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 on Windows 2000

There are more vulnerabilities and attacks for web servers than any other type. With the convenience of the Internet and the growing pressure to "have a web presence", people and businesses are installing web servers right and left. Windows 2000 and Internet Information Server (IIS) are making this incredibly easy, but what about the risks? By its very design, a web server is intended to make information accessible, not protect it. A software company will always install their product with most of the features turned on...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn
More

Securing IIS on Windows 2000

by Carl Denowh

Introduction

There are more vulnerabilities and attacks for web servers than any other type. With the convenience of the Internet and the growing pressure to "have a web presence", people and businesses are installing web servers right and left. Windows 2000 and Internet Information Server (IIS) are making this incredibly easy, but what about the risks? By its very design, a web server is intended to make information accessible, not protect it. A software company will always install their product with most of the features turned on, to reduce help calls, and to show the product in its best light. That means that IIS installs in an insecure format, but that does not mean that the platform is any less secure or desirable than any other.[1] With this understanding, we can now proceed with the task of making it secure.

Best Practices

If you are fortunate enough to be starting from scratch, you will get to design your solution with security in mind. Consider these best practices when you set up your Internet servers:

1. Isolate your web farm.
   Discussion: Web servers and FTP servers are notoriously vulnerable. If these systems are connected to the rest of your network, you are creating a back door into your network.[2] Isolating these systems with a filtering router or a firewall is always a good idea.[3] The more obstacles you place in an attacker's path, the better.
2. Separate the server functions.
   Discussion: FTP servers, WWW servers, database servers, and authentication servers should all be separate if possible. It is also a good idea to run publicly accessible sites on separate systems from restricted access sites. The more complicated your configuration, the more vulnerable it is.
3. Use internal DNS for back-end servers.
   Discussion: Your publicly accessible servers must be advertised on public DNS, but some systems should never even be hinted at outside your web farm. Put back-end systems like database servers and authentication servers on private DNS or simply code their addresses into the operating system or application. Never give anything away unless you must.
4. Keep current with service packs and patches.
   Discussion: The service packs and patches will keep you ahead of over 90% of the attackers. It is, of course, always a good idea to test the configuration before considering it production. The dependencies your server and software have can be surprising.
5. Use SSL encryption.

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

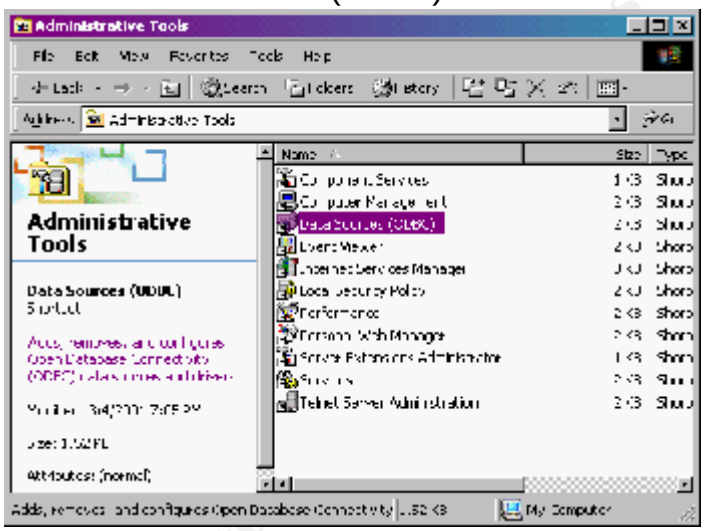
Discussion: Because the Internet is global, you are opening yourself to international legal issues. Encryption certainly impacts performance, but where a user's privacy is concerned, you must take all reasonable steps. Authentication and a customer's personal and account information should always be protected. SSL is a simple and effective way to accomplish this.

Securing the Environment

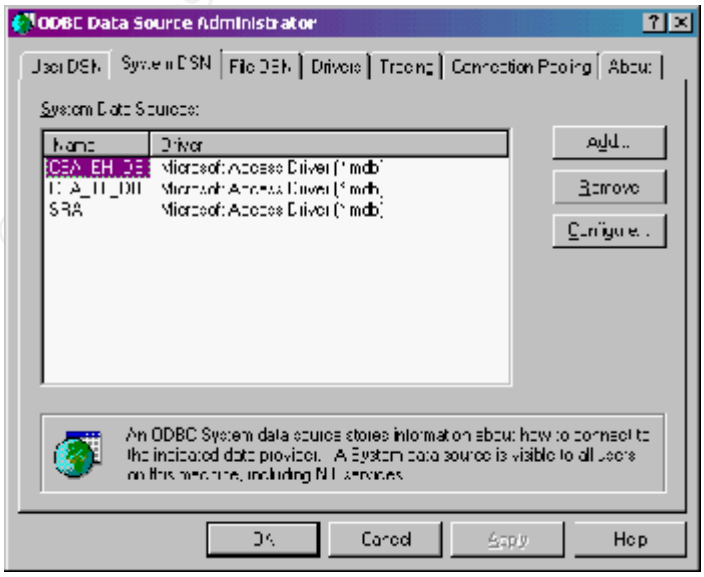
1. Remove unnecessary ODBC connections.

How:

- Choose Administrative Tools from the Control Panel.
- Choose Data Sources (ODBC) from the Administrative Tools window.

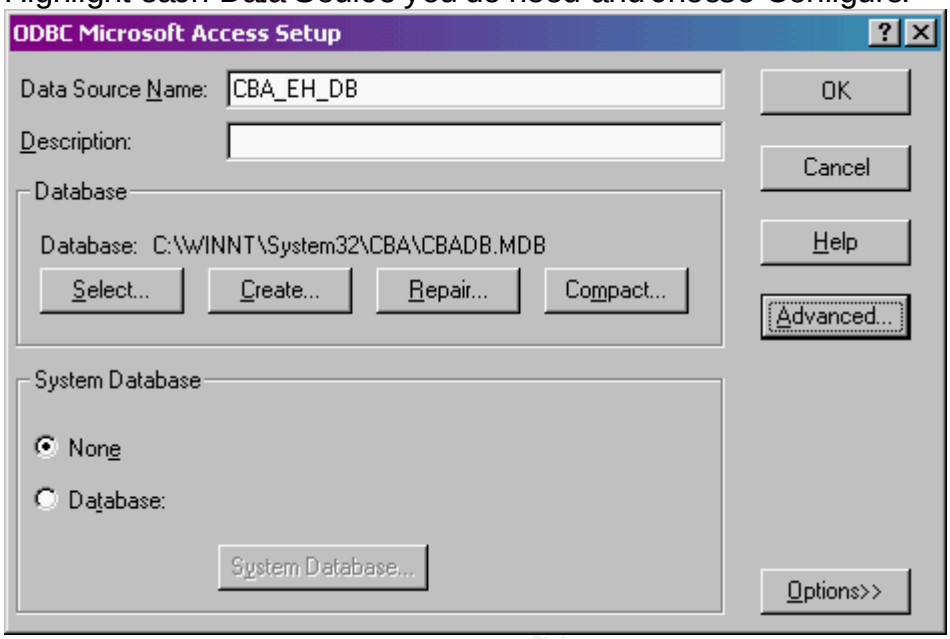


- Choose the System DSN tab and remove any data sources you do not need.

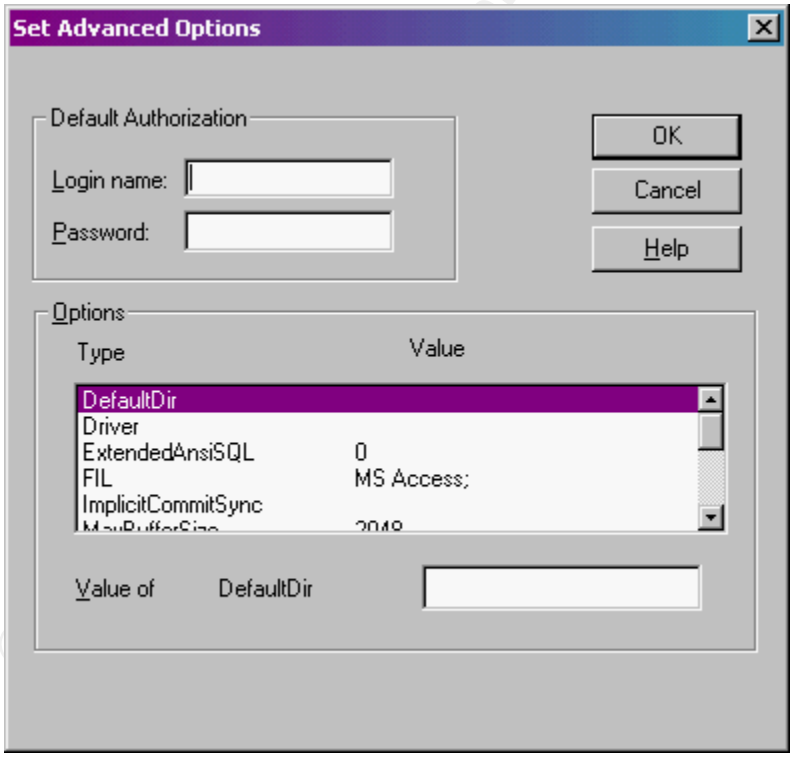


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Highlight each Data Source you do need and choose Configure.



- Click the Advanced button to bring up the Set Advanced Options window.



- Add a username and password (be sure to coordinate with the programmers)

Discussion: ODBC connections allow applications to use a standard interface to a variety of databases. Most systems have some ODBC connections set up by default. Unless you are using a database

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

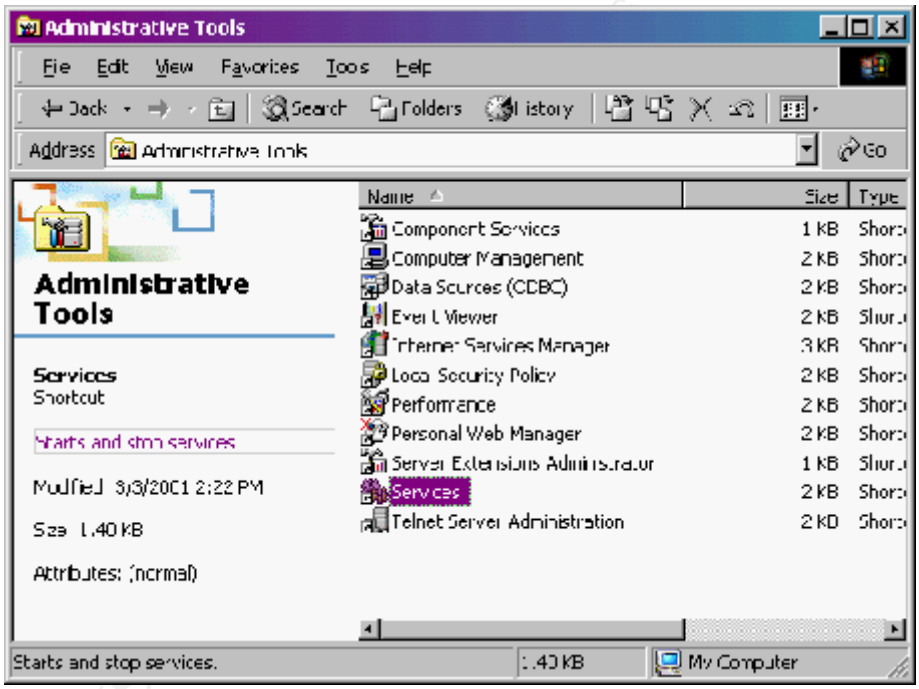
connection, it is a good idea to remove it. Such connections allow access to your system over the network. It is possible to impact performance or gain unauthorized access to information through these connections. If you are using an ODBC connection, be sure to restrict access. By adding a username and password, you are forcing any applications that make use of the database to authenticate. Obviously, you will need to work with those application programmers to make sure they have this information.

Best Practice: Put your databases on a separate server from your web based application.

2. Remove unnecessary services.

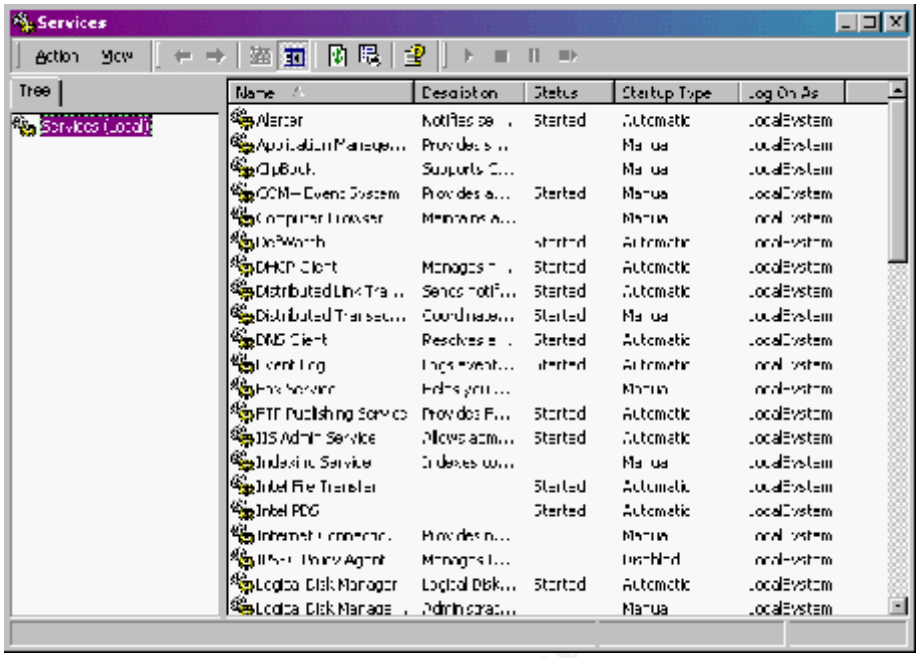
How:

- Choose Services from the Administrative Tools window.

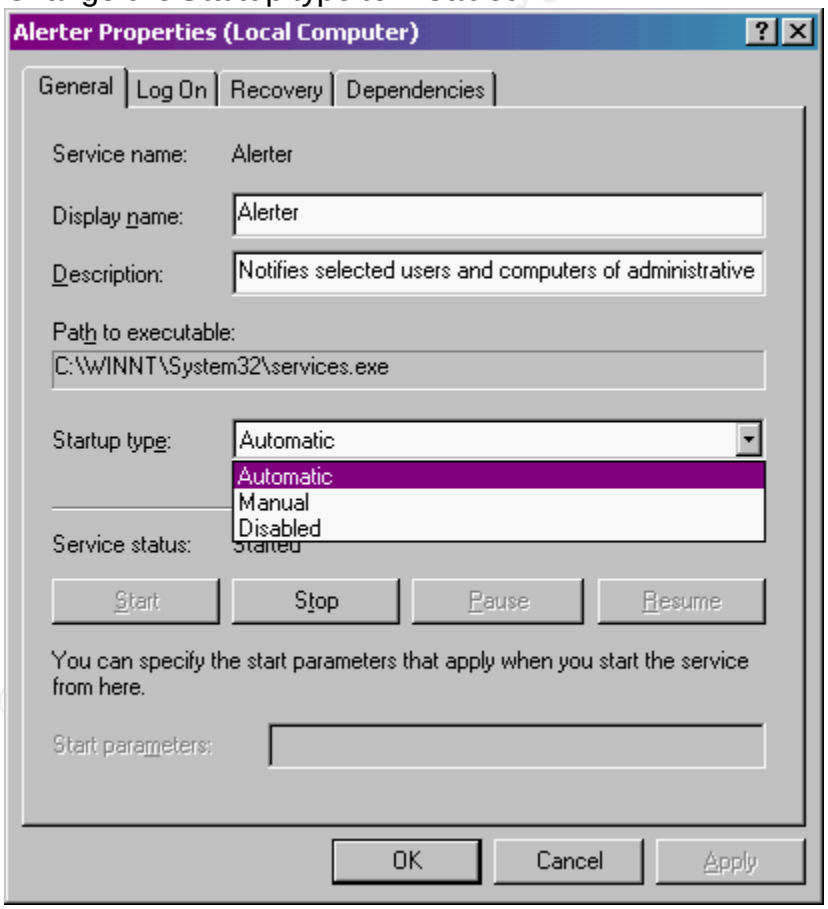


- Select each service you wish to cancel and pull up its properties window.

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



- Change the Startup type to Disabled.



- Test the configuration!

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

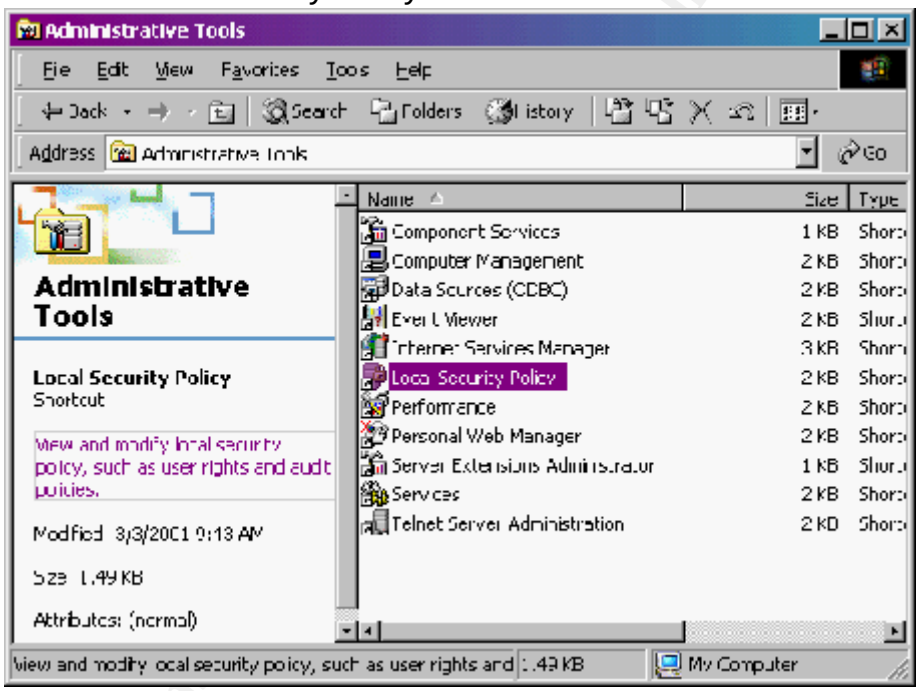
Discussion: Any service is, of course, a potential vulnerability. It is a good idea to make your configuration as simple as possible. It is also critical to test your configuration each time you make a change. Some dependencies may not be very evident.

Best Practice: Separate. Separate. Separate.

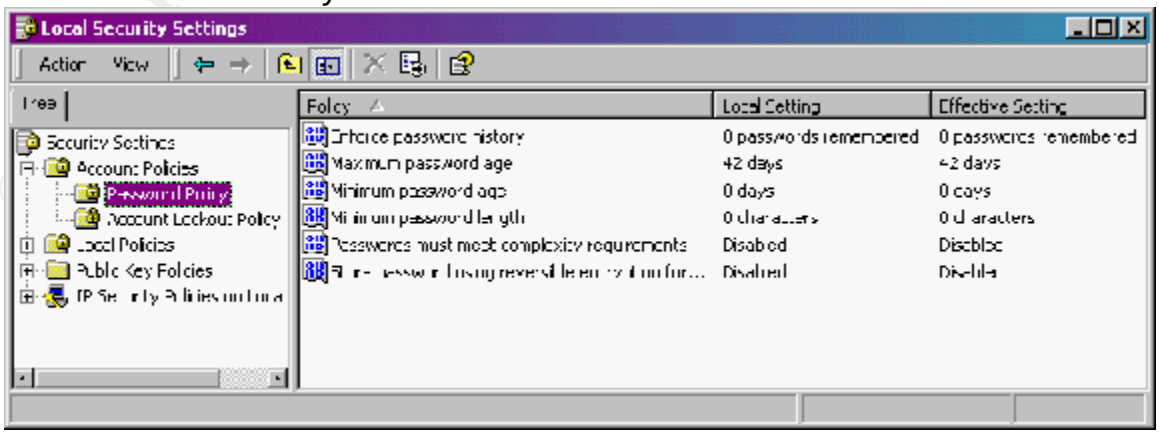
3. Set up your account policies.

How: These settings may have to happen at your domain controllers. Below are instructions for local changes. The Best Practice area includes recommended settings.

- Choose Local Security Policy from the Administrative Tools window.

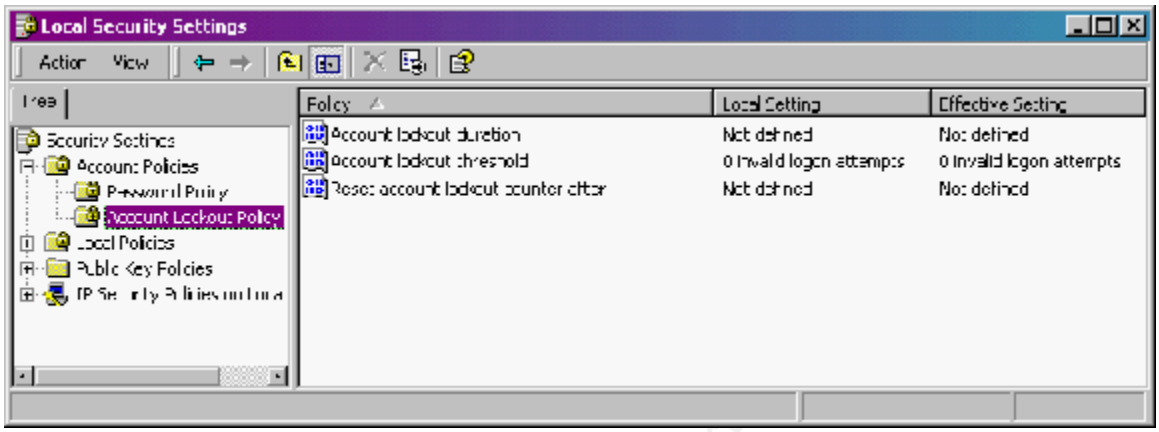


- Select Password Policy from the Account Policies tree.



- Change the policy settings to reflect your policy.
- Select Account Lockout Policy from the Account Policies tree.

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



- Change the policy settings to reflect your policy.

Discussion: The goal here is to make password related attacks ineffective. Changing passwords regularly reduces the window of opportunity for attackers who manage to compromise a password. The Password history setting prevents a user from reusing a password for as many as are remembered. The Maximum password age is when a password is required to be changed. The Minimum password age prevents the user from changing the password repeatedly all at one time to circumvent the password history. The Minimum password length is important because each additional character can increase the time required to break it exponentially. The Passwords must meet complexity requirements setting forces the passwords to use a combination of upper case, lower case, and non-alpha characters. Reversible encryption is generally considered less secure. The Account lockout duration does not have to be large. Even a 3 minute lockout time will make a brute force attack take too long to be practical. The Account lockout threshold setting is how many failed login attempts are allowed before the account is disabled for the duration set. The Reset account setting has no impact on brute force password attacks.

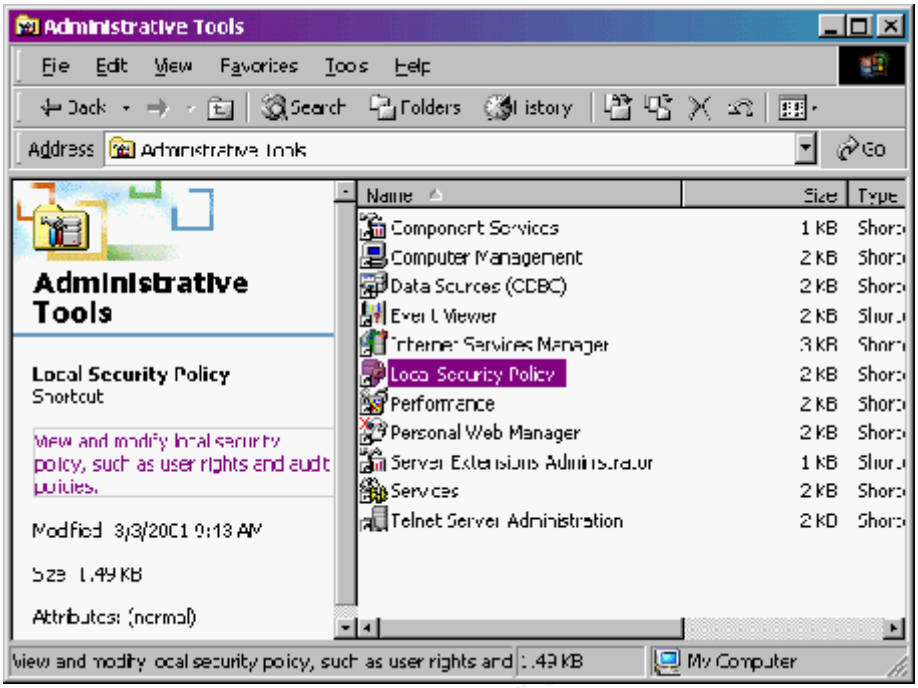
Best Practice: The following settings are recommended:
Password history = 7 passwords remembered
Maximum password age = 180 days (or less)
Minimum password age = 1 day (or more)
Minimum password length = 8
Passwords must meet complexity requirements = Enabled
Reversible encryption = Disabled
Account lockout duration = 3 minutes (or more)
Account lockout threshold = 5 (between 3 and 7)

4. Set up your audit policies.

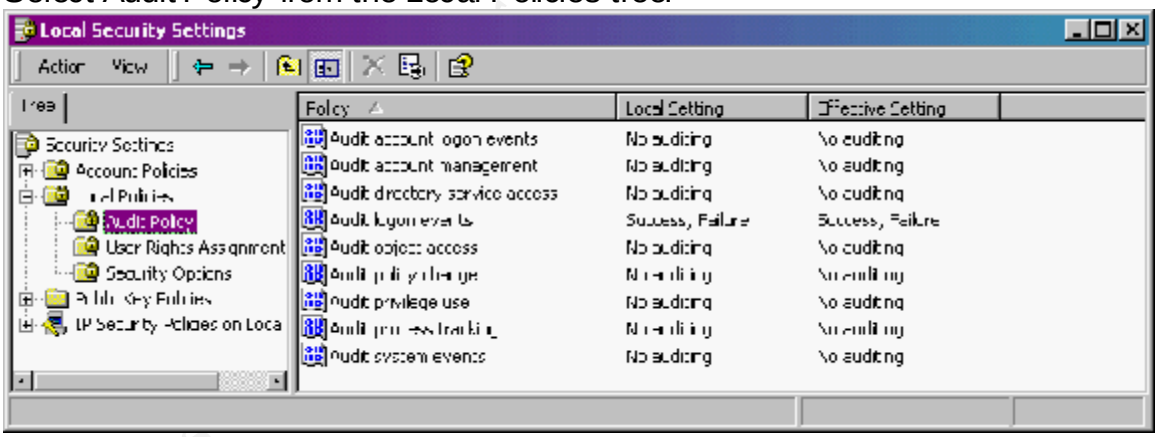
How:

- Choose Local Security Policy from the Administrative Tools window.

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



- Select Audit Policy from the Local Policies tree.



- Change the policy settings to reflect your preferred policy.

Discussion: The goal here is to provide the information you will need to detect or troubleshoot problems. There are issues with too much logging, however. You do not want to fill your drive, nor do you want to overwrite log data before you get a chance to use them. At a minimum, you should set the following: Audit account management, Audit logon events, and Audit policy change.

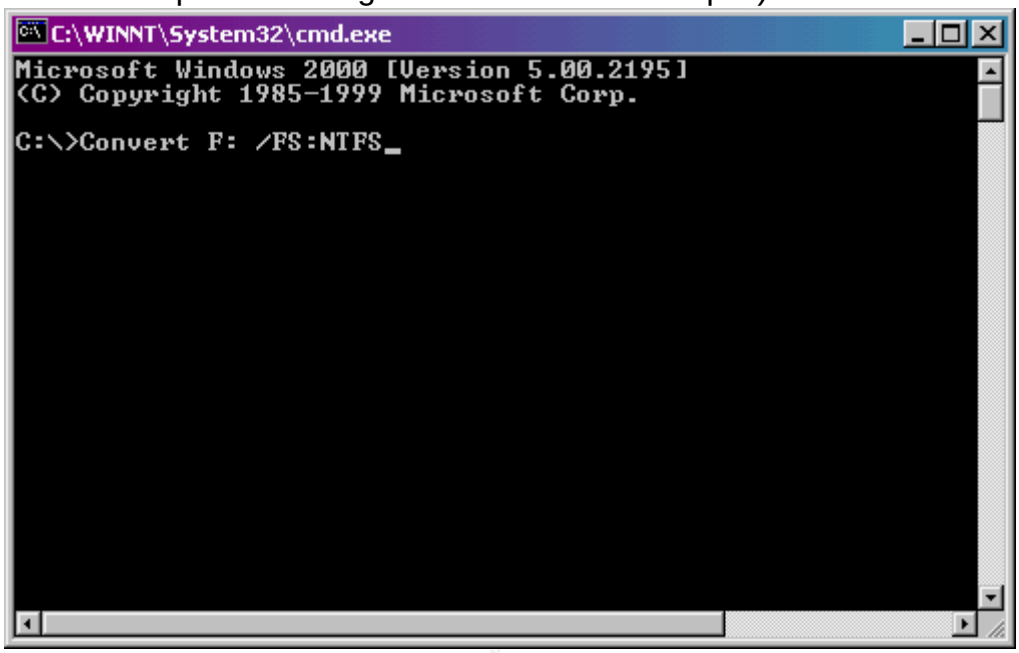
Best Practice: Run a utility or script to copy logs to a remote, secure system regularly, and run a utility or script to scan the logs.

5. Set up your NTFS partitions.

How:

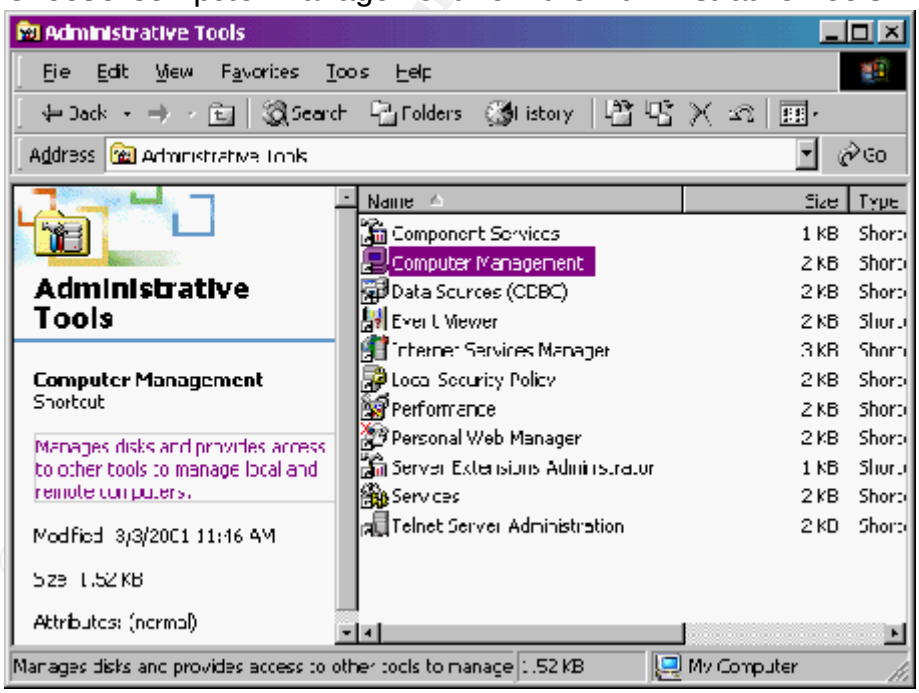
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Use the Convert command from a command window. (F is the drive letter of the partition being converted in this example.)



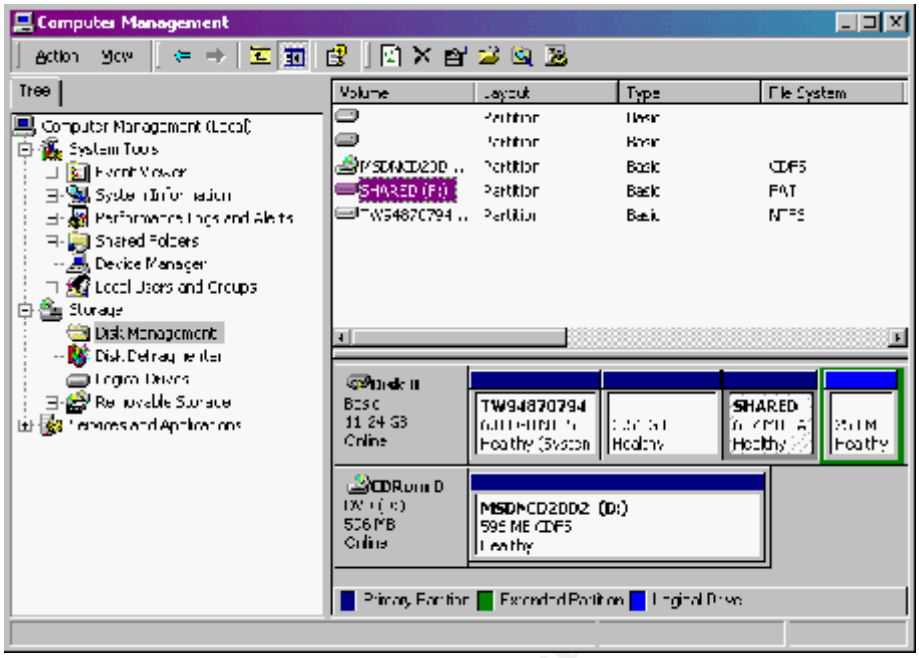
Alternate Method:

- Choose Computer Management from the Administrative Tools window.

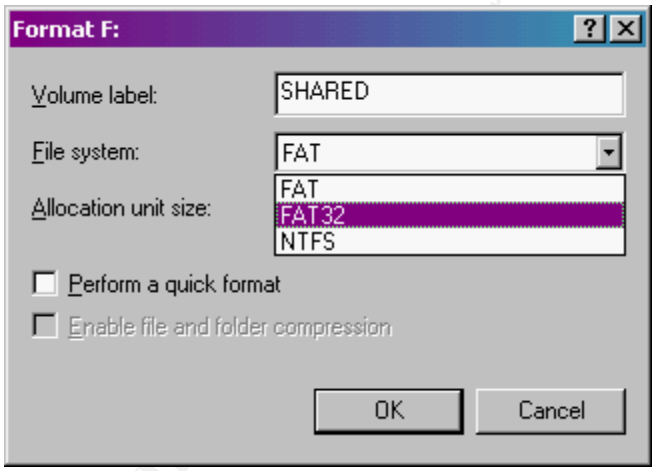


- Select Disk Management from the Storage tree.

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



- Right click on the partition you want to make NTFS, and choose Format.



- Select NTFS from the File system menu (this will delete all information on the partition).

Discussion: NTFS format allows individual permissions to be set on directories and files. This allows much more control for the administrator, and makes it more difficult for an attacker to upload malicious code to your server. Most of the fixes for WWW and FTP server vulnerabilities rely on NTFS permissions. The convert command may be used to convert a FAT partition to NTFS without losing the data already on that partition.

Best Practice: Use a partition separate from your boot and operating system partitions for your Internet services.

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

Securing IIS on Windows 2000

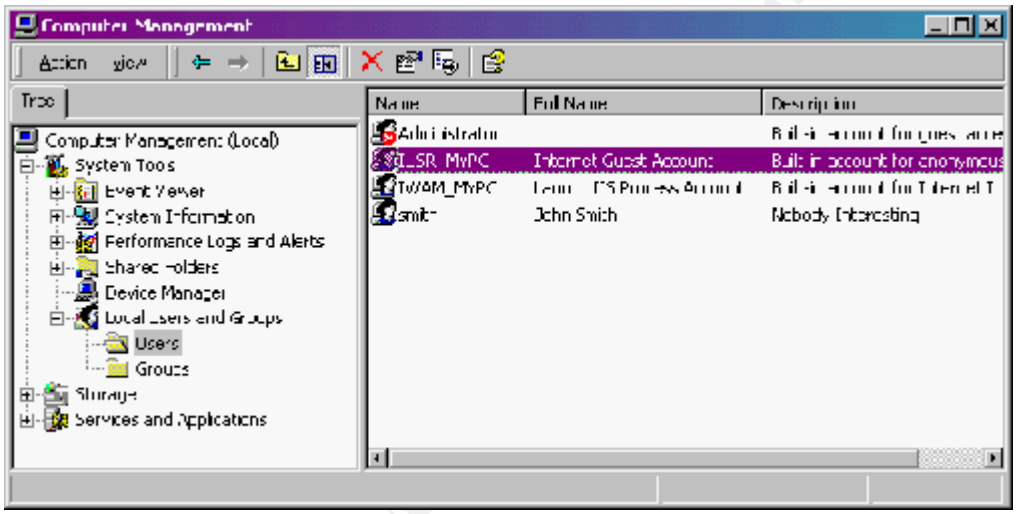
by Carl Denowh

Securing Internet Information Server

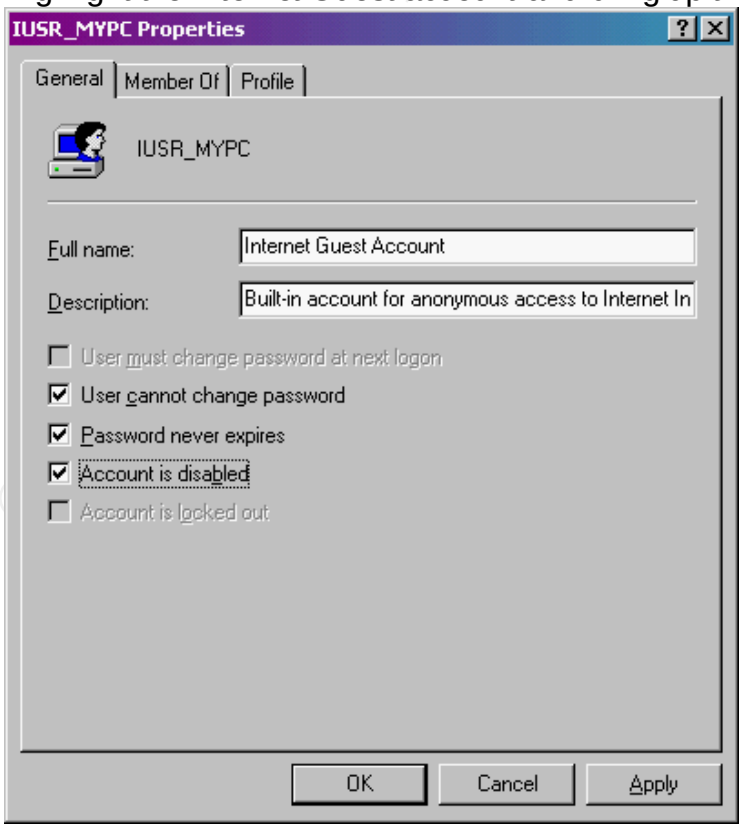
1. Set up alternate user accounts.

   How:

   - Choose Administrative Tools from the Control Panel.
   - Choose Computer Management from the Administrative Tools window.
   - From the System Tools tree choose Local Users and Groups, then Users.

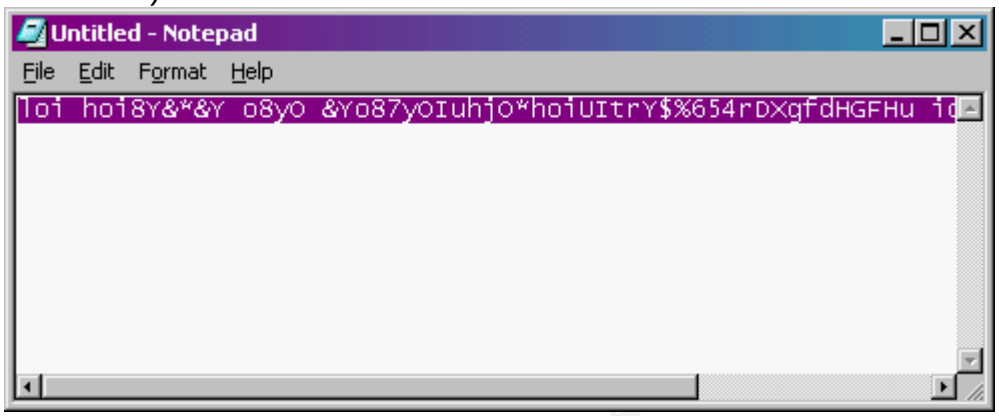


   - Highlight the Internet Guest account and bring up the Properties.

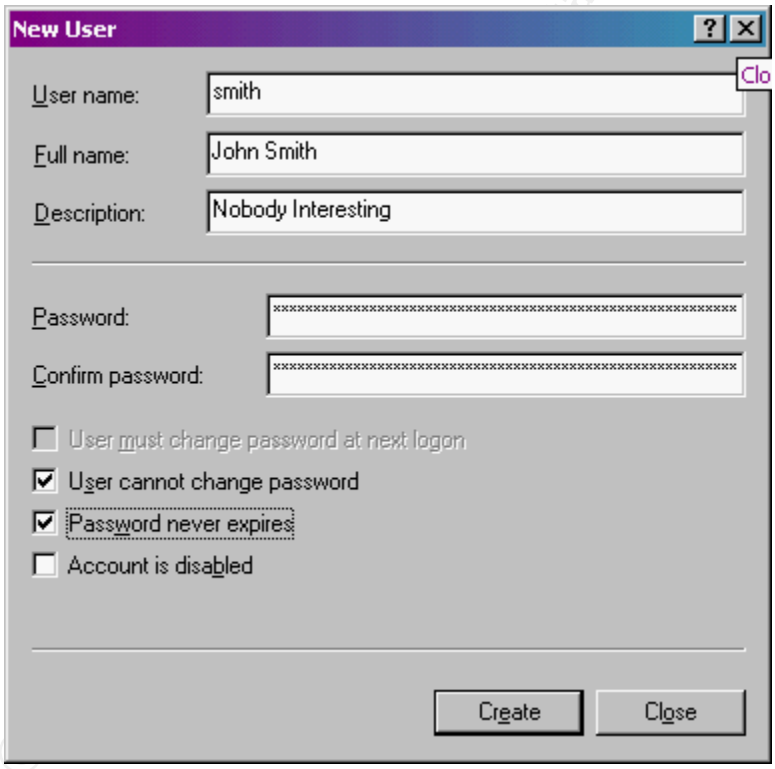


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Check the Account is disabled box and select OK.
- In the background, bring up a text editor such as notepad and type a long random string. (Keep this window up; you will need it for future reference.)



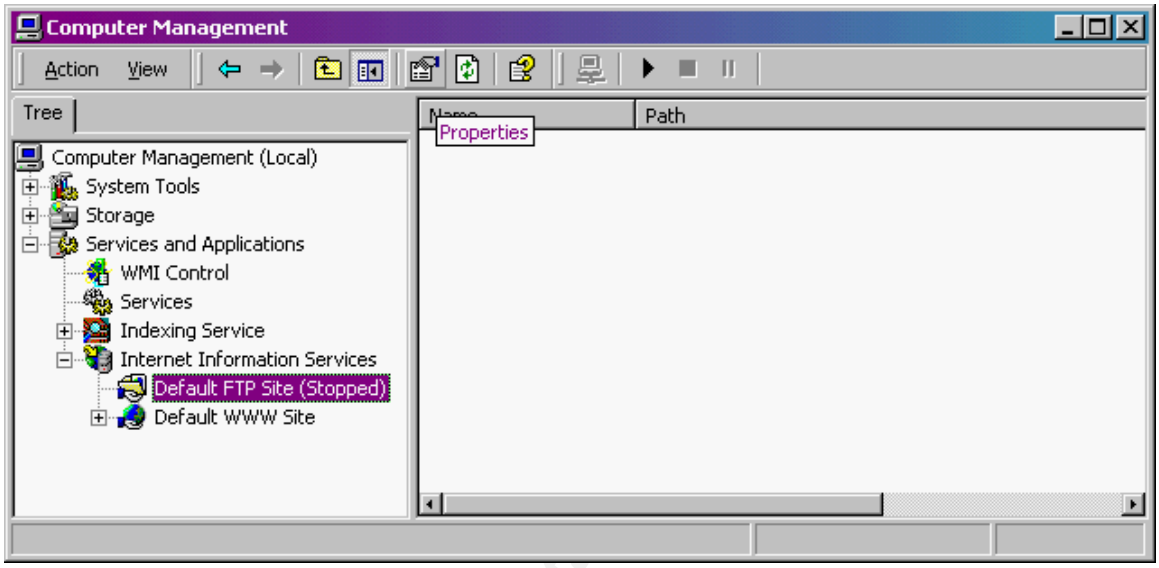
- From the Computer Management window, highlight the Users folder and select New User from the Action menu.



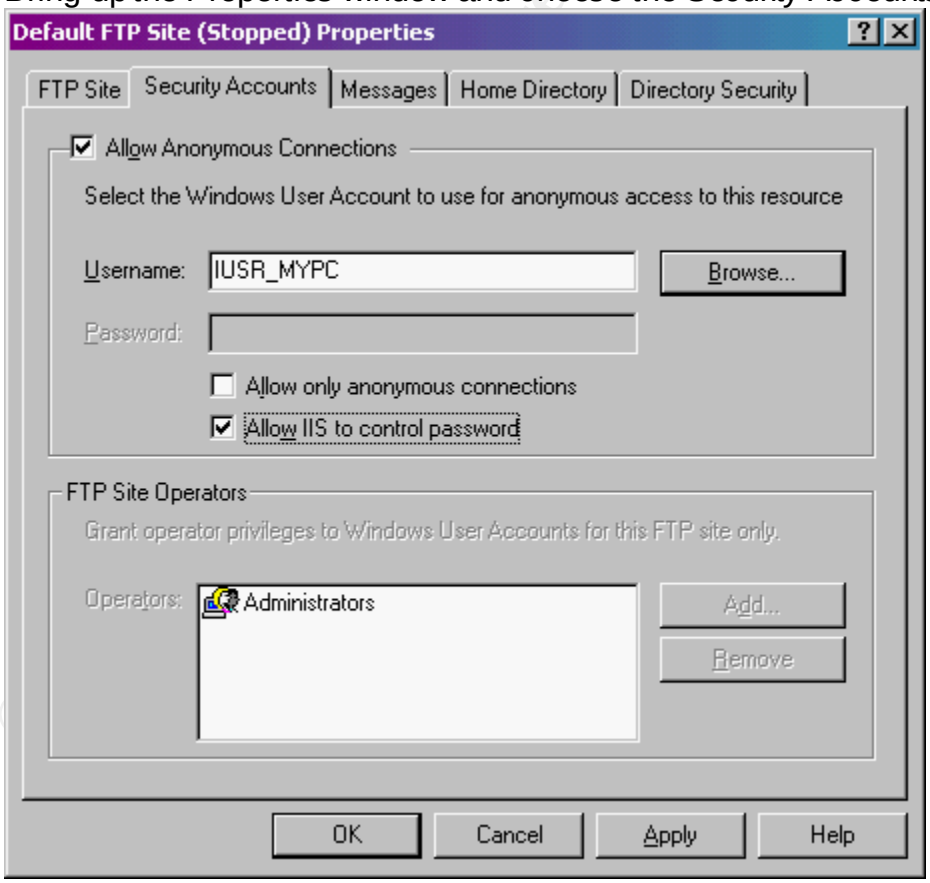
- Create a fictitious account with the User must change password option unchecked, the User cannot change password checked, and the Password never expires option checked. (This will be the real Internet guest account.)
- Cut the long string from the text editor and paste it into the password fields.
- Choose Create then Close.

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

- From the Services and Applications tree choose Internet Information Services, then Default FTP Site.



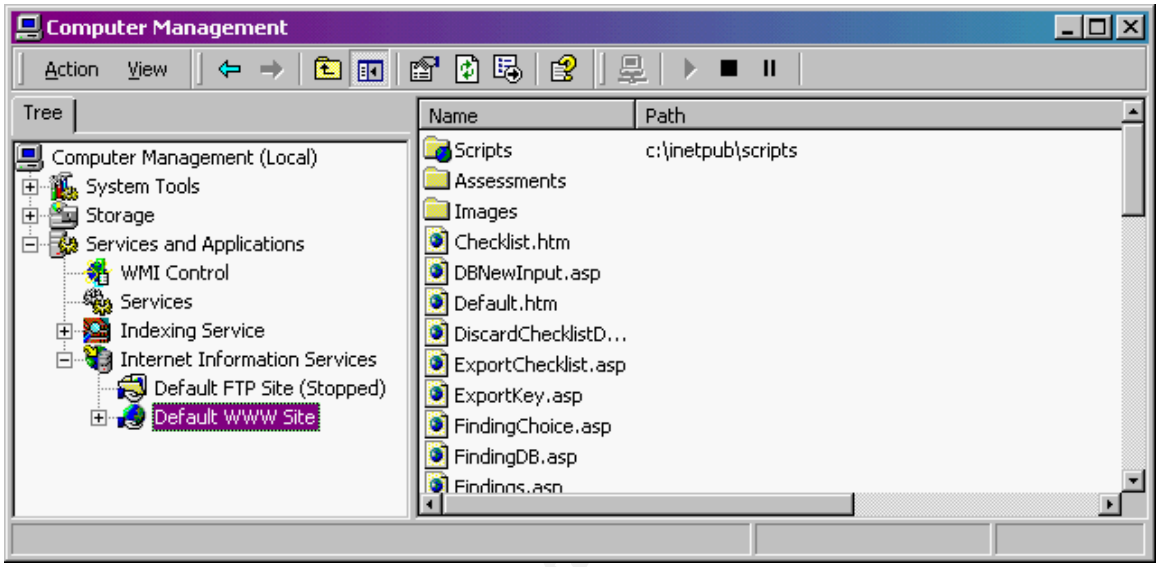
- Bring up the Properties window and choose the Security Accounts tab.



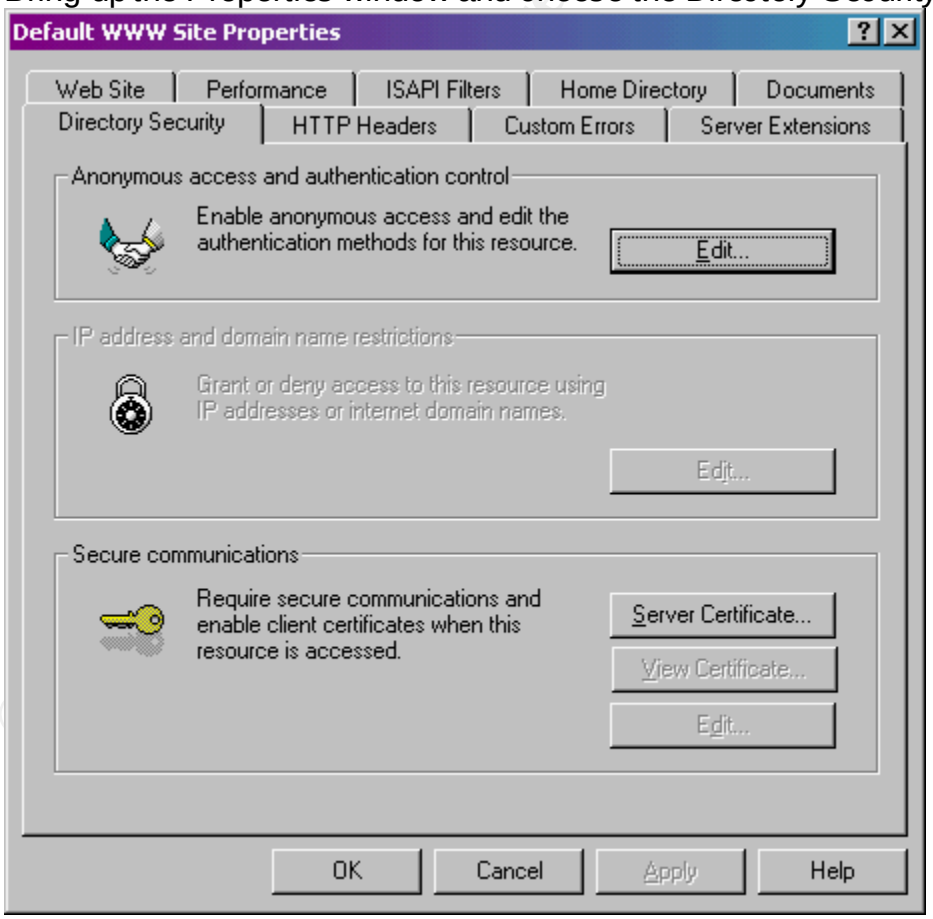
- Use Browse to select the new account you just created.
- Do not select the Allow IIS to control password option.
- Cut the long string from the text editor and paste it into the password fields and apply the changes.

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

- From the Internet Information Services tree, choose Default WWW Site.

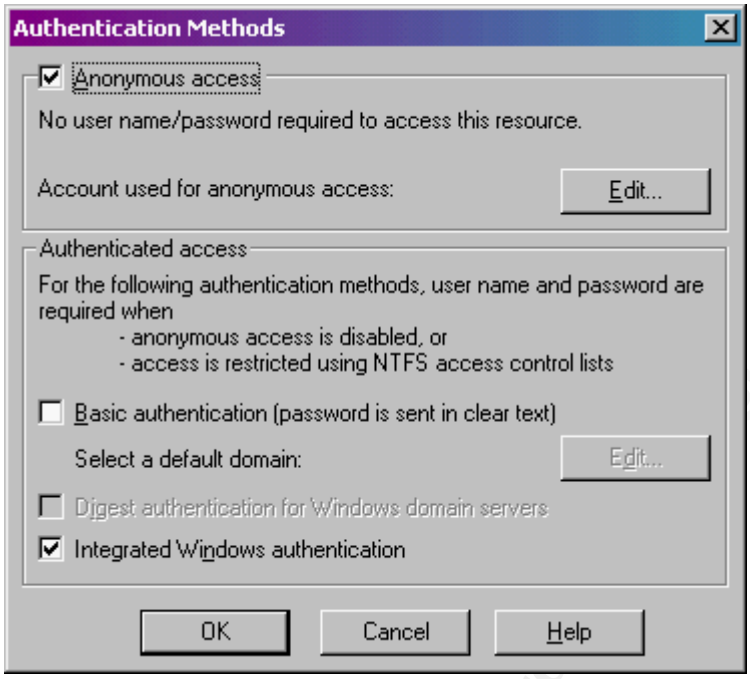


- Bring up the Properties window and choose the Directory Security tab.

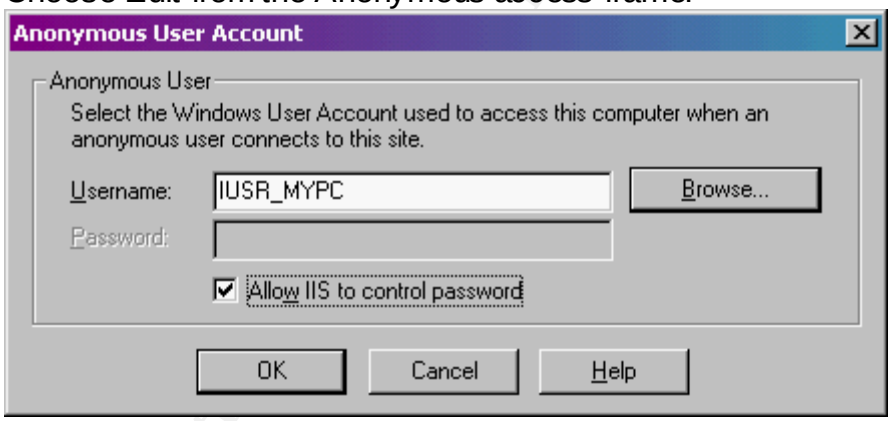


- Choose Edit from the Anonymous access and authentication control frame.

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



- Choose Edit from the Anonymous access frame.



- Use Browse to select the new account you created.
- Do not select the Allow IIS to control password option.
- Cut the long string from the text editor and paste it into the password fields and apply the changes. (You may now close the text editor without saving.)

Discussion: It is not required to keep the original anonymous user account, but this is a little bit of extra misdirection meant to delay an intruder. These accounts could be used to access your machine.

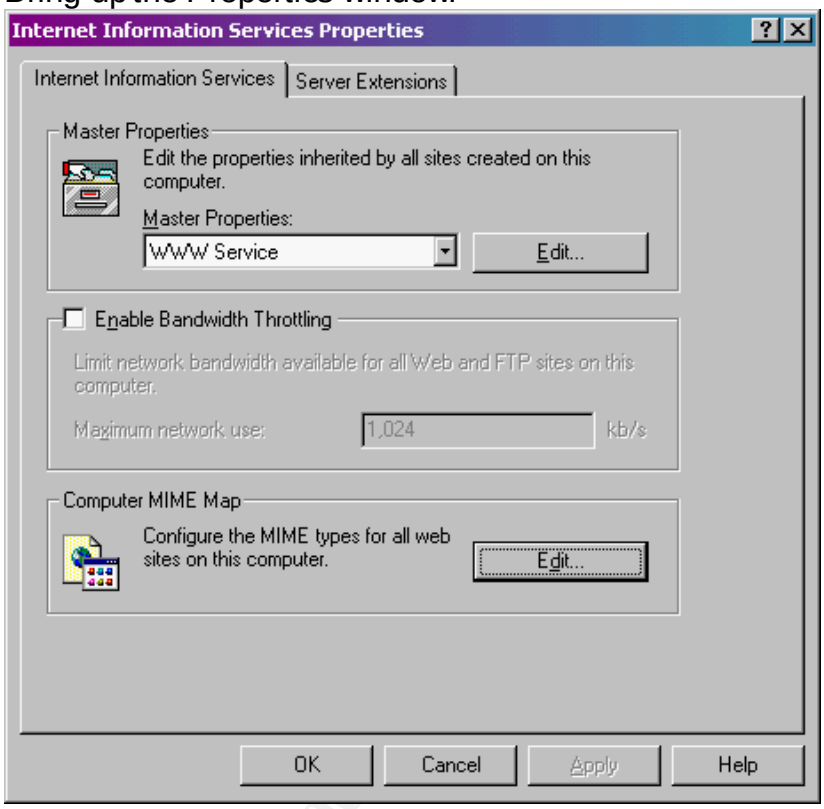
Best Practice: If you are extra paranoid, you will want to remember to change the passwords on these accounts periodically.

2. Disable unnecessary file types.

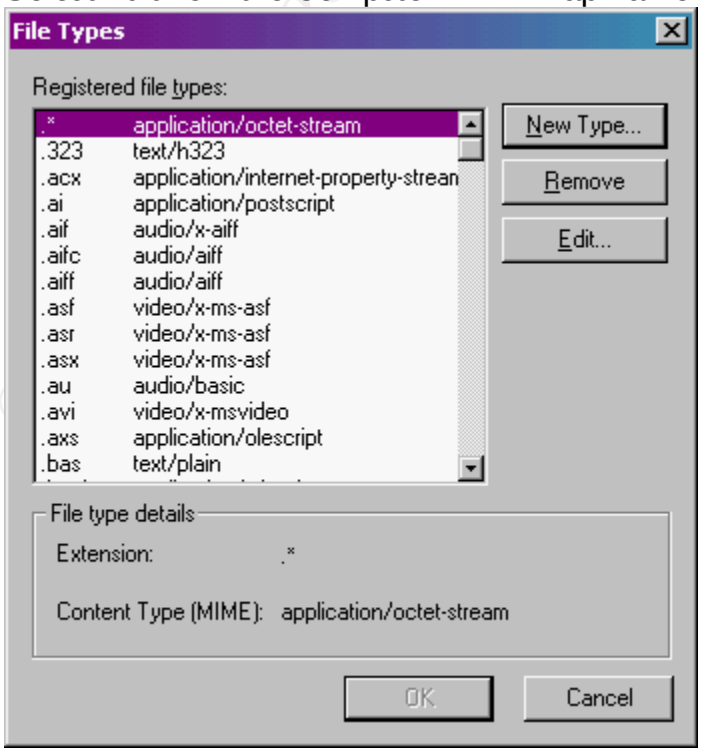
How:

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

- Choose Computer Management from the Administrative Tools window.
- From the Services and Applications tree, select Internet Information Services.
- Bring up the Properties window.



- Select Edit from the Computer MIME Map frame.



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

- Select and remove unneeded entries.

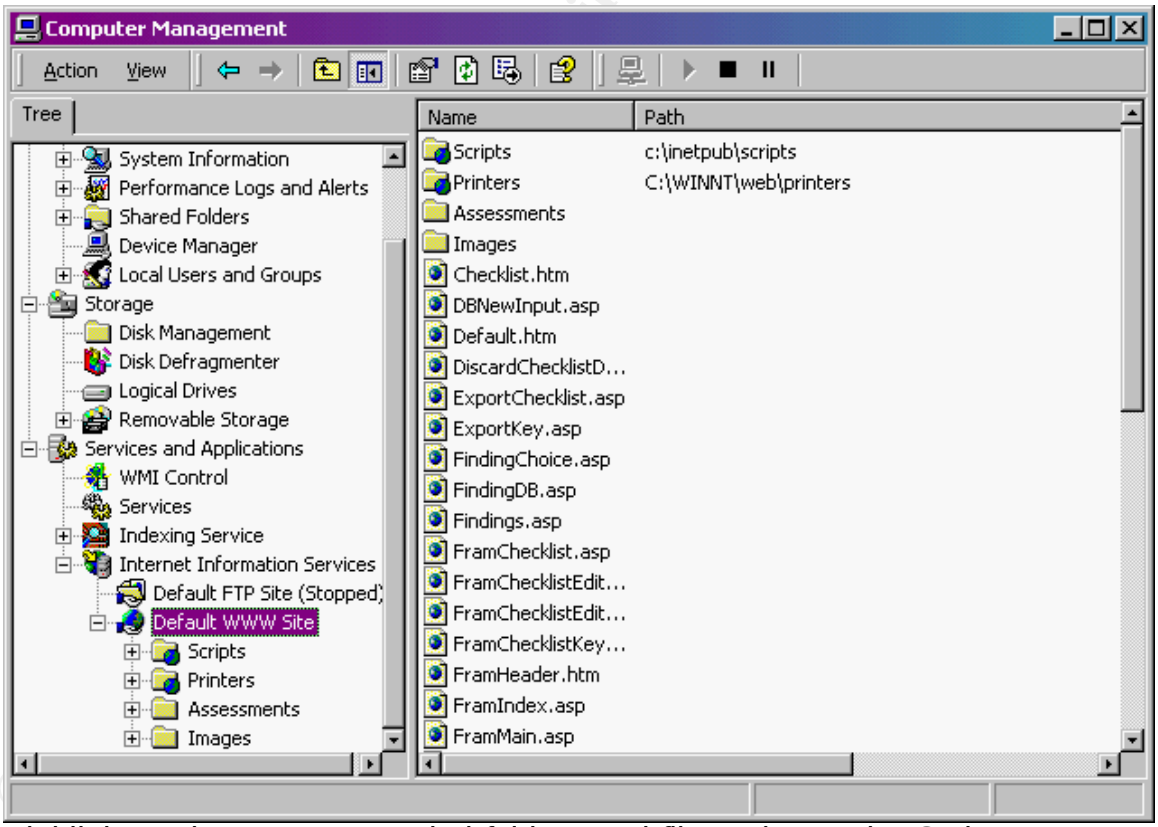
Discussion: These extensions tell IIS what application or DLL to run when that extension is encountered. An attacker may attempt to substitute a malicious file for the original and exploit the vulnerability thus created.

Best Practice: As a rule of thumb, it is more secure to change the defaults for everything you can. The more an intruder has to figure out, the harder his job.

3. Remove unnecessary files and folders.

How:

- Choose Computer Management from the Administrative Tools window.
- From the Services and Applications tree, select Internet Information Services, then the Default WWW Site.



- Highlight and remove unneeded folders and files. (Keep the Scripts folder.)

Discussion: Many vulnerabilities are due to the sample files that are installed by default. These should be removed. Keep the Scripts folder only if you will be using scripts on this web site.

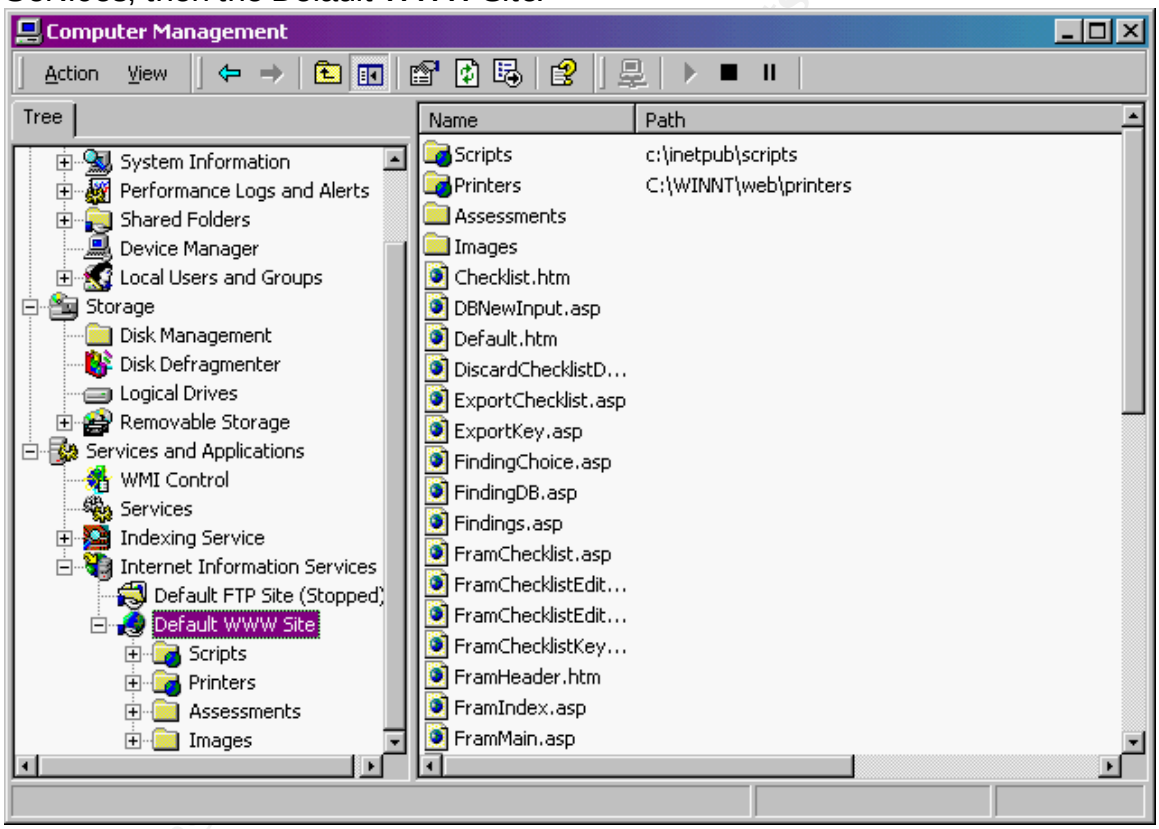
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Best Practice: Windows Explorer can be used to further restrict access to scripts through NTFS file permissions.

4. Set properties for each web folder.

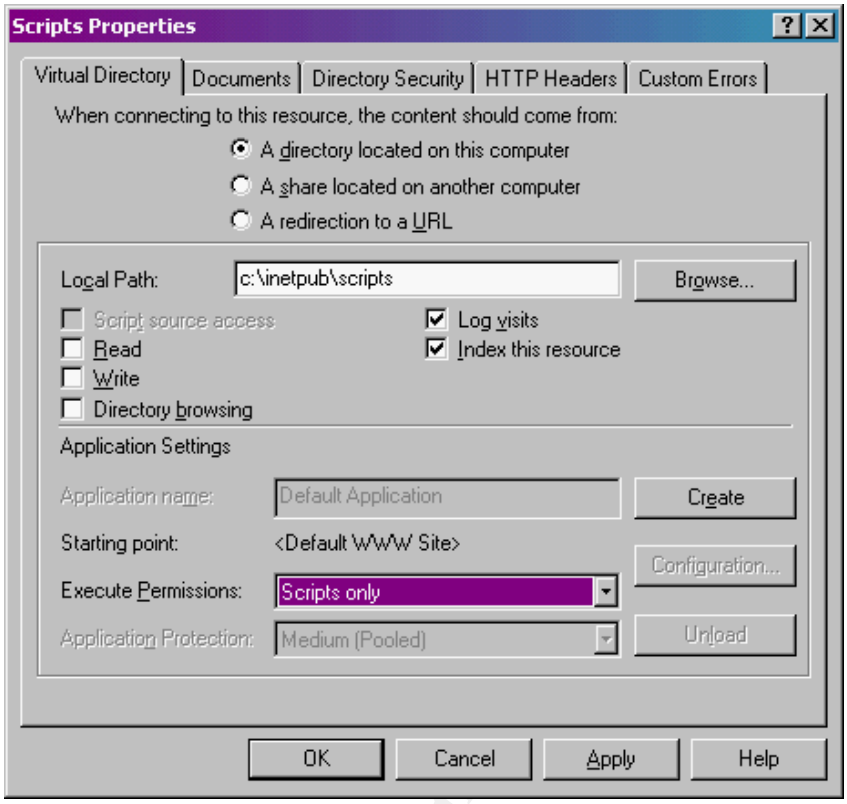
How:

- Choose Computer Management from the Administrative Tools window.
- From the Services and Applications tree, select Internet Information Services, then the Default WWW Site.

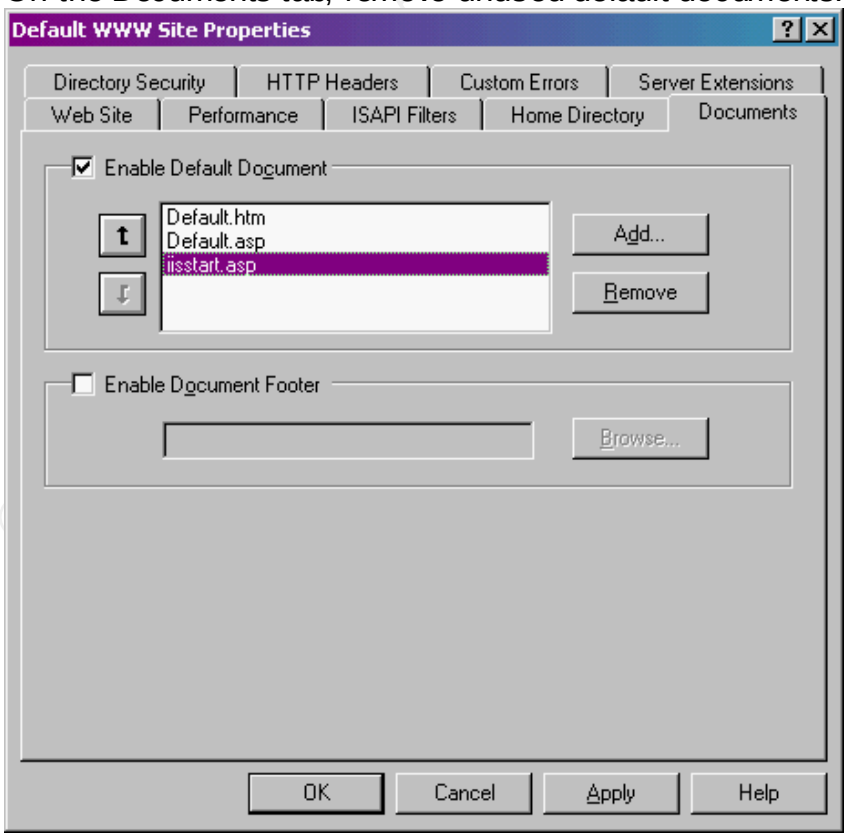


- Bring up the Properties window of all folders (including the root).

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

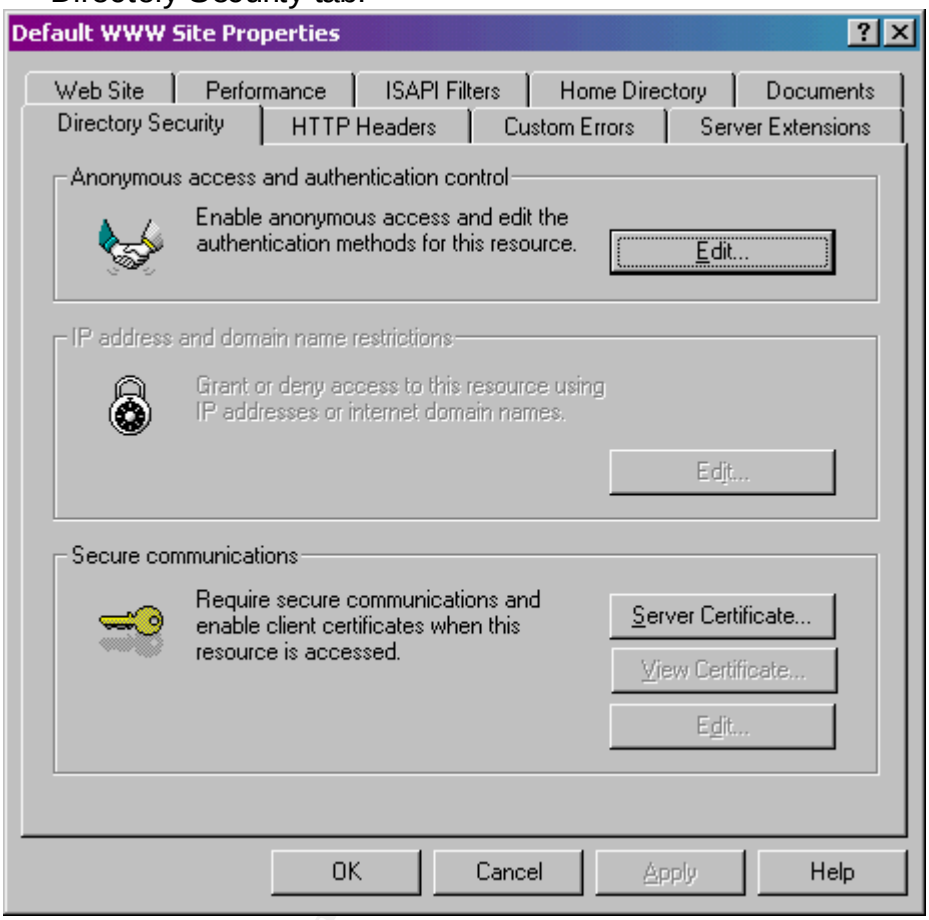


- Set appropriate Read, Write, and Execute permissions on each folder.
- On the Documents tab, remove unused default documents.



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

- If you are running Windows 2000 Server, you will have the option to Edit the IP address and domain name restrictions settings on the Directory Security tab.



Discussion: Permissions on folders should be as restrictive as possible. If you need to run scripts, use a scripts folder with Execute Permissions set to Scripts only and no Read or Write Permissions. Avoid executables whenever possible. Other directories should have no Execute Permissions and be set to Read only. Directory browsing should always be off. IP address and domain name restrictions should be set to duplicate your firewall rules. This adds another layer of security.

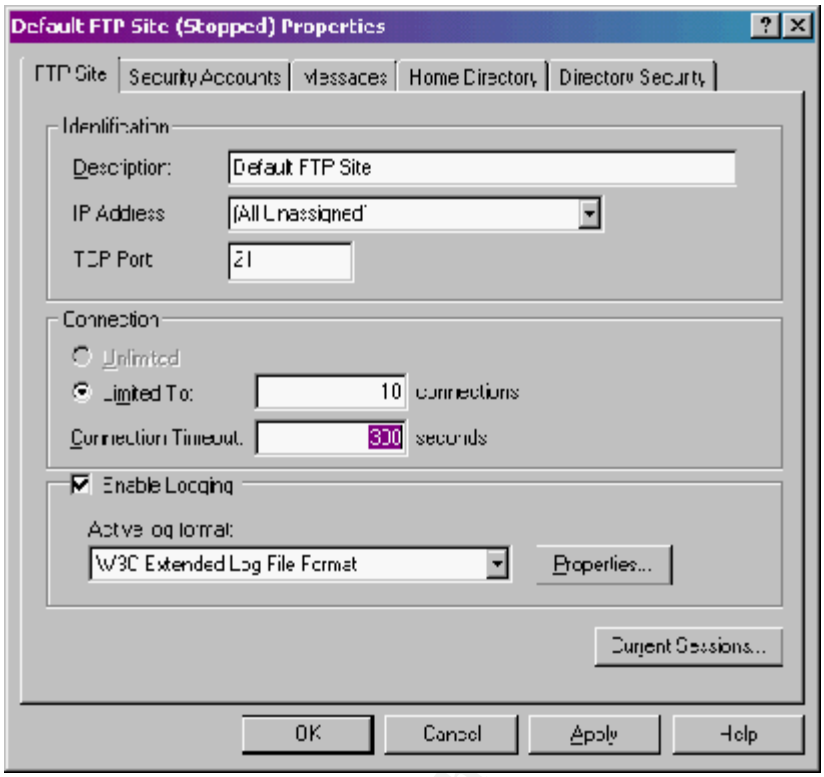
Best Practice: Windows Explorer can be used to further restrict access to files and folders to authenticated users.

5. Set properties for each FTP folder.

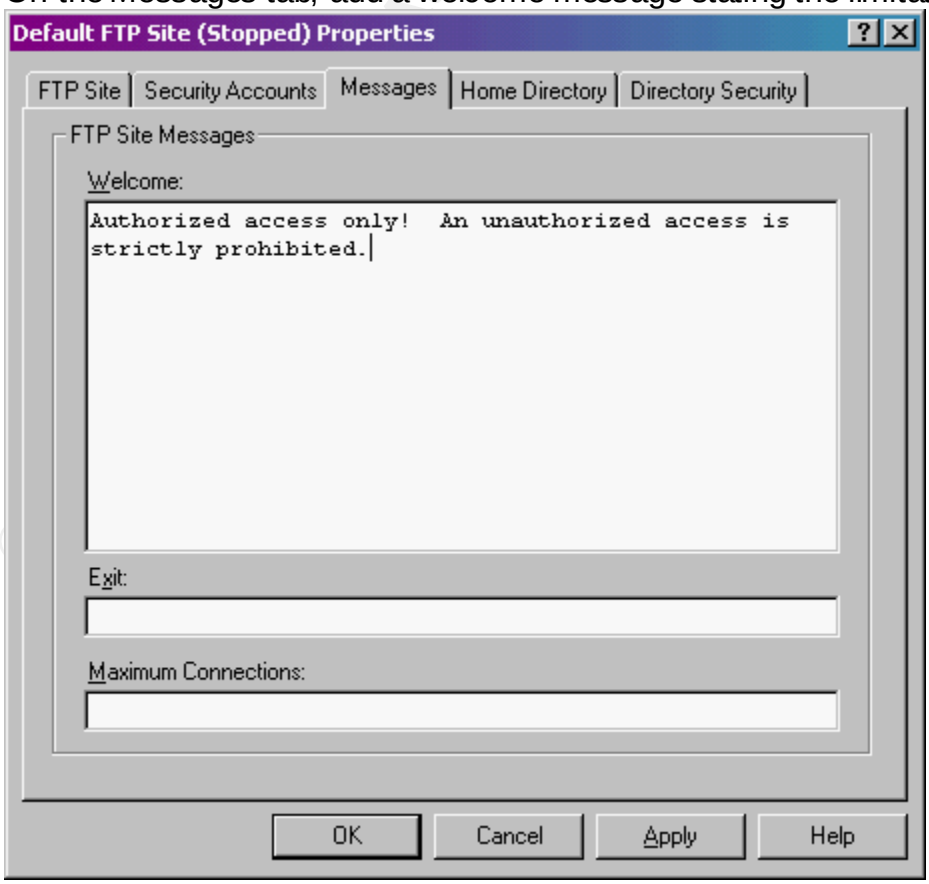
How:

- Choose Computer Management from the Administrative Tools window.
- From the Services and Applications tree, select Internet Information Services.
- Bring up the Properties window for your Default FTP Site.

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

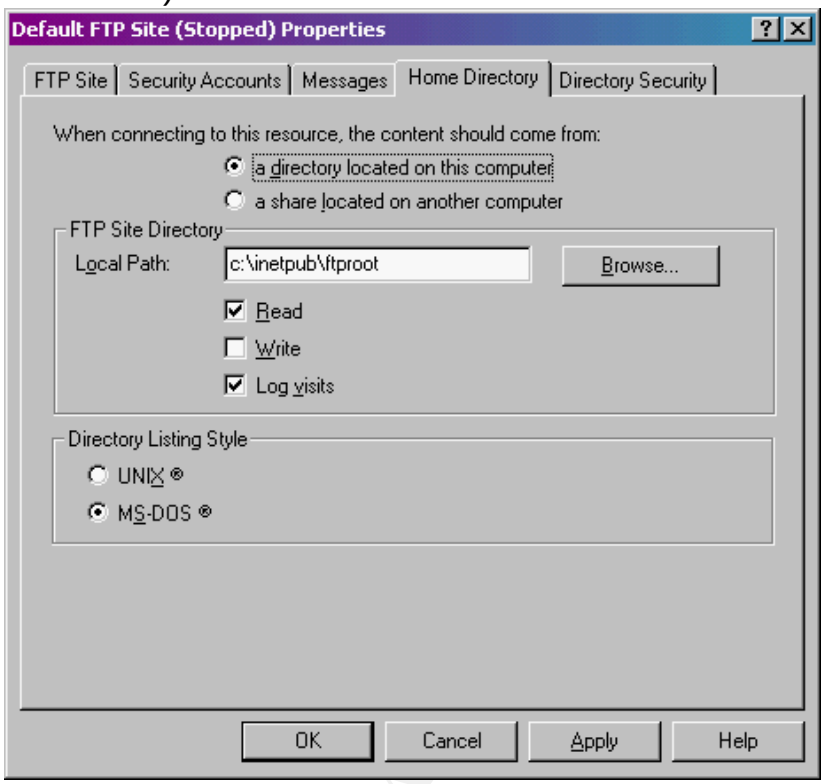


- The Connection Timeout setting should be fairly short.
- On the Messages tab, add a welcome message stating the limitations.

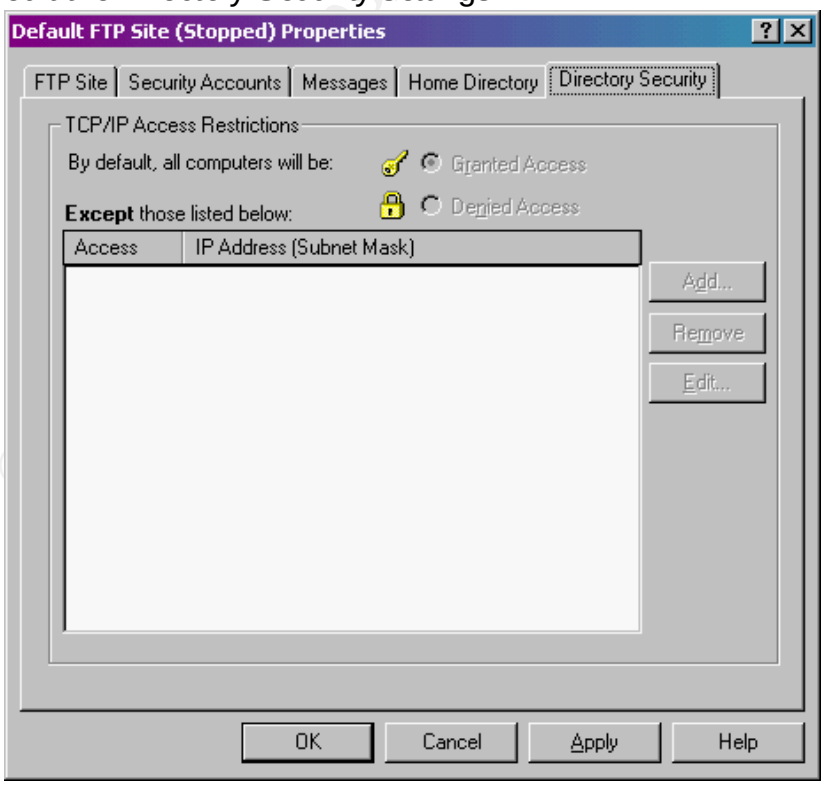


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- On the Directory tab, restrict permissions. (Do this for all FTP directories.)



- If you are running Windows 2000 Server, you will have the option to edit the Directory Security settings.



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

Discussion: Permissions on folders should be as restrictive as possible and as separated as possible. It is a good idea to have separate folders for upload and download. The welcome message allows you to figuratively post your no trespassing sign, or in this case, no fooling around sign. This gives you legal recourse for malicious attackers. Directory Security settings should mirror your firewall settings to add an additional layer of security.

Best Practice: FTP servers and WWW servers should be separate systems with the other service(s) stopped.

Sources

[1] Fennelly, Carole. "According to statistics." January 26, 2001. http://www.sunworld.com/unixinsideronline/swol-01-2001/swol-0126-unixsecurity.html.

[2] Stein, Lincoln D. "The World Wide Web Security FAQ." September 13, 1999. http://www.w3.org/Security/Faq/wwwsf1.html.

[3] Smith, Danny. "Improving Computer Security Through Network Design." 1997. http://www.auscert.org.au/Information/Auscert_info/Papers/Security_Domains.html.

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

Last Updated: September 4th, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced