

# 110 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：110 年 9 月 25 日

第 1 頁，共 12 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

B	<p>1. 某公司正在研究網路型防火牆（Layer 4 Firewall）如何有效防止網站應用程式（Web application）攻擊的方法，下列敘述何者正確？</p> <p>(A) 網路型防火牆可以偵測惡意的網站訪問攻擊</p> <p>(B) 網路型防火牆無法阻擋此類型攻擊，因為連接埠 80, 443 必須開啟</p> <p>(C) 如果正確設定，網路型防火牆可阻擋此類型攻擊</p> <p>(D) 無須進行設定，網路型防火牆預設能阻擋此類型攻擊</p>
D	<p>2. 關於跨站請求偽造（Cross-Site Request Forgery, CSRF or XSRF）與跨站腳本攻擊（Cross-Site Scripting, XSS）的比較，下列敘述何者較正確？</p> <p>(A) 兩者都是利用瀏覽器（Browser）對伺服器端（Server site）的信任</p> <p>(B) 兩者都是利用伺服器端（Server site）對瀏覽器（Browser）的信任</p> <p>(C) XSS 是利用伺服器端（Server site）對瀏覽器（Browser）的信任，CSRF 是利用瀏覽器（Browser）對伺服器端（Server site）的信任</p> <p>(D) CSRF 是利用伺服器端（Server site）對瀏覽器（Browser）的信任，XSS 是利用瀏覽器（Browser）對伺服器端（Server site）的信任</p>
D	<p>3. 使用公眾網路上網時應該注意下列哪些事項以防範公眾網路的中間人攻擊（Man-In-The-Middle Attack, MITM）？1.使用 WPA3 最新一代 Wi-Fi 安全技術，保護通訊安全、2.避免瀏覽未加密的網站，減少資料被竊取風險、3.使用虛擬專用網路（VPN）連接公司網路或專屬系統、4.網路驗證採用雙因子認證，減少帳密被竊取的問題</p> <p>(A) 1、2</p> <p>(B) 1、3</p> <p>(C) 2、3</p> <p>(D) 3、4</p>
A	<p>4. 關於 SQL 資料庫中常見的攻擊，下列敘述何者「不」正確？</p> <p>(A) OOB 注入攻擊（Out of Band），屬於 inband 的注入模式</p> <p>(B) SQL 注入類型區分成 Boolean-based blind SQL injection、Error-based SQL injection、UNION query SQL injection、Stacked queries SQL injection、Time-based blind SQL injection</p> <p>(C) Error-based SQL injection 屬於 inband 的注入模式，被戲稱盲注入</p> <p>(D) OOB 透過其他傳輸方式來獲得資料，如：利用 DNS 解析協定和</p>

# 110 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：110 年 9 月 25 日

第 2 頁，共 12 頁

	電子郵件來竊取資料庫資料
D	<p>5. 在規劃建置異地的連網系統時，為了達到大量資料傳輸與通訊的安全，下列何者通訊安全之防護與應變實務規劃較佳？</p> <p>(A) 採用數位簽章提升訊息交換安全，並使用對稱式加密進行金鑰交換</p> <p>(B) 採用非對稱式加密處理大量訊息，並使用對稱式加密進行金鑰交換</p> <p>(C) 採用對稱式加密處理大量訊息，並使用數位簽章進行金鑰交換</p> <p>(D) 採用對稱式加密處理大量訊息，並使用非對稱式加密進行金鑰交換</p>
D	<p>6. 入侵檢測系統（Intrusion-Detection System, IDS）與入侵預防系統（Intrusion Prevention System, IPS）具監測及防禦的雙重功能，可即時偵測到攻擊事件的發生，並中止或阻絕入侵行為，包括自動攔截棄置攻擊封包，下列敘述何者較「不」正確？</p> <p>(A) IDS 防禦方式為被動監聽（Passive sniffer mode）</p> <p>(B) IDS 防禦動作可透過 TCP reset 來中斷連線</p> <p>(C) IPS 防禦方式為主動防禦（Active in-line mode）</p> <p>(D) IPS 防禦動作為通知防火牆丟棄惡意封包、中斷連線</p>
A	<p>7. 關於資料隱碼攻擊，可透過下列何種方式防範以避免類似事件再發生？</p> <p>(A) 執行輸入檢查</p> <p>(B) 使用 SSL 加密</p> <p>(C) 加入圖形驗證</p> <p>(D) 加裝防毒軟體</p>
C	<p>8. 關於零信任安全架構（Zero Trust Architecture），下列敘述何者「不」正確？</p> <p>(A) 零信任基礎認知，也就是假設不信任任何人為前提的安全架構</p> <p>(B) 從網路到裝置都是零信任控制點。換言之，不管是連接裝置、應用程式或是組件，都視為威脅向量，必須經過認可及驗證</p> <p>(C) 零信任包含：網路、設備、使用者、資料，不包含 Workloads</p> <p>(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</p>
C	<p>9. 容錯式磁碟陣列（Redundant Array of Independent Disks, RAID）建置時，RAID 0, RAID 1, RAID 5, RAID 10 最小需要的實體硬碟數量依序為下列何者？</p> <p>(A) 1, 1, 2, 2</p> <p>(B) 2, 2, 3, 3</p>

# 110 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：110 年 9 月 25 日

第 3 頁，共 12 頁

	<p>(C) 2, 2, 3, 4</p> <p>(D) 2, 2, 5, 10</p>
D	<p>10. 下列何者機制的目的是用來確保資料的完整性 (Integrity) ?</p> <p>(A) RC4 (Rivest Cipher 4)</p> <p>(B) RSA (Rivest, Shamir, Adleman)</p> <p>(C) Diffie-Hellman</p> <p>(D) MD5 (Message Digest Algorithm 5)</p>
D	<p>11. 某公司的資料容錯策略是使用遠端日誌抄寫 (Remote Journaling)，關於遠端日誌抄寫，下列敘述何者正確？</p> <p>(A) 即時複製資料庫或檔案到遠端存放，並進行即時同步</p> <p>(B) 傳送資料副本至備份磁帶，拿到遠端存放</p> <p>(C) 使用備份軟體備份資料至遠端，有更新時透過備份軟體同步</p> <p>(D) 傳送交易紀錄至遠端，當原始資料遺失時，在遠端透過交易紀錄重建</p>
B	<p>12. 關於網站應用程式之資料安全性，下列敘述何者正確？</p> <p>(A) 網站應用程式所使用之安全傳輸協定 (HTTPS)，目前最新版加密層協議為透過 SSL 3.0 實作</p> <p>(B) HTTPS 協議需透過金鑰交換機制 (如：RSA 非對稱加密演算法) 取得用於加密資料之密鑰 (如：AES 對稱加密演算法) 以確保傳輸效能</p> <p>(C) HTTPS 協議僅可保護應用程式傳送之資料內容，攻擊者仍可透過竊聽攻擊 (Sniffing Attack) 獲取未加密之表頭資訊 (HTTP Header)</p> <p>(D) 使用者密碼若透過 HTTPS 協議傳送，即可保護其不受攻擊者竊聽，因此可明文儲存於網站應用程式資料庫中</p>
A	<p>13. 關於附圖程式碼，下列敘述何者「不」正確？</p> <pre>String firstname = req.getParameter("firstname"); String lastname = req.getParameter("lastname"); // FIXME: do your own validation to detect attacks String query = "SELECT id, firstname, lastname FROM authors WHERE forename = ? and surname = ?"; PreparedStatement pstmt = connection.prepareStatement( query ); pstmt.setString( 1, firstname ); pstmt.setString( 2, lastname ); try {     ResultSet results = pstmt.execute( ); }</pre> <p>(A) Hard-coded Password 為 FIXME</p> <p>(B) 此程式碼語言為 Java</p> <p>(C) preparedStatement 為預存式查詢</p> <p>(D) setString 為參數化查詢</p>
A	<p>14. 某 MIS 人員欲對公司一重要伺服器 (功能包含檔案伺服器、資料庫</p>

# 110 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：110 年 9 月 25 日

第 4 頁，共 12 頁

	<p>功能) 使用 Nmap 來執行進行滲透測試，以便瞭解該資訊設備之漏洞是否全數修補完成，請問該 MIS 使用此工具最主要之目的為下列何者？</p> <p>(A) 利用該伺服器已知對外開放之服務埠進行情蒐</p> <p>(B) 利用該伺服器已知之漏洞提升權限</p> <p>(C) 利用該伺服器已知之漏洞竊取檔案</p> <p>(D) 利用該伺服器已知之漏洞下載資料庫</p>
B	<p>15. 下列何種檢測方式較「不」能證明網站防禦機制跟企業認知的資安防護程度一樣好？</p> <p>(A) 網站弱點掃描</p> <p>(B) 主機弱點掃描</p> <p>(C) 滲透測試</p> <p>(D) 網頁源碼檢測</p>
A B D	<p>16. 暴力破密 (Brute-Force) 攻擊是最需要大量運算資源的攻擊手法，下列哪些作法能有效避免暴力破密攻擊？(複選)</p> <p>(A) 密鑰延伸 (Key stretching)</p> <p>(B) 密碼複雜度要求 (Password Complexity Requirements)</p> <p>(C) 雜湊演算 (Hashing)</p> <p>(D) 加鹽 (Salting)</p>
B C	<p>17. 下列哪些 HTTP Header 標頭之安全性設定，「不」能讓網站與使用者瀏覽器之間有更多的安全防護功能？(複選)</p> <p>(A) HTTP Strict Transport Security</p> <p>(B) Access-Control-Max-Age</p> <p>(C) Accept-Encoding</p> <p>(D) X-Frame-Options</p>
A B D	<p>18. 關於勒索病毒傳遞媒介、與常用技術手法，下列敘述哪些正確？(複選)</p> <p>(A) 勒索病毒會透過郵件、網頁的網址連結、USB 裝置來傳遞</p> <p>(B) 勒索病毒會利用 DLL Hijacking 技術取得高權限</p> <p>(C) 勒索病毒會利用 OS 黑名單程式，迴避防毒系統檢查</p> <p>(D) 勒索病毒會利用 Power Shell 無檔案式 (File-less)，取得高權限</p>
A C D	<p>19. 公司在協助客戶建置客制化應用軟體系統時，為方便進行遠端維護，下列哪些措施可以增加「系統維護」的安全性？(複選)</p> <p>(A) 在公司政策允許下建立 VPN 機制，提供作業人員可以進行遠端安全連線</p> <p>(B) 建立單一登入 (Single Sign-On, SSO) 作業，統一連線帳密管理</p> <p>(C) 設定網路防火牆遠端連線機制及限制存取的主機位置</p>

# 110 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：110 年 9 月 25 日

第 5 頁，共 12 頁

	(D) 使用雙因子認證，確保連線使用者
A B C	<p>20. 搜尋引擎的進階搜尋指令常被用來刺探網站重要資訊，更被用在滲透測試上，其中最知名就是 Google Hacking Database (GHDB)，關於搜尋引擎進階指令發展、應用與技術分析，下列敘述哪些正確？（複選）</p> <p>(A) 駭客利用 google 進階搜尋技巧與運算，搜索網際網路中定位特定的文本字，作為滲透入侵易受攻擊的 Web 應用程序</p> <p>(B) site:tw 此指令是限制搜尋標的為台灣網站</p> <p>(C) intitle:index.of site:tw 描述是列出該網站 index.of 網站目錄清單</p> <p>(D) 在另一個知名搜尋引擎 Bing，並沒有類似的應用</p>
	<p>(題組 1)</p> <p>//網路</p> <p>身為公司網路管理人員的您，正在為公司的網路架構進行調整，將目前的網路架構進行區隔，在 R1 所屬的區域建立多個 VLAN 以隔離廣播 (Broadcast)，提升服務存取的效能。調整後之架構如下：</p> <pre> graph LR     R1[R1] --- E0_1_1[192.168.0.1/30] --- E0_1_2[192.168.0.2/30] --- R2[R2]     R2 --- E0_2_1[192.168.0.5/30] --- E0_2_2[192.168.0.6/30] --- R3[R3]     R1 --- E0_0_1[192.168.8.1/24] --- E0_0_2[192.168.9.1/24] --- SW1[SW1]     R2 --- E0_0_3[192.168.4.1/28] --- SW2[SW2]     R3 --- E0_0_4[192.168.4.17/28] --- SW3[SW3]     SW1 --- Host_A[Host A VLAN 8 192.168.8.21/24]     SW1 --- Host_B[Host B VLAN 9 192.168.9.21/24]     SW1 --- Host_C[Host C VLAN 10 192.168.10.11/24]     SW2 --- Host_E[Host E 192.168.4.11/28]     SW2 --- Host_F[Host F 192.168.4.12/28]     SW3 --- Host_G[Host G 192.168.4.21/28]     SW3 --- Host_H[Host H 192.168.4.22/28]     </pre>
C	<p>21. 題組背景描述如附圖。Host C 反應無法存取 Host B 分享的資源的原因為何下列何者？</p> <p>(A) Host C 與 Host B 在不同 VLAN</p> <p>(B) SW1 未設定 Gateway IP 192.168.10.1</p> <p>(C) R1 未設定 Gateway IP 192.168.10.1</p> <p>(D) Host C 未設定 Gateway IP 192.168.0.1</p>
B	<p>22. 題組背景描述如附圖。請問 R1 &lt;----&gt; SW1 之間所建立的架構稱為下列何者？</p> <p>(A) Multiple VLAN Routing</p> <p>(B) Router on a stick</p> <p>(C) Routing cross switch</p> <p>(D) One-armed routing</p>



# 110 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：110 年 9 月 25 日

第 6 頁，共 12 頁

D	<p>23. 題組背景描述如附圖。公司預計明年進行擴廠需求，您計畫導入動態路由協定（Dynamic Routing Protocol）讓路由可自動更新至所有節點，以降低中斷的影響時間，下列何者「不」是避免路由迴圈的技術？</p> <p>(A) Route Poisoning (B) Split Horizon (C) Hold-down timers (D) Route Convergence</p>																					
D	<p>24. 題組背景描述如附圖。承上題，R1 之現行路由表如附圖，若導入動態路由協定，並於 R1 進行路由匯總（route summarization），讓 SW2 及 SW3 的所有 Host 可以連接到 SW1 的所有 Host，請問 R1 應如何宣告 SW1 匯總後的路由？</p> <table><tr><th>network</th><th>interface</th><th>next-hop</th></tr><tr><td>192.168.0.0/30</td><td>Ethernet 0/1</td><td>directly connected</td></tr><tr><td>192.168.8.0/24</td><td>Ethernet 0/0.8</td><td>directly connected</td></tr><tr><td>192.168.9.0/24</td><td>Ethernet 0/0.9</td><td>directly connected</td></tr><tr><td>192.168.0.4/30</td><td>Ethernet 0/1</td><td>192.168.0.2</td></tr><tr><td>192.168.4.0/28</td><td>Ethernet 0/1</td><td>192.168.0.2</td></tr><tr><td>192.168.4.16/28</td><td>Ethernet 0/1</td><td>192.168.0.2</td></tr></table> <p>(A) 192.168.8.0/19 (B) 192.168.8.0/20 (C) 192.168.8.0/21 (D) 192.168.8.0/22</p>	network	interface	next-hop	192.168.0.0/30	Ethernet 0/1	directly connected	192.168.8.0/24	Ethernet 0/0.8	directly connected	192.168.9.0/24	Ethernet 0/0.9	directly connected	192.168.0.4/30	Ethernet 0/1	192.168.0.2	192.168.4.0/28	Ethernet 0/1	192.168.0.2	192.168.4.16/28	Ethernet 0/1	192.168.0.2
network	interface	next-hop																				
192.168.0.0/30	Ethernet 0/1	directly connected																				
192.168.8.0/24	Ethernet 0/0.8	directly connected																				
192.168.9.0/24	Ethernet 0/0.9	directly connected																				
192.168.0.4/30	Ethernet 0/1	192.168.0.2																				
192.168.4.0/28	Ethernet 0/1	192.168.0.2																				
192.168.4.16/28	Ethernet 0/1	192.168.0.2																				
	<p><b>（題組 2）</b></p> <p>某企業使用第三方 ERP 系統已經 15 年，該系統安裝於實體主機中，其作業系統為 Windows Server 2003，資料庫為 MS-SQL 2008 版本，其 ERP 資料庫相容層級為 100。該 ERP 只購買維護及三次新增客製功能，未購買升級更新版本。</p> <p>後端使用 Single Fiber Controller 連結 EMC storage，發現硬碟使用率已達 90%，資料庫檔 erp.mdf 900 GB，資料庫 erp.ldf 檔 1.5TB。該公司 ISMS 制度中 ERP 服務級別協定（Service-Level Agreement, SLA）要求妥善率 99.9%。</p> <p>因主機警示燈亮起，必須停機檢修，發現 RAID 卡電池組膨脹，頻繁當機。</p>																					

# 110 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：110 年 9 月 25 日

第 7 頁，共 12 頁

	<p>而 ERP 授權及容量限制，無法進行 P2V 全系統備份。緊急採購新主機進行替換，並安裝 Esxi，新主機規格為 HP-DL380 G10 為 8 核心 CPU*2、記憶體 256 GB、硬碟為 SAS 6TB*12。</p>
B	<p>25. 題組背景描述如附圖。您身為資安工程師，在面臨系統老舊且要求高妥善率的情況下，找來主機保固公司進行更換 RAID 卡電池組，下列敘述何者正確？</p> <p>(A) RAID 資訊遺失不會造成系統毀損</p> <p>(B) 在硬碟也保留一份 RAID 資訊，可當作 RAID 的資料備份</p> <p>(C) 這是正常故障更換，不需要進行 ISMS 資安通報</p> <p>(D) 檢修前不需要再取主機故障資訊及進行分析</p>
D	<p>26. 題組背景描述如附圖。承上題，在掌握相關資訊後應注意的資料庫安全性評估事項，下列敘述何者正確？</p> <p>(A) 資料庫版本為 MS-SQL 2008 已經被微軟終止更新服務，應在新主機抵達時更換成 MS-SQL 2019，未經相容性測試將 ERP 資料庫相容層級直接升級至 150 模式</p> <p>(B) MS-SQL 2008 ERP 資料庫 ldf 檔已達 1.5TB 時，應 transaction log，其指令為 dump transaction erp with no_log</p> <p>(C) MS-SQL 2008 ERP 資料庫 ldf 檔已達 1.5TB 時，發現無法使用 SQL Query 指令方式壓縮資料庫，直接刪除 ldf 檔後，而後再掛回 ERP 資料庫</p> <p>(D) ERP 資料庫更換前，應先檢查 ERP 系統對資料庫連線方式以及連線的資料庫帳號密碼，且需要查核資料庫所屬安全性使用者群組</p>
A	<p>27. 題組背景描述如附圖。承上題，關於新主機虛擬化之安全規劃應注意的主機與虛擬化之安全性評估事項，下列敘述何者較正確？</p> <p>(A) 若該新主機決定採用 ESXi 6.7 U.3 版本，因 ESXi 對主機硬體規格有其要求，所以必須合法下載支援 HP-DL380 G10 版本，如不採用專用版本會有不相容問題</p> <p>(B) 新主機採用 ESXi 為求更大硬碟使用需要，決定採用 RAID 0 模式是兼具安全與容量使用規劃</p> <p>(C) ESXi 可採用永久免費的版本，且可滿足新主機硬體更新需要</p> <p>(D) 網路上可以找到 ESXi 序號，可直接使用在公司正式環境上</p>
B	<p>28. 題組背景描述如附圖。承上題，若在 ISMS 制度中之服務級別協定 (Service-Level Agreement, SLA) 要求妥善率 99.9%，請問一年最大可容許停機時間約為多久？</p> <p>(A) 7 天 15 小時 36 分</p>

# 110 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：110 年 9 月 25 日

第 8 頁，共 12 頁

	(B) 8 小時 45 分 36 秒 (C) 15 分 33.6 秒 (D) 55.36 秒																																																																																																				
	<div>(題組 3)</div> <p>小明是公司的資安工程師，早上有同仁通知電腦似乎發生異常，防毒軟體好像也失效，因此小明調閱了公司在網路出口的封包側錄檔案，如下圖，請就上述情境回答下列問題。</p> <table><tr><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>[TCP Port numbers reused] 80 → 1065 [SYN, ACK] Seq=1 Ack=1 Win=642</td></tr><tr><td>192.168.23.129</td><td>59.53.91.102</td><td>TCP</td><td>60</td><td>1065 → 80 [ACK] Seq=1 Ack=2 Win=64240 Len=0</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>[TCP Port numbers reused] 80 → 1064 [SYN, ACK] Seq=1 Ack=1 Win=642</td></tr><tr><td>192.168.23.129</td><td>59.53.91.102</td><td>TCP</td><td>60</td><td>1064 → 80 [ACK] Seq=1 Ack=2 Win=64240 Len=0</td></tr><tr><td>192.168.23.129</td><td>59.53.91.102</td><td>HTTP</td><td>314</td><td>GET /q.jar HTTP/1.1</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>80 → 1065 [ACK] Seq=2 Ack=261 Win=64240 Len=0</td></tr><tr><td>192.168.23.129</td><td>59.53.91.102</td><td>HTTP</td><td>317</td><td>GET /sdfg.jar HTTP/1.1</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>80 → 1064 [ACK] Seq=2 Ack=264 Win=64240 Len=0</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>NBNS</td><td>110</td><td>Refresh NB TICKLAB&lt;00&gt;</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>1514</td><td>80 → 1065 [ACK] Seq=2 Ack=261 Win=64240 Len=1460 [TCP segment of a</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>1514</td><td>80 → 1065 [PSH, ACK] Seq=1462 Ack=261 Win=64240 Len=1460 [TCP segm</td></tr><tr><td>192.168.23.129</td><td>59.53.91.102</td><td>TCP</td><td>60</td><td>1065 → 80 [ACK] Seq=261 Ack=2922 Win=64240 Len=0</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>NBNS</td><td>110</td><td>Refresh NB TICKLAB&lt;00&gt;</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>NBNS</td><td>110</td><td>Refresh NB TICKLAB&lt;00&gt;</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>1514</td><td>80 → 1064 [ACK] Seq=2 Ack=264 Win=64240 Len=1460 [TCP segment of a</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>1514</td><td>80 → 1064 [PSH, ACK] Seq=1462 Ack=264 Win=64240 Len=1460 [TCP segm</td></tr><tr><td>192.168.23.129</td><td>59.53.91.102</td><td>TCP</td><td>60</td><td>1064 → 80 [ACK] Seq=264 Ack=2922 Win=64240 Len=0</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>1514</td><td>80 → 1064 [ACK] Seq=2922 Ack=264 Win=64240 Len=1460 [TCP segment o</td></tr><tr><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>1514</td><td>80 → 1064 [ACK] Seq=4282 Ack=264 Win=64240 Len=1460 [TCP segment o</td></tr></table>	Source	Destination	Protocol	Length	Info	59.53.91.102	192.168.23.129	TCP	60	[TCP Port numbers reused] 80 → 1065 [SYN, ACK] Seq=1 Ack=1 Win=642	192.168.23.129	59.53.91.102	TCP	60	1065 → 80 [ACK] Seq=1 Ack=2 Win=64240 Len=0	59.53.91.102	192.168.23.129	TCP	60	[TCP Port numbers reused] 80 → 1064 [SYN, ACK] Seq=1 Ack=1 Win=642	192.168.23.129	59.53.91.102	TCP	60	1064 → 80 [ACK] Seq=1 Ack=2 Win=64240 Len=0	192.168.23.129	59.53.91.102	HTTP	314	GET /q.jar HTTP/1.1	59.53.91.102	192.168.23.129	TCP	60	80 → 1065 [ACK] Seq=2 Ack=261 Win=64240 Len=0	192.168.23.129	59.53.91.102	HTTP	317	GET /sdfg.jar HTTP/1.1	59.53.91.102	192.168.23.129	TCP	60	80 → 1064 [ACK] Seq=2 Ack=264 Win=64240 Len=0	192.168.23.129	192.168.23.2	NBNS	110	Refresh NB TICKLAB<00>	59.53.91.102	192.168.23.129	TCP	1514	80 → 1065 [ACK] Seq=2 Ack=261 Win=64240 Len=1460 [TCP segment of a	59.53.91.102	192.168.23.129	TCP	1514	80 → 1065 [PSH, ACK] Seq=1462 Ack=261 Win=64240 Len=1460 [TCP segm	192.168.23.129	59.53.91.102	TCP	60	1065 → 80 [ACK] Seq=261 Ack=2922 Win=64240 Len=0	192.168.23.129	192.168.23.2	NBNS	110	Refresh NB TICKLAB<00>	192.168.23.129	192.168.23.2	NBNS	110	Refresh NB TICKLAB<00>	59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [ACK] Seq=2 Ack=264 Win=64240 Len=1460 [TCP segment of a	59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [PSH, ACK] Seq=1462 Ack=264 Win=64240 Len=1460 [TCP segm	192.168.23.129	59.53.91.102	TCP	60	1064 → 80 [ACK] Seq=264 Ack=2922 Win=64240 Len=0	59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [ACK] Seq=2922 Ack=264 Win=64240 Len=1460 [TCP segment o	59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [ACK] Seq=4282 Ack=264 Win=64240 Len=1460 [TCP segment o
Source	Destination	Protocol	Length	Info																																																																																																	
59.53.91.102	192.168.23.129	TCP	60	[TCP Port numbers reused] 80 → 1065 [SYN, ACK] Seq=1 Ack=1 Win=642																																																																																																	
192.168.23.129	59.53.91.102	TCP	60	1065 → 80 [ACK] Seq=1 Ack=2 Win=64240 Len=0																																																																																																	
59.53.91.102	192.168.23.129	TCP	60	[TCP Port numbers reused] 80 → 1064 [SYN, ACK] Seq=1 Ack=1 Win=642																																																																																																	
192.168.23.129	59.53.91.102	TCP	60	1064 → 80 [ACK] Seq=1 Ack=2 Win=64240 Len=0																																																																																																	
192.168.23.129	59.53.91.102	HTTP	314	GET /q.jar HTTP/1.1																																																																																																	
59.53.91.102	192.168.23.129	TCP	60	80 → 1065 [ACK] Seq=2 Ack=261 Win=64240 Len=0																																																																																																	
192.168.23.129	59.53.91.102	HTTP	317	GET /sdfg.jar HTTP/1.1																																																																																																	
59.53.91.102	192.168.23.129	TCP	60	80 → 1064 [ACK] Seq=2 Ack=264 Win=64240 Len=0																																																																																																	
192.168.23.129	192.168.23.2	NBNS	110	Refresh NB TICKLAB<00>																																																																																																	
59.53.91.102	192.168.23.129	TCP	1514	80 → 1065 [ACK] Seq=2 Ack=261 Win=64240 Len=1460 [TCP segment of a																																																																																																	
59.53.91.102	192.168.23.129	TCP	1514	80 → 1065 [PSH, ACK] Seq=1462 Ack=261 Win=64240 Len=1460 [TCP segm																																																																																																	
192.168.23.129	59.53.91.102	TCP	60	1065 → 80 [ACK] Seq=261 Ack=2922 Win=64240 Len=0																																																																																																	
192.168.23.129	192.168.23.2	NBNS	110	Refresh NB TICKLAB<00>																																																																																																	
192.168.23.129	192.168.23.2	NBNS	110	Refresh NB TICKLAB<00>																																																																																																	
59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [ACK] Seq=2 Ack=264 Win=64240 Len=1460 [TCP segment of a																																																																																																	
59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [PSH, ACK] Seq=1462 Ack=264 Win=64240 Len=1460 [TCP segm																																																																																																	
192.168.23.129	59.53.91.102	TCP	60	1064 → 80 [ACK] Seq=264 Ack=2922 Win=64240 Len=0																																																																																																	
59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [ACK] Seq=2922 Ack=264 Win=64240 Len=1460 [TCP segment o																																																																																																	
59.53.91.102	192.168.23.129	TCP	1514	80 → 1064 [ACK] Seq=4282 Ack=264 Win=64240 Len=1460 [TCP segment o																																																																																																	
B	29. 題組背景描述如附圖。若小明想使用常見的封包側錄工具來錄製封包，可以使用下列何種工具做封包錄製？ (A) jpgdump (B) wireshark (C) ipconfig (D) atpx																																																																																																				
A	30. 題組背景描述如附圖。請問附圖是小明下了什麼指令？ <table><tr><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0xfalc A nrtjo.eu</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0xfalc A nrtjo.eu</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0xfalc A nrtjo.eu</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0x5b1d A nrtjo.eu</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>85</td><td>Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>143</td><td>Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>71</td><td>Standard query 0xbca3 A freeways.in</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>235</td><td>Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everyd</td></tr></table> (A) udp.port == 53 (B) tcp.port eq 80 (C) ip.addr==192.168.23.9 (D) arp eq DNS	Source	Destination	Protocol	Length	Info	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfalc A nrtjo.eu	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfalc A nrtjo.eu	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfalc A nrtjo.eu	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com	192.168.23.129	192.168.23.2	DNS	68	Standard query 0x5b1d A nrtjo.eu	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com	192.168.23.129	192.168.23.2	DNS	85	Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa	192.168.23.2	192.168.23.129	DNS	143	Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa	192.168.23.129	192.168.23.2	DNS	71	Standard query 0xbca3 A freeways.in	192.168.23.2	192.168.23.129	DNS	235	Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everyd																																			
Source	Destination	Protocol	Length	Info																																																																																																	
192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfalc A nrtjo.eu																																																																																																	
192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfalc A nrtjo.eu																																																																																																	
192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfalc A nrtjo.eu																																																																																																	
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com																																																																																																	
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com																																																																																																	
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfalc A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com																																																																																																	
192.168.23.129	192.168.23.2	DNS	68	Standard query 0x5b1d A nrtjo.eu																																																																																																	
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com																																																																																																	
192.168.23.129	192.168.23.2	DNS	85	Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa																																																																																																	
192.168.23.2	192.168.23.129	DNS	143	Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa																																																																																																	
192.168.23.129	192.168.23.2	DNS	71	Standard query 0xbca3 A freeways.in																																																																																																	
192.168.23.2	192.168.23.129	DNS	235	Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everyd																																																																																																	
A B	31. 題組背景描述如附圖。小明從附圖中可找出封包中何者是惡意網站，造成同仁連上後下載了惡意程式，請問同仁電腦連上什麼中繼站，以及下載了什麼可疑的惡意檔案？（複選）																																																																																																				



# 110 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：110 年 9 月 25 日

第 9 頁，共 12 頁

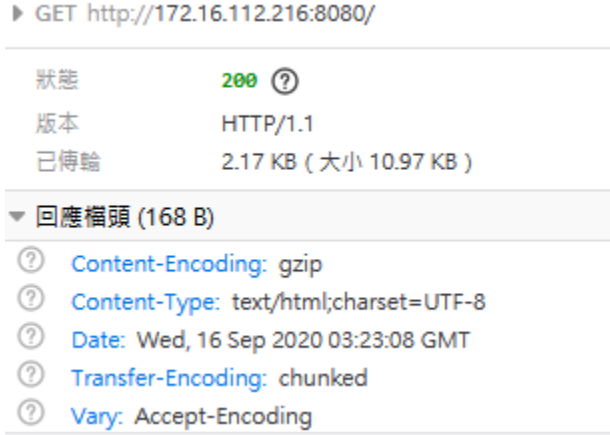
	<table><tr><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0xfa1c A nrtjo.eu</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0xfa1c A nrtjo.eu</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0xfa1c A nrtjo.eu</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>68</td><td>Standard query 0x5b1d A nrtjo.eu</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>162</td><td>Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>85</td><td>Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>143</td><td>Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa</td></tr><tr><td>192.168.23.129</td><td>192.168.23.2</td><td>DNS</td><td>71</td><td>Standard query 0xbca3 A freeways.in</td></tr><tr><td>192.168.23.2</td><td>192.168.23.129</td><td>DNS</td><td>235</td><td>Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everyd</td></tr></table> <table><tr><th>Packet</th><th>Hostname</th><th>Content Type</th><th>Size</th><th>Filename</th></tr><tr><td>13</td><td>nrtjo.eu</td><td>text/html</td><td>6278 bytes</td><td>true.php</td></tr><tr><td>32</td><td>nrtjo.eu</td><td>text/plain</td><td>171 bytes</td><td>xxx.xxx</td></tr><tr><td>55</td><td>nrtjo.eu</td><td>text/html</td><td>409 bytes</td><td>favicon.ico</td></tr><tr><td>85</td><td>nrtjo.eu</td><td>application/x-java-archive</td><td>7079 bytes</td><td>sdfg.jar</td></tr><tr><td>98</td><td>nrtjo.eu</td><td>application/x-java-archive</td><td>5573 bytes</td><td>q.jar</td></tr><tr><td>217</td><td>nrtjo.eu</td><td>application/octet-stream</td><td>68 kB</td><td>loading.php?spl=javad0</td></tr><tr><td>273</td><td>nrtjo.eu</td><td>application/octet-stream</td><td>68 kB</td><td>loading.php?spl=javadnw&amp;J050006010</td></tr><tr><td>295</td><td>freeways.in</td><td>text/html</td><td>672 bytes</td><td>gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7A</td></tr></table> <p>(A) nrtjo.eu 下載 sdfg.jar (B) nrtjo.eu 下載 q.jar (C) nrtjo.eu 下載 favicon.ico (D) freeways.in 下載 gates.php</p>	Source	Destination	Protocol	Length	Info	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com	192.168.23.129	192.168.23.2	DNS	68	Standard query 0x5b1d A nrtjo.eu	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com	192.168.23.129	192.168.23.2	DNS	85	Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa	192.168.23.2	192.168.23.129	DNS	143	Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa	192.168.23.129	192.168.23.2	DNS	71	Standard query 0xbca3 A freeways.in	192.168.23.2	192.168.23.129	DNS	235	Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everyd	Packet	Hostname	Content Type	Size	Filename	13	nrtjo.eu	text/html	6278 bytes	true.php	32	nrtjo.eu	text/plain	171 bytes	xxx.xxx	55	nrtjo.eu	text/html	409 bytes	favicon.ico	85	nrtjo.eu	application/x-java-archive	7079 bytes	sdfg.jar	98	nrtjo.eu	application/x-java-archive	5573 bytes	q.jar	217	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javad0	273	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javadnw&J050006010	295	freeways.in	text/html	672 bytes	gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7A													
Source	Destination	Protocol	Length	Info																																																																																																																								
192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu																																																																																																																								
192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu																																																																																																																								
192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu																																																																																																																								
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com																																																																																																																								
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com																																																																																																																								
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com																																																																																																																								
192.168.23.129	192.168.23.2	DNS	68	Standard query 0x5b1d A nrtjo.eu																																																																																																																								
192.168.23.2	192.168.23.129	DNS	162	Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com																																																																																																																								
192.168.23.129	192.168.23.2	DNS	85	Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa																																																																																																																								
192.168.23.2	192.168.23.129	DNS	143	Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa																																																																																																																								
192.168.23.129	192.168.23.2	DNS	71	Standard query 0xbca3 A freeways.in																																																																																																																								
192.168.23.2	192.168.23.129	DNS	235	Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everyd																																																																																																																								
Packet	Hostname	Content Type	Size	Filename																																																																																																																								
13	nrtjo.eu	text/html	6278 bytes	true.php																																																																																																																								
32	nrtjo.eu	text/plain	171 bytes	xxx.xxx																																																																																																																								
55	nrtjo.eu	text/html	409 bytes	favicon.ico																																																																																																																								
85	nrtjo.eu	application/x-java-archive	7079 bytes	sdfg.jar																																																																																																																								
98	nrtjo.eu	application/x-java-archive	5573 bytes	q.jar																																																																																																																								
217	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javad0																																																																																																																								
273	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javadnw&J050006010																																																																																																																								
295	freeways.in	text/html	672 bytes	gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7A																																																																																																																								
A	<p>32. 題組背景描述如附圖。小明在附圖封包中可以判斷出受害者連線下載惡意程式的網站 IP 位置為下列何者？</p> <table><tr><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>2010-03-17 00:50:18.363025</td><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>80 → 1061 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460</td></tr><tr><td>2010-03-17 00:50:18.363270</td><td>192.168.23.129</td><td>59.53.91.102</td><td>TCP</td><td>60</td><td>1061 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0</td></tr><tr><td>2010-03-17 00:50:18.364685</td><td>192.168.23.129</td><td>59.53.91.102</td><td>HTTP</td><td>517</td><td>GET /true.php HTTP/1.1</td></tr><tr><td>2010-03-17 00:50:18.367012</td><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>80 → 1061 [ACK] Seq=1 Ack=464 Win=64240 Len=0</td></tr><tr><td>2010-03-17 00:50:21.268121</td><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>1514</td><td>80 → 1061 [ACK] Seq=1 Ack=464 Win=64240 Len=1460 [TCP segment of</td></tr><tr><td>2010-03-17 00:50:21.268142</td><td>59.53.91.102</td><td>192.168.23.129</td><td>HTTP</td><td>136</td><td>HTTP/1.1 200 OK (text/html)</td></tr><tr><td>2010-03-17 00:50:21.280061</td><td>192.168.23.129</td><td>59.53.91.102</td><td>TCP</td><td>60</td><td>1061 → 80 [ACK] Seq=464 Ack=1543 Win=64240 Len=0</td></tr><tr><td>2010-03-17 00:50:21.306342</td><td>192.168.23.129</td><td>59.53.91.102</td><td>HTTP</td><td>364</td><td>GET /xxx.xxx HTTP/1.1</td></tr><tr><td>2010-03-17 00:50:21.306361</td><td>59.53.91.102</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>80 → 1061 [ACK] Seq=1543 Ack=774 Win=64240 Len=0</td></tr><tr><td>2010-03-17 00:50:21.420447</td><td>192.168.23.129</td><td>65.55.195.250</td><td>TCP</td><td>62</td><td>1062 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1</td></tr><tr><td>2010-03-17 00:50:21.502696</td><td>65.55.195.250</td><td>192.168.23.129</td><td>TCP</td><td>60</td><td>443 → 1062 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460</td></tr><tr><td>2010-03-17 00:50:21.508176</td><td>192.168.23.129</td><td>65.55.195.250</td><td>TCP</td><td>60</td><td>1062 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0</td></tr></table> <table><tr><th>Packet</th><th>Hostname</th><th>Content Type</th><th>Size</th><th>Filename</th></tr><tr><td>13</td><td>nrtjo.eu</td><td>text/html</td><td>6278 bytes</td><td>true.php</td></tr><tr><td>32</td><td>nrtjo.eu</td><td>text/plain</td><td>171 bytes</td><td>xxx.xxx</td></tr><tr><td>55</td><td>nrtjo.eu</td><td>text/html</td><td>409 bytes</td><td>favicon.ico</td></tr><tr><td>85</td><td>nrtjo.eu</td><td>application/x-java-archive</td><td>7079 bytes</td><td>sdfg.jar</td></tr><tr><td>98</td><td>nrtjo.eu</td><td>application/x-java-archive</td><td>5573 bytes</td><td>q.jar</td></tr><tr><td>217</td><td>nrtjo.eu</td><td>application/octet-stream</td><td>68 kB</td><td>loading.php?spl=javad0</td></tr><tr><td>273</td><td>nrtjo.eu</td><td>application/octet-stream</td><td>68 kB</td><td>loading.php?spl=javadnw&amp;J050006010</td></tr><tr><td>295</td><td>freeways.in</td><td>text/html</td><td>672 bytes</td><td>gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7A&amp;ver=10084&amp;stat=ONLINE&amp;ie=8.0.6001.18702&amp;os=5.1.2600&amp;ut=Admin&amp;cpu=92&amp;cc</td></tr></table> <p>(A) 59.53.91.102 (B) 192.168.23.129 (C) 65.55.195.250 (D) 127.0.0.1</p>	Time	Source	Destination	Protocol	Length	Info	2010-03-17 00:50:18.363025	59.53.91.102	192.168.23.129	TCP	60	80 → 1061 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	2010-03-17 00:50:18.363270	192.168.23.129	59.53.91.102	TCP	60	1061 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0	2010-03-17 00:50:18.364685	192.168.23.129	59.53.91.102	HTTP	517	GET /true.php HTTP/1.1	2010-03-17 00:50:18.367012	59.53.91.102	192.168.23.129	TCP	60	80 → 1061 [ACK] Seq=1 Ack=464 Win=64240 Len=0	2010-03-17 00:50:21.268121	59.53.91.102	192.168.23.129	TCP	1514	80 → 1061 [ACK] Seq=1 Ack=464 Win=64240 Len=1460 [TCP segment of	2010-03-17 00:50:21.268142	59.53.91.102	192.168.23.129	HTTP	136	HTTP/1.1 200 OK (text/html)	2010-03-17 00:50:21.280061	192.168.23.129	59.53.91.102	TCP	60	1061 → 80 [ACK] Seq=464 Ack=1543 Win=64240 Len=0	2010-03-17 00:50:21.306342	192.168.23.129	59.53.91.102	HTTP	364	GET /xxx.xxx HTTP/1.1	2010-03-17 00:50:21.306361	59.53.91.102	192.168.23.129	TCP	60	80 → 1061 [ACK] Seq=1543 Ack=774 Win=64240 Len=0	2010-03-17 00:50:21.420447	192.168.23.129	65.55.195.250	TCP	62	1062 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	2010-03-17 00:50:21.502696	65.55.195.250	192.168.23.129	TCP	60	443 → 1062 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	2010-03-17 00:50:21.508176	192.168.23.129	65.55.195.250	TCP	60	1062 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0	Packet	Hostname	Content Type	Size	Filename	13	nrtjo.eu	text/html	6278 bytes	true.php	32	nrtjo.eu	text/plain	171 bytes	xxx.xxx	55	nrtjo.eu	text/html	409 bytes	favicon.ico	85	nrtjo.eu	application/x-java-archive	7079 bytes	sdfg.jar	98	nrtjo.eu	application/x-java-archive	5573 bytes	q.jar	217	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javad0	273	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javadnw&J050006010	295	freeways.in	text/html	672 bytes	gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7A&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=92&cc
Time	Source	Destination	Protocol	Length	Info																																																																																																																							
2010-03-17 00:50:18.363025	59.53.91.102	192.168.23.129	TCP	60	80 → 1061 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460																																																																																																																							
2010-03-17 00:50:18.363270	192.168.23.129	59.53.91.102	TCP	60	1061 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0																																																																																																																							
2010-03-17 00:50:18.364685	192.168.23.129	59.53.91.102	HTTP	517	GET /true.php HTTP/1.1																																																																																																																							
2010-03-17 00:50:18.367012	59.53.91.102	192.168.23.129	TCP	60	80 → 1061 [ACK] Seq=1 Ack=464 Win=64240 Len=0																																																																																																																							
2010-03-17 00:50:21.268121	59.53.91.102	192.168.23.129	TCP	1514	80 → 1061 [ACK] Seq=1 Ack=464 Win=64240 Len=1460 [TCP segment of																																																																																																																							
2010-03-17 00:50:21.268142	59.53.91.102	192.168.23.129	HTTP	136	HTTP/1.1 200 OK (text/html)																																																																																																																							
2010-03-17 00:50:21.280061	192.168.23.129	59.53.91.102	TCP	60	1061 → 80 [ACK] Seq=464 Ack=1543 Win=64240 Len=0																																																																																																																							
2010-03-17 00:50:21.306342	192.168.23.129	59.53.91.102	HTTP	364	GET /xxx.xxx HTTP/1.1																																																																																																																							
2010-03-17 00:50:21.306361	59.53.91.102	192.168.23.129	TCP	60	80 → 1061 [ACK] Seq=1543 Ack=774 Win=64240 Len=0																																																																																																																							
2010-03-17 00:50:21.420447	192.168.23.129	65.55.195.250	TCP	62	1062 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1																																																																																																																							
2010-03-17 00:50:21.502696	65.55.195.250	192.168.23.129	TCP	60	443 → 1062 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460																																																																																																																							
2010-03-17 00:50:21.508176	192.168.23.129	65.55.195.250	TCP	60	1062 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0																																																																																																																							
Packet	Hostname	Content Type	Size	Filename																																																																																																																								
13	nrtjo.eu	text/html	6278 bytes	true.php																																																																																																																								
32	nrtjo.eu	text/plain	171 bytes	xxx.xxx																																																																																																																								
55	nrtjo.eu	text/html	409 bytes	favicon.ico																																																																																																																								
85	nrtjo.eu	application/x-java-archive	7079 bytes	sdfg.jar																																																																																																																								
98	nrtjo.eu	application/x-java-archive	5573 bytes	q.jar																																																																																																																								
217	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javad0																																																																																																																								
273	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=javadnw&J050006010																																																																																																																								
295	freeways.in	text/html	672 bytes	gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7A&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=92&cc																																																																																																																								
	<p>(題組 4)</p> <p>滲透測試 (Penetration Test) 是通過模擬惡意黑客的攻擊方法，來評估計算機網路系統安全的一種測試，目的是發掘系統漏洞，並提出改善方法，且通常來說是善意的，小李身為 A 公司的資安工程師，請就上述情境回答下列問題。</p>																																																																																																																											
C	<p>33. 題組背景描述如附圖。下列何者較「不」可能是小李滲透測試 (Penetration Test) 會使用到的工具？</p> <p>(A) Wireshark</p>																																																																																																																											

# 110 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：110 年 9 月 25 日

第 10 頁，共 12 頁

	<p>(B) Burp Suit (C) Nagios (D) Nmap</p>
B	<p>34. 題組背景描述如附圖。承上題，當小李完成滲透測試後於報告中發現附圖資訊，判斷公司可能出現下列何種風險漏洞？</p>  <p>(A) 敏感目錄暴露 (Possible sensitive directories) (B) 未強制使用 HTTPS (Unencrypted connection) (C) Session Cookie 未設定為 Secure 安全模式 (Cookie without Secure flag set) (D) 啟用 SSH 較弱 MAC 加密算法 (SSH Weak MAC Algorithms Enabled)</p>
D	<p>35. 題組背景描述如附圖。公司要求小李再協助處理弱點掃描 (Vulnerability Assessment)，請問滲透測試與弱點掃描的差異為下列何者？</p> <p>(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漏洞 (D) 滲透測試為資安專家仿駭客思維、發掘安全漏洞，以實戰方式找出任何可能突破目前網站安全防護的檢測</p>
A B D	<p>36. 題組背景描述如附圖。小李在研究系統安全維運與測試的過程，發現為了讓資訊安全測試與設計有較容易遵循的方法與流程，它是由多位資安領域專家、學者或顧問共同撰寫而成定義出許多資訊安全測試與設計範本，可幫助資安人員對於資訊安全測試與設計有一個較完整的全貌，請問下列哪些是目前業界共同的資訊安全測試參考的（方法論）文件範本？（複選）</p> <p>(A) Open Web Application Security Project Testing Guide (OWASP)</p>

# 110 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：110 年 9 月 25 日

第 11 頁，共 12 頁

	<p>(B) Common Weakness Enumeration (CWE)</p> <p>(C) Open Shortest Path First (OSPF)</p> <p>(D) Information Systems Security Assessment Framework (ISSAF)</p>
	<p>(題組 5)</p> <p>小張為某公司資安工程師，其使用某工具並輸入了下列的指令執行：</p> <p>nc -vzw5 192.168.0.1 1-2048 (操控端)</p> <p>nc -v -z -w5 192.168.0.1 1-2048 (操控端)</p> <p>nc -ltp 80 (操控端)</p> <p>nc -l -p 80 &lt; /test.txt (操控端)</p> <p>nc -t -p 80 &lt; /test.txt (操控端)</p> <p>nc -g -p 80 &gt; /test.txt (操控端)</p> <p>nc -g -p 80 &lt; /test.txt (操控端)</p> <p>nc -l -p 80 (操控端)</p>
D	<p>37. 題組背景描述如附圖。請問小張使用此工具的主要目的為下列何者？</p> <p>(A) NetChannel 工具通常使用於網路管理情境之下，主要目的為建立網路通道之用</p> <p>(B) NoCommand 工具通常使用於將 DOS Command 轉換為 GUI 介面執行</p> <p>(C) NoCommunication 工具通常使用於建立雙方之通訊連線</p> <p>(D) NetCat 工具通常使用於網路管理情境之下，亦為滲透測試常用工具之一</p>
C	<p>38. 題組背景描述如附圖。關於附圖兩個指令的執行結果，何者正確？</p> <p>nc -vzw5 192.168.0.1 1-2048 (操控端)</p> <p>nc -v -z -w5 192.168.0.1 1-2048 (操控端)</p> <p>(A) 結果相同，對 192.168.0.1 主機進行 vpn 連線，且連線時間設定 2048 秒</p> <p>(B) 結果不同，對 192.168.0.1 主機進行監聽，且監聽時間設定 2048 秒</p> <p>(C) 結果相同，對 192.168.0.1 主機之 TCP port 1-2048 進行掃描，且連線逾時設定 5 秒</p> <p>(D) 結果不同，對 192.168.0.1 主機之 UCP port 1-2048 進行掃描，且連線逾時設定 5 秒</p>
B D	<p>39. 題組背景描述如附圖。請問題目中指令 nc -ltp 80 (操控端) 的執行結果為下列何者？(複選)</p> <p>(A) 關閉 telnet 模式</p> <p>(B) 啟動 telnet 模式</p> <p>(C) 阻斷 80 port</p>

# 110 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：110 年 9 月 25 日

第 12 頁，共 12 頁

	(D) 指定 80 port 為監聽 port
A	<p>40. 題組背景描述如附圖。請問操控端下達何種指令時，等待接聽 TCP 80 port，若接收到連線，就可以將 test.txt 傳送給對方？</p> <p>(A) nc -l -p 80 &lt; type test.txt ( 操控端 )</p> <p>(B) nc -t -p 80 &lt; type test.txt ( 操控端 )</p> <p>(C) nc -g -p 80 &gt; type test.txt ( 操控端 )</p> <p>(D) nc -g -p 80 &lt; type test.txt ( 操控端 )</p>