

## 紅隊演練作業參考指引

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	112/12/31	新編



# 目 次

1. 前言 .....	1
1.1 目的 .....	1
1.2 適用對象 .....	1
1.3 章節架構 .....	1
2. 資安檢測方法比較 .....	3
2.1 弱點掃描 .....	3
2.2 滲透測試 .....	5
2.3 紅隊演練 .....	10
2.4 檢測方式比較 .....	11
3. 紅隊演練作業管理程序 .....	13
3.1 規劃階段 .....	13
3.2 執行階段 .....	26
3.3 檢查階段 .....	51
3.4 改善階段 .....	54
4. 結論 .....	57
5. 參考文獻 .....	58
6. 附件 .....	59
附件 1 紅隊演練招標說明文件範本 .....	附件 1-1

## 圖目次

圖 1	弱點掃描作業流程 .....	5
圖 2	滲透測試作業流程 .....	9
圖 3	紅隊演練作業流程 .....	10
圖 4	紅隊演練流程 .....	13
圖 5	規劃階段細部流程 .....	14
圖 6	紅隊演練角色 .....	17
圖 7	執行階段細部流程 .....	27
圖 8	檢查階段細部流程 .....	54
圖 9	改善階段細部流程 .....	55

## 表 目 次

表 1	弱點掃描服務 .....	3
表 2	系統滲透測試項目 .....	6
表 3	物聯網設備滲透測試項目 .....	8
表 4	弱點掃描、滲透測試及紅隊演練比較 .....	11
表 5	紅隊人員額外資格要求 .....	22
表 6	MITRE ATT&CK 技術列表 .....	29
表 7	紅隊演練執行成效評估項目 .....	56



## 1. 前言

國家資通安全研究院承接數位發展部資通安全署(以下簡稱資安署)之「辦理數位發展部資通安全署 112 年政府資通安全防護」補助計畫(以下簡稱本計畫)，執行政府資通安全防護相關工作，「紅隊演練作業參考指引」(以下簡稱本指引)為本計畫「7.3 資安參考指引編修」之交付文件。

### 1.1 目的

本指引目的為提供政府機關(構)選用紅隊演練服務時之相關注意事項，建議於演練專案招標作業前除擬定紅隊演練範圍與目的外，亦可參考本指引制訂招標所需內容以篩選出有能力執行之專業團隊，以及了解雙方應注意事項與配合方式，確保演練可達到預期之目標，以提升資安防護能量。

### 1.2 適用對象

本指引主要提供欲委外執行紅隊演練以評估現有資安防護機制有效性之政府機關(構)(以下簡稱演練機關或藍隊)，從規劃(Plan)、執行(Do)、檢查(Check)及改善(Act)等 4 階段作業之建議執行方式與相關注意事項，協助演練機關委外辦理紅隊演練時，除考量機關所面臨之資安風險與防護需求外，可參考本指引擬定紅隊演練範圍、目的、時程、人員組成及能力要求等內容，除可選出執行能力較優之專業團隊外，亦能達到預期之演練目標，以提升機關資安防護能量。本指引係屬建議性質，演練機關可參考本指引執行紅隊演練，但不以此為限。

### 1.3 章節架構

- 第 1 章「前言」：說明本指引之目的、適用對象及章節架構。
- 第 2 章「資安檢測方法比較」：從檢測重點、方法、時程及適用性等面向說明各項資安檢測之差異。



- 第3章「紅隊演練作業管理程序」：依規劃、執行、檢查及改善等4階段作業說明紅隊演練建議執行方式與相關注意事項
- 第4章「結論」：綜整說明本指引之內容，以及對政府機關(構)之助益。
- 第5章「參考文獻」：詳列本指引所參考之標準與文獻等資料。

## 2. 資安檢測方法比較

弱點掃描、滲透測試及紅隊演練係針對不同需求所採用之資通安全檢測方法，過往資安檢測重點在於針對弱點本身之偵測與利用，故運用弱點掃描偵測是否存在弱點，並透過滲透測試進行弱點利用，以了解該弱點可造成之損害，協助機關於實際發生資安事件前進行弱點修補。紅隊演練則以真實駭客角度，在不影響機關(藍隊)業務運作之前提下，由紅隊在約定之有限時間內，以不限定攻擊手法之方式，協助機關預先發現外部攻擊者可入侵內網之途徑、橫向移動範圍及可取得之資料與系統權限。本章節將介紹弱點掃描、滲透測試及紅隊演練作業方式並進行比較，供機關面臨不同檢測需求時可選擇合適之檢測方式，以達到強化資安防護目的。

### 2.1 弱點掃描

弱點掃描之檢測標的通常為網站、伺服器或網路設備等，運用檢測工具進行大範圍自動化弱點探測，針對已知弱點特徵進行探查，若識別存在相關弱點特徵會搭配弱點資料庫對弱點進行風險等級判定。掃描工具可能出現誤判狀況，此時可輔以人工作業進行結果驗證。

依「112 年共同供應契約資通安全服務品項採購規範」[1]，弱點掃描服務提供主機系統弱點掃描、Web 網頁弱點掃描及網頁個資掃描等項目(詳見表 1)，透過弱點掃描作業協助機關發現安全弱點或個資揭露，提供弱點掃描結果與弱點修補建議，並於協助修補弱點後提供複測，以確認已經完成修正。

表1 弱點掃描服務

弱點掃描服務	說明	服務方式
主機系統弱點掃描	針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設	<ul style="list-style-type: none"><li>▪ 到場/遠端掃描</li><li>▪ 自動化工具/人工掃描</li></ul>

弱點掃描服務	說明	服務方式
	定、帳號密碼設定及管理方式等進行弱點掃描	
Web 網頁弱點掃描	針對機關網頁安全弱點進行掃描，掃描項目應符合 OWASP TOP 10 項目	<ul style="list-style-type: none"> <li>▪ 到場/遠端掃描</li> <li>▪ 自動化工具/人工掃描</li> </ul>
網頁個資掃描	針對機關對外網頁與網頁中之 doc(x)、xls(x)、ppt(x)、pdf、csv 等類型檔案，可能存在之個人資料進行掃描，掃描個資特徵應至少包含中文姓名、地址、電話(含市話/手機)、電子郵件信箱、中華民國身分證字號、健保卡號、護照號碼及信用卡號等個人資料掃描	<ul style="list-style-type: none"> <li>▪ 到場掃描</li> <li>▪ 自動化工具/人工掃描</li> </ul>

資料來源：112 年共同供應契約資通安全服務品項採購規範[1]

一般弱點掃描整體流程會從確認掃描標的開始，分成初測與複測階段，當完成初測報告後，將檢測報告提供給受測單位，待受測單位完成弱點修補後，再執行複測作業，以確保受測單位針對初測報告中發現之弱點已確實修補完成，弱點掃描作業流程詳見圖 1。



資料來源：本計畫整理

圖1 弱點掃描作業流程

## 2.2 滲透測試

滲透測試係透過模擬有心人士之攻擊方式，對目標主機或網路服務進行安全強度的測試，以找出可能的資安弱點，並提出改善建議，並於協助修正資安弱點後提供複測，以確認已經完成修正。

滲透測試之檢測方式較專注於特定資通系統、應用程式或設備之弱點利用，通常檢測範圍為一至數個標的，主要模擬實際駭客行為對標的進行檢測，檢測人員透過資訊蒐集進一步挖掘標的潛在之弱點，並搭配半自動化或特定攻擊程式，實際利用弱點以達到確認弱點存在之目的。

依「112 年共同供應契約資通安全服務品項採購規範」[1]，滲透測試可分為系統滲透測試與物聯網設備滲透測試，系統滲透測試分為作業系統、網站服務、應用程式及密碼破解等測試類型，詳見表 2，物聯網設備滲透測試則分為系統、網站服務、應用程式、密碼破解及無線服務等測試類型，詳見表 3。

表2 系統滲透測試項目

測試類型	測試類別	測試項目
作業系統	遠端服務	在到現場提供服務的條件下，可執行無線服務弱點測試項目
	本機服務	在已取得系統控制權限的條件下，可執行至少包含本機服務套件弱點測試等項目
網站服務	設定管理	至少包含應用程式設定測試、檔案類型處理測試、網站檔案爬行測試、後端管理介面測試及 HTTP 協定測試等項目
	使用者認證	至少包含機敏資料是否透過加密通道進行傳送與使用者帳號列舉測試等項目
	邏輯弱點	至少包含網站功能測試、網站功能設計缺失測試及附件上傳測試等項目
	輸入驗證	至少包含 XSS 弱點測試、SQL Injection 測試、LDAP Injection 測試、XML Injection 測試、SSI Injection 測試、XPath Injection 測試、OS Commanding 測試、偽造 HTTP 協定測試等項目及 Code Injection 測試等項目
	Web Service	至少包含 WSDL 測試、XML 架構測試、XML 內容測試及 XML 參數傳遞測試等項目
	Ajax	至少包含 Ajax 弱點測試等項目，如輸入驗證缺失、權限控管及套件弱點等測試項目

測試類型	測試類別	測試項目
應用程式	電子郵件服務套件	至少包含 SMTP、POP3 及 IMAP 等常見對外郵件服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	檔案傳輸服務套件	至少包含 FTP、NETBIOS 及 NFS 等常見檔案傳輸服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	遠端連線服務套件	至少包含 SSH、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	網路服務套件	至少包含 DNS、PROXY 及 SNMP 等常見網路服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	其他	包含 Firewall、IDS/IPS、Database、LDAP、SMB、LPD、IPP、Jetdirect 及 RTSP 等常見應用程式或網路套件之弱點檢測項目
密碼破解	密碼強度測試	至少包含 WEB、FTP、SSH、TELNET、SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC 及 Database 等常見對外服務之密碼字典檔測試，在到場服務之條件下，可執行 WiFi 密碼字典檔測試

資料來源：112 年共同供應契約資通安全服務品項採購規範[1]

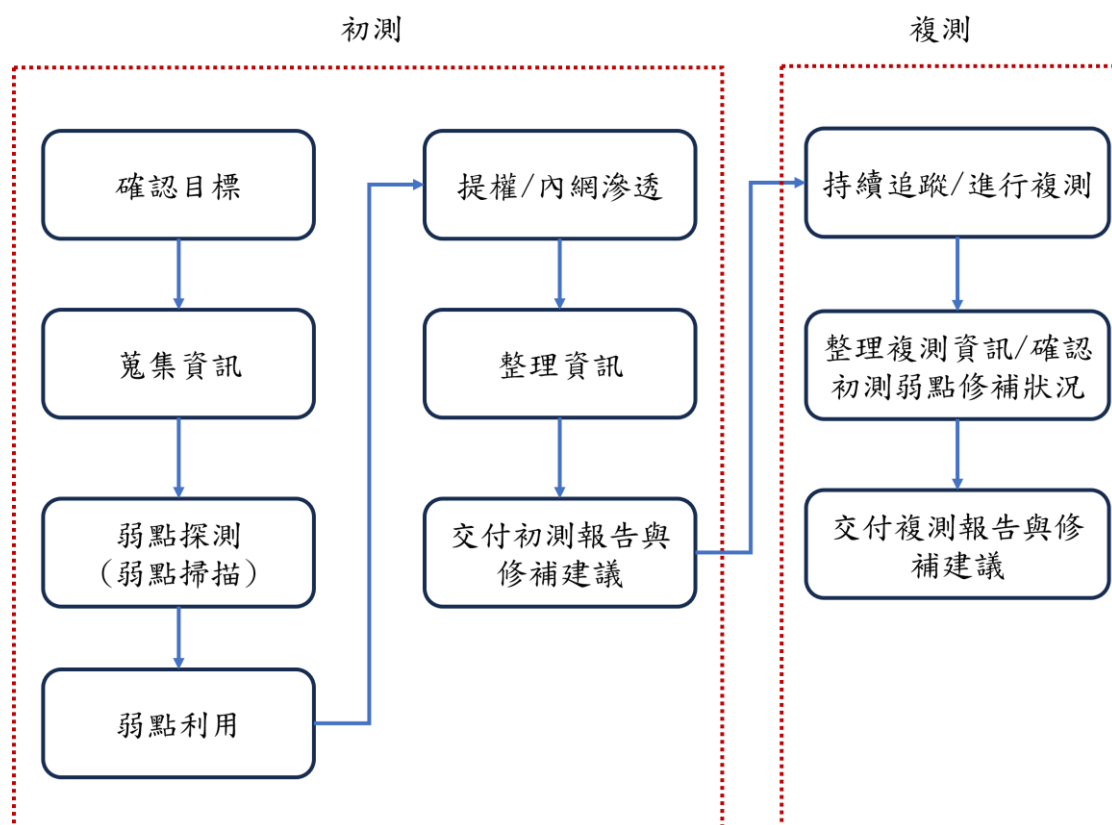
表3 物聯網設備滲透測試項目

測試類型	測試類別	測試項目
系統	本機服務	針對物聯網設備與管理主機，執行服務套件弱點測試等項目
網站服務	設定管理	包含應用程式設定測試、網站檔案爬行測試、後端管理介面測試及 HTTP 協定測試等項
	使用者認證	包含機敏資料是否透過加密通道進行傳送及使用者帳號列舉測試等項目
	連線管理	包含 Session 管理測試、Cookie 屬性測試、Session 資料更新測試及 Session 變數傳遞測試等項目
	使用者授權	包含目錄跨越測試、網站授權機制測試及權限控管機制測試等項目
	邏輯弱點	包含網站功能測試、網站功能設計缺失測試及附件上傳測試等項目
	輸入驗證	包含 XSS 弱點測試、SQL Injection 測試及 Code Injection 測試等項目
應用程式	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	遠端連線服務套件	包含 SSH、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	其他	包含 SMB、LPD、IPP、Jetdirect、SNMP 及 RTSP 等常見應用程式或網路套件之弱點掃描項目
密碼破解	密碼強度測試	包含 WEB、FTP、SSH、TELNET、RDP、VNC 等常見對外服務之密碼字典檔測試

測試類型	測試類別	測試項目
無線服務	無線服務弱點測試	針對無線網路基地台/無線路由器設備，執行包含無線服務套件弱點測試、無線通訊協定及 WiFi 密碼字典檔測試等項目

資料來源：112 年共同供應契約資通安全服務品項採購規範[1]

滲透測試執行過程中，會經歷確認目標、蒐集資訊、弱點探測及弱點利用等階段，再依專案需求與目標進行提權或內網滲透，以達到獲取目標機敏資訊或取得控制權等目的，在此過程中也會執行弱點掃描作業以獲取標的之弱點資訊，滲透測試之流程詳見圖 2。



資料來源：本計畫整理

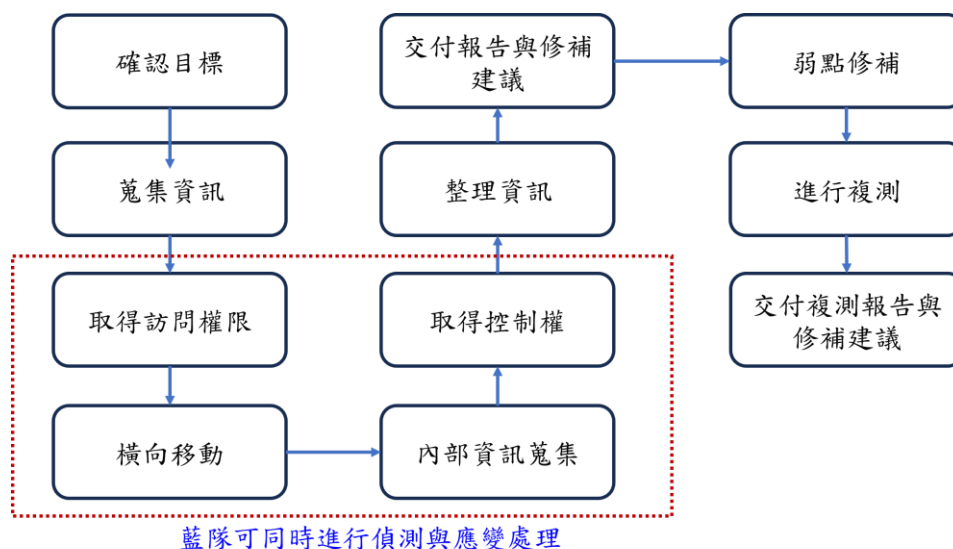
圖2 滲透測試作業流程



## 2.3 紅隊演練

紅隊演練之主要目的係希望藉由模擬實際攻擊之戰略、技術及流程 (Tactics, Techniques, and Procedures, TTP)，找出機關整體資安問題，並確認遭受攻擊時之應變能力，藉由改善機關之人員、流程及技術，以提升資安準備度並降低整體資安風險。相較前兩者，紅隊演練是更全面之檢測方法，檢測標的通常不是單一系統或設備，而是整體機關，檢測方式大都包含多個攻擊面向，包括社交工程、外部與內部攻擊及應用程式弱點等，以檢視受測目標營運上可能存在之資安風險，並檢視受測目標防禦機制有效性，以持續提升資安防護能力[2][3]。

紅隊演練過程包含確認目標、資訊蒐集、取得訪問權限、橫向移動、內部資訊蒐集及取得控制權等。與前2項檢測不同之處在於，演練過程中機關扮演藍隊角色，可依照專案需求與內部作業程序，針對演練攻擊行為依進行偵測、通報及應變等防禦作為，檢測過程中可由機關內部資安人員針對演練之攻擊行為作出偵測與應變處理，有關紅隊演練之作業流程詳見圖3。



資料來源：本計畫整理

圖3 紅隊演練作業流程

## 2.4 檢測方式比較

綜上所述，弱點掃描主要用於快速且大量識別系統或應用程式中已知弱點；滲透測試則由具駭客能力之專業人員模擬攻擊者行為，試圖入侵系統或機關內部網路，尋找弱點並加以利用，進一步取得系統權限或機敏資訊，以衡量可造成之危害；紅隊演練則由專業演練團隊模擬攻擊，找出機關整體安全性問題並確認遭受攻擊時之應變能力。此三者之目的、方法、範圍及時間上皆有不同，有關三種檢測之比較內容詳見表 4。

表4 弱點掃描、滲透測試及紅隊演練比較

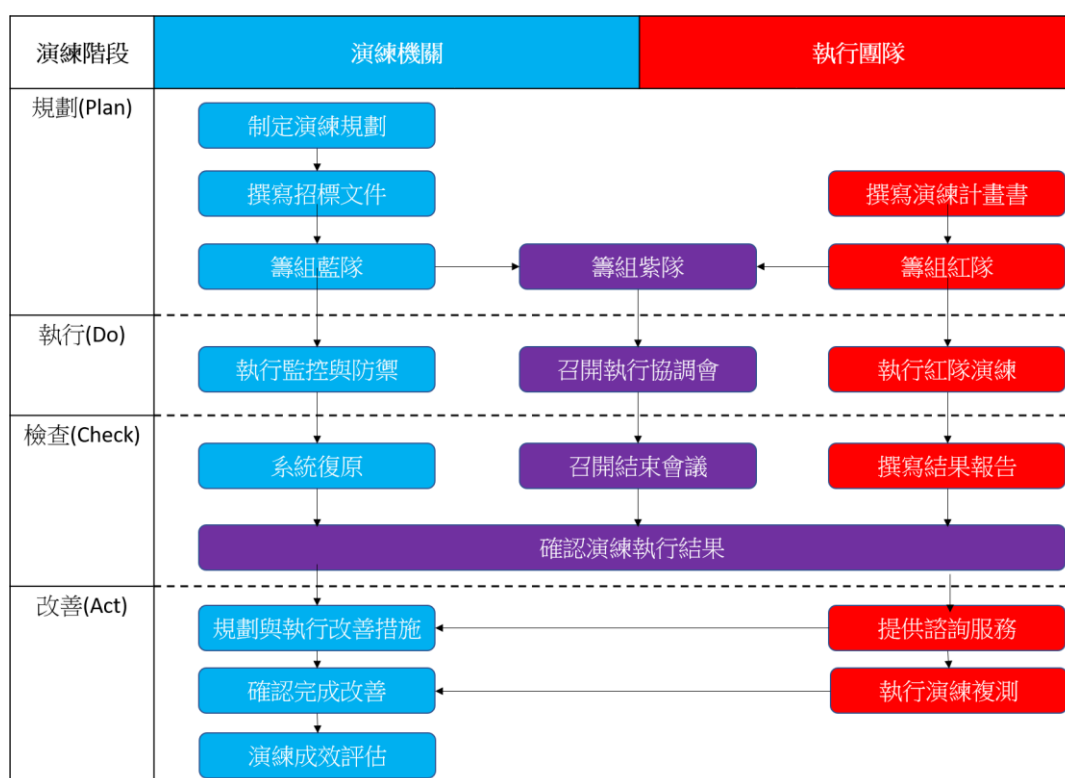
檢測方式 項目	弱點掃描	滲透測試	紅隊演練
目的	主要用於快速且大量識別系統、應用程式或設備之已知弱點	由具駭客能力之專業人員模擬攻擊者行為，試圖找出所有已知與未知之弱點並進行弱點利用，以確認可能造成之危害	由專業演練團隊模擬實際攻擊之戰略、技術及流程，找出機關整體資安問題，並確認遭受攻擊時之應變能力，藉由改善人員、流程及技術，以提升資安準備度並降低整體資安風險
檢測方法	執行自動化工具進行掃描	具駭客思維與能力之專業人員模擬攻擊	專業演練團隊模擬攻擊
工具/手動檢測	100%採用工具	約 10%採用工具，90%採手動檢測	以手動檢測為主，偶有搭配紅隊自動化工具
範圍	單一系統之已知弱點	單一系統或網路之已知或未知弱點	演練機關整體(含設備、系統、網路、人員及作業流程等)

<div> <div>項目</div> <div>檢測方式</div> </div>	弱點掃描	滲透測試	紅隊演練
執行頻率	每季或每半年執行 1 次	每年執行 1 次	每 1~2 年執行 1 次
每次執行所需時間	數日	1~2 週	1~6 月

資料來源：[2][3]

### 3. 紅隊演練作業管理程序

紅隊演練作業採用規劃(Plan)、執行(Do)、檢查(Check)及改善(Act)四大管理循環流程(詳見圖 4)，由內部自我分析需求與目標，規劃、評估及選擇合適之識別與鑑別方式，分析使用環境，進行系統測試，最後對整體流程進行監控與維護，隨環境變化持續改進。本章將介紹紅隊演練各階段之管理程序與作業內容。



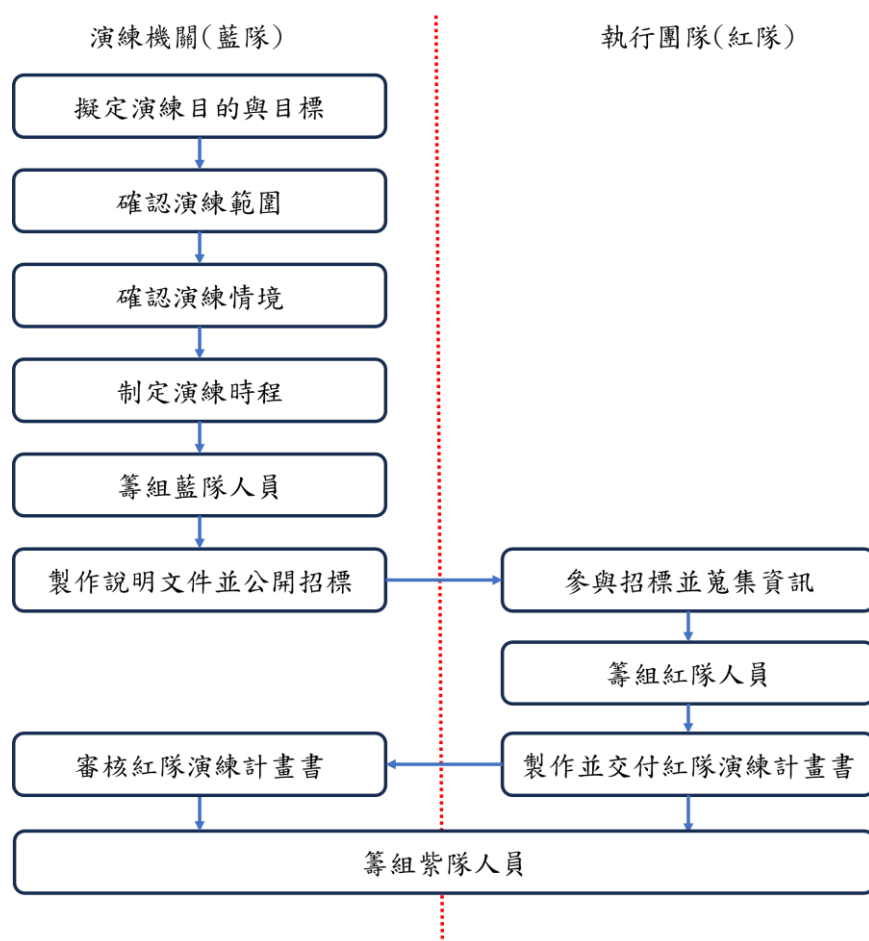
資料來源：本計畫整理

圖4 紅隊演練流程

#### 3.1 規劃階段

紅隊演練作業規劃階段應擬定紅隊演練相關演練時程、範圍、人員組成、情境及文件交付等相關內容，除使機關可了解紅隊演練應包含之作業項目外，亦可供後續撰寫委外招標說明文件之用。確認得標廠商後，得標廠商

除扮演執行團隊之角色，應與機關就紅隊演練內容進行充分溝通與協調，確認各項演練作業細節認知一致，據以撰寫紅隊演練計畫書，以期可如期如質完成演練作業。演練機關(藍隊)與執行團隊(紅隊)於規劃階段應執行之作業流程詳見圖 5。



資料來源：本計畫整理

圖5 規劃階段細部流程

### 3.1.1 擬定演練目的與目標

機關確定要委外執行紅隊演練時，須先釐清執行紅隊演練之目的，以及欲達成之演練目標，演練目標通常可設定為控制特定帳號、取得特定資料、控制特定伺服器及入侵特定主機或位置。

### 3.1.2 確認演練範圍

確認演練目標後，機關接續依該目標與需求確認紅隊演練之範圍，以確保有效評估安全性並滿足機關特定之測試要求。一般應包含演練機關所有人員與擁有之資訊資產但不限於以下範圍：

- 硬體資產：如伺服器、防火牆、入侵防護系統及員工個人電腦等。
- 軟體資產：如作業系統、自行開發之應用程式及套裝軟體等。
- 資訊：如數位與紙本文件資訊等。
- 人員：如正式員工、約聘人員及工讀生等。

### 3.1.3 確認演練情境

紅隊演練通常設計成模擬真實攻擊之情境，以測試機關整體資安防護安全性與應變處置能力。紅隊演練作業情境可以根據機關需求與組織現況而採用不同之演練情境執行。一般紅隊演練之執行，至少包含外部入侵與內部網路滲透，以下依一般機關優先順序羅列，執行紅隊演練時可結合數種情境進行演練：

#### ●外部入侵

模擬外部攻擊者由外部試圖入侵機關之內部網路，例如透過對外服務或系統之弱點或社交工程等攻擊。紅隊成員可能試圖入侵內部系統、竊取敏感資訊或取得內部使用者權限等，協助機關評估外部服務防護之有效性。

#### ●內部網路滲透

紅隊可以試圖進入內部網路，然後橫向移動，試圖存取其他系統和資源，協助機關評估內部網路之安全性。

- 應用程式弱點

紅隊可以模擬對機關應用程式之攻擊，試圖利用應用程式弱點，協助機關發現與修復弱點，以防止遭攻擊者針對應用程式弱點進行攻擊而造成之危害。

- 雲端安全測試

對於使用雲端服務之機關，紅隊可以模擬攻擊雲端環境，試圖入侵或滲透雲端服務，協助機關評估使用雲端服務之安全性。

- 社交工程攻擊

紅隊成員可以模擬釣魚攻擊、偽裝為受信任的人員或單位，或試圖誘導員工洩漏敏感資訊的攻擊，協助機關評估員工對於社交工程之警覺與資安意識。

- 工業控制系統(ICS)攻擊

對於使用工業控制系統之機關，紅隊可以模擬對 ICS 與 SCADA 系統之攻擊，協助機關評估工業控制系統資通安全防護之安全性。若機關本身有使用該系統建議列為優先演練情境。

- 內部威脅

模擬來自內部使用者的威脅情境進行攻擊，如員工故意或不小心洩漏敏感資訊，或試圖濫用其權限存取應用程式或資源，協助機關評估內部安全控制措施與防護偵測機制之有效性。

- 實體入侵

紅隊可以嘗試模擬進入機關設施之攻擊，如潛入辦公區域或機房等敏感區域，協助機關評估實體安全防護措施之有效性。

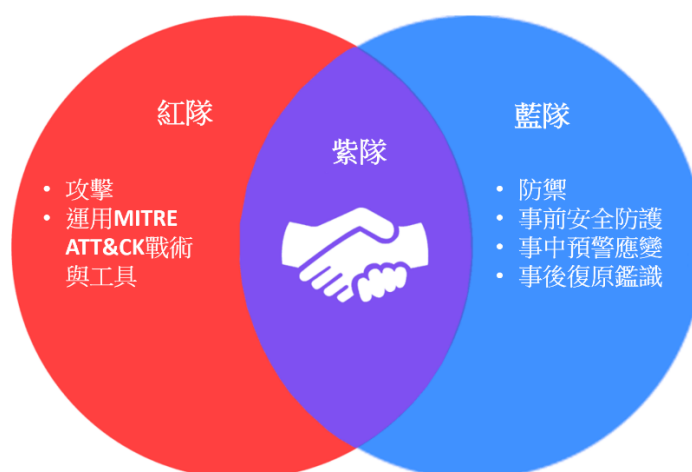
機關可根據自身情況挑選適合之演練情境，如有對外服務並委外開發多項專用軟體時，建議可優先選擇結合外部入侵、內部網路橫向移動及應用程式弱點情境執行紅隊演練。

### 3.1.4 制定演練時程

規劃紅隊演練時程時，除需考量機關需求、資源及規模大小外，亦應評估演練情境複雜度與範圍，以及同時間之業務負擔，並至少包含執行階段與檢查階段所有作業所需時間，如紅、藍隊成員共同確認演練結果，識別弱點與問題，以及撰寫演練執行結果報告等，如欲確實追蹤與掌握演練結果之改善情形，亦可納入改善階段之作業時間。

### 3.1.5 籌組演練團隊

紅隊演練過程中，人員之籌組包含紫隊人員、藍隊人員及紅隊人員[4]，紫隊主要負責整體演練溝通協調任務，並於演練過程進行裁判工作，藍隊人員主要負責演練過程中之監控與防禦，並視演練情境規劃，進行弱點修補與通報應變作業，紅隊人員主要負責執行攻擊，並於演練過程中試圖達成演練目標，並記錄演練過程中之相關軌跡紀錄，詳見圖 6。



資料來源：本計畫整理

圖6 紅隊演練角色



### 3.1.5.1 紫隊人員組成

在演練過程中由於紅隊與藍隊之屬性相異，且績效衡量指標也可能處於對立情況，紅隊與藍隊可能無法順利溝通。因此應以演練機關之資安長或資安單位主管擔任召集人，並結合紅藍兩隊相關成員組成紫隊，讓紅隊與藍隊密切合作，共同參與紅隊演練。紫隊之主要任務為讓雙方可以互相溝通與協調，以找出演練機關潛在威脅。紫隊中之紅隊成員可更加了解演練機關環境架構，而其中藍隊成員可結合原本負責不同面向防護人員進行跨領域合作。當有任何攻擊成功的事件出現時，雙方成員可即時確認，降低偵測與回應時間，使紅隊與藍隊減少對抗而讓紅隊演練作業更具成效[5]。紫隊成員建議包含下列人員：

- 召集人

負責協調紅隊與藍隊之間的活動，確保資訊流通，並協助在弱點發現與修補方面之合作。當紅藍隊有爭議時，作為裁決角色。通常由演練機關資安部門最高負責人擔任。

- 執行秘書

負責將安全測試結果以清晰、易懂之方式報告給組織管理層。這有助於理解潛在風險與後續改善方式。

- 原紅藍隊成員中各分項之資深人員

紫隊中之紅隊成員應至少由專案經理與一名以上執行成員組成，藍隊成員則以資安主管與一名以上分項執行人員組成，紅藍隊成員以紅藍隊各分項有負責人員可說明情況並溝通為原則，無組成比例限制，若紅藍隊成員有資深人員同時兼任兩個以上分項作業，可同時擔任各分項協調人員。

### 3.1.5.2 藍隊人員組成

藍隊是機關之內部安全團隊，負責監控、保護及應對資通系統與資料之安全威脅[6]，主要人員職責與功能如下：

- 監控安全事件人員

負責監控機關之網路流量、系統日誌、警報及其他安全事件，以檢測潛在之威脅與攻擊。

- 威脅檢測人員

藍隊使用入侵偵測系統(IDS)、入侵防禦系統(IPS)及安全資訊與事件管理(SIEM)工具等來檢測異常活動與潛在之威脅。

- 威脅分析人員

分析機關資通安全事件與告警，以確定相關事件與告警是否構成威脅，並評估威脅之嚴重程度。

- 應變處置人員

當檢測到潛在威脅時，採取應變措施來應對威脅，包括隔離受感染系統、調查事件及採取必要之修復措施。

- 弱點管理人員

負責識別機關擁有系統與應用程式中之弱點，並推動修復弱點之流程。

- 復原與應變計畫人員

協助制定應變計畫，以應對故障、攻擊及災難，並測試計畫之有效性。

藍隊人員組成可根據演練機關人力配置情形，考量以原有人員或安排專人擔任，同時亦可由委外廠商協助負責擔任部分項目人員。上述分項人員可由其他分項人員兼任。

機關可根據自身需求，於演練過程中指定藍隊可執行之應變措施，例如僅執行監控而不進行威脅反應與系統修復，以利紅隊能更深入發掘機關之潛在風險。機關可根據自身藍隊能力與演練經驗採取不同演練方式如下：

- 藍隊僅監控攻擊

第一次執行紅隊演練之演練機關建議採取此措施，可讓機關了解紅隊演練之完整攻擊方式，同時避免因藍隊反應過度而執行過度防禦措施(如封鎖所有外來網路流量)導致演練無法順利執行。

- 藍隊可封鎖攻擊來源或修補弱點

藍隊根據自身監控蒐集之資安事件進行分析，可針對當前之攻擊來源進行封鎖、修補弱點且監控攻擊事件是否持續發生。

- 藍隊可調整內部網路架構

藍隊可根據攻擊事件分析攻擊手法，除了修補弱點以外可藉由調整內部架構(如更改受攻擊目標 IP 或網段)以減少受攻擊成功之可能。但此作法應與紅隊事先討論是否會造成演練執行上之困難。

### 3.1.5.3 紅隊人員組成

紅隊人員為紅隊演練執行單位進行編組，演練機關於演練需求說明書中可先針對執行單位進行資格要求，透過以下之要求確保執行單位之品質[7]。

- 本國登記合格之廠商。
- 服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士，亦不得有犯罪紀錄。
- 服務內容涉及敏感資訊，廠商不得轉包或分包其他廠商執行。
- 服務人員須為執行廠商之正式員工，並須檢附成員姓名、在職一年以上

之在職證明、相關工作經驗證明文件、訓練證書或專業證照等以供審查。

紅隊人員通常由多位成員組成，每位成員需擁有特定之專業知識與技術以模擬不同類型之攻擊。建議包含以下各領域之專業人員，一般紅隊成員組成最少包含專案管理人員與紅隊演練檢測人員：

- 專案管理人員

具備 PMP 或 CISM 等證照，負責協調整個紅隊演練、制定演練計畫與訂定目標，並協調紅隊成員之作業方式、內容及演練後之執行結果報告撰寫。

- 紅隊演練檢測人員

具備 CPENT、CPSA 或 OSCP 等證照，同時有多年相關工作經歷，具備專業駭客思維與能力，能模擬各式滲透攻擊以發掘系統或網路中潛在威脅。此項為演練優先情境之需求人員，建議紅隊團隊應具備至少三張以上專業證照。

- 網路工程師

具備 CCNA 或 CCNP 等證照，負責探索演練機關之網路架構，發現網路架構中可能存在之弱點或入侵點。

- 資訊蒐集人員

負責在演練初期蒐集演練機關之相關資訊，包含機關人員資訊、採購設備、軟體資訊、供應商或組織架構等資訊，以利演練作業執行。

- 應用程式檢測人員

檢測演練機關使用之應用程式與軟體安全性，以發現程式可利用之弱點。

●社交工程測試人員

負責模擬社交工程攻擊，試圖通過與演練機關人員之交流來獲取資訊、取得存取權限及植入惡意程式。

●實體安全測試人員

透過實體入侵之方式取得機敏資訊或植入惡意程式以取得控制權限。

●雲端安全測試人員

具備 CCSP 證照，可以滲透雲端服務，取得相關資訊甚至進行雲端跳躍手法攻擊演練機關。

●曾任職相關產業人員

根據自身經驗提供類似機關業務執行或規範限制可能存在之弱點。

除上述紅隊人員資格要求外，演練機關亦可依照檢測需求額外進行紅隊人員之相關能力要求，可參考但不侷限下表，選擇 1 至多項作為人員能力要求，詳見表 5。

表5 紅隊人員額外資格要求

項次	資格要求
1	具備尋找零時差弱點之能力與實績(如三年內有挖掘國際知名產品 CVE 弱點之證明或佐證，且 CVE 弱點之 CVSS 3 分數需達 8.0 分以上)
2	3 年內曾執行至少 5 件以上之紅隊演練專案，且專案規模至少達新臺幣 300 萬元以上
3	團隊成員近三年至少需有 1 位專案團隊成員曾參與國際 CTF 比賽，如 DEFCON CTF 等，且獲得前三名

項次	資格要求
4	具備弱點研究能力，曾於國際知名研討會發表研究成果(如 HITCON、Black Hat、DEF CON、CODE BLUE、CODEGATE 等)
5	曾參與國際企業 Bug Bounty 計畫且獲得獎勵

資料來源：本計畫整理

### 3.1.6 撰寫招標說明文件

演練機關應針對演練專案公開招標提供專案說明文件(詳見附件 1)，內容應包含但不限於以下項目：

#### ●專案概述

##### －專案目標

機關應根據欲驗證之項目詳列目標，如外部威脅、內部威脅、社交工程攻擊及雲端安全等。

##### －演練範圍

一般應為機關全體資產，可視需求增加利害關係人等。

##### －專案期間

應至少包含執行團隊得標後至執行階段、檢查階段各項作業所需時程。

#### ●工作項目

##### －演練方式

詳列可使用或禁止使用之演練攻擊方式。

##### －各階段時程

包含事前準備、演練執行、演練期間討論會議及期中/期末報告繳交等。

- 管理需求

- －團隊資格

- 紅隊成員之負責項目與人員列表。

- －相關證明資料

- 成員專業證照、工作經歷、曾獲得之知名競賽獎項、曾發表之相關研究論文及曾執行之紅隊演練專案。

- －服務水準協定(SLA)與罰則

- 專案廠商根據服務水準協定應詳列之資訊，若與協定不合或有執行逾期之情況應訂定相關罰則。

- －預算經費

- 專案之經費總額與各項經費標準。

- 交付項目

- －預期效益分析

- 廠商應於繳交計畫書時提供專案預期效益分析，即專案可為機關發現之潛在風險。

- －報告書

- 報告書應詳列檢測發現之弱點項目，並與預期效益分析比對是否達成標準。

- 其他

演練機關根據自身情況增加要求說明之項目。

### 3.1.7 交付紅隊演練計畫書

得標之紅隊演練執行團隊應於得標後兩週內，與演練機關協調演練執行內容並交付演練計畫書，以作為後續執行演練之依據，內容包含：

- 簡介

演練的目的、演練的範圍、主要目標及期望結果。

- 演練概述

演練日期、時間及地點、參與人員名單(紅隊成員、藍隊成員及其他相關方)、演練之背景與情境描述、相關法規、標準及合規性要求。

- 演練目標與範圍

明確定義演練之目標、描述攻擊面向及情境，包括攻擊目標、攻擊方式及攻擊目的。

- 準備與資源

準備演練環境之步驟、所需的工具及紅隊成員之培訓與技能需求。

- 時程與計畫

詳細之演練時程表，包括開始與結束時間，不同階段之演練時程如攻擊、分析及報告撰寫等，指定負責人員與提供聯絡方式。

- 演練執行

描述攻擊與演練之實際步驟、以及攻擊軌跡監控與記錄方式及於演練過程中如何報告演練進展。

- 事後分析與報告



說明演練完成後事後分析之流程、撰寫演練報告之架構與內容，以及建立演練報告撰寫時程表與交付日期。

- 演練評估與改進

預先評估演練可能之效果，以及後續如何提供改善建議與措施。

- 附件

任何附加資料，如演練模擬攻擊面向之詳細資訊、技術參考及相關法規文件等。

### 3.1.8 審核紅隊演練計畫書

演練機關於收到計畫書後應由負責防禦之藍隊與紅隊召開討論會議，確認是否符合機關需求或討論演練過程中有可能影響正常業務執行之處，詳細確認雙方作業方式與配合方式。

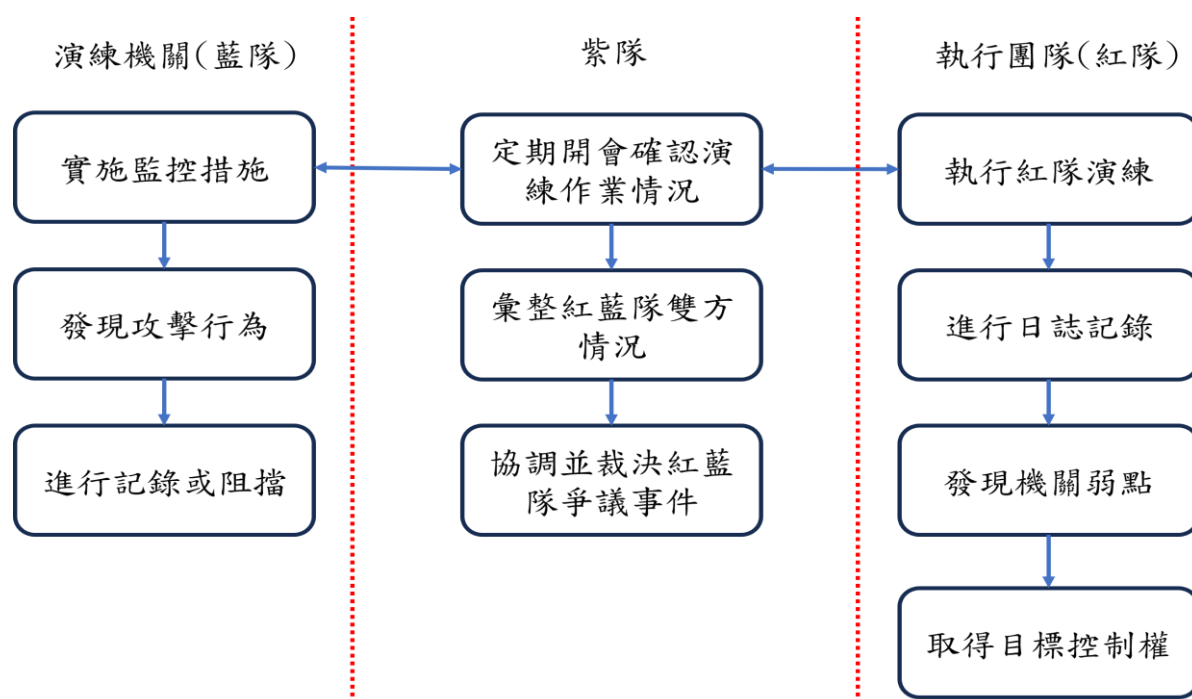
## 3.2 執行階段

本章節說明紅隊演練作業執行時之測試流程與演練機關之應對行動(詳見圖7)。在執行階段，紅隊應以達成擬定之控制特定帳號、取得特定資料、控制特定伺服器或入侵特定主機等演練目標，據以執行紅隊演練，演練攻擊方式可參考 MITRE 之 ATT&CK 框架。紅隊攻擊者在過程中可依照查核表詳細記錄攻擊成功佐證，過程中如攻擊行為可能影響演練機關業務正常運作時，應先行與演練機關確認，獲得同意後方可執行。

演練機關應依照演練需求，決定藍隊採取之監控或防禦模式。機關初次執行演練時建議先以只採取監控模式確認機關偵測威脅能力，並了解紅隊演練可能使用之技術；非初次執行之機關可根據藍隊自身防禦能力評估採取防禦模式。

在演練執行過程中，演練機關與演練團隊有任何爭議應透過紫隊討論裁

決，雙方應以徹底發掘風險並加以改善作為演練共同目標。



資料來源：本計畫整理

圖7 執行階段細部流程

MITRE 是一家美國非營利組織，除協助進行多項資安相關研究，同時也負責維運 CVE 弱點資料庫，相關網路安全之重要研究成果包括資安弱點情資分享、資安威脅情資分享及管理 CVE、CWE 及 CAPEC 網站。

MITRE 於 104 年 5 月發起 ATT&CK 框架之研究計畫，主要是希望建立一個可供全球自由運用，基於真實世界所觀測到之攻擊戰術與技術之知識庫。2023 年 10 月發布之 ATT&CK 知識庫 v14 版內含 14 種網路攻擊戰術與 234 種技術，可被運用在開發政府、企業及網路各項安全產品與服務中之特定威脅模型與方法[8]。本指引參考 MITRE ATT&CK 將演練作業流程分為偵察(Reconnaissance)、資源開發(Resource Development)、初始存取(Initial Access)、執行(Execution)、持續(Persistence)、提權(Privilege Escalation)、避免偵測(Defense Evasion)、憑證存取(Credential Access)、發

現(Discovery)、橫向移動(Lateral Movement)、蒐集(Collection)、命令與控制(Command and Control)、滲漏(Exfiltration)及影響(Impact)等 14 個戰術。有關 14 種網路攻擊戰術與 234 種技術可依照受測範圍與演練情境彈性選擇相關應用。

- 偵察(Reconnaissance)

透過搜尋、掃描及網路釣魚等方式蒐集資訊。

- 資源開發(Resource Development)

紅隊攻擊者自行開發、購買及竊取可用於支援目標資源之技術。

- 初始存取(Initial Access)

透過預設帳戶與網路釣魚等方式以獲得初始立足點。

- 執行(Execution)

執行惡意指令或程式。

- 持續(Persistence)

透過更改憑證或重新啟動等方式維持攻擊者之存取權限。

- 提權(Privilege Escalation)

利用系統弱點、錯誤配置及弱點取得更高等級權限。

- 避免偵測(Defense Evasion)

利用停用防護軟體與混淆資料等方式以避免被偵測。

- 憑證存取(Credential Access)

竊取帳戶名稱與密碼等憑證之技術。

●發現(Discovery)

獲取有關帳戶、系統、內部網路及雲端服務等相關資訊。

●橫向移動(Lateral Movement)

尋找其他系統、資源或權限，以擴大其攻擊範圍與提高其在受感染環境中之控制權限

●蒐集(Collection)

透過中間人攻擊、資料庫及雲端服務等蒐集資訊。

●命令與控制(Command and Control)

攻擊者對已受感染系統進行控制。

●滲漏(Exfiltration)

攻擊者將資料傳送至指定目的地。

●影響(Impact)

操縱、中斷或破壞系統之可用性與資料完整性。

上述各種戰術在執行過程中可結合各種攻擊技術以獲得完整之攻擊成果，詳細之戰術與技術搭配詳見表 6。

表6 MITRE ATT&CK 技術列表

戰術	技術	描述
偵察	主動掃描	執行主動偵察掃描來蒐集可用資訊，主要是透過網路流量探測目標機關之基礎設施
	蒐集目標主機資訊	蒐集有關目標主機資訊(包含主機名稱、作業系統及 IP 等)

戰術	技術	描述
	蒐集目標身分資訊	蒐集機關之員工個人資料
	蒐集目標網路資訊	蒐集目標之網路資訊(包含 IP 範圍、網域名稱及拓撲等)
	蒐集機關資訊	蒐集有關目標之機關資訊(包含部門的名稱、業務運營之具體情況及關鍵員工之角色與職責)
	利用網路釣魚獲取資訊	試圖誘騙目標洩露訊息，通常是憑證或其他可利用之資訊
	購買資訊	從威脅情報供應商或購買目標資訊
	搜尋開放技術資料庫	搜尋技術資料庫，以獲取資訊，例如網域、憑證及蒐集之網路資料
	搜尋開放網站/網域	免費搜尋可用之網站與/或網域(如社群平台)，以獲取目標資訊
	搜尋目標擁有的網站	搜尋目標擁有之網站，以獲取資訊
資源開發	取得存取權限	以購買或以其他方式取得對目標系統或網路之現有存取權
	取得基礎設施	購買或租用可使用之基礎設施或雲端服務
	洩漏帳戶	透過社交工程等方式攻擊與目標有關係帳號，並進一步取得目標信任
	損害基礎設施	攻擊定位目標過程中使用之第三方基礎設施(包含網域、DNS、伺服器及網頁服務等)
	發展能力	建立惡意軟體、漏洞利用和自簽章憑證等以供後續使用
	建立帳戶	建立角色以進行進一步操作之帳戶(社群媒體、電子信箱及雲端帳戶等)

戰術	技術	描述
	獲得能力	透過購買、免費下載或竊取惡意軟體、漏洞利用、憑證以及與漏洞相關之資訊
	階段能力	透過上傳、安裝、惡意連結或以其他方式取得控制第三方基礎設施之能力
初始存取	內容注入	透過線上網路流量將惡意內容注入系統來獲得存取權限並持續與目標進行通訊
	路過式攻擊	透過使用者在正常瀏覽過程中造訪網站來存取系統
	利用應用程式	利用面向網路之主機或系統弱點以進行網路存取
	外部遠端服務	利用遠端服務以進行網路存取
	硬體增加	透過增加新的設備以作為獲取存取權限之媒介
	網路釣魚	透過網路釣魚訊息來獲取目標系統之存取權限
	透過可移動介質複製	透過將惡意軟體複製到可移動介質並在介質插入系統並執行時利用自動運行功能來轉移到系統上
	供應鏈攻擊	透過修改供應鏈中的軟體或硬體以獲取最終產品存取權限
	信賴關係	攻擊或以其他方式利用有權接觸目標的機關，進一步獲取存取權限
	有效帳戶	攻擊者可能會取得並濫用現有帳戶的憑證，作為獲得初始存取、持久性、權限升級或防禦規避之手段
執行	雲端管理命令	利用雲端管理服務在虛擬機器或混合連接裝置內執行命令

戰術	技術	描述
	命令和腳本直譯器	利用命令和腳本解釋器來執行命令、腳本或二進位檔案
	容器管理命令	利用容器管理服務以在容器內執行命令
	部署容器	部署新容器來執行與特定映像或部署關聯的程序，例如執行或下載惡意軟體之程序
	利用客戶端執行	利用客戶端應用程式之軟體漏洞來執行程式碼
	程序間通訊	利用程序間通訊(IPC)機制來執行本機程式碼或命令
	原生 API	利用與本機作業系統應用程式介面(API)互動來執行之行為
	計畫任務/作業	利用任務排程功能來執行惡意程式碼
	無伺服器執行	利用無伺服器運算、整合及自動化服務在雲端環境中執行任意程式碼
	共享模組	透過載入共享模組來執行惡意程式
	軟體部署工具	存取並使用安裝在目標網路內之第三方軟體套件(例如管理、監控及部署系統)，以在網路中橫向移動
	系統服務	利用系統服務或保護程式來執行命令或程式
	使用者執行	透過目標使用者之特定操作，如開啟惡意文件檔案或連結等方式執行惡意程式碼
	Windows 管理工具	利用 Windows Management Instrumentation(WMI)來執行惡意命令
持續	帳戶操縱	透過修改憑證或權限群組來操縱帳戶以維持或提升對目標系統之存取權限

戰術	技術	描述
	後台智慧傳輸服務	利用後台智慧傳輸服務作業來持續執程式碼並執行各種後台任務。Windows 後台智慧傳輸服務是一種透過元件物件模型公開之低頻寬、非同步檔案傳輸機制
	引導或登入自動啟動執行	系統啟動或登入期間自動執行程序，以維持持續性或在受感染之系統上獲得更高級別權限
	啟動或登入初始化腳本	利用在啟動或登入初始化時自動執行之腳本來建立持續存取連線
	瀏覽器擴充	利用網路瀏覽器擴充功能來建立對目標系統之持續存取連線
	洩漏客戶端軟體二進位檔案	修改客戶端軟體二進位檔案以建立對系統之持續存取連線
	建立帳戶	建立本機帳戶、網域帳戶或雲端帳號來維持對目標系統之存取
	建立或修改系統程序	建立或修改系統級程序來重複執行惡意程式
	事件觸發執行	使用基於特定事件觸發執行之系統機制來建立持續性或提升權限
	外部遠端服務	利用對外遠端服務來達成存取並持續留在網路中
	劫持執行流程	透過劫持作業系統運行程式之方式來執行惡意程式
	內部容器植入	在雲端或容器映像中植入惡意程式碼，以在獲得環境存取權限後建立持續存取連線
	修改認證流程	修改身分驗證機制與流程來存取使用者憑證或啟用對帳戶之未經授權存取



戰術	技術	描述
	Office 應用程式啟動	基於 Microsoft Office 應用程式漏洞實現持續存取連線
	電源設定	藉由削弱系統休眠、重新啟動或關閉之功能，以擴大對受感染主機之存取範圍
	預先作業系統啟動	利用預操作系統啟動機制(如韌體和各種啟動服務)在系統上建立持續存取連線
	計畫任務/作業	利用任務排程功能重複執行惡意程式碼
	伺服器軟體元件	利用伺服器之合法可擴展開發功能來建立對系統之持續存取連線
	流量訊號	使用流量訊號來隱藏開放連接埠或用於持續性或命令與控制之其他惡意功能
	有效帳戶	攻擊者可能會取得並濫用現有帳戶憑證，作為獲得初始存取、持久性、權限升級或防禦規避之手段
提權	濫用提權機制	利用內建控制機制來提升系統權限
	存取令牌操縱	修改存取令牌執行操作並繞過存取控制
	帳戶操縱	透過修改憑證或權限群組來操縱帳戶，提升對目標系統之存取權限
	引導或登入自動啟動執行	配置系統設定以在系統啟動或登入期間自動執行程序，在受感染的系統上獲得更高級別權限
	啟動或登入初始化腳本	使用在啟動或登入初始化時自動執行之腳本來建立持續存取連線
	建立或修改系統程序	建立或修改系統級程序來重複執行惡意負載，當作業系統啟動時，可以啟動執行後台系統功能之程序

戰術	技術	描述
	網域策略修改	修改網域設定以提升網域環境中之權限
	跳脫主機	突破容器來存取底層主機，從主機層級或主機本身存取其他容器化資源
	事件觸發執行	基於特定事件觸發執行與系統機制來建立持續性管道與提升權限
	利用權限升級	利用程式漏洞來嘗試提升權限
	劫持執行流程	透過劫持作業系統運行程式之方式來執行惡意程式
	程序注入	將程式碼注入程序中，以逃避程序之防禦並盡可能提升權限
	計畫任務/作業	利用任務排程功能來促進惡意程式碼之初始或重複執行
	有效帳戶	攻擊者可能會取得並濫用現有帳戶之憑證，作為獲得初始存取、持久性、權限升級或防禦規避之手段
避免偵測	濫用提權機制	利用內建控制機制來提升系統權限
	存取令牌操縱	修改存取令牌執行操作並繞過存取控制
	後台智慧傳輸服務	利用後台智慧傳輸服務作業來持續執行程式碼並執行各種後台任務。Windows 後台智慧傳輸服務(BITS)是一種透過元件物件模型公開之低頻寬、非同步檔案傳輸機制
	在主機上建立映像	直接在主機上建立容器映像，以繞過監控從公共註冊表檢索惡意映像之防禦措施
	偵錯工具規避	採用各種手段來偵測和避開除錯器，例如 Black Basta 可以檢查系統標誌、CPU 暫存器、CPU 指令、處理時序、系統函式庫及 API，以確定偵錯器是否存在

戰術	技術	描述
	反混淆/解碼檔案或訊息	攻擊者可以使用混淆之檔案或訊息來隱藏入侵之痕跡以防止分析，欲存取訊息或執行檔案時需要獨特之機制來解碼或反混淆該訊息
	部署容器	部署新容器來執行與特定映像或部署關聯之程序，例如執行或下載惡意軟體之程序
	直接存取磁碟區	Windows 允許程式直接存取邏輯磁碟區，可藉此繞過檔案存取控制和檔案系統監控
	網域策略修改	修改網域之設定以提升網域環境中之權限
	執行護欄	使用執行護欄來根據攻擊者提供之條件與預期目標上出現之環境特定條件來限制執行或操作
	利用防禦規避	利用程式、服務或作業系統軟體或核心本身之程式設計錯誤來執行攻擊者控制的程式碼時，就會發生漏洞，防禦性安全軟體中可能存在漏洞
	檔案和目錄權限修改	修改檔案或目錄權限/屬性來逃避存取控制清單(ACL)並存取受保護之檔案
	隱藏加工	作業系統可能具有隱藏各種工件之功能，例如重要系統檔案與管理任務執行，以避免破壞使用者工作環境並防止使用者更改系統上之檔案或功能，攻擊者可利用這些功能來隱藏檔案、目錄、使用者帳戶或其他系統活動等工件，以逃避偵測
	劫持執行流程	透過劫持作業系統運行程式之方式來執行自己的惡意程式碼
	削弱防禦能力	修改目標環境之元件，以阻礙或停用防禦機制

戰術	技術	描述
	冒充	冒充受信任之個人或機關，以說服與欺騙目標代表他們執行某些操作。例如，攻擊者可能會冒充已知寄件者與目標進行通訊
	指標移除	刪除或修改系統內產生之工具，以消除其存在之證據或阻礙防禦
	間接命令執行	濫用允許命令執行之實用程式來繞過限制命令列解釋器使用之安全限制
	偽裝	嘗試操縱其工具之特徵，使它們對使用者與/或安全工具來說顯得合法或良性
	修改認證流程	修改身分驗證機制與流程來存取使用者憑證或啟用對帳戶之未經授權存取
	修改雲端運算基礎設施	嘗試修改雲端帳戶之運算服務基礎架構以逃避防禦，包括建立、刪除或修改一個或多個元件，例如計算實例、虛擬機器及快照
	修改註冊表	隱藏註冊表項中之配置資訊、刪除資訊或作為其他技術的一部分來幫助持續性與執行
	修改系統映像	更改嵌入式網路設備之作業系統，以削弱防禦並為自己提供新功能
	網路邊界橋接	透過破壞外圍網路設備或負責網路分段之內部設備來橋接網路邊界，使攻擊者能夠繞過流量路由之限制
	混淆的文件或訊息	透過加密、編碼或以其他方式混淆系統上或傳輸中之可執行檔或檔案內容，使可執行檔或檔案難以發現或分析
	屬性清單檔案修改	修改屬性清單檔案(plist 檔案)以啟用其他惡意活動，同時也可能逃避與繞過系統防禦

戰術	技術	描述
	預先作業系統啟動	利用預操作系統啟動機制(如韌體與各種啟動服務)在系統上建立持久存取連線
	程序注入	將程式碼注入程序中，以逃避程序之防禦並盡可能提升權限
	反射程式碼載入	將程式碼載入到程序中，以隱藏惡意程式執行，反射載入涉及直接在程序之記憶體中分配然後執行有效惡意程式
	惡意網域控制器	註冊惡意網域控制站來操縱 Active Directory 資料
	Rootkit	使用 Rootkit 來隱藏程式、檔案、網路連線、服務、驅動程式及其他系統元件之存在，Rootkit 是透過攔截/掛鉤和修改提供系統資訊的作業系統 API 呼叫來隱藏惡意軟體存在之程式
	顛覆信任控制	破壞安全控制以執行不受信任之活動或執行不受信任之程序
	系統二進位代理執行	透過使用簽章或其他受信任之二進位檔案代理惡意內容之執行來繞過基於程序與/或簽章之防禦
	系統腳本代理執行	使用可信任腳本(通常使用憑證簽署)來代理惡意檔案之執行，攻擊者可能會濫用此行為來執行惡意文件，從而繞過系統上之應用程式控制與簽章驗證
	模板注入	在使用者文件範本中建立或修改引用，以隱藏惡意程式碼或強制進行身分驗證嘗試
	流量訊號	使用流量訊號來隱藏開放連接埠或用於持續性或命令和控制之其他惡意功能

戰術	技術	描述
	受信任的開發人員 實用程式代理執行	利用受信任之開發人員實用程式來代理惡意程式執行，有許多用於軟體開發相關任務之程序，可用於執行各種形式之程式碼，以協助開發、調試及逆向工程，這些實用程式通常可能使用合法憑證進行簽章，允許它們在系統上執行，並透過有效繞過應用程式控制解決方案之可信任進程代理惡意程式碼執行
	未使用/不支援的雲端區域	在未使用之地理服務區域中建立雲端實例以逃避偵測，存取權限通常是透過破壞用於管理雲端基礎設施之帳戶獲得
	使用替代驗證材料	使用替代身分驗證材料，例如密碼雜湊、Kerberos 票證及應用程式存取令牌，以便在環境中橫向移動並繞過正常之系統存取控制
	有效帳戶	攻擊者可能會取得並濫用現有帳戶之憑證，作為獲得初始存取、持久性、權限升級或防禦規避之手段
	虛擬化/沙盒規避	用各種手段來偵測和避開虛擬化與分析環境，包括根據對指示虛擬機器環境(VME)或沙箱工具是否存在之檢查結果來改變行為
	弱化加密	破壞網路設備之加密功能，以繞過本來可以保護資料之通訊加密
	XSL 腳本處理	透過在 XSL 檔案中嵌入腳本來繞過應用程式控制並掩蓋程式碼執行
憑證存取	中間攻擊者	攻擊者可能會嘗試使用中間攻擊者技術將自己定位在兩個或多個連網裝置之間，以支援後續行為，例如網路嗅探、傳輸資料操縱或重播攻擊

戰術	技術	描述
	暴力破解	在不知道一個帳戶或一組帳戶密碼之情況下，攻擊者可能會使用重複或迭代機制系統地猜測密碼
	來自密碼儲存的憑證	攻擊者可能會搜尋常見之密碼儲存位置以取得使用者憑證
	利用憑證存取	利用軟體漏洞來嘗試蒐集憑證
	強制認證	攻擊者可以透過呼叫或強迫使用者透過他們可以攔截之機制自動提供身分驗證資訊來蒐集憑證資料
	偽造網路憑證	偽造可用於存取網路應用程式或網際網路服務之憑證資料
	輸入捕捉	攻擊者可能會使用捕獲使用者輸入之方法來獲取憑證或蒐集資訊
	修改認證流程	攻擊者可能會修改身分驗證機制和流程來存取使用者憑證或啟用對帳戶之未經授權存取
	多重身份驗證攔截	攻擊者可能會以多重驗證(MFA)機制(即智慧卡、令牌產生器等)為目標，以獲得可用於存取系統、服務及網路資源憑證之存取權限
	多重身份驗證請求生成	攻擊者可能會嘗試繞過多重身份驗證(MFA)機制，並透過產生發送給使用者之 MFA 請求來取得對帳戶之存取權限
	網路嗅探	攻擊者可能會嗅探網路流量以捕獲有關環境的訊息，包括透過網路傳遞之身分驗證資料
	作業系統憑證轉儲	攻擊者可能會嘗試轉儲憑證以從作業系統與軟體，取得帳戶登入與憑證資料

戰術	技術	描述
	竊取應用程式存取權令牌	攻擊者可以竊取應用程式存取權限作為獲取存取遠端系統與資源憑證之手段
	竊取或偽造身份驗證證書	攻擊者可能會竊取或偽造用於身分驗證以存取遠端系統或資源之憑證
	竊取或偽造 Kerberos 票證	攻擊者可能會嘗試透過竊取或偽造 Kerberos 票證來破壞 Kerberos 身分驗證以啟用傳遞票證
	竊取網路會話 Cookie	攻擊者可能會竊取 Web 應用程式或服務會話 Cookie，並使用它們以經過驗證之使用者身分存取 Web 應用程式或 Internet 服務
	不安全的憑證	攻擊者可能會搜尋受感染之系統以尋找並取得不安全儲存的憑證
發現	帳戶發現	攻擊者可能會嘗試取得系統上或受感染環境中之有效帳戶、使用者名稱或電子郵件地址清單，有助於後續攻擊行為
	應用程式視窗發現	攻擊者可能會嘗試取得開啟之應用程式視窗的清單
	瀏覽器資訊發現	攻擊者可能會列舉有關瀏覽器資訊，以了解有關受感染環境之更多資訊。瀏覽器保存之資料(例如書籤、帳戶及瀏覽歷史記錄)可能會洩露有關用戶的各種個人資訊(例如銀行網站、關係/興趣及社交媒體等)以及有關內部網路資源之詳細資訊，例如伺服器、工具/儀表板或其他相關基礎設施
	雲端基礎設施發現	發現基礎設施即服務(IaaS)環境中可用之基礎設施與資源。這包括計算服務資源(例如實例、虛擬機器及快照)以及其他服務資源(包括儲存與資料庫服務)



戰術	技術	描述
	雲端服務儀表板	使用具有被盜憑證之雲端服務儀表板 GUI 從操作雲環境中獲取有用資訊，例如特定服務、資源及功能
	雲端服務發現	攻擊者可能會在獲得存取權限後嘗試枚舉系統上執行之雲端服務
	雲端儲存物件發現	列舉雲端儲存基礎架構中之物件，攻擊者可能會在自動發現過程中使用此資訊來塑造後續行為，包括從雲端儲存請求所有或特定物件
	容器和資源發現	攻擊者可能會嘗試發現容器與容器環境中可用之其他資源，包括映像、部署、pod、節點及其他資訊(例如叢集狀態)
	偵錯工具規避	採用各種手段來偵測和避開除錯器，例如 Black Basta 可以檢查系統標誌、CPU 暫存器、CPU 指令、處理時序、系統函式庫及 API，以確定偵錯器是否存在
	設備驅動程式發現	攻擊者可能會嘗試列舉受害主機上之本機裝置驅動程式，有關裝置驅動程式之資訊可能會突出顯示影響後續行為之各種見解，例如主機功能/用途、當前安全工具(即安全軟體發現)或其他防禦(例如虛擬化/沙箱規避)以及潛在威脅可利用之漏洞(例如，利用權限升級)
	網域信任發現	蒐集有關網域信任關係資訊，這些資訊可用於識別 Windows 多網域環境中橫向移動機會
	檔案和目錄發現	列舉檔案與目錄，或者可以在主機或網路共享之特定位置搜尋檔案系統內某些資訊

戰術	技術	描述
	群組策略發現	蒐集有關群組原則設定資訊，以識別權限升級之路徑、網域內應用之安全措施，並發現網域物件中可被操縱或用於混合在環境中之模式
	日誌列舉	列舉系統和服務日誌以查找有用資料，例如用戶身分驗證紀錄
	網路服務發現	嘗試取得在遠端主機和本機網路基礎架構設備上執行之服務列表，包括那些可能容易受到遠端軟體利用之服務
	網路共享發現	尋找遠端系統上共享資料夾與驅動程式，作為識別資訊來源手段，以作為蒐集之前兆進行蒐集，並識別潛在橫向移動感興趣之系統
	網路嗅探	攻擊者可能會嗅探網路流量以捕獲有關環境之訊息，包括透過網路傳遞身分驗證資料
	密碼策略發現	嘗試存取有關企業網路或雲端環境中使用密碼策略之詳細資訊
	外圍設備發現	嘗試蒐集有關連接到電腦系統之周邊設備與組件之資訊
	權限群組發現	嘗試發現群組和權限設定，這些資訊可以幫助攻擊者確定哪些使用者帳戶和群組可用、特定群組中使用者之成員資格，以及哪些使用者與群組具有提升之權限
	流程發現	嘗試獲取有關係統上正在運行之程序的資訊。所獲得之資訊可用於了解網路內系統上運行常見軟體/應用程式

戰術	技術	描述
	查詢註冊表	查詢 Windows 註冊表以蒐集有關系統、配置及已安裝軟體之資訊
	遠端系統發現	嘗試透過 IP 位址、主機名稱或網路上可用於從目前系統進行橫向移動之其他邏輯識別碼來取得其他系統的清單
	軟體發現	嘗試取得系統或雲端環境中安裝之軟體與軟體版本的清單
	系統資訊發現	嘗試獲取有關作業系統與硬體詳細資訊，包括版本、修補程式、修補程式、服務包及架構
	系統位置發現	攻擊者可能會蒐集資訊以嘗試計算受害主機之地理位置
	系統網路配置發現	攻擊者可能會查找有關他們存取之系統的網路配置與設定詳細資訊，例如 IP 與/或 MAC 位址，或透過遠端系統資訊發現來查找
	系統網路連線發現	攻擊者可能會嘗試透過網路查詢資訊來取得目前正在存取之受感染系統或遠端系統網路連線清單
	系統所有者/用戶發現	嘗試識別主要使用者、目前登入使用者、經常使用系統之使用者群組，或使用者是否正在使用系統
	系統服務發現	攻擊者可能會嘗試蒐集有關已註冊本地系統服務之資訊
	系統時間發現	從本地或遠端系統蒐集系統時間與/或時區
	虛擬化/沙盒規避	用各種手段來偵測和避開虛擬化與分析環境，包括根據對指示虛擬機器環境(VME)或

戰術	技術	描述
		沙箱之工件是否存在的檢查結果來改變行為
橫向移動	遠端服務的利用	利用遠端服務在網路內部獲得對內部系統未經授權之存取
	內部魚叉式網路釣魚	在已經有權存取環境中的帳戶或系統後，使用內部魚叉式網路釣魚來存取其他資訊或利用同一機關內之其他使用者
	橫向工具傳輸	攻擊者可能會在受感染環境中之系統間傳輸工具或其他檔案，一旦進入受害者環境(即入口工具傳輸)，檔案就可以從一個系統複製到另一個系統，以便在操作過程中暫存工具或其他檔案
	遠端服務會話劫持	透過遠端服務控制預先存在之會話，以便在環境中橫向移動，例如 SSH 或 RDP 劫持
	遠端服務	攻擊者可以使用有效帳戶登入接受遠端連線服務
	透過可移動介質複製	透過將惡意軟體複製到可移動介質並在介質插入系統並執行時利用自動運行功能來轉移到系統上
	軟體部署工具	存取並使用安裝在目標網路內第三方軟體套件(例如管理、監控及部署系統)，以在網路中橫向移動
	污點分享內容	透過將內容新增至共用儲存位置(例如網路磁碟機或內部程式碼資料庫)來向遠端系統傳遞有效惡意程式
	使用替代驗證材料	使用替代身分驗證材料，例如密碼雜湊、Kerberos 票證及應用程式存取令牌，以便在

戰術	技術	描述
		環境中橫向移動並繞過正常之系統存取控制
蒐集	中間攻擊者	攻擊者可能會嘗試使用中間攻擊者技術將自己定位在兩個或多個連網裝置之間，以支援後續行為，例如網路嗅探、傳輸資料操縱或重播攻擊
	存檔蒐集的資料	壓縮或加密蒐集之資料，壓縮資料有助於混淆蒐集之資料並最大限度地減少透過網路發送之資料量
	音訊捕捉	攻擊者可以利用電腦之外圍設備(例如麥克風和網路攝影機)或應用程式(例如語音和視訊通話服務)來擷取音訊紀錄，以監聽敏感對話來蒐集資訊
	自動蒐集	使用自動化技術來蒐集內部資料，執行此技術之方法可以包括使用命令與腳本解釋器來搜尋與複製符合設定標準資訊，例如特定時間間隔之文件類型、位置或名稱
	瀏覽器會話劫持	攻擊者可能會利用瀏覽器軟體中之安全漏洞與固有功能來更改內容、修改使用者行為並攔截訊息
	剪貼簿資料	攻擊者可能會從在應用程式內或應用程式之間複製資訊之使用者蒐集儲存在剪貼簿中的資料
	來自雲端儲存的資料	攻擊者可以存取雲端儲存中之資料
	來自配置資料庫的資料	攻擊者從配置資料庫蒐集與受管設備相關之資料

戰術	技術	描述
	來自資訊資料庫的資料	利用資訊資料庫來挖掘有價值之資訊
	來自本地系統的資料	搜尋本機系統來源(例如檔案系統和設定檔或本機資料庫)，找到敏感資料
	來自網路共享驅動器的資料	在已入侵電腦上搜尋網路共享以查找感興趣之檔案
	來自可移動媒體的資料	在已入侵電腦上搜尋連接之可移動媒體以查找感興趣之檔案
	資料暫存	在滲透之前將蒐集到之資料存放在特定位置或目錄中
	郵件收藏	以使用者電子郵件為目標來蒐集敏感資訊
	輸入捕捉	攻擊者可能會使用捕獲使用者輸入之方法來獲取憑證或蒐集資訊
	螢幕截圖	嘗試截取桌面螢幕以蒐集操作過程中之資訊
	影片截取	利用電腦之周邊設備(例如，整合相機或網路攝影機)或應用程式(例如，視訊通話服務)來擷取視訊紀錄
命令與控制	應用層協定	攻擊者可以使用 OSI 應用層協定進行通信，透過與現有流量混合來避免偵測/網路過濾
	透過可移動媒體進行通訊	使用可移動媒體在系統之間傳輸命令，在可能斷開連接之網路上的受感染主機之間執行命令與控制
	內容注入	透過線上網路流量將惡意內容注入系統來獲得存取權限並持續與目標進行通訊

戰術	技術	描述
	資料編碼	攻擊者可能會對資料進行編碼(如 ASCII、Unicode、Base64、MIME 或其他編碼系統)，以使命令和控制流量之內容更難以偵測
	資料混淆	對手可能會混淆命令與控制流量，使其更難以檢測，例如向協議流量添加垃圾資料、使用隱寫術或模仿合法協議
	動態決議	動態地建立與命令與控制基礎設施之連接，以逃避常見之偵測與修補措施
	加密頻道	採用已知加密演算法來隱藏命令與控制流量，而不是依賴通訊協定提供之任何固有保護
	後備通道	如果主要通道受到損害或無法訪問，攻擊者可能會使用後備或備用通訊通道，以維持可靠命令與控制
	入口工具傳輸	攻擊者可能會將工具或其他檔案從外部系統轉移到受感染環境
	多級通道	建立多個階段來進行命令與控制，並在不同條件下或用於某些功能
	非應用層協定	使用 OSI 非應用層協定在主機和 C2 伺服器之間或網路內受感染之主機間進行通訊，如使用網路層協定 ICMP、傳輸層協定 UDP
	非標準連接埠	用通常不關聯之協定和連接埠配對進行通訊
	協定隧道	攻擊者可能會在特殊協定中透過隧道與受駭系統進行網路通信，以避免偵測、網路過濾或允許存取其他無法存取之系統

戰術	技術	描述
	proxy	攻擊者可以使用連接代理來引導系統之間的網路流量，或充當與命令和控制伺服器之網路通訊中介，以避免與其基礎設施直接連接
	遠端存取軟體	攻擊者可以使用合法之桌面支援和遠端存取軟體來建立到網路內目標系統互動式命令與控制通道
	流量訊號	使用流量訊號來隱藏開放連接埠或用於持續性或命令與控制之其他惡意功能
	網路服務	攻擊者可能會使用現有之合法外部 Web 服務作為與受感染系統間的轉發資料手段
滲漏	自動滲漏	攻擊者在蒐集資料後，透過使用自動處理來洩露資料
	資料傳輸大小限制	攻擊者可能會以固定大小之區塊而不是整個檔案的形式竊取資料，或者將資料包大小限制在特定閾值以下，此方法可用於避免觸發網路資料傳輸閾值警報
	透過替代協議進行滲透	攻擊者可能會透過與現有命令和控制通道不同之協定來竊取資料
	透過命令與控制通道滲漏	透過現有之命令與控制通道竊取資料
	透過其他網路媒體的滲漏	嘗試透過命令與控制通道之外的不同網路媒體竊取資料，如 WiFi
	透過物理介質的滲漏	透過實體媒體(例如 USB)竊取資料
	透過 Web 服務進行滲漏	使用現有的之合法外部 Web 服務來竊取資料



戰術	技術	描述
	預定接送	攻擊者可能會安排僅在一天中特定時間或特定時間間隔執行資料外洩，這樣做可以將流量模式與正常活動或可用性混合在一起
	將資料傳輸至雲端帳戶	透過將資料(包括雲端環境的備份)傳輸到他們在同一服務上控制另一個雲端帳戶來洩露資料
影響	帳戶存取權限刪除	透過禁止存取合法使用者使用之帳戶來中斷系統與網路資源的可用性，帳戶可能會被刪除、鎖定或操縱
	資料銷毀	破壞特定系統上或網路上大量之資料與文件，從而中斷系統、服務及網路資源可用性
	資料加密	對目標系統或網路中大量系統上之資料進行加密，以中斷系統與網路資源可用性
	資料處理	攻擊者可能會插入、刪除或操縱資料，以影響外部結果或隱藏活動，威脅資料完整性
	污損	攻擊者可能會修改機關網路內部或外部可用視覺內容，進而影響原始內容之完整性
	磁碟清除	攻擊者可能會擦除或損壞特定系統上或網路中大量之原始磁碟數據，從而中斷系統和網路資源可用性
	端點拒絕服務	執行端點拒絕服務(DoS)攻擊，以降低或封鎖使用者服務可用性
	金融竊盜	透過勒索、社交工程、技術盜竊或其他旨在獲取經濟利益之方法從目標竊取貨幣資源

戰術	技術	描述
	韌體損壞	攻擊者可能會覆蓋或破壞系統 BIOS 之閃存內容或連接到系統之設備中的其他韌體，以使無法操作或無法啟動，從而拒絕使用設備與/或系統可用性
	禁止系統恢復	攻擊者可能會刪除或移除內建資料並關閉旨在幫助恢復損壞系統之服務以阻止復原，這可能會拒絕存取可用之備份與還原選項
	網路拒絕服務	執行網路拒絕服務攻擊，以降低或阻止目標資源對使用者之可用性
	資源劫持	利用增選系統之資源來完成資源密集型任務，這可能會影響系統與/或託管服務可用性
	服務站	停止或停用系統上之服務，從而使合法用戶無法使用這些服務
	系統關閉/重啟	攻擊者可能會關閉/重新啟動系統以中斷對系統存取

資料來源：<https://attack.mitre.org>

### 3.3 檢查階段

演練完成後，演練機關須視需求進行系統復原作業，確保業務正常運作，紅隊則應就演練所取得之成果，撰寫紅隊演練執行結果報告並交付演練機關。演練機關收到報告後，應與紅隊針對報告內發現之弱點與機關潛在威脅進行確認，並衡量改善方式之可行性[8]。具體之確認項目根據演練情境不同而有所差異，以下為參考項目：

#### ●情報蒐集

確認蒐集可供後續作業之資訊，為機關潛在但不易發現或管理之風險。

- 社交工程攻擊資訊(視演練情境決定是否需要)

社交工程攻擊成功之機關成員名單。

- 弱點探測與利用

演練發現之系統存在已知或未知弱點。

- 身分認證測試

弱密碼與驗證繞過等相關弱點。

- 內部橫向移動

內部可利用橫向移動之設備或系統。

- 偵測系統繞過

機關監控與偵測系統存在可以繞過之弱點。

- 無法及時修補項目

藍隊偵測所轄系統受攻擊但未能及時修補之弱點。

紅隊演練執行結果報告為演練結果與分析之關鍵文件，應該清晰、詳盡地呈現演練之結果與相關發現，以協助機關發現自身資安威脅並加以改善，演練報告可依機關需求於演練過程中要求演練團隊交付期中報告，說明演練執行進度與情形，並於演練完成後交付完整演練結果報告，內容應包含但不限於以下項目：

- 演練概述

詳細描述演練的情境、目標、範圍及參與人員。

- 攻擊詳情

逐一系列與描述每個模擬攻擊之步驟，包括攻擊面向與演練使用之工具與技術、演練達成情形及受影響系統。

- 弱點與問題

詳列發現之弱點、問題及弱點，並對其風險進行評估。

- 證據與日誌

包括攻擊之軌跡、日誌文件及相關資料，以佐證結果報告中之結論。

- 改善建議與措施

提供整體演練發現之改善建議與措施，以協助受測單位後續進行弱點修復與加強整體資通安全防護之安全性。

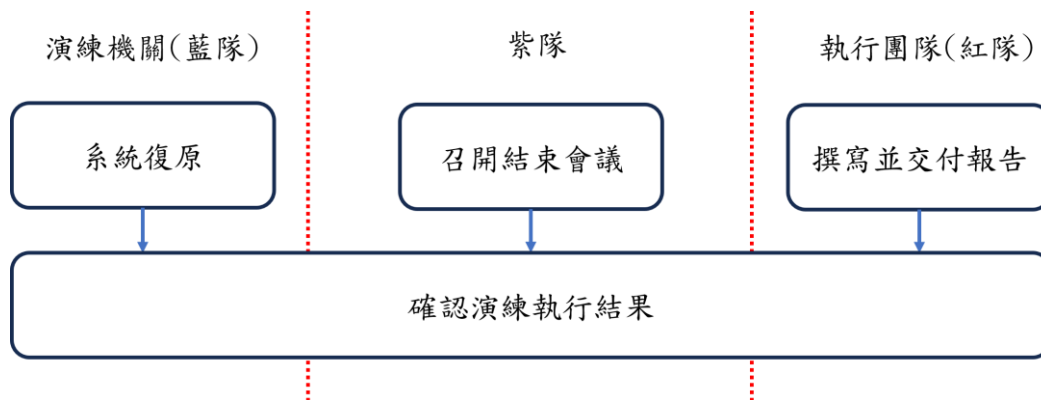
- 結論

總結演練之結果，重點強調改善措施執行之優先順序。

- 附件

包括演練之技術詳細資訊、測試工具及其他參考資料。

交付演練執行結果報告後，所有演練團隊都應派員出席參與說明與討論，以確保所有演練相關單位皆了解報告內容，並能夠提出問題或討論建議之改善措施。檢查階段雙方流程詳見圖 8。



資料來源：本計畫整理

圖8 檢查階段細部流程

### 3.4 改善階段

演練機關於確認演練相關威脅與結果後，依據演練執行結果報告與結束會議討論結果制定改善計畫，詳細流程詳見圖 9，內容應包含但不限於以下項目：

- 弱點修復與防禦強化

根據演練中發現之弱點進行修復，同時加強安全措施，如防火牆、入侵偵測系統及資通安全政策等，以減少攻擊者攻擊成功機會。

- 加強監控與偵測

根據攻擊紀錄修改相關偵測規則，以避免再遭受相同攻擊。

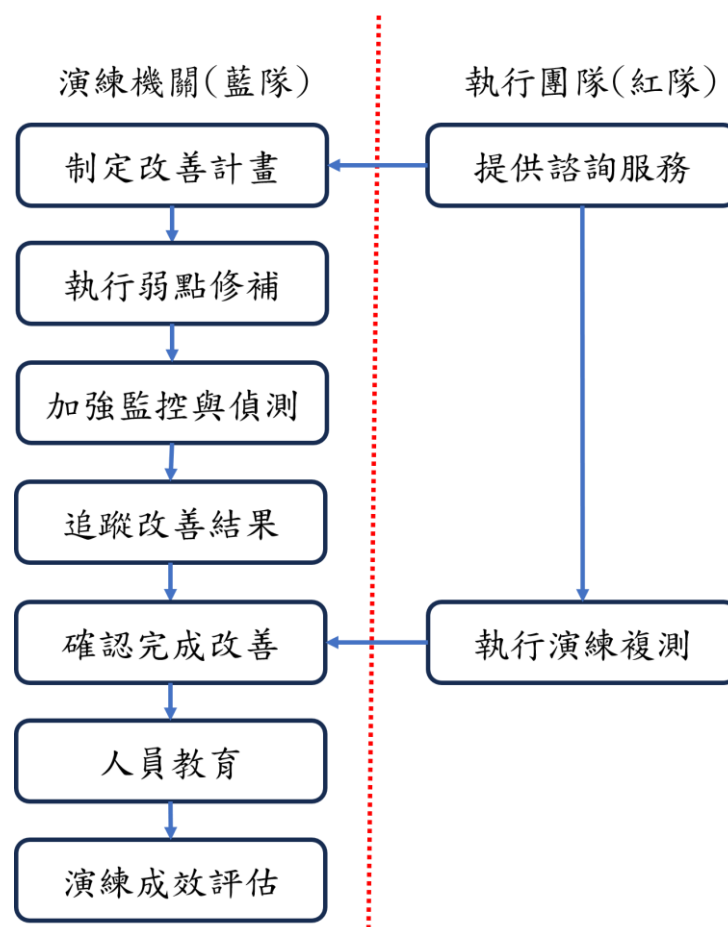
- 進行複測

確認修復後之弱點已不存在，執行複測前，可要求執行團隊交付複測計畫，作為執行複測之依據。

- 人員教育

提供全體員工與相關利害關係人之安全教育與培訓，以提高員工識別與

應對威脅之能力。



資料來源：本計畫整理

圖9 改善階段細部流程

改善階段除針對本次演練提供改善建議之外，更應評估演練整體成效，以作為未來持續辦理紅隊演練之參考。演練成效可參考美國國家安全專家 Zenko 在「Red Team: How to Succeed By Thinking Like the Enemy」一書中所提出之 6 個項目進行評估、檢討及提出改善方案[8]，詳見表 7。

表7 紅隊演練執行成效評估項目

項次	評估項目	說明
1	高層支持	高階管理階層應確實了解紅隊評估效益，並給予相對應之人力、資源及回報層級，才能確保紅隊執行任務順遂
2	若即若離	紅、藍隊於執行過程中應保持適當距離，避免因過多接觸失去模擬真實攻擊之效果
3	擁有技能的專家	要依據演練任務需求，組成具備相關技能及經驗之團隊
4	足智多謀	紅隊開始執行時，應針對目標，採用「大膽假設，小心求證」之方式，逐步找出問題並提供相對應之解決建議
5	願意聽壞消息並據此採取行動	高層應正視及願意撥出時間來瞭解紅隊演練結果及建議
6	適可而止	提出演練重點發現及建議措施後，則應結束此項任務及作業，如同專案管理，沒有完美之專案，只有依計畫管理與進行之專案。

資料來源：本計畫整理

## 4. 結論

本指引提供紅隊演練作業參考指引，協助政府機關人員了解執行紅隊演練作業所需注意之相關事項，各機關應考量自身情況，針對演練時程、範圍、成員及廠商選擇進行綜合評估，並建議參考本指引附件之紅隊演練招標說明文件範本，規劃與研擬適宜之標案內容，以達成紅隊演練之預期效益。

紅隊演練雖相較於弱點掃描與滲透測試係更全面之測試方法，檢測標的通常不是單一系統或設備，而是以整體機關做為檢測標的，檢測方式通常模擬多個攻擊面向，包括外部與內部攻擊及應用程式弱點等，以檢視受測目標營運上可能存在之資安風險，然亦非一體適用，機關仍應依據需求與效益考量，選擇弱點掃描、滲透測試或紅隊演練，依據不同目的、不同標的性質與範圍等，或單獨採用或搭配採用不同之資安檢測手段，以發揮整體綜效，亦即紅隊演練雖能深入發掘機關潛在資安威脅，並加以改善，惟機關仍應持續關注潛在資安弱點，透過持續檢視與改善，方能有效強化自身防護能力。



## 5. 參考文獻

- [1]112 年共同供應契約資通安全服務品項採購規範，  
<https://www.chtsecurity.com/download/service/file/154f2466-4c6f-4403-9ce1-b4be808af3cb>
- [2]Mike Fenton, “Restoring executive confidence: Red Team operations”,  
Network Security, Vol. 2016, Issue 11, pp. 5-7, Nov. 2016.
- [3]SANS SEC565 Red Team Operations and Adversary Emulation,  
<https://www.sans.org/cyber-security-courses/red-team-operations-adversary-emulation/>
- [4]Yuri Diogenes and Erdal Ozkaya, “Cybersecurity – Attack and Defense Strategies”, Packt, 2019.
- [5]Jacob G. Oakley, “Professional Red Teaming: Conducting Successful Cybersecurity Engagements”, USA: Apress, 2019.
- [6]Yuri Diogenes and Erdal Ozkaya, “Cybersecurity – Attack and Defense Strategies”, Packt, 2019.
- [7]Bradley J. Wood and Ruth A. Duggan, “Red Teaming of Advanced Information Assurance Concepts”, 25-27 Jan. 2000, USA, Proceedings DARPA Information Survivability Conference and Exposition.
- [8]MITRE ATT&CK 框架，<https://attack.MITRE.org/>.
- [9]Konstantinos Pantazis and Christos Ilioudis, “An External Red Team Assessment in a Corporate Environment”, ResearchGate, Sep. 2022.
- [10]Micah Zenko, “Red Team: How to Succeed By Thinking Like the Enemy”, Nov. 2016.

## 6. 附件

### 附件1 紅隊演練招標說明文件範本