

115年公務人員高等考試三級考試試題

類 科：資通安全
科 目：資通安全概論
考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)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。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）所發布之網路安全框架（Cybersecurity Framework, CSF）2.0 是目前全球廣泛採用之網路安全治理與風險管理框架。該框架以六大核心功能（Core Functions）作為組織管理網路安全風險之基礎，其中包含治理（Govern）功能。請列出其餘五項核心功能，並詳述各項功能之目的與組織在實務上應執行之重點工作事項。（25 分）
- 二、一般而言，軟體開發生命週期（Software Development Life Cycle）可大致分為需求分析、系統設計、程式開發、測試驗證與系統上線等五個階段。「安全設計（Security by Design）」為安全軟體開發的重要理念，其核心精神在於將資訊安全考量自開發初期即融入軟體開發生命週期各階段，而非於系統完成後再額外補強。請詳述在需求分析階段，應如何落實安全設計理念以及相關資安防禦需求。（25 分）
- 三、後門程式（Backdoor）及遠端存取木馬程式（Remote Access Trojan, RAT）在資安領域代表不同層次的概念與攻擊能力，請回答下列問題：
 - (一)請詳述何謂後門程式（Backdoor），包含其定義、功能以及運作方式。（12 分）
 - (二)遠端存取木馬程式（Remote Access Trojan, RAT）是現今資安威脅最為普遍的一種攻擊技術或能力，請詳述其定義、功能以及運作方式。（13 分）
- 四、弱點掃描（Vulnerability Scanning）是資安防護最基本的措施之一。請詳述弱點掃描之目的、作法與效益。（25 分）