113 年度第 1 次 資訊安全工程師能力鑑定 中級試題

科目：I22 資訊安全防護實務

考試日期： 113 年 4 月 13 日

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

C	1. 關於 MITRE ATT&CK 中的憑證存取（Credential Access）戰術（Tactic），下列何項錯誤？ (A) 中間人攻擊（Adversary-in-the-Middle）屬於此類戰術 (B) 暴力破解攻擊（Brute Force）屬於此類戰術 (C) 密碼政策探索（Password Policy Discovery）屬於此類戰術 (D) 變造網站憑證（Forge Web Credentials）屬於此類戰術
C	2. 關於弱點掃描，下列敘述何者錯誤？ (A) 網路弱點掃描用在尋找網路環境中的脆弱點，舉凡開放的通訊埠及所代表之服務，其服務是否透過未經加密的進行傳輸，或服務未更新漏洞 (B) 應用程式弱點掃描主要針對特定應用程式（尤其是網頁伺服器及其資料庫）的程式及應用環境（例如：Apache 版本漏洞），但主要是尋如 SQL 注入、跨站腳本、敏感目錄外洩…等可被攻擊之漏洞 (C) 主機弱點掃描用在檢查個別主機的脆弱點，例如主機效能負載對外服務能力，或是識別主機防毒系統是否更新 (D) 常見工具，有 OWASP ZAP, OpenVAS, Nessus…等
B C D 或 A B C D	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？ (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 (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
B	4. 【題組 1】情境如附圖所示。Alex 知道 WSL2 雖然為開發人員提供了極大的便利，使他們能夠在 Windows 上無縫地運行 Linux 環境，但同時也帶來了新的安全挑戰。為了保護公司免受潛在的安全威脅，Alex 開始著手制定一套綜合的安全管理措施。下列何項是針對 WSL 所提出提升資安的最佳做法？ 在 TechSecure Inc.，一家前沿的科技安全公司，資安團隊面臨著一項前所未有的挑戰。隨著開發團隊需要更多的彈性和功能來進行軟體開發，公司決定在其開發環境中採用 Windows Subsystem for Linux 2（WSL2）。 這個決策立即吸引了公司的資安政策制定者 Alex 的注意，身為公司資安政策訂定者，在面對公司研發團隊必須使用 Windows Subsystem for Linux 2 (WSL2)，必須對其資安攻防應建立那些安全管理措施。 (A) 經常使用 root 帳戶進行日常操作 (B) 保持 Windows 和 Linux 子系統的定期更新 (C) 在 WSL2 中禁用防火牆和安全軟體 (D) 共用 Windows 和 Linux 子系統的系統管理者密碼
D	5. 【題組 1】情境如附圖所示。駭客首先在 WSL 環境中部署了一個專門編寫的惡意 script，該 script 旨在利用 Windows 與 WSL 之間的互操作性漏洞。請問其目的，最有可能是下列何項？（請選一個最合適的答案）

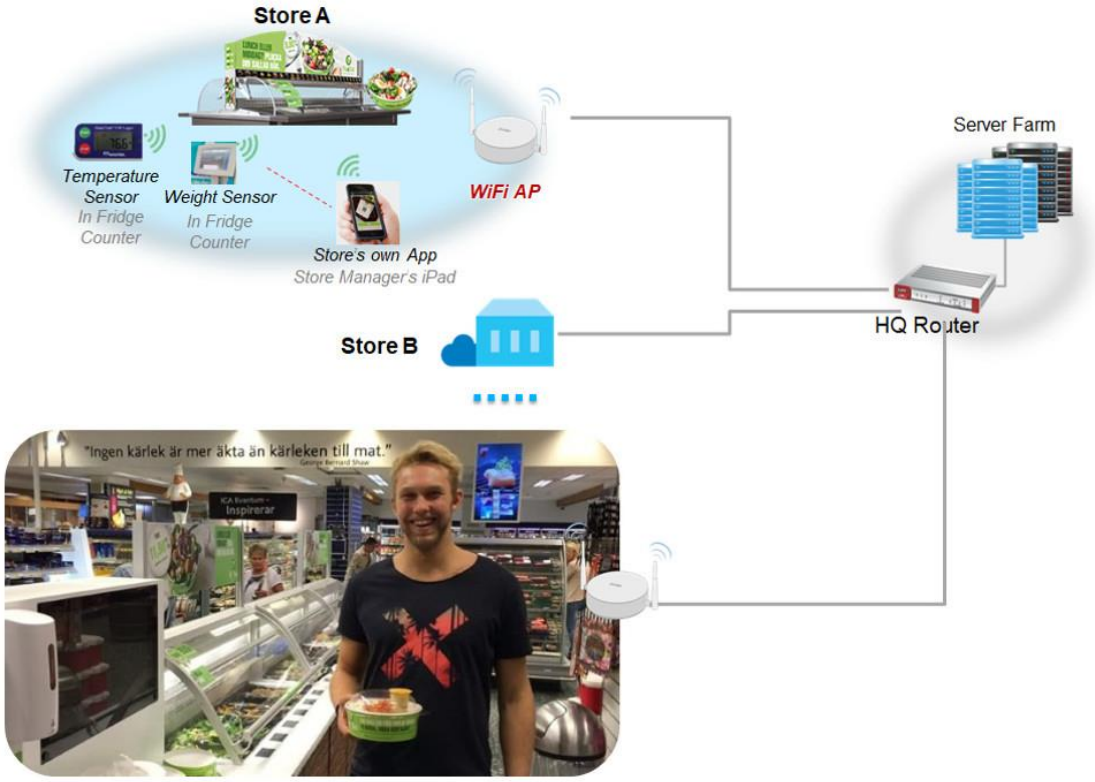
	與此同時，一群駭客正在密切關注 TechSecure 的這一舉措。他們計劃利用 WSL 一個未被廣泛認知的互操作性漏洞來部署惡意腳本，從而進行內部網路入侵。 這個腳本專門設計來利用 WSL2 環境中的漏洞，目標是獲取公司的敏感數據和內部系統的控制權駭客計劃利用 Windows Subsystem for Linux（WSL）來進行網絡入侵。 (A) 在 Windows 創立一個隱藏的管理員帳戶，以便未來存取 (B) 為了直接加密 Windows 系統文件，進行勒索軟體攻擊 (C) 通過 WSL 環境檢索並傳送 Windows 系統日誌，以分析可能的弱點 (D) 利用 WSL 執行環境的特性，隱藏網路流量，以掩蓋資料外洩行為
D	6. 【題組 1】情境如附圖所示。當使用帶有 GTFOBins 的 Windows Linux 子系統（WSL）時，下列何項措施對於增強安全性最重要？ 在進一步的調查中，Alex 發現駭客計劃利用 GTFOBins 來執行權限提升和安全環境逃逸。這個發現迫使他對 WSL2 的安全措施進行了再次強化。 GTFOBins 是一個關於 Unix 二進制文件如何被用於權限提升、文件操作、能力提升以及其他安全環境逃逸的技術文件。 (A) 在 WSL 中使用防病毒軟體 (B) 在 WSL 中安裝弱點掃描工具 (C) 禁用 WSL 的網路功能 (D) 偵測與記錄用戶對敏感二進制文件的使用
A B D	7. 【題組 1】情境如附圖所示。關於 Windows Linux 子系統（WSL）惡意軟體的特點和防禦策略，下列哪些陳述正確？ 通過 Alex 和他的團隊的不懈努力，TechSecure 成功地抵禦了駭客的進攻。他們的先進防禦策略不僅保護了公司的數據安全，也為整個行業樹立了如何安全使用 WSL2 的典範。從歷史軌跡追蹤 2023 年開始，駭客利用 WSL 環境日益增加，其惡意軟體數量也快速的成長。 (A) WSL 惡意軟體有時基於開源的程式碼，使得其較難被檢測出來

	(B) 這些惡意軟體變種包括能夠遠端存取裝置、執行任意程式碼的複雜功能 (C) 目前的防毒解決方案皆能主動偵測、有效識別和防禦這些基於 WSL 的惡意軟體 (D) EDR 監測系統活動和尋找可疑事件是防禦 WSL 類型惡意軟體的手段之一
D	8. 企業資安事件類型「不」包含下列何項？ (A) 機房漏水 (B) 備用發電機啟動故障 (C) 外部廠商發生資料外洩 (D) 私人手機遺失
B	9. 進行資安事件處置時，下列做法何者錯誤？ (A) 將漏洞修補以防止再發生 (B) 原始稽核紀錄可以刪除 (C) 確認事件根因是必要的 (D) 可以委託外部專業廠商進行
C	10. 針對資安防護機制配置，下列何種說明較符合縱深防禦（Defense in Depth）的概念？ (A) 購買符合公司規格流量的防火牆 (B) 定期更新防毒軟體的病毒碼 (C) 針對內部系統、網路、軟體進行多層次的安全控制 (D) 全程使用加密的資料傳輸
C	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 (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
B	12. 事故回應（Incent Response，IR）的處理流程中，依據 NIST SP800-61 r2 在隔離、清除和恢復階段中，下列何項是最佳處理方案？ (A) 立即更新安全政策 (B) 隔離受影響系統 (C) 開始法律行動 (D) 立即針對員工進行安全培訓
A C 或 A B C	13. 近年來 MFA 身份驗證機制遭攻擊者以網路釣魚攻擊破解之趨勢上升，因此抵禦網路釣魚多因素驗證（Phishing-resistant MFA）機制受到重視，因其可有效降低前述之攻擊成功機率。下列哪些身份驗證方式符合抵抗網路釣魚攻擊之特性？ (A) FIDO Auth (B) MMS MFA (C) PKI-based MFA (D) 增加密碼長度
A B	14. 根據 NIST Cybersecurity Framework 中的 Protect 功能，下列哪些項目是組織實施此功能時應考慮的關鍵要素？ (A) 實施身份管理及存取控制 (B) 執行資料加密和保護 (C) 建立災難復原程序 (D) 定期執行弱點掃描
D	15. 【題組 2】情境如附圖所示。由於已建置的簡易型無線網路系統資安防護能力不足，駭客能夠隨意的從各超市發起攻擊行為，參閱國際工業自動化協會（International Society of Automation，ISA）的 ANSI/ISA-95 普渡模型架構，請問在 Level 0 終點裝置層和 Level 1 工業控制層之中如何快速提升物聯設施的通訊安全，下列何項是最適合的解決方案？

S 服務商已經在數百家超級市場中設立自助沙拉吧服務，由於產品的新鮮度掌控不易，加上食材補給量不精確，因此造成自助沙拉吧品質不穩定、需求和供應數量不匹配以及食材的浪費；因此 4 年前 S 服務商規劃將所有的服務超市更換為獨特的冷藏櫃檯設施，內含多重物聯網裝置，配備有溫濕度感測器、重量感測器、溫控裝置與數位標籤系統等智慧裝置，確保冷藏條件、食物新鮮度、現場庫存狀態與整合結帳計費機制；每家商店使用的物聯網裝置也即時連接服務商後台系統，以整合倉庫管理、物流與金流相關資訊作業系統，並且也為不同的連鎖超市開發不同的營運軟體，以配各店現場的運營作業需求。在經過 18 個月的軟體委外開發 Web 營運系統和 2 年半的時間在各超市建置部署，已將其管理的所有超市更換為新的物聯網設施和營運系統，並且收到預期的營業成效。

S 服務商新到任的資訊長在評估持續營運風險時，在面對新興的物聯網資訊安全威脅下，他發現此物聯網設施和營運系統完全未有資安防護設計與建置，請問在此狀況下若您收到此資訊長的需要，要如何以最有效率和經濟的方式提供改善此系統的資安防護。



(A) 各超市更換新一代 NB-IoT 或 LoRa 無線傳輸設備，直接提升無線網路通訊安全

(B) 在物聯網裝置上增加身分認證機制，確認僅有經過認證的設備才能進行內部通訊

(C) 將物聯網裝置更換為有線通訊方式，避免駭客由無線網路造成系統危害

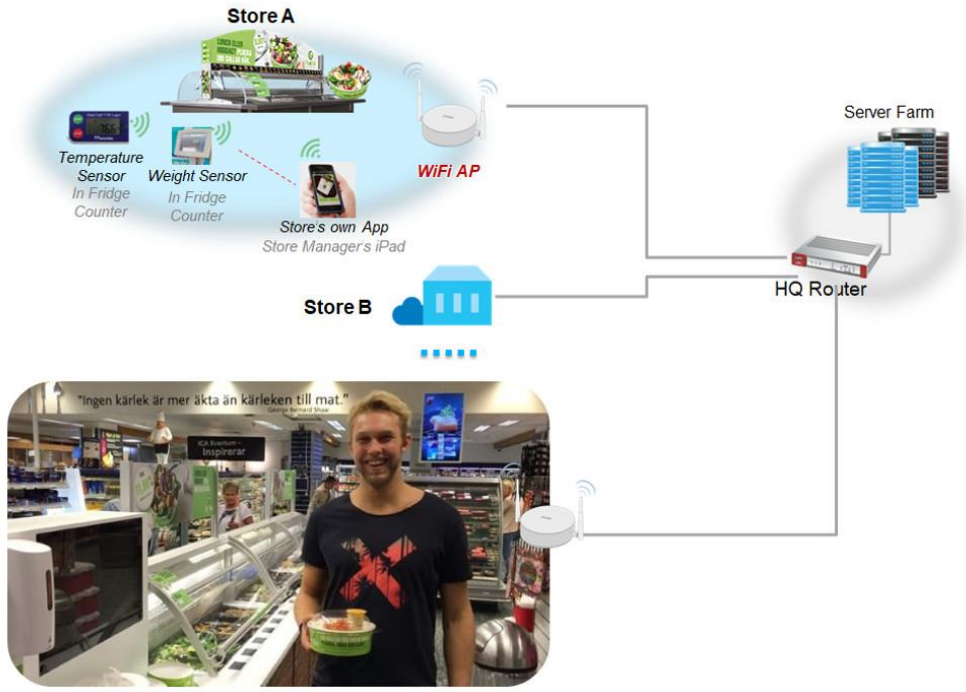
(D) 更換工業用 AP Controllor 設備，管制連線裝置和區分設備與人員連線網段

B

16. 【題組 2】情境如附圖所示。承上題，請問在零信任的原則，於 ANSI/ISA-95 普渡模型架構之下，建立 Level 2 監控層、Level 3 營運作業及 Level 4 管理層之中 OT 工控設施與 IT 資訊系統的安全防護能力，下列何者「不」是適當的解決方案？

S 服務商已經在數百家超級市場中設立自助沙拉吧服務，由於產品的新鮮度掌控不易，加上食材補給量不精確，因此造成自助沙拉吧品質不穩定、需求和供應數量不匹配以及食材的浪費；因此 4 年前 S 服務商規劃將所有的服務超市更換為獨特的冷藏櫃櫃設施，內含多重物聯網裝置，配備有溫濕度感測器、重量感測器、溫控裝置與數位標籤系統等智慧裝置，確保冷藏條件、食物新鮮度、現場庫存狀態與整合結帳計費機制；每家商店使用的物聯網裝置也即時連接服務商後台系統，以整合倉庫管理、物流與金流相關資訊作業系統，並且也為不同的連鎖超市開發不同的營運軟體，以配各店現場的運營作業需求。在經過 18 個月的軟體委外開發 Web 營運系統和 2 年半的時間在各超市建置部署，已將其管理的所有超市更換為新的物聯網設施和營運系統，並且收到預期的營業成效。

S 服務商新到任的資訊長在評估持續營運風險時，在面對新興的物聯網資訊安全威脅下，他發現此物聯網設施和營運系統完全未有資安防護設計與建置，請問在此狀況下若您收到此資訊長的需要，要如何以最有效率和經濟的方式提供改善此系統的資安防護。



(A) 系統 App 需經認證後才能部署使用

(B) 任何裝置應安裝防毒軟體才能進行連網通訊

(C) 任何人員需經認證後才能操作營運系統

(D) 在超市防火牆依連線位置部署不同的資安管理政策（Security Policy）

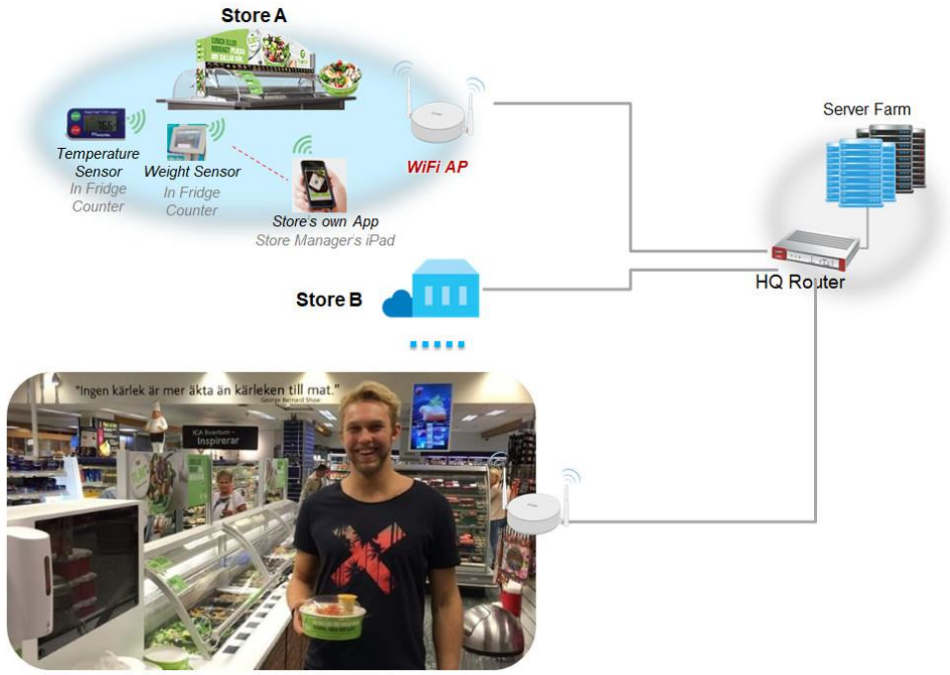
A

17. 【題組 2】情境如附圖所示。承上題，本系統在經過弱點掃瞄後將進行相關安全補正措施，請問下列何者「不」符合最

小管理成本的立即解決方案？

S 服務商已經在數百家超級市場中設立自助沙拉吧服務，由於產品的新鮮度掌控不易，加上食材補給量不精確，因此造成自助沙拉吧品質不穩定、需求和供應數量不匹配以及食材的浪費；因此 4 年前 S 服務商規劃將所有的服務超市更換為獨特的冷藏櫃櫃設施，內含多重物聯網裝置，配備有溫濕度感測器、重量感測器、溫控裝置與數位標籤系統等智慧裝置，確保冷藏條件、食物新鮮度、現場庫存狀態與整合結帳計費機制；每家商店使用的物聯網裝置也即時連接服務商後台系統，以整合倉庫管理、物流與金流相關資訊作業系統，並且也為不同的連鎖超市開發不同的營運軟體，以配各店現場的運營作業需求。在經過 18 個月的軟體委外開發 Web 營運系統和 2 年半的時間在各超市建置部署，已將其管理的所有超市更換為新的物聯網設施和營運系統，並且收到預期的營業成效。

S 服務商新到任的資訊長在評估持續營運風險時，在面對新興的物聯網資訊安全威脅下，他發現此物聯網設施和營運系統完全未有資安防護設計與建置，請問在此狀況下若您收到此資訊長的需要，要如何以最有效率和經濟的方式提供改善此系統的資安防護。



(A) 將各超市無法進行修補的 XP OT 工控主機升版為 Win 10 主機

(B) 關閉各超市資訊主機非必要的通訊埠

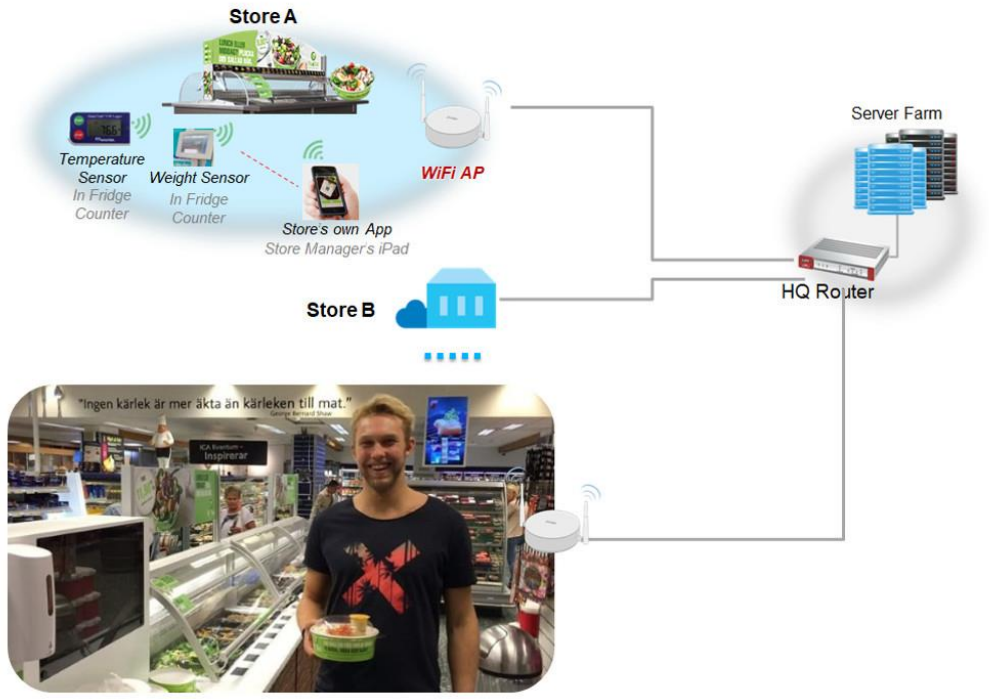
(C) 更新總部營運系統的資安 Patch

(D) 檢視所有營運系統使用者的操作權限，將需求權限最小化

A B D	18. 【題組 2】情境如附圖所示。承上題，S 公司當年委外開發本營運系統時並未有任何軟體安全之要求，當前參閱考 OWASP top10 和 OWASP Mobile Security 評估現階的軟體安全防護規劃，請問下列哪些措施較為適合迅速補強軟體弱點？

S 服務商已經在數百家超級市場中設立自助沙拉吧服務，由於產品的新鮮度掌控不易，加上食材補給量不精確，因此造成自助沙拉吧品質不穩定、需求和供應數量不匹配以及食材的浪費；因此 4 年前 S 服務商規劃將所有的服務超市更換為獨特的冷藏櫃檯設施，內含多重物聯網裝置，配備有溫濕度感測器、重量感測器、溫控裝置與數位標籤系統等智慧裝置，確保冷藏條件、食物新鮮度、現場庫存狀態與整合結帳計費機制；每家商店使用的物聯網裝置也即時連接服務商後台系統，以整合倉庫管理、物流與金流相關資訊作業系統，並且也為不同的連鎖超市開發不同的營運軟體，以配各店現場的運營作業需求。在經過 18 個月的軟體委外開發 Web 營運系統和 2 年半的時間在各超市建置部署，已將其管理的所有超市更換為新的物聯網設施和營運系統，並且收到預期的營業成效。

S 服務商新到任的資訊長在評估持續營運風險時，在面對新興的物聯網資訊安全威脅下，他發現此物聯網設施和營運系統完全未有資安防護設計與建置，請問在此狀況下若您收到此資訊長的需要，要如何以最有效率和經濟的方式提供改善此系統的資安防護。



(A) 駭客的攻擊手法一直不停的在更新、進步、改變，增設網站傳輸監控設備或機制，經由監控傳輸流量，對比病毒、惡意程式資料庫來過濾出可疑的流量，管理系統交易流量、加強防護機制，以提升系統防護能力

(B) 定期安排網站弱點掃描，針對本營運系統潛的在弱點進行 Patch 更新，以及增修網路安全政策（Security Policies），降低加密失效（Cryptographic Failures）和權限控制（Broken Access Control）的風險，提升系統與連線的安全性

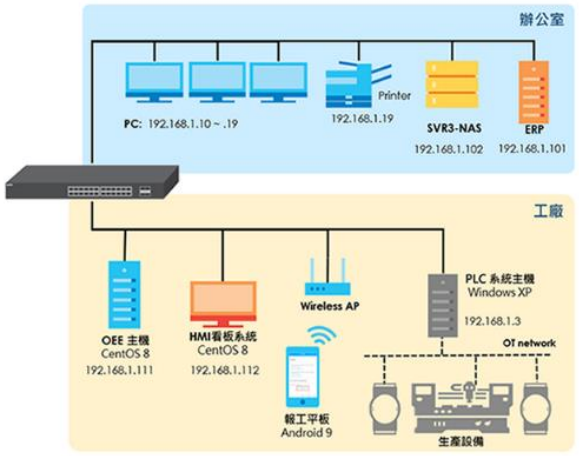
	(C) 重新編寫軟體以符合新世代的軟體安全要求，徹底解決不安全設計(Insecure Design)、安全設定(Security Misconfiguration）與使用過時或危機元件(Vulnerable and Outdated Components）的根本問題 (D) 在總部增設網站應用程式防火牆（Website Application Firewall)，增加注入式攻擊（Injection）的防禦能力，保護 Web 應用程式和交易資訊安全
D	19. 某設備的日誌記錄功能依照 The Syslog Protocol（RFC5424）標準設計，若需要較為詳盡的日誌訊息，以提供除錯(debug）使用，而該系統只提供下列 4 種的記錄等級，請問應該選擇下列何項設定最為合適？ (A) Emergency (B) Alert (C) Warning (D) Debug
B	20. 為提供資通訊系統可以安全進行遠端維護，請問下列何項措施「不」是必要的管理模式？ (A) 設定網路火牆管理遠端連線機制及限制存取的主機位置 (B) 建立 SSO（Single sign-on）單一簽入作業，統一連線帳密管理 (C) 使用多因子認證，確保連線使用者的身份 (D) 建立 VPN 機制，僅限制維護作業人員可以進行遠端安全連線作業
D	21. 廠商攜帶設備至機關進行維護作業，機關允許該設備連線至機房網路，待設備接上網路並操作一段時間後，監控中心即發現符合特定惡意程式行為之連線。下列建議之防護措施何者最「不」合適？ (A) 機關收到監控中心異常通知後，即時將廠商設備斷網 (B) 攜帶之設備或工具應確保安全無虞，方可連線至機

	關內部網路 (C) 廠商應恪守機關資通安全政策及委外廠商管理相關規範要求 (D) 須等相關工作結束後，再關閉網路連線
C	22. 當資訊室主管收到作業系統標準組態的例外請求時，第一步應該處理下列何項？ (A) 報告董事會，並尋求董事會的指導 (B) 確定產業的執行慣例，擬定應變作業計劃 (C) 確認風險並確定補償控制措施 (D) 依據資安管理系統程序，一律禁止例外請求作業
A B C	23. 在勒索軟體事件中，下列哪些日誌的來源可能找到入侵的紀錄或警訊？ (A) 網路面資安防護設備 (B) 重要主機之作業系統事件 (C) 防毒軟體告警 (D) 門禁進出紀錄
B 或 A	24. 【題組 3】情境如附圖所示，廠商 A 配合業務需求，開發新的 Web 訂票系統，請問如要進行弱點掃描，下列何項最為適合進行弱點掃描？ 有一個在我國立案的公司，以下簡稱廠商 A，其為「資通安全事件通報及應變辦法」所稱之特定非公務機關，主要業務為屬於關鍵基礎設施的交通服務。 (A) Checkmarx (B) OpenVAS (C) Hydra (D) Google
A	25. 【題組 3】情境如附圖所示，廠商 A 主要的資訊環境為 Windows 平台，若想檢視其如帳號登出、登入等事件，請問最合適的內建系統或工具為下列何項？

	有一個在我國立案的公司，以下簡稱廠商 A，其為「資通安全事件通報及應變辦法」所稱之特定非公務機關，主要業務為屬於關鍵基礎設施的交通服務。 (A) Event Viewer (B) Logger (C) QRadar (D) Syslog-NG
A	26. 【題組 3】情境如附圖所示，因部分服務主機環境為 Linux，故廠商 A 有一套依照 The Syslog Protocol（RFC5424）標準建置的日誌記錄系統，請問某事件為 NTP 子系統相關的記錄，其優先值（Priority）為 96，試問該事件的重要性（Severity）為下列何項？ 有一個在我國立案的公司，以下簡稱廠商 A，其為「資通安全事件通報及應變辦法」所稱之特定非公務機關，主要業務為屬於關鍵基礎設施的交通服務。 (A) Emergency (B) Error (C) Warning (D) Informational
B C	27. 【題組 3】情境如附圖所示，廠商 A 擬依照 The Syslog Protocol（RFC5424）標準建置的日誌記錄系統，某告警（warning）事件為使用者等級訊息（user-level messages），請問下列描述哪些正確？ 有一個在我國立案的公司，以下簡稱廠商 A，其為「資通安全事件通報及應變辦法」所稱之特定非公務機關，主要業務為屬於關鍵基礎設施的交通服務。 (A) 該事件的重要性（Severity）應為 0 (B) 該事件的重要性（Severity）應為 4 (C) 該事件的優先值（Priority）應為 12 (D) 該事件的 Facility 值（Priority）應為 2
B	28. 因應威脅的複雜度與頻繁，企業設置資訊安全監控中心

	（SOC , Security Operations Center）監看資安事件的服務也日漸普遍。SOC 服務主要分成 3 個階段：事前預防、事中監看、事後處理。下列敘述何者錯誤？ (A) 蒐集資安情資屬於事前預防階段 (B) 控管網路進出流量的設備屬於事前預防階段 (C) SOC 平台的自動過濾功能回報資安事件讓資安人員便於分析與判斷是屬於事中監看階段 (D) 識別威脅種類與來源以防止災害的擴大，並防止再度發生類似事故是屬於事後處理階段
A	29. 關於滲透測試的敘述，下列何者錯誤？ (A) 模擬駭客手法，在不需要系統管理者或公司同意下，進行漏洞驗證 (B) 模擬駭客手法或惡意使用者的行為，試圖找出和利用系統的弱點 (C) 滲透測試要確保不會影響正常的業務運作和資料的完整性 (D) 滲透測試（Penetration Testing，簡稱 Pen Testing）是一種安全測試方法
C	30. 在進行資安健診時，檢測作業最關鍵的活動是下列何項？ (A) 更新所有辦公軟體至最新版本 (B) 監控社交媒體上員工的活動 (C) 評估和識別系統中的潛在安全漏洞 (D) 部署最新的防毒軟體
A B D	31. 關於源碼檢測，下列哪些正確描述了 DLL Side Loading？ (A) DLL Side Loading 涉及到替換正常的 DLL 文件 (B) 通常被用來繞過安全措施並執行惡意程式碼 (C) 此技術概念僅可以在 Linux 系統上實現 (D) DLL Side Loading 可以利用合法軟體的加載行為來隱藏惡意活動
A	32. 關於資安測試工具用途的敘述，下列哪些正確？

B C	(A) Acunetix 為 Web 漏洞掃描程式 (B) Wireshark 提供網路協定、封包等資訊 (C) Sqlmap 用於檢測和利用應用程式 SQL 注入及對資料庫的攻擊 (D) Canvas 社交攻擊用工具
C	33. 【題組 4】情境如附圖所示，有關紅隊、藍隊與紫隊的敘述，下列何者錯誤？ 某企業集團希望徵求紅隊演練測試，來驗證公司內部 IT 資安防護能力，可是又擔心執行過程中讓公司內部 IT 或資安部門無法獲得溝通學習成長，身為該公司重要外部資安顧問專家。 (A) 紅隊演練（Red Team Assessment）在不影響企業營運下，進行模擬入侵攻擊 (B) 藍隊演練（Blue Team Assessment），指的是企業內部的工程部門或資安人員，當紅隊發動攻擊時，藍隊要在第一時間反應，快速防堵漏洞，將傷害降至最低 (C) 紫隊演練（Purple Team Assessment）為書面演練形式，無法進行技術攻防，目的就是讓負責演練的紅隊和藍隊能站在同一陣線 (D) 紅隊演練（Red Team Assessment）在有限的時間內從各種進入點執行攻擊，嘗試達成企業指定的測試任務
C	34. 【題組 4】情境如附圖所示，紅隊進行內部滲透測試攻擊，關於針對滲透的方法，下列何者錯誤？ 某企業集團希望徵求紅隊演練測試，來驗證公司內部 IT 資安防護能力，可是又擔心執行過程中讓公司內部 IT 或資安部門無法獲得溝通學習成長，身為該公司重要外部資安顧問專家。 (A) 找出 DC IP 位址：nmcli dev show (B) DNS 區域轉送：dig axfr (C) 列舉 ldap：nmap -Sp -p<ip> (D) 找出使用者：net user
D	35. 【題組 4】情境如附圖所示，紅隊進行內部滲透測試攻擊，下列哪一項「不」是針對 Password spray 會使用的手法？ 某企業集團希望徵求紅隊演練測試，來驗證公司內部 IT 資安防護能力，可是又擔心執行過程中讓公司內部 IT 或資安部門無法獲得溝通學習成長，身為該公司重要外部資安顧問專家。

	(A) cme smb <dc-ip> -u user.txt -p password.txt –no-bruteforce (B) Cme<IP> -U 'user' -p 'password' –pass-pol (C) Get-ADDefaultDomainPasswordPolicy (D) Smbmap -u "" -p"" -P 445 -H<dc-ip>
A B C	36. 【題組 4】情境如附圖所示，網域控制站（DC）是滲透測試重要的目標，而 ntds.dit 是 AD 主要的資料，可以透過下列哪些方式進行提取？ 某企業集團希望徵求紅隊演練測試，來驗證公司內部 IT 資安防護能力，可是又擔心執行過程中讓公司內部 IT 或資安部門無法獲得溝通學習成長，身為該公司重要外部資安顧問專家。 (A) Ntdsutil.exe 提取 ntds.dit (B) 使用 vssadmin 提取 ntds.dit (C) 利用 diskshadow 匯出 ntds.dit (D) 利用 certutil.exe 提取 ntds.dit
C	37. 【題組 5】情境如附圖所示。依據本案資安檢查報告及公司背景條件，請問 XYZ 公司在工廠端的資安維護作業，下列何項較「不」合適？ XYZ 公司是一家二十餘人的傳統製造業，公司在既有已過保固的 ERP 企業資源規劃系統與 PLC 工控系統已無維護服務，且 PLC 廠商特別說明只能在原作業系統下才能正常運行；近一年來經常發生老闆接的訂單無法即時出貨，為了追蹤管理各生產機台的運作狀況，老闆決定新增整體設備效能(OEE)系統，同時在工廠中導入 Android 平板裝置，讓現場工人不用操作電腦直接刷條碼即可進行報工作業，減少系統操作並達到即時數據蒐集與管理；目前在 OEE 系統驗收之際，整體工廠資安檢查報告摘要如下，身為資訊室主管請評估以下事項，那些是最適的資安防護規劃。 XYZ 公司的主機的網路拓樸圖： 

內部網路資源掃瞄結果摘要如下：

IP Address	MAC Address	Response Time	Host Name
192.168.1.10	58-6D-8F-83-9E-EB	2 ms	
192.168.1.16	6C-0B-84-67-FB-69	0 ms	P710
192.168.1.15	64-D8-14-61-E2-6E	1 ms	
192.168.1.19	00-24-D7-A6-D3-90	5 ms	PrtServer
print$			
192.168.1.13	7C-5C-F8-F2-00-58	5 ms	P710
192.168.1.102	08-00-27-ED-4F-4C	0 ms	SVR3-NAS
Sales			
Public			
Finance			
Factory			
192.168.1.14	C4-0B-CB-A5-A5-CD	273 ms	MaggieNB
Users			
192.168.1.17	88-63-DF-8F-40-7D	84 ms	ANDREWS-IMAC
ShareFloder			

XYZ 公司的主機的弱點偵測掃瞄記錄摘要如下：

192.168.1.101		
Severity	CVSS	Name
HIGH	9.3	PHP < 4.4.4 Multiple Vulnerabilities
HIGH	9.3	OpenSSL < 0.9.8s Multiple Vulnerabilities
MEDIUM	6.8	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
INFO	N/A	Windows Terminal Services Enabled
192.168.1.102		
Severity	CVSS	Name
HIGH	7.5	Unsupported Web Server Detection
MEDIUM	6.4	SSL Certificate Cannot Be Trusted
LOW	2.6	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
192.168.1.111		
Severity	CVSS	Name
CRITICAL	10.0	Rogue Shell Backdoor Detection
HIGH	7.5	SNMP Agent Default Community Name (public)
MEDIUM	6.8	Apache Tomcat Default Files
MEDIUM	6.8	Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK)
MEDIUM	5.0	SSL Certificate Signed Using Weak Hashing Algorithm
LOW	2.6	Terminal Services Encryption Level is not FIPS-140 Compliant
192.168.1.112		
Severity	CVSS	Name
HIGH	7.5	SNMP Agent Default Community Name (public)
MEDIUM	6.4	SSL Certificate Cannot Be Trusted
MEDIUM	5.0	mDNS Detection (Remote Network)
MEDIUM	4.3	SSH Weak Algorithms Supported
LOW	2.6	SSH Server CBC Mode Ciphers Enabled

XYZ 公司網路弱點掃瞄記錄摘要如下：

IP 位置	網路埠		狀態	服務	Reason
192.168.1.3	23	tcp	telnet	ms-wbt-server	syn-ack
192.168.1.3	135	tcp	open	msrpc	syn-ack
192.168.1.3	139	tcp	open	netbios-ssn	syn-ack
192.168.1.3	445	tcp	open	microsoft-ds	syn-ack
192.168.1.3	5357	tcp	open	http	syn-ack
192.168.1.3	49152	tcp	open	unknown	syn-ack
192.168.1.3	49153	tcp	open	unknown	syn-ack
192.168.1.10	53	tcp	open	domain	syn-ack
192.168.1.10	80	tcp	open	http	syn-ack
192.168.1.11	1723	tcp	open	pptp	syn-ack
192.168.1.11	554	tcp	open	rtsp	syn-ack
192.168.1.12	5000	tcp	open	upnp	syn-ack
192.168.1.13	443	tcp	open	https	syn-ack
192.168.1.14	554	tcp	open	rtsp	syn-ack
192.168.1.15	135	tcp	open	msrpc	syn-ack
192.168.1.15	139	tcp	open	netbios-ssn	syn-ack
192.168.1.16	135	tcp	open	msrpc	syn-ack
192.168.1.16	139	tcp	open	netbios-ssn	syn-ack
192.168.1.17	445	tcp	open	microsoft-ds	syn-ack
192.168.1.17	5357	tcp	open	wsdapi	syn-ack
192.168.1.19	515	tcp	open	printer	syn-ack
192.168.1.19	9100	tcp	open	jetdirect	syn-ack
192.168.1.101	135	tcp	open	msrpc	syn-ack
192.168.1.101	139	tcp	open	netbios-ssn	syn-ack
192.168.1.101	445	tcp	open	microsoft-ds	syn-ack
192.168.1.101	3389	tcp	open	ms-wbt-server	syn-ack
192.168.1.101	5357	tcp	open	http	syn-ack
192.168.1.102	23	tcp	telnet	ms-wbt-server	syn-ack
192.168.1.102	8000	tcp	open	http-alt	syn-ack
192.168.1.100	80	tcp	open	http	syn-ack
192.168.1.100	443	tcp	open	http	syn-ack
192.168.1.11	3389	tcp	filtered	ms-wbt-server	no-response

(A) 修補弱點掃瞄和滲透測試的高風險項目

(B) 修補新交付的 OEE 系統源碼掃瞄的高風險項目

(C) 更新既有 PLC 工控系統的 Windows 定期發佈的更新檔案

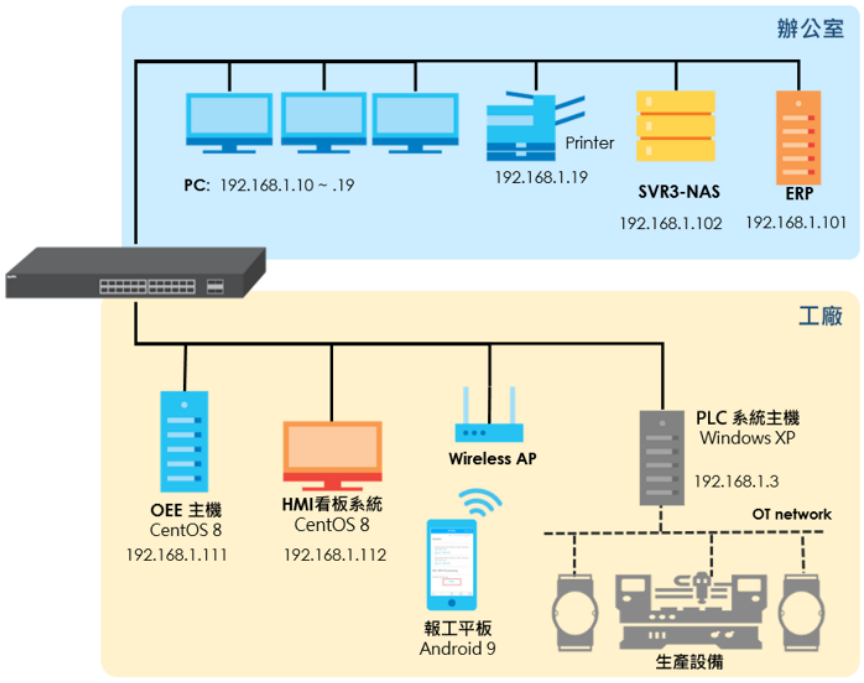
(D) 定期更新新交付報工平板的 Android 發佈的更新檔案

A

38. 【題組 5】情境如附圖所示。承上題，依據本案資安檢查報告及公司背景條件；由於既有工廠內的工控系統(Industrial Control System，ICS)資安防護不足，考量增強維護廠商的遠端作業及工廠工控系統的防護能力，將著手規劃提升相關資安防禦措施，請問下列何項計劃或執行作業有誤？

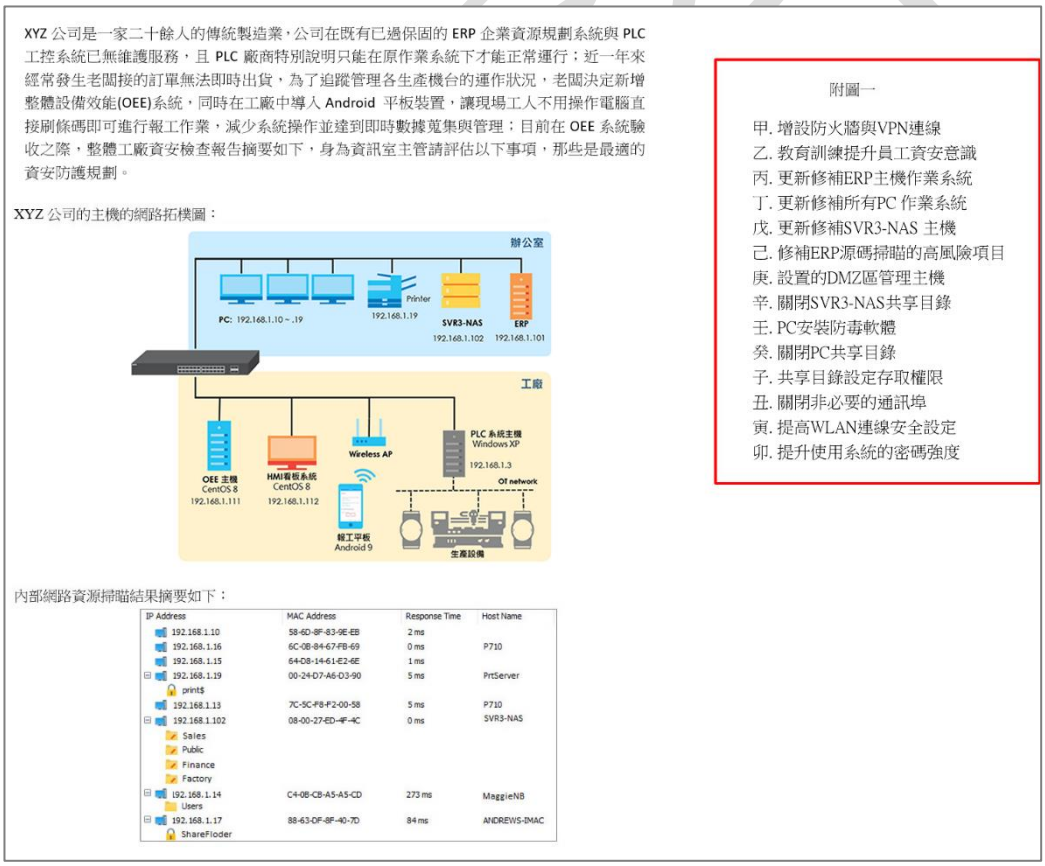
XYZ 公司是一家二十餘人的傳統製造業，公司在既有已過保固的 ERP 企業資源規劃系統與 PLC 工業控制系統已無維護服務，且 PLC 廠商特別說明只能在原作業系統下才能正常運行；近一年來經常發生老闆接的訂單無法即時出貨，為了追蹤管理各生產機台的運作狀況，老闆決定新增 OEE 整體設備效能系統，同時在工廠中導入 Android 平板裝置，讓現場工人不用操作電腦直接刷條碼即可進行報工作業，減少系統操作並達到即時數據蒐集與管理；目前在 OEE 系統驗收之際，整體工廠資安檢查報告摘要如下。身為資訊室主管請評估最適的資安防護規劃。

XYZ 公司的主機的網路拓樸圖：



(A) XYZ 公司的工控系統並非完全實體隔離，因此在資安防護設計必須依序考量：機密性、完整性和可用

	性 (B) 規劃虛擬修補（Virtual Patching）機制，保護實體防護不足與無法更新修補的設備與工控系統 (C) 強化網路通訊安全降低網路連線風險，包含：Internet, Intranet, WLAN & 廠商維護通訊路徑 (D) 遠端連線必須使用 VPN，並且管理所有工業控制系統的操作存取權限
B	39. 【題組 5】情境如附圖所示。承上題，依據本案資安檢查報告及公司背景條件，XYZ 公司討論規劃可能的資安防護事項如附圖一所示。請問 XYZ 公司辦公室區域在不更換及增購設備的情況下，下列何項的資安防護措施較為合適與即時可行？



內部網路資源掃瞄結果摘要如下：

IP Address	MAC Address	Response Time	Host Name
192.168.1.10	58-6D-8F-83-9E-EB	2 ms	
192.168.1.16	6C-0B-84-67-FB-69	0 ms	P710
192.168.1.15	64-D8-14-61-E2-6E	1 ms	
192.168.1.19	00-24-D7-A6-D3-90	5 ms	PrtServer
print$			
192.168.1.13	7C-5C-F8-F2-00-58	5 ms	P710
192.168.1.102	08-00-27-ED-4F-4C	0 ms	SVR3-NAS
Sales			
Public			
Finance			
Factory			
192.168.1.14	C4-0B-CB-A5-A5-CD	273 ms	MaggieNB
Users			
192.168.1.17	88-63-DF-8F-40-7D	84 ms	ANDREWS-IMAC
ShareFloder			

XYZ 公司的主機的弱點偵測掃瞄記錄摘要如下：

192.168.1.101		
Severity	CVSS	Name
HIGH	9.3	PHP < 4.4.4 Multiple Vulnerabilities
HIGH	9.3	OpenSSL < 0.9.8s Multiple Vulnerabilities
MEDIUM	6.8	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
INFO	N/A	Windows Terminal Services Enabled
192.168.1.102		
Severity	CVSS	Name
HIGH	7.5	Unsupported Web Server Detection
MEDIUM	6.4	SSL Certificate Cannot Be Trusted
LOW	2.6	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
192.168.1.111		
Severity	CVSS	Name
CRITICAL	10.0	Rogue Shell Backdoor Detection
HIGH	7.5	SNMP Agent Default Community Name (public)
MEDIUM	6.8	Apache Tomcat Default Files
MEDIUM	6.8	Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK)
MEDIUM	5.0	SSL Certificate Signed Using Weak Hashing Algorithm
LOW	2.6	Terminal Services Encryption Level is not FIPS-140 Compliant
192.168.1.112		
Severity	CVSS	Name
HIGH	7.5	SNMP Agent Default Community Name (public)
MEDIUM	6.4	SSL Certificate Cannot Be Trusted
MEDIUM	5.0	mDNS Detection (Remote Network)
MEDIUM	4.3	SSH Weak Algorithms Supported
LOW	2.6	SSH Server CBC Mode Ciphers Enabled

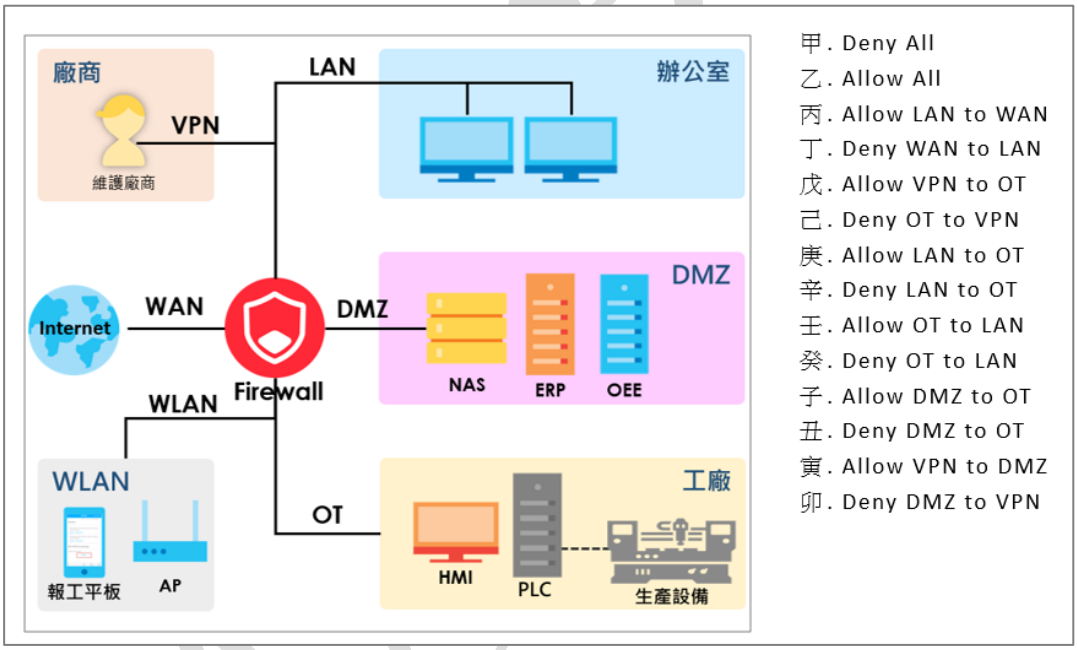
XYZ 公司網路弱點掃瞄記錄摘要如下：

IP 位置	網路埠		狀態	服務	Reason
192.168.1.3	23	tcp	telnet	ms-wbt-server	syn-ack
192.168.1.3	135	tcp	open	msrpc	syn-ack
192.168.1.3	139	tcp	open	netbios-ssn	syn-ack
192.168.1.3	445	tcp	open	microsoft-ds	syn-ack
192.168.1.3	5357	tcp	open	http	syn-ack
192.168.1.3	49152	tcp	open	unknown	syn-ack
192.168.1.3	49153	tcp	open	unknown	syn-ack
192.168.1.10	53	tcp	open	domain	syn-ack
192.168.1.10	80	tcp	open	http	syn-ack
192.168.1.11	1723	tcp	open	pptp	syn-ack
192.168.1.11	554	tcp	open	rtsp	syn-ack
192.168.1.12	5000	tcp	open	upnp	syn-ack
192.168.1.13	443	tcp	open	https	syn-ack
192.168.1.14	554	tcp	open	rtsp	syn-ack
192.168.1.15	135	tcp	open	msrpc	syn-ack
192.168.1.15	139	tcp	open	netbios-ssn	syn-ack
192.168.1.16	135	tcp	open	msrpc	syn-ack
192.168.1.16	139	tcp	open	netbios-ssn	syn-ack
192.168.1.17	445	tcp	open	microsoft-ds	syn-ack
192.168.1.17	5357	tcp	open	wsdapi	syn-ack
192.168.1.19	515	tcp	open	printer	syn-ack
192.168.1.19	9100	tcp	open	jetdirect	syn-ack
192.168.1.101	135	tcp	open	msrpc	syn-ack
192.168.1.101	139	tcp	open	netbios-ssn	syn-ack
192.168.1.101	445	tcp	open	microsoft-ds	syn-ack
192.168.1.101	3389	tcp	open	ms-wbt-server	syn-ack
192.168.1.101	5357	tcp	open	http	syn-ack
192.168.1.102	23	tcp	telnet	ms-wbt-server	syn-ack
192.168.1.102	8000	tcp	open	http-alt	syn-ack
192.168.1.100	80	tcp	open	http	syn-ack
192.168.1.100	443	tcp	open	http	syn-ack
192.168.1.11	3389	tcp	filtered	ms-wbt-server	no-response

(A) 甲丙戊庚辛壬癸子卯
(B) 乙丁戊壬癸子丑寅卯
(C) 甲乙丙丁己辛壬丑寅
(D) 乙丁己庚辛壬子寅卯

A D 或 A B 或 B D 或 A B D

40. 【題組 5】情境如附圖所示。承上題參如本系統情境架構，XYZ 公司為提升安全防護計劃建置防火牆，並且將網路分割為不同網段以管理網路通訊，同時提供維護廠商得以用 VPN 進行連線作業，參考附圖中的網路區塊規劃，請問依以下路由管理項目，防火牆應建立的基本資安政策組合有下列哪些項目？



(A) 丙庚壬
(B) 丁己辛
(C) 癸丑卯乙
(D) 戊子寅甲