

Nessus Scanner

資訊安全是當今企業面臨的重要挑戰之一，因此效率和準確度成為資安團隊不容忽視的關鍵。根據Forrester的調查，有58%的資安團隊過於忙碌，沒有足夠時間主動尋找問題並修補漏洞，以降低企業的風險曝露；同時，有73%的資安團隊認為，如果他們能夠爭取更多時間主動發現並解決問題，企業的風險管理流程將更為成功。

Nessus Scanner是一款功能強大且靈活的漏洞掃描工具，能夠協助組織識別和解決網絡和系統上的安全漏洞，從而提升整體安全性和防禦能力。該產品不僅能夠掃描單個IP位址，還能夠掃描子網路和網域名稱，在各種作業系統上快速辨識並修復弱點，包括軟體缺陷、缺少的修補程式、惡意軟體以及錯誤設定。

功能特色

漏洞掃描和評估：Nessus Scanner可以掃描網絡上的設備、應用程序和服務以識別安全漏洞和配置錯誤。它使用廣泛的漏洞和安全配置數據庫，能夠檢測已知的漏洞和風險。

可定制性：用戶可以根據自己的需求配置掃描，包括指定目標IP地址、端口範圍、掃描深度等。這使得Nessus Scanner能夠適應各種不同規模和類型的網絡環境。

報告和分析：Nessus Scanner生成詳細的漏洞報告，包括漏洞的等級、風險評估、建議的解決方案等信息。這些報告通常以易於理解和操作的格式呈現，以便安全專業人員進行進一步的分析和解決問題。

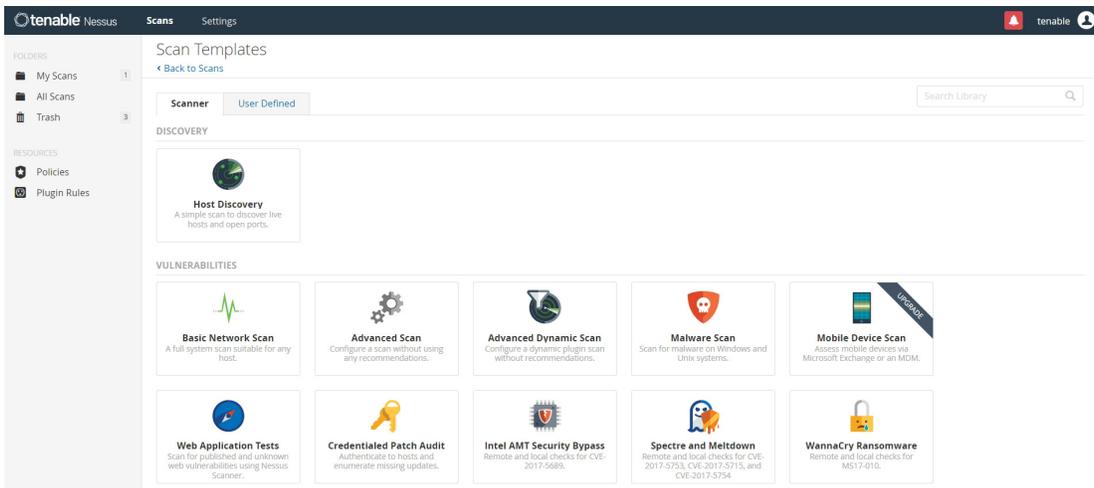
持續監測：Nessus Scanner支持定期或持續性掃描，以確保組織的網絡和系統始終處於最佳安全狀態。它可以自動檢測新的漏洞和風險，並通過更新的漏洞庫持續跟進。

軟體需求

作業系統	支援版本
Linux	Amazon Linux 2, 2023 Debian 10,11, and 12 / Kali Linux 2020 Fedora 38 and 39 Raspberry Pi OS Red Hat / CentOS / Oracle Linux FreeBSD 12 SUSE Enterprise 12 and 15 SP1 and later Ubuntu
Windows	Windows Server 2012, , Server 2016, Server 2019, Server 2022 Windows 10, 11
macOS	macOS 12, 13, and 14

硬體需求

使用情境	最低硬體配置
Scanning up to 50,000 hosts per scan	CPU: 4 2GHz cores Memory: 4 GB RAM (8 GB RAM recommended) Disk space: 30 GB, not including space used by the host operating system
Scanning more than 50,000 hosts per scan	CPU: 8 2GHz cores Memory: 8 GB RAM (16 GB RAM recommended) Disk space: 30 GB, not including space used by the host operating system



關於 TENABLE

Tenable®, Inc. 是一家 Cyber Exposure 分析公司。全球超過有 30,000 家企業仰賴 Tenable 協助瞭解並降低網路風險。身為 Nessus® 的創造者，Tenable 拓展了自己在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。在 Tenable 的客戶中，包含超過 50% 的財星 500 大企業、超過 30% 的全球 2000 大企業以及大型政府機構。如需深入瞭解，請前往 zh-tw.tenable.com。