知識問答題庫

AI 認知 (必考題，為知識問答第一題)

1. 隨著 AI 技術的普及，「AI 詠唱師」(AI Prompter) 已成為科技業中的新興職務。這個角色需要能夠精確地向 AI 系統下達指令，以生成所需的內容。
   現在若是給你一張圖片，請你設計一個能夠利用 AI 生成一張與原圖高度相似圖像的指令 (prompt)，你會怎麼設計？你的說明可以包含但不限於：使用的 AI 模型或工具、具體的指令內容、關鍵詞選擇等。
   （本題圖片情境採現場抽題，給予 10 秒的思考時間，並在 50 秒內完成作答。）

(以下領域題目皆採現場抽題，出題機率請參照領域標題說明。)

個人資料保護 (領域出題機率約 40%)

2. 如何判定使用者設定的密碼是強密碼？你的說明可以包含：弱密碼與強密碼的定義、數學上如何表示密碼的強弱、設定強密碼的原則、你認為最強的密碼是哪一種密碼。
3. 為什麼我們總是說公共 Wi-Fi 很危險？你的說明可以包含：公共 Wi-Fi 的風險、攻擊者可以透過公共 Wi-Fi 攻擊使用者的方法、使用公共 Wi-Fi 時如何保護自己及其原理。
4. 個人資料包括哪些類型？你的說明可以包含：一般的個人資料、特種個人資料有哪些、哪些行為會觸犯「個人資料保護法」。
5. 請說明資料備份的 3-2-1 原則。你的說明可以包含：3-2-1 原則是什麼、資料備份的模式有哪些、舉例你在生活中如何利用 3-2-1 原則進行資料備份。

6. 使用密碼管理器有哪些好處和潛在風險？你的說明可以包含：密碼管理器的工作原理、使用密碼管理器的優點、可能存在的安全隱患、如何選擇可靠的密碼管理器、使用密碼管理器的最佳實踐。

7. 為什麼及時更新軟體很重要？你的說明可以包含：軟體更新的目的、不更新可能帶來的具體風險、自動更新與手動更新的優缺點、企業環境中的更新策略、如何平衡更新和系統穩定性。

8. 你平常會採取哪些方法來保護自己的網路隱私？你的說明可以包含：常見的網路隱私威脅、保護隱私的具體措施、這些方法的有效原理、技術性和非技術性的保護手段、隱私保護與便利性之間的平衡。

9. 如果你發現自己遇到了資安事件，你會採取哪些立即行動？你的說明可以包含：資安事件的定義和類型、事件響應的步驟、每個步驟的重要性、可能需要聯繫的相關方、如何預防類似事件再次發生。

網路與資安基礎知識 (領域出題機率約 30%)

10. 請說明 OSI 模型的七層結構。你的說明可以包含：每一層的名稱和主要功能、每一層常見的協定或設備。

11. 請比較 TCP 和 UDP 協定的主要差異。你的說明可以包含：連線方式、可靠性的比較、資料傳輸模式、速度，並舉例說明哪些網路使用情境適合使用 TCP，哪些適合使用 UDP。

12. 請說明當我們在瀏覽器（browser）的網址列輸入 https://www.fhsh.tp.edu.tw/ 並按下 Enter 後，到瀏覽器成功呈現復興高中網站前的整個網路傳輸過程。你的說明應包括 DNS 解析、TCP 連線建立、HTTP 請求和回應等步驟。

13. 請說明 HTTP 與 HTTPS 的差異。你的說明會包含：HTTP 與 HTTPS 在網路傳輸過程的差異、HTTPS 如何保護使用者的上網安全、使用 HTTP 可能遭受到的網路攻擊方式。

14. 請說明 IPv4 和 IPv6 的差異。你的說明可以包含：地址格式的差異、地址空間大小、安全性、效能，以及為什麼需要從 IPv4 過渡到 IPv6。

15. 請說明子網路遮罩（Subnet Mask）的概念和作用。你的說明可以包含：子網路遮罩的格式、如何使用子網路遮罩劃分網路、子網路劃分對網路效能和安全性的影響。

16. 請說明資訊安全中的 C、I、A。你的說明可以包含：C、I、A 各自的意義、舉例說明生活中的 C、I、A。

17. 你能解釋病毒和蠕蟲的主要區別嗎？你的說明可以包含：病毒和蠕蟲的定義、兩者的傳播方式、對系統的影響、防護方法、哪一種可能更具破壞性及其原因。

18. 請說明「駭客 (Hacker)」的含意，以及攻擊者的類型。你的說明可以包含：駭客的意思、駭客的通用分類、攻擊者類型的劃分與舉例。

藍隊防禦知識 (領域出題機率約 20%)

19. 請說明資安事件應變計畫（Incident Response Plan）。你的說明可以包含：一個典型的資安事件應變流程、應變團隊的組成、事件分類和優先順序劃分、以及為什麼制定這樣的計畫很重要。

20. 請說明最小權限原則（Principle of Least Privilege）。你的說明可以包含：該原則的核心概念、在系統管理中如何應用這一原則、實施最小權限原則的挑戰、該原則如何提高系統安全性。

21. 請說明資料加密。你的說明可以包含：對稱加密和非對稱加密的差異、常見的加密演算法（如 AES、RSA）、加密在資料傳輸和儲存中的應用、金鑰管理的重要性。

22. 請說明 Zero Trust（零信任）安全模型的核心原則和主要特點。你的說明可以包含：Zero Trust 的定義和起源、傳統邊界

安全模型與 Zero Trust 模型的主要差異、Zero Trust 的基本原則、實施 Zero Trust 架構的關鏈技術。

23. 請說明 CVE（常見漏洞和曝險）系統的目的和運作方式。你的說明可以包含：CVE 的定義、CVE 識別碼的格式和意義、CVE 在資訊安全管理中的重要性、如何使用 CVE 資料庫來增強組織的資安防護。

24. 請解釋 CVSS（通用漏洞評分系統）的作用和評分方法。你的說明可以包含：CVSS 的主要組成部分（基本指標群組、時間指標群組、環境指標群組）、CVSS 分數的計算方式、CVSS v3.0 相較於 v2.0 的主要改進、如何利用 CVSS 分數來優先處理安全漏洞。請舉例說明一個實際的 CVSS 評分，並解釋其中的邏輯。

25. 請詳細說明身分驗證（Authentication）的概念和主要類型。你的說明可以包含：身分驗證 AAA 的定義、單因子 (Single-Factor Authentication，SFA)與多因子身分驗證 (Multi-Factor Authentication，MFA)的定義、常見的身分驗證因素及其例子、這些因素的優缺點比較、多因素身分驗證如何提升系統安全性、為什麼單一因素驗證（如單純使用密碼）不足以保護重要系統，並舉例說明一個結合多種因素的強大身分驗證方案。

26. 請討論新興的身分驗證技術及其在資訊安全中的應用。你的說明可以包含：生物特徵識別技術（如指紋、臉部辨識、虹膜掃描等）的原理和應用場景、行為生物特徵（如擊鍵動態、步態分析等）在持續身分驗證中的運用、無密碼身分驗證（passwordless authentication）的概念和實現方式。

27. 如果你要負責提高一個組織的資安意識，你會採取哪些方法？你的說明可以包含：培訓計劃的內容、執行方式、評估成效的指標、為什麼你認為這些方法會有效、可能遇到的挑戰及解決方案。

紅隊攻防知識 (領域出題機率約 10%)

28. 請說明什麼是密碼攻擊。你的說明可以包含：暴力破解 (brute force attack)和字典攻擊 (dictionary attack)的差異、彩虹表攻擊 (rainbow table)的原理、如何建立和儲存安全的密碼。

29. 請說明中間人攻擊（Man-in-the-Middle Attack）。你的說明可以包含：攻擊的實施過程、可能造成的危害、常見的中間人攻擊類型、以及如何防禦中間人攻擊。

30. 請說明社交工程攻擊。你的說明可以包含：常見的社交工程攻擊方法與媒介、為什麼社交工程攻擊經常非常有效、如何識別和防範社交工程攻擊。

31. 請說明 OWASP 2021 Top 10 中的「A01：失效的存取控制（Broken Access Control）」。你的說明可以包含：這種安全風險的定義、它們可能造成的危害、常見的攻擊方式。

32. 請比較 OWASP 2021 Top 10 與 2017 版本的主要差異。你的說明可以包含：新增的風險項目、被移除的風險項目、排名顯著變化的項目，以及這些變化反映出的網路安全趨勢。

33. 請說明跨站腳本攻擊（XSS）。你的說明可以包含：儲存型 XSS 和反射型 XSS 的差異、XSS 攻擊的原理和可能造成的危害、如何偵測和防禦 XSS 攻擊。

34. 請說明緩衝區溢位攻擊（Buffer Overflow Attack）。你的說明可以包含：攻擊原理、可能造成的危害、常見的攻擊類型（如堆疊溢位、堆積溢位）、以及如何防範這種攻擊。

35. 請詳細說明 網路狙殺鏈 (Cyber Kill Chain) 模型。你的說明可以包含：網路狙殺鏈的定義和目的、七個階段的名稱和內容（偵察、武器化、遞送、攻擊、安裝、命令與控制、行動）、模型的局限性以及它如何與其他威脅模型互補。

36. 請解釋 MITRE ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）框架的結構和應用。你的說明可以包含：ATT&CK 框架的定義和目標、主要組成

部分、ATT&CK 矩陣的結構和內容、ATT&CK 如何區分不同的作戰環境（如企業網路、雲端、行動裝置）、比較 ATT&CK 與 Cyber Kill Chain 的異同。