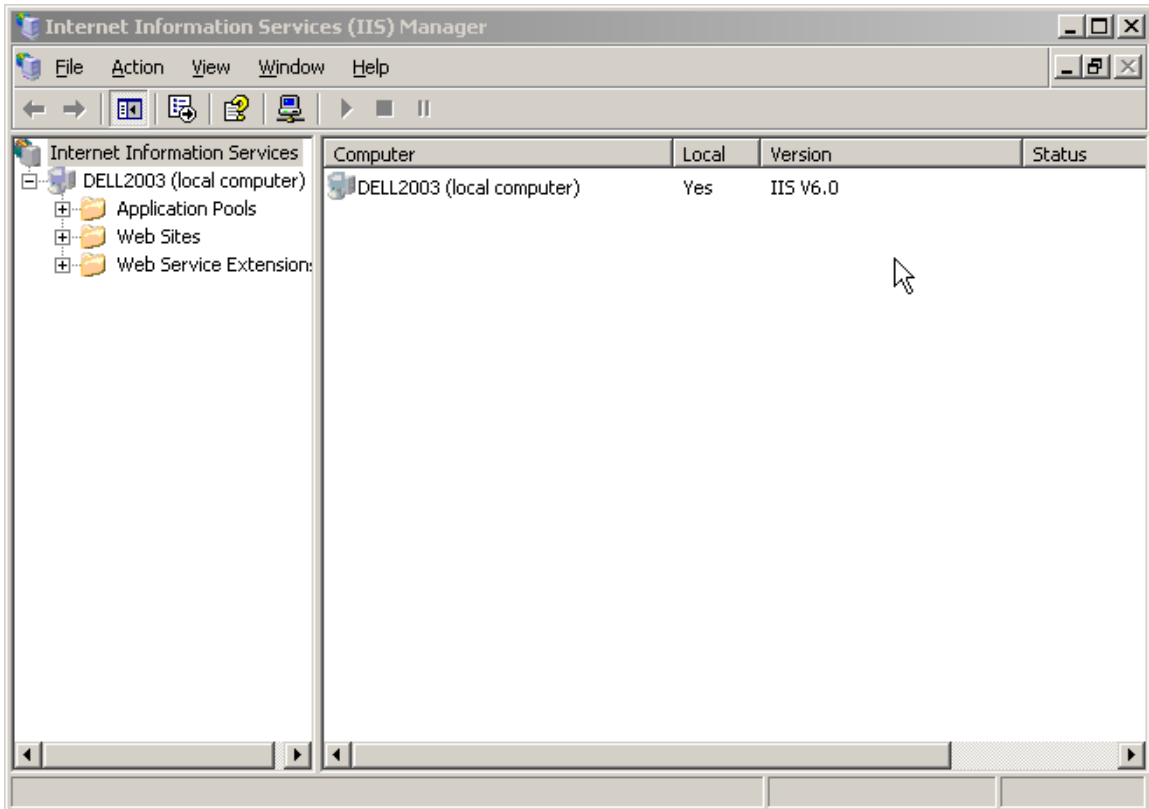


Securing IIS in Windows Server 2003

Version 1



September 3, 2004

Laboratory Overview

Objective

At the end of this lab students will be able to apply security measures to a Windows Server 2003 running IIS version 6.0.

Information for Laboratory

- A. Students will utilize several tabs in the IIS Manager in Windows Server 2003 to “lockdown” IIS.
- B. Students will utilize the Microsoft Baseline Security Analyzer(MBSA) to scan and verify that the server is secure
- C. Students will attempt to connect to the server through both secure and insecure modes.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion. Students should also have a basic understanding of how IIS works.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that IIS has been installed on a Windows Server 2003 system, using the default installation. The latest version of the MBSA (found at <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>) should also be installed on the server system.

Warning[s]

Please do not attempt to do this lab with an unpatched server. Ideally, this lab should be performed with servers on their own switch, as not to disrupt a normal operating network.

Estimated Completion Time

30 Minutes

Securing IIS in Windows Server 2003

In earlier versions of Windows Server, IIS was part of the default installation, leaving many security vulnerabilities. By default, IIS is NOT installed on Windows Server 2003. When IIS is initially configured on Windows Server 2003, it is in a highly secure mode. Still, there are steps which should be taken to further lock down IIS on the server to protect the Web sites and applications hosted on the server.

IIS Manager

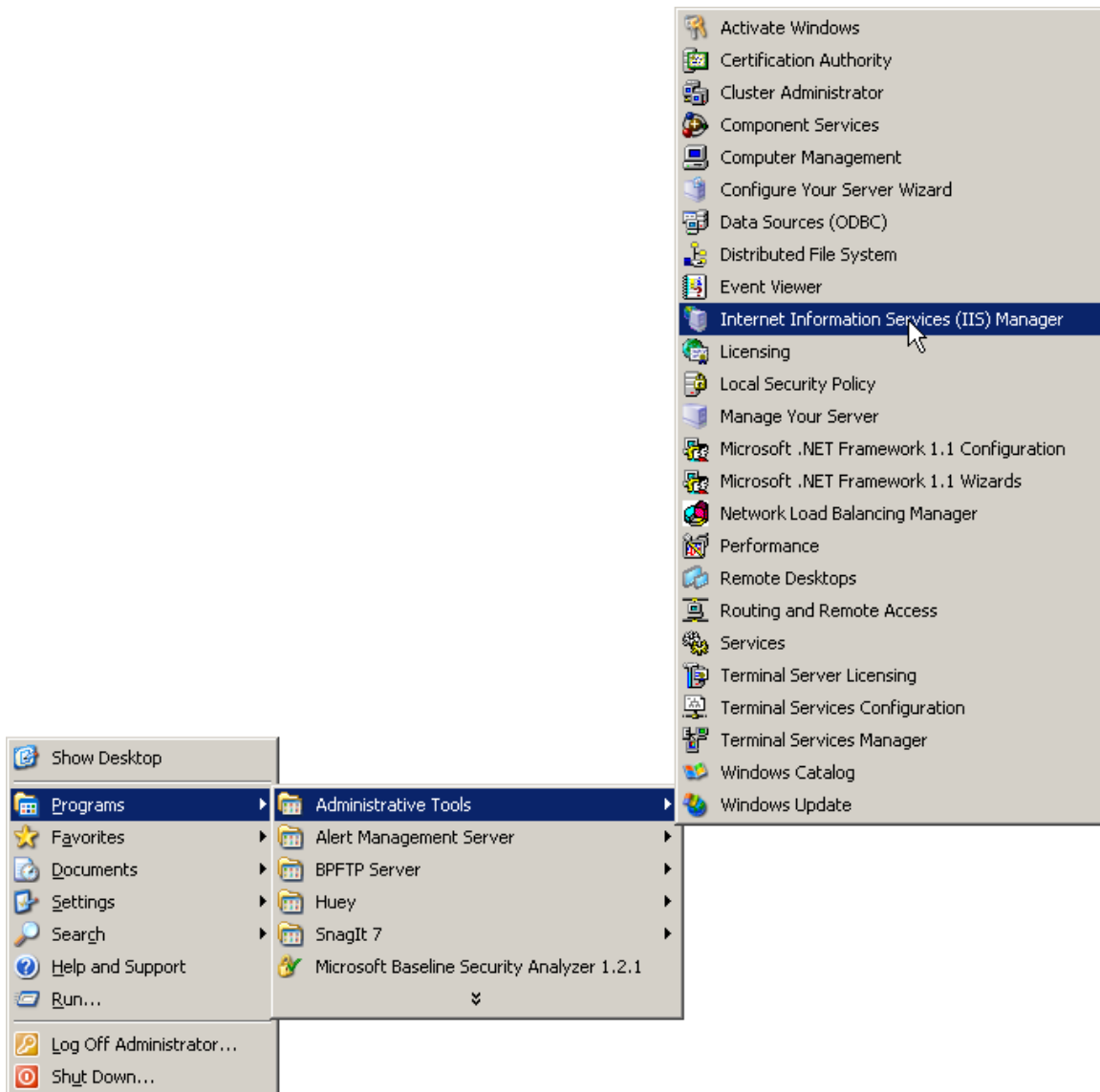
The IIS manager snap-in is installed when IIS is loaded on the server. It is accessed through the Administrative Tools section of the Programs menu.

MBSA

Microsoft Baseline Security Analyzer is a free tool provided by Microsoft. In addition to pointing out security 'holes' on a server, it can also scan other Microsoft applications (such as Office) for vulnerabilities. However, this lab will focus on IIS vulnerabilities.

Step I: Running IIS Manager

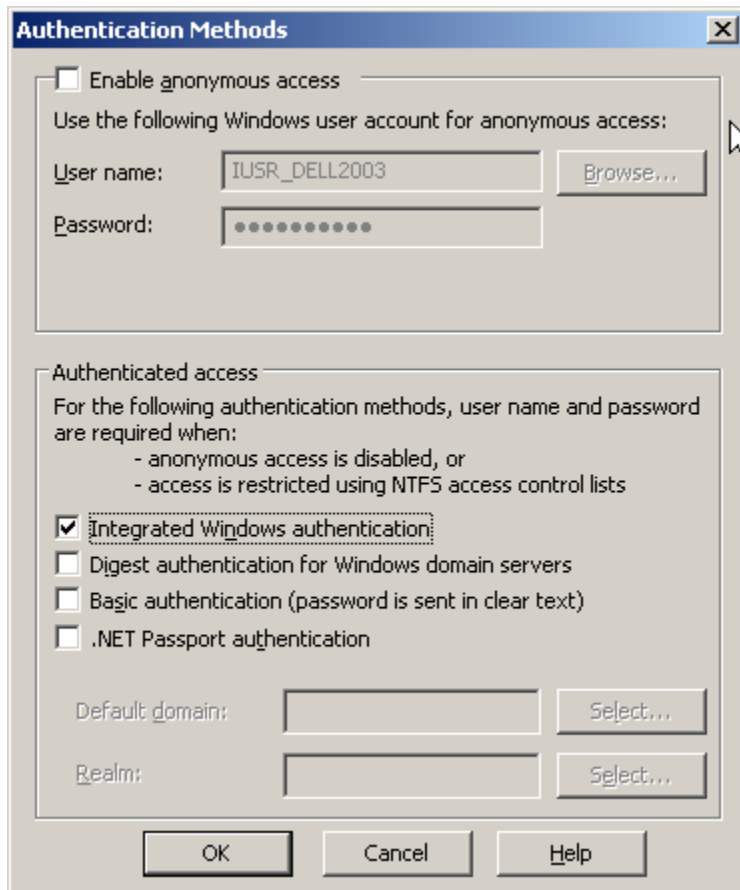
- 1) Go to Start → Programs → Administrative Tools → IIS Manager



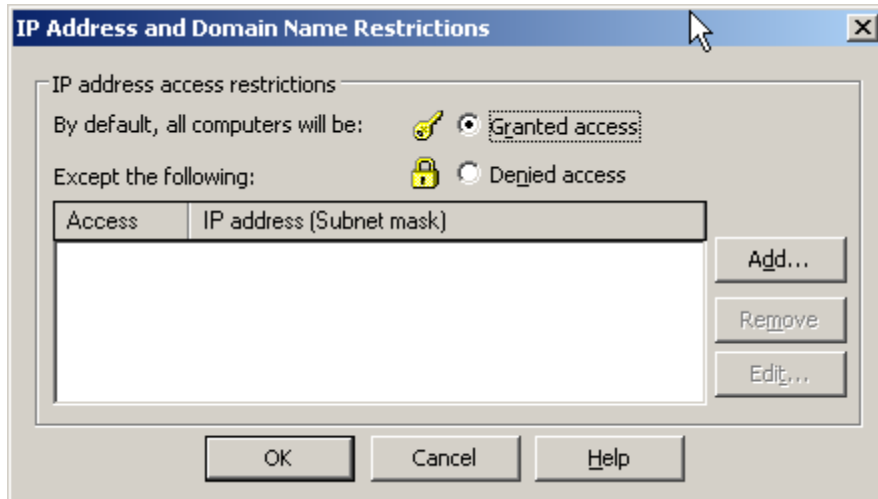
- 2) Right-click on Web Sites (in the left-hand pane) and choose Properties. This is where most of the security enhancements will need to be applied. Explore the tabs on the Web site properties. There are eight tabs. The most important one for our exercises will be the Directory Security Tab. Note that if your IIS server hosts several web sites, they will appear underneath Web Sites on the left pane.
- 3) Click on the Directory Security tab. Notice that there are three main parts to this tab. First, there is the Authentication and Access Control, then IP address and domain name restrictions, then Secure Communications.

Step 2: Managing IIS Security Settings

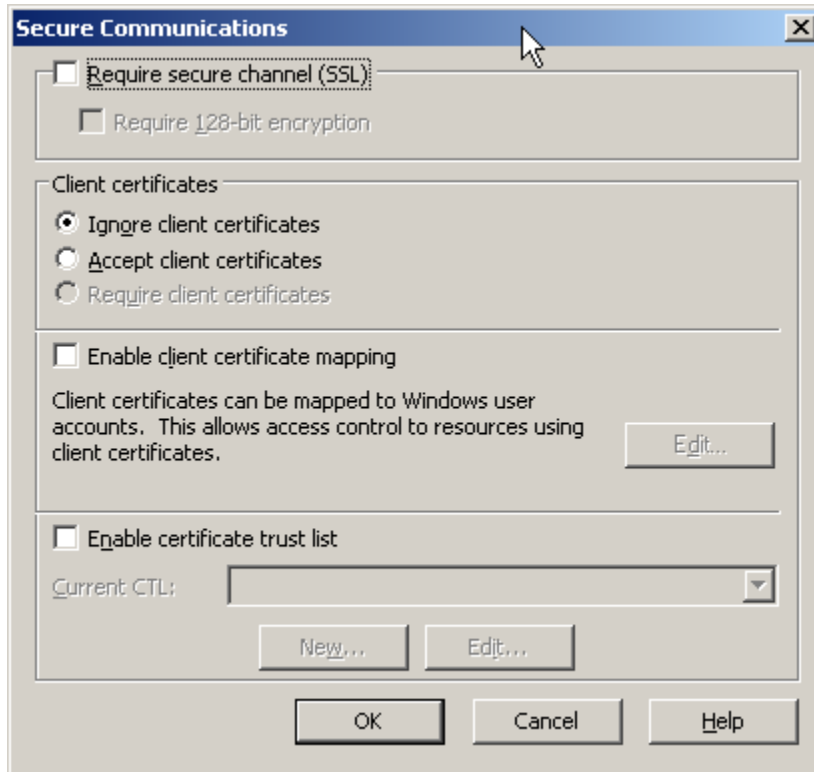
- 1) From the Directory Security tab, under Authentication and access control, click Edit.
- 2) To prevent anonymous users from attaching to your Web site, un-check "Enable Anonymous Access".
- 3) Now, choose the method of authentication. Notice that there are four options. The first option, Integrated Windows Authentication, will use the credentials supplied when the user first logs into Windows. The second option, Digest Authentication for Windows Domain servers, is used when there is a need to transmit a hashed security challenge; the password itself is never actually transmitted. The third option, Basic Authentication, is just a bad idea. This method should only be used when no other form of authentication will work. In Basic Authentication, both the username and password are transmitted in clear text. The fourth option, .Net Passport authentication, allows the .NET passport username and password to be used for authentication. This service is provided by Microsoft. We will choose the default, or Integrated Windows authentication. Click OK to confirm this selection.



- 4) Now, when you are back at the Web Site Properties dialog box, on the Directory Security tab, click Edit in the IP address restrictions section. The IP address and Domain Name restrictions dialog box is displayed.



- 5) Notice, by default, that all computers will be granted access. There are two options; Granted access or Denied access. If you wish to deny certain IP addresses access to your Web pages, you should add them to the list. For practice, click on Add, enter the IP address of one of your lab mates, and click OK. Then have that person attempt to connect to your Web server. Troubleshoot as necessary.
- 6) Next, when back at the Directory Security tab of the Web Site Properties, under the Secure communications section, click on Edit.

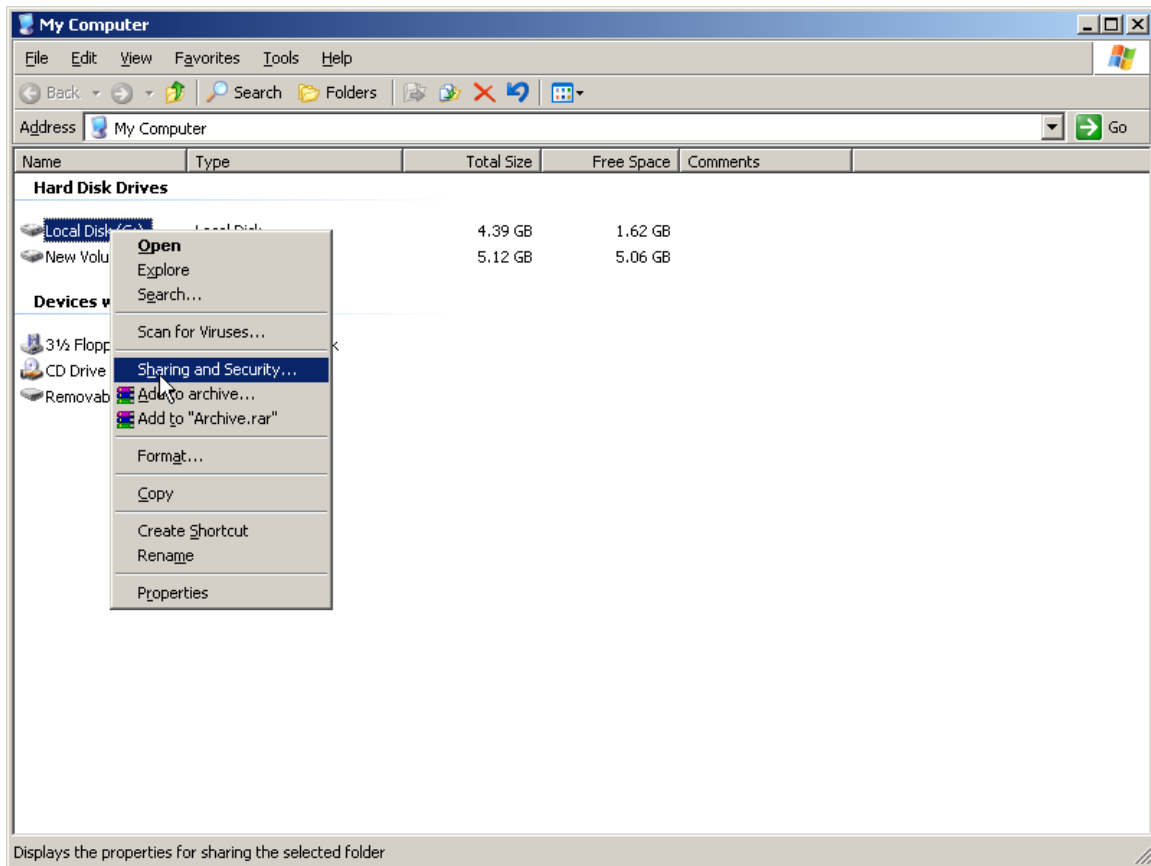


- 7) Notice that SSL is not required by default. To assure secure communications with your Web server, you can check Require secure channel (SSL), and enable 128-bit encryption. Click Require secure channel (SSL) and check Require 128-bit encryption.
- 8) The default settings for client certificates are set to Ignore. In what type of scenario would you want to choose Accept or Require client certificates?
- 9) Finally, click OK to return to the Web site properties dialog box.

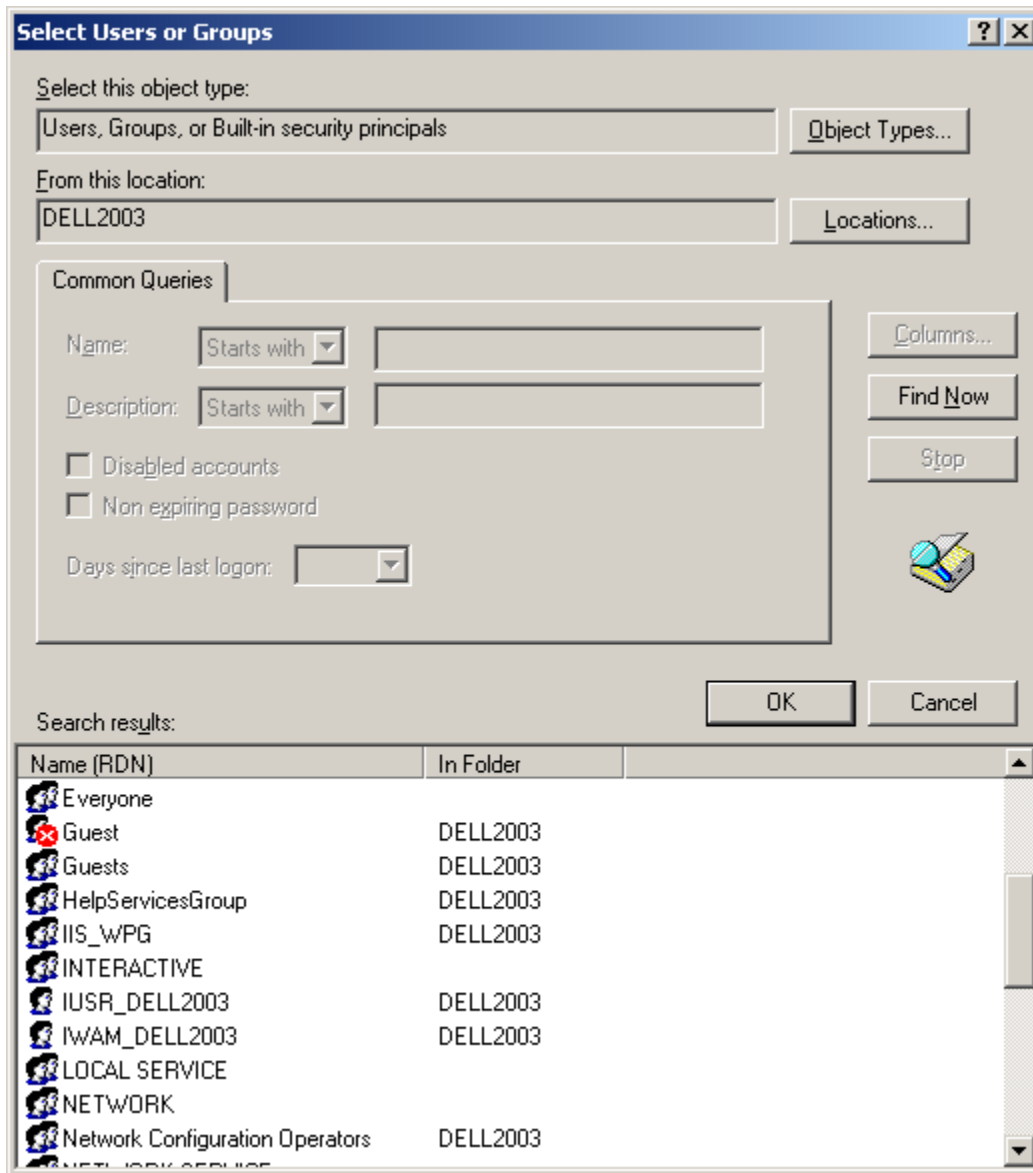
Step 3: NTFS Permissions for IUSR Account

We need to prevent the IUSR anonymous account from accessing files outside of the Web root. There are a couple of ways to accomplish this, but this one seems to be the most effective.

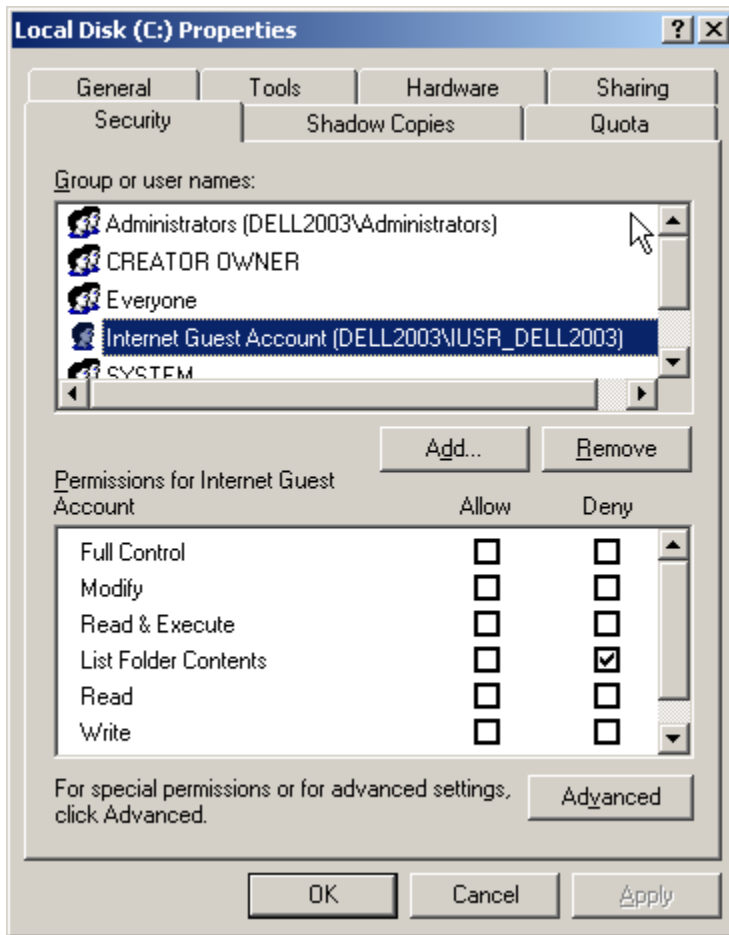
- 1) Open My Computer and right-click on the C: drive. Select "Sharing and Security"



- 2) You will probably need to add the IUSR account to the list of accounts, if so, follow these steps: Click Add. The Select Users or Groups dialog box will appear. Click Advanced, then click Find Now. All users and groups will appear.



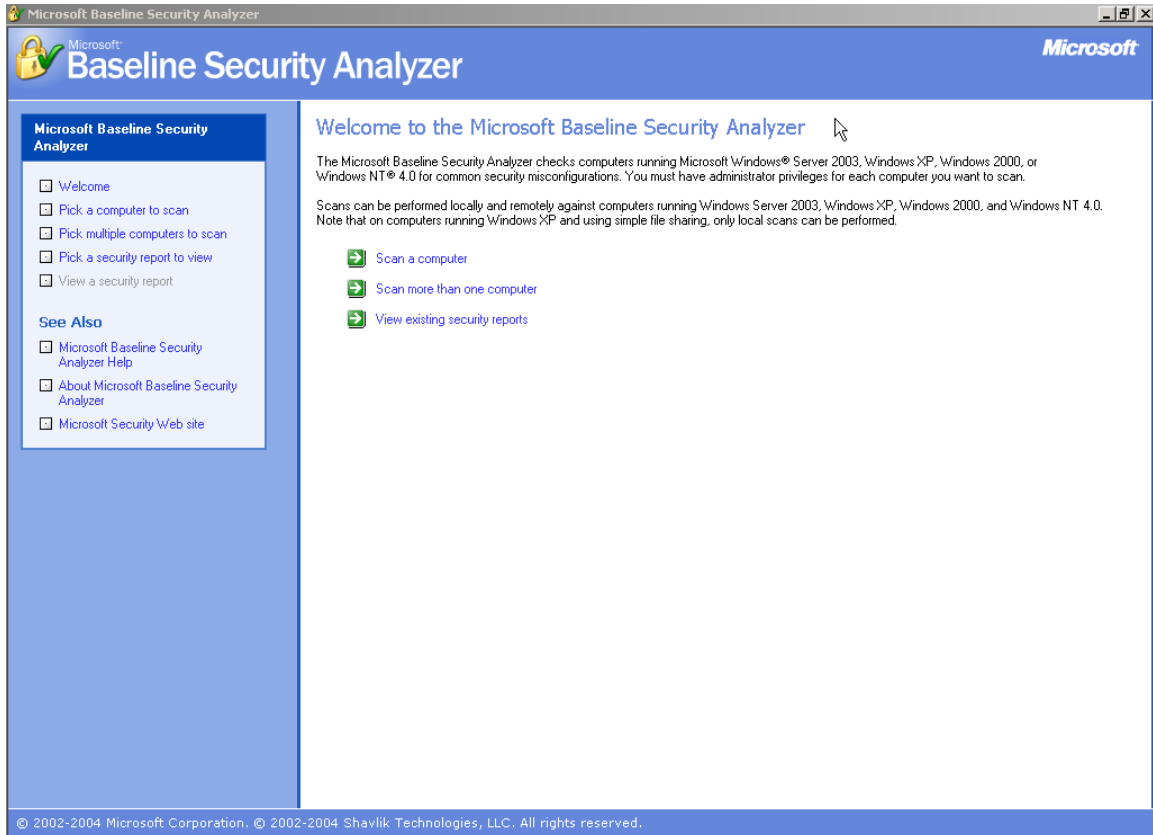
- 3) From this list, choose the *IUSR_COMPUTERNAME* account and click OK. Click OK again at the first Select Users and Groups dialog box.
- 4) From the security tab, choose the IUSR account, and click on the Deny button for the “List Folder Contents” option.



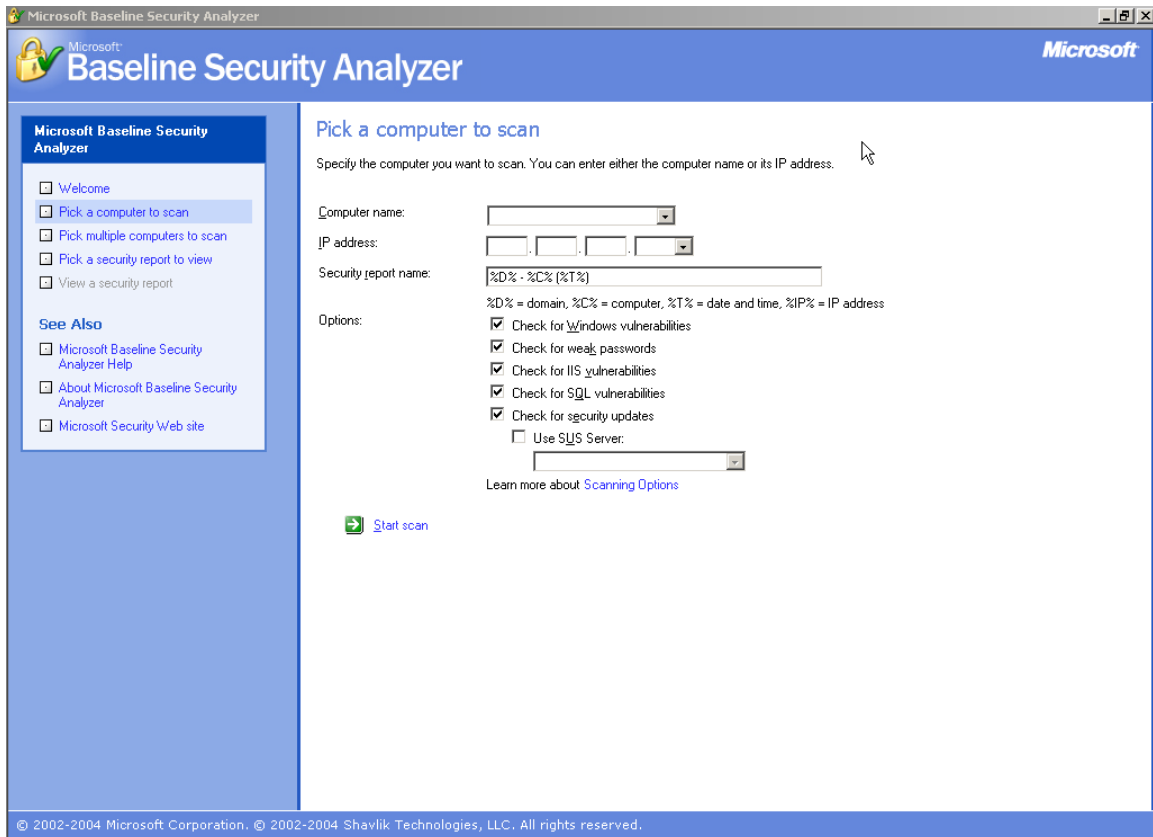
5) Click Apply, then OK to close the dialog box.

Step 4: Running MBSA

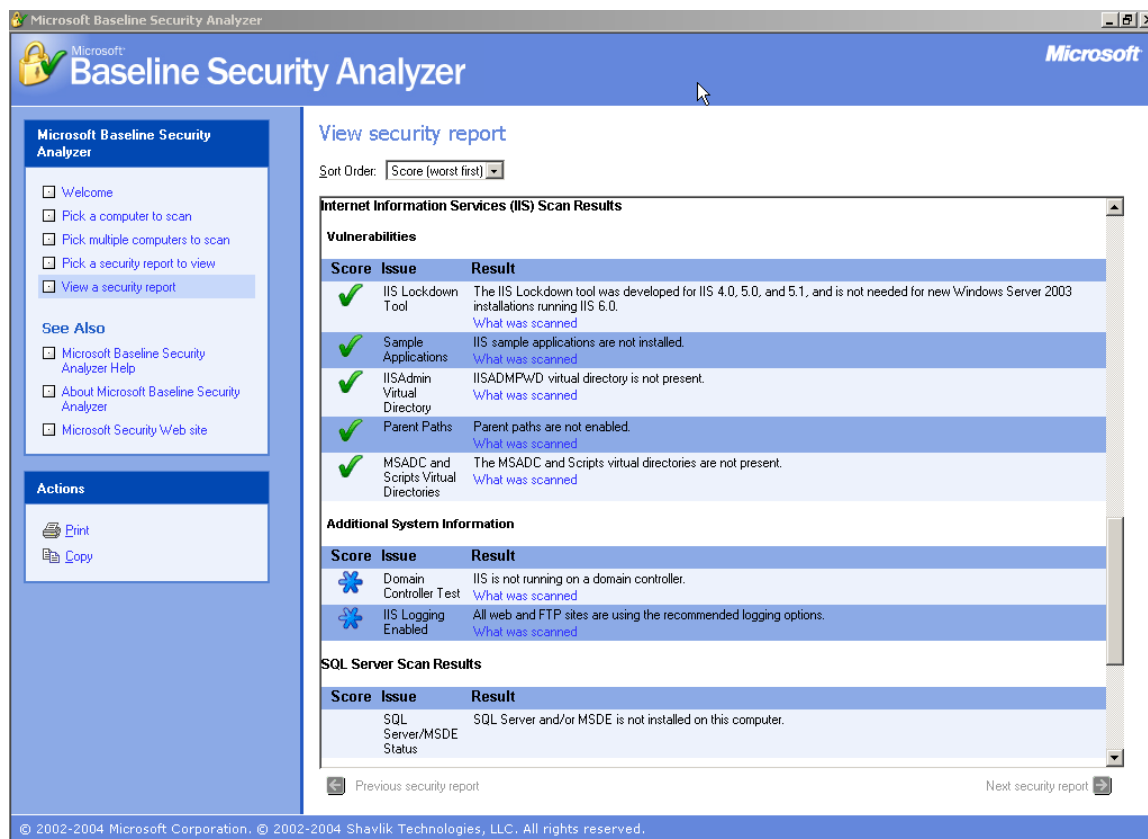
- 1) From your desktop or Start menu, run Microsoft Baseline Security Analyzer 1.2.1.



- 2) Choose Scan a computer. The following screen will appear. Make sure that your server name is in the computer name box. If not, choose it from the dropdown list. Then click Start Scan.



- 3) This will start the scanning process on your server. First, the program connects to Microsoft for any updates to the list of security patches and service packs for your operating system version. Then MBSA starts a security scan on your server. When the scan is complete, a screen similar to the following should appear. Notice that the IIS scan had very good results. The results on your server may vary, especially if necessary security patches have not been applied.



Step 5: Analysis

- 1) If there are other security warnings after your MBSA scan, click on the links underneath the scan results. They will show what was scanned, details of the scan, and how to correct any problems. If there are any missing updates, try to get the server as patched as possible.
- 2) Do you think that Microsoft did a better job with the default installation of IIS 6.0 in Windows 2003 Server than in previous versions? Research the IIS Lockdown Tool that is used with previous versions of IIS.
- 3) The default installation of IIS 6.0 on Windows 2003 server will not allow the “dot-dot” (..) vulnerability that existed with previous versions. Research this vulnerability.

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Research the IIS Lockdown Tool for earlier versions of IIS.

Try to attach to a lab partner's server using several different methods. Change the authentication methods, IP address restrictions, etc.

Appendix

These steps were performed using a default installation of Windows Server 2003 Enterprise Edition. Similar results will be obtained if using Standard Edition. All operating system updates and patches as of 8/27/2004 have been installed. Students should be able to attach to each other's servers, without the use of dedicated workstations.