

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 1 頁，共 11 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

D	1. MIS 人員在維護非軍事區（Demilitarized Zone, DMZ）的電子郵件服務器時，發現有隱藏惡意程式的 rootkit 工具軟體，懷疑此時機器已經被駭客入侵了，在此狀況下，公司面臨最大的潛在資安風險為下列何者？ (A) 如果客戶知道公司發生資安事件，將對公司聲譽產生影響 (B) 機敏性電子郵件可能會被駭客攔截利用 (C) 如果駭客可以干擾經銷通路，將會影響公司的市場佔有率 (D) 駭客也可能已經入侵了其他系統，造成更大的資安風險
B	2. 關於容錯式磁碟陣列（RAID, Redundant Array of Independent Disks）當中的 RAID 5，下列敘述何者「不」正確？ (A) 最大容錯 1 顆硬碟異常 (B) 最少需要 5 顆硬碟 (C) 讀取效能比 RAID 1 低 (D) 容錯能力比 RAID 0 高
A	3. 要達成「資安聯防」目標，下列何者機制較為重要？ (A) 資安情資分享 (B) 公開金鑰基礎建設 (C) 分散式滲透測試 (D) 開放原始碼
A	4. 在網站弱點檢測報告中，發現系統存在路徑竄改（Path Manipulation）問題時，可以採取下列何種方案進行修補？ (A) 可以使用白名單路徑跟黑名單危險字串 (B) 可以採用圖像式驗證即可根治 (C) HTML.Encode (D) Prepared Statement
A	5. 美國國家安全局 NSA 的永恆之藍（EternalBlue）漏洞利用程式及 WannaCry 勒索病毒之攻擊手法，至今仍有攻擊事件，其主要是利用下列何者？ (A) Windows SMB 漏洞（MS17-010） (B) POODLE 漏洞（Padding Oracle On Downgraded Legacy Encryption） (C) 零時差漏洞攻擊（Zero-day attack） (D) 微軟 Office 記憶體毀損漏洞（CVE-2017-11882）
A	6. Heartbleed（CVE-2014-0160）漏洞主要是攻擊有問題的 SSL 機制，嘗試取得未加密的記憶體訊息，請問當發生此漏洞時，攻擊者一次可從記憶體中讀取多大的資料？ (A) 64K

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 2 頁，共 11 頁

	<p>(B) 640K</p> <p>(C) 1024K</p> <p>(D) 1280K</p>
D	<p>7. 關於跨站請求偽造 (Cross-Site Request Forgery, CSRF 或 XSRF) 的防禦方式，下列何者「不」適用？</p> <p>(A) 檢查請求 (Request) 的來源位址 (驗證 HTTP Referer)</p> <p>(B) 在 Server Site 產生 token，存在 Server 的 session 中</p> <p>(C) 使用圖型驗證碼</p> <p>(D) Prepared Statement</p>
D	<p>8. 關於集線器 (Hub)，下列敘述何者「不」正確？</p> <p>(A) 為開放式系統互聯模型 (Open System Interconnection Model, OSI) 中，實體層 (Physical Layer) 的設備</p> <p>(B) 駭客可利用介接此設備監聽網路封包</p> <p>(C) 進入到任一埠 (Port) 的封包，都會被廣播到其他 Port</p> <p>(D) 可用來區隔廣播領域 (Broadcast domain)</p>
A	<p>9. 某駭客成功滲透進入公司的內部網路，藉由控制一台電腦發動生成樹協定 (Spanning Tree Protocol, STP) 控制攻擊，請問駭客接下來最有可能執行下列何項動作？</p> <p>(A) 在受欺騙的根交換器 (Root Bridge) 啟用鏡像流量，並轉送所有網路流量到受到控制的電腦</p> <p>(B) 在受欺騙的根交換器 (Root Bridge) 啟用開放式最短路徑優先 (Open Shortest Path First, OSPF) 協定</p> <p>(C) 對內部網路中的所有第二層交換器重複相同的攻擊</p> <p>(D) 重複相同的攻擊形成阻斷服務攻擊，癱瘓內部網路</p>
B	<p>10. 當資安外洩事件發生後，若須確保證據的完整性，應對已被入侵的硬碟做下列何項處理？</p> <p>(A) 將原硬碟加密並進行鑑識工作後，再進行雜湊比對</p> <p>(B) 將原硬碟進行雜湊比對、位元層級複製，並對複製後的新硬碟進行雜湊比對，確認與原硬碟相符，對新硬碟進行鑑識工作</p> <p>(C) 在系統安裝一顆新硬碟，複製原硬碟所有檔案到新硬碟，對新硬碟進行鑑識工作</p> <p>(D) 對原硬碟直接進行鑑識工作</p>
C	<p>11. 關於優良保密協定 (Pretty Good Privacy, PGP)，下列敘述何者「不」正確？</p> <p>(A) 使用 IDEA 的演算法作為加密驗證之用</p> <p>(B) 支援訊息的身份認證和完整性檢查</p>

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 3 頁，共 11 頁

	<p>(C) 使用了公鑰基礎設施 (PKI) 進行身份的鑑別 (Authentication)</p> <p>(D) 同時做用了對稱式金鑰 (Symmetric Key) 加密與非對稱金鑰 (Asymmetric Key) 加密</p>
B	<p>12. 物聯網是當前應用發展最快速的科技之一，為確保國內相關產品的資訊安全，經濟部工業局規劃從：實體安全、系統安全、通訊安全、身分鑑別與授權機制安全、及隱私保護等五個安全構面，參照國際物聯網相關資安標準/規範，制訂物聯網資安環境標準以推升國內資安產業自主研發能量，建立國內穩定且安全的產業發展環境。以影像監控系統資安標準為例，下列何者「不」是引用開放網頁應用程式安全計畫 (Open Web Application Security Project, OWASP) 的規範項目？</p> <p>(A) 實體安全要求出廠產品之實體埠必須具備安全管控</p> <p>(B) 產品硬體設計須具備異常狀態之警示機制</p> <p>(C) 敏感性資料傳輸之通訊安全必須使用 FIPS 140-2 所核可之加密演算法，以確保機密性</p> <p>(D) 身分鑑別機制要求，在透過管理介面存取產品資源前，須透過具備防止重送攻擊之身分鑑別機制</p>
D	<p>13. 關於網站應用程式中之注入攻擊 (Injection)，下列敘述何者「不」正確？</p> <p>(A) 此攻擊是因為網站應用程式未對輸入資料進行驗證 (validated)、過濾 (filtered) 或清除 (sanitized)</p> <p>(B) 輸入之惡意資料被應用程式直接使用或串連查詢條件，如：改變 SQL 查詢來取得未授權資料或執行系統指令</p> <p>(C) 如欲防止此類漏洞產生，需要將輸入之資料與指令或查詢語法隔離，避免應用程式執行非預期之行為</p> <p>(D) 應用程式伺服器透過「白名單」方式來驗證資料正確性，並直接傳入解譯器 (Interpreter)，可完全避免此攻擊</p>
C	<p>14. 關於滲透測試 (Penetration Test, PT)，下列敘述何者「不」正確？</p> <p>(A) 模擬駭客攻擊並評估網路、資訊系統安全性之活動，於產出報告中詳述弱點如何利用與影響，並給予修復建議</p> <p>(B) 滲透測試可分非破壞測試 (Nondestructive Test) 與破壞測試 (Destructive Test)</p> <p>(C) 滲透測試有五種類別：黑箱 (Black-box)、白箱 (White-box)、灰箱 (Grey-box)、紅箱 (Red-box) 與藍箱 (Blue-box)，差異為提供測試人員受測目標資訊之詳細程度</p> <p>(D) 弱點掃描與滲透測試差異在於，前者僅關注於找到已知弱點，後者則引入縱深防禦的概念於發現組織之安全問題</p>

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 4 頁，共 11 頁

C	15. 系統管理人員於網站日誌中看見大量訊息含有類似字串「%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E」，可能為下列何種攻擊？ (A) SQL 資料隱碼攻擊 (SQL Injection Attack) (B) 阻斷服務攻擊 (Denial of Service Attack) (C) 跨網站指令碼攻擊 (Cross Site Scripting Attack) (D) 不安全的反序列化漏洞 (Insecure Deserialization)
A C	16. 企業發生勒索軟體感染事件後，在下列哪些安全維運的記錄中可以找到線索進行判斷事件規模？（複選） (A) SIEM (B) OS Application Event Log (C) AntiVirus Detection Log (D) SNMP Log
B C D 或 B D	17. 關於源碼檢測與滲透測試，下列敘述何者正確？（複選） (A) 滲透測試的使用時機通常會在程式開發過程中分次執行，而源碼檢測常會在系統開發完成後才使用 (B) SQL Injection 的問題，不論是執行源碼檢測或滲透測試，都是有機會可以被發現 (C) XSS 的問題只會出現在可執行 JavaScript 的環境中 (D) Google Hacking 常與滲透測試搭配使用，用以蒐集待測網站的資訊與漏洞
A C D	18. 關於網站應用程式中之跨網站指令碼攻擊 (Cross-Site Scripting, XSS)，下列敘述何者正確？（複選） (A) 跨網站指令碼攻擊分為反射式 (Reflected)、儲存式 (Stored) 與檔案物件模型 (Document Object Model) (B) 跨網站指令碼攻擊僅能透過 JavaScript 執行 (C) 儲存式跨網站指令碼攻擊通常被置入於資料庫，並於受害者所瀏覽特定功能、頁面後執行 (D) 反射式跨網站指令碼攻擊將惡意資料透過瀏覽器對網站的請求 (Request) 送出後，於受害者瀏覽之功能、頁面執行
A B C	19. 關於入侵偵測系統 (Intrusion Detection System) 與入侵防護系統 (Intrusion Prevention System) 之應用，下列敘述何者正確？（複選） (A) 入侵偵測系統透過旁接模式 (TAP or SPAN Mode) 或將特定網路介面設定為混雜模式 (Promiscuous Mode)，來取得監聽網路之流量副本 (B) TAP 和 SPAN Mode 之差異在於前者透過硬體 1:1 複製流量至分



# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 5 頁，共 11 頁

	<p>接網路介面；而後者透過軟體轉送流量副本至目的網路介面並可能因其容量限制而造成封包遺失</p> <p>(C) 如欲阻擋網路攻擊，入侵防護系統需設置為串連模式（In-line Mode）才能於攻擊傳遞過程中攔截</p> <p>(D) 入侵防護系統除偵測各式網路攻擊外也能進行阻擋，對於分散式阻斷服務攻擊（Distributed Denial-of-Service, DDoS）之阻擋成效尤其明顯</p>
C D	<p>20. 關於網站應用程式之安全性監控，下列敘述何者「不」正確？（複選）</p> <p>(A) 使用者登錄、存取控制與輸入驗證之錯誤資訊，均需詳細記錄至日誌中，以利分析與識別可能之攻擊</p> <p>(B) 網站應用程式日誌應即時產生並集中管理，確保無法遭受攻擊者竄改或抹除相關資訊</p> <p>(C) 為確保遭受之異常操作時能即時處置，網站應用程式除進行日誌記錄外，也需詳細呈現錯誤資訊供使用者回報</p> <p>(D) 網站應用程式已具備短時間連續認證錯誤之帳號鎖定機制，並於特定時間後自動解除。由於已可阻擋自動化攻擊，此類異常僅需記錄即可而無需關注</p>
題 組	<p>某公司為軟體系統開發商，主要業務為協助客戶進行客製化軟體系統之開發，若您為公司資安官，負責公司所有資訊安全之防護與管理事宜，公司近期剛通過第三方之 ISO/IEC 27001 驗證，範圍包含：系統開發與機房管理、機房納管設備包含網路設備、防火牆、官網伺服器、檔案伺服器、防毒伺服器以及資料庫伺服器。</p> <p>根據上列資訊，請回答下列問題：</p>
D	<p>21. 題組背景描述如附圖。某日您透過防毒伺服器主控台發現 A 部門同仁電腦均攔截到病毒，下列處理何者較「不」正確？</p> <p>(A) 持續更新防毒伺服器病毒碼</p> <p>(B) 追查與分析部門 A 所有同仁電腦所攔截之病毒</p> <p>(C) 持續更新部門 A 所有同仁電腦之病毒碼</p> <p>(D) 病毒已攔截，無須後續追蹤</p>
C	<p>22. 題組背景描述如附圖。某日同仁通報公司檔案伺服器內之文件檔案均因不明原因被加密，所有儲存於檔案伺服器之檔案均無法開啟，導致該業務中斷服務，請問此為下列何種攻擊手法？</p> <p>(A) 社交工程攻擊</p> <p>(B) 水坑式攻擊</p> <p>(C) 勒索軟體攻擊</p>

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 6 頁，共 11 頁

	(D) 分散式阻斷服務攻擊
A	<p>23. 題組背景描述如附圖。為了機房能夠正常提供納管設備之運作，避免某些因素而導致機房中斷服務，下列何種控制措施較為正確？</p> <p>(A) 機房增加不斷電系統</p> <p>(B) 各伺服器均定期更新病毒碼</p> <p>(C) 網路設備變更預設出廠值</p> <p>(D) 防火牆設定合適參數</p>
A B C	<p>24. 題組背景描述如附圖。公司為客戶開發的軟體系統，於交付客戶前，為確保其安全性，應先執行下列哪些工作？（複選）</p> <p>(A) 弱點掃描</p> <p>(B) 原始碼檢測</p> <p>(C) 滲透測試</p> <p>(D) 使用者體驗檢測</p>
題組	<p>一位資安專家正在對內部網站進行連接埠掃描，使用工具為 Nmap，伺服器 IP 為 10.0.1.1，掃描後看到的結果如下：</p> <pre> PORT      STATE    SERVICE  VERSION 21/tcp    open    ftp      vsftpd 2.2.6 110/tcp   open    pop3     courier pop3d 123/tcp   closed  ntp </pre> <p>Device type: general purpose Running: Linux 4.1.x</p> <p>OS details: Linux 4.1.18 Uptime: 215 days (since Thu Jan 4 15:30:20 2018) Network Distance: 0 hops Server Info: OS: Unix</p> <p>根據上列資訊，請回答下列問題：</p>
B	<p>25. 題組背景描述如附圖。上述掃描結果是 Nmap 的哪個完整指令？</p> <p>(A) Nmap -A -sV -p21,110,123 10.0.1.1</p> <p>(B) Nmap -O -sV -p21,110,123 10.0.1.1</p> <p>(C) Nmap -F -p21,110,123 10.0.1.1</p> <p>(D) Nmap -T -p21,110,123 10.0.1.1</p>
A	<p>26. 題組背景描述如附圖。若要提升 vsftpd 傳輸的安全性，應該使用下列</p>

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 7 頁，共 11 頁

或 D	何種方式最安全？ (A) vsftpd over SSH (B) vsftpd over SSL/TLS，SSL v3.0 以上 (C) vsftpd over SSL/TLS，TLS v1.1 以上 (D) vsftpd over SSL/TLS，TLS v1.2 以上
C	27. 題組背景描述如附圖。若要在應用式防火牆（Application Firewall）開啟 FTP 服務提供 Internet 存取，下列何種開啟方式最佳？ (A) 防火牆設定允許連入的連接埠 20, 21 (B) 防火牆設定允許連入的連接埠 21 (C) 防火牆設定允許連入的應用服務 FTP (D) 防火牆設定允許連入的連接埠 20
C	28. 題組背景描述如附圖。若要提升 POP3 服務的安全性，應使用下列何種協定及連接埠？ (A) POP3s, 443 (B) POP3s, 1443 (C) POP3s, 995 (D) POP3s, 110
題 組	免費憑證組織 Let's Encrypt，於 2019 年 2 月 27 日，宣佈該組織所頒發的免費憑證數量，已正式突破 10 億大關，該組織發佈免費憑證的目的是為了協助網站業者啟用 HTTPS 加密傳輸，由於該組織的大力協助使得全球啟用 HTTPS 的網頁數量已達到 81%，美國更高達 91%，有效提升全球使用 HTTPS 的普及率。  根據上列資訊，請回答下列問題：
B	29. 題組背景描述如附圖。下列何者「不」是採用 HTTPS 的好處？ (A) 增加網頁連線的安全性 (B) 加速網頁的連線 (C) 有助確認網站伺服器的身份 (D) 可有效減中間人攻擊（Man-In-The-Middle attack, MITM）的發生
C	30. 題組背景描述如附圖。關於 Let's Encrypt 及其機制，下列敘述何者「不」正確？ (A) Let's Encrypt 是一家全球性的憑證頒發機構（Certificate Authority, CA） (B) 所頒發的憑證有效期限較傳統 CA 短 (C) Let's Encrypt 協助確認網站的身份，有效避免詐欺與釣魚 (D) 可將憑證用在任何使用域名的服務上，如：網頁伺服器、郵件伺

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 8 頁，共 11 頁

	服务器和 FTP 伺服器
A	<p>31. 題組背景描述如附圖。若想用 openssl 的指令完成產生並儲存自簽伺服器憑證，下列指令何者正確？</p> <p>(A) openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout selfsigned.key -out selfsigned.crt</p> <p>(B) openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout selfsigned.key</p> <p>(C) openssl req -x509 -days 365 -newkey rsa:2048 -keyout selfsigned.key -out selfsigned.crt</p> <p>(D) openssl generatekey -x509 -nodes -days 365 -newkey rsa:2048 -keyout selfsigned.key -out selfsigned.crt</p>
C	<p>32. 題組背景描述如附圖。由於 Let's Encrypt 無法產生 localhost 憑證，請問如何在本機測試時避免 localhost 使用 HTTPS 時的警示訊息，以確保 HTTPS 的正常運作？</p> <p>(A) 可向其他憑證機構提出申請本機憑證，如：TWCA 或 CHTCA</p> <p>(B) 可向網頁伺服器業者提供本機憑證申請</p> <p>(C) 可由利用本機工具產生自簽憑證並設定信任自簽憑證解決此問題，如：openssl</p> <p>(D) 無法解決本機測試產生的 HTTPS 時警示訊息</p>
題組	<p>對於公司內部資安維運而言，資安漏洞或弱點的修補常是重要的工作，收到漏洞或弱點通報後，資安人員常依據漏洞或弱點之嚴重性，加上公司本身是否為漏洞或弱點影響範圍等資訊，來決定漏洞或弱點修補的優先性，以避免公司遭受更大的資安危害，A 公司係屬我國資通安全管理法所規範之“特定非公務機關”，且被主管機關核定資安責任等級為 A 級，對日常資安漏洞的修補投入許多心力。</p> <p>根據上列資訊，請回答下列問題：</p>
B	<p>33. 題組背景描述如附圖。某日 A 公司內部資安人員收到一則漏洞資安通報資訊如附圖，關於內容中通用漏洞評分系統（Common Vulnerability Scoring System, CVSS），下列敘述何者「不」正確？</p>




# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 9 頁，共 11 頁

	<div><h2>CVE-2019-19781 Detail</h2><div>MODIFIED</div><p>This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.</p><h3>Current Description</h3><p>An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.</p><p>Source: MITRE <a href="#">View Analysis Description</a></p><div><div>Severity</div><div>CVSS Version 3.x</div><div>CVSS Version 2.0</div></div><div>CVSS 3.x Severity and Metrics:</div><div><div> NIST: NVD</div><div>Base Score: 9.8 CRITICAL</div><div>Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</div></div></div> <p>(A) CVSS 的分數愈高，代表這個漏洞的嚴重等級愈高 (B) CVSS 的評分基準中，會考量這個漏洞已被公開的天數 (C) CVSS 的評分基準中，會考量這個漏洞或弱點在使用時，所需擁有的權限等級 (Privileges Required) (D) CVSS 的分數滿分為 10 分</p>
D	<p>34. 題組背景描述如附圖。承上題，關於這則漏洞通報（如附圖）中所揭露的訊息，下列敘述何者正確？</p> <p>(A) 通報內容有揭露此一漏洞的公布日期 (B) 通報內容沒有揭露受此一漏洞所影響的產品與版本 (C) 通報內容有揭露受此一漏洞所影響的產品、版本與解決方案 (D) 通報內容有揭露受此一漏洞所會造成的影響或弱點類型</p>
B	<p>35. 題組背景描述如附圖。承上題，當漏洞被公布後，資安人員在檢查受漏洞影響設備的 Access Log 時，發現了附圖疑似遭攻擊的紀錄，由於 /vpn 路徑項下不是此 web 服務公開路徑，下列敘述何者正確？</p> <pre>112.187.10.104--[15 / Feb / 2020:22:29:03 +0000] "POST /vpn/..../vpns/portal/scripts/newbm.pl HTTP / 1.1" 200 15 "-" 112.187.104.104--[15 / Feb / 2020:22:29:23 +0000] "GET /vpn/..../etc/passwd HTTP / 1.1" 400 226 "-" 112.187.104.104--[15 / Feb / 2020:22:29:33 +0000] "GET /vpn/..../vpns/cfg/smb.conf HTTP / 1.1" 404 48 "-" 112.187.104.104--[15 / Feb / 2020:22:29:42 +0000] "GET /vpn/..../vpns/cfg/smb.conf HTTP / 1.1" 200 83 "-" 112.187.104.104--[15 / Feb / 2020:22:29:51 +0000] "GET /vpn/..../vpns/portal/A0UnCfwrjIjrpngpwxaddqADAttcban.xml HTTP / 1.1" 200- "-"</pre> <p>(A) 疑似駭客嘗試讀取該主機的使用者帳號密碼列表 (B) 這個主機的 vpns 路徑不是 web 的公開目錄，但駭客曾成功讀取這個目錄內的特定檔案內容 (C) 透過存取紀錄，可以推斷駭客是使用工具進行攻擊 (D) 透過存取紀錄，可以推斷這個漏洞會造成 XSS 的威脅</p>
A D	<p>36. 題組背景描述如附圖。承上題，因為透過 Access Log 研判駭客攻擊可能成功，請問對於該事件後續的處理，下列敘述何者正確？（複選）</p> <p>(A) 資安人員應於知悉資安事件 1 小時內，依中央目的事業主管機關指定之方式，進行資通安全事件之通報</p>

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 10 頁，共 11 頁

	<p>(B) 資安人員應於資安事件發生 8 小時內，依中央目的事業主管機關指定之方式，進行資通安全事件之通報</p> <p>(C) 對一般而言，如果漏洞所屬的產品為網路設備或 Appliance，除設備換新外，只能接受這個漏洞存在，亦無需關注與設備有關的漏洞與處理方式等資訊</p> <p>(D) 由於在進行資安事件通報時，主管機關核定該資安事件為二級，資安人員最遲應於 72 小時內，完成損害控制或復原作業，並依指定方式回報或通知</p>
題組	<p>某公司為了符合國際標準要求，將年度定期舉行之滲透測試（Penetration Test, PT）作業，委由外部資安檢測團隊 X 來進行。</p> <p>根據上列資訊，請回答下列問題：</p>
C	<p>37. 題組背景描述如附圖。關於該公司與資安檢測團隊於滲透測試之前置工作，下列敘述何者「不」正確？</p> <p>(A) 簽訂保密協議（Non-Disclosure Agreement），要求測試細節與結果未經授權不可任意揭露</p> <p>(B) 招開起始會議（Kickoff Meeting）溝通雙方於專案之目標與期望，並說明團隊分工、測試計畫、方法論與程序</p> <p>(C) 執行預測試（Early Testing）以評估測試目標之可能範圍、弱點類型、時間與投入資源，以利測試計畫產出</p> <p>(D) 簽訂滲透測試契約使檢測團隊取得測試許可，內容需包含：測試目標、時間、方法、限制、規範與聯繫方式等，並說明受測服務可能遭受之影響</p>
A	<p>38. 題組背景描述如附圖。滲透測試分三階段「攻擊前（Pre-Attack）」、「攻擊中（Attack）」與「攻擊後（Post-Attack）」。檢測團隊 X 欲執行主動式偵查（Active Reconnaissance）而透過網際網路對受測目標使用掃瞄器，探測目標網路邊界、網路服務與其應用程式資訊，此行為屬於下列何種階段？</p> <p>(A) 「攻擊前（Pre-Attack）」</p> <p>(B) 「攻擊前（Pre-Attack）」與「攻擊中（Attack）」</p> <p>(C) 「攻擊中（Attack）」</p> <p>(D) 「攻擊後（Post-Attack）」</p>
A	<p>39. 題組背景描述如附圖。檢測團隊 X 測試公司網站，發現可竄改傳遞至應用程式之 XML 內容引入特定資源並回應其內容，再透過此漏洞列舉網站伺服器其中 Web 目錄，其中含有不尋常 PHP 檔案內容如下： &lt;?php eval(\$_POST['cmd'])&gt;。關於檔案內容，下列敘述何者「不」正</p>

# 109 年度中級資訊安全工程師能力鑑定試題

科目 2：資訊安全防護實務

考試日期：109 年 8 月 15 日

第 11 頁，共 11 頁

	<p>確？</p> <p>(A) 檔案推測為「一句話木馬」但無需理會，因其內容可顯示所以無法被網站伺服器執行</p> <p>(B) 檢測團隊第一時間於網站所發現之漏洞類型為本地文件包含漏洞 (Local File Inclusion, LFI)</p> <p>(C) 檔案可能為遭受攻擊者所植入的後門程式 (Web-Shell)，又常被稱為「一句話木馬」</p> <p>(D) 檢測團隊第一時間所發現之漏洞可能透過 XML 外部實體 (XML External Entity, XXE) 進行注入攻擊</p>
D	<p>40. 題組背景描述如附圖。檢測團隊 X 最終依照計畫如期完成公司測試案，並交付測試報告，關於滲透測試報告，下列敘述何者正確？</p> <p>(A) 滲透測試報告主要目的為提升組織合規性與其適法性，並能有效促進商業行為發展</p> <p>(B) 滲透測試報告弱點分級通常使用緊急 (Emergency)、急迫 (Urgent)、一般 (Standard)、普通 (Normal)</p> <p>(C) 為提升滲透測試可讀性，對於安全弱點技術細節應考量精簡或忽略，並詳述問題改善與修復方案</p> <p>(D) 滲透測試報告使高階管理人員更易於決策安全措施之執行，也協助資安單位順利修復弱點與實踐安全控制</p>