代號：50430
頁次：1－1

115年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員及移民行政人員考試試題

考 試 別：國家安全情報人員考試
等　　別：三等考試
類科組別：資訊組（選試英文）
科　　目：網路應用與安全
考試時間：2 小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、傳統網路安全採取邊界防禦模式（Perimeter Defense Model），但現代企業逐漸轉向零信任架構（Zero Trust Architecture, ZTA）。請說明兩者核心理念與差異，並解釋永不信任、持續驗證與最小權限原則的意涵。（10 分）請舉例說明零信任環境下，身分驗證與授權邏輯如何改變，並說明設備健康狀態（Device Posture）如何影響存取決策。（10 分）

二、近年來供應鏈攻擊（Supply Chain Attack）已成為國家級威脅。請解釋何謂供應鏈攻擊，並各舉一個軟體與硬體層面的實際案例。（10 分）請說明攻擊者為何鎖定第三方供應商而非直接攻擊最終目標，並說明軟體物料清單（SBOM）如何協助降低此類風險。（10 分）

三、企業通常同時部署防火牆（Firewall）、入侵偵測系統（IDS）與入侵防禦系統（IPS）。請分析三者在功能定位、運作方式與回應行為上的差異。（10 分）並說明下一代防火牆（NGFW）如何整合上述功能。（10 分）

四、緩衝區溢位（Buffer Overflow）是許多系統漏洞的根源。請解釋其原理，並說明堆疊溢位（Stack Overflow）與堆積溢位（Heap Overflow）的差異。（10 分）請說明攻擊者如何利用此漏洞達成任意程式碼執行（ACE），並列舉兩種現代緩解機制及其常見繞過手法。（10 分）

五、跨站腳本攻擊（Cross-Site Scripting, XSS）是 OWASP Top 10 中常見的網頁應用程式漏洞。請說明 XSS 的攻擊原理，並比較儲存型與反射型的差異。（10 分）請說明攻擊者如何利用 XSS 竊取使用者的 Session Cookie，並列舉至少兩種有效的防禦機制及其原理。（10 分）