Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows. It is a security vulnerability tool designed to help determine the security state in accordance with Microsoft security recommendations and offers specific remediation guidance.

Microsoft Baseline Security Analyzer (MBSA)

Vulnerability Scanner

Jamaal Green and Angela Richardson
11/16/2011

Microsoft Baseline Security Analyzer

Table of Contents

Project Introduction 1

Project Description 2

Project Security Issues 4

Completed Project Tasks, Challenges, and Lessons Learned 5

- Completed Project Tasks 5
- Project Challenges 7
- Lessons Learned 8

Hands on Labs - Microsoft Baseline Security Analyzer Labs 1 & 2 9

- Project - Microsoft Baseline Security Analyzer Lab 1 – Angela Richardson 10
- Project - Microsoft Baseline Security Analyzer Lab 2 – Jamaal Green 15

Conclusion 18

References 19

Project MBSA Team 1 Evaluations 20

- Evaluated by Jamaal Green 20
- Evaluated by Angela Richardson 21

Project Introduction

A vulnerability scanner is one of many security tools used to improve the security of networks. The goal of running a vulnerability scanner is to identify devices on a network that are open to known vulnerabilities. A vulnerability tool can help secure a network or it can be used by potential attackers to identify weaknesses in you system to mount an attack against. The tool can be used to identify and fix weaknesses before potential attacker use them to exploit victims. There are many different types of scanners that accomplish similar goals through different means. Some scanners work better than others. Some of the highly rated vulnerability scanning packages including SAINT, SARA and QualysGuard carry a hefty price tag. Some companies do not mind the cost of the tools because they add network security and peace of mind. With recent budget shortfalls within companies, many others do not have the budget needed for these products. Companies that primarily use Microsoft Windows products use a freely available tool called Microsoft Baseline Security Analyzer (MBSA). MBSA can be used to scan systems and identify missing patches and missing or weak passwords and other common security issues. MBSA tool is used to assess security settings within Microsoft (MS) Windows components such as: Internet Explorer, Web Server, Products Microsoft SQL server, MS Office Settings and is compatible with the Windows Operating Systems Windows – NT, 2000, XP, 2003, Vista, and 7. It average scans over three million computers each week and is used by many leading third-party vendors, security auditors, medium to large businesses, home Networks - Local Hosts.

Project Description

MBSA (Microsoft Baseline Security Analyzer) is a security vulnerability scanner designed to assess computers, computer systems, networks or applications for weaknesses. MBSA will scan Windows-based computer(s) and check the operating system(s) and other installed components. MBSA 2.2 will be used in this project to help determine how safe a Windows system is by checking for common misconfigurations and missing security updates and by using the recommendations provided to improve the system safeguards in accordance with the Microsoft security standards. The objectives of this project are to use the tool to scan a computer system for system vulnerabilities, determine how to detect the misconfigurations of the computer system and learn how to correct these misconfigurations. Our project team will check certain settings to determine whether they are secure We will determine whether the Auto Logon feature is enabled. If enabled, it could allow other users to access personal files and use the host name to commit malicious acts. Automatic updates will be checked to identify whether the feature is enabled and if so, how it is configured. It should be configured to best fit the security needs of the host. Guest Account check will be checked to determine whether the built-in guest account is enabled. It may be enabled and used by all user connections from the network as part of the security model. The Firewall will be checked to determine whether it is enabled for allowing or denying access in and out of the host network. Local Account passwords will be checked to identify any local user accounts that are using blank or simple passwords. Since the tool was designed to work on windows based Operating Systems, a check will be performed to see if windows server 2003, XP 2000, or Windows 7 version is running on the local host. Local user accounts will be checked for non-expiring passwords because passwords should be changed regularly to mitigate against password attacks. Anonymous users should be restricted on the scanned computer because anonymous users can list certain types of system information, including user names and details, account policies, and share names. To provide enhanced security, these administrative vulnerabilities will be checked and

updated as recommended. The resulting security scan report will be analyzed for critical issues, non-critical issues, and best practices and passed checks. The critical scans will be addressed and corrected as recommended by the tool. Non-critical issues and best practices will be reviewed the recommended updates will be considered. Passed checks will also be reviewed for informational purposes.

Project Security Issues

The MBSA 2.2 tool offers multiple scan options for identifying weaknesses. The MBSA provides the ability to check for Windows administrative vulnerabilities, weaknesses in administrative tools used to administer computers, services, other system components, and networks which will be the primary focus area for this project. The Windows administrative vulnerabilities are the main Security Issues focused on in this project. We will focus on checking settings like auto-updates, weak passwords, user accounts, auto-login, anonymous users, guest accounts, firewall, non-expiring passwords and operating system version that could be exploited by attackers if they are not set up and secured properly. We will also focus on any best practices, critical and non-critical scan issues identified by the MBSA tool to improve the security state of the scanned hosts. Since the tool provides the ability to check for weak passwords - passwords that are blank or considered simple and easy to crack, we will focus on these to see if vulnerabilities exist and correct all critical issues. The tool also provides the ability to check for Internet Information Services (IIS) admin vulnerabilities, weaknesses in the administration of Web and RP services through the internet Information Services; and the ability to check for SQL vulnerabilities, weaknesses in administrative tools used in database development, maintenance and administration. While these features are available, we are not planning to focus on these security vulnerabilities in this project.

Completed Project Tasks, Challenges, and Lessons Learned

Completed Project Tasks

There were a few project scenarios that were completed, in order to see how the tool actually operates. Of course, there are many different tasks that can be administered to check the security state of the system but not all were chosen in this particular scan. In this scan, the MBSA tool performed Windows checks. These checks consisted of checking the administrator's group membership, the auto log on, the local account passwords, the automatic updates that the system may have needed, and if there was a firewall in place. The purpose of checking the administrator's group membership is to verify the individual user accounts that belong to the local administrator, to keep administrators to a minimum, and correct any misconfigurations or missing security updates. The tool also scans for auto logons to determine whether the Auto Logon feature is either enabled or disabled. Local account password checks are administered in order to determine if a password is blank, if a particular password is the same as the username, and if the password is considered weak. Checking for automatic updates reveal information about whether the Automatic Update feature is enabled or disabled, how the automatic update is configured, and corrects any misconfigurations or missing security updates. The MBSA tool also checks the firewall to determine whether it is enabled or disabled. Checking the firewall also determines whether any static bound ports are open in the firewall.

Once this scan was completed, the results were astounding. There were not many issues, but the information that was given was very vital. The administrator's group membership was considered sufficient because there were only two administrators on that particular system. The auto logon check was not configured on this computer, which was also a considered a good report. The local account passwords check however, did not have a good report. Some user accounts, maybe 3 or 4, had simple or blank passwords, or could not be analyzed. The solution to this problem was to

adopt a strong password policy, which is one the most effective ways to ensure system security. When the tool scanned the Automatic Update feature, it resulted in a good score. This meant that updates were automatically downloaded and installed on the system. The firewall that was scanned was enabled but had exceptions configured. This was not considered a critical issue, but comments were made stating that the MBSA cannot scan other firewalls that may have been on the system, in result of it not being a Windows program.

Project Challenges

MBSA was a very simple and very easy to use yet powerful and intuitive tool to identify system weaknesses. Our project team was very fortunate because of the tool's simple tasks/features identified in <Figure 1>; we did not have any project challenges. We were able to download the tool without any issues, we easily navigated the tool features and because of the scan report simplicity in <Figure 2>, we were able to easily read and access the results. We did not face any challenges working with this tool. It can be very useful for anyone that would like to know the security state of their machine(s). The Microsoft Baseline Security Analyzer is far from cumbersome, and can be used by any entry-level Information Technology personnel. MBSA not only informs the administrator of the issues that may be associated with a system, it also provides suggestions of how to correct these particular problems.

Figure 1.

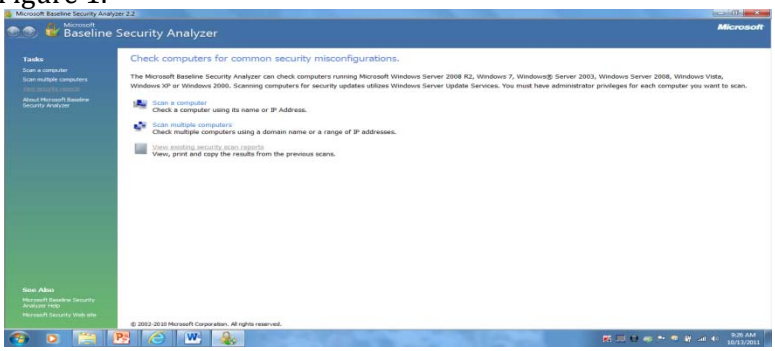
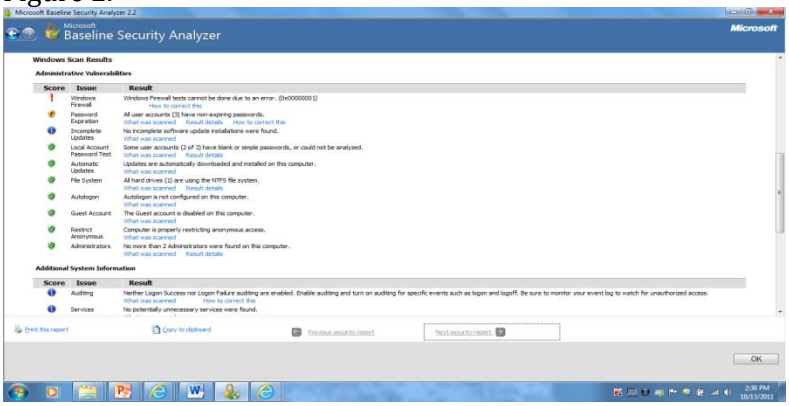


Figure 2.



Lessons Learned

MBSA was a very good tool in that it provided really good and helpful information to help seek out analyze and correct Windows Administrative vulnerabilities on a windows-based computer. We did not run into any challenges working with the tool. It can be very useful for anyone that would like to know the security state of their local network or any commercial IT infrastructure. The Microsoft Baseline Security Analyzer is far from cumbersome, and can be used by any entry-level Information Technology personnel and for in home use. The tool not only informs the administrator of the issues that may be associated with the system, it also provides suggestions of how to correct any identified problems.

We learned how to:

- Improve the IT Infrastructure of a local host
- Use MBSA to perform a security updates scan on a local host
- Use MBSA to check for current settings that are not secure on a local host
- Determine how to detect the misconfigurations of a local host by scanning a local host and analyzing the scan results
- Correct the misconfigurations of a local host using the scan results recommendations generated by the MBSA tool

Hands on Labs - Microsoft Baseline Security Analyzer Labs 1 & 2

Author: Angela Richardson & Jamaal Green
Ref: Network Security - Term Project
Semester: Fall 2011
Date: 11/16/2011
Type of Investigation: Detecting System Vulnerabilities - Vulnerability Scanner
Software: Microsoft Baseline Security Analyzer
Version: 2.2
Source: Freeware
Hardware: Gateway, HP Pavilion
Operating Systems: Windows – NT, 2000, XP, 2003, Vista, and 7
Files/Data/Documents (optional): XML

Download:
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=7558

Background:

In these Labs we will use Microsoft Baseline Security Analyzer 2.2 (MBSA), vulnerability scanner to check for Windows Administrative Vulnerabilities.

Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to Determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. MBSA determines which critical security updates are available for particular Microsoft products by referring to an Extensible Markup Language (XML) file that contains security bulletin names and titles, and detailed data about product specific security updates. It can scan a single computer or multiple computers and generates security reports that are saved in an XML format. The tool allows users to scan one or more Windows-based computers for common security misconfigurations. It will scan a Windows-based computer and check the operating system and other installed components for security misconfigurations and whether or not they are up-to-date with respect to recommended security updates.

MBSA 2.2 is the latest version of Microsoft's free security and vulnerability assessment scan tool for administrators, security auditors, and IT professionals.

Project Goals of Labs (Lab 1 & Lab 2):
In these labs we will learn to:

- **Improve the IT Infrastructure of a local host** (Lab 1 - Activities 4 & 5; Lab 2 –Activity 3)
- **Use MBSA to perform a security updates scan (**Lab 1 **-** Activity 4; Lab 2 – Activity 3)
- **Use MBSA to check for current settings that are not secure** (Lab 1 - Activity 4; Lab 2 – Activity 3)
- **Determine how to detect the misconfigurations of a local host** (Lab 1 - Activities 1 – 4; Lab 2 – Activities 1 - 3)
- **Correct the misconfigurations** (Lab 1 - Activities 4 & 5; Lab 2 – Activity 3)

Project - Microsoft Baseline Security Analyzer Lab 1 – Angela Richardson

Author: Angela Richardson
Ref: Network Security - Term Project
Semester: Fall 2011
Date: 11/16/2011
Type of Investigation: Detecting System Vulnerabilities - Vulnerability Scanner
Software: Microsoft Baseline Security Analyzer
Version: 2.2
Source: Freeware
Hardware: Gateway
Operating Systems: Windows – NT, 2000, XP, 2003, Vista, and 7
Files/Data/Documents (optional): XML

Download:
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=7558

Background:

In these Labs we will use Microsoft Baseline Security Analyzer 2.2 (MBSA), vulnerability scanner to check for Windows Administrative Vulnerabilities.

Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to Determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. MBSA determines which critical security updates are available for particular Microsoft products by referring to an Extensible Markup Language (XML) file that contains security bulletin names and titles, and detailed data about product specific security updates. It can scan a single computer or multiple computers and generates security reports that are saved in an XML format. The tool allows users to scan one or more Windows-based computers for common security misconfigurations. It will scan a Windows-based computer and check the operating system and other installed components for security misconfigurations and whether or not they are up-to-date with respect to recommended security updates.

MBSA 2.2 is the latest version of Microsoft's free security and vulnerability assessment scan tool for administrators, security auditors, and IT professionals.

Goals of Lab 1:
In this lab we will learn to:

- **Improve the IT Infrastructure of a local host** (Activities 4 – 5)
- **Check Operating System Version** (Activity 4)
- **Check Password Expiration** (Activity 4)
- **Check Anonymous Users** (Activity 4)
- **Detect Misconfigurations of a local host** (Activities 1-4)
- **Analyze Scan Report** (Activity 4)
- **Correct Critical Issues** (Activities 4 – 5)

Detail Procedures: (Detecting System Vulnerabilities using MBSA 2.2)

MBSA requires administrator privileges on both the computer with MBSA installed and the target computers that you scan. Users of the MBSA tool must provide a valid computer name (s) or Ip address (es) in order to invoke a scan.

ACTIVITY 1: (Log onto a Computer as Admin and Launch the MBSA tool)
(GET READY!)

- Log onto a local host
- Make sure that the account used to log onto the host has admin privileges:
  - Select **< Start>**
  - Select **<Control Panel>**
  - Select **<User Accounts>**
  - Select **<User>**
  - Select **<Properties>**
  - Close the window
- Launch MBSA 2.2 by selecting the following:
  - **< Start>**
  - **<All Programs>**
  - **<Microsoft Baseline Security Analyzer 2.2>**

ACTIVITY 2: (Validate the Computer Name Before Starting the Scan)
(GET SET!)

- Minimize the MBSA tool to get back to the computer's desk top
- Verify the computer properties:
  - Select **< Start>**
  - Right click **<Computer>**
  - Select **<Properties>**
  - Close the window

Questions:

1. Which operating systems are supported by MBSA? **Windows – NT, 2000, XP, 2003, Vista, and 7**
2. What is the name of the Operating System? **Windows 7**
3. What is the name of the computer? **DEVIN-PC**
4. What is the full computer name? **DEVIN-PC**
5. What is the name of the workgroup? **WORKGROUP**
6. Please list the steps to rename the computer or change its domain or workgroup.
   Click **< Start>,** Right click <**Computer>,** Select **<Remote Settings>,** Select **<Computer name>** tab**,** Select **<Change>,** Enter **"new name here",** Select **<ok>**
7. Is there a description of the computer? **No** If so, what is it?
8. What other information is provided in this section and give a brief description of the information? **System information like manufacture, model, rating, processor, installed memory (RAM), and system type**

ACTIVITY 3: (Select MBAA Tasks and Options for Scanning)
(GET SET!)

- Go back to the MBSA tool
- Check a Single Computer using the name obtained from the tasks in ***Activity 2*** and perform the following Windows Checks: Check Guess Accounts, Check Operating System Version, Check Password Expiration, Check Restrict Anonymous Users, and Check Security Reports.

  - Double Click **< Scan a Computer>**
  - Enter the name or the IP address of the computer you wish to scan.
    Note: By default the computer name displayed will be the local computer on which the tool is running.
  - Enter the security scan report name to be generated after the scan.
  - Determine scan options:
    Select **<Check for Windows Administrative vulnerabilities >**
    Select **<Check for weak passwords>**

Questions:

1. What are weak passwords? **Weak passwords are blank or simple passwords**
2. What are "Windows Administrative Vulnerabilities? **Weaknesses in administrative tools used to administer computers, services, other system components, and networks.**
3. What are "IIS Admin vulnerabilities"? **Weaknesses in the administration of Web and FTP services through the Internet Information Services.**
4. What are "SQL administrative vulnerabilities"? **Weaknesses in administrative tools used in database development, maintenance and administration.**

ACTIVITY 4: (Scan the Computer and Analyze the Scan)
(GO!)

- Start MBSA scan:
  - Select **< Start Scan>**
- Review the Scan Report for details of the issues found for Guess Accounts, Operating System Version, Password Expiration, Restrict Anonymous Users, and Security Reports.

Questions:

1. What format are the security reports saved in? **XML**

2. Was the Operating System flagged in the security report? **No, the OS was not be flagged in the security report because Windows 7 is windows based**

3. Was the Guest account enabled? **No.** How do you know? **If the Guest account is enabled, it should be flagged in the security report as vulnerability.**

4. If the users account is non-expiring, it should be flagged in the security report. Was the Users account flagged? **Yes.**

5. Where there any best practice found? What type of information does the tool provide regarding the best practice?

   Score: Best Practice

   Issue: Incomplete Updates

   Result: No incomplete software updates installations were found

   What was scanned: Incomplete Updates - This check determines whether the system has a software update installed that required a system restart that has not yet taken place. This is flagged in the scan report as a potential vulnerability, because if the update was for security purposes, it may not be providing needed protection until the restart has completed.

6. Where there any non-critical checks found? Yes. What type of information/recommendations did the tool offer to correct the problem?

   Score: Check Failed

   Issue: Password Expiration

   Result: All user accounts have non-expiring passwords

   What was scanned: Password Expiration - This check determines whether any local accounts have passwords that do not expire. Each local user account that has a password that does not expire will be listed in the security scan report, with the exception of any user accounts specified in the NoExpireOk.txt file in the MBSA installation folder.

7. Where there any passed checks found? **Yes.** List at least three passed checks. **Local Account password tests, automatic updates, and restrict anonymous users.**

ACTIVITY 5: (Correct any Issues)

- Use the recommended security updates in ***Activity 4*** to update the missing misconfigurations and missing security updates. For each issue listed in the scan report, click the ***How to correct this*** link. The page that appears provides the solution to the issue and the instructions to correct the issue.

Questions:

1. What type of recommendations did the tool offer to correct the problem with ***Password Expiration***?

   Solution: Passwords should be changed regularly to prevent password attacks.

2. What type of information did the tool provide for ***Restrict Anonymous Users***?

   Passed Check

   Note: For enhanced security, restrict this function so that anonymous users cannot access confidential information.

3. What type of information/recommendations did the tool provide for ***Guess Accounts?*** **It determined whether the built-in Guest account was enabled on the scanned computer. The guest account is disabled on the computer.**

Project - Microsoft Baseline Security Analyzer Lab 2 – Jamaal Green

Author: Jamaal Green
Ref: Network Security - Term Project
Semester: Fall 2011
Date: 11/16/2011
Type of Investigation: Detecting System Vulnerabilities - Vulnerability Scanner
Software: Microsoft Baseline Security Analyzer
Version: 2.2
Source: Freeware
Hardware: HP Pavilion
Operating Systems: Windows – NT, 2000, XP, 2003, Vista, and 7
Files/Data/Documents (optional): XML

Download:
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=7558

Background:

In these Labs we will use Microsoft Baseline Security Analyzer 2.2 (MBSA), vulnerability scanner to check for Windows Administrative Vulnerabilities.

Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to Determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings. MBSA determines which critical security updates are available for particular Microsoft products by referring to an Extensible Markup Language (XML) file that contains security bulletin names and titles, and detailed data about product specific security updates. It can scan a single computer or multiple computers and generates security reports that are saved in an XML format. The tool allows users to scan one or more Windows-based computers for common security misconfigurations. It will scan a Windows-based computer and check the operating system and other installed components for security misconfigurations and whether or not they are up-to-date with respect to recommended security updates.

MBSA 2.2 is the latest version of Microsoft's free security and vulnerability assessment scan tool for administrators, security auditors, and IT professionals.

Goals of Lab 2:
In this lab you will learn to:

- **Check administrator's group membership** (Activity 3)
- **Check auto log on** (Activity 3)
- **Check local account passwords** (Activity 3)
    - **Check automatic updates** (Activity 3)
    - **Check firewall** (Activity 3)
    - **Learn how to correct the misconfigurations** (Activity 3)

Detail Procedures: (Detecting System Vulnerabilities using MBSA 2.2)

MBSA requires administrator privileges on both the computer with MBSA installed and the target computers that you scan. Users of the MBSA tool must provide a valid computer name (s) or Ip address (es) in order to invoke a scan.

Activity 1: (Log onto a Computer and Launch the MBSA tool)

- Log onto a local host
- Log into the **<Admin>** account
- Launch MSBA 2.2 by selecting the following:
    - **< Start>**
    - **<All Programs>**
    - **<Microsoft Baseline Security Analyzer 2.2>**

Activity 2:(Select MBSA tasks and options for scanning)

- Check a Single Computer using its name obtained from the tasks in step 2:
    - Double Click **< Scan a Computer>**

    - Enter the name or the ip address of the computer you wish to scan.(The name of the system should automatically be entered)
    - Determine scan options:

      Select **<Check for Windows Administrative vulnerabilities >**

      Select **<Check for weak passwords>**

      Select<**Check for security updates>**

      Select<**Configure computers for Microsoft Updates and scanning prerequisites>**

    - **Questions:**

1. Why is it imperative that you have security updates? **To ensure that your system remains uncompromised.**

Activity 3(Begin Scanning the Computer for System Vulnerabilities):

- Start MBSA scan:
    - Select **< Start Scan>**
- Review the Security Report:
    - **Questions:**

1. What is the IP address of the system you are scanning? **192.168.2.7**
2. What is the result of the "Windows Security Updates" issue? **No security updates are missing.**
3. Are there any accounts that have non-expiring passwords? If so, how many? **Yes, all user accounts (4) have non-expiring passwords.**
4. How do you correct this issue? **Any local accounts identified in the security report as having passwords that do not expire should be reviewed to determine why the option is set, and if it should be removed.Accounts in the NoExpireOk.txt file (in the MBSA installation folder) will not be reported during the password expiration check. Users can add or remove account names in this file to be skipped during the scan**
5. What is the result of the "Local Account Password Test" issue? **Some user accounts (3 or 4) have blank or simple passwords, or could not be analyzed.**
6. How do you correct this issue? **Adopt a strong password policy. This is one of the most effective ways to ensure system security.**

Conclusion

Vulnerabilities are situations or conditions that increase the probably of a threat, which in turn increases risk. The web is packed with free projects that are designed to protect systems from vulnerabilities, malware, device misconfigurations, internet attacks, and a variety of other threats and weaknesses. Fortunately, MBSA helped us in our project to build an impressive security arsenal without spending a cent because it is free. It is a windows based application that is ideal for running on numerous servers and is capable of handling heavy workloads. It is one of the top ten vulnerability scanners and one of the best free security tools that is essential for any server, particularly one online. MBSA can detect common security misconfigurations and missing security updates on a computer system to improve a security management process. MBSA was a very good tool in that it provided really good and helpful information to help seek out weakness on a single computer. The project demonstrated an easy way to identify, analyze and correct Windows administrative weaknesses on local hosts.

References

The 10 Best Free Security Tools. (2008). Retrieved from http://www.itsecurity.com/features/10-best-free-security-tools-011708/

Top 10 Web Vulnerability Scanners. (2011). Retrieved from http://sectools.org/web.scanners.html

Microsoft Baseline Security Analyzer. (2011). Retrieved from http://technet.microsoft.com/en-us/security/cc184922

Microsoft Baseline Security Analyzer. (2011). Retrieved from http://technet.microsoft.com/en-us/security/cc1849224

Benefits of a Vulnerability Scanner. (2011) Retrieved from

http://guidance-consulting.com/articles/90-benefits-of-a-vulnerability-scanner.html

Guide to Network Defense and Countermeasures, 2nd Edition

Project MBSA Team 1 Evaluations

Evaluated by Jamaal Green

CNT4406 Individual Peer Evaluation Form for Midterm Project

If you are the only member in your team, please write down your name and circle here

ONLY ONE MEMBER

Ratings: for each team member

A: members who contributed above average 80% of her/his assigned work

B: members who contributed effectively

C: members who did not always complete work

D: members who did less than 50% of his/her assigned work

F: members who did not contribute to the team

Task:

Researched project topics. Reviewed MBSA tool requirements, features and specifications. Assisted in the installation of MSBA and other tools required to complete all deliverables of the project. Performed project research and provided contents for all project artifacts (abstract, presentation, final report and labs). Researched, created and implemented Lab 1- Check Guest Account, Check Operating System Version, Check Password Expiration, Check Anonymous Users, Analyze Scan Report and Correct Critical Issues.

Name of your team__MBSA____ TEAM #__1__

Name of your team members		Ratings	Task
Last Name	First Name		
1. __Richardson__	__Angela___	__A__	__All Task Identified Above__

Project MSBA Team 1 Evaluations

Evaluated by Angela Richardson

CNT4406 Individual Peer Evaluation Form for Midterm Project

If you are the only member in your team, please write down your name and circle here

ONLY ONE MEMBER

Ratings: for each team member

A: members who contributed above average 80% of her/his assigned work

B: members who contributed effectively

C: members who did not always complete work

D: members who did less than 50% of his/her assigned work

F: members who did not contribute to the team

Tasks:

Researched project topics. Reviewed MBSA tool requirements, features and specifications. Assisted in the installation of MSBA and other tools required to complete all deliverables of the project. Performed project research and provided contents for all project artifacts (abstract, presentation, final report and labs). Researched, created and implemented Lab 2 - Check Administrator's Group Membership, Check Auto Log On , Check Local Account Passwords, Check Automatic Updates, Check Firewall, and Learn How to Correct Misconfigurations.

Name of your team__MSBA_____ TEAM #__1__

Name of your team members		Ratings	Task
Last Name	First Name		
1. __Green___,	__Jamaal__	__A__	__All Task Identified Above_____