課程名稱：18508_醫療資安防護與攻防演練實務應用 課程摘要

🎯 1. 適合對象與能力門檻

- **適合族群**：醫療院所與企業之資訊/資安人員、網管人員、系統管理員、資安主管，以及負責事件應變與危機處理之團隊成員。本課程針對第一線人員在面對駭客攻擊與威脅時，提供實務案例與救援決策指導。
- **能力門檻**：普通。建議具備基礎網路架構（如對外服務區、內網、Internet）、伺服器管理及系統日誌（Log）之基本概念。

📚 2. 課程核心大綱與架構圖

- **章節架構**：
  - **章節一：前言與傳統寓言的資安啟示** — 透過「神父救災」與「曲薪徙薪」典故，解析資安維運的困境、攻守時間不對等（紅隊可休息，藍隊需 24 小時守護） 及資安影響病安/人命的真實案例。
  - **章節二：資安攻防演練與攻擊手法拆解** — 透過實場演練架構，剖析黑客如何透過 Web 漏洞、WAF/MDR 告警繞過、Mimikatz 提取帳密、及 2025 年新興的 Bring Your Own Vulnerable Driver (BYOVD) 驅動程式漏洞攻擊。
  - **章節三：資安事件實戰案例復盤** — 探討隱蔽長達一年半的潛伏攻擊案例、多層次主機擴散、以及 2025 年醫療產業連鎖勒索事件之決策脈絡。
  - **章節四：駭客心理與「木桶理論」破口** — 分析駭客選擇次要/後媽生系統（如停車場系統、公播系統）作為破口入侵的策略。
  - **章節五：資安事件處置的電車難題與復原策略** — 探討第一時間「斷網 vs. 持續服務」的抉擇困境、備份檔安全性確認、DNS 優先還原邏輯 及主管機關通報時程。
  - **章節六：事件後續改善與長效防禦措施** — 提出全院/全體系部署 MDR、強制啟用 MFA 多因素驗證、夜間離峰斷網管制、Web

前端防護與分院自救機制。

🛠️ 3. 必備前置知識清單

- **基礎網路與服務概念**：了解基本 TCP/IP 協定、DNS 解析原理、Web 服務（HTTP/HTTPS） 及網段隔離（VLAN/DMZ）概念。
- **系統防護與維運觀念**：了解 WAF（Web 應用程式防火牆）、IPS（入侵防禦系統）、EDR/MDR（端點偵測與回應） 及備份機制（RTO/RPO）之運作基礎。

📖 4. 專有名詞與概念辭典

- **BYOVD (Bring Your Own Vulnerable Driver)**：駭客利用合法但帶有漏洞的舊版驅動程式植入系統，繞過作業系統與 EDR/防毒軟體限制，直接在 Kernel 底層建立最高權限帳號的攻擊手法。
- **木桶理論 (Bucket Theory)**：企業或醫院的防護強度取決於「最短的那塊木板」。駭客往往不直接挑戰防護最強的核心系統，而是從被忽視的次要服務（如停車場系統、公播系統）作為破口入侵。
- **電車難題（資安斷網抉擇）**：當偵測到疑慮主機遭入侵時，第一時間「斷網」能阻止擴散，但可能導致醫療/業務服務全面中斷；若「不斷網」則面臨駭客進一步擴散至 AD 主機與抹除備份檔的巨大風險。
- **Shadow Backup (影子備份 / Shuttlebay)**：採用被動式、線上無法直接存取或看到的備份機制，確保在主要備份檔遭駭客搜尋並抹除時，仍有最後安全的基底可進行還原。

💼 5. 課程學習職能對照

- **對應職能名稱**：資安事件應變工程師 / 資訊安全分析師 / 醫療資訊安全管理師
- **主要工作任務/能力指標**：
  - **資安威脅識別與應變決策能力**：能分析多層次入侵行為（如 Web/MDR/WAF 告警），並在緊急事件發生時評估系統邏輯，決定正確的還原優先順序（如先還原 DNS）與斷網決策。
  - **事故復盤與長效防護規劃能力**：能剖析系統弱點（如未防護的次

要系統與備份安全性），推動全域 MFA、MDR 全面導入 及離線/影子備份機制建置。