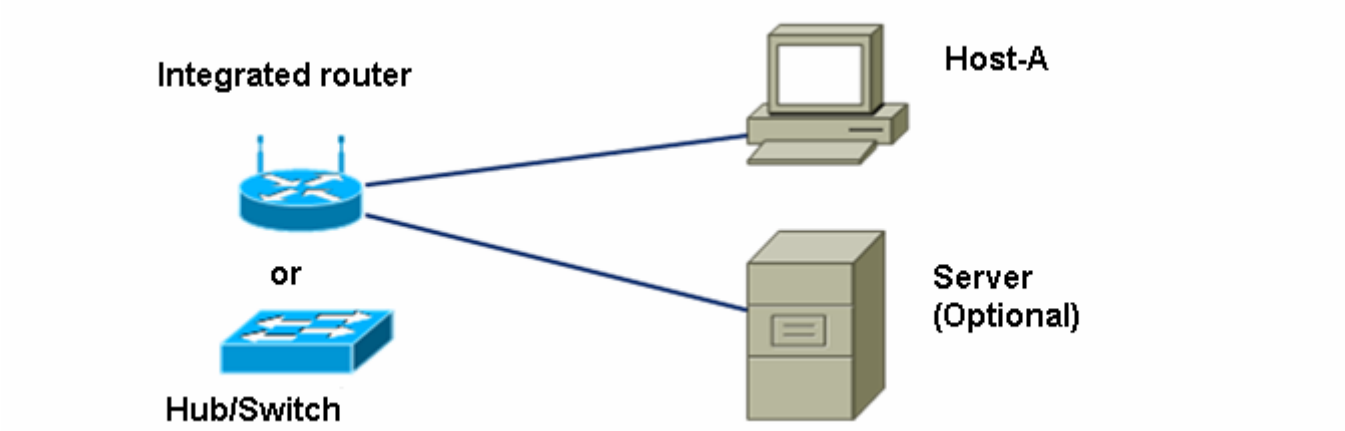
Lab 8.4.3 Performing a Vulnerability Analysis

CAUTION: This lab may violate legal and organizational security policies. The security analyzer downloaded in this lab should only be used for instructional purposes in a lab environment. Before using a security analyzer on a live network, check with your instructor and network administration staff regarding internal policies concerning the use of these tools.



Objectives

- Download and install security analyzer software.
- Test a host to determine potential security vulnerabilities.

Background / Preparation

Security analyzers are valuable tools used by network administrators and auditors to identify network and host vulnerabilities. There are many vulnerability analysis tools, also known as security scanners, available to test host and network security. In this lab, you will download and install the Microsoft Baseline Security Analyzer (MBSA). MBSA is designed to identify potential security issues related specifically to Microsoft operating systems, updates, and applications. It also identifies unnecessary services that may be running, as well as any open ports.

MBSA runs on Windows Server and Windows XP systems and scans for common security misconfigurations and missing security updates for the operating system as well as most versions of Internet Information Server (IIS), SQL Server, Internet Explorer (IE), and Office products. MBSA offers specific recommendations to correct potential problems.

This lab can be done individually or in teams of two.

The following resources are required:

- Computer running Windows XP Professional to act as the test station.
- High-speed Internet connection for downloading MBSA (unless pre-installed).
- Computer must be attached to the integrated router switch or a standalone hub or switch.
- Optionally, you can have a server running a combination of DHCP, HTTP, FTP, and Telnet (preconfigured).

Step 1: Download and install MBSA

a. Open a browser and go to the MBSA web page at: http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx

b. What is the latest version of MBSA available? _____

c. What are some of the features MBSA provides? _____

_____

d. Scroll down the page and select the desired language to begin the download process.

e. Click **Continue** to validate the copy of Microsoft Windows you are running.

f. Click **Download Files below** and select the file you want to download. (The English setup file is MBSASetup-EN.msi). Click the **Download** button on the right of this file. How many megabytes is the file to download? _____

g. When the **File Download – Security Warning** dialog box displays, click **Save** and download the file to a specified folder or the desktop. You can also run it from the download website.

h. Once the download is complete, make sure all other applications are closed. Double-click the downloaded file. Click **Run** to start the Setup program, and then click **Run** if you are prompted with a Security Warning. Click **Next** on the MBSA Setup screen.

i. Select the radio button to accept the license agreement and click **Next**. Accept the defaults as the install progresses, and then click **Finish**. Click **OK** on the final MBSA Setup screen, and close the folder to return to the Windows desktop.

Step 2: Build the network and configure the hosts

a. Connect the host computer(s) to the integrated router, a hub, or a switch as shown in the topology diagram. Host-A is the test station where MBSA will be installed. The server is optional.

b. Set the IP configuration for the host(s) using Windows XP Network Connections and TCP/IP properties. If the host is connected to the integrated router, configure it as a DHCP client; otherwise go to Step 2c.

c. If the host is connected to a hub or switch and a DHCP server is not available, configure it manually by assigning a static IP address.

Which IP address and subnet mask does Host-A and the server (optional) have?

_____

Step 3: Run MBSA on a host

a. Double-click the desktop icon for MBSA or run it from **Start > All Programs**.

When the main screen displays, which options are available? _____

_____

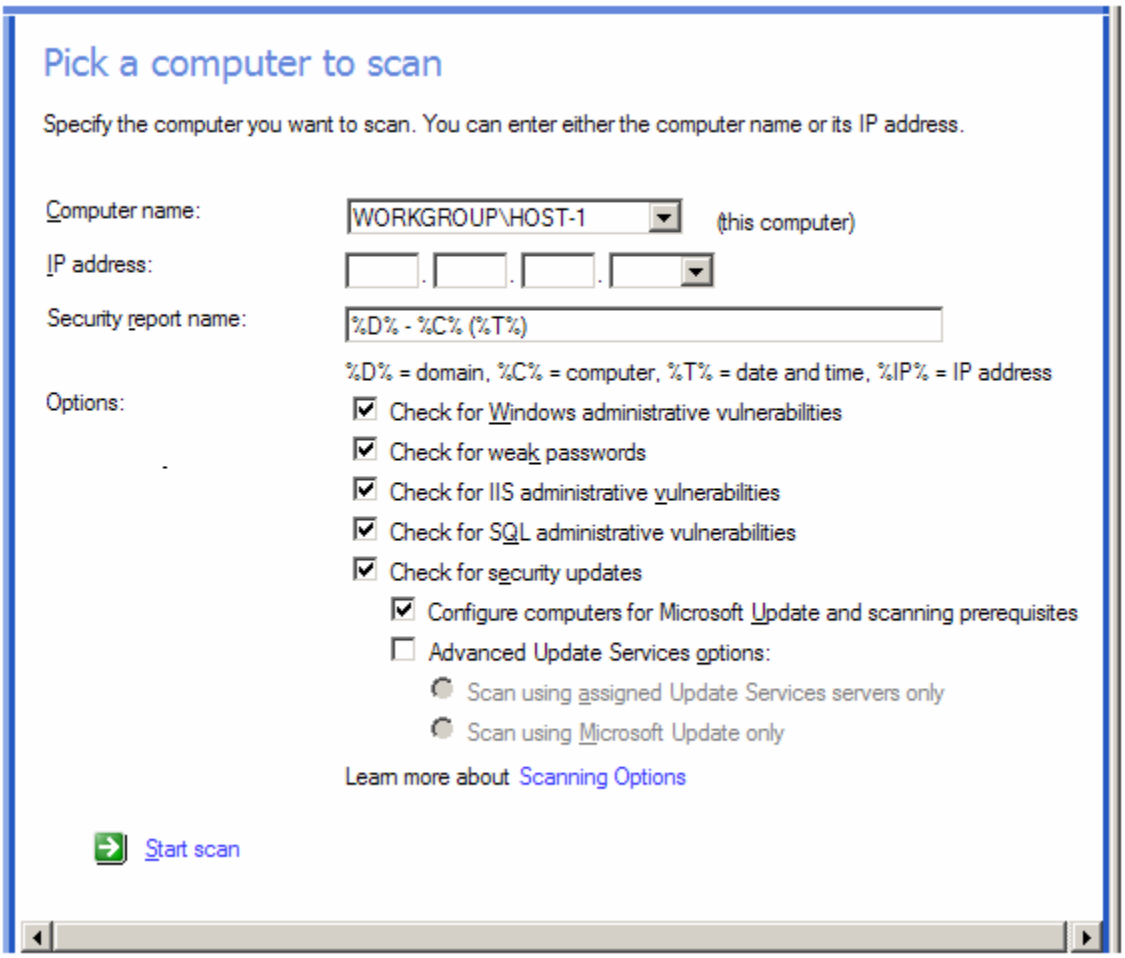
Step 4: Select a computer to scan

a. On the left side of the screen, click **Pick a computer to scan**. The computer shown as the default is the one on which MBSA is installed.

b. What are the two ways to specify a computer to be scanned? _____

_____

c. Accept the default computer to be scanned. De-select Check for IIS and SQL administrative vulnerabilities, since these services are not likely to be installed on the computer being scanned. Click **Start Scan**.



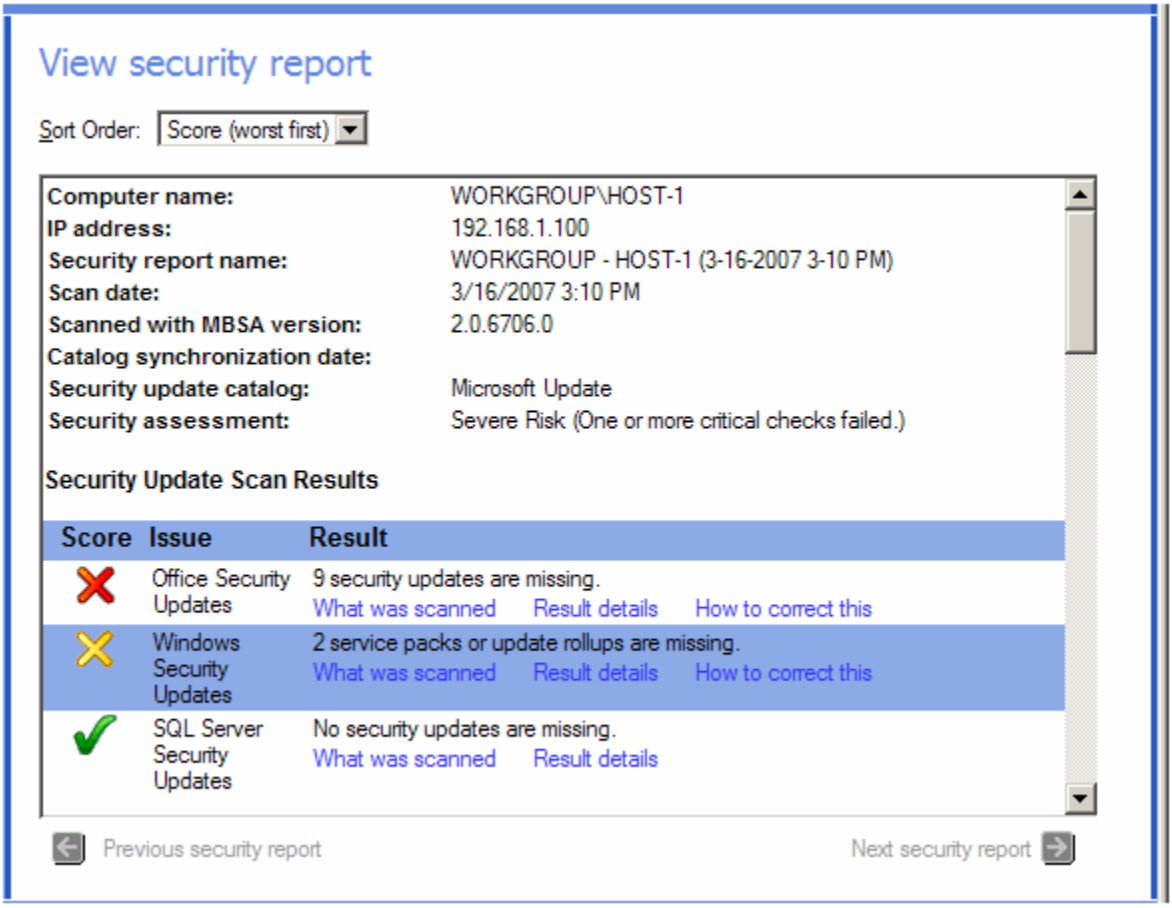
Step 5: View security update scan results

a. View the security report. What are the results of the security update scan? _____

_____

b. If there are any red or yellow Xs, click **How to correct this**. Which solution is recommended?

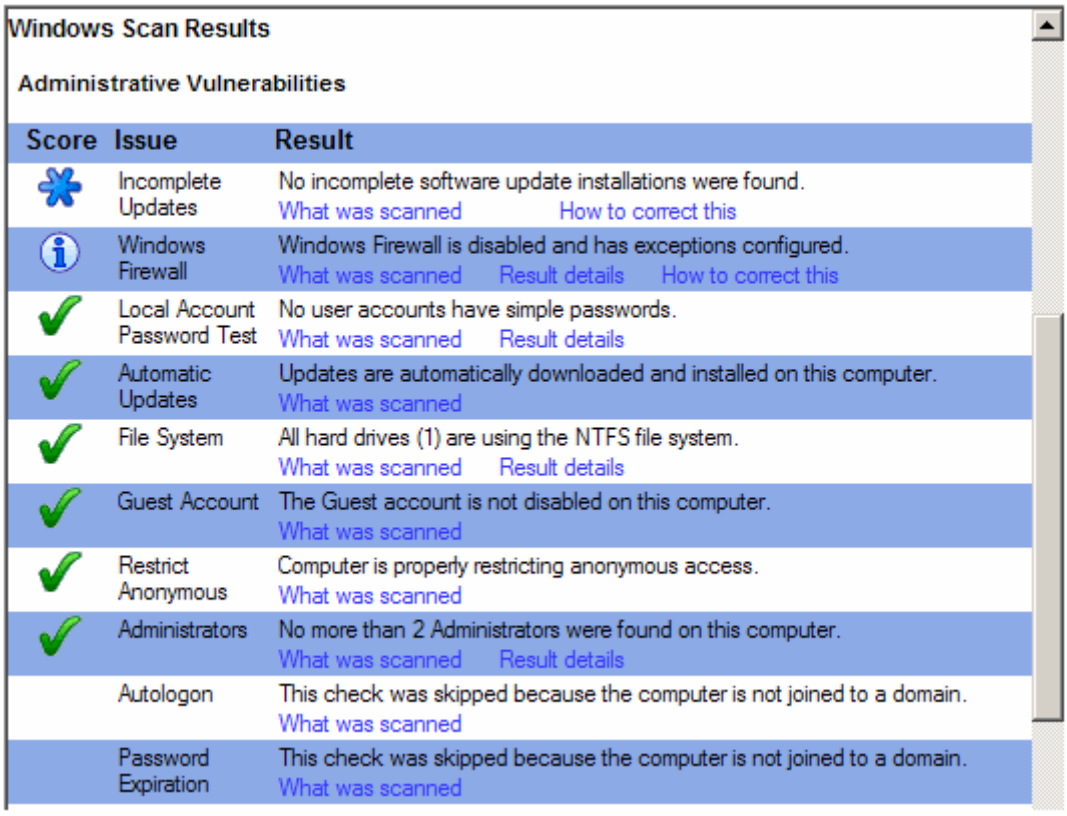
_____



Step 6: View Windows scan results in the security report

a. Scroll down to view the second section of the report that shows **Windows Scan Results**. Were there any administrative vulnerabilities identified?

_____



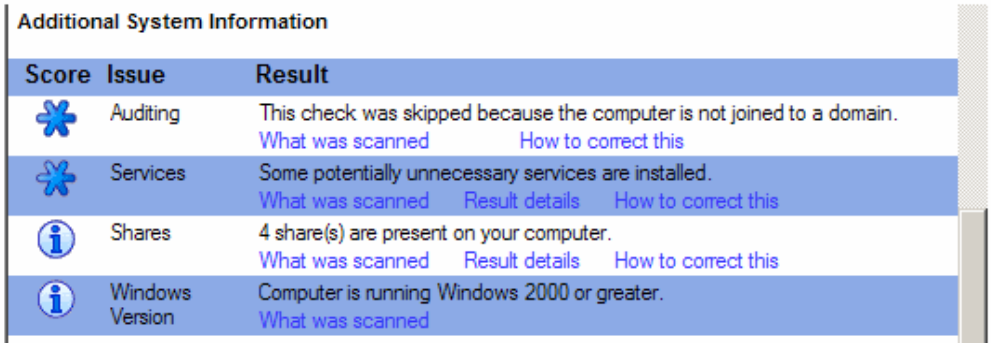
Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Guest Account	The Guest account is not disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Autologon	This check was skipped because the computer is not joined to a domain. What was scanned
	Password Expiration	This check was skipped because the computer is not joined to a domain. What was scanned

b. On the **Additional System Information** section of the screen (below), in the **Issue** column for **Services**, click **What was scanned,** and click **Result details** under the **Result** column to get a description of the check that was run. What did you find? When finished, close both popup windows to return to the security report.

_____



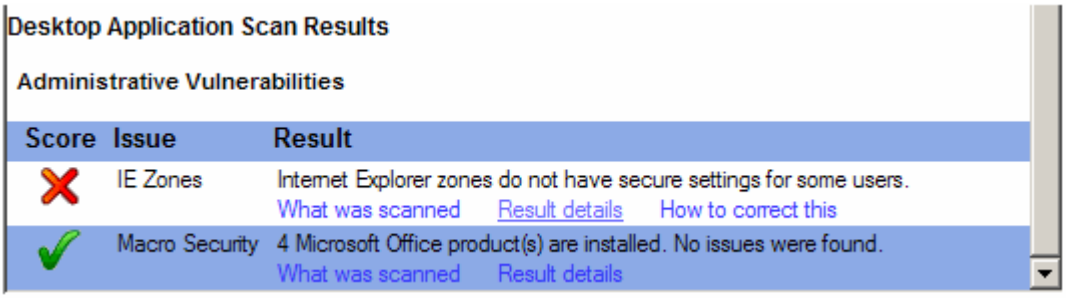
Additional System Information

Score	Issue	Result
	Auditing	This check was skipped because the computer is not joined to a domain. What was scanned How to correct this
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	4 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Windows 2000 or greater. What was scanned

Step 7: View Desktop Application Scan Results in the Security report

a. Scroll down to view the last section of the report that shows **Desktop Applications Scan Results**. Were there any administrative vulnerabilities identified?

_____



b. How many Microsoft Office products are installed? _____

c. Were there any security issues with **Macro Security** for any of them?

_____

Step 8: Scan a server, if available

a. If a server with various services is available, click Pick a computer to scan from the main MBSA screen and enter the IP address of the server, and then click Start Scan. Which security vulnerabilities were identified?

_____

_____

_____

b. Were there any potentially unnecessary services installed? Which port numbers were they on?

_____

_____

Step 9: Uninstall MBSA using Control Panel Add/Remove Programs

a. This step is optional, depending on whether the host will be automatically restored later by a network process.

b. To uninstall MBSA, click **Start > Control Panel > Add/Remove Programs**. Locate the MBSA application and uninstall it. It should be listed as Microsoft Baseline Security Analyzer 2.0.1. Click **Remove**, and then click **Yes** to confirm removal of the MBSA application. When finished, close all windows to return to the desktop.

Step 10: Reflection

a. The MBSA tool is designed to identify vulnerabilities for Windows-based computers. Search the Internet for other tools that might exist. List some of the tools discovered.

_____

b. Which tools might there be for non-Windows computers? Search the Internet for other tools that might exist and list some of them here.

_____

c. Which other steps could you take to help secure a computer against Internet attacks?

_____