Lab LC19: Performing Vulnerability Assessment Scans with Systems Management Server 2003 R2

Objectives

After completing this lab, you will be able to:

- Install the SMS 2003 R2 Scan Tool for Vulnerability Assessment.
- Perform a vulnerability assessment scan.
- Use SMS Reporting to report vulnerability status.
- Repair specific vulnerabilities.
- Verify vulnerability resolution.

Before You Begin

In this lab, you need an SMS 2003 SP2 primary site server and a SMS 2003 SP2 Advanced Client. These could be the same computer. You can have additional SMS 2003 SP2 Advanced Clients if you want to scan for and deploy updates to multiple client platforms.

The VPCs for this lab include a Windows Server 2003 site server (SMS 2003 R2 Site Server VPC), a Windows Server 2003 member computer (SMS 2003 R2 Member Computer VPC), a Windows XP Professional client (SMS 2003 R2 Windows XP VPC), and a Windows 2000 S4 Professional client (SMS 2003 R2 Windows 2000 VPC). The lab is written for the SMS site server and the Windows XP Professional Client computer. Ensure that at least those two images are started. You can also use the additional clients if you wish.

Estimated time to complete this lab: 75 minutes
Exercise 0
Preparing the Virtual Computer Clients for the Lab

In this exercise, you will update the collection membership of the All Systems collection. When you do, you will see the SMSClient computer appear twice in the membership list. This is due to Virtual PC 2004 virtualizing the SMBios serial number of the host computer, which SMS detects as being different than the original SMBios serial number. Because of this, SMS generates a new GUID for the client, which causes a new record to be generated.

Note Complete this procedure from the primary site server computer only.

To update the collection membership
1. Log on as administrator with a password of password.
2. On the Start menu, click SMS Administrator Console.
   The SMS Administrator Console window appears.
3. In the console tree, expand Site Database, expand Collections, and then click All Systems.
   The members of the All Systems collection appear in the details pane.
   Notice that there are multiple members, including the site server computer (SMSServer) the Windows XP Professional client computer (SMSClient), the Windows 2000 Professional client (SMSClient2) and the Windows Server 2003 Member server (SMSMember).
4. On the Action menu, point to All Tasks, and then click Update Collection Membership.
   The All Systems message box appears prompting to update subcollection membership.
5. Click OK, and then on the Action menu, click Refresh.
   The collection membership is updated, and the current membership of the All Systems collection is displayed. Notice that the SMSClient computer is now displayed twice. Notice also that one of the instances is listed as being Obsolete and inactive. This is the old reference of the client.
6. In the details pane, click the obsolete record for the SMSClient computer, and then on the Action menu, click Delete.
   AConfirm Delete message box appears prompting to delete the record.
7. Click Yes.
   The collection membership is updated, and the current membership of the All Systems collection is displayed. Notice that the SMSClient computer is now displayed only once and it is an Active record (not Obsolete).
8. Delete any other Obsolete records from the All Systems collection.
   You have now prepared your images for the lab and may proceed to Exercise 1.
Exercise 1
Installing the SMS 2003 R2 Scan Tool for Vulnerability Assessment

In this exercise, you will install the SMS 2003 R2 Scan Tool for Vulnerability Assessment. This is one of the tools in the SMS 2003 R2 bundle. You will begin by extracting SMS 2003 R2 from the download bundle.

Note  Complete this exercise from the primary site server computer.

짐 To install SMS 2003 R2
1. Start C:\SMS2003_R2_Beta.exe.
   The WinZip Self-Extractor window appears. Notice that the default folder to extract files to is SMS2003_R2_Beta.
2. Click Unzip.
   The files are extracted from the download bundle to the C:\SMS2003_R2_Beta folder. When complete, the WinZip Self-Extractor message box appears indicating that 12 files were extracted successfully.
3. Click OK, and then click Close.
4. Start C:\SMS2003_R2_Beta\Autorun.exe.
   The Systems Management Server 2003 R2 window appears displaying available options.
5. Click Scan Tool for Vulnerability Assessment.
   The Microsoft SMS 2003 Vulnerability Assessment Tool Setup window appears.
6. Click Next.
   The Microsoft SMS 2003 Vulnerability Assessment Tool Setup License agreement dialog box appears displaying the end user license agreement.
7. Read the end user license agreement, click I accept the license agreement, and then click Next.
   The Microsoft SMS 2003 Vulnerability Assessment Tool Setup Destination Folder dialog box appears prompting for the location to install the vulnerability assessment scan tool.
8. Click Next to accept the default path of C:\Program Files\Microsoft Vulnerability Assessment Tool.
   The Microsoft SMS 2003 Vulnerability Assessment Tool Setup Choose Vulnerabilities to Check dialog box appears prompting for the category of vulnerabilities to scan for. Notice that there are checks for Windows, passwords, Internet Information Server, and SQL Server.
9. Verify that all four default options are selected, and then click Next.
   The Microsoft SMS 2003 Vulnerability Assessment Tool Setup Distribution Setting dialog box appears prompting to automatically create the SMS collections, packages, and advertisements necessary for automated scanning of clients. Notice the default name to use for the creation of SMS objects.
10. In the **Enter the computer name of an SMS Advanced Client to use as the test computer** box, type **SMSServer** and then click **Next**.

   The **Microsoft SMS 2003 Vulnerability Assessment Tool Setup Distribution Settings for Microsoft MBSA Scan Engine** dialog box appears prompting to create SMS objects to deploy the MBSA 2.0 scan tool, which is required for the SMS Scan Tool for Vulnerability Assessment. Notice that by default SMS will automatically distribute the agent and use the name MBSA 2.0 for the SMS objects created. Also notice that this program must be deployed prior to a vulnerability assessment scan, and will be done so as a dependent program for the vulnerability assessment scan.

11. Click **Next** to accept the default values.

   The **Microsoft SMS 2003 Vulnerability Assessment Tool Setup Installation** dialog box appears indicating the installation is ready to complete.

12. Click **Next**.

   The Scan Tool for Vulnerability Assessment is installed. This process will take a few minutes to complete. When complete, a **Microsoft SMS 2003 Vulnerability Assessment Tool Setup Complete** dialog box appears indicating the installation was successfully completed.

13. Click **Finish**.

   The VAST_SP2 window appears displaying the product documentation for the Scan Tool for Vulnerability Assessment. You can keep this open for reference while completing this lab as necessary.


In the following procedure, you will view the additions to the SMS site as a result of the Scan Tool for Vulnerability Assessment installation.

---

**Note**  Complete this procedure from the primary site server only.

---

**To verify Scan Tool for Vulnerability Assessment installation**

1. If not already running, on the **Start** menu, point to **All Programs**, point to **Systems Management Server**, and then click **SMS Administrator Console**.

   The SMS Administrator Console window appears.

2. In the console tree, expand **Site Database**, and then click **Collections**.

   The list of collections appears in the details pane.

3. What collections were created as a result of installing the Scan Tool for Vulnerability Assessment?

   **Vulnerability Assessment Tool (default) and Vulnerability Assessment Tool (pre-production)**
4. In the console tree, expand Collections, and then click Vulnerability Assessment Tool (default).

The list of collection members appears in the details pane. Notice by default this includes a single Advanced Client computer that you designated during installation of the Scan Tool for Vulnerability Assessment. This collection is the production collection used to scan for vulnerabilities in your enterprise.

5. On the Action menu, click Properties.

The Vulnerability Assessment Tool (default) Collection Properties dialog box appears displaying the general collection properties.

6. Click the Membership Rules tab.

The Vulnerability Assessment Tool (default) Collection Properties dialog box appears displaying the collection membership rule.

7. Under Rule, click Collection Query, and then click Properties.

The Query Rule Properties dialog box appears displaying the collection query properties. Notice that by default the collection is limited to your test computer (through the pre-production collection) until you are ready for full production deployment. The query looks for Advanced Client computers that are running supported SMS 2003 SP2 operating system platforms.

8. To scan all supported SMS 2003 SP2 Advanced Clients, click Not collection limited, and then click OK.

The Vulnerability Assessment Tool (default) Collection Properties dialog box appears displaying the collection membership rule.

9. Click OK.

The list of collections appears.

10. Refresh the membership list for the Vulnerability Assessment Tool (default) collection.

The list of collection members appears in the details pane. Notice this now includes all Advanced Client computers running Windows 2000 SP4 and later.

11. In the console tree, click Vulnerability Assessment Tool (pre-production).

The list of collection members appears in the details pane. Notice that by default this includes a single Advanced Client computer that you designated during the installation of the Scan Tool for Vulnerability Assessment. This collection is the collection used to test the vulnerability scans in your enterprise.


The Vulnerability Assessment Tool (pre-production) Collection Properties dialog box appears displaying the general collection properties.

13. Click the Membership Rules tab.

The Vulnerability Assessment Tool (pre-production) Collection Properties dialog box appears displaying the collection membership rule. Notice that by default, the test computer has been added by a direct membership rule for the client’s resource ID to limit the test environment.

14. Click Cancel.

The list of collections appears.
15. In the console tree, click **Packages**.
   The list of packages appears in the details pane.

16. What packages were created as a result of installing the Vulnerability Assessment Tool?
   **Vulnerability Assessment Tool and MBSA 2.0**

17. In the console tree, expand **Packages**, and then expand **Vulnerability Assessment Tool**.

18. Under **Vulnerability Assessment Tool**, click **Programs**.
   The list of programs appears in the details pane.

19. What programs were created as a result of installing the Scan Tool for Vulnerability Assessment?
   **Vulnerability Assessment (regular) and Vulnerability Assessment (expedited)**

20. In the details pane, click **Vulnerability Assessment (regular)**, and then on the **Action** menu, click **Properties**.
   The **Vulnerability Assessment (regular) Program Properties** dialog box appears displaying the general program properties. Notice that the command line is VulnerabilityAssessment.exe. Also notice that the Run mode is set to “Hidden”.

21. Click the **Advanced** tab.
   The **Vulnerability Assessment (regular) Program Properties** dialog box appears displaying the advanced properties for the program. Notice that the Vulnerability Assessment (regular) program requires that the MBSA Install Silently (without shortcuts) program from the MBSA 2.0 package is run before the scan is run. This process will install the MBSA 2.0 scan engine on the client when first run, which is a requirement for the Scan Tool for Vulnerability Assessment.

22. Click **Cancel**.
   The list of programs appears.

23. In the details pane, click **Vulnerability Assessment (expedited)**, and then on the **Action** menu, click **Properties**.
   The **Vulnerability Assessment (expedited) Program Properties** dialog box appears displaying the general program properties. Notice that the command line is VulnerabilityAssessment.exe /kick. The “/kick” parameter forces an immediate hardware inventory cycle to occur after the vulnerability assessment scan completes. Also notice that the Run mode is set to “Hidden”.
24. Click the Advanced tab.

The Vulnerability Assessment (expedited) Program Properties dialog box appears displaying the advanced properties for the program. Notice that the Vulnerability Assessment (expedited) program requires that the MBSA Install Silently (without shortcuts) program from the MBSA 2.0 package is run before the scan is run. This process will install the MBSA 2.0 scan engine on the client when first run, which is a requirement for the Scan Tool for Vulnerability Assessment.

25. Click Cancel.

The list of programs appears.

26. In the console tree, expand Packages, and then expand MBSA 2.0.

27. Under MBSA 2.0, click Programs.

The list of programs appears in the details pane.

28. What programs were created as a result of installing the Scan Tool for Vulnerability Assessment?

MBSA Install Silently, MBSA Install Silently (without shortcuts) and MBSA Uninstall Silently

29. In the details pane, click MBSA Install Silently, and then on the Action menu, click Properties.

The MBSA Install Silently Program Properties dialog box appears displaying the general program properties. Notice that the command line is msiexec.exe /m mbsa.mif /I mbsasetup-en.msi /qn. The “/m mbsa.mif” parameter causes a status MIF file to be created to be used to identify status of the installation.

Also notice that the Run mode is set to “Hidden”.

30. Click Cancel.

The list of programs appears.

31. In the details pane, click MBSA Install Silently (without shortcuts), and then on the Action menu, click Properties.

The MBSA Install Silently (without shortcuts) Program Properties dialog box appears displaying the general program properties. Notice that the command line is msiexec.exe /I mbsasetup-en.msi /n mbsa.mif TRANSFORMS=MBSA-SHORTCUT.mst /qn. The “/n mbsa.mif” parameter causes a status MIF file to be created to be used to identify status of the installation. The “Transforms” parameter uses a custom transform to modify the default installation, in this case to not install any shortcuts for the MBSA 2.0 engine.

Also notice that the Run mode is set to “Hidden”.

32. Click Cancel.

The list of programs appears.
33. In the console tree, click **Advertisements**.

The list of advertisements appears in the details pane.

34. What advertisement was created as a result of installing the Scan Tool for Vulnerability Assessment?

**Vulnerability Assessment Tool**

35. In the details pane, click **Vulnerability Assessment Tool**, and then on the **Action** menu, click **Properties**.

The **Vulnerability Assessment Tool Advertisement Properties** dialog box appears displaying the general advertisement properties. Notice that the advertisement is targeting the Vulnerability Assessment (regular) program to the Vulnerability Assessment Tool collection.

36. How often will the members of the collection perform a scan for vulnerabilities?

**Every 7 days from the installation time of the tool**

37. Click **Cancel**.

The SMS Administrator Console appears.
Exercise 2
Scanning for Vulnerabilities on the SMS Client

In this exercise, you will force the client to run the Scan Tool for Vulnerability Assessment, and then force the client to collect hardware inventory. You will then verify that the SMS client computer has run the scan tool to perform the vulnerability assessment.

**Note**  Complete this procedure from the SMS 2003 SP2 Advanced Client computer. If you have multiple computers in the Vulnerability Assessment Tool (default) collection, you can complete this procedure on all collection members.

🎨 To force the Scan Tool for Vulnerability Assessment to run on the client

1. In Control Panel, start Systems Management.

   The Systems Management Properties dialog box appears.

2. Click the Actions tab.


3. Click Machine Policy Retrieval & Evaluation Cycle, and then click Initiate Action.

   The Advanced Client will request new policies, which will include the policy related to the advertised program. A Machine Policy Retrieval & Evaluation Cycle message box appears indicating the action was initiated, and may take several minutes to complete.

4. Click OK.

   The Systems Management Properties dialog box appears.

5. Click OK.

   It will take two minutes before the downloaded policies are evaluated and run. It will then take a few minutes for the scan process to complete.
In the following procedure, you will verify that the SMS client computer has successfully run the Scan Tool for Vulnerability Assessment program.

**Note** Complete this procedure from the primary site server with the SMS Administrator Console running. Do not begin this procedure for a few minutes to allow time for the client to complete the scan process.

ফাইলের উচ্চতম বিন্দুতে বিভক্তিগুলি সম্পূর্ণভাবে দেখতে পাওয়া যায়।

**To verify the Vulnerability Assessment Tool (regular) has run on the client**

1. In the console tree, expand **Site Database**, expand **System Status**, and then expand **Advertisement Status**.

   The list of advertisements appears in the console tree.

2. In the console tree, click **Advertisement Status**, and then on the **Action** menu, click **Refresh**.

   The list of advertisements appears in the console tree.

3. In the console tree, click **Vulnerability Assessment Tool**.

   The statistics for the advertisement at the local site appears in the details pane. Notice that there has been at least one client that has received the advertisement, started the program, and successfully completed the advertised program. Notice that there are two programs started and successfully installed for each system that ran the program. This is due to the dependent program to install the MBSA 2.0 scan engine. The numbers here will depend on the collection membership and the number of systems you've forced the scan process to occur on.

4. In the details pane, click **MCM**, and then on the **Action** menu, point to **Show Messages**.

   A new menu appears.

5. Click **All**.

   The SMS Status Message Viewer for <MCM> window appears. Notice the status messages with message IDs of 10002, 10005, and 10008 for receiving, starting and successfully completing the Vulnerability Assessment Tool (regular) program. There also is a message with an ID of 10035, which indicates the program has not started as a request was to download the content was initiated. You will also see 10005 and 10008 status messages for the running of the MBSA Install Silently (without shortcut) dependent program.

6. Close the SMS Status Message Viewer for <MCM> window.

   The list of advertisements appears in the console tree.
In the following procedure, you will force the SMS client computer to collect hardware inventory in order to report the patch status as generated by the Scan Tool for Vulnerability Assessment.

**Note**  Complete this procedure from the SMS 2003 SP2 Advanced Client. This could be multiple clients if you have scanned multiple clients. Perform this procedure on all clients you have scanned with the Scan Tool for Vulnerability Assessment.

 ZX **To force inventory to run on the client**

1. In Control Panel, start Systems Management. 
   The Systems Management Properties dialog box appears displaying discovery data for the client.
2. Click the Actions tab. 
   The Systems Management Properties dialog box appears displaying the available actions for the client.
3. Under Actions, click Hardware Inventory Cycle, and the click Initiate Action. 
   A Hardware Inventory Cycle message box appears indicating the request was issued, and may take several minutes to complete.
4. Click OK. 
   The Systems Management Properties dialog box appears displaying the available actions for the client.
5. Click OK.

In the following procedure, you will verify that the SMS client computer has reported updated hardware inventory.

**Note**  Complete this procedure from the primary site server with the SMS Administrator console running. It will take a minute for the client to report the inventory data to the site. Wait a minute before completing this procedure.

 ZX **To view hardware inventory data**

1. In the console tree, expand Collections, and then click All Systems. 
   The list of collection members appears in the details pane.
2. In the details pane, click an SMS 2003 SP2 Advanced Client computer that has been scanned and has reported hardware inventory, and then on the Action menu, point to All Tasks, and click Start Resource Explorer. 
   The Resource Explorer window appears.
3. Expand Hardware, and then in the console tree, click Workstation Status. 
   The last date and time hardware inventory was reported appears in the details pane. Verify that the current inventory data is the most recent inventory (should be within a few minutes).
4. In the console tree, click **System Vulnerabilities**.
   The list of inventoried vulnerabilities appears. Notice values reported
   include the vulnerability ID and the score.

5. In the console tree, click **System Vulnerabilities Detail**.
   The list of inventoried vulnerabilities appears. Notice values reported now
   include the detail key, detail values (1 through 3), the score for the
   vulnerability, and the vulnerability ID.
   This is not a very easy way to look at the vulnerability data. Using SMS
   Reporting is a much easier way to identify your system vulnerabilities,
   which you will do in the next exercise.

Exercise 3
Using SMS Reporting for Vulnerability Status

In this exercise, you will use SMS Reporting for analysis and reporting of vulnerability status. This is much easier than viewing the data for a single computer in Resource Explorer.

**Note** Complete this exercise from the SMS site server.

♫ To generate an update status report for vulnerabilities
1. In the console tree, expand **Site Database**, and then expand **Reporting**.
   The available SMS Reporting tool functions appear in the console tree.
2. In the console tree, click **Reports**.
   The list of available reports appears in the details pane. Notice that there are over 160 reports available, with five new specific reports for vulnerability reporting.
3. In the details pane, click **Severity of vulnerabilities across all clients**, and then on the **Action** menu, point to **All Tasks**.
   A new menu appears.
4. Point to **Run**, and then click **SMSServer**.
   Internet Explorer starts, and displays the View SMS Reports window. This report is a prompted report, and requires the name of the collection that you want to view vulnerabilities against. Notice that the default value for Collection ID is an “*”, which means the All Systems collection.
5. To report on only the systems that were scanned, under **Collection ID**, delete the *, and then click **Values**.
   The **Select Value** dialog box appears displaying the list of available collections.
6. Click **Vulnerability Assessment Tool (default)**.
   The View SMS Reports window appears displaying the name of the collection to report vulnerabilities for.
7. Click **Display**.
   A SMS Report window appears displaying the **Severity of vulnerabilities across all clients** report. Notice the list of vulnerabilities scanned. Notice also that the report includes the vulnerability ID, title, type (operating systems, SQL Server, IIS, desktop app, other), severity score, the percent of computers that have not reported vulnerability scan results, and information and correction URLs.
8. Click the arrow to the left of 104 (Local Account Password Test).
   A SMS Report window appears displaying the **Count of computers with different vulnerability scores for a specific vulnerability type** report. Notice that this report only includes vulnerabilities for Local Account Password Test. This includes the vulnerability title, type (Operating Systems), vulnerability score description, the number of computers that have reported this vulnerability, information and correction URLs, the vulnerability ID and score.

9. Click the arrow to the left of Check Failed (Critical).
   A SMS Report window appears displaying the **Computers with a vulnerability score for a specific vulnerability** report. Notice that this report includes the list of computers that have reported this vulnerability.

10. Click the arrow to the left of SMSClients.
    A SMS Report window appears displaying the **Vulnerability details for a specific computer** report. Notice that this report includes the list of user accounts that generated this vulnerability. To resolve this vulnerability, you’d need to click the Correction URL (which won’t work in the lab due to lack of Internet access). In our VPC case, this is as expected, as there are weak passwords in use in the VPC images to make it easier for you to log on.

11. In the SMS Report window, click **Back** until you reach the **Severity of vulnerabilities across all clients** report.
    The SMS Report window appears displaying the **Severity of vulnerabilities across all clients** report.

12. Click the arrow to the left of 218 (Service Accounts).
    A SMS Report window appears displaying the **Count of computers with different vulnerability scores for a specific vulnerability type** report. Notice that this report only includes vulnerabilities for Service Accounts for SQL Server.

13. Click the arrow to the left of **Service Account (Best Practice)** with a count of 1.
    The SMS Report window appears displaying the **Computers with a vulnerability score for a specific vulnerability** report. Notice that this report includes the list of computers that have reported this vulnerability. Notice that the vulnerability information URL points to Check5334.html and the correction URL points to Check5334fix.html.

14. Click the arrow to the left of SMSServer.
    The SMS Report window appears displaying the **Vulnerability details for a specific computer** report. Notice that this report includes the usage of user accounts that generated this vulnerability. In this case, it is because the SQL Server Agent service is running under the Local System account, which is not a best practice. You will correct this issue in the next exercise.

15. In the SMS Report window, click **Back** until you reach the **Severity of vulnerabilities across all clients** report.
    The SMS Report window appears displaying the **Severity of vulnerabilities across all clients** report.
16. Click the arrow to the left of **106 (Password Expiration)**.
   A SMS Report window appears displaying the *Count of computers with different vulnerability scores for a specific vulnerability type* report. Notice that this report only includes vulnerabilities for non-expiring account passwords.

17. Click the arrow to the left of **Check Failed (Non-Critical)** with a count of **4**.
   The SMS Report window appears displaying the *Computers with a vulnerability score for a specific vulnerability* report. Notice that this report includes the list of computers that have reported this vulnerability. Notice that the vulnerability information URL points to Check5317.html and the correction URL points to Check5317fix.html.

18. Click the arrow to the left of **SMSServer**.
   The SMS Report window appears displaying the *Vulnerability details for a specific computer* report. Notice that this report includes the usage of user accounts that generated this vulnerability. In this case, you can see that there are a number of accounts with passwords that do not expire. You will correct this issue for the Guest account in the next exercise.

19. In the SMS Report window, click **Back** until you reach the *Severity of vulnerabilities across all clients* report.
   The SMS Report window appears displaying the *Severity of vulnerabilities across all clients* report.

20. Click the arrow to the left of **179 (Automatic Updates)**.
   A SMS Report window appears displaying the *Count of computers with different vulnerability scores for a specific vulnerability type* report. Notice that this report only includes vulnerabilities for Automatic Updates.

21. Click the arrow to the left of **Check Failed (Non-Critical)** with a count of **4**.
   The SMS Report window appears displaying the *Computers with a vulnerability score for a specific vulnerability* report. Notice that this report includes the list of computers (including SMSServer) that have reported this vulnerability. Notice that the vulnerability information URL points to Check53178.html and the correction URL points to Check53178fix.html.
   You will correct this issue in the next exercise.

22. In the SMS Report window, click **Back** until you reach the *Severity of vulnerabilities across all clients* report.
   The SMS Report window appears displaying the *Severity of vulnerabilities across all clients* report.

23. Click the arrow to the left of **307 (IIS Logging Enabled)**.
   A SMS Report window appears displaying the *Count of computers with different vulnerability scores for a specific vulnerability type* report. Notice that this report only includes vulnerabilities for IIS logging not enabled.
24. Click the arrow to the left of **Best Practice** with a count of 1.

   The SMS Report window appears displaying the **Computers with a vulnerability score for a specific vulnerability** report. Notice that this report includes the list of computers (including SMSServer) that have reported this vulnerability. Notice that the vulnerability information URL points to Check5328.html and the correction URL points to Check5328fix.html.

   You will correct this issue in the next exercise.

25. Click the arrow to the left of **SMSServer**.

   The SMS Report window appears displaying the **Vulnerability details for a specific computer** report. Notice that this report includes the lack of logging for IIS. You will correct this issue in the next exercise.


   To correct any vulnerability reported, you would need to view the Correction URL and follow the steps recommended in the appropriate link, which you will do in the next exercise.
Exercise 4
Resolving Vulnerabilities

In this exercise, you will install resolve various vulnerabilities that were reported by the Scan Tool for Vulnerability Assessment.

Note Complete this exercise from the primary site server computer.

To identify the vulnerability resolution

1. Open C:\Program Files\Microsoft Baseline Security Analyzer 2\Help\Check5334.html.
   An Internet Explorer window appears displaying the MBSA information on this specific vulnerability. This is an offline version of the MBSA 2.0 information that the report pointed to.

2. Close the Internet Explorer window, and then open C:\Program Files\Microsoft Baseline Security Analyzer 2\Help\Check5334fix.html.
   An Internet Explorer window appears displaying the MBSA information on how to resolve this specific vulnerability. This is an offline version of the MBSA 2.0 correction information that the report pointed to.

In the following procedure, you will resolve the vulnerability for the SQL Server Agent running under the Local System account.

To resolve the SQL Server Agent account vulnerability

1. On the Start menu, point to Administrative Tools, and then click Services.
   The Services window appears.

2. Under Name, click SQLSERVERAGENT, and then on the Actions menu, click Properties.
   The SQLSERVERAGENT Properties dialog box appears.

3. Click the Log On tab.
   The SQLSERVERAGENT Properties dialog box appears displaying the current service log on configuration. Notice that the current configuration is to use the Local System account, which is not a best practice.

4. Click This account, and then in the This account box, type SMSCDomain\SQLUser

5. In the Password and Confirm password boxes, type password and then click OK.
   A Services message box appears indicating the account was granted Log On As A Service right.

6. Click OK.
   The Services window appears. Notice that the SQL Server Agent service is now running under a user account instead of the Local System account.

7. Close the Services window.
In the following procedure, you will resolve the vulnerability for the Guest account with no password expiration.

**To resolve the password expiration vulnerability**

1. On the Start menu, point to Administrative Tools, and then click Active Directory Users and Computers.
   
The Active Directory Users and Computers window appears.
2. Under Name, click Guest, and then on the Actions menu, click Properties.
   
The Guest Properties dialog box appears.
3. Click the Account tab.
   
The Guest Properties dialog box appears displaying the account properties for the Guest account.
4. Under Account options, clear Password never expires, and then click OK.
   
The Active Directory Users and Computers window appears.
5. Close the Active Directory Users and Computers window.

In the following procedure, you will resolve the vulnerability for Automatic Updates not being enabled.

**To resolve the Automatic Updates vulnerability**

1. In Control Panel, start Automatic Updates.
   
The Automatic Updates dialog box appears. Notice that Automatic Updates is not set to Automatic.
2. Click Automatic (recommended), and then click OK.

In the following procedure, you will resolve the vulnerability for IIS logging not being enabled.

**To resolve the IIS logging vulnerability**

1. On the Start menu, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
   
The Internet Information Services (IIS) Manager window appears.
2. Expand SMSServer, click Web Sites, and then on the Action menu, click Properties.
   
The Web Sites Properties dialog box appears. Notice that logging is not enabled.
3. Click Enable logging, and then click OK.
   
The Internet Information Services (IIS) Manager window appears.
4. Close the Internet Information Services (IIS) Manager window.

You have now resolved four vulnerabilities that will be verified in the next exercise.
Exercise 5
Verifying the Vulnerability Resolution

In this exercise, you will verify that the resolutions to the vulnerabilities are no longer reported as vulnerabilities. You will begin by configuring the advertisement for the Vulnerability Assessment scan to be available to be run manually by a user.

**Note** Complete this procedure from the SMS site server with the SMS Administrator Console running.

✔ To modify the advertisement configuration

1. In the console tree, click **Advertisements**.
   
   The list of advertisements appears in the details pane.
2. In the details pane, click **Vulnerability Assessment Tool**, and then on the **Action** menu, click **Properties**.
   
   The **Vulnerability Assessment Tool Advertisement Properties** dialog box appears displaying the general advertisement properties. Notice that the advertisement is targeting the Vulnerability Assessment (regular) program to the Vulnerability Assessment Tool collection.
3. Click the **Schedule** tab.
   
   The **Vulnerability Assessment Tool Advertisement Properties** dialog box appears displaying the schedule properties for the advertisement. Notice that the program runs on a weekly basis, and that the advertisement is not able to be run manually by a user.
4. Click **Allow users to run the program independently of assignments**, and then click **OK**.
   
   The SMS Administrator Console appears. This change allows the advertised program to be run manually by the user, without having to wait for the assigned time.
In the following procedure, you will force the client to check for new policies. You will only need to do this on the site server, as that is where SQL Server is installed.

**Note**  Complete this procedure on the site server computer.

< To check for updated policies

1. In Control Panel, start Systems Management.
   
   The Systems Management Properties dialog box appears.

2. Click the Actions tab.
   

3. Click Machine Policy Retrieval & Evaluation Cycle, and then click Initiate Action.
   
   The Advanced Client will request new policies, which will include the policy related to the advertised program. A Machine Policy Retrieval & Evaluation Cycle message box appears indicating the action was initiated, and may take several minutes to complete.

4. Click OK.
   
   The Systems Management Properties dialog box appears.

5. Click OK.
   
   This causes the SMS software distribution agent to check for new policies.

**Note**  It will take two minutes for the policy to be downloaded and evaluated before the advertised program will be available to run manually.

In the following procedure, you will run the Vulnerability Assessment Tool on the SMS site server computer.

**Note**  Complete this procedure on the site server computer.

< To manually run the Vulnerability Assessment Tool

1. In Control Panel, start Run Advertised Programs.
   
   The Run Advertised Programs dialog box appears displaying the available advertised programs. Notice that the Vulnerability Assessment Tool program is listed.
2. Under **Program Name**, click **Vulnerability Assessment Tool**, and then click **Run**.

   The Vulnerability Assessment Tool runs. It runs hidden, so you do not see any status of the run.

   **Note**  You can start Task Manager to monitor the running of VulnerabilityAssessment.exe. After it terminates, proceed with the lab.

   The **Run Advertised Programs** dialog box appears displaying the available advertised programs.

3. Click **F5** to refresh the display.

   The **Run Advertised Programs** dialog box appears displaying the available advertised programs. Notice that the Vulnerability Assessment Tool program is listed with a status of success for the current date and time.

4. Click **Close**.

   In the following procedure, you will force the SMS client computer to collect hardware inventory in order to report the patch status as generated by the Scan Tool for Vulnerability Assessment.

   **Note**  Complete this procedure from the SMS site server.

   To force inventory to run on the client

1. In **Control Panel**, start **Systems Management**.

   The **Systems Management Properties** dialog box appears displaying discovery data for the client.

2. Click the **Actions** tab.

   The **Systems Management Properties** dialog box appears displaying the available actions for the client.

3. Under **Actions**, click **Hardware Inventory Cycle**, and the click **Initiate Action**.

   A **Hardware Inventory Cycle** message box appears indicating the request was issued, and may take several minutes to complete.

4. Click **OK**.

   The **Systems Management Properties** dialog box appears displaying the available actions for the client.

5. Click **OK**.
In this exercise, you will use SMS Reporting to verify vulnerability status. The new report should identify that the previous vulnerability no longer exists.

**Note** Complete this exercise from the SMS site server.

_to generate an update status report for vulnerabilities_

1. In the console tree, expand Site Database, and then expand Reporting.
   The available SMS Reporting tool functions appear in the console tree.

2. In the console tree, click Reports.
   The list of available reports appears in the details pane. Notice that there are over 160 reports available, with five new specific reports for vulnerability reporting.

3. In the details pane, click **Severity of vulnerabilities across all clients**, and then on the Action menu, point to All Tasks.
   A new menu appears.

4. Point to Run, and then click SMSServer.
   Internet Explorer starts, and displays the View SMS Reports window. This report is a prompted report, and requires the name of the collection that you want to view vulnerabilities against. Notice that the default value for Collection ID is an *, which means the All Systems collection.

5. To report on only the systems that were scanned, under Collection ID, delete the *, and then click Values.
   The Select Value dialog box appears displaying the list of available collections.

6. Click **Vulnerability Assessment Tool (default)**.
   The View SMS Reports window appears displaying the name of the collection to report vulnerabilities for.

7. Click Display.
   A SMS Report window appears displaying the Severity of vulnerabilities across all clients report. Notice the list of vulnerabilities scanned. Notice also that the report includes the vulnerability ID, title, type (operating systems, SQL Server, IIS, desktop app, other), severity score, the percent of computers that have not reported vulnerability scan results, and information and correction URLs.

8. Click the arrow to the left of 218 (Service Accounts).
   A SMS Report window appears displaying the Count of computers with different vulnerability scores for a specific vulnerability type report. Notice that this report only includes vulnerabilities for Service Accounts for SQL Server.

9. Click the arrow to the left of Service Account Check Failed (Non-Critical) with a count of 1.
   The SMS Report window appears displaying the Computers with a vulnerability score for a specific vulnerability report. Notice that this report includes the list of computers that have reported this vulnerability.
10. Click the arrow to the left of `SMSServer`.

   The SMS Report window appears displaying the **Vulnerability details for a specific computer** report. Notice that this report includes the usage of user accounts that generated this vulnerability. In this case, it is because the SQL Server service is running under a local administrator account, which is not a best practice. Also notice that the SQL Server Agent vulnerability is no longer listed.

11. In the SMS Report window, click **Back** until you reach the **Severity of vulnerabilities across all clients** report.

   The SMS Report window appears displaying the **Severity of vulnerabilities across all clients** report.

12. Click the arrow to the left of **106 (Password Expiration)**.

   A SMS Report window appears displaying the **Count of computers with different vulnerability scores for a specific vulnerability type** report. Notice that this report only includes vulnerabilities for non-expiring account passwords.

13. Click the arrow to the left of **Check Failed (Non-Critical)** with a count of **4**.

   The SMS Report window appears displaying the **Computers with a vulnerability score for a specific vulnerability** report. Notice that this report includes the list of computers that have reported this vulnerability.

14. Click the arrow to the left of `SMSServer`.

   The SMS Report window appears displaying the **Vulnerability details for a specific computer** report. Notice that this report includes the usage of user accounts that generated this vulnerability. In this case, you can see that the Guest account is no longer listed as a vulnerability.

15. In the SMS Report window, click **Back** until you reach the **Severity of vulnerabilities across all clients** report.

   The SMS Report window appears displaying the **Severity of vulnerabilities across all clients** report.

16. Click the arrow to the left of **179 (Automatic Updates)**.

   A SMS Report window appears displaying the **Count of computers with different vulnerability scores for a specific vulnerability type** report. Notice that this report only includes vulnerabilities for Automatic Updates. Notice also that there are no entries for the Check Failed (Non-Critical), and now there is a computer for Check Passed.

17. Click the arrow to the left of **Check Passed** with a count of **1**.

   The SMS Report window appears displaying the **Computers with a vulnerability score for a specific vulnerability** report. Notice that this report includes the list of computers (including SMSServer) that have passed this vulnerability test.

18. In the SMS Report window, click **Back** until you reach the **Severity of vulnerabilities across all clients** report.

   The SMS Report window appears displaying the **Severity of vulnerabilities across all clients** report.
19. Click the arrow to the left of **307 (IIS Logging Enabled)**.

A SMS Report window appears displaying the **Count of computers with different vulnerability scores for a specific vulnerability type** report. Notice that this report only includes vulnerabilities for IIS logging not enabled.

20. Click the arrow to the left of **Best Practice** with a count of **1**.

The SMS Report window appears displaying the **Computers with a vulnerability score for a specific vulnerability** report.

21. Click the arrow to the left of **SMSServer**.

The SMS Report window appears displaying the **Vulnerability details for a specific computer** report. Notice that this report states there are no records found for this issue, as it is now resolved.

22. Close the SMS Report and View SMS Reports windows.

You have now successfully used the Scan Tool for Vulnerability Assessment to scan for and report on vulnerabilities in the enterprise.