Microsoft Baseline Security Analyzer

簡介暨使用說明

V1.0

TANet CERT 台灣學術網路危機處理中心團隊

2010/12/8

[此文件主要簡介 Microsoft Baseline Security Analyzer 工具，並提供使用說明。]

目錄

簡介

Microsoft Baseline Security Analyzer (MBSA) 是一個簡單易用的工具，可協助中小型企業判斷其安全性狀態是否符合 Microsoft 的安全性建議，並會根據結果提供具體的矯正指示。使用 MBSA 偵測一般常犯的安全性設定錯誤和電腦系統所遺漏的安全性更新，以增強您的安全性管理流程。

概觀

為了方便地評估安裝 Windows 電腦之安全狀態，微軟提供了免費的 Microsoft Baseline Security Analyzer (MBSA)掃描工具。MBSA 包括圖型和命令列界面，可以進行本地或遠程掃描微軟 Windows 系統。
MBSA 運行在 Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Visat, Windows Server 2003, Windows XP 和 Windows 2000 系統上時，將使用微軟更新的技術掃描缺少的安全更新(security updates)和匯整服務包(rollups and service packs)。
MBSA 將同時掃描常見的安全錯誤(也稱為漏洞評估檢查)使用一個已知的列表列出所有版本的 Windows 安全設定和組態, Internet Information Server (IIS) 5.0, 6.0 and 6.1, SQL Server 2000 and 2005, Internet Explorer (IE) 5.01 and later, and Office 2000, 2002 and 2003。

支援作業系統

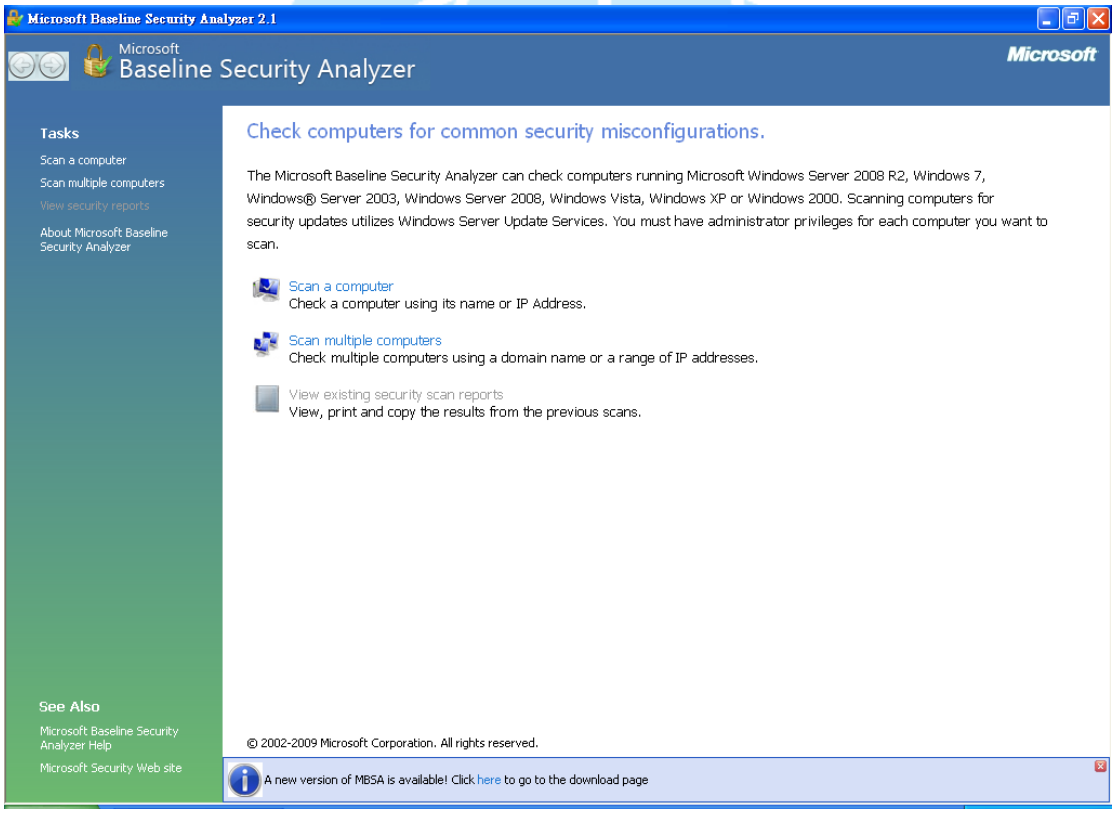
- Windows Server 2008 R2
- Windows 7
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Windows XP
- Windows 2000

檢查項目

- 安全更新(security updates)
- 匯整服務包(rollups and service packs)
- 系統安全設定和組態
- Internet Information Server (IIS) 5.0, 6.0 and 6.1
- SQL Server 2000 and 2005
- Internet Explorer (IE) 5.01 and later
- Office 2000, 2002 and 2003

圖形界面

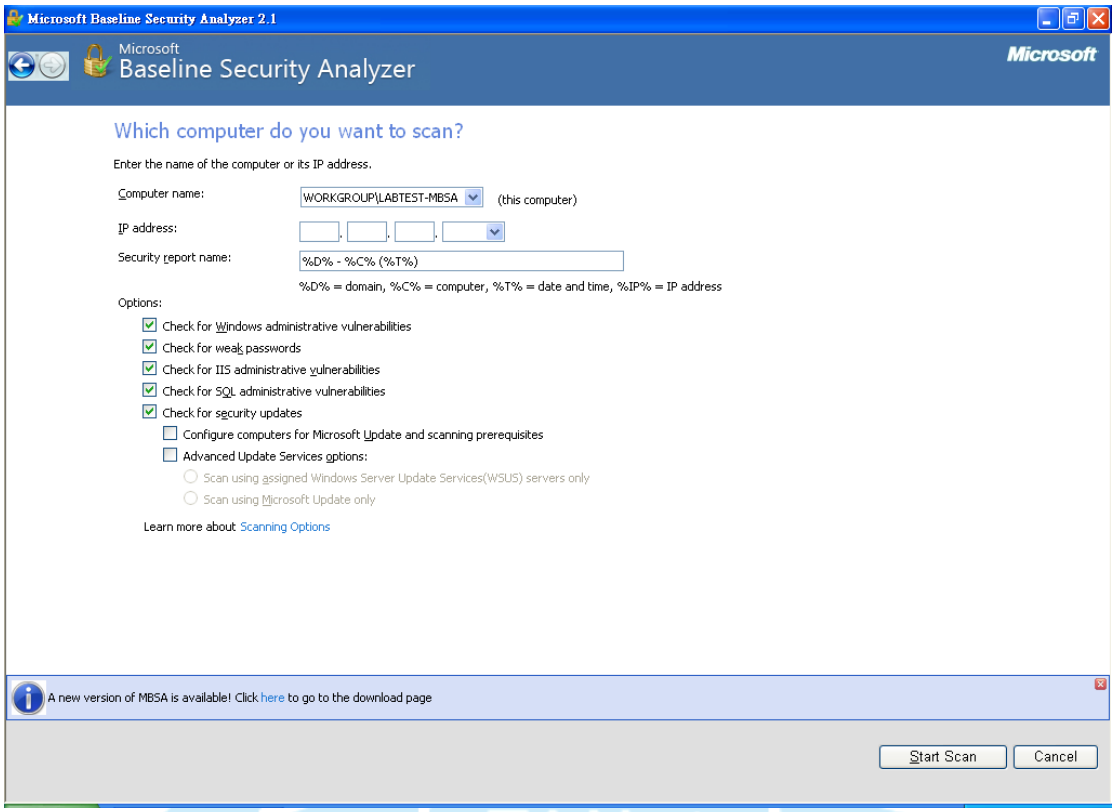
工作畫面



功能說明

- Scan a computer – 掃描本機電腦
- Scan multiple computer – 掃描多台電腦
- View existing security scan reports – 檢視現存的安全掃描報告

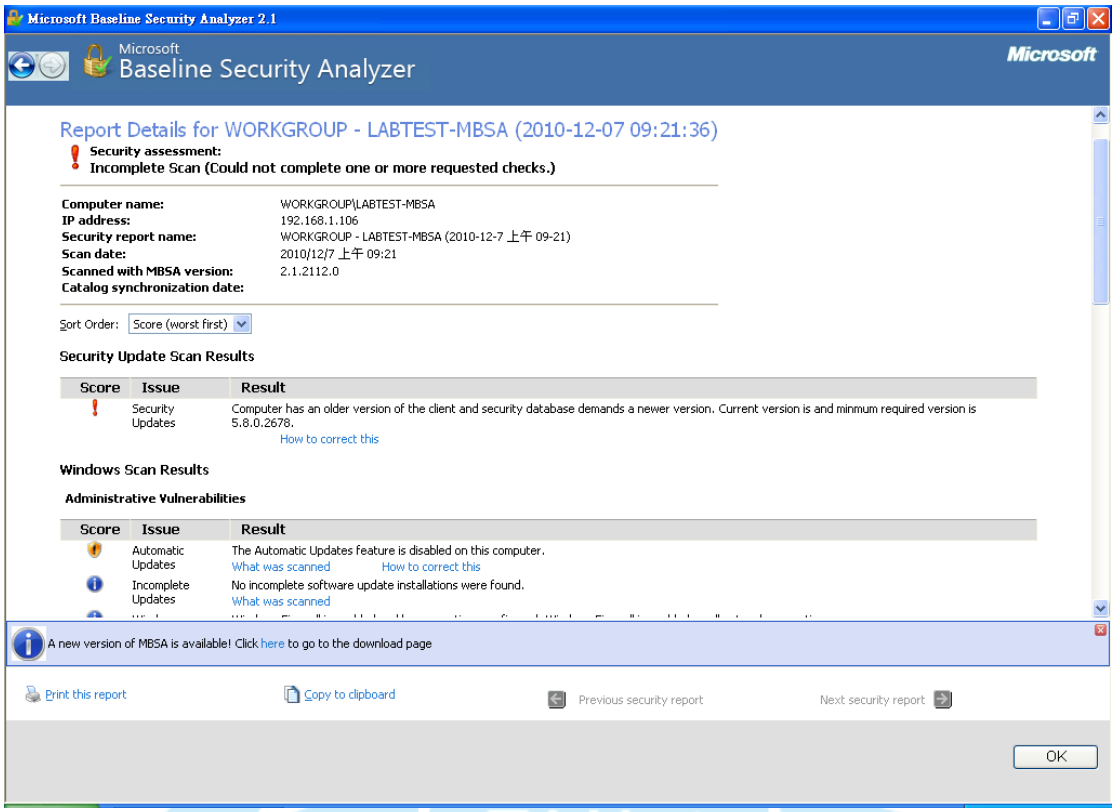
掃描畫面



選項說明

- Check for Windows administrative vulnerabilities – 檢查 Windows 管理漏洞
- Check for weak password – 密碼強度檢查
- Check for IIS administrative vulnerabilities – 檢查 IIS 管理漏洞
- Check for SQL administrative vulnerabilities – 檢查 SQL 管理漏洞
- Check for security updates – 檢查安全更新
- Configure computers for Microsoft Update and scanning prerequisites – 微軟更新和掃描先決條件之電腦設定
- Advanced Update Service Options – 進階更新服務選項
- Scan using assigned Windows Server Update Services(WSUS) Servers only – 掃描只使用指定的 Windows Server Update Services(WSUS)伺服器
- Scan using Microsoft Update only – 掃描只使用 Microsoft Update。

掃描結果



命令列界面

Microsoft Baseline Security Analyzer
Version 2.1.1 (2.1.2112.0)
(C) Copyright 2002-2009 Microsoft Corporation. All rights reserved.

使用方式

使用前於命令列模式下，先行切換到安裝目錄下(C:\Program Files\Microsoft Baseline Security Analyzer 2)

MBSACLI [/target | /r | /d domain] [/n option] [/o file] [/qp] [/qe] [/qr]
[/qt] [/listfile file] [/xmlout] [/wa | /wi] [/catalog file] [/nvc] [/ia] [/mu] [/nd]
[/rd directory] [/?]
MBSACLI [/l] [/ls] [/lr file] [/ld file] [/unicode] [/nvc] [/?]

說明(Description)

This is a command line interface for Microsoft Baseline Security Analyzer。

參數列表(Parameter List)

參　　數	使　用　方　式	說　　明
/target	domain\computer	Scan named computer.
/target	IP	Scan named IP address.
/r	IP-IP	Scan named IP addresses range.
/listfile	File	Scan named IP address or computer listed in the specified file.
/d	Domain	Scan named domain (use NetBIOS compatible domain name (Ex:MyDomain) instead of Fully Qualified Domain Name(Ex:Mydomain.com)).
/n	Option	Select which scans to NOT perform.Allchecks are performed by default. Valid values:"OS", "SQL", "IIS", "Updates", "Password", Can be concatenated with "+"(no spaces).
/wa		Show only updates approved on the WSUS server.
/wi		Show all updates even if not approved on the WSUS server.
/nvc		Do not check for a new version of MBSA.
/o	filename	Output XML file name template. Default: %D% - %C% (%T%).
/qp		Don't display scan progress.
/qt		Don't display the report by default following a single-computer scan.
/qe		Don't display error list.
/qr		Don't display report list.
/q		Do not display any of the preceding items.
/unicode		Output Unicode.
/u	username	Scan using the specified username.
/p	password	Scan using the specified password.
/catalog	filename	Specifies the data source that contains the available security update information.
/ia		Updates the prerequisite Windows Update Agent components during a scan.
/mu		Configures computers to use the

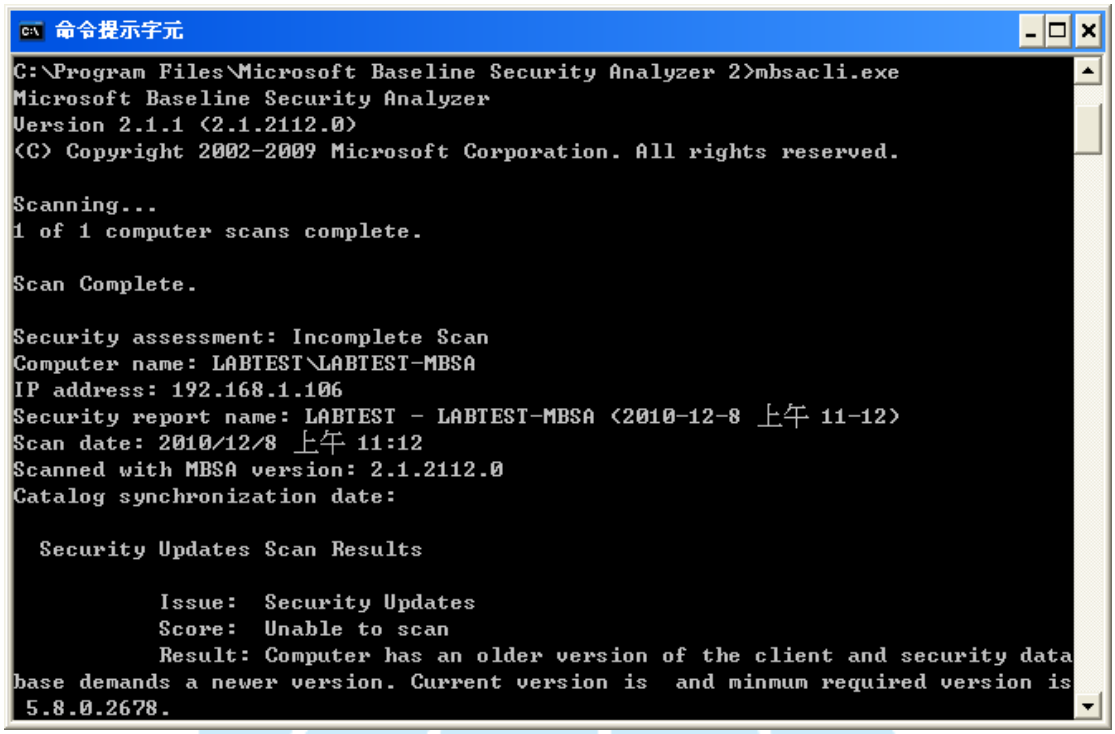
		Microsoft Update site for scanning.
/nd		Do not download any files from the Microsoft Web site when scanning.
/xmlout		Run in updates only mode using only mbsacli.exe and wusscan.dll. Only these switches can be used with this option: /catalog, /wa, /wi, /nvc, /unicode
/l		List all reports available.
/ls		List reports from the latest scan.
/lr	filename	Display overview report.
/ld	filename	Display detailed report.
/rd	directory	Save or Retrieve reports from the specified directory.
/?		Display this help/usage.

執行 MBSACLI 且不帶參數將會掃描本機電腦並進行全面檢查和顯示報告於文字模式(Executing MBSACLI with no parameters scans the local computer for all checksand displays the report in text-mode.)

使用範例(Examples)

MBSACLI
MBSACLI /n Password+IIS+OS+SQL
MBSACLI /d MyDomain
MBSACLI /target 200.0.0.1
MBSACLI /r 200.0.0.1-200.0.0.50
MBSACLI /listfile export.txt
MBSACLI /ld "Domain - Computer (03-01-2002 12-00 AM)"
MBSACLI >c:\results.txt
MBSACLI /catalog c:\wsusscn2.cab /ia /nvc
MBSACLI /wa
MBSACLI /xmlout /catalog c:\temp\wsusscn2.cab /unicode >results.xml
MBSACLI /l /rd c:\scanreports

掃瞄結果



參考資料

Microsoft Baseline Security Analyzer 2.1 網頁：
http://technet.microsoft.com/zh-tw/security/cc184923

Microsoft Baseline Security Analyzer 2.1 下載網址：
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b1e76bbe-71df-41e8-8b52-c871d012ba78&displaylang=en

Microsoft Baseline Security Analyzer 2.1 Q&A 網址：
http://technet.microsoft.com/zh-tw/security/cc184922

補充說明

文件內容整理自微軟網站，提供英翻中及排版，如有內容任何問題以微軟網站文件為主，特此告知。