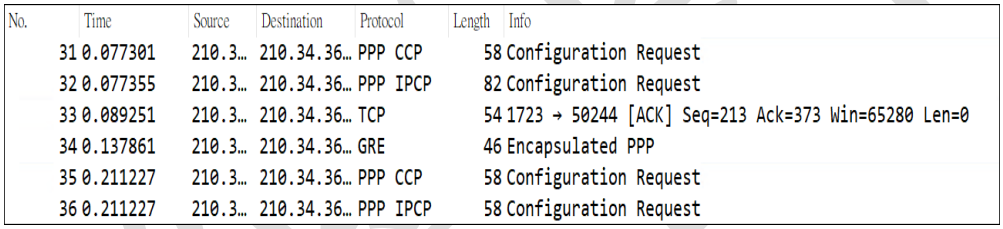
111 年度初級資訊安全工程師能力鑑定試題

科目 2：資訊安全技術概論
考試日期：111 年 05 月 28 日　　第 1 頁，共 10 頁

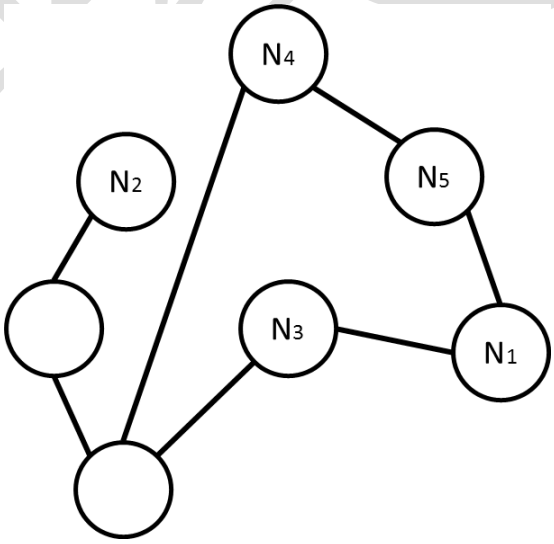
單選題 50 題（佔 100%）

D	1. 下列 OSI 模型層次，何者定義 IPSec 協定？ (A) 資料鏈結層（Data Link Layer） (B) 傳輸層（Transport Layer） (C) 會議層（Session Layer） (D) 網路層（Network Layer）
D	2.「攻擊者利用網站的漏洞把惡意程式腳本注入到網頁內，當使用者瀏覽其網頁時，將會執行網頁內注入的惡意程式碼，可能造成 Cookie 資料被竊取、Session 連線被劫持或釣魚欺騙等攻擊。」請問上述屬於下列何種攻擊方法？ (A) 安全性設定疏失（Security Misconfiguration） (B) 身分驗證功能缺失（Broken Authentication and Session Management） (C) 跨網站偽造請求（Cross-Site Request Forgery, CSRF） (D) 跨站指令碼攻擊（Cross-Site Scripting, XSS）
B	3. 下列何者為 L7 layer Firewall？ (A) Antivirus (B) WAF (C) IPS (D) IDS
B	4. 下列何者為探測通訊埠（Port）的軟體？ (A) Appscan (B) Nmap (C) Burp Suite (D) Telnet
C	5. 請問下列何種工具常被用來建立 Backdoor？ (A) telent (B) ipconfig (C) NC (D) cat
C	6. 下列何者為輕型目錄存取協定（Lightweight Directory Access Protocol, LDAP）較常使用之通訊埠（Port）？ (A) 311 (B) 123 (C) 389 (D) 390

D	7. 有心人士將電腦網卡設定為混雜模式，再加上由網路上下載網路監看（Sniffing）工具（如：Wireshark），就可以側錄到下列何種應用協定的密碼封包？ (A) IPSec (B) PGP (C) HTTPS (D) Telnet
C	8. 欲將外部網路（Internet）建立連線至內部網路（Intranet），採用下列何種連線方式，單一使用者可以較安全連接至某個私人網路？ (A) WAF (B) SSD (C) VPN (D) PBX
D	9. 某公司管理人員正在診斷 VPN 的安全性問題，附圖為其截取到的部份 VPN 封包，請問這家公司使用下列何種 VPN 通道協定？  No. Time Source Destination Protocol Length Info 31 0.077301 210.3… 210.34.36… PPP CCP 58 Configuration Request 32 0.077355 210.3… 210.34.36… PPP IPCP 82 Configuration Request 33 0.089251 210.3… 210.34.36… TCP 54 1723 → 50244 [ACK] Seq=213 Ack=373 Win=65280 Len=0 34 0.137861 210.3… 210.34.36… GRE 46 Encapsulated PPP 35 0.211227 210.3… 210.34.36… PPP CCP 58 Configuration Request 36 0.211227 210.3… 210.34.36… PPP IPCP 58 Configuration Request (A) OpenVPN (B) IPSec VPN (C) SSL VPN (D) PPTP VPN
B	10. 某組織內部新購置了 100 部個人電腦與伺服器，為了資訊安全考量，在內部安裝 WSUS（Windows Server Update Services）伺服器，以利管控個人電腦與伺服器的修補更新狀態，另外為了提高防毒效率，也分別為內部個人電腦安裝 A 牌防毒軟體、伺服器安裝 B 牌防毒軟體，內部網路亦加裝了入侵偵測系統。某日 MIS 發現該組織內部敏感資料外洩，經調查分析後發現組織內部之所有個人電腦與伺服器均在短短的 5 分鐘之內，遭受同一支惡意程式植入，請問下列何者為較可能之發生原因？ (A) 入侵偵測系統遭入侵派送惡意程式 (B) WSUS（Windows Server Update Services）伺服器遭入侵派送惡意程式 (C) 伺服器防毒軟體失效並感染個人電腦 (D) 個人電腦防毒軟體失效並感染伺服器

B	11. 下列何者「不」是 Windows 執行檔？ (A) COM (B) ELF (C) BAT (D) EXE
C	12. 下列何者「不」是作業系統更新所使用的指令？ (A) wuauclt (B) apt-get (C) update (D) yum
B	13. 下列何種惡意程式會寄生或附著在別的電腦程式、文件檔案裡面？ (A) 蠕蟲 (B) 電腦病毒 (C) 木馬程式 (D) 後門程式
B	14. 關於儲存媒體之報廢與處理方式，下列敘述何者「不」正確？ (A) 針對具機敏性之儲存媒體，當發生同位元檢查錯誤，或已達使用期限時，應由管理人員依據其特性進行銷毀 (B) 備份媒體需報廢時，應將媒體置於開放區域以利報廢作業 (C) 無法使用之儲存媒體經適當之銷毀後，即可依照進行資產報廢 (D) 為防範機敏性資料外洩，所有不再使用的儲存媒體應施以適當破壞，方式包含搗碎、焚毀及邏輯性之破壞，以確保儲存媒體無法讀取或使用
C	15. 在其他備份環境與條件相同情況下，下列何者備份方式，其還原時速度最慢？ (A) 完整備份（Full Backup） (B) 差異備份（Different Backup） (C) 增量備份（Incremental Backup） (D) 選擇式備份（Selective Backup）
A	16.「將備份資料採取批次處理方式，進行電子傳輸至備用站點。」請問上述屬於下列何種作法？ (A) 遠端電子備份（Electronic Vaulting） (B) 遠端日誌（Remote Journaling） (C) 遠端控制（Remote Control） (D) 增量備份（Incremental Backup）
B	17. 關於查看網頁事件記錄檔時，會看到 HTTP 狀態代碼段中找不到原始

	碼檔案，下列何者為事件記錄檔中看到找不到原始碼的實際錯誤代碼？ (A) 202 (B) 404 (C) 505 (D) 909
A	18. 請查看附圖的事件記錄檔並回答問題。下列防火牆的規則中，哪一條內容可防範此種攻擊？ Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 ->172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-versionquery: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07 [5875]: IDS277/DNSversion-query: 63.226.81.13:4630 -> 172.16.1.101:53 (A) 不允許從外部連接到內部 DNS UDP 53 (B) 允許 UDP 53 從 DNS 服務器到外部 (C) 不允許 TCPCS 從二級或 ISP 服務器到 DNS 服務器 (D) 阻止所有 TCP 流量
C	19. 請問若某公司，將存有機密性資料系統的日誌，以 Syslog 的方式透過網際網路（Internet）傳輸到 30 公里之外的異地備援機房，請問就安全的考量上來說，下列議題，何者最需優先處理？ (A) 備援機房的進出管理 (B) 日誌審查（Log Review）的頻率 (C) 傳輸過程的加密/保護

	(D) 30 公里的距離過遠
C	20. 下列何者「不」是常見的雲端運算的部署模式？ (A) 公有（Public）雲 (B) 私有（Private）雲 (C) 自由（Free）雲 (D) 混合（Hybrid）雲
B	21. 關於行動裝置中安全的使用軟體，請問下列敘述何者較「不」正確？ (A) 只在官方、原廠網站或可信任來源下載合法軟體 (B) 將手機進行越獄（Jailbreak, JB），以利執行所需的各式各樣軟體 (C) 安裝軟體前，確認軟體所需權限與軟體功能相符 (D) 當軟體出現版本更新時，應評估後下載更新
D	22. 請問下列何者「並非」行動裝置上唯一識別號嗎？ (A) 通用唯一識別碼（Universally Unique Identifier, UUID） (B) 國際移動用戶識別碼（International Mobile Subscriber Identity, IMSI） (C) 國際移動設備識別碼（International Mobile Equipment Identity, IMEI） (D) 國際基頻版本識別碼（International Baseband Version Identity, IBVI）
B	23. 附圖中，只有節點 N5 具備有向外連網能力，其他節點皆必須透過節點 N5 才能與外界進行網際網路連結，請問當節點 N5 為絕對安全的情況下，哪個節點消失時對整體網路的影響最小？  (A) N1 (B) N2 (C) N3 (D) N4

B	24. Linux 作業系統中，下列何者用於儲存使用者帳號密碼之雜湊（Hash）檔案？ (A) /etc/passwd (B) /etc/shadow (C) /etc/password (D) /etc/secret
D 全體送分	25. 請問下列何種工具主要可用來攻擊或竊取 Windows credentials？ (A) NMAP (B) Aircrack-ng (C) Burp Suite (D) Minikatz
A	26. 在 OWASP Top 10 2021 中，其 A6 項目說明使用含有已知漏洞的元件。而在軟體開發時，為減少 A6 項目的發生，下列何種作法較佳？ (A) 限制可以使用的元件 (B) 使用強的加密演算法 (C) 使用入侵防禦系統 (D) 限制使用的網路埠
D	27. 下列何者「不」屬於滲透測試之手段？ (A) 社交攻擊 (B) 密碼破解 (C) 弱點掃描 (D) 分散式服務阻斷攻擊
A	28. 在駭客工具中，常見到中國菜刀（China Chopper）或相似工具，其主要手法為下列何者？ (A) 通過向網站提交一句簡短的程式碼，來達到向伺服器插入木馬，並最後獲取 webshell (B) 針對網站，建立一個連接，以很低的速度發包，並保持住這個連接不斷開，最後將可用的連線佔滿 (C) 客戶使用主機 M 訪問並登錄合法網站 webA 後，再去訪問惡意網站 webB，然後惡意網站 webB 冒充該客戶透過使用者主機 M 去向網站 webA 發起請求 (D) 使用不安全的反序列化漏洞，利用遠端執行任意程式碼進行注入攻擊
D	29. 小忍想發送秘密訊息給合作夥伴，為了保護這些消息，他使用下列何種的技術，可在普通消息中隱藏秘密消息，通過隱蔽性提供安全性？ (A) RSA (B) Public key cryptography

	(C) Encryption (D) Steganography
D	30. 請問撰寫安全程式碼，可參考下列何項資料？ (A) NIST SP 800 系列 (B) FIPS 系列 (C) ISO 27000 系列國際標準 (D) OWASP 指南
B	31.「系統管理員將所有稽核日誌存放於另一台獨立的日誌伺服器（Log Server），並由非管理系統之人員管理該伺服器。」下列何者為其最重要的目的？ (A) 強化機密性 (B) 保護日誌 (C) 避免 SQL Injection 攻擊 (D) 降低分析資安事故的時間
B	32. 下列何者屬於網頁攻擊手法？（1）SQL Injection、（2）Parameterized Query、（3）Cross-Site Request Forgery、（4）Cross-Site Scripting (A)（1）（2）（3） (B)（1）（3）（4） (C)（2）（3）（4） (D)（1）（2）（3）（4）
D	33. 要防禦（Cross-Site Scripting, XSS），下列何者最有效？ (A) 過濾輸入參數長度 (B) 過濾輸出頁面 (C) 以黑名單過濾輸入參數 (D) 以白名單過濾輸入參數
B	34. 請問反組譯器（Disassemblers）、除錯器（Debuggers）和反編譯器（Decompilers）主要可用來判斷與檢查下列何種程式碼的弱點？ (A) 注入缺失（Injection Flaw） (B) 缺乏逆向工程（Reverse Engineering）保護 (C) 跨網站指令碼（Cross-Site Scripting） (D) 不安全的物件參考（Insecure Direct Object Reference）
A	35. 下列何種「不」是企業作為大量資料備份用途之儲存媒體？ (A) SD Memory Card（安全數位記憶卡） (B) LTO Tape（磁帶數據存儲） (C) Disk Array（磁碟陣列系統） (D) Tape Library（磁帶櫃）

B	36.「封包來源端 IP 與目的端 IP 相同的攻擊。」屬於下列何種攻擊方法？ (A) Smurf Attack (B) Land Attack (C) UDP Flood Attack (D) ICMP Flood Attack
B	37. 關於「駭客入侵，獲得存取權限階段」，下列敘述何者較「不」正確？ (A) 為駭客真正入侵的時期，屬於滲透階段 (B) 使用工具探索或掃描該組織有哪些主機、IP 或服務 (C) 手法包括緩衝區溢位、攔截及密碼破解等 (D) 可以獲取應用程式等級（Application level）、作業系統等級（Operating system level）或網路等級（Network level）的權限
C	38. 關於 Cross-Site Scripting，下列敘述何者「不」正確？ (A) 置換網頁的對話框 (B) 取得瀏覽者的 Cookie (C) 下載網頁原始程式碼 (D) 強迫轉址
B	39. 下列何種語言為 Cross-Site Scripting 攻擊主要使用的語言？ (A) Java (B) Javascript (C) C++ (D) C
A	40. 下列何種作法與保護資料機密性較「無」直接相關？ (A) 將資料複製成數個副本，放在不同的儲存媒體 (B) 將資料進行加密 (C) 將資料拆分成不同片段交由不同人分持 (D) 將資料設定特定權限，只有被授權的人才可開啟
D	41.「消費者使用應用程式，但並不掌控作業系統、硬體或運作的網路基礎架構」，請問上述屬於下列何種服務之定義？ (A) PaaS（Platform as a Service） (B) IaaS（Infrastructure as a Service） (C) QaaS（Quality as a Service） (D) SaaS（Software as a Service）
~~C~~ A	42. 在 Linux 系統中，下列何檔案存放了「使用者的登入歷史紀錄」？ (A) /var/log/wtmp

	(B) /var/log/messages (C) /etc/login.defs (D) /var/log/dmesg
B	43. 關於行動裝置的安全使用方式，請問下列敘述何者較「不」正確？ (A) 只在可信任來源下載應用程式，如：Google Play、Apple Store (B) 即時通訊軟體（例如 Line），可直接開啟陌生人傳送的檔案 (C) 收到訊息中含有連結網址時，仍要提防是否有危險性 (D) 安裝防毒軟體並定期更新病毒碼
D	44. 下列何者攻擊「不」屬於第七層攻擊？ (A) SQL Injection (B) Command Injection (C) Cross Site Scripting (D) SSL Hijacking
D	45. 下列何者「不」是 SSH 所使用的密碼學技術？ (A) 對稱加密（Symmetric Encryption） (B) 非對稱加密（Asymmetric Encryption） (C) 金鑰雜湊訊息鑑別碼（Keyed-hash Message Authentication Code） (D) 三重資料加密演算法（3DES）
B	46. 關於入侵檢測系統（Intrusion-Detection System, IDS），下列敘述何者「不」正確？ (A) 需定期更新特徵碼 (B) 可阻擋偽造 IP 之攻擊 (C) 不會因設備異常導致網路環境異常 (D) 可完整紀錄流量特徵
C	47. 關於連線劫持（Session Hijacking），下列敘述何者「不」正確？ (A) 指攻擊者繞過驗證機制直接劫持了受害目標的 Session (B) Session 是指兩個或多個通信設備之間，或設備與用戶之間的臨時交互信息 (C) Session 是一種用於存儲多個頁面的資訊（以變數形式）的方式，且會將該訊息存儲在使用者本機上 (D) 惡意使用者冒用受害目標的 Session 進行網路存取活動，活動可以是金錢交易、資料竄改
D	48. 關於中間人攻擊（Man-In-The-Middle Attack, MITM），下列敘述何者「不」正確？ (A) 屬於網路竊聽分類的一種攻擊形式 (B) 攻擊者會將自己穿插到兩者受害目標之間

	(C) 可攔截受害目標雙方間的通訊資訊 (D) 若受害目標雙方的連線有做加密則無法實現中間人攻擊
D	49. 下列何者為超文本傳輸安全協定（HTTPS）較常使用之通訊埠（Port）？ (A) 22 (B) 25 (C) 80 (D) 443
B	50. 關於物聯網設備的安全使用方式，請問下列敘述何者較「不」正確？ (A) 將預設密碼改為高強度密碼 (B) 使用 Telnet 進行遠端連線控制 (C) 定期進行韌體更新 (D) 對物聯網設備定期進行掃描