# Auditing Exchange 2000 server
# With Outlook Web access
# An Auditor's perspective

Alexander Pickar

16th February 2004

## Abstract

This document describes audit results of Exchange 2000 Back-end server with Outlook Web Access Front-end server providing company's communication and collaboration services. It describes tests of the operating system, IIS and Exchange system. The document is divided into four parts, first identifies the audited system, second contains descriptions of current state of practice and checklist used for the audit, third part contains audit evidence and the fourth part presents audit findings and recommendations.

ABSTRACT 1

RESEARCH IN AUDIT, MEASUREMENT PRACTICE AND CONTROL 5

DESCRIPTION OF THE AUDITED SYSTEM 5
ORGANIZATION'S SECURITY POLICY 6
AUDIT OBJECTIVE 6
RISK EVALUATION 6
PHYSICAL AND ENVIRONMENTAL RISKS 6
NETWORK ACCESS RISKS 6
OPERATING SYSTEM RISKS 7
APPLICATION RISKS 7
ADMINISTRATIVE RISKS 7
CURRENT STATE OF PRACTICE 7
ON-LINE RESOURCES 8

AUDITING CHECKLIST 10

PHYSICAL SECURITY 10
OPERATING SYSTEM SECURITY 11
IIS SECURITY 15
EXCHANGE SERVER SECURITY 19
NETWORK SECURITY 22
MANAGEMENT SECURITY 23

AUDIT EVIDENCE 24

PHY1 – CHECK PHYSICAL ACCESS TO EQUIPMENT ROOM 24
PHY2 – CHECK PHYSICAL ACCESS TO EQUIPMENT 24
PHY3 – CHECK EQUIPMENT ENVIRONMENTAL CONDITIONS 24
PHY4 – CHECK BACKUPS STORAGE 24
NET1 – CHECK FIREWALL OWA RULES 24
NET2 – CHECK FIREWALL EXCHANGE RULES 24
MGMT1 – CHECK SYSTEM BACKUP PROCEDURES 24
MGMT2 – CHECK LOGS REVIEW POLICY 24
EXCHANGE BACK-END SERVER 25
OS1 – CHECK NTFS DISK FORMAT 25
OS2 – CHECK LATEST SERVICE PACK AND SECURITY HOTFIXES 25
OS3 – CHECK UNNECESSARY ACCOUNTS PRESENCE 27
OS4 – CHECK ACCOUNT PASSWORD POLICY 28
OS5 – CHECK RUNNING AND DISABLED SERVICES 29
OS6 – CHECK ANONYMOUS LOGON PROBLEMS 31
OS7 – CHECK OS LOGGING 31
OS8 – RUN AN OUTSIDE NETWORK VULNERABILITY SCAN 32
IIS1 – CHECK IIS LOCKDOWN TOOL IMPLEMENTATION 37
IIS2 – CHECK URLSCAN INSTALLATION 38
IIS3 – CHECK IIS VIRTUAL DIRECTORIES ACLS 38
IIS4 – CHECK IIS LOG FILES ACL 38

IIS5 – Check IIS Sample application presence 39
IIS6 – Check IIS IISADMPWD directory presence 39
IIS7 – Check IIS ISAPI extension mappings 39
IIS8 – Check IIS logging 40
EXCH1 – Check latest Exchange 2000 Service pack and hotfixes 41
EXCH2 – Check running and disabled Exchange 2000 services 42
EXCH3 – Check Mailbox size limits 43
EXCH4 – Check Exchange directory location and access rights 43
EXCH5 – Check antivirus software 45
EXCH6 – Check Exchange logfile permissions 45
EXCH7 – Check if SMTP banner has been changed 46
**Exchange Front-end server (OWA) 47**
OS1 – Check NTFS disk format 47
OS2 – Check latest Service pack and security hotfixes 48
OS3 – Check unnecessary accounts presence 50
OS4 – Check account password policy 50
OS5 – Check running and disabled services 51
OS6 – Check Anonymous Logon problems 53
OS7 – CHECK OS logging 54
OS8 – Run an outside network vulnerability scan 55
IIS1 – Check IIS Lockdown tool implementation 65
IIS2 – Check URLScan installation 66
IIS3 – Check IIS virtual directories ACLs 67
IIS4 – Check IIS Log files ACL 68
IIS5 – Check IIS Sample application presence 69
IIS6 – Check IIS IISADMPWD directory presence 70
IIS7 – Check IIS ISAPI extension mappings 71
IIS8 – Check IIS logging 72
EXCH1 – Check latest Exchange 2000 Service pack and hotfixes 73
EXCH2 – Check running and disabled Exchange 2000 services 74
EXCH3 – Check Mailbox size limits – Not Applicable 74
EXCH4 – Check Exchange directory location– Not Applicable 74
EXCH5 – Check antivirus software 74
EXCH6 – Check Exchange logfile permissions – Not Applicable 75
EXCH7 – Check if SMTP banner has been changed – Not Applicable 75
EXCH8 – Check that no local Exchange data reside on OWA server 75
EXCH9 – Check adequate OWA user authentication 76

**AUDIT REPORT – FINDINGS AND RECOMMENDATIONS 78**

**System Operation and Management 78**
Finding – There is no Company security and operational policy 78
Finding – Logs are not reviewed on a regular basis 78
**Exchange Back-end server 79**
Finding – missing patches 79
Finding – Weak account password policy 79
Finding – unnecessary services 80
Finding – Operating system logging is not set up 80
Finding – SMTP Vulnerability on Exchange Back-end server 81
Finding – EXCHRVR directory is readable by Everyone 81
Finding – Exchange server is running on a Domain controller 82
Finding – SMTP banner not changed 82
**Exchange Front-end server 82**
Finding – missing patches 82

FINDING – WEAK ACCOUNT PASSWORD POLICY 83
FINDING – UNNECESSARY SERVICES 83
FINDING – ANONYMOUS LOGON ACCESS NOT RESTRICTED 84
FINDING – OPERATING SYSTEM LOGGING IS NOT SET UP 84
FINDING – IIS SAMPLE APPLICATION AND IISADMPWD DIRECTORIES ARE PRESENT 85
FINDING – URLSCAN.INI IS NOT SET UP ACCORDING TO THE RECOMMENDATIONS 85
FINDING – SOME IIS ISAPI MAPPINGS ARE NOT UNMAPPED 87
FINDING – SOME EXCHANGE SERVICES ARE NOT NECESSARY 88
FINDING – OWA SSL ACCESS DOESN'T REQUIRE 128 BIT ENCRYPTION 88

**AUDIT REPORT – EXECUTIVE SUMMARY 89**

**REFERENCES 90**

## Research in Audit, Measurement practice and Control

### *Description of the audited system*

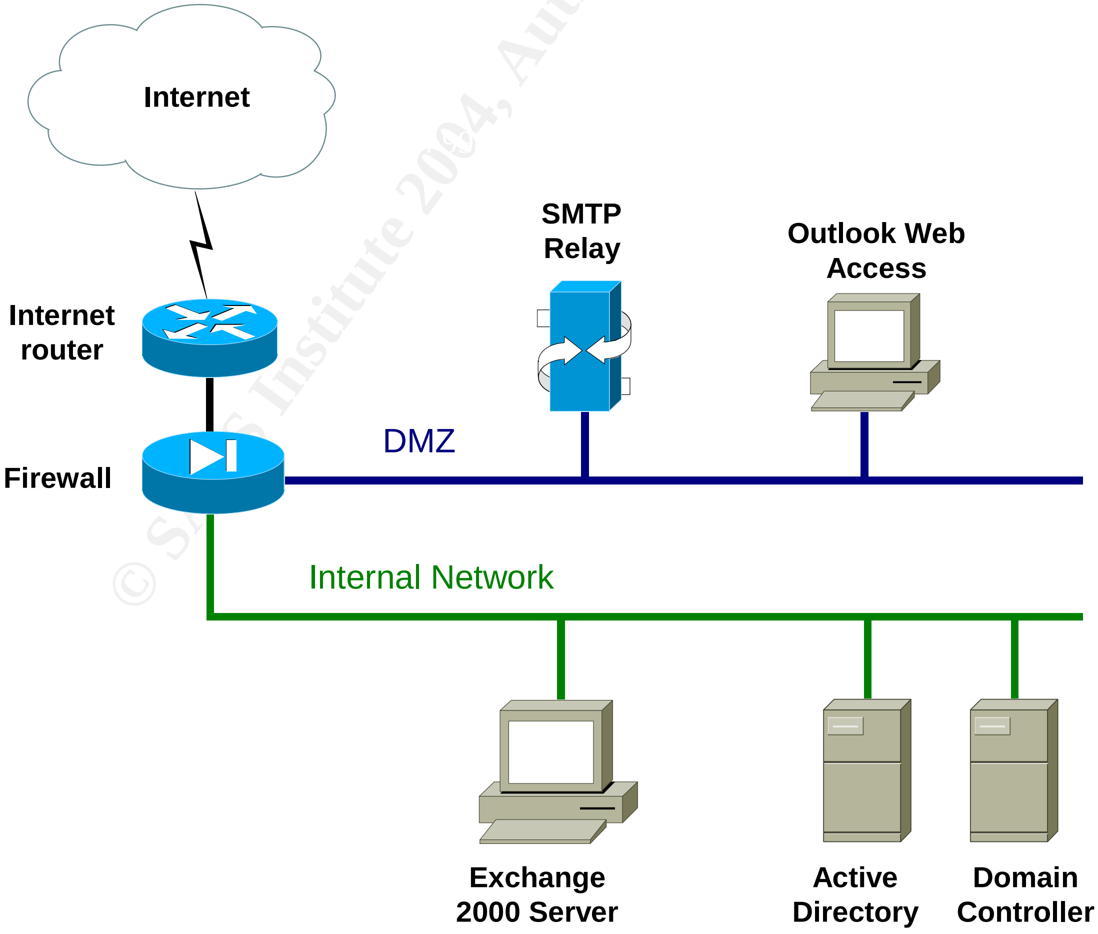
The audited system being reviewed is an internal Microsoft Exchange 2000 system complemented by Outlook Web Access located in a secured DMZ.

The company uses Microsoft Exchange 2000 as it's main communication and collaboration system. Outlook Web Access is used to allow remote users and telecommuters to access corporate mail system and enterprise information from any location using a Web browser.

The company has a dedicated Internet connection. Internal network is secured by a firewall with three interfaces – external, internal and DMZ. All mail traffic from Internet is sent to the internal Exchange 2000 server using an SMTP relay agent running on a Linux machine. The SMTP relay agent is located in the company's DMZ.

Outlook Web Access is located in the company DMZ. It connects to the internal Exchange server using Front-end Back-end topology and allows access to the user's mail boxes and shared documents from the Internet.
Outlook Web Access publishes information available on the internal Exchange server. Users are authenticated through the Active directory.

Figure 1 – Network Topology



## *Organization's Security policy*

The audited company doesn't have any written policy regarding installation and / or service of Exchange server infrastructure. Audit interviews showed that there are only weak informal security and operational policies. Hence the audit couldn't compare the Exchange server infrastructure conformance against internal policies and procedures.

Policies help the company to implement, operate and protect their systems. They define a set of rules, roles and areas of responsibility for system operation, management and disaster recovery, conditions of information use, etc. Policies provides also guidelines how to handle various situations and decisions concerning purchasing of new equipment, data restoration or security incident handling.

## *Audit objective*

The audit focuses on the Exchange 2000 Front-end server with Outlook Web Access Back-end server. It targets operating system security of the servers, IIS installation, Exchange server security and firewall rules determining access to and from the audited servers.
Audit of the SMTP relay agent, e-mail clients and the firewall itself are out of scope of the audit. Audit of the active directory, another essential part, not only of the Exchange 2000 server, is also out of this audit objective.

## *Risk evaluation*

Audit of Exchange server architecture is a complex task involving operating system, IIS, active directory, domain controllers, firewalls and different clients used by the users. Exchange system depends on all of these components. Each of them represents a possible security threats and therefore needs to be audited.

### Physical and environmental risks

Physical security is fundamental to every system operation and security. If an unauthorized person gains physical access to the Exchange equipment, he could much more easily obtain inappropriate access or conduct Denial of service. Therefore the equipment should be located in a well secured place with controlled access. All access to restricted areas should be logged.
Another part of physical risks involves proper operating electrical and environmental conditions, which are necessary for high availability and continuous service of the system.

### Network access risks

To minimize risks concerning the unauthorized network access to the Exchange subsystem, the underlying network infrastructure must assure well controlled and secured communication. Firewalls should have strict policies allowing only necessary traffic passing from the Internet to the DMZ and from DMZ to the internal network. Mail system function should be divided among SMTP mail relay, OWA acting only as Exchange Front-end server and an internal Exchange server. Application layer inspection should be implemented on the Firewall to mitigate risk of well known and new vulnerabilities in the SMTP and HTTP / HTTPS protocols involved in e-mail communication.

### Operating system risks

Both internal Exchange 2000 server and Outlook Web access rely on underlying Windows 2000 server operating system. Secure operating system is a fundamental pre-requisite for any upper layer applications. Exchange 2000 Front-end Back-end topology requires also a secure and properly configured IIS server for it's operation. IIS is considered to be one of the top 20 internet security threats and its securing is one of the most important things to assure safe operation. Major operating system and IIS threats are unauthorized use, denial-of-service attacks and the improper configuration or maintenance of the system.

### Application risks

Mail system is exposed to various application layer threats. E-mails can contain viruses, Trojan horses or other malicious code. Spam e-mails are becoming another application problem of today. Sending large e-mail messages can lead to Denial of Service attacks. Also improper access rights to shared folders can lead to information theft or misuse of sensitive company data. Antivirus software and spam counter measurements are important to minimize application threats.

### Administrative risks

Also proper configuration and maintenance, administrative policies and procedures are critical to assure secure and reliable operation of the Exchange 2000 system. Backup and restore procedures are also very important for failure recovery after a technical or security issue.
User training can prevent accidental security issues after opening e-mails with malicious code or viruses etc.
Risks linked to administration are loose of data through bad backup procedures, overseeing or loss of suspicious and malicious activity and of course common operational problems that could be detected by careful logging analysis.

## *Current state of practice*

There are many on-line resources and books concerning Windows 2000 operating system security, used as a foundation for the Microsoft Exchange 2000 server, and also resources concerning IIS 5 used in conjunction with Outlook Web Access. Many of them include also audit checklists.

On the Internet, there are also many documents concerning installation, securing and operating the Microsoft Exchange 2000 server. Most of them mention also settings concerning the Outlook Web Access security.  Unfortunately most of them don't include Exchange 2000 specific security checklists.

Because of this state I decided to make a checklist divided into the corresponding parts verifying Operating system, IIS, Exchange security and also management tasks.

## On-line resources

First to mention among on-line resources are the **Microsoft web pages** which contain many valuable information about planning, deployment and also security setup of Exchange 2000 server.

The main page for technical information can be found here:
http://www.microsoft.com/exchange/techinfo/2000.asp
These pages contain links to documents concerning planning, development, deployment and administration of Exchange 2000 system.

Informations regarding recommended service packs, security updates and fixes for the servers running Exchange 2000 can be found on the following pages:
http://www.microsoft.com/exchange/techinfo/security/bestconfig.asp

Links to security documents concerning Exchange 2000 can be found on the following page:
http://www.microsoft.com/exchange/techinfo/security/2000.asp

Security Operations Guide for Exchange 2000 Server is a document describing steps necessary for a secure Exchange 2000 environment installation and operation. I found this document most useful since it contains the IIS / Exchange environment and security settings including directory access-rights, URLScan settings etc.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/opsguide/default.asp

Microsoft has also published Windows 2000 Server Baseline Security Checklist, which can be used as a good background for making a security checklist or for an audit of operating system used by the Exchange 2000 server.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp

Microsoft IIS 5.0 Baseline Security Checklist concerns basic IIS 5 settings
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp

**National Security Agency** has published freely accessible Windows 2000 Security Recommendation Guides, including also Guide to the Secure Configuration and Administration of Microsoft Exchange 2000.
http://www.nsa.gov/snac/win2k/download.htm

Especially the guide number 21, named “Guide to the Secure Configuration and Administration of Microsoft Exchange 2000“ contains detailed informations about Exchange 2000 installation, operation and security.
http://www.nsa.gov/snac/win2k/guides/w2k-21.pdf

**GIAC.ORG** site has many student practicals concerning Exchange 2000 security in the GSNA (audit), GSEC (Security essential) and GCWN (Windows Security Administrator) sections:
http://www.giac.org/cert.php

**SANS Reading room** also contains valuable informations concerning the topics. I have found very usefull their description of Null sessions in NT/2000 environment and also articles about Exchange 2000 security.
http://www.sans.org/rr/

**SecurityFocus** has published some articles concerning Exchange 2000 scenarios, topology and security, especially in the articles published in the "infocus" section.
http://www.securityfocus.com/

A complete list of on-line references used in this audit can be found at the end of the document.

## Auditing Checklist

In the following section there is a checklist used for auditing of the Exchange 2000 system. The checklist is divided into six parts corresponding to the areas of audit. Each check is divided into following sections with following meaning :

| | |
|---|---|
| ID | Unique test identification |
| Objective | Description of the check |
| Reference | Reference for the particular test |
| Risk | Points out possible implications |
| Test | Describes what and how should be verified |
| Compliance | Describes a test evidence of a compliant system |
| O/S | Describes objectivity or subjectivity of the test |

### *Physical security*

| | |
|---|---|
| ID | PHY1 |
| Objective | Verify physical access to rooms with server and network equipment |
| Reference | Personal Experience |
| Risk | If an unauthorized person gains physical access to the Exchange equipment, he could easily conduct Denial of service or obtain inappropriate access. |
| Test | Review physical location of the corresponding equipment (data center) and check if appropriate controlled access was implemented.<br>Review up-to-date list of authorized persons and evidence of entry into the secured area. |
| Compliance | Physical access to rooms is compliant if<br>- All relevant servers and other equipment are located in a locked room<br>- Only authorized employees or other persons under authorized supervision can access the room.<br>- Appropriate access controls are in place and must be used for entering the room.<br>- An up-to-date list of authorized persons must exist.<br>- Monitoring of access to the secured area must be implemented and shown to the auditor. |
| O/S | Objective |

| | |
|---|---|
| ID | PHY2 |
| Objective | Verify physical access to the equipment including console, drives, input / output ports |
| Reference | Personal Experience |
| Risk | If an unauthorized person gains physical access to the Exchange equipment, he could easily conduct Denial of service or obtain inappropriate access. |
| Test | Verify if each rack containing Exchange servers and network equipment – switches, firewalls, routers – is physically locked and all power and network and other cabling is routed through the bottom of the rack |
| Compliance | - Adequate controls / locks must be in place for every equipment involved in the system.<br>- Cabling must be routed securely. |
| O/S | Objective |

| | |
|---|---|
| ID | PHY3 |
| Objective | Verify Environmental conditions of the equipment |
| Reference | Personal Experience |
| Risk | Damage of the equipment and loss of functionality could happen if working environmental conditions were not assured.<br>Power interruptions could lead to system unavailability or damage of the equipment. |
| Test | Verify that appropriate air-condition, fire detection system are in place.<br>Verify that all equipment has power connection from the UPS. Check documentation proving that UPS power system is being verified on a regular basis. |
| Compliance | - Data center must have required air-condition, fire detection system and monitoring of temperature, humidity and other environmental variables.<br>- All systems must have power from UPS system.<br>- Documentation proving that UPS power system is being verified on a regular basis must exist and be verified by a responsible person<br>- All systems must have power from UPS system.<br>- Documentation proving that UPS power system is being verified on a regular basis must exist and be verified by a responsible person |
| O/S | Objective |

| | |
|---|---|
| ID | PHY4 |
| Objective | Verify that Backups are stored safely |
| Reference | Personal Experience |
| Risk | Backups of Exchange System can contain a copy of valuable data – corporate e-mails, contacts or documents within the public folders. They can be target for an attacker. On the other hand, Backups are the only resource for recovery after a hard system crash. |
| Test | Review Exchange 2000 backup procedures.<br>Verify that backups of Exchange system are stored off-site and on a place with controlled access. |
| Compliance | - System must be backed up regulary<br>- Backups must be stored in a safe place with controlled access |
| O/S | Objective |

## *Operating System security*

| | |
|---|---|
| ID | OS1 |
| Objective | Verify that all disk partitions are formatted with NTFS |
| Reference | Windows 2000 Server Baseline Security Checklist |
| Risk | FAT or FAT32 file systems do not support the use of file and directory level permissions, auditing and encryption. Only NTFS File format provides reasonable security. |
| Test | Check system's disk configuration information through the Computer Management MMC: Go to "*Start / Programs / Administrative Tools / Computer Management*"; under "*Storage*" highlight "*Disk Management*". |

| | |
|---|---|
| Compliance | - All partitions must be NTFS formatted. |
| O/S | Objective |

| | |
|---|---|
| ID | OS2 |
| Objective | Verify latest service pack and appropriate post-Service Pack security hotfixes |
| Reference | Windows 2000 Server Baseline Security Checklist |
| Risk | Unpatched servers represent a major threat to the system security, which can lead to misuse of the target system by an attacker, lower immunity to various viruses and Trojan horse programs or incompliance with current and future OS enhancements. |
| Test | Microsoft Baseline Security Analyzer (MBSA) evaluates system's configurations, lists and recommends missing updates and hotfixes.<br>Download MBSA and run it on the audited server. Look for the *"Security Update Scan Results"* section and review the scan results.<br>MBSA download page:<br>http://www.microsoft.com/technet/security/tools/mbsahome.asp. |
| Compliance | - Latest service pack for the operating system ( currently SP4 ) must be installed<br>- All appropriate post-Service Pack security hotfixes must be installed |
| O/S | Objective |

| | |
|---|---|
| ID | OS3 |
| Objective | Disable or delete unnecessary, unused or obsolete accounts |
| Reference | Windows 2000 Server Baseline Security Checklist |
| Risk | Unnecessary, unused or obsolete user accounts can help an attacker to gain unauthorized access to audited systems through brute-force password and other attacks. |
| Test | In the MBSA report, review the *"Windows Scan Results"* section.<br>Review especially these sections:<br>- *"Administrators"*<br>- *"Guest Account"* |
| Compliance | - Only necessary accounts can be present<br>- Guest account must be disabled |
| O/S | Objective |

| | |
|---|---|
| ID | OS4 |
| Objective | Verify user password policy |
| Reference | Windows 2000 Server Baseline Security Checklist |
| Risk | Weak passwords and password change policy make the system more vulnerable to password guessing or brute-force attacks leading to unauthorized use of the system. |
| Test | Open "*Start / Programs / Administrative tools / Local Security Policy*". Under "*Account Policies*" verify password settings. |
| Compliance | Compliant if password policy fulfills following criteria:<br>- Minimum password length 8 characters<br>- Maximum password age 90 days or less<br>- Password history at least 5 passwords<br>- Account lockout duration 30 minutes<br>- Account lockout duration 5 attempts |

| | |
|---|---|
| | - Meet password complexity |
| O/S | Objective |

| | |
|---|---|
| ID | OS5 |
| Objective | Check running and disabled services |
| Reference | Windows 2000 Server Baseline Security Checklist<br>Microsoft Security Operations Guide for Exchange 2000 Server – chapter 3 |
| Risk | Services not necessary for Exchange server operation may contain vulnerabilities which give a possible attacker more possibilities to compromise the system. |
| Test | Open "*Start / Programs / Administrative tools / Services*".<br>Deny any unnecessary services. Verify especially, if following services are running and really needed on the audited systems:<br>*Alerter*<br>*ClipBook*<br>*Computer Browser*<br>*DHCP Client*<br>*Distributed File System*<br>*File Replication*<br>*Fax Services*<br>*Indexing Service ( OWA server only )*<br>*License Logging Service*<br>*Messenger*<br>*NetMeeting Remote Desktop Sharing*<br>*Network News Transport Protocol*<br>*Print Spooler*<br>*Remote Registry Service*<br>*Removable Storage*<br>*Routing and Remote Access*<br>*Simple Mail Transport Protocol ( OWA server )*<br>*SNMP Service*<br>*Telnet*<br>*Windows Installer* |
| Compliance | - System is compliant if unnecessary services are disabled on the audited servers |
| O/S | Objective |

| | |
|---|---|
| ID | OS6 |
| Objective | Check Anonymous Logon problems |
| Reference | Windows 2000 Server Baseline Security Checklist;<br>SANS organization – NULL Sessions in NT/2000<br>http://support.microsoft.com/default.aspx?scid=kb;EN-US;q246261 |
| Risk | Anonymous users can list certain types of system information, including user names and details, account policies, and share names. |
| Test | Run MBSA and check the "*Restrict Anonymous*" section for the corresponding MBSA vulnerability scan result<br>On the the registry key:<br>„*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA*". |

| | |
|---|---|
| | Check the "*RestrictAnonymous*" value |
| Compliance | - OWA server is compliant if “*RestrictAnonymous*” is not equal to 0.<br>- Exchange Back-end server should have the “*RestrictAnonymous*” value equal to 0 (See Microsoft document Securing Exchange 2000 Servers Based on Role, Table 3.2 - Security Option on Domain Controllers to Support Exchange 2000). |
| O/S | Objective |

| | |
|---|---|
| ID | OS7 |
| Objective | Verify OS logging |
| Reference | Windows 2000 Server Baseline Security Checklist |
| Risk | Logging monitors user activity on the Windows 2000 server. Logging is an important step to prevent and track unauthorized user activity. |
| Test | Open “*Start / Programs / Administrative tools / Local Security Policy*”. Under “*Local Policies / Audit Policy*” check logging settings. |
| Compliance | - Following settings must be used:<br>System events – success and failure<br>Privilege use – failure<br>Policy change – success and failure<br>Object access – failure<br>Logon events – success and failure (OWA)<br>failure (Exchange Back-end server)<br>Account management – success and failure<br>Account login – success and failure (OWA),<br>failure (Exchange Back-end server) |
| O/S | Objective |

| | |
|---|---|
| ID | OS8 |
| Objective | Run a network vulnerability scan |
| Reference | Personal Experience |
| Risk | Running Nessus or another 3rd party Vulnerability scanner like for example Eeye Retina security scanner can reveal some overseen vulnerabilities |
| Test | Ask for permissions and notice the system administrator about network vulnerability scanning before running the vulnerability scan !<br>Conduct a network vulnerability scan on the audited systems using Nessus using all appropriate plugins including Denial-of-Service.<br>Review vulnerability listings from the Nessus report. Check all of the found vulnerabilities, eliminating possible false positive messages.<br>Nessus can be downloaded from following web site:<br>http://www.nessus.org/ |
| Compliance | - No relevant High-severity vulnerabilities should be found on the audited server<br>- Only Medium-severity vulnerabilities with medium or low risk factor should be found on the audited server |
| O/S | Objective |

### IIS Security

| | |
|---|---|
| ID | IIS1 |
| Objective | Verify that IIS Lockdown tool has been implemented |
| Reference | IIS 5.0 Baseline Security Checklist<br>Microsoft Knowledge Base Article - Q309508 - IIS Lockdown and URLscan Configurations in an Exchange Environment |
| Risk | IIS Lockdown tool automatically performs many steps needed for a more secure IIS environment, like for example removing sample application or ISAPI application mappings, that a less keen administrator might oversee. |
| Test | Run MBSA and look for "*IIS Lockdown tool*" test results in the "*Internet Information Services (IIS) Scan Results"* section. |
| Compliance | - IIS Lockdown tool must have been run on the audited system with IIS installed |
| O/S | Objective |

| | |
|---|---|
| ID | IIS2 |
| Objective | Verify IIS URLScan.dll ISAPI filter installation |
| Reference | IIS 5.0 Baseline Security Checklist<br>Microsoft Knowledge Base Article - Q309508 - IIS Lockdown and URLscan Configurations in an Exchange Environment |
| Risk | URLScan.dll is a Microsoft tool that checks all incoming URL requests based on rules found in the URLScan.ini file. This mitigates a risk that an attacker constructs a malformed URL request which would allow him to execute arbitrary code on the target machine. |
| Test | Check the UrlScan.ini file installed by the IIS Lockdown tool.<br>URLScan.ini is typically located in the following directory:<br>*%systemroot%\ System32\Inetsrv\Urlscan* |
| Compliance | - Compliant system must have UrlScan.ini file configuration compliant with the company requirements.<br><br>The URLscan configuration file for OWA proposed by Microsoft Knowledge Base Article Q30950:<br><br>`[Options]`<br>`UseAllowVerbs=1`<br>`UseAllowExtensions=0`<br>`NormalizeUrlBeforeScan=1`<br>`VerifyNormalization=1`<br>`AllowHighBitCharacters=1`<br>`AllowDotInPath=1`<br>`RemoveServerHeader=0`<br>`EnableLogging=1`<br>`PerProcessLogging=0`<br>`AllowLateScanning=0`<br><br>`[AllowVerbs]`<br>`GET`<br>`POST`<br>`SEARCH`<br>`POLL`<br>`PROPFIND`<br>`BMOVE` |

| | |
|---|---|
| | BCOPY<br>SUBSCRIBE<br>MOVE<br>PROPPATCH<br>BPROPPATCH<br>DELETE<br>BDELETE<br>MKCOL<br><br>[DenyVerbs]<br><br>[DenyHeaders]<br>If:<br>Lock-Token:<br><br>[DenyExtensions]<br>.asp<br>.cer<br>.cdx<br>.asa<br>.exe<br>.bat<br>.cmd<br>.com<br>.htw<br>.ida<br>.idq<br>.htr<br>.idc<br>.shtm<br>.shtml<br>.stm<br>.printer<br>.ini<br>.log<br>.pol<br>.dat<br><br>[DenyUrlSequences]<br>..<br>./<br>\<br>%<br>& |
| O/S | Objective |

| | |
|---|---|
| ID | IIS3 |
| Objective | Set appropriate ACLs on virtual directories |
| Reference | IIS 5.0 Baseline Security Checklist |
| Risk | Improper rights of files can be used by an attacker to change the files and compromise the target server |
| Test | The files for web access on Exchange server are located in the */exchweb* directory. Verify that proper rights have been assigned to all users / groups. |
| Compliance | Compliant system must have following rights assigned either for individual files or for corresponding directories:<br>Administrators (Full Control) |

| | |
|---|---|
| | System (Full Control)<br>Everyone (X) or Authenticated Users ( X ) |
| O/S | Objective |

| | |
|---|---|
| ID | IIS4 |
| Objective | Set Appropriate IIS Log File ACLs |
| Reference | IIS 5.0 Baseline Security Checklist |
| Risk | Ability to modifying log files permits malicious user to cover his tracks |
| Test | Verify the ACLs on the IIS-generated log files<br>(*%systemroot%\system32\LogFiles*) |
| Compliance | Rights of the files must be as follows:<br>- Administrators (Full Control)<br>- System (Full Control)<br>- Everyone (RWC) |
| O/S | Objective |

| | |
|---|---|
| ID | IIS5 |
| Objective | Disable or Remove All Sample Applications |
| Reference | IIS 5.0 Baseline Security Checklist |
| Risk | IIS Sample Applications can be exploited by hackers to break into an IIS system because they contain sample scripts. A production Web server should not have any sample code or scripts on the system. |
| Test | Run MBSA and look for "*Sample Applications*" test results in the "*Internet Information Services (IIS) Scan Results"* section.<br>Look if the following directories are present on the audited server:<br>\IISSamples<br>\IISHelp<br>\MSADC |
| Compliance | - All sample scripts and applications must be removed. |
| O/S | Objective |

| | |
|---|---|
| ID | IIS6 |
| Objective | Remove the IISADMPWD Virtual Directory |
| Reference | IIS 5.0 Baseline Security Checklist |
| Risk | An attacker may use *.htr file located in the IISADMPWD directory to launch a brute force attack to gain valid username/password. A valid user may also use it to change his password on a locked account. |
| Test | Run MBSA and look for "IIS Admin Virtual Directory"<br>test results in the "*Internet Information Services (IIS) Scan Results"* section. |
| Compliance | - Compliant IIS server must have the IISADMPWD directory removed |
| O/S | Objective |

| | |
|---|---|
| ID | IIS7 |
| Objective | Remove all unnecessary ISAPI extensions and filters |
| Reference | IIS 5.0 Baseline Security Checklist<br>Microsoft Security Operations Guide for Exchange 2000 Server – chapter 3 |
| Risk | Requests to files with common filename extensions are handled by a DLL. Unnecessary ISAPI extensions extend attackers possibilities to break into the |

| | |
|---|---|
| | system. |
| Test | Test whether ISAPI extensions mappings are needed:<br>The extensions mapped by default include .htw, .ida, .idq, .asp, .cer, .cdx, .asa, .htr, .idc, .shtm, .shtml, .stm and .printer<br>Open “*Start / Programs / Administrative tools / Internet Service Manager*”<br>Right-click on the *Web server* – “*Properties*”<br>Click on “*Home Directory*” – “*Configuration*” and verify ISAPI extension mapping entries. |
| Compliance | - Compliant if unnecessary ISAPI mapping entries don’t exist:<br>OWA requires these scripts to run: *.asp* and *.htr* scripts<br>All the others, including *.idc, .stm, .shtml, .printer, .htw, .ida* and *.idq* can be disabled. |
| O/S | Objective |

| | |
|---|---|
| ID | IIS8 |
| Objective | Verify IIS logging |
| Reference | IIS 5.0 Baseline Security Checklist |
| Risk | Logging monitors user activity on the IIS server. Without logging there would be no evidence about any malicious activity. |
| Test | Open “*Start / Programs / Administrative tools / Internet Service Manager*”<br>Right-click on the *Web server* – “*Properties*”<br>Check if “*Enable logging”* option is checked.<br><br>In the “*Extended Logging Properties / Extended properties*” tab, verify settings of IIS Extended logging options. |
| Compliance | - IIS Web server logging must be enabled<br>- Following parameters should be logged:<br>Client IP Address<br>User Name<br>Server IP Address<br>Server Port<br>Method<br>URI Stem<br>HTTP Status<br>Win32 Status /*recommended setting<br>User Agent |
| O/S | Objective |

| | |
|---|---|
| ID | IIS9 |
| Objective | Verify IIS Metabase permissions |
| Reference | IIS 5.0 Baseline Security Checklist |
| Risk | Security and other IIS configuration settings are maintained in the IIS Metabase file. The default file permissions could allow an attacker to directly edit the Metabase file. |
| Test | The IIS Metabase file is located in the *%systemroot%\system32\inetsrv* directory. On the file *Properties / Security* tab verify the file permissions. |
| Compliance | - Full access must be granted only to Administrators and SYSTEM. |

| | |
|---|---|
| | - Access to the metabase file should be removed from all other users |
| O/S | Objective |

### *Exchange server security*

| | |
|---|---|
| ID | EXCH1 |
| Objective | Check latest Exchange 2000 Service packs and Hotfixes |
| Reference | Microsoft Security Bulletin Search<br>Microsoft - Securing Exchange 2000 Servers Resource Guide |
| Risk | Unpatched servers represent a major threat to the system security, which can lead to misuse of the target system by an attacker, lower immunity to various viruses and Trojan horse programs or incompliance with current and future OS enhancements. |
| Test | In the MBSA report, review the "*Exchange Server Security Updates*". |
| Compliance | - Compliant if all relevant Service packs and Hotfixes are installed on the audited servers |
| O/S | Objective |

| | |
|---|---|
| ID | EXCH2 |
| Objective | Disable all unnecessary Exchange services |
| Reference | Microsoft - Securing Exchange 2000 Servers Resource Guide<br>Microsoft Security Operations Guide for Exchange 2000 Server – chapter 3 |
| Risk | Unused Exchange services could give an attacker another possibility to break into the system |
| Test | Open "*Start / Programs / Administrative tools / Services*".<br>Verify running and stopped Exchange services |
| Compliance | - Compliant if unnecessary services are stopped<br>Exchange 2000 Back-end server services recommended startup mode:<br>*Microsoft Exchange Event* *Disabled*<br>*Microsoft Exchange IMAP4* *Disabled*<br>*Microsoft Exchange Information Store* *Automatic*<br>*Microsoft Exchange Management* *Automatic*<br>*Microsoft Exchange MTA Stacks* *Automatic*<br>*Microsoft Exchange POP3* *Disabled*<br>*Microsoft Exchange Routing Engine* *Automatic*<br>*Microsoft Exchange Site Replication Service* *Disabled*<br>*Microsoft Exchange System Attendant* *Automatic*<br><br>Exchange 2000 Front-end (OWA) server services recommended startup mode:<br>*Microsoft Exchange Event* *Disabled*<br>*Microsoft Exchange IMAP4* *Disabled*<br>*Microsoft Exchange Information Store* *Disabled*<br>*Microsoft Exchange Management* *Disabled*<br>*Microsoft Exchange MTA Stacks* *Disabled*<br>*Microsoft Exchange POP3* *Disabled*<br>*Microsoft Exchange Routing Engine* *Automatic*<br>*Microsoft Exchange Site Replication Service* *Disabled*<br>*Microsoft Exchange System Attendant* *Disabled* |

| | |
|---|---|
| O/S | Objective |

| | |
|---|---|
| ID | EXCH3 |
| Objective | Verify mailbox size limitation |
| Reference | Microsoft - Securing Exchange 2000 Servers Resource Guide<br>Microsoft Knowledge Base Article 319583 - Configure Storage Limits on Mailboxes in Exchange 2000 |
| Risk | Exchange database will be shut down when it reaches its limitation (16 GB by default). Without Mailbox size limits, this can be used to launch Denial of Service attack. |
| Test | Open "*Start / Programs / Microsoft Exchange / System Manager*"<br>Expand the *Servers* container, click the server that hosts the mailbox store that you want to verify, and then double-click *Storage group* in the right pane.<br>Right-click the mailbox store that you want to configure, click *Properties*, and then click the *Limits* tab.<br>Verify the following check boxes under Storage limits:<br>*Issue warning at*<br>*Prohibit send at:*<br>*Prohibit send and receive at:* |
| Compliance | - Compliant if storage limits are set in accordance with company requirements. Recommended maximum limits are 100 MB for ordinary users and 200 MB for power users. |
| O/S | Objective + Subjective limits |

| | |
|---|---|
| ID | EXCH4 |
| Objective | Check Exchange directory location and access rights |
| Reference | National Security Agency - Guide to the Secure Configuration and Administration of Microsoft Exchange 2000 |
| Risk | Operating system should be installed on its own partition for integrity reasons.<br>Also, default permissions of the *\Exchsrvr* directory are set by Windows 2000 to full control for the EVERYONE group. This introduces a risk that somebody could read messages from the directory or delete the Exchange database. |
| Test | Verify that Exchange server is not installed on a domain controller<br>Verify that *\WINNT* and *\Exchsrvr* directories are on different partitions.<br>Check permissions on the *\Exchsrvr* directory. |
| Compliance | - Exchange server should not be installed on a domain controller<br>- *\WINNT* and *\Exchsrvr* directories must be installed on different partitions.<br>- The "*Everyone*" group must have no permissions on the *\Exchsrvr* directory<br>- "*Full control*" permission should be given to following groups: System, Creator owner, Domain Admins, Exchange administrative groups.<br>- On OWA, Authenticated users need Read and Execute permissions. |

| | |
|---|---|
| O/S | Objective |

| | |
|---|---|
| ID | EXCH5 |
| Objective | Verify anti-virus software |
| Reference | Microsoft Security Operations Guide for Exchange 2000 Server |
| Risk | Viruses and Trojan horse programs are one of the most common security issues. |
| Test | Verify that antivirus software has been installed and that the virus signature updates are up-to-date. |
| Compliance | - Antivirus software must be installed to verify all messages and attachments<br>- Virus signatures must be up-to-date |
| O/S | Objective |

| | |
|---|---|
| ID | EXCH6 |
| Objective | Verify Exchange logfile permissions |
| Reference | Securityfocus Securing Exchange 2000 |
| Risk | Tracking logs contain e-mail addresses that typically correspond directly to usernames, which is a very valuable information for an attacker. The tracking logs are available to *Everyone* group “Read only” by default. |
| Test | Open *\Exchsrvr\%COMPUTERNAME%.log*.<br>Verify access rights for the Tracking logs directory / files |
| Compliance | - The Read-only access permission for Everyone must be removed |
| O/S | Objective |

| | |
|---|---|
| ID | EXCH7 |
| Objective | Check if SMTP banner has been changed |
| Reference | Microsoft Security Operations Guide for Exchange 2000 Server – chapter 3 |
| Risk | The less information you provide an attacker, the more difficult it is to attack your system. |
| Test | Telnet to the audited Exchange Back-end server, TCP port 25.<br>Verify SMTP banner provided by the server.<br>(OWA – Exchange Front-end server should not run the SMTP service) |
| Compliance | - The "*ESMTP MAIL Service, Version: 5.0.2195.1600*" banner must not be displayed. However the fully qualified domain dame and the date and time are still displayed. |
| O/S | Objective |

| | |
|---|---|
| ID | EXCH8 |
| Objective | No local Exchange data should reside on OWA server |
| Reference | Microsoft Security Operations Guide for Exchange 2000 Server – chapter 3 |
| Risk | The Information Store service is not required since no mail is delivered to this server. |
| Test | Open “*Start / Programs / Microsoft Exchange / System Manager*”<br>In the Exchange 2000 hierarchy in the left pane, find the Server container. |

| | |
|---|---|
| | Expand the *Servers* container; click the server that hosts the mailbox store that you want to verify. An error message should pop up notifying that Microsoft Exchange Information Server is not available. |
| Compliance | - Information Store service must not run on the OWA server |
| O/S | Objective |

| | |
|---|---|
| ID | EXCH9 |
| Objective | Assure adequate OWA user authentication |
| Reference | Security focus - Exchange 2000 in the Enterprise: Tips and Tricks Part Two |
| Risk | Inadequate OWA authentication can lead to password sniffing, unauthorized use and system compromise.<br>Without SSL, reader-to-writer confidentiality is not assured by any means. SSL also protects the authentication name/password when using basic authentication. |
| Test | Open "*Start / Programs / Administrative tools / Internet Service Manager*"<br>Right-click on the *Web server* – "*Properties*"<br>Under "*Directory security*" - "*Anonymous access and authentication method*" check, if basic authentication is used.<br>Under "*Directory security*" - "*Secure communication*" check, if SSL is required to connect to the audited server. |
| Compliance | - Basic Authentication or Integrated Windows authentication must be used<br>- SSL encryption 128 kbps must be used |
| O/S | Objective |

## *Network Security*

| | |
|---|---|
| ID | NET1 |
| Objective | Verify Firewall rules restricting access to OWA from the Internet |
| Reference | Microsoft Security Operations Guide for Exchange 2000 Server |
| Risk | Open ports give an attacker better chances to break into the target server |
| Test | Check firewall rules defining Internet user access to the OWA server |
| Compliance | - Only Http / Https access must be allowed from the Internet to the OWA server |
| O/S | Objective |

| | |
|---|---|
| ID | NET2 |
| Objective | Verify Firewall rules restricting access from OWA to the internal network |
| Reference | Microsoft Security Operations Guide for Exchange 2000 Server |
| Risk | Open ports give an attacker better chances to break into the target server |
| Test | Check firewall rules defining access from OWA to the internal network |
| Compliance | - Only following ports must be allowed between OWA server and internal Exchange server:<br>Http - 80 TCP<br>- Only following ports must be allowed between OWA server and internal Active Directory server: |

| | |
|---|---|
| | DNS – 53 TCP/UDP<br>Kerberos – 88 TCP / UDP<br>Endpoint Mapper – 135 TCP<br>LDAP – 389 TCP / UDP<br>SMB/CIFS – 445 TCP<br>RPC – 1024+ TCP ( or any RPC static port )<br>GC – 3268 TCP |
| O/S | Objective |

### *Management Security*

| | |
|---|---|
| ID | MGMT1 |
| Objective | Verify system backup procedures |
| Reference | Personal Experience |
| Risk | Data and information loss can result into financial and operational loss. |
| Test | Interview all systems administrators for the system backup procedures |
| Compliance | - System must be backed up regularly<br>- Backups must be kept safely |
| O/S | Objective |

| | |
|---|---|
| ID | MGMT2 |
| Objective | Verify that logs are reviewed and archived regularly |
| Reference | Personal Experience |
| Risk | Without early detection of possible attacks, the system can be compromised without a notice of system administrators and security staff<br>Safely stored logs can provide evidence of unauthorized activities. |
| Test | Interview all system administrators responsible for the Exchange Servers for the system and procedures for logs review and archiving.<br>Verify that logs are backed up offsite and are stored in a safe place. |
| Compliance | - Logs must be reviewed on daily basis<br>- Logs must be archived for at least 6 months<br>- Logs must be stored in a safe place with controlled access |
| O/S | Subjective |

## Audit evidence

### PHY1 – Check physical access to equipment room

Physical access to the room containing network equipment is limited and only by authorized personnel. Up-to-date list of authorized persons exists. Access to the equipment room is recorded and has been showed to the auditor.

### PHY2 – Check physical access to equipment

All equipment is located in locked racks and all power and network and other cabling is routed through the bottom of the rack

### PHY3 – Check equipment environmental conditions

Data center has appropriate air-condition, fire detection system and monitoring of temperature, humidity and other environmental variables.
All systems have power from uninterruptible power supply.
Evidence about regular UPS verification was shown during the audit.

### PHY4 – Check Backups storage

Backups are stored in a safe place with controlled access.

### NET1 – Check Firewall OWA rules

Review of the firewall rules showed that only Http / Https access is allowed from the Internet to the OWA server. Also traffic from OWA server towards the internal network is set up according to the recommendations.

### NET2 – Check Firewall Exchange rules

Only necessary ports are opened for communication between the OWA server in the DMZ and Exchange Back-end server and Active Directory server located in the internal network.

### MGMT1 – Check system backup procedures

All Systems are backed up on a regular basis and backups are kept in a remote location.

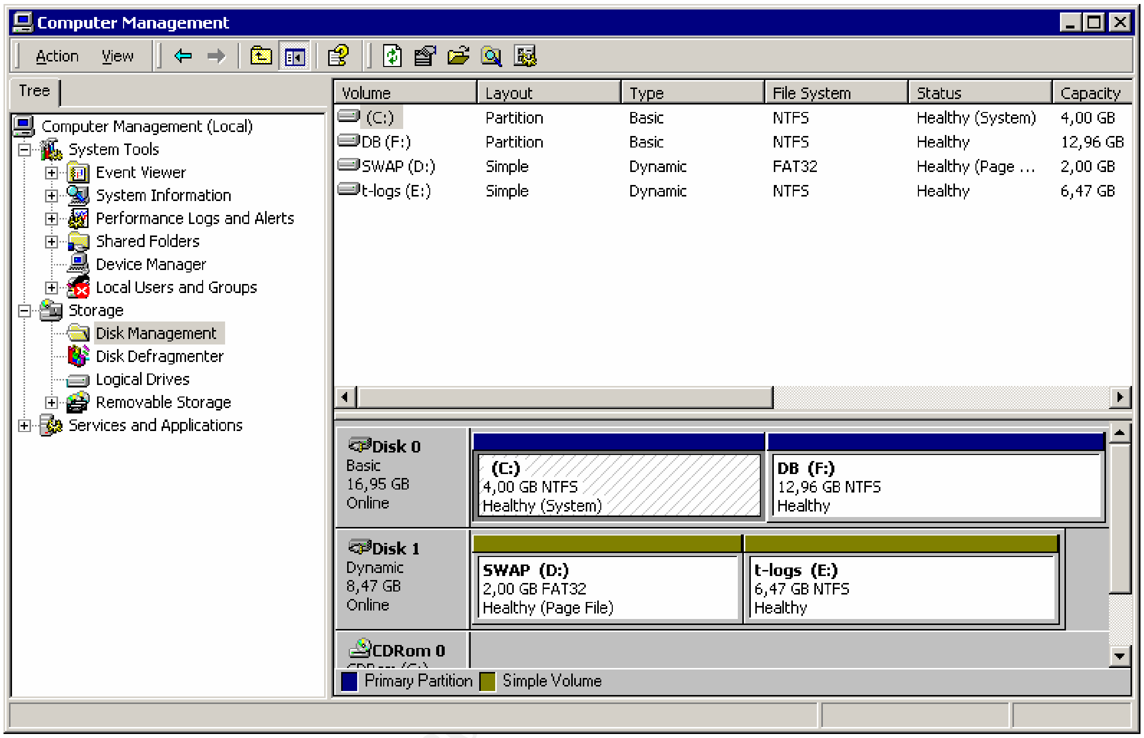
### MGMT2 – Check logs review policy

Administrators were asked about the company logging analysis policy and procedures. In their responses they stated that logs are reviewed only occasionally and that no log analysis tools are in place.
Available logs are backed up on a tape and stored off-site.

## *Exchange Back-end server*

### OS1 – Check NTFS disk format

The test shows that although there is a partition that is not NTFS formatted, it is used only as the system Swap partition.  Partitions used for storing user data are NTFS formatted.



| Volume | Layout | Type | File System | Status | Capacity |
|---|---|---|---|---|---|
| (C:) | Partition | Basic | NTFS | Healthy (System) | 4,00 GB |
| DB (F:) | Partition | Basic | NTFS | Healthy | 12,96 GB |
| SWAP (D:) | Simple | Dynamic | FAT32 | Healthy (Page ... | 2,00 GB |
| t-logs (E:) | Simple | Dynamic | NTFS | Healthy | 6,47 GB |

Disk 0
Basic
16,95 GB
Online

(C:)
4,00 GB NTFS
Healthy (System)

DB (F:)
12,96 GB NTFS
Healthy

Disk 1
Dynamic
8,47 GB
Online

SWAP (D:)
2,00 GB FAT32
Healthy (Page File)

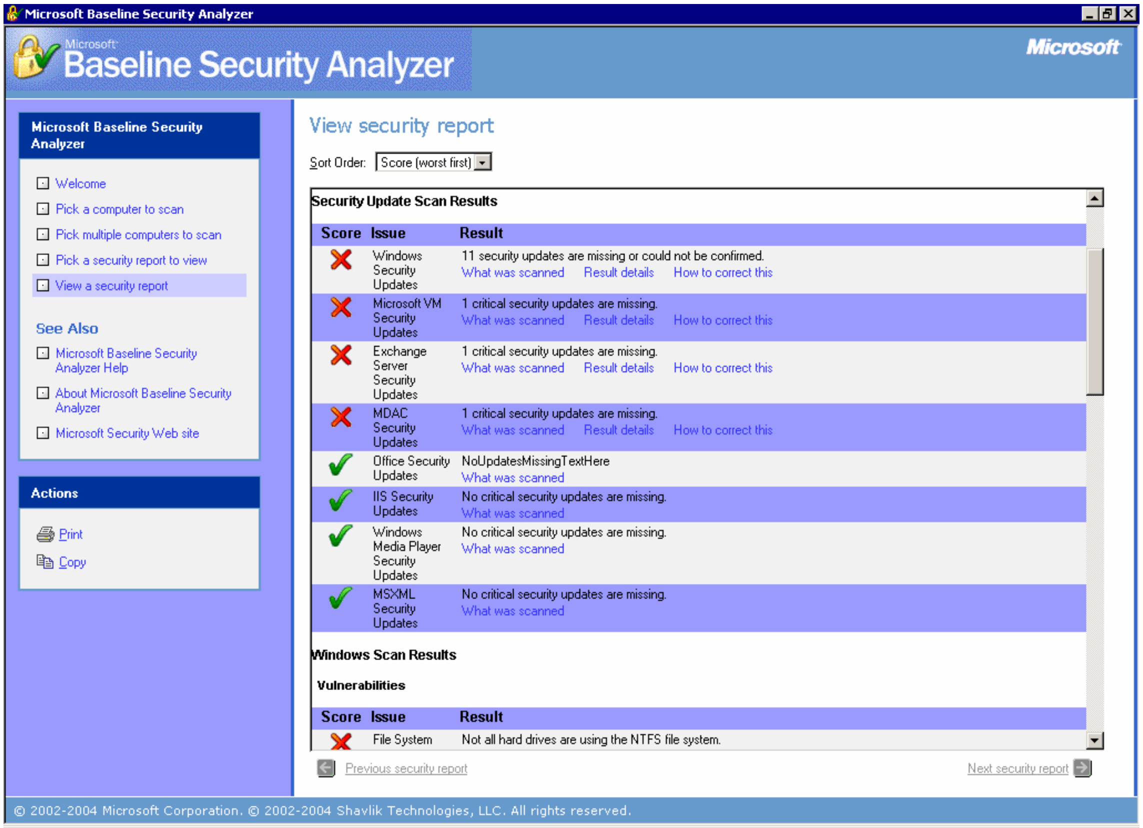
t-logs (E:)
6,47 GB NTFS
Healthy

CDRom 0

■ Primary Partition ■ Simple Volume

### OS2 – Check latest Service pack and security hotfixes

The tests conducted with MBSA show that there are 11 operating system updates missing. Although the server is not directly exposed to the Internet, attacks from the internal network – not only from the corporate users, but maybe from a virus or a Trojan horse – are possible. One Critical Microsoft Virtual Machine security update is missing.


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy

View security report

Sort Order: Score (worst first)

**Security Update Scan Results**

| Score | Issue | Result |
|---|---|---|
| ✗ | Windows Security Updates | 11 security updates are missing or could not be confirmed.<br>What was scanned Result details How to correct this |
| ✗ | Microsoft VM Security Updates | 1 critical security updates are missing.<br>What was scanned Result details How to correct this |
| ✗ | Exchange Server Security Updates | 1 critical security updates are missing.<br>What was scanned Result details How to correct this |
| ✗ | MDAC Security Updates | 1 critical security updates are missing.<br>What was scanned Result details How to correct this |
| ✓ | Office Security Updates | NoUpdatesMissingTextHere<br>What was scanned |
| ✓ | IIS Security Updates | No critical security updates are missing.<br>What was scanned |
| ✓ | Windows Media Player Security Updates | No critical security updates are missing.<br>What was scanned |
| ✓ | MSXML Security Updates | No critical security updates are missing.<br>What was scanned |

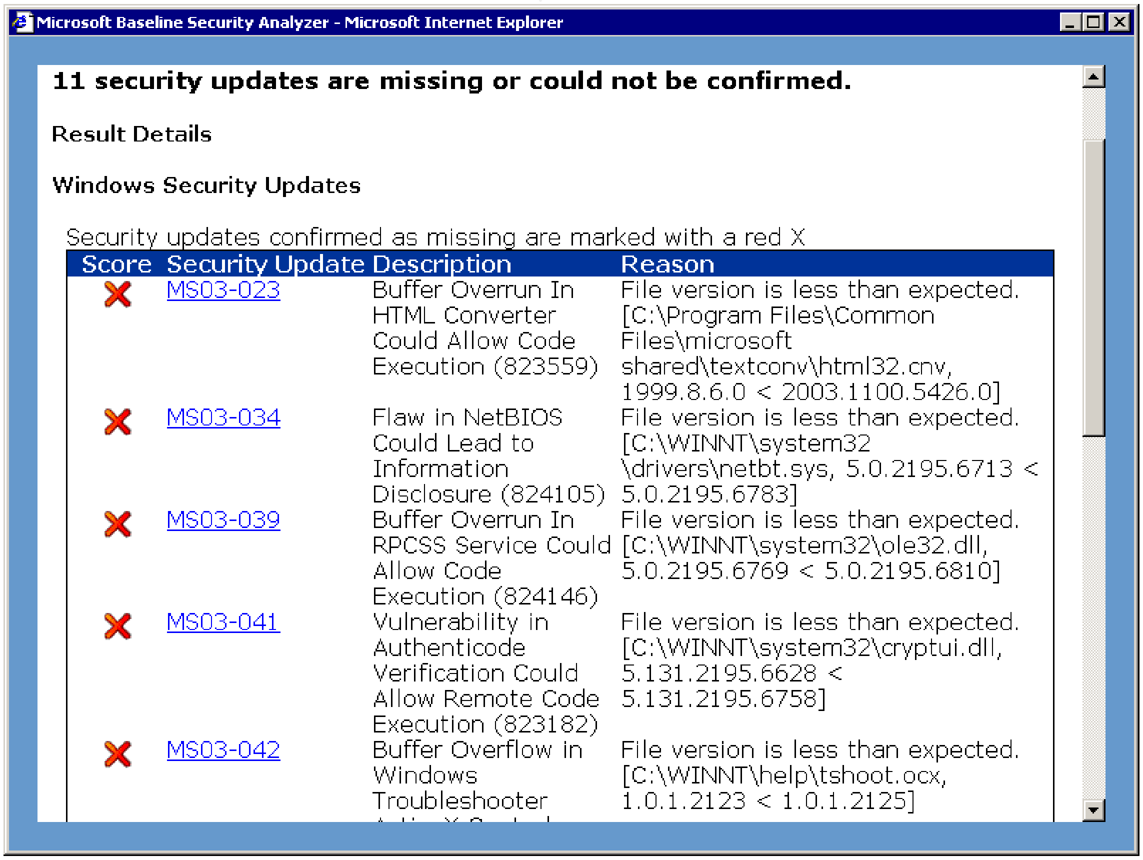
**Windows Scan Results**

**Vulnerabilities**

| Score | Issue | Result |
|---|---|---|
| ✗ | File System | Not all hard drives are using the NTFS file system. |

Previous security report    Next security report

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.


Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

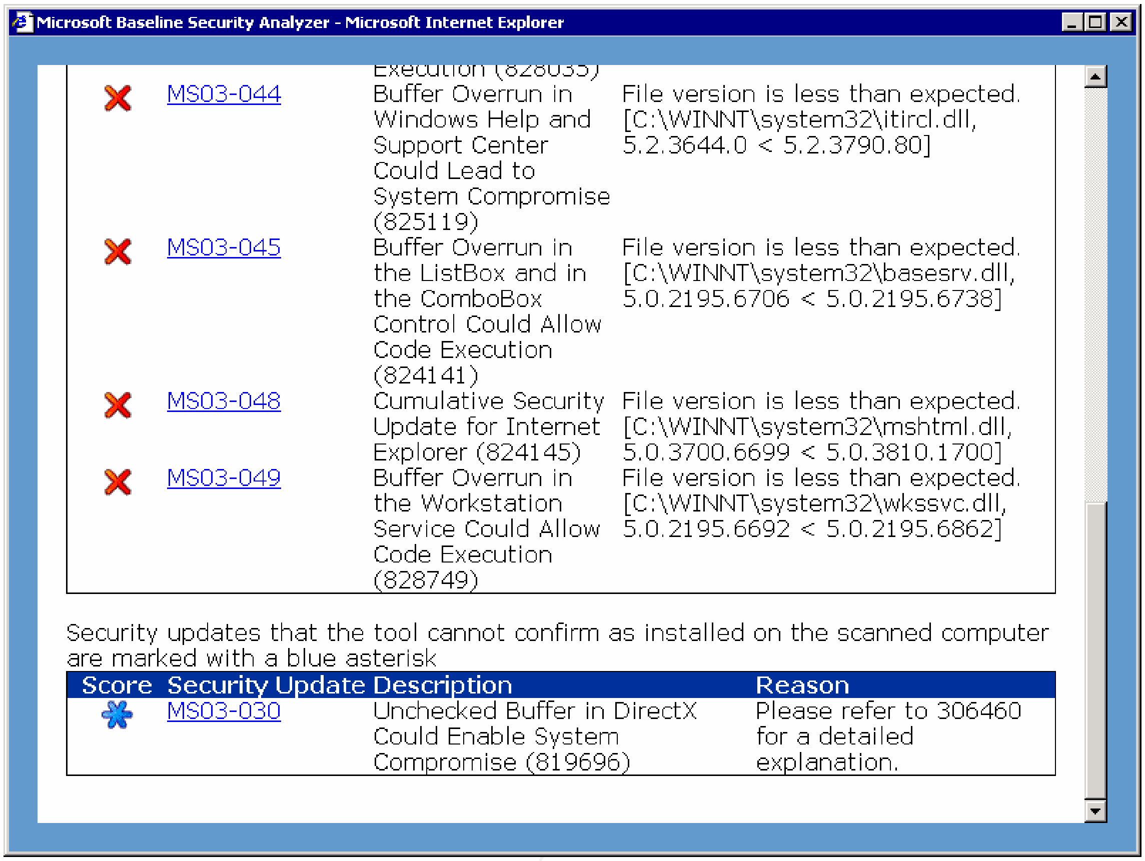
**11 security updates are missing or could not be confirmed.**

Result Details

Windows Security Updates

Security updates confirmed as missing are marked with a red X

| Score | Security Update | Description | Reason |
|---|---|---|---|
| ✗ | MS03-023 | Buffer Overrun In HTML Converter Could Allow Code Execution (823559) | File version is less than expected. [C:\Program Files\Common Files\microsoft shared\textconv\html32.cnv, 1999.8.6.0 < 2003.1100.5426.0] |
| ✗ | MS03-034 | Flaw in NetBIOS Could Lead to Information Disclosure (824105) | File version is less than expected. [C:\WINNT\system32 \drivers\netbt.sys, 5.0.2195.6713 < 5.0.2195.6783] |
| ✗ | MS03-039 | Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) | File version is less than expected. [C:\WINNT\system32\ole32.dll, 5.0.2195.6769 < 5.0.2195.6810] |
| ✗ | MS03-041 | Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182) | File version is less than expected. [C:\WINNT\system32\cryptui.dll, 5.131.2195.6628 < 5.131.2195.6758] |
| ✗ | MS03-042 | Buffer Overflow in Windows Troubleshooter | File version is less than expected. [C:\WINNT\help\tshoot.ocx, 1.0.1.2123 < 1.0.1.2125] |



Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

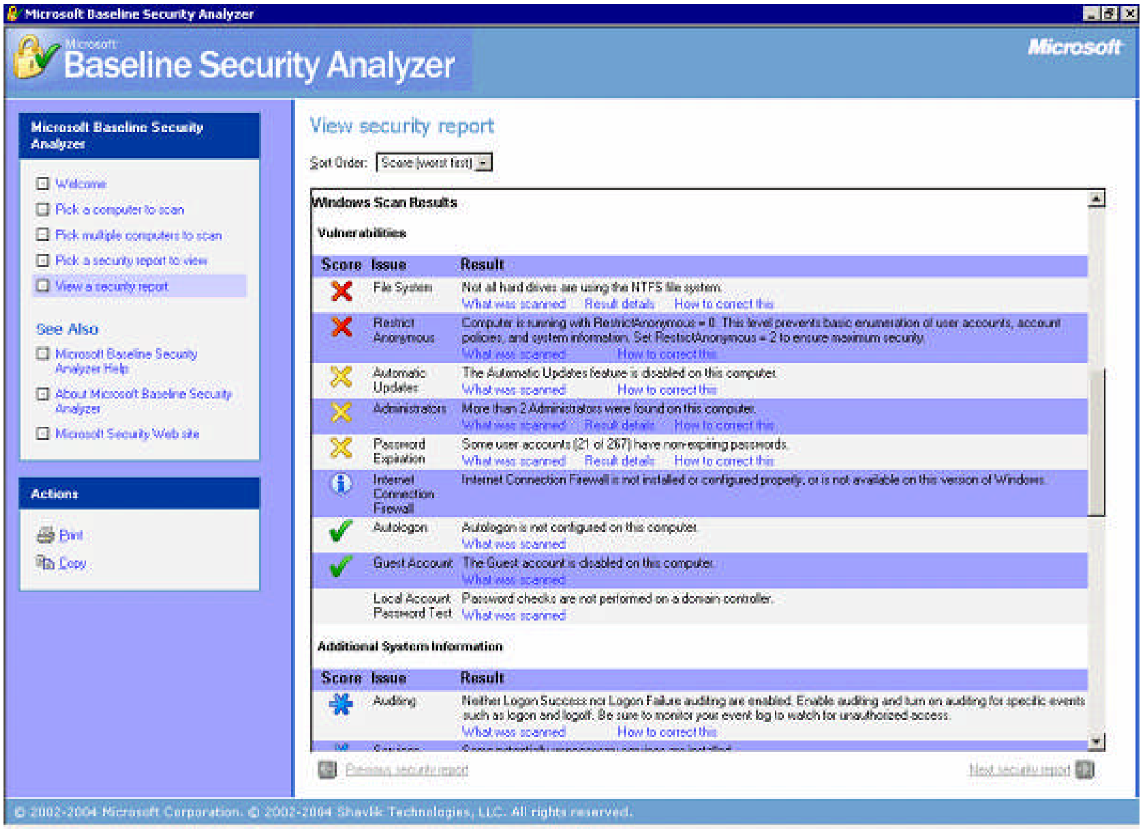
| | | | |
|---|---|---|---|
| | | Execution (828035) | |
| ✗ | MS03-044 | Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (825119) | File version is less than expected. [C:\WINNT\system32\itircl.dll, 5.2.3644.0 < 5.2.3790.80] |
| ✗ | MS03-045 | Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (824141) | File version is less than expected. [C:\WINNT\system32\basesrv.dll, 5.0.2195.6706 < 5.0.2195.6738] |
| ✗ | MS03-048 | Cumulative Security Update for Internet Explorer (824145) | File version is less than expected. [C:\WINNT\system32\mshtml.dll, 5.0.3700.6699 < 5.0.3810.1700] |
| ✗ | MS03-049 | Buffer Overrun in the Workstation Service Could Allow Code Execution (828749) | File version is less than expected. [C:\WINNT\system32\wkssvc.dll, 5.0.2195.6692 < 5.0.2195.6862] |

Security updates that the tool cannot confirm as installed on the scanned computer are marked with a blue asterisk

| Score | Security Update | Description | Reason |
|---|---|---|---|
| ✱ | MS03-030 | Unchecked Buffer in DirectX Could Enable System Compromise (819696) | Please refer to 306460 for a detailed explanation. |

## OS3 – Check unnecessary accounts presence

The audit has shown that all the accounts are taken from the Active directory structure. There are two administrator accounts. Guest account has been disabled.


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
View security report
Previous security report
Next security report
© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

Sort Order: Score (worst first)

**Windows Scan Results**

**Vulnerabilities**

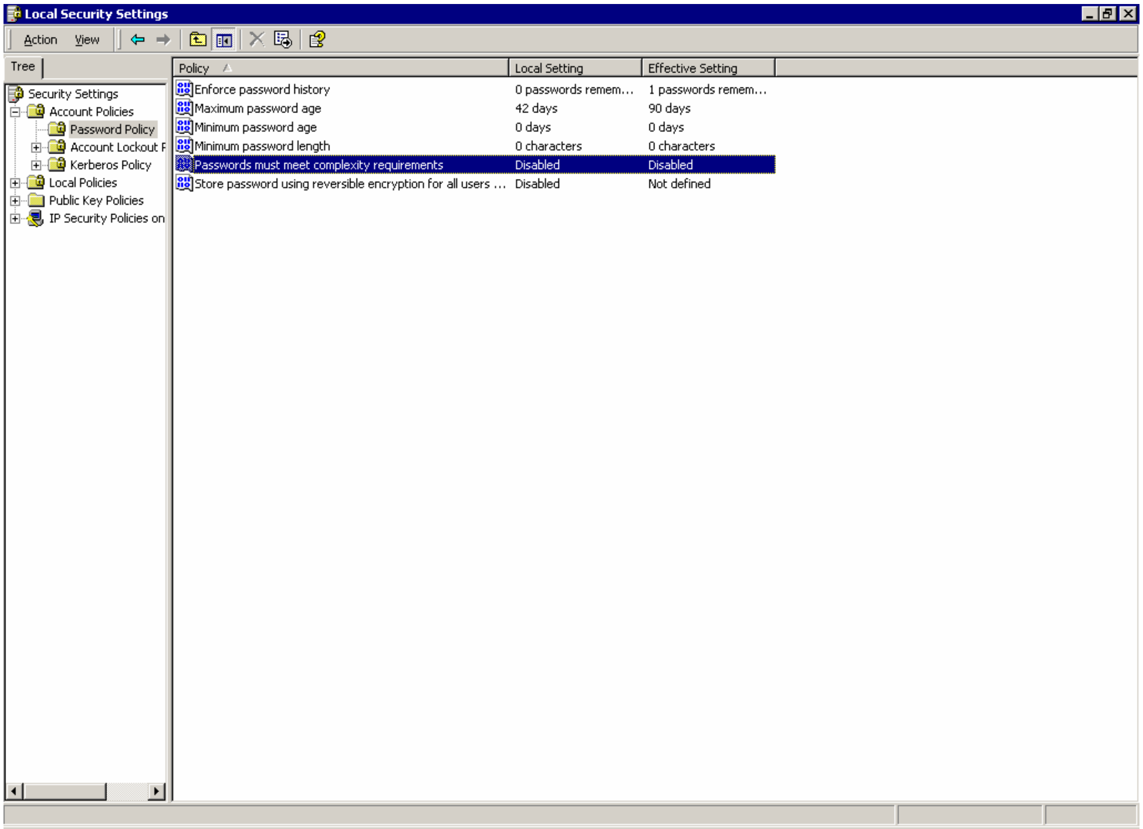
| Score | Issue | Result |
|---|---|---|
| ✗ | File System | Not all hard drives are using the NTFS file system.<br>What was scanned Result details How to correct this |
| ✗ | Restrict Anonymous | Computer is running with RestrictAnonymous = 0. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.<br>What was scanned How to correct this |
| ✗ | Automatic Updates | The Automatic Updates feature is disabled on this computer.<br>What was scanned How to correct this |
| ✗ | Administrators | More than 2 Administrators were found on this computer.<br>What was scanned Result details How to correct this |
| ✗ | Password Expiration | Some user accounts (21 of 267) have non-expiring passwords.<br>What was scanned Result details How to correct this |
| ℹ | Internet Connection Firewall | Internet Connection Firewall is not installed or configured properly, or is not available on this version of Windows. |
| ✓ | Autologon | Autologon is not configured on this computer.<br>What was scanned |
| ✓ | Guest Account | The Guest account is disabled on this computer.<br>What was scanned |
|  | Local Account Password Test | Password checks are not performed on a domain controller.<br>What was scanned |

**Additional System Information**

| Score | Issue | Result |
|---|---|---|
| ✱ | Auditing | Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.<br>What was scanned How to correct this |

## OS4 – Check account password policy

Audit of the Exchange Back-end server showed that the password policy is not enforced on the reviewed system. Although administrators stated that they are aware of the need for complex passwords and abide strong passwords, there is no password policy.



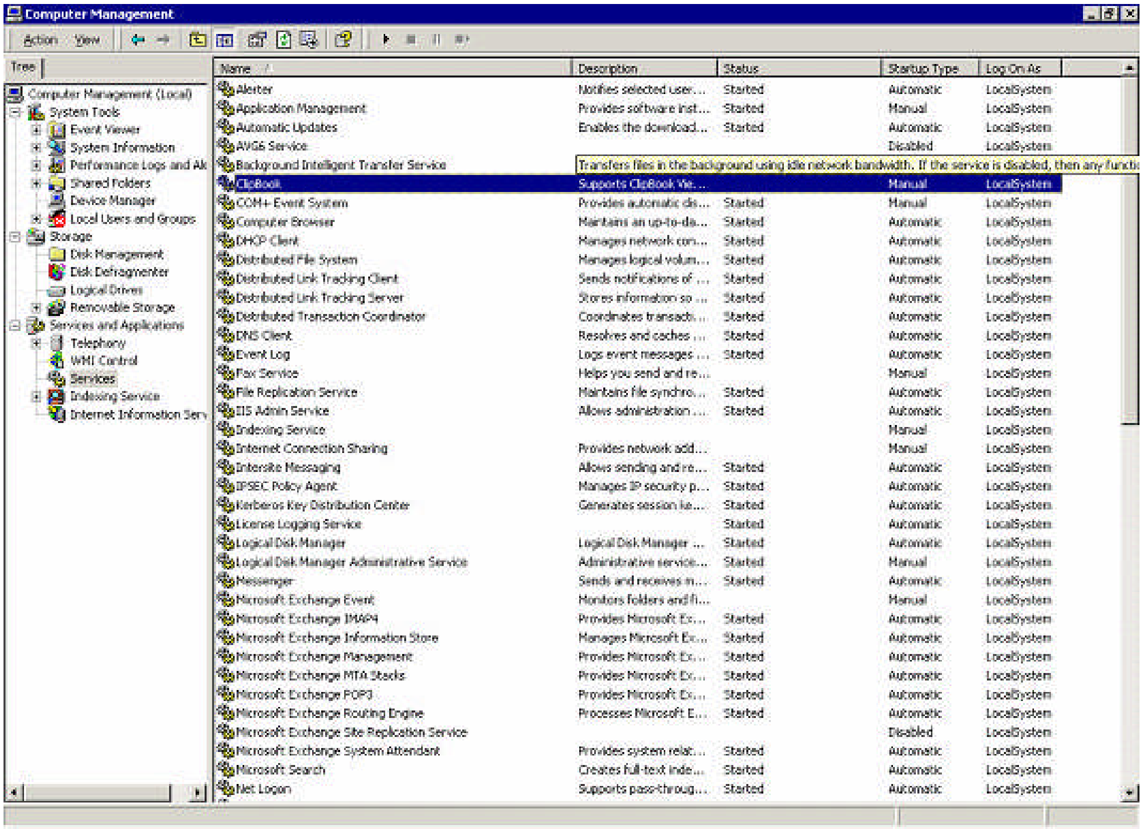
| Policy | Local Setting | Effective Setting |
|---|---|---|
| Enforce password history | 0 passwords remem... | 1 passwords remem... |
| Maximum password age | 42 days | 90 days |
| Minimum password age | 0 days | 0 days |
| Minimum password length | 0 characters | 0 characters |
| Passwords must meet complexity requirements | Disabled | Disabled |
| Store password using reversible encryption for all users ... | Disabled | Not defined |

## OS5 – Check running and disabled services

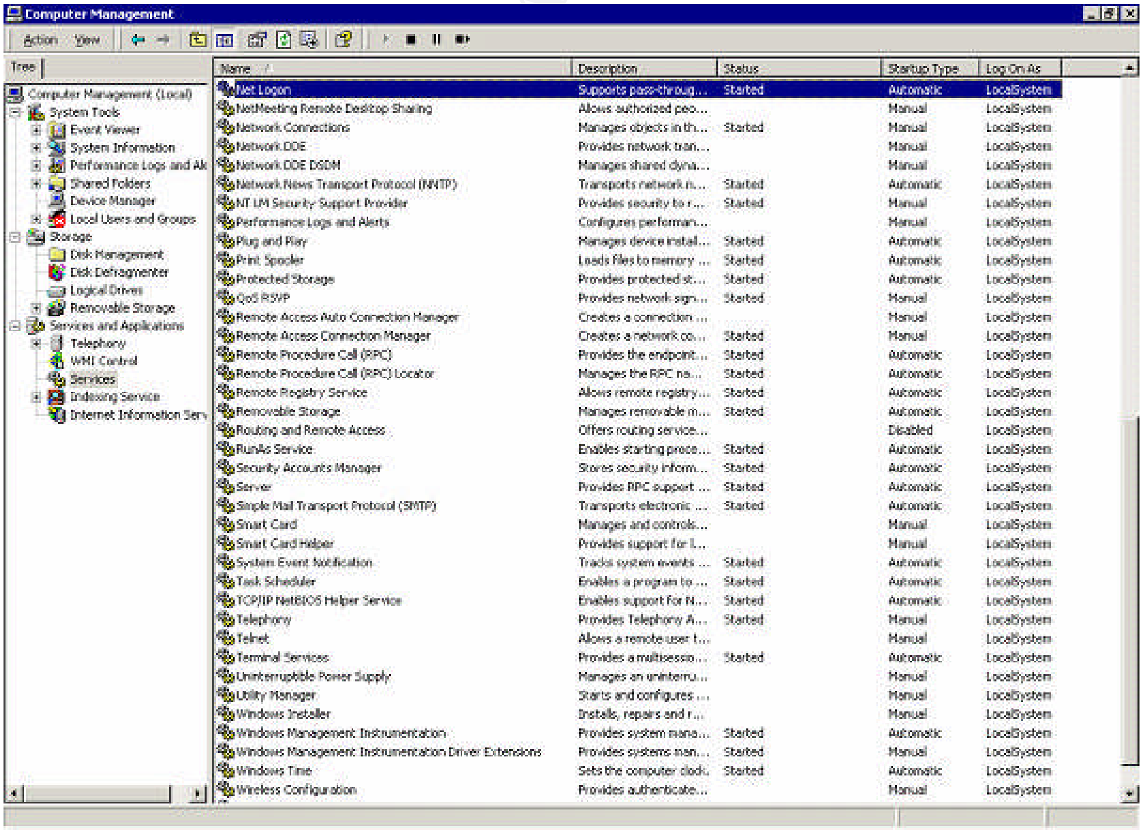
Following table lists of running services was found on the Exchange 2000 Back-end server during the audit. Among others, these services could be stopped:

Alerter
Computer Browser
DHCP Client
File Replication Server
License Logging Service
Messenger
Network News Transport Protocol (NNTP)
Print Spooler
Terminal Services
Remote Registry Service
Removable Storage

Some of the listed services are needed because Exchange 2000 Back-end was installed on a domain controller. Running Exchange 2000 on a domain controller is generally not recommended for security and integrity reasons; one of them is a need for more services to be running on the audited system.



| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Alerter | Notifies selected user... | Started | Automatic | LocalSystem |
| Application Management | Provides software inst... | Started | Manual | LocalSystem |
| Automatic Updates | Enables the download... | Started | Automatic | LocalSystem |
| AVG6 Service | | | Disabled | LocalSystem |
| Background Intelligent Transfer Service | Transfers files in the background using idle network bandwidth. If the service is disabled, then any functi | | | |
| ClipBook | Supports ClipBook Vie... | | Manual | LocalSystem |
| COM+ Event System | Provides automatic dis... | Started | Manual | LocalSystem |
| Computer Browser | Maintains an up-to-da... | Started | Automatic | LocalSystem |
| DHCP Client | Manages network con... | Started | Automatic | LocalSystem |
| Distributed File System | Manages logical volum... | Started | Automatic | LocalSystem |
| Distributed Link Tracking Client | Sends notifications of ... | Started | Automatic | LocalSystem |
| Distributed Link Tracking Server | Stores information so ... | Started | Automatic | LocalSystem |
| Distributed Transaction Coordinator | Coordinates transacti... | Started | Automatic | LocalSystem |
| DNS Client | Resolves and caches ... | Started | Automatic | LocalSystem |
| Event Log | Logs event messages ... | Started | Automatic | LocalSystem |
| Fax Service | Helps you send and re... | | Manual | LocalSystem |
| File Replication Service | Maintains file synchro... | Started | Automatic | LocalSystem |
| IIS Admin Service | Allows administration ... | Started | Automatic | LocalSystem |
| Indexing Service | | | Manual | LocalSystem |
| Internet Connection Sharing | Provides network add... | | Manual | LocalSystem |
| Intersite Messaging | Allows sending and re... | Started | Automatic | LocalSystem |
| IPSEC Policy Agent | Manages IP security p... | Started | Automatic | LocalSystem |
| Kerberos Key Distribution Center | Generates session ke... | Started | Automatic | LocalSystem |
| License Logging Service | | Started | Automatic | LocalSystem |
| Logical Disk Manager | Logical Disk Manager ... | Started | Automatic | LocalSystem |
| Logical Disk Manager Administrative Service | Administrative service... | Started | Manual | LocalSystem |
| Messenger | Sends and receives m... | Started | Automatic | LocalSystem |
| Microsoft Exchange Event | Monitors folders and fi... | | Manual | LocalSystem |
| Microsoft Exchange IMAP4 | Provides Microsoft Ex... | Started | Automatic | LocalSystem |
| Microsoft Exchange Information Store | Manages Microsoft Ex... | Started | Automatic | LocalSystem |
| Microsoft Exchange Management | Provides Microsoft Ex... | Started | Automatic | LocalSystem |
| Microsoft Exchange MTA Stacks | Provides Microsoft Ex... | Started | Automatic | LocalSystem |
| Microsoft Exchange POP3 | Provides Microsoft Ex... | Started | Automatic | LocalSystem |
| Microsoft Exchange Routing Engine | Processes Microsoft E... | Started | Automatic | LocalSystem |
| Microsoft Exchange Site Replication Service | | | Disabled | LocalSystem |
| Microsoft Exchange System Attendant | Provides system relat... | Started | Automatic | LocalSystem |
| Microsoft Search | Creates full-text inde... | Started | Automatic | LocalSystem |
| Net Logon | Supports pass-throug... | Started | Automatic | LocalSystem |

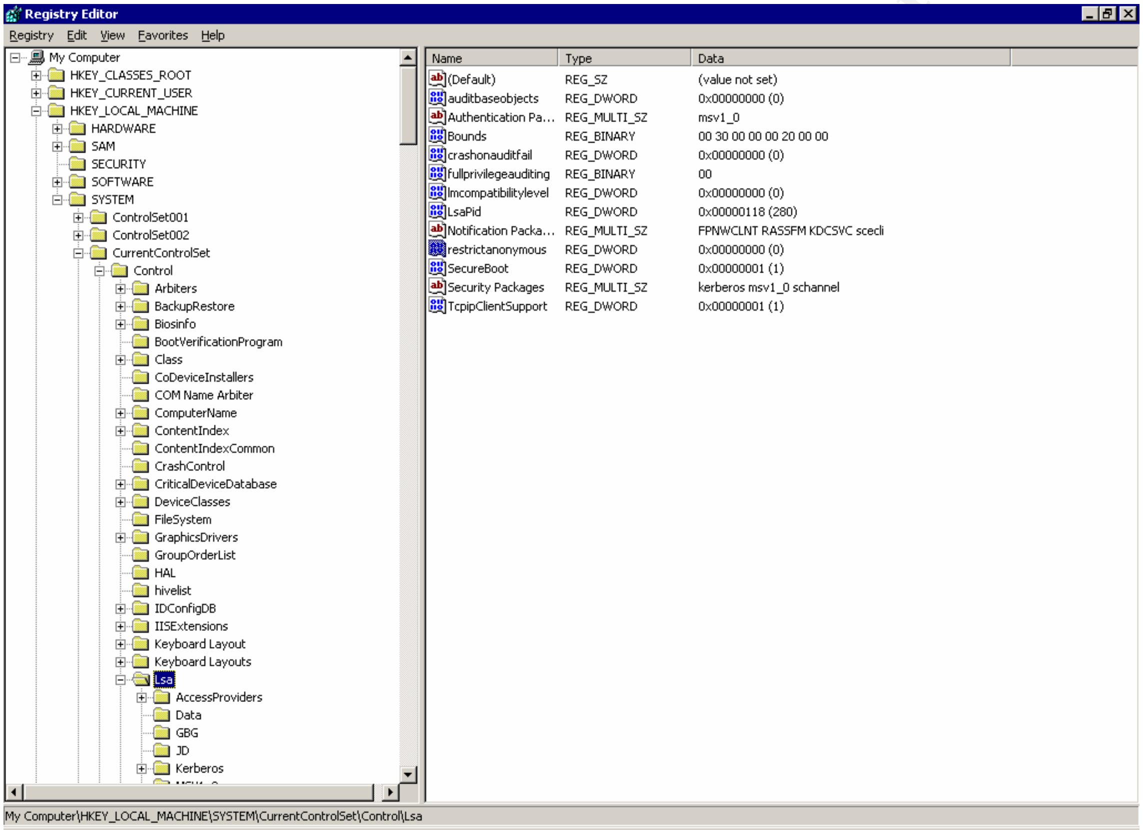


| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Net Logon | Supports pass-throug... | Started | Automatic | LocalSystem |
| NetMeeting Remote Desktop Sharing | Allows authorized peo... | | Manual | LocalSystem |
| Network Connections | Manages objects in th... | Started | Manual | LocalSystem |
| Network DDE | Provides network tran... | | Manual | LocalSystem |
| Network DDE DSDM | Manages shared dyna... | | Manual | LocalSystem |
| Network News Transport Protocol (NNTP) | Transports network n... | Started | Automatic | LocalSystem |
| NT LM Security Support Provider | Provides security to r... | Started | Manual | LocalSystem |
| Performance Logs and Alerts | Configures performan... | | Manual | LocalSystem |
| Plug and Play | Manages device instal... | Started | Automatic | LocalSystem |
| Print Spooler | Loads files to memory ... | Started | Automatic | LocalSystem |
| Protected Storage | Provides protected st... | Started | Automatic | LocalSystem |
| QoS RSVP | Provides network sign... | Started | Manual | LocalSystem |
| Remote Access Auto Connection Manager | Creates a connection ... | | Manual | LocalSystem |
| Remote Access Connection Manager | Creates a network co... | Started | Manual | LocalSystem |
| Remote Procedure Call (RPC) | Provides the endpoint... | Started | Automatic | LocalSystem |
| Remote Procedure Call (RPC) Locator | Manages the RPC na... | Started | Automatic | LocalSystem |
| Remote Registry Service | Allows remote registry... | Started | Automatic | LocalSystem |
| Removable Storage | Manages removable m... | Started | Automatic | LocalSystem |
| Routing and Remote Access | Offers routing service... | | Disabled | LocalSystem |
| RunAs Service | Enables starting proce... | Started | Automatic | LocalSystem |
| Security Accounts Manager | Stores security inform... | Started | Automatic | LocalSystem |
| Server | Provides RPC support ... | Started | Automatic | LocalSystem |
| Simple Mail Transport Protocol (SMTP) | Transports electronic ... | Started | Automatic | LocalSystem |
| Smart Card | Manages and controls... | | Manual | LocalSystem |
| Smart Card Helper | Provides support for l... | | Manual | LocalSystem |
| System Event Notification | Tracks system events ... | Started | Automatic | LocalSystem |
| Task Scheduler | Enables a program to ... | Started | Automatic | LocalSystem |
| TCP/IP NetBIOS Helper Service | Enables support for N... | Started | Automatic | LocalSystem |
| Telephony | Provides Telephony A... | Started | Manual | LocalSystem |
| Telnet | Allows a remote user t... | | Manual | LocalSystem |
| Terminal Services | Provides a multisessio... | Started | Automatic | LocalSystem |
| Uninterruptible Power Supply | Manages an uninterru... | | Manual | LocalSystem |
| Utility Manager | Starts and configures ... | | Manual | LocalSystem |
| Windows Installer | Installs, repairs and r... | | Manual | LocalSystem |
| Windows Management Instrumentation | Provides system mana... | Started | Automatic | LocalSystem |
| Windows Management Instrumentation Driver Extensions | Provides systems man... | Started | Manual | LocalSystem |
| Windows Time | Sets the computer clock | Started | Automatic | LocalSystem |
| Wireless Configuration | Provides authenticate... | | Manual | LocalSystem |

## OS6 – Check Anonymous Logon problems

Audit showed that the *"RestrictAnonymous"* registry value is set to 0, which means that no restrictions concerning anonymous access to the registry are in place. This Allows collecting names of domain accounts and network shares. While this vulnerability does not allow an attacker to compromise the server, it could provide the attacker with additional information to mount an attack. To better secure anonymous access, this option can be changed through Group Policy or via the registry.

Because this setting is on a domain controller, it probably cannot be changed because it is not in a pure 2000 environment and also because of the Exchange server functionality.

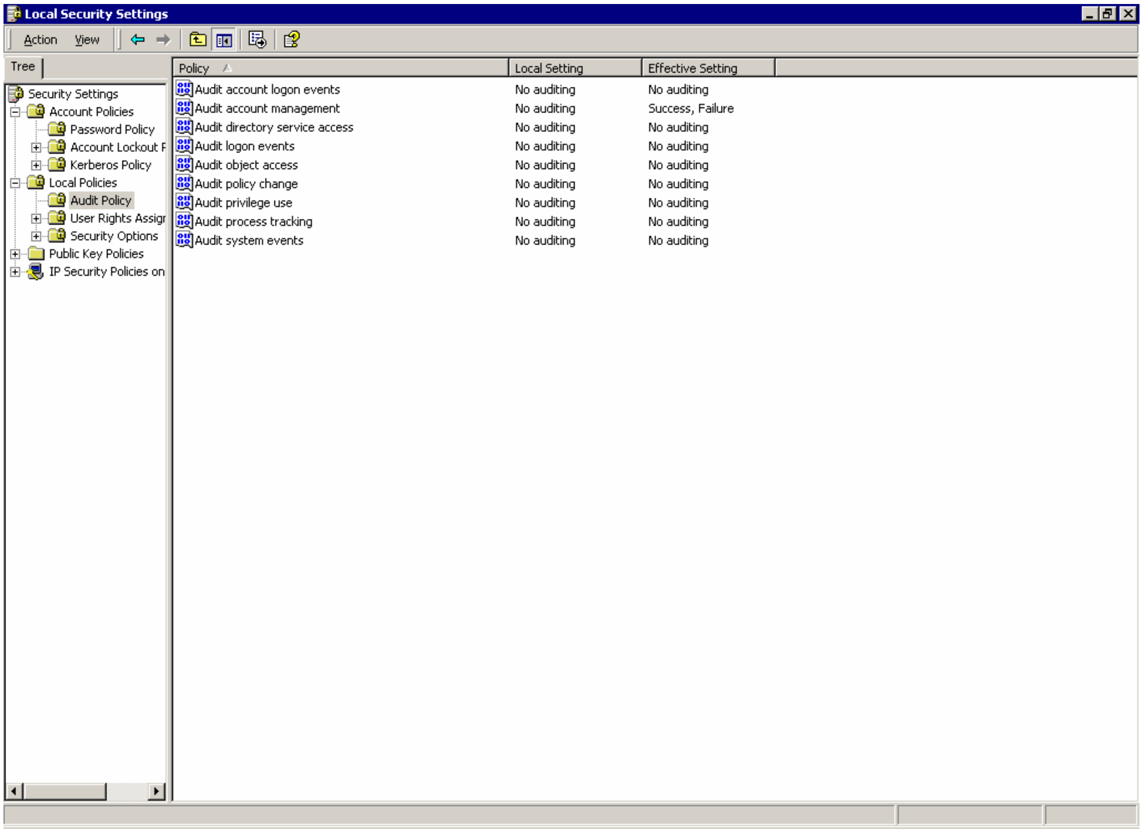


| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| auditbaseobjects | REG_DWORD | 0x00000000 (0) |
| Authentication Pa... | REG_MULTI_SZ | msv1_0 |
| Bounds | REG_BINARY | 00 30 00 00 00 20 00 00 |
| crashonauditfail | REG_DWORD | 0x00000000 (0) |
| fullprivilegeauditing | REG_BINARY | 00 |
| lmcompatibilitylevel | REG_DWORD | 0x00000000 (0) |
| LsaPid | REG_DWORD | 0x00000118 (280) |
| Notification Packa... | REG_MULTI_SZ | FPNWCLNT RASSFM KDCSVC scecli |
| restrictanonymous | REG_DWORD | 0x00000000 (0) |
| SecureBoot | REG_DWORD | 0x00000001 (1) |
| Security Packages | REG_MULTI_SZ | kerberos msv1_0 schannel |
| TcpipClientSupport | REG_DWORD | 0x00000001 (1) |

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

## OS7 – CHECK OS logging

Checking operating system log settings showed that except of account management, no audit is set up. Because of that, no evidence of possible unauthorized activity is available.



| Policy | Local Setting | Effective Setting |
|---|---|---|
| Audit account logon events | No auditing | No auditing |
| Audit account management | No auditing | Success, Failure |
| Audit directory service access | No auditing | No auditing |
| Audit logon events | No auditing | No auditing |
| Audit object access | No auditing | No auditing |
| Audit policy change | No auditing | No auditing |
| Audit privilege use | No auditing | No auditing |
| Audit process tracking | No auditing | No auditing |
| Audit system events | No auditing | No auditing |

## OS8 – Run an outside network vulnerability scan

Following check result shows extract from Nessus security scan audit that was run on the audited Exchange Back-end server.
10 **high severity** issues that were found by Nessus are listed below.
Most of the vulnerabilities correspond to findings in the section covering missing operating system patches etc. LDAP and Etherleak vulnerabilities are out of scope of the audit and are therefore not mentioned among the audit findings.

# Network Vulnerability Assessment Report

**30.01.2004**

**Sorted by host names**

**Session name:** Faust

**Start Time:** 30.01.2004 17:25:08
**Finish Time:** 30.01.2004 17:42:23
**Elapsed:** 0 day(s) 00:17:15

**Total records generated:** 121
**high severity:** 10
**low severity:** 68
**informational:** 43

**Summary of scanned hosts**

| Host | Holes | Warnings | Open ports | State |
|---|---|---|---|---|
| faust | 10 | 68 | 43 | Finished |

**Faust**

| Service | Severity | Description |
|---|---|---|
| ms-lsa (1029/tcp) | Info | Port is open |
| kerberos (88/tcp) | Info | Port is open |
| http (80/tcp) | Info | Port is open |
| pop3 (110/tcp) | Info | Port is open |
| nntp (119/tcp) | Info | Port is open |
| netbios-ssn (139/tcp) | Info | Port is open |
| loc-srv (135/tcp) | Info | Port is open |
| imap (143/tcp) | Info | Port is open |
| ldap (389/tcp) | Info | Port is open |
| https (443/tcp) | Info | Port is open |
| kpasswd (464/tcp) | Info | Port is open |
| microsoft-ds (445/tcp) | Info | Port is open |
| nntps (563/tcp) | Info | Port is open |
| http-rpc-epmap (593/tcp) | Info | Port is open |
| ldaps (636/tcp) | Info | Port is open |
| resvc (691/tcp) | Info | Port is open |
| pop3s (995/tcp) | Info | Port is open |
| imaps (993/tcp) | Info | Port is open |
| NFS-or-IIS (1025/tcp) | Info | Port is open |
| cichlid (1377/udp) | Info | Port is open |
| unknown (1274/udp) | Info | Port is open |
| loc-srv (135/udp) | Info | Port is open |
| unknown (1247/udp) | Info | Port is open |
| unknown (1151/udp) | Info | Port is open |
| ntp (123/udp) | Info | Port is open |
| unknown (1070/udp) | Info | Port is open |
| ms-lsa (1028/udp) | Info | Port is open |
| unknown (1192/tcp) | Info | Port is open |
| unknown (1152/tcp) | Info | Port is open |
| elan (1378/tcp) | Info | Port is open |
| unknown | Info | Port is open |

| | | |
|---|---|---|
| (1150/tcp) | | |
| ibm-pps (1376/tcp) | **Info** | Port is open |
| unknown (1275/tcp) | **Info** | Port is open |
| ms-term-serv (3389/tcp) | **Info** | Port is open |
| unknown (1069/tcp) | **Info** | Port is open |
| unknown (1273/tcp) | **Info** | Port is open |
| unknown (1193/tcp) | **Info** | Port is open |
| instl_bootc (1068/tcp) | **Info** | Port is open |
| unknown (1065/tcp) | **Info** | Port is open |
| sns_credit (1076/tcp) | **Info** | Port is open |
| netbios-ns (137/udp) | **Info** | Port is open |
| nimreg (1059/tcp) | **Info** | Port is open |
| smtp (25/tcp) | **Info** | Port is open |
| ldap (389/tcp) | **High** | Improperly configured LDAP servers will allow the directory BASE to be set to NULL. This allows information to be culled without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user can query your LDAP server using a tool such as 'LdapMiner'<br>Solution: Disable NULL BASE queries on your LDAP server<br>Risk factor : Medium |
| general/icmp | **High** | The remote host is vulnerable to an 'Etherleak' - the remote ethernet driver seems to leak bits of the content of the memory of the remote operating system.<br>Note that an attacker may take advantage of this flaw only when its target is on the same physical subnet.<br>See also : http://www.atstake.com/research/advisories/2003/a010603-1.txt<br>Solution : Contact your vendor for a fix<br>Risk factor : Serious<br>CVE : CAN-2003-0001<br>BID : 6535 |
| loc-srv (135/tcp) | **High** | The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. |

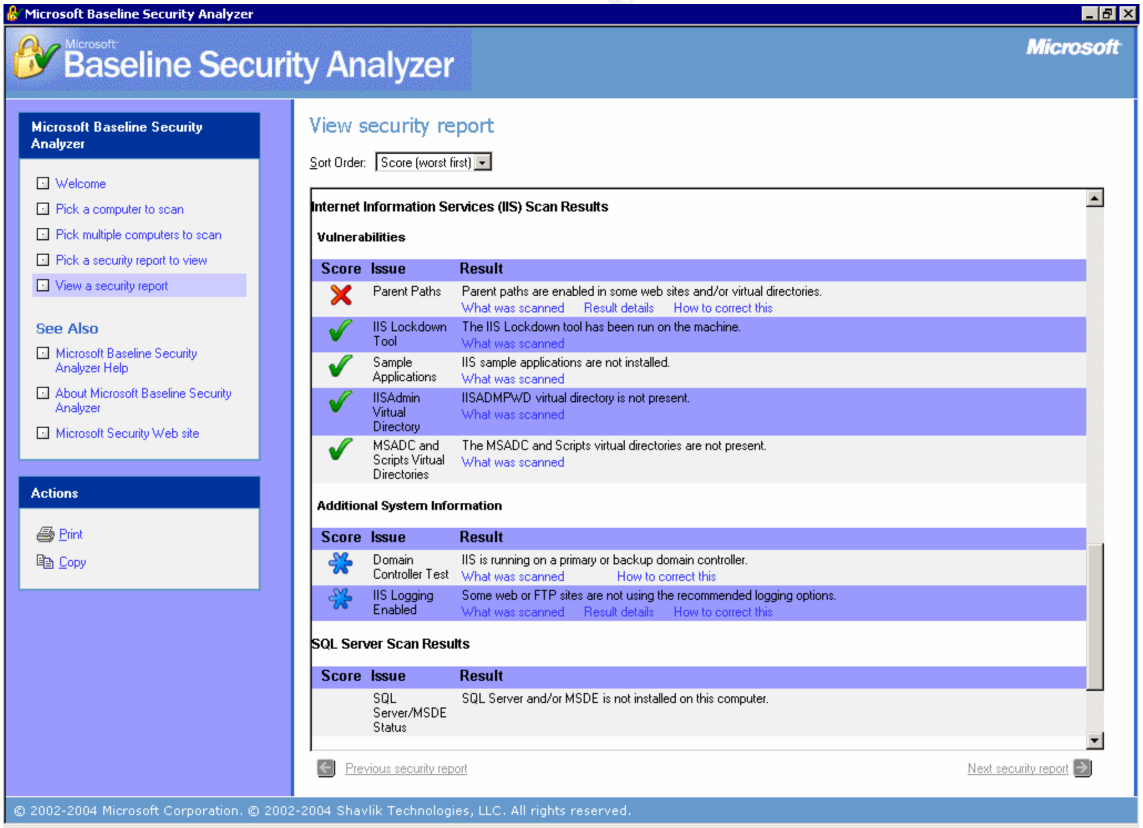
| | | |
|---|---|---|
| | | An attacker or a worm could use it to gain the control of this host.<br><br>Note that this is NOT the same bug as the one described in MS03-026 which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.<br>Solution: see<br>http://www.microsoft.com/technet/security/bulletin/MS03-039.asp<br>Risk factor : High<br>CVE : CAN-2003-0715, CAN-2003-0528, CAN-2003-0605<br>BID : 8458<br>Other references : IAVA:2003-A-0012 |
| ldap (389/tcp) | **High** | Improperly configured LDAP servers will allow any user to connect to the server and query for information.<br><br>Solution: Disable NULL BIND on your LDAP server<br><br>In addition, the LDAP bind function in Exchange 5.5 has a buffer overflow that allows a user to conduct a denial of service or execute commands in all versions prior to Exchange server SP2. Coupled with a NULL BIND, an anonymous user can mount a remote attack against your server.<br><br>Note: no test was done to see what version of Exchange server is running, nor attempt to verify the service pack.<br><br>Solution: see<br>http://www.microsoft.com/technet/security/bulletin/ms99-009.asp<br>Risk factor: Medium<br>CVE : CVE-1999-0385<br>BID : 503 |
| microsoft-ds (445/tcp) | **High** | It was possible to log into the remote host using a NULL session.<br>The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access<br><br>To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$<br>Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html<br><br>All the smb tests will be done as "/" in domain XYZXYZ<br>CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117<br>BID : 494, 990 |
| loc-srv (135/udp) | **High** | A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack. |

|  |  |  |
|---|---|---|
|  |  | This plugin actually checked for the presence of this flaw.<br><br>Solution : see<br>http://www.microsoft.com/technet/security/bulletin/ms03-043.asp<br><br>Risk factor : High<br>CVE : CAN-2003-0717<br>BID : 8826<br>Other references : IAVA:2003-A-0028 |
| microsoft-ds (445/tcp) | **High** | The following shares can be accessed using a NULL session :<br><br>- G - (readable?, writeable?)<br><br>Solution : To restrict their access under WindowsNT, open the explorer, do a right click on each, go to the 'sharing' tab, and click on 'permissions'<br>Risk factor : High<br>CVE : CAN-1999-0519, CAN-1999-0520<br>BID : 8026 |
| microsoft-ds (445/tcp) | **High** | A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail.Disabling the Messenger Service will prevent the possibility of attack.<br><br>This plugin determined by reading the remote registry that the patch MS03-043 has not been applied.<br><br>Solution : see<br>http://www.microsoft.com/technet/security/bulletin/ms03-043.asp<br><br>Risk factor : High<br>CVE : CAN-2003-0717<br>BID : 8826<br>Other references : IAVA:2003-B-0007 |
| microsoft-ds (445/tcp) | **High** | The registry key<br>HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon<br>is writeable by users who are not in the admin group.<br><br>This key contains a value which defines which program should<br>be run when a user logs on.<br><br>As this program runs in the SYSTEM context, the users who have the right to change the value of this key can gain more privileges on this host.<br><br>Solution : use regedt32 and set the permissions of this<br>key to : |

| | | |
|---|---|---|
| | | - admin group : Full Control<br>- system : Full Control<br>- everyone : Read<br><br>Risk factor : High<br>CVE : CAN-1999-0589 |
| smtp (25/tcp) | **High** | This system appears to be running a version of the Microsoft Exchange SMTP service that is vulnerable to a flaw in the XEXCH50 extended verb. This flaw can be used to completely crash Exchange 5.5 as well as execute arbitrary code on Exchange 2000.<br><br>Solution : See http://www.microsoft.com/technet/security/bulletin/MS03-046.asp<br>Risk factor : High<br>CVE : CAN-2003-0714<br>BID : 8838<br>Other references : IAVA:2003-A-0031 |

## IIS1 – Check IIS Lockdown tool implementation

The MBSA report shows that ISS Lockdown tool has been implemented.



Microsoft Baseline Security Analyzer
Microsoft Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
Previous security report
Next security report

View security report

Sort Order: Score (worst first)

**Internet Information Services (IIS) Scan Results**

**Vulnerabilities**

| Score | Issue | Result |
|---|---|---|
| ✗ | Parent Paths | Parent paths are enabled in some web sites and/or virtual directories.<br>What was scanned Result details How to correct this |
| ✓ | IIS Lockdown Tool | The IIS Lockdown tool has been run on the machine.<br>What was scanned |
| ✓ | Sample Applications | IIS sample applications are not installed.<br>What was scanned |
| ✓ | IISAdmin Virtual Directory | IISADMPWD virtual directory is not present.<br>What was scanned |
| ✓ | MSADC and Scripts Virtual Directories | The MSADC and Scripts virtual directories are not present.<br>What was scanned |

**Additional System Information**

| Score | Issue | Result |
|---|---|---|
| ✱ | Domain Controller Test | IIS is running on a primary or backup domain controller.<br>What was scanned How to correct this |
| ✱ | IIS Logging Enabled | Some web or FTP sites are not using the recommended logging options.<br>What was scanned Result details How to correct this |

**SQL Server Scan Results**

| Score | Issue | Result |
|---|---|---|
| | SQL Server/MSDE Status | SQL Server and/or MSDE is not installed on this computer. |

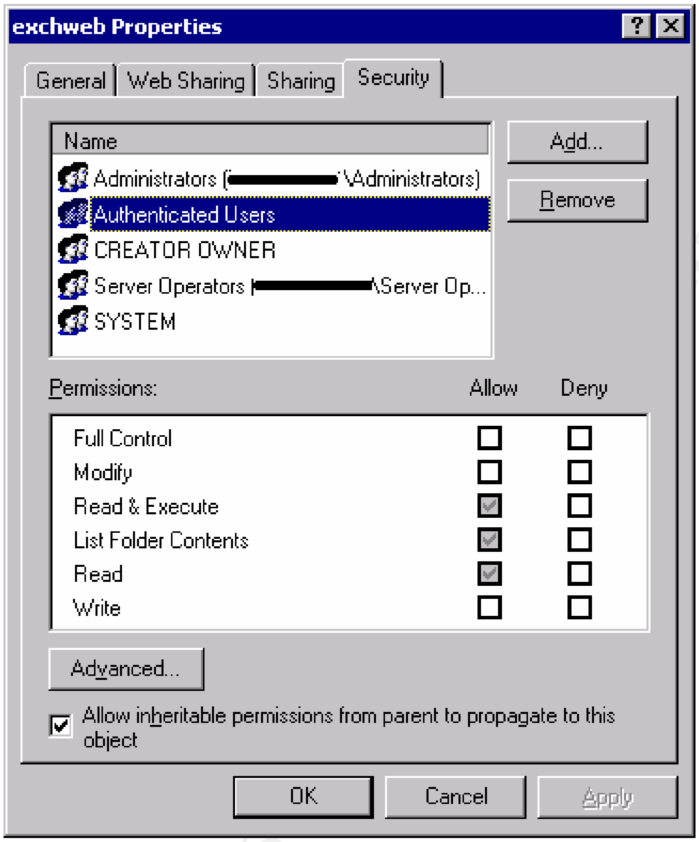
© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

### IIS2 – Check URLScan installation

Search for URLScan.ini was unsuccessful and no evidence about URLScan installation was found on the Exchange Back-end server. This might be because providing HTML access to user mail folders is not a required function for IIS on the Exchange Back-end server and IIS is running only to provide data to the OWA Front-end server.

### IIS3 – Check IIS virtual directories ACLs

Audit of IIS exchange web directory ACLs showed that the security permissions restrict access to Authenticated Users group on the /Exchweb directory.



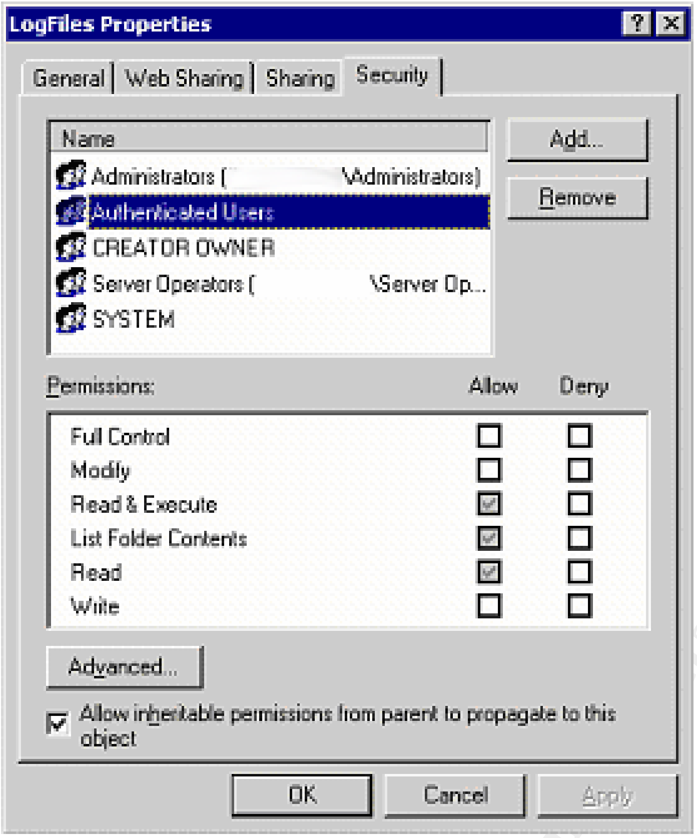
Name
- Administrators ([redacted]\Administrators)
- Authenticated Users
- CREATOR OWNER
- Server Operators ([redacted]\Server Op...
- SYSTEM

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Modify | □ | □ |
| Read & Execute | ☑ | □ |
| List Folder Contents | ☑ | □ |
| Read | ☑ | □ |
| Write | □ | □ |

☑ Allow inheritable permissions from parent to propagate to this object

### IIS4 – Check IIS Log files ACL

Audit of IIS Log files permissions shows that only administrators have full control over the log files. The rights of authenticated users have been set up to read-only access.



| Name |
|---|
| Administrators ( \Administrators) |
| Authenticated Users |
| CREATOR OWNER |
| Server Operators ( \Server Op... |
| SYSTEM |

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Modify | □ | □ |
| Read & Execute | ☑ | □ |
| List Folder Contents | ☑ | □ |
| Read | ☑ | □ |
| Write | □ | □ |

☑ Allow inheritable permissions from parent to propagate to this object

### IIS5 – Check IIS Sample application presence

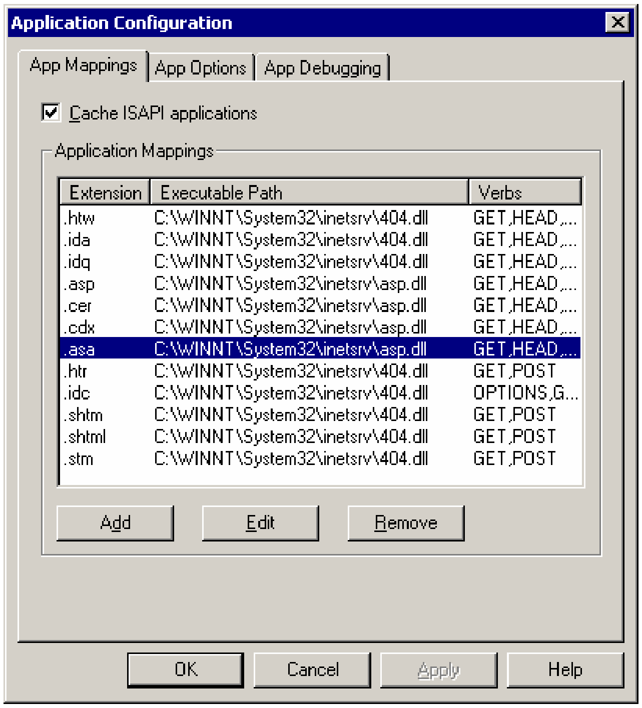
MBSA output shows that sample applications have been removed from the Exchange 2000 Back-end server (see IIS1 test results).

### IIS6 – Check IIS IISADMPWD directory presence

MBSA output shows that IISADMPWD directory has been removed from the Exchange 2000 Back-end server (see IIS1 test results)

### IIS7 – Check IIS ISAPI extension mappings

Test result shows that mapping of some unused IIS ISAPI extensions is handled by the 404.dll library. Anyway, these extensions were not unmapped - .cer ; .cdx ; .asa .



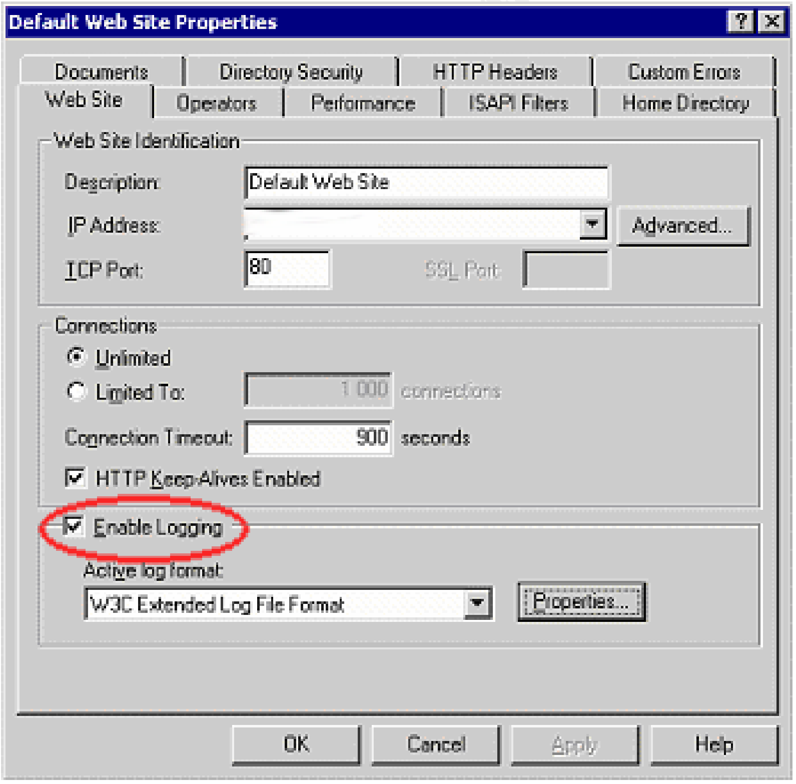
☑ Cache ISAPI applications

Application Mappings

| Extension | Executable Path | Verbs |
|---|---|---|
| .htw | C:\WINNT\System32\inetsrv\404.dll | GET,HEAD,... |
| .ida | C:\WINNT\System32\inetsrv\404.dll | GET,HEAD,... |
| .idq | C:\WINNT\System32\inetsrv\404.dll | GET,HEAD,... |
| .asp | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .cer | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .cdx | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .asa | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .htr | C:\WINNT\System32\inetsrv\404.dll | GET,POST |
| .idc | C:\WINNT\System32\inetsrv\404.dll | OPTIONS,G... |
| .shtm | C:\WINNT\System32\inetsrv\404.dll | GET,POST |
| .shtml | C:\WINNT\System32\inetsrv\404.dll | GET,POST |
| .stm | C:\WINNT\System32\inetsrv\404.dll | GET,POST |

## IIS8 – Check IIS logging

Audit shows that logging has been enabled for the IIS system including all recommended request details.



Web Site Identification

Description: Default Web Site

IP Address:

TCP Port: 80

SSL Port:

Connections

● Unlimited

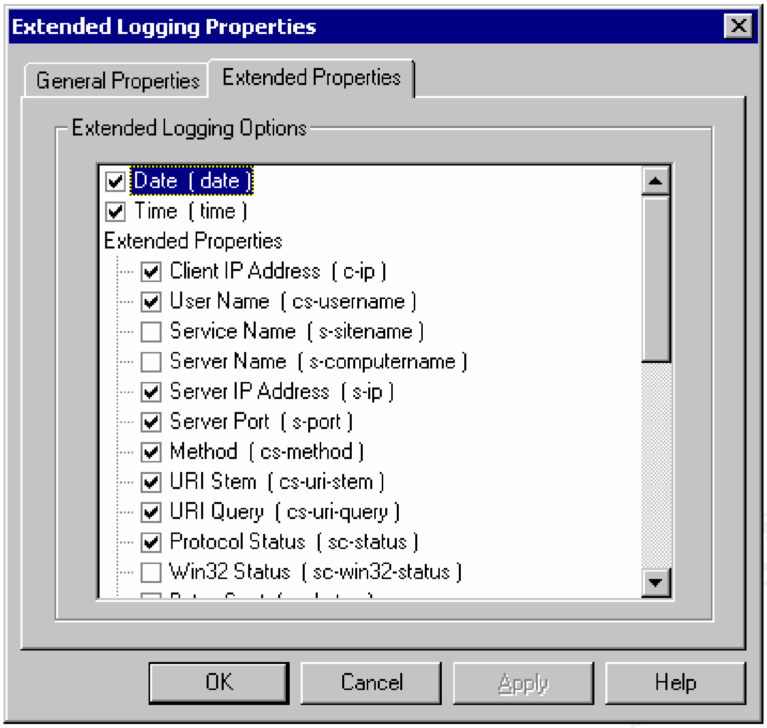
○ Limited To: 1 000 connections

Connection Timeout: 900 seconds

☑ HTTP Keep-Alives Enabled

☑ Enable Logging

Active log format: W3C Extended Log File Format

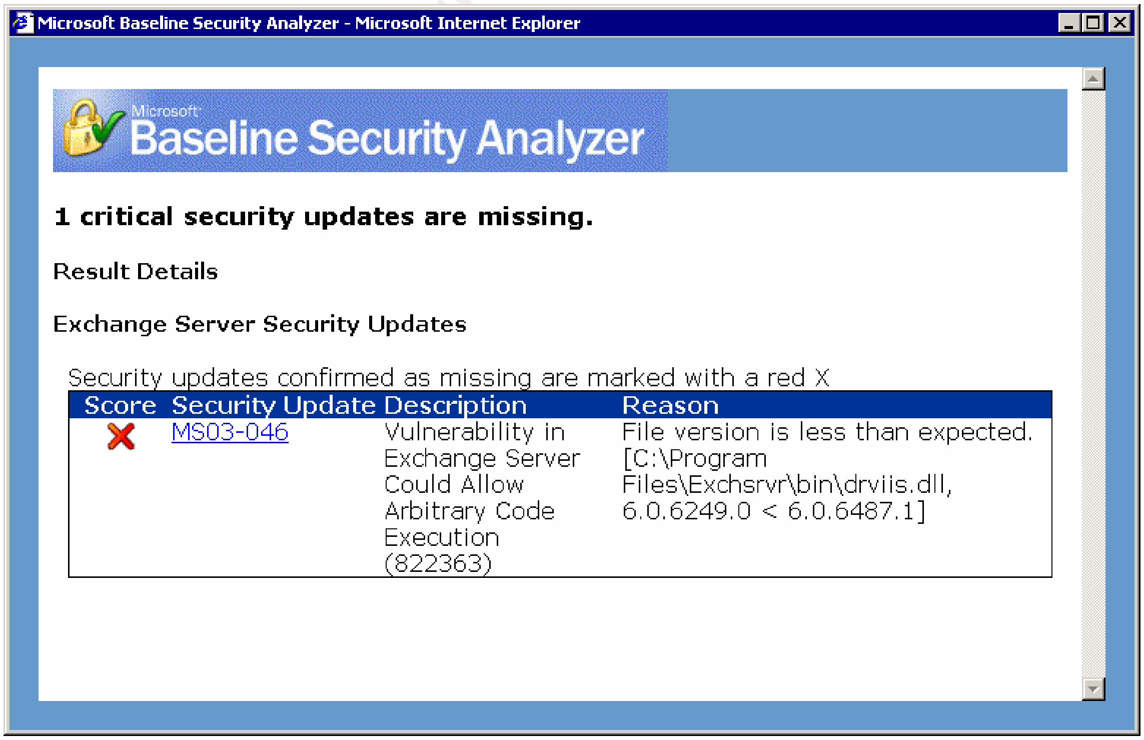


Extended Logging Options

- ☑ Date ( date )
- ☑ Time ( time )
- Extended Properties
  - ☑ Client IP Address ( c-ip )
  - ☑ User Name ( cs-username )
  - □ Service Name ( s-sitename )
  - □ Server Name ( s-computername )
  - ☑ Server IP Address ( s-ip )
  - ☑ Server Port ( s-port )
  - ☑ Method ( cs-method )
  - ☑ URI Stem ( cs-uri-stem )
  - ☑ URI Query ( cs-uri-query )
  - ☑ Protocol Status ( sc-status )
  - □ Win32 Status ( sc-win32-status )

### EXCH1 – Check latest Exchange 2000 Service pack and hotfixes

Audit through the MBSA showed, that one Exchange 2000 critical security update is missing, allowing arbitrary code execution. Microsoft recommendation is that administrators should apply the security patch to Exchange servers immediately.


Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Microsoft
Baseline Security Analyzer

**1 critical security updates are missing.**

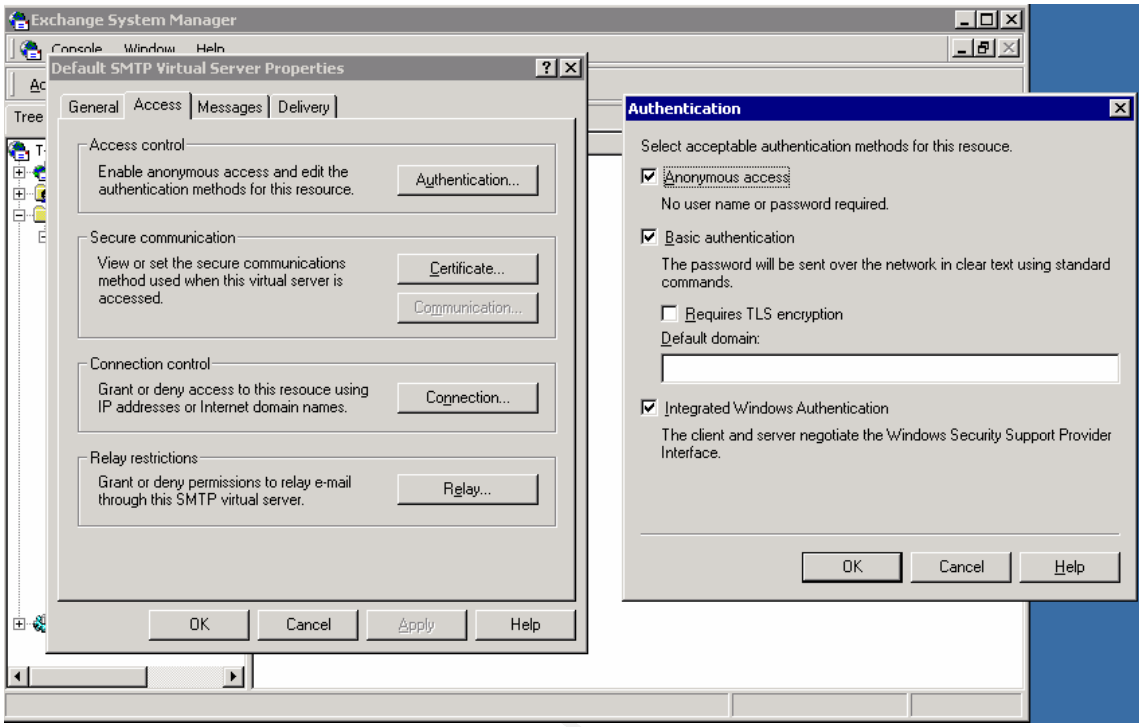
**Result Details**

**Exchange Server Security Updates**

Security updates confirmed as missing are marked with a red X

| Score | Security Update | Description | Reason |
|---|---|---|---|
| ✗ | MS03-046 | Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (822363) | File version is less than expected. [C:\Program Files\Exchsrvr\bin\drviis.dll, 6.0.6249.0 < 6.0.6487.1] |

Further audit showed, that Microsoft proposed workaround allowing only connections from SMTP servers that authenticate themselves was not applied.



Default SMTP Virtual Server Properties

Access control

Enable anonymous access and edit the authentication methods for this resource.

Secure communication

View or set the secure communications method used when this virtual server is accessed.

Connection control

Grant or deny access to this resouce using IP addresses or Internet domain names.

Relay restrictions

Grant or deny permissions to relay e-mail through this SMTP virtual server.

Authentication

Select acceptable authentication methods for this resouce.

☑ Anonymous access

No user name or password required.

☑ Basic authentication

The password will be sent over the network in clear text using standard commands.

☐ Requires TLS encryption

Default domain:

☑ Integrated Windows Authentication

The client and server negotiate the Windows Security Support Provider Interface.

## EXCH2 – Check running and disabled Exchange 2000 services

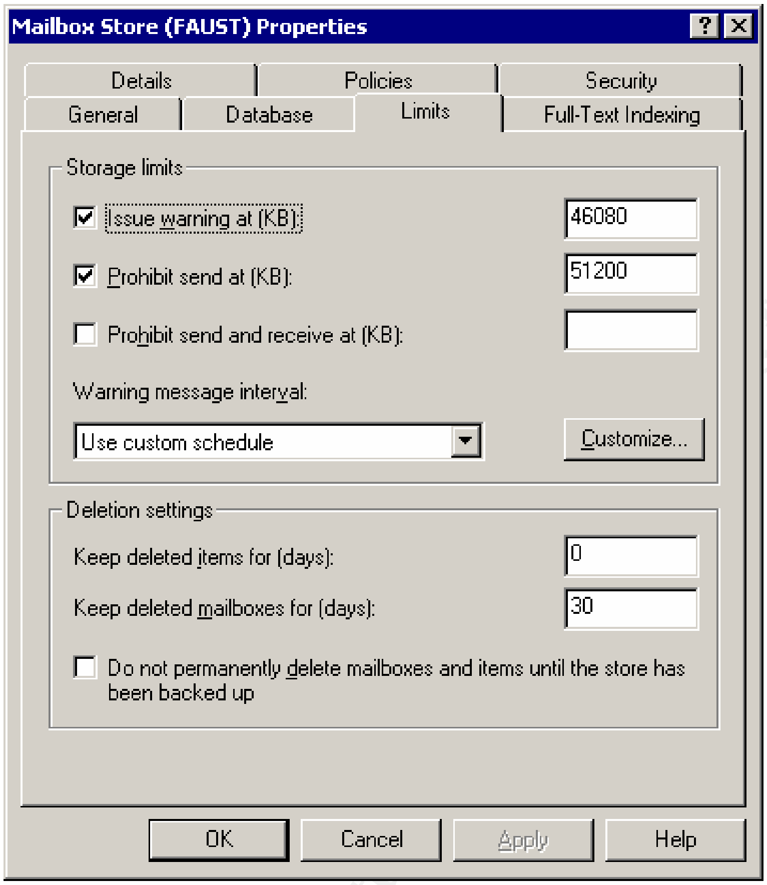
Audit of running Exchange 2000 services show that Exchange running services are set up according to the recommendations.

Two services, IMAP4 and POP3 are running because of corporate user requirements.

| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Microsoft Exchange Event | Monitors folders and fires events, for Exchange 5.5-compatible server applications. | | **Manual** | LocalSystem |
| Microsoft Exchange IMAP4 | Provides Microsoft Exchange IMAP4 Services. | Started | Automatic | LocalSystem |
| Microsoft Exchange Information Store | Manages Microsoft Exchange Information Storage | Started | Automatic | LocalSystem |
| Microsoft Exchange Management | Provides Microsoft Exchange management information through WMI. | Started | Automatic | LocalSystem |
| Microsoft Exchange MTA Stacks | Provides Microsoft Exchange X.400 services | Started | Automatic | LocalSystem |
| Microsoft Exchange POP3 | Provides Microsoft Exchange POP3 Services. | Started | Automatic | LocalSystem |
| Microsoft Exchange Routing Engine | Processes Microsoft Exchange routing information | Started | Automatic | LocalSystem |
| Microsoft Exchange Site Replication Service | | | **Disabled** | LocalSystem |
| Microsoft Exchange System Attendant | Provides system related services for Microsoft Exchange | Started | Automatic | LocalSystem |

## EXCH3 – Check Mailbox size limits

Check results show, that mailbox size limits have been implemented on the Exchange 2000 Back-end server.



Storage limits

☑ Issue warning at (KB): 46080

☑ Prohibit send at (KB): 51200

☐ Prohibit send and receive at (KB):

Warning message interval: Use custom schedule

Deletion settings

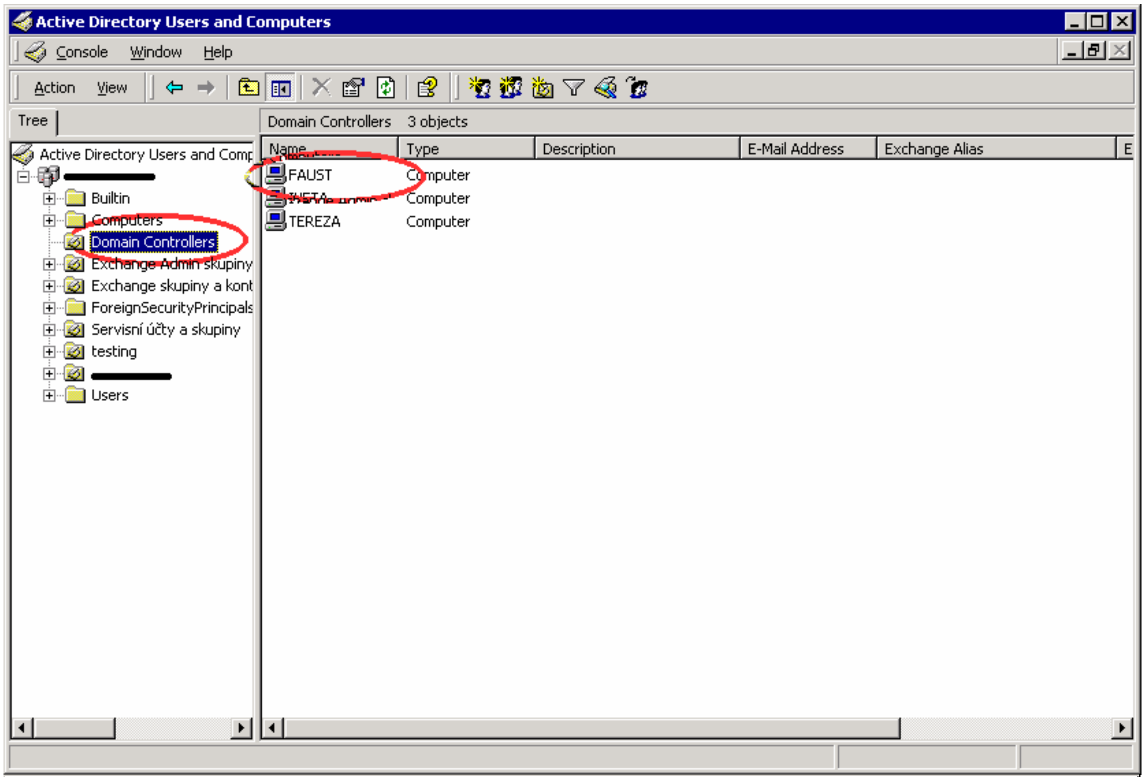
Keep deleted items for (days): 0

Keep deleted mailboxes for (days): 30

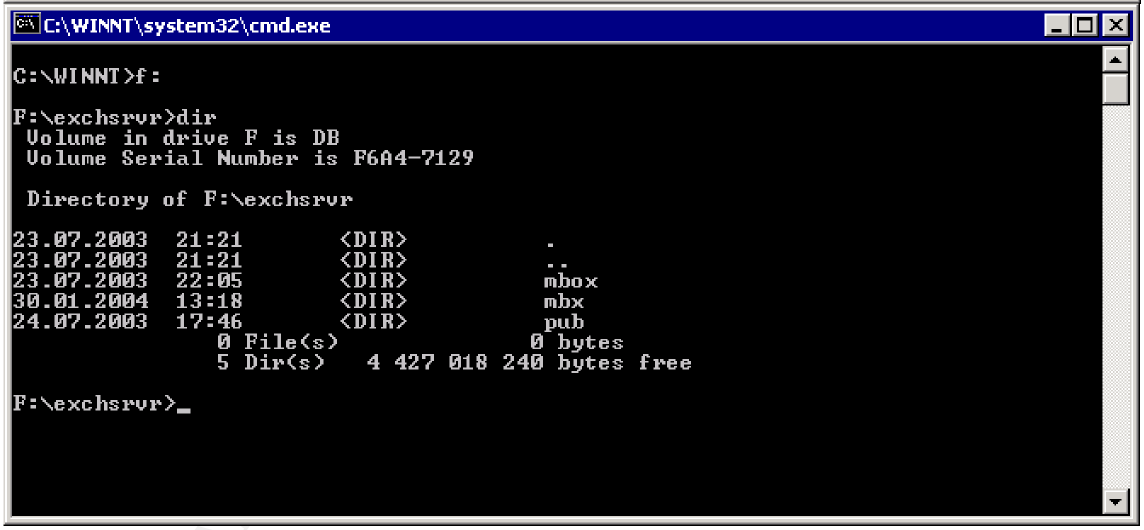
☐ Do not permanently delete mailboxes and items until the store has been backed up

## EXCH4 – Check Exchange directory location and access rights

Audit shows that the Exchange server is also one of the Domain controllers.
Exchange directory resides on a separate disc partition than the operating system. Because the system uses RAID with disc mirroring, the system and exchange partitions are not located on physically different discs.

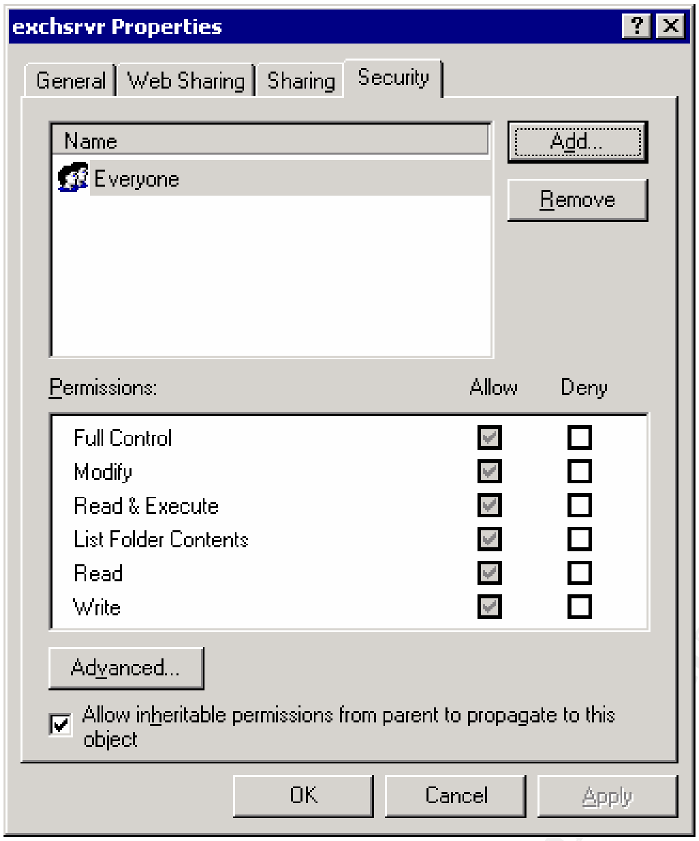


| Name | Type | Description | E-Mail Address | Exchange Alias | E |
|---|---|---|---|---|---|
| FAUST | Computer | | | | |
| [redacted] | Computer | | | | |
| TEREZA | Computer | | | | |



```
C:\WINNT>f:

F:\exchsrvr>dir
 Volume in drive F is DB
 Volume Serial Number is F6A4-7129

 Directory of F:\exchsrvr

23.07.2003  21:21       <DIR>          .
23.07.2003  21:21       <DIR>          ..
23.07.2003  22:05       <DIR>          mbox
30.01.2004  13:18       <DIR>          mbx
24.07.2003  17:46       <DIR>          pub
               0 File(s)              0 bytes
               5 Dir(s)   4 427 018 240 bytes free

F:\exchsrvr>_
```

Checking access permissions revealed that default permissions of the *\Exchsrvr* directory, which are set by Windows 2000 to full control for the EVERYONE group, were not changed.



Name

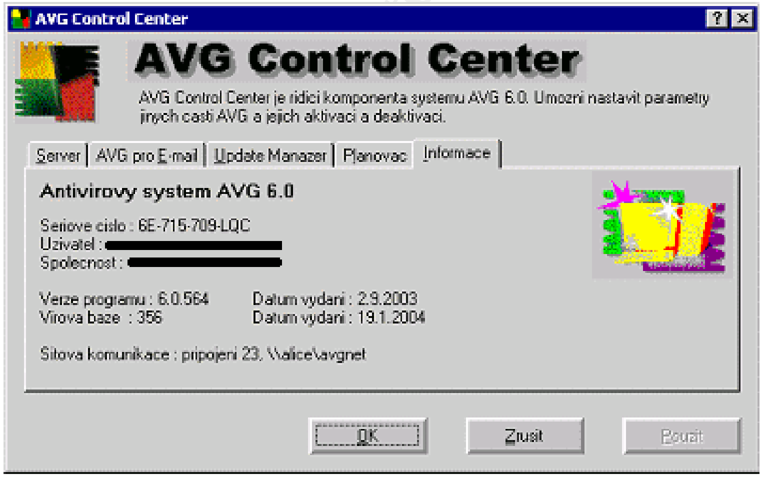
Everyone

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | ☑ | □ |
| Modify | ☑ | □ |
| Read & Execute | ☑ | □ |
| List Folder Contents | ☑ | □ |
| Read | ☑ | □ |
| Write | ☑ | □ |

☑ Allow inheritable permissions from parent to propagate to this object

## EXCH5 – Check antivirus software

Audit showed that antivirus program was running and the virus database was up-to-date.



AVG Control Center je ridici komponenta systemu AVG 6.0. Umozni nastavit parametry jinych casti AVG a jejich aktivaci a deaktivaci.

Antivirovy system AVG 6.0

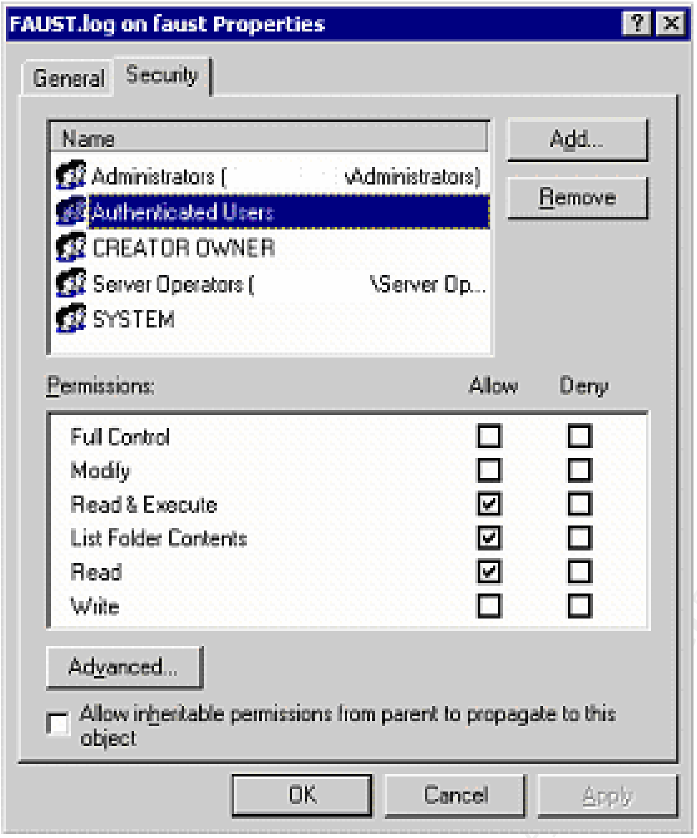
Seriove cislo : 6E-715-709-LQC
Uzivatel : [redacted]
Spolecnost : [redacted]

Verze programu : 6.0.564 Datum vydani : 2.9.2003
Virova baze : 356 Datum vydani : 19.1.2004

Sitova komunikace : pripojeni 23. \\alice\avgnet

## EXCH6 – Check Exchange logfile permissions

Audit of Exchange Log files permissions shows that only administrators have full control over the log files. The rights of authenticated users have been set up to read-only access.



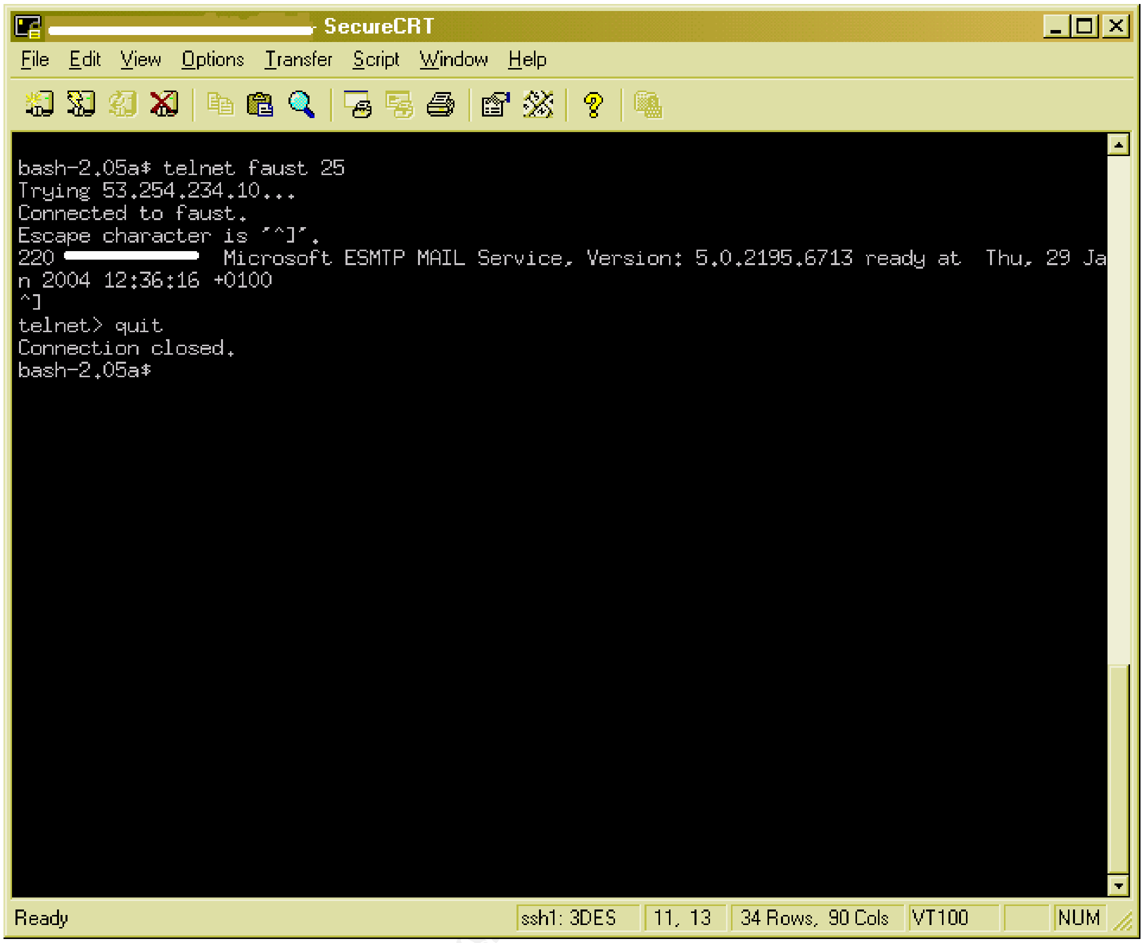
| Name |
|---|
| Administrators ( \Administrators) |
| Authenticated Users |
| CREATOR OWNER |
| Server Operators ( \Server Op... |
| SYSTEM |

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Modify | □ | □ |
| Read & Execute | ☑ | □ |
| List Folder Contents | ☑ | □ |
| Read | ☑ | □ |
| Write | □ | □ |

□ Allow inheritable permissions from parent to propagate to this object

## EXCH7 – Check if SMTP banner has been changed

Telnet to the TCP port 25 shows that SMTP Banner was not modified by the Exchange system administrators.

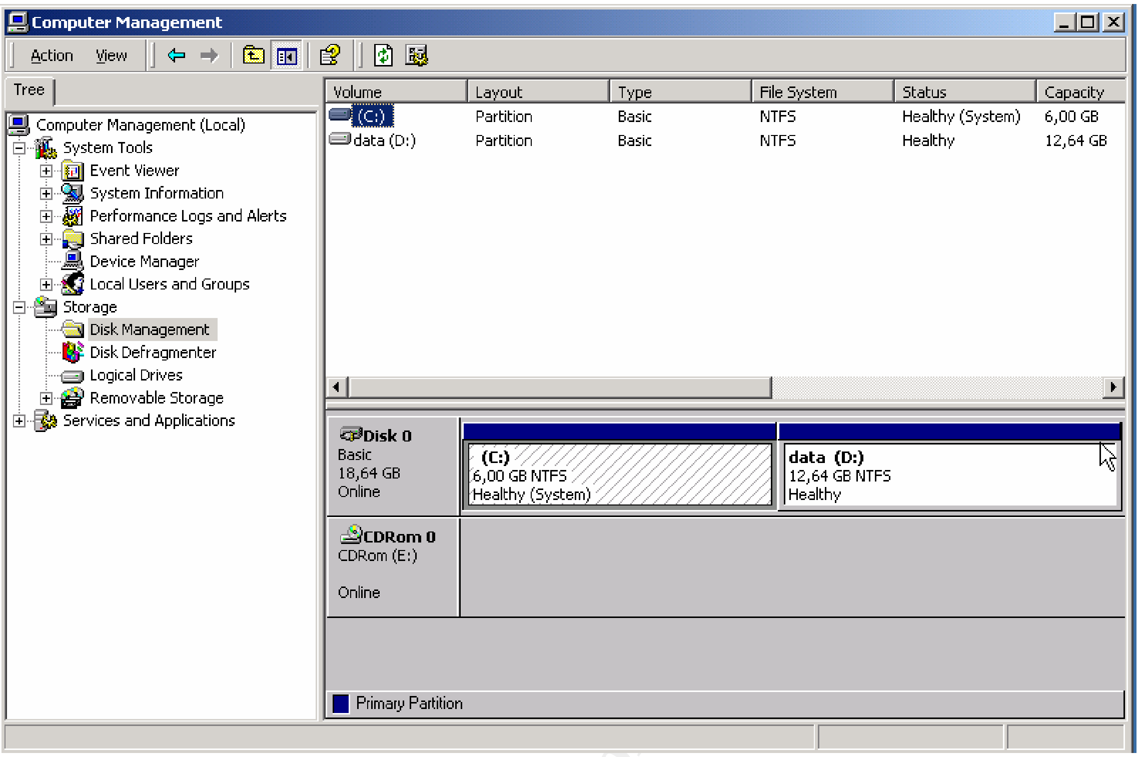


```
bash-2.05a$ telnet faust 25
Trying 53.254.234.10...
Connected to faust.
Escape character is '^]'.
220 [redacted]  Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at  Thu, 29 Ja
n 2004 12:36:16 +0100
^]
telnet> quit
Connection closed.
bash-2.05a$
```

## *Exchange Front-end server (OWA)*

### OS1 – Check NTFS disk format

Results of the audit show that there are two partitions on the audited system, both NTFS formatted.



| Volume | Layout | Type | File System | Status | Capacity |
|---|---|---|---|---|---|
| (C:) | Partition | Basic | NTFS | Healthy (System) | 6,00 GB |
| data (D:) | Partition | Basic | NTFS | Healthy | 12,64 GB |

Disk 0
Basic
18,64 GB
Online

(C:)
6,00 GB NTFS
Healthy (System)

data (D:)
12,64 GB NTFS
Healthy

CDRom 0
CDRom (E:)

Online

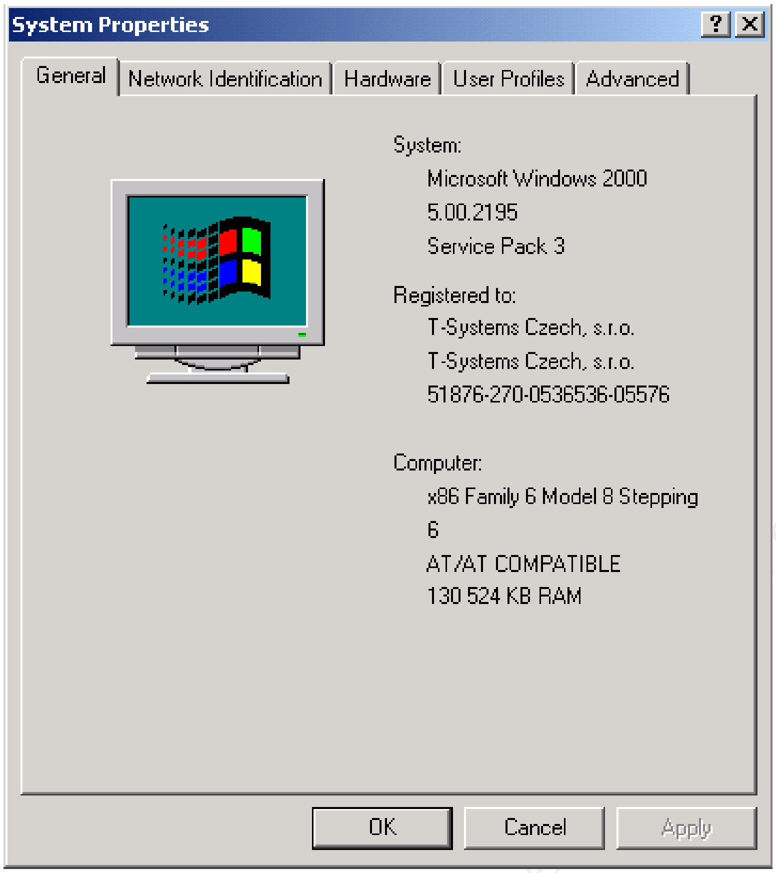
## OS2 – Check latest Service pack and security hotfixes

Audit of the Exchange Front-end server (OWA) revealed that the system is running with Service Pack 3.

The tests conducted with MBSA show that there are 32 operating system updates missing. Although the server is not directly exposed to the Internet, attacks from the internal network not only from the corporate users, but maybe from a virus or a Trojan horse – are possible.

One Critical Microsoft Virtual Machine security update is missing.

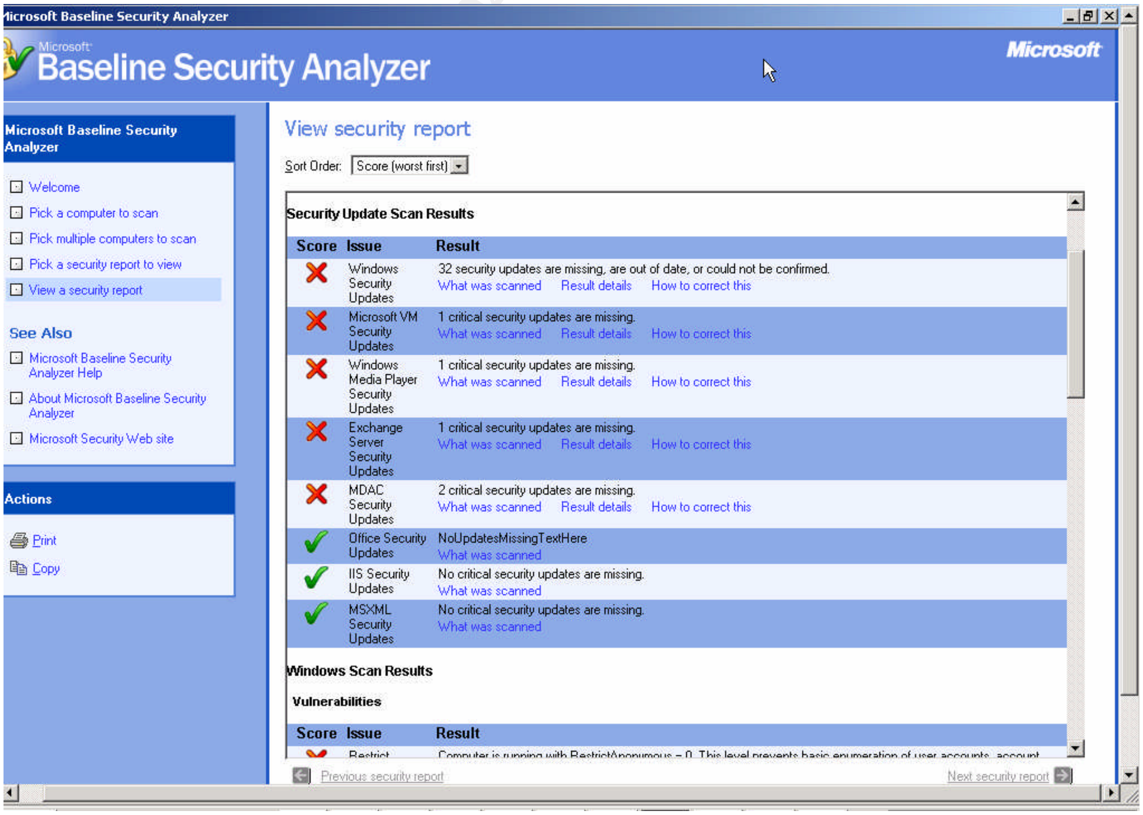
Fortunately, no IIS updates are missing; OWA server is reachable from the Internet and could be easily compromised.



System:
Microsoft Windows 2000
5.00.2195
Service Pack 3

Registered to:
T-Systems Czech, s.r.o.
T-Systems Czech, s.r.o.
51876-270-0536536-05576

Computer:
x86 Family 6 Model 8 Stepping
6
AT/AT COMPATIBLE
130 524 KB RAM



icrosoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
□ Welcome
□ Pick a computer to scan
□ Pick multiple computers to scan
□ Pick a security report to view
□ View a security report
See Also
□ Microsoft Baseline Security Analyzer Help
□ About Microsoft Baseline Security Analyzer
□ Microsoft Security Web site
Actions
Print
Copy

View security report

Sort Order: Score (worst first)

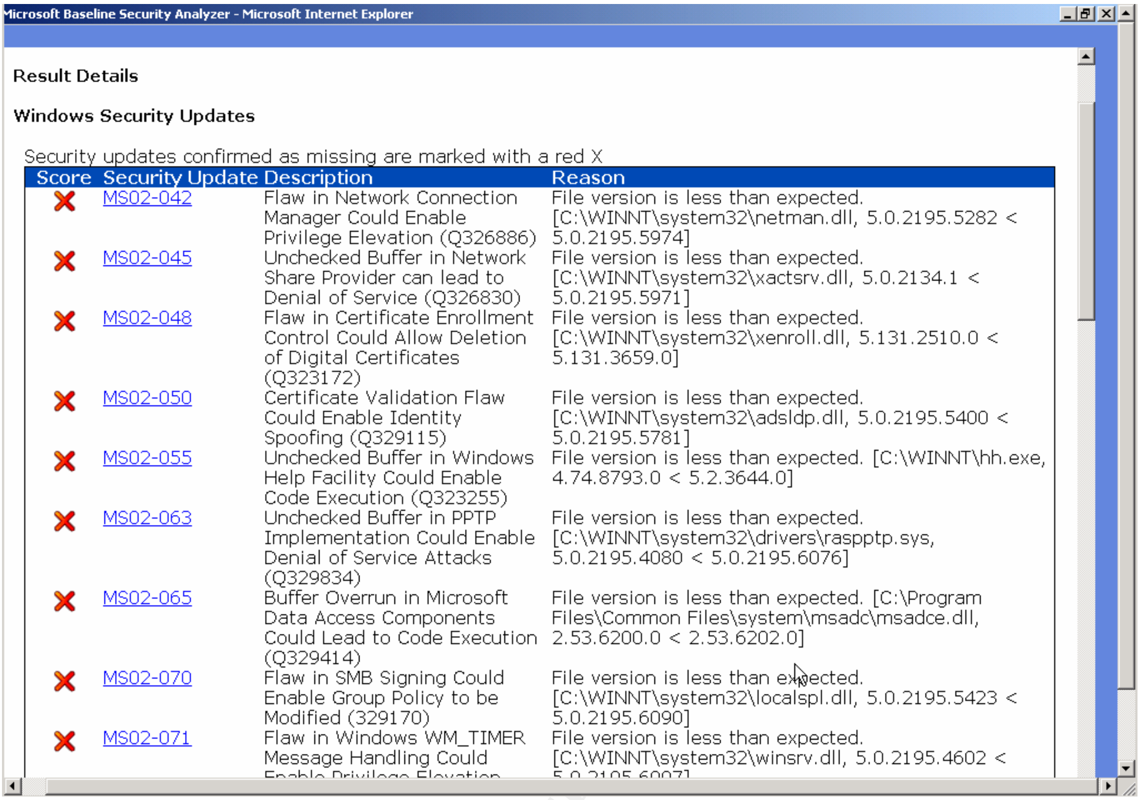
Security Update Scan Results

| Score | Issue | Result |
|---|---|---|
| ✗ | Windows Security Updates | 32 security updates are missing, are out of date, or could not be confirmed.<br>What was scanned   Result details   How to correct this |
| ✗ | Microsoft VM Security Updates | 1 critical security updates are missing.<br>What was scanned   Result details   How to correct this |
| ✗ | Windows Media Player Security Updates | 1 critical security updates are missing.<br>What was scanned   Result details   How to correct this |
| ✗ | Exchange Server Security Updates | 1 critical security updates are missing.<br>What was scanned   Result details   How to correct this |
| ✗ | MDAC Security Updates | 2 critical security updates are missing.<br>What was scanned   Result details   How to correct this |
| ✓ | Office Security Updates | NoUpdatesMissingTextHere<br>What was scanned |
| ✓ | IIS Security Updates | No critical security updates are missing.<br>What was scanned |
| ✓ | MSXML Security Updates | No critical security updates are missing.<br>What was scanned |

Windows Scan Results

Vulnerabilities

| Score | Issue | Result |
|---|---|---|
| ✗ | Restrict | Computer is running with RestrictAnonymous = 0. This level prevents basic enumeration of user accounts, account |



Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

Result Details

Windows Security Updates

Security updates confirmed as missing are marked with a red X

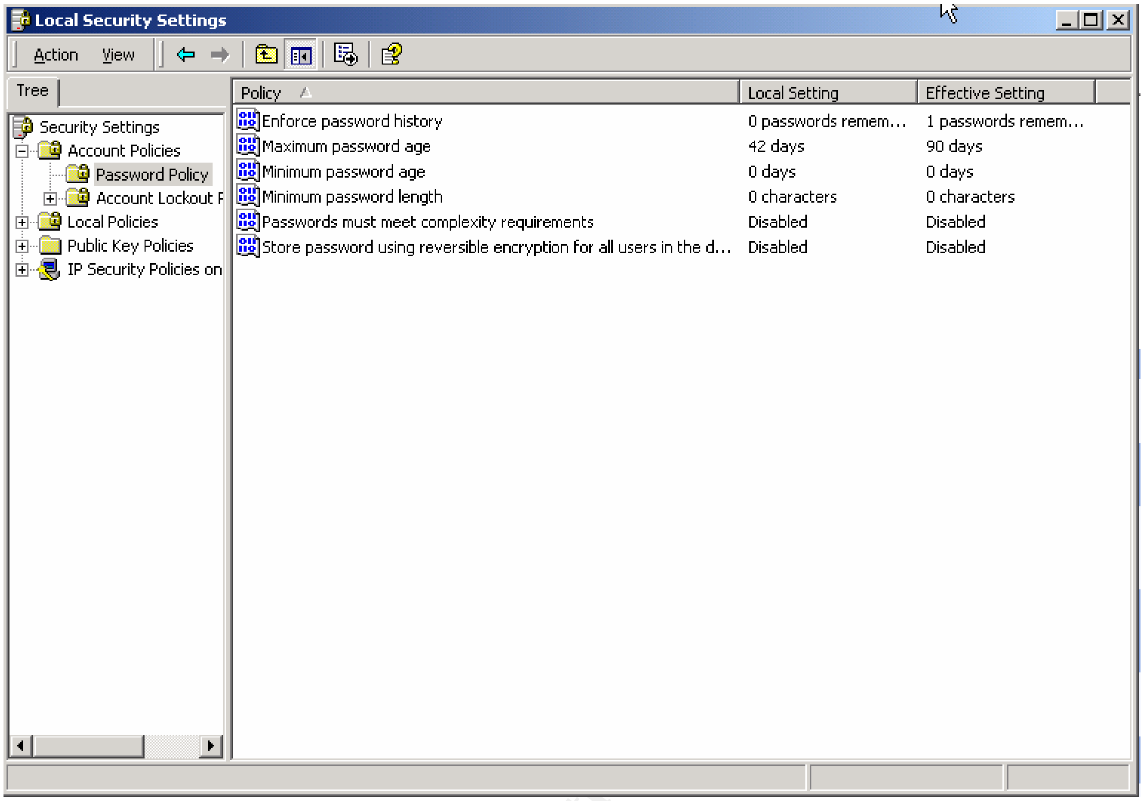
| Score | Security Update | Description | Reason |
|---|---|---|---|
| ✘ | MS02-042 | Flaw in Network Connection Manager Could Enable Privilege Elevation (Q326886) | File version is less than expected. [C:\WINNT\system32\netman.dll, 5.0.2195.5282 < 5.0.2195.5974] |
| ✘ | MS02-045 | Unchecked Buffer in Network Share Provider can lead to Denial of Service (Q326830) | File version is less than expected. [C:\WINNT\system32\xactsrv.dll, 5.0.2134.1 < 5.0.2195.5971] |
| ✘ | MS02-048 | Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172) | File version is less than expected. [C:\WINNT\system32\xenroll.dll, 5.131.2510.0 < 5.131.3659.0] |
| ✘ | MS02-050 | Certificate Validation Flaw Could Enable Identity Spoofing (Q329115) | File version is less than expected. [C:\WINNT\system32\adsldp.dll, 5.0.2195.5400 < 5.0.2195.5781] |
| ✘ | MS02-055 | Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255) | File version is less than expected. [C:\WINNT\hh.exe, 4.74.8793.0 < 5.2.3644.0] |
| ✘ | MS02-063 | Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks (Q329834) | File version is less than expected. [C:\WINNT\system32\drivers\raspptp.sys, 5.0.2195.4080 < 5.0.2195.6076] |
| ✘ | MS02-065 | Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414) | File version is less than expected. [C:\Program Files\Common Files\system\msadc\msadce.dll, 2.53.6200.0 < 2.53.6202.0] |
| ✘ | MS02-070 | Flaw in SMB Signing Could Enable Group Policy to be Modified (329170) | File version is less than expected. [C:\WINNT\system32\localspl.dll, 5.0.2195.5423 < 5.0.2195.6090] |
| ✘ | MS02-071 | Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation | File version is less than expected. [C:\WINNT\system32\winsrv.dll, 5.0.2195.4602 < 5.0.2195.6097] |

## OS3 – Check unnecessary accounts presence

No unnecessary accounts were found on the Exchange 2000 Back-end system.
Guest account has been disabled.

## OS4 – Check account password policy

Audit of the Exchange Front-end server showed that the password policy is not enforced on the reviewed system. Although administrators showed that they are aware of the need for complex passwords, there is no password policy enforced, not even on the OWA which is exposed to the Internet.

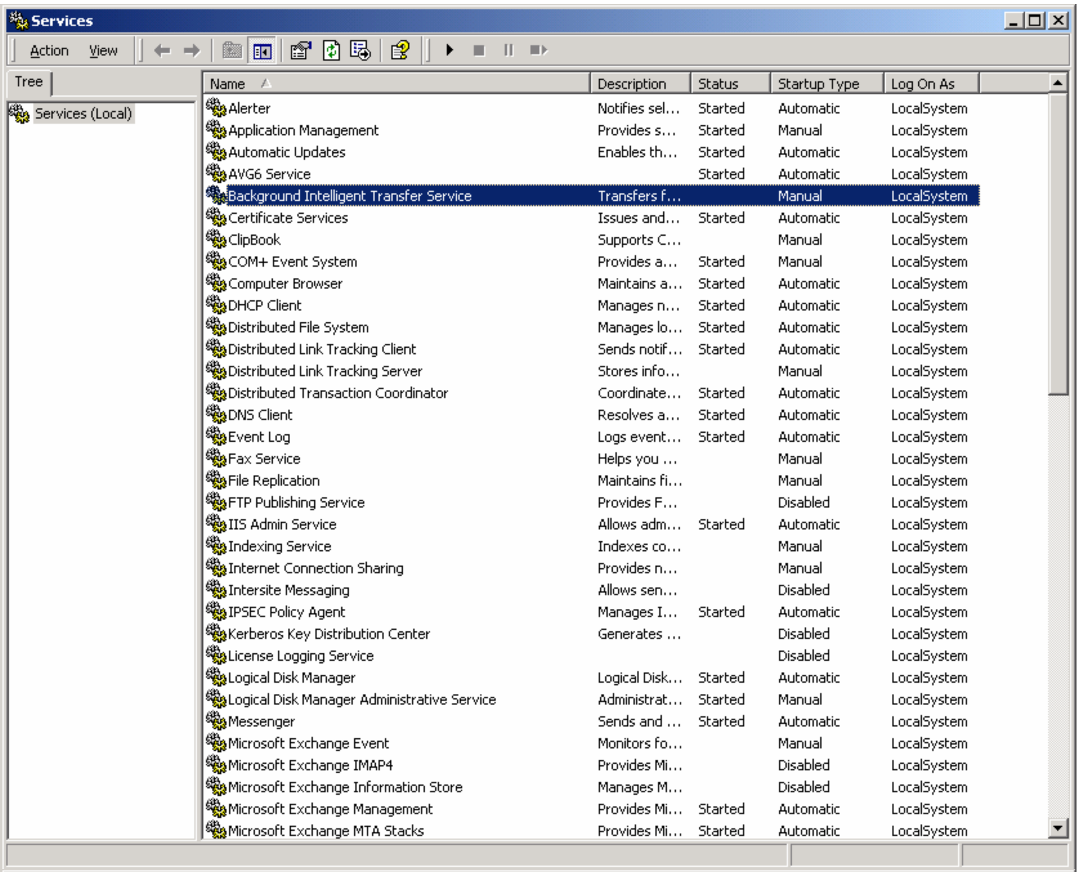


| Policy | Local Setting | Effective Setting |
|---|---|---|
| Enforce password history | 0 passwords remem... | 1 passwords remem... |
| Maximum password age | 42 days | 90 days |
| Minimum password age | 0 days | 0 days |
| Minimum password length | 0 characters | 0 characters |
| Passwords must meet complexity requirements | Disabled | Disabled |
| Store password using reversible encryption for all users in the d... | Disabled | Disabled |

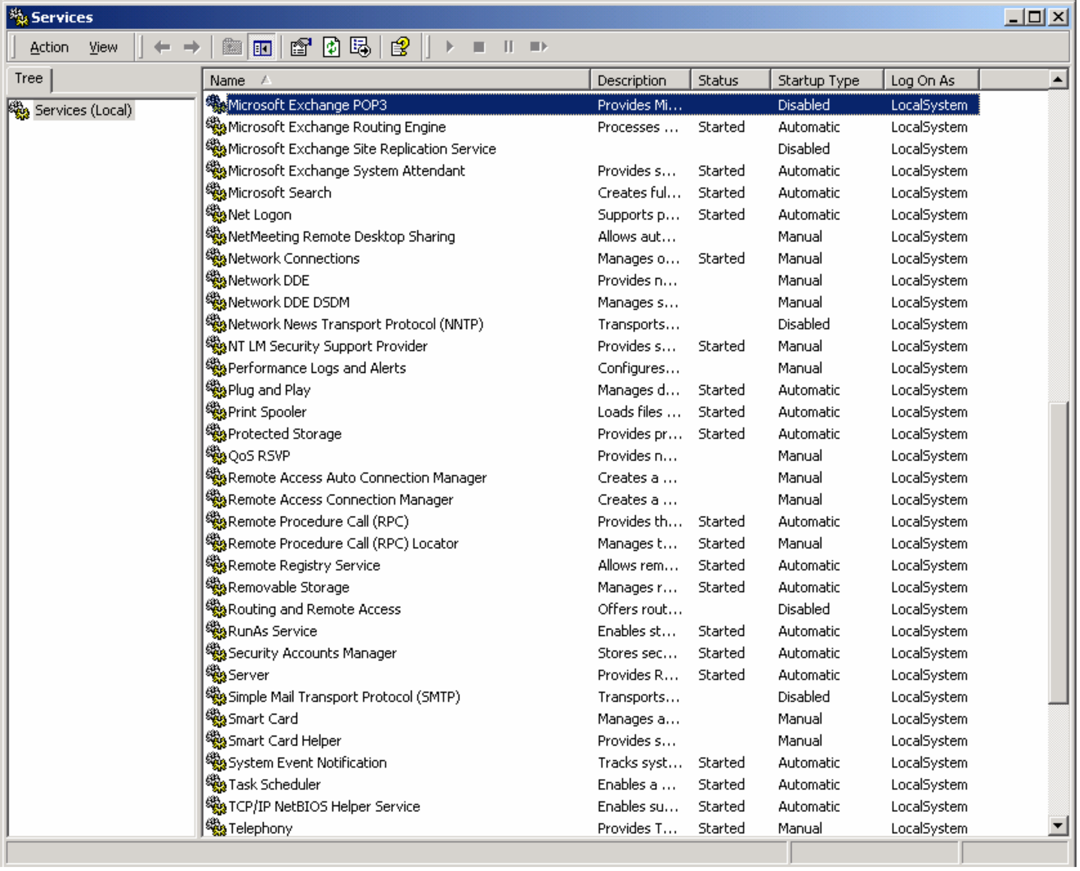
## OS5 – Check running and disabled services

Following table lists of running services was found on the Exchange 2000 Front-end server during the audit. Among others, these services could be stopped:

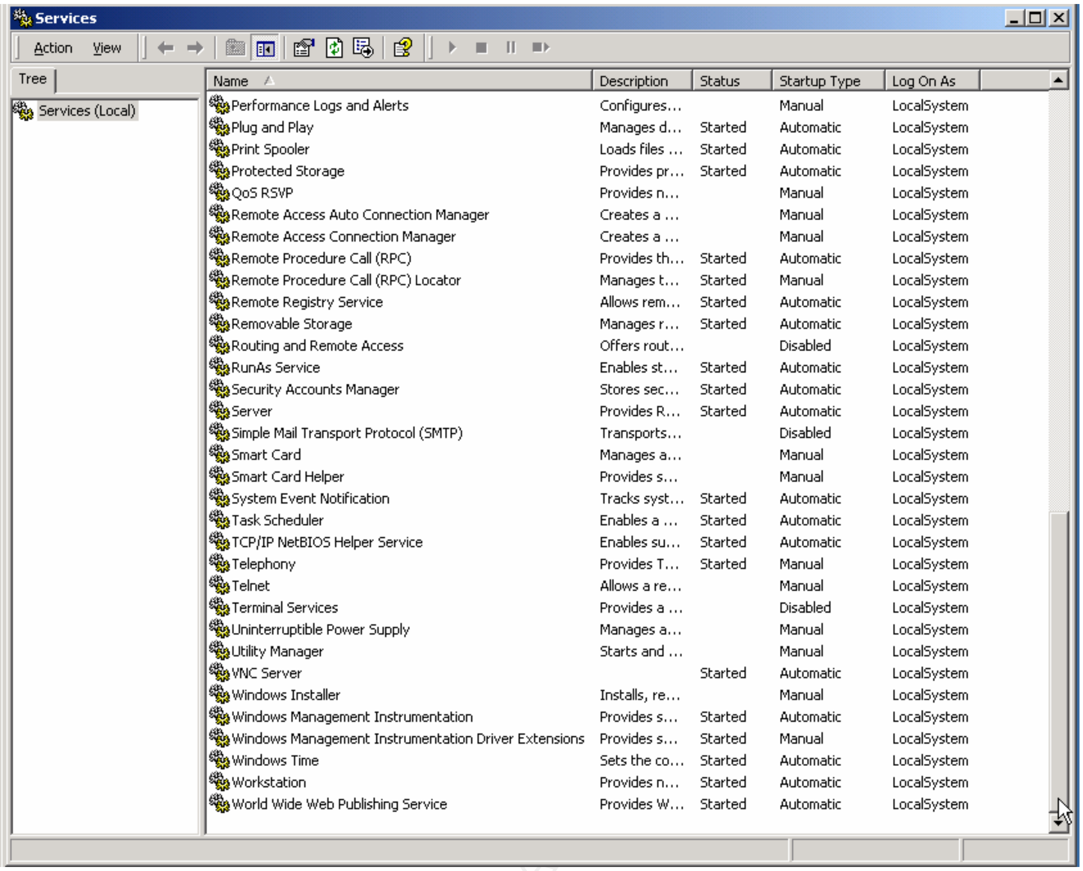
Alerter
Computer Browser
DHCP Client
Distributed File System
Messenger
Print Spooler
Protected Storage
Remote Registry Service
Removable Storage



| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Alerter | Notifies sel… | Started | Automatic | LocalSystem |
| Application Management | Provides s… | Started | Manual | LocalSystem |
| Automatic Updates | Enables th… | Started | Automatic | LocalSystem |
| AVG6 Service |  | Started | Automatic | LocalSystem |
| Background Intelligent Transfer Service | Transfers f… |  | Manual | LocalSystem |
| Certificate Services | Issues and… | Started | Automatic | LocalSystem |
| ClipBook | Supports C… |  | Manual | LocalSystem |
| COM+ Event System | Provides a… | Started | Manual | LocalSystem |
| Computer Browser | Maintains a… | Started | Automatic | LocalSystem |
| DHCP Client | Manages n… | Started | Automatic | LocalSystem |
| Distributed File System | Manages lo… | Started | Automatic | LocalSystem |
| Distributed Link Tracking Client | Sends notif… | Started | Automatic | LocalSystem |
| Distributed Link Tracking Server | Stores info… |  | Manual | LocalSystem |
| Distributed Transaction Coordinator | Coordinate… | Started | Automatic | LocalSystem |
| DNS Client | Resolves a… | Started | Automatic | LocalSystem |
| Event Log | Logs event… | Started | Automatic | LocalSystem |
| Fax Service | Helps you … |  | Manual | LocalSystem |
| File Replication | Maintains fi… |  | Manual | LocalSystem |
| FTP Publishing Service | Provides F… |  | Disabled | LocalSystem |
| IIS Admin Service | Allows adm… | Started | Automatic | LocalSystem |
| Indexing Service | Indexes co… |  | Manual | LocalSystem |
| Internet Connection Sharing | Provides n… |  | Manual | LocalSystem |
| Intersite Messaging | Allows sen… |  | Disabled | LocalSystem |
| IPSEC Policy Agent | Manages I… | Started | Automatic | LocalSystem |
| Kerberos Key Distribution Center | Generates … |  | Disabled | LocalSystem |
| License Logging Service |  |  | Disabled | LocalSystem |
| Logical Disk Manager | Logical Disk… | Started | Automatic | LocalSystem |
| Logical Disk Manager Administrative Service | Administrat… | Started | Manual | LocalSystem |
| Messenger | Sends and … | Started | Automatic | LocalSystem |
| Microsoft Exchange Event | Monitors fo… |  | Manual | LocalSystem |
| Microsoft Exchange IMAP4 | Provides Mi… |  | Disabled | LocalSystem |
| Microsoft Exchange Information Store | Manages M… |  | Disabled | LocalSystem |
| Microsoft Exchange Management | Provides Mi… | Started | Automatic | LocalSystem |
| Microsoft Exchange MTA Stacks | Provides Mi… | Started | Automatic | LocalSystem |



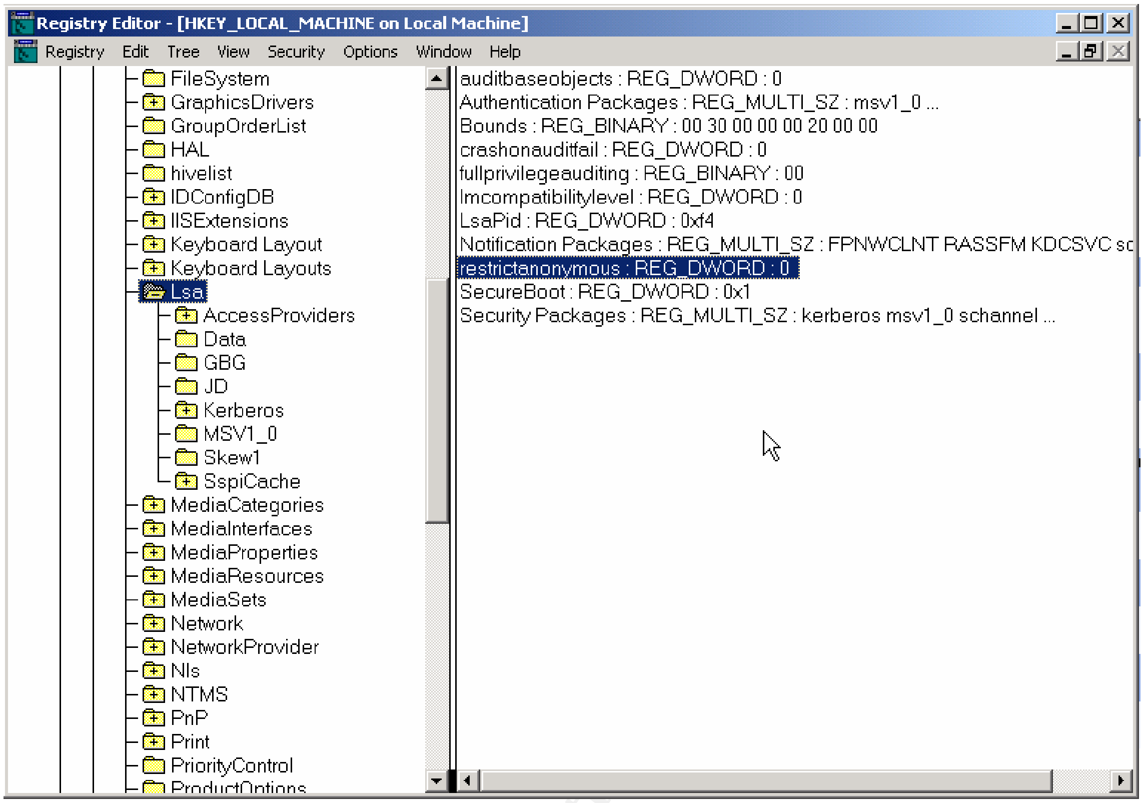
| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Microsoft Exchange POP3 | Provides Mi… |  | Disabled | LocalSystem |
| Microsoft Exchange Routing Engine | Processes … | Started | Automatic | LocalSystem |
| Microsoft Exchange Site Replication Service |  |  | Disabled | LocalSystem |
| Microsoft Exchange System Attendant | Provides s… | Started | Automatic | LocalSystem |
| Microsoft Search | Creates ful… | Started | Automatic | LocalSystem |
| Net Logon | Supports p… | Started | Automatic | LocalSystem |
| NetMeeting Remote Desktop Sharing | Allows aut… |  | Manual | LocalSystem |
| Network Connections | Manages o… | Started | Manual | LocalSystem |
| Network DDE | Provides n… |  | Manual | LocalSystem |
| Network DDE DSDM | Manages s… |  | Manual | LocalSystem |
| Network News Transport Protocol (NNTP) | Transports… |  | Disabled | LocalSystem |
| NT LM Security Support Provider | Provides s… | Started | Manual | LocalSystem |
| Performance Logs and Alerts | Configures… |  | Manual | LocalSystem |
| Plug and Play | Manages d… | Started | Automatic | LocalSystem |
| Print Spooler | Loads files … | Started | Automatic | LocalSystem |
| Protected Storage | Provides pr… | Started | Automatic | LocalSystem |
| QoS RSVP | Provides n… |  | Manual | LocalSystem |
| Remote Access Auto Connection Manager | Creates a … |  | Manual | LocalSystem |
| Remote Access Connection Manager | Creates a … |  | Manual | LocalSystem |
| Remote Procedure Call (RPC) | Provides th… | Started | Automatic | LocalSystem |
| Remote Procedure Call (RPC) Locator | Manages t… | Started | Manual | LocalSystem |
| Remote Registry Service | Allows rem… | Started | Automatic | LocalSystem |
| Removable Storage | Manages r… | Started | Automatic | LocalSystem |
| Routing and Remote Access | Offers rout… |  | Disabled | LocalSystem |
| RunAs Service | Enables st… | Started | Automatic | LocalSystem |
| Security Accounts Manager | Stores sec… | Started | Automatic | LocalSystem |
| Server | Provides R… | Started | Automatic | LocalSystem |
| Simple Mail Transport Protocol (SMTP) | Transports… |  | Disabled | LocalSystem |
| Smart Card | Manages a… |  | Manual | LocalSystem |
| Smart Card Helper | Provides s… |  | Manual | LocalSystem |
| System Event Notification | Tracks syst… | Started | Automatic | LocalSystem |
| Task Scheduler | Enables a … | Started | Automatic | LocalSystem |
| TCP/IP NetBIOS Helper Service | Enables su… | Started | Automatic | LocalSystem |
| Telephony | Provides T… | Started | Manual | LocalSystem |



| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Performance Logs and Alerts | Configures... | | Manual | LocalSystem |
| Plug and Play | Manages d... | Started | Automatic | LocalSystem |
| Print Spooler | Loads files ... | Started | Automatic | LocalSystem |
| Protected Storage | Provides pr... | Started | Automatic | LocalSystem |
| QoS RSVP | Provides n... | | Manual | LocalSystem |
| Remote Access Auto Connection Manager | Creates a ... | | Manual | LocalSystem |
| Remote Access Connection Manager | Creates a ... | | Manual | LocalSystem |
| Remote Procedure Call (RPC) | Provides th... | Started | Automatic | LocalSystem |
| Remote Procedure Call (RPC) Locator | Manages t... | Started | Manual | LocalSystem |
| Remote Registry Service | Allows rem... | Started | Automatic | LocalSystem |
| Removable Storage | Manages r... | Started | Automatic | LocalSystem |
| Routing and Remote Access | Offers rout... | | Disabled | LocalSystem |
| RunAs Service | Enables st... | Started | Automatic | LocalSystem |
| Security Accounts Manager | Stores sec... | Started | Automatic | LocalSystem |
| Server | Provides R... | Started | Automatic | LocalSystem |
| Simple Mail Transport Protocol (SMTP) | Transports... | | Disabled | LocalSystem |
| Smart Card | Manages a... | | Manual | LocalSystem |
| Smart Card Helper | Provides s... | | Manual | LocalSystem |
| System Event Notification | Tracks syst... | Started | Automatic | LocalSystem |
| Task Scheduler | Enables a ... | Started | Automatic | LocalSystem |
| TCP/IP NetBIOS Helper Service | Enables su... | Started | Automatic | LocalSystem |
| Telephony | Provides T... | Started | Manual | LocalSystem |
| Telnet | Allows a re... | | Manual | LocalSystem |
| Terminal Services | Provides a ... | | Disabled | LocalSystem |
| Uninterruptible Power Supply | Manages a... | | Manual | LocalSystem |
| Utility Manager | Starts and ... | | Manual | LocalSystem |
| VNC Server | | Started | Automatic | LocalSystem |
| Windows Installer | Installs, re... | | Manual | LocalSystem |
| Windows Management Instrumentation | Provides s... | Started | Automatic | LocalSystem |
| Windows Management Instrumentation Driver Extensions | Provides s... | Started | Manual | LocalSystem |
| Windows Time | Sets the co... | Started | Automatic | LocalSystem |
| Workstation | Provides n... | Started | Automatic | LocalSystem |
| World Wide Web Publishing Service | Provides W... | Started | Automatic | LocalSystem |

## OS6 – Check Anonymous Logon problems

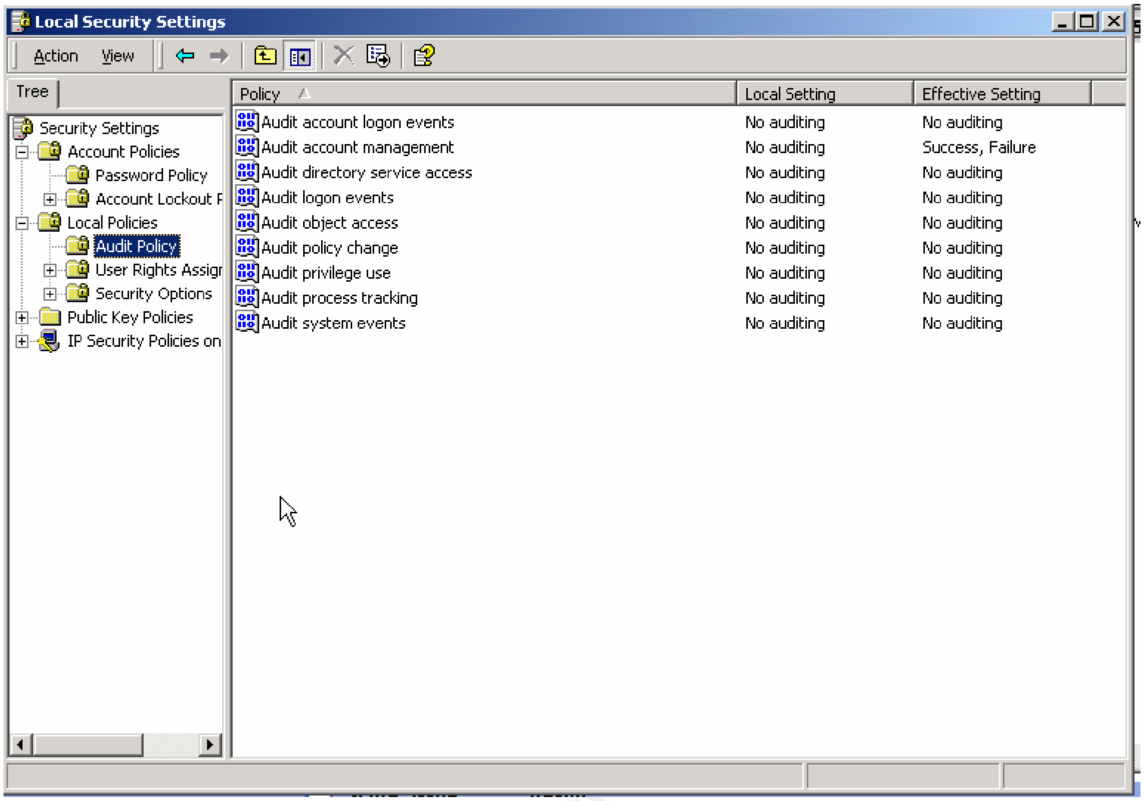
Audit showed that the *"RestrictAnonymous"* registry value is set to 0, which means that no restrictions concerning anonymous access to the registry are in place. This Allows collecting names of domain accounts and network shares. While this vulnerability does not allow an attacker to compromise the server, it could provide the attacker with additional information to mount an attack. To better secure anonymous access, this option can be changed through Group Policy or via the registry.



```
auditbaseobjects : REG_DWORD : 0
Authentication Packages : REG_MULTI_SZ : msv1_0 ...
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
crashonauditfail : REG_DWORD : 0
fullprivilegeauditing : REG_BINARY : 00
lmcompatibilitylevel : REG_DWORD : 0
LsaPid : REG_DWORD : 0xf4
Notification Packages : REG_MULTI_SZ : FPNWCLNT RASSFM KDCSVC sc
restrictanonymous : REG_DWORD : 0
SecureBoot : REG_DWORD : 0x1
Security Packages : REG_MULTI_SZ : kerberos msv1_0 schannel ...
```

## OS7 – CHECK OS logging

Checking operating system log settings showed that except of account management, no audit is set up. Because of that, no evidence of possible unauthorized activity is available.
For the OWA Front-end server, which is directly exposed to the Internet, it is very important to log and analyze details of the activity on the system.



| Policy | Local Setting | Effective Setting |
|---|---|---|
| Audit account logon events | No auditing | No auditing |
| Audit account management | No auditing | Success, Failure |
| Audit directory service access | No auditing | No auditing |
| Audit logon events | No auditing | No auditing |
| Audit object access | No auditing | No auditing |
| Audit policy change | No auditing | No auditing |
| Audit privilege use | No auditing | No auditing |
| Audit process tracking | No auditing | No auditing |
| Audit system events | No auditing | No auditing |

### OS8 – Run an outside network vulnerability scan

Following check result shows extract from Nessus security scan audit that was run on the audited Exchange Front-end server.
22 **high severity** problems that were found by Nessus are listed below.
Most of the vulnerabilities correspond to findings in the section covering missing operating system patches etc. Because of such a high number of High severity vulnerabilities, it would be better to patch the system fully first and then run the network scan by Nessus again. This would definitely provide more clear results about system threats.

# Network Vulnerability Assessment Report

**30.01.2004**

**Sorted by host names**

**Session name:** OWA

**Start Time:**30.01.2004 14:27:46
**Finish Time:**30.01.2004 16:11:39
**Elapsed:**0 day(s) 01:43:52

| | |
|---|---|
| **Total records generated:** | 109 |
| **High severity:** | 22 |
| **Low severity:** | 63 |
| **informational:** | 24 |

**Summary of scanned hosts**

| Host | Holes | Warnings | Open ports | State |
|---|---|---|---|---|
| webmail | 22 | 63 | 24 | Finished |

**Webmail**

| Service | Severity | Description |
|---|---|---|
| unknown (1052/udp) | **Info** | Port is open |
| netbios-ssn (139/tcp) | **Info** | Port is open |
| loc-srv (135/tcp) | **Info** | Port is open |
| microsoft-ds (445/tcp) | **Info** | Port is open |
| https (443/tcp) | **Info** | Port is open |
| http-rpc-epmap (593/tcp) | **Info** | Port is open |
| resvc (691/tcp) | **Info** | Port is open |
| unknown (1048/tcp) | **Info** | Port is open |
| unknown (1047/tcp) | **Info** | Port is open |
| unknown (1062/tcp) | **Info** | Port is open |
| unknown (1064/tcp) | **Info** | Port is open |
| unknown (1065/tcp) | **Info** | Port is open |
| unknown (1113/tcp) | **Info** | Port is open |
| unknown (1111/tcp) | **Info** | Port is open |
| msdtc (3372/tcp) | **Info** | Port is open |
| unknown (4858/tcp) | **Info** | Port is open |
| vnc-http (5800/tcp) | **Info** | Port is open |
| vnc (5900/tcp) | **Info** | Port is open |
| unknown (26383/tcp) | **Info** | Port is open |
| unknown (26382/tcp) | **Info** | Port is open |
| unknown (1112/udp) | **Info** | Port is open |
| unknown (1063/udp) | **Info** | Port is open |
| http (80/tcp) | **Info** | Port is open |
| netbios-ns (137/udp) | **Info** | Port is open |
| loc-srv (135/tcp) | **High** | The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. |

| | | |
|---|---|---|
| | | An attacker or a worm could use it to gain the control of this host.<br>Note that this is NOT the same bug as the one described in MS03-026 which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.<br>Solution: see http://www.microsoft.com/technet/security/bulletin/MS03-039.asp<br>Risk factor : High<br>CVE : CAN-2003-0715, CAN-2003-0528, CAN-2003-0605<br>BID : 8458<br>Other references : IAVA:2003-A-0012 |
| microsoft-ds (445/tcp) | **High** | A flaw in the Windows 2000 Network Connection Manager could enable privilege elevation.<br>Impact of vulnerability: Elevation of Privilege<br>Affected Software:  Microsoft Windows 2000<br>Recommendation: Users using any of the affected products should install the patch immediately.<br>Maximum Severity Rating: Critical<br>See http://www.microsoft.com/technet/security/bulletin/ms02-042.asp<br>Risk factor : High<br>CVE : CVE-2002-0720<br>BID : 5480 |
| https (443/tcp) | **High** | The file /iisadmpwd/aexp2.htr is present.<br>(or, aexp2b.htr, aexp3.htr, or aexp4.htr, search for aexp*.htr)<br>An attacker may use it in a brute force attack to gain valid username/password. A valid user may also use it to change his password on a locked account.<br>Solution : Delete the file<br>Risk factor : Serious<br>CVE : CVE-1999-0407, CAN-2002-0421<br>BID : 2110 |
| microsoft-ds (445/tcp) | **High** | The remote version of Windows has a flaw in the way the kernel passes error messages to a debugger. An attacker could exploit it to gain elevated privileges on this host.<br>To successfully exploit this vulnerability, an attacker would need a local account on this host.<br>Solution : see http://www.microsoft.com/technet/security/bulletin/MS03-013.asp |

|  |  |  |
|---|---|---|
|  |  | Risk factor : High<br>CVE : CAN-2003-0112<br>BID : 7370 |
| microsoft-ds (445/tcp) | **High** | A flaw exists in the RPC endpoint mapper, which can be used by an attacker to disable it remotely.<br><br>An attacker may use this flaw to prevent this host from working properly<br><br>Affected Software:<br>Microsoft Windows NT 4<br>Microsoft Windows 2000<br>Microsoft Windows XP<br><br>Solution for Win2k and XP: see http://www.microsoft.com/technet/security/bulletin/ms03-010.asp<br><br>There is no patch for NT4.<br><br>Microsoft strongly recommends that customers still using Windows NT 4.0 protect those systems by placing them behind a firewall which is filtering traffic on Port 135.<br><br>Risk factor : Serious<br>CVE : CAN-2002-1561 |
| microsoft-ds (445/tcp) | **High** | An unchecked buffer in Windows help could allow an attacker to could gain control over user's system.<br><br>Maximum Severity Rating: Critical<br><br>Recommendation: Customers should install the patch immediately.<br><br>Affected Software:<br>Microsoft Windows 98<br>Microsoft Windows 98 Second Edition<br>Microsoft Windows Millennium Edition<br>Microsoft Windows NT 4.0<br>Microsoft Windows NT 4.0, Terminal Server Edition<br>Microsoft Windows 2000<br>Microsoft Windows XP<br><br>See http://www.microsoft.com/technet/security/bulletin/ms02-055.asp<br><br>Risk factor : High<br>CVE : CAN-2002-0693, CAN-2002-0694 |
| microsoft-ds (445/tcp) | **High** | Hotfix to fix Certificate Validation Flaw (Q329115) is not installed.<br><br>The vulnerability could enable an attacker who had a valid end-entity certificate to issue a subordinate certificate that, although bogus, |

| | | |
|---|---|---|
| | | would nevertheless pass validation. Because CryptoAPI is used by a wide range of applications, this could enable a variety of identity spoofing attacks.<br>Impact of vulnerability: Identity spoofing.<br><br>Maximum Severity Rating: Critical<br><br>Recommendation: Administrators should install the patch immediately.<br><br>Affected Software:<br>Microsoft Windows 98<br>Microsoft Windows 98 Second Edition<br>Microsoft Windows Me<br>Microsoft Windows NT 4.0<br>Microsoft Windows NT 4.0, Terminal Server Edition<br>Microsoft Windows 2000<br>Microsoft Windows XP<br>Microsoft Office for Mac<br>Microsoft Internet Explorer for Mac<br>Microsoft Outlook Express for Mac<br><br>See http://www.microsoft.com/technet/security/bulletin/ms02-050.asp<br><br>Risk factor : High<br>CVE : CAN-2002-1183, CAN-2002-0862<br>BID : 5410 |
| microsoft-ds (445/tcp) | **High** | A vulnerability in the Certificate Enrollment ActiveX Control in Microsoft Windows 98, Windows 98 Second Edition, Windows Millennium, Windows NT 4.0, Windows 2000, and Windows XP allows remote attackers to delete digital certificates on a user's system via HTML.<br><br>Impact of vulnerability: Denial of service<br><br>Maximum Severity Rating: Critical<br><br>Recommendation: Customers should install the patch immediately<br><br>Affected Software:<br>Microsoft Windows 98<br>Microsoft Windows 98 Second Edition<br>Microsoft Windows Millennium<br>Microsoft Windows NT 4.0<br>Microsoft Windows 2000<br>Microsoft Windows XP<br><br>See http://www.microsoft.com/technet/security/bulletin/ms02-048.asp |

| | | |
|---|---|---|
| | | Risk factor : High<br>CVE : CAN-2002-0699 |
| microsoft-ds (445/tcp) | **High** | The remote host is vulnerable to a denial of service attack, which could allow an attacker to crash it by sending a specially crafted SMB (Server Message Block) request to it.<br><br>Impact of vulnerability: Denial of Service / Elevation of Privilege<br><br>Maximum Severity Rating: Moderate<br><br>Solution : http://www.microsoft.com/technet/security/bulletin/ms02-045.asp<br><br>Risk factor : High<br>CVE : CAN-2002-0724<br>BID : 5556 |
| microsoft-ds (445/tcp) | **High** | It was possible to log into the remote host using a NULL session.<br>The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access<br><br>To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$<br>Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html<br><br>All the smb tests will be done as "/" in domain XYZXYZ<br>CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117<br>BID : 494, 990 |
| microsoft-ds (445/tcp) | **High** | Remote Data Protocol (RDP) version 5.0 in Microsoft Windows 2000 and RDP 5.1 in Windows XP does not encrypt the checksums of plaintext session data, which could allow a remote attacker to determine the contents of encrypted sessions via sniffing, and Remote Data Protocol (RDP) version 5.1 in Windows XP allows remote attackers to cause a denial of service (crash) when Remote Desktop is enabled via a PDU Confirm Active data packet that does not set the Pattern BLT command.<br><br>Impact of vulnerability: Two vulnerabilities:<br>information disclosure, denial of service.<br><br>Maximum Severity Rating: Moderate.<br><br>Recommendation: Administrators of Windows 2000 terminal servers and Windows XP users who have enabled Remote Desktop should apply the patch.<br><br>Affected Software: |

| | | |
|---|---|---|
| | | Microsoft Windows 2000<br>Microsoft Windows XP<br><br>See<br>http://www.microsoft.com/technet/security/bulletin/ms02-051.asp<br><br>Risk factor : High<br>CVE : CAN-2002-0863<br>BID : 5410 |
| http (80/tcp) | **High** | The IIS server appears to have the .HTR ISAPI filter mapped.<br><br>At least one remote vulnerability has been discovered for the .HTR filter. This is detailed in Microsoft Advisory MS02-018, and gives remote SYSTEM level access to the web server.<br><br>It is recommended that, even if you have patched this vulnerability, you unmap the .HTR extension and any other unused ISAPI extensions if they are not required for the operation of your site.<br><br>Solution :<br>To unmap the .HTR extension:<br>1.Open Internet Services Manager.<br>2.Right-click the Web server choose Properties from the context menu.<br>3.Master Properties<br>4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .htr from the list.<br><br>In addition, you may wish to download and install URLSCAN from the Microsoft Technet Website. URLSCAN, by default, blocks all requests for .htr files.<br><br>Risk factor : High<br>CVE : CVE-2002-0071<br>BID : 4474 |
| https (443/tcp) | **High** | The IIS server appears to have the .HTR ISAPI filter mapped.<br><br>At least one remote vulnerability has been discovered for the .HTR filter. This is detailed in Microsoft Advisory MS02-018, and gives remote SYSTEM level access to the web server.<br><br>It is recommended that, even if you have patched this vulnerability, you unmap the .HTR extension and any other unused ISAPI extensions if they are not required for the operation of your site.<br><br>Solution :<br>To unmap the .HTR extension:<br>1.Open Internet Services Manager.<br>2.Right-click the Web server choose Properties from the context menu. |

| | | |
|---|---|---|
| | | 3.Master Properties<br>4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .htr from the list.<br><br>In addition, you may wish to download and install URLSCAN from the Microsoft Technet Website. URLSCAN, by default, blocks all requests for .htr files.<br><br>Risk factor : High<br>CVE : CVE-2002-0071<br>BID : 4474 |
| microsoft-ds (445/tcp) | **High** | Hotfix to fix Unchecked Buffer in PPTP Implementation (Q329834) is not installed.<br><br>A security vulnerability results in the Windows 2000 and Windows XP implementations because of an unchecked buffer in a section of code that processes the control data used to establish, maintain and tear down PPTP connections. By delivering specially malformed PPTP control data to an affected server, an attacker could corrupt kernel memory and cause the system to fail, disrupting any work in progress on the system.<br><br>Impact of vulnerability: Denial of service<br>Maximum Severity Rating: Critical<br><br>Recommendation: Administrators should install the patch immediately.<br><br>Affected Software:<br>Microsoft Windows 2000<br>Microsoft Windows XP<br><br>See http://www.microsoft.com/technet/security/bulletin/ms02-063.asp<br><br>Risk factor : High<br>CVE : CAN-2002-1214 |
| microsoft-ds (445/tcp) | **High** | The remote Windows 2000 does not have the Service Pack 4 applied. (it uses Service Pack 3 instead) You should apply it to be up-to-date<br><br>Risk factor : High<br>Solution : go to http://www.microsoft.com/windows2000/downloads/<br>CVE : CAN-1999-0662<br>BID : 7930, 8090, 8128, 8154 |
| microsoft-ds (445/tcp) | **High** | A security issue has been identified in WM_TIMER that could allow an attacker to compromise a computer running Microsoft Windows and gain complete control over it.<br><br>Recommendation: Users using any of the affected products should install the patch immediately. |

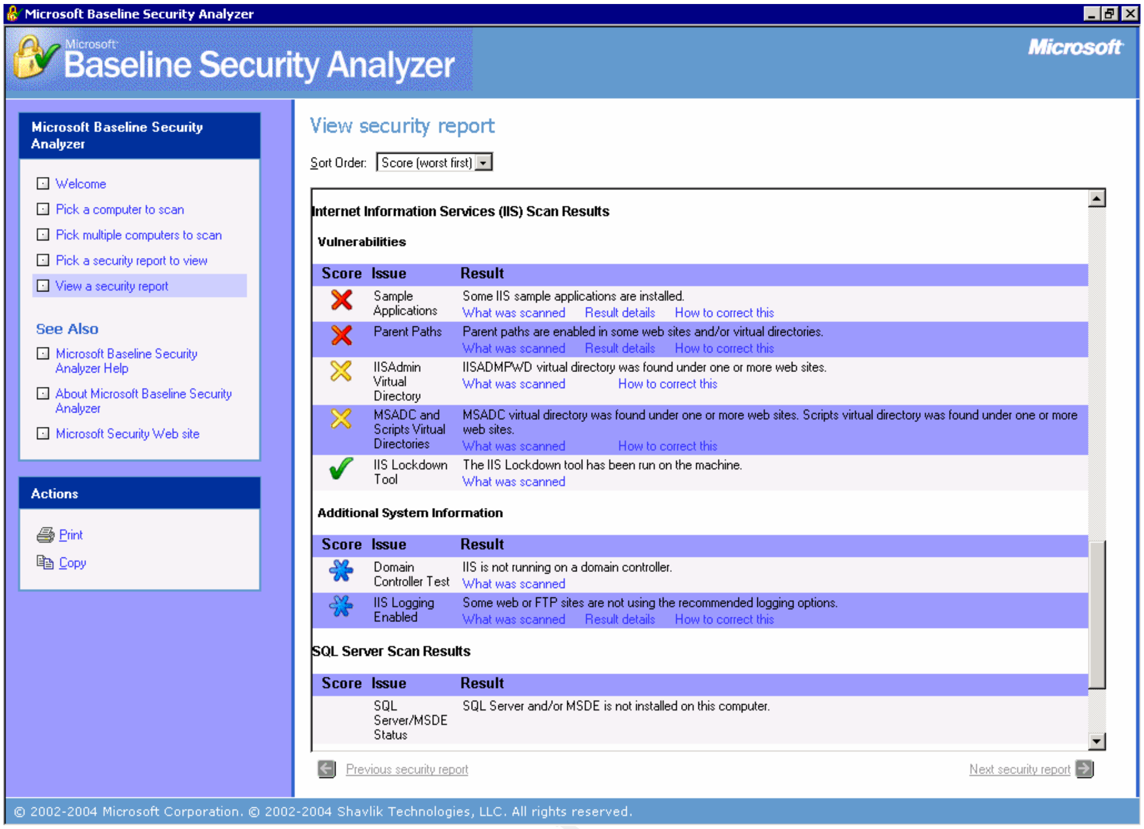
| | | |
|---|---|---|
| | | Maximum Severity Rating: Critical<br><br>Affected Software:<br>Microsoft Windows NT 4.0<br>Microsoft Windows NT 4.0, Terminal Server Edition<br>Microsoft Windows 2000<br>Microsoft Windows XP<br><br>See http://www.microsoft.com/technet/security/bulletin/ms02-071.asp<br><br>Risk factor : High<br>CVE : CAN-2002-1230<br>BID : 5927 |
| microsoft-ds (445/tcp) | **High** | The following shares can be accessed using a NULL session :<br>- E - (readable?, writeable?)<br><br>Solution : To restrict their access under WindowsNT, open the explorer, do a right click on each,<br>go to the 'sharing' tab, and click on 'permissions'<br>Risk factor : High<br>CVE : CAN-1999-0519, CAN-1999-0520<br>BID : 8026 |
| microsoft-ds (445/tcp) | **High** | A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack.<br><br>This plugin determined by reading the remote registry that the patch MS03-043 has not been applied.<br><br>Solution : see<br>http://www.microsoft.com/technet/security/bulletin/ms03-043.asp<br><br>Risk factor : High<br>CVE : CAN-2003-0717<br>BID : 8826<br>Other references : IAVA:2003-B-0007 |
| microsoft-ds (445/tcp) | **High** | The remote host is running a version of Windows with a version of DirectX which is vulnerable to a buffer overflow in the module which handles MIDI files.<br><br>To exploit this flaw, an attacker needs to craft a rogue MIDI file and send it to a user of this computer. When the user attempts to read the file, it will trigger the buffer overflow condition and the attacker may gain a shell on this host. |

|  |  |  |
|---|---|---|
|  |  | Solution : see<br>http://www.microsoft.com/technet/security/bulletin/MS03-030.asp<br>Risk factor : High<br>CVE : CAN-2003-0346<br>BID : 7370<br>Other references : IAVA:2003-A-0024 |
| microsoft-ds (445/tcp) | **High** | The Microsoft Locate service is a name server that maps logical names to network-specific names.<br><br>There is a security vulnerability in this server which allows an attacker to execute arbitrary code in it by sending a specially crafted packet to it.<br><br>Maximum Severity Rating: Critical<br><br>Recommendation: Administrators should install the patch immediately.<br><br>Affected Software:<br>Microsoft Windows NT 4.0<br>Microsoft Windows NT 4.0, Terminal Server Edition<br>Microsoft Windows 2000<br>Microsoft Windows XP<br><br>See<br>http://www.microsoft.com/technet/security/bulletin/ms03-001.asp<br><br>Risk factor : High<br>CVE : CAN-2003-0003<br>Other references : IAVA:2003-A-0007 |
| microsoft-ds (445/tcp) | **High** | Hotfix to fix Flaw in Microsoft VM<br>could Allow Code Execution (810030)<br><br>Impact of vulnerability: Three vulnerabilities, the most serious of which could enable an attacker to gain complete control over a user's system.<br><br>Maximum Severity Rating: Critical<br><br>Recommendation: Administrators should install the patch immediately.<br><br>Affected Software:<br><br>Versions of the Microsoft virtual machine (Microsoft VM) are identified by build numbers, which can be determined using the JVIEW tool as discussed in the FAQ. All builds of the Microsoft VM up to and including build 5.0.3805 are affected by these vulnerabilities. |

| | | |
|---|---|---|
| | | Supersedes :<br>http://www.microsoft.com/technet/security/bulletin/ms02-052.asp<br><br>See: http://www.microsoft.com/technet/security/bulletin/ms02-069.asp<br><br>Also Note: Requires full registry access (Administrator) to run the test.<br><br>Risk factor : High<br>CVE : CAN-2002-1257, CAN-2002-1258, CAN-2002-1183, CAN-2002-0862 |
| http (80/tcp) | **High** | The file /iisadmpwd/aexp2.htr is present.<br>(or, aexp2b.htr, aexp3.htr, or aexp4.htr, search for aexp*.htr)<br><br>An attacker may use it in a brute force attack to gain valid username/password. A valid user may also use it to change his password on a locked account.<br><br>Solution : Delete the file<br>Risk factor : Serious<br>CVE : CVE-1999-0407, CAN-2002-0421<br>BID : 2110 |

## IIS1 – Check IIS Lockdown tool implementation

The MBSA report shows that ISS Lockdown tool has been implemented.



Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Actions

- Print
- Copy

View security report

Sort Order: Score (worst first)

Internet Information Services (IIS) Scan Results

Vulnerabilities

| Score | Issue | Result |
|---|---|---|
| ✗ | Sample Applications | Some IIS sample applications are installed.<br>What was scanned  Result details  How to correct this |
| ✗ | Parent Paths | Parent paths are enabled in some web sites and/or virtual directories.<br>What was scanned  Result details  How to correct this |
| ✗ | IISAdmin Virtual Directory | IISADMPWD virtual directory was found under one or more web sites.<br>What was scanned  How to correct this |
| ✗ | MSADC and Scripts Virtual Directories | MSADC virtual directory was found under one or more web sites. Scripts virtual directory was found under one or more web sites.<br>What was scanned  How to correct this |
| ✓ | IIS Lockdown Tool | The IIS Lockdown tool has been run on the machine.<br>What was scanned |

Additional System Information

| Score | Issue | Result |
|---|---|---|
| ✱ | Domain Controller Test | IIS is not running on a domain controller.<br>What was scanned |
| ✱ | IIS Logging Enabled | Some web or FTP sites are not using the recommended logging options.<br>What was scanned  Result details  How to correct this |

SQL Server Scan Results

| Score | Issue | Result |
|---|---|---|
|  | SQL Server/MSDE Status | SQL Server and/or MSDE is not installed on this computer. |

Previous security report  Next security report

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

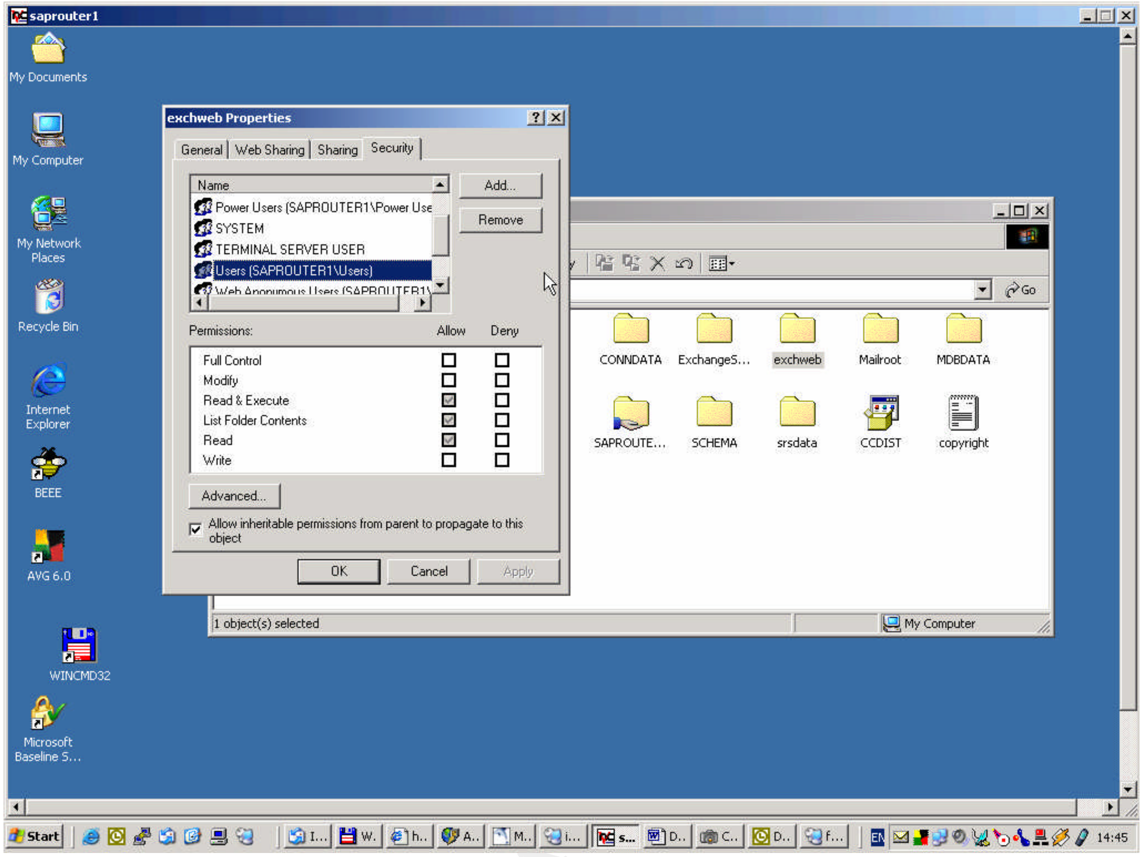
## IIS2 – Check URLScan installation

Following UrlScan.ini file was found on the OWA server. Microsoft has proposed a slightly different URLScan.ini file for use on the OWA servers. There are small differences of the [AllowVerbs] section and also, [AllowExtensions] section is used instead of [DenyExtensions].

```
[options]
UseAllowVerbs=1
UseAllowExtensions=1
NormalizeUrlBeforeScan=1
VerifyNormalization=1
AllowHighBitCharacters=1
AllowDotInPath=1
RemoveServerHeader=0
EnableLogging=1
PerProcessLogging=0
AllowLateScanning=0
PerDayLogging=1
RejectResponseUrl=
UseFastPathReject=0
AlternateServerName=

[AllowVerbs]
GET
HEAD
POST
OPTIONS
SEARCH
POLL
PROPFIND
BMOVE
BCOPY
SUBSCRIBE
MOVE
PROPPATCH
BPROPPATCH
DELETE
BDELETE
MKCOL
UNSUBSCRIBE
SUBSCRIPTIONS
COPY
LOCK
UNLOCK
PUT
ACL
NOTIFY

[DenyVerbs]


[DenyHeaders]


[AllowExtensions]
.asp
.cer
.cdx
.asa
.htm
.html
.txt
.jpg
.jpeg
.gif
.htr

;.idq
;.htw
;.ida
;.idc
;.shtm
;.shtml
;.stm

;.printer
[DenyExtensions]

.exe
.bat
.cmd
.com

; Deny infrequently used scripts
.htw
.ida
.idq
.htr
.idc
.shtm
.shtml
.stm
.printer

; Deny various static files
.ini     ; Configuration files
.log     ; Log files
.pol     ; Policy files
.dat     ; Configuration files

;.asp
;.cer
;.cdx
;.asa
[DenyUrlSequences]
;..
./
\
%
&
```

## IIS3 – Check IIS virtual directories ACLs

The audit of IIS virtual directory ACLs shows that only administrators have full control access. Rights of ordinary users have been set up to read-only access.



exchweb Properties

General | Web Sharing | Sharing | Security

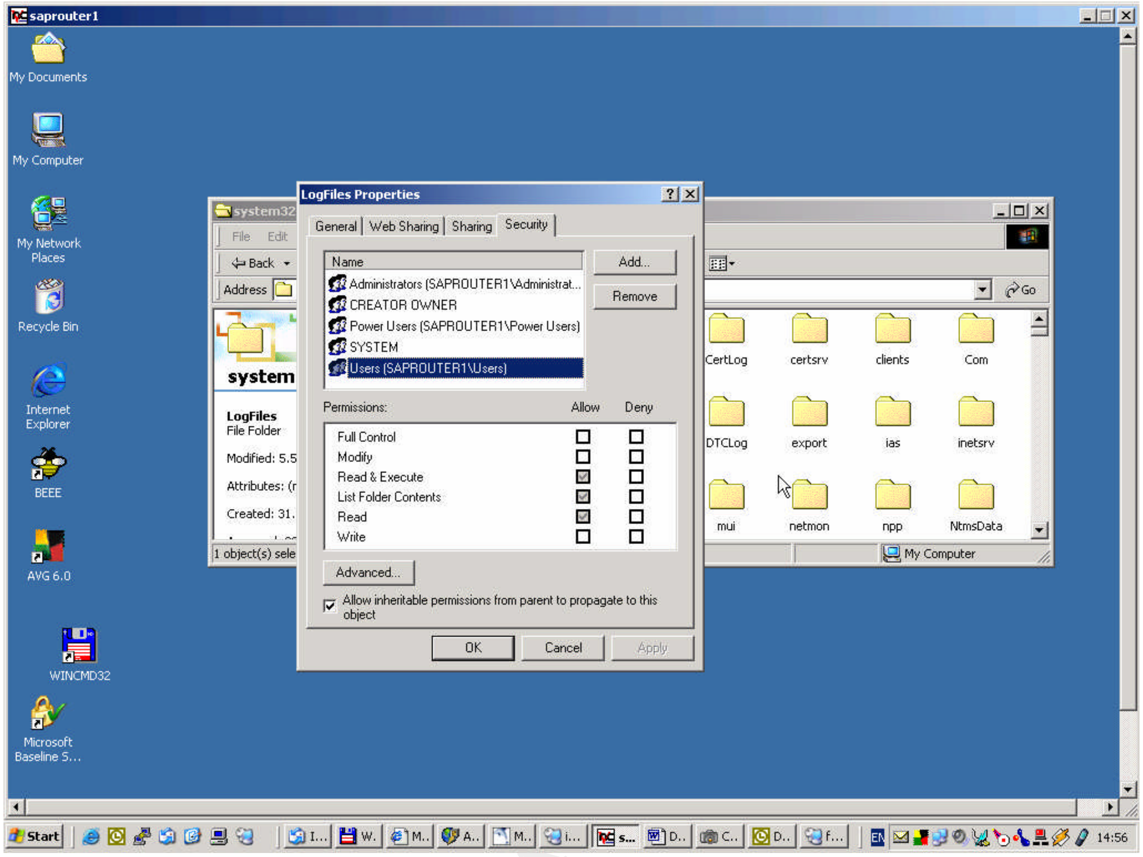
| Name |
|---|
| Power Users (SAPROUTER1\Power Use |
| SYSTEM |
| TERMINAL SERVER USER |
| Users (SAPROUTER1\Users) |
| Web Anonymous Users (SAPROUTER1\ |

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Modify | □ | □ |
| Read & Execute | ☑ | □ |
| List Folder Contents | ☑ | □ |
| Read | ☑ | □ |
| Write | □ | □ |

☑ Allow inheritable permissions from parent to propagate to this object

## IIS4 – Check IIS Log files ACL

Audit of IIS Log files permissions shows that only administrators have full control over the log files. The rights of authenticated users have been set up to read-only access.



LogFiles Properties

General | Web Sharing | Sharing | Security

Name
- Administrators (SAPROUTER1\Administrat...
- CREATOR OWNER
- Power Users (SAPROUTER1\Power Users)
- SYSTEM
- Users (SAPROUTER1\Users)

| Permissions: | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Modify | □ | □ |
| Read & Execute | ☑ | □ |
| List Folder Contents | ☑ | □ |
| Read | ☑ | □ |
| Write | □ | □ |

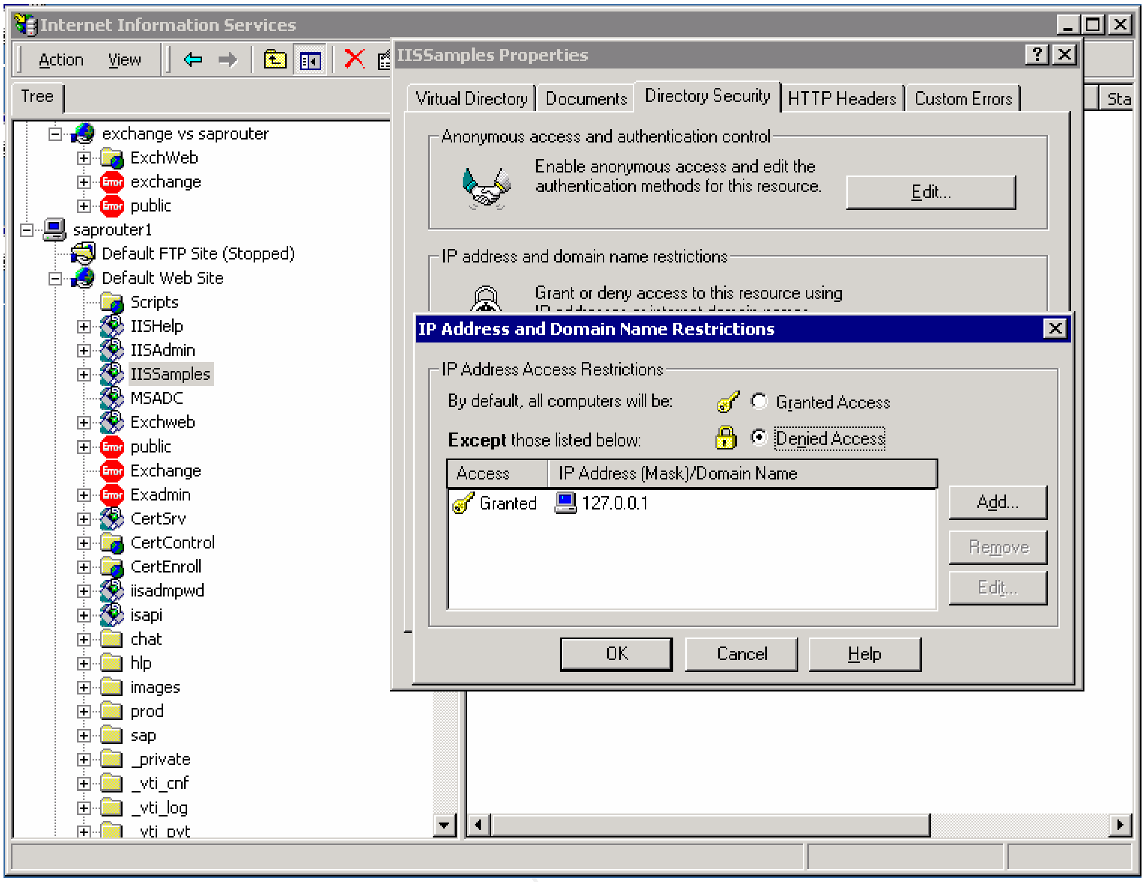
☑ Allow inheritable permissions from parent to propagate to this object

## IIS5 – Check IIS Sample application presence

IIS Sample application directories were found (see the screen output of IIS1 test). This is a strange finding, since IIS Lockdown tool removes sample application directories under normal circumstances.

Consultation with the IIS administrators showed that they had to restore some of the IIS Lockdown tool settings, but this lead also to the restoration of sample applications.

Review of the sample application security settings shows that access to the directories is granted only from local machine. This setting mitigates risks associated with the presence of the sample application directories.



Internet Information Services

Action View

Tree

```
exchange vs saprouter
    ExchWeb
    exchange
    public
saprouter1
    Default FTP Site (Stopped)
    Default Web Site
        Scripts
        IISHelp
        IISAdmin
        IISSamples
        MSADC
        Exchweb
        public
        Exchange
        Exadmin
        CertSrv
        CertControl
        CertEnroll
        iisadmpwd
        isapi
        chat
        hlp
        images
        prod
        sap
        _private
        _vti_cnf
        _vti_log
        _vti_pvt
```

IISSamples Properties

Virtual Directory | Documents | Directory Security | HTTP Headers | Custom Errors

Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or internet domain names

IP Address and Domain Name Restrictions

IP Address Access Restrictions

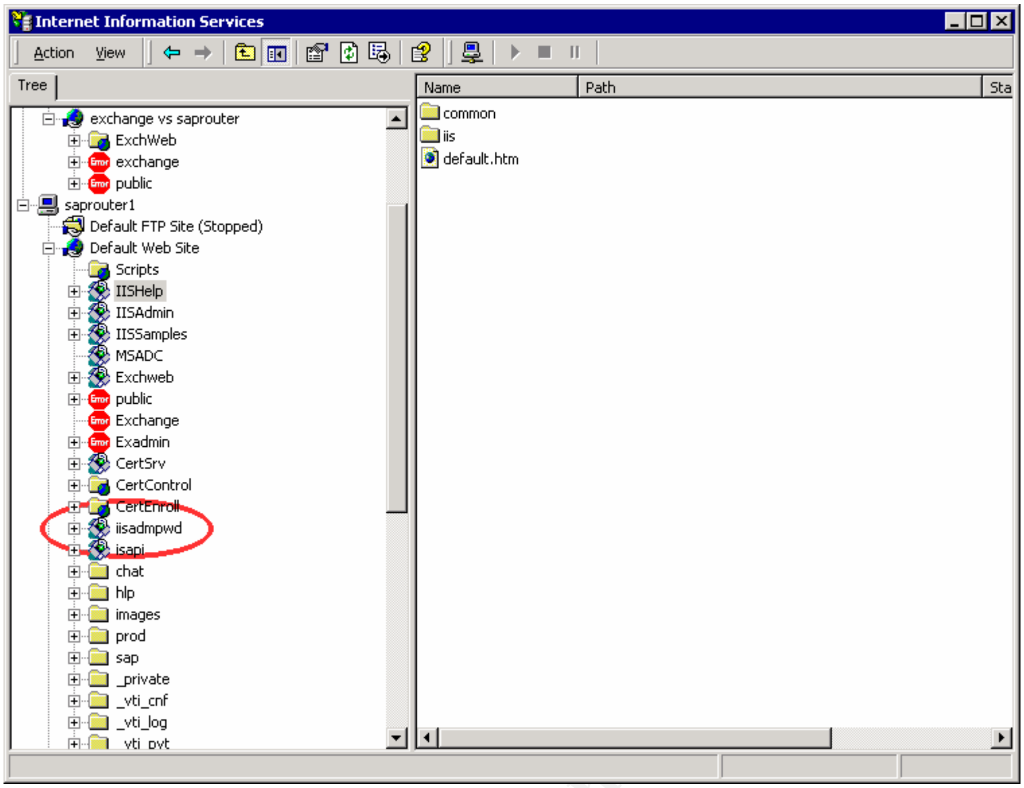
By default, all computers will be: ○ Granted Access

**Except** those listed below: ● Denied Access

| Access | IP Address (Mask)/Domain Name |
|---|---|
| Granted | 127.0.0.1 |

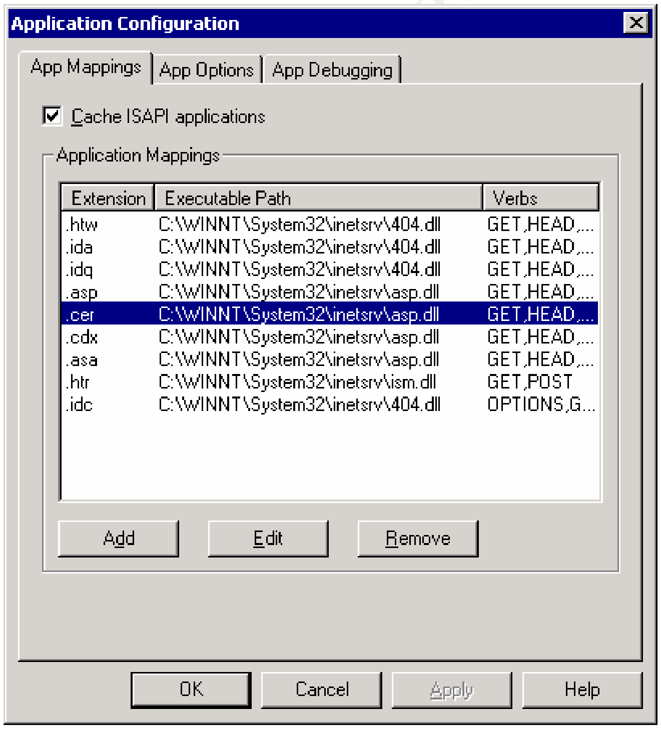
## IIS6 – Check IIS IISADMPWD directory presence

IIS IISADMPWD directory was found on the OWA server. This is due to the same problems like with IIS Sample application directories which were restored after IIS Lockdown settings restoration (see previous section).



## IIS7 – Check IIS ISAPI extension mappings

Audit result showed that mapping of most unused IIS ISAPI extensions is handled by the 404.dll library. Anyway, these extensions were not unmapped - .cer ; .cdx ; .asa .



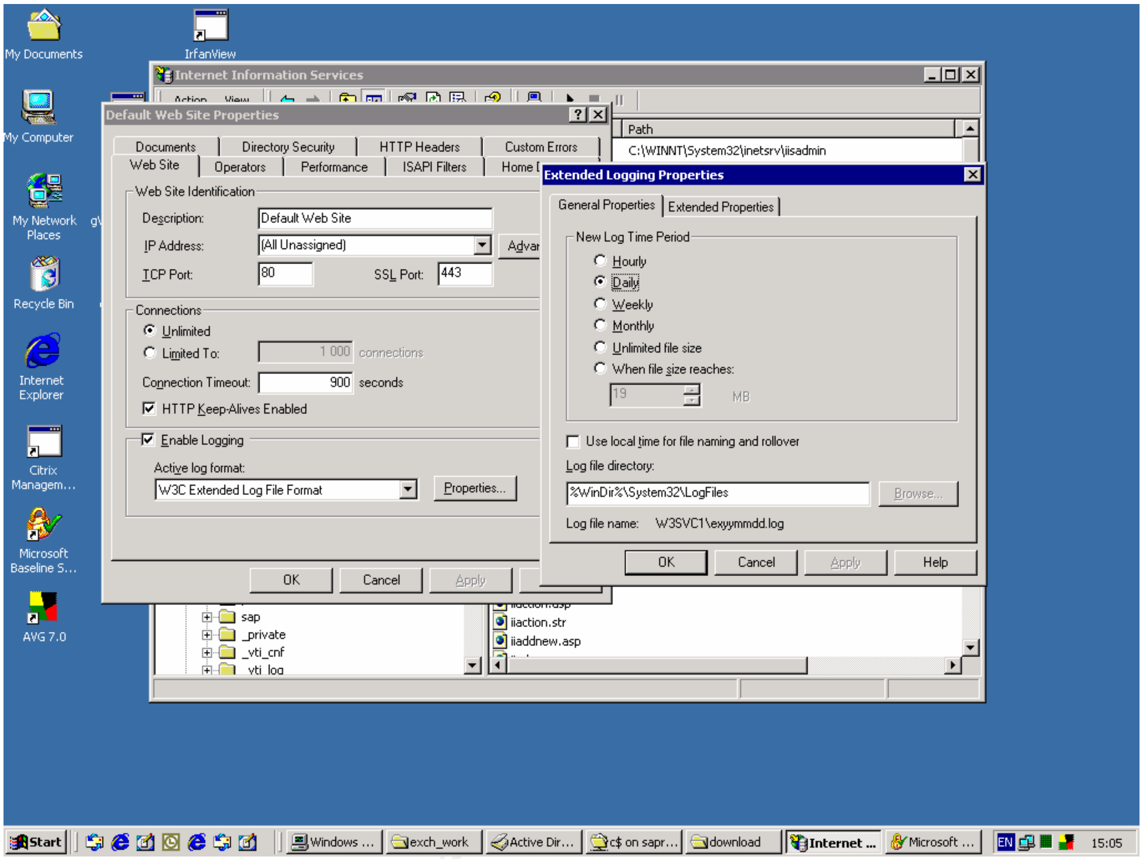
☑ Cache ISAPI applications

Application Mappings

| Extension | Executable Path | Verbs |
|---|---|---|
| .htw | C:\WINNT\System32\inetsrv\404.dll | GET,HEAD,... |
| .ida | C:\WINNT\System32\inetsrv\404.dll | GET,HEAD,... |
| .idq | C:\WINNT\System32\inetsrv\404.dll | GET,HEAD,... |
| .asp | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .cer | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .cdx | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .asa | C:\WINNT\System32\inetsrv\asp.dll | GET,HEAD,... |
| .htr | C:\WINNT\System32\inetsrv\ism.dll | GET,POST |
| .idc | C:\WINNT\System32\inetsrv\404.dll | OPTIONS,G... |

## IIS8 – Check IIS logging

Audit shows that logging has been enabled for the IIS system including all recommended request details.



Default Web Site Properties

Web Site Identification
Description: Default Web Site
IP Address: (All Unassigned)
TCP Port: 80 SSL Port: 443

Connections
● Unlimited
○ Limited To: 1 000 connections
Connection Timeout: 900 seconds
☑ HTTP Keep-Alives Enabled

☑ Enable Logging
Active log format: W3C Extended Log File Format

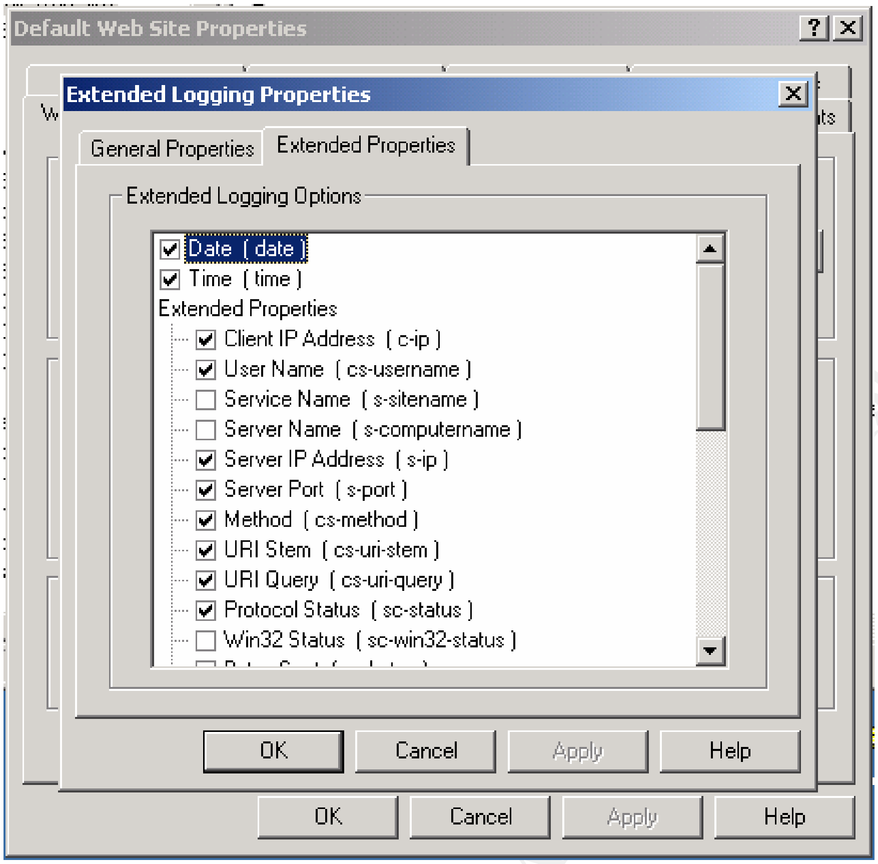
Path
C:\WINNT\System32\inetsrv\iisadmin

iiaction.str
iiaddnew.asp

Extended Logging Properties

New Log Time Period
○ Hourly
● Daily
○ Weekly
○ Monthly
○ Unlimited file size
○ When file size reaches: 19 MB

□ Use local time for file naming and rollover
Log file directory: %WinDir%\System32\LogFiles
Log file name: W3SVC1\exyymmdd.log

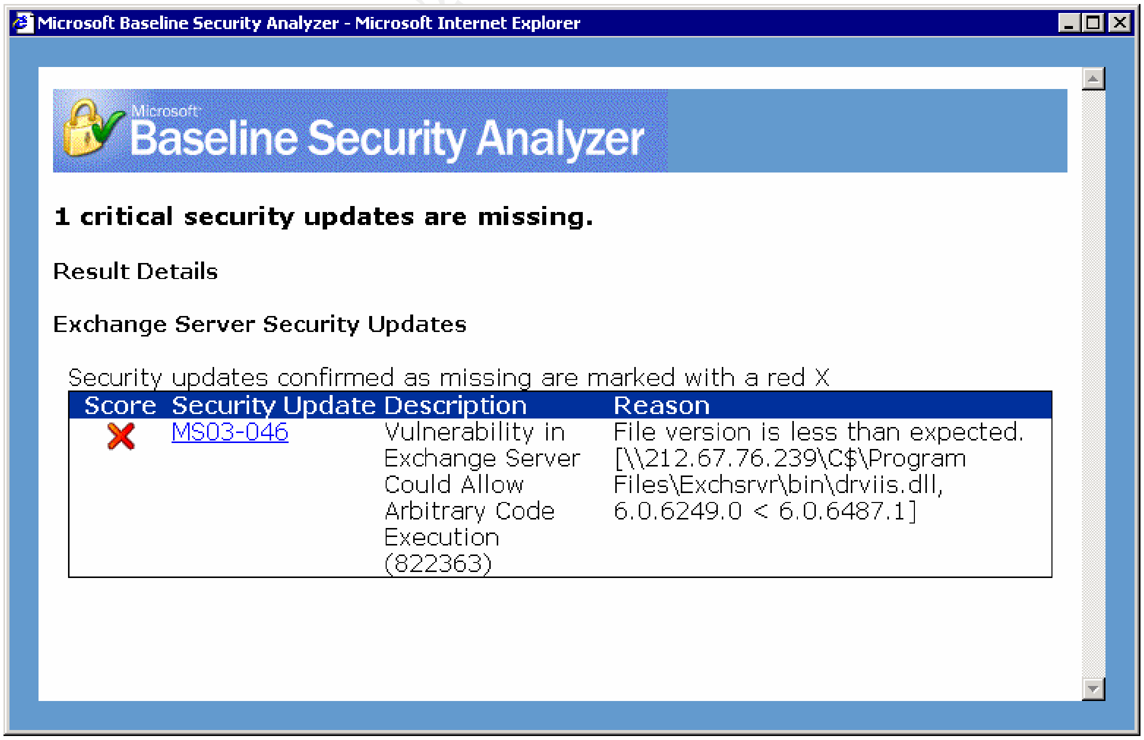


Extended Logging Options

☑ Date ( date )
☑ Time ( time )
Extended Properties
☑ Client IP Address ( c-ip )
☑ User Name ( cs-username )
☐ Service Name ( s-sitename )
☐ Server Name ( s-computername )
☑ Server IP Address ( s-ip )
☑ Server Port ( s-port )
☑ Method ( cs-method )
☑ URI Stem ( cs-uri-stem )
☑ URI Query ( cs-uri-query )
☑ Protocol Status ( sc-status )
☐ Win32 Status ( sc-win32-status )

## EXCH1 – Check latest Exchange 2000 Service pack and hotfixes

Although one Exchange 2000 critical security update is missing, it is concerning the SMTP service that was disabled on the OWA Front-end server.



Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Microsoft
Baseline Security Analyzer

**1 critical security updates are missing.**

**Result Details**

**Exchange Server Security Updates**

Security updates confirmed as missing are marked with a red X

| Score | Security Update | Description | Reason |
|---|---|---|---|
| ✗ | MS03-046 | Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (822363) | File version is less than expected. [\\212.67.76.239\C$\Program Files\Exchsrvr\bin\drviis.dll, 6.0.6249.0 < 6.0.6487.1] |

### EXCH2 – Check running and disabled Exchange 2000 services

Audit of running Exchange 2000 services shows that following Exchange services have been started automatically on startup and could be disabled:

Microsoft Exchange Management
Microsoft Exchange MTA Stacks
Microsoft Exchange System Attendant

| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Microsoft Exchange Event | Monitors folders and fires events, for Exchange 5.5-compatible server applications. |  | Manual | LocalSystem |
| Microsoft Exchange IMAP4 | Provides Microsoft Exchange IMAP4 Services. |  | Disabled | LocalSystem |
| Microsoft Exchange Information Store | Manages Microsoft Exchange Information Storage |  | Disabled | LocalSystem |
| Microsoft Exchange Management | Provides Microsoft Exchange management information through WMI. | Started | Automatic | LocalSystem |
| Microsoft Exchange MTA Stacks | Provides Microsoft Exchange X.400 services | Started | Automatic | LocalSystem |
| Microsoft Exchange POP3 | Provides Microsoft Exchange POP3 Services. |  | Disabled | LocalSystem |
| Microsoft Exchange Routing Engine | Processes Microsoft Exchange routing information | Started | Automatic | LocalSystem |
| Microsoft Exchange Site Replication Service |  |  | Disabled | LocalSystem |
| Microsoft Exchange System Attendant | Provides system related services for Microsoft Exchange | Started | Automatic | LocalSystem |

### EXCH3 – Check Mailbox size limits – Not Applicable

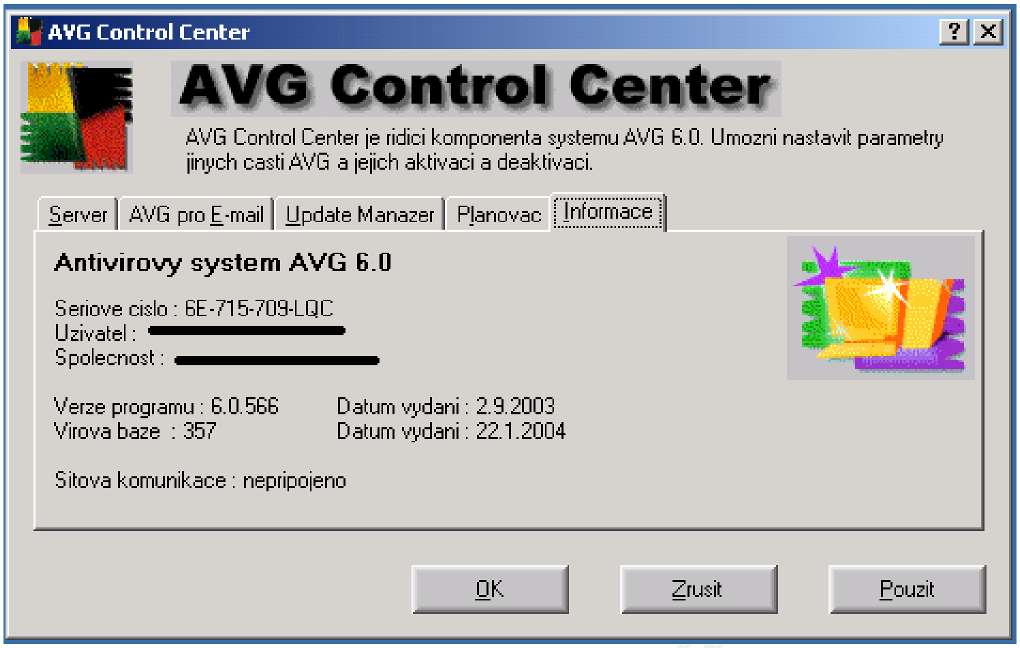
The Microsoft Exchange Information store service is disabled.

### EXCH4 – Check Exchange directory location– Not Applicable

The Microsoft Exchange Information store service is disabled.

### EXCH5 – Check antivirus software

Antivirus program was running and the virus database was up-to-date.



AVG Control Center

AVG Control Center je ridici komponenta systemu AVG 6.0. Umozni nastavit parametry jinych casti AVG a jejich aktivaci a deaktivaci.

Antivirovy system AVG 6.0

Seriove cislo : 6E-715-709-LQC
Uzivatel : [redacted]
Spolecnost : [redacted]

Verze programu : 6.0.566 Datum vydani : 2.9.2003
Virova baze : 357 Datum vydani : 22.1.2004

Sitova komunikace : nepripojeno

### EXCH6 – Check Exchange logfile permissions – Not Applicable

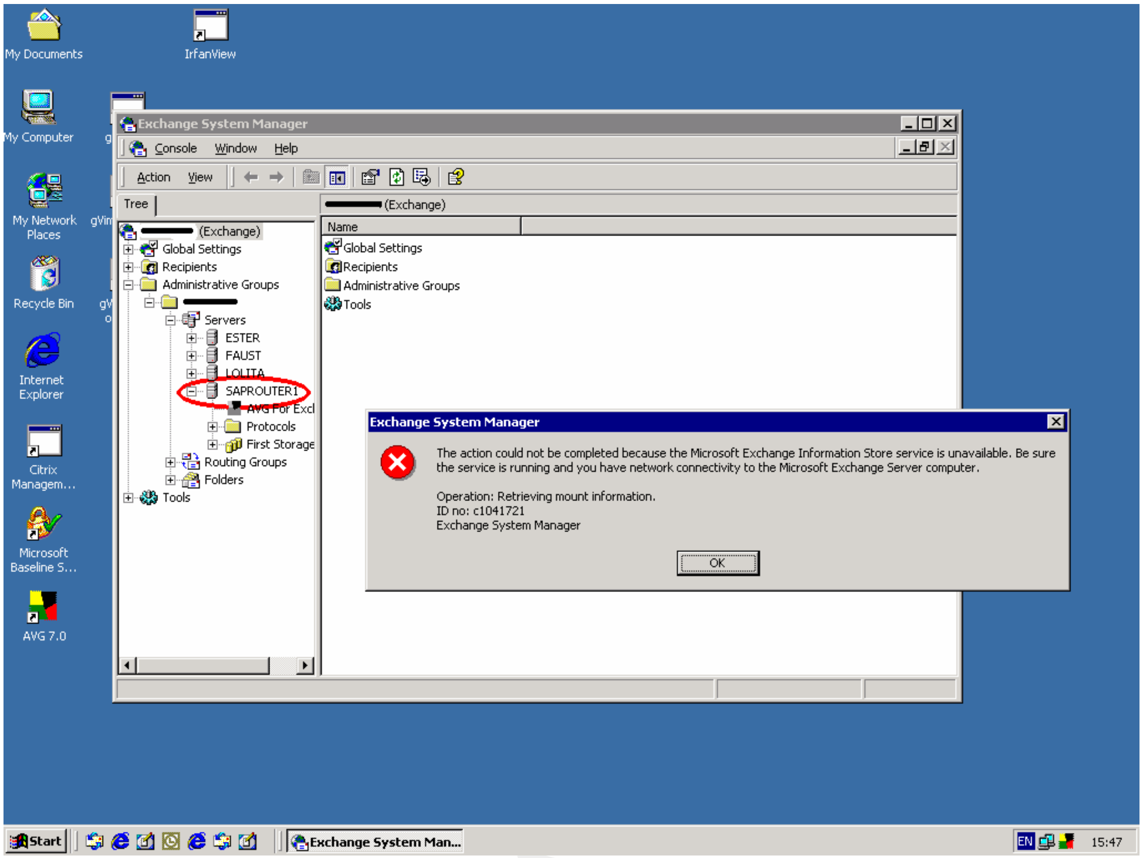
The Microsoft Exchange Information store service is disabled.

### EXCH7 – Check if SMTP banner has been changed – Not Applicable

SMTP service doesn't run on the OWA server

### EXCH8 – Check that no local Exchange data reside on OWA server

The Microsoft Exchange Information store service is disabled.
Attempting to configure the Exchange Information store shows a warning message.



Exchange System Manager

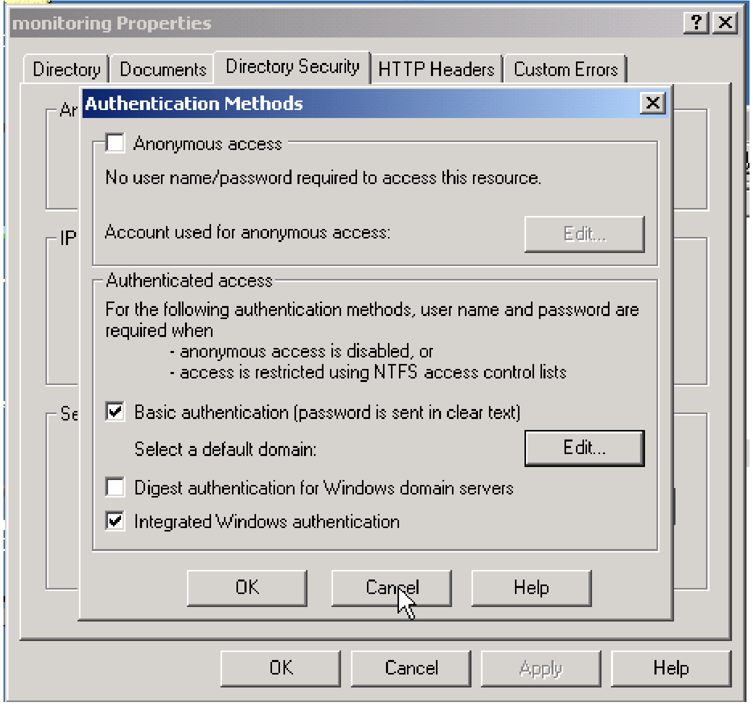
The action could not be completed because the Microsoft Exchange Information Store service is unavailable. Be sure the service is running and you have network connectivity to the Microsoft Exchange Server computer.

Operation: Retrieving mount information.
ID no: c1041721
Exchange System Manager

OK

## EXCH9 – Check adequate OWA user authentication

The audit step revealed that adequate OWA user authentication is used.
Anyway, "require 128-bit encryption" checkbox is unchecked. This setting allows using less secure SSL communication channel making decoding of the data stream easier.



Authentication Methods

□ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access: Edit...

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

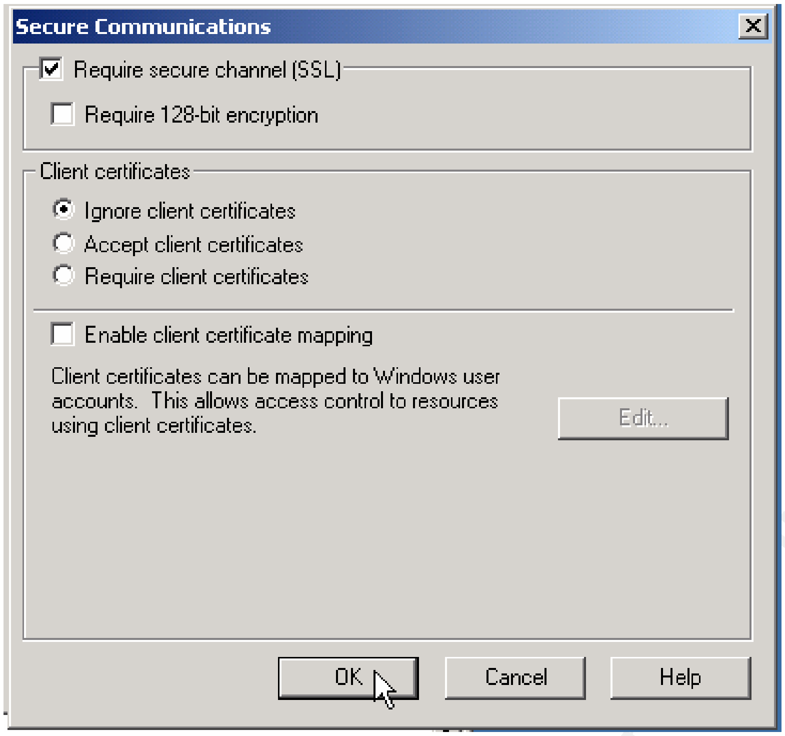
☑ Basic authentication (password is sent in clear text)

Select a default domain: Edit...

□ Digest authentication for Windows domain servers

☑ Integrated Windows authentication

OK Cancel Help



Secure Communications

☑ Require secure channel (SSL)

□ Require 128-bit encryption

Client certificates

● Ignore client certificates

○ Accept client certificates

○ Require client certificates

□ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

# Audit report – findings and recommendations

## *System Operation and Management*

### Finding – There is no Company security and operational policy

Audit interviews showed that there are only weak informal security and operational policies. Policies help the company to implement, operate and protect their systems. They define a set of rules, settings and procedures according to company's requirements.

Without a security policy, there is no definite approach to the security of informational systems, no roles and responsibilities for system operation, management and disaster recovery, there are no conditions of use, right to access informations etc.

**Risk evaluation: high**

**Audit recommendations:**
Company policy should be created to describe rules and requirements of following areas:

- installation of the Windows 2000 servers
- IIS setup, security setup and operation
- Exchange server setup
- Management of the servers

An internal audit procedure should be created to examine the abidance of those policies.
Of course, company policies should not concern only the areas mentioned.

### Finding – Logs are not reviewed on a regular basis

Reference: MGMT2
Administrators were asked during the interview about the company logging analysis policy and procedures. In their responses they stated that logs are reviewed only occasionally and that no automation analysis tools are in place.

Logging analysis in a short period is one of fundamental computer security tasks. Early detection of system compromise mitigates impacts and damages caused by a security incident.

**Risk evaluation: high**

**Audit recommendations:**
Company should introduce logging analysis policy – responsibility, frequency of the checks, control measurements etc.
Automated analysis tools should be introduced to immediately detect security incidents, ease administrators tasks and to lower chance of overseeing important logs.

### *Exchange Back-end server*

### Finding – missing patches

Reference: OS2, OS8, EXCH1
Audit through Microsoft Baseline Security Analyzer showed that 11 operating system updates are missing. This is a very high number indicating that the server is not patched on regular basis. Except of operating system updates, another updates are missing:
One critical Microsoft Virtual Machine security update
One critical Exchange server update concerning SMTP

Independent Nessus security scan proved critical security holes caused by missing updates

Having the server patched and up-to-date is one of the most important security rules. Applying patches lowers the probability of system being compromised not only by unauthorized user activity, but also by viruses and Trojan horse programs like RedCode etc.

The server is vulnerable to RPC related issues. An immediate action is needed. An attacker or a worm could use the vulnerabilities to execute arbitrary code or even gain the control of this host.
Messenger Service vulnerability was found by the Nessus security scanner. This vulnerability could allow running code with local system privileges on the affected system.

SMTP Service is not updated and the “XEXCH50” extended verb could be used to execute arbitrary code on Exchange 2000.

**Risk evaluation: High**

**Audit recommendations:**
Download up-to-date Microsoft security patches from the Microsoft web pages. Apply them in a test environment first and after function verification patch the production server.

### Finding – Weak account password policy

Reference: OS4
Audit of the account password policy showed that password policy was not set up. Although during the interview administrators stated that they have an informal password policy, no password policy is not enforced. Because of that, security of audited system is weakened relying only on administrator’s awareness of brute-force password attacks.

**Risk evaluation: Medium**

**Audit recommendations:**
Enforce strong password policy. Apply following settings to Account policies:

- Set minimum password length 8 characters - with at least one character from following groups: numbers, uppercase, lowercase
- Set maximum password age 90 days or less
- Set minimum password age 5 days or more
- Set password history at least 5 passwords

- Set account lockout duration 30 minutes
- Set account lockout duration 5 attempts
- Enable password complexity"

## Finding – unnecessary services

Reference: OS5

Some of the services running on the audited server are not necessary for the function and could be stopped. Among these are:

Alerter
Computer Browser
DHCP Client
File Replication Server
License Logging Service
Messenger
Network News Transport Protocol (NNTP)
Print Spooler
Terminal Services
Remote Registry Service
Removable Storage

Some of other services, which are not running on the audited system, are set to "manual".

For one of the running services, two high-risk vulnerabilities have been found.

Unnecessary services provide possible "open doors" to the system. It is a good practice to disable all unneeded services to mitigate the risk of system compromise.
Nessus security scan revealed that there are two high-risk vulnerabilities linked to the Messenger Service. Although the main purpose is insufficient operating system patch application, if the Messenger Service wasn't running, the system wouldn't be affected by the vulnerability.

**Risk evaluation: medium-high**

**Audit recommendations:**
The recommendation is to disable all services that are not necessary for the system function.
Services set to "manual" Startup type should be changed to "disable" on start-up.

## Finding – Operating system logging is not set up

Reference: OS7

Checking operating system log settings revealed that except of account management, no audit is set up. Because of that, no evidence of possible unauthorized activity is available.
There is no evidence about who and when logged into the server, what services have been used or that system policy has changed.

**Risk evaluation: medium**

**Audit recommendations:**

Turn on important operating system events logging. Review logs on a daily basis. Consider automated logging analyze tools

Recommended logging settings for Exchange Back-end server:

System events – success and failure
Privilege use – failure
Policy change – success and failure
Object access – failure
Logon events – failure
Account management – success and failure
Account login – failure

## Finding – SMTP Vulnerability on Exchange Back-end server

Reference: EXCH1
Audit showed that SMTP Service is not updated and the “XEXCH50” extended verb could be used to execute arbitrary code on Exchange 2000.
Workaround for the vulnerability proposed by Microsoft has not been implemented.

**Risk evaluation: High**
Missing patch could allow arbitrary code execution or denial of service shutting down the Internet mail service.

**Audit recommendations:**
Download the security patch from Microsoft web site according to Microsoft Security Bulletin MS03-046.

## Finding – EXCHRVR directory is readable by Everyone

Reference: EXCH4
Permissions of the *\Exchsrvr* directory are set by Windows 2000 to full control for the EVERYONE group, were not changed.

**Risk evaluation: Medium**

**Audit recommendations:**
Change the permissions of *\Exchsrvr* directory so that the Everyone group doesn’t have any rights. Instead, assign following rights:

SYSTEM – Full Control
CREATOR OWNER – Full Control
Domain Admins – Full Control
< All Exchange Administrative Groups> – Full Control
Authenticated Users - read and execute access.

The local computer account should also be given full control over the shared directories created during the installation.

### Finding – Exchange server is running on a Domain controller

Reference: EXCH4

Listing of the Active directory Users and Computers shows that Exchange Back-end server is installed on one of the company's domain controllers.

Since Exchange Server security, logons, registry settings, running services etc. are tightly coupled with the operation system, it would be better to move the Exchange server from domain controller.

**Risk evaluation: Medium**

**Audit recommendations:**

Separate Exchange server and Domain Controller functionality of the Exchange Back-end server.

### Finding – SMTP banner not changed

Reference: EXCH7

Telnet to the TCP port 25 shows that SMTP Banner was not modified by the Exchange system administrators.

**Risk evaluation: low**

The less information you provide an attacker, the more difficult it is to attack your system.

**Audit recommendations:**

The SMTP banner should be changed to provide an attacker less information about the system. Microsoft knowledge base article 281224 contains detailed informations about how to change the banner.

http://support.microsoft.com/?kbid=281224

## *Exchange Front-end server*

### Finding – missing patches

Reference: OS2, OS8, EXCH1

Audit of the Exchange Front-end server (OWA) revealed that the system is running with Service Pack 3!

Microsoft Baseline Security Analyzer showed that 32 operating system updates are missing, many of them marked as critical.

One critical Microsoft Virtual Machine security update is missing

One critical Exchange server update concerning SMTP is missing.

Independent Nessus security scan proved critical security holes caused by missing updates

Having the server patched and up-to-date is one of the most important security rules. Applying patches lowers the probability of system being compromised not only by unauthorized user activity, but also by viruses and Trojan horse programs like RedCode etc.

The server is vulnerable to RPC related issues. An immediate action is needed. An attacker or a worm could use the vulnerabilities to execute arbitrary code or even gain the control of this host.
Messenger Service vulnerability was found by the Nessus security scanner. This vulnerability could allow running code with local system privileges on the affected system.

**Risk evaluation: High**

**Audit recommendations:**
Update the server to Service pack 4.
Download up-to-date Microsoft security patches. Apply them in a test environment and after function verification patch the production server.

## Finding – Weak account password policy

Reference: OS4
Audit of the account password policy showed that password policy was not set up. Because password policy is not enforced, security of audited system is weakened relying only on administrator's awareness of brute-force password attacks.

**Risk evaluation: Medium - high**

**Audit recommendations:**
Enforce strong password policy. Apply following settings to Account policies:

- Set minimum password length 8 characters - with at least one character from following groups: numbers, uppercase, lowercase
- Set maximum password age 90 days or less
- Set minimum password age 5 days or more
- Set password history at least 5 passwords
- Set account lockout duration 30 minutes
- Set account lockout duration 5 attempts
- Enable password complexity"

## Finding – unnecessary services

Reference: OS5,
Some of the services running on the audited server are not necessary for the function and could be stopped. Among these are:

Alerter
Computer Browser
DHCP Client
Distributed File System
Messenger
Print Spooler
Protected Storage
Remote Registry Service
Removable Storage

Some of other services, which are not running on the audited system, are set to “manual”. High-risk vulnerabilities have been found concerning unnecessary and running services.

Unnecessary services provide possible “open doors” to the system. It is a good practice to disable all unneeded services to mitigate the risk of system compromise.
Nessus security scan revealed that there are two high-risk vulnerabilities linked to the Messenger Service. Although the main purpose is insufficient operating system patch application, if the Messenger Service wasn’t running, the system wouldn’t be affected by the vulnerability.

**Risk evaluation: high**

**Audit recommendations:**
I would recommend disabling all unnecessary services.
Services set to “manual” Startup type should be changed to “disable”.

## Finding – Anonymous Logon access not restricted

Reference: OS6
Audit showed that the *“RestrictAnonymous”* registry value is set to 0, which means that no restrictions concerning anonymous access to the registry are in place.

A null session is a session established without credentials (i.e. blank username and password). Null sessions can be used to display information about users, groups, shares and password policies. These informations could be listed if DMZ becomes compromised.

Fortunately all firewall traffic except http/https to the Exchange Front-end server is blocked. Anyway, if another server in the DMZ becomes compromised, the vulnerability can be exploited to gain access / informations about the OWA server.

**Risk evaluation: medium**

**Audit recommendations:**
To better secure anonymous access, this option can be changed through Group Policy or via the registry.
Using regedit, open following registry entry:
„*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA*“
Set the "RestrictAnonymous" value to 2 on the Exchange Front-end server.

## Finding – Operating system logging is not set up

Reference: OS7
Checking operating system log settings revealed that except of account management, no audit is set up. Because of that, no evidence of possible unauthorized activity is available.
There is no evidence about who and when logged into the server, what services have been used or that system policy has changed.

Logging is an important step to prevent and track unauthorized user activity, especially on the Exchange Front-end server which is exposed to Internet.

**Risk evaluation: high**

**Audit recommendations:**
Turn on important operating system events logging. Review logs on a daily basis. Consider automated logging analyze tools
Recommended logging settings for OWA server:

System events – success and failure
Privilege use – failure
Policy change – success and failure
Object access – failure
Logon events – success and failure
Account management – success and failure
Account login – success and failure

## Finding – IIS Sample application and IISADMPWD directories are present

Reference: IIS5, IIS6, OS8
IIS Sample application directories were found.
IIS IISADMPWD directory was found on the OWA server.

Consultation with the IIS administrators showed that they had to restore some of the IIS Lockdown tool settings, but this lead also to the restoration of sample applications.

IIS Sample Applications can be exploited by hackers to break into an IIS system because they contain sample scripts. A production Web server should not have any sample code or scripts on the system.
An attacker may use *.htr file located in the IISADMPWD directory to launch a brute force attack to gain valid username/password. A valid user may also use it to change his password on a locked account.

**Risk evaluation: HIGH**

**Audit recommendations:**
Microsoft IIS Lockdown tool should be modified to correspond to the Exchange Front-end functionality. Then, it should be run again on the server.
Administrators should manually verify that both IIS Sample directory and IISADMPWD are remowed.

## Finding – URLScan.ini is not set up according to the recommendations

Reference: IIS2
Some of the URLScan settings of the OWA server differ from the URLScan.ini settings proposed by Microsoft. Following URLScan.ini file has been proposed to use on the OWA server by Microsoft:

```
[Options]
UseAllowVerbs=1
UseAllowExtensions=0
NormalizeUrlBeforeScan=1
VerifyNormalization=1
AllowHighBitCharacters=1
AllowDotInPath=1
RemoveServerHeader=0
EnableLogging=1
PerProcessLogging=0
AllowLateScanning=0

[AllowVerbs]
GET
POST
SEARCH
POLL
PROPFIND
BMOVE
BCOPY
SUBSCRIBE
MOVE
PROPPATCH
BPROPPATCH
DELETE
BDELETE
MKCOL

[DenyVerbs]

[DenyHeaders]
If:
Lock-Token:
```

```
[DenyExtensions]
.asp
.cer
.cdx
.asa
.exe
.bat
.cmd
.com
.htw
.ida
.idq
.htr
.idc
.shtm
.shtml
.stm
.printer
.ini
.log
.pol
.dat

[DenyUrlSequences]
..
./
\
%
&
```

**Risk evaluation: Low**

**Audit recommendations:**
Examine the Urlscan.log file located in the <WinDir>\System32\Inetsrv\Urlscan directory.
Remove these words from [AllowVerb] section:

```
[AllowVerbs]
HEAD
OPTIONS
UNSUBSCRIBE
SUBSCRIPTIONS
COPY
LOCK
UNLOCK
PUT
ACL
NOTIFY
```

Add following entries to the [DenyHeaders] section:

```
[DenyHeaders]
If:
Lock-Token:
```

## Finding – Some IIS ISAPI mappings are not unmapped

Reference: IIS7
Audit result showed that mapping of most unused IIS ISAPI extensions is handled by the 404.dll library. Anyway, these extensions were not unmapped - .cer ; .cdx ; .asa . These mappings are normally not needed for the Exchange Front-end server.

**Risk evaluation: Low**

**Audit recommendations:**
Review if you need to use the .cer, .cdx and .asa ISAPI extensions. If they are not necessary for the OWA functionality, change their mapping.
Alter corresponding entry in the URLScan.ini file section `[AllowExtensions]`.

## Finding – Some Exchange services are not necessary

Reference: EXCH2, OS5

Audit of running Exchange 2000 services shows that following Exchange services have been started automatically on startup and could be disabled0:

Microsoft Exchange Management
Microsoft Exchange MTA Stacks
Microsoft Exchange System Attendant

Descriptions of the services can be found in the Microsoft document "Securing Exchange 2000 Servers Based on Role":

Microsoft Exchange Management -The OWA front-end server is used to access mail rather than to route mail, you should not find that the Microsoft Exchange Management Service needs to run on your OWA front-end servers.

Microsoft Exchange MTA Stacks - Provides Microsoft Exchange X.400 services. It is only needed for backwards compatibility or if there are X.400 connectors

Microsoft Exchange System Attendant - Provides system related services for Microsoft Exchange. On a front-end server, the System Attendant is only required if you wish to make configuration changes to the server. This means that to make any changes to a server which uses the OWA Front-end Server Policy (including making the server an OWA Front-end server), you need to temporarily start the System Attendant and associated services first.

Unnecessary services provide possible "open doors" to the system. It is a good practice to disable all unneeded services to mitigate the risk of system compromise.

**Risk evaluation: Medium**

**Audit recommendations:**

I would recommend disabling Microsoft Exchange Management and Microsoft Exchange MTA Stacks.

Consider changing of the Microsoft Exchange System Attendant from automatic to manual.

## Finding – OWA SSL access doesn't require 128 bit encryption

Reference: EXCH9

The audit showed, that 128-bit encryption is not required to access the OWA server via https. This setting allows using less secure SSL communication channel making decoding of the data stream easier.

**Risk evaluation: low**

**Audit recommendations:**

Contemporary web browsers mostly support 128-bit encryption. To increase message security in transit, the require 128-bit encryption" checkbox should be checked.

## Audit report – executive summary

The document describes audit of Microsoft Exchange 2000 server with Outlook Web access running on a Windows 2000 server. The server relies also on Microsoft Internet Information Server – IIS 5.0.

The scope of the audit was to examine security settings and management of Exchange Back-end and Front-end servers and underlying components – operating system, IIS and firewall rules determining access between these two servers.

Following vulnerabilities and findings were found on the examined servers:

- Missing operating system and application updates
- Services unnecessary for the system operation
- Password policy is not enforced
- Low logging settings and analysis.
- Exchange server installation issues regarding placement
- IIS on Outlook Web access was not locked down correctly
- One critical SMTP vulnerability

The system is not updated on a regular basis. There was a high number of missing updates, some of them critical, allowing Exchange server leakage of information and system compromise.

Missing operating system updates also indicate that installation of the Exchange servers don't take into account internal network threats from malicious code, Trojan horse programs or illegal user activity, relying in particular on antivirus software and firewall rules. Threats from internal network shouldn't be underestimated since they present an important growing danger to any system.

Logs from the operating system are not set up according to Microsoft recommendation or best practices. Logs are not reviewed on a regular basis which extends the period of a possible security incident detection and recovery.

Both of these problems indicate that company should create operational policies which would among others determine procedures, roles and responsibilities of the administrators.

Outlook Web Access server is running on an unpatched and weakly secured IIS server. The system should be revised and security settings should be restricted to highest possible level.

Because company has only a very weak informal security policy, the system couldn't be compared and compliance measured against it. A heavy effort should be spent to create a security and operational policies that meet company's requirements. Policies define a set of rules, roles and areas of responsibility for system operation, management and disaster recovery, conditions of information use, etc.
System management according to well designed security and operational policies could reduce number and impacts of many of the vulnerabilities previously mentioned.

## References

Microsoft Security Operations Guide for Exchange 2000 Server
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/opsguide/default.asp

Microsoft Planning Outlook Web Access Servers
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/deploy/upgrdmigrate/ex2kupgr/planus/p_10_tt1.asp

Microsoft - Windows 2000 Server Baseline Security Checklist
www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp

Microsoft Security Bulletin Search
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

Microsoft - Securing Exchange 2000 Servers Resource Guide
http://www.microsoft.com/technet/security/chklist/ex2ksrg.asp

Microsoft Knowledge Base Article - Q309508 - IIS Lockdown and URLscan Configurations in an Exchange Environment
http://support.microsoft.com/default.aspx?scid=kb;en-us;309508

Microsoft Knowledge Base Article 319583 - Configure Storage Limits on Mailboxes in Exchange 2000
http://support.microsoft.com/default.aspx?scid=kb;en-us;319583&sd=tech

Microsoft IIS 5.0 Baseline Security Checklist
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp

National Security Agency - Windows 2000 Security Recommendation Guides
http://www.nsa.gov/snac/win2k/download.htm

National Security Agency - Guide to the Secure Configuration and Administration of Microsoft Exchange 2000
http://www.nsa.gov/snac/win2k/guides/w2k-21.pdf

Security focus - Securing Exchange 2000
http://www.securityfocus.com/infocus/1572

Security focus - Exchange 2000 in the Enterprise: Tips and Tricks Part One
http://www.securityfocus.com/infocus/1654

Security focus - Exchange 2000 in the Enterprise: Tips and Tricks Part Two
http://www.securityfocus.com/infocus/1658

Security focus - Exchange 2000 in the Enterprise: Tips and Tricks Part Three
http://www.securityfocus.com/infocus/1668

SANS organization – Securing Exchange 2000 Server
http://www.sans.org/rr/papers/19/588.pdf

SANS organization – NULL Sessions in NT/2000
http://www.sans.org/rr/papers/67/286.pdf

VA Security Standard Compliance Checklist (Physical security)
http://www.vascan.org/checklist/physical_security_check.html

Derek Geborek GIAC practical - Auditing IIS server, Windows 2000 server: An Independent Auditors Perspective
http://www.giac.com/practical/GSNA/Derek_Geborek_GSNA.pdf

Dan Holt GIAC practical – Auditing Microsoft Exchange 2000 Server – An Administrator's Perspective
http://www.giac.org/practical/GSNA/Dan_Holt_GSNA.pdf