

INFO6003 LAB-06 MBSA, BPA and SCW

Preparation

If you didn't take them last week, take a snapshot, called After Lab-05, of both your W7 and 2008R2 VMs

- We will be using the **(W7 or Win 10) and 2008R2 VMs from previous labs. Or optionally use Server2016**
 - W7 VM must have both Host Only and NAT adapters
- Use the **Domain Admin** account to logon to the W7 VM

MBSA Install (Windows 7 VM)

- Download the Microsoft Baseline Security Analyzer **version 2.3** to the Windows 7 VM
 - You can get it from a google search. Download the 32 bit version.
 - **MBSASetup-x86-EN.msi**
- Run the MBSA installer using the default options. After the installation completes start MBSA.
 - If you get an error, you probably don't have the 32 bit version, x86

MBSA GUI

- When MBSA starts you receive the following options:
 - Scan a computer
 - Scan multiple computers
 - View existing security scan reports
- Select **scan a computer**
 - By default the local system should already be listed next to the Computer name field.
 - You could also enter the IP address of the device.
 - Look at the scanning options available to you in the **Learn more about** section.
- Leave the default options checked and in addition, select **Configure Computers for Microsoft Update and scanning prerequisites**
- This ensures the Windows Update Agent is current and you get a proper scan
- Ensure that your system's name is listed as the Computer Name and then click **Start Scan**.
 - You don't need to enter an IP Address
- When the scan starts the tool will connect to Microsoft to get updated security information, after the download is complete, the scan will start automatically. **This will take several minutes**.
 - If this doesn't take a while, you probably have lost connectivity to the internet on your host computer

Slide 1: take a screenshot of the top of the results page. Make sure you include your computer name and some of the Security Update Scan Results

Note: There is a sample screenshot on the following page.

Report Details for SMILEY - W7-ISMILEY2 (2015-03-03 11:43:21)



Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name: SMILEY\W7-ISMILEY2
IP address: 10.0.0.50
Security report name: SMILEY - W7-ISMILEY2 (3-3-2015 11-43 AM)
Scan date: 3/3/2015 11:43 AM
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date:
Security update catalog: Microsoft Update

Sort Order:

Security Update Scan Results

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	1 security updates are missing. What was scanned Result details How to correct this

Scan Results

- By default, the worst problem is displayed first in the results. You can change the report listing by changing the Sort Order (top of report).
- Spend some time looking at the issues reported. In practice the report will be different on each computer based on the local security settings and update state.
- Note some of the security areas summarised:
 - Windows Security Updates
 - Automatic updates
 - Password expirations
 - Windows Firewall
 - File System

Questions:

Note: To answer the following questions you will need to look at the result details for individual results.

- What accounts failed the **password expiration** check?


Password Expiration All user accounts (6) have non-expiring passwords.
[What was scanned](#) [Result details](#) [How to correct this](#)

- Did any accounts pass the password expiration check?
- What is the status of the windows firewall?
- What is the result of the Local Account Password Test?
- Is autologon set for this system?
- Is the guest account enabled?
- Are there multiple administrators on this system?
- Are there any potentially unnecessary services running on this system?
- What shares are available on the system?
- When you are done reviewing the report, go to the **Windows Security Updates** entry and click **Result details**.
- The Results Detail Windows lists each missing security update.
 - The security updates are listed in numerical order by security bulletin number.


- The ID and Description fields are links to the security bulletins, from these links you can get more information and install the update.
- If you click through for one of the updates, it will take you to a site that should look familiar
- Scroll through the list to view the severity levels of the updates.
- The range is from critical to low. **(you can find more information about these levels through the link at the bottom of the screen)**
- Close the details window and open the results details for Password Expiration
 - If your system is configured correctly, you should have six accounts, all with password expiration errors
 - Close the windows, then click **How to correct this** to learn how to fix this problem
 - **Fix the problem for both User-Admin and User-Limited**
 - Hint: you are trying to **manage** the **users** on your **computer**
- Once you have fixed the problem fixed **click OK** to close the report window
- **Because we don't need the NAT network anymore, shut your VM down and configure your NAT network so that it doesn't connect at power on (uncheck the box)**
- Power the Windows 7 VM back up and logon as the domain admin
- Open MBSA
 - MBSA can also scan an entire network, a range of IP addresses, or an entire domain Choose to **scan multiple computers** from the main window.
 - Enter your domain name (you can find this with net config workstation if you forgot it)
 - To save time, only check for **Windows Administrative Vulnerabilities and Weak Passwords**
 - Start the scan. This should be quick, and should find two computers.
 - Open the W7 scan and open the results details window for Password Expiration

Slide 2: take a screenshot showing all the information you can see below

Report Details for smiley - W7-ISMLEY2 (2015-03-03 12:21:32)

 **Security assessment:**
Severe Risk (One or more critical checks failed.)





Microsoft Baseline Security Analyzer -- Webpage Dialog

 Microsoft
Baseline Security Analyzer

Some user accounts (4 of 6) have non-expiring passwords.

Result Details

Accounts with a green check have passwords that do not expire but were specified in NoExpireOk.txt

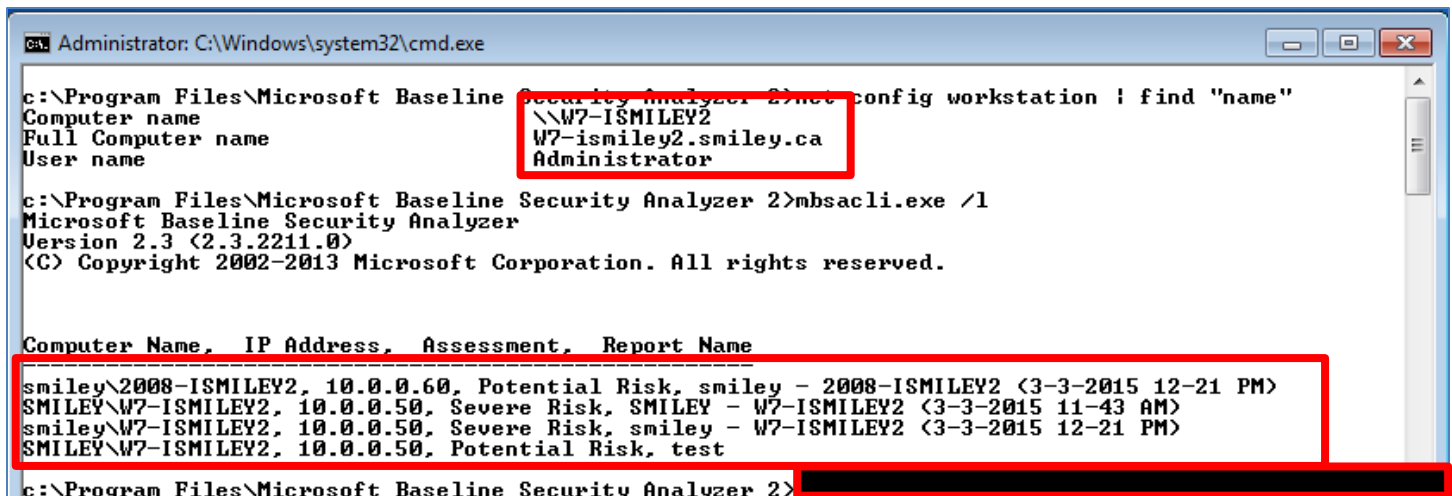
Score	User
	Administrator
	Guest
	HomeGroupUser\$
	User

Close MBSA.

MBSA Command Line Tool

- With the command line tool, scan results are output to the screen and can be stored as a text file.
 - These text files could be amalgamated and used in a security audit, proving to the auditor the security level of your systems
- Open a command line shell and **navigate to the directory with mbsaccli.exe**
 - Hint: MBSA is an installed program (you can also use search from My Computer to find it)
- Because the directory path is so long the output of our commands will scroll over onto the next line making it difficult to read
- To change this, right click on the title bar for your command prompt and edit the properties
 - Under layout, change the 2 100 entries to 120, the **Windows Height** to 40 and select OK
 - You may need to double click on the title bar to get the change to take effect.
- To see a list of command line options type **mbsaccli.exe /?**
 - Note the numerous options and example commands.
 - Find the options to limit the type of scans performed, to scan a computer by its IP and to specify an output filename (you will use these below)
- Build the command that will scan the local computer (W7) with the following options: **(You are building a single command with 3 options and 3 arguments)**
 - **IP of Windows 7 VM**
 - **Only scan for OS and Password problems, not IIS, SQL, or Updates**
 - **Output to an XML file called test.mbsa**
 - The scan should be pretty fast
 - Scroll through the information provided by mbsa
- To see a list of existing security scan reports type **mbsaccli.exe /l**

Slide 3: show the output of the net config workstation command (only showing lines with name), the mbsaccli /l command and the command you used to perform your scan (use the up arrow to find this)



```
Administrator: C:\Windows\system32\cmd.exe

c:\Program Files\Microsoft Baseline Security Analyzer 2>net config workstation /find "name"
Computer name          \\W7-ISMILEY2
Full Computer name     W7-ismiley2.smiley.ca
User name              Administrator

c:\Program Files\Microsoft Baseline Security Analyzer 2>mbsaccli.exe /l
Microsoft Baseline Security Analyzer
Version 2.3 (2.3.2211.0)
(C) Copyright 2002-2013 Microsoft Corporation. All rights reserved.

Computer Name, IP Address, Assessment, Report Name
-----
smiley\2008-ISMILEY2, 10.0.0.60, Potential Risk, smiley - 2008-ISMILEY2 (3-3-2015 12-21 PM)
SMILEY\W7-ISMILEY2, 10.0.0.50, Severe Risk, SMILEY - W7-ISMILEY2 (3-3-2015 11-43 AM)
smiley\W7-ISMILEY2, 10.0.0.50, Severe Risk, smiley - W7-ISMILEY2 (3-3-2015 12-21 PM)
SMILEY\W7-ISMILEY2, 10.0.0.50, Potential Risk, test

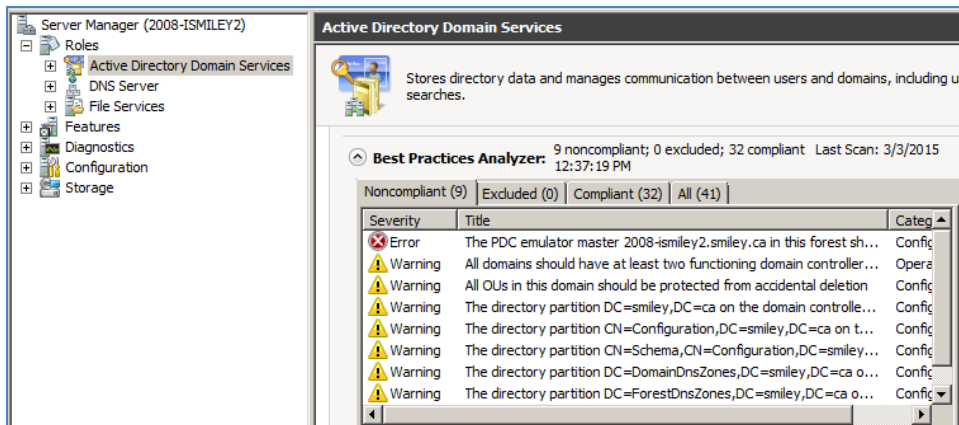
c:\Program Files\Microsoft Baseline Security Analyzer 2>
```

Note: It must show Server 2008 and Windows 7.

Best Practice Analyzer (Server 2008 R2 VM)

- Ignore the Windows is not genuine error if you get one
- If it isn't already open, open Server Manager and navigate to the Active Directory Domain Services Role
- Find and run the best practice analyzer for this role

Slide 4: show the results of the scan, make sure you include your computer name



Security Configuration Wizard

- Under Administrative Tools, open the Security Configuration Wizard
 - Choose to create a new security policy
 - Use your server as the baseline server
 - You can view the current settings in the configuration database
 - You will need to accept the ActiveX dialog
- Role Based Service Configuration (you won't be changing these settings)
 - You can choose to analyze Installed Roles, All Roles, or Uninstalled Roles or a Selection of Roles
 - We will analyze the installed roles
 - For each of the following dialogs you have similar choices for: features, options and additional services
 - We will accept the defaults, in production you would tailor this to you security policies
 - You can set how SCM will deal with services that aren't part of the policy
 - Accept the default
 - The next screen shows you the changes your current settings will trigger (accept them)
- Network Security (you won't be changing these settings)
 - Accept the defaults. These settings will affect your firewall rules.
- Registry Settings (you won't be changing these settings)
 - In Windows you can enable different security settings depending on how current your environment is. The next couple screens deal with letting SCW know what kind of an environment you have
 - Accept the defaults
 - The Registry Settings Summary page lets you see the changes SCW is going to make

- Audit Policy (**you are making a change in this section**)
 - This section controls the type of auditing that will be done
 - **Set it** to audit successful and unsuccessful activities

Slide 5: show the audit policy summary, include net config workstation lines with “name”

If applied to the selected server, this security policy would use the following auditing configuration:

Audit Event Type	Current Setting	Policy Setting
Account Logon Events	Not audited	Success, failure
Account Management	Not audited	Success, failure
Directory Service Access	Not audited	Success, failure
Logon Events	Not audited	Success, failure
Object Access	Not audited	Success, failure
Policy Change	Not audited	Success, failure
Privilege Use	Not audited	Not audited

Administrator: Command Prompt

```

C:\Users\Administrator>net config workstation ! find "name"
Computer name          \\2008-ISMILEY2
Full Computer name     2008-ismiley2.smiley.ca
User name              Administrator
C:\Users\Administrator>
  
```

- Save your policy in the default folder as INFO6003 and choose to apply it later

Convert The Policy to a GPO

- Open a command shell and navigate to the C:\Windows\security\msscw\Policies\ directory
- Use the **scwcmd transform /?** command to see how this command works
- Build the command to convert your **INFO6003.xml** Policy to a **INFO6003** GPO
 - Make sure it runs successfully
- Open the Group Policy Management Console and display the settings for the INFO6003 GPO you just created (show all)

Slide 6: show your domain, the INFO6003 GPO and the audit policy settings

Group Policy Management

Forest: smiley.ca

- Domains
 - smiley.ca
 - Default Domain Policy
 - WSUS
 - Domain Controllers
 - INFO6030
 - Group Policy Objects
 - Default Domain Contro
 - Default Domain Policy
 - INFO6030
 - WSUS
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

INFO6030

Scope | Details | Settings | Delegation

INFO6030
Data collected on: 3/3/2015 12:45:49 PM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Take a snapshot of both VMs called After Lab-06