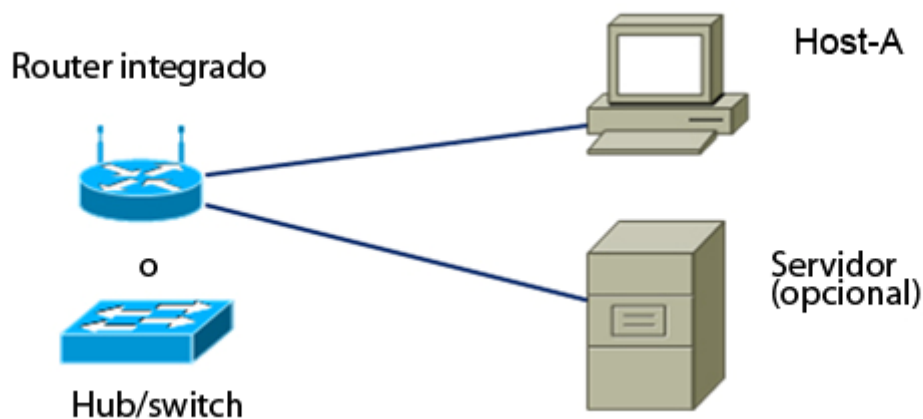


Práctica de laboratorio 8.4.3 Realización de un análisis de vulnerabilidad

PRECAUCIÓN: Es posible que este laboratorio no cumpla con las políticas de seguridad legales y de la organización. El analizador de seguridad descargado en este laboratorio sólo se debe utilizar con fines instructivos en el entorno del laboratorio. Antes de utilizar un analizador de seguridad en una red activa consulte con el instructor y el personal de administración de redes las políticas internas relacionadas con el uso de estas herramientas.



Objetivos

- Descargar e instalar el software del analizador de seguridad.
- Probar un host para determinar las vulnerabilidades de seguridad potenciales.

Información básica / Preparación

Los analizadores de seguridad son herramientas valiosas que utilizan los auditores y los administradores de redes para identificar vulnerabilidades de la red y de los hosts. Hay muchas herramientas de análisis de vulnerabilidades disponibles para probar la seguridad de las redes y los hosts. En este laboratorio descargará e instalará Microsoft Baseline Security Analyzer (MBSA). MBSA está diseñado para identificar problemas de seguridad potenciales relacionados específicamente con los sistemas operativos, las actualizaciones y las aplicaciones de Microsoft. También identifica los servicios innecesarios que están en ejecución y los puertos abiertos.

MBSA se ejecuta en sistemas Windows Server y Windows XP, y busca errores comunes de configuraciones de seguridad y actualizaciones de seguridad faltantes para el sistema operativo y la mayoría de las versiones de Internet Information Server (IIS), SQL Server, Internet Explorer (IE) y productos de Office. MBSA ofrece recomendaciones específicas para corregir problemas potenciales.

Este laboratorio se puede llevar a cabo de manera individual o en grupos de dos.

Se necesitan los siguientes recursos:

- Una computadora con Windows XP Professional para que actúe como estación de prueba.
- Una conexión a Internet de alta velocidad para descargar MBSA (a menos que se haya instalado previamente).

- La computadora debe estar conectada al switch del router integrado o a un hub o switch independiente.
- De manera opcional, puede disponer de un servidor que ejecute una combinación de DHCP, HTTP, FTP y Telnet (configurados previamente).

Paso 1: Descargue e instale el MBSA

- Abra un explorador y vaya a la página Web del MBSA:
<http://technet.microsoft.com/es-mx/security/cc184924.aspx>
- ¿Cuál es la última versión del MBSA disponible? _____
- ¿Cuáles son algunas de las funciones que proporciona el MBSA? _____

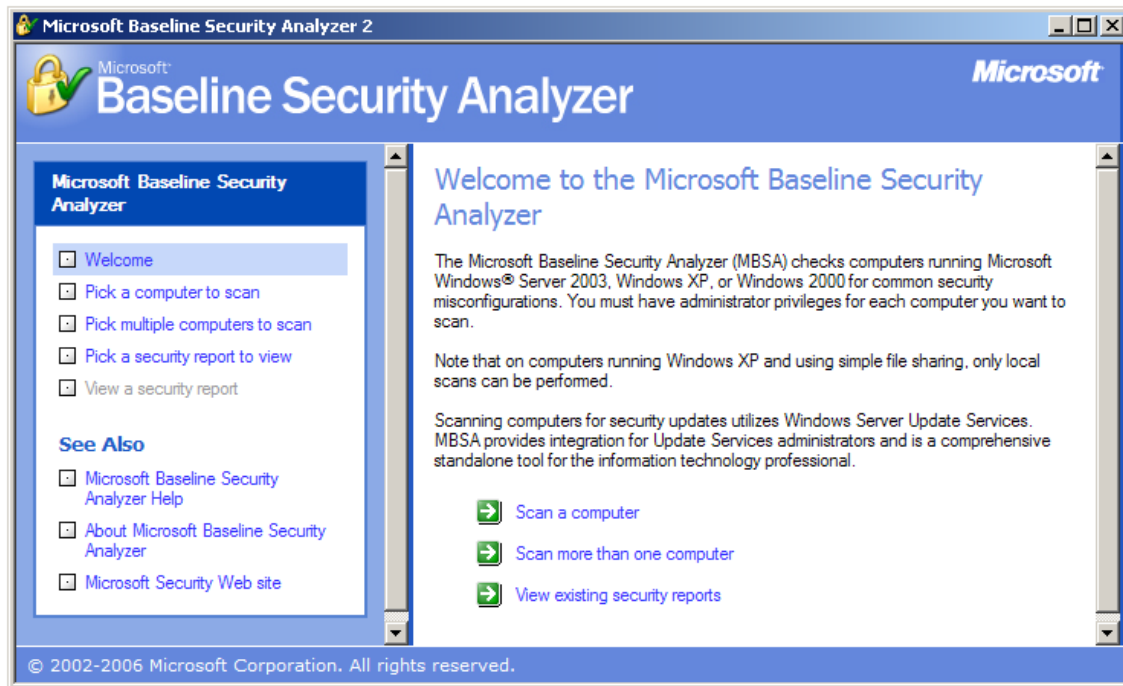
- Desplácese hacia abajo en la página y seleccione el idioma deseado para comenzar el proceso de descarga.
- Haga clic en **Continue** (Continuar) para validar la copia de Microsoft Windows que está utilizando.
- Haga clic en **Download Files below** (Descargar los siguientes archivos) y seleccione el archivo que desea descargar. (El archivo de instalación en inglés es MBSASetup-EN.msi). Haga clic en el botón **Download** (Descargar) ubicado a la derecha de este archivo. ¿Cuántos megabytes tiene el archivo que descargará? _____
- Cuando aparezca el cuadro de diálogo **File Download – Security Warning** (Descarga de archivos: advertencia de seguridad) haga clic en **Save** (Guardar) y descargue el archivo en una carpeta específica o en el escritorio. También puede ejecutarlo desde el sitio Web de descarga.
- Una vez que la descarga haya finalizado asegúrese de que las otras aplicaciones estén cerradas. Haga doble clic en el archivo descargado. Haga clic en **Run** (Ejecutar) para iniciar el programa de instalación y después haga clic en **Run** si aparece una advertencia de seguridad. Haga clic en **Next** (Siguiente) en la ventana de instalación del MBSA.
- Seleccione el botón de opción para aceptar el contrato de licencia y haga clic en **Next**. Acepte los valores predeterminados a medida que avance la instalación y luego haga clic en **Finish** (Finalizar). Haga clic en **OK** (Aceptar) en la última pantalla de instalación del MBSA y cierre la carpeta para volver al escritorio de Windows.

Paso 2: Construya la red y configure los hosts

- Conecte las computadoras host al router integrado, a un hub o a un switch, como se muestra en el diagrama de la topología. El Host A es la estación de prueba donde se instalará el MBSA. El servidor es opcional.
- Establezca la configuración IP de los hosts mediante la opción Conexiones de red de Windows XP y las propiedades TCP/IP. Si el host está conectado al router integrado, configúrelo con un cliente DHCP; de lo contrario vaya al Paso 2c.
- Si el host está conectado a un hub o a un switch y no hay un servidor de CDP disponible, configúrelo de forma manual mediante la asignación de una dirección IP estática.
¿Qué dirección IP y qué máscara de subred tienen el Host A y el servidor (opcional)?

Paso 3: Ejecute el MBSA en un host

- a. Haga doble clic en el ícono del MBSA en el escritorio o ejecútelo desde **Inicio > Todos los programas**. Cuando aparece la pantalla principal, ¿qué opciones están disponibles? _____
-



Paso 4: Seleccione una computadora para analizar

- a. En la parte izquierda de la pantalla haga clic en **Pick a computer to scan** (Elegir una computadora para analizar). The computer shown as the default is the one on which MBSA is installed.
- b. ¿Cuáles son las dos maneras de especificar una computadora para analizar? _____
- c. Acepte la computadora predeterminada que se analizará. Anule la selección de las opciones "Check for IIS administrative vulnerabilities" (Buscar vulnerabilidades administrativas de IIS) y "Check for SQL administrative vulnerabilities" (Buscar vulnerabilidades administrativas de SQL), ya que es probable que estos servicios no estén instalados en la computadora que se analizará. Haga clic en **Start Scan** (Iniciar análisis).

The screenshot shows the 'Pick a computer to scan' window. It has a title bar and a main area with the following elements:

- Title:** 'Pick a computer to scan' in blue.
- Instruction:** 'Specify the computer you want to scan. You can enter either the computer name or its IP address.'
- Computer name:** A dropdown menu showing 'WORKGROUP\HOST-1' with '(this computer)' to its right.
- IP address:** Four input boxes separated by dots, with a dropdown arrow on the right.
- Security report name:** A text box containing '%D% - %C% (%T%)'.
- Options:**
 - A legend: '%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address'.
 - Five checked checkboxes:
 - Check for Windows administrative vulnerabilities
 - Check for weak passwords
 - Check for IIS administrative vulnerabilities
 - Check for SQL administrative vulnerabilities
 - Check for security updates
 - One checked checkbox: 'Configure computers for Microsoft Update and scanning prerequisites'.
 - One unchecked checkbox: 'Advanced Update Services options:'.
 - Two radio buttons:
 - Selected: 'Scan using assigned Update Services servers only'.
 - Unselected: 'Scan using Microsoft Update only'.
- Footer:** 'Learn more about [Scanning Options](#)'.
- Buttons:** A green button with a right arrow and the text 'Start scan'.

Paso 5: Vea los resultados del análisis de actualizaciones de seguridad

- a. Vea el informe de seguridad. ¿Cuáles son los resultados del análisis de actualizaciones de seguridad? _____
- b. Si aparece alguna X roja o amarilla, haga clic en **How to correct this** (Cómo corregir esto). ¿Cuál es la solución recomendada? _____

View security report

Sort Order: Score (worst first) ▼

Computer name:	WORKGROUP\HOST-1
IP address:	192.168.1.100
Security report name:	WORKGROUP - HOST-1 (3-16-2007 3-10 PM)
Scan date:	3/16/2007 3:10 PM
Scanned with MBSA version:	2.0.6706.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update
Security assessment:	Severe Risk (One or more critical checks failed.)









Security Update Scan Results

Score	Issue	Result
	Office Security Updates	9 security updates are missing. What was scanned Result details How to correct this
	Windows Security Updates	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





Previous security report Next security report

Paso 6: Vea los resultados del análisis de Windows en el informe de seguridad

- a. Desplácese hacia abajo para ver la segunda sección del informe, es decir: **Windows Scan Results** (Resultados del análisis de Windows). ¿Se identificó alguna vulnerabilidad administrativa?

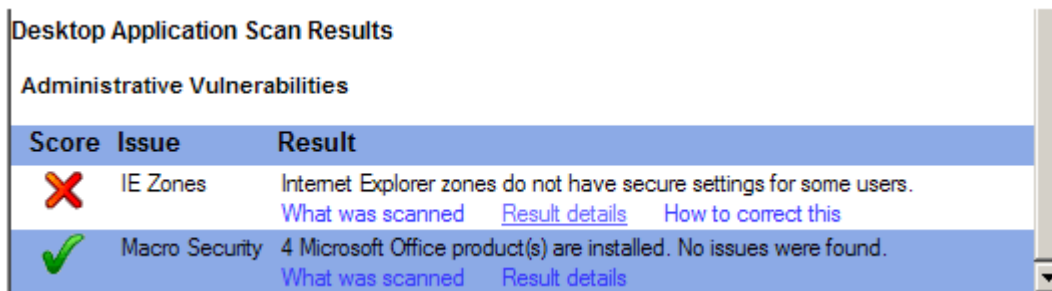
Windows Scan Results		
Administrative Vulnerabilities		
Score	Issue	Result
	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Guest Account	The Guest account is not disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Autologon	This check was skipped because the computer is not joined to a domain. What was scanned
	Password Expiration	This check was skipped because the computer is not joined to a domain. What was scanned

- b. En la sección **Additional System Information** (Información adicional del sistema) que aparece a continuación, en la opción **Services** (Servicios) de la columna **Issue** (Problema) haga clic en **Result details** (Detalles de resultado), en la columna **Result** (Resultado) para obtener una descripción de la comprobación realizada. ¿Qué descubrió? Al finalizar cierre ambas ventanas emergentes para volver al informe de seguridad.

Additional System Information		
Score	Issue	Result
	Auditing	This check was skipped because the computer is not joined to a domain. What was scanned How to correct this
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	4 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Windows 2000 or greater. What was scanned

Paso 7: Vea los resultados del análisis de aplicaciones de escritorio en el informe de seguridad

- a. Desplácese hacia abajo para ver la última sección del informe, es decir: **Desktop Applications Scan Results** (Resultados del análisis de aplicaciones de escritorio). ¿Se identificó alguna vulnerabilidad administrativa?



The screenshot shows a window titled "Desktop Application Scan Results" with a sub-header "Administrative Vulnerabilities". It contains a table with three columns: "Score", "Issue", and "Result".

Score	Issue	Result
✗	IE Zones	Internet Explorer zones do not have secure settings for some users. What was scanned Result details How to correct this
✓	Macro Security	4 Microsoft Office product(s) are installed. No issues were found. What was scanned Result details

- b. ¿Cuántos productos de Microsoft Office hay instalados? _____
- c. ¿Se detectó algún problema de seguridad con **Macro Security** (Seguridad de macros) en alguno de ellos?
- _____

Paso 8: Analice un servidor (si hay uno disponible)

- a. Si hay disponible un servidor con varios servicios, haga clic en "Pick a computer to scan" (Elegir una computadora para analizar) en la pantalla principal del MBSA, escriba la dirección IP del servidor y a continuación haga clic en "Start Scan" (Iniciar análisis). ¿Qué vulnerabilidades de seguridad se identificaron?
- _____
- _____
- _____

- b. ¿Se encontró algún servicio instalado que pueda ser innecesario? ¿Qué números de puerto tenían?
- _____
- _____

Paso 9: Desinstale el MBSA mediante la opción Agregar o quitar programas del Panel de control

- a. Este paso es opcional, en función de que algún proceso de red restaure (o no) más tarde el host de forma automática.
- b. Para desinstalar el MBSA haga clic en **Inicio > Panel de control > Agregar o quitar programas**. Busque la aplicación MBSA y desinstálela. Debe aparecer como Microsoft Baseline Security Analyzer 2.0.1. Haga clic en **Quitar** y luego en **Sí** para confirmar la eliminación de la aplicación MBSA. Al finalizar cierre todas las ventanas para volver al escritorio.

Paso 10: Reflexión

- a. La herramienta MBSA está diseñada para identificar vulnerabilidades en computadoras basadas en Windows. Utilice Internet para buscar otras herramientas. Indique algunas de las herramientas encontradas.

b. ¿Qué herramientas existen para las computadoras que no están basadas en Windows? Utilice Internet para buscar otras herramientas e indique algunas.

-
- c. ¿Qué otros pasos podría realizar para proteger una computadora de los ataques de Internet?
-