

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering "Auditing Systems, Applications, and the Cloud (Audit 507)" at http://www.giac.org/registration/gsna

Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

GSNA Practical Version 2.1 – Option 1

Dan Holt

June 2003

liting Microsoft Exchange 2000 Server	An Administrator's Perspe
TABLE OF CONTENTS	
ABSTRACT	4
RESEARCH IN AUDIT. MEASUREMENT PRACTICE. AN	D CONTROL 4
,	
Identify the system to be audited	4
Evaluate the risk to the system	7
What is the current state of practice, if any?	
	10
	10
Inter-destion 6	N AN
Introduction	10
Checklist	10
Audit Step #1	10 11
Audit Stop #2	I1 12
Audit Step #3	12 12
Δudit Step #4	12 13
Audit Step #6	13 14
Audit Step #7	14
Audit Step #8	15
Audit Step #9	10
Audit Step #10	17
Audit Step #11	17
Audit Step #12	18
Audit Step #13	19
Audit Step #14	19
Audit Step #15	21
Audit Step #16	23
Audit Step #17 📉	24
Audit Step #18	25
Audit Step #19	25
Audit Step #20	26
Audit Step #21	27
	~~~
	28
Conduct the audit	28
Audit Step #3FAIL	28
Audit Step #4FAIL	
Audit Step #5PASS	36
Audit Step #7PASS	38
Audit Step #8PASS	39

Auditing Microsoft Exchange 2000 Server	An Administrator's Perspective
Audit Step #9PASS	40
Audit Step #14FAIL	42
Audit Step #16FAIL	47
Audit Step #18FAIL	49
Audit Step #20FAIL	50
Measure Residual Risk	51
Is the system auditable?	53
RISK ASSESSMENT – FOR ADMINISTRATORS	53
Summary	53
Background / Risk	53
System changes and further testing	55
System justification	66
· · ·	
	68
<u>REFERENCES</u>	00
APPENDIX A	

## ABSTRACT

Email systems have gone from nice to have communication mediums to businesscritical in today's Corporate World. Even as a business critical system, companies are experiencing unnecessary downtime, compromised data, and loss of productivity. Understanding the security practices and having a standardized auditing procedure can significantly decrease risks. Naturally, the importance of these risks require us administrators to maintain the highest level of confidentially, integrity, and availability of a messaging server. Coupled with these facts, we have a consolidated messaging and collaboration server designed to provide email, calendaring, chat rooms, message boards, and even be a web server. The complexity in Microsoft Exchange 2000 Server demands that security takes a front seat and auditing becomes a regular process for the administrators.

## **Research in Audit, Measurement Practice, and Control**

### Identify the system to be audited

I am auditing the production Microsoft Exchange 2000 Server infrastructure (Front-End and Back-End servers) in a biotech company that builds software and manages genomic data for major pharmaceutical companies. The systems act as the central messaging and workflow collaboration for the company employees. For privacy reasons, the company is referred to as Soft4Genome. At Soft4Genome, it is critical to maintain the highest level of confidentiality for their Trade Secrets that are commonly called Intellectual Property (IP). Additionally, confidentiality is extremely critical to Big Pharma, because our solutions help Therapeutical Researchers target and discover new drugs. The loss of confidentiality is potentially a loss in excess of \$1 billion. How does this relate to Microsoft Exchange Server 2000? Exchange is the central form of communication amongst employees, clients, and partners. At times, confidential data crosses the Exchange Server. Note: "Exchange Server" will be commonly used throughout the paper. Exchange Server refers to both the Front-End and Back-End servers unless specified.

Besides email, the Exchange Server provides calendaring, resource management, customer support, and other collaboration and work flow operations. Sensitive data with engineering designs, product schedules, roadmaps, and financial information are on the Exchange Server. It is common for users to forget the sensitivity of data moving across email and other parts of the Exchange Server.

In 2001, Filipe Custodio wrote a GSNA paper on Exchange 5.5 and Outlook with a focus on AntiVirus protection.¹ This paper will build upon Filipe's AntiVirus and the Outlook client auditing by focusing on the design of the Exchange Server and include Outlook Web Access (OWA). Additionally, there are significant differences in the newer version, Exchange 2000, especially with the Active Directory and IIS integration that changed the underlying security. Today, almost every organization is now including

¹ Custodio, Filipe, "Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000)." September 2001. URL: <u>http://www.giac.org/practical/Filipe_Custodio_GSNA.zip</u> (Feb 1, 2003).

Outlook Web Access with their Exchange 2000 implementation. For confidentiality, it is also imperative that OWA has the proper design to secure the box, email, and accounts. OWA is used to publish email in a web browser through a secure session over the Internet with similar functionality as the Outlook client.

It is important to note that Exchange has only become a more prominent player in corporate messaging and collaboration server market. Microsoft increased their market share to 58% with the closest competitor, Notes, at 28% market share.² Compare this to 1997 when Notes had almost 3 users to every 1 Exchange user.³ As we have seen in other market leading products like Windows operating systems, the exploits increase exponentially with the increase in market share. Moreover, with Microsoft's "easy to administer" philosophy, we still have too many administrators without the proper training and experience managing the security of critical Exchange Servers. Therefore, this paper gives back to the Systems Administrator, Auditing, and Security community a solid checklist to ensure that all administrators are properly securing their Exchange 2000 Servers.

The methodology of auditing a Microsoft Exchange 2000 Server will be the result of Best Practices by technology leaders, Microsoft, and personal experience.

Due to the limited scope of this paper, the following audit and risk assessment will not be included: Routers, Firewalls, detailed Microsoft Windows 2000 Server. Although, it is critical to note that without proper security steps taken on the network layer and on the host operating system, Windows 2000 Server, all Microsoft Exchange 2000 Server auditing and security enhancements are nullified. This paper is meant to build upon a strong security foundation security and auditing process already being completed on the network and Windows 2000 Server. Moreover, new vulnerabilities are discovered on a regular basis; therefore, it is important that administrators stay current with the new vulnerabilities/exploits and learn how to mitigate their risks.

Exchange 2000 is a unique application, where the controls are mainly managed by another application, Active Directory. Therefore the input controls for Active Directory on Windows 2000 Server are critical to the security of Exchange 2000. An entire paper can be devoted to the controls of Exchange 2000 and dependent applications and devices. I'll briefly mention the major controls.

² Ferris, David & Sampson, Michael, "The Corporate Email Market, 2001-2005," Ferris Research, March 2001.

³ Hudgins-Bonafield, Christy, "Messaging Migration: It Pays To Do You Homework," Network Computing, Jun 15, 1998. URL: <u>http://www.networkcomputing.com/911/911f1.html</u> (Apr 21, 2003).

#### Controls

Active DirectoryXActive Directory—User rightsXAntivirusXBackup System, Process, & TapesXChange Management Policy and ProceduresXDisaster Recovery PlanXEmail Use PolicyXEncryption (128-bit) for web server (OWA)XExchange System ManagerXFile Level SecurityXLogging—Network, OS and ExchangeXMultiLayered Network & Security DesignXGeneral Operating System ControlsXPassword complexityXPhysical AccessXUser and Administrator AwarenessX	CONTROLS	Input	Processing	Output
Active Directory—User rightsXXXAntivirusXXXXBackup System, Process, & TapesXXXChange Management Policy and ProceduresXXXDisaster Recovery PlanXXXEmail Use PolicyXXXEncryption (128-bit) for web server (OWA)XXExchange System ManagerXXFile Level SecurityXXLogging—Network, OS and ExchangeXXMultiLayered Network & Security DesignXXGeneral Operating System ControlsXXPassword complexityXXPhysical AccessXXCorporate IT PoliciesXXUser and Administrator AwarenessXX	Active Directory			Х
AntivirusXXXXBackup System, Process, & TapesXXXChange Management Policy and ProceduresXXXDisaster Recovery PlanXXXEmail Use PolicyXXXEncryption (128-bit) for web server (OWA)XXExchange System ManagerXXFile Level SecurityXXLogging—Network, OS and ExchangeXXMultiLayered Network & Security DesignXXGeneral Operating System ControlsXXPassword complexityXXPhysical AccessXXCorporate IT PoliciesXXUser and Administrator AwarenessXX	Active Directory—User rights	Х		0
Backup System, Process, & TapesXXChange Management Policy and ProceduresXXDisaster Recovery PlanXXEmail Use PolicyXXEncryption (128-bit) for web server (OWA)XXExchange System ManagerXXFile Level SecurityXXLogging—Network, OS and ExchangeXXMultiLayered Network & Security DesignXXGeneral Operating System ControlsXXPassword complexityXXPatch ManagementXXPhysical AccessXXUser and Administrator AwarenessXX	Antivirus	Х	Х	$\langle X \rangle$
Change Management Policy and ProceduresXXDisaster Recovery PlanXXEmail Use PolicyXXEncryption (128-bit) for web server (OWA)XXExchange System ManagerXXFile Level SecurityXXLogging—Network, OS and ExchangeXXMonitoring logsXXMultiLayered Network & Security DesignXXGeneral Operating System ControlsXXPatch ManagementXXPhysical AccessXXUser and Administrator AwarenessXX	Backup System, Process, & Tapes	Х	2	20
Disaster Recovery PlanXXEmail Use PolicyXXXEncryption (128-bit) for web server (OWA)XExchange System ManagerXFile Level SecurityXLogging—Network, OS and ExchangeXXMonitoring logsXXMultiLayered Network & Security DesignXGeneral Operating System ControlsXPatch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	Change Management Policy and Procedures	Х		V (
Email Use PolicyXXEncryption (128-bit) for web server (OWA)XExchange System ManagerXFile Level SecurityXLogging—Network, OS and ExchangeXMonitoring logsXMultiLayered Network & Security DesignXGeneral Operating System ControlsXPassword complexityXPatch ManagementXPhysical AccessXUser and Administrator AwarenessX	Disaster Recovery Plan			Х
Encryption (128-bit) for web server (OWA)XExchange System ManagerXFile Level SecurityXLogging—Network, OS and ExchangeXMonitoring logsXMultiLayered Network & Security DesignXGeneral Operating System ControlsXPassword complexityXPatch ManagementXPhysical AccessXCorporate IT PoliciesXValue Administrator AwarenessX	Email Use Policy	Х		Х
Exchange System ManagerXFile Level SecurityXLogging—Network, OS and ExchangeXMonitoring logsXMultiLayered Network & Security DesignXGeneral Operating System ControlsXPassword complexityXPatch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	Encryption (128-bit) for web server (OWA)	X		
File Level SecurityXXLogging—Network, OS and ExchangeXXMonitoring logsXXMultiLayered Network & Security DesignXXGeneral Operating System ControlsXXPassword complexityXXPatch ManagementXXPhysical AccessXXCorporate IT PoliciesXXUser and Administrator AwarenessXX	Exchange System Manager	X		
Logging—Network, OS and ExchangeXXMonitoring logsXXMultiLayered Network & Security DesignXGeneral Operating System ControlsXPassword complexityXPatch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	File Level Security	Х		
Monitoring logsXMultiLayered Network & Security DesignXGeneral Operating System ControlsXPassword complexityXPatch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	Logging—Network, OS and Exchange		Х	Х
MultiLayered Network & Security DesignXGeneral Operating System ControlsXPassword complexityXPatch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	Monitoring logs			Х
General Operating System ControlsXPassword complexityXPatch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	MultiLayered Network & Security Design	Х		
Password complexityXPatch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	General Operating System Controls	Х		
Patch ManagementXPhysical AccessXCorporate IT PoliciesXUser and Administrator AwarenessX	Password complexity	Х		
Physical Access     X       Corporate IT Policies     X       User and Administrator Awareness     X	Patch Management	Х		
Corporate IT PoliciesXUser and Administrator AwarenessX	Physical Access	Х		
User and Administrator Awareness 🔊 X	Corporate IT Policies	Х		
	User and Administrator Awareness	Х		

Figure 1



### Evaluate the risk to the system

There are three foundational risks to a messaging and collaboration system like Exchange. If a vulnerability, threat, and exploit are combined, we could potentially lose one or a combination of the following: Confidentiality, Integrity, and Availability.

A compromise of confidentially on the system is a very high risk to Soft4Genome, its customers, and its partners. The loss of confidentiality could not only sever the relationship with multi million dollar clients, but also make Soft4Genome lose its reputation as a secure provider of data and not be trusted by any Pharmaceutical companies. Their reputation as a trusted source for research operations would diminish to the point of stopping all future sales. Once confidentiality is lost, it wouldn't be too difficult to put together the emails to find out the pathways, proteins, and genes being researched by another company. This exploit could potentially allow a targeted new drug or research area to escape to a competitor and result in a loss in excess of \$1

billion. Ultimately, it could even put Soft4Genomic in the state of bankruptcy or out of business. All of this because the appropriate security steps and due diligence weren't taken to protect the confidentiality of Exchange. The likelihood of confidentiality being lost is high with the default configuration of Exchange and the lack of a strong password policy. A few other specific risks to confidentiality are the misuse of privileges, intercepting the data, social engineering a password, and identity theft.⁴ Taking corrective measures and proactive auditing can greatly reduce the chance of an exploit from happening.

After obtaining a password or some type of access to the Exchange 2000 Server, it is possible to forge an email, modifying an existing email, destroy email, and corrupt the database. Any loss of data integrity is a high risk to the company. However, after taking the necessary countermeasures to these threats, it would be unlikely and challenging for a hacker to do all but forge an email. The consequences of comprised data integrity on Exchange are very similar to those of compromised confidentiality. Soft4Genome could go out of business. Other data integrity risks are viruses that manipulate the data, any malicious code, or a Trojan horse.⁴

A Denial of Service (DOS) attack whether from a virus, being a relay server, spam, or bulk email, is a very likely problem that hasn't been contained as well as it could be. It doesn't take much to send 100 emails from 100 different forged users to a distribution list with all employees (100). That is 1,000,000 messages, which I can guarantee will even bring a 4 CPU, 2GB memory Exchange 2000 Server to its knees (unavailable). If the message had a 1MB attachment, it would be even worse. The alarming speed of viruses and worms being distributed world-wide is also a risk that must be addressed. Finally, Exchange 2000 has a unique vulnerability with the requirement of Internet Information Server (IIS) being installed on the system, leaving it vulnerable to attacks outside of SMTP. Any corruption of the data is also another risk to availability. The consequences are loss of operations, loss of revenue, and finally an embarrassment to Soft4Genome.

The risk of compromised Confidentiality, Integrity, and/or Availability is of the utmost importance with confidentiality being the top risk to the company's reputation and business status.

When evaluating the risk to the system it is important to note that security for the Exchange Server is tightly integrated with the security of the operating system, Windows 2000 Server. User rights, file permissions, services, and registry settings have a direct impact on the security of an Exchange Server. Therefore, it is imperative to follow the Securing Windows 2000 Step By Step⁵ guide and audit the OS before auditing Exchange.

⁴Microsoft, "Exchange 2000 Server Resource Kit, Chapter 30 – Security." URL: <u>http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/reskit/resguide/c30scrty.asp</u> (May 26, 2003).

⁵ SANS Institute, "Securing Windows 2000 Step By Step," The SANS Institute, V 1.5, Jul 1, 2001.

The security control objectives are to minimize risks while allowing proper operations of Exchange. In general, we are ensuring that only authorized users can use the system and with the least privilege necessary, ensuring that the system maintains the highest availability, and ensuring that the proper design is minimizing their risks.

#### What is the current state of practice, if any?

I searched everywhere for an audit checklist for Exchange 2000 Server. I checked with several friends in the IT Auditing Industry. Out of five different Fortune 500 companies with Exchange 2000 implemented, not a single one of them had an audit checklist for Exchange 2000 besides for the operating system, Windows 2000 Server. I was able to locate checklists for Exchange 5.5, but Exchange 2000 is a completely different product. They are so different that Microsoft doesn't recommend administrators to do an in-place upgrade. Although Windows 2000 Server security is extremely important to Exchange just like a foundation is to a home, without implementing security best practices for Exchange is like building a mud house on a foundation of 1000 feet of bedrock. It just doesn't matter how strong the bedrock is, because when it rains the home will be destroyed. Yes, the foundation is very important, but we can't forget the important of the home built on the foundation.

Fortunately, there is a plethora of information on securing email systems in general and Exchange 2000, especially from Microsoft. I believe Microsoft's unpopular notoriety for the lack of security focus in their products is taking a change for the better. Microsoft published numerous helpful "How 2" procedures rather than checklists (<u>http://www.microsoft.com/technet</u>). Additionally, I found an excellent document from the NSA, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (<u>http://nsa2.www.conxion.com/win2k/guides/w2k-21.pdf</u>)⁶. Couple the How 2s and NSA guide with Exchange Administrator experience and best practices; we'll create a solid checklist to audit Exchange 2000 Server.

The research consisted of searching the Internet for Exchange 2000 Server auditing and security material, attending Webcasts, attending Microsoft TechNet presentations, Microsoft's website (<u>http://www.microsoft.com</u>), SANS Reading Room (<u>http://www.sans.org/rr</u>), SecurityFocus articles (<u>http://www.securityfocus.com</u>), reading two excellent books on Exchange 2000 Server and Secure Messaging, GIAC paper on Exchange 5.5 (<u>http://www.giac.org/practical/Filipe_Custodio_GSNA.zip</u>)⁷, and setting up a lab to test different configurations. Please see the List of References for the full set of resources utilized.

Since audit checklist were not found, an audit checklist will be created from personal experience, books, presentations, and articles on Exchange 2000 Server.

⁶ Pitsenbargar, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000," <u>http://nsa2.www.conxion.com/win2k/guides/w2k-21.pdf</u>, National Security Agency (NSA), v1.12, Aug 8, 2002. ⁷ Custodio, Filipe, "Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000)." September 2001. URL: <u>http://www.giac.org/practical/Filipe_Custodio_GSNA.zip</u> (Feb 1, 2003).

### **Create an Audit Checklist**

#### Introduction

Due to the lack of a specific technical policy regarding mail at Soft4Genome, "Best Practices" in the security industry will be utilized.

#### Checklist

Is Security Awareness training specific to email policies and procedures		
conducted at least	once per year?	
Reference	Personal Experience	
Control Objective	Security encompasses everyone and everything from the building to the server to the end user. It is critical to ensure that everyone is trained on what they are supposed to do to prevent an email security incident and how to react if one has already occurred.	
Risk	Without training, end users may not know what to do if someone pretends to be the Help Desk and ask for a password. The end user needs to know what to do with spam and how to deal with attachments. Otherwise, there is a risk that someone could either obtain information through social engineering and possible breach the security of the email system.	
Compliance	<ul> <li>Look for a positive (yes) answer for the following questions:</li> <li>1. Does a formal policy for Security Awareness training exist?</li> <li>2. Are their slides from the presentation available?</li> <li>3. Are there meeting requests or a list of attendees available to prove the training happened?</li> <li>4. Is there an attendee list that the security group maintains?</li> <li>5. Did the attendees sign the list?</li> </ul>	
Testing	<ul> <li>Search for policy on intranet. Seek policy from IT or HR. Ask for slides for last Security Awareness training to see if it covered the following objectives:</li> <li>Never open attachments from unknown source &amp; be skeptical of known sources</li> <li>Never send passwords in an email unless it is encrypted</li> <li>Log off Outlook, OWA, and system when not in use (work, home, or remote location).</li> <li>Don't respond to unsolicited commercial email (spam). It only confirms your address.</li> <li>Don't respond to requests for personal information, including passwords. The Help Desk should never ask for your password.</li> <li>Review of current email policy with end users.</li> </ul>	
Objective/Subjective	Objective-whether it was actually given or not Subjective-Content and effectiveness of the training	

Verify appropriate	Physical Security
Reference	Bois, Justin, "Protect Yourself," SANS Reading Room, Apr 4, 2002. URL: <u>http://www.sans.org/rr/physical/protect.php</u> (Apr 2, 2003). Personal Experience
Control Objective	Prevent unauthorized access to the systems. Verify that sufficient physical and procedural controls are in place to protect the system. Prevent loss of availability.
Risk	With physical access to a system it is nearly impossible to stop a determined intruder. It is as simple as placing a boot disk into the system and rebooting the box. Now, an attacker can completely control the system. There is also the risk of an accidental denial of service if someone unplugs the wrong device.
Compliance	Ensure the following is followed and in place: 1. Server is behind locked door with "least privileged" access. Only personnel that need to be in this room have access. Pay particular attention to contractor badges for cleaning crew and IT contractors. Many times access is not necessary for people to do their jobs. 2. A log is kept for everyone that enters the data center. "No piggy backing" In other words, everyone that goes into the room uses their access card instead of following someone else in the room. 3. There is a process to review the logs on at least a weekly basis. 4. The server is password protected from the console. 5. There is a documented process for gaining and removing access including temporary personnel
Testing	Test the following: 1. Ensure that the server behind a locked door? 2. Check the log to the data center to ensure that the logs are working properly. The facilities manager should be able to allow you to view the log. 3. Additionally, check the group that has access to the Data Center (where the server is located). Ensure that only people that need access to the room are members of the group. This is applicable for keys and security badges (proximity cards, swipe cards, etc). 4. Attempt console access without a password.
Objective/Subjective	<ul> <li>Objective for locked door, log, and password protected. However, there are many other subjective measures for physical security. Here are a few examples:</li> <li>1. Are there security cameras at the entry/exit of the server room?</li> <li>2. Is the Data Center surrounded by firewalls to ensure that the room cannot be accessed through the ceiling?</li> <li>3. Number of personnel with access to the Data Center. This is subjective in nature.</li> <li>4. Are there any windows or direct external access from the building?</li> </ul>

Ensure Outlook client is not installed on Exchange 2000 Server			
Reference	1. "Can I install Outlook on my Exchange server?" Mar 27, 2002. URL:		
	http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=24446		
	(Apr 25, 2003).		
	2000 Server and Outlook 2000 or Later on the Same Computer," Knowledge Base Article-2666418. URL:		
	http://support.microsoft.com/default.aspx?scid=kb;en-us;266418		
	(May 26, 2003).		
	3. McBee, Jim, "Exchange 2000 Security," Microsoft TechNet Webcast, Jan 29, 2003.		
Control Objective	Prevent unauthorized access to the data. Prevent client viruses to		
	run on the Exchange Server.		
Risk	If the system ever is compromised, then you give the attacker full		
	power with Outlook.		
	In a virus situation, you simply don't want the server to have a		
	compromised version of Outlook on the system. If you must have a		
	MAPI client on the Exchange server use this Microsoft Knowledge		
	base Afficie to up so.		
	us:a306962&id=kb:en-us:a306962		
Compliance	The client is either installed or it isn't installed.		
Testing	Look for client icon on the desktop. Attempt to execute.		
5	If not on the desktop, open Add/Remove Programs.		
	If not in Add/Remove Programs, search for outlook.exe under		
	\Program Files\Microsoft Office\Office. It could be in another		
	directory, therefore a search for outlook.exe is necessary. Finally, it		
	could possibly be renamed, This is why the first two steps are		
	taken.		
Objective/Subjective	Objective		

Check for latest Security Updates (Service packs & hotfixes) using Microsoft Baseline Security Analyzer.			
Reference	Microsoft Baseline Security Analyzer (MBSA) v1.1 http://www.microsoft.com/technet/security/tools/tools/mbsahome.asp		
Control Objective	Reports if the system is missing any hotfixes or has an insecure configuration.		

## Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

Risk	Most of the current vulnerabilities are fixed by simply keeping the patches up to date on servers. Without knowing your risks, you can't take any action. It is highly likely that an intruder to your email system will use a known vulnerability that is reported in MBSA. There is a specific security update scan just for Exchange Server to ensure that your application isn't at risk.
Compliance	The scan will give a score of Red, Yellow, or Green. Red is a failure. Yellow needs further investigation, because it might be that a patch or setting is not at the top security level because of the application's needs.
Testing	Install MBSA from http://www.microsoft.com/technet/security/tools/tools/mbsahome.asp Run MBSA locally on the system or remotely if you have administrative rights to the server. Review all results. Red=Failure
Objective/Subjective	Objective

Check for known vulnerabilities by a 3rd party application (Nessus-FREE, ISS			
Reference	Cima, Susan. "Vulnerability Assessment," SANS Institute. 6 July 2001. URL: <u>http://www.sans.org/rr/securitybasics/VA.php</u> (3 Apr 2003). Personal Experience		
Control Objective	Ensuring that the Exchange Server is not susceptible to the enormous amount of known vulnerabilities.		
Risk	"99% of network intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available" Source: CERT, Carnegie Mellon University We need to limit the number of vulnerabilities to a minimum limit while meeting business priorities.		
Compliance	Run Nessus or a 3rd party tool to check for vulnerabilities. 1 or more high level = non-compliant 6 or more medium level = non-compliant 16 or more low level = non-compliant		
Testing	Run a full Nessus or other 3rd party scan on the Exchange Server with all vulnerabilities and exploits available and applicable to a Windows 2000 Server running Exchange 2000 Server. Note: Some exploits may cause a DOS. It is imperative that management approval is received prior to running any scan.		
Objective/Subjective	Objective There is some subjectivity, since not all vulnerability scanners measure vulnerabilities at the same level, nor will they catch the same vulnerabilities.		

Verify that Mailbox	size limits are enforced.
Reference	McBee, Jim. <u>Exchange 2000 Server 24seven</u> . San Francisco: Sybex, 2002. 231-233. Personal Experience
Control Objective	Stopping DOS attack whether accidental or planned (bad).
Risk	DOS. The standard version of Exchange, the most popular version, has a limitation of 16GB database. Unfortunately, Microsoft designed the database to shutdown when it reaches 16GB. This makes it very important to manage the sizes of your mailboxes. Anybody that pulls your SMTP banner and finds out that you have an Exchange server can simply send the server a bunch of large messages to cause a denial of service.
Compliance	If Storage Limits are set in accordance with company policy and deletion settings are set in accordance with company policy.
Testing	From Exchange System Manager, Select the server being audited, Select the appropriate Storage Group, Select Mailbox Store, Select Properties, Select the Limits Tab. 1. "Issue warning at (KB)" is set (90,000 KB in accordance with policy) 2. "Prohibit send at (KB)" is set (100,000 KB in accordance with policy) 3. "Prohibit send and receive at (KB)" is set (150,000 KB in accordance with policy) 4. "Keep deleted items for (days) is set (7 in accordance with policy) 5. "Keep deleted mailboxes for (days) is set (30 in accordance with policy)
Objective/Subjective	ObjectiveEnsuring that storage limits are set SubjectiveThe level of the limits

Verify there is a message size limit for incoming and outgoing messages			
Reference	McBee, Jim. <u>Exchange 2000 Server 24seven</u> . San Francisco: Sybex, 2002. 680-681. Personal Experience		
Control Objective	Ensure that the server cannot send or receive a message that is too large for the server to handle. Protecting the server from DOS by accident or as a part of an attack.		

uditing Micro	soft Exchange 2000 Server	An Administrator's Perspective
Risk	The risk is that someone could send a from the server to the outside, which co service on the Exchange Server and th availability. In a worst situation, someo distributed attack with multiple large file locations. By default, the setting is "no Additionally, you don't want to become inside your organization so it is best to messages too. The same risk associated with mailbox here.	1 GB file to the server or ould cause a denial of ne users would lose one could accomplish a es being sent from various o maximum size." a spam server for someone limit the number of outgoing a size limits is applicable
Compliance	Verify that message limits are set for in messages. Additionally, verify that the limited according to your business need	ncoming and outgoing number of recipients is ds.
Testing	From Exchange System Manager, Sele Message Delivery, Select Properties, S 1. Ensure "Sending message size" and have a maximum set. (10,000 KB or les a. Attempt to send a message of 10,0 b. Attempt to receive a message of 1 2. Ensure "Recipient limits has a maxin or less is recommended)	ect Global Settings, Select Select Defaults. d "Receiving message size" ss is recommended) 000 KB or more 0,000 KB or more mum recipients set. (1000
Objective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/Subjective/S	tiveObjective	

Verify that Top Level Distribution Lists are restricted and limited		
Reference	Personal Experience	
Control Objective	Ensure that the Exchange Server's distribution lists have limited control of causing a DOS by a virus or a simple email flood.	
Risk	DOS. One message marked with a read receipt to the original address (All users) that is spoofed to 100 users would generate 10,101 messages. 1 original +100 users on the DL + 100*100 read receipts = 10,101.	
Compliance	Verify that the top level distribution lists (all employees or groups of 25 or more) have a restricted and limited number of internal users that can send to that address.	
Testing	From the Exchange Server or systems with Exchange System Manager, Open Active Directory Users and Computers, Select the domain, Select User (default) or the Group for your Distribution Lists in Exchange. Select the properties for each Distribution List with 25 or more people, Select the Exchange General tab. 1. Ensure that the Accept message "Only from" is selected. 2. Ensure that the members are limited in accordance with your	

	needs	
	Repeat for each distribution list	
Objective/Subjective	ObjectiveEnsure the restrictions are set.	SubjectiveDifferent
	companies have different requirements.	-

Verify that SMTP relay is off and SMTP traffic is being logged		
Reference	Robichaux, Paul. <u>Securing Messaging with Microsoft Exchange</u> <u>Server 2000</u> . Redmond: Microsoft Press, 2003. 139-160. Personal Experience	
Control Objective	Prevent unauthorized use of the server as an SMTP relay.	
Risk	DOS and loss of the ability to take corrective action if someone is using your server without authorization.	
Compliance	The system has SMTP relay turned off The SMTP traffic is being logged.	
Testing	In Exchange 2000, relay is closed by default unlike Exchange 5.5. However, there are many complexity issues with SMTP Virtual Servers that relay mail back and forth to one another. The important test is to ensure that the external mail server is not a relay agent. We will test this through the command line, since the rule sets can be confusing in Exchange. However, the command line will always give us the true results. Further test can be taken to ensure that relaying on internal mail servers is limited. -Open a Telnet session "telnet mailserver.mydomain.com 25" You should receive a banner response starting with 220 -Type "HELO myPC.mydomain.com" You should receive a banner starting with 250 -Type "MAIL FROM:myemailaddress@mydomain.com" You should receive, "550 5.7.1 Unable to relay for myemailaddress@mydomain.com" If you receive "250 2.1.5 desinationaddress@theirdomain.com" then the Exchange server is a relay agent and is not in compliance. <b>Test Logging</b> Open Exchange System Manager, Select the server being audited, Select Protocols, Select SMTP, Test each SMTP Virtual Server. -Open Properties, Enable Logging should be selected.	
Objective/Subjective	ObjectiveEnsure the restrictions are set. SubjectiveDifferent companies have different requirements.	

Verify encryption is being used for sensitive emails.	
Reference	Personal Experience
Control Objective	Ensure that sensitive data is protected by encryption.
Risk	Loss of confidentiality. Without encryption, a determined attacker can read emails with ease once the system or a backup tape is accessible. With an extra control, encryption, an attacker is going to have a difficult time to decrypt any emails
Compliance	Sensitive emails are being encrypted according to the users.
Testing	Ask 2 of any of the following people to demonstrate the use of using encryption for sensitive emails. CEO, a Vice President, Finance personnel, Human Resources personnel, or any IT member. Verify with any of the 2 members to show you an encrypted email that was sensitive. You should only see the encrypted message.
Objective/Subjective	SubjectiveToo many emails are distributed to actually view every mail to first check if it is sensitive or not and secondly check when it is encrypted or not.

Verify that there is a tested Disaster Recovery Plan		
Reference	Personal Experience	
Control Objective	Ensure that proper procedures are in place and tested to have the	
	ability to restore the application and the data.	
Risk	Email is a critical functionality in the company. Customer Support	
	nearly stops and internal communication reverts to primitive	
	methods. Additionally, a complete loss of the email server	
	database could take years to restore the knowledge and	
	resources.	
Compliance	Review the current Disaster Recovery Plan (DRP). Determine if	
	the DRP is still applicable by basic information about the server	
	and comparing it to the current server.	
Testing	Ask for a current copy of the Disaster Recovery Plan.	
GV.	Interview the administrator(s) and ask when was the last DRP test	
6	completed. This must be within 6 months according to policy.	
	Is there a process for periodic updates to the DRP? Was the last	
	update within 6 months or the last major change?	
Objective/Subjective	SubjectiveThere is no way to verify the last successful restore in	
	a subjective manner.	

Verify logging for	the Exchange Server.
Reference	Microsoft Baseline Security Analyzer (MBSA) v1.1 http://www.microsoft.com/technet/security/tools/tools/mbsahome.as Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000." <u>National Security</u> Agency (NSA) August 2002: 43-45.
Control Objective	Detection and correction
Risk	If an incident goes unnoticed and hacker continues to escalate permissions and possibly corrupt or steal data. No correction actions can happen for incident handling since logs are unavailable Logs are also needed to troubleshoot problems, helping the availability of the server.
	useful analyzing. Plus, you can overwrite important information.
Compliance	Part 1 The system is compliant if the server is collecting the minimum logs recommend by Microsoft Baseline Security Analyzer (MBSA). Part 2 Diagnostic Logging
Testing	For <b>Part 1</b> , verify by running MBSA and opening the Event Viewer on the Exchange Server. Additionally, view the Global Policy settings for Maximum log sizes (all should be at least 25MB). For <b>Part 2</b> , Select the Diagnostics Logging tab from the Exchange Server properties page. Here are the absolute minimum settings: MSExchangeMTA: not applicable if the MTA isn't utilized (service is disabled) Security: set to <b>Maximum</b> MSExchangeIS, Public Folder & Mailbox Logons: set to <b>Maximum</b> Access Control: set to <b>Maximum</b> Send On Behalf Of: set to <b>Maximum</b> Send As: set to <b>Maximum</b>
6	IMAP4Svc & POP3Svc: not applicable if IMAP & POP isnt utilized (service is disabled) Authentication: set to Maximum
Objective/Subjectiv	

Verify that logs ar	e reviewed regularly and archived?	
Reference	Robichaux, Paul. <u>Securing Messaging with Microsoft Exchange</u> <u>Server 2000</u> . Redmond: Microsoft Press, 2003. 139-160. Personal Experience	
Control Objective	Detection and correction. If this system is attacked then, we need to ensure that Exchange Administrators are reviewing the log files on a regular basis to recognize the attack. This information could be utilized to correct the problem and perform incident handling.	
Risk	The administrators and security staff will never know that the system is being attacked. If the Exchange Server is compromised, it would be relatively easy for an experienced hacker to elevate permissions on other servers like the domain controllers and sensitive file servers.	
Compliance	Interview Questions: Are the logs reviewed on a daily basis? YES=compliant NO=non-compliant Are the log files are being archived for at least 6 months. YES=compliant NO=non-compliant This step cannot be verified in an Objective manner.	
Testing	Interview all systems administrators responsible for the Exchange Servers. Verify that an automated process (system) is in place that notifies an administrator(s) of unusual activity.	
Objective/Subjective Subjective		
Audit Stop #14		

Verify that unnecessary services are not running based on the role of the server (i.e. Front-End or Back-End).		
Reference	McBee, Jim. Jim's Exchange 2000 Notes, FAQs, and Useful Information. Honolulu: Jim McBee, 2002. Robichaux, Paul. <u>Securing Messaging with Microsoft Exchange</u> <u>Server 2000</u> . Redmond: Microsoft Press, 2003. 318-321. Personal Experience	
Control Objective	Remove any existing and potential vulnerabilities using a least privilege concept. It is difficult to determine which services are required by the name of the service and the description by Microsoft. So, we will give more details related to each service as applicable to Exchange 2000 Server.	
Risk	The more services that are running on a server, the larger the attack surface is. Decreasing unnecessary services will dramatically decrease vulnerabilities. One example: By default, Exchange has POP and IMAP running, which gives an attacker an extra set of hacker tools available to escalate permissions, modify data integrity, and intrude upon confidentiality.	

<b>Auditing Micros</b>	soft Exchange 2000 Server	An Administrator's Perspective
Auditing Micros	All of the following services should be I Servers unless required by functionality Alerter: only if needed for OS alerts Computer Browser: It is best to remo Neighborhood. May need for AntiVirus this isn't typically needed on an Exchan Distributed File System: Only for DFS domain controllers. File Replication: Only needed for file among other servers. IIS Admin Service: This can be disab needs to be administered, enable serv Indexing Service: Only for full-text ind License Logging Service: only if requ Exchange Event: For Exchange 5.5 co Messenger Microsoft Exchange IMAP4: Do you f Microsoft Exchange Information Store Back-End server. Not needed for From Front-End server is also the SMTP rela messages are required to be sent direct Exchange. Microsoft Exchange MTA Stacks: On communicating with Exchange 5.5 or a Event ID 2000 will be generated as a v cause any problems. Microsoft Exchange Site Replication Exchange 5.5 compatibility. Microsoft Exchange Site Replication Exchange 5.5 compatibility. Microsoft Exchange Site Replication Exchange 5.5 compatibility. Microsoft Exchange Site Replication Exchange 5.5 compatibility. Nicrosoft Exchange Site Replication Exchange Site Replication Exchange Server Removable Storage: Only for tape dr media. Routing and Remote Access: Only for server, which is not recommended for Simple Mail Tran	An Administrator's Perspective
	folder administration and Outlook Web	Access.

## Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

Testing	From the Control Panel, select Administrative Tools, select
-	Services. Verify services are Disabled unless otherwise required.
	Verify Windows Services available from the ports and associated
	service name in the vulnerability assessment scan in Appendix A.
	The services can also be verified by running SuperScan or NMAP.
Objective/Subjective	Objective

Audit Step #15	
Verify that only th Controllers, DNS	e required ports are open between Exchange Servers, Domain servers, End Users, and Administrators
Reference	McBee, Jim. "Exchange 2000 Security," Microsoft TechNet Webcast, Jan 29, 2003. McBee, Jim. <u>Exchange 2000 Server 24seven</u> . San Francisco: Sybex, 2002. 630-635. Personal Experience
Control Objective	Remove any existing and potential vulnerabilities from unused ports being opened.
Risk	The more ports open on a server, the larger the attack surface is. Decreasing unnecessary open ports on the server will dramatically decrease vulnerabilities. Hackers are increasingly running port scans to find which ports are open on a server. Once the ports are found, it is simply a matter of the bad guy figuring out the right tool to exploit the port and escalate permissions on the server.
Compliance	Only the following ports are required to be open for a secure Exchange environment. However, it does depend our your organization's business needs. <i>Assumption: DNS is on the Domain Controller (DC). If not, ensure that TCP 53 and UDP 53 are open.</i>

Auditing Microsoft Exchange 2000 Server An Administrator's Pers	pective
Exchange Front-End to Exchange Back-End Only IPSec, requiring only IP protocol 50 and 51, UDP 500, TCP 88, UDP 88.	
IP protocol 50: Encapsulating Security Payload (ESP) IP protocol 51: Authentication Header (AH)	
ODP 500: Internet Key Exchange (IKE) The exception is if there is a reverse-proxy (i.e. ISA Server) facing the Internet and the Front-End Server is behind an internal firewall. It is still recommended to use IPSec; however, enough controls are in place with the reverse-proxy for the Exchange	
server to be in compliance.	
TCP 25: SMTPonly if FE server is designated to send & receive outside SMTP mail	
TCP 80: HTTPused for HTTP for OWA. SSL is not used here. Microsoft :-(	
TCP 135: RPC endpoint mapper	_
Only IPSec, requiring only IP protocol 50 and 51, UDP 500, TCP 88, UDP 88.	
IP protocol 50: Encapsulating Security Payload (ESP) IP protocol 51: Authentication Header (AH) UDP 500: Internet Key Exchange (IKE)	
The exception is if there is a reverse-proxy (i.e. ISA Server) facing the Internet and the Front-End Server is behind an internal	
controls are in place with the reverse-proxy for the Exchange	
Ports inside IPSec tunnel TCP & UDP 53: DNS	
TCP & UDP 88: Kerberos TCP 135: RPC endpoint mapper	
TCP & UDP 389: LDAP to AD TCP 445: SMB / Netlogon	
TCP 1024+: All ports above 1024!!! Recommend that you statically map the RPC replication ports. See KB 298369 on	
Exchange Back-end to DC	-
TCP & UDP 53: DNS TCP & UDP 389: LDAP to AD	
TCP 3268/3269: LDAP to Global Catalog TCP & UDP 88: Kerberos	

	Clients to Exchange Back-end TCP 135: RPC endpoint mapper TCP 445: Netlogon TCP 1024+: RPC service ports (ensure the right services are being used by these ports)
	Internet to Exchange Front-End TCP 25: SMTP
Testing	Run FPort or NMAP or SuperScan
Objective/Subjective	Objective

_	
Are the file level pe privilege tenet?	ermissions for the Exchange directory secured to the least
Reference	Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000." National Security Agency (NSA) August 2002: 12, 26.
Control Objective	Ensures least privilege access to the Exchange Server. Everyone is Full Control by default.
Risk	There is a risk of someone being able to read messages on the Excharver directory and/or being able to corrupt or delete the Exchange databases. The risk is likely with the default permissions giving "Everyone" Full Control rights. Additionally, IIS runs with Exchange. IIS has numerous vulnerabilities, which could allow an intruder access to the system. Moving the Exchange directory on a physically separated disk helps all but eliminate the risk. It is extremely important that the administrator also takes into account the security of the OS itself
Compliance	Ensure that \Exchsrvr is install on a physically separated disk(s) than the Operating System. Ensure that \Exchsrvr only allows the appropriate rights.
Testing	From Windows Explorer or command line, verify that the \WINNT and \Exchsrvr directories are on different disks. Open Disk Administrator to ensure that logical disks are on separate physical disks too. Check the permissions on the \Exchsrvr directory for the following: -Full Control to Domain Admins, System, Creator Owner, and the Exchange Administrator Group. -The Everyone group does NOT have any permissions. -If this is an Outlook Web Access Server, Authenticated Users will need Read & Execute permissions.
Objective/Subjective	Objective

Verify password co	omplexity with Password Policy
Reference	Soft4Genome Company Password Policy Robichaux, Paul. <u>Securing Messaging with Microsoft Exchange</u> <u>Server 2000</u> . Redmond: Microsoft Press, 2003. 106.
Control Objective	Ensure that passwords meet the complexity requirements of the Company Password Policy. The ultimate object is to protect the data from unauthorized access.
Risk	One of the primary methods of attacking a system is through easily guessed passwords either through intuition or password cracking tools. Not having an account lockout threshold, means that an attacker can attempt to guess the password until infinity, yet there is a statistically finite number when the password will be guessed.
Compliance	Passwords meet the Company Password Policy: -Minimum of 8 characters with at least one character from the following groups: number, uppercase, lowercase, and special character -Must change passwords every 90 days or less -Be significantly different from prior 12 passwords -Not contain your name or username
Testing	From the Group Policy, under Computer Configuration, Security Settings, Account Policies verify the following under Password Policy: -Enforce password history: at least <b>10 passwords remembered</b> -Maximum password age: <b>90 days</b> -Minimum password length: <b>8 characters</b> -Password must meet complexity requirements: <b>Enabled</b> under Account Lockout: -Account lockout duration: <b>0</b> -Account lockout duration: <b>0</b> -Account lockout threshold: <b>5 invalid logon attempts</b> -Reset account lockout counter after: <b>60 minutes</b> The second part of the test is to valid the password complexity, history, length, and lockout by changing a user's passwords without the complexity and length, changing the new password to something similar (history), and verifying that the account is locked
Objective/Subjective	out atter 5 bad attempts.

Verify that the SM	P banner does not display the version of Exchange.
Reference	Mullen, Tim. "Exchange 2000 in the Enterprise: Tip and Tricks Part One" SecurityFocus. Jan 2, 2003. URL:
	http://www.securityfocus.com/infocus/1654 (Mar 21, 2003).
	McBee, Jim. Exchange 2000 Server 24seven. San Francisco:
	Sybex, 2002. 690.
	Microsoft, "TechNet Briefing-Exchange and SQL 2K Security," Mountain View, CA, Microsoft, Jan 29, 2003.
Control Objective	Ensure that the Exchange Server is not allowing too much
	information to the attacker through the banner, which can give
	away vulnerabilities that you don't want advertised.
Risk	There is something to be said about security through obscurity.
	What the attacker doesn't know won't hurt you. If the attacker can
	find out the version of your Exchange Server including the patch
	level, then the attacker can narrow down the exact vulnerabilities
	that are potential exploits.
Compliance	If you can read the version of the Exchange Server via the SMTP
Tartar	
lesting	Open the Command Line by Start, Run, Type cmd, hit enter.
	Open a Teinet session "teinet mailserver.mydomain.com 25"
	The response should be 220 mailserver.mydomain.com
	"something other than the version number" Time of Day. If this
	displays the version number, the system is non-compliant.
Objective/Subjective	Objective

Verify that IIS Lock	down Tool has been implemented.
Reference	Microsoft, "TechNet Briefing-Exchange and SQL 2K Security," Mountain View, CA, Microsoft, Jan 29, 2003. Robichaux, Paul. <u>Securing Messaging with Microsoft Exchange</u> <u>Server 2000</u> . Redmond: Microsoft Press, 2003. 106. 88. Microsoft "Troubleshooting Outlook Web Access in Microsoft Exchange 2000 Server: Q309508," URL: <u>http://www.microsoft.com/technet/prodtechnol/exchange/exchange</u> <u>2000/support/trowae2k.asp</u> (Mar 15, 2003). Microsoft "Securing Exchange 2000 Servers Based on Role: 309677," URL: <u>http://www.microsoft.com/technet/prodtech/mailexch/opsguide/e2k</u> <u>sec03.asp</u> (Mar 15, 2003).
Control Objective	Ensure that access to the system is limited by the vulnerabilities of IIS.

## Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

Risk	The risk is that an attacker can use a plethora of easy to use hacker tools to gain access to an Exchange System even if all the security measures in place, except for locking down IIS. An IIS vulnerabilities by itself and especially combined with other IIS vulnerabilities can give an attacker a road map directly into your system allowing them to escalate permissions to administrator and "own" your system.
Compliance	If IIS Lockdown tool was run with the correct settings, it is in compliance
Testing	Run Microsoft Baseline Security Analyzer (MBSA). Download at: http://download.microsoft.com/download/e/5/7/e57f498f-2468- 4905-aa5f-369252f8b15c/mbsasetup.msi Under Internet Information Services (IIS) Scan Results, ensure that a green checkmark is beside IIS Lockdown Tool.
Objective/Subjective	Objective

Verify that the Exc send as another us	hange Administrator cannot open another user's mailbox or ser.
Reference	McBee, Jim. "Exchange 2000 Security," Microsoft TechNet Webcast, Jan 29, 2003.
Control Objective	Ensure that administrators are not abusing their privileges. Ensure that confidentiality is maintained on the email system.
Risk	There is a risk that the company can be liable for the access that administrators have. Additionally, in court an administrator that has access to a mailbox could be the one that sent the pornographic material under someone else's username instead of the perpetrator. This is just one example. The laws on privacy with company email are not completely clear in every state and nation, and it is definitely better to error on the safe side. If access to another mailbox is need, then wait for written permission by your Human Resources Department.
Compliance	The system is compliant if the systems administrator cannot read another user's email box and cannot send as another user.
Testing	Part 1:Check the Organization Level and the Administrative Group(s)levels in Exchange System Manager to ensure that nobody has"Send As" or "Receive As" permissions.Part 2:Have an administrator attempt to open another user's mailboxusing the administrator's credentials.Have an administrator attempt to send a mail as another userusing the administrator's credentials.If the administrator can do either, then this is non-compliant.

Objective/Subjective Objective

Verify that sufficie Server(s) from viru	nt measures have been taken to protect the Exchange uses.
Reference	Robichaux, Paul. <u>Securing Messaging with Microsoft Exchange</u> <u>Server 2000</u> . Redmond: Microsoft Press, 2003. 180. Custodio, Filipe, "Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000). September 2001. URL: <u>http://www.giac.org/practical/Filipe_Custodio_GSNA.zip</u> (1 February 2003).
Control Objective	The goal is to ensure that the "email infrastructure" is protected from even receiving viruses by taken the proper precautions.
Risk	It is critical to protect the gateway to your network, the Exchange Server(s), and the clients from receiving and/or distributing viruses. If 3 layers are not present, then any of the 3 layers could potentially miss a virus and distribute it. If you only have server side protection, the current 3rd party solutions have been known to miss the virus over the first several minutes, which is too late. If you only have antivirus on the gateway, the virus could be transferred to the server via client POP3 (personal email) and then to Exchange. The true risk is that critical business operations could cease, resulting in a loss of customer service, tarnished reputation, and loss of work.
Compliance	The system must have 3 layers of antivirus protection, including gateway, server, and client. <i>Note: The antivirus application on the server must NOT be file-based virus scanning, rather it needs to be an Exchange based solution (i.e. MAPI, AVAPI).</i> The system must have an automated update technique for all 3 layers. The system must have up-to-date virus definition (signature) files.
Testing	Review the architecture of the email infrastructure. Verify that all 3 layers are present through the diagrams and manually log into each system and verify that the antivirus application is present. Open each antivirus application on all 3 layers and check that each has an automated technique to update the virus definitions (signatures) and engine. Check the latest virus definition files. All 3 layers should be within 7 days. <i>Please refer to the 3rd party antivirus application's manual for</i> <i>exactly how to check for automated updates and the latest virus</i> <i>definition files. This is very straightforward on for all of the major</i> <i>vendors.</i>
Objective/Subjective	eObjective

## **Audit Evidence**

#### Conduct the audit

#### Audit Step #3--FAIL

#### Ensure Outlook client is not installed on Exchange 2000 Server.

On the server verify that all of the following give negative results:

- Locate and execute Outlook icon on the desktop
- Open Add/Remove Programs from the Control Panel. Locate Microsoft Outlook. Locate Microsoft Office and select change to see if Outlook is selected.
- Search for outlook.exe

#### Front-End Server--FAIL

Locate and execute Outlook icon on the desktop--Positive

My Documents Microsoft					
Dasell			R		
My Network Places					
Recycle Bin					
Internet Explorer					
Microsoft Outlook					
🗿 Start 🛛 🕝 🍎 🗳	🕽 📔 🐣 Microsoft Baseline	Securit		🗐 🏠 🏠 11:33	PM
∰start ]] 🗹 🏈 ⊄ Figure 3	🕯 🗍 🔗 Microsoft Baseline	Securit		J 🛱 🏠 🏷 🛛 11:33	PM
<mark>∰start</mark> ] ☑ @ ⊄ Figure 3	Microsoft Baseline	Securit		D 11:33	PM
<mark>∰start</mark> ]] ☑ @ ⊈ Figure 3	Microsoft Baseline	Securit		D 11:33	PM
∰start Figure 3	Microsoft Baseline	Securit		D 11:33	PM
∰start Figure 3	Microsoft Baseline	Securit		D 11:33	PM

Open Add/Remove Programs from the Control Panel. Locate Microsoft Outlook. Locate Microsoft Office and select change to see if Outlook is selected. --Positive

× □ 5
Vord for Windows xcel for Windows owerPoint for Windows Dutlook for Windows p iorters and Exporters tionery k E-mail Folders Jal Basic Scripting Support Jaboration Data Objects tronic Forms Designer Runtime nantec Fax Starter Edition (Internet Mail Only Cor- agrated File Management is toontent and tools.
1280KB Free Disk Space: 3424MB

#### Figure 4

#### Search for outlook.exe--Positive

💐 Search Results				_ 🗆 ×
Eile Edit View Favorites Tools Help				<b>11</b>
📔 🖙 Back 👻 🔿 👻 🔁 🛛 🚳 Search 🖓 Folde	ers 🔇 History   📴 🖗	šX ທ ⊞•		
Address 🔕 Search Results				<b>▼</b> ∂60
Search	Search Resul	Select an item to view its description.		
outlook eve				
Containing text:		In Folder D:\Program Files\Mi	Releva	Size Type 57 KB Applica
Look in:				
Search Now Stop Gearch				
Search for other items:	•			•
1 object(s)				11

#### Figure 5

#### **Back-End Server--PASS**

- Locate and execute Outlook icon on the desktop--Negative
- Open Add/Remove Programs from the Control Panel. Locate Microsoft Outlook. Locate Microsoft Office and select change to see if Outlook is selected--**Negative**

1	Currently installed programs:	Sort by: Name	-
		520	1100000
lange or lemove	💕 MetaEdit 2.0 (x86)	Size	434KB
ograms	🜔 Microsoft Exchange 2000	Size	8.73MB
	🙆 Microsoft Update Q319743 for Exchange Server 2000	Size	52.2MB
<u>-</u>	👩 Microsoft Update Q320436 for Exchange Server 2000	Size	41.9MB
id New ograms	😂 Norton AntiVirus for Microsoft Exchange		
-	🔄, NtdsAtrb	Size	1.17MB
	PowerChute network shutdown v2.0.1	Size	3.85MB
Remove	Terminal Services Client	Size	1.26MB
indows popepts	🛃 Windows 2000 Application Compatibility Update		
poriories	Windows 2000 Hotfix (Pre-SP4) [See Q320206 for more		
	Windows 2000 Hotfix (Pre-SP4) [See Q322842 for more		
	Windows 2000 Hotfix (Pre-SP4) [See Q322913 for more		
	Windows 2000 Hotfix (Pre-SP4) [See q323172 for more		
	III information] Windows 2000 Hotfix (Pre-SP4) [See O324096 for more		<b>_</b>

#### Figure 6

#### Search for outlook.exe--Negative

💐 Search Results		l ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	
📙 🖙 Back 👻 🚽 👻 🔁 🛛 🔕 Search 🖓	Brolders 🔇 History 🖹 🕆 🖈 🗠 🏢 -	
Address 🔕 Search Results	▼ ∂	'Go
Search	×	
🤻 <u>N</u> ew 🥔		
Search for Files and Folders	Search Results	
Search for files or folders named:		
loutlook.exe		
Containing text:	Name In Folder R	eleva.
	Search is complete. There are no results to display.	
Look in:		
🖃 Local Harddrives (C:;E:;M:)		
Stop Search		
Search Options >>		
Course for other items:	-	
Files or Folders		
Computers		
Printers	<b>-</b>	Þ
0 file(s) found		
Figure 7		

There were positive results of the Outlook client being installed on the Front-End Server.

#### Audit Step #4--FAIL

Check for service packs, hotfixes, and recommendations from Microsoft Baseline Security Analyzer.

#### Front-End Server—FAIL

Three "critical" Windows security updates are not installed on the server. MBSA reports 9 security updates are missing, but 6 of them are already installed. This is definitely something to consider when using MBSA as an audit tool. Fortunately, all IIS and Exchange Server updates have been applied. The **red X** under the score column determined a failure.



Figure 8

Figure 9 displays the details of the missing Windows Security Updates. Note the flaw in Microsoft Virtual Machine that could allow a system compromise.⁸

⁸ Microsoft," Flaw in Microsoft VM ould Enable System Compromise (816093)," Apr 14, 2003. URL: <u>http://www.microsoft.com/technet/security/bulletin/MS03-011.asp</u> (Jun 7, 2003).

## Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

_	indows Security Updates					
secur Scor	e Security Updates cor	ate Description R	narked with a red X eason			
×	<u>MSU2-063</u>	Unchecked Fi Buffer in PPTP Implementation \d Could Enable th Denial of Service Attacks	ie rivers\raspptp.sys has a at is less than what is e	system32 file version [5.0.2195.4080] xpected [5.0.2195.6076].		
×	<u>MS03-011</u>	(Q329834) Flaw in Microsoft Fi VM Could Enable System \n Compromise th (816093)	le nsjava.dll has a file vers an what is expected [5.0	system32 ion [5.0.3805.0] that is less 0.3810.0].		
osoft B	aseline Security Analy:	zer - Microsoft Internet Explorer			_	
×	<u>MS03-015</u>	System \n Compromise th (816093) Cumulative Patch Th for Internet Explorer A8 (813489) It	nsjava.dll has a file versi an what is expected [5.0 plorer\ActiveX Compatib 0D-00C04FD74AD8}** s has a value of 32.	on [5.0.3805.0] that is less 0.3810.0]. ARE\Microsoft\Internet ility\{06DD38D3-D187-11CF- hould have a value of 1024.		
Secur	ity updates tha	t the tool cannot confirr	n as installed on the sca	nned computer are marked		
with a Score	a blue asterisk e Security Upd	ate Description		Reason		
₩ ₩	<u>MS01-022</u> <u>MS02-008</u>	WebDAV Service Pro to Levy Requests as XMLHTTP Control Ca	vider Can Allow Scripts User In Allow Access to Local	Please refer to Q306460 for a detailed explanation. Please refer to Q306460 for a datailed explanation		
*	<u>MS02-053</u>	Buffer Overrun in Sn Could Allow Code Ex	nartHTML Interpreter (0324096)	Please refer to Q306460 for a detailed explanation.		
*	<u>MS02-064</u>	Windows 2000 Defa Allow Trojan Horse (	ult Permissions Could Program (Q327522)	Please refer to Q306460 for a detailed explanation.	R	
*	<u>MS02-065</u>	Buffer Overrun in Mi Components Could L	crosoft Data Access Lead to Code Execution	Please refer to Q306460 for a detailed explanation.		
*	<u>MS03-008</u>	Flaw in Windows Sci code execution (814	ript Engine could allow 078)	Please refer to Q306460 for a detailed explanation.		
					'	



 Score
 Drive Letter
 File System

 X
 C:
 FAT

 V
 D:
 NTFS

#### Figure 11

The FAT file system on the C: Drive was also confirmed by verifying the properties of the local drive.

#### Back-End Server--FAIL

Two Windows security updates are not installed on the server. One is considered critical. Although MBSA shows 8 security updates are missing, 6 of the updates cannot be confirmed by MBSA, but they were installed. Please see Security Update MS02-055 in figure13. Fortunately, all IIS and Exchange Server updates have been applied. The **red X** under the score column determined a failure.

Baseline Securi	ty Analyzer	Microsoft
Microsoft Baseline Security Analyzer         Welcome         Pick a computer to scan         Pick multiple computers to scan         Pick a security report to view         View a security report         See Also         Microsoft Baseline Security Analyzer Hein	View security re Sort Order: Score (worst Computer name: IP address: Security report name: Scan date: Scanned with MBSA we Security update databa Security update databa Security update databa	first)  Fision: 1.1 Severe Risk (One or more critical checks failed.)
About Microsoft Baseline Security	Security Update Scan i	Resurts
Analyzer Microsoft Security Web site	Score         Issue           X         Windows           Security         Updates	Result 8 security updates are missing, are out of date, or could not be confirmed. What was scanned Result details How to correct this
Actions	<ul> <li>IIS Security Updates</li> </ul>	No critical security updates are missing. What was scanned
을 Print 말 Copy	Windows Media Player Security Updates	No critical security updates are missing. What was scanned
	Exchange Server Security Updates	No critical security updates are missing. What was scanned
	SQL Server Security Updates	SQL Server is not installed on this computer.
		Previous security report Next security report

Figure 12

8 sec confi	urity updates rmed.	are missing, are out of date, or could not be	
Result	t Details	dates	
Secu	rity updates con	nfirmed as missing are marked with a red X	
Scor X	e Security Upd. MS03-011	ate DescriptionReasonFlaw in MicrosoftFile C:\WINNT\system32VM Could Enable\msjava.dll has a file versionSystem[5.0.3809.0] that is less thanCompromisewhat is expected(816093)[5.0.3810.0].	
Secu	rity updates tha	at are out of date are marked with a yellow X	
×	MS02-055	are DescriptionReasonUnchecked BufferFile C:\WINNT\system32in Windows Help\hhctrl.ocx has a file versionFacility Could[5.2.3718.0] that is greaterEnable Codethan what is expectedExecution[5.2.3669.0].(Q323255)(Q323255)	
Secu scan	rity updates tha ned computer ar	at the tool cannot confirm as installed on the re marked with a blue asterisk	
*	MS01-022	WebDAV Service Provider Please refer to Can Allow Scripts to Levy Q306460 for a Requests as User detailed	
*	<u>MS02-008</u>	XMLHTTP Control Can Allow Please refer to Access to Local Files Q306460 for a detailed	
<u>.</u>	M902-053	explanation.	
gure 13	0		
osoft B	aseline Security Analy	zer - Microsoft Internet Explorer	
-------------------------	--------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------
Score	2 Security Upd MS02-055	ate Description Reason Unchecked Buffer File C:\ in Windows Help \hhctrl. Facility Could [5.2.37: Enable Code than wh Execution [5.2.366 (Q323255)	WININT\system32 ocx has a file version 18.0] that is greater nat is expected 59.0].
Secur scanr Score	ity updates tha ied computer ar e <mark>Security Upd</mark> <u>MS01-022</u>	It the tool cannot confirm as in re marked with a blue asterisk ate Description WebDAV Service Provider Can Allow Scripts to Levy	stalled on the Reason Please refer to Q306460 for a
**	<u>MS02-008</u>	Requests as User XMLHTTP Control Can Allow Access to Local Files	explanation. w Please refer to Q306460 for a detailed
*	<u>MS02-053</u>	Buffer Overrun in SmartHTML Interpreter Could Allow Code Executio (0324096)	explanation. Please refer to Q306460 for a n detailed explanation.
*	<u>MS02-064</u>	Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)	Please refer to Q306460 for a detailed explanation.
*	<u>MS02-065</u>	Buffer Ovérrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)	: Please refer to Q306460 for a detailed explanation.
*	<u>MS03-008</u>	Flaw in Windows Script Engine could allow code execution (814078)	Please refer to Q306460 for a detailed explanation.

#### Figure 14

#### Audit Step #5—PASS

ISS Internet Scanner was used to check the vulnerabilities of both Front-End and Back-End Exchange Servers. The full reports are included in Appendix A.

#### Front-End Server--PASS

Although critical risks were found from running MBSA, not a single vulnerability was found by ISS Internet Scanner or Nessus. This was tested from the external network and internal network. Vulnerabilities may be found if the scanner was plugged directly into the same switch, and the switch opened traffic from another port. Due to company security policies, this was not allowed. The scan only gave one result; the fact that https is running. See results below. The fact that the server couldn't be fully scanned even in stealth mode, gives the server a PASS. An intruder would need to break physical security, and at that point he might as well take the server instead of information gathering via a vulnerability scanner.

	ty Severity: H	High	м		$\Lambda_{-}$	Low			
Session Info	<u>rmation</u>								
Session Name:	WebMailEXT[2]			File Name:					
Policy:	W2K Scan custom			Key:					
Hosts Scanned:				Hosts Active :					
Scan Start:	5/26/2003_11:14:13AM			Scan End:					
Comment:	Web mail from external								
IP Address (DNS Name)				Operating System			] [	Status	
1.1.1.1 {(Unresolved Name)}				(Unreachable Host)				Not	reachable
1.1.1.1 {(Unre									
1.1.1.1 {(Unre Service De	tails:								
1.1.1.1 {(Unre <u>Service De</u> Service M	<u>tails:</u> me	Short	Descrip	tion			Por	t#	Type

#### Figure 15

#### **Back-End Server--PASS**

The Back-End Server had "No" high risk level vulnerabilities were found. Five medium risk level vulnerabilities were found, and 10 low risk level vulnerabilities were discovered.

#### Medium Risk Vulnerabilities Summary:

- HttpTraceEnabled: HTTP TRACE is enabled
- IisFrontpageInfo: IIS with FrontPage information gathering (CAN-2000-0114)
- IisWebdavRunning: Microsoft IIS WebDAV service is running on the system
- MsLocatorRunning: Microsoft Locator service is running on the system
- Registry null session: Registry opened through a null session

Of the 5 medium risk vulnerabilities, two are expected and even required. Outlook Web Access on Exchange 2000 Server replaces the WebDAV with its own version, which is not vulnerable to the WebDAV exploit according to Microsoft and SANS.¹⁰ Additionally, the registry setting for RestrictAnonymous can only be set to 0 or 1 for proper Exchange functionality.¹¹ RestrictAnonymous is set to 1 to not allow enumeration of SAM accounts and names.¹² The other 3 vulnerabilities can be easily fixed by running IIS lockdown tool, uninstall FrontPage support, and disabling the RPC Locator service.

#### Low Risk Vulnerabilities Summary:

- EhloCheck: SMTP daemon supports EHLO (CAN-1999-0531)
- Guest Exists: Guest account name exists
- IcmpTstamp: ICMP timestamp requests (CAN-1999-0524)

¹⁰ Fossen, Jason, Weber, Chris, Ingevaldson, Dan, Johansson, Jesper, "WebDav Buffer Overflow Exploit Against IIS 5.0," SANS Institute, Mar 18, 2003. URL: <u>http://www.sans.org/webcasts/031803.php</u>.

¹¹ Microsoft "How to Use the RestrictAnonymous Registry Value in Windows 2000: KB 246261." URL: <u>http://support.microsoft.com/default.aspx?scid=kb;EN-US;246261</u> (May 26, 2003).

¹² Microsoft "XADM: Clients Cannot Browse the Global Address List After You Apply the Q299687 Windows 2000 Security Hotfix: KB 309622." URL: <u>http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309622</u> (May 26, 2003).

- IisRunning: Microsoft IIS is running on the system (CAN-1999-0633)
- 5x Local User: Windows local user on workstation Vuln count = 5
- MtaDiscovery: Message Transfer Agent service is running

Exchange 2000 servers require EHLO for ESMTP verbs that are needed for communication between Exchange 2000 Servers. The Guest account can be renamed; however, an attacker can still easily guess it. ICMP timestamps are not applicable, since they are blocked at the firewall. IIS is required by Exchange 2000 Server. The five local users are required on this server. The Microsoft Exchange MTA service can be disabled without disruption since it is only required with other Exchange 5.5 or X.400 systems.

### Audit Step #7--PASS

Verify there is a message size limit for incoming and outgoing messages. The first figure is a screen shot of the "Global Settings" on the Exchange Server.

essage Delive	y Properti	es	? ×
General Defau	lts Filtering	Details Security	k,
Select the defa organization.	ult delivery r	estrictions and options for reci	ipients in this
┌─ Sending mes	sage size —		
C <u>N</u> o limit		Maximum (KB):	10000
-Receiving me	essage size-		
C No limit		Maximum (KB):	10000
Recipient limi	ts		
O No li <u>m</u> it		Maximum (recipients):	1000
	UK		Help

#### Figure 16

Verifying the settings isn't always good enough for an audit. To test the true results from the server a test message was sent to an external address and from an external address to the internal Exchange server. The file sizes were over 10,000 KB. As you can see from two figures below, both of the tests (sending and receiving messages > 10,000 KB) produced negative results, which passes this audit checklist item. The figures look very similar, but they are from different servers. Note: This test should be performed during non-business hours for the sake of bandwidth utilization.

An Administrator's Perspective

😻 Undeliverable: test file - Report		
Eile Edit View Insert Tools Actions Help		
🔄 Send Again 😡 🎒 🎦 🗙 🔺 - 🕈 - 😰 🗸		
From: System Administrator	Sent: Mon 5/26/2003 1:41 AM	
To: Subject: Undeliverable: test file		
Your message did not reach some or all of the intended recipients.		<u> </u>
Subject: test file Sent: 5/26/2003 1:41 AM		
The following recipient(s) could not be reached:		
on 5/26/2003 1:41 AM This message is larger than the current system limit or the recipient's mailbox is full. remove attachments and try sending it again. #5.2.3>	Create a shorter message body o	r
		~
Figure 17		
🥙 Undeliverable: test - Report		

<u>File Edit View Insert Tools Actions H</u> elp	
🖃 Send Again 😡 🎒 🎦 🗙 🔺 🔹 🔹 😰 🗸	
om: System Administrator	Sent: Mon 5/26/2003 1:44 AM
): Jbject: Undeliverable: test	
our message did not reach some or all of the intended recipients.	
Subject: test Sent: 5/26/2003 1:43 AM	
he following recipient(s) could not be reached:	
This message is larger than the current system limit or the re emove attachments and try sending it again. <	copient s mailbox is ruli. Create a shorter message body or

Figure 18

### Audit Step #8--PASS

Verify that Top Level Distribution Lists are restricted and limited.

Collected a list of 6 distribution lists with 25 or more personnel. All lists were tested by verifying in the settings in Active Directory Users and Computers that the distribution lists were limited to the designated personnel. In this case, only the CEO, VPs, HR, and the Help Desk only had permission to send to the distribution lists in accordance with IT and HR policies.

Active Directory Users and Computers. Same properties for all 6 distribution lists.



Figure 19

#### Message failed to send for all 6 distribution lists.



Figure 20

### Audit Step #9--PASS

Verify SMTP relay is off and SMTP traffic is being logged.

#### SMTP Relay

Running the following commands gave us the resulting output for an SMTP relay test.

- Open a Telnet session "telnet mailserver.mydomain.com 25"
  - You should receive a banner response starting with 220
- Type "HELO myPC.mydomain.com"

- You should receive a banner starting with 250
- Type "MAIL FROM:myemailaddress@mydomain.com"
- **Type** "RCPT TO:destinationaddress@theirdomain.com"
  - You should receive, "550 5.7.1 Unable to relay for myemailaddress@mydomain.com"
  - If you receive "250 2.1.5 desinationaddress@theirdomain.com" then the Exchange server is a relay agent and is not in compliance.

C:\WINNT\System32\cmd.exe	- telnet			<u> </u>
220 9 ready at Mon, 26 May 250 250 2.1.0 joe@test.com	.com Microsoft 1 2003 16:58:46 -( .com Hello [10.3 Sender 0A	ESMTP MAIL Service, 0700 32.16.25]	Version: 5.0	.2195.532
550 5.7.1 Unable to rela	ly for	Uyahoo.com		

Figure 21

#### **SMTP** Logging

There were a total of 3 SMTP Virtual Servers between the Front-End and Back-End servers. The virtual servers are used for the Event Sink script that produces the warning message for all outgoing mail. All three have logging enabled as verified through Exchange System Manager and the actual log file.

efault SMTP Virtual Server Properties	?
General Access Messages Delivery	
Default SMTP Virtual Server	
I <u>P</u> address:	
(All Unassigned)	Ad <u>v</u> anced
Limit number of connections to:	
Connection time- <u>o</u> ut (minutes):	10
Enable logging	
Enable logging	
✓ Enable logging Active log format: W3C Extended Log File Format	Properties

Figure 22	
Note that SMTP is always in GMT.	
🗾 extend1.log - Notepad	- 🗆 ×
Eile Edit Format Help	
#Software: Microsoft Internet Information Services 5.0	<b>_</b>
#Date: 2003-05-27 00:10:38	
#Fields: date time c <u>-in cs-username s-sitename s-compute</u> rname s-ip	s-p
2003-05-27 00:10:38	VC1
2003-05-27 00:10:38	vc1
2003-05-27 00:10:38 .com SMTPS	VC1
2003-05-27 00:10:38	VC1
2003-05-27 00:10:38 - OutboundConnectionResponse SMIPSVCI	mand
2003-05-27 00:10:38 .com OutboundConnectionRes	pons
2003-05-27 00:10:38	nand
2003-05-27 00:10:38	mand
2003-05-27 00:10:38 .com OutboundConnectionRes	pons
2003-05-27 00:10:38 .com OutboundConnectionCom	nand
2003-05-27 00:10:38	pons
2003-05-27 00:10:38 .com OutboundConnectionCom	mand
2003-05-27 00:10:38 .com OutboundConnectionRes	pons
2003-05-27 00:10:38	
Figure 23	

### Audit Step #14--FAIL

Verify that unnecessary services are Disabled and Stopped based on the role of the server (i.e. Front-End or Back-End).

### Front-End--FAIL

All exceptions are highlighted. If the service status is Stopped with the Startup Type still set to Manual and it is highlighted, then the service needs to be set to Disabled for compliance. None of the out of compliance services are necessary according to policies or functionality. From the non-compliant services, there was a double check with SuperScan and NMAP to ensure nothing was missed.

An Administrator's Perspective

Name 🛆	Description	Status	Startun Tvr
Renter Alerter	Notifies sel.		Manual
Application Management	Provides s		Manual
Se Automatic Undates	Fnables th	Started	Automatic
Reckaround Intelligent Transfer Service	Trapefore f	Started	Macunado
Backup Evec Remote Agent for Windo	Indianaicia		Manual
ClipRook	Supports C		Manual
	Brouidos a	Started	Manual
COM+ Event System	Provides a	Starteu	Manual
Computer Browser	Maintains a	Chaubad	Manual
No Der Watch	Managara	Started	Disabled
September Client	Manages h	Charlend	Disabled
Souther the System Client	Foods polif	Starteu	Macual
Distributed Link Tracking Clienc	Steres info		Manual
Barrishikukad Turanashing Canudiashan	Stores Info		Manual
Republic Clark	Coordinate	Charles	Manual
No Client	Resolves a	Started	Automatic
ange Event Log ∰a	Logs event	Started	Automatic
Max Service	Helps you		Manual
No. File Replication	Maintains fi		Manual
No. 115 Admin Service	Allows adm	Started	Automatic
New Address of Service	Indexes co	Started	Automatic
nternet Connection Sharing	Provides n		Manual
ntersite Messaging	Allows sen	<i></i>	Disabled
* IPSEC Policy Agent	Manages I	Started	Automatic
Serberos Key Distribution Center	Generates		Disabled
Service Logging Service			Disabled
Section 2015 Manager	Logical Disk	Started	Automatic
Logical Disk Manager Administrative S	Administrat		Manual
Messenger	Sends and		Manual
Microsoft Exchange Event	Monitors fo		Disabled
Microsoft Exchange IMAP4	Provides Mi		Disabled
Microsoft Exchange Information Store	Manages M	Started	Automatic
🎇 Microsoft Exchange Management	Provides Mi	Started	Automatic
🎇 Microsoft Exchange MTA Stacks	Provides Mi		Disabled
Microsoft Exchange POP3	Provides Mi		Disabled
Microsoft Exchange Routing Engine	Processes		Disabled
Microsoft Exchange Site Replication S			Disabled
Microsoft Exchange System Attendant	Provides s	Started	Automatic
Microsoft Search	Creates ful	Started	Automatic
	Supports p	Started	Automatic
Ret Logon	Allows out	Dianica	Macunatic
Renote Desktop Sharing	Allows auc	Charles	Manuar
Network Connections	Manages o	Started	Automatic
Network DDE	Provides n		Manual
Network DDE DSDM	Manages s		Manual
Network News Transport Protocol (NN	Transports		Disabled
🖓 Norton AntiVirus Client			Disabled
🎇 NT LM Security Support Provider	Provides s	Started	Manual
Rerformance Logs and Alerts	Configures		Manual
Plug and Play	Manages d	Started	Automatic
PowerChute network shutdown	-	Started	Automatic
Print Spooler	Loads files	Started	Automatic
Protected Storage	Provides pr	Started	Automatic
	Provides p		Manual
Bernote Access Auto Connection Man	Creates a		Manual
Remote Access Addo Connection Man	Creates a		Manual
Remote Access Connection Manager	Creates a	character of	Manual
Remote Procedure Call (RPC)	Provides th	Started	Automatic
*@Remote Procedure Call (RPC) Locator			
State	Manages t	Started	Automatic
Remote Registry Service	Manages t Allows rem	Started Started	Automatic Automatic

An Administrator's Perspective

Routing and Remote Access	Offers rout		Disabled
RunAs Service	Enables st		Manual
🙀 Security Accounts Manager	Stores sec	Started	Automatic
Server 👘	Provides R	Started	Automatic
Simple Mail Transport Protocol (SMTP)	Transports	Started	Automatic
🆓 Smart Card	Manages a		Manual
🆏 Smart Card Helper	Provides s		Manual
🎭 SNMP Service	Includes a		Manual
🆏 SNMP Trap Service	Receives tr		Disabled
🏶 System Event Notification	Tracks syst	Started	Automatic
🆏 Task Scheduler	Enables a		Manual
🏶 TCP/IP NetBIOS Helper Service	Enables su	Started	Automatic
🆏 Telephony	Provides T	Started	Manual
🍓 Telnet	Allows a re		Disabled
🆏 Terminal Services	Provides a	Started	Manual
🏶 UPS - APC PowerChute plus	Manages a		Manual
🆏 Utility Manager	Starts and		Manual
🏶 Windows Installer	Installs, re		Manual
🏶 Windows Management Instrumentation	Provides s	Started	Automatic
🏶 Windows Management Instrumentatio	Provides s	Started	Manual
🏶 Windows Time	Sets the co	Started	Automatic
🏶 Workstation	Provides n	Started	Automatic
🏶 World Wide Web Publishing Service	Provides W	Started	Automatic
4			

Figure 24

#### Back-End--FAIL

All exceptions are highlighted. None of the out of compliance are necessary according to policies or functionality. From the non-compliant services, there was a double check with SuperScan and NMAP to ensure nothing was missed. The "dellw3c" service is also in question. A question has been sent to Dell to verify the necessity of the driver, but no response has been received. Later, we discovered that Microsoft Exchange POP3 service is required for business needs.

An Administrator's Perspective

Name 🛆	Description	Status	Startup Type
🎭 Alerter	Notifies sel	Started	Automatic
🏶 Application Management	Provides s		Manual
🏶 Automatic Updates	Enables th	Started	Automatic
Background Intelligent Transfer Service	Transfers f		Manual
Backup Exec Remote Agent for Windo		Started	Automatic
🖏 ClipBook	Supports C		Manual
🖏 COM+ Event System	Provides a	Started	Manual
Somputer Browser	Maintains a	Started	Automatic
🍓 dellw3c		Started	Automatic
DHCP Client	Manages n	Started	Automatic
Distributed File System	Manages lo	Started	Automatic
🖏 Distributed Link Tracking Client	Sends notif	Started	Automatic
🖏 Distributed Link Tracking Server	Stores info		Manual
Sistributed Transaction Coordinator	Coordinate	Started	Automatic
DNS Client	Resolves a	Started	Automatic
Event Log	Logs event	Started	Automatic
Fax Service	Helps you		Manual
File Replication	Maintains fi		Manual
IIS Admin Service	Allows adm	Started	Automatic
🖓 Indexing Service	Indexes co		Manual
🖏 Internet Connection Sharing	Provides n		Manual
🏶 Intersite Messaging	Allows sen		Disabled
Sec Policy Agent	Manages I	Started	Automatic
Kerberos Key Distribution Center	Generates		Disabled
License Logging Service	Tracks Clie		Manual
Second Contract Contr	Logical Disk	Started	Automatic
Logical Disk Manager Administrative S	Administrat		Manual
Messenger .	Sends and	Started	Automatic
🏶 Microsoft Exchange Event	Monitors fo		Manual
Microsoft Exchange IMAP4	Provides Mi	Started	Automatic
🏶 Microsoft Exchange Information Store	Manages M	Started	Automatic
🏶 Microsoft Exchange Management	Provides Mi	Started	Automatic
Microsoft Exchange MTA Stacks	Provides Mi	Started	Automatic
Microsoft Exchange POP3	Provides Mi	Started	Automatic
Microsoft Exchange Routing Engine	Processes	Started	Automatic
Microsoft Exchange Site Replication S			Disabled
🏶 Microsoft Exchange System Attendant	Provides s	Started	Automatic
🖓 Microsoft Search	Creates ful	Started	Automatic
NAV for Microsoft Exchange		Started	Automatic

An Administrator's Perspective

🏶 Net Logon	Supports p	Started	Automatic
🏶 NetMeeting Remote Desktop Sharing	Allows aut		Manual
Setwork Connections	Manages o	Started	Manual
🏶 Network DDE	Provides n		Manual
🏶 Network DDE DSDM	Manages s		Manual
Network News Transport Protocol (NN	Transports		Manual .
NT LM Security Support Provider	Provides s	Started	Manual
Performance Logs and Alerts	Configures		Manual
🖏 Plug and Play	Manages d	Started	Automatic
SoverChute network shutdown		Started	Automatic
အိမ္မွာPrint Spooler	Loads files	Started	Automatic
Reprotected Storage	Provides pr	Started	Automatic
QoS RSVP	Provides n		Manual
Remote Access Auto Connection Man	Creates a		Manual
Remote Access Connection Manager	Creates a	Started	Manual
Remote Procedure Call (RPC)	Provides th	Started	Automatic
Remote Procedure Call (RPC) Locator	Manages t	Started	Manual
Remote Registry Service	Allows rem	Started	Automatic 🗦
Removable Storage	Manages r	Started	Automatic
Routing and Remote Access	Offers rout		Disabled
RunAs Service	Enables st	Started	Automatic
Security Accounts Manager	Stores sec	Started	Automatic
Server	Provides R	Started	Automatic
Simple Mail Transport Protocol (SMTP)	Transports	Started	Automatic
Smart Card	Manages a		Manual
Smart Card Herber	Provides s		Manual
SMS Client Service		Started	Automatic
SMS Hardware Inventory Agent Service			Manual
SMS Remote Control Agent		Started	Automatic
SNMP Service	Includes a		Manual
SNMP Trap Service	Receives tr		Manual
System Event Notification	Tracks syst	Started	Automatic
Task Scheduler	Enables a	Started	Automatic
TCP/IP NetBIOS Helper Service	Enables su	Started	Automatic
Telephony	Provides T	Started	Manual
Telnet	Allows a re		Manual
Terminal Services	Provides a	Started	Automatic
Uninterruptible Power Supply	Manages a		Manual
Utility Manager	Starts and		Manual
Windows Installer	Installs, re		Manual
Windows Management Instrumentation	Provides s	Started	Manual
🏶 Windows Management Instrumentatio	Provides s	Started	Manual
🖏 Windows Time	Sets the co	Started	Automatic
🆓 Workstation	Provides n	Started	Automatic
🏶 World Wide Web Publishing Service	Provides W	Started	Automatic
•			► F

Figure 25

#### Audit Step #16--FAIL

Are the file level permissions for the Exchange directory secured to the least privilege tenet?

#### Front-End—FAIL

Both the OS and Exchange Server are installed on the same logical and physical drive. FAIL

See Ex	kchsrvr
--------	---------

	-		
D:\Program Volume in Volume Ser	Files>dir drive D h ial Numbe	as no label. r is F457-9D56	
Directory	of D:\Pro	gram Files	
04/04/2003 04/04/2003 08/31/2000 05/17/2001 08/31/2000 05/17/2003	01:53p 01:53p 10:52a 04:57p 03:49p 08:14p	<dir> <dir> <dir> <dir> <dir> <dir> <dir></dir></dir></dir></dir></dir></dir></dir>	Accessories Common Files ComPlus Applications Exchsrvr

Figure 26

Note that WIN2K is the directory for the OS instead of WINNT.

D:\>dir			
Volume in	drive D h	as no label.	
Volume Sei	ial Numbe	r is F457-9D56	
Directory	of D:\		
04 /04 /2002	02 • 1 0 ₂₂		040E02 Patabaa
04/04/2003	0Z-T0h		ort nos net l
05/17/2003	07:58p		051703_Patches
03/14/2002	10:50a	<dir></dir>	Documents and Sett
05/17/2003	08:20p	5,406,288	Exchange Server Se
05/21/2001	11:18a	1,932,412	Exchange Server Se
09/14/2001	01:28p	<dir></dir>	Inetpub
03/02/2001	Ø6:23p	<dir></dir>	intranet_log
09/14/2001	07:00p	2,346	mpextranet.cer
04/04/2003	01:53p	<dir></dir>	Program Files
07/20/2002	08:09p	1,812	Q319743.MIF
04/05/2003	08:41p	1,824	Q320436.MIF
11/08/2001	03:38p	<dir></dir>	TEMP
05/24/2003	10:14p	<dir></dir>	WIN2K

Figure 27

## Auditing Microsoft Exchange 2000 Server An Administ

The directory permissions for \exchsrvr are correct. Full Control is limited to Domain Admins, System, Creator Owner, and the Exchange Administrator Group. The Everyone Group does NOT have any permissions. PASS

xchsrvr Properties	? ×
General   Web Sharing   Sharing   Se	ecurity
Name Administrators CREATOR OWNER Power Users SYSTEM TERMINAL SERVER LISER	Add
Permissions:	Allow Deny
Full Control Modify Read & Execute List Folder Contents Read Write	
Advanced	parent to propagate to this
ОК	Cancel Apply

Figure 28

#### Back-End--FAIL

The Exchange Server and the OS were installed on separate physical drives. **PASS** 

E:\Program Volume in Volume Ser	Files≻dir drive E is Ne ∙ial Number is	w Volume 1CØF-335	3	
Directory	of E:\Program	Files		
08/04/2001 08/04/2001 05/17/2003	12:35a 12:35a 08:20p 0 File(s) 3 Dir(s)	<dir> <dir> <dir> <dir> 79,793,6</dir></dir></dir></dir>	Exchsr Ø bytes Ø6,656 bytes	free
Figure 29				
05 <b>/17/2</b> 003	08:28p 5 File(s) 19 Dir(s)	<dir> 6,2 1,848,8</dir>	WINNT 65,840 bytes 49,920 bytes	free
C:∖≻cd winn	t			
C:\WINNT>_				
Figure 30				

An Administrator's Perspective

Only the Everyone Group has permissions. The Everyone Group is the one group that specifically should not have any permissions. Figure 31 below shows the actual and the default setting. FAIL

Name Reveryone			A	<u>d</u> d
	Q		<u><u> </u></u>	move
ermissions:		All	ow I	Deny
Full Control		Ŷ	e	
Modify Bead & Execute		2	e e	님
List Folder Contents		~	¢	ŏ
Read		>	e.	
Write		~	f	
Advanced				
<u> </u>				

Figure 31

### Audit Step #18--FAIL

Verify that the SMTP banner does not display the version of Exchange.

From an external test, both servers fail to give any information. The results were only accessible from the internal network. However, the checklist item is to see if the SMTP banner doesn't display information gathering type data. Both of the servers failed the test. Note the version numbers given from the SMTP banner.

Front-End

🚾 C:\WINNT\System32\cmd.exe - t	elnet 25		
220 .5329 ready at Mon, 26 Ma -	.com Microsoft ESM ay 2003 19:31:10 -070	TP MAIL Service, Vers Ø	sion: 5.0.2195
Figure 32			
Back-End		Second granulation - Management	
C:\WINNT\System32\cmd.exe - t	elnet 25		
220	com Microsoft ESMTP M 003 19:33:21 -0700	AIL Service, Version:	5.0.2195.532
Figure 33			

### Audit Step #20--FAIL

Verify that the Exchange Administrator(s) cannot open another user's mailbox or send as that user. Security Properties from the Organization Level and the Administrative Group Levels in Exchange System Manager need to be checked to verify the appropriate permissions are set.

Receive As and Send As give the user permissions to open another user's mailbox and send email as that user.

Name		<b>_</b>	Add
Domain Admins     Domain Admins     Enterprise Admins     Everyone     Constant Density Constant	Domain Admins Enterprise Ad	) 1	Пенноче
Permissions:		Allo	w Deny
Remove PF from admin group Administer information store Create named properties in the ir View information store status Receive As Send As	nformation store	N N N N N N N N N N N N N N N N N N N	
Advanced	m parent to pro	pagate ti	o this

#### Figure 34

The permissions for the Organization and the Administrative Group levels are the same. Figure 34 represents both, but is the Administrative Group permissions as you can see the inheritable permissions in gray. Note that inheritable permissions were given to the Domain Administrators to Receive As and Send As another user. Explicit Deny permissions should be selected here.

### Measure Residual Risk

Simply applying the resources available to ensure that vulnerabilities are patched will decrease many of the threats. The cost vs. benefit analysis determines that the extra couple of hours per month from the Exchange Administrator are well worth the potential loss of availability, confidentiality, and integrity of the system. Some minor policy changes with strict enforcement will mitigate risks.

OWA still has a risk through port 443. OWA is a server that is part of the same domain as the Back-End server and is on the Internet. With the Front-End server being on the same domain as the Back-End server, there is a risk that cached credentials on the Front-End server could allow an attacker to parse the registry and get a domain administrator's password. Plus, all ports are open on the VPN tunnel between the Front-End and Back-End servers.

Recommendation: Improved Design of Outlook Web Access. (see Figure 35)¹³¹⁴

- Implement ISA Server in the DMZ. This server will not be part of the domain. ISA server acts as an additional application firewall and a reverse proxy for publishing web content over SSL. No content is on the server.
- Have a second DMZ with OWA with no access from the Internet. The OWA (Front-End) server will be on a separate domain from the Back-End Server. The OWA server will have an IPSec tunnel to its Domain Controller, ISA server, and the Back-End Server.¹⁵
- The DMZ Domain Controller will be a part of the same forest with limited permissions.¹⁵
- Costs associated with this mitigation are ISA Server 2000 at ~\$1400, (2) Windows 2000 Server at ~\$700 each, hardware at ~\$2000 (consider using existing hardware), and the administration costs associated with personnel. See diagram below.

¹³Weber, Chris, "Securing Exchange 2000," SecurityFocus, Part One, Apr 23, 2002. URL: http://www.securityfocus.com/infocus/1572 (Mar 26, 2003).

¹⁴ Weber, Chris, "Securing Exchange 2000," SecurityFocus, Part Two, May 8, 2002. URL: <u>http://www.securityfocus.com/infocus/1578</u> (Mar 26, 2003).

¹⁵ SANS Institute, Track 5 – Securing Windows, The SANS Institute, 2003.





#### Figure 35

Additionally, POP3 is a residual risk on the internal server that cannot be eliminated. Users need the ability to access their email on a PDA device. The solution uses the VPN and accessing the Back-End Exchange Server. This is an acceptable procedure by management. However, a policy needs to be written supporting this residual risk.

With 8 of the 21 audit checklist steps failing, the control objections were not met from an overall audit. The great news is that almost every single checklist item that didn't PASS the audit can be implemented during the next maintenance window with minimal impact to business operations and cost.

### Is the system auditable?

The Front-End and Back-End Exchange 2000 Servers are auditable using the control objectives and checklist items. Most are considered to be stimulus and response checklist items that are truly objective. However, it is debatable whether the "Subjective" checklist items are auditable. Particularly, the security awareness training and verifying that encryption is being used for sensitive emails. Only questions with subjective answers can give you the answer. On the other hand, both security awareness and encryption are critical to the security of Exchange 2000 Servers.

In order to audit an Exchange 2000 Server environment in a quality manner, it is critical that all related systems are involved in the audit. Including both the Front-End and Back-End servers and having limited network access, made the audit very time consuming. I would recommend that there is a completely separate and specific audit related to virus protection. Virus protection now includes desktops (clients), servers, gateway servers, hardware devices, and even 3rd party managed services. A solid Anti-Virus solution is extremely important in today's ever increasing world of malicious viruses.

Overall, the system is auditable with a consolidation of best practices into 21 welldefined steps.

# **Risk Assessment – For Administrators**

### Summary

The audit found interesting results concerning multiple layered security. Although the network was extremely secure about keep ports and services closed, there were numerous unnecessary services running on the servers. Just because someone lives in a gated community with security guards doesn't mean that they shouldn't take the next layer of security by locking their front door. This was seen here by not implementing least privilege concepts to file permissions, applications, services, and giving out information (banner). Additionally, many of the "High" risk patches (service packs and/or HotFixes) were applied, but some of the medium to low risk items were ignored. The non-compliant audit steps need to be addressed and fixed.

## Background / Risk

- #3 Outlook client installed on Front-End server
  - Outlook on an Exchange Server could give an attacker full power of manipulating the system. Once the attacker accessed the system through Outlook, the controls to stop DOS through millions of emails or to eliminate viruses would be significantly deterred.
- #4 HotFixes were not updated. Found that FE server has FAT partition on C:
  - There were several HotFixes missing; however, one potential exploit stood out. Microsoft says it best "could allow an attacker to run code of his or

her choice."¹⁶ After getting Netcat on the box, I would choose Back Orifice or VNC, giving one complete control of a system. Confidentiality goes out the window at this point.

- C: drive could be directly accessed. A FAT partition offers no access controls. Once an attacker has access to the system, she could install agents to monitor the system remotely or even go to the point of shutting down the system.
- #14 Unnecessary services
  - We simply don't know what vulnerabilities and exploits lie ahead. There is no reason to increase your attack zone by allowing additional services running on a critical system. The risk is that a new exploit that you didn't think could harm your system (i.e. having the Distributed File System service started) could be the next widespread exploit. The result could be a DOS attack or even loss of confidentiality or data integrity.
- #16 File Level permission to Exchange directory
  - Once an attacker gains access to a system, the attacker will likely attempt to escalate permissions. With the file level permissions giving access to the "Everyone" group, the intruder can read and write to any file. The risk is a loss of all three security tenets, and the disruption could mean loss of revenue for the company.
- #18 SMTP banner
  - Before attempting to hack into a system, an attacker will gather information about system. Giving information about the Exchange version through the SMTP banner allows the attacker to focus on the known exploits to this version.
- #20 Exchange Administrator access
  - There is a two-fold risk with liability and confidentiality. Under current privacy laws, a company could be held liable for the access that the administrator has. If you were trying to prosecute someone for illegal actions using the company resources, the defense could come back with, "but, this could have been the administrator, right?" Confidentiality is also important for business development and sales. Without it, a loss of revenue could happen.

¹⁶ Microsoft," Flaw in Microsoft VM ould Enable System Compromise (816093)," Apr 14, 2003. URL: <u>http://www.microsoft.com/technet/security/bulletin/MS03-011.asp</u> (Jun 7, 2003).



### System changes and further testing

Outlook was removed from the Front-End Server without causing any disruptions. Retesting the system gave us PASS results.

Locate	and	execu	te O	utlook	icon	on the	e desk	topN	legat	ive	
My Documents	Microsoft Baseli										
My Computer											
My Network Places											
Recycle Bin											
(C) Internet				R							
Explorer											

Open Add/Remove Programs from the Control Panel. Locate Microsoft Outlook and/or Microsoft Office--**Negative** 

🗐 🏠 12:33 PM

Services

🏽 🚮 🔁

Figure 36

🖬 Add/Remov	e Programs		_ 🗆 ×
	Currently installed programs:	Sort by: Name	•
Change or Remove	** more information j		<b>_</b>
Programs	To change this program or remove it from your computer, click Change/Remove.	<u>C</u> hange/Re	move
<u></u>	Java 2 Runtime Environment Standard Edition v1.2.2	Size	15.2MB
Add New	🛗 LiveUpdate	Size	1.43MB
Programs	💕 MetaEdit 2.1 (x86)	Size	448KB
92 <b>4</b>	₿⁄ Microsoft Baseline Security Analyzer	Size	4.01MB
Sand Con	🛃 Microsoft Exchange 2000	Size	8.84MB
Add/Remove Windows	🞇 Microsoft Update Q299535 for Exchange Server 2000	Size	15.4MB
Components	📷 Microsoft Update Q319743 for Exchange Server 2000	Size	58.8MB
	🞇 Microsoft Update Q320436 for Exchange Server 2000	Size	43.5MB
	In Norton AntiVirus Corporate Edition	Size	58.4MB
	PowerChute network shutdown v2.0.1	Size	3.97MB
	🛐 PowerChute plus 5.2	Size	7.44MB
	Terminal Services Client	Size	1.28MB 👻
			Cl <u>o</u> se

Figure 37

#### Search for outlook.exe on all drives--Negative

💐 Search Results		_ 🗆 ×
<u> </u>	Help	-
← Back → → → 🔁 🛛 🔇 Search 🖓	Folders 🞯 History 🛛 🕆 🌾 🗙 🖄 🗐 🎫	
Address 🔊 Search Results		<b>-</b> ∂⊙
Search	*	
Search for Files and Folders	Search Results	
Search for files or folders na <u>m</u> ed: outlook.exe		
Containing text:	Name In Folder Releva	Size Type
	Bearch is complete. There are no results to display.	
Look in: Local Harddrives (C:;D:;M:)		
Stop Search		
Search Options >>		
Search for other items:		•
0 object(s)		
Figure 38		

• #4 HotFixes were not updated. Found that FE server has FAT partition on C:

#### Front-End Server



#### Figure 39

Note: All of the 7 security updates have been installed; however, MBSA is reporting them as a version "greater than what is expected" or "cannot confirm" if the update was installed. All security updates were installed.

© SANS Institute 2003,

t I	Details			
οw	is Security Upo	lates		
irii	ty updates tha	it are out of date are marked	with a yellow X	
re	MS02-055	Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255)	File a file version [5.2.3735.1] expected [5.2.3669.0].	system32\hhctrl.ocx has that is <mark>greater than</mark> what is
irii ris	ty updates tha sk	t the tool <mark>cannot confirm</mark> as	installed on the scanned com	nputer are marked with a blue
e	MS01-022	WebDAV Service Provide	r Can Allow Scripts to Levv	Please refer to 0306460 for a
	<u>MS02-008</u>	Requests as User XMLHTTP Control Can All	ow Access to Local Files	detailed explanation. Please refer to Q306460 for a detailed explanation
	<u>MS02-053</u>	Buffer Overrun in Smart⊢ Code Execution (Q32409	ITML Interpreter Could Allow 6)	Please refer to Q306460 for a detailed explanation.
	<u>MS02-064</u>	Windows 2000 Default P Trojan Horse Program (Q	ermissions Could Allow 327522)	Please refer to Q306460 for a detailed explanation.
	MS02-065	Could Lead to Code Exec	oft Data Access Components ution (Q329414) ingine could allow code	Please refer to Q306460 for a detailed explanation.
	<u>M303-006</u>	execution (814078)	ingine could allow code	detailed explanation.
		k		
1	40		Y Y	

Score	e Issue	Result			
×	Restrict Anonymous	Computer is running with RestrictAnonymous = 1. This I prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymou to ensure maximum security.			
		What was scanned		How to correct this	
X	Administrator	s More than 2 Administ	rators were fo	und on this computer.	
U V		What was scanned	Result details	How to correct this	



An Administrator's Perspective

🖵 Computer Management 📃 🗆 🗙							
$]$ Action View $]$ $\Leftrightarrow$ $\Rightarrow$ $]$ $\textcircled{E}$	3 🛛 🕼 😼						
Tree	Volume	Layout	Туре	File System			
Computer Management (Local) System Tools Computer Viewer Computer Viewer System Information Computer Viewer Computer Viewer Shared Folders Computer Viewer Computer Vie	(C:)	Partition Partition	Basic Basic	NTFS NTFS			
Disk Management Disk Defragmenter Disk Defragmenter Disk Defragmenter Disk Defragmenter Disk Defragmenter Disk Management Disk Management Disk Management Disk Defragmenter Disk Defragmenter Di	Disk 0 Basic 9.53 GB Online CDRom 0 CDRom (E:) No Media	(C:) 2.00 GB NTF5 Healthy (System)	(D:) 7.53 GB NTI Healthy (Bo	FS ot)			
	Primary Partition						



#### **Back-End Server**

The Back-End Server previously failed because it was missing a security update to fix a flaw in Microsoft Virtual Machine.



Just like the Front-End Server, of the 7 security updates reported as missing, all have been installed as seen in the figure 44.

icrosoft Baseline Security Anal	yzer - Microsoft Internet Explorer		- 15			
Baseline	Security Analyzer					
7 security updates	are out of date or could not	be confirmed.				
Result Details						
Windows Security Up	dates					
Security updates th	at are out of date are marked wit	h a yellow X				
Score Security Upo X MS02-055 ↓	Jate DescriptionReasonUnchecked BufferFile C:\Vin Windows Help\hhctrl.oFacility Could[5.2.373Enable Codethan whoExecution[5.2.366(Q323255)[5.2.366]	VINNT\system32 cx has a file version 5.1] that is <mark>greater</mark> at is expected 9.0].	_			
Security updates that the tool <mark>cannot confirm</mark> as installed on the scanned computer are marked with a blue asterisk						
Score Security Upo	late Description WebDAV Service Provider Can Allow Scripts to Levy Requests as User	Reason Please refer to Q306460 for a detailed explanation				
<b>₩</b> <u>MS02-008</u>	XMLHTTP Control Can Allow Access to Local Files	Please refer to Q306460 for a				

Figure 44

• #14 Unnecessary services

Unnecessary services were stopped and disabled with no disruption of availability. Thoroughly test the disabling of services on a lab environment before implementing on a production system. Please note that the IIS Admin Service needs to be Disabled and Paused. If the service is stopped then, World Wide Web Publishing Service stops and Outlook Web Access becomes unusable.

# **Front-End**

Starts on the next page

An Administrator's Perspective

_

Name 🛆	Description	Status	Startup Ty	
Alerter .	Notifies sel		Disabled	
Application Management	Provides s		Manual	
Automatic Updates	Enables th	Started	Automatic	
Background Intelligent Transfer Service	Transfers f		Manual	
Backup Exec Remote Agent for Windo	Increases		Manual	
Sector Se	Supports C		Manual	
COM+ Event System	Provides a	Started	Manual	
Computer Browser	Maintains a		Disabled	
Sefwatch		Started	Automatic	
	Manages n		Disabled	
Sa Distributed File System	Manages Io		Disabled J	
Sistributed Link Tracking Client	Sends notif		Manual	
Server	Stores info		Manual	
Source and the second s	Coordinate		Manual	
South and the second se	Resolves a	Started	Automatic	
Serventing	Logs event	Started	Automatic	
Service	Helps you		Manual	
	Maintains fi	1	Disabled	
Sente Replication	Allows adm	Paused		
Sandexing Service	Indexes co	1 dasca		
Sendering Service	Provides p		Manual	
	Allows sep		Disabled	
Se IDSEC Policy Agent	Milowys Schul	Started		
Kerberos Key Distribution Center	Generates	Juliu		
	denerates		Disabled	
Service	Logical Dick	Started		
Set Logical Disk Manager	Administrat	Starteu	Manual	
Mossepaer	Aunimistrat			
We Missenger	Senas ana		Disabled	
Microsoft Exchange Event	Monitors ro		Disabled	
Microsoft Exchange IMAP4	Provides Mi			
Microsoft Exchange Management	Drouidos Mi	Started	Automatic	
Microsoft Exchange MTA Stacks	Provides Mi	Starteu	Disabled	
Microsoft Exchange POP3	Provides Mi		Disabled	
	Processes		Disabled	
Microsoft Exchange Site Penlication S	FI0C63363		Disabled	
Microsoft Exchange System Attendant	Provides s	Started	Automatic	
Microsoft Search	Creates ful	Starteu	Disabled	
Sent Logon	Supports p	Started	Automatic	
Service Logish	Allows aut	Juliu	Manual	
Service Connections	Manages o	Started	Automatic	
	Provides n	Started	Manual	
	Manages s		Manual	
Network News Trapsport Protocol (NN	Transports		Disabled	
WasNorton AntiVirus Client	mansportsm		Disabled	
WANT I M Security Support Provider	Provides s	Started	Manual	
Reperformance Logs and Alerts	Configures	Startoa	Manual	
	Manages d	Started	Automatic	
PowerChute network shutdown		Started	Automatic	
Ript Spooler	Loads files		Disabled	
Protected Storage	Provides pr	Started	Automatic	
Cos RSVP	Provides p	2-2-00	Manual	
Remote Access Auto Connection Man	Creates a		Manual	
Remote Access Connection Manager	Creates a		Manual	
Remote Procedure Call (RPC)	Provides th	Started	Automatic	
Remote Procedure Call (RPC) Locator	Manages t	Started	Automatic	
Remote Registry Service	Allows rem	Started	Automatic	
Removable Storage	Manages r		Disabled	

An Administrator's Perspective

🏶 Routing and Remote Access	Offers rout		Disabled
🆓 RunAs Service	Enables st		Manual
🆓 Security Accounts Manager	Stores sec	Started	Automatic
Server 🗧	Provides R	Started	Automatic
🆓 Simple Mail Transport Protocol (SMTP)	Transports		Disabled
🏶 Smart Card	Manages a		Manual
🏶 Smart Card Helper	Provides s		Manual
SNMP Service	Includes agents	s that monito	the activity
SNMP Trap Service	Receives tr		Disabled
🏶 System Event Notification	Tracks syst	Started	Automatic
🍓 Task Scheduler	Enables a		Manual
🍓 TCP/IP NetBIOS Helper Service	Enables su	Started	Automatic
🎇 Telephony	Provides T	Started	Manual
🍓 Telnet	Allows a re		Disabled
🏶 Terminal Services	Provides a	Started	Automatic
🏶 UPS - APC PowerChute plus	Manages a		Manual
🍓 Utility Manager	Starts and		Manual
🏶 Windows Installer	Installs, re		Disabled
🏶 Windows Management Instrumentation	Provides s	Started	Automatic
🏶 Windows Management Instrumentatio	Provides s	Started	Manual
🏶 Windows Time	Sets the co	Started	Automatic (
🍓 Workstation	Provides n	Started	Automatic
🎇 World Wide Web Publishing Service	Provides W	Started	Automatic
Figure 45			

#### **Back-End**

Alerter Alerter	Notifies sel		Disabled
🆏 Application Management	Provides s		Manual
🏶 Automatic Updates	Enables th	Started	Automatic
🎇 Background Intelligent Transfer Service 🛛	Transfers f		Manual
Backup Exec Remote Agent for Windo			Automatic
🏶 ClipBook	Supports C		Manual
🏶 COM+ Event System	Provides a	Started	Manual
Computer Browser	Maintains a		Disabled
🤹 φχμω3c		Started	Automatic
DHCP Client	Manages n	Started	Automatic
System	Manages lo		Disabled
🖏 Distributed Link Tracking Client	Sends notif	Started	Automatic
🏶 Distributed Link Tracking Server	Stores info		Manual
🖏 Distributed Transaction Coordinator	Coordinate	Started	Automatic
💑 DNS Client	Resolves a	Started	Automatic
🖏 Event Log	Logs event	Started	Automatic
💑 Fax Service	Helps you	1	Manual
🙀 File Replication	Maintains fi	1	Disabled
🖗 IIS Admin Service	Allows adm	Paused	Disabled
🖏 Indexing Service	Indexes co		<b>Disabled</b>
🙀 Internet Connection Sharing	Provides n		Manual
🖏 Intersite Messaging	Allows sen		Disabled
🏶 IPSEC Policy Agent	Manages I	Started	Automatic
🏶 Kerberos Key Distribution Center	Generates		Disabled
🖏 License Logging Service	Tracks Clie		<b>Disabled</b>
🍓 Logical Disk Manager	Logical Disk	Started	Automatic
💑 Logical Disk Manager Administrative S	Administrat		Manual
Messenger	Sends and		Disabled
🆓 Microsoft Exchange Event	Monitors fo		Disabled
Microsoft Exchange IMAP4	Provides Mi		Disabled
Microsoft Exchange Information Store	Manages M	Started	Automatic
Microsoft Exchange Management	Provides Mi	Started	Automatic
Microsoft Exchange MTA Stacks	Provides Mi		Disabled
Microsoft Exchange POP3	Provides Mi	Started	Automatic
Microsoft Exchange Routing Engine	Processes	Started	Automatic
Microsoft Exchange Site Replication S			Disabled
Microsoft Exchange System Attendant	Provides s	Started	Automatic
Microsoft Search	Creates ful		Disabled
NAV for Microsoft Exchange		Started	Automatic

🍓 Net Logon Supports p... Started Automatic NetMeeting Remote Desktop Sharing Allows aut... Manual Wetwork Connections Manages o... Started Manual 🍓 Network DDE Provides n... Manual 🍓 Network DDE DSDM Manages s... Manual Network News Transport Protocol (NN... Transports... Disabled 
 WIT LM Security Support Provider
 Provides s...
 Started
 Manual

 Performance Logs and Alerts
 Configures...
 Manual

 Plug and Play
 Manages d...
 Started
 Automatic

 PowerChute network shutdown
 Started
 Automatic
 Loads files ... Rint Spooler Disabled Protected Storage Provides pr... Started Automatic 🏶 QoS RSVP Provides n... Manual 🍓 Remote Access Auto Connection Man... Creates a ... Manual Remote Access Connection Manager Creates a ... Started Remote Procedure Call (RPC) Provides th... Started Remote Procedure Call (RPC) Locator Manages t... Started Manual Automatic Manual Remote Registry Service Allows rem... Started Automatic Removable Storage Manages r... Disabled Routing and Remote Access Offers rout... Disabled RunAs Service Enables st... Started Automatic Security Accounts Manager Stores sec... Started Automatic Server Provides R... Started Automatic 🍓 Server Provides R... Started Automatic 🎇 Simple Mail Transport Protocol (SMTP) Transports... Started Automatic Smart Card Manages a... Manual 🍓 Smart Card Helper Provides s... Manual Started Automatic 🍓 SMS Client Service 🍓 SMS Hardware Inventory Agent Service 🚽 Manual 🆓 SMS Remote Control Agent Started Automatic SNMP Service Includes a... Manual SMP Service Includes a... Manual SMP Trap Service Receives tr... Manual System Event Notification Tracks syst... Started Automatic Task Scheduler Enables a ... Started Automatic TCP/IP NetBIOS Helper Service Enables a ... Started TCP/IP NetBIOS Helper Service Enables su... Started Telephony Provides T Children Telephony Automatic Manual Allows a re... 🍓 Telnet Disabled 
 Terminal Services
 Provides a ... Started
 Automatic

 Uninterruptible Power Supply
 Manages a...
 Manual

 Utility Manager
 Starts and ...
 Manual
 🍓 Windows Installer Installs, re... Disabled. 🐝 Windows Management Instrumentation 🛛 Provides s... Started 👘 Manual 🦓 Windows Management Instrumentatio... Provides s... Started 🚽 Manual Sets the co... Started 🍓 Windows Time Automatic 🍓 Workstation Provides n... Started Automatic 🏶 World Wide Web Publishing Service 👘 Provides W... Started Automatic Figure 46

• #16 File Level permission to Exchange directory

On the Front-End Server, both the OS and the Exchange Server application were installed on the same logical and physical hard drive. The system could not be fixed during the audit phase. The system will be upgraded with the new infrastructure using Microsoft ISA Server in 3 months.

The Back-End Server had the "Everyone" Group with full rights to the /exchsrvr directory. This has been corrected.

An Administrator's Perspective

chsrvr Properties		?
General   Web Sharing   Sharing   Security		
Name		A <u>d</u> d
CREATOR OWNER	.d	<u>R</u> emove
🚮 Exchange Domain Servers	h	
SYSTEM		
<u> </u>		
Permissions:	Allov	v Deny
Full Control	V	
Modify Board & Evenue		
List Folder Contents		H
Read		ä
Write	$\checkmark$	
Advanced		
All and independent and a second strain of the second state to the second state of the	o propa	agate to this
Allow ingentable permissions from parent t object		

Figure 47

• #18 SMTP banner

Since the SMTP service was disabled and stopped on the Front-End Server, no information is given through the SMTP banner. Telnet will only attempt to connect on port 25 and fail.

Select C:\WINNT\S	ystem32\telnet.exe	
Connecting To		▲ · · · · · · · · · · · · · · · · · · ·

Figure 48

On the Back-End Server, the SMTP banner was modified using the MetaEdit 2.2 from http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B232068#3.17 From MetaEdit open the LM/smtpsvc/1 directory. "1" is the number of the virtual server. You may need to repeat for multiple virtual servers. "String 36907" was added with anything you would like in the data field. The SMTP Service needs to be restarted before the change takes effect.

C:\WINNT\System32	telnet.exe							
220 0700	.com	Authorized	Users	Only!!!	Sat,	7 Jun	2003	17:12
Figure 49								

¹⁷ Microsoft," HOW TO: Download, Install, and Remove the IIS MetaEdit 2.2 Utility," May 20, 2003, URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B232068#3 (Jun 7, 2003).

• #20 Exchange Administrator access

Access to mailboxes was restricted to only the individual owner of his or her mailbox. The only exceptions were for executive assistants that were given specific rights by the mailbox owner. Receive As and Send As permissions were removed as seen below. Plus, access to any mailbox by an administrator fails on each attempt.

	Proper	ties				? ×
eneral   Detai	Is Security	1				
Name				•	A <u>d</u> d	
🥵 Authentic	ated Users:			7-		
				-	<u>H</u> emov	e
		<b>N</b>				
Domain A	idmins a Admins	Domain A	imins) se Ad			
		Lincipi	se Ad	-		
ermissions:				Allow	Deny	,
Read metal	oase propertie	es				
Administer i	nformation sto	ore		$\checkmark$		
Create nam	ed properties	in the information	store	$\checkmark$		
View inform	ation store sta	atus				
Receive As				Ц.		
SendAs				ш		<b>-</b>
Advanced.	.					
- Allow inho	 ritable permis:	sions from parent t		to to H	nia	
object	itable permist	sions nom parent t	o propaga		110	
	OK	Cancel	App	ly I	Н	elp
E 30						

Microsoft Outlook File Edit View Favorites Tools Help	_ <b>_</b> X
Unable to display the folder	Unable to display the folder.
Figure 51	

### System justification

Fortunately, only two of the Audit Steps that failed could not be corrected at this time. In audit Step #14--Unnecessary Services, it is recommended to Disable and Stop the Microsoft Exchange POP3 service as another Technical Control. However, in today's world of mobile wireless devices, we need to meet the needs of the business and communication by making a POP3 exception for the wireless devices. Several compensating controls were implemented to decrease risk.

- POP3 (port 110) is blocked from the firewall.
- All POP3 activity is logged.
- POP3 can only be accessed after 2-factor authentication through the VPN.

The file permissions on the Front-End Server could not be corrected at this time. The failure in Audit Step #16 was due to the Exchange application and the OS being on the same physical and logical drive. The current plan at Soft4Genome is to improve the security of the Outlook Web Access Solution and the Exchange infrastructure by implementing Microsoft ISA Server. The upgrade is scheduled in the next 3 months, and the budget has been approved to purchase the appropriated hardware and software as discussed earlier. The current compensating controls are:

• Only SSL (port 443) is allowed from the Internet. The firewall blocks all other ports to the Front-End Server from the outside.

• All communication between the Front-End Server and the Back-End Server and two Domain Controllers is forced through IPSEC.

# References

- Bayne, James, "An Overview of Threat and Risk Assessment," SANS Info Sec Reading Room, Jan 22, 2002. URL: <u>http://www.sans.org/rr/audit/overview.php</u> (Feb 26, 2003).
- Bois, Justin, "Protect Yourself," SANS Reading Room, Apr 4, 2002. URL: <u>http://www.sans.org/rr/physical/protect.php</u> (Apr 2, 2003).
- "Can I install Outlook on my Exchange server?," Mar 27, 2002. URL: <u>http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=24446</u> (Apr 25, 2003).
- Cima, Susan. "Vulnerability Assessment," SANS Institute. Jul 6, 2001. URL: <u>http://www.sans.org/rr/securitybasics/VA.php</u> (Apr 3,2003).
- Custodio, Filipe, "Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000)." September 2001. URL: http://www.giac.org/practical/Filipe_Custodio_GSNA.zip (Feb 1, 2003).
- English, Bill, "Securing Exchange 2000 Server E-mail," Mar 14, 2002. URL: <u>http://www.sans.org/rr/email/sec_exchange.php</u> (Feb 26, 2003).
- Ferris, David & Sampson, Michael, "The Corporate Email Market, 2001-2005," Ferris Research, March 2001.
- Fossen, Jason, Weber, Chris, Ingevaldson, Dan, Johansson, Jesper, "WebDav Buffer Overflow Exploit Against IIS 5.0," SANS Institute, Mar 18, 2003. URL: <u>http://www.sans.org/webcasts/031803.php</u>.
- GFI, "Protecting your network against email threats: How to block email attacks & viruses," <u>http://www.gfi.com/mailsecurity/wpemailprotection.htm</u> (Feb 26, 2003).
- Gurowicz, Marian B., "Secure eMail: Determining an Enterprise Strategy and Direction," Sep 16, 2002, URL: <u>http://www.sans.org/rr/email/direction.php</u>, (Feb 26, 2003).
- Hudgins-Bonafield, Christy, "Messaging Migration: It Pays To Do You Homework," Network Computing, Jun 15, 1998. URL: <u>http://www.networkcomputing.com/911/911f1.html</u> (Apr 21, 2003).
- McBee, Jim, "Exchange 2000 Security," Microsoft TechNet Webcast, Jan 29, 2003.
- McBee, Jim. Exchange 2000 Server 24seven. San Francisco: Sybex, 2002.
- McBee, Jim. <u>Jim's Exchange 2000 Notes, FAQs, and Useful Information</u>. Honolulu: Jim McBee, 2002.
- Microsoft, "Exchange 2000 Server Operations Guide," Microsoft Press, 2002. URL: <u>http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/maintain</u> /operate/opsguide/default.asp (May 26, 2003).
- Microsoft, "Exchange 2000 Server Planning and Installation, Chapter 13 System Security." URL: <u>http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/proddoc</u> <u>s/ex2kplan/c13secur.asp</u> (May 26, 2003).

- Microsoft, "Exchange 2000 Server Resource Kit, Chapter 30 Security." URL: http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/reskit/re squide/c30scrty.asp (May 26, 2003).
- Microsoft," Flaw in Microsoft VM ould Enable System Compromise (816093)," Apr 14, 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-011.asp (Jun 7, 2003).
- Microsoft," HOW TO: Download, Install, and Remove the IIS MetaEdit 2.2 Utility," May 20, 2003, URL: http://support.microsoft.com/default.aspx?scid=kb%3Benus%3B232068#3 (Jun 7, 2003).
- Microsoft "How to Use the RestrictAnonymous Registry Value in Windows 2000: KB 246261." URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;246261 (May 26, 2003).
- Microsoft, "Microsoft Does Not Recommend Installing Exchange 2000 Server and Outlook 2000 or Later on the Same Computer," Knowledge Base Article-2666418. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;266418 (May 26, 2003).
- Microsoft "Securing Exchange 2000 Servers Based on Role: 309677." URL: http://www.microsoft.com/technet/prodtech/mailexch/opsquide/e2ksec03.asp (Mar 15,2003).
- Microsoft, "Securing Microsoft Windows 2000 Server," Microsoft Press, Feb 5, 2003. URL: http://www.microsoft.com/technet/security/prodtech/windows/secwin2k/default.as p (May 26, 2003).
- Microsoft, "Security Operations Guide for Microsoft Exchange 2000 Server," Microsoft Press, 2002, URL: http://www.microsoft.com/technet/security/prodtech/mailexch/opsquide/default.as **p** (May 26, 2003).
- Microsoft, "TechNet Briefing-Exchange and SQL 2K Security," Mountain View, CA, Microsoft, Jan 29, 2003.
- Microsoft "Troubleshooting Outlook Web Access in Microsoft Exchange 2000 Server: Q309508." URL: http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/support/t rowae2k.asp (Mar 15, 2003).
- Microsoft "XADM: Clients Cannot Browse the Global Address List After You Apply the Q299687 Windows 2000 Security Hotfix: KB 309622." URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309622 (May 26, 2003).
- Mullen, Tim. "Exchange 2000 in the Enterprise: Tip and Tricks Part One" SecurityFocus. Jan 2, 2003. URL: http://www.securityfocus.com/infocus/1654 (Mar 21, 2003).
- Mullen, Tim. "Exchange 2000 in the Enterprise: Tip and Tricks Part Two" SecurityFocus. Jan 15, 2003. URL: http://www.securityfocus.com/infocus/1658 ( Mar 21, 2003).
- Pitsenbargar, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000," http://nsa2.www.conxion.com/win2k/guides/w2k-21.pdf, National Security Agency (NSA), v1.12, Aug 8, 2002.

- Robichaux, Paul, Controlling SMTP Relaying with Microsoft Exchange, Microsoft Press, 2002. URL: http://www.microsoft.com/technet/security/prodtech/mailexch/opsguide/default.as p (May 26, 2003).
- Robichaux, Paul. <u>Securing Messaging with Microsoft Exchange Server 2000</u>. Redmond: Microsoft Press, 2003.
- SANS Institute, "Securing Windows 2000 Step By Step," The SANS Institute, V 1.5, Jul 1, 2001.
- SANS Institute, Track 4 Hacker Techniques, Exploits and Incident Handling, The SANS Institute, 2003.
- SANS Institute, Track 5 Securing Windows, The SANS Institute, 2003.
- SANS Institute, Track 7 Auditing Networks, Perimeters and Systems, The SANS Institute, 2003.
- Travers, Shawn, "How to secure your Exchange 2000 Environment," Microsoft TechNet Webcast, Jan 10, 2003.
- Weber, Chris, "Securing Exchange 2000," SecurityFocus, Part One, Apr 23, 2002. URL: http://www.securityfocus.com/infocus/1572 (Mar 26, 2003).
- Weber, Chris, "Securing Exchange 2000," SecurityFocus, Part Two, May 8, 2002. URL: http://www.securityfocus.com/infocus/1578 (Mar 26, 2003).

## Appendix A

Comment:

Assessment Report of Back-End Exchange Server

#### Network Host Assessment Report

05/26/2003

This report lists the hosts discovered by Internet Scanner after scanning the network, and for each host, identifies network services, user details, banner details, and vulnerabilities.

Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).

Purpose: For each host, the report provides the IP address , the DNS Name , the operating system type , and the status of the host (reachable or unreachable). The report also provides information about services, users, and barners identified by Internet Scanner.

Related reports : For a brief description of the hosts identified by Internet Scarner after scarning the network, see the Line Management/Host Assessment reports.

anerability S	evenity: H High	🐹 Medium	A Low
Session Info	<u>rmation</u>		
Session Neme: Polic <del>y:</del>	W2K SanCuston	File Neme: Koy:	
Hosts Scenned: Scen Stert: Comment:	1 5/24/2003 11828AM initialscan	Hosts Active Scen End:	1 5/24/2003 1:5844AM

P Address (DNS Name)		Operating System		Status
.1.1.1 (BACK-END) Service Detaik:		Windows NT		Reachable
Service Name	Short Description		Port #	Type
httpd.	httpd.		8D80	TĈP
bttps	btters		443	TCP
inar.	imap.		143	TCP
İMARS	inars.		993	TCP
microsoft-ds	Microsoff-DS		445	TCP
nethios-ssn	nethios-ssn		139	TCP
BOBY	BOBY		110	TCP
BORAE	BODIE		995	TCP
RPC	RPC		135	TCP
STUD.	SHID.	Death	25	TCP
Unknown Service Poll#20	Unknown Service	POIL#20 Doxt#S07	∡0 507	TCP
Iblocame Service Poil#595	Unknown Service	PoilH095	601	TCP
www.http	World Wide Web	HTTP	80	TCP
User Details:				
Account Name	Account Type	Commerts		
Guest	User			
200000	User			
XXXXXX	User			
300000	User			
None	Group			
200000	User			
200000	User			
300000	User			
Technicisn.				
# Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

				Status
Barmer Detaik				
Barner Ivve	Banner Text			
HTTPD	Microsoft-IIS/5.0			
Others				
<u>Additional Information</u>	Mare	Information		
IIS. version=5.0	Children C	a gor meanore		
IUSR_D2438G01				
IWAM_D2438G01				
Microsoft ESMTP MAIL Service,				
Bott-20	COTUOT	=Microsoft-IIS/5.0		
	====	hsFrontpageInfo_starts==	_	
	<html< td=""><td>&gt;<head><title>vermeet</title></head></td><td>RPC packet≺</td><td>title≻≺/head&gt;</td></html<>	> <head><title>vermeet</title></head>	RPC packet≺	title≻≺/head>
	<000) SD3m	⊳ ethod=men service:3.0.1	2 1 1 0 5	
	st	ањ=		
	<ul> <li>sul&gt;</li> </ul>			
	≤lj≥st	abus=917 <i>5</i> 05		
		For Frankriss on Buffs and		
300000		eserveeforsennor enne==		
300000				
X0000X				
Address (DATE Man a)		<b>b</b> a anud <b>ia</b> a <b>f</b> a aita -		Chadren
wm.es (nue name)		peranng system		STATUS
Interability Details: Hitp TraceProbled: HTTP TRACE is en TP TRACE upport is enabled on the Web server ically used for debugging and network analysis pu or. On Web server with HTTP TRACE support ipting and other Web browser vulnerabilities to ob- hertication information. This information could the Ref. medy: medy: ministrators should disable HTTP TRACE support	abled The HTTP TRACE met mossito requisithe on mabled, a remote strake tain servitive information enbaused by the attache conthe Web server. HT	hod & described in RFC 25 dents of HTTP request mess r could loverage this function about the Web server, incl r to lound further studies; IP TRACE apport can be d	ilo of the HTII sages received mality with hu hiling server o gainst fite affect is abled on Ap-	911 standard is by the Web own cross-site ockriss and ted Web whe HTTP
uherability Details: Hitp DraceRnabled: HTTP TRACE is en TTP TRACE/support is enabled on the Web server pically used for debugging and network analysis pu- mer. On Web servers with HTTP TRACE/support ipting and other Web boraser unherabilities to ob fiveritarian information. This information could the wer. enedy: ministrators should disable HTTP TRACE/support rerusing the mod_creative module and on Microson <b>DisEcondopageInfo: HS with FrontPagein</b> isosoft Windows NT4 running Internet Information formation to an attacker. A remote attacker could no conymous Internet account and physical paths on the enedy:	abled The HTTP TRACE met moses to request the on wabled, a remote attach, tain sers five information embeused by the attach ton the Web server. HT off, internet information S formation gathering on Server with FurntPage ake specific HTTP reque e affected system.	hod & described in RFC 25 terits of HTTP request mess r could loverage this function a shout the Web server, incl r to lound further stadies to lound further stadies IP TRACE apport can be dervices (IE) using the UKI (CAN-2000-0114) e Server Extensions 97 or 96 ests to the server that would	iló of the HTTI ages received mality with In Inding sever of goinst the affect is abled on Apa Scan tool. B could no eals neveal the nam	P 11 standard is syfthe Web own cross-site okkies and tedWeb whe HTTP ansitive te of the
Interability Details: Http: DraceRnabled: HTTP TRACE is er TTP TRACE/support is enabled on the Web server pically used for debugging and network analysis pu- mer. On Web servers with HTTP TRACE/support inpring and other Web boraser vulnerabilities to ob theritation information. This information could the wer. enedy: Intristrators should disable HTTP TRACE/support merusing the mod_require module and on Micros <b>Ins. Record age: Information</b> Micros <b>Ins. Record age: Information</b> icrosoft Windows NT4 running Internet Information icrosoft Windows NT4 running Internet Information insymous Internet account and physical paths on the enedy: wanload and install the patches in the order listed in ferences.	abled The HTTP TRACE met moses to request the orn availed, a remote stracks tain sensitive information embeused by the attacks ton the Web server. HT of internet information S formation gathering in Server with ForntPage ake specific HTTP requ e affected system. The "Microsoft FrontPage	hod as described in RFC 25 farts of HTTP request meas r could lowerage this function about the Web server, incl r to lownch further stacks a IP TRACE support can be of Services (IE) using the UKI (CAN-2000-0114) e Server Extensions 97 or 98 ests to the server that would ge Server Extensions 2002 f	ilo of the HTI ages received mality with bu haling sever co gainst fite affect is abled on Apa Scan tool. Could no eals investithe nam	9 11 standardis oyfhe Web own cross-site odkies and tedWeb adhe HTTP ansitive e of the borment. See
<ul> <li>Intrability Details:</li> <li>Ittip TraceRnabled: HTTP TRACE is en</li> <li>Ittip TraceRnabled: HTTP TRACE is en</li> <li>TTP TRACEsupport is enabled on the Web server pically used for debugging and network malysis puters. On Web servers with HTTP TRACEsupport in the information information. This information could the meters and other Web bookser with enablisis to obtain the information. This information could the wet.</li> <li>enedy:</li> <li>intrastructors should disable HTTP TRACE support over using the mod_require module and on Micros <b>Its Ecouph ageInfo</b>; <b>HS with FrontPage in</b> icrosoft Windows NT4 running Internet Information on stacker. A remote stacker could not mymous Internet account and physical paths on the enedy:</li> <li>wanload and install the patches in the order listed informers.</li> <li>a savekaround, if you donot require the functiona anthage Server Extensions. Microsoft HIS With an Web and and missions.</li> </ul>	abled The HTTP TRACE met moses to request the one availed, a remote stracho ended set information ended set information ended set information S formation gathering in Server with ForntPage ake specific HTTP reque affected system. The "Microsoft FrontPage itypnovided by ForntPage	hod as described in RFC 25 fants of HTTP request mess r could lowerage this function about the Web server, include r to low characteristic structures (I and the Support cambe of Services (IIS) using the UKS (CAN-2000-0114) e Server Extensions 97 or 98 ests to the server that would ge Server Extensions 2002 f ge Server Extensions 2002 f ge Server Extensions 2002 f	ilo of the HTI ages received mality with bu haling server co gainst fite affect is abled on Apa Scan tool. Could neveals investithe nam for Windows" of re all the files a	9 11 standardis oyfhe Web own cross-site okties and tedWeb adhe HTTP ensitive e of the bournent. See ssociated with
<ul> <li>Hitp DraceRnabled: HTTP TRACE is en</li> <li>Hitp DraceRnabled: HTTP TRACE is en</li> <li>TTP TRACE/upport is enabled on the Web server pically used for debugging and network analysis power. On Web servers with HTTP TRACE/upport information. This information could the web servers with HTTP TRACE/upport ments information. This information could the wet.</li> <li>enedy:</li> <li>Instructors should disable HTTP TRACE/upport is module and on Micros</li> <li>Instructors should disable HTTP TRACE/upport reversing the mod result module and on Micros</li> <li>Instructors should disable HTTP TRACE/upport reversing the mod result module and on Micros</li> <li>Instructors should disable HTTP TRACE/upport reversing the mod result module and on Micros and Provide and on Micros and Exercise.</li> <li>Instructors and tracker. A remote attacker could no onymous Internet account and physical paths on the enedy:</li> <li>wankanound, if you donot require the functiona anthese Server Extensions.</li> <li>Instruction of Microsoft IIS Web1</li> <li>Bayth day Burnning: Microsoft IIS Web1</li> <li>Bayth day Burnning: Microsoft IIS Web1</li> <li>Bayth day Burnning and Versioning (WebDA sources on the Web.</li> </ul>	abled The HTTP TRACE met moses to request the one walled, a remote strach- ended set in enderstade enderstade information enderstade by the attack toon the Web server. HT of internet information S formation gathering in Server with ForntPage also specific HTTP reque affected system. The "Microsoft FrontPage itypowided by ForntPage DAV service is number V) extends the HTTP/1 J	hod as described in RFC 25 fants of HTTP request mess r could lowerage this function about the Web server, include the lower function of the trades of the lower function of the trades for the support cambe of cervices (IIS) using the UK (CAN-2000-0114) a Server Extensions 97 or 96 ests to the server that would ge Server Extensions 2002 f ge Server Extensions 2002 f	iló of the HTI sages received) mality with bu haling server co gainst fike affect is abled on Apa Scan tool. Could neveals neveal the ram for Windows" of re all the files a	2 11 standardis syfthe Web own cooses site ookies and ted Web adne HTTP ensitive e of the boomment. See ssociated with and manage
<ul> <li>Intrability Details:</li> <li>Http: TraceRnabled: HTTP TRACE is en</li> <li>ITP TRACE/support is enabled on the Web sewer pically used for debugging and network analysis power. On Web sewers with HTTP TRACE/support in the information information. This information could the statement with the trace of the statement of the sewer with HTTP TRACE support reversing the moder provide module and on Microsoft Windows NT4 running Internet Information on stacker. A remote stacker could not yours with enter the second and install the patches in the order listed inferences.</li> <li>Is Web dev Running: Microsoft IIS Web 2 Sewer Extensions.</li> <li>Is Web dev Running: Microsoft IIS Web 2 Sewer Extensions.</li> <li>Is Web dev Running: Microsoft IIS Web 2 Sewer Extensions.</li> <li>Is Web dev Running: Microsoft IIS Web 2 Sewer Sewer Extensions.</li> <li>Is Web dev Running: Microsoft IIS Web 2 Sewer Sewer Extensions.</li> </ul>	abled The HTTP TRACE met moses to request the one maked, a remote attacks tain seria the information subsused by the attacks ton the Web server. HT off internet information S formation gathering on Saver with FurtPage alse specific HTTP requires a frected system. The "Microsoft FrontPage itypovided by FortPage DAV service is running V) extends the HTTP/11 he system for legitimate is lied for best security pro-	hod as described in RFC 25 terris of HTTP request mess r could loverage this function is about the Web server, include the lowich further stacks a IP TRACE apport can be of Services (IE) using the URI (CAN-2000-0114) e Server Extensions 97 or 96 ests to the server that would ge Server Extensions 2002 f ge Ser	ilo of the HTTI sages received) mality with bu hing sever co- gainst the affect is abled on Ap- Scan tool. Could reveals reveal the nam for Windows" of re all the files a opublish, lock, s required, ensu- tor required, ensu-	P 11 standard is syfthe Web own cross-site okties and tedWith whe HTTP ensitive e of the boomnent. See ssociated with and manage re that seconity if it was
<ul> <li>alterability Details:</li> <li>Http: TraceRnabled: HTTP TRACE is en</li> <li>TTP TRACE/support is enabled on the Web sewer pically used for debugging and network analysis power. On Web sewers with HTTP TRACE/support in the information information. This information could the set of the sever with HTTP TRACE support reversing the moder provide module and on Microsoft Windows NT4 running Internet Information on tracker. A remote attaker could not you will be the arder listed in formation on attaker. A remote attaker could not you will be the arder listed in formation on attaker. A remote attaker could not you will be the arder listed in formation on attaker. A remote attaker could not you will be and install the patches in the order listed in formations.</li> <li>Is Web dev Running: Microsoft IIS Web Sources on the Web.</li> <li>anedy:</li> <li>anyona attaker and Versioning (Web DA sources on the Web.</li> <li>anedy:</li> <li>anyona attaker and Versioning (Web DA sources on the Web.</li> <li>anedy:</li> <li>and hat intra and you do not require the functiona antipage Sever Extensions.</li> <li>Is Web dev Running: Microsoft IIS Web A sources on the Web.</li> <li>anedy:</li> <li>antip Microsoft web day. Service is naming onfitting had been configured or patches habeen apply abled under supprince groups and sources, disable it for the superior.</li> </ul>	abled The HTTP TRACE met moses to request the one makel, a remote stacks, tain sets the information subsused by the attacks ton the Web server. HT off internet information S formation gathering on Saver with ForntPage alse specific HTTP reque a affected system. The "Microsoft FrontPage ity provided by ForntPage ity provided by ForntPage DAV service is number V) extends the HTTP/1.1 he system for legitimate a liked for best security pra- m the system.	hod as described in RFC 25 farts of HTTP request mess r could lowerage this function about the Web server, include the lower function of the trades. IP TRACE support cambe of Services (IS) using the USI (CAN-2000-0114) a Server Extensions 97 or 98 ests to the server that would ge Server Extensions 2002 f ge S	ilo of the HTTI sages received) mality with lan hiring sever co- goinst fite affect is abled on Apri- Scan tool. 8 could reveal so inveal the ran for Windows" of re all the files a opublish, lock, s required, ensu- to required, ensu-	P 11 standard is syfthe Web own cross-site okties and tedWith whe HTTP ensitive e of the boarment. See ssociated with and manage re that seconity if it was
<ul> <li>Intrability Details:</li> <li>Http: TraceRnabled: HTTP TRACE is en</li> <li>ITP TRACE/support is enabled on the Web server pically used for debugging and network analysis porter. On Web servers with HTTP TRACE/support in the information. This information could the server with HTTP TRACE support reversing the nod, result module and on Micros         <ul> <li>Intributed and results module and on Micros</li> <li>Internet account and physical paths on the energy:</li> <li>windows MT4 running Internet Information could and install the pathes in the order listed information.</li> <li>Internet account and physical paths on the energy:</li> <li>walload and install the pathes in the order listed information.</li> <li>Intervent account and physical paths on the energy:</li> <li>walload and install the pathes in the order listed information.</li> <li>Intervent Authoring and Versioning (WebDA sources on the Web.</li> <li>Intervent Authoring and Versioning (WebDA sources on the Web.</li> <li>anthistrators may temp orarily disable webDA's stribute the superiors of particular sources.</li> </ul> </li> </ul>	abled The HTTP TRACE met moses to request the one abled, a remote stracky tain servine information subsussed by the attacky ton the Web server. HT: at internet information S formation gathering an Save with FurntPage alse specific HTTP requ- e affected system. The "Microsoft FrontPage alse specific HTTP requ- ity provided by FortPage DAV service is number V) extends the HTTP/11 he system for legitimates list for best security pra- m the system. Vapport on HS 5 servers	hod as described in RFC 25 fants of HTTP request mess r could lowerage this function about the Web server, include the lower function of the trades. IP TRACE support cambe of Services (IS) using the UK (CAN-2000-0114) as Server Extensions 97 or 98 ests to the server that would ge Server Extensions 2002 f ge Server Extensions 2002 f ge Server Extensions 2002 f ge Server Extensions 2002 f reasons. If use of webdan is times. If use of webdan is times. If use of webdan is times. If use of webdan is	iló of the HTI sages received mality with bu hiling server co gainst fixe affec is abled on Aps Scan tool. Could reveal s in which we all the real the ran for Windows" of the all the files a opublish, lock, s required, ensu- to required, ensu- to required or avledge Base At	<ul> <li>211 standardis syrfhe Web own cross-site okcies and tedWith</li> <li>adve HTTP</li> <li>ensitive e of the</li> <li>loomnent. See</li> <li>sociated with and manage</li> <li>re fluit seconity if it was</li> <li>tticle 241.520</li> </ul>
<ul> <li>Intrability Details:</li> <li>Http: TraceRnabled: HTTP TRACE is er</li> <li>ITP TRACE/support is enabled on the Web server pically used for debugging and network malysis pointer. On Web servers with HTTP TRACE/support is enabled on the Web servers with HTTP TRACE/support is enabled.</li> <li>Intrastrators should disable HTTP TRACE/support reversing the mod_result module and on Microsoft Windows NT4 running Internet Information on Marker. A remote stacker could normation to an attacker. A remote stacker could normation to an attacker. A remote stacker could normation and install the patches in the order listed inferences.</li> <li>Intrastrators of yoghdar, Service is norming on the Servers.</li> <li>Intervention of the Web.</li> <li>Intrastrators of the web.</li> <li>Intrastrators of the web.</li> <li>Intervention of the support of the state of the support of the s</li></ul>	abled The HTTP TRACE met moses to request the one model, a remote stracky tain sets five information enbeursed by the attacky toon the Web server. HTT off Internet Information S formation gathering in Server with ForntPage ake specific HTTP reque a sefected system. The "Microsoft FrontPage ake specific HTTP reque it ypnovided by FrontPage <b>DAV service is runnin</b> W) extends the HTTP/11 the system for legitimate a lied for best security pra- im the system. Vapport on HS 5 servers <b>service is running on</b> maps legital names torm- com service is exhled to yow NT 4.0 workstations	hod as described in RFC 25 farts of HTTP request mess r could lowerage this function about the Web server, include the low of the Server, include Server Extensions of the USE (CAN-2000-0114) e Server Extensions 97 or 96 ests to the server that would ge Server Extensions 2002 f ge Server Extensions 2002 f the system twoke-specific names. It sh maly on Windows 2000 dom for member servers, Window	ilo of the HTII sages received malify with bu- haling server co- gainst file affect (Scan tool. Could neveal s is abled on Apri- Scan tool. Could neveal s investible nam for Windows" of re all the files a opublish, lock, s required, ensu- tot required or a viedge Base Ar aps with Windo ain controllers ws 2000 works	<ul> <li>P 11 standardis syrfne Web own cross-site oddies and ted Web</li> <li>adae HTTP</li> <li>ensitive e of the</li> <li>boarment. See</li> <li>ssociated with</li> <li>and manage</li> <li>re fluit security</li> <li>if it was</li> <li>rticle 241.520</li> <li>ras NT4.0, and Windows</li> <li>tations or</li> </ul>
<ul> <li>Intrability Details:</li> <li>Http: TraceRnabled: HTTP TRACE is en</li> <li>TTP TRACE/support is enabled on the Web server pically used for debugging and network analysis porter. On Web servers with HTTP TRACE/support is enabled on the Web server switch HTTP TRACE/support is enabled.</li> <li>IntraceRnabled: HTTP TRACE/support is enabled on the trace of t</li></ul>	abled The HTTP TRACE met moses to request the one makeled, a remote stracky tain sensitive information subcussed by the attacky ton the Web server. HTT off internet information S formation gathering on Save with FundPage alse specific HTTP requ- e affected system. The "Microsoft FrontPage alse specific HTTP requ- ity provided by FortPage <b>DAV service is runnin</b> W) extends the HTTP/1.1 re system for legitimate : lied for best security pra- m the system. 'support on HS 5 servers service is running on- maps legital names to ru- color service is enabled ows NT 4.0 workstations the system for legitimate : lied for best security pra- maps legital names to ru- color service is enabled ows NT 4.0 workstations the system for legitimate : lied for best security pra- stem.	hod as described in RFC 25 farts of HTTP request mess r could lowerage this function about the Web server, inclu- ate lowed further, stacks, st in the web server, inclu- ate lowed further, stacks, st inclusion further, stacks, st inclusion further, stacks, st (CAN-2000-0114) is Server Extensions 97 or 98 ests to the server that would ge Server Extensions 2002 f ge Server Extensions 2002 f ge Server Extensions, remov- ing on the system I protocol to allow clients to reasons. If use of webday, is three. If use of webday is if possible. Microsoft From twoke-specific names. It sh may on Windows 2000 dom for member servers, Window these of Locator is to these. If use of Locator is to the set of Locator is to the set.	iló of the HTTI sages received) mality with bu hirg sever co gainst file affect is abled on Aps Scan tool. Could reveal s is could reveal s reveal the ram for Windows" of re all the files a opublish, lock, s required, ensu- not required or i all swith Windo ain controllers ws 2000 works required, ensu- ot required or i	<ul> <li>211 standardis syrfne Web own cross site okcies and ted With</li> <li>ache HTTP</li> <li>ensitive e of the</li> <li>loarment. See</li> <li>ssociated with and manage</li> <li>re that security fit was</li> <li>rticle 241,520</li> <li>ras NT4.0, and Windows</li> <li>tations or</li> <li>e that security fit was enabled</li> </ul>
<ul> <li>Intrability Details:</li> <li>Http: TraceRnabled: HTTP TRACE is en</li> <li>TTP TRACE/support is enabled on the Web server pically used for debugging and network maly sign over. On Web servers with HTTP TRACE support is enabled on the Web server witherabilities to obtain information. This information could the Web servers with HTTP TRACE support reversing the mod, results module and on Micros Treversing the mod, results module and on Micros Instructions information. A remote attacker could not your on attacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker. A remote attacker could not your on a stacker.</li> <li>Is Web day Running: Microsoft IIS Web 20 Statistical Authoring and Versioning (WebDA sources on the Web.</li> <li>In Statistical Authoring and Versioning (WebDA sources on the Web.</li> <li>Administrators may temporarily disable WebDAV stribes the process in detail. See References.</li> <li>Microsoft Locator service is a running onfittings halbeen configured or pathes halbeen with the full of a domain controllers; it is not enabled on Wind mber servers, or Windows XP. By default, the Locator service is a running onfittings halbeen configured or pathes halbeen appeders are with the source is norming on fittings halbeen configured or pathes halbeen appeders are wither the source is a running on fittings halbeen configured or pathes halbeen appeders appeders appeders appeders appeders appeders appeders appeder appeders appeders appeder appeders appede</li></ul>	abled The HTTP TRACE met moses to request the one and led, a remote stracky tain service is reinformation subsused by the attacky ton the Web server. HTT off internet information S formation gathering on Save with FundPage alse specific HTTP requ- e affected system. The "Microsoft FrontPage alse specific HTTP requ- ity provided by FortPage <b>DAV service is runnin</b> W) extends the HTTP/1.1 re system for legitimate : lied for best security pra- m the system. Service is running on- maps legital names to ru- color service is enabled ows NT 4.0 workstations the system for legitimate : lied for best security pra- stem. The system for legitimate : lied for best security pra- stem. The system for legitimate : lied for best security pra- stem.	hod as described in RFC 25 farts of HTTP request mess r could lowerage this function about the Web server, inclu- ate lower function that is a server, include for TRACE support cambe of Services (IIS) using the URI <b>(CAN-2000-0114)</b> is Server Extensions 97 or 98 ests to the server that would ge Server Extensions 2002 f ge Server Extensions 2002 f ge Server Extensions 2002 f ge Server Extensions, remov- ing on the system I protocol to allow clients to reasons. If use of webday is three. If use of webday is three. If use of webday is removed and windows 2000 dom for member servers, Window commember servers, Window the servers. If use of locator is a three. If use of locator is a three of locator is a	iló of the HTI sages received) mality with bu hirg sever co gainst file affect is abled on Aps Scan tool. Could reveal s is could reveal s reveal the ram for Windows" of re all the files a opublish, lock, s required, ensu- not required or i all or with Windo ain controllers ws 2000 works required, ensu- ot required or i mity of the syste	<ul> <li>211 standardis syrfne Web own cross site okcies and ted With</li> <li>and HTTP</li> <li>ensitive e of the</li> <li>loarment. See</li> <li>ssociated with and manage</li> <li>re that security fit was</li> <li>rticle 241,520</li> <li>ras NT4.0, and Windows</li> <li>tations or</li> <li>e that security fit was enabled</li> <li>em.</li> </ul>

# Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

P	Address	(DNS	Name}
ш	MILLIO,	(DIA9	mannej

Operating System

Status

Apply the latest Windows NT 4.0 Service Pack (SP3 or later), available from the Windows NT Service Packs Webpage. See Enterences .

--AND--

Restrict anonymous connections by changing the registry. Changing the Registry entries is only effective after applying Windows NT -SP3 or later.

To restrict anonymous connections in Windows NT:

CAUTION: Use Registry Effior at your own risk. Any charge made with Registry Effior may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that publisms caused by the use of Registry Effior can be solved.

1. If you have not already done so, apply the latest Windows NT4.0 Service Pade (SP3 or later).

- 2. Open Registry Editor. From the Windows NT Start menu, select Run, type regedi32, and click OK.
- 3. Go to HKEY_LOCAL_MACHINE SYSTEM ControlSet ControlVLSA.
- 4. From the Edit menu, select Add Value to display the Add Value dialog box.
- 5. In the Value Name field, type Restrict Anonymoux.
- 6.Select REG_DWORD as the Data Type.
- 7. Click OK to display the DWORD Ellior.
- 8. In the Data field, type 1. (Ignore the Radix setting.)
- 9. Click OK. Registry Editor adds the keyto the registry.

#### A Khio Check: SMTP daemon supports EHL O (CAN-1999-0531).

SMTP daemons that support Extended HELO (EHLO) can release information that could be useful to an attacker in performing an attack. Attackers have been boown to use the EHLO command to determine configuration information on SMTP daemons.

#### Remedy:

SMTP as defined in RFC 2821 (see References ) requires EHLO. Some SMTP implementations allowyou to disable EHLO, but this capability is neither required nor consistent across products.

If you are uncomfortable with the information that the Extended SMTP features can reveal, you may choose to disable EHLO on your nail sewer (if applicable), or switch to a mail sewer that allows EHLO to be disabled. Consult your mail sewer doomentation or contact your vendor for information on whether it is possible to modify your mail sewer configuration to disable EHLO.

# A Guest Exists: Guest account name exists

The Gust account is named "Gust." If your security policy requires that the gust account be renamed, then this name should be changed. Be aware, however, that an attacker can easily determine which account is the gust user, so this action is of very limited use in most situations. **Remedy**:

To rename the Guest account, follow the steps below appropriate for your platform.

For Windows NT:

- Open User Manager. (Brom the Windows NT Start menu, select Programs, Administrative Tools (Common), User Manager.)
- 2. Select the Guest account.
- 3. From the User mengi, select. Rename.
- 4. Type a new name for the Guest Account.
- 5. Click OK.

# For Windows 2000:

- 1. From the command prompt...
- For a Windows 2000 domain, start Active Directory Users and Computers Management, Console (dsa.msc.).
- For a stand-alone Windows 2000 computer, start Local Users and Gioups Management Console (hsimigrinsc).
- 2. Double-click on the Users folder.
- 3. Right-click on user Object of interest.
- Select Rename to change the username
- Type in new username and click on OK to save the setting.

Technician

4

# Auditing Microsoft Exchange 2000 Server An Administrator's Perspective

IP Address (DNS Name)

Operating System

Status

# A Icmp Tstamp: ICMP timestamp requests (CAN-1999-0524)

The target computer responded to an ICMP timestamp request. By accurately determining the target's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them.

### Remedy:

Configure your firewall or filtering router to block outgoing ICMP packets. Block ICMP packets of type 13 or 14 and/or code 0.

#### A lisRunning: Microsoft IIS is running on the system (CAN-1999-0633)

Microsoft Internet Information Server (IIS) is running on this computer. IIS is a Web server platform that is included in some common installations of Microsoft Windows NT and Windows 2000. IIS includes many important features, but for best security practices, it should only be present if Web services are needed on the system. When running IIS, it is important to ensure that the proper security settings are configured for best security practices.

#### Remedy:

If this system is designed to host Web content, then verify that the installation of IIS has been configured according to your corporate security policy, or use the IIS security checklist provided by Microsoft. See References. If Web services are not needed on this system, then disable IIS.

#### A Local User: Windows local user on workstation Yuln count = 5

A local user account has been found on a non-domain controller. Some sites require that all user accounts on workstations and standalone servers be managed through the domain.

# Remedy;

Remove the local user. To delete (permanently remove) a user account, follow the steps below appropriate for your platform.

For Windows NT:

- 1. Open User Manager. (From the Windows NT Start menu, select Programs, Administrative Tools (Common), User Manager.)
- 2. Select the local user from the list.
- 3. Press Delete and confirm the removal.

For a Windows 2000 domain:

- 1. Start Active Directory Users and Computers Management Console (dsa.msc) from a command prompt.
- 2. Double-click on the Users folder.
- 3. Right-click on the user of interest.
- 4. Select Delete to remove the user permanently.

For a stand-alone Windows 2000 computer:

#### MtaDiscovery: Message Transfer Agent service is running

The system is running a Message Transfer Agent (MTA) service.

#### Remedy:

If this system is intended to run a MTA service, then verify that the installation of the MTA has been configured according to your corporate security policy.

(C)