Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing IIS within an Outook Web Access 2000 environment

In the past couple of years, e-mail has become an essential work tool that many people use on a daily basis. What used to be an easy way to send jokes and letters to family and friends is now for some businesses the most important tool of their enterprise. With the increase of people working on the road or from home, accessing the corporate e-mail has become a difficult task. Even though there exists many ways of accessing e-mail while out of the office, many of these solutions can lead to high security risks for serve...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Securing IIS within an Outook Web Access 2000 environment

January 23th 2003
SANS Institute
GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

Dave Munger
Sinc, Inc.
MCT, MCSE, CCNA, CCSA, CCSE & A+

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Abstract 3
What is Outlook Web Access (OWA)? 3
Accessing OWA 3
Securing the OWA 2000 Web based application 4
Securing (hardening) the operating system 4
Installation of a Front-end Server 5
The function of the Front-end server with incoming connections 5
Securing the location of the server within the network architecture 5
Configuration of Group Policy's within Active Directory 9
Securing Internet Information Service 5.0 (IIS 5.0) 11
Securing of the IIS "Metabase" 11
Securing the IIS registry keys. 12
Removal of unnecessary virtual folders 13
Automatic redirection of the default web site 14
Configuration of folder security 14
Removal of application mappings 16
Policy Configuration in Windows 2000 17
Configuration of the Web Site Operators 18
Securing the client-server communication with SSL 19
Auditing configuration 20
Event recording from IIS 20
Recording of events from Windows 2000 22
Introduction to SecureIIS 23
Installation of SecureIIS on the server 24
Now secure the OWA server with SecureIIS 25
Information 30
Working with « Log Viewer » 30
Troubleshooting 30
Conclusion 31
Appendix A 31
Appendix B 41
Citations: 42
Other references: 44

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

In the past couple of years, e-mail has become an essential work tool that many people use on a daily basis. What used to be an easy way to send jokes and letters to family and friends is now for some businesses the most important tool of their enterprise.

With the increase of people working on the road or from home, accessing the corporate e-mail has become a difficult task. Even though there exists many ways of accessing e-mail while out of the office, many of these solutions can lead to high security risks for servers on the internal network. Furthermore, it is possible for communication between the employee and the office to be altered or listened to while transmission of the e-mail occurs.

One method of accessing e-mail externally of the network is using Outlook Web Access (OWA). The purpose of this document is to show you how to harden the security on the Internet Information Service 5.0 (IIS 5.0) on a Windows 2000 server where OWA is running. Once this step has been completed, a detailed procedure on the installation and configuration of the SecureIIS software on the OWA server will be given.

What is Outlook Web Access (OWA)?

Originally created as a simple program based on ASP pages, Microsoft Outlook Web Access (OWA) has become a true e-mail client which is based on an ISAPI (Internet Server Application Programming Interface) interface. One of OWAs strongest features is its ability to utilize any web browser regardless of what platform the client is using. In short, users will have access to their e-mails via a web browser from anywhere in the world, providing they have an Internet connection. [1]

Accessing OWA

The following steps detail how to gain access to OWA:[2]

1- A user attempts to access his or her inbox by specifying the URL of the OWA server. For example: HTTP://www.toto.com/exchange.
2- The World Wide Web publication service, located on OWA, receives the request from the Web browser for a component from a folder that is virtually mapped to an Inbox or to a Public folder.
3- The IIS Web service determines the Microsoft Windows 2000 user account of the person trying to access the server and prompts him or her for authentication.

[1] Unkroth, Kay. "MCSE Trainning Kit". p, 668.
[2] Unkroth, Kay. "MCSE Trainning Kit". p, 669.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4- IIS then transmits the user's request to OWA's ISAPI interface, which obtains information from the Active Directory. A chain or request transmitted to OWA via a URL enables the system to identify which action the user is trying to execute. For example, access to an Inbox, a Public folder or even opening a particular e-mail message.
5- If the inbox resides on another computer and if the local server is configured as a front-end system, then OWA will transmit the user's request as a proxy server towards the users associated server. If the inbox finds itself on the local server, then OWA's ISAPI interface communicates with the Web storage devices using the Exchange Installable File System (ExIFS) component and the ExOLEDB provider. ExIFS is used to access streaming media (.stm) files, but does not take control of access to the properties of elements. OWA call upon ExOLEDB to extract properties from the element required to process forms.
6- Both ExIFS and ExOLEDB communicate with the Information Store.
7- Depending on the users authorization, the information store permits or refuses a user to access a resource, for example: an inbox. If the request is authorized, then the information store forwards the information to OWA.
8- OWA determines how to render the components, retrieves data from the information store, applies specific parameters for the language used and renders the page in either the HTML or XML format.
9- IIS then returns the Web page to the users web browser.

Securing the OWA 2000 Web based application

The first step of implementing OWA is configuration and security hardening the server that will host the Outlook Web Access service on the Internet.

Securing (hardening) the operating system

Outlook Web Access is a service that is included in the installation of Microsoft Exchange 2000. This product is only functional when using the following Microsoft products:[3]

- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Data Center Server

One of these operating systems must be used to make it as secure as possible to deploy Outlook Web Access (OWA). Even though this document is not intended to be a how-to harden the security of a Windows 2000 server, below are a few recommendations to follow to be sure that there is good security on the operating system.

[3] Unkroth, Kay. "MCSE Trainning Kit". p, 15.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- First of all, install the latest Service pack available for the product. (It is available at the following URL: Http://support.microsoft.com/default.aspx?scid=kb;en-us;Q260910)
- The next step is to install all the updates available for the operating system at the following URL: http://www.windowsupdate.com
- Install and run the following utilities: HFNetChK, QFCHECK to verify that all the available updates have been installed on the server.
- After installing all the necessary updates and choosing a secure physical location for the server, it is very important to secure Windows 2000 itself. In other words:
    - Make sure that all the partitions use the NTFS file system.
    - Verify that that only the TCP/IP protocol is activated on the system.
    - Disable Netbios over TCP/IP.
    - Disable File and Printer Sharing for Microsoft Networks.

Installation of a Front-end Server

Once the server that will host the Outlook Web Access (OWA) service for the users has been installed, patched and secured install Microsoft Exchange 2000 and configure it as a Front-end Server. By configuring the server as a Front-end Server, it will not contain the Information Store or any mailboxes, securing the server from hackers that will not be able to access user mailboxes uniquely by hacking the Front-end server.

The function of the Front-end server with incoming connections

The server will regroup all the incoming connections and will route them like a proxy server towards the main server or servers where the inboxes reside (Back-end server).[4] This will limit the amount of data that has a direct link to the Internet.

NB: The steps for the installation of a Front-end server are available at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/deploy/upgrdmigrate/ex2kupgr/deploy/d_08_tt1.asp

Securing the location of the server within the network architecture

The server that will host the OWA service will be accessed from the Internet. This is why we must place this server in an appropriate location without putting at risk the security of other production servers on the network.

[4] Unkroth, Kay. "MCSE Trainning Kit". p, 670

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Here are two network architectures examples.

Ex

Figure 1: Network Archite

The above diagram shows two network architectures that could be used to deploy OWA 2000. The main difference between the two rests on the fact that in example 1, only one firewall (Three-homed) is used to separate the Internet, the DMZ and the production network. In example 2, two firewalls are used; one that separates the Internet from the DMZ, and another, which separates the DMZ from the production network. Even though example 1 is very effective, example 2 has the advantage of adding another obstacle for hackers to get through before gaining access to the “Corporate Network”.

As shown in the above examples, the OWA server located in the DMZ must be able to exchange information with the Exchange 2000 server that contains the

[5] Diagram created by Dave Munger.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Information Store. This server must also communicate with the Domain Controller, which contains the Active Directory database and acts as a DNS server.

In order for these servers to communicate, all traffic can simply pass through the firewall, which becomes very insecure or only allow the following ports to pass in both directions on the firewall that separates the internal network and the DMZ (Intranet Firewall):

On Intranet Firewall Communication of the server with Active Directory	
Port number / Transport	**Protocol**
389 / TCP	LDAP to Directory Service
389 / UDP	
3268 / TCP	LDAP to Global Catalogue Server
88 / TCP	Kerberos authentication
88 / UDP	

On Intranet Firewall Communication of the server with the DNS service	
Port number / Transport	**Protocol**
53 / UDP	DNS Lookup

On Intranet Firewall Communication of the server with the e-mail services	
Port number / Transport	**Protocol**
80 / TCP	Http
143 / TCP	IMAP
110 / TCP	POP
25 / TCP 691 / TCP	SMTP Link State algorithm routing

On Intranet Firewall RPCs: Service Discovery and authentication	
Port number / Transport	**Protocol**
135 / TCP	RPC port end point
1024+ / TCP Or 1600 / TCP	All services ports (Example) RPC Service port, if restricted

Table 1: Sample of front-end back-end open ports.[6]

The above table can cause some confusion. The important thing to remember is that port 135 must be left open to let the OWA server communicate with the servers located on the internal network (Domain controller and Exchange 2000 server).

[6] Microsoft Corporation. "Exchange 2000 Windows 2000".

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Secondly you must either open a range of ports between 1024 and 65535 or configure a static port in the server's registry.

Here is how to configure this registry key.[7]
HKEY_LOCAL_MACHINE\CurrentControlSet\Services\NTDS\Parameters
Registry value: TCP/IP Port
Type of value: REG_DWORD
Value: (A port greater than 1024)

NOTE!!! The key configuration must be done on the OWA server and all servers acting as Domain controllers.

In order to give access to the external users uniquely for the OWA service, the following ports must be allowed to pass on the Internet firewall (the one which separates the Internet from the DMZ):

On Internet Firewall Communication of the server with the OWA service	
Port number / Transport	**Protocol**
80 / TCP	Http
443 / TCP	Https (SSL)

Table 2: Sample of Internet and front-end open ports.[8]

[7] Microsoft Corporation. "Exchange 2000 Windows 2000".
[8] Microsoft Corporation. "Exchange 2000 Windows 2000".

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Configuration of Group Policy's within Active Directory

Microsoft recommends that Group Policy Objects (GPO) be used when deploying security strategies on workstations and servers. Here is a look on how to configure the organizational unit structure and the application of Group Policy Objects for a Front-end server.

© SANS Institute 2003, Author retains full rights

Figure 2: Groupe policy object.[9]

According to the above diagram, three group policies are applied to the server acting as a Front-end server.

- **Domain Policy**
  The Domain Policy contains information, restrictions and policies that should be applied to all computers and users accounts of the domain.
  It is extremely important to configure the following policies at this level:
  - Password Policy
  - Account Lockout Policy

    Recommanded Settings :[10]
    - Password history = 7 passwords remembered
    - Maximum password age = 180 days (or less)

[9] Microsoft Corporation. "Chapter 3 - Securing Exchange 2000 Servers Based on Role ".
[10] Denowh, Carl. "Securing IIS on Windows 2000".

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Minimum password age = 1 day (or more)
- Minimum password length = 8
- Passwords must meet complexity requirements = Enabled
- Reversible encryption = Disabled
- Account lockout duration = 3 minutes (or more)
- Account lockout threshold = 5 (between 3 and 7)

- **Baseline Policy**
  The Baseline Policy contains information, restrictions and policies that should be applied to all servers in the network. (Servers OU)
  Applying the Baseline Policy will:
  - Choose the Auditing Policy to be used.
  - Configure and add many registry keys that will increase the level of security of the server.
    (Example: configure the server so that it will be able to defend itself against SYN FLOOD attacks.)
  - Applies more restricted permissions to the critical registry keys.
  - Applies more restricted permissions on many local files. (Example: System files, utilities that work from the command line (example: Format.com, cmd.exe, Command.com etc.))
  - Disable unnecessary services.

    For additional information on the Baseline Policy please view appendix A.

- **OWA Front-end Incremental Policy**
  The OWA Front-end Incremental Policy contains information and restrictions pertaining to the OWA server. (OWA Servers OU)
  Applying this policy will:
  - Disables many Microsoft Exchange 2000 services that are not necessary and which could represent a security threat.
    (Example: IMAP4, MS-Exchange Information Store, POP3, Microsoft Search, MS-Exchange Event, MS-Exchange Site Replication Service, MS-Exchange Management and MS-Exchange MTA)
  - Activates certain services that other policies might have disabled, which are necessary for MS-Exchange 2000 to function. (Example: World Wide Web Publishing Service)
  - Applies more restricted permissions on certain folders.

    For additional information on the OWA Front-end Incremental Policy please view appendix B.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Please note that the security models that Microsoft recommends for the Baseline Policy and the OWA Front-end Incremental Policy are available at the following URL:
http://www.microsoft.com/downloads/release.asp?releaseid=36834

Securing Internet Information Service 5.0 (IIS 5.0)

The IIS service running on the OWA server is a critical component to the exchange between the OWA server and the Back-end server (Exchange server) as it is the service that receives the e-mail requests from the Internet. So many steps must take place on the server to make sure that the IIS 5.0 application is secure from within.

Securing of the IIS "Metabase"

The IIS metabase is a data storage structure that resides in memory and contains the configuration information for IIS. It is also used to store and manage configuration parameters for the personalized IIS applications. In short it is comparable to the Windows registry. It performs the same operations with the exception that the IIS metabase is reserved for only IIS. The metabase is located by default in the %SYSTEMROOT%\System32\InetSRV\MetaBase.bin folder.[11]
To be on the safe side, it is recommended to take a backup copy of this file.
To backup the metabase folder:

- Click on Start, Programs, Administrative tools, Internet Services Manager.
- Once the console is open, right click on the computer and then click on "Backup/Restore Configuration".
- Then click on "Backup".
- To complete the task, enter the name to give to the backup copy and click "OK".

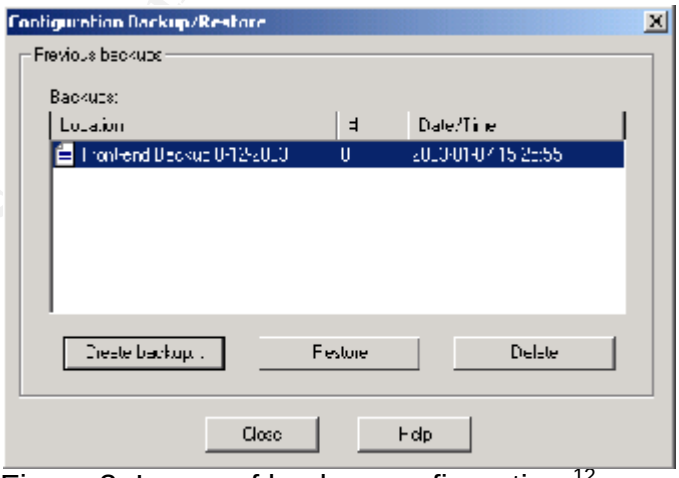


Figure 3 :Image of backup configuration.[12]

[11] Microsoft Corporation, "How TO: Hide the Metabase to Increase IIS Security".
[12] Screen capture taken from IIS Backup/Restore Configuration menu.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

It is strongly recommended to perform constant backups of the IIS metabase.

Do to the fact that the IIS metabase contains all the essential and configuration data of the web site, it is very important to secure access to this file.
To do so;

- Stop the IIS service.
- Rename and move the "MetaBase.bin" file (located in the %SYSTEMROOT%\System32\Inetsrv folder).
- Then modify the registry key indicated in the table below so that IIS will be able to reload the metabase.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InetMgr\Parameters
MetaDataFile REG_SZ
Value: Path and name of the Metabase.bin (example: c:\metabase\iismdb.bin)

Table 3 : Metabase registry key.[13]

- Be sure that only the administrator has access to modify the content of the folder where the metabase is located.
- Restart the IIS service.

Securing the IIS registry keys.

In addition to the previous configurations, the following modification of registry keys will also help harden the security of the server.

Add or modify the following registry keys.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
AllowSpecialCharsInShell REG_DWORD
Accepted values: 0, 1 **Default value:** 0 (deactivated)
This value controls whether the Cmd.exe special characters (which include | (, ; % < and >) are allowed on the command line when running batch files (.bat and .cmd files). These special characters can pose a serious security risk. If the value of this entry is set to 1, malicious users can execute commands on the server. Therefore, it is highly recommended to leave this setting as 0, the default. By default, these special characters cannot be passed to script-mapped CGI applets. If set to 1, these special characters can be passed to script-mapped CGI applets, with the exception of the pipe character (|) and the standard I/O redirection characters (< and >), which have a special meaning to the command processor.

[13] Microsoft Corporation. "How TO: Hide the Metabase to Increase IIS Security".

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
LogSuccessfulRequests REG_DWORD
Accepted values: 0, 1 **Default value:** 1 (activated)
Determines whether or not to record successful activities in the log file. The value 1 logs successful activities, and 0 turns it off.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
SSIEnableCmdDirective REG_DWORD
Accepted values: 0, 1 **Default value:** 1 (activated)
To execute shell commands, the **#exec cmd** directive of server-side includes is used. Security-conscious sites may wish to disable the **#exec cmd** directive by setting this value to 0 as an added security precaution, especially when untrusted parties are allowed to place files on the server. This value does not exist in the registry by default; to allow this directive to execute shell commands, you must first create the value and set it to 1.

Table 4: IIS Security Keys.[14]

Removal of unnecessary virtual folders

During the installation of IIS, two web sites are created by default. One used for administration that is called "Administration web site" and another with the name "Default web site". Many virtual folders are also created. The following virtual folders should be deleted, in addition to the corresponding windows folder, which are not necessary for OWA to function properly:

IIS virtual Folders that can be erased	
Virtual folder	**Default location**
/IISamples	C:\Inetpub\iissamples
/IISHelp	C:\Winnt\help\iishelp
/MSADC	C:\Program Files\common files\system\msadc
/Scripts	C:\Inetpub\scripts
/Printers	C:\Winnt\Web\Printers
/IISAdmin	C:\Winnt\system32\inetsrv\iisadmin

Table 5: Virtuel folders.[15]

To avoid unauthorized access to the administration web site, it is strongly recommended that it should be disabled.

[14] Microsoft Coporation. " WWW Service Registry Entries".
[15] Tested by Dave Munger through trial and error.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Automatic redirection of the default web site

Connecting to an Outlook Web Access server is usually established by typing the address of the server into the address bar of the users local Internet browser, followed by (/exchange). For example (http://YourServer/exchange). Now we must configure a redirection of the default web site so that it can automatically send all request made to its attention towards the "virtual/exchange" virtual folder. Here is how to configure the redirection:

1- Click on Start, Programs, Administrative tools, Internet Services Manager.
2- Right click on the "Default web site" and click on properties.
3- Browse to the "Home Directory".
4- Under the "When Connection to this resource, the content should come from:" option, select "A redirection to a URL".
5- In the "Redirect to:" box, type "/exchange".
6- To finish, select the box "A directory below this one" which finds itself under the "The client will be sent to:"

Configuration of folder security

When users connect to OWA, they make requests, view files and use forms. In order to access these files, users must have sufficient rights on these files. Here is the complete list of the folders where these files are located. Users must be able to access these files on the OWA server in order to use OWA without encountering any problems.

Outlook Web Access folders		
Folders	**Content of these folders**	**NTFS permissions**
\exchsrvr\bin	Contains server's general dll files and the executable files. Wmtemplates.dll for example, defines the default model used for the creation of HTML forms.	Everyone = Read Administrators = Full Control
\exchsrvr\exchweb\bin	Files used for the installation of the Outlook 2002 multimedia extensions program are contained in this folder.	Everyone = Read Administrators = Full Control
\exchsrvr\exchweb\controls	Contains server and client script files. IIS uses Jscript for the server and the client also receives the script elements to implement the dynamic user interface for OWA.	Everyone = Read Administrators = Full Control
\exchsrvr\exchweb\lang	Contains the local OWA help files, which are only created if	Everyone = Read Administrators = Full

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

	languages other than English are activated.	Control
\exchsrvr\exchweb\img	Contains logos and other graphics that are used by OWA, such as Logo-ie5.gif and Icondoc-excel.gif. You can replace these files by personalized versions in order to modify the user interface of OWA.	Everyone = Read Administrators = Full Control

Table 6: Exchange folder.[16]

[16] Microsoft Corporation. " Exchange 2000 Outlook Web Access ".

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Removal of application mappings

In order to determine if ISAPI or CGI should be used to execute requests made on the Web server, the (IIS) Internet services will use the file extension name of the requested resource. For example, when requesting a file with the .asp extension, the Web server will call upon the ASP (asp.dll) program in order to process the request. Application mapping occurs when a filename extension is associated to an ISAPI or CGI program. IIS is preconfigured to take control of all application mappings. By default IIS maps several scripts for ISAPI applications. The removal of some of these mapped scripts increases IIS's level of security.[17]

Here is how to proceed:

1- Click on Start, Programs, Administrative tools, Internet Services Manager.
2- Then right click on "Default Web Site" and click on properties.
3- Click on "Home Directory".
4- Now click on "Configuration".
5- The following dialog box will show on the screen:

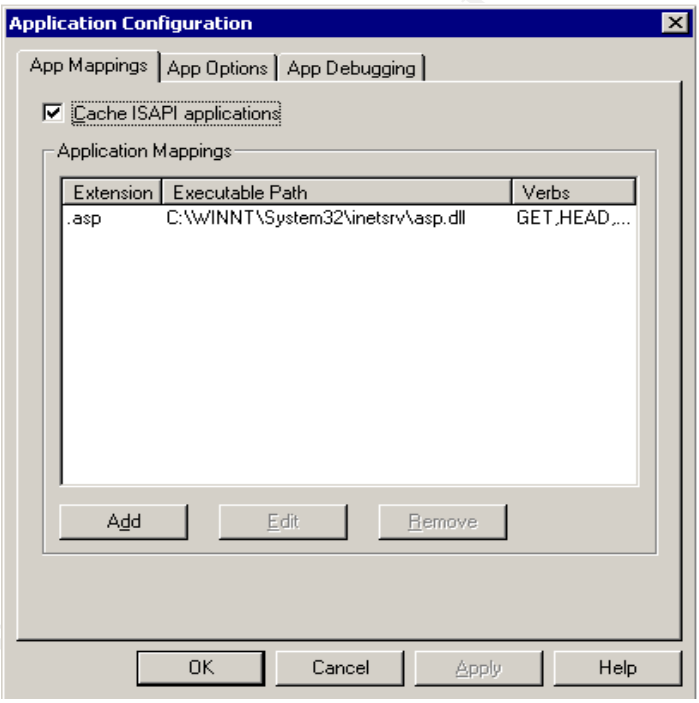


Figure 4 : Application mappings.[18]

6- Delete all mapped scripts with the exception of the one for "Active Server Page" (.asp) as shown above.

[17] Microsoft Corporation. "Secure Internet Information Services 5 Checklist".
[18] Screen capture taken from IIS Application Configuration dialog box.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Policy Configuration in Windows 2000

Windows 2000 contains policies that let administrators restrain access to a computer, therefore increasing the level of security. Right now, we are interested in two policies.

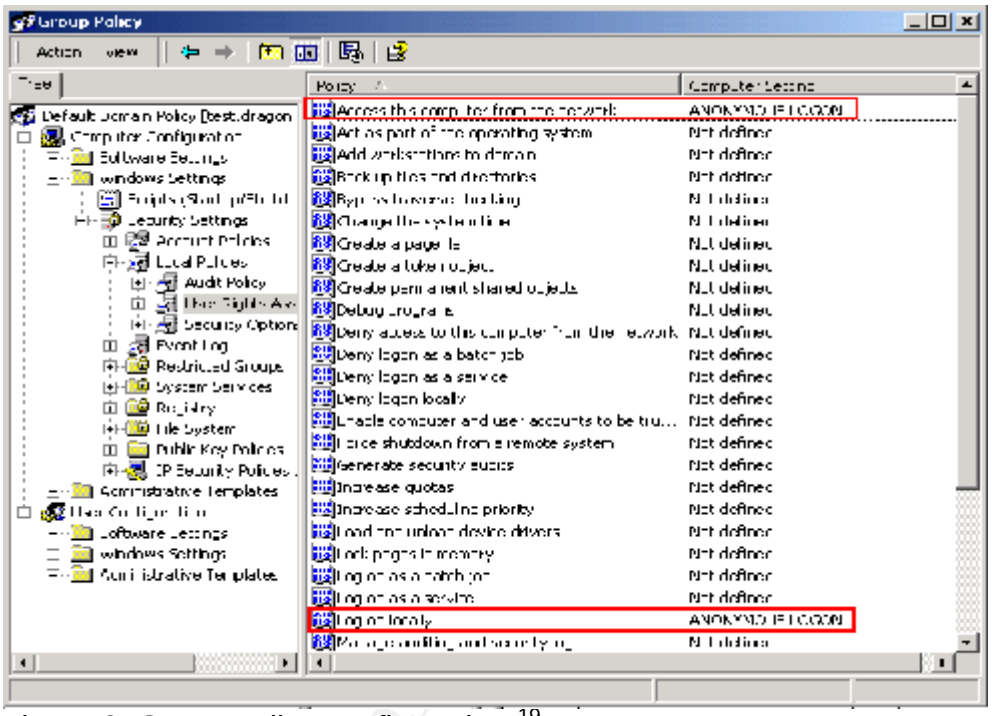


Figure 8: Group policy configuration.[19]

If the two policies have already been configured on the computer, the following information needs to be add[20]:

- Log on Locally = Anonymous Users
- Access this computer front Network = Anonymous Users

The configured policies must absolutely contain the above information. If not the users will not be able to connect to their inboxes. For added security an administrator can configure the policies by replacing "Anonymous Users" to "Domain Users" restricting access to the server to only Domain Users. However if only "Domain Users" is selected, the users "Public Folders" will not be accessible from OWA.

[19] Screen capture taken from Group policy management console.
[20] Microsoft Corporation, « XWEB: Permissions Required for Outlook Web Access».

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Quick Compare [21]

Anonymous Users

- Pros > Access to all user folders including the Public Folders.
- Cons > less secure do to the fact that access to the server is open to all.

Domain Users

- Pros > Restricts access to the server to only users that are defines as Domain Users.
- Cons > Users will not be able to access their Public Folders.

Configuration of the Web Site Operators

The "Operators" tab under the properties of the web site permits administrators to specify which users or user groups will be considered as "Operator" of the web site.
The tasks that a "Web Site Operator" will handle are:[22]

- Configuration of permissions to access the Web site.
- Activate auditing (logging).
- Modify the default document or the default footer.
- Modifications to the properties of the http headers.

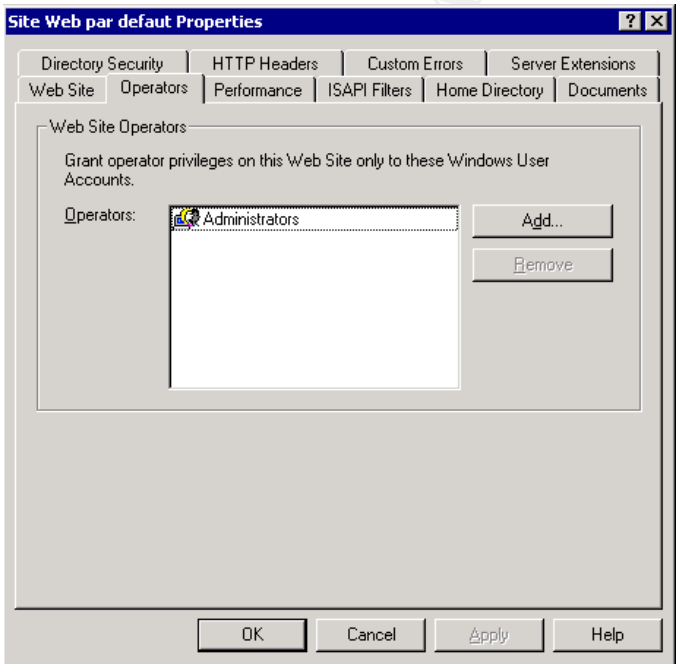


Figure 9 :IIS Operators.[23]

[21] Tested by Dave Munger through trial and error.
[22] Microsoft Corporation. " Web Site Operator Capabilities and Limitations ".
[23] Screen capture taken from IIS Default Web site properties under Operators tab.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Securing the client-server communication with SSL

Imagine that at this very moment, a user is reading their e-mail from home using OWA. If a hacker captures the exchange of information made between the users computer at home and the Exchange server at work at the moment in which data is being transferred across the Internet, he would most probably have access to the users confidential information.

IIS fixes this problem by permitting the implementation of the SSL protocol, which relies on public and private certificates, better known as public key encryption. SSL assures the integrity and confidentiality of data transmitted over a public network.

Encryption by means of public keys implies the use of two corresponding keys, a private key and a public key.

1. The user's Web browser establishes a secure (https://) communication link with the Web server.
2. The user's Web browser and the server engage in a handshake exchange in order to determine the encryption level to use to secure the communication.
3. The Web server sends its public key to the user's Web browser.
4. The Web browser then encrypts the information used to generate a session key with the Web server's public key and sends it to the Web server.
5. With the help of the private key, the Web server deciphers the message, generates a session key, encrypts the session key using the public key and sends it to the user's Web browser.
6. The Web server and the Web browser both use the session key to encrypt and decipher the transmitted data.

Figure 10: SSL communication.[24]

[24] Diagram created by Dave Munger.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Level of encryption:

The Web server can be configured to demand a session key with a minimum of 128 bits of encryption, instead of the default value of 40 bits, for all SSL communication sessions. However, if a minimum level of 128 bits is determined then the user who tries to establish a secure communication channel with the Web server must use a Web browser with the capabilities of communicating with a session key of 128 bits.

Please consult the following Web page to review the details of certificate installation.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/maintain/featusability/c06iis.asp

Auditing configuration

Event recording from IIS

Through IIS, it is possible to record information relative to the Web sites. This information can then be used to troubleshoot a problem regarding IIS or even help plan security needs. These recorded events are available in a file located in the %WinDir%\System32\LogFiles folder.[25]

It is a good security practice to configure the following NTFS permissions on this folder to avoid unauthorized modification to the content of the log files.

Administrators = Full Control
Everyone = Read Only

[25] Taken from properties of IIS default web site.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Here is how to activate and configure auditing within IIS.

1- First of all, open the “Internet Services Manager” (Click on Start, Programs, Administrative Tools, Internet Services Manager).
2- Next, right click on the Web site and click on properties.

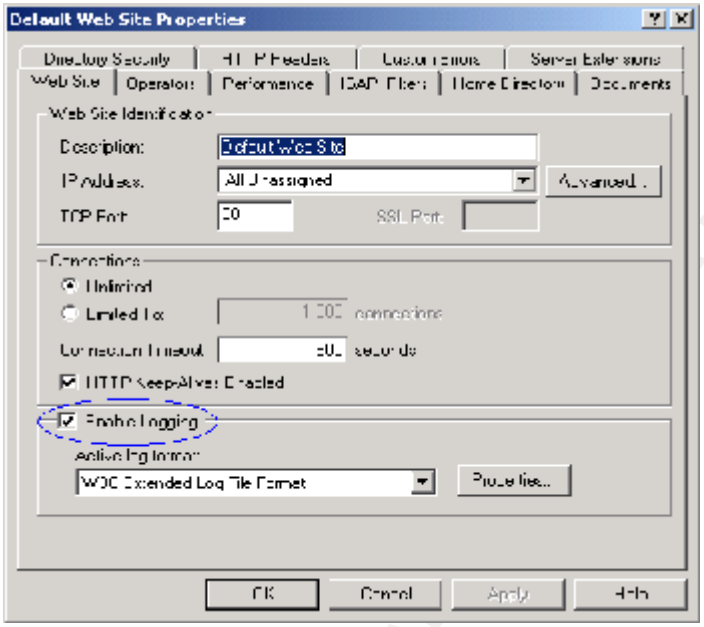


Figure 11: Enabling Logging.[26]

3- To activate the recording into a journal log file, check the following box “Enable Logging” as illustrated above.
4- Then it will be possible to choose four types of formats for the event journal.
   - W3C Extended Log File Format
   - NCSA Common Log File Format
   - Microsoft IIS Log File Format
   - ODBC Logging

The most used and recommended of these four formats is the W3C. It can be personalized to include the following fields in the log file: (Source IP address, User, Date, Time etc…). The NCSA and IIS formats include less information in the log file than W3C and do not permit a personalized view.

Using the W3C format, here are the steps involved to create a personalized view of the log file.

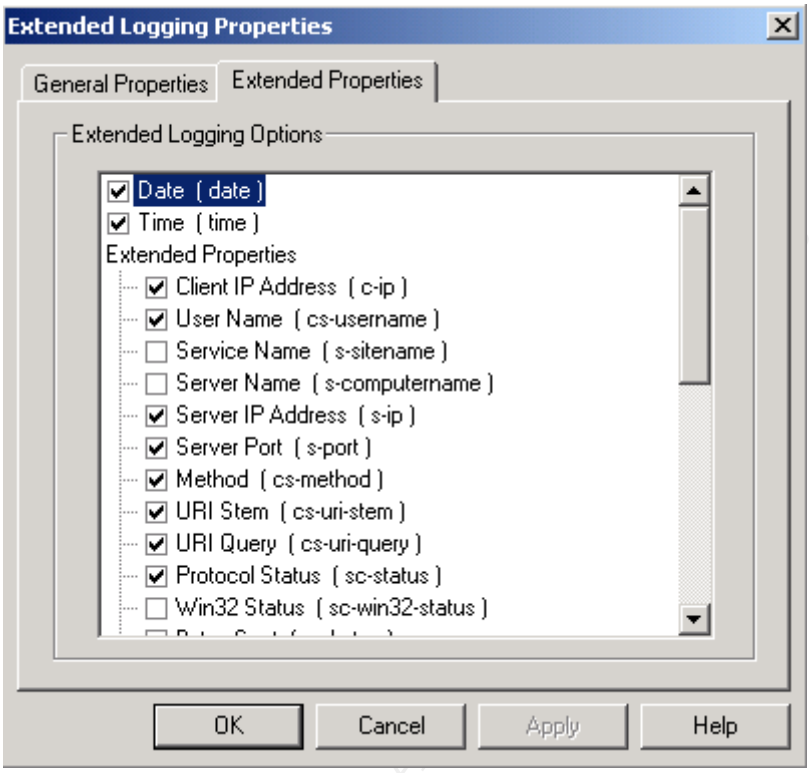
1- First, open the ‘’ Internet Services Manager ‘’. (Click on Start, Programs, Administrative Tools, Internet Services Manager)
2- Make sure that W3C is the active format.

[26] Screen capture taken from IIS Default Web Site properties.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3- Click on Properties.
4- Now click on Extended Properties.



Picture 12: Logging properties.[27]

5- You can now choose the desired fields from the list.

Though the W3C format is the most used format of logging, it is not the most secure. That title goes to the ODBC format. With this format you can record log files into a table on a database server. This way, the log files are never recorded on the local server. The downside and the reason why the ODBC format is not as used as the W3C format is due to the fact that ODBC requires the use of a SQL server and a lot more configuration.

Recording of events from Windows 2000

Windows 2000 permits the recording of certain types of events. Here are the options that should be audited to increase the level of security on the server.

- "Account logon Event": Success and Failure
- "Logon event auditing": Success and Failure

[27] Screen capture taken from IIS logging properties.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

By consulting the security journal located in the event viewer, an administrator can see the results of the events and determine attacks. By default unsuccessful attempts will be shown.

Now lets take a look at how to add a level of security under IIS 5.0 and Outlook Web Access with the help of SecureIIS by Eeye.

Introduction to SecureIIS

Application vulnerabilities are responsible for most of today's hacker attacks. OWA works with IIS 5.0 and although IIS is a very good product, it has many security holes and is often the target of many attacks.

Microsoft develops and regularly makes security updates available on its Web site in order to counter these attacks. Even though updates are constantly applied, the server still remains a potential target for hackers. It is therefore highly recommended that additional software be used to secure every request made to the IIS service via the Web. Two software's that are highly recommended to perform this task are: IISLockdown and SecureIIS. In this case SecureIIS 2.0.2 will be discussed and configured.

SecureIIS is a product that was developed by Eeye Digital Security. It is an application firewall, which operates with IIS and inspects all requests made to IIS without diminishing the performance of the Web server.

SecureIIS protects against the following attack types: [28]

- **Buffer Overflow Attacks**
  SecureIIS checks the lengths of all client-supplied buffers. If the data is larger than the maximum size allowed SecureIIS would drop the connection, thereby avoiding a buffer overflow.
- **Parser Evasion Attacks**
  Insecure string parsing can allow attackers to remotely execute commands on the machine running the web server. SecureIIS checks for various characters in a string that would allow an attacker to add on commands to a normal value. If these characters are found, SecureIIS will drop the connection.
- **Directory Traversal Attacks**
  In certain situations, various characters and symbols can be used to break out of the web server's root directory and access files on the rest of the file system. SecureIIS checks for these characters and also blocks access to specific directories.
- **General Exploitation**
  By checking for common attacker "payloads" such as cmd.exe in the

[28] Eeye. Within the SecureIIS Help.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

exploiting data, SecureIIS can prevent an attacker from gaining unauthorized access to the web server and its data.

- **High-Bit Shellcode Protection**
  Normal English-language web traffic does not contain high-bit characters. SecureIIS will drop all requests containing high-bit characters, which often signal a potential buffer overflow attack.
- **RFC Compliancy**
  SecureIIS prevents attackers from manipulating the HTTP protocol in attempts to bypass security systems and exploit security holes.
- **Other Attacks**
  SecureIIS has additional checks in place to identify — and drop — requests that contain recognized patterns. Limitations are also placed on the size of uniform resource locators (URL/URI), HTTP variables, request methods, request header size and other HTTP-related content.

Installation of SecureIIS on the server

Here are the steps for deploying SecureIIS with the objective of securing access to the OWA server:

1- Before installing, verify that the downloaded was properly done and all security updates available on Microsoft's Web page were installed from the following URL: http://www.windowsupdate.com.
2- Secondly, download the software. To do this, communicate with the vendor to buy the product. They will send a copy of the software or a demo can be downloaded that is valid for 15 days at the following URL: http://www.eeye.com/html/products/SecureIIS/Download.html.
3- Next proceed to the installation of the software by clicking on the following file "SecureIIS201Demo.exe". The welcome window will then appear, click on next.
4- Read and check the "I accept the terms of the license agreement" box to accept the terms of the license and click next.
5- The installation program will then display some recommendations (that it is preferable to close and exit all applications before continuing with the installation). Click next to continue.
6- The installation program will show where the installation files will be located.
7- A prompt window will pop up asking if a backup of the files that will be replaced during the installation is wanted. By taking a copy of these files, an administrator has the possibility of uninstalling the product and restoring the original configuration. Choose yes to make a backup and select a destination folder for the file, if not click on no.
8- Click on next to continue.
9- Then click on next to copy the installation files. (Before clicking on next, make sure you have the Windows 2000 CD-ROM with you. You might need it during the installation.)

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10- Once the program is installed, click on click on Finish to terminated the installation and the SecureIIS administration console will appear on the screen).

Now secure the OWA server with SecureIIS.

Here is how to optimize the configuration of SecureIIS to adapt it to the system.

1- Open the SecureIIS console. (Start, Programs, SecureIIS)

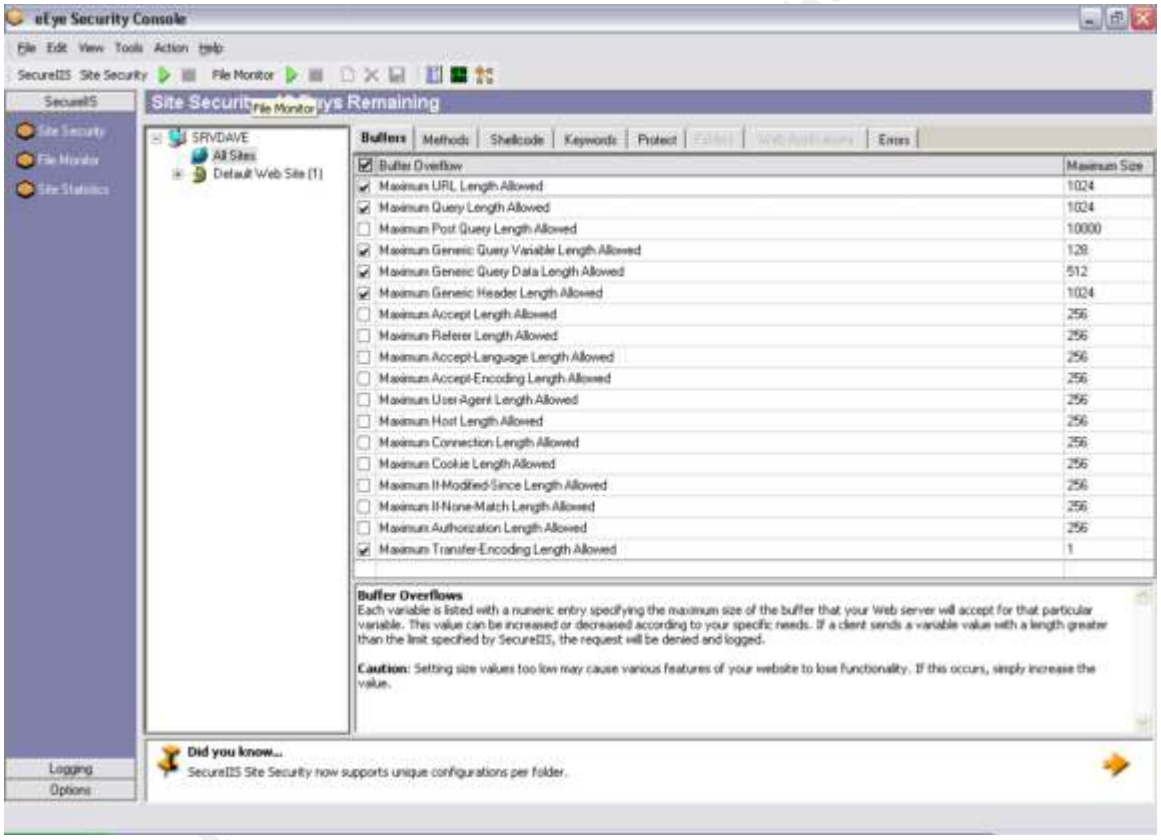


Figure 13 : SecureIIS Console.[29]

2- Click on Site Security and then click on “Default Web Site”.

3- Now click on “Web Applications” and check the box beside “Enable Outlook Web Access 2000”. This will load all secure configurations that are predefined in the SecureIIS software.

[29] Screen capture taken from SecureIIS console.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Note : The settings in the following steps have been taken from the default configuration of SecureIIS after selecting the OWA checkbox in the Web Applications tab. Steps 4 to 11 should already be configured and are provided only to verify that no previous modifications have been made prior to the selection of the OWA checkbox.

4- Click on the "Buffers" tab and check all the options. Configure these options so that they correspond with the table shown below:

Buffer Overflow	**Maximum Size**
Maximum URL Length Allowed	1024
Maximum Query Length Allowed	1024
Maximum POST Query Length Allowed	10000
Maximum Generic Query Variable Length Allowed	128
Maximum Generic Query Data Length Allowed	512
Maximum Generic Header Length Allowed	1024
Maximum Accept Length Allowed	256
Maximum Referrer Length Allowed	256
Maximum Accept-Language Length Allowed	256
Maximum Accept-Encoding Length Allowed	256
Maximum User-Agent Length Allowed	256
Maximum Host Length Allowed	256
Maximum Connection Length Allowed	256
Maximum Cookie Length Allowed	256
Maximum If-Modified-Since Length Allowed	256
Maximum If-None-Match Length Allowed	4000
Maximum Authorization Length Allowed	1

Table 7: Buffer Overflow Settings

This tab lets the administrator restrict the size of data that is transmitted to the OWA server via a Web browser. SecureIIS can verify the size at certain levels of the packet and of the requests made via the Web browser.

To obtain the list of locations where the size of requests can be limited, please refer to Buffers under (Site Security) in the integrated help of SecureIIS.

5- Click on the "Methods" tab and select only the following methods:

- GET
- POST
- DELETE
- MKCOL
- PROPFIND

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- PROPPATCH
- SEARCH

Methods

Enables you to permit or refuse the use of certain http methods. (GET, POST etc…)

To obtain a description of the default methods in IIS, please refer to Methods under (Site Security) in the integrated help of SecureIIS.

6- Click on the "Shellcode" tab and make sure that all methods are checked with the exception of "High Bit shellcode Protection in Post Data".

- High Bit Shellcode Protection in URL.
- High Bit Shellcode Protection in Query.
- High Bit Shellcode Protection in Header.

Shellcode Protection

This tab permits you to activate options so that SecureIIS can search for "High-bit" data that resembles "Shellcode". When this property is activated SecureIIS drops any connection that contains "High-bit" data.

To obtain a description of the default methods, please refer to Shellcode under (Site Security) in the integrated help of SecureIIS.

7- Click on the "Keywords" tab and enter the below words. Make sure that the following list of words is entered correctly:

Keywords	URL	Query String	Header	Post
CMD.EXE	X	X	X	X
SYSTEM32	X	X	X	X
ROOT.EXE	X	X	X	X
XP_CMDSHELL	X	X	X	X
COPY	X	X	X	X
COMMAND	x	X	X	X

Table 8: Keyword

Keywords

Stops hackers from accessing the server by using certain key words, like CMD, ROOT etc… Everyday hackers try to execute Shell commands on servers to take control of them. SecureIIS permits key words whether they are in the URL, the query string, and the header or in POST to be blocked.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

8- Click on the “Protect” tab and verify that all these methods are checked.

- Protect against Directory Traversal Exploits in URL.
- Protect against Directory Traversal Exploits in Headers.
- Protect against Directory Traversal Exploits in Query String.
- Protect against Directory Traversal Exploits in Post Data.
- Protect against Encoding Abuse Exploits in URL.
- Protect against Encoding Abuse Exploits in Headers.

Protect

The “Protect” tab allows the administrator to disable unused data schemes that can be used to bypass security systems such as the %u encoding IDS bypass vulnerability.

To obtain a description of all these methods, please refer to Protect under (Site Security) in the integrated SecureIIS help.

9- Click on the “Folders” tab
This tab lets an administrator configure access to a site and to folders. An example of this would be if a folder on the Web site contains data that should not be accessed by a Web user, then the administrator should restrict the access by checking the box located to the left of the folder. If certain folders are missing, be sure to add them. However if there are folders present that do not appear on the list below, they should be deleted. Make sure that only the following folders are selected:

- C:\Program files\exchsrvr\exchweb
- C:\Program files\exchsrvr\exchweb\bin
- M:\yourdomain.com\public folders
- M:\yourdomain.com\mbx
- \\.\backofficestorage

10- Click on the “File Monitor” tab located to the left of the screen. Then click on “Folders”, and add the following folders:

Path	Recursive	Add	Remove	Modify	Rename
C:\		X	X	X	X
C:\winnt\system32		X	X	X	X
C:\Document and settings	X	X	X	X	X
C:\inetpub\wwwroot		X	X	X	X
C:\program files\common files\Microsoft shared\web server extensions\40\isapi		X	X	X	X
C:\winnt\web\printers		X	X	X	X
C:\program		X	X	X	X

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

files\exchsrvr\exchweb					
M:\yourdomain.com\public folders		X	X	X	X
M:\yourdomain.com\mbx		X	X	X	X
\\.\backofficestorage		X	X	X	X

Table 9: Path configuration

Folders

This tab lets you specify which folders you would like to observe. To audit the behavior of a particular folder, you must first click on "Click here to add a new item", then type the folder's path, check the box to the left of the folder to indicate to SecureIIS that it must audit this folder and select the actions that you wish to observer in the folder. The choices are between Recursive, Add, Remove, Modify and Rename.

11- Click on the "Files" tab and add the following files:

Files	Remove	Modify	Rename
C:\winnt\system32\cmd.exe	X	X	X
C:\winnt\explorer.exe	X	X	X
C:\winnt\system32\command.com	X	X	X

Table 10: File Configuration

Files

Allows an administrator to specify what files on the server to audit. All that needs to be done is enter the name and full path of the file that will be audited by clicking on "Click here to add a new item'', check the box located to the left of the file and to finish select a methods to observe. The possible methods available are: Remove, Modify and Rename.

12- Click on "Action" then on "Apply changes".

13- Now arm the "Site Security" module by clicking on Action, Arm Site Security and arm the "File Monitor" module by clicking on Action, Arm File Monitor.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Information

Even though SecureIIS is an excellent tool to secure the Web server, it also has its disadvantages. For security reasons, SecureIIS will restrain many of the actions that the users can carry out on the Web server.

Here are some of the actions that will not work via OWA:[30]

- The users will be unable to move folders within their inboxes. (Methods Http: BMOVE & MOVE)
- The users will be unable to empty the folder "deleted items". (Methods Http: BMOVE & MOVE)
- The OWA2000 function that warns users every two minutes if they have new mail will not work either. (Method Http: POLL)
- Automatic updates via the RVP (Rendezvous) will stop. (Method Http: SUBSCRIBE)

For the above mentioned actions be activated, the following methods must be activated:

- BMOVE
- MOVE
- POLL
- SUBSCRIBE

Caution: Activating these methods will lower the level of security and SecureIIS will not be as effective.

Working with « Log Viewer »

Once SecureIIS is configurated and put in place on the server hosting the OWA service, it is possible to view the activities going on. SecureIIS's "Log Viewer" will let you see if people are attempting to attack the server.

Troubleshooting

At certain times, it is possible that an administrator will execute a task and without knowing why, the Web site stops responding. For example if a method in SecureIIS that allows the users use the Web site is unchecked then the Web site will no longer work properly. To fix this problem, execute the method in question on the Web site and an event will be written to SecureIIS's event log. This event will also indicate which method must be activated for the users to be able to execute the desired task.

[30] Tested by Dave Munger through trial and error.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

This document described how to secure Microsoft's Exchange 2000 Outlook Web Access service running on Windows 2000 server. It explained in detailed steps how to secure a server hosting this service, secure the IIS service and add additional security by installing SecureIIS. Going through all the setup steps, it is necessary to consider all aspects of security. They must be thought out, treated, analyzed and executed in the best way possible in order to obtain an effective secure solution.

Appendix A

Here are the policies that must be imported in the GPO, under the « Servers » organizational unit.[31]

```
Baseline.inf
; Security Configuration Template for Security Configuration Editor
;
; Template Name:       Baseline.INF
; Template Version:    05.00.HW.0000

[Profile Description]
%SCEBaselineProfileDescription%

[version]
signature="$CHICAGO$"
Revision=1

[System Access]
ForceLogoffWhenHourExpire = 1

;-----------------------------------------------------------------
;Event Log - Log Settings
;-----------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

[System Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1

[Application Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1

;-------------------------------------------------------------------
```

[31] Baseline.inf file avalaible from Microsoft web site.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
;           Local Policies\Audit Policy
;-----------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 2
AuditAccountLogon = 3
CrashOnAuditFull = 1

;-----------------------------------------------------------------
;Registry Permissions
;-----------------------------------------------------------------
[Registry Keys]

"MACHINE\Software",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\Software\Classes",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(
A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\SystemCertificates",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;
CI;GA;;;SY)(A;CI;GA;;;CO)"

;The following keys do not exist when we run
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Accessibility",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;
CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AEDebug",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO
)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)(A;CI;GRGWSD;;;BO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Classes",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Drivers32",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO
)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\EFS",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font
Drivers",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\FontMapper",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;
CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,"D:AR"
```

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\ProfileList",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;C
O)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\SecEdit",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY
)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Svchost",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time
Zones",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Windows",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO
)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO
)"
"MACHINE\System",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SYSTEM\Clone",1,"D:AR"
"MACHINE\SYSTEM\ControlSet001",1,"D:AR"
"MACHINE\SYSTEM\ControlSet002",1,"D:AR"
"MACHINE\SYSTEM\ControlSet003",1,"D:AR"
"MACHINE\SYSTEM\ControlSet004",1,"D:AR"
"MACHINE\SYSTEM\ControlSet005",1,"D:AR"
"MACHINE\SYSTEM\ControlSet006",1,"D:AR"
"MACHINE\SYSTEM\ControlSet007",1,"D:AR"
"MACHINE\SYSTEM\ControlSet008",1,"D:AR"
"MACHINE\SYSTEM\ControlSet009",1,"D:AR"
"MACHINE\SYSTEM\ControlSet010",1,"D:AR"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;CI;GA;;;BA)(A;;GR;;;BO)
"
"MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security",2,"D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;
CO)"

;Allowed Paths
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",2,"D:(A;CI;GR;;;WD)"
;NT CurrentVersion is also an allowed path

"MACHINE\SYSTEM\CurrentControlSet\Enum",1,"D:AR"

"MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles",1,"D:AR"

"USERS\.DEFAULT",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"USERS\.DEFAULT\Software\Microsoft\NetDDE",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"USERS\.DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,"D:AR"

[File Security]
;-----------------------------------------------------------------------------------------
;x86 Boot Files
;-----------------------------------------------------------------------------------------
"%SystemDrive%\boot.ini",2,"D:PAR(A;CIOI;FA;;;BA)(A;CIOI;FA;;;SY)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;CIOI;FA;;;BA)(A;CIOI;FA;;;SY)"
"%SystemDrive%\ntldr",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
"%SystemDrive%\io.sys",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
```

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;CIOI;FA;;;BA)(A;CIOI;0x1200a9;;;AU)(A;CIOI;FA;;;SY)"
"%SystemDrive%\config.sys",2,"D:P(A;CIOI;GXGR;;;AU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
"%SystemDrive%\",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"

;-----------------------------------------------------------------------------------------
;System Drive (\)
;-----------------------------------------------------------------------------------------
"%ProgramFiles%",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemDrive%\Documents and Settings",1,"D:PAR"
"%SystemDrive%\Inetpub",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;WD)(A;OICI;FA;;;SY)"

;-----------------------------------------------------------------------------------------
;System Root (Typically \WINNT)
;-----------------------------------------------------------------------------------------
"%SystemRoot%",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)(A;CIOI;GRG
X;;;WD)"
"%SystemRoot%\explorer.exe",2,"D:(A;CIOI;GRGX;;;WD)"

;Ignored Dirs do not exist when security applied during setup.
"%SystemRoot%\CSC",1,"D:AR"
"%SystemRoot%\debug",1,"D:AR"
"%SystemRoot%\Offline Pages",1,"D:AR"
"%SystemRoot%\Profiles",1,"D:AR"
"%SystemRoot%\Registration",1,"D:AR"
"%SystemRoot%\repair",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Temp",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

;New Dirs for Windows 2000
"%SystemRoot%\addins",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\Connection
Wizard",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\Driver
Cache",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\java",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\msagent",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\security",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\speech",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\twain_32",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\Web",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"

;-----------------------------------------------------------------------------------------
;System Directory (Typically \Winnt\System32)
;-----------------------------------------------------------------------------------------

"%SystemDirectory%",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)(A;CIOI;
GRGX;;;WD)"

;Dirs which do not exist when security applied during setup.
"%SystemRoot%\system32\appmgmt",1,"D:AR"
"%SystemRoot%\system32\DTCLog",1,"D:AR"
"%SystemRoot%\system32\GroupPolicy",1,"D:AR"
"%SystemRoot%\system32\NTMSData",1,"D:AR"
"%SystemRoot%\system32\Setup",1,"D:AR"
"%SystemRoot%\system32\ReinstallBackups",1,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A
;CIOI;GA;;;CO)"
"%SystemRoot%\system32\repl",1,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;C
O)"
"%SystemRoot%\system32\repl\import",1,"D:(A;CIOI;GRGWGXSD;;;RE)"
"%SystemRoot%\system32\repl\export",1,"D:(A;CIOI;GRGWGXSD;;;RE)"
"%SystemRoot%\system32\spool\printers",1,"D:P(A;CI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;
GA;;;CO)"
```

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
;Dirs that are different from parent
"%SystemRoot%\system32\config",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\system32\logfiles",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\system32\dhcp",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;C
O)"
"%SystemRoot%\system32\dllcache",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\system32\drivers",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;
;CO)"

;New Dirs for Windows 2000
"%SystemRoot%\system32\CatRoot",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA
;;;CO)"
"%SystemRoot%\system32\ias",2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%SystemRoot%\system32\mui",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;C
O)"
"%SystemRoot%\system32\ShellExt",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA
;;;CO)"
"%SystemRoot%\system32\wbem",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;
CO)"
"%SystemRoot%\system32\wbem\mof",2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;
GA;;;CO)"

;ACL System32 command files
"%SystemRoot%\system32\append.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\at.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\attrib.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\cacls.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\cmd.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\command.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\cscript.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\debug.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\exe2bin.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\finger.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\ftp.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\hostname.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\mmc.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\mountvol.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\nbtstat.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\net.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\net1.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\netsh.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\netstat.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\nslookup.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\ntsd.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\pathping.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\ping.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\regini.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\regsvr32.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\route.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\runas.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\runonce.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\share.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\telnet.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\termsrv.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tftp.exe",2,"D:PAR(A;OICI;FA;;;BA)"
```

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
"%SystemRoot%\system32\tracert.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tsadmin.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tscon.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tskill.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tsprof.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tsshutdn.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\wscript.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\xcopy.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\arp.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\change.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\chglogon.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\chgport.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\chguser.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\chkdsk.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\chkntfs.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\cipher.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\cluster.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\compact.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\convert.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\dfscmd.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\doskey.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\edlin.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\expand.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\fc.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\find.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\findstr.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\forcedos.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\iisreset.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\ipxroute.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\label.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\logoff.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\lpq.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\lpr.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\makecab.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\mem.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\msg.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\print.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\query.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\rasdial.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\recover.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\register.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\replace.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\reset.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\setpwd.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\shadow.exe",2,"D:PAR(A;OICI;FA;;;BA)"I
"%SystemRoot%\system32\snmp.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\snmptrap.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\subst.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tsdiscon.exe",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\chcp.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\diskcomp.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\diskcopy.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\format.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\mode.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\more.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\tree.com",2,"D:PAR(A;OICI;FA;;;BA)"
"%SystemRoot%\system32\usrmgr.com",2,"D:PAR(A;OICI;FA;;;BA)"

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
```

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users
SceInfProgramFiles = Program Files
SceBaselineProfileDescription = Increases SecureWS Settings. Restricts Power User and Terminal Server ACLs.

[Registry Values]
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
MACHINE\System\CurrentControlSet\Control\LSA\MSV1_0\NtlmMinServerSec=4,536870912
MACHINE\System\CurrentControlSet\Control\LSA\NoLMHash=4,1
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta=4,10
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxPortsExhausted=4,5
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmission
s=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,
0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=1,
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1

[Service General Setting]
Alerter,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;WD)"
AppMgmt,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;WD)"
BINLSVC,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;WD)"
CertSvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
ClipSrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
ClusSvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
EventSystem,3,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOC
RSDRCWDWO;;;WD)"
Browser,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
DHCPServer,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCR
SDRCWDWO;;;WD)"
Dhcp,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;WD)"
Dfs,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCW
DWO;;;WD)"
TrkWks,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
TrkSvr,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;WD)"
MSDTC,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
Dnscache,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;WD)"
DNS,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;WD)"
Eventlog,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;WD)"
Fax,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCW
DWO;;;WD)"
NtFrs,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;WD)"
MacFile,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDR
CWDWO;;;WD)"
MSFTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCR
SDRCWDWO;;;WD)"
```

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IISADMIN,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
cisvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
IAS,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SharedAccess,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
IsmServ,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
PolicyAgent,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
kdc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LicenseService,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
dmserver,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
dmadmin,3,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MSMQ,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Messenger,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
mnmsrvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Netman,3,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDE,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDEdsdm,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NntpSvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NtLmSsp,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NSLService,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Netlogon,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NWCWorkstation,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SysmonLog,3,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
PlugPlay,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MacPrint,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Spooler,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ProtectedStorage,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RSVP,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RasAuto,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RasMan,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RpcSs,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RpcLocator,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

RemoteRegistry,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Remote_Storage_Engine,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Remote_Storage_File_System_Agent,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Remote_Storage_Subsystem,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Remote_Storage_User_Link,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NtmsSvc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RemoteAccess,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RSVP,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
seclogon,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SamSs,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
lanmanserver,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SimpTcp,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Groveler,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LDAPSVCX,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NwSapAgent,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SCardSvr,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SCardDrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SNMP,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SNMPTRAP,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SENS,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LmHosts,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LPDSVC,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TapiSrv,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TlntSvr,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TermService,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TermServLicensing,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TFTPD,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
UPS,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
UtilMan,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

MSIServer,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
WINS,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
WinMgmt,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Wmi,3,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
nsmonitor,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
nsprogram,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
nsstation,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
nsunicast,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
W32Time,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
lanmanworkstation,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
W3SVC,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Appendix B

Here are the policies that must be imported in the GPO, under the «OWA Servers » organizational unit.[32]

OWA FrontEnd Incremental.inf

```
; Security Configuration Template for Security Configuration Editor
;
; Revision History
; 0000  -      Original

[Profile Description]
%SCEOWAProfileDescription%

[version]
signature="$CHICAGO$"
Revision=1

[Strings]
SceOWAProfileDescription = Incremental Policy that allows Exchange 2000 to function as an OWA Exchange Front End server.

[File Security]
"%SystemDrive%\inetpub\mailroot",2,"D:PAR(A;OICI;FA;;;DA)(A;OICI;FA;;;SY)"
"%SystemDrive%\inetpub\nntpfile",2,"D:PAR(A;OICI;FA;;;DA)(A;OICI;FA;;;SY)"
"%SystemDrive%\inetpub\nntpfile\root",2,"D:PAR(A;OICI;GA;;;WD)"

[Service General Setting]
msexchangees,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
imap4svc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
msexchangeIS,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

[32] OWA FrontEnd Incremental.inf file avalaible from Microsoft web site.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

msexchangemgmt,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
msexchangemta,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
pop3svc,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
resvc,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
msexchangesrs,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
msexchangesa,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
mssearch,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RpcLocator,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
iisadmin,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
W3SVC,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
PolicyAgent,2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

Citations:

1-2-3-4. Microsoft Corporation & Unkroth, Kay. MCSE Training Kit, Microsoft Exchange 2000 Server implémentation et administration. Microsoft Press, 2002. 667-686 & 15.

5. Diagram created by Dave Munger.

6-7-8. Microsoft Corporation, « Exchange 2000 Windows 2000 Connectivity Through Firewalls ». Article ID: Q28013. Revised October 3, 2002. URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q280132& (December 12, 2002).

9. Microsoft Corporation, « Chapter 3 - Securing Exchange 2000 Servers Based on Role ». URL : http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/opsguide/e2ksec03.asp (December 15, 2002).

10. Denowh, Carl. “Securing IIS on Windows 2000”. Published March 6, 2001. URL : http://www.sans.org/rr/win2000/sec_IIS.php (January 15, 2003).

11. Microsoft Corporation, « How TO: Hide the Metabase to Increase IIS Security ». Article ID: Q321142. Revised October 26, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb;en-us;321142 (December 15, 2002).

12. Screen capture taken from IIS Backup/Restore Configuration menu.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

13. Microsoft Corporation, « How TO: Hide the Metabase to Increase IIS Security ». Article ID: Q321142. Revised October 26, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb;en-us;321142 (December 15, 2002).

14. Microsoft Coporation, « WWW Service Registry Entries ». URL : http://www.microsoft.com/windows2000/en/server/iis/htm/core/iiregwww.htm (January 13, 2003).

15. Tested by Dave Munger through trial and error.

16. Microsoft Corporation, « Exchange 2000 Outlook Web Access ». Revised May 2002. URL : http://www.microsoft.com/exchange/techinfo/outlook/2000/0WA2000.asp. E2K_OWA.DOC page 16. (December 7, 2002).

17. Microsoft Corporation, « Secure Internet Information Services 5 Checklist ». URL : http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/tips/iis5chk.asp (November 22, 2002).

18. Screen capture taken from IIS Application Configuration dialog box.

19. Screen capture taken from Group policy management console.

20. Microsoft Corporation, « XWEB: Permissions Required for Outlook Web Access». Revised October 22, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b175892 (January 10, 2003).

21. Dave Munger through trial and error.

22. Microsoft Corporation, « Web Site Operator Capabilities and Limitations ». Article ID: Q298969. Revised March 20, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B298969 (December 7, 2002).

23. Screen capture taken from IIS Default web site properties under Operators tab.

24. Figure created by Dave Munger.

25. Taken from properties of IIS default web site.

26. Screen capture taken from IIS Default Web Site properties.

27. Screen capture taken from IIS logging properties.

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

28. SecureIIS Software – Help. « Gettting Started ». Download software at : http://www.secureiis.com/html/Products/SecureIIS/Download.html.

29. Screen capture taken from SecureIIS console.

30. Tested by Dave Munger through trial and error.

31-32. Microsoft Corporation, « Security Guide Scripts download ». URL : http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9989D151-5C55-4BD3-A9D2-B95A15C73E92 (January 8, 2003)

Other references:

Microsoft Corporation, « HOW TO : Set Up an HTTPS Service in IIS». Article ID: 324069. Revised October 26, 2002. URL: http://support.microsoft.com/default.aspx?scid=KB;en-us;324069&#2 (January 8, 2003).

Microsoft Corporation, « Pratical Recommandations for Securing Internet-Connected Windows NT Systems ». Article ID: 164882. Revised June 10, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B164882 (January 4, 2003).

Microsoft Corporation, « Chapter 9 – Security ». URL : http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/reskit/iis50rg/introiis.asp (January 9, 2003).

Microsoft Corporation, « Exchange 2000 Static Port Mappings ». Article ID: Q270836. Revised October 26, 2002. URL : http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q270836& (December 10, 2002).

Microsoft Corporation, « Installing the Front-End Servers ». URL : http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/deploy/upgrdmigrate/ex2kupgr/deploy/d_08_tt1.asp (December 10, 2002).

Microsoft Corporation, « Security Operations ALL Chapters Download ». Published March 14, 2002. URL : http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F0B7B4EE-201A-4B40-A0D2-CDD9775AEFF8 (December 15, 2002).

Harper, Jason, « Eight Tips to Secure Exchange ». URL : http://archive.devx.com/upload/free/features/exchange/2000/10oct00/jh0010/jh0010.asp (December 14, 2002).

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Microsoft Corporation, « HOW TO: Enable Logging in IIS 5.0 ». Article ID : 313437. Revised October 26, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B313437 (November 23, 2002).

Microsoft Corporation, « HOW TO: Redirect URLs to Different Web Sites ». Article ID : Q324000. Revised October 26, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B324000 (December 3, 2002).

Microsoft Corporation, « List of NTFS Permissions Required for IIS Site to Work ». Article ID: Q187506. Revised August 13, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb;EN-US;187506 (December 16, 2002).

Microsoft Corporation, « How to: Configure ODBC Logging in IIS ». Article ID: Q245243. Revised December 12, 2002. URL : http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B245243 (December 20, 2002).

Microsoft Corporation, « Chapter 25 – Outlook Web Access ». URL : http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/reskit/part5/c25owa.asp (December 8, 2002).

Robichaux, Paul, « Maximize OWA 2000 ». Article ID : 22253. Published October 2001. URL : http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=22253 (December 8, 2002).

Eeye, Digital Security, « SecureIIS Web Server Protection ». URL : http://www.eeye.com/html/Products/SecureIIS/Features.html (November 22, 2002).

Zegiorgis, Seymoum, « Thwarting Hackers ». Published August 2, 2002. URL : http://www.eeye.com/html/Products/SecureIIS/Reviews/RV20020802.html (November 25, 2002).

Ludlow, David, « eEye Captain of the IIS Protection Army ». Published December 9, 2001. URL : http://www.eeye.com/html/Products/SecureIIS/Reviews/RV20011004.html (November 23, 2002).

Joseph Edwards, Mark, « Three Great Security Tools ». Published May 16, 2001. URL : http://www.eeye.com/html/Products/SecureIIS/Reviews/RV20010516.html (November 26, 2002).

SecureIIS Software – Help. « Installation ». Download software at :

© SANS Institute 2003,
Author reserves all rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

http://www.secureiis.com/html/Products/SecureIIS/Download.html.

SecureIIS Software – Help. « Site Security ». Download software at : http://www.secureiis.com/html/Products/SecureIIS/Download.html.

SecureIIS Software – Help. « File Monitor ». Download software at : http://www.secureiis.com/html/Products/SecureIIS/Download.html.

SecureIIS Software – Help. « Log Viewer ». Download software at : http://www.secureiis.com/html/Products/SecureIIS/Download.html.

SecureIIS Software – Help. « Troubleshooting ». Download software at : http://www.secureiis.com/html/Products/SecureIIS/Download.html.

Microsoft Corporation & Unkroth, Kay. MCSE Training Kit, Microsoft Exchange 2000 Server implémentation et administration. Microsoft Press, 2002. 667-686.

Glenn, Warlter & Chellis, James. Exchange 2000 Server Administration. Sybex, Inc, 2001. 633-635.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**