Vulnerability Assessment Guide

弱點掃描服務指引

文件編號： VA_TRA_2025_GUS_02

機密等級： CONFIDENTIAL

雲森數位有限公司

版本：V 1.0.2　2025/03/18

目錄

一、弱點掃描服務簡介

弱點掃描 (Vulnerability Scanning) 是一種自動化的安全評估技術，用於識別系統、網路設備、應用程式或伺服器中的安全漏洞。這項技術通常由資安團隊或 IT 部門執行，以確保組織的資訊系統不易受到攻擊。

二、弱點掃描的目的

1. **識別已知漏洞**：偵測系統中的安全弱點，如過時軟體、不安全的設定或已知的攻擊向量。
2. **預防安全威脅**：在攻擊者利用漏洞前，企業可以提前修補問題，降低風險。
3. **符合法規與標準**：幫助企業達成 ISO 27001、PCI-DSS、NIST 等資安標準的要求。
4. **提升企業安全性**：確保系統、伺服器及應用程式的安全性，減少資料外洩與駭客入侵的風險。

三、弱點掃描的類型

1. **網路層掃描** (Network Vulnerability Scanning)

   掃描 IP、伺服器、交換機、防火牆等網路設備的漏洞。

   例：開放未受保護的遠端存取端口 (如 Telnet, SSH)。
2. **應用程式掃描** (Application Vulnerability Scanning)

   掃描 Web 應用程式，如網站或 API 是否存在 OWASP Top 10 漏洞 (如 SQL Injection, XSS)。

   例：登入頁面允許暴力破解密碼。
3. **作業系統與伺服器掃描** (Host-based Vulnerability Scanning)

   掃描 Windows、Linux 等作業系統的安全性，確認是否有未更新的漏洞 (CVE)。

   例：伺服器上的 PHP 或 OpenSSL 版本過舊，可能有已知漏洞。

四、常見的弱點掃描工具

弱點掃描工具(Vulnerability Scanning Tools)是一種自動化的安全檢測技術，用來識別系統、網路設備、應用程式或伺服器中的已知安全漏洞。

常見工具有下列幾種其他(亦有其他未列出之工具)：

工具名稱	主要用途	開發公司/開源專案
Nessus	網路與應用程式漏洞掃描	Tenable
OpenVAS	開源漏洞掃描框架	Greenbone Networks
Qualys	雲端漏洞管理與合規性檢測	Qualys
Nmap + NSE	掃描開放端口與網路漏洞	開源工具

弱點掃描工具雖然能夠自動化檢測系統漏洞，但它的公正性可能受到供應商影響、漏洞庫更新頻率、掃描演算法、評分標準等多種因素影響。因此，建議應搭配下列指引執行：

- ✧ 搭配經驗判斷、手動驗證與滲透測試，確保掃描結果準確，降低誤報影響。
- ✧ 檢查工具的漏洞庫更新頻率，隨時更新漏洞資料庫，確保能夠偵測最新的漏洞。

透過這些方式，可以確保弱點掃描工具的公正性，並有效提升資訊安全管理的可信度。

五、漏洞標準 CVSS 與 CVE 的介紹

CVSS 和 CVE 是資訊安全領域中常見的標準，用於衡量與管理軟體漏洞。它們之間的關係如下：

- ✧ **CVE (Common Vulnerabilities and Exposures，通用漏洞與暴露編號)→ 負責「識別」漏洞**，提供一個統一的漏洞編號。
- ✧ **CVSS (Common Vulnerability Scoring System，通用漏洞評分系統)→ 負責「評估」漏洞的嚴重程度**，透過數據量化風險。

1. CVE（通用漏洞與暴露編號）

CVE 是一個全球通用的漏洞識別系統，由 **MITRE(https://cve.mitre.org/)** 組織管理，每個已知的軟體或系統漏洞都會獲得一個**唯一的 CVE 編號**。

CVE 編號格式

CVE-YYYY-XXXXX（例如：CVE-2024-12345）

- **CVE**：代表該漏洞來自 CVE 資料庫

- **YYYY**：代表漏洞發現的年份
- **XXXXX**：為該年中該漏洞的編號（不一定連號）

2. CVSS（通用漏洞評分系統）

- CVSS 是用來**評估漏洞嚴重程度**的標準，由 **FIRST (Forum of Incident Response and Security Teams)(https://www.first.org/)**組織維護。
- CVSS 評分標準

  CVSS 分數範圍為 **0.0 - 10.0**，數值越高代表風險越大。

CVSS 分數	風險等級
0.0	無風險
0.1 - 3.9	低風險 (Low)
4.0 - 6.9	中風險 (Medium)
7.0 - 8.9	高風險 (High)
9.0 - 10.0	極高風險 (Critical)

CVSS 計算方式

CVSS 透過 **三大評分指標** 來計算：

A. **基本評分 (Base Score)**：漏洞的核心特性，如攻擊向量、影響範圍等。

B. **時間評分 (Temporal Score)**：漏洞的可利用性與修復狀況。

C. **環境評分 (Environmental Score)**：漏洞對特定組織的影響程度。

六、產出報告的公正性與可信度

為了確保報告的公正性與可信度，應考量以下因素：

1. **使用國際標準**

   採用 **CVSS、CVE、OWASP、NIST、ISO 27001 等或其他**標準，確保漏洞評估的**一致性與公正性**。

2. **交叉驗證與人工審核**

   除了自動化掃描，應由資安專家手動驗證，避免誤報（False Positives）。

3. **提供客觀修復建議**

   以**技術風險**為優先，而非基於供應商利益提供修復方案。

七、弱點掃描與其他測試技術的差別

1. 弱點掃描 (Vulnerability Scanning)

目的：**識別系統、網路或應用中的已知漏洞**

方式：使用自動化工具掃描，找出過時軟體、不安全設定、已知漏洞(CVE)

特點：

- 自動化，速度快、可大範圍掃描。
- 不會驗證漏洞是否可被攻擊利用，會進行初步誤判判斷，僅提供報告。
- 適合日常安全維護，企業可定期執行。

2. 滲透測試 (Penetration Testing，簡稱 Pentest)

目的：**驗證漏洞是否可被利用**，模擬真實攻擊場景方式：由安全專家(白帽駭客)結合自動與手動測試，進行實際攻擊特點：

- 深度測試，評估漏洞是否能被駭客攻擊
- 模擬真實駭客行為，但範圍通常受限於合約約定
- 可能影響系統運行(需事先授權與風險評估)

3. 攻擊與入侵模擬 (BAS, Breach and Attack Simulation)

目的：持續測試企業安全防禦能力，類似「自動化滲透測試」方式：**模擬已知攻擊技術**(如 MITRE ATT&CK)，測試企業資安系統能否偵測與防禦

特點：

- 自動化持續運行，可在企業內部不斷測試安全防禦
- 測試防禦機制是否有效(如端點防護、SIEM、SOC 等)
- 不會影響系統運行，但能發現企業安全缺口

4. 紅藍演練 (Red Team vs Blue Team)

目的：模擬真實駭客攻擊，測試企業整體資安應變能力

方式：由**紅隊(Red Team)負責攻擊，藍隊(Blue Team)負責防禦**

特點：

- 全面測試企業防禦能力（人員 + 技術 + 流程）
- 紅隊（攻擊者） 模擬 APT 攻擊，試圖滲透企業內部
- 藍隊（防禦者） 需偵測、回應、阻擋攻擊，強化資安應變

適用對象：金融機構、政府機關、大型企業（需要強化資安應變能力）

以下是這四種測試的主要差異說明

測試類型	目的	測試方式	是否驗證漏洞可利用性	是否影響系統	適用場景
弱點掃描	發現系統漏洞	自動化掃描	❌ 否	❌ 不影響	日常資安維護
滲透測試	測試漏洞可否被攻擊利用	手動+自動攻擊	✅ 是	⚠️ 可能影響	系統安全評估
攻擊與入侵模擬	模擬已知攻擊，測試防禦機制	自動化攻擊模擬	❌ 否	❌ 不影響	企業防禦測試
紅藍演練	測試企業整體資安應變能力	紅隊攻擊 vs. 藍隊防禦	✅ 是	⚠️ 可能影響	高級攻擊模擬

八、產出報告的格式與結構

大多數遵循以下結構，資安報告可能因測試過程或結果進行斟酌調整：

1. 封面
   - 報告名稱（如「滲透測試報告」、「弱點掃描報告」）
   - 機密等級（如「Confidential」、「Internal Use Only」）
   - 報告編號
   - 日期
   - 受測單位
   - 執行單位
2. 摘要 (Executive Summary)
   - 測試目標與範圍
   - 測試方法
   - 主要發現與風險等級
   - 關鍵修復建議
3. 測試方法
   - 測試工具與技術
   - 掃描與攻擊向量
   - 測試範圍
   - 限制條件
4. 測試結果
   - 漏洞分類（高風險 / 中風險 / 低風險）
   - 漏洞分析
     - 漏洞名稱
     - 影響系統
     - CVE 編號
     - CVSS 評分
     - OWASP 分類
     - 漏洞描述
     - 攻擊方法
     - 風險評估
     - 修復建議
5. 結論與建議
   - 總結測試結果
   - 建議修復優先順序
   - 未來安全強化建議
6. 附錄
   - 完整掃描數據
   - 技術細節
   - 參考文獻