Intro to Cybersecurity

3.1.2 – MBSA Vulnerability Scan

GALANTECH —with— GARDEN STATE CYBER

CYBER.ORG

Getting Started

- In this lab we will perform an initial vulnerability assessment on Windows OS systems using the Microsoft Baseline Analyzer (MBSA) tool
- An MBSA scan will identify security updates and common security misconfigurations for a Windows OS device

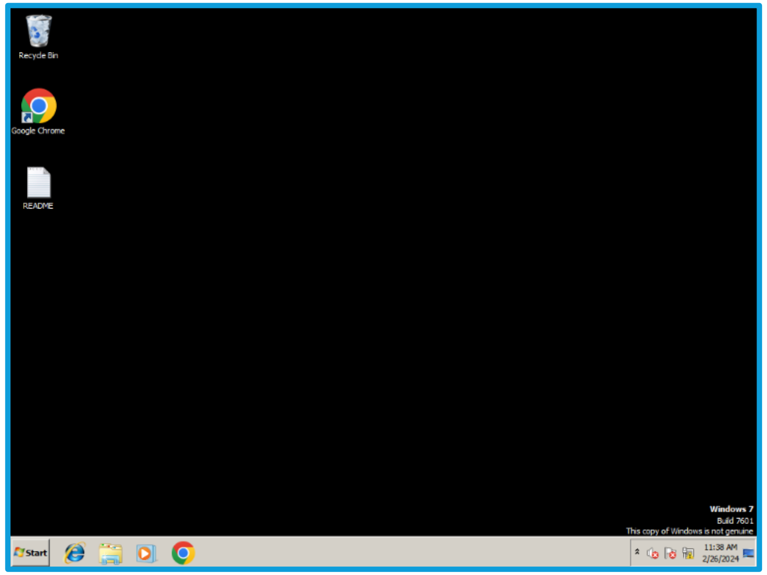
MBSA Vulnerability Scan Lab

- Materials needed
  - Windows 7 Virtual Machine

- Software Tools used
  - MBSA

Setup Environment

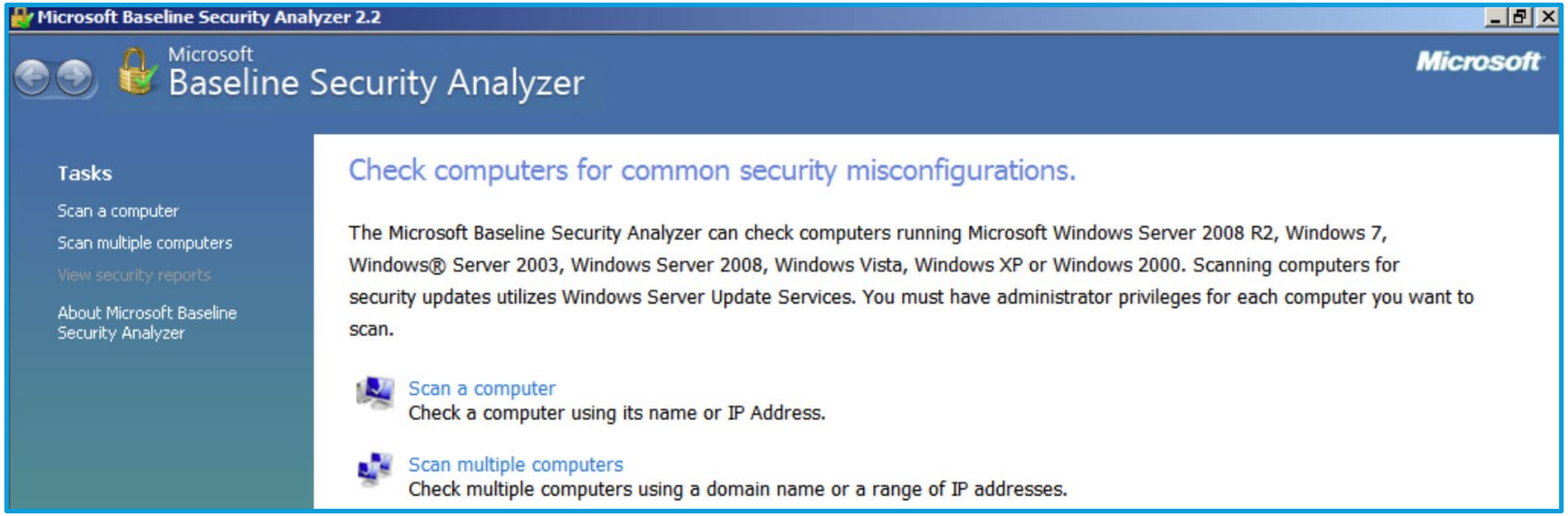
- Log into your range
- Open the Windows 7 Environment
  - You should be on your Windows 7 Desktop



Windows 7
Build 7601
This copy of Windows is not genuine

Launch MBSA

- Click “Start | All Programs | Microsoft Baseline Analyzer 2.2”
- Select Yes on the UAC window that appears
- On the main page, select Scan a Computer


Microsoft Baseline Security Analyzer 2.2
Microsoft
Baseline Security Analyzer
Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer

Check computers for common security misconfigurations.

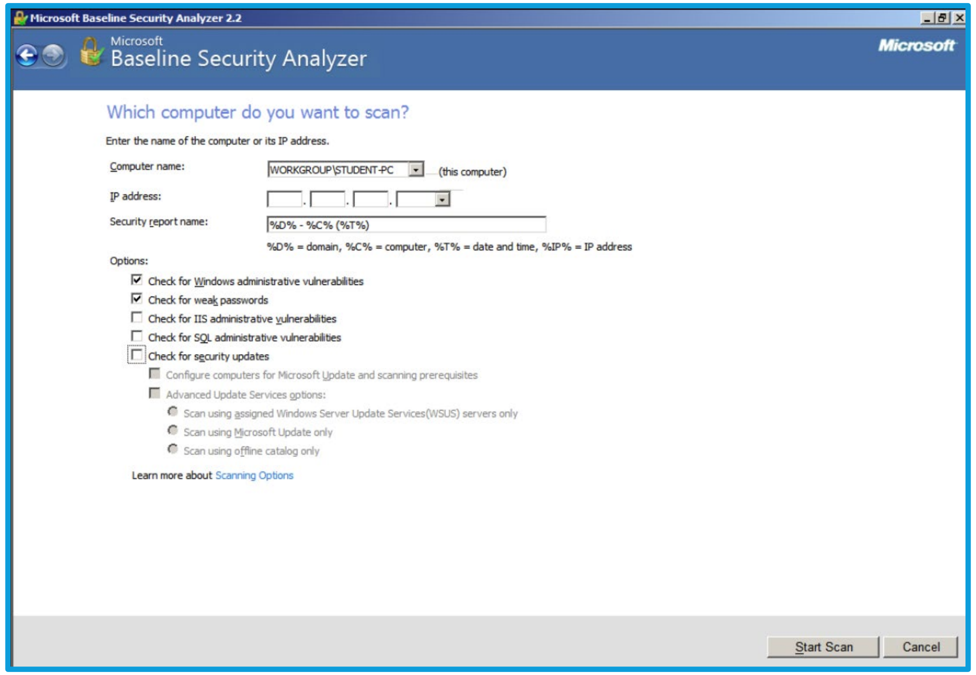
The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, Windows XP or Windows 2000. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator 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.

Running the Scan

- For Which computer do you want to scan?, accept the defaults
- Under Options, check ONLY the top 2 boxes
- Click Start Scan
  - This may take 2 – 3 minutes


Microsoft Baseline Security Analyzer 2.2
Microsoft
Baseline Security Analyzer
Microsoft
Start Scan
Cancel

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: WORKGROUP\STUDENT-PC (this computer)

IP address: . . .

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

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

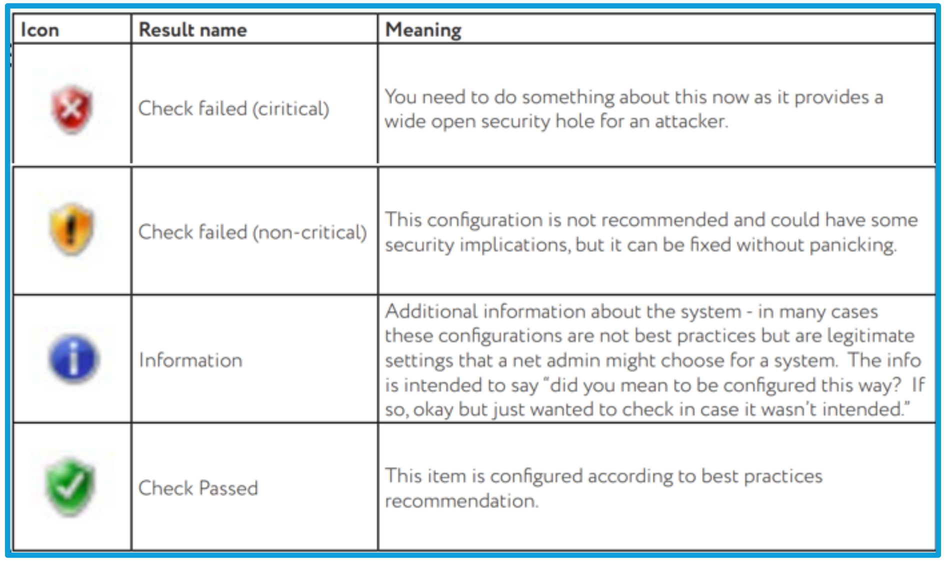
Options:

- ☑ 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

Viewing the Results

- The scan will deliver results sorted with the highest risk items at the top
- Each reported item has an icon that indicates the level of risk



Icon	Result name	Meaning
✗	Check failed (ciritical)	You need to do something about this now as it provides a wide open security hole for an attacker.
!	Check failed (non-critical)	This configuration is not recommended and could have some security implications, but it can be fixed without panicking.
i	Information	Additional information about the system - in many cases these configurations are not best practices but are legitimate settings that a net admin might choose for a system. The info is intended to say "did you mean to be configured this way? If so, okay but just wanted to check in case it wasn't intended."
✓	Check Passed	This item is configured according to best practices recommendation.

Viewing the Results cont’d

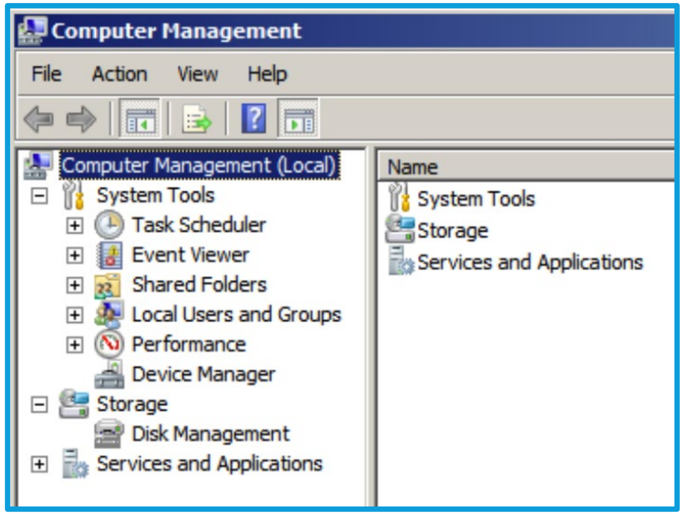
- Use the scan results to answer questions and mitigate vulnerabilities on the system
- Which issues have Check Failed (Critical) score results?
- Which user accounts have weak passwords?
- What are the Administrative Vulnerabilities that are categorized as Check Failed (Non-Critical)?
- Which users are listed as having a password that doesn’t expire?
- What users are identified as Administrators?
- Are there any potentially unnecessary services installed?
- What is the status of the Firewall?

Mitigating Identified Vulnerabilities

- Click the X in the upper right to close MBSA Vulnerability Scan
- Turn on Automatic Updates
    - Type “updates” in the Search field under the Start button
    - Select Windows Updates
    - Click Turn On Automatic Updates
        - You will get a notification “Windows could not search for new updates.” This is because Windows 7 is out of support but the setting for Automatic Updates is now correct
    - Close the update window

Mitigating Identified Vulnerabilities

- Correct User-base vulnerabilities
  - Type “Computer” in the Search field under the Start button
  - Select Computer Management
  - In the left column click to select Local Users and Groups
  - In the right column double-click on the Users folder
  - Secure Guest Account
    - Right-click on the Guest account
    - Select Properties
    - Click to check Account is Disabled
    - Click OK



Mitigating Identified Vulnerabilities

- Correct User-base vulnerabilities
  - Secure Guest Account
    - Right-click on the windows account
    - Select Set Password
    - Click Proceed
    - Enter P@ssword! in New Password and Confirm Password
    - Click OK
    - Do the same password changing step for the Infosec account

Mitigating Identified Vulnerabilities

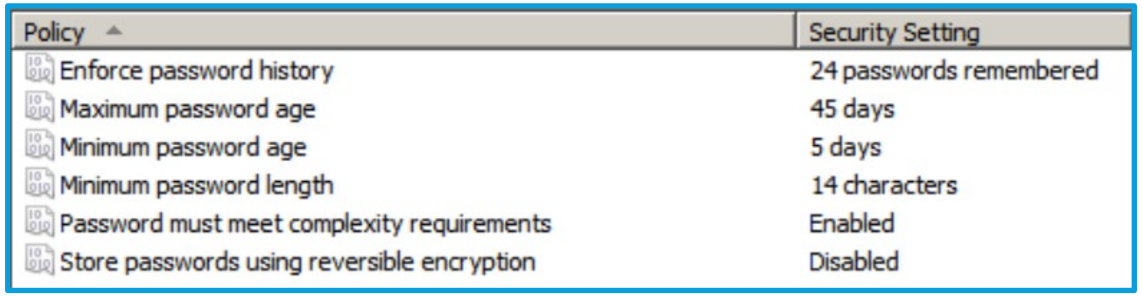
- Correct User-base vulnerabilities
  - Secure Guest Expirations
    - Right-click on the windows account
    - Select Properties
    - Click to uncheck Password Never Expires
    - Click Apply then OK
    - Do the same password expiration steps for the Administrator account and the Infosec account

Mitigating Identified Vulnerabilities

- Correct User-base vulnerabilities
  - Secure Administrator Group
    - In the left column click to select Local Users and Groups
    - Select the Groups folder
    - Double-click on Administrators to open this group
    - Click to select BackupAdmin
    - Click on Remove
    - Click to select Infosec
    - Click on Remove
    - Click OK
  - Close the Computer Management window

Mitigating Identified Vulnerabilities

- Correct Local Policy settings
  - Type “Local” in the Search field under the Start button
  - Select Local Security Policy
  - Configure Policy for strong passwords
    - In the left column click on Account Policies
    - In the right column double-click on Password Policy
    - Change each setting to match the following



Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	45 days
Minimum password age	5 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Mitigating Identified Vulnerabilities

- Correct Local Policy settings
  - Configure Policy for secure logon
    - In the left column click on Local Policies
    - In the right column double-click on Security Options
    - Scroll down to Network Access: Let Everyone permissions apply to anonymous users
    - Double-click to open and change to Disabled
    - Click OK
  - Close Local Security Policy window

Mitigating Identified Vulnerabilities

- Secure running services
  - Type “Services” in the Search field under the Start button
  - Select Services
  - Scroll down to the bottom and double-click World Wide Web Services
  - Click Stop then change the field from Automatic to Disabled
  - Click OK
  - Close the Services window

Mitigating Identified Vulnerabilities

- Turn off Autologon
  - Type “netplwiz” in the Search field under the Start button
  - Select to open
  - Click to check the box “Users must enter a username and password to use this computer”
  - Click OK to close the User Accounts window

Rescanning to Confirm Changes

- Click “Start | All Programs | Microsoft Baseline Analyzer 2.2”
- Select Yes on the UAC window that appears
- On the main page, select Scan a Computer
- For Which computer do you want to scan?, accept the defaults
- Under Options, check ONLY the top 2 boxes
- Click Start Scan
- Your results should now show all vulnerabilities corrected EXCEPT the HOMEUSER$ has a non-expiring password
    - This setting is needed for the virtual environment.