GIAC
CERTIFICATIONS

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

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, Author retains full rights.

ABSTRACT

Email systems have gone from nice to have communication mediums to business-critical 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: http://www.giac.org/practical/Filipe_Custodio_GSNA.zip (Feb 1, 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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: http://www.networkcomputing.com/911/911f1.html (Apr 21, 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Controls

CONTROLS	Input	Processing	Output
Active Directory			X
Active Directory—User rights	X		
Antivirus	X	X	X
Backup System, Process, & Tapes	X		
Change Management Policy and Procedures	X		
Disaster Recovery Plan			X
Email Use Policy	X		X
Encryption (128-bit) for web server (OWA)	X		
Exchange System Manager	X		
File Level Security	X		
Logging—Network, OS and Exchange		X	X
Monitoring logs			X
MultiLayered Network & Security Design	X		
General Operating System Controls	X		
Password complexity	X		
Patch Management	X		
Physical Access	X		
Corporate IT Policies	X		
User and Administrator Awareness	X		

Figure 1

© SANS Institute 2003, Author retains full rights.

DIAGRAM OF CURRENT MAIL INFRASTRUCTURE

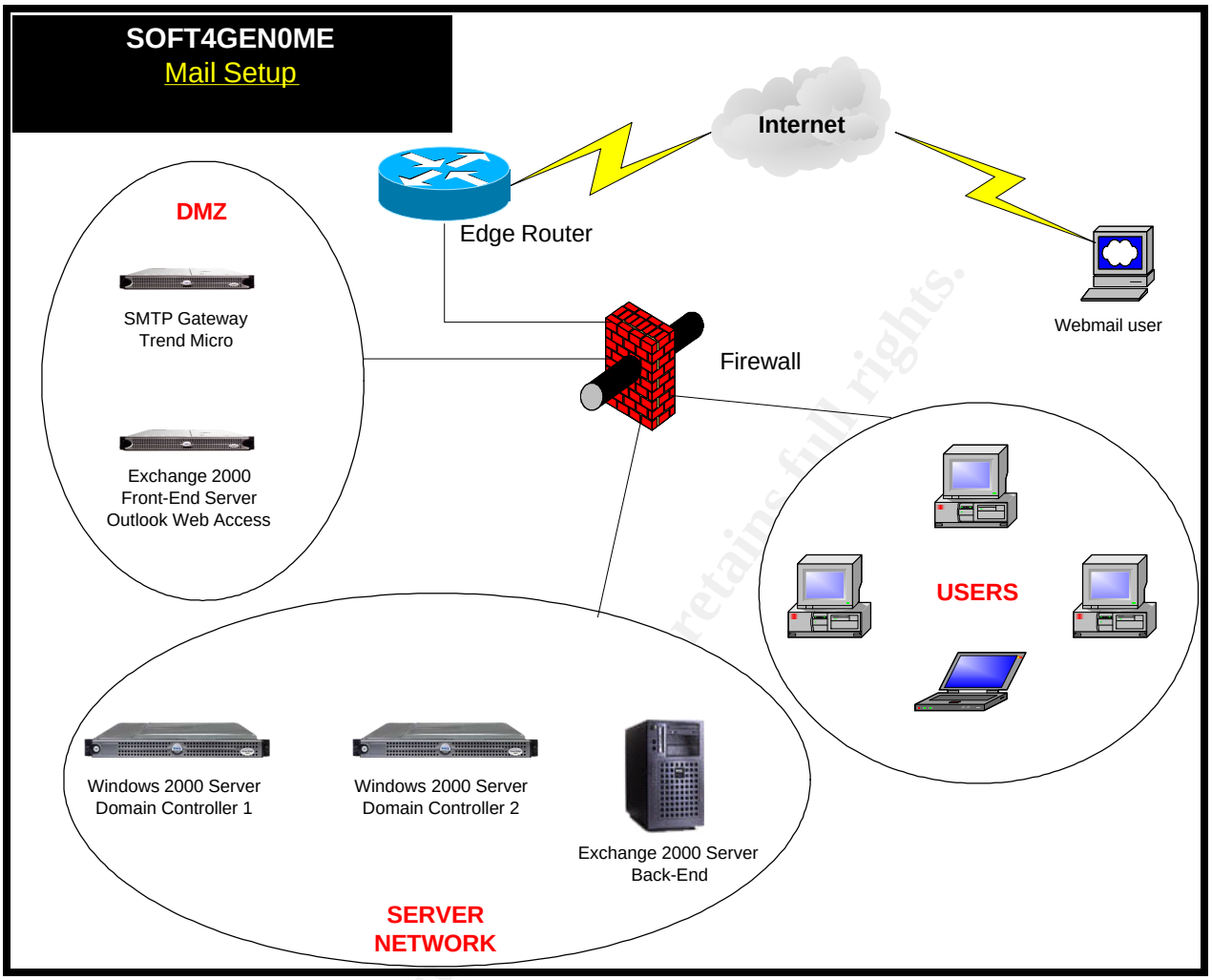


Figure 2

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 Step[5] guide and audit the OS before auditing Exchange.

---

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

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 (http://www.microsoft.com/technet). Additionally, I found an excellent document from the NSA, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000" (http://nsa2.www.conxion.com/win2k/guides/w2k-21.pdf)[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 (http://www.microsoft.com), SANS Reading Room (http://www.sans.org/rr), SecurityFocus articles (http://www.securityfocus.com), reading two excellent books on Exchange 2000 Server and Secure Messaging, GIAC paper on Exchange 5.5 (http://www.giac.org/practical/Filipe_Custodio_GSNA.zip)[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," http://nsa2.www.conxion.com/win2k/guides/w2k-21.pdf , 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: http://www.giac.org/practical/Filipe_Custodio_GSNA.zip (Feb 1, 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

Audit Step #1

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	Look for a positive (yes) answer for the following questions: 1. Does a formal policy for Security Awareness training exist? 2. Are their slides from the presentation available? 3. Are there meeting requests or a list of attendees available to prove the training happened? 4. Is there an attendee list that the security group maintains? 5. Did the attendees sign the list?
Testing	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: 1. Never open attachments from unknown source & be skeptical of known sources 2. Never send passwords in an email unless it is encrypted 3. Log off Outlook, OWA, and system when not in use (work, home, or remote location). 4. Don't respond to unsolicited commercial email (spam). It only confirms your address. 5. Don't respond to requests for personal information, including passwords. The Help Desk should never ask for your password. 6. Review of current email policy with end users.
Objective/Subjective	Objective-whether it was actually given or not Subjective-Content and effectiveness of the training

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #2

Verify appropriate Physical Security	
Reference	Bois, Justin, "Protect Yourself," SANS Reading Room, Apr 4, 2002. URL: http://www.sans.org/rr/physical/protect.php (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	Objective for locked door, log, and password protected. However, there are many other subjective measures for physical security. Here are a few examples: 1. Are there security cameras at the entry/exit of the server room? 2. Is the Data Center surrounded by firewalls to ensure that the room cannot be accessed through the ceiling? 3. Number of personnel with access to the Data Center. This is subjective in nature. 4. Are there any windows or direct external access from the building?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #3

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). 2. 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). 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 Article to do so. http://support.microsoft.com/default.aspx?scid=kb;en-us;q306962&id=kb;en-us;q306962
Compliance	The client is either installed or it isn't installed.
Testing	Look for client icon on the desktop. Attempt to execute. 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

Audit Step #4

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

Audit Step #5

Check for known vulnerabilities by a 3rd party application (Nessus-FREE, ISS Scanner, or similar tool)	
Reference	Cima, Susan. "Vulnerability Assessment," SANS Institute. 6 July 2001. URL: http://www.sans.org/rr/securitybasics/VA.php (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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #6

Verify that Mailbox size limits are enforced.	
Reference	McBee, Jim. Exchange 2000 Server 24seven. 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	Objective--Ensuring that storage limits are set Subjective--The level of the limits

Audit Step #7

Verify there is a message size limit for incoming and outgoing messages	
Reference	McBee, Jim. Exchange 2000 Server 24seven. 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk	The risk is that someone could send a 1 GB file to the server or from the server to the outside, which could cause a denial of service on the Exchange Server and the users would lose availability. In a worst situation, someone could accomplish a distributed attack with multiple large files being sent from various locations. By default, the setting is "no maximum size." Additionally, you don't want to become a spam server for someone inside your organization so it is best to limit the number of outgoing messages too. The same risk associated with mailbox size limits is applicable here.
Compliance	Verify that message limits are set for incoming and outgoing messages. Additionally, verify that the number of recipients is limited according to your business needs.
Testing	From Exchange System Manager, Select Global Settings, Select Message Delivery, Select Properties, Select Defaults. 1. Ensure "Sending message size" and "Receiving message size" have a maximum set. (10,000 KB or less is recommended) a. Attempt to send a message of 10,000 KB or more b. Attempt to receive a message of 10,000 KB or more 2. Ensure "Recipient limits has a maximum recipients set. (1000 or less is recommended)
Objective/Subjective	Objective

Audit Step #8

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

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

Audit Step #9

Verify that SMTP relay is off and SMTP traffic is being logged	
Reference	Robichaux, Paul. Securing Messaging with Microsoft Exchange Server 2000. 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" -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. **Test Logging** 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	Objective--Ensure the restrictions are set. Subjective--Different companies have different requirements.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #10

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	Subjective--Too 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.

Audit Step #11

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. Interview the administrator(s) and ask when was the last DRP test 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	Subjective--There is no way to verify the last successful restore in a subjective manner.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #12

Verify logging for the Exchange Server.	
Reference	Microsoft Baseline Security Analyzer (MBSA) v1.1 http://www.microsoft.com/technet/security/tools/tools/mbsahome.asp Pitsenbarger, Trent, "Guide to the Secure Configuration and Administration of Microsoft Exchange 2000." National Security 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. If too much logging is set, then the files will be too large to make for 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 **Part 1**, 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 **Part 2**, 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 **Maximum** --MSExchangeIS, Public Folder & Mailbox ---Logons: set to **Maximum** ---Access Control: set to **Maximum** ---Send On Behalf Of: set to **Maximum** ---Send As: set to **Maximum** --IMAP4Svc & POP3Svc: not applicable if IMAP & POP isnt utilized (service is disabled) ---Authentication: set to **Maximum**
Objective/Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #13

Verify that logs are reviewed regularly and archived?	
Reference	Robichaux, Paul. Securing Messaging with Microsoft Exchange Server 2000. 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 Step #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. Securing Messaging with Microsoft Exchange Server 2000. 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Compliance	All of the following services should be Disabled on Exchange Servers unless required by functionality: --Alerter: *only if needed for OS alerts* --Computer Browser: It is best to remove from Network Neighborhood. *May need for AntiVirus product and/or SMS, but this isn't typically needed on an Exchange Server.* --Distributed File System: *Only for DFS shares, enabled on domain controllers.* --File Replication: *Only needed for file servers synchronizing data among other servers.* --IIS Admin Service: *This can be disabled and **paused**. When IIS needs to be administered, enable service and resume.* --Indexing Service: *Only for full-text indexing of web content* --License Logging Service: *only if required by policy* --Microsoft Exchange Event: *For Exchange 5.5 compatible server applications* --Messenger --Microsoft Exchange IMAP4: *Do you have IMAP4 clients?* --Microsoft Exchange Information Store: *Required to be running for Back-End server. Not needed for Front-End server unless the Front-End server is also the SMTP relay / gateway and external messages are required to be sent directly to Public Folders in Exchange.* --Microsoft Exchange MTA Stacks: *Only needed for communicating with Exchange 5.5 or another X.400 system. FYI. Event ID 2000 will be generated as a warning, but this doesn't cause any problems.* --Microsoft Exchange POP3: *Do you have POP3 clients?* --Microsoft Exchange Site Replication Service: *Only needed for Exchange 5.5 compatibility.* --Microsoft Search: *Breaks content indexing if stopped; typically not needed on an Exchange Server.* --Network News Transport Protocol (NNTP): *Only required at installation.* --Print Spooler: *Only for sharing printers, which is not recommended on an Exchange Server*. --Removable Storage: *Only for tape drives and other removable media.* --Routing and Remote Access: *Only for VPN or dialup to the server, which is not recommended for Exchange Servers.* --Simple Mail Transport Protocol: *Required for Back-End server. Not required for the Front-End server unless used for sending and receiving SMTP mail.* --Telnet --Windows Installer: *Disabled, especially for front-end servers.* --World Wide Web Publishing Service: *Typically needed for public folder administration and Outlook Web Access.*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 the required ports are open between Exchange Servers, Domain Controllers, DNS servers, End Users, and Administrators	
Reference	McBee, Jim. "Exchange 2000 Security," Microsoft TechNet Webcast, Jan 29, 2003. McBee, Jim. Exchange 2000 Server 24seven. 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. *Assumption: DNS is on the Domain Controller (DC). If not, ensure that TCP 53 and UDP 53 are open.*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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) ---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 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. --Ports inside IPSec tunnel ---TCP 25: SMTP--only if FE server is designated to send & receive outside SMTP mail ---TCP 80: HTTP--used for HTTP for OWA. SSL is not used here. Microsoft :-(---TCP 135: RPC endpoint mapper
	Exchange Front-End to DC (very similar to above) --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 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. --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 3268/3269: LDAP to Global Catalog ---TCP 1024+: All ports above 1024!!! Recommend that you statically map the RPC replication ports. See KB 298369 on www.technet.com.
	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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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 --TCP 443: SSL for HTTP (OWA)
Testing	Run FPort or NMAP or SuperScan
Objective/Subjective	Objective

Audit Step #16

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #17

Verify password complexity with Password Policy	
Reference	Soft4Genome Company Password Policy Robichaux, Paul. Securing Messaging with Microsoft Exchange Server 2000. 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 **10 passwords remembered** -Maximum password age: **90 days** -Minimum password length: **8 characters** -Password must meet complexity requirements: **Enabled** under Account Lockout: -Account lockout duration: **0** -Account lockout threshold: **5 invalid logon attempts** -Reset account lockout counter after: **60 minutes** 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 out after 5 bad attempts.
Objective/Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Step #18

Verify that the SMTP 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 banner, the system is non-compliant.
Testing	Open the Command Line by Start, Run, Type cmd, hit enter. Open a Telnet session "telnet 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

Audit Step #19

Verify that IIS Lockdown Tool has been implemented.	
Reference	Microsoft, "TechNet Briefing-Exchange and SQL 2K Security," Mountain View, CA, Microsoft, Jan 29, 2003. Robichaux, Paul. Securing Messaging with Microsoft Exchange Server 2000. Redmond: Microsoft Press, 2003. 106. 88. Microsoft "Troubleshooting Outlook Web Access in Microsoft Exchange 2000 Server: Q309508," URL: http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/support/trowae2k.asp (Mar 15, 2003). Microsoft "Securing Exchange 2000 Servers Based on Role: 309677," URL: http://www.microsoft.com/technet/prodtech/mailexch/opsguide/e2ksec03.asp (Mar 15, 2003).
Control Objective	Ensure that access to the system is limited by the vulnerabilities of IIS.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

Audit Step #20

Verify that the Exchange Administrator cannot open another user's mailbox or send as another user.	
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 mailbox using the administrator's credentials. Have an administrator attempt to send a mail as another user using the administrator's credentials. If the administrator can do either, then this is non-compliant.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Objective/Subjective	Objective

Audit Step #21

Verify that sufficient measures have been taken to protect the Exchange Server(s) from viruses.	
Reference	Robichaux, Paul. Securing Messaging with Microsoft Exchange Server 2000. Redmond: Microsoft Press, 2003. 180. 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 (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. *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).* 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. *Please refer to the 3rd party antivirus application's manual for exactly how to check for automated updates and the latest virus definition files. This is very straightforward on for all of the major vendors.*
Objective/Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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**

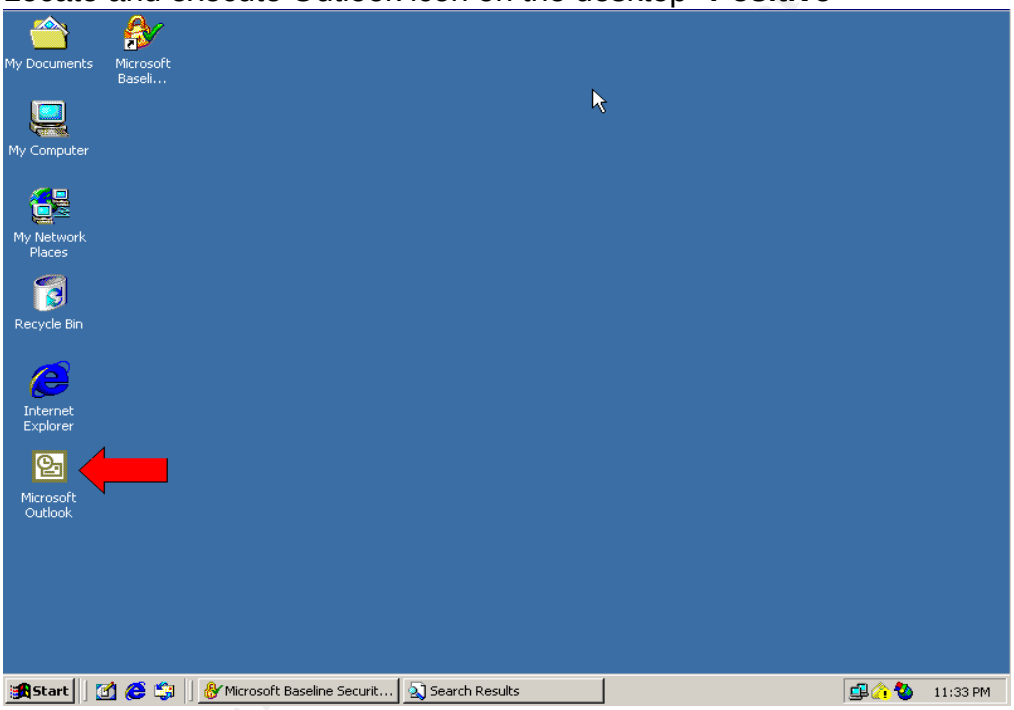


Figure 3

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

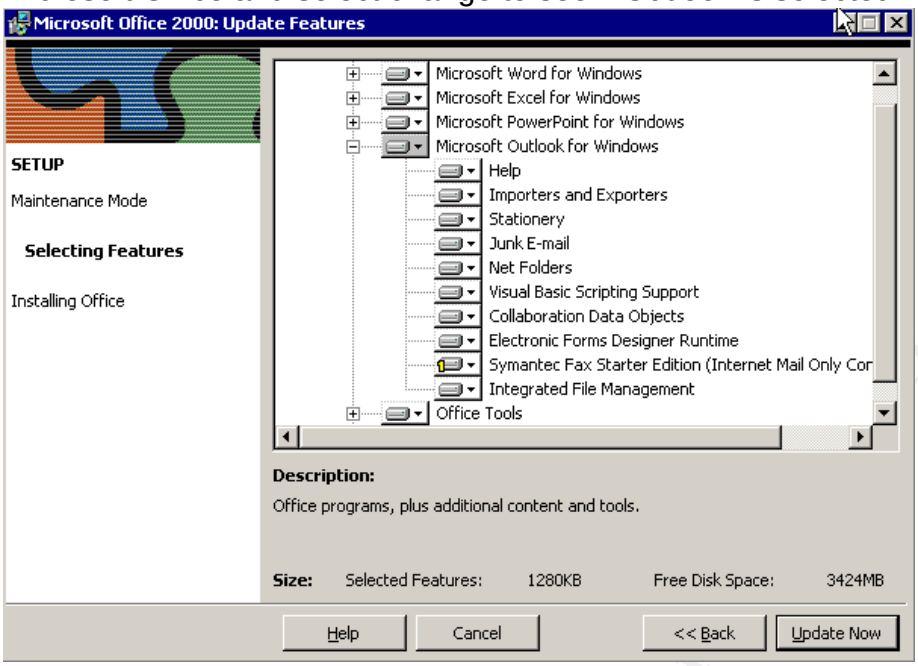


Figure 4

Search for outlook.exe--**Positive**

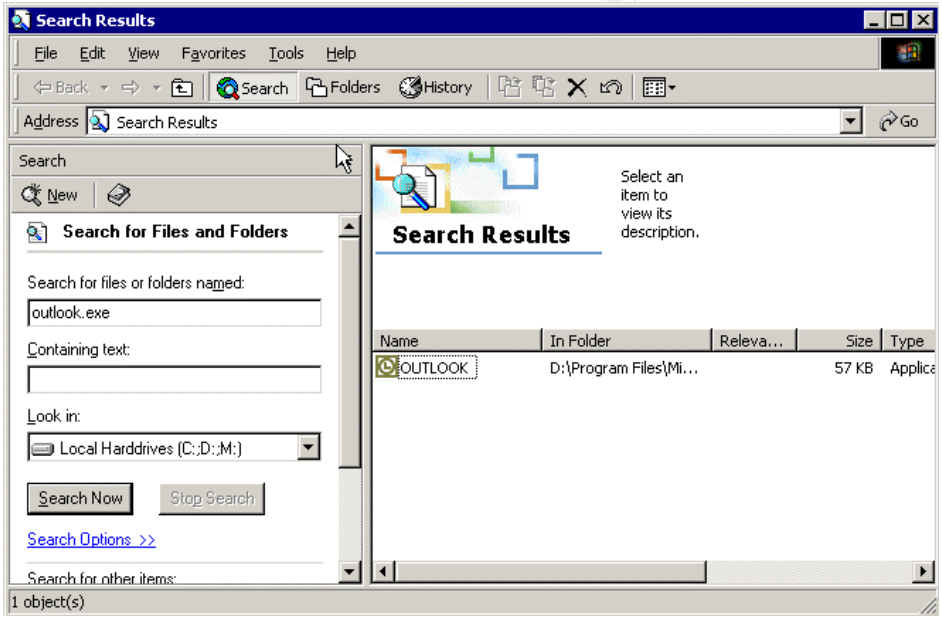


Figure 5

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**

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

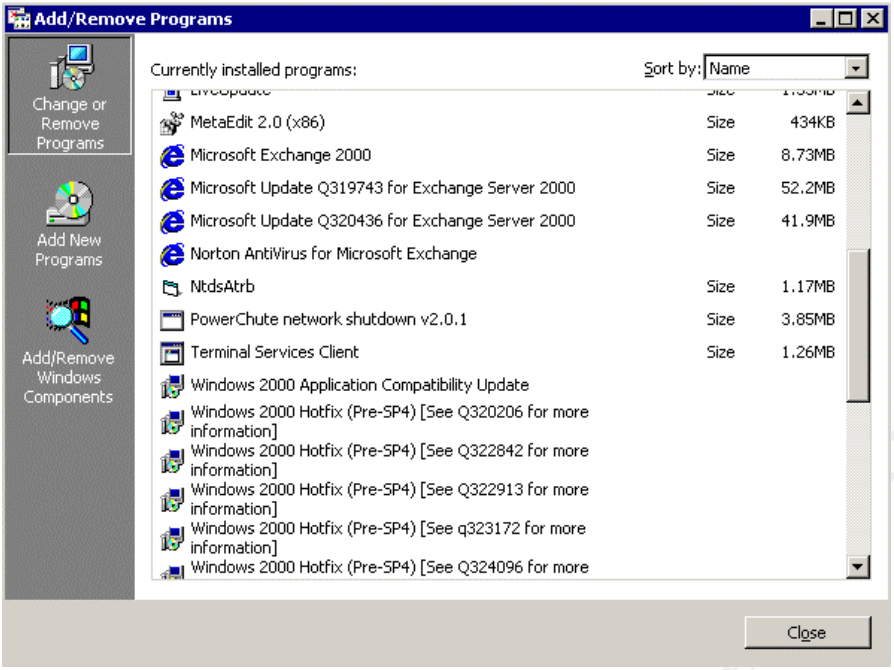


Figure 6

Search for outlook.exe--**Negative**

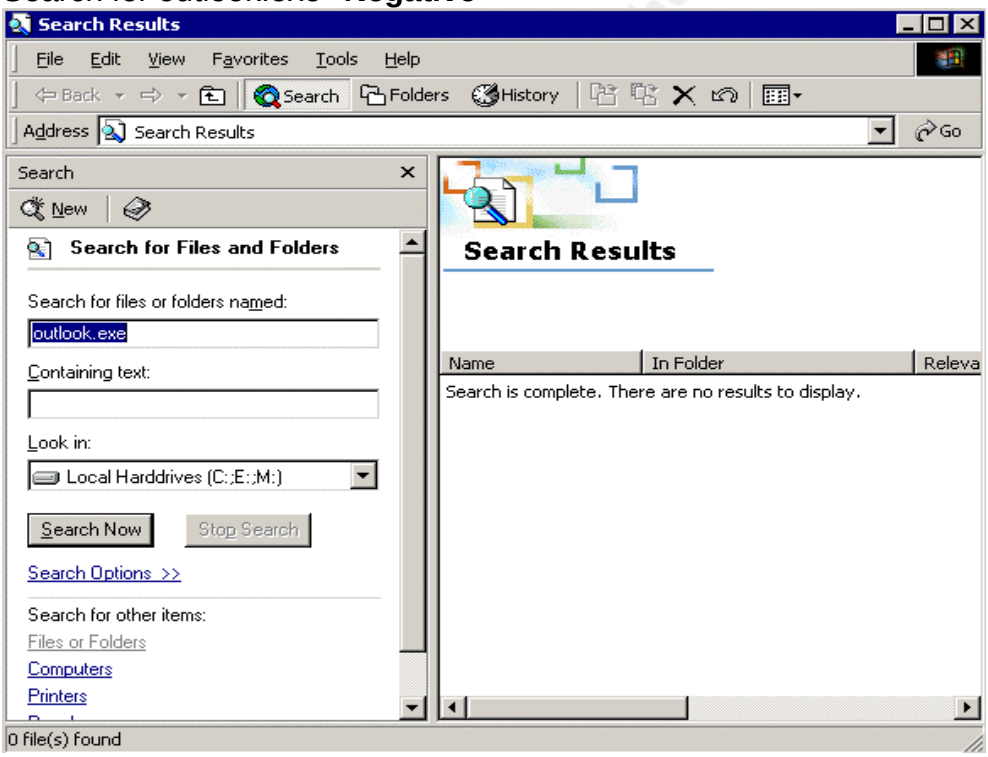


Figure 7

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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.

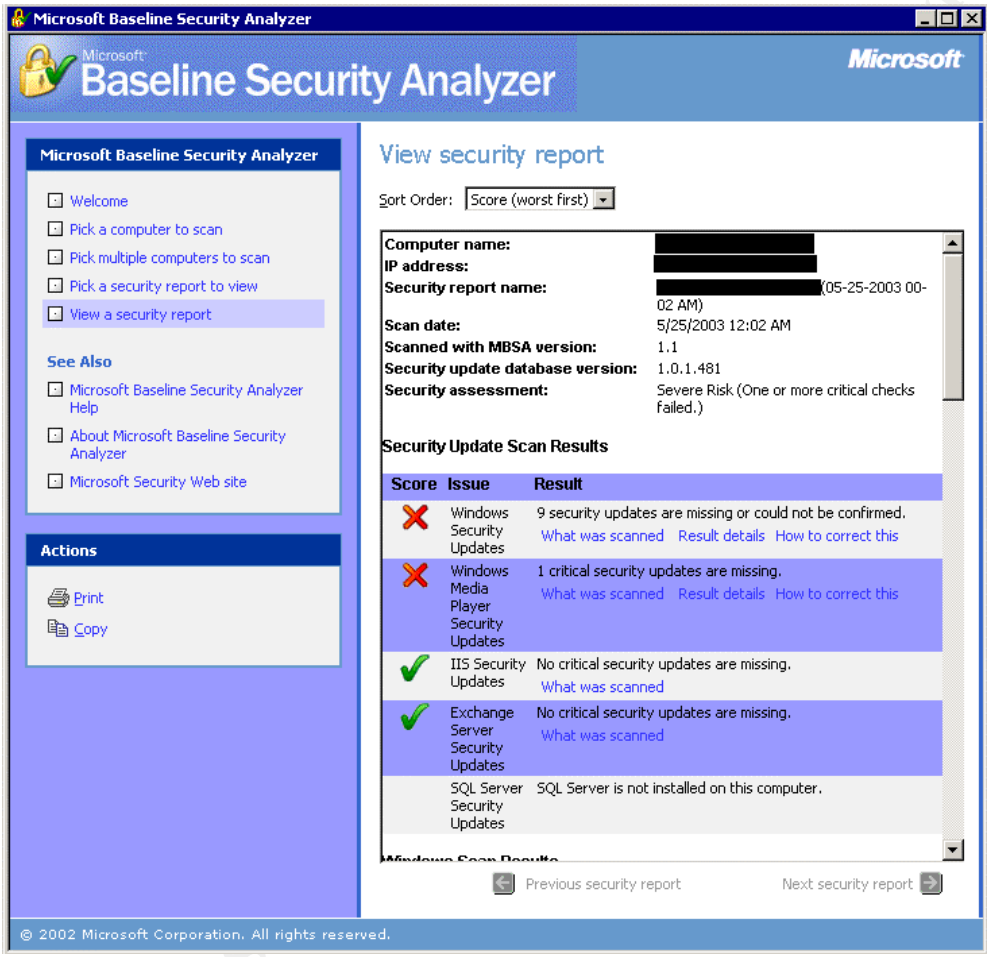


Figure 8

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: http://www.microsoft.com/technet/security/bulletin/MS03-011.asp (Jun 7, 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

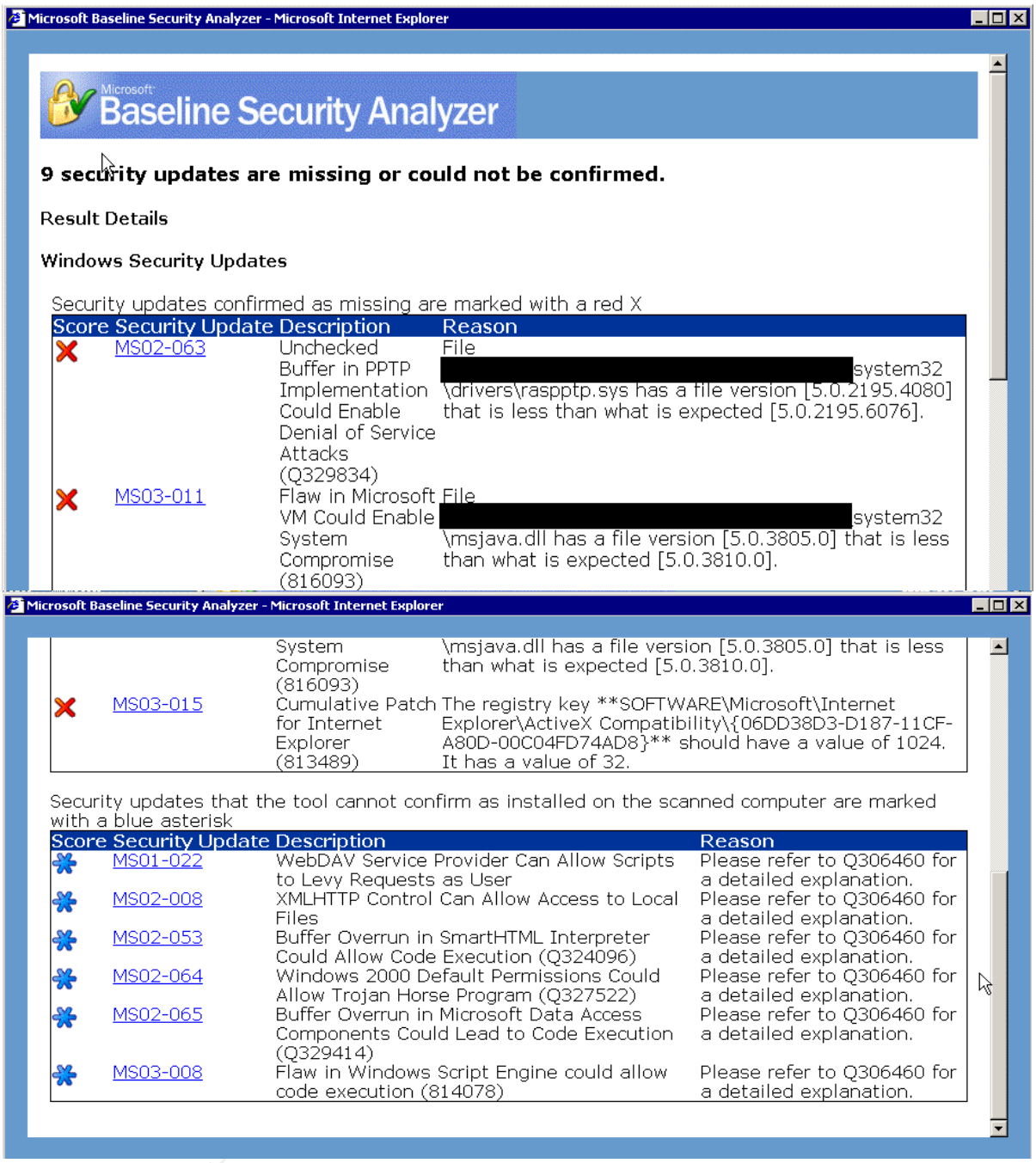


Figure 9

Although the following information from MBSA is not part of the checklist. It is found to be such a critical security flaw that action must be taken immediately. The Exchange Front-End Server that is exposed to the Internet does **not** have the C: (OS & programs) hard drive formatted as an NTFS file system. See figures 10 and 11 below.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 10

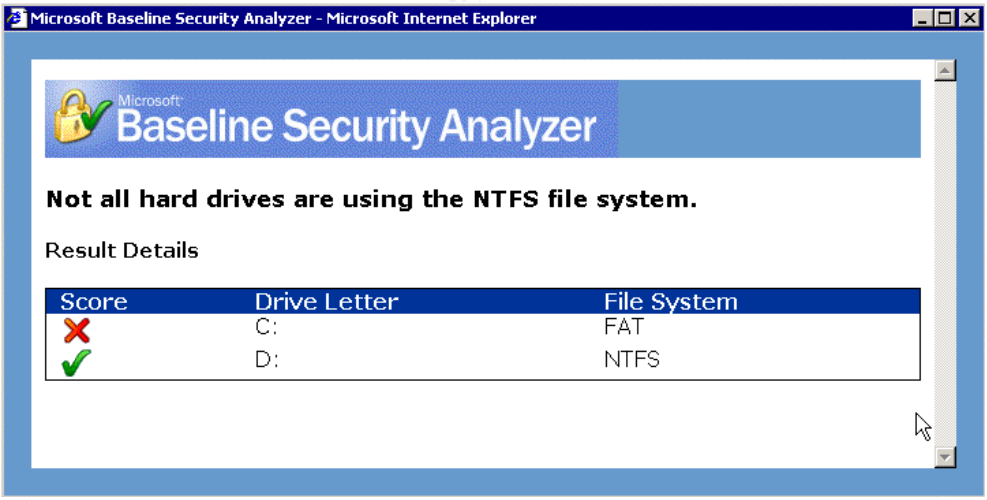


Figure 11

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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.

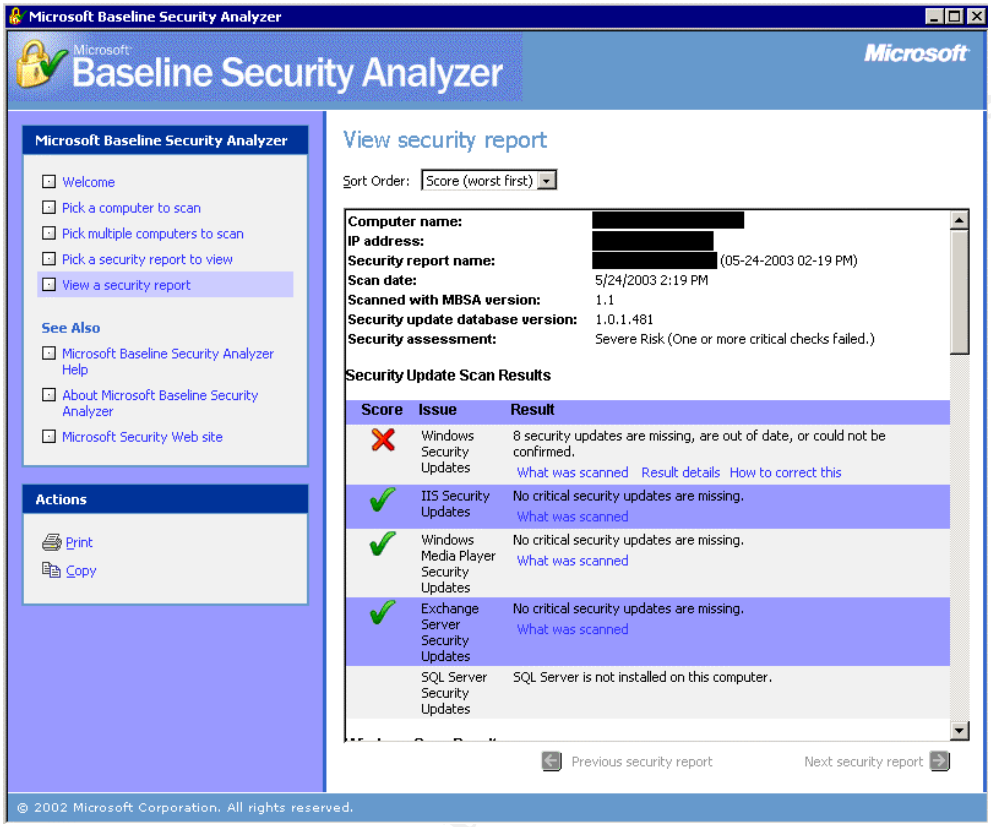


Figure 12

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 13 displays the details of the missing Windows Security Updates. Note the flaw in Microsoft Virtual Machine that could allow a system compromise.[9] .

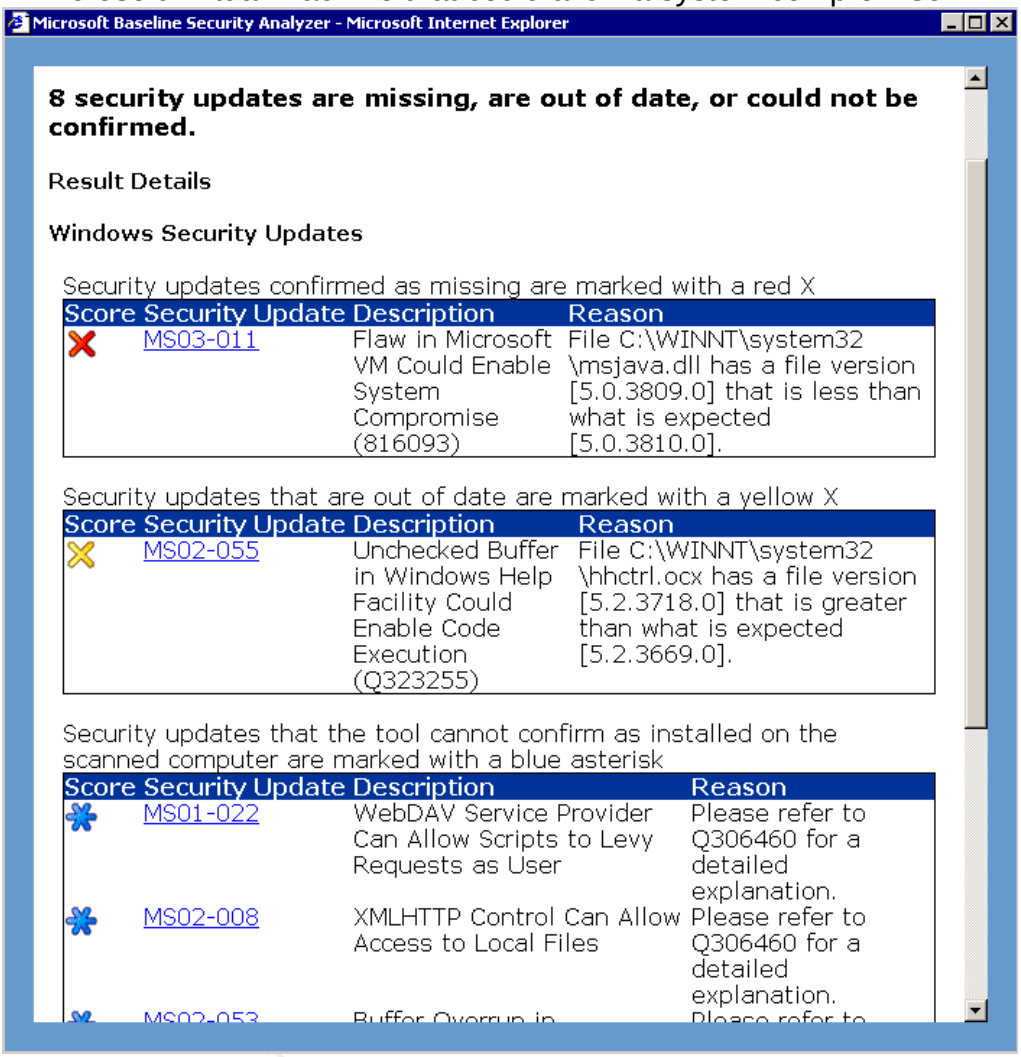


Figure 13

[9] 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).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

More results from the missing Windows Security Updates:

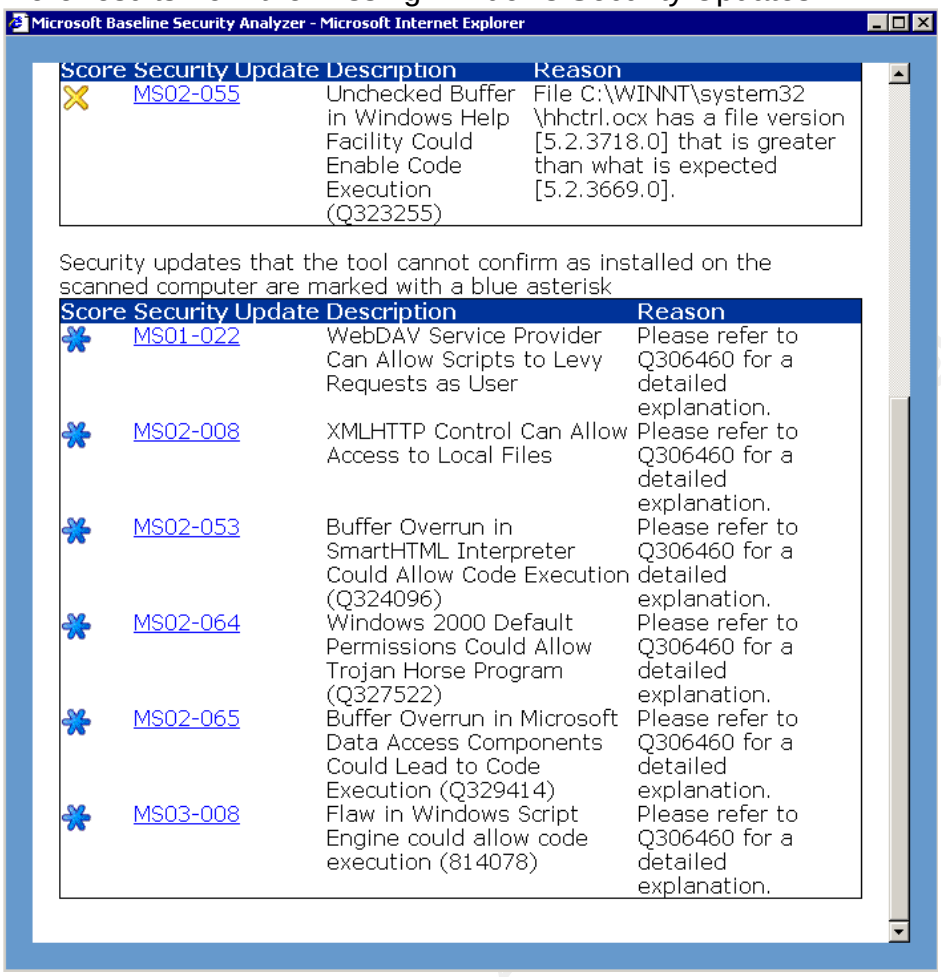


Figure 14

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

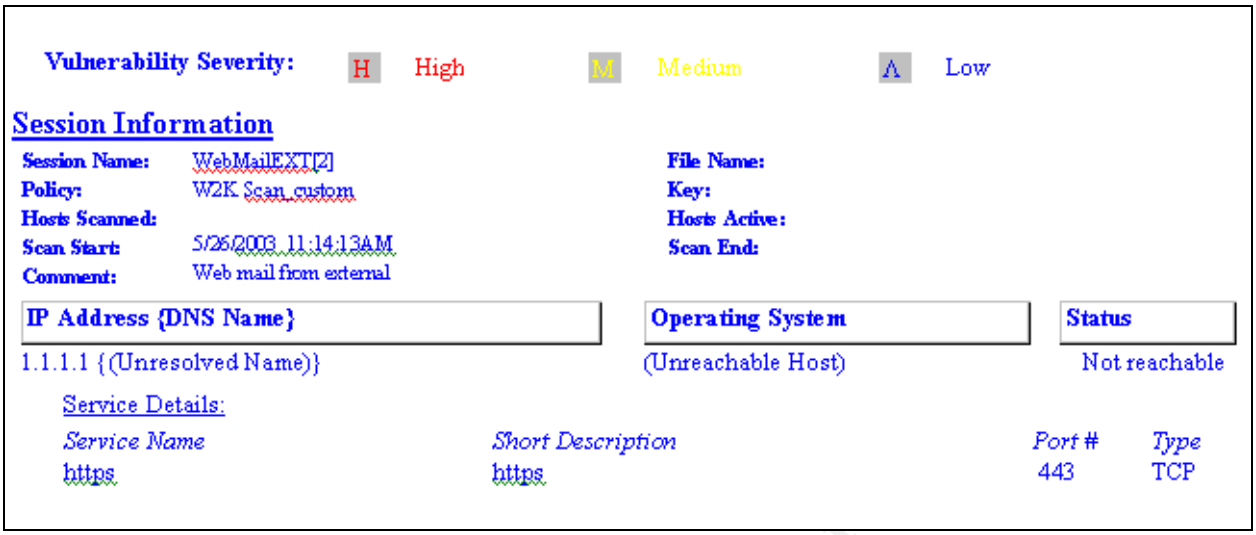


Figure 15

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: http://www.sans.org/webcasts/031803.php.

[11] 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).

[12] 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).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- 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.

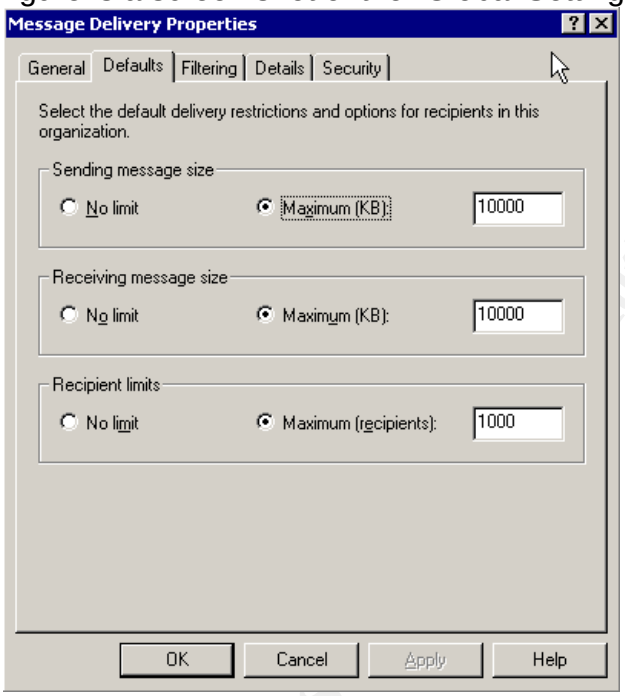


Figure 16

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

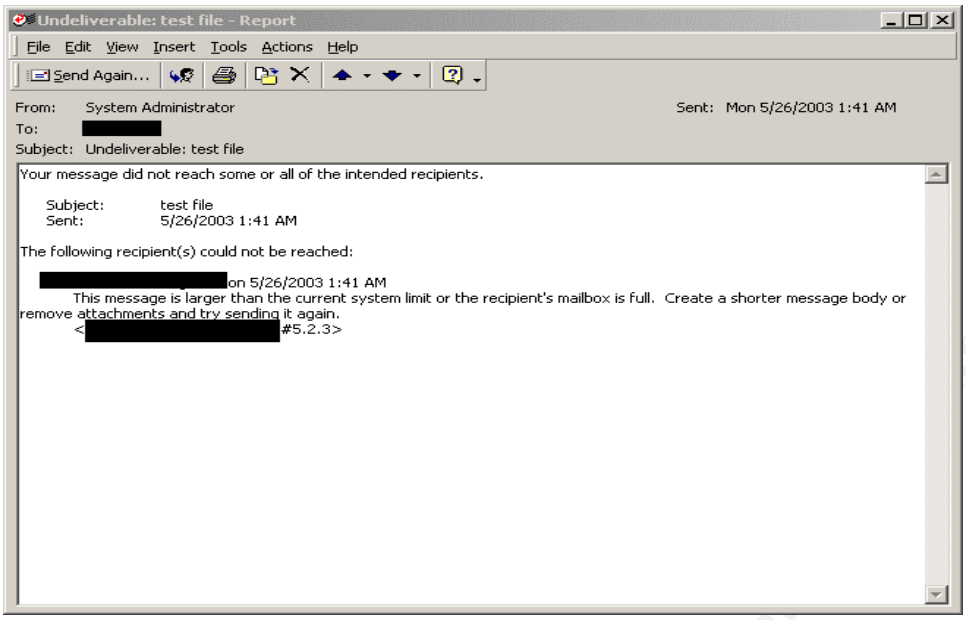


Figure 17

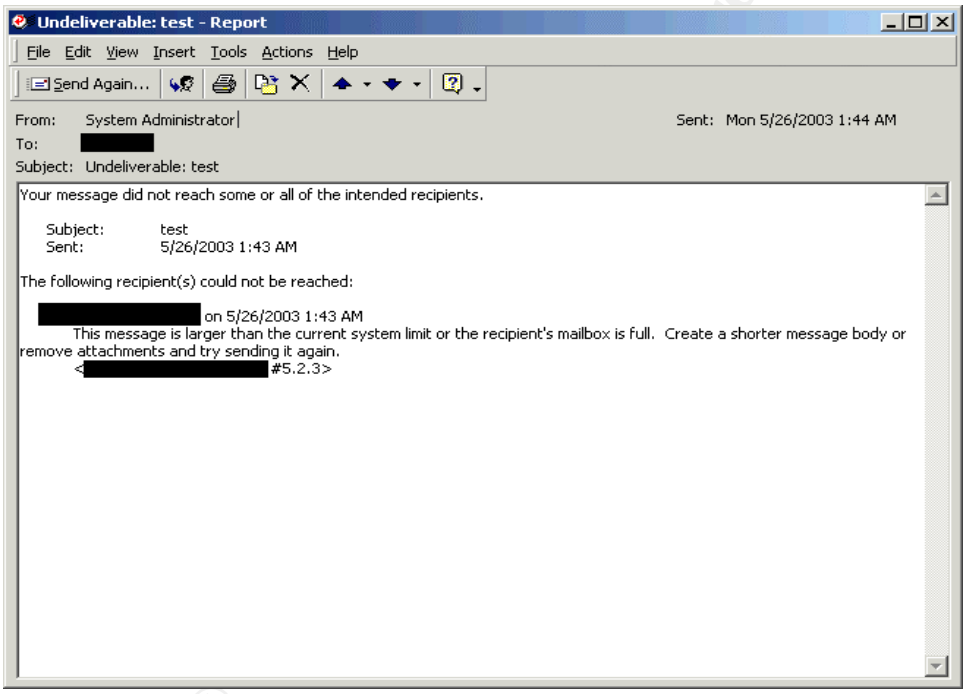


Figure 18

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

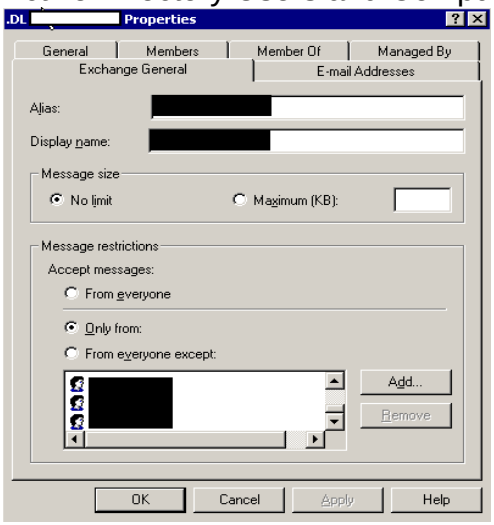


Figure 19

Message failed to send for all 6 distribution lists.

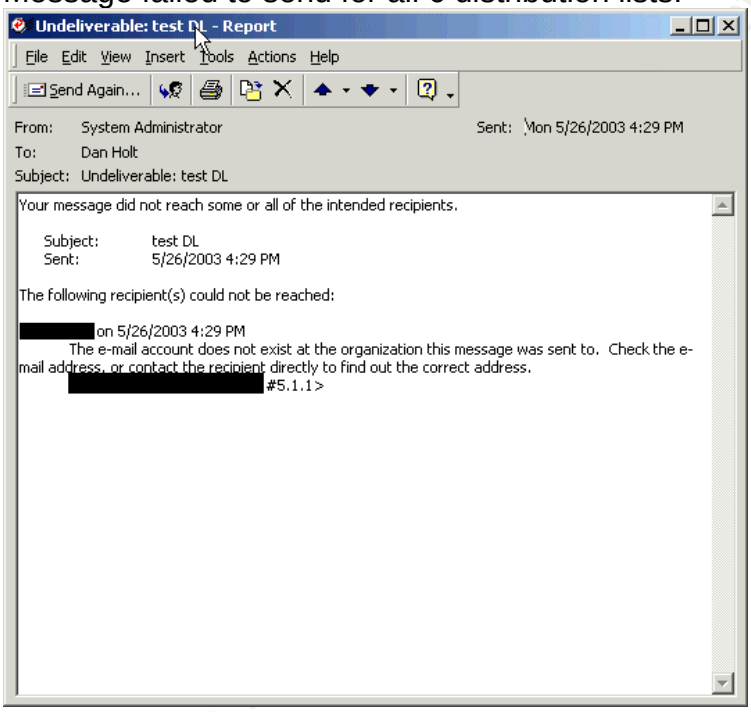


Figure 20

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`"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

  - 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.

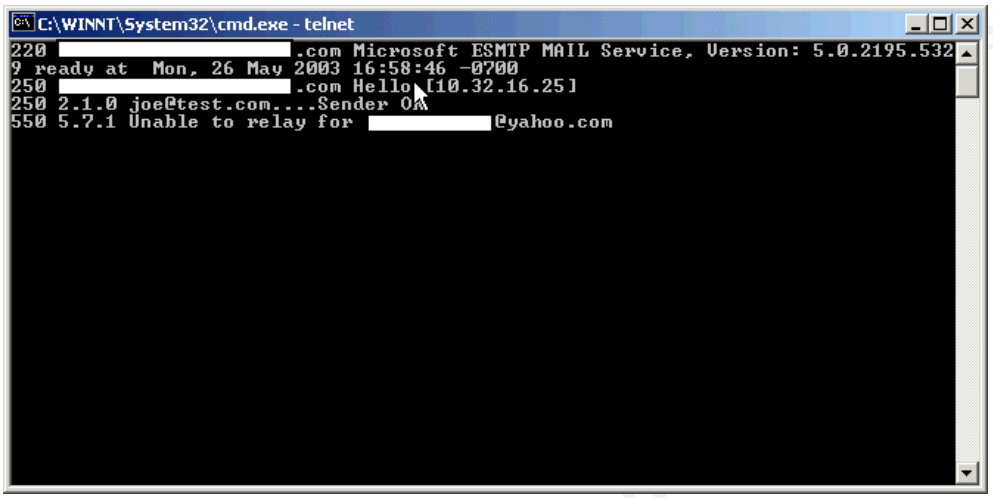
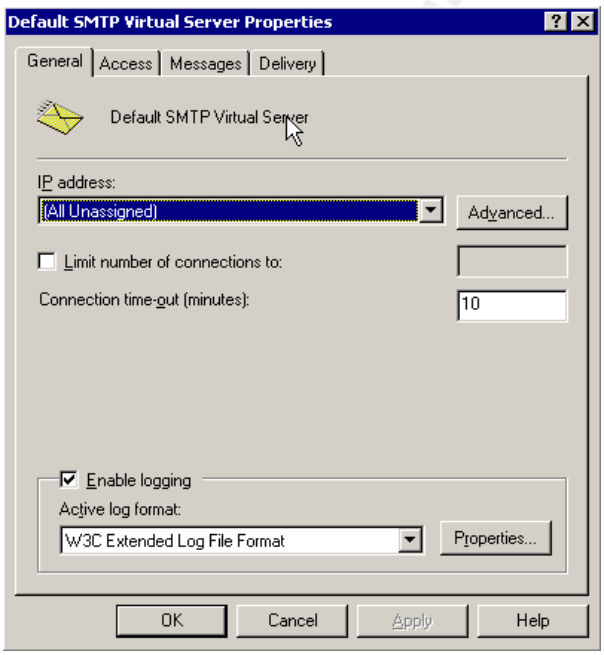


Figure 21

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.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 22

Note that SMTP is always in GMT.

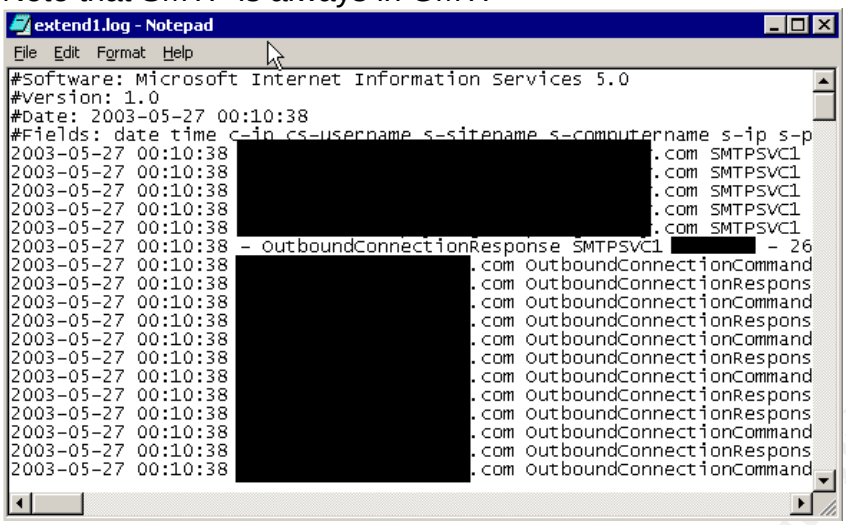


Figure 23

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).

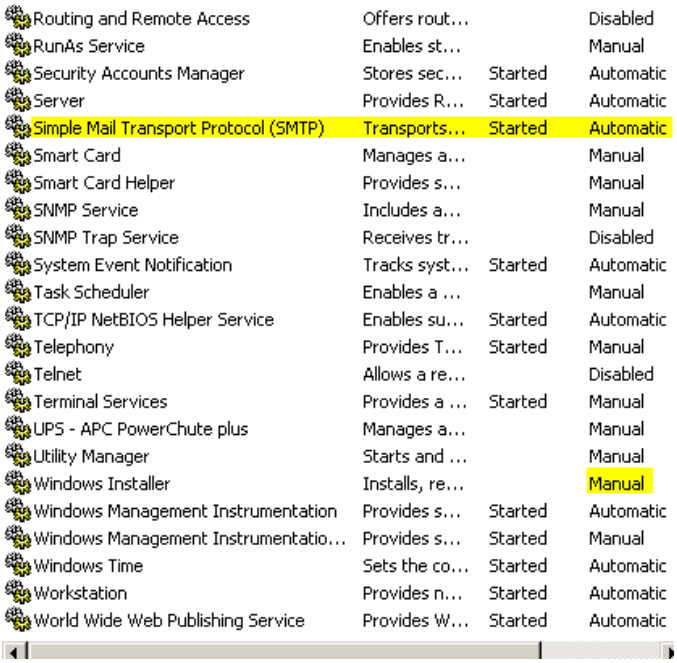
Front-End--FAIL

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Name	Description	Status	Startup Typ
Alerter	Notifies sel...		Manual
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
ClipBook	Supports C...		Manual
COM+ Event System	Provides a...	Started	Manual
Computer Browser	Maintains a...		Manual
DefWatch		Started	Automatic
DHCP Client	Manages n...		Disabled
Distributed File System	Manages lo...	Started	Automatic
Distributed Link Tracking Client	Sends notif...		Manual
Distributed Link Tracking Server	Stores info...		Manual
Distributed Transaction Coordinator	Coordinate...		Manual
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...	Started	Automatic
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			Disabled
Logical Disk 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
Net Logon	Supports p...	Started	Automatic
NetMeeting Remote Desktop Sharing	Allows aut...		Manual
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
Performance 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
QoS RSVP	Provides n...		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...	Started	Automatic

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



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

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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
Computer 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
Distributed 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
IPSEC Policy Agent	Manages I...	Started	Automatic
Kerberos Key Distribution Center	Generates ...		Disabled
License Logging Service	Tracks Clie...		Manual
Logical Disk Manager	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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Net Logon	Supports p...	Started	Automatic
NetMeeting Remote Desktop Sharing	Allows aut...		Manual
Network 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
PowerChute network shutdown		Started	Automatic
Print Spooler	Loads files ...	Started	Automatic
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	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 Helper	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

Figure 25

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 Exchsrvr

```
D:\Program Files>dir
 Volume in drive D has no label.
 Volume Serial Number is F457-9D56

 Directory of D:\Program Files

04/04/2003  01:53p      <DIR>          .
04/04/2003  01:53p      <DIR>          ..
08/31/2000  10:52a      <DIR>          Accessories
05/17/2001  04:57p      <DIR>          Common Files
08/31/2000  03:49p      <DIR>          ComPlus Applications
05/17/2003  08:14p      <DIR>          Exchsrvr
```

Figure 26

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

```
D:\>dir
 Volume in drive D has no label.
 Volume Serial Number is F457-9D56

 Directory of D:\

04/04/2003  02:10p      <DIR>          040503_Patches
05/17/2003  07:58p      <DIR>          051703_Patches
03/14/2002  10:50a      <DIR>          Documents and Set
05/17/2003  08:20p           5,406,288 Exchange Server S
05/21/2001  11:18a           1,932,412 Exchange Server S
09/14/2001  01:28p      <DIR>          Inetpub
03/02/2001  06:23p      <DIR>          intranet_log
09/14/2001  07:00p                2,346 mpextranet.cer
04/04/2003  01:53p      <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>          TEMP
05/24/2003  10:14p      <DIR>          WIN2K
```

Figure 27

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

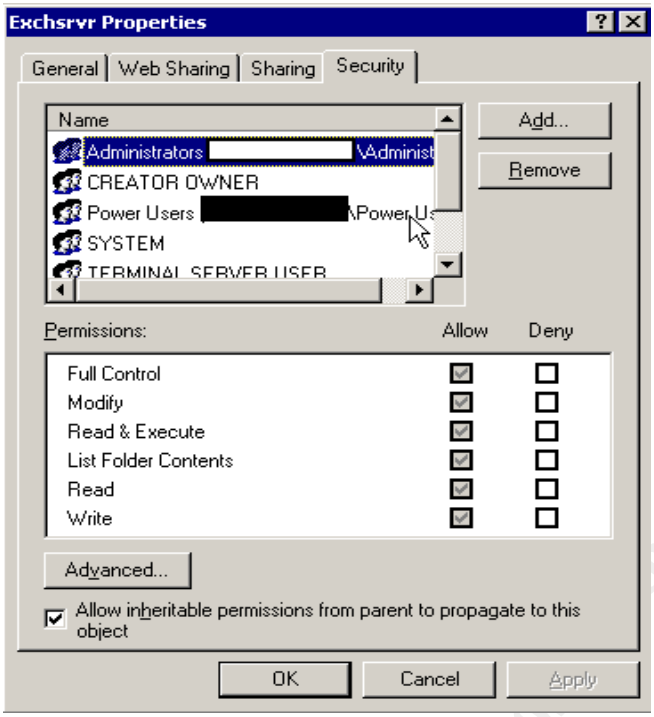


Figure 28

Back-End--FAIL

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

```
E:\Program Files>dir
 Volume in drive E is New Volume
 Volume Serial Number is 1C0F-3353

 Directory of E:\Program Files

08/04/2001  12:35a      <DIR>          .
08/04/2001  12:35a      <DIR>          ..
05/17/2003  08:20p      <DIR>          Exchsrvr
               0 File(s)              0 bytes
               3 Dir(s)  79,793,606,656 bytes free
```

Figure 29

```
05/17/2003  08:28p      <DIR>          WINNT
               5 File(s)      6,265,840 bytes
              19 Dir(s)   1,848,849,920 bytes free

C:\>cd winnt

C:\WINNT>_
```

Figure 30

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

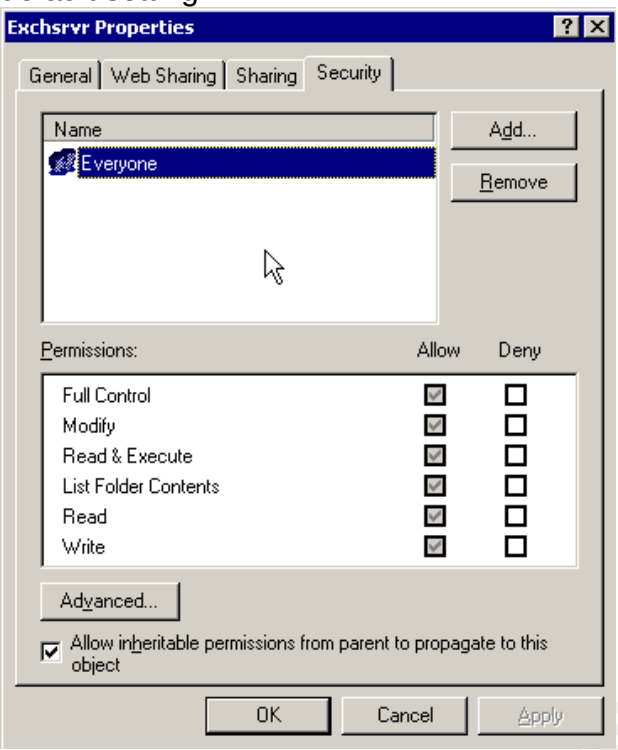


Figure 31

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

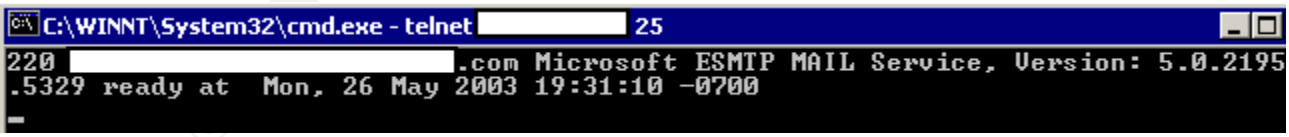


Figure 32

Back-End

Figure 33

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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.

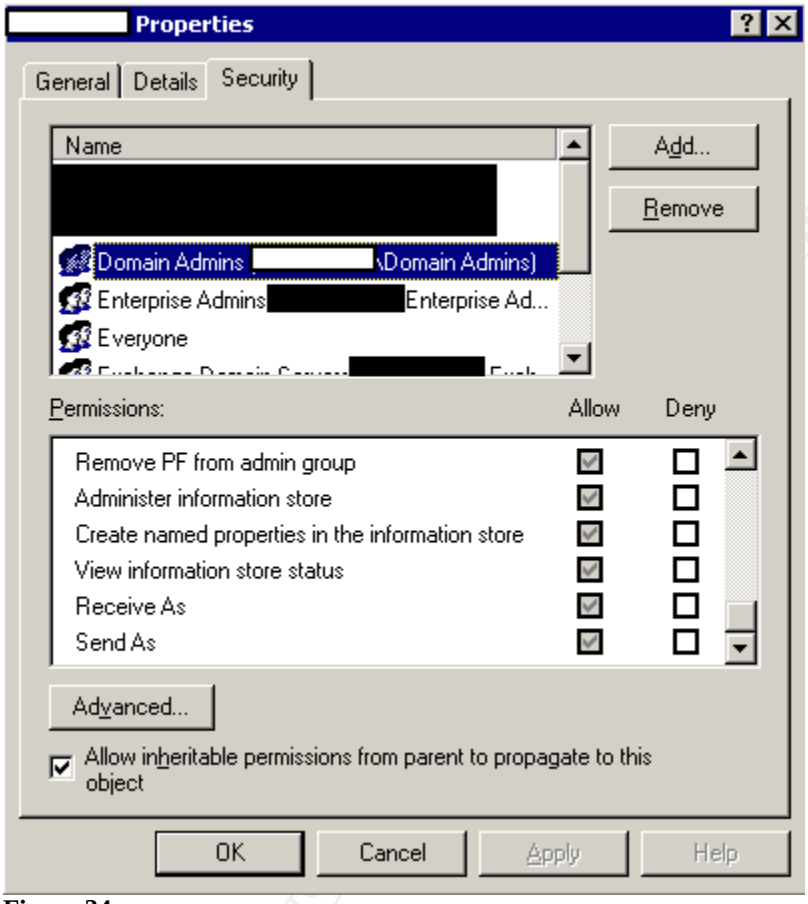


Figure 34

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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)[13][14]

- 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.

© SANS Institute 2003, Author retains full rights.

[13] Weber, 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: http://www.securityfocus.com/infocus/1578 (Mar 26, 2003).
[15] SANS Institute, Track 5 – Securing Windows, The SANS Institute, 2003.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

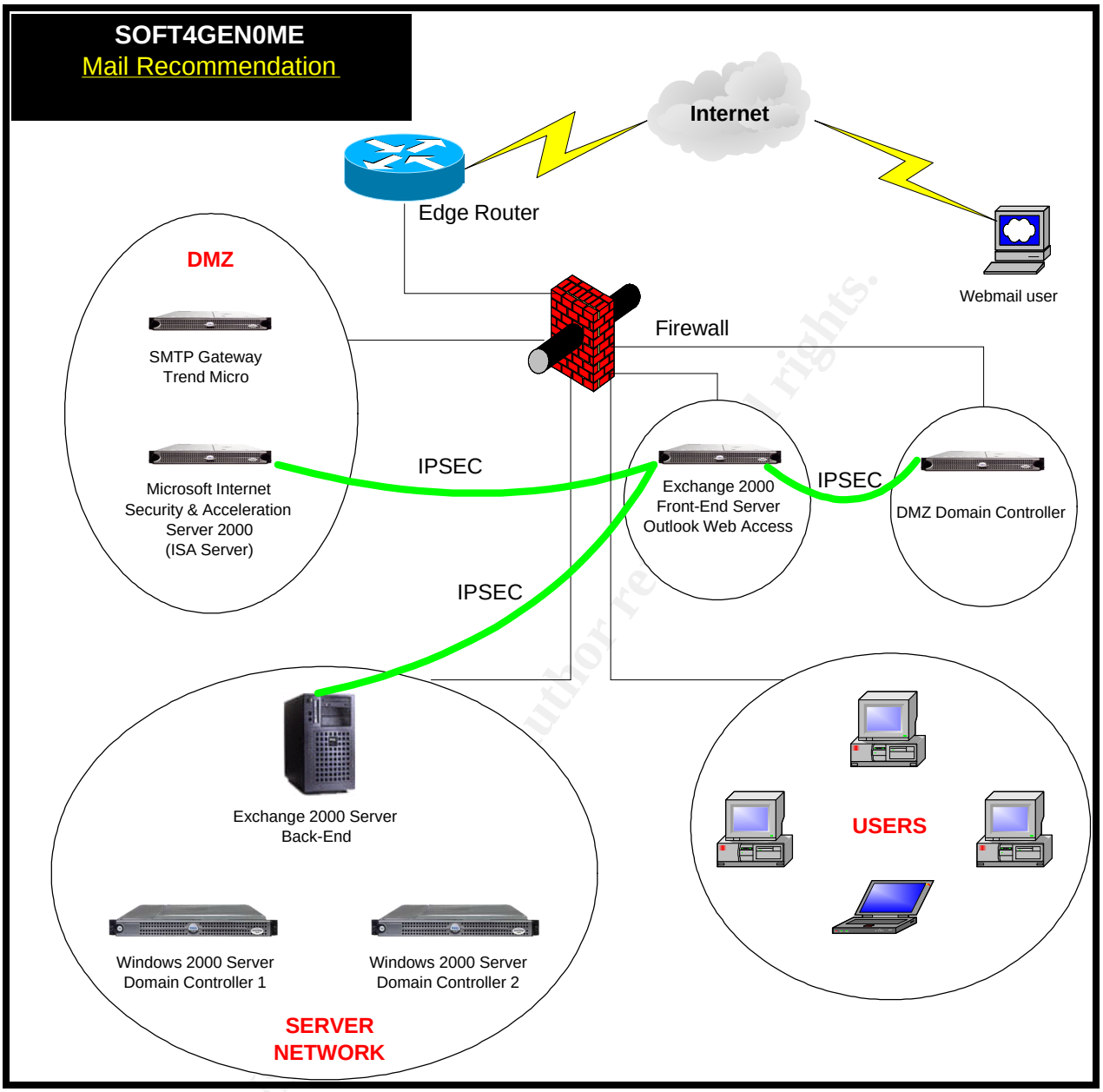


Figure 35

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 well-defined 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

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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: http://www.microsoft.com/technet/security/bulletin/MS03-011.asp (Jun 7, 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

System changes and further testing

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

Locate and execute Outlook icon on the desktop--**Negative**

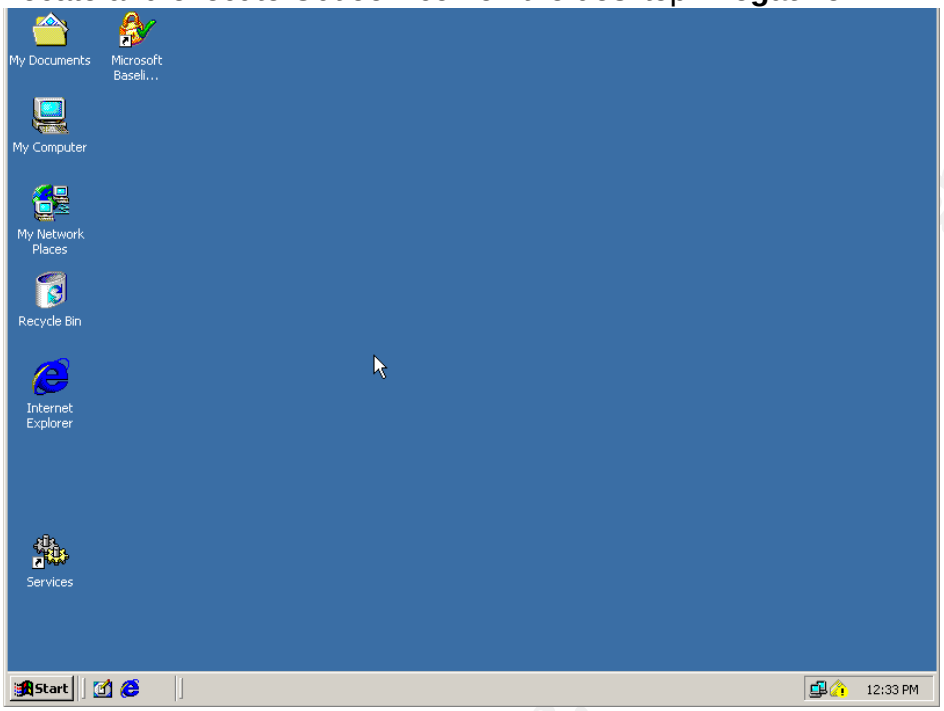


Figure 36

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

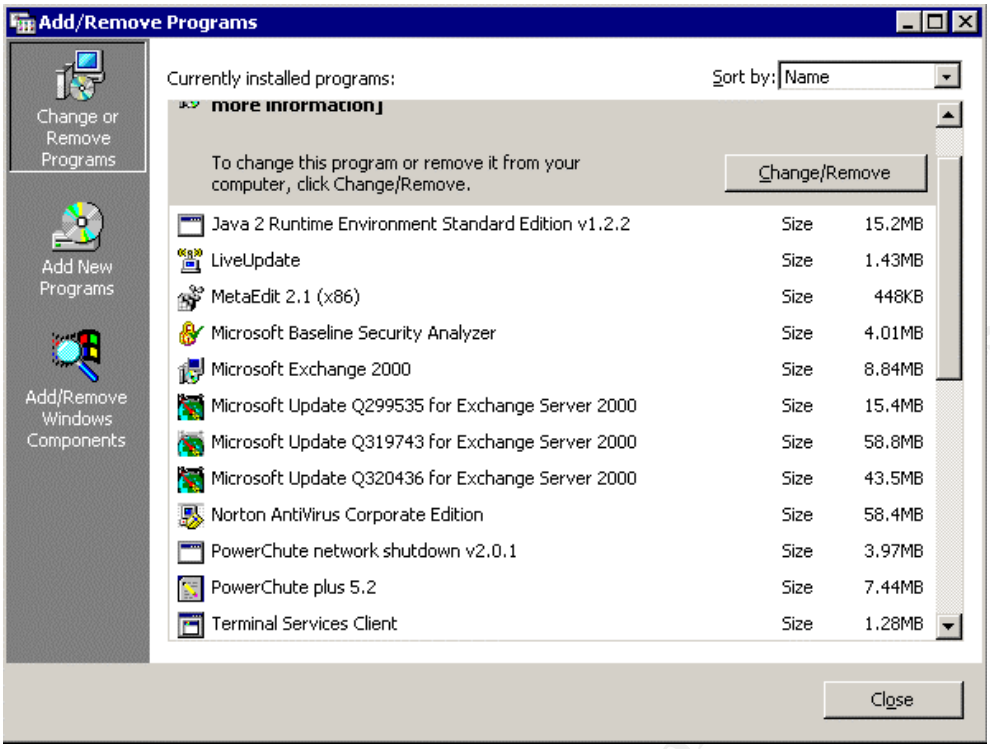


Figure 37

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

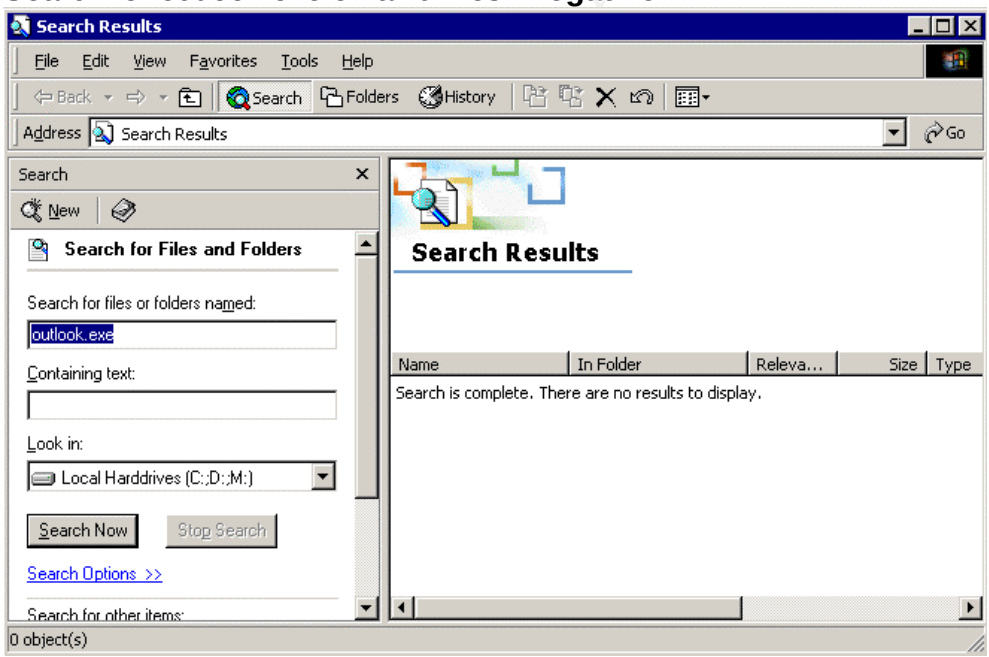


Figure 38

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Front-End Server

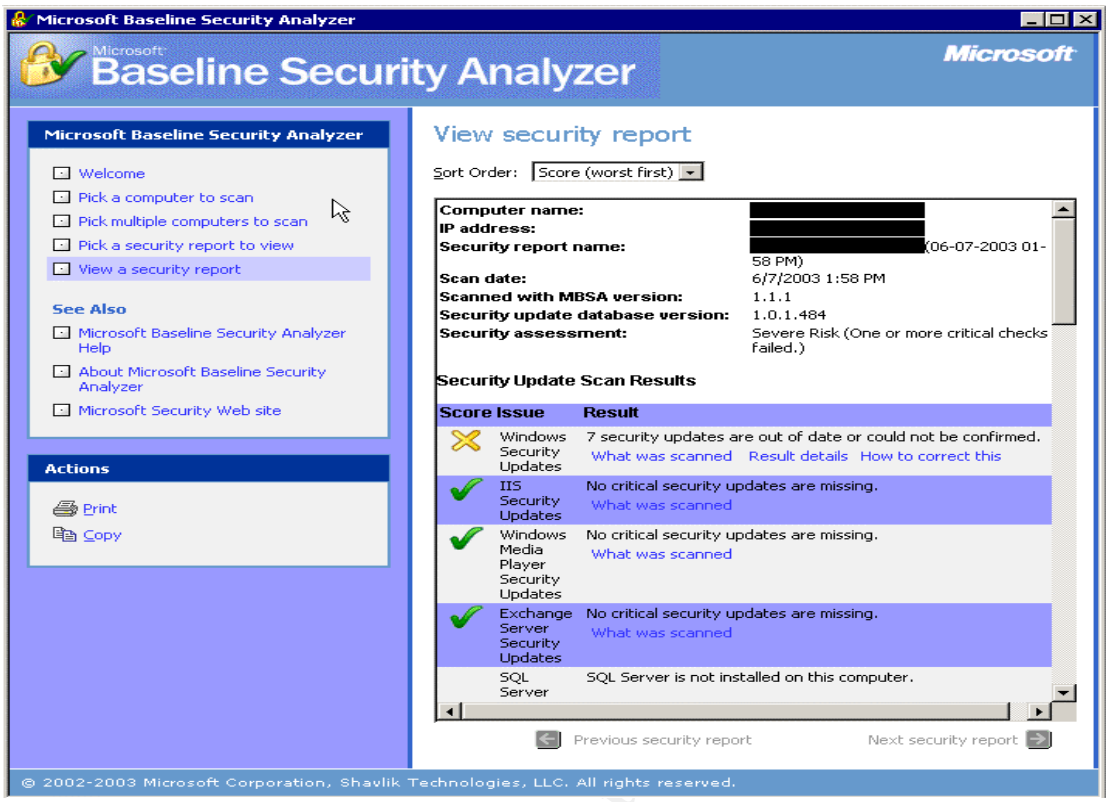


Figure 39

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, As part of GIAC practical repository. Author retains full rights.

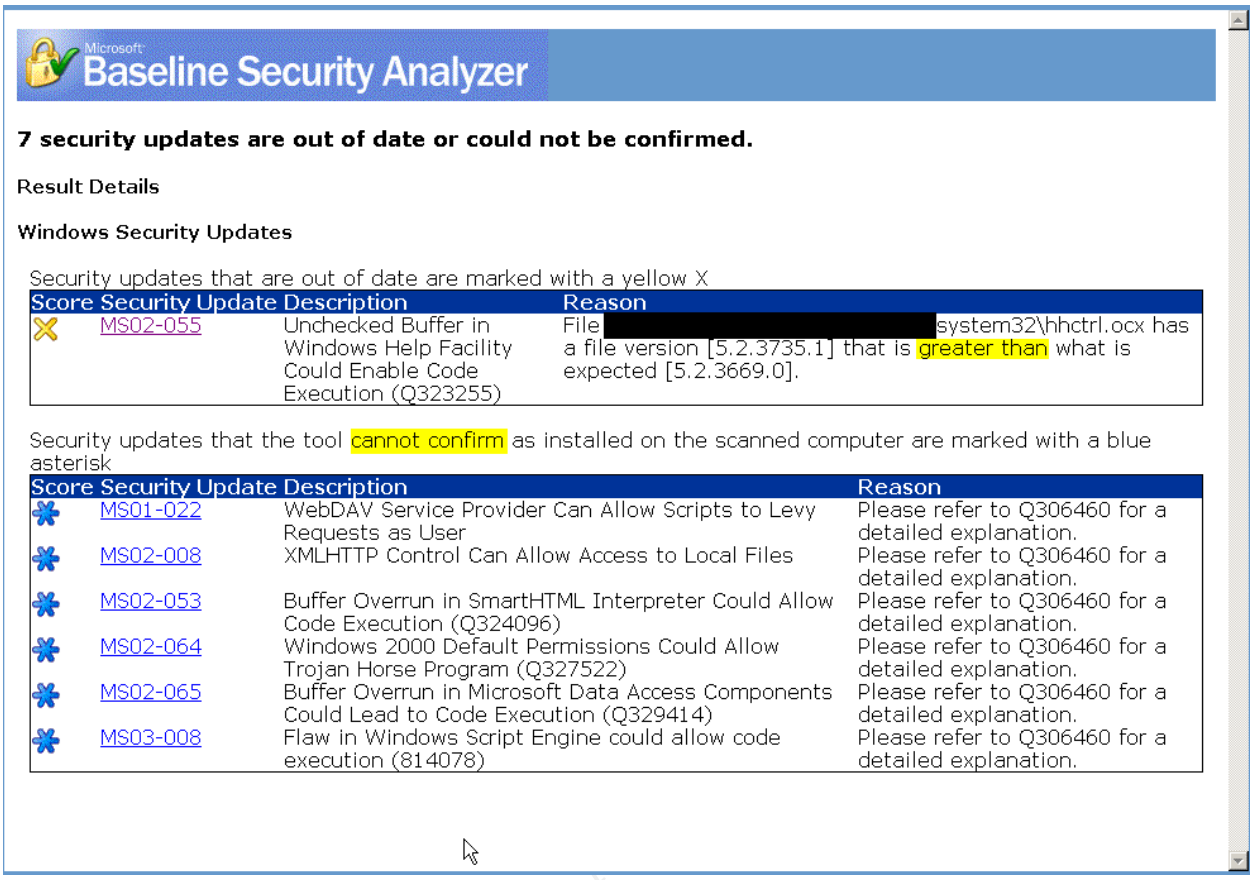


Figure 40

The drive was converted to NTFS as confirmed in the Windows Scan Results (figure 41) and in the Disk Management Properties (figure 42).

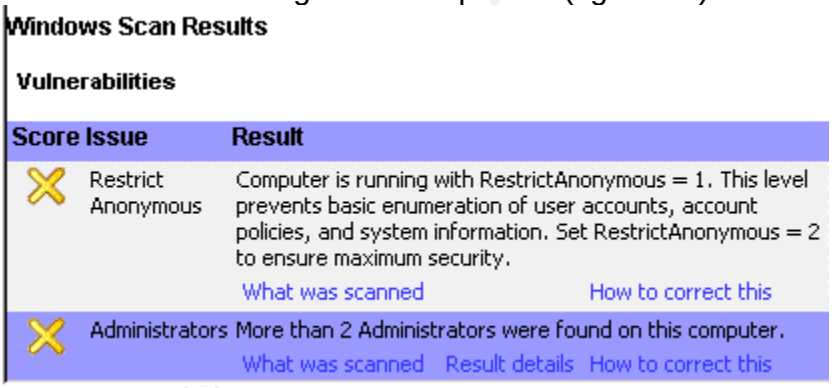


Figure 41

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

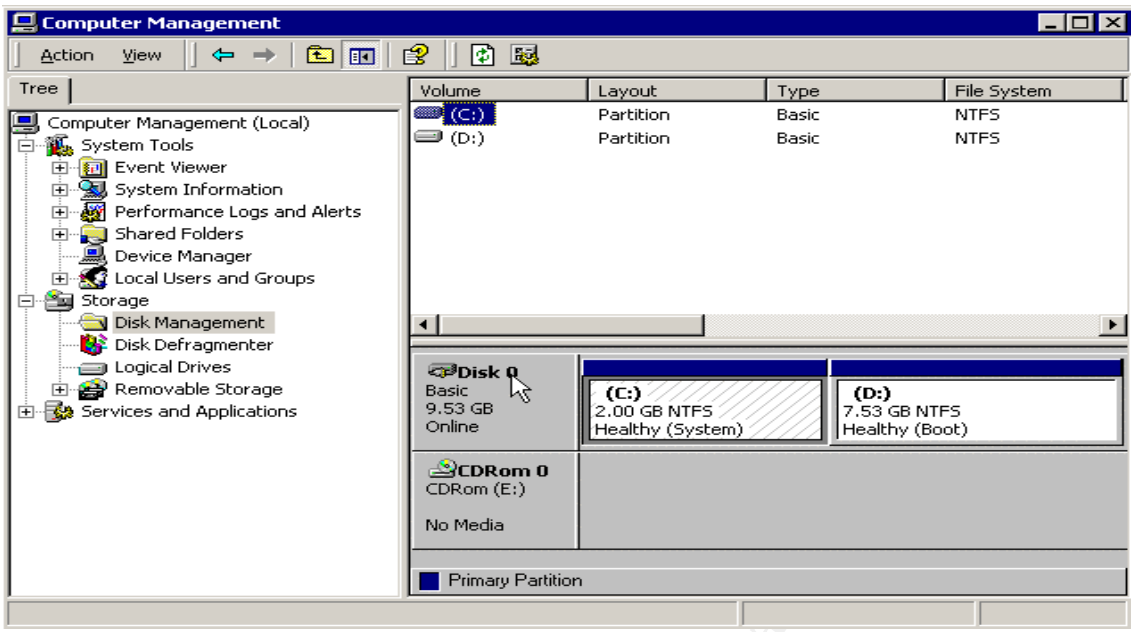


Figure 42

Back-End Server

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

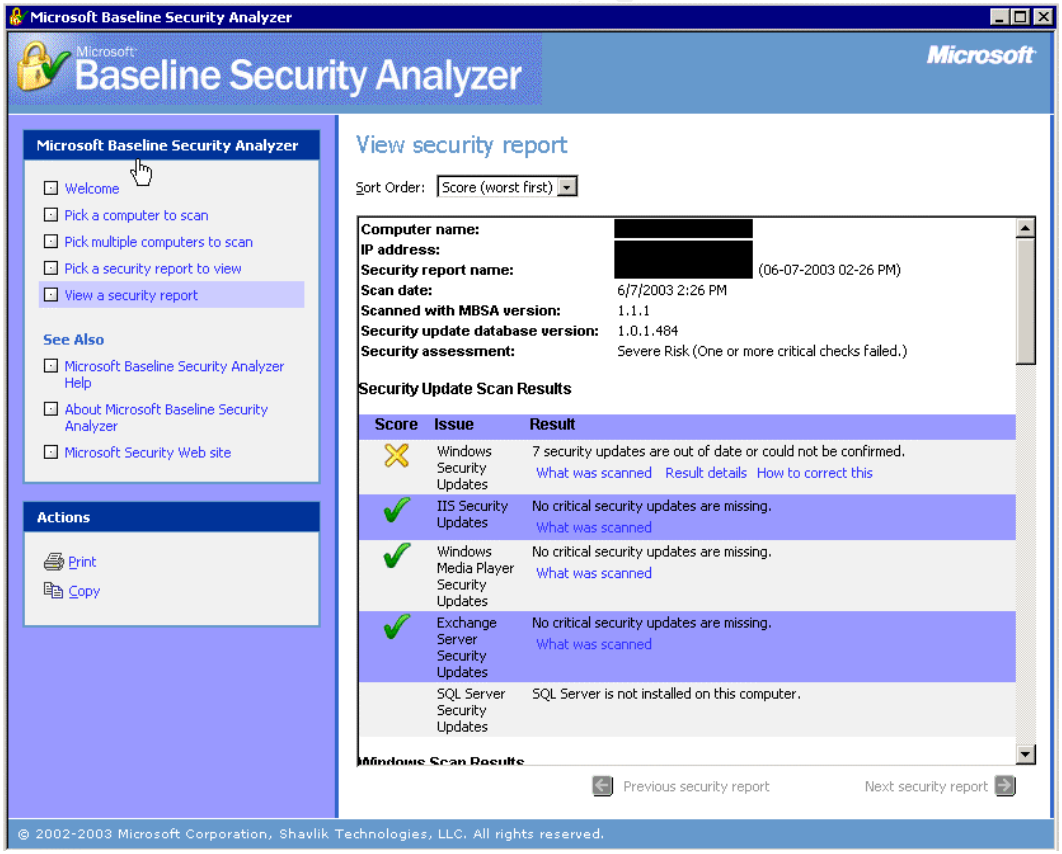


Figure 43

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

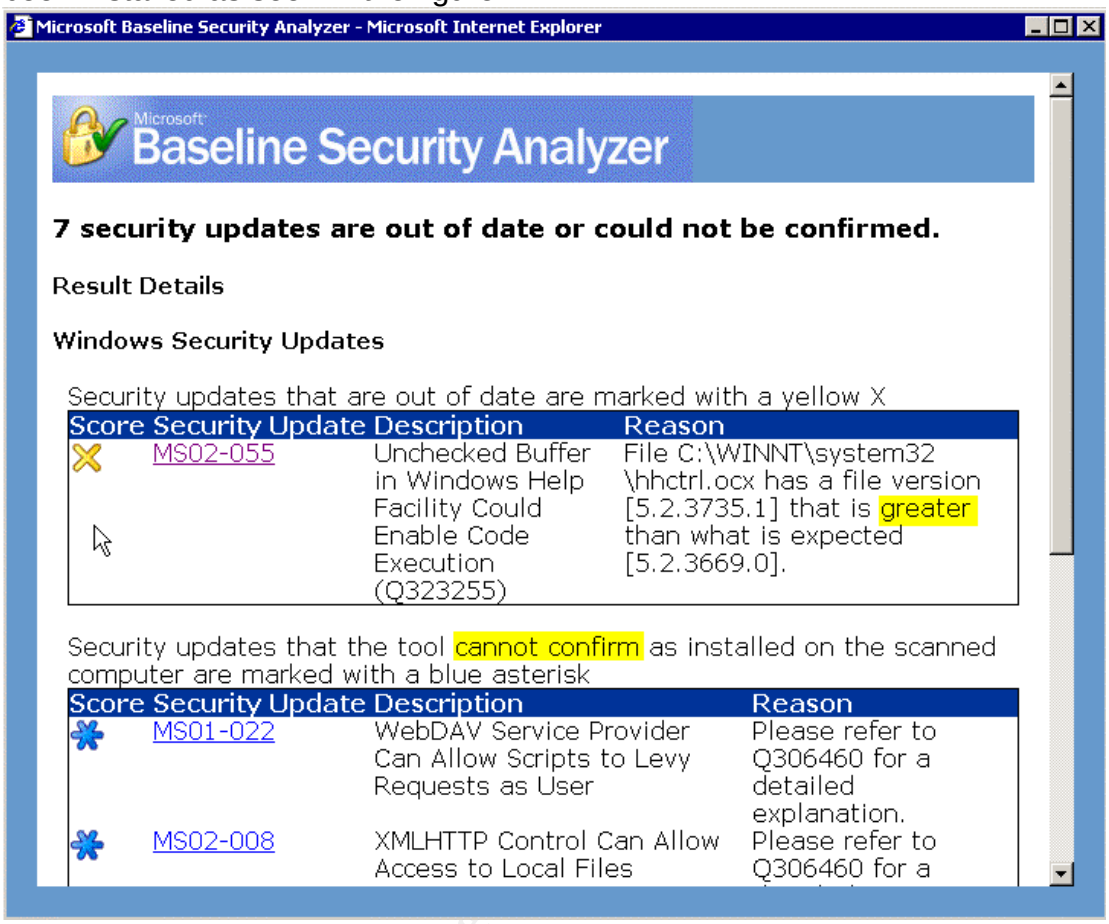


Figure 44

- #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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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
ClipBook	Supports C...		Manual
COM+ Event System	Provides a...	Started	Manual
Computer Browser	Maintains a...		Disabled
DefWatch		Started	Automatic
DHCP Client	Manages n...		Disabled
Distributed File System	Manages lo...		Disabled
Distributed Link Tracking Client	Sends notif...		Manual
Distributed Link Tracking Server	Stores info...		Manual
Distributed Transaction Coordinator	Coordinate...		Manual
DNS Client	Resolves a...	Started	Automatic
Event Log	Logs event...	Started	Automatic
Fax Service	Helps you ...		Manual
File Replication	Maintains fi...		Disabled
IIS Admin Service	Allows adm...	Paused	Disabled
Indexing Service	Indexes co...		Disabled
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			Disabled
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...		Disabled
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...		Disabled
Net Logon	Supports p...	Started	Automatic
NetMeeting Remote Desktop Sharing	Allows aut...		Manual
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
Performance Logs and Alerts	Configures...		Manual
Plug and Play	Manages d...	Started	Automatic
PowerChute network shutdown		Started	Automatic
Print Spooler	Loads files ...		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 ...		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

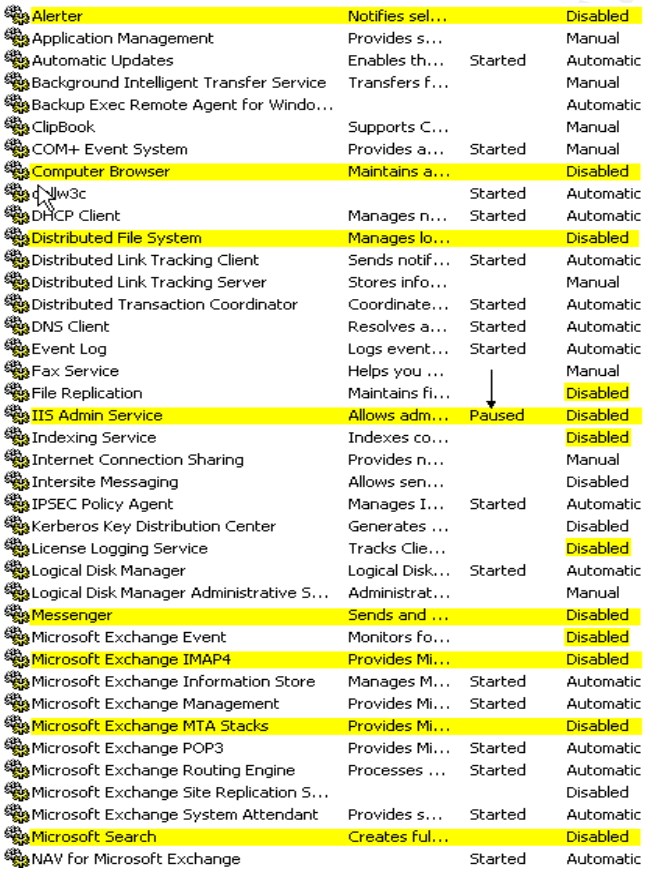
retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 that monitor 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	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
Iiw3c		Started	Automatic
DHCP Client	Manages n...	Started	Automatic
Distributed File 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 ...		Manual
File Replication	Maintains fi...		Disabled
IIS Admin Service	Allows adm...	Paused	Disabled
Indexing Service	Indexes co...		Disabled
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...		Disabled
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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Net Logon	Supports p...	Started	Automatic
NetMeeting Remote Desktop Sharing	Allows aut...		Manual
Network Connections	Manages o...	Started	Manual
Network DDE	Provides n...		Manual
Network DDE DSDM	Manages s...		Manual
Network News Transport Protocol (NN...	Transports...		Disabled
NT 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
Print Spooler	Loads files ...		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	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...		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
Simple Mail Transport Protocol (SMTP)	Transports...	Started	Automatic
Smart Card	Manages a...		Manual
Smart Card Helper	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...		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
Windows Time	Sets the co...	Started	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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

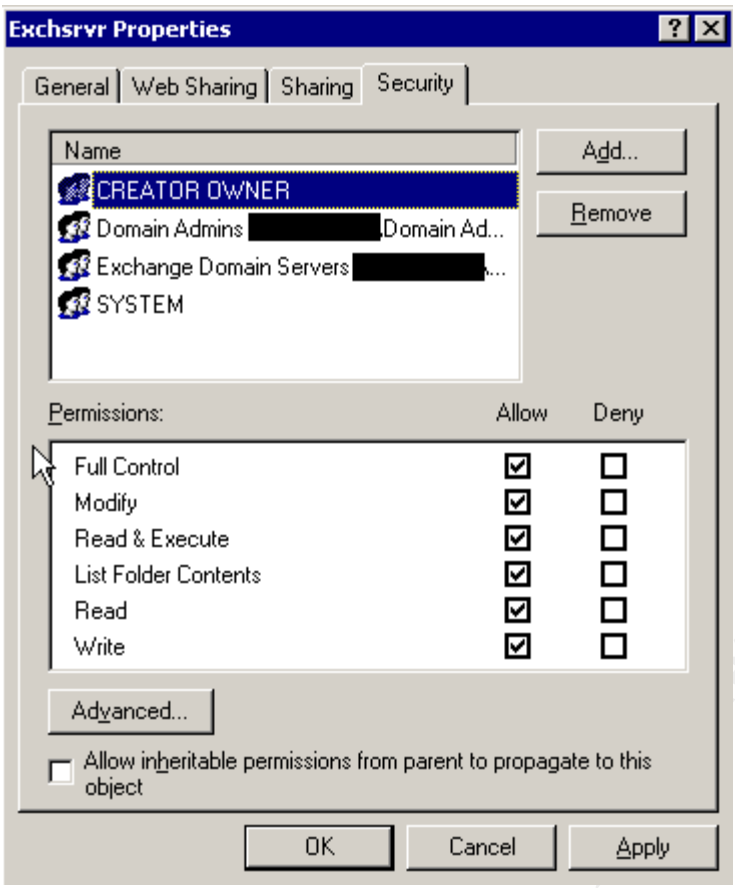


Figure 47

- #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.

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.

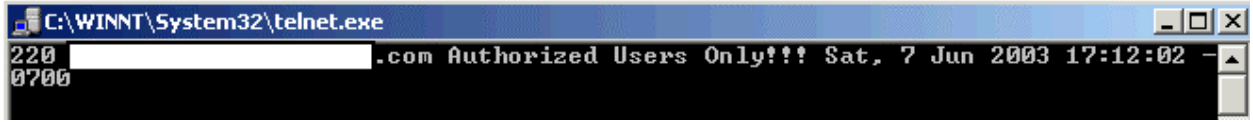


Figure 49

[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).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- #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.

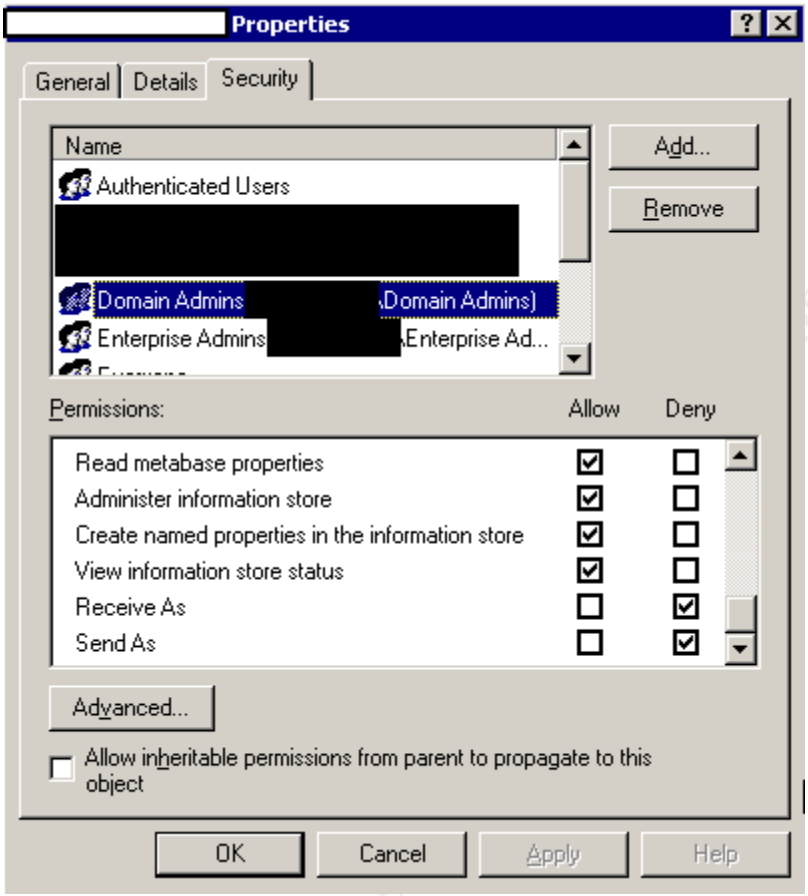


Figure 50

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

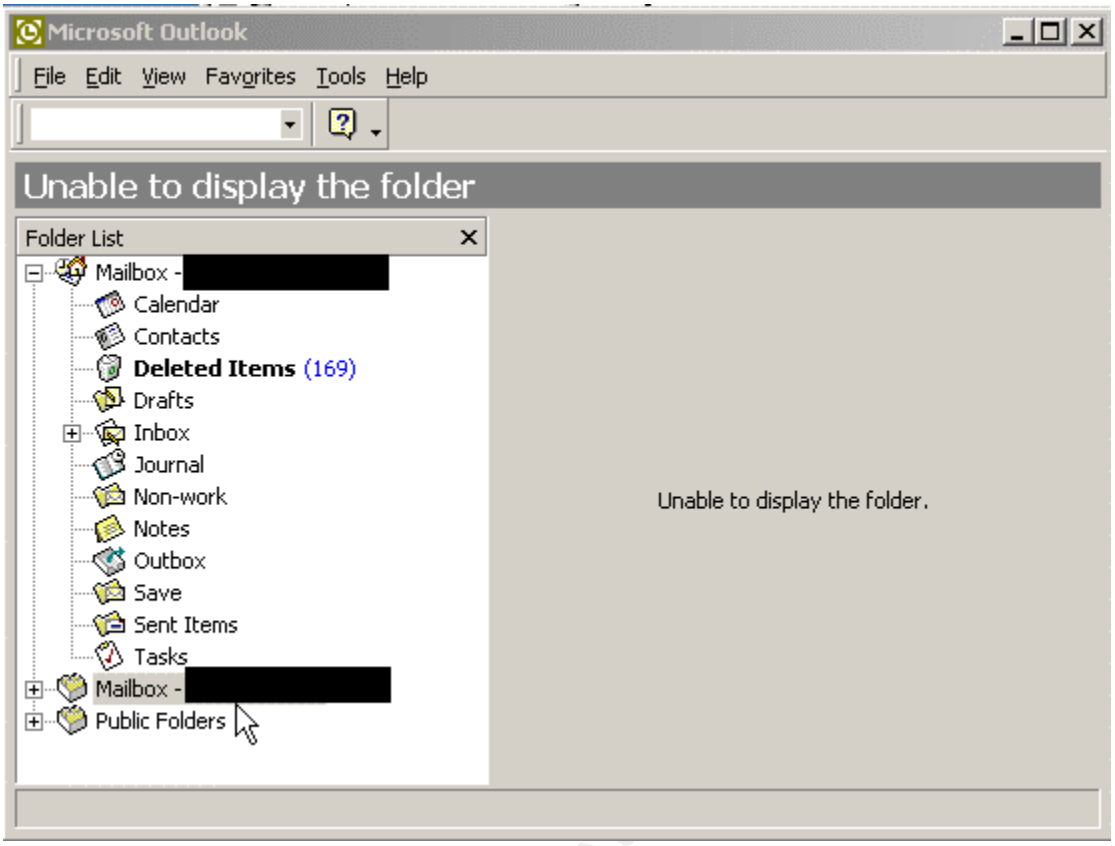


Figure 51

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

© SANS Institute 2003, Author retains full rights.

References

- Bayne, James, "An Overview of Threat and Risk Assessment," SANS Info Sec Reading Room, Jan 22, 2002. URL: http://www.sans.org/rr/audit/overview.php (Feb 26, 2003).
- Bois, Justin, "Protect Yourself," SANS Reading Room, Apr 4, 2002. URL: http://www.sans.org/rr/physical/protect.php (Apr 2, 2003).
- "Can I install Outlook on my Exchange server?," Mar 27, 2002. URL: http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=24446 (Apr 25, 2003).
- Cima, Susan. "Vulnerability Assessment," SANS Institute. Jul 6, 2001. URL: http://www.sans.org/rr/securitybasics/VA.php (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: http://www.sans.org/rr/email/sec_exchange.php (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: http://www.sans.org/webcasts/031803.php.
- GFI, "Protecting your network against email threats: How to block email attacks & viruses," http://www.gfi.com/mailsecurity/wpemailprotection.htm (Feb 26, 2003).
- Gurowicz, Marian B., "Secure eMail: Determining an Enterprise Strategy and Direction," Sep 16, 2002, URL: http://www.sans.org/rr/email/direction.php, (Feb 26, 2003).
- Hudgins-Bonafield, Christy, "Messaging Migration: It Pays To Do You Homework," Network Computing, Jun 15, 1998. URL: http://www.networkcomputing.com/911/911f1.html (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. Jim's Exchange 2000 Notes, FAQs, and Useful Information. Honolulu: Jim McBee, 2002.
- Microsoft, "Exchange 2000 Server Operations Guide," Microsoft Press, 2002. URL: http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/maintain/operate/opsguide/default.asp (May 26, 2003).
- Microsoft, "Exchange 2000 Server Planning and Installation, Chapter 13 – System Security." URL: http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/proddocs/ex2kplan/c13secur.asp (May 26, 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Microsoft, "Exchange 2000 Server Resource Kit, Chapter 30 – Security." URL: http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/reskit/resguide/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%3Ben-us%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/opsguide/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.asp (May 26, 2003).
- Microsoft, "Security Operations Guide for Microsoft Exchange 2000 Server," Microsoft Press, 2002. URL: http://www.microsoft.com/technet/security/prodtech/mailexch/opsguide/default.asp (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/trowae2k.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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Robichaux, Paul, Controlling SMTP Relaying with Microsoft Exchange, Microsoft Press, 2002. URL: http://www.microsoft.com/technet/security/prodtech/mailexch/opsguide/default.asp (May 26, 2003).
- Robichaux, Paul. Securing Messaging with Microsoft Exchange Server 2000. 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).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

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 banners identified by Internet Scanner.

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

Vulnerability Severity: H High M Medium A Low

Session Information

Session Name:		File Name:	
Policy:	W2K Scan Custom	Key:	
Hosts Scanned:	1	Hosts Active:	1
Scan Start:	5/26/2003 1:18:28AM	Scan End:	5/26/2003 1:38:46AM
Comment:	initial scan		

IP Address (DNS Name)	Operating System	Status
1.1.1.1 (BACK-END)	Windows NT	Reachable

Service Details:

Service Name	Short Description	Port #	Type
httpd	httpd	8080	TCP
https	https	443	TCP
imap	imap	143	TCP
imaps	imaps	993	TCP
microsoft-ds	Microsoft-DS	445	TCP
netbios-ssn	netbios-ssn	139	TCP
pop3	pop3	110	TCP
pop3s	pop3s	995	TCP
RPC	RPC	135	TCP
Smtp	Smtp	25	TCP
Unknown Service Port#26	Unknown Service Port#26	26	TCP
Unknown Service Port#593	Unknown Service Port#593	593	TCP
Unknown Service Port#691	Unknown Service Port#691	691	TCP
www-http	World Wide Web HTTP	80	TCP

User Details:

Account Name	Account Type	Comments
Guest	User	
XXXXX	User	
XXXXX	User	
XXXXX	User	
None	Group	
XXXXX	User	
XXXXX	User	
XXXXX	User	

Technician	1

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IP Address (DNS Name)	Operating System	Status

Banner Details

Banner Type	Banner Text
HTTPD	Microsoft-IIS/5.0

Others

Additional Information	More Information
IIS_version=5.0 IUSR_D24XB3G01 IWAM_D24XB3G01 Microsoft ESMTP MAIL Service, port=80	server=Microsoft-IIS/5.0 ====IisFrontpageInfo starts==== <html><head><title>vermeer RPC packet</title></head> <body> <p>method=open service:3.0.2.1105 <p>status= status=917505 ====IisFrontpageInfo ends====

XXXXX
XXXXX
XXXXX

IP Address (DNS Name)	Operating System	Status

Vulnerability Details:

Http TraceEnabled: HTTP TRACE is enabled

HTTP TRACE support is enabled on the Web server. The HTTP TRACE method as described in RFC 2516 of the HTTP 1.1 standard is typically used for debugging and network analysis purposes to request the contents of HTTP request messages received by the Web server. On Web servers with HTTP TRACE support enabled, a remote attacker could leverage this functionality with known cross-site scripting and other Web browser vulnerabilities to obtain sensitive information about the Web server, including server cookies and authentication information. This information could then be used by the attacker to launch further attacks against the affected Web server.

Remedy:
Administrators should disable HTTP TRACE support on the Web server. HTTP TRACE support can be disabled on Apache HTTP Server using the mod_rewrite module and on Microsoft Internet Information Services (IIS) using the URLScan tool.

IisFrontpageInfo: IIS with FrontPage information gathering (CAN-2000-0114)

Microsoft Windows NT4 running Internet Information Server with FrontPage Server Extensions 97 or 98 could reveal sensitive information to an attacker. A remote attacker could make specific HTTP requests to the server that would reveal the name of the anonymous Internet account and physical paths on the affected system.

Remedy:
Download and install the patches in the order listed in the "Microsoft FrontPage Server Extensions 2002 for Windows" document. See References.

As a workaround, if you do not require the functionality provided by FrontPage Server Extensions, remove all the files associated with FrontPage Server Extensions.

IisWebdavRunning: Microsoft IIS WebDAV service is running on the system

Web Distributed Authoring and Versioning (WebDAV) extends the HTTP/1.1 protocol to allow clients to publish, lock, and manage resources on the Web.

Remedy:
Verify that Microsoft webdav Service is running on the system for legitimate reasons. If use of webdav is required, ensure that security settings had been configured or patches had been applied for best security practices. If use of webdav is not required or if it was enabled under suspicious circumstances, disable it from the system.

IIS administrators may temporarily disable WebDAV support on IIS 5 servers if possible. Microsoft Knowledge Base Article 241520 describes the process in detail. See References.

MsLocatorRunning: Microsoft Locator service is running on the system

The Microsoft Locator service is a name service that maps logical names to network-specific names. It ships with Windows NT4.0, Windows 2000, and Windows XP. By default, the Locator service is enabled only on Windows 2000 domain controllers and Windows NT4.0 domain controllers; it is not enabled on Windows NT4.0 workstations or member servers, Windows 2000 workstations or member servers, or Windows XP.

Remedy:
Verify that Microsoft Locator Service is running on the system for legitimate reasons. If use of locator is required, ensure that security settings had been configured or patches had been applied for best security practices. If use of Locator is not required or if it was enabled under suspicious circumstances, disable it from the system.

registry - null session: Registry opened through a null session

The registry was accessed through a null session. Information may be obtained that compromises the security of the system.

Remedy:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IP Address (DNS Name)	Operating System	Status

Apply the latest Windows NT 4.0 Service Pack (SP3 or later), available from the Windows NT Service Packs Web page. See References.

--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 Editor at your own risk. Any change made with Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems caused by the use of Registry Editor can be solved.

1. If you have not already done so, apply the latest Windows NT 4.0 Service Pack (SP3 or later).
2. Open Registry Editor. From the Windows NT Start menu, select Run, type regedt32, and click OK.
3. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA.
4. From the Edit menu, select Add Value to display the Add Value dialog box.
5. In the Value Name field, type RestrictAnonymous.
6. Select REG_DWORD as the Data Type.
7. Click OK to display the DWORD Editor.
8. In the Data field, type 1. (Ignore the Radix setting.)
9. Click OK. Registry Editor adds the key to the registry.

Ehlo Check: SMTP daemon supports EHLO (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 known 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 allow you 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 mail server (if applicable), or switch to a mail server that allows EHLO to be disabled. Consult your mail server documentation or contact your vendor for information on whether it is possible to modify your mail server configuration to disable EHLO.

Guest Exists: Guest account name exists

The Guest account is named "Guest." If your security policy requires that the guest account be renamed, then this name should be changed. Be aware, however, that an attacker can easily determine which account is the guest 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:
1. Open User Manager. (From the Windows NT Start menu, select Programs, Administrative Tools (Common), User Manager.)
2. Select the Guest account.
3. From the User menu, 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 Groups Management Console (lusrmgr.msc).
2. Double-click on the Users folder.
3. Right-click on user Object of interest.
4. Select Rename to change the username.
5. Type in new username and click on OK to save the setting.

Technician	4

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IP Address {DNS Name}	Operating System	Status

IcmpTstamp: 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.

IisRunning: 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.

Local User: Windows local user on workstation
Vuln 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.