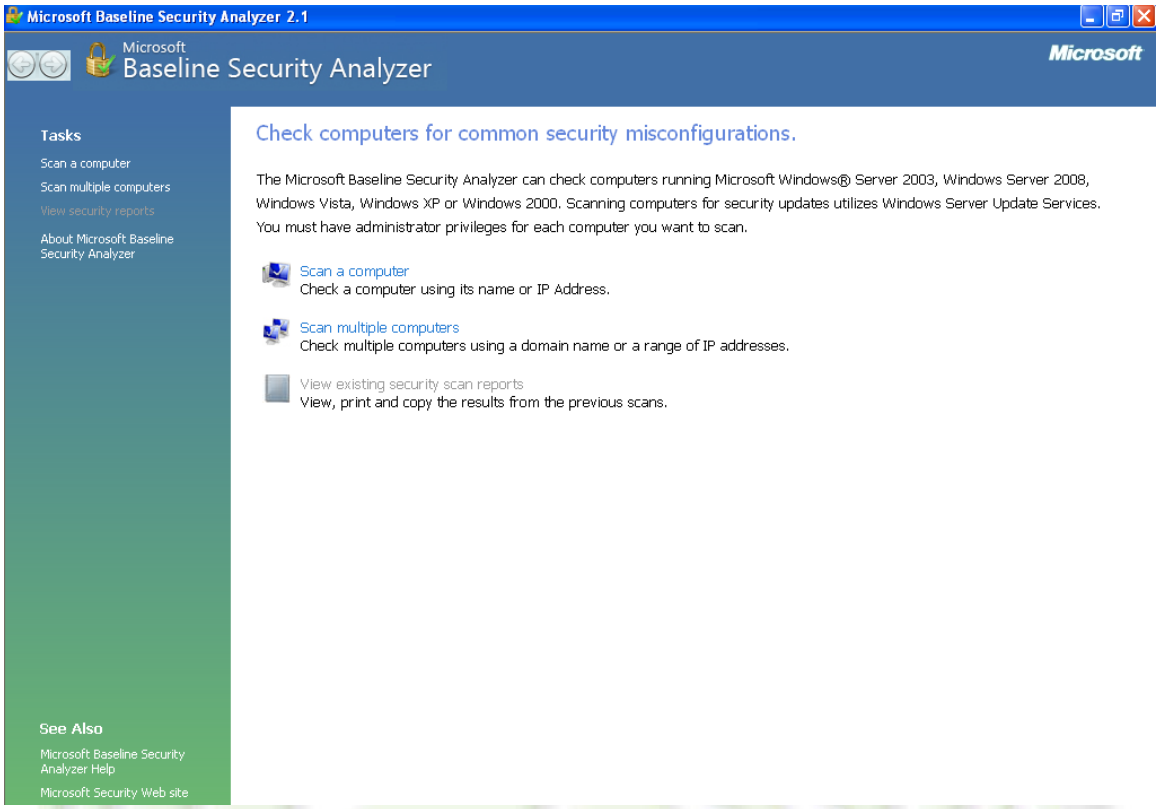
4.2.1

WINDOWS OS HARDENING

(Microsoft Baseline Security Analyzer)



JUNE 2008

Laboratory Overview

Objective

At the end of this lab students will be able to analyze a Windows operating system for weaknesses such as missing security patches, weak passwords, MS Office vulnerabilities and be able to correct these.

Information for Laboratory

A. Students will utilize the MS Baseline Security Analyzer program to scan the laboratory Windows XP computer.
B. Students will list the vulnerabilities and make recommendations to resolve the problems.
C. Students will fix some of the problems and run the MS Baseline Security Analyzer again to see if the problem is resolved.

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.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that there are some vulnerabilities on the Windows XP computers and that the MS Baseline Security Analyzer program is installed on the lab computers. The lab computers must have Internet connectivity.

Estimated Completion Time

30 Minutes

Security Analysis

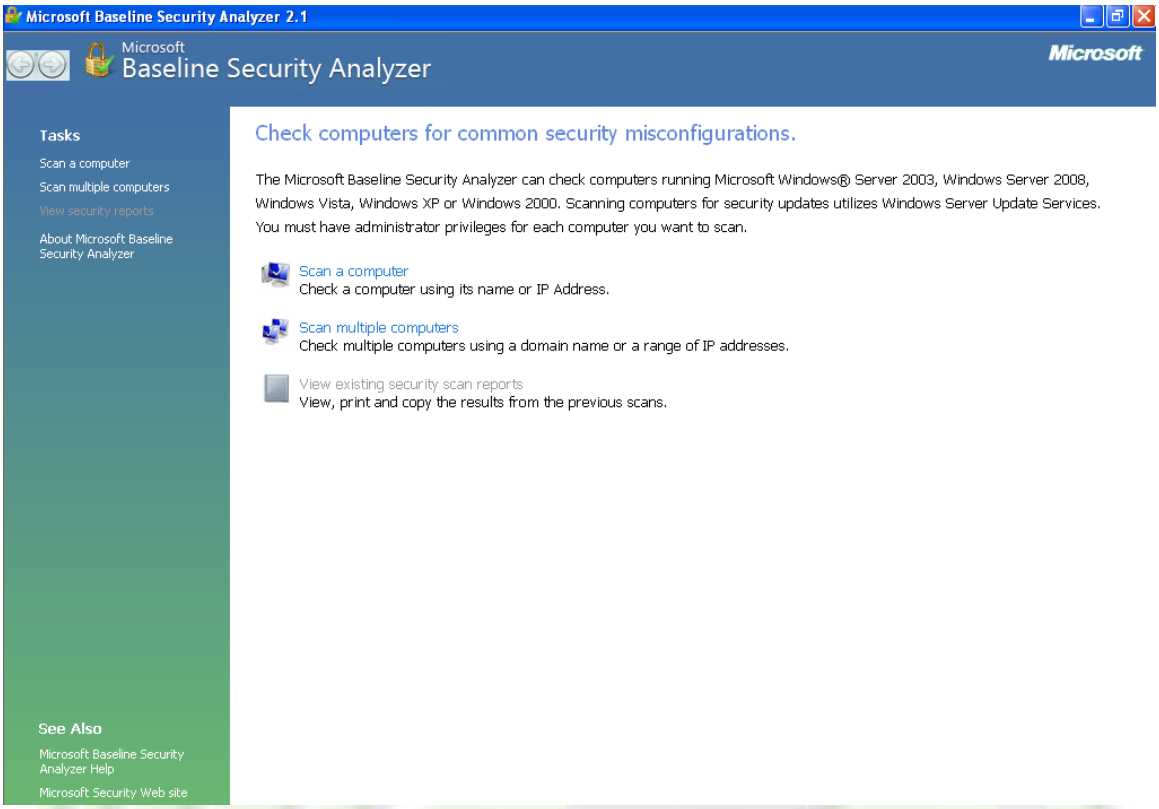
Performing a security analysis on desktop/server platforms helps administrators identify vulnerabilities on those platforms. Operating systems and certain applications with missing or out-of-date patches are vulnerable to attacks from a variety of sources including e-mail and DoS attacks.

Microsoft Baseline Security Analyzer

Using this tool can help a network administrator identify common security misconfigurations. Capabilities of the tool include examining Windows desktops and servers for common security best practices such as strong passwords, scanning servers running IIS and SQL Server for common security misconfigurations, and checking for misconfigured security zone settings in Microsoft Office and Internet Explorer. MBSA also scans for missing security updates, update rollups and service packs available from Microsoft By identifying these weaknesses, an administrator can develop a more comprehensive plan when installing the Windows operating system in order to harden it.

Step 1:

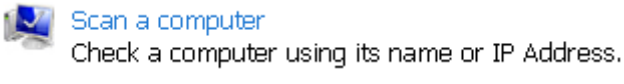
Go to **S**tart, **P**rograms, **M**icrosoft **B**aseline **S**ecurity **A**nalyzer**.** Your screen should be similar to this:



As you can see, you have three options to choose from. We are going to pick the first option, but let's discuss the other two. You can scan more than one computer at once with this tool. You can either scan by putting in a range of IP addresses or by domain name. If you put in the domain name, it will scan all the computers within that domain. Whichever option you choose, remember that you must have administrative rights to run these scans. The reports option will allow you to look at or print off results of a scan.

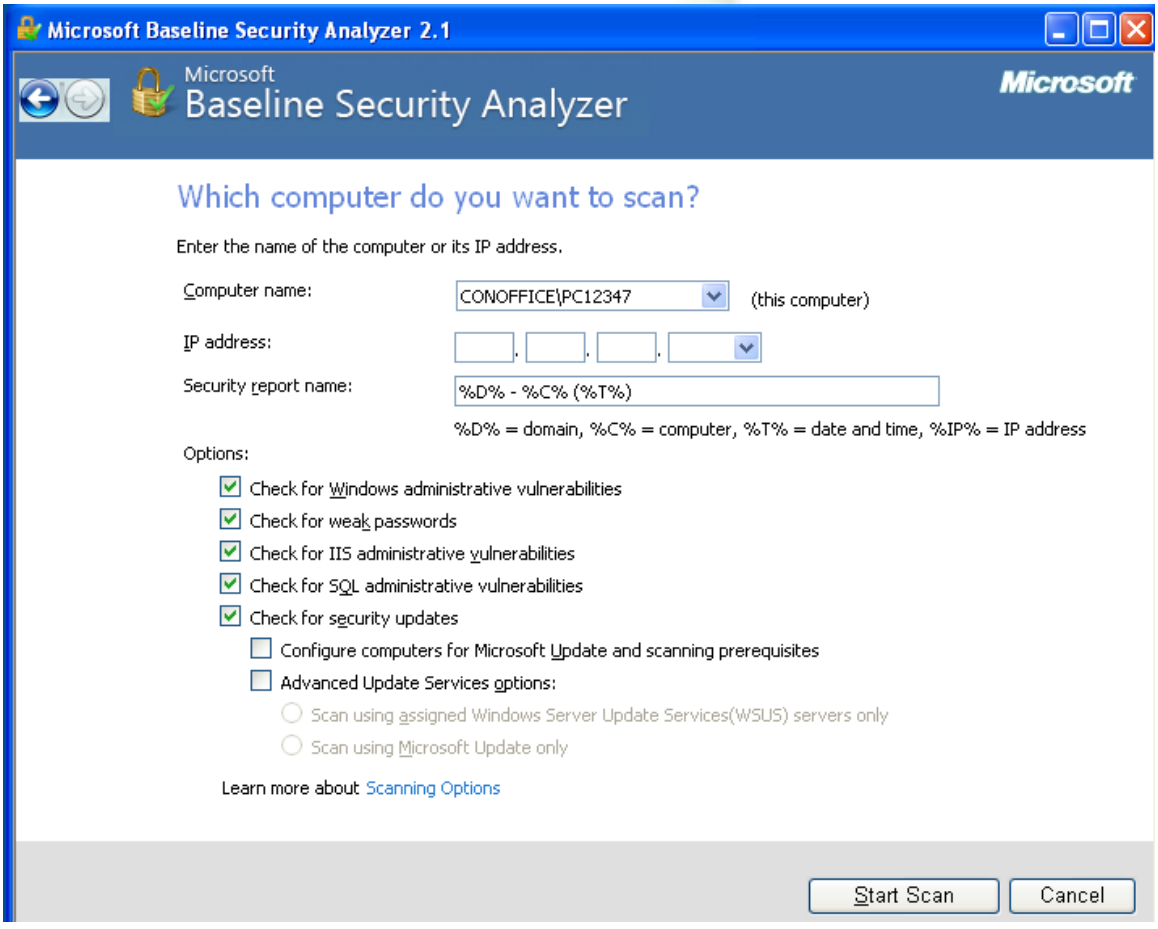
Step 2:

Click on the link titled

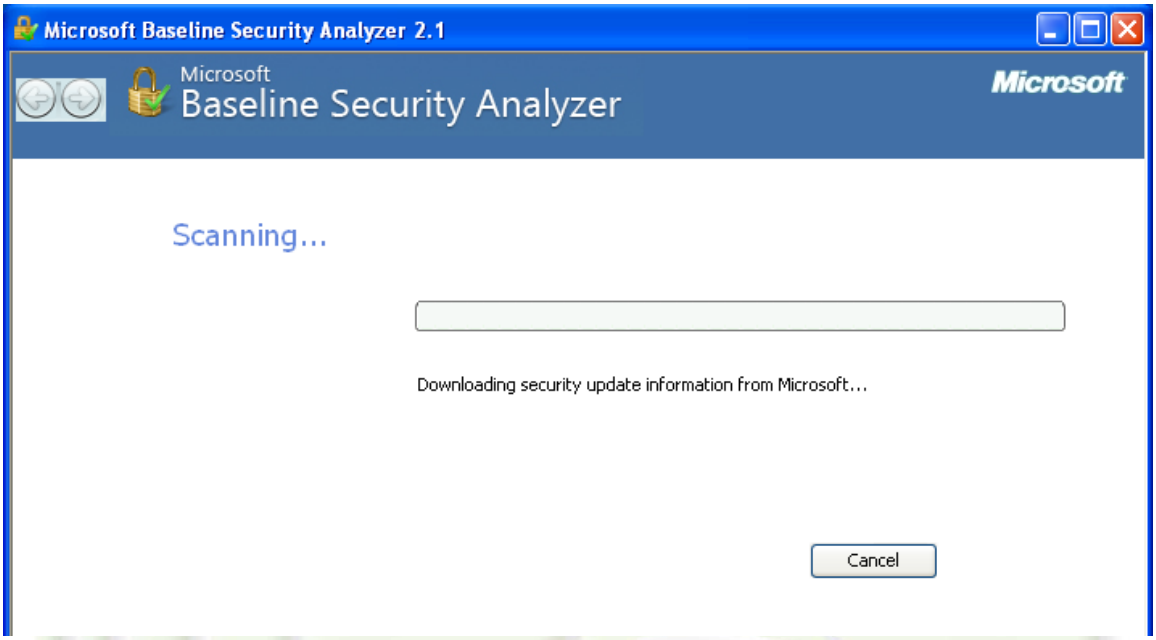


Step 3:

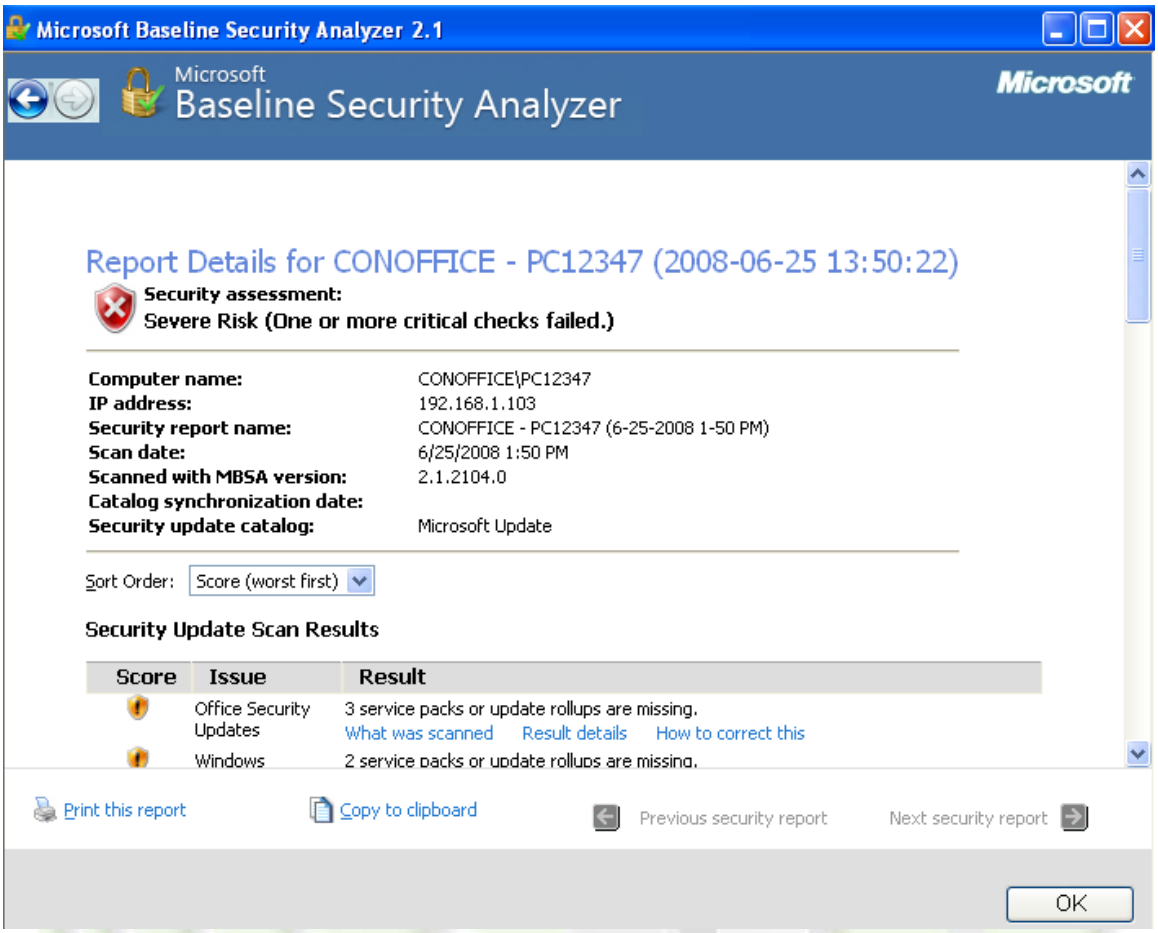
Your screen will look like the one shown below. Your computer name will be in the dialog box by default. You can also scan by its IP address. Look at the option check boxes shown below. By default, they are all checked. The Windows vulnerabilities option will check items such as guest account (enabled or disabled), check the local password and see if Automatic updates are being done. The security updates option will not only check for operating system security issues, but also application security issues such as Media Player and Office security issues. Use the default checked boxes and start your scan.



You will see a screen like this:

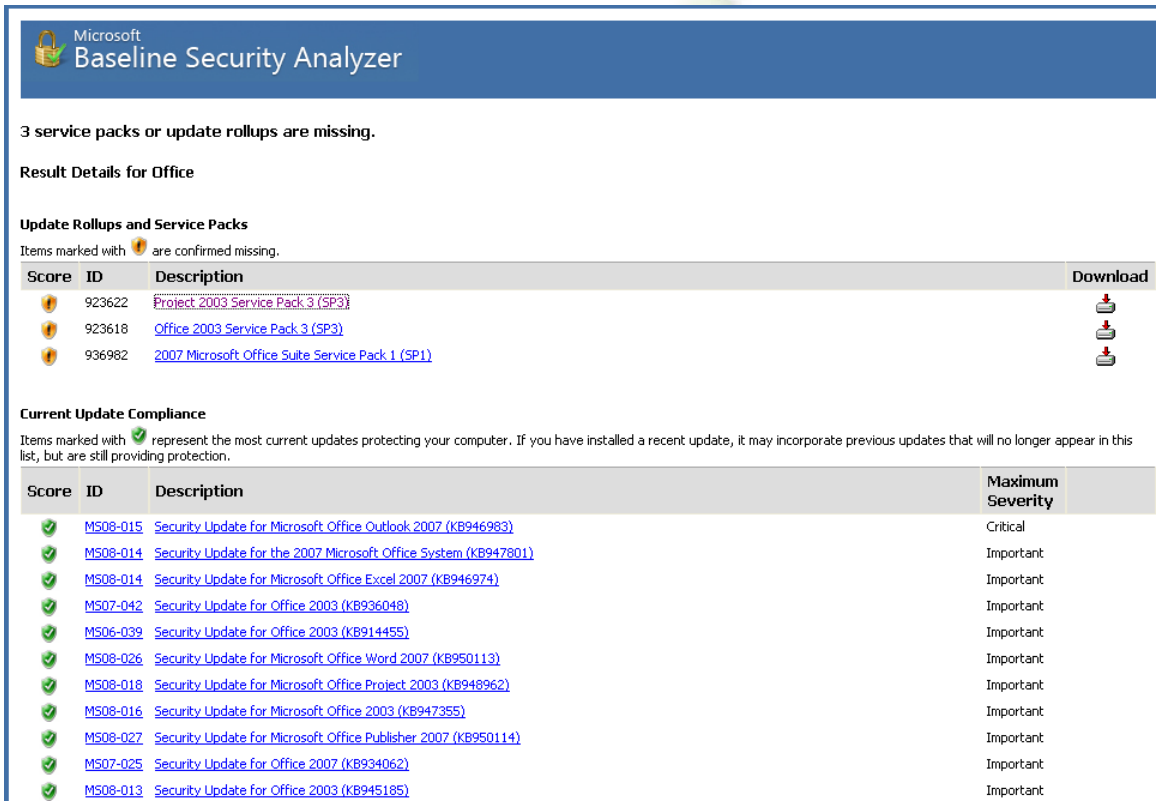


When the scan has finished you will see a screen similar to this:


Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Report Details for CONOFFICE - PC12347 (2008-06-25 13:50:22)
Security assessment:
Severe Risk (One or more critical checks failed.)
Computer name: CONOFFICE\PC12347
IP address: 192.168.1.103
Security report name: CONOFFICE - PC12347 (6-25-2008 1-50 PM)
Scan date: 6/25/2008 1:50 PM
Scanned with MBSA version: 2.1.2104.0
Catalog synchronization date:
Security update catalog: Microsoft Update
Sort Order: Score (worst first)
Security Update Scan Results
Score
Issue
Result
Office Security Updates
3 service packs or update rollups are missing.
What was scanned
Result details
How to correct this
Windows
2 service packs or update rollups are missing.
Print this report
Copy to clipboard
Previous security report
Next security report
OK

Step 4:

You now have a wealth of information at your fingertips, once your scan is completed. **Do a printscreen of it and save to a MS Word file.** Make sure you put your name within the document for your instructor. Again, you have a variety of options to choose from. If you click on the What was scanned option, it will bring up another screen telling you exactly what the analyzer checked. This is fairly generic information. A better option is to click on the Result Details. This will give you the items as well as links to what you need to update your computer. A sample screen shot is shown below:



Microsoft Baseline Security Analyzer

3 service packs or update rollups are missing.

Result Details for Office

Update Rollups and Service Packs

Items marked with are confirmed missing.

Score	ID	Description	Download
	923622	Project 2003 Service Pack 3 (SP3)	
	923618	Office 2003 Service Pack 3 (SP3)	
	936982	2007 Microsoft Office Suite Service Pack 1 (SP1)	

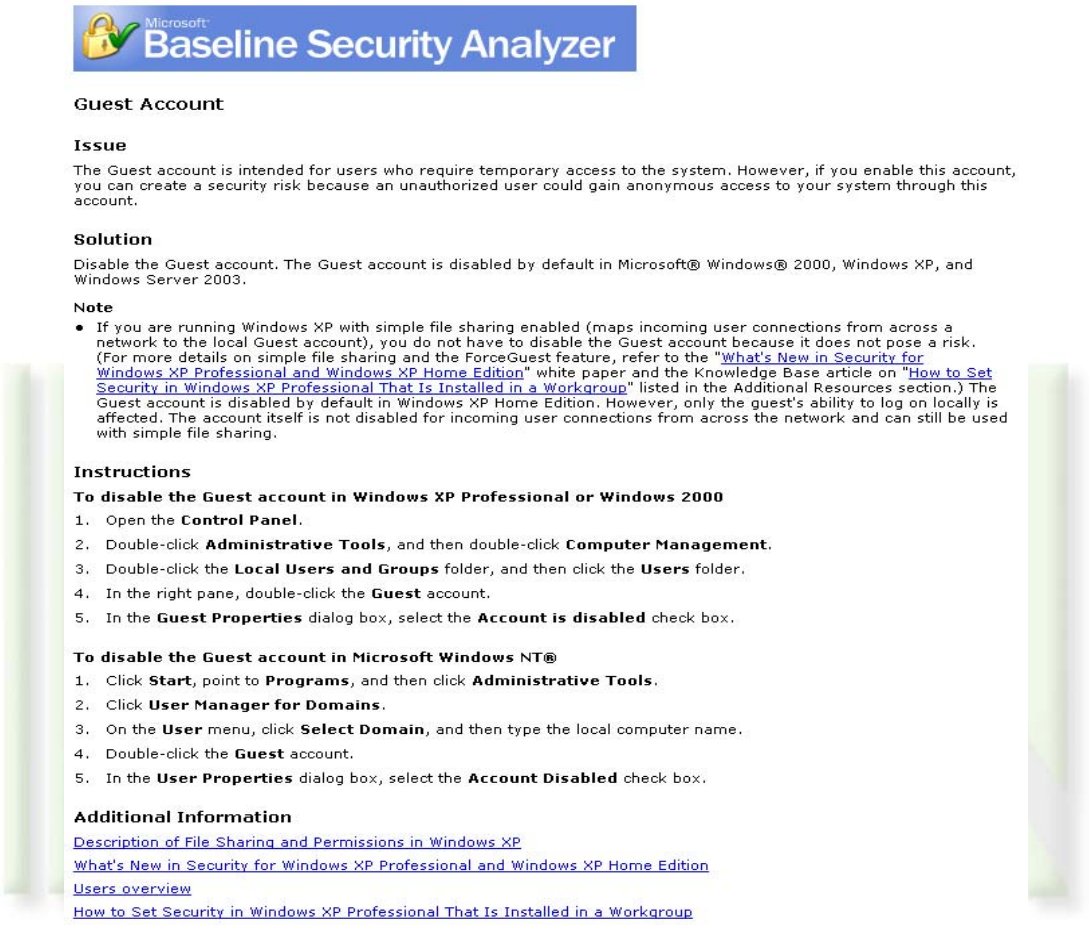
Current Update Compliance

Items marked with represent the most current updates protecting your computer. If you have installed a recent update, it may incorporate previous updates that will no longer appear in this list, but are still providing protection.

Score	ID	Description	Maximum Severity
	MS08-015	Security Update for Microsoft Office Outlook 2007 (KB946983)	Critical
	MS08-014	Security Update for the 2007 Microsoft Office System (KB947801)	Important
	MS08-014	Security Update for Microsoft Office Excel 2007 (KB946974)	Important
	MS07-042	Security Update for Office 2003 (KB936048)	Important
	MS06-039	Security Update for Office 2003 (KB914455)	Important
	MS08-026	Security Update for Microsoft Office Word 2007 (KB950113)	Important
	MS08-018	Security Update for Microsoft Office Project 2003 (KB948962)	Important
	MS08-016	Security Update for Microsoft Office 2003 (KB947355)	Important
	MS08-027	Security Update for Microsoft Office Publisher 2007 (KB950114)	Important
	MS07-025	Security Update for Office 2007 (KB934062)	Important
	MS08-013	Security Update for Office 2003 (KB945185)	Important

This gives you the severity level as well as the direct download links for the various products. Do a print screen of your Result Details and save in your Word document. Print off for your instructor.

If you go back to main page of MSBA, and click on the How to correct this link for an item, it will give the user step-by-step instructions on how to correct the problem. For example, let's say that the Guest account on this Windows XP computer is not disable. If you click on the How to correct this link, you would see the screen shown below.



Microsoft Baseline Security Analyzer

Guest Account

Issue

The Guest account is intended for users who require temporary access to the system. However, if you enable this account, you can create a security risk because an unauthorized user could gain anonymous access to your system through this account.

Solution

Disable the Guest account. The Guest account is disabled by default in Microsoft® Windows® 2000, Windows XP, and Windows Server 2003.

Note

- If you are running Windows XP with simple file sharing enabled (maps incoming user connections from across a network to the local Guest account), you do not have to disable the Guest account because it does not pose a risk. (For more details on simple file sharing and the ForceGuest feature, refer to the "What's New in Security for Windows XP Professional and Windows XP Home Edition" white paper and the Knowledge Base article on "How to Set Security in Windows XP Professional That Is Installed in a Workgroup" listed in the Additional Resources section.) The Guest account is disabled by default in Windows XP Home Edition. However, only the guest's ability to log on locally is affected. The account itself is not disabled for incoming user connections from across the network and can still be used with simple file sharing.

Instructions

To disable the Guest account in Windows XP Professional or Windows 2000

1. Open the **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Computer Management**.
3. Double-click the **Local Users and Groups** folder, and then click the **Users** folder.
4. In the right pane, double-click the **Guest** account.
5. In the **Guest Properties** dialog box, select the **Account is disabled** check box.

To disable the Guest account in Microsoft Windows NT®

1. Click **Start**, point to **Programs**, and then click **Administrative Tools**.
2. Click **User Manager for Domains**.
3. On the **User** menu, click **Select Domain**, and then type the local computer name.
4. Double-click the **Guest** account.
5. In the **User Properties** dialog box, select the **Account Disabled** check box.

Additional Information

Description of File Sharing and Permissions in Windows XP
What's New in Security for Windows XP Professional and Windows XP Home Edition
Users overview
How to Set Security in Windows XP Professional That Is Installed in a Workgroup

As you can see from the screen shot shown on the previous page, it is extremely helpful, giving you the step-by-step instructions necessary to correct the problem.

Analysis

1) Review your notes and answer the following questions.
2) What operating system items listed on the computer would you view as most vulnerable to exploitation?

3) What application software items listed on the computer would you view as most vulnerable to exploitation?
4) Based on the information gathered, what items would you correct first?
5) After working with this utility, do you see any potential items that it missed?

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

1) Research software with similar functionality
2) After fixing some of the items, scan the computer with another security scanner such as GFiLANguard (www.gfi.com) to see what vulnerabilities it found.

Appendix:

This lab was developed using MS Baseline Security Analyzer version 2.1 (5/22/08), which can be obtained from:
http://www.microsoft.com/downloads/details.aspx?FamilyID=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en#filelist

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).