Hackers are ready, Are you?

APEXSYS 入侵及攻擊模擬(BAS)檢測平台

BAS 是「Breach and Attack Simulation」的縮寫，是一種新興的資安技術。它運行模擬自動化攻擊，模仿可能由駭客部署的攻擊，以幫助企業識別安全系統中的潛在漏洞，並測試偵測和防禦能力。

這些模擬攻擊旨在測試組織對攻擊的檢測、分析和應對能力。

BAS 平台可執行的功能

1. Reconnaissance（偵察）：
   攻擊者通過各種方法收集關於目標環境的資訊，包括網路拓撲、系統架構、使用者資訊等。
2. Resource Development（資源開發）：
   在收集到足夠的情報後，攻擊者會繼續開發和籌備攻擊所需的資源，包括創建、收集或獲取工具、腳本、惡意代碼等。
3. Initial Access（初始訪問）：
   A. Phishing（釣魚）
   B. External Remote Services（外部遠程服務）
4. Execution（執行）：
   A. Command and Scripting Interpreter（命令和腳本解析器）
   B. Execution through API（通過 API 執行）
5. Persistence（持久性）：
   A. Scheduled Task/Job（定時任務/工作）
   B. Registry Run Keys / Start Folder（註冊表運行鍵/啟動文件夾）
6. Privilege Escalation（特權升級）：
   A. Exploitation of Privilege Escalation Vulnerability（利用特權升級漏洞）
   B. Windows Admin Shares（Windows 管理共享）
7. Defense Evasion（防禦逃避）：
   A. Masquerading（偽裝）
   B. File Deletion（文件刪除）
8. Credential Access（憑證訪問）：
   A. Credential Dumping（憑證轉儲）
   B. Input Capture（輸入捕獲）
9. Discovery（發現）：
   A. Account Discovery（帳戶發現）
   B. System Network Configuration Discovery（系統網絡配置發現）
10. Lateral Movement（橫向移動）：
    A. Remote File Copy（遠程文件複製）
    B. Remote Desktop Protocol（RDP）Hijacking（遠程桌面協議（RDP）劫持）
11. Collection（收集）：
    A. Automated Collection（自動化收集）
    B. Data from Local System（本地系統數據）
12. Command and Control（命令與控制）：
    一旦攻擊成功入侵目標系統，需要建立一種方式來與受感染的系統進行通信和控制。
13. Exfiltration（外泄）：
    A. Exfiltration Over Command and Control Channel（命令與控制通道外泄）
    B. Exfiltration Over Alternative Protocol（替代協議外泄）
14. Impact（影響）：
    A. Data Encrypted for Impact（用於影響的數據加密）
    B. Data Destruction（數據破壞）

功能架構圖

進行攻擊前準備 → 產生攻擊劇本 → 攻擊演練

檢視資安建設的可靠

提升威脅處理的經驗

驗證資安規劃的成效

強化新興風險的評估