1.如果出現(需要存取權)，代表你不是使用 @ms.tyc.edu.tw 的帳戶(登入 Google)。

2.請開一個新的 Chrome(瀏覽器)，

網址如下(登入 google)：

https://reurl.cc/vQYdbl

，登入您教育局給的 Google 帳戶 @ms.tyc.edu.tw。

帳號(單一認證帳號) 密碼(單一認證密碼)。

3.完成登入後。

再貼上資安研習評量網址：(如下)

https://forms.gle/oRE6Gr9WfZ6Fu4Sj6

4.完成評量只要有分數即可，請截圖上傳到中埔資安 3 小時上傳區，

https://reurl.cc/eMR3bM

5.如果老師們不會的話，可以將題目複製，貼到 AI 的對話中，就會有正確的解答。

以下，僅供參考

新興數位威脅中，AI生成的深偽（Deepfake）技術可能被用於下列哪項攻擊情境？ * 20 分

- (●) 偽造高階主管影像進行財務詐騙。
- ( ) 暴力破解網站帳號密碼。
- ( ) 快速定位系統漏洞進行攻擊。
- ( ) 利用IoT裝置發動大規模DDoS攻擊。

關於應對新興數位威脅，零信任（Zero Trust）架構的推廣主要解決下列哪項問題？ * 20 分

- ○ 降低硬體維護成本。
- ◉ 防範內外部未經驗證的存取行為。
- ○ 提升網站載入速度。
- ○ 簡化員工遠端辦公流程。

「供應鏈攻擊」最常利用企業的下列哪一種安全弱點作為入侵途徑？ * 20 分

- ○ 最終用戶端點防護失效
- ◉ 委外廠商或第三方服務提供者的安全漏洞
- ○ 應用程式授權錯誤配置
- ○ 備份機制頻率不足

下列哪一種網路攻擊手法最常利用分散式節點發起大量請求，導致目標伺服器資源耗盡而無法提供正常服務？ * 20 分

- ○ SQL注入攻擊。
- ○ 中間人攻擊。
- ○ 跨網站指令碼攻擊。
- ◉ 分散式阻斷服務攻擊。

2024年過後，可以預見下列哪一種威脅將會更加突出？ * 20 分

- ○ 傳統的病毒和蠕蟲感染。
- ○ 針對過時作業系統和軟體的漏洞利用。
- ◉ 結合物聯網 (IoT) 設備漏洞的複合式網路攻擊。
- ○ 大規模的垃圾郵件和網路釣魚郵件。