Global Information Assurance Certification Paper

Mary LaRoche
Submission for Option 1
SANS DC 2000, Track 5

Audit Guidelines for Microsoft IIS with Windows 2000

Part 1: Files and Folders

Disclaimer

This paper was written to complete requirements for GIAC Certification in NT Security. Securing an Internet Information Server (IIS) attached to the Internet is a complex effort involving many tasks, only one of which is discussed in this document. Furthermore, each enterprise needs to balance requirements for use against requirements for security, and will arrive at a solution that is to some extent unique. The following guidelines represent best practices that should be the default starting point of a security policy for files and directories associated with Microsoft IIS running under Windows 2000.

1 Introduction

This document is based on a the model of single IIS with all files local to the server. It is a set of instructions both for auditing file and directory settings and for changing the settings when needed. The instructions are applicable, with some exceptions, to more complex environments with multiple servers and distributed file systems (DFS).

However, be aware that specific vulnerabilities apply to remote files that do not apply to local files and vice versa. For example:

> IDQ, IDA, and HTX files cannot be served from a network share. If a website is set up in this manner, and a user clicks on a link that links to one of these files, the share path will be disclosed to the user in the resulting error message.[Bugtraq ID 1065]

Also:

> If a virtual host root is mapped to a UNC share, a backward slash "\" appended to an ASP or HTR extension in a URL request to that virtual host will cause Microsoft Internet Information Server to transmit full source code of the file back to a remote user. Files located on the local drive where IIS is installed is [sic] not affected by this vulnerability. [Bugtraq ID 1081]
>
> (from www.securityfocus.com/bugtraq)

It is not possible in a few pages to cover all of the security-relevant file and directory issues with IIS. The following is only a subset of the most common issues:

- Default installation of services, applications and protocols

- Folder names and locations
- ISAPI extensions and HTML verbs

The complex issue of file permissions is not discussed, let alone multiple other areas, such as network-level protection, authentication methods, and so forth.

2 Default Installation – Services, Applications and Protocols

2.1 Introduction

IIS is installed under Windows 2000 with a default set of services, protocols, and applications, not all of which are needed in most environments. These defaults need to be restricted in a production environment, particularly one connected to the Internet.

2.2 Risks

Web services provide remarkable capabilities to users, at the expense of potentially opening servers to a wide range of attacks. One example among many is offering FTP to Web users. FTP is a highly effective means of transferring large files. It is also such a security risk that many organizations do not allow FTP either into or out of their firewalls.

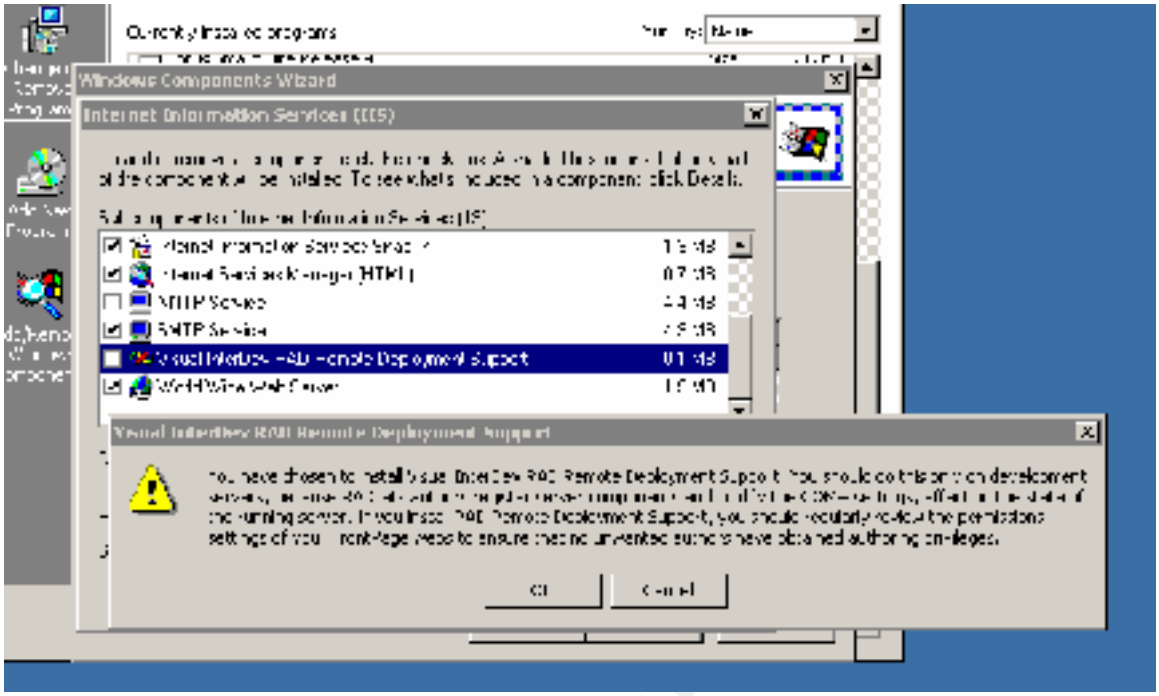
In addition, other services that are not Web-specific also open vulnerabilities, such as the ability to see what services are running on remote machines (nbtstat over NetBios), the ability to connect to remote machines (netlogon), ability to monitor and map the IP network (Network Monitor Agent).

Another dangerous service that is probably not needed on the IIS machine is the ability of HTTP users to **install printer drivers**. Printer drivers run with System privileges. Malicious printer drivers can be used to execute arbitrary commands.

The same is true of unnecessary bindings. In particular, the NetBios protocol has many security vulnerabilities. It is not needed on the Internet side of the server and is not needed in the internal Windows 2000 environment if no NT 4.0 domain controllers or workstations belong to the internal environment. NetBios is not used by HTTP.

Many security vulnerabilities for **FrontPage** in IIS for NT have been corrected in Windows 2000. However, new security vulnerabilities are still being discovered, for example, the Microsoft Security Bulletin MS00-034, published May 12, 2000, describes a vulnerability that allows malicious programs to execute on a browser user's PC.

The **RDS Data Factory Object** was designed for Web development use only. It is *not* installed by default, and a warning (shown below) is posted if installation is attempted.



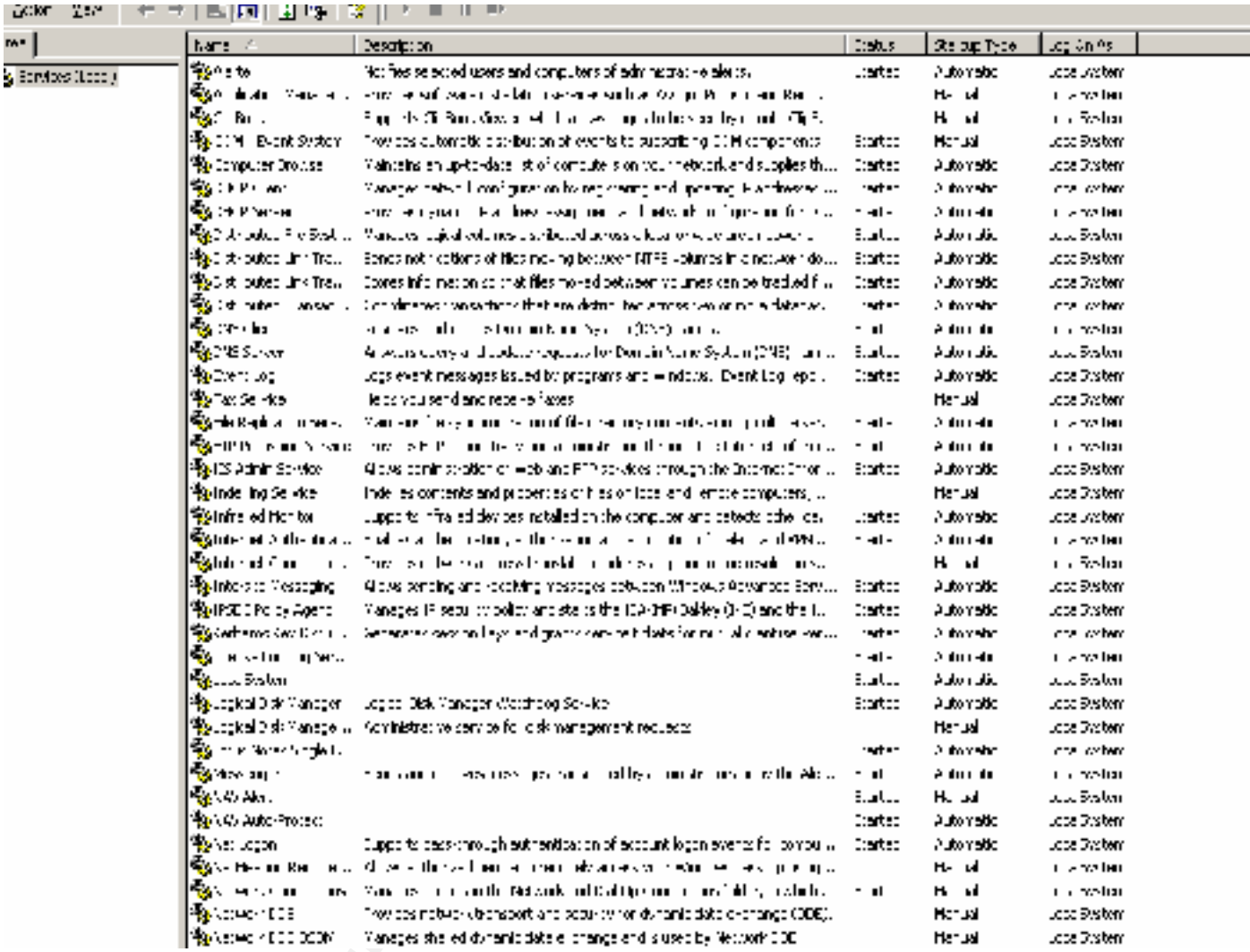
2.3 Best Practices

Disable and/or remove applications, services and bindings that are not needed. Even if no vulnerability is known today, it is better to disable the unneeded service in case a new vulnerability is discovered in the future. Remove FrontPage and replace it with WebDAV if possible. Otherwise, carefully secure FrontPage.

2.4 Analysis

2.4.1 Disable Services

Go to Start/Programs/Administrative Tools and click on Services. The screenshot below shows the first screen of the standard set of installed services.

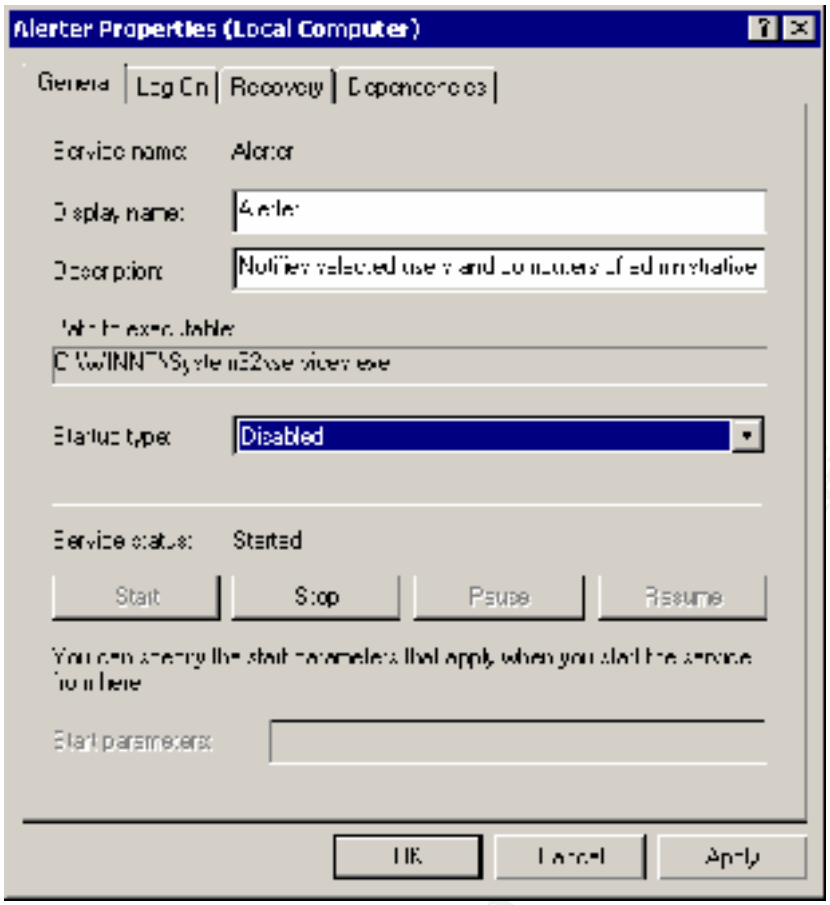


Verify that the following services have either been disabled, or removed completely, or have a documented purpose.

Service	*Disabled*	*Removed*	*Comments*
Alerter	Y		
ClipBook Server	Y		
Computer browser	Y		
DHCP client	Y		
Messenger	Y		
NetLogon (required if the computer is a member of a domain)	N		Computer is a member of a domain
Network DDE	Y		
Network DDE DSM	Y		

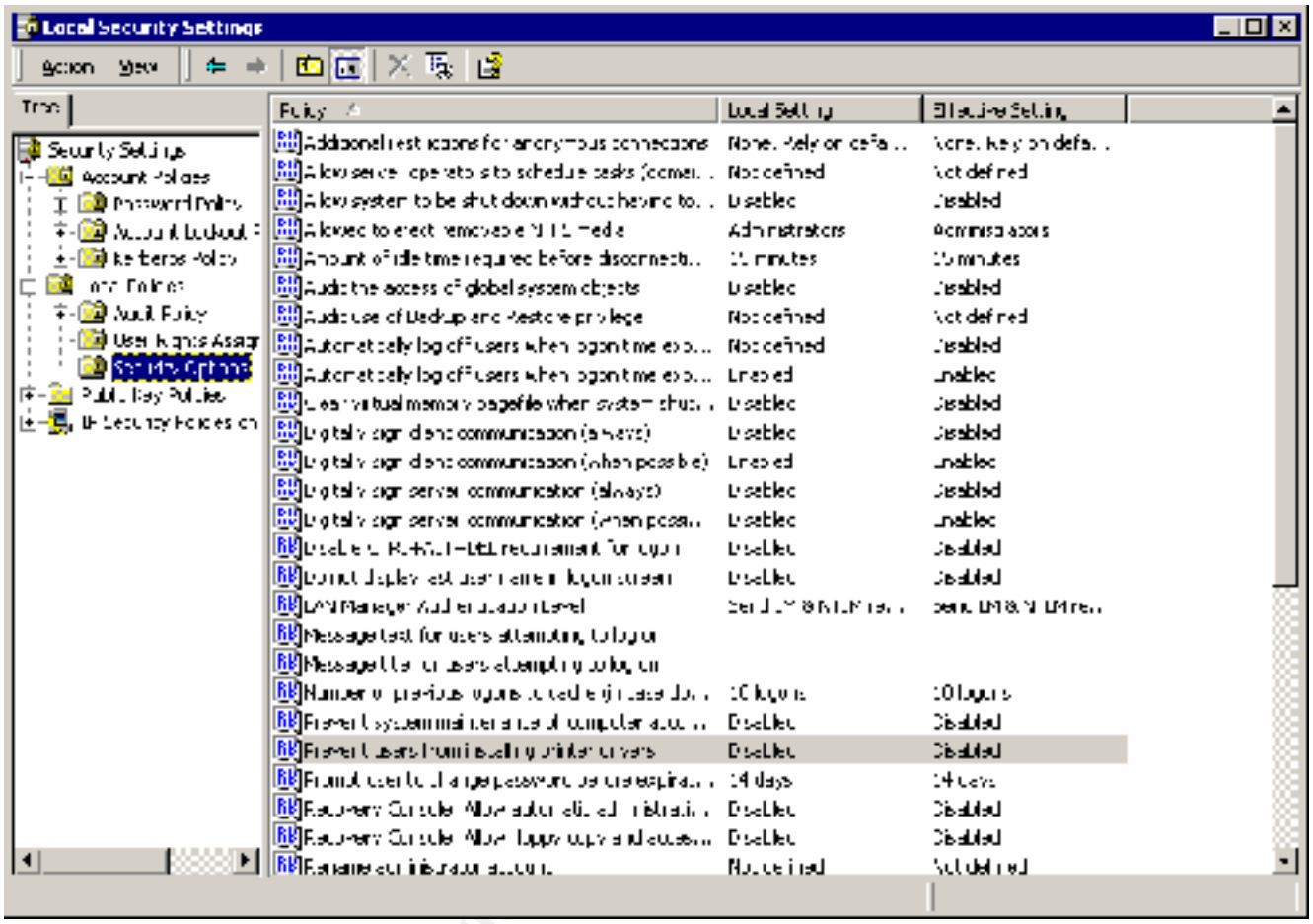
Network Monitor Agent	Y		Much safer to run the agent on an internal computer
Simple TCP/IP Services	Y		Services such as Echo
Print Spooler	N		This machine has a local printer
NetBios	Y		Not needed in Windows 2000
TCP/IP NetBios Helper	Y		
NWLink NetBios	Y		
FTP Publishing			
NNTP	Y		
SMTP	Y	Y	Not needed and dangerous
Server	N		Needed for authentication
Workstation	Y		Files are all local to the machine
RPC Locator	Y		
Uninterruptible Power Supply	N		Machine has UPS
Certificate server	N		Plan to use certificate-based authentication for administrators
Content Index	N		Needed for applications

To disable, select the service in the Services list. Change the Startup Type to Disabled, select Stop, select Apply, select OK



2.4.2 Prevent Installing Printer Drivers

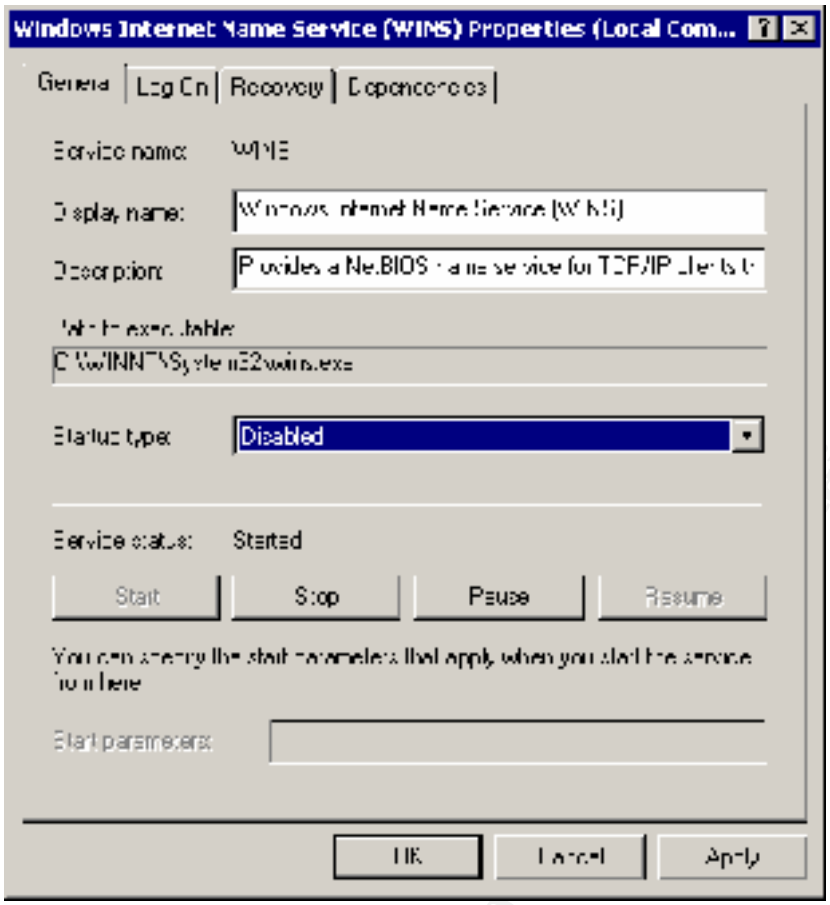
To prevent HTTP users from installing printer drivers, select Start/Programs/Administrative Tools/Local Security Policy. In the navigator, select Local Policies/Security Options/Prevent Users from Installing Printer Drivers. Select enabled, enter OK. If the IIS is a member of a domain, repeat for Domain Security, because domain policies override local policies. Select Domain Security Policy/Security Settings/Local Policies/Security Options/Prevent Users from Installing Printer Drivers. In addition, unless the IIS server has to be used for printing, delete the /printers folder (%systemroot\web\printers), unmap the .printers ISAPI extension (see below), and disable the Print Spooler service.



2.4.3 Disable Unused Bindings

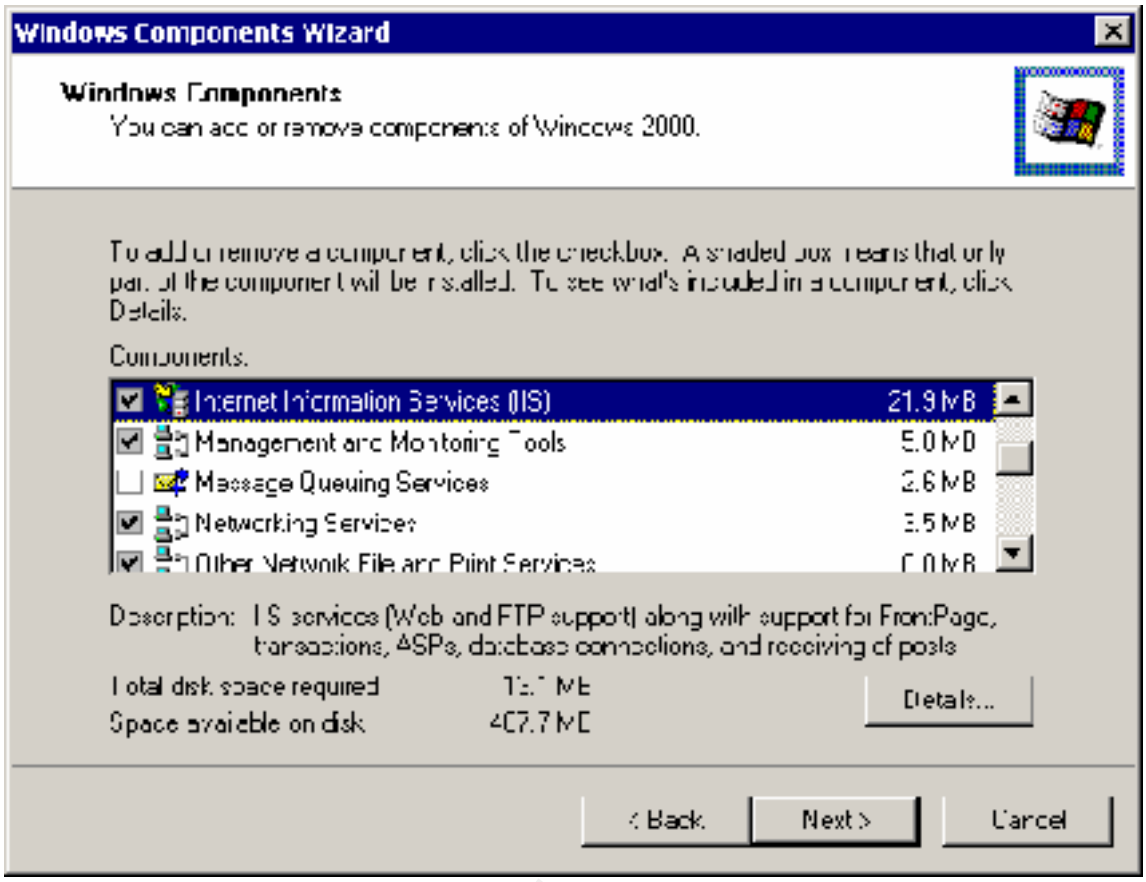
To disable IPX/SPX or WINS (NetBios over TCP) or any other unneeded protocol, select Start/Settings/Network and Dial-up Connections, then select each used connection in turn. Right-click, select Properties, and disable all services that are not needed. For an Internet-facing connection, only TCP/IP needs to be enabled. For a connection to an internal Windows network, the Microsoft Client for Windows (WINS), file and printer sharing, and NetBuei may or may not be needed.

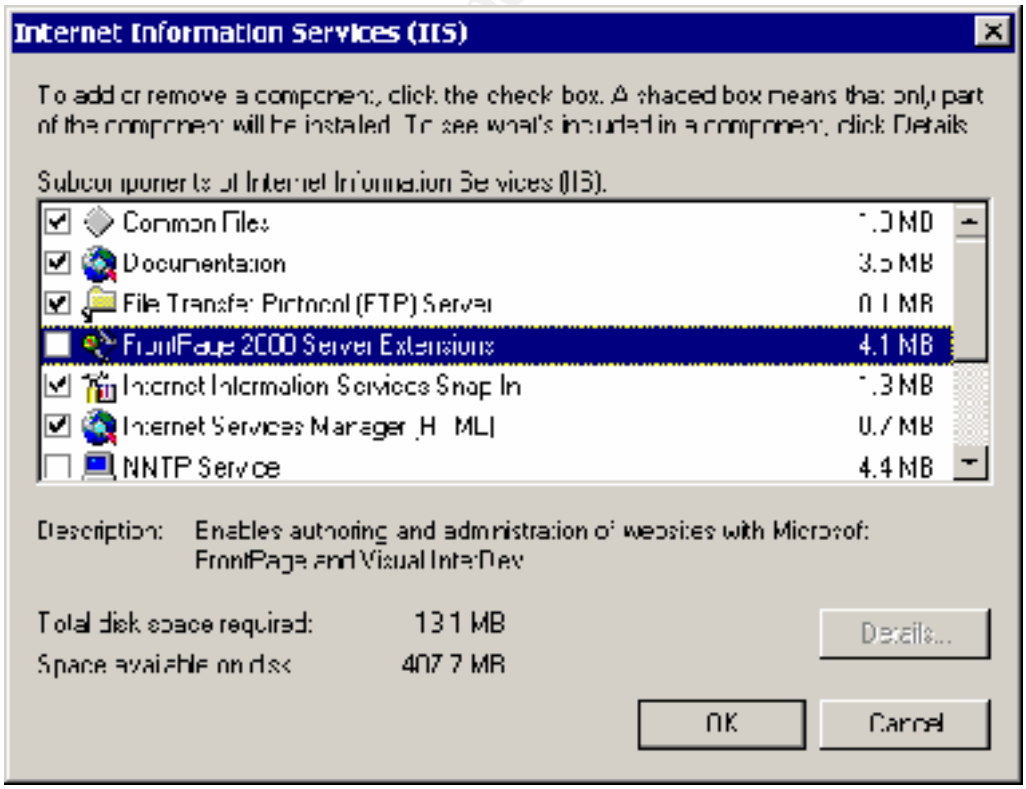
An alternative way to disable WINS is to select Start/Programs/Administrative Tools/Services. Select Windows Internet Name Service. Change the Startup Type to Disabled, select Stop, select Apply, select OK. To disable it only on the server's Internet interface, run RRAS.



2.4.4 Remove Applications

To remove FrontPage, go to Control Panel, Add/Remove Programs, Add/Remove Windows Components. Select IIS, select Details, uncheck FrontPage Server Extensions, select OK, select Next, and wait for the process to complete.





To remove SMTP and FTP servers, remove the server as a component of IIS in the same way that FrontPage is removed. However, remember that with the removal of FTP server service, you will have lost one of the easiest means of moving files to and from the IIS. An alternative is to disable the FTP ports on the Internet connection, but not on the internal connection (see below).

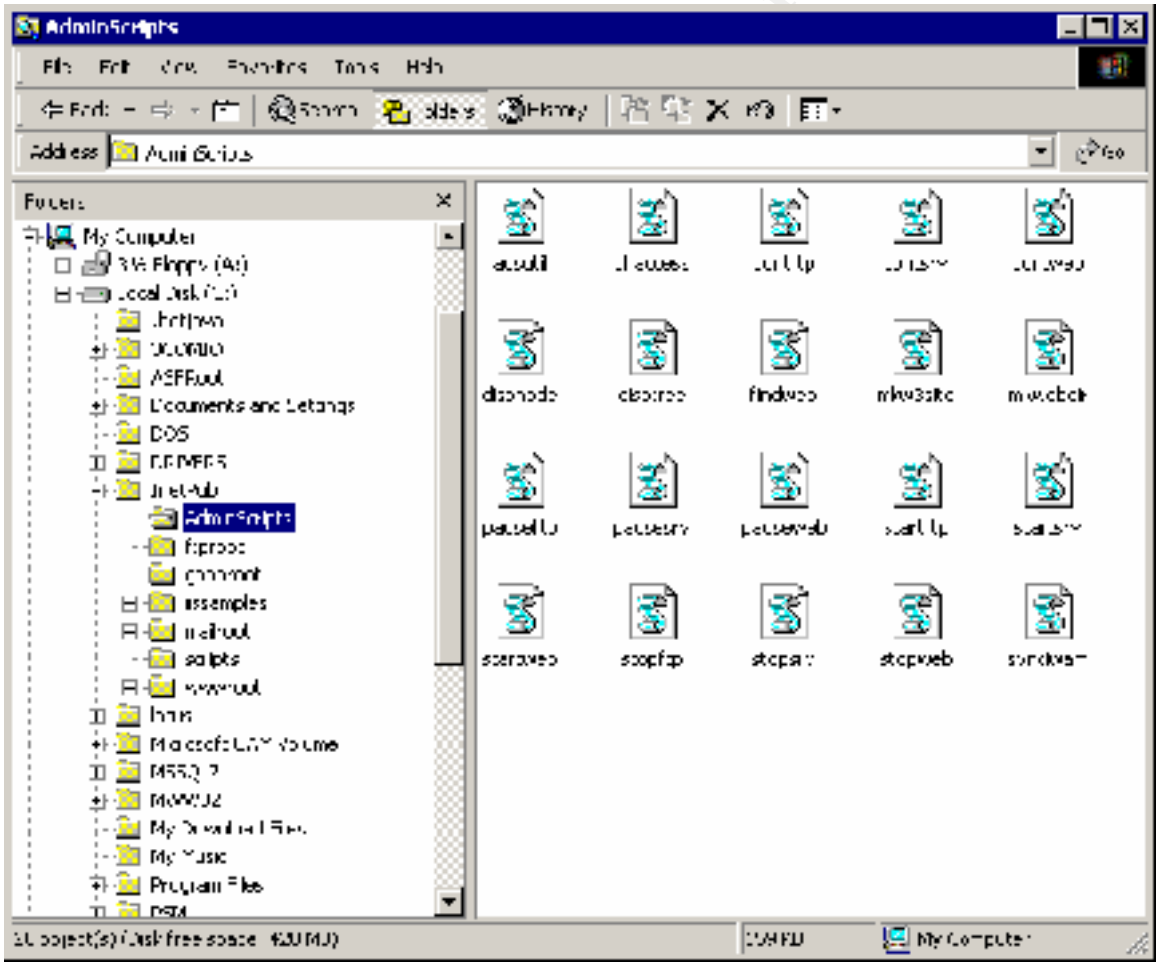
If RDS is installed, remove it in the same way.

3 Folder Security

3.1 Introduction

The default set of files and folders installed with IIS (see below) is ideal for the inexperienced user but is unnecessarily vulnerable to attack if left unchanged on a production server.

The entire set of Web folders is put in the same partition as the operating system.



3.2 Risks

- Any directory that can quickly grow large, such as log files or the default FTP root directory, has the potential of creating intentional or unintentional Denial of

Service from filling up the file system if the directory is on the same partition as the operating system.

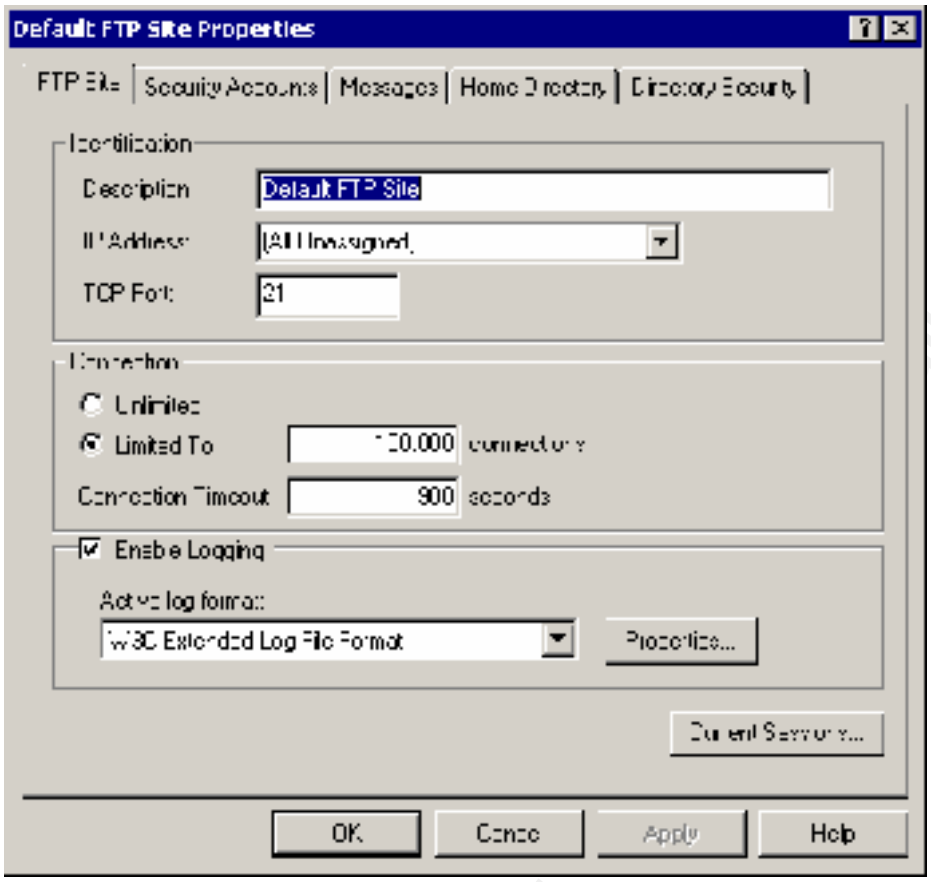
- Although IIS 5.0 does not have the sample page execution vulnerability of IIS 4.0, inadvertent permission errors will make these files accessible and possibly executable from the Internet, in which case multiple vulnerabilities are opened up, including one that allows source code to be shown when +htr is appended to a known file (see Bugtraq 1193 and others, MS patch Q267559_W2K_SP2_x86_en).
- The Administration Website for the entire server is by default a subfolder under InetRoot, and is therefore easily found.
- By default, both scripts and executables are stored in the Scripts directory. . The Executables permission is dangerous and should be given to as few files as possible.
- The installed location for admin scripts is under InetPub. Admin scripts are powerful and need to be protected. need to be moved to a protected location, such as under %systemroot%.

3.2.1 Best Practices

- Any directory that can quickly grow large, such as log files or the default FTP root directory, needs to be moved to a different partition from the operating system, to avoid intentional or unintentional denial of service if the file system fills up. In addition, it is important that enough space be made available and log file settings be established so that log files are not overwritten. Optimally, the entire set of IIS files needs to be moved to a different partition.
- Sample Web files should be deleted from production servers.
- Since the Administration Website is mapped to the same physical folder (%systemroot%\System32\Inetsrv\IISAdmin) as the Default website IISAdmin folder, delete the Administration Website and rename the physical IISAdmin folder.
- Since executables need Scripts and Executables permissions, while scripts need only Scripts permissions, create two separate directories. Using separate directories reduces the number of files that have dangerous permissions.
- Move admin scripts to a protected location, such as under %systemroot%, and make sure that permissions are set correctly.

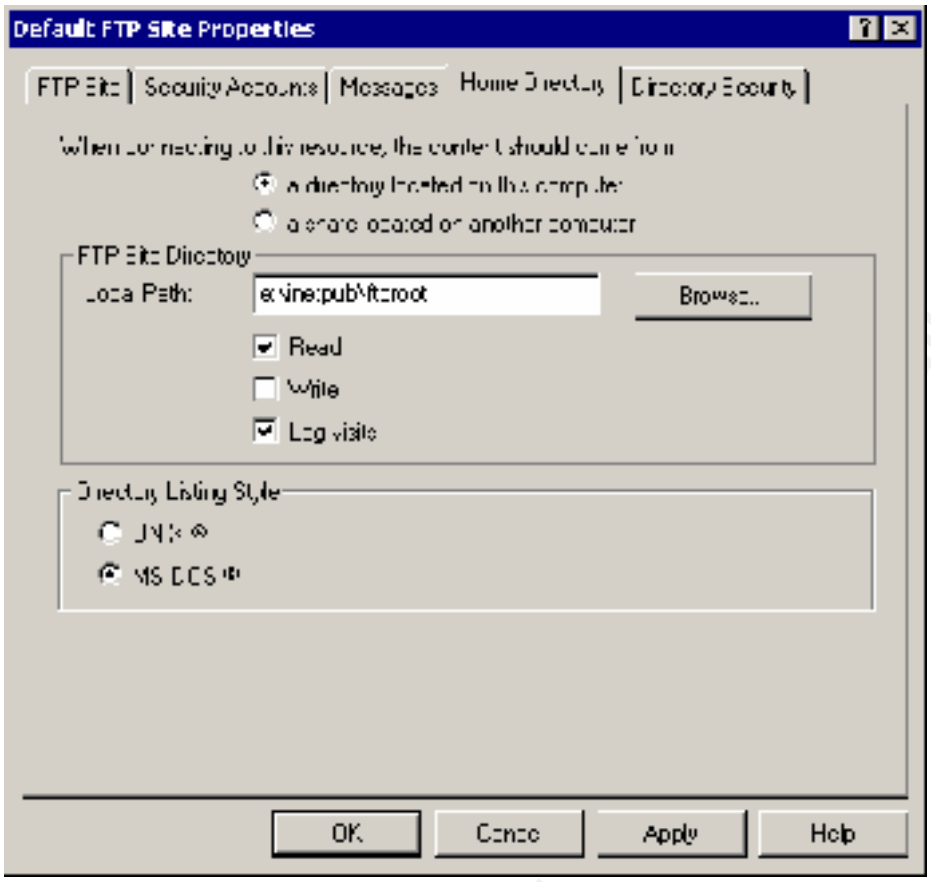
3.2.2 Analysis

ftproot is a virtual folder visible via the Internet Services Manager snap-in. In addition to creating an new physical folder, it is essential to change the properties of the virtual folder. After creating the new physical folder, select Start/Programs/Internet Services Manager; right-click on the Default FTP Site folder; select Properties. The following window appears.



Note the connection limits. These should be changed to whatever is appropriate for the server, to avoid Denial of Service attacks from multiple ftp opens.

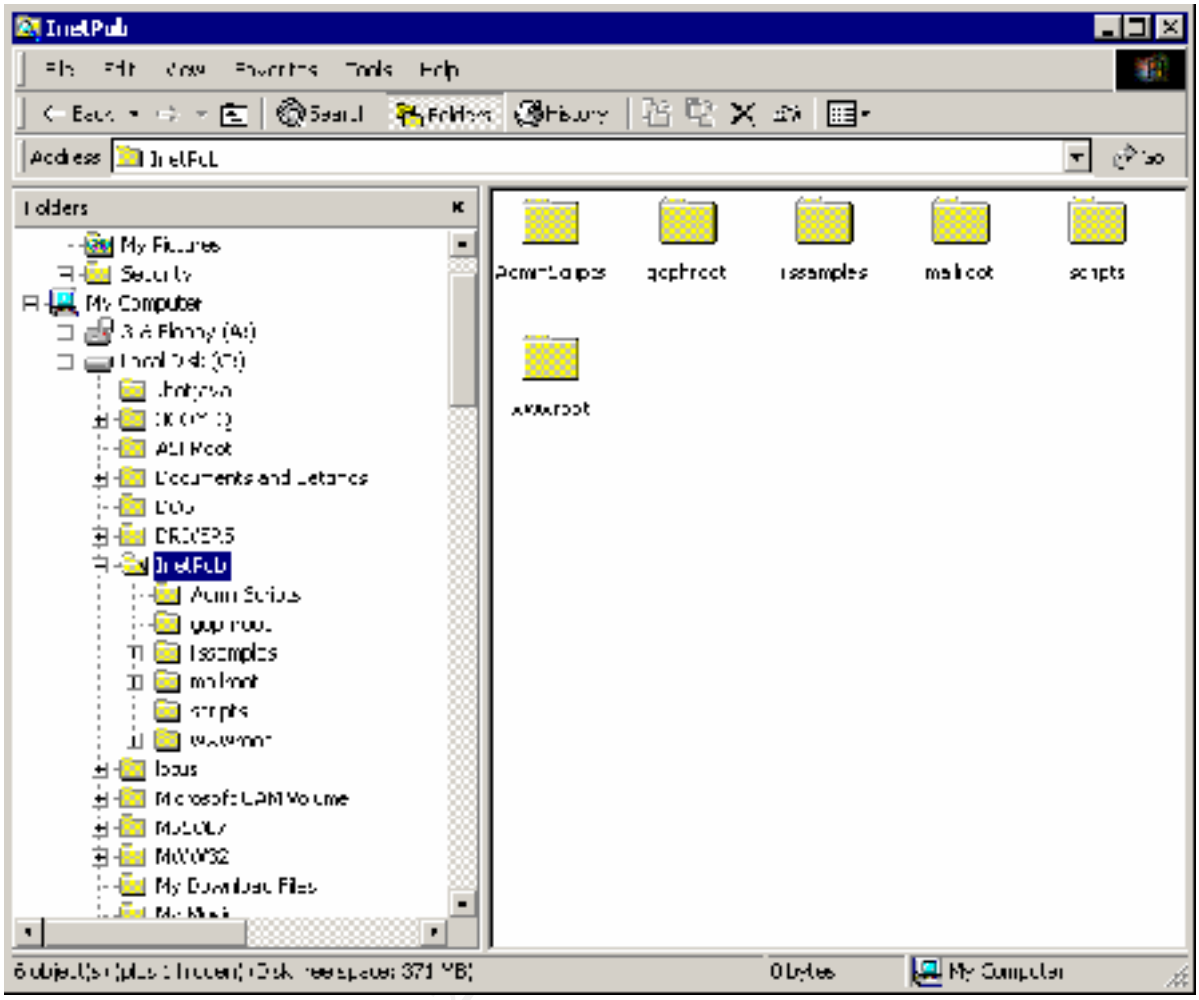
Change to the Home Directory tab and change the path.



Select Write if appropriate; select Apply/OK.

IMPORTANT – This action does not delete the old c:\inetpub\ftproot folder. The folder could be left as a decoy or deleted, as shown below.

Follow the same procedure when renaming the IISAdmin folder.



C:\inetpub\ftproot is gone, but ftp still works:

```
C:\Program Files\Common Files\System\Mapi\1033\NT>ftp mlaroche
Connected to mlaroche.lotus.com.
220 mlaroche Microsoft FTP Service (Version 5.0).
User (mlaroche.lotus.com:(none)): mlaroche
331 Password required for mlaroche.
Password:
230 User mlaroche logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
hi.txt
226 Transfer complete.
ftp: 8 bytes received in 0.03Seconds 0.27Kbytes/sec.
ftp>
```

4 ISAPI Extensions and HTTP Verbs

4.1 Introduction

Microsoft IIS is installed with a default set of ISAPI extensions and the full complement of HTTP verbs. Since ISAPI extensions and HTTP verbs are executed on the server, each extension and each verb add possible vulnerabilities, and most Web sites do not use all of the extensions or verbs.

4.2 Risks

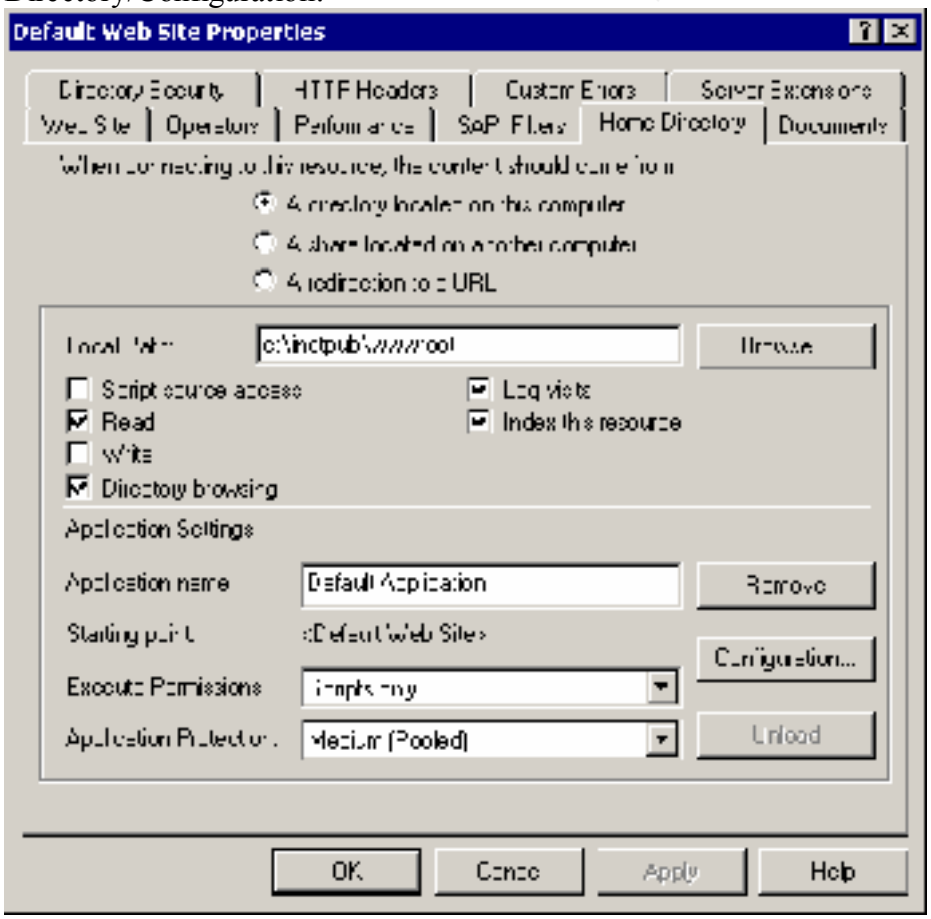
The Introduction mentions some of the many vulnerabilities associated with ISAPI extensions. To a lesser extent, HTTP verbs also introduce vulnerabilities.

4.3 Best Practices

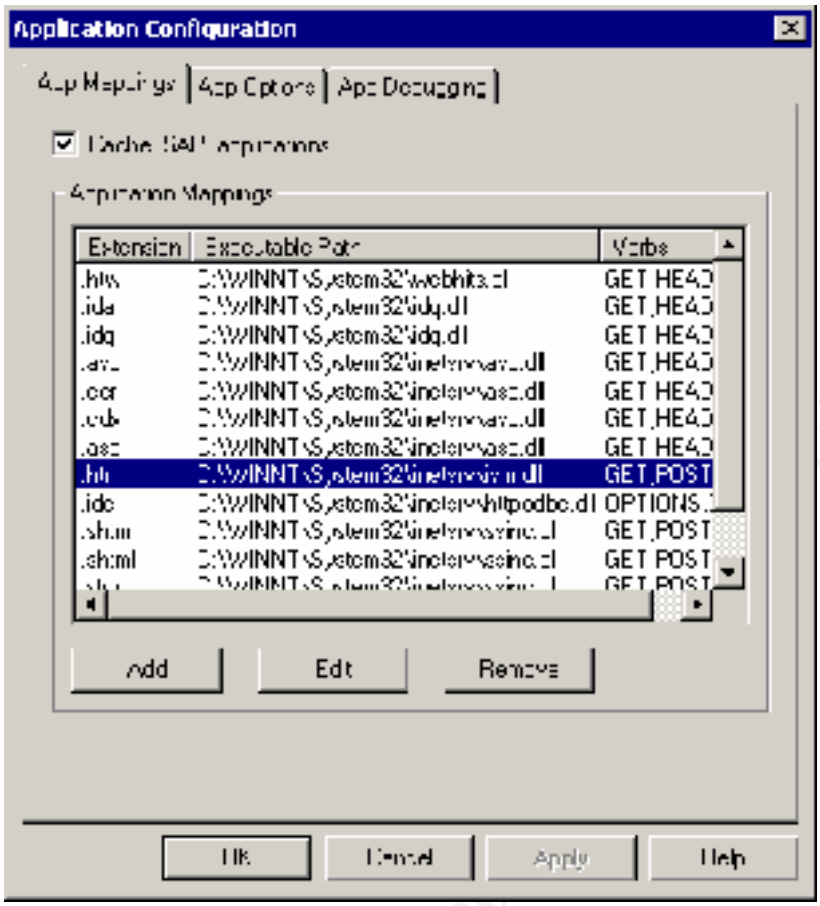
As always, it is best to unmap unused ISAPI extensions and HTTP verbs. However, this needs to be done in concert with developers.

4.4 Analysis

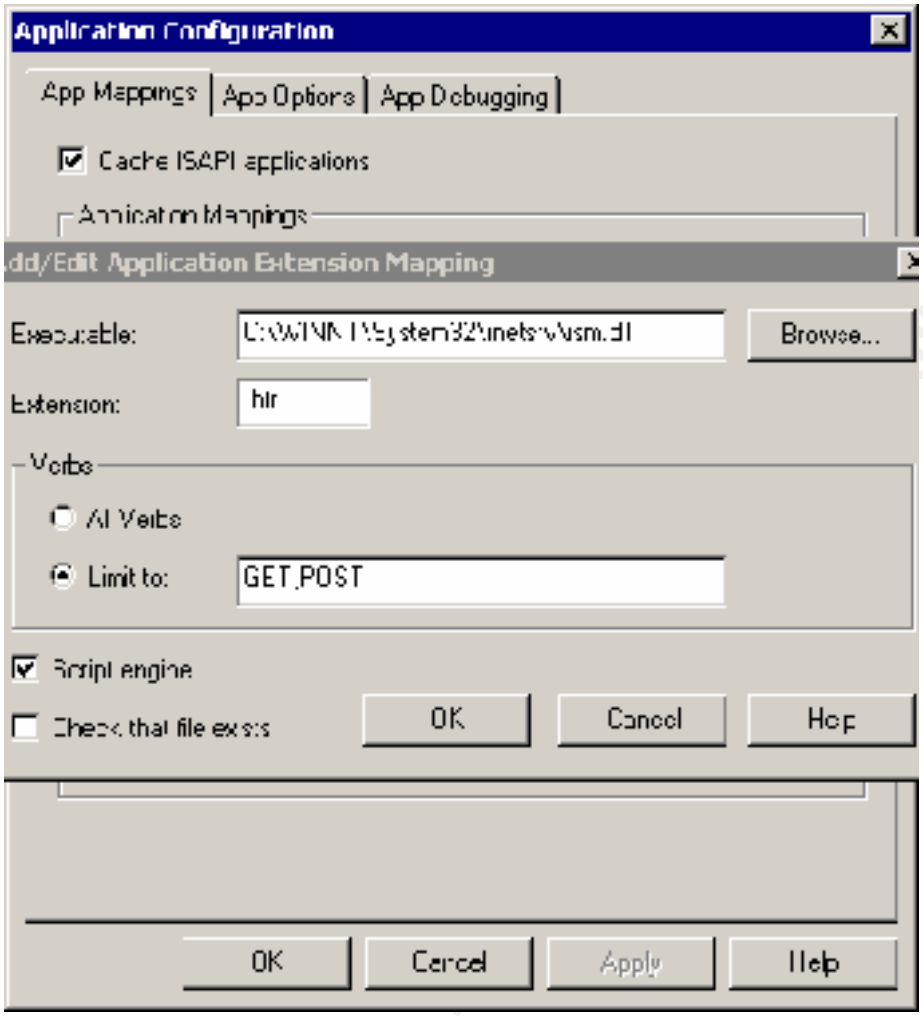
To remove unused extension mappings, select Start/Programs/Internet Services Manager. Select the Website in question. Right click; select Properties. Select Home Directory/Configuration.



Select App Mappings.



Select Remove for unused extensions. Select Edit for extensions that are used.



Remove any HTTP verbs that are not used with this extension. For example, a static Web site almost never needs POST. Verify whether the extension should be allowed to run with just the Scripts permission (Script engine checkbox is checked), or whether the Scripts and Executables permission should be required (Scripts engine checkbox is left unchecked).

5 Conclusion

Securing IIS under Windows 2000 is a complex task that requires careful planning and detailed analysis. However, even implementing the simple safeguards described in this document will significantly improve the security of an IIS that is running from a default installation.

References

Fossen, Jason. *Internet Information Server*. The SANS Institute GIAC Training, 2000.

Fossen, Jason. . *Active Directory for Win2000 in a Nutshell.* The SANS Institute GIAC Training, 2000.

Shinder, Thomas W. et al. *Configuring Windows 2000 Server Security,* November 1999. ISBN: 1928994024.

McLean, Ian and Edward, Austin. *Windows 2000 Security: Little Black Book*, February 2000. ISBN: 1576103870.

Microsoft Security Bulletin MS00-030, Patch Available for "Malformed Extension Data in URL" Vulnerability. Published: May 11, 2000 - Updated: May 12, 2000

Microsoft Security Bulletin MS00-057, Patch Available for "File Permission Canonicalization" Vulnerability. Published August 10, 2000.