

APEXSYS 入侵及攻擊模擬(BAS)檢測平台_資安健檢分析檢測_單次授權

APEXSYS 入侵及攻擊模擬(BAS)檢測平台_資安健檢分析檢測是協助防駭的最佳選擇!

➤ 如何健診環境以掌握發現攻擊的最佳契機 現今是網路世代，需要針對網路資訊個資作維護以及有效阻擋駭客攻擊，究竟需要哪些產品來保護資訊呢?如何了解電腦存在哪些風險?

*網路架構檢視如何健診環境以掌握發現攻擊的最佳契機

*任何運作中的電腦環境都有可能受到攻擊

*成功的攻擊通常是經過不斷失敗的攻擊之後發生

*越早發現攻擊就越容易遏制損害的發生

*資安健診與入侵偵測

*可以辨識攻擊模式

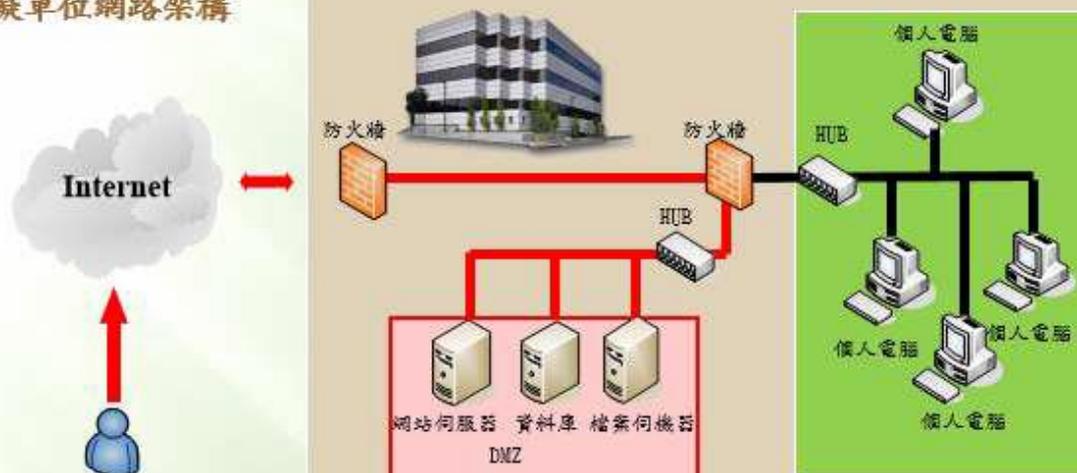
*找出未知的安全性設定問題

*協助判斷哪些網路資源是漏洞所在

誰該為攻擊負責可以辨識攻擊模式

找出未知的安全性設定問題 協助判斷哪些網路資源是漏洞所在

□ 模擬單位網路架構



✓ 服務細則說明

資安健診作業係透過「ISO27001 資訊安全管理制資訊安全管理制導入暨驗證及相關資安檢測與作業服務案」委託本公司針對 貴單位進行各項檢測作業，以協助 貴單位檢視現有資安防禦設備及措施部署情形，並找出潛在安全性弱點與風險，作業方式將依以下三階段進行：



➤ 項目內容說明

組別名稱		內容	單位
資安健診服務	1	網路架構檢視	網路架構(式)
	2	網路惡意活動檢視(有線)-封包監聽與分析	側錄設備(台)
		網路惡意活動檢視(有線)-網路設備紀錄檔分析	資安設備(台)
	3	使用者端電腦惡意活動檢視-使用者端電腦惡意程式或檔案檢視	使用者電腦(台)
		使用者端電腦惡意活動檢視-使用者電腦更新檢視	
	4	伺服器主機惡意活動檢視-伺服器主機惡意程式或檔案檢視	伺服器主機(台)
		伺服器主機惡意活動檢視-伺服器主機更新檢視	
	5	目錄伺服器 設定檢視	伺服器主機(台)
	6	防火牆連線設定檢視	防火牆設備
	7	政府組態基準(GCB)檢視-作業系統 _使用者電腦組態設定檢視	使用者電腦(台)
		政府組態基準(GCB)檢視-作業系統 _伺服器組態設定檢視	伺服器主機(台)
		政府組態基準(GCB)檢視-作業系統 _瀏覽器組態設定檢視	瀏覽器
		政府組態基準(GCB)檢視-作業系統 _網通設備組態設定檢視	網通設備
政府組態基準(GCB)檢視-作業系統 _應用程式組態設定檢視		伺服器主機(台)	
	資料庫安全檢視_特權帳號管理 資料庫安全檢視_資料加密 資料庫安全檢視_存取授權 資料庫安全檢視_稽核紀錄 資料庫安全檢視_委外管理 資料庫安全檢視_備份保護 資料庫安全檢視_弱點管理	資料庫	



➤ 特色與優勢

- 1、提供網路架構圖，並安排相關人員接受訪談。
- 2、提供受測之使用者端電腦清單、伺服器清單及目錄伺服器等資訊。
- 3、提供欲檢視之網路設備紀錄檔。例如：防火牆、入侵偵測／入侵防護系統等。
- 4、提供群組原則(Group Policy)。
- 5、提供防火牆開啟通訊埠(Port)的資訊。資安健診服務是透過整合各項資訊安全項目的檢視服務作業，提供受檢單位資安改善建議，藉以實施技術面與管理面相關控制措施。

資安健診係針對組織之網路面、系統面、終端面，進行客戶整體環境的資安強度評估，找出整體架構的資安缺陷，並提供改善建議，提供客戶做為強化資安防護之參考。