01_外部專案 - 專案資訊 #1084

專案資訊 # 1064 (New-新增): 2025-PenTest

Object Owner Anomalies

2025-11-10 13:32 - Joy Liao

狀態:	In process-進行中	**開始日期:**	2025-08-01
優先權:	Normal	**完成日期:**	2025-12-31
被分派者:	益利 周	**完成百分比:**	10%
分類:		**預估工時:**	0:00 小時
版本:		**耗用工時:**	0:00 小時

概述

bookmark202304241526075413782029O7 "Object Owner Anomalies

" When domain objects are owned by non-admin users or groups, they may mismanage them due to a lack of authority, leading to increased risks of unauthorized access and accidental data alterations. Additionally, tracking responsibility for changes becomes more challenging, complicating accountability and security. "All objects (users, groups, sMSA, gMSA, computers, OU, GPO) must be owned by one of the following objects:

Domain Admins

Enterprise Admins

Administrators

Local System

"

歷史

#1 - 2025-11-10 13:34 - Joy Liao

- 完成日期 設定為 2025-12-31

- 被分派者 設定為 益利 周

- 開始日期 從 2025-11-10 變更為 2025-08-01

#2 - 2025-11-28 10:50 - 益利 周

- 狀態 從 New-新增 變更為 In process-進行中

- 完成百分比 從 0 變更為 10

1. 識別目前所有權配置現況

2. 變更所有權至標準化管理群組
一旦識別出錯誤配置的物件，就需要將所有權重新分配給組織定義的標準管理群組，例如 Domain Admins、Enterprise Admins 或 Administrators。
標準化所有權歸屬的目標群組：
Domain Admins
Enterprise Admins
Administrators (**通常指內建的 Administrators 群組**)
Local System (**極少用於 AD 物件所有權，主要用於服務內容，但仍是受信任的系統實體**)

3. 實施嚴格的存取控制和政策
變更所有權後，必須確保未來不會再發生類似的誤設。
可行之做法：
移除非管理員的「變更所有者」權限：
審查整個網域的委派權限。確保標準使用者或低權限群組沒有 Write Owner 的擴展權限。這項權限應嚴格限制在高階管理員群組。
建立自動化監控與警報機制：
設定監控系統（如 SIEM 工具）來追蹤 Windows 安全事件日誌，特別是當物件的所有權發生變更時（Event ID 4670 或相關的 ACL 變更事件）。一旦發生未經授權的變更，立即發出警報。
標準化委派流程：
建立明確的 IT 政策，規範誰可以管理 AD 物件。所有物件管理和所有權變更都必須遵循正式的變更管理流程，並由標準的管理員帳戶執行。