Tenable Passive Vulnerability Scanner™ 被動式安全掃描

產品概觀

Tenable Passive Vulnerability Scanner™ 被動式安全掃描是一項已取得專利的網路探索及漏洞分析技術，可藉由非侵入性方式，提供持續即時的網路狀態剖析及監控。Tenable Passive Vulnerability Scanner 被動式安全掃描能在網路通訊中監控 IPv4 與 IPv6 網路，以判定拓樸結構、網路服務、網路流量和漏洞。而整合了 Passive Vulnerability Scanner 被動式安全掃描的 Tenable SecurityCenter™，還能集中分析日誌、管理漏洞，讓您全面檢視企業的安全情勢。

持續不間斷地監控網路流量，找出未經授權的裝置、漏洞及混合在 IPv4/IPv6 網路中的殭屍網路

產品效益

核心及顯著效益包括，可擷取所有網路設備、伺服器與應用程式，找出系統漏洞並偵測 IPv6 資產：

- 加速發現威脅，消弭與主動式漏洞掃描之間的落差
- 自動找出資產、新系統或惡意系統所帶來的潛在安全威脅
- 透過驗證設定管理，讓企業可確認內部政策及重要法規的合規性
- 可找出可能造成個資外洩的敏感資料
- 可對「真正」的威脅發出警示，讓您專心因應資安事件
- 可找出不當使用的情形及揪出一般設備偵測不到的「內部威脅」
- 可保護因為政策或系統設定而無法進行主動式掃描的系統與應用程式
- 無需登入系統即可執行高效率的掃描，且不會影響服務及不會造成服務中斷

主要功能特色

即時漏洞監控

Tenable Passive Vulnerability Scanner 被動式安全掃描可持續監控網路通訊中各種安全相關資訊，包括：

- 追蹤所有用戶端、伺服器和應用程式漏洞
- 第一時間確認應用程式是否因遭攻擊而造成資訊外洩或破壞
- 偵測及記錄加入網路的新主機
- 第一時間發現是否有系統開始對其他系統進行通訊埠掃描
- 顯示所有連線及加密的網路通訊
- 找出個別系統運作的通訊埠以及瀏覽過的通訊埠
- 被動式確認各個運作中主機的作業系統
- 偵測網路上的漏洞，以及所使用的通訊協定與應用程式

Tenable Passive Vulnerability Scanner 被動式安全掃描採用非侵入性方式，提供即時網路監控及剖析功能，以持續掃描及評估組織的安全性，將組織的安全威脅可視化、數據化。Passive Vulnerability Scanner 被動式安全掃描能監控網路通訊以判定網路拓樸、讓您深入檢視伺服器與用戶端的漏洞、監測網路環境中的敏感性資訊及常見通訊協定與服務的使用情況（例如：HTTP、SQL、共享檔案…等）。Passive Vulnerability Scanner 被動式安全掃描甚至可在混合式網路中找出 IPv4 與 IPv6 資產。

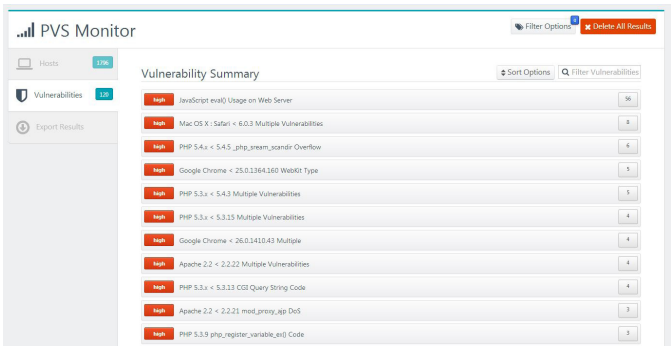
Passive Vulnerability Scanner 被動式安全掃描完善的介面與安裝精靈，能讓您毫不費力快速地安裝在網路上，它能被動式偵測網路上的設備（包括行動裝置），連有越獄 (Jailbroken) 的 iOS 裝置都找得到。Passive Vulnerability Scanner 被動式安全掃描可偵測作業系統、服務、應用程式及所有網路通訊中的漏洞問題，有效識別行動裝置的應用程式與漏洞。

Passive Vulnerability Scanner 被動式安全掃描可連接一到多個網段，持續監控網路資料流、發出即時警示，並產生綜合性報告供安全團隊、IT 團隊及管理團隊參考。

網路與 FTP 監控

Passive Vulnerability Scanner 被動式安全掃描可直接分析封包資料流，擴大監控網路與 FTP 活動。它能藉著被動式監控所有 HTTP 或 FTP 封包，對網路上的各個主機做出判定，並產生實用的報告，例如：

- 所有用戶端及伺服器的漏洞及相關的應用程式
- 完整列出每部主機使用的網路代理程式
- 列舉經由 FTP 共享的所有檔案
- 即時記錄 Web Server 所有 GET、POST 或下載的檔案
- 即時記錄所有 FTP 檔案 GET 或 PUT
- 即時記錄所有 DNS 查詢數據



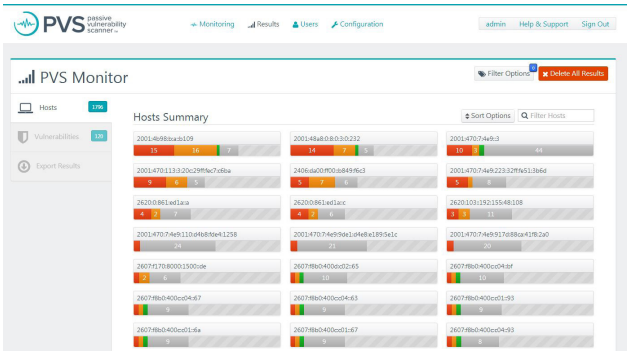
這些高實用性資料，能有效分析內部活動、員工活動以及惡意程式感染或進階持續性滲透攻擊 (APT)。大部份這類記錄也能傳送至 Tenable Log Correlation Engine™ 日誌關聯引擎，做進一步分析、搜尋相互關聯性及長期儲存。

不需在伺服器上安裝代理程式也不需要登入到伺服器

Passive Vulnerability Scanner 被動式安全掃描可提供 Microsoft SMB 通訊協定的進階通訊協定分析。如果將 Passive Vulnerability Scanner 被動式安全掃描部署在內部網路，系統就能查看 Active Directory 網路流量，並自動學習：

- 各個系統的主機名稱與工作群組名稱
- 所有資料夾中全部共用檔案的清單
- 即時登入資訊和從網路共享下載的檔案

以上被動式判定資訊的能力，給予企業在法律舉證方面極高的價值。在大型網路上，若能被動式判定所有共用資料夾內容，那麼要找出潛在敏感資料就不再是難事。只要將網路上共用的各個檔案記錄傳送至 Tenable Log Correlation Engine 日誌關聯引擎，即可分析員工活動與惡意程式活動是否合法。



SQL 資料庫記錄與監控

Passive Vulnerability Scanner 被動式安全掃描也能透過網路通訊內容識別 SQL 資料庫及與其相關聯的漏洞，並即時記錄活動。PVS 被動式安全掃描將 SQL資料庫查詢的即時記錄傳送至 Log Correlation Engine 日誌關聯引擎，便能為您搜尋、儲存、關聯及分析攻擊事件，例如來自網路服務的 SQL Injection（SQL資料隱碼攻擊）。而利用 PVS 被動式安全掃描，Nessus SQL 掃描及審查 LCE SQL 代理程式，企業就能全面性了解 SQL資料庫的活動。

被動式的探索網路拓樸與服務

藉著重新建構來源和目標兩端的網路通訊內容，PVS被動式安全掃描能夠以 HTTP、SMTP 和 FTP 的通訊特徵去識別它們，並以特定的漏洞測試插件去測試漏洞。

部署選擇

Tenable Passive Vulnerability Scanner 被動式安全掃描可單獨安裝也可搭配 SecurityCenter Continuous View (SC CV) 使用。相當適合持續監控小型網路區段或大型網路中特定網段；而 Passive Vulnerability Scanner 被動式安全掃描單機版提供的整合式介面，能輕鬆監控高敏感性的網路或網路區段，準確點無與倫比。即使是在一般的網路節點，Passive Vulnerability Scanner 被動式安全掃描也能提供有別於傳統的優異結果。SC CV 是一款安全風險管理解決方案，能以獨一無二的方式結合了主動式漏洞掃描、被動式安全掃描以及安全資訊與事件管理 (SIEM)。

如需更多資訊

或有其他問題，或有意購買或評估試用，請洽：

ap@tenable.com
Twitter：@TenableSecurity
YouTube：youtube.com/tenablesecurity
Tenable 部落格：blog.tenable.com
Tenable 論壇：discussions.nessus.org
www.tenable.com

tenable™ network security