

甄試類別【代碼】：資訊稽核類八職等【C21106108】

專業科目：(1)系統管理(含作業系統管理、資料庫系統管理與網路管理)
(2)資訊安全管理(含資訊安全管理制度、Firewall、IPS、WAF、AD 與 SOC、SIEM、防毒等)

*入場通知書編號：_____

注意：①作答前應先檢查答案卡（卷），測驗入場通知書編號、座位標籤、應試科目是否相符，如有不同應立即請監試人員處理。使用非本人答案卡（卷）作答者，該節不予計分。
②本試卷為一張雙面，測驗題型分為【四選一單選選擇題 30 題，每題 2 分，共 60 分；非選擇題 3 大題，請見各題配分，共 40 分】，共 100 分。
③四選一單選選擇題限以 2B 鉛筆於答案卡上作答，請選出一個正確或最適當答案，答錯不倒扣；以複選作答或未作答者，該題不予計分。
④非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採橫式作答，並請依標題指示之題號於各題指定作答區內作答。
⑤請勿於答案卡（卷）上書寫應考人姓名、入場通知書編號或與答案無關之任何文字或符號。
⑥本項測驗僅得使用簡易型電子計算器（不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝（錄）影音、資料傳輸、通訊或類似功能），且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。
2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑦答案卡（卷）務必繳回，未繳回者該節以零分計算。

壹、四選一單選選擇題 30 題（每題 2 分）

- 【3】1.下列有關 IPv6 的敘述何者錯誤？
① IPv6 位址共有 128 位元
② IPv6 的標頭和 IPv4 不同
③ IPv6 的標頭欄位長度是可變的
④ IPv6 沒有廣播(Broadcast)封包
- 【3】2.下列哪個欄位不會出現在封包中？
①來源 IP 位址
②目的 IP 位址
③閘道器 IP 位址
④來源 MAC 位址
- 【1】3. IP 位址不容易被人們記住，而是採用網域名稱。請問網域名稱需要靠下列哪個服務轉換成 IP 位址？
① DNS
② SNMP
③ SMTP
④ POP3
- 【3】4.電子郵件之發送是采用下列哪個服務？
① DNS
② SNMP
③ SMTP
④ POP3
- 【2】5.具安全機制之遠端登入是采用下列哪個服務？
① SNMP
② SSH
③ TELNET
④ SFTP
- 【3】6.網頁採用 HTTPS 可以保障資料傳輸的安全性，請問預設的通訊埠是多少？
① 80
② 591
③ 443
④ 8080
- 【2】7.請問要保護網頁應用的安全，應該採用下列哪個設備最好？
① Firewall
② WAF
③ IPS
④ IDS
- 【4】8.第二層交換器(Layer-2 Switch)是靠哪一個項目作為識別來轉送封包？
①網域名稱
②傳輸層埠號(Port)
③網路 IP 位址
④實體位址(MAC Address)
- 【2】9.下列何種技術被普遍使用在私有網路(Private Networek)中，多台主機共同通過一個公有 IP 位址(Public IP Address)訪問網際網路？
① Firewall
② NAT
③ VPN
④ SSH
- 【2】10.下列哪個協定用於網際網路協定(IP)中傳送控制訊息，提供可能發生在通訊環境中的各種問題回饋？
① ARP
② ICMP
③ IGMP
④ PPTP

- 【3】11.無線網路協定 802.11ax、802.11b、802.11n，依速度快慢排列應為下列何者？
① 802.11ax > 802.11b > 802.11n
② 802.11n > 802.11b > 802.11ax
③ 802.11ax > 802.11n > 802.11b
④ 802.11n > 802.11ax > 802.11b
- 【3】12.在微軟視窗系統中，要透過 DNS 伺服器查詢網域名稱之 IP，要用下列哪個指令？
① ipconfig
② mkdir
③ nslookup
④ tracert
- 【4】13.資料鏈結層(Data Link Layer)的封包中，最後加入的封包尾端的欄位是什麼？
①封包目的地
②封包路由紀錄
③封包長度
④檢查碼
- 【2】14.下列何者不是雲端運算主要的類型？
①基礎架構即服務(IaaS)
②資料即服務(DaaS)
③平台即服務(PaaS)
④軟體即服務(SaaS)
- 【4】15.下列關於虛擬區域網路(VLAN)的敘述何者錯誤？
①不同 VLAN 之間不能相互直接通訊
②同一台交換器可以設定屬於不同的 VLAN
③增加 VLAN 會增加廣播群組的數量，而減少廣播群組的大小
④設定 VLAN 會增加網路資安的風險
- 【4】16.在資安事件分析中，為了深入瞭解駭客的入侵技術和行為模式，一些組織會特意設置具有脆弱性的伺服器，吸引駭客進行攻擊。這樣的行為被歸類為哪一種安全措施？
①滲透測試(Penetration Test)
②多層次防禦(Layered Defense)
③白箱測試(White-Box Testing)
④蜜罐(Honeypot)
- 【2】17. B 公司預計使用一個新的客戶關係管理工具。在進行適當的研究後，他們決定購買雲端託管解決方案的訂閱。B 公司需要執行的唯一管理任務為管理使用者帳戶。供應商將負責硬體、作業系統及軟體管理，包含修補與監控。下列何者類型為該上述解決方案？
① PaaS
② SaaS
③ CaaS
④ IaaS
- 【1】18.在進行稽核時，下列何者原則為錯誤？
①稽核測試應在非工作時間進行，以減少對系統可用性的影響
②應與合適的管理者商定對系統與資料存取的稽核要求
③稽核測試應限於對軟體與資料的唯讀存取
④技術稽核測試的範圍應商定並被控制
- 【3】19. FIDO(Fast Identity Online)認證機制的主要特點是什麼？
①它依賴於使用者的帳號密碼來進行身份驗證
②它允許單一伺服器存儲所有使用者的私鑰
③它使用生物辨識技術，如指紋或臉部識別，來進行身份驗證
④它需要使用者在每次登錄時都提供新的個人資料
- 【3】20.電子郵件常用的數位簽章(Digital Signature)，其目的是保護下列哪些資訊安全要素？
①完整性(Integrity)與可用性(Availability)
②機密性(Confidentiality)與不可否認性(Non-Repudiation)
③完整性(Integrity)與不可否認性(Non-Repudiation)
④機密性(Confidentiality)與可用性(Availability)

【4】21.使用惡意軟體感染系統並取得系統或網頁應用程式的憑證與使用者帳號、密碼。上述攻擊屬於網路攻擊鏈(Cyber Kill Chain)的哪一個階段？

- ①安裝 ②偵查 ③遞送 ④行動

【2】22.關於電腦機房安全管理，下列敘述何者錯誤？

- ①廠商維護人員進入機房，應由機房管理人員全程陪同
②攜帶非工作所需物品進入機房需經過登記
③不可裝設自動灑水之滅火設備
④應定期執行清潔作業

【2】23.關於密碼管理之敘述，下列何者正確？

- ①通行碼需由大小寫字母、數字及特殊符號組成，長度則與安全性無關
②使用者初次登入電腦系統後必須立即更改預設之通行碼
③通行碼之設定如果夠安全，則無須限制輸入錯誤之次數
④可將個人有關資訊如生日、身份證字號、電話等混合成通行碼使用，以達到安全又好記的通行碼設定

【3】24.職責分離(Separation of Duties)在資訊安全中的主要目的是什麼？

- ①確保所有員工都能夠執行所有任務
②確保所有員工都能夠訪問所有數據
③防止單一員工擁有完成一項任務所需的所有權限
④防止員工休假時的工作中斷

【4】25.零信任(Zero Trust)為一種資訊安全的架構，透過個人身分驗證與設備驗證，進而保護個人行動裝置、第三方應用程式、電子郵件及網路等。零信任架構包含多項要素，請問下列何者非零信任架構之要素？

- ①特權存取管理(PAM)
②持續監控
③身分與存取管理(IAM)
④使用預設密碼進行帳號驗證

【1】26.若 A 公司不能接受重要系統中斷超過 1 小時，下列何項異地備援方式最不適合該公司？

- ①冷備援 ②熱備援 ③溫備援 ④機房內自主備援

【3】27.當小政在掃描一台主機時，他想確認目標主機是否開啟防火牆。為了確定防火牆運作狀態，建議他使用下列何者 Nmap 指令選項？

- ① -sF ② -sT ③ -sA ④ -sX

【2】28.資訊安全的基本原則中，下列哪一項原則是指系統能夠防止未經授權的存取？

- ①可用性(Availability)
②機密性(Confidentiality)
③完整性(Integrity)
④可認證性(Authenticity)

【3】29.網路防火牆(Firewall)一般不具備下列哪一項功能？

- ①網路連線管理稽核
②集中安全控管
③病毒偵測
④阻絕異常存取

【1】30. Smurf 攻擊是一種分散式阻斷服務(DDoS)攻擊。在 Smurf 攻擊中，攻擊者通常會做什麼？

- ①透過偽造來源位址為目標受害者的 IP 位址，將詐騙封包傳送至路由器或防火牆的 IP 廣播位址
②直接向目標受害者的 IP 位址發送大量的請求，以達到 DDos 的目的
③刪除目標受害者的所有數據，使其無法提供正常服務
④立即關閉目標受害者的網路連接，使其無法對外連線

貳、非選擇題 3 大題（占 40 分）

第一題：

請回答下列作業系統之相關問題：

- （一）何謂 GCB(Government Configuration Baseline)？【4 分】
（二）為什麼須對作業系統訂定 GCB？【3 分】
（三）列舉三項與作業系統有關的 GCB 項目。【3 分】

第二題：

請回答下列資料庫系統管理的相關問題：

- （一）下列二道 SQL 指令的目的分別為何？【4 分】
`grant view definition on scheme:: members to public`
`revoke select on members from public`
（二）列舉三項使用資料庫可能潛在的缺點。【3 分】
（三）說明何謂 NoSQL？為什麼需要它？【3 分】

第三題：

請回答下列資訊安全相關問題：

- （一） SIEM (Security Information and Event Management)如何進行威脅偵測和威脅回應？其與 SOC 之相關性為何？【5 分】
（二）請舉出 3 種 WAF(Web Application Firewall)可以防止的網路攻擊類型。並說明其與防毒之關聯。【5 分】
（三）請說明 IPS(Intrusion Prevention System)與防火牆的差異為何？【5 分】
（四） Kerberos 是 Windows AD(Active Directory)的身分驗證協定之一，請說明該驗證方式的運作原理。【5 分】