# Assignment #3.

|  |
| --- |
| Instructions:  - Show the results using screen shots or by describing the results. Follow the instructions in RED.  - Submit via BB and bring a hard copy to the class.  - Individual or group work (one submission per team)  - Due date: Feb 13, 2012, 5:30 pm (late submission accepted w/ penalty) |

# EX1. CIS-CAT Scoring Tool

The class uses the tool by the courtesy of The Center for Internet Security (CIS). This trial version expires in 30 days.

CIS-CAT is a scoring tool that allows administrators to assess a system’s security status using a predefined template.

- Trial Version can be downloaded from the following link.

<http://community.cisecurity.org/trial/?code=a3efd0fc1f5721995143c378bcbac8db>

- Also, the downloaded file is posted on BB.

## Profiles

|  |  |
| --- | --- |
| **Title** | **Description** |
| Enterprise Domain | Settings in this level are designed for systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows XP SP3 or later and Windows Server 2003 SP2 of later. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls. |
| Enterprise Desktop | Settings in this level are designed for systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows XP SP3 or later and Windows Server 2003 SP2 of later. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls. |
| Enterprise Laptop | Settings in this level are designed for systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows XP SP3 or later and Windows Server 2003 SP2 of later. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls. |
| SSLF Domain | Settings in this level are designed for systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment. |
| SSLF Desktop | Settings in this level are designed for systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment. |
| SSLF Laptop | Settings in this level are designed for systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment. |

\* SSLF: Specialized Security Limited Functionality

## Installing CIS-CAT

- To install CIS-CAT, you need to install Java Runtime Environment (JRE) first. For the latest JRE, go to the following websites:

<http://www.cnet.com/1770-5_1-0.html?query=jre&tag=srch>

or

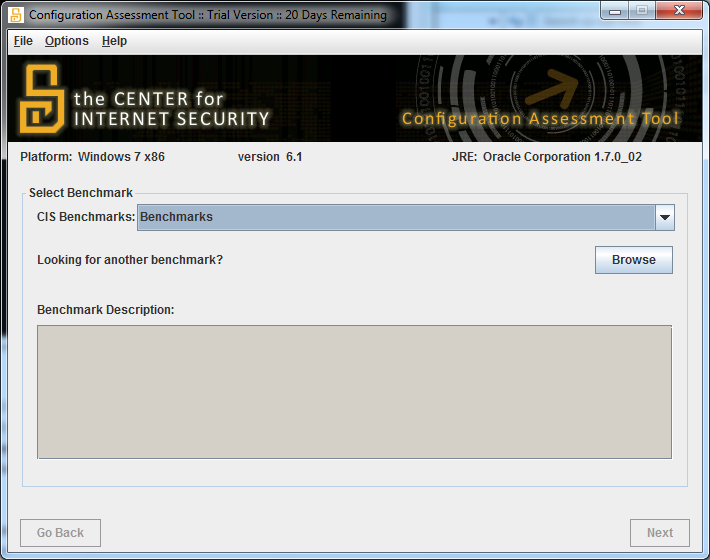
<http://www.oracle.com/technetwork/java/javase/downloads/jre-7u2-download-1377135.html>

- To install CIS-CAT, simply unzip the archive. No further action is required.

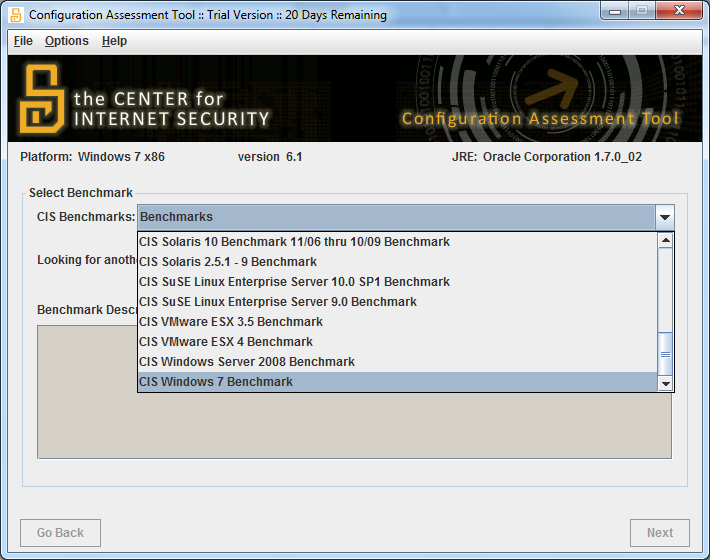
## Using CIS-CAT within a Graphical User Interface (GUI)

1. To execute CIS-CAT in a GUI environment, simply double click on CIS-CAT.jar.
2. Note: If the system has an archive manager associated with .jar files, you will need to double click on CIS-CAT.sh for Unix and Linux systems or CIS-CAT.bat for Windows systems. This will cause the following dialog to appear:

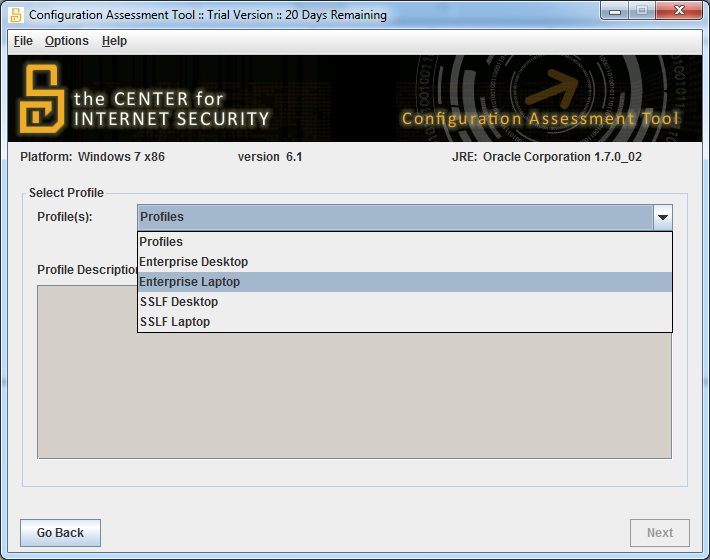
For me, either option works fine in launching the tool.



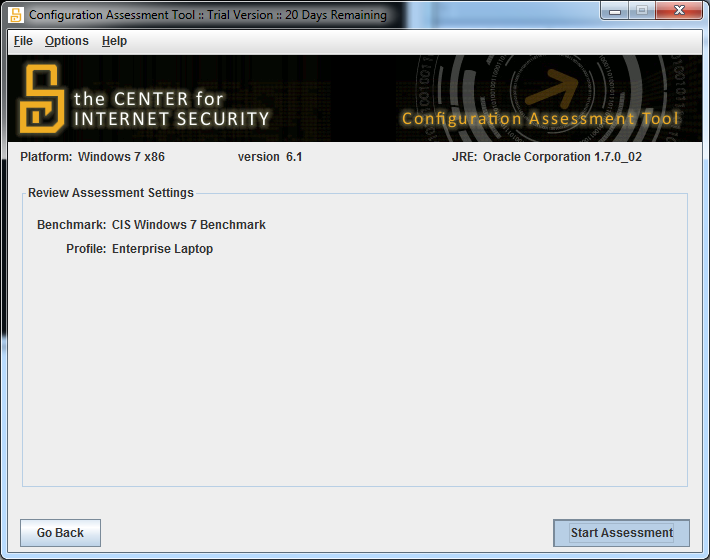
- Select the benchmark that fits your system.



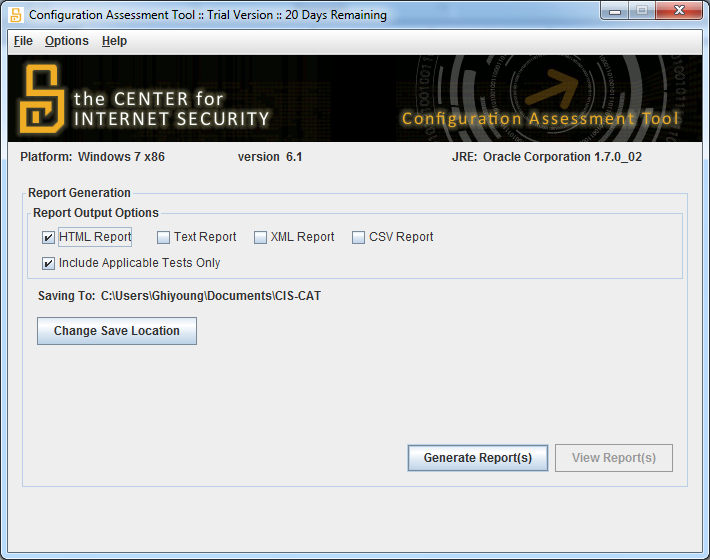
- Select the Enterprise profile. The details of each profile are provided above.



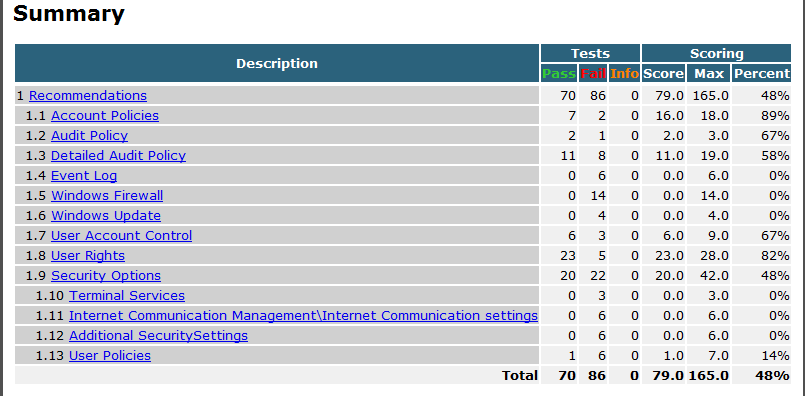
- Start the assessment.



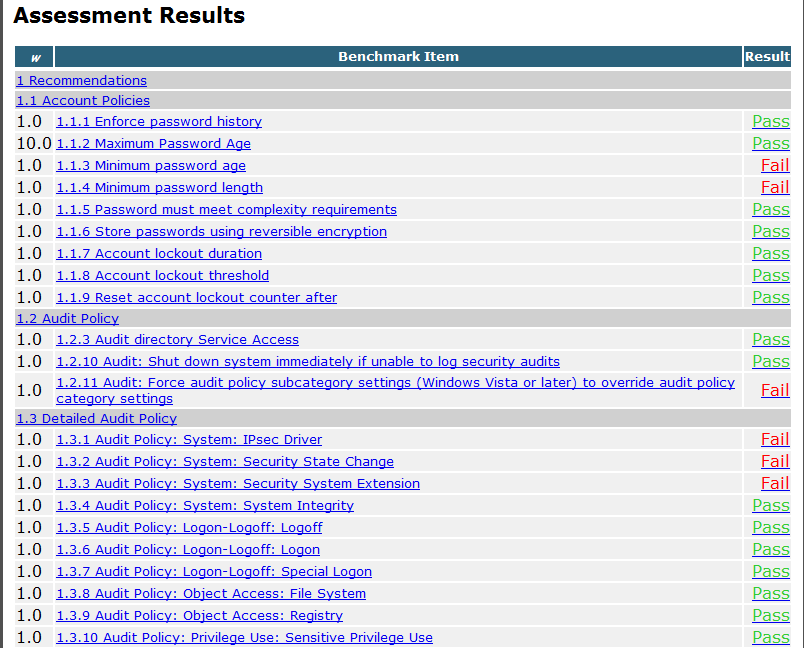
- Generate the report.



- Here is a summary of the report.



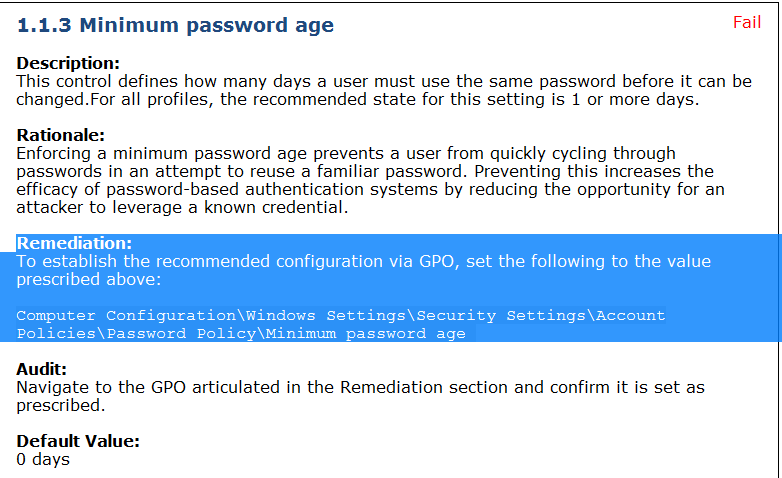
- Here are the details of the assessment results.



- Select one benchmark item from the category 1.1 (Account Policies) that has the benchmark result of “Fail.” Then, follow the remediation procedure listed in the benchmark result (see the next screen for example) and change the setting to the recommended default value.

- And rerun the assessment. In this case, you need to close out CIS-CAT and re-run it for the change to take effect.

- Report the summary before and after the change (this can be screen shots). Also, describe the change you have made to the system. After the assessment, restore to the original setting for safety. If you are 100% sure of the change, leave the setting as it is.



# EX2. Security Configuration and Analysis (SCA)

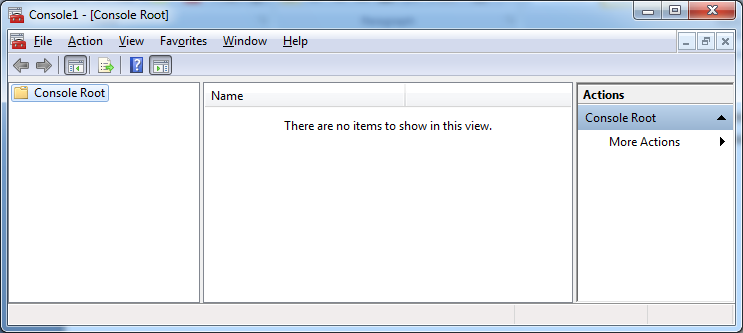
SCA is a snap-in in MMC that allows administrator to roll out predefined security templates. It comes with default templates that are provided by Microsoft. In my system (Windows 7 Professional), the templates are located in the following.

C:\Users\Ghiyoung\Documents\Security\Templates

## Installing CIS-CAT

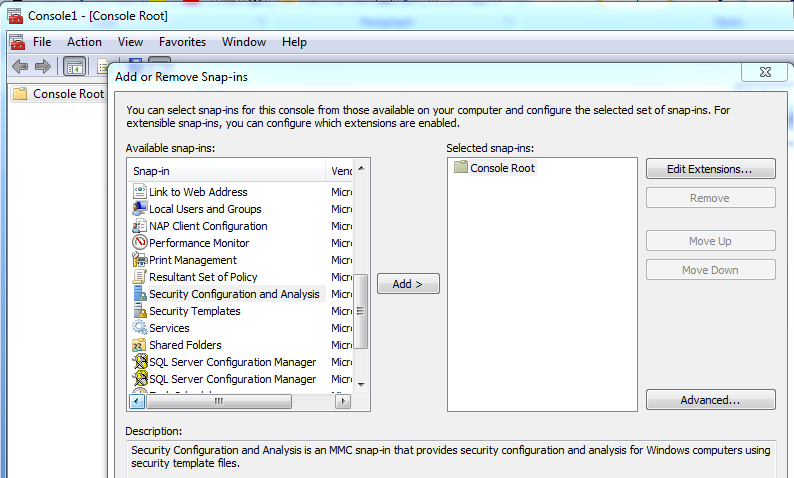
- Start / Run / type **MMC**

**- If you can’t use MMC in your computer, you need to find a computer that runs MMC. Windows XP Professional and Windows 7 Professional run MMC. I think Windows 7 Home Premium doesn’t allow running MMC.**



- On Console Root, File / Add/Remove Snap-in

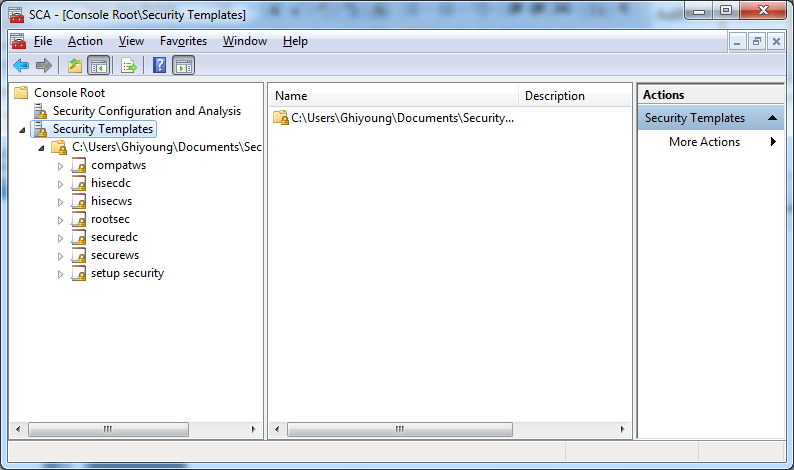
- Add “Security Configuration and Analysis” and “Security Templates” / OK



- You should save before going any further.

- Save the file on the Desktop: File / Save As / SCA.msc / Save

- The following security templates are displayed.



## Predefined Security Templates

**If you can’t find the predefined security templates in the above screen, go to BB. I posted mine. You can use them.**

Compatible (Compatws.inf)

“Default permissions for workstations and servers are primarily granted to three local groups: Administrators, Power Users, and Users.”

Highly Secure (hisec\*.inf)

“The Highly Secure templates are supersets of the secure templates that impose further restrictions on the levels of encryption and signing that are required for authentication and for the data that flows over secure channels and between SMB clients and servers.”

Secure (Secure\*.inf)

“The Secure templates define enhanced security settings that are least likely to impact application compatibility.”

\* Source: <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_scedefaultpols.mspx?mfr=true>

Administrators can configure the following security areas.

|  |  |
| --- | --- |
| **Area** | **Configurable Items** |
| Account Policies | Password, lockout, and Kerberos policies |
| Local Policies | Audit, user rights, and security options |
| Event Log | Log size, guest group, application, security and directory service logs |
| Restricted Groups | If placed in this group, a group cannot have new members added |
| System Services | Startup modes for system services (Automatic, Manual, or Disabled). |
| Registry | Access control for registry keys. |
| File System | Access control for folders and files. |

Let us select “hisecdc.inf” and examine the settings.

The settings you see are the ones in the template, NOT on your system.

## Analyzing your system using the template

Select the template (hisecdc.inf) to analyze your system.

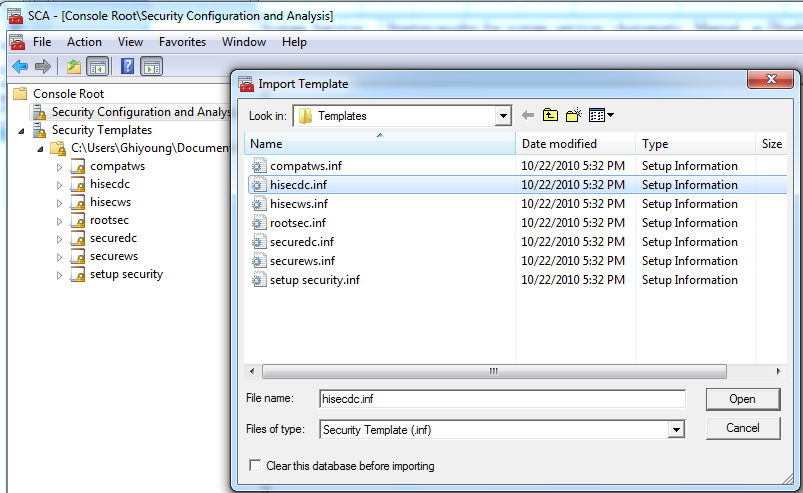
First, you need to create a new database.

- Right-click the Security Configuration and Analysis scope item

- Click Open Database

- In the file name field, type **analysis.sdb**. In my case, the default directory for the database is “C:\Users\Ghiyoung\Documents\Security\Database.” Change the directory if necessary.

- click Open



- In Import Template, select **hisecdc.inf**.

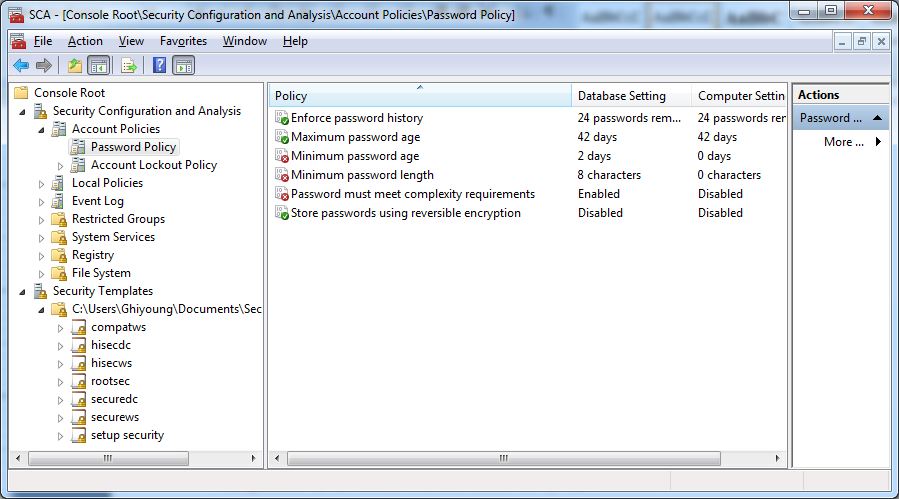
- Right-click the Security Configuration and Analysis scope item

- Select Analyze Computer Now.

\*\*\*VERY IMPORTANT: Don’t try Configure Computer Now. You may be locked out after the configuration. In this case, you need to format the system. There is NO UNDO.

- In the dialog, type the log file path, and then click OK

- Summarize what you have found for “Account Policies” (password and account lockout policies) after the analysis. Include a screen shot and describe briefly the analysis results.



# EX3. Microsoft Baseline Security Analyzer (MBSA)

- MBSA is used to determine patch levels, vulnerabilities, and security holes in applications.

- MBSA can be downloaded from the following site:

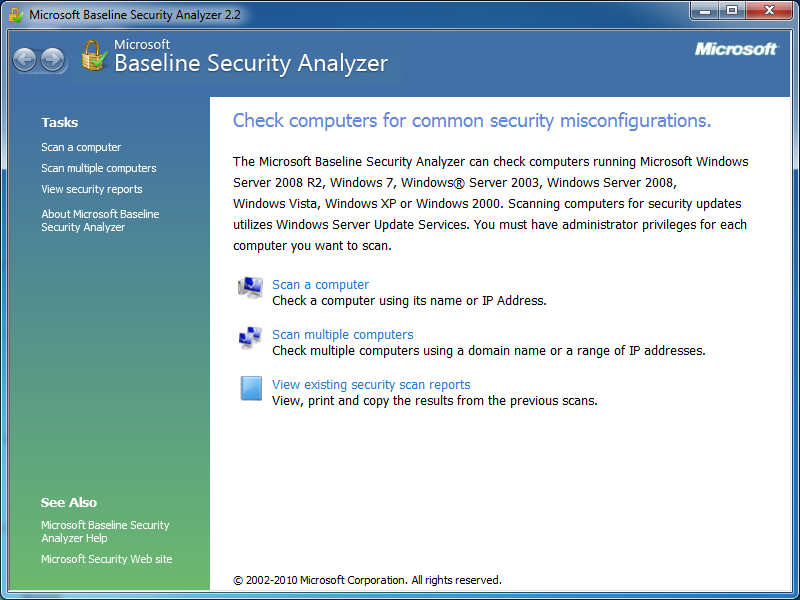
<http://www.microsoft.com/download/en/details.aspx?id=7558>

## Installing MBSA

- Install following the instructions on the screen.

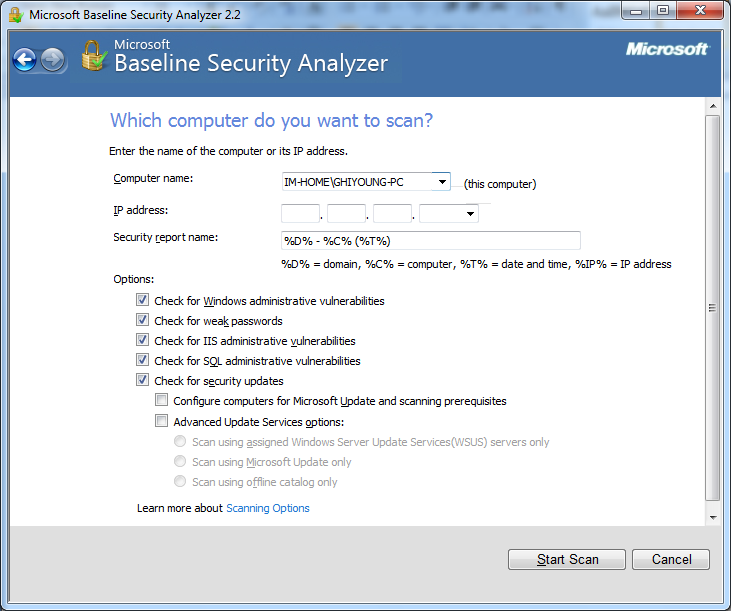
## Running MBSA

- Click on the MBSA icon.



- Select **Scan a computer**.

- Accept the default values and Start Scan.



- Report the results: 1) include a screen shot of the result (only the beginning part), and 2) summarize the results that have the Critical score (Check failed (critical)).