台灣電力公司 110 學年度大學及研究所獎學金甄選試題

類科:電網資訊安全 **節次:第一節**

科目:網路安全

注意事項	1.本試題共 4 頁，採雙面印刷，請注意正、背面試題。 2.僅限使用簡易型計算器（不限廠牌、型號，功能以不超出＋、－、×、÷、%、√、MR、MC、MU、M+、M-、GT、TAX+、TAX-之運算為限；其他具有文數字編輯、發聲、振動、記憶儲存、內建程式、外接插卡、通訊或類似功能之計算工具一律禁止使用）。 3.本試題為單選題共 50 題，每題各 2 分，共 100 分，須用 2B 鉛筆在專業科目答案卡畫記作答，於本試題、英文答案卡或其他紙張作答者不予計分。 4.測驗式試題均為單選題，每題選項應有 4 個，以(A) (B) (C) (D)標示，請就各題選項中選出最適當者為答案；各題答對得該題所配分數，答錯不倒扣；畫記多於 1 個選項或未作答者，該題不予計分。 5.考試結束前離場者，試題須隨答案卡繳回，俟該節考試結束後，始得至原試場索取。 6.考試時間：與英文合併一節考試，共120分鐘。

1.下列哪種技術可以解決 IPv4 位址不足的問題？

(A) VPN (B) DMZ (C) POP3 (D) NAT

2.下列關於網路通訊協定 TCP 與 UDP 之敘述，何者正確？

(A) TCP 傳送較不可靠 (B) UDP 保證正確傳送 (C)僅 TCP 屬傳輸層 (D) UDP 傳輸較不可靠

3.下列何者為常用之網管協定？

(A) SNMP (B) SMTP (C) Kerberos (D) DNS

4.常用來進行區域網路故障排除的指令 ping，其送出的封包為下列何者？

(A) TCP (B) ICMP (C) HTTP (D) UDP

5.路由器屬於 OSI 七層中的哪一層？

(A)傳輸層 (B)實體層 (C)網路層 (D)連結層

6.某台主機的 IP 及子網路表示法為 200.1.1.130/28，請問其十進位遮罩(Subnet Mask)為何？

(A) 255.255.255.32 (B) 255.255.255.64 (C) 255.255.255.128 (D) 255.255.255.240

7.某公司擁有 Class C 的 IP 位址，其 IP 位址範圍為 203.74.205.0~203.74.205.255，遮罩為 255.255.255.0，若此公司再將內部分成 4 個獨立的子網路，其子網域遮罩為下列何者？

(A) 255.255.255.128 (B) 255.255.255.192 (C) 255.255.255.224 (D) 255.255.255.240

8.下列何者的服務與預設通訊埠有誤？

(A) SMTP/25 (B) DNS/53 (C) HTTPS/443 (D) SSH/43

9.下列關於網路設備之敘述，何者有誤？

(A)中繼器(repeater)主要目的為增加訊號強度，將訊號傳送到更遠處

(B)橋接器(bridge)可讓資料通過，連接到同網路的不同區段

(C)路由器(router)可以連接到不同的區域網路

(D)閘道器(gateway)無法連接到不同通訊協定的異質網路

10.下列何種區域網路的佈建方式具較高故障容忍度(Fault Tolerance)？

(A)網狀(mesh) (B)星狀(star) (C)環狀(ring) (D)樹狀(tree)

11.下列何者不是 IPv6 的特性？

(A)提供比 IPv4 更多的位址 (B)較 IPv4 更好的路由效率

(C)具有自動設定(Auto-Configuration)機制 (D)位址長度為 256 位元

【請翻頁繼續作答】

12.下列關於 TCP/IP 通訊協定之敘述，何者有誤？
(A)電子郵件對應於應用層　(B) Port Number 對應於傳輸層
(C) IP 位址對應於實體層　(D) MAC 位址對應於連結層

13.下列何者不是 VPN 通訊協定？
(A) IPSec　(B) L2TP　(C) HTTPS　(D) PPTP

14.使用 SSL 進行通訊時，雙方須取得對方憑證並確認是否有效，主要在防止下列何種攻擊？
(A)跨站腳本攻擊(XSS Attack)　(B)中間人攻擊(Man-in-the-middle Attack)
(C)重送攻擊(Replay Attack)　(D)阻斷服務攻擊(Denial of Service)

15.下列何者不是資料安全(Security)機制的目標？
(A)確認網路上收到的資料沒有被竄改過　(B)發送者無法假冒他人身分發送
(C)發送者無法否認所發送的資料　(D)資料異地備份

16.網路竊聽器是指會執行下列哪個動作的軟體或硬體？
(A)記錄使用者活動，並將其傳送至伺服器　(B)保護工作站避免遭入侵
(C)將網路資料歸類以建立安全索引　(D)擷取並分析網路通訊

17.下列關於網路安全之敘述，何者有誤？
(A)蠕蟲(worm)會自我大量複製散播到網路，並癱瘓其他電腦及網路資源
(B) Ping 封包攻擊是屬於「阻斷服務(DOS)」攻擊
(C) WannaCry 病毒是利用資料庫的漏洞進行攻擊
(D)網路釣魚(phishing)是利用垃圾郵件、假網站等技術，來誘騙機密資訊

18.下列何者不是雜湊函數(Hash)的特性？
(A)無論輸入雜湊函數的資料長度為何，產生的雜湊值長度固定
(B)從雜湊值無法反推出輸入的資料
(C)輸入資料雖僅一個位元不同，但是產生的雜湊值卻有很大的差異
(D)使用公開金鑰加密

19.下列何者不是 PKI 公開金鑰基礎建設的目的？
(A)存放私密金鑰的地方　(B)建立具公信力的憑證管理中心
(C)防止公開金鑰的冒充　(D)公佈公開金鑰提供大眾取用

20.下列何者不是預防勒索病毒的方法？
(A)安裝防毒軟體　(B)修補作業系統漏洞　(C)避免跨站腳本漏洞　(D)加強社交工程訓練

21.下列何者為對稱式金鑰加解密使用的函數？
(A) RSA　(B) DES　(C) MD5　(D) SHA

22.下列何者不是非對稱金鑰的特性？
(A)私鑰用於資料加密，公鑰用來確認身分
(B)從公鑰無法推導出私鑰
(C)公鑰必須公佈
(D)利用一對公鑰與私鑰，搭配加解密函數，執行加密與解密

23.下列何者不是電子簽章的特性？
(A)必須依附於電子文件
(B)必須能辨識簽署人的身份
(C)必須能利用電子簽章辨識電子文件的真偽
(D)把自己的簽名，以掃描器製作成圖檔，附加於電子文件

24.下列何者不是預防網路竊聽的方法？
(A)使用 HTTPS　(B)使用 SFTP 傳檔案
(C)使用 hub 取代 switch　(D)監控 ARP TABLE 的改變

【請另頁繼續作答】

25.下列何者為將多個 TCP 同步化(SYN)封包傳送到端點，造成端點持續傳送同步化確認(SYN/ACK)回應，最後耗盡端點記憶體而當機的攻擊手法？
(A) LAND Attack (B) SYN Flood
(C) Overlapping Fragment (D) Ping of Death

26.下列何者不是駭客攻擊網頁的手法？
(A)資料庫隱碼攻擊法(SQL Injection) (B)隱藏欄位法(Hidden-field-tampering)
(C)混淆攻擊法(URL Obfuscation) (D) ARP 欺騙(ARP spoofing)

27.下列何種攻擊是利用社交工程達成目的？
(A)重送攻擊 (B)網路釣魚攻擊 (C)中間人攻擊 (D)反射式攻擊

28.下列何者為使用 10 進位或 2 進位的數字來替代原網站 IP，以避過網路檢查的攻擊方式？
(A)資料庫隱碼攻擊法(SQL Injection) (B)隱藏欄位法(Hidden-field-tampering)
(C)混淆攻擊法(URL Obfuscation) (D)搜尋引擎攻擊法(Google-hacking)

29.規劃縱深防禦時，我們常採用多種不同面向的管控措施，下列何者屬預防性存取管控措施？
(A)入侵偵測系統(Intrusion Detection System) (B)異地備份
(C)加密 (D)側錄系統(Session recording system)

30.下列關於降低網站風險之敘述，何者正確？
(A)已經建立網站應用程式防火牆(WAF)系統，故主機作業系統不需再升級更新
(B)系統更新新版程式後，應將舊版程式留存於上線主機，作為將來改錯後的原始碼修正使用
(C)網站前端與後台管理的資料庫連線帳號密碼，不須區隔讀取與寫入刪除的資料庫權限
(D)定期進行網站黑箱檢測及系統弱點掃描，對其程式碼應進行 Code Review

31.在網站弱點檢測報告中，發現系統本身有存在路徑暴露(Path Manipulation)問題時，可以採取下列何種方案進行修補？
(A)使用 Prepare Statement (B)使用 HTML.Encode
(C)使用圖像式驗證 (D)使用白名單路徑及黑名單危險字串過濾

32.勒索病毒使用對稱式加密技術與非對稱式加密技術，加密電腦內的檔案，讓使用者無法使用，此現象主要影響資訊系統的何種特性？
(A)機密性(Confidentiality) (B)完整性(Integrity)
(C)可用性(Availability) (D)鑑別性(Authenticity)

33.採暴力攻擊的方式破解以小寫英文和數字所組成的八位密碼，最多要嘗試多少次？
(A) $(26+10)^8$ (B) 26^8+10^8 (C) $(10+26)\times 8$ (D) $C_8^{(10+26)}$

34.下列何種技術不適合作為身分驗證使用？
(A) RMON (B) RADIUS (C) LDAP (D) TACACS

35.憑證記載了個人資料、公開金鑰、數位簽章、有效期限等資訊，下列何者不是憑證的特性？
(A)可用性 (B)身分識別 (C)不可否認性 (D)完整性

36.下列何者不是遭受 DDoS(Distributed Denial-of-Service)攻擊的常見特徵？
(A)網站內容只有影片可以播放 (B)電腦與伺服器作業系統或服務超載
(C)網路設備或防火牆不堪負載 (D)網路頻寬滿載

37.下列何種無線網路通訊協定的傳輸速度最快？
(A) 802.11a (B) 802.11ac (C) 802.11b (D) 802.11n

38.下列關於入侵檢測系統(IDS)與入侵預防系統(IPS)之敘述，何者有誤？
(A) IDS 的防禦方式為被動監聽
(B) IPS 的防禦方式為主動防禦
(C) IDS 的防禦動作可透過 TCP Reset 中斷連線
(D) IPS 不具備特徵值偵測(Signature-based Detection)的技術

【請翻頁繼續作答】

39.下列關於零信任安全架構(Zero Trust Architecture)之敘述，何者有誤？
(A)假設不信任任何人為前提的安全架構
(B)網路、連線設備、軟體程式等，都必須經過認可及驗證
(C)零信任包含：網路、設備、使用者、資料，但不包含工作負載(Workloads)
(D)零信任安全架構四大支柱：身分可信、架構可信、存取可信、服務可信

40.使用 Nmap 對某重要主機(具檔案伺服器與資料庫功能)進行滲透測試，以瞭解該主機漏洞是否已全數修補完成，下列何者為此工具最主要之目的？
(A)利用該主機已知之漏洞下載資料庫 (B)利用該主機已知之漏洞竊取檔案
(C)利用該主機已知之漏洞提升權限 (D)利用該主機已知對外開放之服務埠進行情蒐

41.下列哪種作法無法有效避免暴力破解密碼(Brute-Force)？
(A)加鹽(Salting) (B)雜湊演算 (C)密碼複雜度要求 (D)金鑰延伸

42.下列關於滲透測試與弱點掃描(Vulnerability Assessment)差異之敘述，何者正確？
(A)滲透測試主要為自動化掃描軟體檢測，只檢測既有安全漏洞
(B)弱點掃描為針對客戶的目標系統模擬、發掘安全漏洞並提出改善方法的善意行為
(C)弱點掃描能檢測出最新的資安或邏輯思維的漏洞並給予修補建議
(D)滲透測試為模擬惡意駭客的攻擊方法，目的在於驗證與評估資訊系統與硬體安全性

43.下列何種方式可以防範資料隱碼攻擊？
(A)字串輸入檢查過濾 (B)使用 SSL 加密 (C)加入圖形驗證 (D)加裝防毒軟體

44.下列何種工具最不適合進行滲透測試？
(A) NetCat (B) Burp Suit (C) Putty (D) Charles

45.下列關於零時差攻擊(Zero Day Attack)之敘述，何者正確？
(A)惡意攻擊系統的時間在午夜 12 點
(B)惡意攻擊系統的時間不超過 1 天
(C)當系統被惡意攻擊後，立即失效無法使用
(D)系統被發現具有風險性弱點後，修正程式發佈前所進行的惡意攻擊行為

46.驗證應用程式並識別潛在的安全性缺陷，一般會使用下列哪 2 種技術？
①滲透測試 ②弱點掃描 ③源碼檢測 ④單元測試
(A) ①③ (B) ①④ (C) ②③ (D) ②④

47.搜尋引擎攻擊主要在破壞資訊系統的何種特性？
(A)機密性 (B)完整性 (C)可用性 (D)責任性

48.下列何者為預防社交工程攻擊的最好方法？
(A)教育訓練及宣導 (B)安裝入侵偵測系統 (C)安裝端末管理機制 (D)安裝網站過濾伺服器

49.下列關於蜜罐(Honeypot)之敘述，何者正確？
(A)設置於正式運作環境之中 (B)任何連線蜜罐的行為都是可疑的
(C)偽裝價值且具漏洞的系統，誘使駭客攻擊 (D)提供網路服務

50.下列關於模糊測試之敘述，何者有誤？
(A)是一種軟體測試技術 (B)建立測試的程序並發現未知錯誤
(C)測試工具主要分為變異測試以及生成測試 (D)模糊測試無法找出資料隱碼的漏洞