112 年度第 2 次 資訊安全工程師能力鑑定 初級試題

科目 1：I12 資訊安全技術概論

考試日期： 112 年 11 月 25 日

單選題 50 題（佔 **100%**）

	1. 下列何項是「不好」的網路安全使用習慣？ (A) 監控自己的帳戶是否有任何可疑活動 (B) 慎防社交工程詐騙 (C) 在公共場所使用不明公共無線網路 (D) 實行良好的密碼管理
	2. 關於網路安全敘述，下列何者錯誤？ (A) 網路安全包含：網路裝置安全、網路資訊安全、網路軟體安全 (B) 駭客可透過網路的入侵來達到竊取敏感資訊的目的 (C) 好的網路安全設計只需要單層防護即可 (D) 開啟電子郵件時，相關附件或鏈結務必小心判別
	3. 下列何項「不」屬於網路安全的威脅？ (A) Network Attack (B) USB Attack (C) IP Spoofing (D) Network Eavesdropping
	4. 有關 OWASP Top 10 之敘述，下列何者正確？ (A) 為網路安全的法律規範 (B) 為網路攻擊的報告 (C) 為 ISO 發布的網路安全標準 (D) 為網路應用程式漏洞的指南
	5. 有關 OWASP Top 10 的 A03:2021-Injection 漏洞之敘述，下列何者錯誤？ (A) 將命令與查詢資料分開防止注入攻擊漏洞的發生 (B) 使用安全的應用程式界面（API）防止注入攻擊漏洞的發生 (C) 應用程式相互驗證時容易發生 (D) 使用正向表列或白名單可有效避免此注入攻擊
	6. 當突然發現區域網路中，有大量的電腦連線並傳輸不明的資料時，請問最有可能是下列何種網路攻擊？

	(A) 病毒 (B) 中間人攻擊 (C) 蠕蟲 (D) 鍵盤側錄
	7. 請問 DNS 放大攻擊，最屬於下列何種網路攻擊？ (A) 病毒 (B) 木馬 (C) 蠕蟲 (D) 阻斷服務攻擊
	8. 在系統或網路之間建立一條虛擬的專屬通道，屬於下列何種網路安全技術？ (A) DMZ (B) Tunneling (C) VLAN (D) NAT
	9. 有關防火牆之敘述，下列何者錯誤？ (A) 防火牆是安裝在多個網路之間的網路安全防護裝置，主要目的係用來過濾資料封包 (B) 防火牆是提供控制存取網路資源等服務 (C) 封包是輸入向的（Inbound）都應先經過防火牆的檢查，輸出向的（Outbound）封包則無需檢查 (D) 封包必須符合管理者制定之規則才能予以放行，以防止內部網路受到攻擊
	10. 下列何項技術可以讓組織在公開網路上共用一個外部 IP 位址，與外部只有一個接點有效隱藏內部網路，並能監控進入組織的資料兼具防火牆過濾功能？ (A) NAT (B) DMZ (C) VPN (D) VLAN
	11. 有關位址解析協定（Address Resolution Protocol, ARP）功能

	之敘述，下列何者正確？ (A) 以 IP 位址查詢其相對應之媒體存取控制（MAC）位址 (B) 管理網路流量並決定封包路徑 (C) 對網路流量進行加密與解密，確保安全的通訊 (D) 控制網路流量以防止分段與碎片產生
	12. 在我們使用網路掃描工具 nmap 進行網路探勘時，nmap 通常會先透過 ping 來確認目標伺服器是否可以連線，如果目標伺服器關閉 ping 回應功能，可能會導致 nmap 誤判目標伺服器並未上線。請問下列何項 nmap 指令可以跳過 ping 功能直接開始掃 port？ (A) -sL (B) -Pn (C) -p- (D) -sn
	13. 中間人攻擊（Man-in-the-Middle Attack，又稱為 MITM Attack）是一種用來竊聽、竄改流量的攻擊行為。以下列舉了幾種用來防範中間人攻擊的防禦機制，請問哪一種防範機制已經被驗證有明顯的弱點並且已被建議棄用？ (A) 將位址解析協定設定為靜態（Static ARP），避免 ARP 位址被污染 (B) 在 HTTPS 或 SMTPS 使用 SSLv2 協定來保護傳輸資料，避免被看到明文內容 (C) 使用 DNSSEC 來驗證 DNS 的安全性，避免存取假冒的網域名稱 (D) 只使用家中自行設定的 Wi-Fi 或 4G 網路，並且連上網路之後全程使用公司 VPN，確保網路環境在掌控範圍之內
	14. 關於作業系統安全的描述，下列何者錯誤？ (A) 作業系統的安全架構中希望達到的行程隔離（Process isolation）指作業系統內的各個行程獨立完成，每個行程有隔離機制，互不影響

	(B) 作業系統保護環（Protection rings）的作業系統核心是運行在 Ring3 層 (C) 作業系統的抽象介面（Abstraction interface）指提供使用者使用系統的友善介面，不需要了解使用資源的細節，即可使用系統資源 (D) 安全模式（Safe mode）只有最基本的驅動程式被載入系統執行，以最低程度的狀態啟動電腦，常被用於問題排除時使用
	15. 下列何項「不」屬於作業系統安全性的操作？ (A) 定期更新作業系統：安全更新通常包含重要的修補程式，可修復已知的安全漏洞，因此定期更新作業系統至最新版本是保持安全的一個關鍵步驟 (B) 安裝防病毒軟體：安裝防病毒軟體可以檢測和清除惡意軟體，並且可以提供實時保護，避免系統受到病毒、木馬等威脅 (C) 密碼保護和管理：使用強固的密碼可以保護帳號和機密資訊免於被盜取或破解，定期更換密碼也是保持安全的重要步驟，或採用 2FA 認證登入 (D) 不需要限制權限，可以防止非授權使用者或應用程式存取與執行
	16. 有關作業系統資源配置發生死結（deadlock）之敘述，下列何者錯誤？ (A) 當一系列程序相互持有其他程序所需要的資源時是發生死結（deadlock）的可能因素之一 (B) 系統資源可被強制從一個程序中退出時發生死結（deadlock）的可能因素之一 (C) 某個程序可以在等待同時持有系統資源是發生死結（deadlock）的可能因素之一 (D) 資源只能同時分配給一個程序，無法多個程序共享

	是發生死結（deadlock）的可能因素之一
	17. 當攻擊者取得作業系統存取權限時，通常會想盡辦法翻找伺服器中的系統設定檔，期望在系統中找到其他可用的帳號密碼，以便做為權限控制的備案。下列哪一個 Linux 的檔案內容，包含使用者帳號名稱與密碼雜湊函數？ (A) /etc/shells (B) /etc/sudoers (C) /etc/issue (D) /etc/shadow
	18. 為了讓作業系統變得更安全、更難以入侵，通常企業會對作業系統進行安全強化（Harden），下列何項不是 Linux 作業系統經常採用的安全強化機制？ (A) 設定密碼原則、登入錯誤次數限制，並且使用 fail2ban 服務將登入錯誤次數太多的使用者列入黑名單 (B) 關閉所有非必要的系統服務與通訊協定，但是保留 nmap，以便進行自我掃描跟檢測 (C) 禁止使用 root 帳號登入 SSH 服務，只能使用一般使用者的帳號，若要提升權限變成 root 則必須使用 sudo 指令 (D) 使用 iptables 防火牆功能限制存取來源，讓連線來源最小化
	19. 關於滲透測試（Penetration Test）的敘述，下列何者錯誤？ (A) 滲透測試的工作由一群對網路及系統安全有完整知識與豐富經驗的成員組成，為確保組織資訊安全，不可能委託由第三方負責 (B) 滲透測試是藉由對企業網路採取各種攻擊的手段以便找出系統可能存在的漏洞 (C) 雙黑箱滲透測試主要對內部人員保密下進行 (D) 滲透測試主要考驗系統的安全防護能力
	20. 關於注入攻擊（Injection Attack）的敘述，下列何者錯誤？ (A) 為防止 SQL 注入攻擊，可以採用使用參數化查詢

（Parameterized Query）或預處理語句（Prepared Statement），以將用戶輸入與 SQL 代碼進行隔離

(B) 攻擊者在客戶端和伺服器之間建立兩個獨立的加密通道，讓客戶端和伺服器誤以為他們在進行安全通信，但實際上攻擊者可以監控和篡改通信內容

(C) `SELECT * FROM users WHERE username = 'admin'--' AND password = '用戶輸入的密碼';`
此語法也是一種注入攻擊

(D) `string query = "SELECT * FROM accounts WHERE custID='" + request.getParamter("id") + "'"`
此語法也是一種注入攻擊

21. 關於 Web 攻擊手法的敘述，下列何者錯誤？
(A) SQL 注入攻擊：輸入特定的數據，將 SQL 指令插入到應用程式的資料庫中，獲取敏感資訊或執行未授權的操作，甚至破壞資料
(B) 跨網站腳本攻擊（XSS）：通過在網頁中注入惡意腳本，攻擊者僅可置換網頁內容，但無法對伺服器電腦造成任何影響
(C) 跨站請求偽造攻擊（CSRF）：利用受害者已經驗證過的會話，攻擊者可以在受害者不知情的情況下，執行某些操作，例如更改密碼
(D) 文件上傳漏洞：攻擊者可以通過在網站上上傳惡意檔案，例如病毒、木馬、後門等，從而取得對受害者系統的控制權

22. 當你收到一封電子郵件，告知你因為帳號有異常登入的情況，需要你從信件中的連結去重新設定密碼。請問最有可能是下列何項的情況？
(A) 這是網管善意的提醒，依照指示進行操作
(B) 這是一種釣魚攻擊（Phishing）
(C) 這是一種阻斷服務攻擊（DoS）
(D) 這是一種文件上傳漏洞

23. 下列何種攻擊手法是運用輸入超過預設資料長度的方式，影

	響記憶體中資料的正確性？ (A) 緩衝區溢位攻擊（Buffer Overflow） (B) 釣魚攻擊（Phishing） (C) 阻斷服務攻擊（DoS） (D) XSS 攻擊（Cross-Site Scripting）
	24. 如附圖所示，攻擊者可竄改查詢參數並存取所有帳號資訊，關於此應用程式缺陷的敘述，下列何者錯誤？ https://vulnerable.site/app/account?id=' or '1'='1 (A) 此為結構化查詢語言注入（Structured Query Language Injection） (B) 使用安全 API 來查詢以降低解譯器錯誤之風險 (C) 跳脫（Escape）系統保留字元避免查詢語法遭竄改 (D) 參數檢查機制必須實做於用戶端且使用黑名單過濾
	25. 網站應用程式伺服器允許顯示錯誤訊息給使用者，如：Stack traces，將可能導致機敏資訊外洩或底層元件的弱點被發現，關於此應用程式缺陷的描述，下列何者較正確？ (A) 跨站請求偽造（Cross-Site Request Forgery） (B) 安全設定錯誤（Security Misconfiguration） (C) 認證和驗證失效（Identification and Authentication Failures） (D) 伺服器端請求偽造（Server-Side Request Forgery）
	26. 關於應用程式軟體與資料完整性的敘述，下列何者錯誤？ (A) 使用數位簽章（Digital Signature）來驗證軟體未被竄改 (B) 僅於信任的儲存庫（Repository）取得應用程式套件 (C) 整合測試流程（CI/CD）應適當隔離與存取控制以確保安全 (D) 源碼掃描可有效檢查是否遭植入惡意程式碼（如：後門程式）

	27. 關於 DevOps 的描述，下列何者錯誤？ (A) 為 Development 和 Operations 的混成詞，是一種重視「軟體開發人員（Dev）」和「IT 運維技術人員（Ops）」之間溝通合作的文化、運動或慣例 (B) DevOps 考慮的不止是軟體部署，它是一套針對這幾個部門間溝通與協同運作問題的流程和方法 (C) DevOps 的引入能對產品交付、測試、功能開發和維護，起到意義深遠的影響。在缺乏 DevOps 能力的組織中，開發與運營之間存在著資訊「鴻溝」 (D) 因採用自動化部署手段確保部署任務的可重複性，增加部署出錯的可能性
	28. 從 Microsoft 安全性開發週期（Secure Development Life, SDL）的觀點，靜態程式分析（Static Analysis）主要是下列何項階段的考量？ (A) 需求階段（Requirements） (B) 設計階段（Design） (C) 實作階段（Implementation） (D) 分析階段（Analysis）
	29. 關於電子郵件安全威脅的敘述，下列何者錯誤？ (A) 電子郵件可能會遇到的資安問題，例如：冒名郵件、垃圾郵件、詐騙郵件、黑函郵件、病毒（木馬）郵件、釣魚郵件等 (B) 一般詐騙郵件的手法，都會要求收信者點選一個連結網址，並將收信者引導到一個仿冒的假網站，然後再要求他提供、更新或確認機密的個人資料 (C) 詐騙郵件通常企圖獲取個人的重要資訊 (D) 電子郵件的安全以詐騙為主，未曾發現針對技術性弱點的攻擊
	30. 關於惡意程式的敘述，下列何者錯誤？ (A) 蠕蟲（worm）是一種獨立的惡意程式，它透過網路

	主動傳播自身以感染其他系統計算機，可在不感染文件、檔案的情況下複製自己 (B) 特洛伊木馬（Trojan horse）是一種有害程式，它會偽裝成普通的良性程式或實用程式，以使受害者安裝它 (C) Rootkit 透過修改作業系統程式取得 Root 權限的惡意程式 (D) 電腦病毒是通常隱藏在另一個看似無害的程序中的軟體，它可以生成自身的副本並將其插入到其他程序或文件中，並且通常會執行有害的作業
	31. 關於惡意程式防護與弱點管理的敘述，下列何者錯誤？ (A) IOC（Indicators of Compromise）稱作入侵威脅指標 (B) TTPs（Tactics, Techniques and Procedures）是指戰術、技術與程序，被應用在網路安全 (C) IOA（Indicators of attack）攻擊指標，會記錄攻擊來源、hash 值或 URL (D) Zero Trust Security 也是一種惡意程式防護與弱點管理手段
	32. 通用漏洞評分系統（Common Vulnerability Scoring System, CVSS）定義了數個指標組用來評定電腦系統安全的嚴重性及風險程度，請問有關 CVSS 3.1 評分指標組之敘述，下列何者正確？ (A) 強制的基本指標組、強制的時間指標組以及可選擇的環境指標組 (B) 強制的基本指標組、強制的環境指標組以及可選擇的時間指標組 (C) 可選擇的基本指標組、強制的時間指標組以及可選擇的環境指標組 (D) 強制的基本指標組、可選擇的環境指標組以及可選擇的時間指標組

	33. 企業為了檢查自己是否會被已知的弱點攻擊，通常會定期安排弱點掃描，以便檢查是否有應用程式或作業系統的漏洞出現在企業的環境中。下列何項「不」是常見的弱點掃描工具？ (A) OSV-Scanner (B) Nessus (C) OpenVAS (D) Masscan
	34. 資料治理（Data Governance）是近期重要的政策推動目標，關於資料治理的敘述，下列何者錯誤？ (A) 資料治理對於許多組織和行業都很重要，尤其是那些具有法規遵從性的組織和行業，如金融和保險業 (B) 資料保管人須負起安全保管、傳輸、儲存和其執行業務 (C) 資料治理並不包含個人資料以及隱私資訊 (D) 資料進行利用分析時，仍需要注意資料安全相關保護措施
	35. 確保資料安全的防護措施，下列敘述何者錯誤？ (A) 手機上啟用雙因子身份驗證（2FA），這將減少駭客對工作相關系統與資料惡意存取 (B) 網路零信任設計主要強調在人對系統資料存取安全防護，例如帳號密碼，可以不用考慮到何種裝置連線信任關係 (C) 加密軟體是一種安全程式，可在傳輸和儲存時保護資料的機密性 (D) 員工應該使用虛擬專用網路（VPN）來存取公司資料
	36. 利用零信任（Zero Trust）來保護資料完整性，下列敘述何者錯誤？ (A) 在零信任設計上，存取決策不受加密控制 (B) 在零信任設計上，資料須能夠自動分類和標記

	(C) 可以透過敏感度標籤和內容檢查的資料外洩防護（Data Loss Prevention, DLP）策略防止資料洩露 (D) 定期審核資料以瞭解用戶標籤、分類和保護活動
	37. 當 A 公司的備份策略是每個月底最後一天的晚上 6 點後進行一次全備份，而每週六凌晨 1 點進行一次差異備份，假設所有備份檔案都完整，今天 3 月 10 日剛好是週五，中午時不幸系統中毒，所有資料遺失，請問當備份順利還原後，最近的資料是下列哪一天的備份？ (A) 2 月 28 日 (B) 3 月 4 日 (C) 3 月 9 日 (D) 3 月 10 日
	38. 異地備援是資料備份最好的選擇，其復原速度最快的是下列何種方式？ (A) 冷備援（Cold Site） (B) 暖備援（Warm Site） (C) 熱備援（Hot Site） (D) 全備援（Mirrored Site）
	39. 企業透過日誌管理，處理大量且複雜的日誌資訊（例如：logs & events），IT 部門或是資安部門將這些記錄使用在容量監控管制、故障排除、合規性記錄留存、資安威脅檢測與鑑識…等目的，關於日誌管理的敘述，下列何者錯誤？ (A) 可用於事件取證，日誌資訊對於原因的判別是關鍵點，而在還不確定原因之前，則需要全面性的收集日誌資訊 (B) 為了滿足不同的法規規範，日誌成為稽核重要的參考資料 (C) 日誌管理，可以用在事件警示，卻不適用在 SOC（Security Operation Center）管理 (D) 沙賓法案（SOX）或是醫療保險相關法案

（HIPAA）這一類的法遵，都會要求讓日誌成為重要稽核軌跡（audit trail）

40. 關於 Linux 系統日誌資料的敘述，下列何者正確？
(A) /var/log/lastlog 記錄系統中所有用戶最後一次的登錄時間。可直接用 vi 查閱，但需搭配使用 lastlog 命令進行
(B) /var/log/cron 記錄與系統設定任務相關的日誌
(C) /var/log/dmesg 記錄系統關機時，內核自我檢查資訊，也可以使用 dmesg 命令直接查看內核自檢資訊
(D) /var/log/secure 記錄郵件資訊的日誌

41. Windows Event Log 是重要稽核與資安鑑識記錄檔，關於 Windows Event Log 的敘述，下列何者錯誤？
(A) windows event log 預設位置為：%SystemRoot%\System32\winevt\Logs\
(B) 關於 windows event log 相關設定與調整在：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
(C) windows event log 只有三類，無法再擴充其他類型 event log
(D) 以 Security.evtx 為例，包含主機的 Login/Logout 資訊，還有其他安全事件相關的 log

42. 如附圖所示，關於此筆 Apache 記錄的敘述，下列何者錯誤？

```
218.19.140.242
--[10/Dec/2010:09:31:17 +0800]
"GET /query/trendxml/district/todayreturn/month/2009-12-14/2010-12-09/haizhu_tianhe.xml HTTP/1.1"
200
1933
"-"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)"

註：為方便閱讀，將記錄分段呈現
```

(A) 218.19.140.242 這是一個 apache 伺服器的 local 端 IP
(B) [10/Dec/2010:09:31:17 +0800]格式為[day/month/year:hour:minute:second zone]，最後的+0800 表示伺服器所處的時區
(C) 1933 表示伺服器向客戶端傳送多少位元組，把這些位元組加起來得知伺服器在某點時間內總的傳送資料量

	(D) "Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)" 這項主要記錄客戶端的瀏覽器資訊
	43. 關於「日誌管理」的敘述，下列何者錯誤？ (A) 日誌管理不會與法律合規性有任何關連性 (B) 日誌未安全存放，很有可能被駭客或惡意破壞者刪除或修改 (C) 安全資訊和事件管理（Security Information and Event Management，SIEM）其中功能是達成降低資安威脅 (D) 透過日誌管理系統統一分析，可以用在鑑識攻擊事件追蹤分析
	44. 依照雲端運算聯盟（Cloud Security Alliance, CSA）於 2019 年 8 月發表雲端運算面臨十一大安全威脅報告中，請問賦予超過實際所需的權限是下列何種安全威脅？ (A) 資料外洩 (B) 設定錯誤 (C) 策略缺乏 (D) 認證不足
	45. 使用雲端資料庫與應用程式十分方便，但若設定稍有不慎將導致資料外洩或是服務遭到攻擊，下列何項是因設定不慎而導致問題，同時也列為 OWASP TOP 10 2021 之一的漏洞？ (A) Cryptographic Failures (B) Security Misconfiguration (C) Vulnerable and Outdated Components (D) Software and Data Integrity Failures
	46. 行動裝置資通安全應注意事項，下列敘述何者錯誤？ (A) 安裝來自可信任來源之軟體，確保軟體來自於官方軟體商店（如 App Store、Google Play） (B) 行動裝置 App 或 OS 應定期自動或手動安裝更新修補程式 (C) 公司可利用行動裝置管理系統（Mobile Device

Management, MDM）管理公司或單位內配發的行動裝置

(D) 使用者在行動裝置上安裝軟體時，可以信任該 App 並授權 App 所要求之權限，例如：GPS 資訊、通訊錄、及啟用系統工具

47. 關於行動裝置的安全保護措施，下列敘述何者錯誤？
(A) 軟體下載與使用應該檢視權限的要求，確保沒有資料外洩的風險
(B) 軟體應定期自動或手動安裝更新修補程式
(C) 資安威脅不會影響行動裝置的電池壽命
(D) 行動裝置管理系統（Mobile Device Management, MDM）會限制行動裝置的行為，甚至可以遠端變更與清除行動裝置的內容

48. 在資安標準作業規範 ISO/IEC 27002 中，針對 BYOD 的指導綱要與安排項目，「不」包含下列何項？
(A) 提供適當的通信設備，包括保護遠端存取的方法
(B) 提供軟硬體支援與維護
(C) 稽核與安全監視
(D) 對行動裝置進行滲透測試

49. 開放網路軟體安全計畫（Open Web Application Security Project, OWASP）組織針對物聯網裝置安全問題進行統計，歸納出物聯網常見的十項安全性問題（OWASP IoT TOP 10）。請問下列何項是附圖中物聯網常見的十項安全性問題的前三名（不分順序）？

1.Weak, Guessable, or Hardcoded Passwords（弱密碼、可猜測密碼或裝置預設密碼）
2.Insecure Default Settings（不安全的預設設定）
3.Insecure Ecosystem Interfaces（不安全的環境設定介面）
4.Lack of Secure Update Mechanism（缺乏安全的更新機制）
5.Insecure Data Transfer and Storage（不安全的資料傳輸和儲存）
6.Insecure Network Services（不安全的網路服務）

(A) 1、3、5
(B) 2、4、6

	(C) 1、3、6 (D) 1、2、3
	50. 下列何項標準「不」是針對物聯網設備？ (A) NIST SP 800-213 (B) ETSI EN 303 645 (C) ISO 27400 (D) IEC 62443-3-2