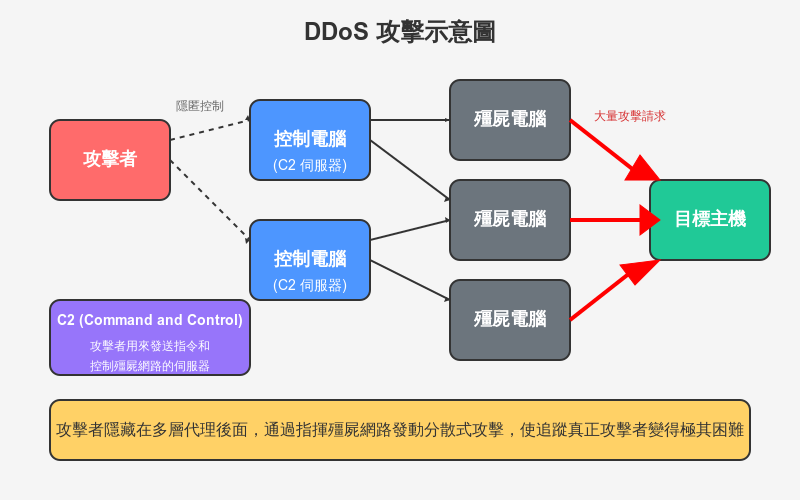
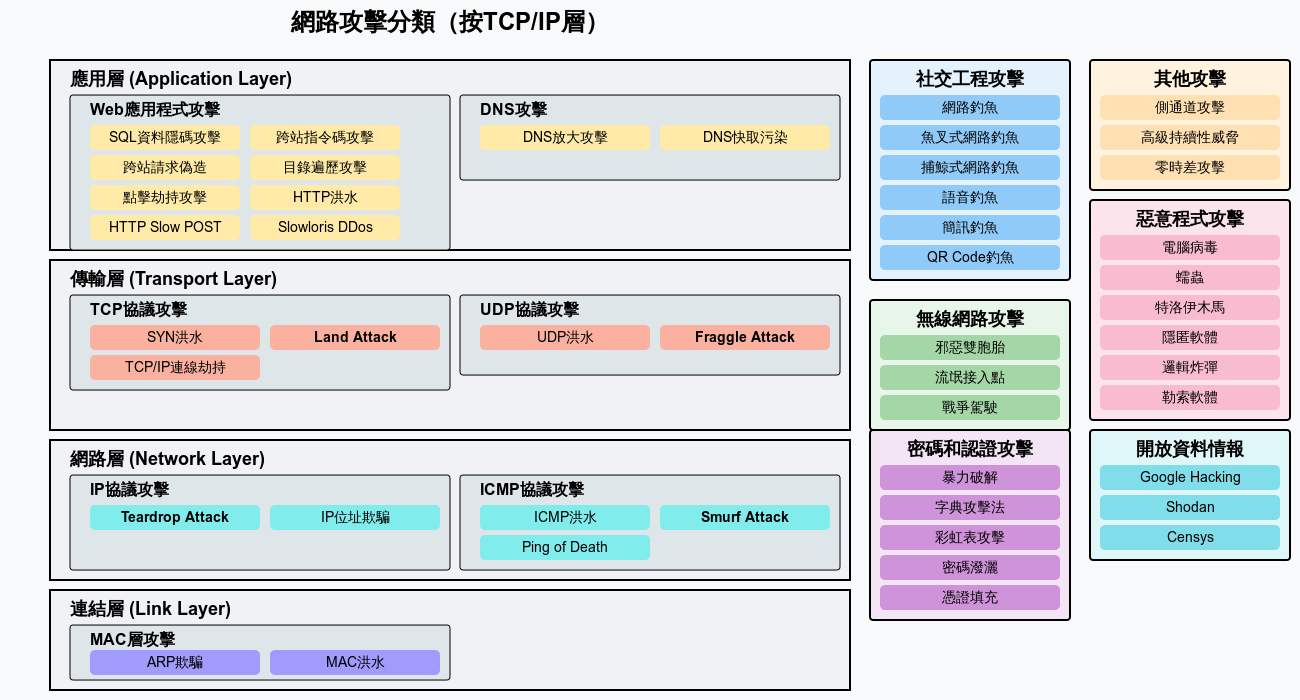
攻擊手法

**攻擊分類與手法：**

* 公開來源情報
  + 公開來源情報 (Open Source Intelligence, ONIST) ：是從公開來源收集到的情報，例如Facebook、Twitter上資訊發動攻擊，例如蒐集到使用者生日來猜密碼。
  + 谷歌駭侵法 (Google Hacking)：利用Google搜尋指令（如site:、filetype:、inurl:）來尋找目標資訊，例如找出網站中包含個人資料的檔案（如PDF、Excel）。
  + 常用工具與網站：
    - Shodan、Censys：用於網路裝置、協議的公開搜尋。
    - Exploit-DB：蒐錄Google Hacking別人已經寫好的搜尋指令。
* 網路協議攻擊
  + 重送攻擊 (Replay Attack)：重播先前合法封包以執行重複操作。
  + Teardrop Attack (IP層)：一種針對IP分片重組機制的攻擊。攻擊者發送具有重疊偏移量的IP分片封包，當目標系統嘗試重組這些分片時，由於處理異常的偏移值，會導致系統崩潰或當機。
  + 死亡之Ping (Ping of Death)：透過發送超出IP協議允許最大大小(65,535位元組)的ICMP回顯請求(ping)封包攻擊系統。當目標系統嘗試處理這些異常大小的ping封包時，會導致緩衝區溢出，使系統崩潰。
  + 中間人攻擊 (Man-in-the-Middle, MITM) ：攔截雙方通訊。
    - DNS 快取汙染 (DNS Cache Poisoning) ：修改 DNS 回應資料，劫持流量。
    - IP 位址欺騙 (IP Spoofing) ：偽造 IP 位址以隱藏攻擊者身份。
    - ARP 欺騙 (ARP Spoofing) ：攻擊本地區域網路的 ARP 資料，誘導流量。
    - MAC 洪水 (MAC flood)：向交換機發送大量偽造的MAC位址，使其MAC位址表溢出，當交換機的MAC位址表滿時，會將所有流量廣播到所有連接埠，讓攻擊者可以竊聽到本來無法看見的網路流量。
    - TCP/IP 連線劫持 (TCP/IP Session Hijacking) ：攻擊者劫持合法 TCP 連線，插入惡意封包並繼續會話。
    - SSL連線劫持 (SSL Hijacking) ：攻擊者劫持已建立的 SSL/TLS 加密連線，解密並篡改通訊內容，竊取敏感資訊或偽裝成合法用戶。
    - SSLStrip 攻擊：SSLStrip 是一種常見的中間人攻擊手法，可以將 HTTPS 連線降級為 HTTP。如果網站沒有設定 HSTS，攻擊者可以利用 SSLStrip 攻擊，攔截使用者的連線，並將使用者導向至偽造的 HTTP 網站，進而竊取使用者的帳號密碼或其他敏感資訊。
    - 邪惡雙胞胎 (Evil Twin)：邪惡雙胞胎是通常配置有相似或相同的SSID和密碼設置的偽造的無線訪問點 (AP) 。
    - 流氓接入點 (Rogue Access Point)：指的是任何未經授權的無線訪問點(AP)。
* Web應用程式攻擊
  + SQL資料隱碼攻擊 (SQL Injection) ：注入惡意 SQL 語句竊取資料。
  + 跨站指令碼攻擊 (XSS) ：嵌入惡意腳本，竊取用戶資訊。
  + 跨站請求偽造 (CSRF) ：冒充使用者向伺服器發送請求。
  + 緩衝區溢位 (Buffer Overflow) ：輸入超過預設資料長度的方式，影響記憶體中資料的正確性。
  + 目錄遍歷攻擊 (Directory Traversal) ：存取未授權檔案，可能導致遠端程式碼執行 (RCE) 。
  + 點擊劫持攻擊 (Clickjacking) ：攻擊者使用透明的網頁層覆蓋在正常網頁上，誘騙使用者點擊。
* 阻斷服務攻擊 (DoS)
  + DoS 攻擊分類：
    - 流量消耗型：消耗網路頻寬 (如SYN flood、UDP flood、ICMP flood、Fraggle Attack (UDP層)、Smurf Attack (ICMP層)、DNS放大攻擊等)。
    - 資源消耗型：耗盡伺服器 CPU 、記憶體、連線數資源(如HTTP Slow POST、Slowloris攻擊、Land Attack (TCP層)、HTTP flood等)。
  + 如果多台發動我們稱為分散式阻斷服務攻擊 (DDos)。
    - 攻擊者隱藏在多層代理後面，通過指揮殭屍網路發動分散式攻擊，使追蹤真正攻擊者變得極其困難。
    - 指令和控制 (Command and Control, C2)：攻擊者用來發送指令和控制殭屍網路的伺服器。

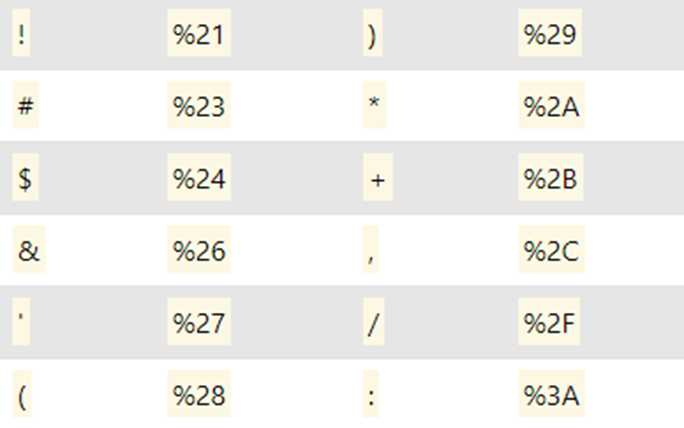


* 社交工程攻擊
  + 網路釣魚 (Phishing) ：透過假網站或郵件竊取憑證。
  + 魚叉式網路釣魚 (Spear Phishing) ：針對特定目標的釣魚攻擊。
  + 捕鯨式網路釣魚 (Whaling) ：針對高層管理者的釣魚攻擊。
  + 語音釣魚 (Vishing) ：透過語音誘導洩密。
  + 簡訊釣魚 (Smishing)：利用簡訊進行的釣魚攻擊，攻擊者會發送含有惡意連結或要求提供敏感資訊的訊息。
  + QR Code釣魚 (Quishing)：透過QR Code進行的釣魚攻擊，攻擊者將惡意連結隱藏在QR Code，因本身為圖像檔案，故部分防禦機制無法偵測圖像檔案之連結是否為惡意。
  + 同形異義字釣魚攻擊 (Punycode Phishing)：這是一種利用視覺混淆的攻擊手法，攻擊者會註冊看似與合法網站相同的網域名稱，實際上卻包含不同字元。例如可能使用外觀相似的拉丁字元（如數字「0」與字母「O」、數字「1」與小寫「l」）或跨語系的同形字（如西里爾字母「а」取代拉丁字母「a」、希臘字母「ο」取代拉丁字母「o」）。這些差異在瀏覽器網址列中極難察覺，使使用者誤以為自己進入的是正確網站，進而輸入敏感資訊，導致個資外洩。
* 惡意程式攻擊
  + 電腦病毒 (Virus) ：感染其他檔案或系統，需使用者觸發。
  + 蠕蟲 (Worm) ：自我複製並在網路中傳播。
  + 特洛伊木馬程式 (Trojan Horse) ：偽裝成合法軟體的惡意程式是一種偽裝成合法或有用軟體的惡意程式，當用戶執行時，木馬會在系統中執行未經授權的操作，如資料竊取、後門建立等。
  + 隱匿軟體 (Rootkit) ：隱藏惡意活動。
  + Bootkit：與 Rootkit 類似，但是它是安裝在操作系統的引導 (boot) 區塊，以實現在操作系統啟動之前攻擊的目的。
  + 邏輯炸彈 (Logic Bomb) ：在特定條件觸發時才會執行的惡意程式，例如：員工離職後，系統在特定日期自動刪除重要資料。
  + 無檔案惡意軟體 (Fileless Malware)：無文件惡意軟體僅存在於受感染電腦的記憶體中，不會向磁碟寫入任何內容。
  + 後門程式 (Backdoor) ：提供未經授權的存取入口。
  + 勒索軟體 (Ransomware) ：加密資料後勒索贖金，或是不付錢就公開公司資料。
  + 遠端程式碼執行 (Remote Code Execution, RCE)：攻擊者透過漏洞在目標系統中遠端執行任意指令，通常可完全控制系統，廣泛用於滲透、植入後門或橫向移動等攻擊階段。RCE 本身不是惡意程式，而是由多種漏洞（如輸入驗證不當、命令注入、記憶體漏洞等）造成的攻擊結果。
* 密碼和認證攻擊
  + 暴力破解 (Brute Force Attack) ：嘗試所有可能組合。
  + 字典攻擊法 (Dictionary Attack) ：使用預設常見密碼組合。
  + 彩虹表攻擊 (Rainbow Table Attack) ：使用預先計算的雜湊值形成一個表利用查表來破解密碼。
  + 密碼潑灑 (Password Spraying) ：單一密碼試用多個帳號，避免帳號試密碼被偵測。
  + 憑證填充 (Credential Stuffing) ：使用其他網站洩漏的憑證嘗試登入。
* 其他攻擊
  + 旁通道攻擊 (Side-Channel Attack) ：利用電磁波、耗電量、鍵盤打字的聲音等間接特徵偷取資訊。
  + 高級持續性威脅 (Advanced Persistent Threat, APT) ：針對特定目標的長期滲透攻擊，通常會使用多種混合技術並搭配零時差攻擊。
  + 零時差攻擊 (Zero-Day Attack) ：指駭客在軟體或系統的弱點尚未被揭露，或雖然已被揭露但尚未有修補程式釋出前，利用該弱點發動攻擊，類似新冠肺炎剛出來一樣，已經知道有病毒 ，但是還沒有疫苗製作出來。
    - 1-Day 攻擊：漏洞已經公開且已有修補程式，但某些系統尚未來得及更新。駭客利用這種「已知且可修補」的漏洞對未更新的目標發動攻擊。
    - N-Day 攻擊："N" 代表漏洞公開後經過了若干天、幾個月甚至幾年，駭客針對長期未修補漏洞的系統發起攻擊。
  + 垃圾桶攻擊法 (Dumpster Diving) ：翻看垃圾桶查看有無沒有碎掉的公司機密資訊。
  + 隱寫術 (Steganography) ：可在普通消息中隱藏秘密消息，例如把圖片的RGB第一個bit改成傳遞隱藏資料，或是我們常說的藏頭詩。
  + 誤植域名攻擊 (Typosquatting Attack)：這是一種被動式攻擊，攻擊者會註冊與合法網站極為相似、但拼寫上略有差異的網域名稱，藉此誘騙用戶誤入惡意網站。這類拼寫錯誤可能來自鍵入錯誤（如將「google.com」打成「goolge.com」）、記憶混淆（如將「citibank.com」誤認為「citybank.com」）、甚至是品牌讀音相近所導致的誤解。一旦用戶誤入這些偽造網站，可能會面臨帳號被竊、資料外洩等資安風險。
  + DLL 劫持 (DLL Side Loading)：是一種攻擊技術，它利用 Windows 應用程式載入動態連結程式庫 (DLL) 的方式來執行惡意程式碼。攻擊者會將惡意的 DLL 放置在特定的目錄中，誘使應用程式載入惡意的 DLL，而不是原本應該載入的合法 DLL。
  + 戰爭駕駛 (WarDriving)：通常是指有人開車尋找免費的無線網路使用，考試通常指公司由有線變成無線網路，導致駭客可以不進公司攻擊，增加被攻擊的風險。
  + BYOVD (Bring Your Own Vulnerable Driver)：攻擊者利用具合法微軟簽章但存在漏洞的驅動程式，載入系統後利用其漏洞獲取Kernel權限的技術。由於驅動程式具有認可的數位簽章，能繞過系統的驅動程式簽章驗證機制。攻擊者藉此執行惡意操作，如關閉防毒軟體或安裝Rootkit等。



**常見攻擊與防禦**

* SQL資料隱碼攻擊 (SQL Injection)
  + 攻擊手法：' OR '1'='1, %27+OR+%271%27%3D%271%27(URL 編碼)。

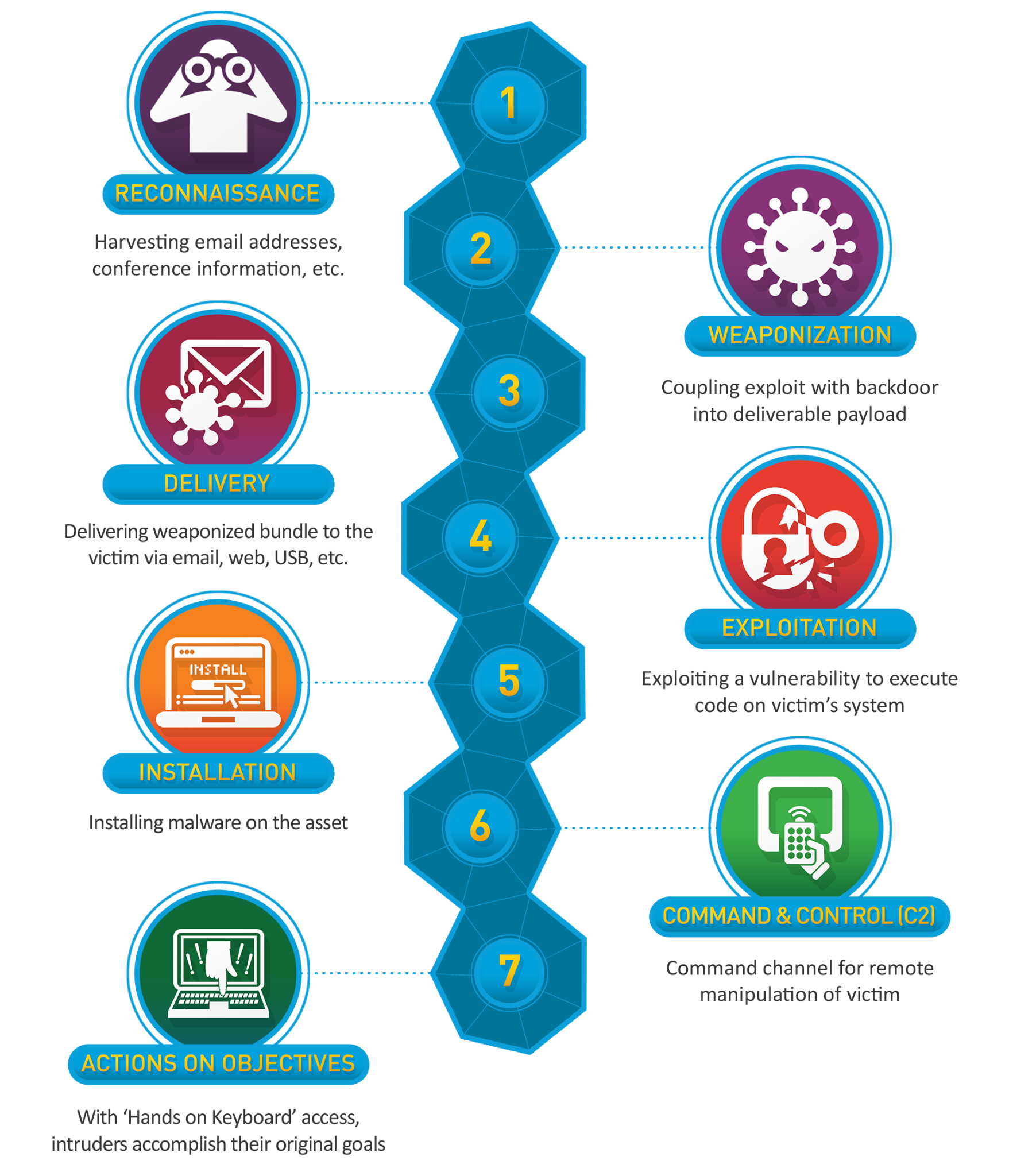


(URL編碼，資料來源：網際網路)

* + 題目提示：若提到拼接用戶輸入到 SQL 查詢語句。
  + 防禦方法：
    - 參數化查詢 (Parameterized Queries)。
    - 預編譯語句 (Prepared Statement) 和預存程序 (Stored Procedures)。
    - 使用安全的應用程式界面 (API) 防止注入攻擊漏洞的發生。
    - 使用白名單過濾輸入資料，避免僅依賴黑名單 (因為黑名單很難列舉所有攻擊)。
* 跨站指令碼攻擊 (XSS)
  + <script>alert(’abc’);</script>, <OMG SRC=javascript:alert(’lol’)>, %3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E(URL編碼型式)。
  + 題目提示：若提到未檢查的用戶輸入在瀏覽器中執行。
  + 常用攻擊語言：JavaScript
  + 防禦方法**：**
    - 白名單過濾輸入參數。
    - HTML 編碼 (HTMLEncode) 。
    - 使用 Content Security Policy (CSP) 。
* 跨站請求偽造 (CSRF)
  + 攻擊手法：未經用戶授權執行敏感操作。
  + 題目提到：敏感操作的跨站請求。
  + 防禦方式：
    - 使用 CSRF Token。
    - 啟用 SameSite Cookie。
    - 檢查 HTTP Referer 或 Origin 標頭。
* 命令注入(Cmd Injection)：
  + 攻擊手法：&, ;, |, &&, ||, $(command), `command` (Linux常用sh和ls，Window常用cmd和dir)。
  + 題目提示：若提到用戶輸入直接用於執行系統命令。
* 目錄遍歷攻擊 (Directory Traversal)
  + 攻擊手法：../../etc/passwd, ..%2F..%2F (URL 編碼)。
  + 題目提示：提到通過修改路徑訪問未授權檔案。
  + 防禦方法：
    - 使用白名單路徑限制訪問範圍。
    - 過濾常見危險字串，例如 ".."、"/"、"\ "，不能單一使用搭配其他方法。
* 拒絕服務攻擊 (DoS/DDoS)
  + 攻擊手法：DNS 放大攻擊、HTTP Slow POST或Ping of Death。
  + 防禦方法：
    - 流量型：使用 CDN 提供的流量清洗服務。
    - 資源消耗型：需要WAF防護和連線管理。
* 社交工程 (Social Engineering)
  + 攻擊手法：釣魚郵件、偽裝客服、假網站。
  + 題目提示：描述利用人性弱點誘導行為。
  + 防禦方法：
    - 加強員工郵件安全教育訓練。
    - 定期進行釣魚攻擊模擬和社交工程演練。
* ARP 欺騙 (ARP Spoofing)
  + 攻擊手法：偽造 ARP 回應，劫持本地區域網路流量。
  + 防禦方法：使用靜態 ARP 表，設定固定 IP 並綁定 MAC 地址。
* 中間人攻擊 (Man-in-the-Middle, MITM)
  + 攻擊手法：
    - 攻擊者攔截雙方通訊，竊聽或篡改傳輸的資訊，讓雙方以為正在與對方通訊。
    - 常見於公共 Wi-Fi、中間代理伺服器或 ARP 欺騙場景。
  + 防禦方法：
    - 使用 SSH 或 HTTPS 加密傳輸，確保機密性與完整性。
    - 驗證伺服器憑證，防止假冒網站或伺服器。
    - 避免使用公共網路，或通過 VPN 加密所有流量。

**網路攻擊鏈 (Cyber Kill Chain)**

* 作為進階補充，描述攻擊的階段性流程。適合題目提到攻擊全流程或特定階段時快速定位。
* 偵查 (Reconnaissance)：收集目標資訊，為攻擊做準備。
* 武裝 (Weaponization)：製造惡意工具 (如惡意程式或文件)。
* 遞送 (Delivery)：將攻擊工具傳送至目標 (如釣魚郵件)。
* 漏洞利用 (Exploitation)：利用漏洞或誘使目標執行惡意代碼。
* 安裝 (Installation)：將惡意程式安裝到目標系統，建立後門。
* 發令與控制 (Command & Control)：攻擊者遠端控制受害者系統。
* 行動 (Actions)：實現攻擊目標 (如竊密、勒索、破壞)。



**MITRE ATT&CK框架**

* 針對具體技術進行分類，與 Cyber Kill Chain 結構互補，提供更細緻的攻擊描述。
* Reconnaissance (偵查)：收集目標資訊，為攻擊準備。
* Resource Development (資源開採)：建立攻擊所需資源。
* Initial Access (初始存取)：獲得進入目標系統的途徑。
* Execution (執行)：執行惡意程式或命令。
* Persistence (持久性)：設置後門，保持長期控制。
* Privilege Escalation (權限提升)：提升權限至管理級 (如 root)。
* Defense Evasion (防禦規避)：繞過安全防護機制。
* Credential Access (憑證存取)：竊取帳號憑證或密碼。
* Discovery (發現)：探測內部環境資訊。
* Lateral Movement (橫向移動)：在內部網路中移動到其他設備。
* Collection (收集)：收集機密數據或敏感資訊。
* Command and Control (指令與控制)：與目標設備建立通信。
* Exfiltration (外洩)：將蒐集的資料傳輸到攻擊者伺服器。
* Impact (影響)：對目標系統進行破壞或達成攻擊目的。



**考古題：**

1. 為避免所建置之網購系統遭受憑證填充攻擊，下列何項舉措最無效果？

(A) 使用一次性密碼（One Time Password）

(B) 使用多因子驗證方式（Multi-factor authentication）

(C) 使用雙因子驗證方式（Two-factor authentication）

(D) 強化密碼複雜度（Password Complexity）

規劃 114-1 答案D

(憑證填充攻擊主要利用使用者在不同平台上重複使用帳號與密碼的漏洞，透過已洩漏的帳密資料進行大規模嘗試登入。採用一次性密碼、多因子驗證或雙因子驗證，可以增加額外的安全層級，減少因帳密洩露帶來的風險；但單純強化密碼複雜度對於防範憑證填充攻擊效果有限，因為攻擊者利用的是已洩漏的正確密碼，而非破解密碼的困難度。)

2. 關於弱點攻擊的敘述，下列何者正確？（複選）

(A) 軟體弱點或稱應用程式弱點，通常存在於軟體程式碼中，例如，錯誤的邏輯處理、未正確驗證輸入、設定配置錯誤造成危害等，都屬於這類的弱點

(B) 硬體弱點：這些弱點存在於硬體設備或韌體中，例如，沒有正確處理記憶體的設置，而導致裝置超載當機，甚至資料外洩

(C) 零日弱點：泛指廠商已經提供升級修補，卻沒進行升級更新的漏洞，攻擊者可以利用這些未被修補的弱點進行攻擊 (零日弱點指的是在廠商尚未發布修補前，攻擊者即能利用的漏洞，而非指已有補丁但未更新的漏洞)

(D) 網路弱點：這種弱點可能因為網路設計、配置或安全政策的問題，例如，開放不必要的網路通訊埠或服務，或者沒有使用安全加密的通訊協定

防護 114-1 答案ABD

3. 當企業遇到資安攻擊時，可以思考各種不同的方式來進行防禦，以便修補漏洞或暫時緩解。開發人員或資安維運人員必須選擇最合適的防禦機制來修補資安漏洞。下列何種防禦手法的「效果最差」，很容易被攻擊者用其他方式繞過？

(A) Filter Input and Escape Output，也就是過濾使用者輸入的特殊字元，並且在後端輸出內容時將特殊字元進行轉化，避免發生XSS攻擊

(B) 實作上傳功能時，檢查上傳檔案的內容與路徑，也限制上傳檔案的副檔名，並且將檔案搬移至上傳檔案專屬目錄，甚至是上傳到靜態檔案專屬的伺服器，同時也將該目錄設定為不可執行檔案，避免有網頁程式碼在該目錄被執行

(C) 撰寫資料庫查詢功能時，無論參數是不是使用者所輸入的，都必須針對參數內容進行過濾，移除所有非必要的特殊字元，並且對無法移除的特殊字元進行轉化。同時建議使用Prepared Statement來撰寫資料庫查詢功能會較為安全

(D) 在一個需要串接系統指令的網頁應用程式中，開發人員在網頁程式前端使用JavaScript來過濾特殊字元，防止攻擊者在參數中注入特殊字元來執行系統指令並達成Command Injection攻擊

防護 114-1 答案D

(使用前端 JavaScript 進行防禦是一種客戶端驗證，這種方式非常容易被繞過，因為攻擊者可以直接發送經過修改的請求，而不必通過前端介面。)

9. 勒索軟體與資料外洩攻擊之準備、預防、緩解與應變之實務上，可透過分析系統執行特定指令來進行威脅獵補（Threat hunting），以即早偵測並發現異常行為。下列何種Windows指令「非」勒索軟體常用於竄改系統檔案/備份之目的？

(A) fsutil.exe

(B) ntfsbackup.exe

(C) vssadmin.exe

(D) wbadmin.exe

防護 114-1 答案B

(勒索軟體常利用其他指令（如 fsutil.exe、vssadmin.exe 與 wbadmin.exe）來竄改或刪除系統檔案與備份，例如利用 vssadmin.exe 刪除影子備份、或用 wbadmin.exe 進行備份操作干擾；而 ntfsbackup.exe 並非勒索軟體常用來達成此類目的指令)

29. 在C#源碼檢測中，下列何種方法最有可能引起緩衝區溢位？

(A) 使用List<T> 類型的集合並頻繁添加元素 (由 .NET Framework 或 .NET Core/5+ 進行管理，不會直接導致緩衝區溢位，最多只會拋出例外（OutOfMemoryException 或 ArgumentOutOfRangeException）)

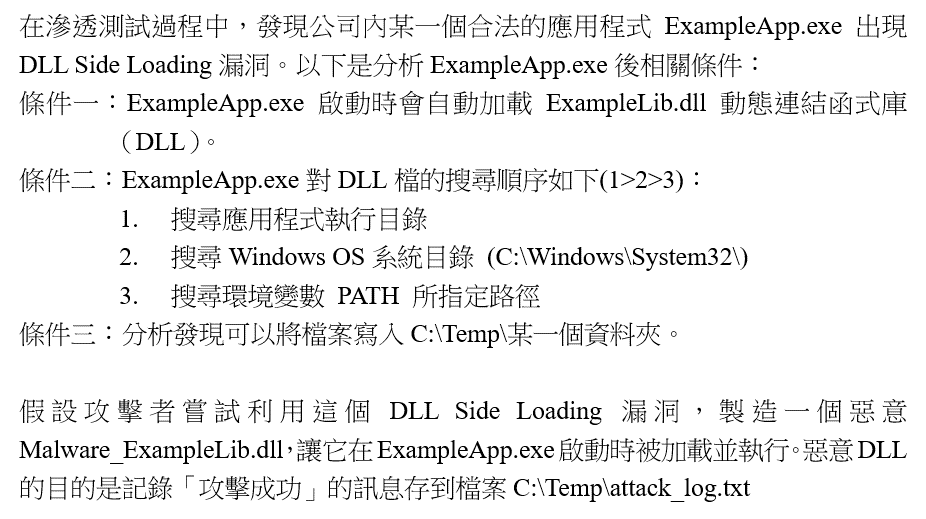
(B) 在遞迴函數中未設置適當的退出條件 (主要會引發 **堆疊溢位**（StackOverflowException）而非「緩衝區溢位」，概念上不太一樣。)

(C) 使用不安全的程式模組並直接操作指標 (在 C# 中最有可能引發類似 C/C++ 的緩衝區溢位風險。)

(D) 進行大量的非同步操作和多執行緒存取 (可能導致 Race Condition、Thread Safety 等問題，但不太會直接造成緩衝區溢位。)

防護 114-1 答案C

30. 如附圖所示，下面何項行為最有可能驗證ExampleApp.exe存在DLL Side Loading漏洞？



(A) 在 C:\Windows\System32\ 資料夾放置惡意ExampleLib.dll，觀察是否被載入

(B) 在 C:\Temp\ 資料夾放置惡意ExampleLib.dll，並修改環境變數PATH指向該路徑

(C) 在 C:\Program Files\ExampleApp\ 資料夾放置惡意ExampleLib.dll，並檢查是否覆蓋合法DLL

(D) 在 C:\Temp\ 資料夾放置惡意ExampleLib.dll，觀察是否被載入

防護 114-1 答案B

(根據題干提供的資訊，ExampleApp.exe 會依以下順序尋找要載入的 ExampleLib.dll：

應用程式所在資料夾

Windows 系統目錄 (C:\Windows\System32)

搜尋環境變數 PATH 指定的路徑

若我們在 C:\Temp 放置惡意的 ExampleLib.dll，並修改環境變數 PATH 使得 C:\Temp 先被搜尋，則 ExampleApp.exe 很可能會在找不到合法 DLL 之前，就載入我們放置的惡意 DLL。這正是「DLL Side Loading」漏洞常見的利用手法之一。)

1. 針對駭客攻擊手法，下列敘述何者錯誤？

(A) SQL注入式攻擊（SQL Injection）：攻擊者會嘗試將惡意 SQL代碼注入到一個網站的資料庫查詢中，從而獲得未授權的 存取 權限或提取 資料

(B) 跨站腳本攻擊（Cross-site Scripting XSS）：攻擊者會將惡意腳本注入到信任的網站中。當其他使用者存取該網站時，他們的瀏覽器會執行這些腳本，可能導致資料洩露

(C) 中間人攻擊（Man in the middle attack）：這種攻擊包括使用多台電腦（通常是受感染的，並被攻擊者控制的電腦）來發起大量的請求，導致竊取偷聽、重新導向通訊 (中間人攻擊的重點在於**攻擊者秘密地攔截、竊聽或篡改通訊雙方之間的通訊**，而雙方都以為自己是在直接與對方通訊。它並**不涉及使用多台電腦發起大量請求**。選項中描述使用多台電腦發起大量請求更像是**分散式阻斷服務攻擊 (DDoS)** 的特徵)

(D) 釣魚攻擊（Phishing）：攻擊者會偽裝成可信任的實體（例如銀行或社交媒體網站），嘗試欺騙使用者透露他們的登錄資訊、信用卡號或其他敏感資訊

防護 113-2 答案C

2. 針對APT攻擊（Advanced Persistent Threat），下列敘述何者

正確？

(A) APT常用技術手法，如：Privilege Escalation提權、Lateral Movement橫向移動

(B) 常見於一般腳本小子（Script Kiddie） (腳本小子通常指的是缺乏技術能力、使用現成工具發動攻擊的駭客新手。而 APT 攻擊則是由高度組織化、資源充足（通常是國家支持的）的團體所發動，其技術水準遠高於腳本小子)

(C) 非針對特定對象之入侵行為 (APT 攻擊最大的特點就是**針對特定對象**，例如特定國家、組織或企業，並非隨機攻擊。攻擊者會進行長時間的偵察和策劃，以達到特定目的，例如竊取機密資料、破壞關鍵基礎設施等)

(D) 利用零日漏洞、 客製化的惡意軟體，缺點是不具備匿名性與持久性 (APT 攻擊通常會利用**零日漏洞**（尚未被公開或修復的安全漏洞）和**客製化的惡意軟體**來躲避偵測。而且，APT 攻擊非常注重**匿名性**和**持久性**，攻擊者會盡力隱藏其蹤跡，並長時間潛伏在目標系統中，以實現其長期目標)

防護 113-2 答案A

4. 在殭屍網路（Botnet）的架構中，攻擊者通常會將惡意軟體散佈到多台受害者電腦上，將這些受感染的電腦轉變為「殭屍電腦」。當攻擊者累積足夠數量的殭屍電腦後，通常會透過一台「中介主機」來下達指令，進而發動對特定目標的網路攻擊。請問下列何項是這種中介主機的專有名稱？

(A) SQL伺服器

(B) C&C（Command and Control）伺服器

(C) DNS（Domain Name System）伺服器

(D) FTP（File Transfer Portocal）伺服器

技術 113-2 答案B

(駭客需要在伺服器和遭入侵的網路或機器之間建立隱蔽的頻道或後門。網路罪犯伺服器，無論是單一電腦或電腦殭屍網路，都被稱為命令與控制伺服器 （C&C） 伺服器或 C2 伺服器)

7. 在釣魚攻擊中，攻擊者通常會使用下列何種方式來欺騙受害者？

(A) 直接入侵受害者的電腦

(B) 假冒合法機構發送電子郵件

(C) 利用病毒感染受害者的系統

(D) 竊取網路流量

技術 113-2 答案B

(釣魚攻擊常透過電子郵件入侵)

8. 下列哪一種攻擊手法是利用「不」安全的無線網路來竊取資料？

(A) 拒絕服務攻擊（Denial of Service, DoS）

(B) 中間人攻擊（Man-in-the-Middle attack, MITM）

(C) 跨站腳本攻擊（Cross-Site Scripting, XSS）

(D) SQL注入攻擊（SQL Injection）

技術 113-2 答案B

(無線網路中的中間人攻擊，可以架設不合法的AP竊取訊號，如Evil Twins或Rouge AP)

10. 機關對外服務網站無法正常提供服務，經分析DNS遭受混合式 DDoS攻擊下列建議之 DDoS防護措施何者最「不」合適？

(A) 可透過採購網路流量清洗服務，來緩解 DDoS攻擊

(B) 可透過限制 DNS查詢次數，來緩解 DDoS攻擊 (選項 B 的描述雖然在技術上是正確的，但是在特定情境下，特別是面對「混合式 DDoS 攻擊」時，單純依賴限制 DNS 查詢次數可能效果有限，甚至可能影響正常服務)

(C) 如果網路頻寬無須考量，可使用過濾機制來緩解DDoS攻擊 (這個選項的主要問題在於「如果網路頻寬無須考量」這個前提在現實中幾乎不可能存在。DDoS 攻擊的本質就是利用大量流量癱瘓目標系統，耗盡其頻寬資源。即使有強大的過濾機制，如果沒有足夠的頻寬來承載攻擊流量，過濾機制本身也會成為瓶頸，甚至自身先被擊垮。過濾機制是必要的，但**頻寬才是基礎**。就好比你的過濾器再好，如果水管很細或者被塞住，水也流不出來)

(D) 可透過避免成為Open Resolver來緩解DDoS攻擊

防護 113-2 答案 C、B

11. 如附圖所示，駭客透過某機關網頁上傳功能漏洞植入 APT惡意程

式，並嘗試取得系統資料，恐有資料外洩之虞。下列建議之防範措

施何者最「不」合適？



(A) 機關建立資通安全威脅偵測管理機制

(B) 為落實軟體及資訊完整性防護，上傳檔案不限格式且一律透

過防毒軟體告警

(C) 對於目錄進行完整性監控及驗證，即時偵測目錄異動行為

(D) 辦理服務安全性檢測作業時，可評估採多家廠商交互驗證為

宜

防護 113-2 答案B  
(**不限格式**：這會大幅增加安全風險，允許上傳任意格式的檔案，意味著攻擊者可以上傳各種惡意程式或腳本，例如 webshell、後門程式等，進而控制伺服器。

**一律透過防毒軟體告警**：雖然防毒軟體是重要的安全防禦措施，但並非萬無一失，特別是針對進階的、客製化的 APT 惡意程式，防毒軟體可能無法偵測到。而且，只依賴告警而沒有阻擋機制，無法有效阻止攻擊。

應該做的是:**限制可上傳的檔案類型**（例如只允許圖片、PDF 等常見且風險較低的檔案類型），並對上傳的檔案進行**嚴格的檢查和驗證**（例如檢查檔案簽章、限制檔案大小、沙箱檢測等），並搭配 **防毒軟體掃描** 作為額外的安全防禦，而**不是不設防**。)

16. 某網站存在跨站請求偽造（Cross Site Request Forgery, CSRF）漏洞，攻擊者可能會利用該漏洞發起攻擊。下列何種方法最常用來防止CSRF攻擊？

(A) 在URL中加入Session ID

(B) 將所有表單設為唯讀權限（Read only）

(C) 在使用者的請求中加入Token

(D) 將所有網頁設置為不可被搜索引擎索引

技術 113-2 答案C

(這是**最常用且有效的 CSRF 防禦方法**。通常稱為 **Anti-CSRF Token** 或 **Synchronizer Token Pattern**。伺服器會產生一個隨機的 Token，並將其嵌入到表單中 (通常是隱藏欄位)。當使用者提交表單時，Token 會一起送回伺服器。伺服器會驗證收到的 Token 是否與原本產生的 Token 相符。如果相符，則請求被視為合法；如果不符，則請求被拒絕。由於攻擊者無法事先取得或偽造這個 Token，因此可以有效防止 CSRF 攻擊。)

22. 下列哪一種攻擊手法會利用應用程式的權限設定不當，讓攻擊者取得對應用程式或作業系統的未授權存取，並可能進一步提權成為系統管理員？

(A) 點擊劫持攻擊（Clickjacking）

(B) 旁通道攻擊（Side-channel Attack）

(C) 特權提升攻擊（Privilege Escalation）

(D) 特洛伊木馬攻擊（Trojan Horse）

技術 113-2 答案C

(因為駭客剛登入系統時，取得的權限可能不夠，因此為了做更多事情，提權是必要的)

32. 對惡意程式的管理方式，下列何項正確？

(A) 系統已安裝防範惡意程式偵測的軟體，不需要定期再執行掃描

(B) 定期蒐集到對系統軟體的威脅情資，無法做為防範惡意程式的來源依據

(C) 已於系統中安裝偵測惡意程式的防毒軟體，經由網路取得的資訊，使用前不需要額外進行掃描

(D) 定期實施社交工程測試，也是針對防範惡意軟體認知的提升

技術 113-2 答案D

(A、B、C選項最後一句都語意顛倒)

32. 在進行網站檢查時，發現其未設定 HTTP Strict Transport Security （HSTS）標頭，請問下列敘述那些較為適切 ？（複選）

(A) 可能遭受中間人攻擊（Man-in-the-Middle MITM） (HSTS 可以強制瀏覽器使用 HTTPS 連線到網站，即使使用者在網址列中輸入 HTTP，或點擊了 HTTP 的連結。如果沒有設定 HSTS，攻擊者可以透過中間人攻擊，將 HTTPS 連線降級為 HTTP，進而竊聽或竄改通訊內容)

(B) 可能遭受 SSLStrip攻擊 (SSLStrip 是一種常見的中間人攻擊手法，可以將 HTTPS 連線降級為 HTTP。如果網站沒有設定 HSTS，攻擊者可以利用 SSLStrip 攻擊，攔截使用者的連線，並將使用者導向至偽造的 HTTP 網站，進而竊取使用者的帳號密碼或其他敏感資訊)

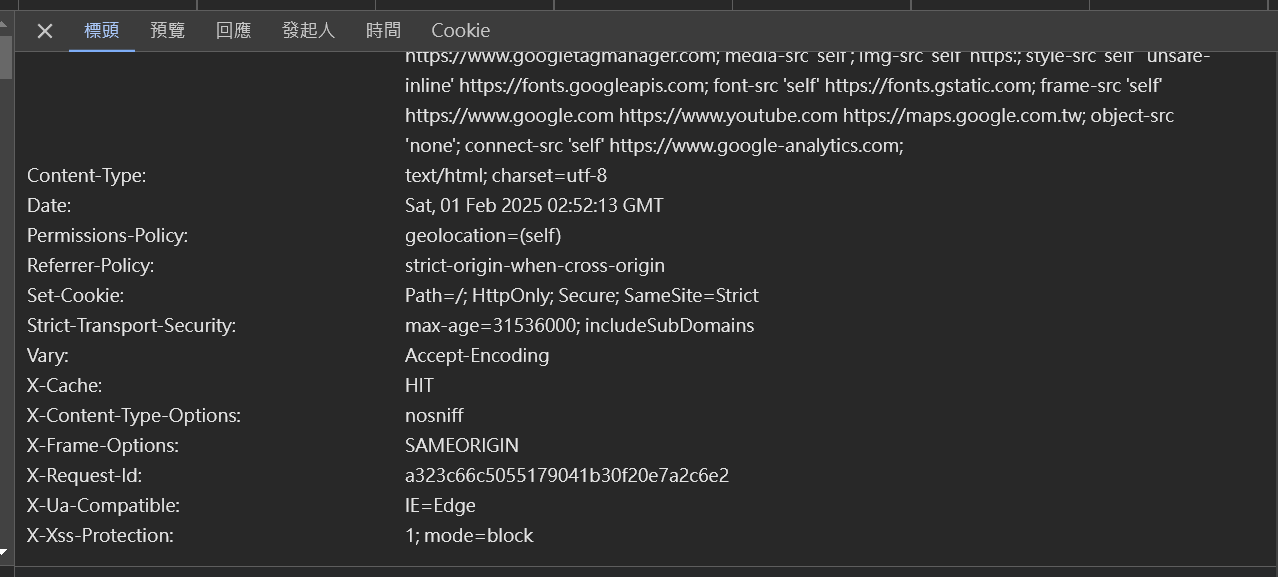
(C) 可於網站伺服器中停用 Port 80 的服務來修補這問題 (停用 Port 80 (HTTP) 可以強制使用者使用 HTTPS 連線，這在一定程度上可以降低風險，但並不能完全取代 HSTS 的作用。例如，如果使用者曾經透過 HTTP 訪問過網站，瀏覽器可能會記住這個設定，即使網站停用了 Port 80，瀏覽器也可能嘗試使用 HTTP 連線。此外，停用 Port 80 可能會導致某些依賴 HTTP 的服務無法正常運作)

(D) 可於網站伺服器中停用 Port 443 的服務來修補這問題 (Port 443 是 HTTPS 服務的預設埠口，停用 Port 443 會導致網站無法透過 HTTPS 訪問，這會嚴重影響網站的可用性和安全性)

防護 113-2 答案A、B

(**建議的修補措施：**

1. **設定 HSTS 標頭：** 在網站伺服器的設定檔中加入 HSTS 標頭，並設定 max-age 參數，指定瀏覽器在一定時間內強制使用 HTTPS 連線到該網站。例如：Strict-Transport-Security: max-age=31536000; includeSubDomains; preload



1. **將 HTTP 重新導向到 HTTPS：** 在網站伺服器的設定檔中設定 HTTP 到 HTTPS 的重新導向，確保所有使用者都透過 HTTPS 連線到網站。
2. **確保網站所有資源都透過 HTTPS 載入：** 避免混合內容 (Mixed Content) 的問題，確保網頁中的所有圖片、腳本、樣式表等資源都透過 HTTPS 載入。)

33. 為了防止企業遭受勒索軟體攻擊而發生損害，下列敘述何者較「不」適當？

(A) 啟用端點防護軟體（Endpoint Protection），並定期更新病毒定義庫，可阻擋已知的威脅

(B) 將所有的備份資料移至雲端，以避免勒索軟體威脅

(C) 對所有員工進行資安意識訓練，讓其識別釣魚郵件及可疑的附件，並啟用多重要素驗證（Multi-factor authentication, MFA），可降低被滲透機會

(D) 設定網路分區隔離（Network Segmentation），限制不同網段間的通信，可減少破壞範圍

技術 113-2 答案B

(把所有備份資料移至雲端，如果安全控管沒有做好，也是會受到勒索軟體威脅)

50. 駭客常使用下列何種技術破解物聯網中Wi-Fi AP的WPA2密碼？

(A) SQL注入攻擊

(B) 分散式拒絕服務（DDoS）攻擊

(C) 字典攻擊（Dictionary Attack）

(D) 跨站腳本攻擊（Cross-Site Scripting, XSS）

技術 113-2 答案C

(字典攻擊是一種密碼破解技術。攻擊者會使用一個預先定義好的單詞列表 (字典檔)，逐一嘗試這些單詞作為密碼，直到找到正確的密碼。這種方法對於破解較弱的 WPA2 密碼 (例如使用常見單詞或片語的密碼) 特別有效。駭客可以結合暴力破解法針對特定的 Wi-Fi AP 進行離線破解。)

1. 有關阻斷服務攻擊（DoS攻擊）之敘述，下列何者正確？

(A) 攻擊者偽造傳輸層封包來破壞網路的攻擊行為

(B) 攻擊者使用惡意軟體在設備上執行未經授權的攻擊行為

(C) 攻擊者向目標伺服器發送大量請求，使其無法處理其他請求的攻擊行為

(D) 攻擊者使用偽造的電子郵件來詐騙用戶的攻擊行為

技術 113-1 答案C

3. 隨著無線網路盛行，在伺服器與客戶端之間放置雙方都無法察覺的軟體進行攔截、備份、竄改資料等動作會再傳送給接收方的是下列何種攻擊手法？

(A) 重放攻擊

(B) 中間人攻擊

(C) 網路釣魚

(D) 社交工程

技術 113-1 答案B

(雙方無法察覺是典型中間人攻擊手法)

3. 關於在資訊安全中，威脅或攻擊具多種因素與手法的敘述，下列哪些正確？（複選）

(A) 基於地緣政治動機的威脅分類： 如政治意識形態；社會報復等台灣近期有發生製造業遭勒索加密案例 ，就屬於這類型態 (也有經濟動機)

(B) 內部威脅（Insider threats）：這種威脅來自組織內部的人員，可能無意或故意地洩漏敏感資訊，或損害系統及公司利益

(C) 零日攻擊（Zero-day attacks）：這類攻擊利用尚未正式公開漏洞，在廠商還沒修補漏洞前，就被利用發動攻擊

(D) 惡意軟體（Malware）：這包括了病毒、蠕蟲、特洛伊木馬、勒索軟體等，他們可以破壞系統，竊取數據，或無授權地使用系統資源

防護 113-1 BCD或ABCD

7. 請問 DNS放大攻擊（DNS Amplification Attacks），最屬於下

列何種網路攻擊？

(A) 病毒

(B) 木馬

(C) 蠕蟲

(D) 阻斷服務攻擊

技術 113-1 答案D

(DNS放大攻擊是一種利用域名系統（DNS）漏洞發動的 分布式拒絕服務攻擊（DDoS），其核心是通過「偽造請求」和「流量放大」來癱瘓目標服務器或網絡。)

11. 勒索軟體與資料外洩攻擊之準備、預防、緩解與應變之實務上，可透過調校與強化主機系統其網路服務設定來降低所曝露之弱點。下列何種系統強化措施最「不」合適？

(A) 於面向網際網路之主機執行弱點掃描以識別系統弱點並修復

(B) 於主機系統停用並關閉未使用RDP遠端桌面協定TCP/3389連接埠

(C) 於主機系統啟用 SMBv1, SVBv2伺服器訊息區協定以達傳輸加密 (這是不合適的措施。SMBv1 和 SMBv2 是過時且存在已知漏洞的協定，容易被攻擊者利用，例如 WannaCry 勒索軟體就是利用 SMBv1 的漏洞進行傳播。應該停用 SMBv1 和 SMBv2，並使用更安全的 SMBv3 協定，SMBv3 支援加密傳輸)

(D) 於防火牆設定阻擋TCP/445連接埠對網際網路之內外連線規則

防護 113-1 答案C

15. 關於Rootkit和Bootkit的敘述，下列何項最「不」適切？

(A) Rootkit是一種惡意軟體，用於隱藏攻擊者對操作系統的控制權

(B) Rootkit的偵測防禦容易，因為它易被防毒軟體發現

(C) Bootkit是一種惡意軟體，與 Rootkit類似，但是它是安裝在操作系統的引導（boot）區塊，以實現在操作系統啟動之前攻擊的目的

(D) 與 Rootkit一樣 Bootkit可以隱藏攻擊者的存在和攻擊行為，例如隱藏進程、檔案、目錄、登錄項目、網路連接等等，從而繼續控制和攻擊受害者系統

技術 113-1 答案B

(Rootkit的特性就是高度隱藏，因此很難被防毒軟體偵測)

19. 關於SQL Injection攻擊及其防範的敘述，下列何者錯誤？

(A) SQL Injection攻擊主要是利用應用程式撰寫上的疏忽，使得執行非預期的SQL指令，非法存取資料庫中的內容

(B) SQL Injection攻擊所採用之攻擊方法，是一種利用未做好輸入查驗（ Input Validation）所衍生的問題

(C) 發生SQL Injection攻擊最大的原因，在於未對輸入文字進行過濾，未作完善的輸入條件檢查

(D) 關於SQL Injection攻擊之預防拒絕輸入單引號、雙引號、分號等特殊字元即可

技術 113-1 答案D

(黑名單無法列舉所有的攻擊，應該要使用白名單才對)

21. 下列何種攻擊手法是透過瀏覽器執行攻擊者插入到網頁中的Script指令，來竊取使用者輸入的資料？

(A) 緩衝區溢位攻擊（Buffer Overflow）

(B) 釣魚攻擊（Phishing）

(C) 阻斷服務攻擊（DoS）

(D) XSS攻擊（Cross-Site Scripting）

技術 113-1 答案D

31. 下列何種惡意程式可以自己存在不需要寄生在其他的程式與檔案中，而且可以自己複製、自行在網路上傳播？

(A) 蠕蟲

(B) 木馬

(C) 邏輯炸彈

(D) 病毒

技術 113-1 答案A

3. 下列何項「不」屬於網路安全的威脅？

(A) Network Attack (網路攻擊)

(B) USB Attack

(C) IP Spoofing (IP欺騙)

(D) Network Eavesdropping (網路竊聽)

技術 112-2 答案B

6. 當突然發現區域網路中，有大量的電腦連線並傳輸不明的資料時，請問最有可能是下列何種網路攻擊？

(A) 病毒

(B) 中間人攻擊

(C) 蠕蟲

(D) 鍵盤側錄

技術 112-2 答案C

(區域網路中有大量的電腦連線並傳輸不明的資料時，符合蠕蟲的攻擊特徵)

7. 請問DNS放大攻擊，最屬於下列何種網路攻擊？

(A) 病毒

(B) 木馬

(C) 蠕蟲

(D) 阻斷服務攻擊

技術 112-2 答案D

(DNS放大攻擊是一種阻斷服務攻擊)

12. 在Cyber Kill Chain 模型中，Delivery 階段通常包括下列何項

攻擊手法？

(A) 惡意軟體安裝 (Installation (安裝)) (屬於 Installation 階段，發生在 Delivery 之後。)

(B) 網站水坑攻擊 (Weaponization (武器化)) (雖然受害者最終會接觸到惡意內容，但這發生在 **Weaponization** 階段。攻擊者預先設置好陷阱（被感染的網站），**並非主動傳送**，而是「被動」等待目標落入陷阱。這與 Delivery 階段的「主動傳送」有本質上的區別。)

(C) 電子郵件附件或內文URL 連結 (Delivery (投送)) (完全符合 Delivery 階段的定義，是攻擊者「主動」將惡意內容（透過附件或連結）傳送給目標。)

(D) 帳號密碼填充攻擊 (Exploitation (漏洞利用)) (屬於 Exploitation 階段，利用已洩露的憑證嘗試登入，與 Delivery 無關。)

防護 112-2 答案C

20. 關於注入攻擊（Injection Attack）的敘述，下列何者錯誤？

(A) 為防止 SQL注入攻擊，可以採用使用參數化查詢

（Parameterized Query）或預處理語句（Prepared Statement）

以將用戶輸入與 SQL代碼進行隔離

(B) 攻擊者在客戶端和伺服器之間建立兩個獨立的加密通道，讓客戶端和伺服器誤以為他們在進行安全通信，但實際上攻擊者可以監控和篡改通信內容

(C) 此語法也是一種注入攻擊 (註釋符號 -- 的作用：

在 SQL 中，-- 是單行註釋符號，其後的內容會被視為註釋而忽略，典型注入攻擊特徵)

(D) 此語法也是一種注入攻擊 (直接將用戶輸入（request.getParameter("id")）拼接到 SQL 語句中，未進行任何過濾或參數化處理，容易遭受注入攻擊)

技術 112-2 答案B

(B選項是Man in the Middle攻擊說明)

21. 關於 Web攻擊手法的敘述，下列何者錯誤？

(A) SQL注入攻擊：輸入特定的數據，將 SQL指令插入到應用程式的資料庫中，獲取敏感資訊或執行未授權的操作，甚至破壞資料

(B) 跨網站腳本攻擊（XSS）：通過在網頁中注入惡意腳本，攻擊者僅 可置換網頁內容，但無法對伺服器電腦造成任何影響

(C) 跨站請求偽造攻擊（CSRF）：利用受害者已經驗證過的會話，攻擊者可以在受害者不知情的情況下，執行某些操作，例如更改密碼

(D) 文件上傳漏洞：攻擊者可以通過在網站上上傳惡意檔案，例如病毒、木馬、後門等，從而取得對受害者系統的控制權

技術 112-2 答案B

( XSS 攻擊能夠不只能置換網頁內容，可以竊取用戶 cookie，可以執行任意 JavaScript 代碼，可能導致用戶端遭受攻擊，在某些情況下可能影響到伺服器)

21. 就勒索軟體事件而言，最有可能降低事件衝擊的控制措施為下列何項？

(A) 原始碼檢測

(B) 日誌分析

(C) 社交工程演練

(D) 離線資料備份

防護 112-2 答案D

(離線資料備份被降低垃圾軟體事件衝擊的方式)

22. 當你收到一封電子郵件，告知你因為帳號有異常登入的情況，需要你從信件中的連結去重新設定密碼。請問最有可能是下列何項的情況？

(A) 這是網管善意的提醒，依照指示進行操作

(B) 這是一種釣魚攻擊（Phishing）

(C) 這是一種阻斷服務攻擊（DoS）

(D) 這是一種文件上傳漏洞

技術 112-2 答案B

(情境描述就是一個社交工程網路釣魚的情形)

23. 下列何種攻擊手法是運用輸入超過預設資料長度的方式，影響記憶體中資料的正確性？

(A) 緩衝區溢位攻擊（Buffer Overflow）

(B) 釣魚攻擊（Phishing）

(C) 阻斷服務攻擊（DoS）

(D) XSS攻擊（Cross-Site Scripting）

技術 112-2 答案A

(情境描述就是一個緩衝區溢位攻擊情境)

24. 如附圖所示，攻擊者可竄改查詢參數並存取所有帳號資訊，關於此應用程式缺陷的敘述，下列何者錯誤？



(A) 此為結構化查詢語言注入（Structured Query Language Injection）

(B) 使用安全 API來查詢以降低解譯器錯誤之風險

(C) 跳脫（Escape）系統保留字元避免查詢語法遭竄改

(D) 參數檢查機制必須實做於用戶端且使用黑名單過濾

技術 112-2 答案D

(‘or’1’=1判斷此題是考SQL injection攻擊，參數檢查應該在伺服器端實作，而不是僅在客戶端，應該使用白名單而不是黑名單過濾，因為黑名單可能會遺漏某些攻擊模式)

29. 關於電子郵件安全威脅的敘述，下列何者錯誤？

(A) 電子郵件可能會遇到的資安問題，例如：冒名郵件、垃圾郵件、詐騙郵件、黑函郵件、病毒（木馬）郵件、釣魚郵件等

(B) 一般詐騙郵件的手法，都會要求收信者點選一個連結網址，並將收信者引導到一個仿冒的假網站，然後再要求他提供、更新或確認機密的個人資料

(C) 詐騙郵件通常企圖獲取個人的重要資訊

(D) 電子郵件的安全以詐騙為主，未曾發現針對技術性弱點的攻擊

技術 112-2 答案D

(CVE-2024-21410就是針對Exchange Server 的技術性攻擊)

30. 關於惡意程式的敘述，下列何者錯誤？

(A) 蠕蟲（worm）是一種獨立的惡意程式，它透過網路主動傳播自身以感染其他系統計算機，可在不感染文件、檔案的情況下複製自己

(B) 特洛伊木馬（Trojan horse）是一種有害程式，它會偽裝成普通的良性程式或實用程式，以使受害者安裝它

(C) Rootkit透過修改作業系統程式取得Root權限的惡意程式

(D) 電腦病毒是通常隱藏在另一個看似無害的程序中的軟體，它可以生成自身的副本並將其插入到其他程序或文件中，並且通常會執行有害的作業

技術 112-2 答案C

(Rootkit 的主要目的是 **隱藏** 自身以及其他惡意程式的存在，例如透過修改工作管理員讓你無法察覺某一隻Process)

2. 試問運用網頁文字輸入欄位中，以輸入「 ' or 1=1」訊息內容的方式，讓該網頁顯示出所有的資料內容，這種攻擊型態屬於下列那種攻擊手法？

(A) XSS

(B) SQL Injection

(C) CSRF

(D) DDoS

防護 112-1 答案B

3. 駭客為了追求最大利益，將亂槍打鳥的隨機攻擊轉換成目標式攻擊， 進階持續性威脅（Advanced Persistent Threats, APT）即是最難防禦的目標式攻擊。關於APT攻擊的敘述，下列何者錯誤？

(A) 具有隱匿性高且長期潛伏於目標系統的特性

(B) APT攻擊的模式通常都是透過老舊的網路設備進行攻擊 (雖然老舊的網路設備可能存在未修補的漏洞，更容易受到攻擊，但 APT 攻擊並不局限於此)

(C) 潛伏期可以只是幾天，也可能長達一年半載

(D) 遭受攻擊後，被害者多數只能盡快修補漏洞並設定災害停損點，無法有效根除攻擊

防護 112-1 答案B

4. 下列何種攻擊，無法透過主機實體（Physical）或邏輯（Logical）安全機制直接防禦？

(A) 暴力攻擊（Brute-Force Attack）

(B) 阻斷服務攻擊（Denial-of-Service Attack）

(C) 社交工程（Social Engineering）

(D) 通訊埠掃描（Port Scan）

技術 112-1 答案C

(社交工程透過人性的弱點，是一種非技術性的攻擊)

5. 下列何者「不」是阻斷式服務攻擊（Denial-of-Service Attack）？

(A) 持續發送惡意封包，導致主機當機

(B) 消耗系統全部的CPU運算能力

(C) 寄送有惡意連結的郵件給公司所有人員

(D) 向特定收件者發送成千上萬封電子郵件

技術 112-1 答案C

(寄送有惡意連結的郵件給公司所有人員應該是社交工程)

10. 社交工程是利用人性弱點誘騙受害者透漏機敏性資料或是允許授權等行為，下列敘述何者錯誤？

(A) 網路釣魚是最常見的社交工程的攻擊手法

(B) 社交工程演練的目的是要培養員工反擊的能力，進而破壞駭客的攻擊手法 (員工的警覺心)

(C) 駭客會利用偽造網站網址誘騙使用者上當也是屬於社交工程的攻擊手法之一

(D) 企業組織會透過教育訓練宣導資安觀念，並委託廠商設計測試的釣魚郵件進行檢視員工點擊郵件與連結的行為是否違法資安規定

防護 112-1 答案B

20. 請問一般所謂的 Google Hacking 是指下列何項？

(A) 遭Google公司入侵

(B) Google公司被入侵

(C) 指透過大型搜尋引擎，收集欲入侵（滲透）標的之資訊

(D) 指透過Google，對欲入侵（滲透）之公司直接發動攻擊

技術 112-1 答案C

(使用搜尋語法 intitle:"index of" "parent directory" 來尋找公開的伺服器目錄列表，這些目錄可能意外暴露敏感檔案（如資料庫備份、密碼文件等）。例如，攻擊者可透過此方法發現未受保護的檔案，進而取得目標系統的資訊或漏洞。

其他常見語法：

filetype:sql "password"：搜尋包含「password」字樣的 SQL 資料庫檔案。

inurl:/admin/login.php：尋找網站的管理員登入頁面。

site:example.com intitle:"login"：鎖定特定網站（如 example.com）的登入頁面。)

21. 關於憑證填充攻擊（Credential Stuffing）的敘述，下列何者錯誤？

(A) 通常使用殭屍網路（Botnet）進行攻擊

(B) 會以自動化方式試圖登入網路服務

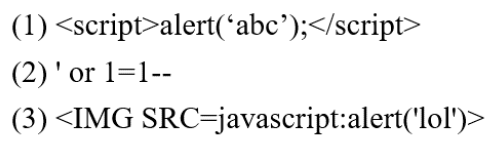
(C) 可使用雙因子認證（two-factor authentication）

(D) 會直接造成網路服務中斷，影響可用性

技術 112-1 答案D

(C選項可使用「可使用雙因子認證（two-factor authentication）」只有這樣寫會讓人誤會是否是攻擊，比較好的寫法是「可使用雙因子認證（two-factor authentication）防禦」，D選項憑證填充攻擊重點是登入系統，與可用性無關)

22. 如附圖所示，下列何項組合是 XSS（Cross-Site Scripting）攻擊語法？



(A) (1)(2)

(B) (1)(3)

(C) (2)(3)

(D) (1)(2)(3)

技術 112-1 答案B

(B選項是SQL INJECTION，其他都是XSS常見攻擊特徵語法)

30. 網際網路已成為日常生活不可或缺的一部分，但部分使用者對安全防護不足容易受到惡意程式的危害。下列哪一項「不」是惡意程式？

(A) 木馬程式

(B) 勒索軟體

(C) 中間人攻擊

(D) 蠕蟲

技術 112-1 答案C

(中間人攻擊非傳統意義上的惡意程式，而是一種攻擊手法)

32. 關於病毒（Virus）與蠕蟲（Worm）之比較，下列何者較正確？

(A) 蠕蟲通常不具破壞性，病毒則通常為惡意 (蠕蟲和病毒都可能具有破壞性)

(B) 蠕蟲的檔案，通常比病毒小，不易被偵測 (檔案大小並非區分兩者的特徵)

(C) 蠕蟲會自行擴散，病毒常透過事觸發 (蠕蟲能夠自主尋找目標並傳播，不需人為干預，病毒需要依附在其他程式上，需要特定事件（如執行受感染的檔案）才會啟動)

(D) 蠕蟲無法自行存在，但病毒可以 (完全相反，蠕蟲是獨立的程式，可以自行存在和運作，病毒需要寄生在其他檔案或程式中才能存活)

技術 112-1 答案C

4. 請問下列哪一種攻擊手法，最主要目的是讓合法授權的使用者無法使用系統或網路資源？

(A) 社交工程（Social Engineering）

(B) 蠕蟲（Worm）

(C) 暴力破解（Brute-Force Attack）

(D) 拒絕服務（Denial-of-services）

管理 111-2 答案D

(拒絕服務透過大量伺服器頻寬連線導致服務資源耗盡以破壞可用性)

45. 關於企業組織遭遇DoS或DDoS攻擊的常見特徵，下列何者錯誤？

(A) 網路頻寬滿載

(B) 網通設備或防火牆不堪負載

(C) 電腦與伺服器作業系統或服務超載

(D) 網站內容只有影片無法播放

管理 111-2 答案D

(DDOS的情況下，網站應該完全不能存取，不會只有影片無法播放)

3. 下列何者攻擊是透過 UDP（User Datagram Protocol）協定送出假造來源的廣播封包至目標網路，以便產生擴大資料流量效果的阻絶服務攻擊？

(A) Smurf (ICMP) (攻擊者偽造受害者主機的 IP，並向網路的**廣播位址**發送大量 ICMP echo request（ping 請求）。 網路上所有主機都會向被偽造的受害者 IP 發送 ICMP echo reply（回應），造成受害者主機接收大量回應訊息而癱瘓。)

(B) Fraggle (UDP) (攻擊者以 UDP 協定為基礎（通常為UDP port 7或19），偽造受害者主機的 IP，對網路上的**廣播位址**發送大量的 UDP 請求封包。 當主機回應大量的 UDP 訊息給偽造的 IP 位址（即受害者），導致受害者主機被大量的封包淹沒。)

(C) Land (TCP) (攻擊者將封包來源位址與目的位址設定為**受害者自身的 IP 位址**，並且 TCP 封包的來源埠與目的埠也是相同的。 這導致受害者主機無法處理這種異常封包，可能會使主機崩潰或失去反應。)

(D) Teardrop (IP fragmentation) (攻擊者透過 IP 分片（fragmentation）封包，故意傳送\*\*重疊且有矛盾片段(offsets不一致)\*\*的資料片段，迫使受害者主機在組合封包時發生錯誤，導致系統無法處理這種情況而當機或重啟。)

技術 111-2 答案 B



7. 網路上有許多駭客組織，都會介紹不同的攻擊方式，每種方式都會有不同的攻擊效果。關於攻擊的敘述，下列何項錯誤？

(A) 阻斷服務攻擊：利用網路通訊協定的弱點，傳送大量的封包使系統負荷過重、發生錯誤或是系統當機無法服務

(B) 網路監看：利用人際關係上溝通疏誤，取得特殊的存取帳號密碼或是重要資訊 (社交工程)

(C) 系統漏洞：利用系統程式設計、維護時，所留下的錯誤或漏洞進行入侵

(D) 緩衝區溢位：利用寫入資料超過原本分配緩衝區的大小，造成執行錯誤指令

技術 111-2 答案 B

13. 某甲欲使用檔案傳輸軟體將一敏感檔案傳給某乙，某甲除了將敏感檔案加密之外，在傳輸過程中，某甲可以使用下列何種安全協定， 而 此安全協定的使用亦可防止哪一種攻擊？

(A) 使用 SSH協定、防止 DNS攻擊

(B) 使用 SSH協定、防止中間人攻擊

(C) 使用 HTTPS協定、防止 DNS攻擊

(D) 使用 HTTPS協定、防止 DDoS攻擊

技術 111-2 答案 B

(SSH協定可以防止中間人攻擊)

1. 主機密鑰驗證：
   * 首次連線時會記錄伺服器的主機指紋（host key），之後只要指紋被竄改或不符，SSH 就會警告或中止連線。
   * 攻擊者若要偽裝伺服器，必須掌握真正的主機私鑰，否則無法通過驗證。
2. 安全的密鑰交換與加密：

* SSH 使用像 Diffie-Hellman 等安全協定交換一次性會話密鑰，通訊內容以對稱加密保護，同時透過完整性校驗防篡改。
* 具有「前向安全性」：即使日後伺服器私鑰外洩，也無法解密先前記錄的通訊。

1. 用戶端警示與操作：

* SSH 會在偵測到新或不匹配的主機密鑰時發出明確警告，避免用戶盲目接受偽裝的伺服器。
* 只要使用者謹慎對待這些警示，中間人就難以悄悄插入連線。

整體而言，SSH 透過「主機指紋校驗＋安全加密交換＋用戶端嚴格警示」，使攻擊者即便攔截流量，也無法輕易假冒或篡改資料而不被發現。)

19. 系統管理人員於網站日誌中看見大量訊息含有類似字串「 ..%2F..%2F..%2F..%2Fetc%2Fpasswd」，請問可能為以下何種攻擊？

(A) SQL Injection (' OR 1=1 --)

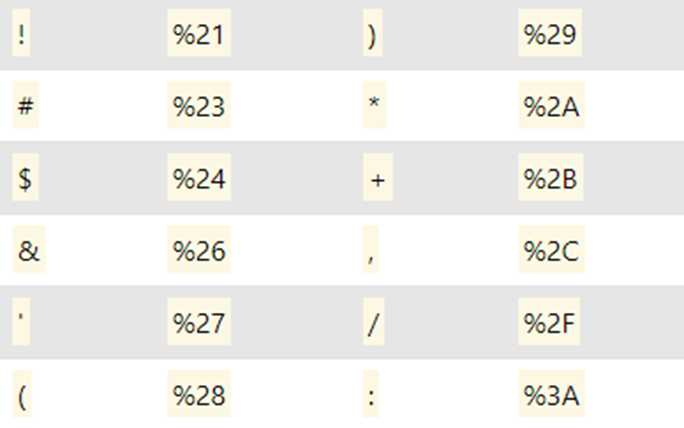
(B) Directory Traversal (../../../../etc/passwd)

(C) Cross-Site Scripting (<script>alert(1)</script>)

(D) Cmd Injection (http://127.0.0.1/delete.php?filename=bob.txt;ls)

技術 111-2 答案 B

(%2F 代表「/」的 URL encode；連續的 ..%2F 表示「往上一層目錄」；最後指向 /etc/passwd，解碼後實際上是 "../../../etc/passwd")



24. 如附圖所示，攻擊者透過修改查詢參數「account」為任意帳號即可存取資訊，關於此應用程式缺陷的敘述，下列何者正確？



(A) 存取控制失效（Broken Access Control）(OWASP Top 10 2021:A01)

(B) 密碼機制失效（Cryptographic Failures）(OWASP Top 10 2021:A02)

(C) 注入攻擊（Injection）(OWASP Top 10 2021:A03)

(D) 安全日誌與監控失效（Security Logging and Monitoring Failures）(OWASP Top 10 2021:A09)

技術 111-2 答案 A

(https://vulnerable.site/app/profile?account=victim，攻擊者嘗試更換帳號參數未經授權登入系統)

25. 下列何者「不」是因為開發過程中，未留意程式安全造成的問題？

(A) 魚叉式網路釣魚（Spear Phishing）

(B) SQL資料隱碼攻擊（SQL Injection）

(C) 跨站指令碼攻擊（Cross-Site Scripting, XSS）

(D) 跨站請求偽造（Cross-Site Request Forgery, CSRF）

技術 111-2 答案A

(魚叉式網路釣魚屬於社交工程攻擊，跟技術無關)

28. 針對網站常見的跨站指令碼攻擊（Cross-site scripting, XSS），請問攻擊成功的常見原因是資通系統未過濾或防範以下何種程式語言的注入攻擊？

(A) Python

(B) ASP.NET

(C) ShellScript

(D) JavaScript

技術 111-2 答案D

(XSS的攻擊特徵碼為<script>alert(1)</script>，是一種JavaScript語法)

30. 利用社交工程的概念，將惡意程式或是惡意連結等隱藏在電郵件中，看似好友所寄的，誘騙使用者打開郵件。下列何項「不」是有效防止惡意郵件社交工程的方案？

(A) 定期舉辦資訊安全教育訓練，建立對惡意程式的認知

(B) 資訊部門導入防毒及郵件過濾解決方案

(C) 定期進行社交工程演練測試

(D) 導入封包過濾防火牆進行防禦

技術 111-2 答案D

(社交工程主要是利用人性的弱點，跟技術無關)

48. 下列何種對使用行動裝置的攻擊，主要是利用人與人的互動？

(A) 中間人攻擊（Man in the Middle Attack）

(B) 重送攻擊（Replaying Attack）

(C) 阻斷式服務攻擊（Denial-of-Service Attack）

(D) 社交工程（Social Engineering）

技術 111-2 答案D

1. 「有人假冒大學電算中心人員，打電話向你詢問，並騙取你的帳號密

碼。」請問上述屬於下列何種攻擊法？

(A) 社交工程（Social Engineering）

(B) 垃圾桶攻擊法（Dumpster Diving） (垃圾桶翻沒有碎掉的機密資訊)

(C) 中間人攻擊法（Man-in-the-middle Attack）

(D) 後門攻擊法（Backdoor Attack）

管理 111-1 答案A

2. 「攻擊者利用網站的漏洞把惡意程式腳本注入到網頁內，當使用者瀏

覽其網頁時，將會執行網頁內注入的惡意程式碼，可能造成Cookie資料被竊取、 Session連線被劫持或釣魚欺騙等攻擊。」請問上述屬於下列何種攻擊方法？

(A) 安全性設定疏失（Security Misconfiguration）

(B) 身分驗證功能缺失（Broken Authentication and Session Management）

(C) 跨網站偽造請求（Cross-Site Request Forgery, CSRF）

(D) 跨站指令碼攻擊（Cross-Site Scripting, XSS）

技術 111-1 答案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 (WAF)

(D) 使用圖型驗證碼

防護 111-1 答案D

(圖形驗證碼不能防禦XSS攻擊)

4. 下列何者「不」屬於主動式攻擊（Active Attack）？

(A) DDoS Attack（分散式阻斷服務攻擊）

(B) Buffer Overflow（緩衝區溢位）

(C) Typosquatting Attack（誤植域名攻擊）

(D) Brute Force（暴力破解）

規劃 111-1 答案C

(Typosquatting Attack 這是一種被動式攻擊，攻擊者註冊與合法網站類似的錯誤拼寫域名，目的是欺騙用戶訪問惡意網站，而不是直接干擾或破壞系統，比方說 1 和 l 或 0 和 O)

13. 下列何種惡意程式會寄生或附著在別的電腦程式、文件檔案裡面？

(A) 蠕蟲

(B) 電腦病毒

(C) 木馬程式

(D) 後門程式

技術 111-1 答案B

29. 小忍想發送秘密訊息給合作夥伴，為了保護這些消息，他使用下列何種的技術，可在普通消息中隱藏秘密消息，通過隱蔽性提供安全性？

(A) RSA

(B) Public key cryptography

(C) Encryption

(D) Steganography

技術 111-1 答案D

(隱寫術的定義)

32. 下列何者屬於網頁攻擊手法？（1） SQL Injection、（2） Parameterized Query、（3） Cross-Site Request Forgery、（4） Cross-Site Scripting

(A) 1 2 3

(B) 1 3 4

(C) 2 3 4

(D) 1 2 3 4

技術 111-1 答案B

(2為SQL injection的防禦方式)

33. 要防禦（Cross-Site Scripting, XSS），下列何者最有效？

(A) 過濾輸入參數長度

(B) 過濾輸出頁面

(C) 以黑名單過濾輸入參數

(D) 以白名單過濾輸入參數

技術 111-1 答案D

(黑名單要阻擋的符號太多了，因此白名單才對)

36. 「封包來源端 IP與目的端 IP相同的攻擊。」屬於下列何種攻擊方

法？

(A) Smurf Attack (利用偽造源IP（受害者IP）的ICMP請求，發送至廣播地址，觸發大量主機回應受害者，形成放大攻擊)

(B) Land Attack (發送源IP和目的IP完全相同的封包，使目標主機陷入自我連接的循環，導致資源耗盡或崩潰)

(C) UDP flood Attack (通過大量UDP封包淹沒目標，消耗其處理能力)

(D) ICMP flood Attack (直接發送大量ICMP請求（如Ping），壓垮目標頻寬或處理能力)

技術 111-1 答案B

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？

(A) XSS可以透過過濾此符號 “<”根治 (黑名單無法完全預防)

(B) Open Redirect可採用圖像式驗證根治 (Open Redirect 漏洞通常涉及未經驗證的重定向 URL，應通過嚴格的 URL 驗證和限制重定向目標來防範)

(C) 採用參數化查詢（Prepared Statement）可以解決 XSS (SQL 注入 攻擊)

(D) HTML.Encode是可以解決XSS的一種方法

防護 111-1 答案D

38. 關於 Cross-Site Scripting，下列敘述何者「不」正確？

(A) 置換網頁的對話框 (XSS 攻擊可以注入惡意腳本來修改網頁內容，包括替換或插入偽造的對話框（如 alert、confirm），用於欺騙用戶輸入敏感資訊)

(B) 取得瀏覽者的 Cookie (XSS 攻擊的典型危害之一是竊取用戶的 Cookie（尤其是未標記為 HttpOnly 的 Cookie），從而進行會話劫持)

(C) 下載網頁原始程式碼 (XSS 攻擊主要在客戶端執行，僅能操作或獲取瀏覽器渲染後的頁面內容（如 DOM 結構），但無法直接下載伺服器端的原始程式碼（如 PHP、Java 等後端程式碼）)

(D) 強迫轉址 (XSS 攻擊可通過注入 window.location 等腳本強制將用戶重定向至惡意網站，例如進行釣魚攻擊)

技術 111-1 答案C

39. 下列 何種語言為 Cross-Site Scripting攻擊主要使用的語言？

(A) Java

(B) Javascript

(C) C++

(D) C

技術 111-1 答案B

47. 關於連線劫持（Session Hijacking），下列敘述何者「不」正確

(A) 指攻擊者繞過驗證機制直接劫持了受害目標的Session

(B) Session是指兩個或多個通信設備之間，或設備與用戶之間的臨

時交互信息

(C) Session是一種用於存儲多個頁面的資訊（以變數形式）的方式，且會將該訊息存儲在使用者本機上 (Session 的資料存儲在伺服器端，而非使用者本機。客戶端僅保存 Session ID（通常透過 Cookie 或 URL 傳遞），伺服器根據此 ID 查找對應的 Session 資料。若資料存於本機，則屬於 Cookie 或其他本地儲存機制，而非 Session 本身)

(D) 惡意使用者冒用受害目標的 Session進行網路存取活動，活動可

以是金錢交易、資料竄改

技術 111-1 答案C

48. 關於中間人攻擊（ Man-In-The-Middle Attack, MITM），下列敘述何者「不」正確？

(A) 屬於網路竊聽分類的一種攻擊形式

(B) 攻擊者會將自己穿插到兩者受害目標之間

(C) 可攔截受害目標雙方間的通訊資訊

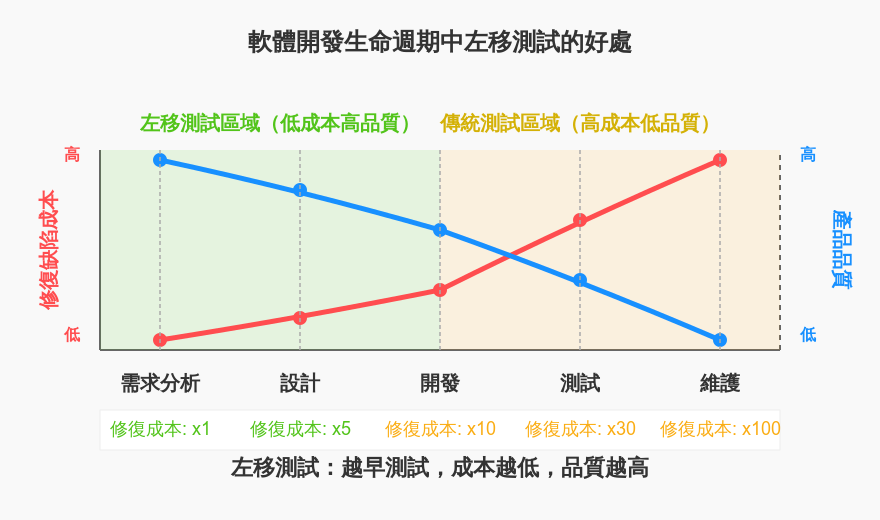
(D) 若受害目標雙方的連線有做加密則無法實現中間人攻擊 (即使通訊有加密，若加密機制存在漏洞（例如未驗證憑證、使用弱加密演算法），或使用者忽略安全警告（如無效的HTTPS憑證），攻擊者仍可能成功執行中間人攻擊。因此，加密本身並非絕對防護)

技術 111-1 答案D

程式與開發安全

**程式與開發安全的重要性**

* 在現代軟體開發中，資安已不再是事後才考量的議題，而應該融入整個開發流程，成為不可或缺的核心元素。這正是「安全軟體開發生命週期（SSDLC）」的價值所在—它根基於「測試左移（Shift Left Testing）」的理念，強調在開發初期就納入安全測試，以降低整體成本並提升軟體品質。
* 測試左移：早期投入，高效回報
  + 「測試左移」是指將測試活動（尤其是安全測試）提前至開發週期的早期階段，包括需求分析與設計階段。正如下圖或常見示意所示，早期發現問題的修復成本相對低，並可帶來更高的品質；後期才發現問題，修復成本會呈指數級上升，品質風險也顯著提高。
* 成本與品質對比：修復成本的實證
  + 以下數據為常見的經驗法則，說明在不同階段修復安全漏洞所需的成本倍數：
  + 需求分析階段：×1（基準值）
  + 設計階段：×5
  + 開發階段：×10
  + 測試階段：×30
  + 維護/上線階段：×100
  + 換句話說，越晚才發現安全問題，修復成本越高，同時也會造成更大的風險與更複雜的返工流程。
* 具體案例說明，SQL注入漏洞
  + 左移測試情境：在需求分析階段就考量到資料庫互動的安全需求，並將參數化查詢的準則納入設計，從源頭預防SQL注入風險。
  + 傳統測試情境：在上線後才發現SQL注入漏洞，必須重構整個資料存取層，不但成本驚人，還可能導致系統停機、資料洩露甚至損害企業品牌聲譽。
* SSDLC的核心價值：將安全融入整個開發流程
  + SSDLC將安全考量整合到軟體開發生命週期的每個階段，並奉行主動防禦而非事後補救的策略。與「測試左移」的理念如出一轍，在問題真正造成危害前，就以相對低成本主動識別並消除風險。
  + 通過SSDLC，組織不僅能大幅降低修復安全漏洞的成本，也能提升最終產品的品質與可靠性，達到客戶與企業雙贏的效果。



**什麼是 DevOps？**

* **詞源**：由 Development（開發）與 Operations（運維）組合而成
* **核心價值**：強調開發人員（Dev）與 IT 運維人員（Ops）之間的溝通與協作
* **主要目的**：
  + 打破開發與運維之間的「資訊鴻溝」
  + 建立快速而可靠的軟體交付流程
  + 使用自動化部署技術，確保部署任務的可重複性與降低出錯風險
* **影響層面**：
  + **產品交付**：藉由更快且自動化的流程，縮短軟體從開發到上線的時間
  + **測試**：利用持續整合（Continuous Integration, CI）與持續交付（Continuous Delivery, CD）等機制，提升測試效率
  + **功能開發**：開發與運維互相協作，迭代更迅速，能更快回應市場需求
  + **維護**：持續監控與即時回饋，讓問題能被提早發現與修復

**例子說明：傳統做法 vs. DevOps**

* **傳統做法**：
  + **申請資源冗長**：開發人員（Dev）需要一台新的虛擬機（VM），必須向基礎架構管理人員（Intra）申請，經過層層程序，可能要等七天以上。
  + **人工換版速度慢**：上線新版本時，需要人工作業打包、上傳並依序在各台伺服器上執行更新，過程繁瑣且容易出錯。
  + **責任推託**：當程式執行變慢，開發人員可能推給網路或系統，系統人員則推給資料庫管理員，責任歸屬不明確。
* **導入 DevOps 之後**：
* **自動化工具與流程**：開發與運維團隊密切合作，使用自動化建置、測試與部署（CI/CD），使部署流程可重複且快速。
* **資源申請快速**：利用虛擬化或雲端平台，自動化申請與配置環境，大幅縮短等待時間。
* **問題即時追蹤**：每個部署環節都有紀錄，若發生異常，能立即追蹤並通知負責人，降低互相推託的情況。

**什麼是 DevSecOps？**

* **詞源**：DevOps + Security，代表在 DevOps 的流程中融入安全（Security）的概念
* **核心理念**：將「安全」視為開發與運維過程中不可或缺的一部分
* **主要目的**：
  + **提早偵測安全風險**：在開發初期就導入安全掃描與檢測機制
  + **自動化安全測試**：降低人工作業失誤並快速回應安全漏洞
  + **整合安全與合規要求**：減少反覆修補，提高整體交付品質
* **優勢**：
  + 兼顧快速交付與安全性
  + 降低後期維護成本
  + 建立「安全即程式碼」的團隊文化

**例子說明：傳統 DevOps vs. DevSecOps**

* **傳統 DevOps：**
  + **安全檢測後置**：雖然已經透過自動化流程縮短了開發與部署時間，但安全檢測往往在上線前或事後才進行。
  + **修改流程冗長**：若在上線前才發現漏洞，需要臨時修補並再次部署，導致整個修改流程依然耗時且麻煩。
* **導入 DevSecOps 之後**：
  + **全面自動化安全檢測**：在每次程式碼提交（CI）與部署（CD）時，都自動進行原始碼掃描、弱點掃描以及必要的滲透測試。
  + **安全左移（Shift Left）**：若測試發現漏洞，系統會立即通知開發者進行修正，讓安全問題在最早階段就被解決，避免後期臨時補救造成高成本與高風險。

**安全軟體開發生命週期 (SSDLC)**

* 傳統 SDLC (Software Development Life Cycle)：
  + 階段：需求分析 → 設計 → 開發 → 測試 → 維護。
  + 傳統問題：資安通常被忽略或延後，問題多發現在測試或上線後。
* SSDLC 的特點：在每個階段加入資安考量：
  + 需求分析：加入安全需求 (如認證、授權、防止資料洩露)。
  + 設計：威脅建模，設計安全架構。
  + 開發：遵循安全編碼標準 (如 OWASP Code Review Guide 。
  + 測試：加入安全測試工具與流程 (如 SAST、DAST) 。
  + 維護：定期漏洞掃描與修補。
* Microsoft 安全性開發生命週期 (SDL) ：微軟提出的「具體實踐方法」，屬於 SSDLC 的 一種實作方式，SDL 是一套將安全性深植於軟體開發全流程的系統化方法，涵蓋需求分析到產品退役的每個階段，核心目標是透過早期風險預防與持續驗證，最小化可被利用的漏洞，並確保符合業界安全標準。
  + **訓練：**所有員工都必須完成一般安全性和隱私權感知訓練，以及與其角色相關的特定訓練，藉此確保團隊成員具備良好的安全意識與基本能力。
  + **需求**：此階段主要定義產品需遵守的安全規範與法規要求，例如強制資料加密或多因素驗證機制，並產出明確的安全需求文件作為後續開發基準。
  + **設計**：設計階段需執行威脅建模，透過 STRIDE 模型系統化識別假冒、篡改等六大威脅類型，並可考慮搭配 CVSS 等評分機制，對潛在風險進行量化評估，進而設計對應防禦架構如 API 簽章驗證。例如：縮小攻擊面向主要就是這個階段的考量，重點在系統架構層面上避免不必要的功能與介面，預先降低潛在攻擊向量。
  + **實作**：開發時需遵循安全編碼準則 (如避免 SQL 注入) ，並整合靜態程式分析工具 (如 SonarQube) 自動掃描原始碼漏洞。例如：靜態程式分析主要就是這個階段的考量。
  + **驗證**：使用滲透測試、模糊測試等方法模擬真實攻擊，檢測系統運作時可能出現的安全漏洞（如 XSS、邏輯錯誤等）。評估在運行環境下可被外部利用的所有介面與功能，確認是否符合先前在需求、設計階段設定的安全規範，並針對找到的弱點進行修正或通報。
  + **發行**：在正式上線前，依照驗證階段的測試結果，關閉不必要的服務或連接埠，移除測試帳號或測試介面，以最小化潛在暴露面。執行最後的安全檢查，確保系統已符合所有安全需求與法規要求，將已知風險降到最低後再行發佈。
  + **回應**：產品上線後持續監控漏洞並及時修補，例如透過微軟安全回報中心 (MSRC) 接收外部回報，定期發布更新檔。
* 威脅建模 (Threat Modeling) ：系統化識別、評估與應對應用程式潛在安全威脅的方法，目標在攻擊發生前預先防禦，降低風險並提升安全性。
  + **定義目標與範圍**：明確保護對象(關鍵資產)與資料流動範圍(如用戶輸入、API互動)。
  + **分解應用程式**：繪製資料流圖(DFD)，標示元件(伺服器、資料庫)、信任邊界與攻擊入口點。
  + **識別威脅(STRIDE 模型)**：依「假冒、篡改、否認、洩露、阻斷、提權」系統化列舉潛在攻擊手法。
  + **評估風險(CVSS 模型)：**根據 CVSS 的評分規則(如基本度量、時間度量、環境度量)，計算整體風險分數並排序威脅優先級。
  + **制定對策**：針對高風險威脅設計防禦(如MFA防假冒、輸入驗證防篡改)。
  + **驗證與持續更新**：定期審核模型並以滲透測試驗證，確保防禦措施與時俱進。

**軟體測試**

* 一般測試方法：
  + 單元測試 (Unit Testing)：
    - 目標：驗證軟體中最小可測試單元 (通常是函數或方法) 的行為是否符合預期。
    - 執行人員：主要由**開發者**執行。因為開發者最了解自己寫的程式碼。
    - 通常屬於白箱測試。
  + 整合測試 (Integration Testing)：
    - 目標：驗證不同模組或組件組合在一起後，是否能夠協同工作，資料和控制是否正確傳遞。
    - 執行人員：主要由開發者主導，因為開發者最了解模組之間的介面和互動方式。測試工程師或品保工程師 (QA) 也可以協作。
    - 屬於白箱測試。
  + 系統測試 (System Testing)：
    - 目標：將軟體作為一個整體，驗證它是否滿足所有功能和非功能需求。
    - 執行人員：通常由測試工程師或品保工程師 (QA) 執行。他們從使用者的角度出發，驗證整個系統的行為。
    - 功能性需求測試：驗證系統的功能是否符合需求規格書 (SRS) 中定義的功能需求。
      * 例如：驗證使用者登入、資料查詢、資料新增、資料修改、資料刪除等功能。
    - 非功能性需求測試：驗證系統的非功能特性，例如性能、安全性、可靠性、可用性、可維護性等。
      * 壓力測試：在高負載下測試系統的穩定性和可靠性，找出系統的瓶頸。
      * 效能測試：評估系統的反應時間、吞吐量、資源利用率等性能指標。
      * 資安測試：識別系統的安全漏洞，防止惡意攻擊。 (如 SQL Injection、XSS) 。
      * 兼容性測試：驗證系統在不同的作業系統、瀏覽器、硬體平台等環境下的相容性。
    - 屬於黑箱測試。
  + 驗收測試 (Acceptance Testing)：
    - 目標：由客戶或最終使用者驗證系統是否滿足他們的業務需求，是否可以接受。
    - 執行人員：通常由業務代表、最終使用者或客戶指定的測試人員執行。
    - 使用者驗收測試 (User Acceptance Testing, UAT)： 由最終使用者執行，模擬真實的使用場景。
    - 屬於黑箱測試。
* 安全測試方法：
  + 白箱測試 (White-box Testing)
    - 定義：檢查程式內部邏輯和結構，了解原始碼後進行測試，更容易鑑別出軟體問題的根因。
    - 範例：靜態程式碼分析，原始碼掃描。
  + 黑箱測試 (Black-box Testing)
    - 定義：不瞭解內部結構，僅根據輸入和輸出測試系統行為，更容易鑑別出軟體部屬後的問題。
    - 範例：弱點掃描、動態應用程式測試。
  + 靜態程式碼分析(SAST)：
    - 定義：程式不執行的情況下，分析原始碼或二進位檔案中的安全漏洞。
    - 適用階段：撰寫程式碼階段(程式撰寫完成後)。
    - 特性：早期檢測漏洞，修復成本低。
    - 範例漏洞：直接寫進程式的密碼。
    - 缺點：
      * 無法檢測業務邏輯漏洞 (如販賣機按一下掉兩瓶可樂) 。
      * 修補需要熟悉程式碼，可透過程式碼審查 (Code Review) 補充。
    - 範例工具：SonarQube、Fortify和Checkmarx。
  + 動態應用程式測試 (DAST) ：
    - 定義：執行應用程式並模擬攻擊行為，檢測運行中的漏洞。
    - 適用階段：測試階段末期或使用者驗收階段 (UAT) 。
    - 特性：模擬攻擊者行為，適合實際環境漏洞檢測。
    - 範例漏洞：SQL Injection、XSS。
    - 缺點：
      * 無法涵蓋所有情境，可能遺漏部分功能分支或業務流程。
      * 測試範圍受限於腳本和工具的設置。
    - 工具：OWASP ZAP、Burp Suite。
  + 模糊測試 (Fuzzing) ：是一種軟體測試技術，它向程式提供隨機或半隨機的輸入資料，並監控程式是否出現異常 (例如崩潰、記憶體洩漏等)，以發現潛在的漏洞和錯誤。它不是產生程式碼到原始程式中，而是產生輸入資料到應用程式中

**考古題：**

20. 在安全開發生命週期（Secure System Develop Life Cycle，SSDLC）中，有關開發與測試階段，可以協助降低資安風險的有下列哪些項目？（複選）

(A) 部署網頁應用程式防火牆

(B) 滲透測試

(C) 原始碼檢測

(D) 第三方元件資安檢測

規劃 114-1 答案BCD

(在安全開發生命週期 (SSDLC) 的開發與測試階段，主要目標在於及早發現並修正程式碼及組件中的安全漏洞。

滲透測試（B）：模擬攻擊者行為，找出潛在的安全漏洞。

原始碼檢測（C）：檢視程式碼以發現安全缺陷。

第三方元件資安檢測（D）：確保所使用的第三方軟體組件沒有已知漏洞。

相較之下，部署網頁應用程式防火牆（A）屬於運維或部署階段的防禦措施，不直接屬於開發與測試階段。)

27. 黑箱測試是軟體開發常見的安全檢測方式。下列何項「不」是黑箱測試的特性？

(A) 檢測人員不需要具備應用程式開發知識與經驗

(B) 檢測人員必需知道該受測軟體內部結構，以利測出正確結果 (白箱測試定義)

(C) 檢測人員僅須從使用者角度，進行軟體介面、功能及外部結構進行測試

(D) 檢測人員必須利用有效輸入與無效輸入來驗證是否有正確的輸出結果

技術 113-2 答案B

(黑箱測試的定義就是不需要知道軟體的內部結構、程式碼或實作細節。檢測人員將軟體視為一個「黑盒子」，只關注輸入和輸出，以及外部行為)

26. 關於應用程式安全的描述，下列何者最「不」適切？

(A) 應用程式弱點掃描可以瞭解是不是有既有的技術性弱點

(B) 應用程式碼的掃描可及早偵測程式撰寫的問題及可能產生的安全性問題

(C) 模糊測試（Fuzzing）指自動產生程式碼到原始程式中，以偵測程式碼的問題

(D) 應用程式的業務邏輯問題需要由熟悉業務的測試人員仔細的核實確認

技術 113-1 答案C

(模糊測試 (Fuzzing) 是一種軟體測試技術，它向程式提供**隨機或半隨機的輸入資料**，並監控程式是否出現異常 (例如崩潰、記憶體洩漏等)，以發現潛在的漏洞和錯誤。**它不是產生程式碼到原始程式中，而是產生輸入資料到應用程式中。**)

27. 關於DevOps的描述，下列何者錯誤？

(A) 為Development和 Operations的混成詞，是一種重視「軟體開發人員（Dev）」和「 IT運維技術人員（Ops）」之間溝通合作的文化、運動或慣例

(B) DevOps考慮的不止是軟體部署，它是一套針對這幾個部門間溝通與協同運作問題的流程和方法

(C) DevOps的引入能對產品交付、測試、功能開發和維護，起到意義深遠的影響。在缺乏 DevOps能力的組織中，開發與運營之間存在著資訊「鴻溝」

(D) 因採用自動化部署手段確保部署任務的可重複性增加部署出錯的可能性

技術 112-2 答案D

28. 從 Microsoft安全性開發週期（Secure Development Life, SDL）的觀點，靜態程式分析（Static Analysis）主要是下列何項階段的考量？

(A) 需求階段（Requirements）

(B) 設計階段（Design）

(C) 實作階段（Implementation）

(D) 分析階段（Analysis）

技術 112-2 答案C

(在 Microsoft SDL 流程中，實作階段（Implementation）強調程式碼撰寫與品質控制。此時導入「靜態程式分析工具」(如 SonarQube、Checkmarx 等)能針對原始碼進行自動化掃描，及早找出常見的安全弱點(例如 SQL 注入、XSS 等風險)。)

26. 關於軟體測試的敘述，下列何者錯誤？

(A) 整合測試可以由程式設計師或軟體品保工程師進行

(B) 基本路徑測試是根據程式設計的內部架構產生測試資料

(C) 黑箱測試用於測試程式的輸出資料與對應輸入資料之間的正確性，需考慮軟體內部的結構

(D) 功能測試指測試系統是否能符合預期的功能需求

技術 112-1 答案C

(黑箱測試不考慮軟體內部的結構)

28. 從Microsoft安全性開發週期（Secure Development Life, SDL）的觀點，縮小攻擊面向（Attack Surface Reduction）主要是下列何項階段的考量？

(A) 需求階段（Requirements）

(B) 設計階段（Design）

(C) 實作階段（Implementation）

(D) 發佈階段（Release）

技術 112-1 答案B

(根據 Microsoft SDL，設計階段(Design)會進行威脅建模(Threat Modeling)，在功能與架構設計時就要考慮「哪些功能或介面是多餘的？」「哪些服務應該預設關閉？」這些預先的系統與功能規劃，能避免在未來留下不必要的暴露面。雖然在發布前(Release)也會再次檢查並關閉不必要介面，但主要的架構與功能規劃都在「設計」時期就要決定，因此 SDL 中會將「縮小攻擊面向」歸在設計階段作為主要考量。)

22. 下列何者 「 不 」 是評估應用程式安全性的檢測方法？

(A) Penetration Testing (滲透測試)

(B) Ransomware Testing (勒索病毒測試)

(C) Threat Modeling (威脅建模)

(D) Source Code Review (原始碼掃描)

技術 111-2 答案B

(滲透測試、威脅建模和原始碼掃描是常見評估應用程式安全性的檢測方法)