMTP messages entering or leaving the organization went through one of two Trend InterScan VirusWall SMTP gateways. An administrative policy was put in place that the virus signatures were checked twice daily for updates on both the Antigen and VirusWall products.

Further, the IT department defined a series of rules for the types of attachments that the company would receive. The InterScan VirusWall SMTP gateway would not allow messages with specific attachments to be sent through the gateway to Exchange 2000.

Though it took VVV Corporation a few painful lessons to get serious about virus protection, since implementing up-to-date, multi-layer virus protection and prohibiting certain types of file attachments, they have not had a single virus outbreak.

Exchange 2000 and Firewalls

Exchange 2000 servers should always be protected by a firewall. I have seen many configurations that actually left network connections to the Exchange 2000 server open and visible to the Internet with no filtering or blocking of any type. This is a very bad idea. A properly configure d firewall should always be in place to protect the Exchange server.

So the question now remains, what ports should be open between the Exchange server and the public network. This is going to depend on the type of client and the level of functionality. Ideally, we would block everything and require the Internet client to first establish a secure, encrypted VPN connection to the network. However, that is not going to be practical for most user communities and especially for users that move from one machine to another.

Νοτε

What ports are open on your Exchange server? The Windows 2000 Netstat tool is usually not sufficient for finding open ports and easily identifying which of these ports are in use by which processes. In an article titled *Securing Exchange 2000, Part 1*, author Chris Weber describes how to use a tool called FScan (from Foundstone at www.foundstone.com), a tool from the FPort (also from Foundstone), and the Windows 2000 resource kit utility *TList* to identify which process or service is using which port. You can find this article at http://online.securityfocus.com/infocus/1572. Another useful tool is called ActivePorts, which you can download from Beverly Hills Software at www.bhs.com.

Exchange 2000 opens a lot of ports on a Windows 2000 computer. Table 10 lists many of the common ports that you may find in your Exchange environment. This is not to say that these ports should be opened, but you should be aware of these ports and decide if they are necessary.

Table 10 Common Exchange 2000 TCP/UDP Ports

Port number	Description
25	SMTP
80	HTTP (OWA, Instant Messaging)
102	X.400 message transfer agent (MTA)
110	POP3
119	NNTP
135	Remote procedure calls (RPC) end-point-mapper (necessary for MAPI clients)
143	IMAP4
379	LDAP port for site replication service (SRS)
390	Microsoft recommended port for configuring Exchange 5.5 servers running on a Windows 2000
	domain controller
443	HTTP using SSL
563	NNTP using SSL
691	Link state table updates within a routing group
993	IMAP4 using SSL
995	POP3 using SSL
1503	T.120 data conferencing services (used with Exchange 2000 Conference Server)
1720	H.323 video conferencing services (used with Exchange 2000 Conference Server)
1731	Audio conferencing services (used with Exchange 2000 Conference Server)
6667/7000	IRC and IRCX chat clients

There are also a number of TCP/UDP ports that an Exchange 2000 must have open in order for it to function properly. Table 11 shows a list of TCP/UDP ports that Exchange 2000 may require to communicate with other Exchange servers, domain controllers, and global catalog servers.

Table 11 Ports that Exchange 2000 Requires

Port number	Description/requirement
25	SMTP mail to other servers or the Internet
53	DNS to internal DNS server if used only internally or also to external DNS servers if used with SMTP Connector
80	HTTP is being used as a front-end server
88	Kerberos used for authentication
102	MTA used for X.400 Connector and communicating with Exchange 5.5 servers
110	POP3 if used as a front-end server
119	NNTP if used as a front-end server
143	IMAP4 if used as a front-end server
135	RPC end-point-mapper
389	LDAP port to query domain controllers
445	CIFS used for SMB file sessions and DFS discovery
636	LDAP using SSL
691	Link state updates
3268	LDAP to global catalog servers
3269	LDAP to global catalog servers using SSL

Νοτε

See Microsoft KB article Q27839 for more information about ports that are used by Exchange 2000.

MAPI Clients and Firewalls

MAPI clients such as Outlook 97, 98, 2000, and 2002 require special consideration when accessing an Exchange server through a firewall. The Outlook client requires access to three ports when it connects to the Exchange server. The first port is the RPC end-point-mapper port (port 135), the second is the

directory service, and the third is the information store service. The problem is that the "directory service" (picture Dr. Evil saying this) and information store ports are dynamic ports, meaning they change each time Exchange 2000 is restarted. The MAPI clients use port 135 to "look up" the port numbers for the directory service and the information store.

Since the ports are dynamically assigned, this means we have to statically map these ports. In general, I think this is a good practice during setup of Exchange servers to always statically map the directory service and information-store ports.

Most firewall and infrastructure administrators will become rather nervous if you tell them you must open up the RPC end-point-mapper (TCP port 135). After all, there have been a couple of well publicized denial-of-service vulnerabilities against this port over the years. Unless you are opening these ports for your data center or backbone firewall, you might want to consider requiring remote MAPI clients access the network through a VPN rather than opening ports through the firewall. After all, if they are a remote MAPI client, that requires that they have some version of Outlook installed and configure d, so the probability of being able to configure a VPN connection from that client is good.

Accessing the Exchange 2000 Directory Service

Wait a minute, the Exchange 2000 "directory service?" I know you are saying to yourself, "Self, there is no Exchange 2000 directory service." And you are correct. However, MAPI clients do not know this. When a MAPI client first loads, it contacts what it *thinks* is the Exchange 5.*x* directory service via MAPI over RPC. The Exchange 2000 System Attendant runs two processes that answer these calls. The first process is the *DSProxy* process that is used for Outlook 97 and 98 clients and Outlook clients that may be outside the firewall. DSProxy merely forwards the MAPI requests on to a global catalog server on behalf of the MAPI client.

The second process run by the System Attendant is the *referral interface* or *NSPI* (name service provider interface); this process detects that whether or not the Outlook client is capable of handling a referral (such as Outlook 2000 and 2002). If the client is capable of receiving a referral to another directory service, the NSPI sends a list of global catalog servers to the MAPI client. From that point forward, the Outlook client will make queries directly to the global catalog server using MAPI over RPC.

Νοτε

For more information about the DSProxy, NSPI, and how MAPI clients access the directory, see Microsoft KB article Q256976.

Each time the Exchange 2000 System Attendant starts, it dynamically picks an unused port above 1,024. This is not very practical when configuring a firewall because you would have to change the port number each time the Exchange server restarts. You can statically map the ports that NSPI and DSProxy uses by creating a Registry value called *TCP/IP NSPI port* of type *REG_DWORD* and a value called *TCP/IP port* of type *REG_DWORD*. Create these values in the following Registry key:

\HKLM\System\CurrentControlSet\Services\MSExchangeSA\Parameters

When you put in data for this value, make sure that you realize that the default is hexadecimal; I click the decimal radio button so that I don't have to convert the port numbers I'm entering into hex first. I usually pick values like 4000 and 4001 decimal for the TCP/IP NSPI port and the TCP/IP port.

You can also statically map the MAPI port on which the global catalog servers respond. This is done by creating a Registry valued called *TCP/IP port* of type *REG_DWORD* in the following key:

\HKLM\System\CurrentControlSet\Services\NTDS\Parameters

Accessing the Information Store

Like the System Attendant, the Information Store picks an unused port above 1,024 for MAPI clients to use when accessing the store. You will also need to configure this port to be a static port. To do this, create a Registry value called *TCP/IP port* of type *REG_DWORD* in the following Registry key:

Keep in mind that the data for *REG_DWORD* values defaults to hexadecimal, so you might want to click the decimal radio button to enter the data. I usually pick a port immediately above the NSPI port, such as 4002.

Νοτε

For more information on statically mapping the system attendant, information store, and global catalog MAPI ports, see Microsoft KB articles Q298369, Q270836, and Q148732.

Where Are My New Mail Notifications?

One of the most common questions that I get asked about Outlook clients sitting outside of a tightly locked firewall is why new mail is not immediately arriving in the client's inbox. New mail notifications are sent via a UDP packet from the Exchange server to the Outlook client. Unfortunately, the client, not the Exchange server, picks this port at startup, thus it cannot be statically mapped at the Exchange server.

The only solution to this quandary is to configure the firewall to allow all outbound communication on UDP port 1,024 and above to leave the firewall when it comes from the Exchange server. This may not be a desirable solution. Thus, if you choose not to open up these outbound ports, the client will simply have to manually poll the Exchange server (pressing the F5 key) for new mail or simply wait until the Outlook client polls the Exchange server manually for new mail (about once an hour).

POP3, IMAP4, NNTP, and HTTP Clients

As with any other firewall configuration, only open up explicitly the ports that are required. This includes any of the Internet client protocol ports such as POP3, IMAP4, NNTP, and HTTP. One improvement Microsoft has made with Exchange 2000 is that they offloaded the responsibility of these protocols to IIS; thus, these protocols can be "answered" by a different server. This capability is called front-end servers. Simply put, Internet clients (not MAPI clients) can connect to an Exchange 2000 front-end server, the front-end server performs an Active Directory query (to a global catalog server) to find out in which back-end server the mailbox is stored, and then proxies the client request to that back-end server. Figure 21 shows a simple diagram of how a front-end server might set in a DMZ in order to provide an additional layer of protection for the back-end servers. Only the front-end server is allowed to communicate through the DMZ to the back-end servers.

Figure 21 Simple Exchange Front-End/Back-End Server Configuration



Some of the advantages of front-end servers in addition to providing better security is that the SSL encryption is handled on the front-end server, not the back-end server. Adding additional front-end servers allows you to perform load balancing between the front-end servers (using a tool such as Network Load Balancing, Local Director or Big IP), but still allow the client to use the same FQDN regardless of the back-end server name.

NOTE

A complete discussion of front-end and back-end servers is beyond the scope of this book. Microsoft has an excellent whitepaper called *Exchange 2000 Front-End and Back-End Topology*, which is available on Microsoft's Web site at www.microsoft.com/exchange.

SMTP Security

Each Exchange 2000 server has at least one SMTP virtual server. The only exception to this may be a front-end server that is not providing message routing functions. There are a couple of SMTP issues that you are going to want to consider when planning Exchange 2000 security. These include making sure that you do not leave SMTP open for relay, providing security for data transmissions, and making sure that the SMTP server is properly patched. You may even want to change the default SMTP banner.

Restricting SMTP Relay

One of the biggest mistakes the Exchange 5.5 Internet Mail Service (IMS) team made was that when the IMS was installed it is automatically open for relay. Fortunately, the Windows 2000 SMTP team saw the error of evil ways of the Exchange 5.5 IMS team and changed the default configuration of SMTP. By default, the Windows 2000 SMTP virtual server (which Exchange 2000 uses) now only allows relay for authenticated clients. Figure 22 shows the default relay configuration for an SMTP virtual server.

Figure 22 Default SMTP Relay Configuration

Relay Restrictions		×	
Select which computer may relay through this virtual server:			
Only the list below	,		
C All except the list	below		
Computers:			
Access	IP Address (Mask) / Domain Name		
Add Ren	nove		
Allow all computers which successfully authenticate to relay, regardless of the list above.			
	OK Cancel Help		

Do not clear the **Allow all computers which successfully authenticate to relay** check box, regardless of the above list check box. If you do this, then other Exchange 2000 virtual servers in your organization will not be able to successfully send mail to this SMTP virtual server.

There is never a valid reason to enable SMTP relay to the Internet. As I mentioned earlier in the chapter, doing so will only cause you some grief down the road in the form of clogged message queues and ending up on lists of known spam addresses. However, if you are supporting POP3 or IMAP4 users, they must be given the address of an SMTP server that will provide SMTP relay functions for them. I strongly recommend that you develop documentation for your POP3 and IMAP4 users that includes how to configure their client SMTP configurations to include the capability to authenticate to the SMTP virtual server. However, authentication to an SMTP virtual server introduces a new problem: usernames and passwords may be sent over the network in clear text.

For this reason, you should configure a separate SMTP virtual server that is used by POP3 and IMAP4 clients. This SMTP virtual server should require the clients to support SSL so that client authentication is encrypted. This SMTP virtual server, of course, will not be used by the general public that wants to send your servers SMTP mail since not all SMTP clients on the Internet are going to support SSL.

Just the Bugs, Ma'am

Since Windows 2000 has been released, a number of bugs have been found in the Windows 2000 SMTP service that may allow a malicious person to take advantage of SMTP relay even if you are only permitting authenticated SMTP relay. A couple of these bugs are outlined in Microsoft Security Bulletin MS02-011 and MS02-12. (These are fixed by Windows 2000 Service Pack 3, by the way.)

These relay bugs that have arisen since Windows 2000 RTM merely emphasize the need to keep your service packs and security fixes as up-to-date as possible.

Providing Encrypted Data Streams of SMTP Traffic

If you are concerned about SMTP traffic being intercepted on the network, I generally recommend using IPSec between Exchange 2000 servers. IPSec can be used to encrypt not only the SMTP traffic, but also LDAP queries to domain controllers and global catalog servers. However, IPSec cannot be used to Exchange 2000 servers operating in a cluster, and it is not practical to enable IPSec to all of your client computers.

For this reason, you may want to enable TLS/SSL on one or more of your SMTP virtual servers in your organization. However, if you are going to enable TLS/SSL on any of your SMTP virtual servers, you need to have a clear strategy of what you want to accomplish. There are two main reasons (in my opinion) that you might want to enable TLS/SSL on your SMTP virtual servers.

The first is if you merely want to provide secure SMTP authentication and data transmission for your remote POP3 and IMAP4 clients. In this case, create an SMTP virtual server that will be made available from the public network. The instructions for assigning a certificate to an SMTP virtual server are almost identical to the instructions for assigning a certificate to a POP3 or IMAP4 server, which was detailed earlier in this ebook. Once you have assigned the certificate to the SMTP virtual server, if this virtual server is going to be used only by remote POP3 or IMAP4 clients you should require SSL. This is enabled on the Access property page (Communication button).

The second common situation in which you may want to enable TLS/SSL is if you want all internal SMTP traffic to be encrypted. Assign a certificate to all of the SMTP virtual servers in the organization, configure them to require TLS/SSL, and then on each SMTP virtual server's **Delivery** property page click the **Outbound security** button. On the **Outbound Security** dialog box (shown in Figure 23), click the **TLS encryption** check box.

Figure 23 Requiring Outbound TLS/SSL on the Properties of an SMTP Virtual Server

Outbound Security		×
Anonymous access		
No user name or pas	sword required.	
C Basic authentication		
The password will be commands.	sent over the network in clear tex	t using standard
User name:		Browse
Password:	*********	
C Integrated Windows	Authentication	
The client and server Interface.	negotiate the Windows Security S	Support Provider
Account:		Browse
Password:	******	
✓ TLS encryption		
	OK Cancel	Help

If you have outbound SMTP communication to SMTP servers outside of your organization, you must create an SMTP virtual server that does not require outbound TLS/SSL. You then assign this SMTP virtual server to be used as a local bridgehead by the SMTP Connector.

Changing the SMTP Banner

When you connect to a Windows 2000 SMTP virtual server, you are presented with the default SMTP banner. This banner is going to be quite similar to this:

220 hnlex02.somorita_hnl.com Microsoft ESMTP MAIL Service, Version: 5.0.2195.532

9 ready at Wed, 4 Sep 2002 00:26:18 -1000

Some administrators want the ability to change this since they may want to mask the fact that this is an Exchange 2000 system. It is possible to change not only the SMTP banner, but also the POP3 and IMAP4 banners. In order to change this, you are going to have to do some IIS Metabase editing. For detailed instructions on changing the SMTP banner, see the Microsoft KB article Q281224. KB Article Q303513 instructs you on how to change the POP3 and IMAP connection and disconnection banners, but they cleverly assume that you have a copy of the smtpd.exe utility. As of this writing, I can find no way to get this utility short of calling Microsoft PSS.

WARNING

If you believe that changing the SMTP/POP3/IMAP4 banners will make your server much safer, you are mistaken. This might be enough to fool an unsophisticated bot or an entry-level script kiddie looking for a Windows 2000 or Exchange 2000 machine, but simply modifying the banners will not deter a knowledgeable intruder in the least.

Giving Away the Store

Would you advertise your internal IP addresses and host names on the Internet? No, of course you would not. One of the golden rules of any secure military network is that you do not reveal your internal host and IP addresses. Giving a potential intruder information about your internal network may give them a starting point for an attack.

Yet, each time you send an e-mail message to someone outside your network, you are giving them information about your network via the SMTP headers of the message. Here is a sample SMTP message header.

```
Microsoft Mail Internet Headers Version 2.0
Received: from exchangel.bobsboogieboards.com ([10.36.210.96]) by
  smtprelay.bobsboogieboards.com with Microsoft SMTPSVC(5.0.2195.2966);
  Wed, 7 Aug 2002 03:03:42 -1000
Received: from smtpgate.somorita.com [172.30.121.84] by
  smtprelay.bobsboogieboards.com with XWall v3.20a; Wed, 7 Aug 2002
  03:04:38 -1000
Received: from sfoex04.namerica.somorita.com ([192.168.41.2]) by
  smtpgate.somorita.com with Microsoft SMTPSVC(5.0.2195.4905); Wed, 7
 Aug 2002 05:59:31 -0700
Received: from hnlex01.pacific.somorita.com ([192.168.41.2]) by
sfoex04.namerica.somorita.com (InterScan E-Mail VirusWall NT); Wed, 07
Aug 2002 05:59:48 -0700
Received: from hnlex03.pacific.somorita.com ([192.168.23.80]) by
 hnlex01.pacific.somorita.com with Microsoft SMTPSVC(5.0.2195.5329);
 Wed, 7 Aug 2002 05:59:29 -0700
x-mimeole: Produced By Microsoft Exchange V6.0.6249.0
content-class: urn:content-classes:message
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="---_=_NextPart_001_01C23E12.42DD6818"
```

Securing Exchange Server 2000 and Outlook Web Access

Subject: Order status for new long boards Date: Wed, 7 Aug 2002 07:59:27 -0500 Message-ID: <90FDFCE1CC02B147B4948A1F17CC182F05308620@hnlex03.pacific .somorita.com> X-MS-Has-Attach: yes X-MS-TNEF-Correlator: Thread-Topic: Order status for new long boards Thread-Index: AcI5qyfkvY6mPmp0R6+vwS0VTufMeQ== From: "Suriya Supatanasakul" <SSuriya@somorita.com> To: "Bessara, Robert" <RBessara@BobsBoogieBoards.com>

Note that you can trace the path from where the message originated by looking at the earliest hostname and IP address. In this case, the message originated on a server called HNLEX03 with an IP address of 192.168.23.80. It was then transferred to another internal server called HNLEX01, then to a server called SFOEX04, and finally to the organization's SMTP gateway (SMTPGATE).

There is currently not a solution in Exchange 2000 that will allow you to rewrite the SMTP headers or clean them up, though this could be implemented with an SMTP sink. I don't recommend cleaning up the SMTP headers of messages that are being transferred internally because this can make message transport issues more difficult. However, I do recommend finding a way clean up the headers of the message prior to the message leaving your organization. Two products that currently support this feature include the Cisco PIX firewall (www.cisco.com), Check Point's Firewall-1 (www.checkpoint.com), and Clearswift Mail Sweeper (www.mimesweeper.com). Additional vendors have planned for support in their firewall and SMTP scanners in the future.

Auditing for Possible Security Breaches

Auditing Exchange 2000 is essential. If you are not currently auditing your E2K system, you may not even realize you are having security problems. Still worse, you may discover that you have a security problem, and you may not even be able to actually track it down. Auditing breaks down into a couple of categories. These are Windows 2000 event auditing, Exchange 2000 event auditing, and auditing the usage of Internet protocols.

Windows 2000 Event Auditing

One of the essential security auditing tools that you need to take advantage of is the built-in Windows 2000 event auditing that you can turn on through the Local Security Policy or collectively for an entire OU of computers through an Active Directory Group Policy Object. Figure 24 shows the typical audit policy events that I like to configure .

Figure 24 Audit Policy Events for Exchange Servers

🚅 Group Policy			
$ \underline{A}ction \underline{V}iew \Leftarrow \rightarrow \textcircled{E} \overline{\blacksquare} \times \ \overline{\blacksquare} \cancel{2} $			
Tree	Policy 🛆	Computer Setting	
🛃 Exchange Auditing Policies [hnle: 🔺	Audit account logon events	Success, Failure	
🚊 🔬 Computer Configuration	Audit account management	Success, Failure	
😥 💼 Software Settings	Audit directory service access	Not defined	
🚊 👘 🛄 Windows Settings	🕰 Audit logon events	Success, Failure	
Scripts (Startup/Shu	颱Audit object access	Not defined	
🖻 😳 📴 Security Settings	Audit policy change	Success, Failure	
🗄 🤯 Account Policies	🕮 Audit privilege use	Not defined	
Er 🛃 Local Policies	🕮 Audit process tracking	Not defined	
Audit Policy	Audit system events	Success, Failure	
🕀 🖓 User Rights i			
E Security Opt			
Event Log			
System Services			
Hie System			
Software Settings			
	•	 	
J			

The events that I choose to audit typically tell me when someone accesses the server, makes securityor account-related changes to the server, and when someone may have restarted the server. Table 12 shows the events that I tend to log along with an explanation.

Table 12 Recommended Audit Policy Events

Policy	Explanation
Audit account logon events	Audits logons using domain accounts
Audit account management	Audits changes to accounts, such as passwords being reset or group membership changes. This audit event does not always generate the detail I would like, such as if an account is enabled or disabled, just that the account is changed.
Audit logon events	Audits logons using accounts that are local to the member server
Audit policy changes	Audits policy changes such as changing the audit policy
Audit system events	Audits events such as system shutdown or restart

Although I am not a fan of configuring an audit policy that logs every single activity that occurs on a server, I also shy away from minimal auditing or auditing that examines *only* failures. Each additional audit policy you place on the server increases the load on the server by some amount, and it increases the size of the security log files. If you are truly concerned about logging events that may affect the security of your system, you will log not only events where someone has tried and *failed* to accomplish something, but you will also look at events where someone has tried and *succeeded*. This has been my philosophy for some time and it has served me well; though some people think I'm a bit paranoid.

Νοτε

Windows 2000 event logs can grow to quite a significant size very quickly. The default size for these logs is 512KB, and they overwrite data that is only older than seven days. Administrators frequently ignore the warning that an audit log is full and then later wonder why they don't have complete information in their audit logs. Increase the size of your audit logs to a useful and reasonable size. For a typical Exchange 2000 server hosting 1,000 mailboxes, I don't believe it is unreasonable to have log file sizes of 20,480KB (20MB) or even larger. I highly recommend you increase all of your servers' maximum event log sizes to at least 20MB.

Exchange 2000 Event Auditing

There are also a few events that you should enable for Exchange 2000 auditing. In Exchange 5.5, you could find the Diagnostics Logging property page in a couple of different locations, but in Exchange 2000, these events are all centrally located on a single property page on the properties of each server. To enable any type of diagnostics logging for Exchange, you must configure the Diagnostics Logging property page for each server individually. Figure 25 shows the Diagnostics Logging property page for an Exchange 2000 server.

INLEX02 Properties		<u>? ×</u>	
Directory Access Policies General Locales Mailbox M	Security Monitoring anagement Diagnosti	Full-Text Indexing	
Services	Categories		
 \\HNLEX02 MAP4Svc MSExchangeAL MSExchangeDSAcce System Public Folder Mailbox MSExchangeMU MSExchangeMU MSExchangeSA MSExchangeSA MSExchangeSRS Logging level 	Category Transport General General Transport Sending Transport Delivering Transfer Into Gateway Transfer Out Of Gat MTA Connections Logons Access Control Send On Behalf Of Send As Rules Storage Limits	Logging level ▲ None None None None None Medium Medium None Medium None Medium None ▼	
◯ None ◯ Minimum . ⓒ Medium ◯ Maximum			
ОК	Cancel Apply	Help	

Figure 25 Diagnostics Logging for Exchange 2000

In order to accurately track usage of the Exchange 2000 mailboxes, there are a number of event types that I recommend you enable. Table 13 has a list of these categories and the location in which you will find them.

Table 13 Diagnostics Logging Categories for Exchange 2000 Servers

Category	Explanation
MSExchangeIS Mailbox Logons	Tracks access to mailboxes
MSExchangeIS Mailbox Access	Logs events when users attempt to access a mailbox to which they
Control	have no permissions or insufficient permissions
MSExchangelS Mailbox Send As	Logs events when a user uses the Send As permission
MSExchangelS Public Folder Logons	Tracks access to the public folder store
MSExchangeIS Public Folder Access	Logs events when users attempt to access a public folder to which
Control	they have no permissions or insufficient permissions
MSExchangeIS System Virus	Logs events related to virus scanning programs that are AVAPI 2.0–
Scanning	compliant
IMAP4 Connections	Logs information about IMAP4 client connections such as IP address
IMAP4 Authentication	Logs information about IMAP4 client authentication
POP3Svc Connections	Logs information about IMAP4 client connections such as IP address
POP3Svc Authentication	Logs information about POP3 client authentication

Although these are not the only categories of events you can log with Exchange 2000, I consider these to be the bare essential events from a security perspective. Many organizations have requirements for logging additional information such as replication, X.400 MTA connections, and transport-related events. The categories in the preceding table should be set to at least minimum.

When you are scanning your event logs looking for possible intrusions or things that just don't look right, the event IDs in Table 14 may be helpful. These are by no means the only events you should be looking at, but they will help you to narrow down the events that indicate when a user is accessing the store.

Source	ID	Explanation
MSExchangeIS Mailbox	1009	Mailbox access
MSExchangelS Mailbox	1016	Mailbox access by someone other than the mailbox owner
MSExchangeIS Mailbox	1029	Attempted access to mailbox by unauthorized user or user with insufficient
		rights
MSExchangelS Mailbox	1032	Successful use of Send As right
MSExchangelS Public	1235	Attempted access to public folder by unauthorized user or user with
		insufficient rights
IMAP4SVC	1000	IMAP4 client connection established
IMAP4SVC	1010	IMAP4 client successfully logged on
IMAP4Svc	1011	IMAP4 client authentication failed
IMAP4Svc	1043	Maximum number of invalid commands from IMAP4 client has been
		reached; connection dropped
POP3SVC	1000	POP3 client connection established
POP3SVC	1010	POP3 client successfully logged on
POP3SVC	1011	POP3 authentication failed
POP3SVC	1043	Maximum number of invalid commands from POP3 client has been
		reached; connection dropped

Table 14 Exchange 2000 Security-Related Events Found in the Application Log

Logging Internet Client Access

You may also want to log access to the Internet protocol clients for either diagnostics purposes or to track an intruder accessing the server using one of these protocols. I am holding out hope that some third-party vendor will eventually develop a reporting tool so that this information can also be used to generate usage reports for each of the protocols. Though a number of reporting tool vendors do read the HTTP log files, the data they report is from the perspective of Web page usage, and this does not necessarily lend itself to reporting on OWA usage.

Each of the Internet client virtual servers allows you to turn on logging. This is done for each virtual server on the General property page. The only exception is HTTP, which is performed through Internet Services Manager. Each publicly exposed POP3, IMAP4, SMTP, NNTP, and HTTP virtual server has logging enabled. I recommend using the W3C Extended Log File Format.

Once you enable logging and select the file type, click the **Properties** button (the resulting dialog box is shown in Figure 26). The Properties button allows you to specify how much information is in each log file (one hour, day, week, month, etc.), the maximum log file size, whether or not to use the local time when rolling over log files, and the directory for the log files.

X

Extended Logging I	Properties
General Properties	Extended Properties
⊢ New Log Time F	Period
C Hourly	
• Daily	
O Weekly	
O Monthly	
O Unlimited	file size
O When file	e size reaches:

MB

NntpSvc1\exyymmdd.log

Cancel

Figure 26 General Properties for IIS Logging

*

Use local time for file naming and rollover

0K

WARNING

Log file directory: c:NIS-Logs

Log file name:

The default directory for the log files is the \WINNT\SYSTEM32\LOGFILES directory. I recommend moving this to another directory. There is no file management for these log files, so you must purge or archive them manually.

Browse...

Help

Once you have selected the configuration for the log file rollover, directory, and how much information should be in each log, click the **Extended Properties** tab. The Extended Properties tab (shown in Figure 27) is the property page where you select which properties will be logged into the log files. Each type of virtual server will generally require slightly different list properties depending on what you want to find out. For more information on the W3C extended log file format, visit www.w3.org/TR/WD-logfile.html for more information.

Figure 27 Extended Properties Allows You to Configure What Information Will Be Contained in the Log Files



These log files are usually not pretty, and the entries are stored in the log file in the order in which the protocol commands were received. This means that if the SMTP virtual server has more than one simultaneous SMTP conversation, the entries will be interspersed in the log file. The following are recommendations for a minimum amount of logging for SMTP and HTTP. Figure 28 shows a screen capture of an HTTP log as viewed through Visual Notepad.Net. Each field that is logged is separated by a space. To make this more readable, I trim out the first three lines plus the *#Fields:* entry from the fourth line. That leaves me with only the column headings and data. I then do a global search and replace and replace all spaces with commas (,). I can then save this file as a CSV file and retrieve it into Excel.

Figure 28 Sample Log File Generated by an HTTP Virtual Server

🖉 ex020908.log - Notepad
File Edit Format Help
₩Software: Microsoft Internet Information Services 5.0
#version: 1.0
#Date: 2002-09-08 10:01:55
2002-09-08 20:41:03 127 0 1 administrator W35V/1 HNIEX02 127 0 1 443 POLI /exchange/Hait
2002-09-08 20:43:03 127.0.0.1 administrator W35VC1 HNLEX02 127.0.0.1 443 POLL /exchange/keit
2002-09-08 20:45:03 127.0.0.1 administrator W3SVC1 HNLEX02 127.0.0.1 443 POLL /exchange/keith
2002-09-08 20:45:22 192.168.254.50 - W3SVC1 HNLEX02 192.168.254.12 80 OPTIONS / - 403 5 3942
2002-09-08 20:47:03 127.0.0.1 administrator W3SVC1 HNLEX02 127.0.0.1 443 POLL /exchange/keit
2002-09-08 20:49:03 127.0.0.1 administrator W35VC1 HNLEX02 127.0.0.1 443 POLL /exchange/keit
2002-09-08 20:51:03 127.0.0.1 administrator W35VC1 HNLEXU2 127.0.0.1 443 POLL /exchange/Keitr
2002-09-08 20:53:32 192 168 254 50 - W35VC1 HNLEX02 192 168 254 12 80 GET /evchange/keiter
2002-09-08 20:53:46 192.168.254.50 - W35VC1 HNLEX02 192.168.254.12 80 GET /certenroll/hnlex0:
2002-09-08 20:53:51 192.168.254.50 - W3SVC1 HNLEX02 192.168.254.12 443 GET /exchange/keiths
2002-09-08 20:53:57 192.168.254.50 keiths w3SVC1 HNLEX02 192.168.254.12 443 GET /exchange/ke
2002-09-08 20:53:57 192.168.254.50 keiths W3SVC1 HNLEX02 192.168.254.12 443 GET /exchange/ke
2002-09-08 20:53:57 192.168.254.50 Kerths W35VCI HNLEX02 192.168.254.12 443 GET /exchange/ke
2002-09-08 20:53:57 192.108.234.30 - W35VCI HNLEX02 192.108.234.12 443 GET /exchweb/controls,
2002-09-08 20:53:57 192 168 254 50 keite w35VCI INLEAUZ 192.108.254.12 445 GEI / EXClimed/Controls/
2002-09-08 20:53:57 192.168.254.50 - W35VC1 HNLEX02 192.168.254.12 443 GET /exchweb/img/logo
2002-09-08 20:53:57 192.168.254.50 - W3SVC1 HNLEX02 192.168.254.12 443 GET /exchweb/controls,
2002-09-08 20:53:58 192.168.254.50 - W3SVC1 HNLEX02 192.168.254.12 443 GET /exchweb/controls,
2002-09-08 20:53:58 192.168.254.50 - W3SVC1 HNLEX02 192.168.254.12 443 GET /exchweb/controls,
2002-09-08 20:53:58 192.168.254.50 - W35VC1 HNLEX02 192.168.254.12 443 GET /exchweb/controls,

SMTP Logging

For SMTP virtual servers, you are probably most interested in the IP address of the client on the other side of the connection and the SMTP command verb that they are using against your server. Table 15 has the properties that I recommend be configure d for SMTP logging.

Table 13 Logging to Log for Own Vintual Oervers

Property	Explanation
Date	Date (in UTC/GMT) of the connection
Time	Time (in UTC/GMT) of the connection
c-ip	Destination IP address if outgoing SMTP, originating IP
	if inbound
s-ip	IP of the SMTP virtual server if inbound SMTP, "-" if
	outbound
cs-method	SMTP verb (such as MAIL FROM: or DATA)
cs-uri-query	SMTP verb options or response (such as
	<jim@somorita.com 250="" ok)<="" or="" td=""></jim@somorita.com>
cs-bytes	Size of inbound responses and data

HTTP Logging

For inbound Web requests, you are going to be interested in a slightly different set of parameters than you will be for SMTP. One option that may not be of much interest is the *cs(Referrer)*, which indicates if the client was referred to this HTTP virtual server from another Web site or page. The other is the *cs(User-Agent)* which indicates which version of the Web browser is connected; an example of this field is Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0), which indicates Internet Explorer 5.5 running on Windows 2000. This figure may be useful if you are monitoring the different versions of browsers that are using your server. Table 16 shows the properties that I recommend for logging on publicly exposed HTTP virtual servers.

Table 16 Logging to Log for HTTP Virtual Servers

Property	Explanation
56	Securing Exchange Server 2000 and Outlook Web Access

Date	Date (in UTC/GMT) of the connection.
Time	Time (in UTC/GMT) of the connection.
с-ір	Source IP address of the OWA client.
s-ip	Local IP address of the HTTP virtual server through
	which the connection was made.
s-port	The local TCP port that the client is using; this will be
	either 80 or 443 depending on whether you require
	SSL. This may or may not be useful to you; I usually
	log it.
cs-method	Method used by the client, such as GET, POST,
	SUBSCRIBE, POLL, SEARCH.
cs-uri-stem	Web page or virtual directory to which the client was
	connecting.
cs-uri-query	Command executed by the client.
sc-bytes	Amount of data transmitted by the server to the client.
cs-bytes	Amount of data transmitted by the client to the server.
cs(User-Agent)	Web browser and operating system version of client.
Cs(Referer)	Referring Web site or page.

WARNING

Enabling HTTP logging will generate huge log files with just a very few OWA connections due to the number of requests that hit the server for each message opened. A simple request to open the default OWA mailbox page and send a single OWA e-mail message generates 140 entries in the log file. Plus each currently connected OWA client (running IE 5.0 or later) polls the server once every two minutes. Remember to purge or archive older logs.

Damage & Defense

A Lack of Auditing and Logging Will Come Back to Haunt You!

ZZZ Company had a serious incident in their messaging system. Someone was sending death threats to an employee; the message claimed that the employee was being watched and when she was home alone she would be attacked. Naturally, the frightened employee contacted her manager, and the manager contacted the IT department to see from where the messages were originating.

Unfortunately, the only information the IT department could discern from the message was that it had originated on the same server as the user's mailbox; they were able to figure this out because the message had no Internet headers. The Internet headers can be viewed from within Outlook 2000 or 2002 by opening the message and clicking **View | Options**. The message was being sent from a user account that at least eight people had the username and password.

Through a process of elimination and discussion with several people in the employee's department, the manager and the IT staff were able to deduce a possible sender of the threatening e-mails. The person suspected was a former employee that had a disagreement with the person being threatened. However, the evidence was all circumstantial and certainly nothing that would hold up in a court of law.

ZZZ Company made several errors with the operation of their Exchange 2000 and Active Directory organization. All of these led to a serious lack of information about who was using system resources and from where. The following is a list of the problems with ZZZ Company's Exchange 2000 configuration:

No user account with a mailbox should ever be shared by more than one employee.

A Windows 2000 auditing policy should be enabled for all Exchange 2000 servers.

HTTP protocol logging should be enabled to track OWA users.

The Information Store's Mailbox | Logons diagnostics logging level should be set to at least Minimum to track access to mailboxes.

Message tracking logs should be enabled and at least 15 days worth of logs should be kept.

Securing Exchange Server 2000 and Outlook Web Access

SMTP protocol logging should be enabled to track inbound and outbound SMTP communications.

Fortunately, we made some adjustments to their system, and the person making the threats returned for another visit. If you are curious about the source of the problem, we did ascertain that it was the disgruntled former employee, and this person was accessing the server remotely via OWA. Once we enabled HTTP protocol logging, we were able to find the time when that account was accessing the server, and we were able to find the IP address from which the person was accessing OWA. From that point, it was simple matter to turn this incident over to the police department.

Securing MAPI Clients

One of the places that people often forget to focus their security effort is the client side. As far as the messaging system is concerned, this is one of the most vulnerable areas because this is where messages are the easiest to read. This is also the location from which e-mail-based viruses are spread. In this section, I make a couple of recommendations to help keep your messaging system safe from viruses and protect the message content.

Message Content Vulnerabilities

Any messaging content that is stored on the client side is vulnerable to being viewed by an intruder. This is because the local file systems on workstations are usually much easier to compromise than a physically secured Exchange server. The following are some recommendations for helping to ensure that the client-side of the messaging security equation is secure:

If you are concerned about messaging security, do not allow your users to use POP3 or IMAP4 client solutions. Deploy only Outlook MAPI clients. Locally stored data in POP3 and IMAP4 clients is too easily compromised.

Do not allow users to store critical e-mail in PST files; in a very security-conscious organization, PST files should never be used. Even though PST files can be password protected, there are a couple of utilities that are easily downloadable that can crack these passwords.

Require users to lock their workstations prior to leaving their desks.

Enable and require SSL for users using OWA

Protecting Against Message-Based Viruses at the Client

Almost all of the e-mail-based viruses over the past couple of years have been targeted at and spread by MAPI clients. These viruses open your global address list or personal address books and send themselves to everyone in your address list. For this reason, providing additional anti-virus protect at the client is essential. The following is a list of anti-virus precautions that you should take at the client side:

If you are not running Outlook 2002, install the Outlook Security Update for Outlook 98 and 2000. This disables some of the features that allow viruses to spread from the Outlook client.

If you are running Outlook 2002, configure the Outlook Security Template to restrict dangerous attachments from being opened at the Outlook client.

All clients must have anti-virus software installed. The software should be able to scan email messages when they are opened or prepared.

Anti-virus client software and signature files must be kept up to date.

Outlook 2002 SR-1 includes a feature that allows users to read HTML messages as plain text, thus reducing the potential danger associated with HTML mail. See www.slipstick.com/dev/code/zaphtml.htm for more information.

NOTE

For more information about the Outlook Email Security Update, visit Slipstick System's Outlook Security update page at www.slipstick.com/outlook/esecup.htm. If you are interested in learning more about using the Outlook 2002 security features, read about the Outlook Security Template from the Office XP Resource Kit or in Chapter 2 of the NSA's Guide to Secure Configuration and Administration of Microsoft Exchange 2000; you can download it at http://nsa2.www.conxion.com/win2k/download.htm.

Enabling Message Encryption (S/MIME)

If you are truly paranoid about the security of your messaging data, and all of the other precautions you have taken have not made you feel at ease, enabling your users to use S/MIME (Secure/MIME) may be the next step for you. S/MIME defines extensions to the MIME standard that allow a user to send encrypted and/or digitally signed messages between any two messaging clients as long as both clients support S/MIME.

Note

For more information on S/MIME, see RFCs 2311 and 2633. The full text of the RFCs can be found at www.rfc-editor.org.

When using an S/MIME solution, the message body and attachments are encrypted at the sender's computer prior to being sent to the sender's home server. The message remains encrypted while the message is transmitted and while it is stored in the recipient's home message store. It is decrypted only when the intended recipient opens the message. The only catch is that the sender must have a digital certificate (X.509v3) for all intended recipients of the message.

Implementing an S/MIME solution for your users will most definitely increase your support load. Certificates have to be issued to users, certificates expire and have to be renewed, user's computers are rebuilt and they lose their certificates, and users will inevitably have support-related questions about this new feature. One of the biggest decisions you will have to make is whether you are going to get your mail certificates from a trusted authority (such as Thawte, Verisign, etc.) or whether you are going to "roll your own."

If you have only a few users that require message encryption or digital signatures, you are probably better off going to a third-party certificate authority. These can be less than \$15 per e-mail address per year. Once users get their certificates, they can forward them on to users that need to send them encrypted messages, or you can even publish it to Active Directory so that other users in your organization can easily send them secure messages.

On the other hand, if you are going to have many users that require digital certificates, you should consider deploying the Exchange 2000 Key Management Server. The requirements for the Exchange 2000 Key Management Server are as follows:

There must be a Windows 2000 Enterprise CA installed and configure d to issue Enrollment Agent (Computer), Exchange User, and Exchange Signature Only certificates. You cannot install the Exchange 2000 KMS on an Exchange 2000 server in a cluster.

Once the Key Management Server is installed, you will find two new objects in the Administrative Group that contains the Exchange 2000 Key Management Server. This is the Encryption Configuration object and the Key Manager. They Key Manager is used to issue certificates, revoke certificates, and recover lost keys. The Encryption Configuration object is used to configure the type of encryption that users in

this administrative group require. Unless you are supporting older encryption clients from Exchange 4.0 and 5.0, you should always choose S/MIME as the security message format.

Following Best Practices

There are a number of best practices that I recommend all Exchange 2000 administrators follow to keep their Exchange organizations secure and operating. Some of these are administrative practices, but others are simply things that you need to teach your user community about. The following is a list of best practices for keeping your Exchange data secure:

Apply all W2K, E2K, IIS, and IE SPs and fixes.

Apply Prohibit Send and Receive limits for all users.

Apply Maximum incoming and outgoing message size for all users.

Implement SSL for all Internet protocols.

Update all Outlook clients to a minimum of Outlook 2000 or Outlook 2002 with the security updates.

Perform daily reviews of System, Application, and Security logs.

Ensure that daily backups are performed and that the backup tapes are always secure.

Apply NTFS security to all data directories and log directories, including IIS logs.

Restrict who is allowed to send mail to any distribution list with more than 25 members; this will help prevent abuse of the e-mail system and reduce the likelihood that viruses can be sent to large numbers of users.

Remove shared folder Everyone permissions for all shared folders.

Restrict the Everyone group's administrative permission to create top-level public folders.

Designate servers to perform specific roles, and don't allow servers to perform multiple roles (such as a Web server *and* an OWA server.) This allows you to tighten security as much as possible for that specific server role.

Never configure an SMTP server to allow open relay; there is no reason for you to have an open SMTP relay.

Never configure administrative and operator accounts with mailboxes.

Statically map the system attendant's NSPI/DSProxy TCP ports and the information store's TCP port to an organizational standard.

Regularly purge or archive virtual server and message tracking logs. These logs should be protected so that only administrators can access them.

In addition to best practices for security, I have a series of practices that I recommend all Exchange administrators follow in order to keep their Exchange organizations stable and operating. Although most of these practices are not necessarily security-related they are nonetheless important. I recommend these procedures be incorporated into daily operations:

Perform daily backups and examine the event logs to confirm that the backup occurred.

Scan the event logs daily for security- and operations-related events.

Confirm that virus signatures are up to date. Note any recent virus activity.

Check the available disk space on all disks.

Look at the SMTP queues (and MTA queues if applicable) for unusual queue growth.

Finally, there are a couple of things that I recommend be incorporated into an ongoing effort to keep the end-user community educated, to ensure that users make good use of the messaging system, and to keep their own data secure:

Users should be taught to treat e-mail data as they would any other confidential or proprietary information.

OWA users *must* close the Web browser window to terminate the HTTP session with the OWA server.

Users should be reminded not to use their company/organization e-mail address on Web sites when registering for contests, doing online banking, requesting information, etc. This will help keep down the amount of spam they receive.

The organization should develop an acceptable use policy covering the usage of the e-mail system. This policy should define things that the end user should and should not do with the e-mail system. This can include sending out pictures, objectionable jokes, garage sale notices, or large files.

Security Checklist

I have broken down a couple of basic checklists to follow when securing Exchange 2000. Most of the items on these checklists are for all servers regardless of how secure you want to be. However, the last checklist is for those of us that are a little more paranoid. I'll let you decide how paranoid you need to be.

Before Starting Exchange Review

Our first checklist takes us to the operating system and IIS level. Before we even consider securing Exchange 2000, the underlying OS must be secured.

Confirm that the OS is patched to the latest possible level

(http://windowsupdate.microsoft.com).

Disable unnecessary W2k Services .

Remove the IISSamples, IISHelp, IISAdmin, MSADC, Printers, and Scripts IIS virtual directories, or let IIS Lockdown handle that for you.

Confirm that local usernames have strong passwords and that the guest account is disabled (member servers). The local administrator and guest preferably should be renamed.

Disable NetBIOS on all network adapters unless the E2K server is providing file and print services to older clients. Unless you have only a single server in your organization, clients should never use the Exchange 2000 server for file and print services.

Enable auditing (local logons, security policy changes, system events, user and group management).

Organize Exchange 2000 servers into their own Active Directory OU.

Increase event System, Security, and Application event log sizes to at least 20,480K.

Standard Exchange 2000

Now that the platform is secure, let's move on to Exchange 2000. One of the things I'm going to ask you to do is to disable the unnecessary services. However, I can't tell you what is unnecessary without looking at your environment. Based on information in this chapter, you need to look at the Exchange 2000 (and Windows 2000) services and decide if there are services that your Exchange 2000 server does not require.

This checklist should be completed before putting this server into production. This checklist should be good for all Exchange 2000 servers whether they are front-end or back-end servers:

Apply Exchange 2000 SP3.

61

Install Exchange AVAPI 2.0 aware anti-virus software.

Filter or restrict ability to receive forbidden file attachment list.

Enable/require SSL for HTTP, POP3, IMAP4, and NNTP clients if no front-end servers.

Disable unnecessary/unused Exchange services (POP3, IMAP4, NNTP, Event service, MSSearch, SRS, MTA).

Remove Everyone group from file shares.

Enable Exchange 2000 Diagnostics Logging for mailbox store and public folder stores. Enable HTTP protocol logs.

Enable SMTP protocol logs.

Enable message tracking.

Globally apply maximum incoming and outgoing message sizes as well as maximum recipients per message.

For each mailbox store, apply mailbox limits, including Prohibit Send and Receive limits. Implement physical access controls over all Exchange 2000 servers.

Distribute Outlook 98/2000 e-mail security fix.

Confirm (and test) that any externally exposed SMTP system is not allowed to do SMTP relay.

Confirm that only limited users or groups have administrative permissions at the Exchange Organization level.

Confirm that no user or group has been given Receive As or Send As permissions to the Organization or to an Administrative Group.

Front-End/Back-End Server Considerations

Here are a few considerations for servers that are running in a front-end/back-end configuration.

Disable unnecessary services (POP3, IMAP4, NNTP, IS, SMTP, MSSearch, Exchange Event, Exchange Management, MTA).

Enable/require SSL for HTTP, POP3, IMAP4, and NNTP clients.

High Security Exchange 2000

If you have decided to go for "extreme" security, you have come to the right checklist. Each of these is going to require a bit more work on your part, especially if you decide to distribute certificates:

Put all Exchange 2000 servers on switched segments.

Implement IPSec between all Exchange 2000 servers and to/from Windows 2000 domain controllers.

Distribute X.509v3 certificates to all users to allow use of message signing and encryption. Implement a data center firewall between users and all servers on the organization backbone.

Configure E2K to accept only specific MAPI client versions.

Configure storage groups to zero out deleted database pages.

Require Outlook client to do MAPI over RPC encryption.

Implement tight tape backup/backup media access controls.

Configure hubs and switches to accept communication from specified MAC addresses only (requires manageable hubs and switches).

Alternative Controls

I have almost ignored the subject of content inspection and anti-spam systems, mainly because antispam systems and content inspection systems increase the amount of administrative overhead by quite a bit. This is because anything that falls under the scrutiny of these systems usually has to be inspected manually by an administrator. I know a number companies that successfully use content inspections systems such as Mail Sweeper, but be aware, these systems will increase your overall overhead.

Implement content inspection to look for unauthorized content, naughty words, etc. Deploy anti-spam measures.

Educate users about spam, viruses, and acceptable use of the messaging system; also educate them about giving out their e-mail addresses.

Summary

How secure do you want to be today? I know the answer already. You want to be as secure as you can possibly be. There is a fairly well known security axiom that states "You should be exactly as paranoid as it is cost-effective to be." Most all of the things I have mentioned in this ebook are more than reasonable steps when it comes to securing your messaging data. The only thing that I consider "extreme" is rolling out S/MIME capabilities for your entire user community.

This is the paradox of security. How much administrative effort (and thus cost) is worth securing your organization? If your organization is using Exchange primarily for sending messages about having lunch, storing contacts, and appointments, you should take reasonable efforts to secure this data. But the more sensitive the data you are sending back and forth, the more "extreme" you should become. No one can make this decision except for you and your superiors. The question that you need to be asking is "How much more money is it worth to be "extremely" secure versus just secure?"

Throughout this chapter, I covered some of the basic architectural components of Exchange 2000 and outlined Exchange's dependency on Windows 2000, Internet Information Server, and Active Directory. When you begin the process of securing Exchange 2000, these are the components you have to start with first.

I also discussed many of the vulnerabilities with Exchange 2000 (and other messaging systems.) You must take steps to identify these problems in your own environment and decide which of these vulnerabilities needs to be fixed and balance the cost and benefit of addressing some of these.

Finally, you need to ensure that you are auditing the important events that occur on your system so that you can adequately respond to problems and potential intrusions. As long as you follow good operational procedures and best practices, you can keep your Exchange 2000 system running and safe from intruders.

Solutions Fast Track

Introducing Exchange 2000

Exchange 2000 is tightly integrated with Windows 2000 and Internet Information Server. Exchange 2000's basic architecture is similar in some respects to Exchange 5.5, but the significant difference is that Exchange 2000 does not have its own directory service. An additional load will be placed on the Windows 2000 domain controllers and global catalog servers for each Exchange 2000 server.

Understanding the Basic Security Risks Associated with Exchange 2000

Administrative mistakes can give users or unauthorized administrators permissions to manage Exchange 2000 servers or even to open users' mailboxes.

E-mail messages, when transmitted via SMTP, are inherently insecure.

Using Windows 2000 logon names as part of the SMTP address is a bad security practice.

Exchange data files and log files on Exchange 2000 servers can give away a lot of information to an intruder.

The Windows 2000 operating system must be properly secured; this is the biggest vulnerability for Exchange 2000.

Preventing Exchange Security Problems

Service packs and security fixes must be up-to-date on all Exchange 2000 servers as well as Windows 2000 domain controllers.

Adequate steps must be taken to prevent or control the outbreak of e-mail-based viruses through a combination of client side, Exchange server, and SMTP virus scanning.

Message size limits and mailbox storage limits should be imposed.

Implementing SSL is one of the critical steps necessary to improve Internet client security. Internet Information Server should be locked down with IIS Lockdown using the Exchange 2000 template.

Auditing for Possible Security Breaches

Windows 2000 auditing is critical to understanding who is doing what with the operating system.

Exchange 2000 diagnostics logging will provide you with a better understanding of the types of access happening on the Exchange server.

Protocol logging is the key to tracking potential access from the outside world.

Following Best Practices

Develop good operational procedures, including plans for what will be done daily on each Exchange 2000 server.

Keep Exchange 2000 and Windows 2000 up-to-date with patches and security updates. Properly manage the event logs and protocol logs that each Exchange server creates.

Links to Sites

Here are some additional resources that you may find useful when coming up to speed on Exchange 2000 security and deployments:

Exchange 2000 Security Operations Guide There is a lot of information on generic Windows 2000 security issues, but not as much information can be found about Exchange 2000 security. In the summer of 2002, Microsoft released their Exchange 2000 Security Operations Guide. This includes a 123-page document on securing Exchange 2000 and refers to some template files that you can use to further tighten security on Exchange 2000

through Active Directory Group Policy Objects. This includes a template for baseline security of Exchange 2000 servers and then an incremental template for either front-end servers or back-end servers. In some instances, I think these templates lock down security almost too tightly on some servers. This becomes apparent when you have certain procedures you have to follow to enable some services in order to apply service packs. You can download the guide at www.microsoft.com/downloads/release.asp?releaseid=40807.

Exchange 2000 Front-End and Back-End Topology Guide Microsoft also publishes an excellent white paper on Exchange 2000 front-end/back-end server planning and deployment called the Exchange 2000 Front-End and Back-End Topology guide. It can be downloaded from

www.microsoft.com/exchange/techinfo/deployment/2000/E2KFrontBack.asp.

National Security Agency's Guide to Secure Configuration and Administration of Microsoft Exchange 2000 Another excellent resource on securing Exchange 2000 is the National Security Agency's Guide to Secure Configuration and Administration of Microsoft Exchange 2000. This 160-page guide can be downloaded from http://nsa2.www.conxion.com/win2k/download.htm.

SecurityFocus One of the best sites on the Internet for security-related information and discussion is SecurityFocus (www.securityfocus.com). This site has information about a number of security related mailing lists, bugs, and articles. A couple of articles that you should search for and read include "Securing your Exchange Server Installation" by Monty Hall and "Securing Exchange 2000 Part One and Part Two" by Chris Weber.

www.exchangeadmin.com The Exchange & Outlook Administrator newsletter is one of the few publications for which I actually pay. Their Web site has an archive of all articles, Q&A columns, and features. These can be found at www.exchangeadmin.com. Reading recent articles does require a subscription.

Mailing Lists

There are two primary mailing lists for Exchange administrators, but neither of these are securityspecific. Before posting to either of these lists, I *strongly* recommend that you read the Exchange 5.5 and Exchange 2000 FAQs. On lists with the volume of postings that these lists see, a lot of questions are asked multiple times. These FAQs are generously hosted and maintained by Simpler-Webb, Inc along with help of the regular members on these lists. You can find both FAQs at www.swinc.com/resource/exchange.htm.

Swynk: Microsoft Exchange Discussions The Swynk list offers a mix of Exchange 2000 and Exchange 5.5 questions. Go to www.swynk.com and click on the Discussion Lists link in the side menu for information on joining this list. Be warned, on a busy day, this list generates 100+ messages, and there is a pretty high "noise to signal" ratio on this list. I have about a two-year archive of this list which contains over 71,000 messages. You might actually want to subscribe a public folder SMTP address to the list rather than your own mailbox. This makes management of the data you receive a little easier.

Yahoo: Exchange2000 This list has over 1,500 members and is generally a little more on topic than the Swynk list. You can become a member of this list by visiting http://groups.yahoo.com/group/Exchange2000.

Other Books of Interest

The following are some additional books that you may find useful when installing, configuring, and securing Exchange 2000.

McBee, Jim. Exchange Server 2000 24seven. Sybex, 2000.

Redmond, Tony. *Microsoft Exchange Server for Windows 2000: Planning, Design and Implementation.* Digital Press, 2000.

McClure, Stuart, Joel Scambray. *Hacking Exposed: Windows 2000*. Osborne/McGraw-Hill, 2001.

Exchange 2000 Resource Kit. Microsoft Press, 2000.

he Honeynet Project. *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community.* Addison-Wesley, 2002.

Tung, Brian. Kerberos: A Network Authentication System. Addison-Wesley, 1999.

Feghhi, Jalal, Jalil Feghhi, Peter Williams. *Digital Certificates: Applied Internet Security.* Addison-Wesley, 1999.

Stallings, William. *Cryptography and Network Security: Principals and Practice,* Second Edition. Prentice Hall, 1995.

Frequently Asked Questions

- **Q:** Do I need Exchange server-based anti-virus software if all of my clients already have client-based scanning software?
- A: Absolutely. There is always the possibility that the signatures on the client will get out of date or will not catch a virus. A good practice is to use a different vendor's virus software on the server than you do on the workstation.
- Q: Should I enable SSL for my Outlook Web Access clients?
- **A:** This is another definitive YES! You should enable and require SSL for all Internet protocol clients such as OWA (HTTP), POP3, IMAP4, and NNTP.
- Q: You did not mention Exchange 2000's Instant Messaging feature; how secure is Instant Messaging?
- A: Not secure at all. The method of authentication is NTLM; NTLM is reasonably easy to crack given the right tools and some time to mount a brute force attack. The data is transferred from the IM client to the IM server using HTTP and XML in clear text. This currently cannot be changed to SSL and, in my opinion, is inherently insecure and should not be used for critical business communications.
- **Q:** Do you have a specific recommendation for anti-virus software, SMTP scanners, or content inspection?
- A: No. There are many good systems on the market, and it is difficult to point to one tool that would do everything you might need it to do. I have a list of these tools at www.somorita.com/exchange2000/vapi20.asp. I suggest you develop a list of criteria that you require and review each of these to find the tool or tools that is right for you.
- Q: Do you think that remote users can safely be allowed to read their e-mail on the internal network?
- A: Yes. With reasonable precautions, I think remote users can be allowed into the network. For Outlook MAPI clients, I think the remote client should come in through a VPN connection. VPN connections can be made even more secure with authentication devices such as SecureID. For other remote clients, I recommend using only OWA. Configuring an OWA front-end server in a well-secured DMZ provides a reasonable good level of security.
- **Q:** What three points should we focus on to get started that will give us the highest return for our investment?
- A: For starters: a properly configure d firewall, W2K/IIS/IE/E2K service packs, and Exchange-aware anti-virus software.

- **Q:** How can administrators disallow the Exchange server to return internal IP addresses in the e-mail headers?
- A: Exchange 2000 cannot strip out headers without custom programming. I recommend you use a third-party product such as the Cisco PIX firewall or Clearswift's Mail Sweeper. Direct all outbound mail through one of these products and have it rewrite the SMTP headers for you so that internal hosts are removed from the SMTP header.
- Q: Where are the biggest risks?
- A: Most of the vulnerabilities associated with Exchange have actually come through IIS. That is why W2K/IIS/E2K service packs, IIS lockdown, and URLscan are so important.
- Q: What do you see as the most neglected Exchange 2000 security procedures?
- A: All of them! Servers that are directly exposed to the Internet; no service packs; missing or out-ofdate virus scanning; non-existent tape media security procedures; no physical security; administrators that have access to all users mailboxes.