代號：22630
頁次：1－1

113年公務人員高等考試二級考試試題

等　　別：高考二級
類　　科：資訊處理
科　　目：資訊管理與資通安全研究
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請以黑色鋼筆或原子筆在申論試卷上作答。
㈣本科目得以本國文字或英文作答。

一、紅隊演練（Red Team Assessment）是一個機構用來發覺本身存在的資安漏洞的方式之一，請說明紅隊演練中，紅隊、藍隊、紫隊各自的目標，這三者如何合作來達到演練的效果，以及機構可以有什麼做法來防止或限縮紅隊演練的進行所造成的資安危害？（25 分）

二、請試述零時差漏洞（zero-day vulnerability）的定義以及為何零時差漏洞會層出不窮？零時差攻擊（zero-day attack）與零時差漏洞是否有關？對應零時差攻擊，有效的資安防護手段為何？（25 分）

三、近年來供應鏈安全成為資安界的熱門討論議題，請試從軟體產品在技術面以及社交工程兩個面向的資安風險著眼，申論供應鏈安全為何應被重視；亦請說明 SBOM（Software Bill of Material）在軟體產品供應鏈管理的重要性。（25 分）

四、資訊安全三要素是機密性、完整性與可用性，然而若考量到資訊的使用者，則尚可加入可鑑別性（Authenticity）與可歸責性（Accountability）。請說明這兩個性質為何？兩者間是否有關？並舉例說明兩者的必要性。（25 分）