Using MBSA Software list all the security updates missing in Window OS

What is MBSA (Microsoft Baseline Security Analyzer)?

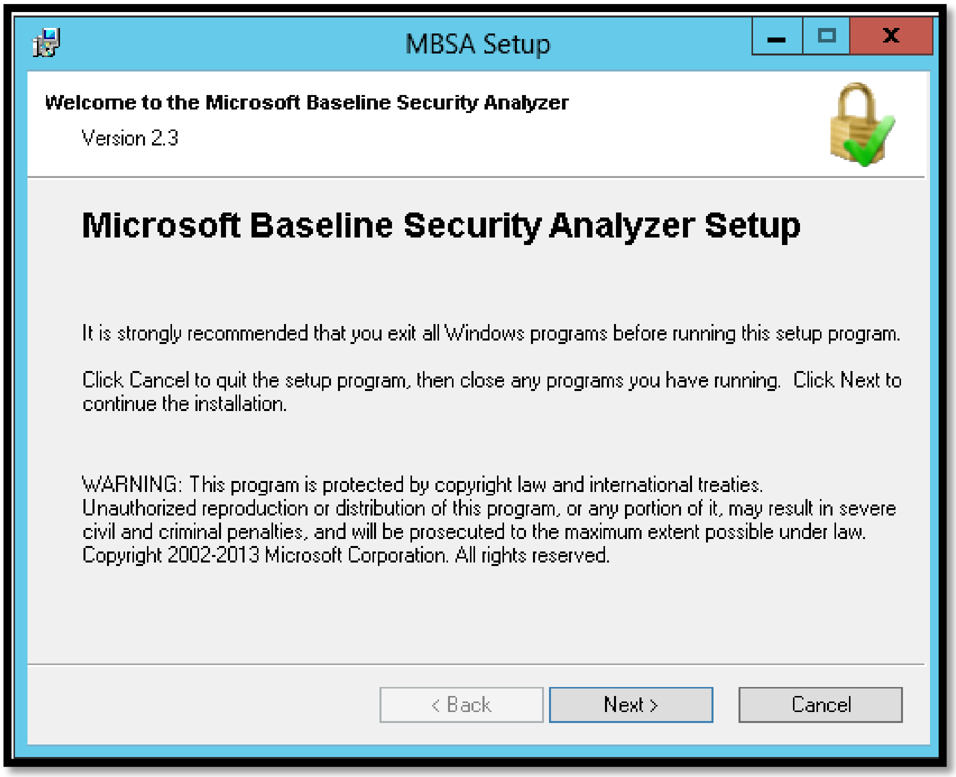
Microsoft Baseline Security Analyzer is one of the tools provided by Microsoft to help administrators to scan systems (local and remote) for missing security updates and common security misconfigurations. It can scan the server operating system and SQL Server but also other products as well, such as Microsoft web server IIS.

Installation procedure –

Once the files have been downloaded, put them on the server you'll use as a host for the tool, or on a network share and go to the server of your choice.

Running the installer

We can now run the installer corresponding to our language and architecture. The following window will pop up



MBSA Setup

Welcome to the Microsoft Baseline Security Analyzer

Version 2.3

Microsoft Baseline Security Analyzer Setup

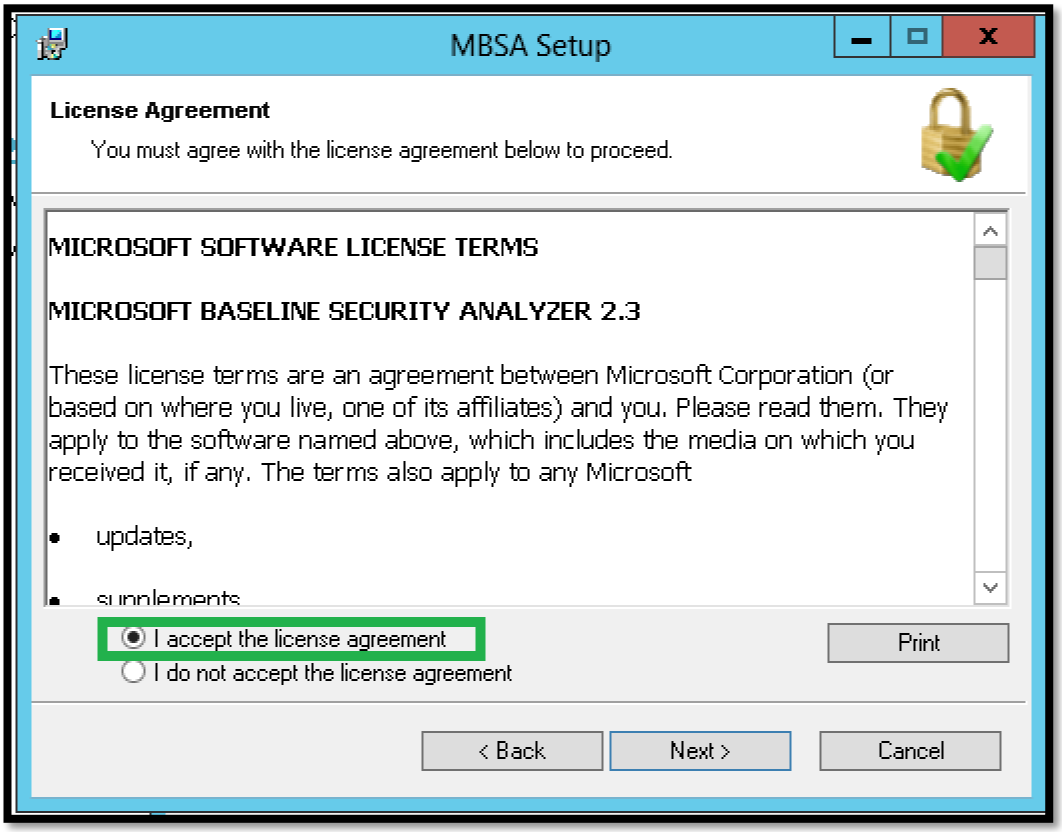
It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Copyright 2002-2013 Microsoft Corporation. All rights reserved.

Just click on “Next” button.

The next panel is the license agreement you will have to approve and click on “Next” button:



License Agreement

You must agree with the license agreement below to proceed.

MICROSOFT SOFTWARE LICENSE TERMS

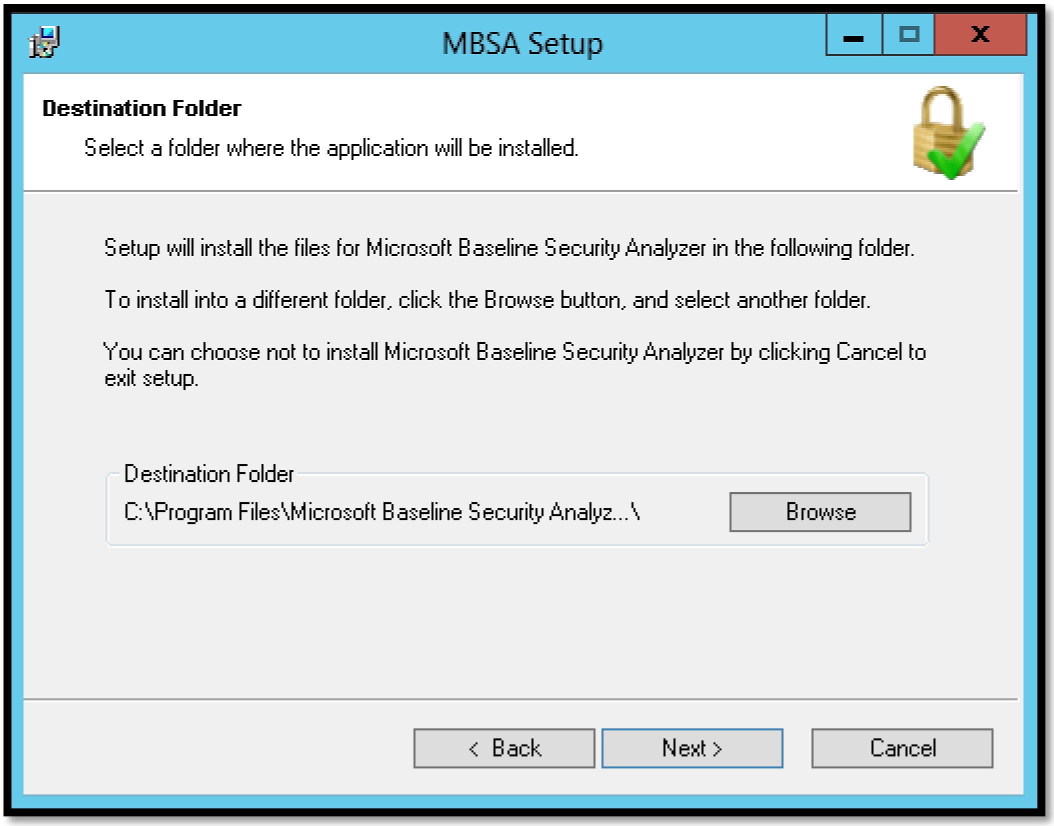
MICROSOFT BASELINE SECURITY ANALYZER 2.3

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements

● I accept the license agreement
○ I do not accept the license agreement

Now we must choose the destination directory. We can let it to its default or change it then click on the “Next” button:



Destination Folder

Select a folder where the application will be installed.

Setup will install the files for Microsoft Baseline Security Analyzer in the following folder.

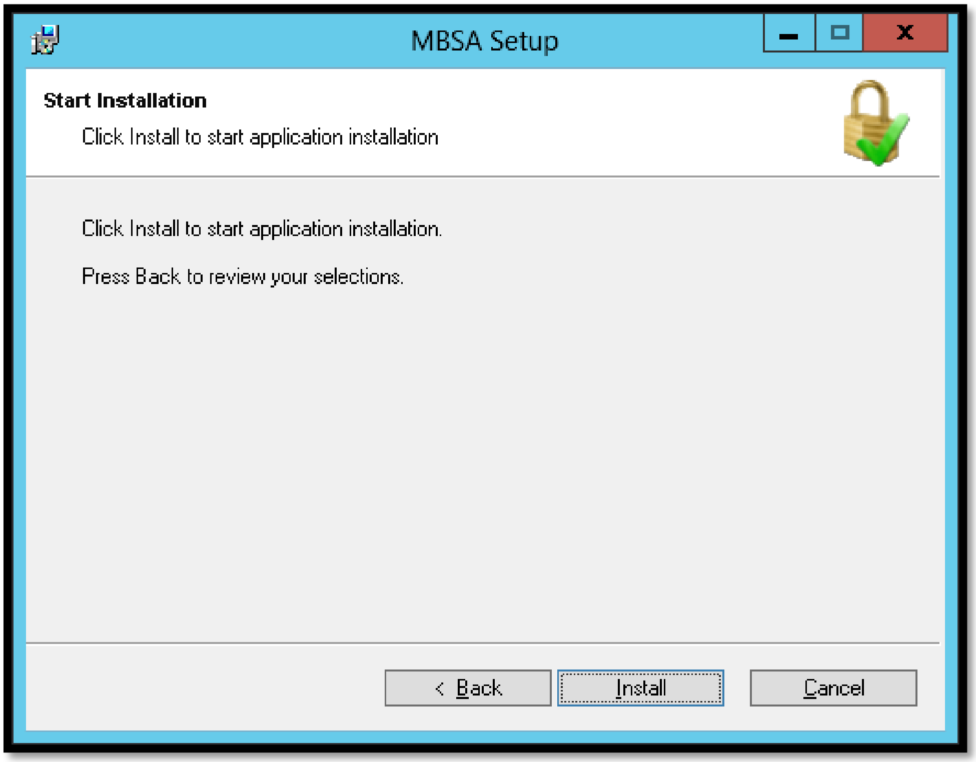
To install into a different folder, click the Browse button, and select another folder.

You can choose not to install Microsoft Baseline Security Analyzer by clicking Cancel to exit setup.

Destination Folder

C:\Program Files\Microsoft Baseline Security Analyz...\

Now we just have to confirm the install and let it run by clicking on the “Install” button:



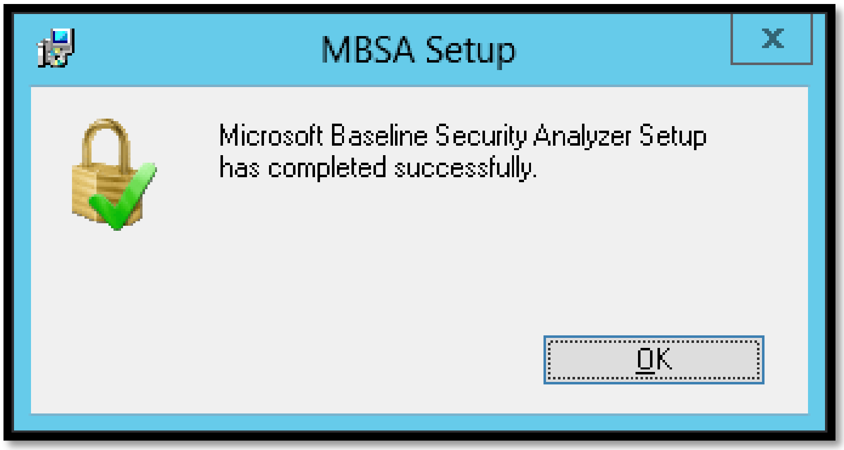
Start Installation

Click Install to start application installation

Click Install to start application installation.

Press Back to review your selections.

Once the installation is done, you’ll get the following popup on which you just have to click OK:

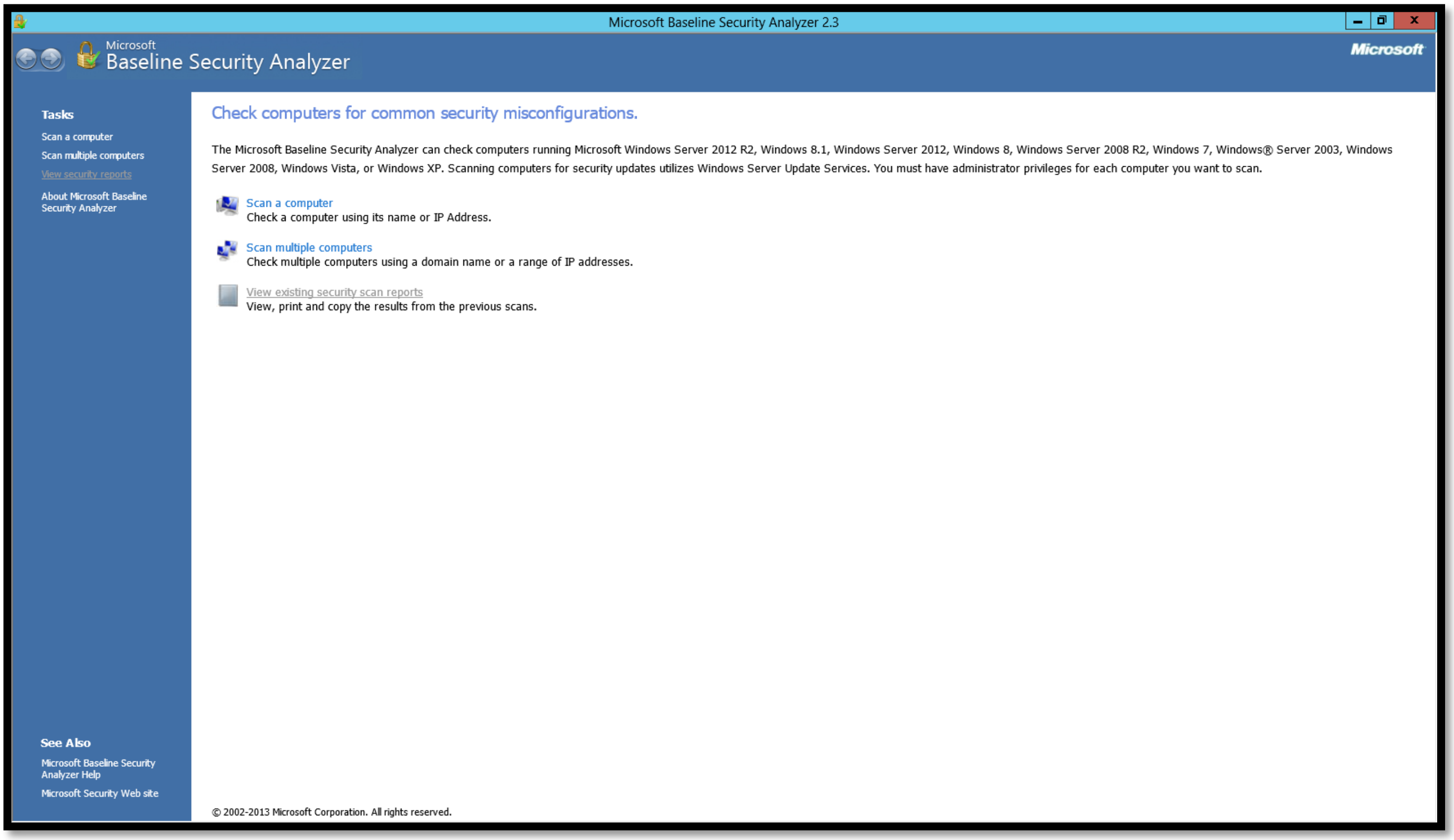


Microsoft Baseline Security Analyzer Setup has completed successfully.

Congratulations, Microsoft Baseline Security Analyzer is now installed. Let's now see how to use it.

Running the tool graphically -

Let's run it and see what the graphical interface look like:


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
See Also
Microsoft Baseline Security Analyzer Help
Microsoft Security Web site

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

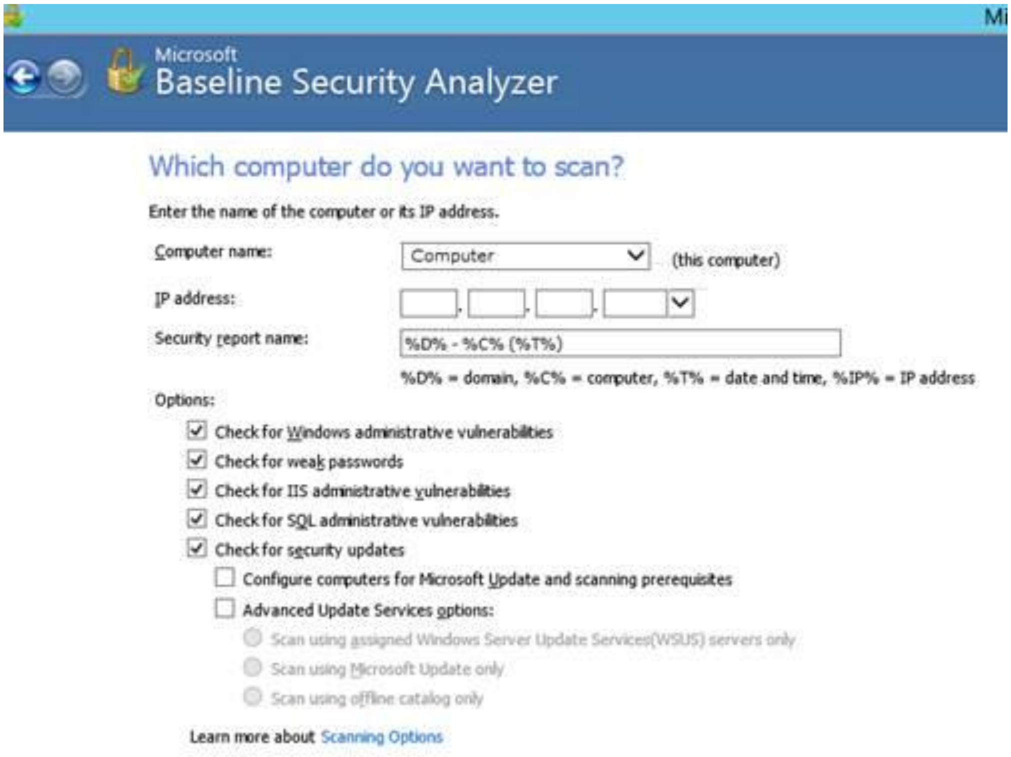
© 2002-2013 Microsoft Corporation. All rights reserved.

As we can see directly from the image above, this tool can:

- Scan a single computer by providing an IP or its NetBIOS name.
- Do this scan for a group of computers
- Have a look at existing reports (when we have some)

Let’s just click on “Scan a computer”:

This switches to another dialog, where you’ll need to provide some parameters. The parameters are a NetBIOS computer name, an IP address and the name of the final report which is can be parameterized. In addition, we can check or uncheck options. These options will change the behavior of MBSA. They are shown in the following image:



Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: Computer (this computer)

IP address: ___ . ___ . ___ . ___

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

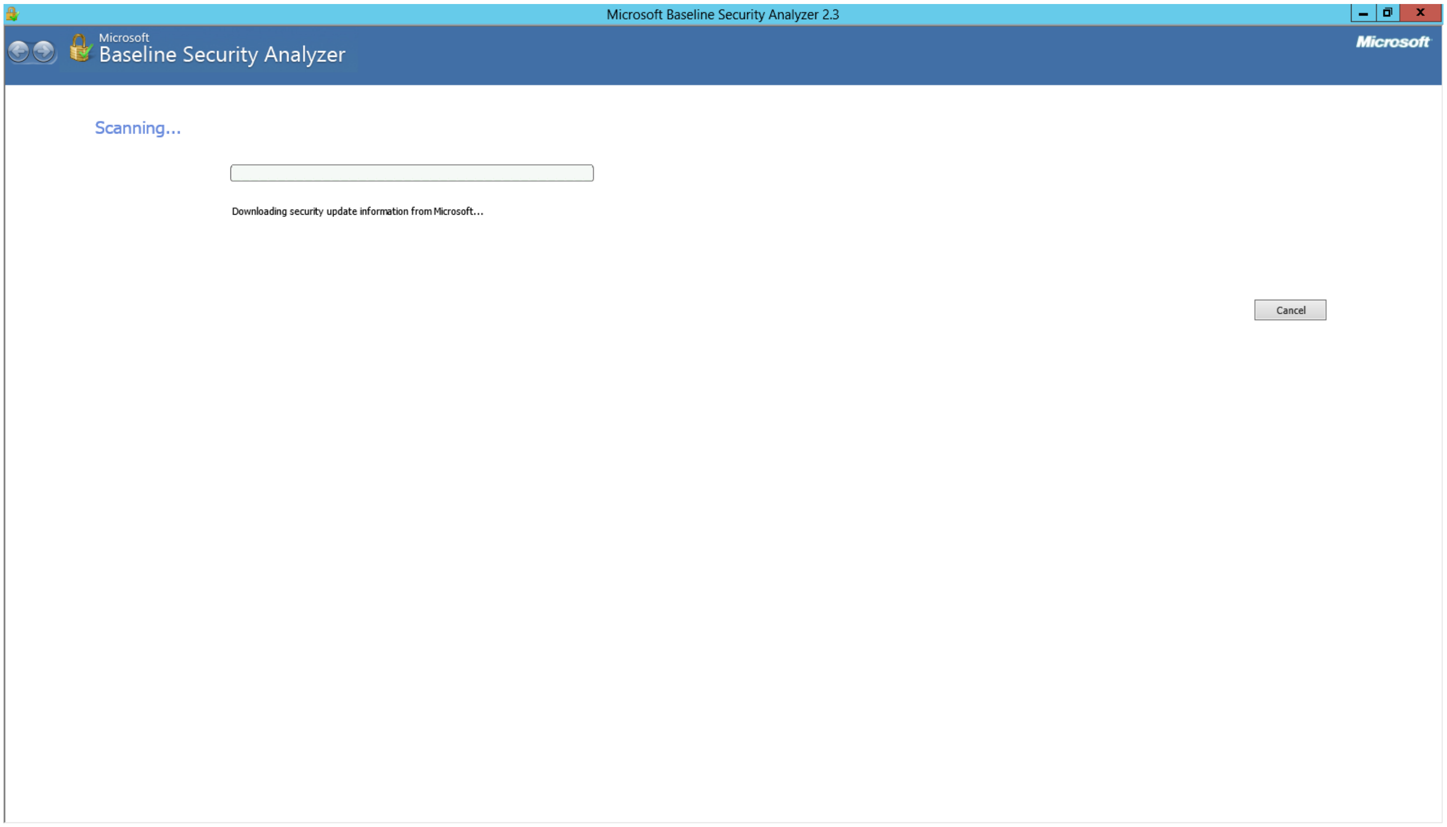
Options:

☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
  □ Configure computers for Microsoft Update and scanning prerequisites
  □ Advanced Update Services options:
    ○ Scan using assigned Windows Server Update Services(WSUS) servers only
    ○ Scan using Microsoft Update only
    ○ Scan using offline catalog only

Learn more about Scanning Options

Once everything is set up appropriately, you’ll find a button at the bottom right of the screen called “Start scan”. Just click on it.

Here we go. The process can take several minutes.



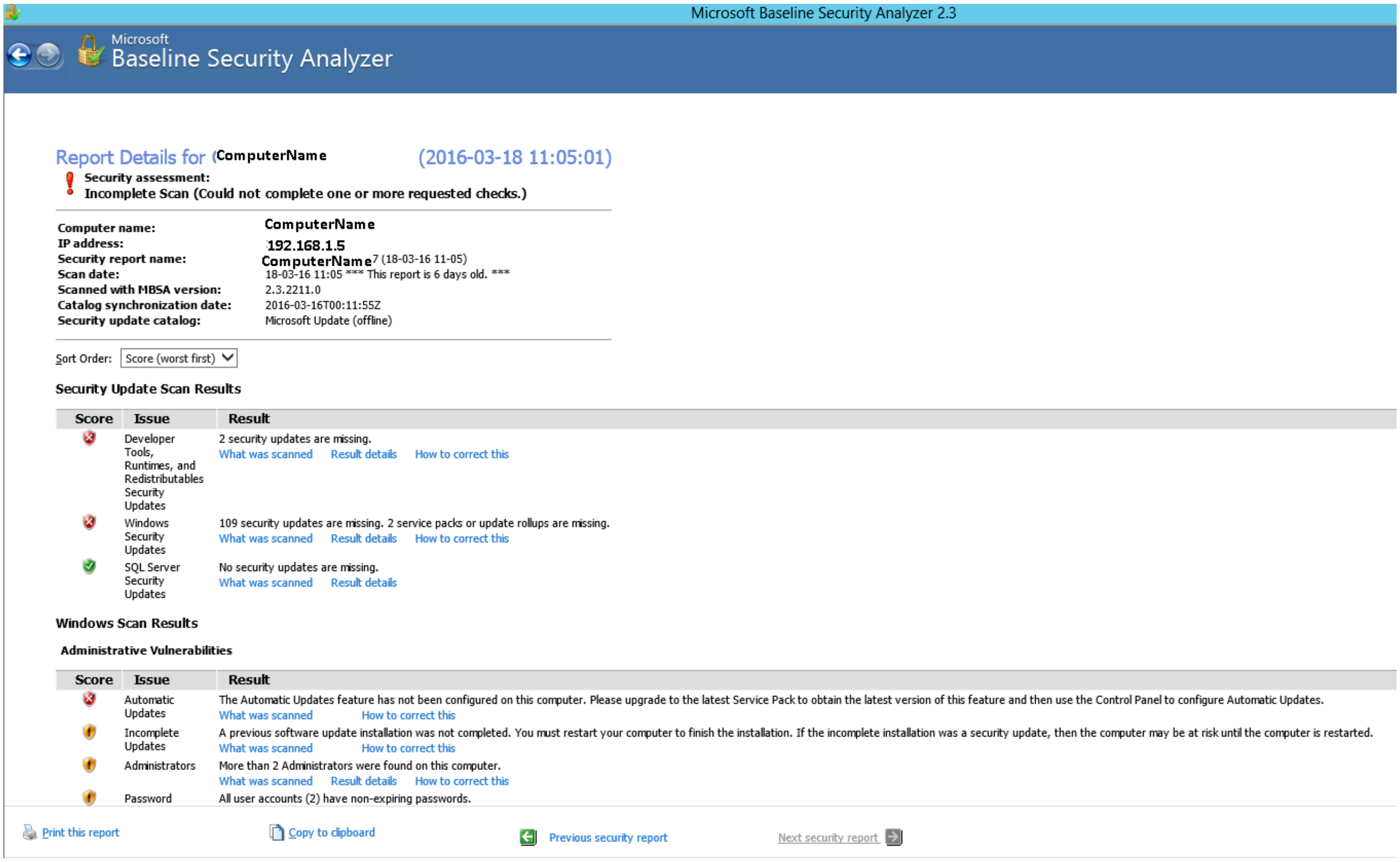
Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer

Scanning...

Downloading security update information from Microsoft...

It took approximately 10 minutes to complete without taking that much memory (16 MB) or CPU (0%).



Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer

Report Details for (ComputerName (2016-03-18 11:05:01)

! **Security assessment:**
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	ComputerName
IP address:	192.168.1.5
Security report name:	ComputerName7 (18-03-16 11-05)
Scan date:	18-03-16 11:05 *** This report is 6 days old. ***
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	2016-03-16T00:11:55Z
Security update catalog:	Microsoft Update (offline)

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
✗	Developer Tools, Runtimes, and Redistributables Security Updates	2 security updates are missing. What was scanned Result details How to correct this
✗	Windows Security Updates	109 security updates are missing. 2 service packs or update rollups are missing. What was scanned Result details How to correct this
✓	SQL Server Security Updates	No security updates are missing. What was scanned Result details

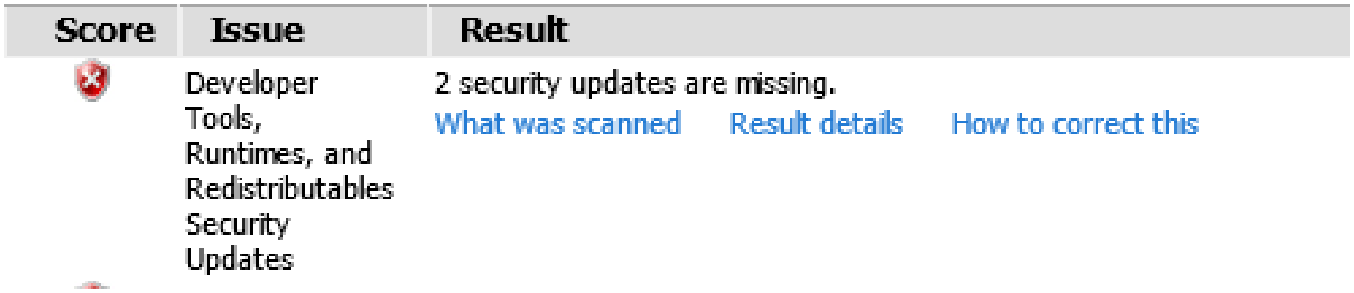
Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
⚠	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
⚠	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
⚠	Password	All user accounts (2) have non-expiring passwords.

I have to go through the whole report as it’s not an all green “everything is OK” message that is given by MBSA.

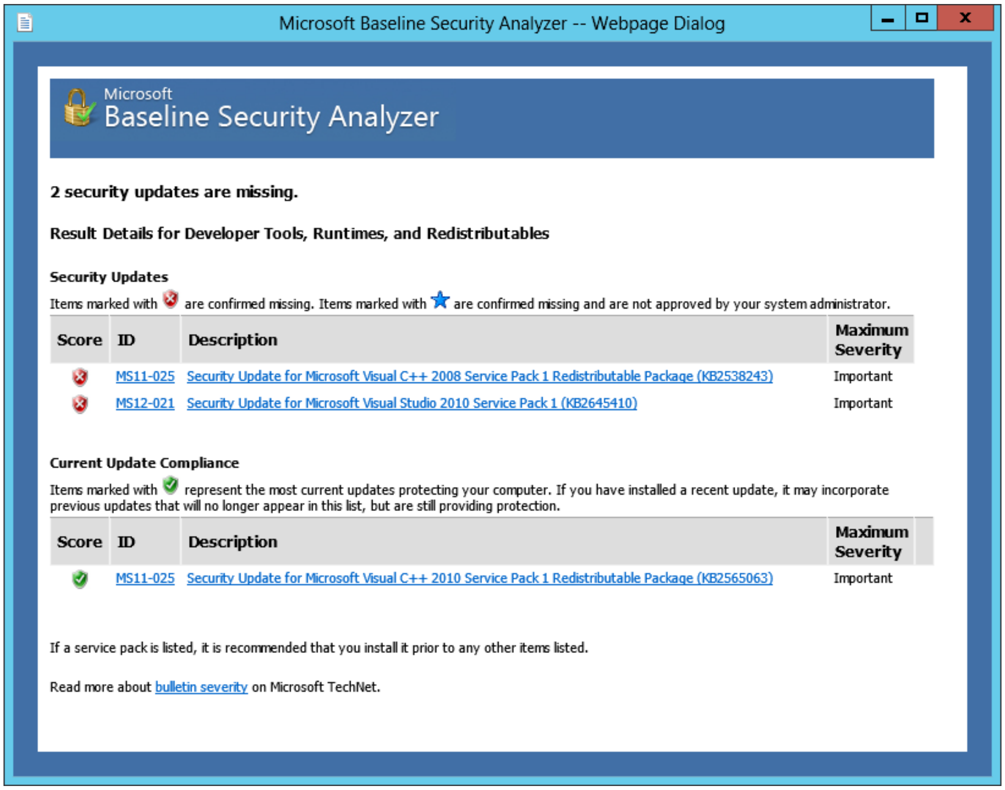
One thing we can see is that the report is organized by default with “worst first” which is to me very valuable. The next thing that is really helpful is that for every scan issue, we can see at least what was scanned, in some cases a detailed report may be accessible and/or eventually a way to correct the issue:



Score	Issue	Result
✗	Developer Tools, Runtimes, and Redistributables Security Updates	2 security updates are missing. What was scanned Result details How to correct this

The “What was scanned” link opens an HTML description of the scanned aspect.

The “Result details” presents a detailed report of the analysis made by MBSA. For example, you will find this dialog displayed:



Microsoft Baseline Security Analyzer -- Webpage Dialog
Microsoft
Baseline Security Analyzer

2 security updates are missing.

Result Details for Developer Tools, Runtimes, and Redistributables

Security Updates

Items marked with ✗ are confirmed missing. Items marked with ★ are confirmed missing and are not approved by your system administrator.

Score	ID	Description	Maximum Severity
✗	MS11-025	Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	Important
✗	MS12-021	Security Update for Microsoft Visual Studio 2010 Service Pack 1 (KB2645410)	Important

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
✓	MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Important

If a service pack is listed, it is recommended that you install it prior to any other items listed.

Read more about bulletin severity on Microsoft TechNet.

The last thing we can see in the report, are the actions that we can do on the report, as shown at the bottom of the window:

- Print the report
- Copy the report to clipboard
- Switch to another report

Other ways to run the tool: command-line

As the description stated, there is a command-line interface for the tool. Let's introduce "mbsacli". To run it, we have to open an invite or a Power Shell window and go to the installation directory of MBSA (or adapt PATH environment variable so that this folder is included).

Here is a sample command I used to run against a remote server:

```
.\mbsacli.exe -target CHULG\si-s-serv236 /n os+sql+updates+password /qt /nd
```