資訊處
Office of Information Technology

弱點掃描常見問題修補建議

中華民國114年3月24日 1.3版

編號：

主要原則

- 任何服務與設備，若不需要對外提供服務，建議阻擋所有外部連線，若有需求建議以白名單的方式授權使用
- 個人電腦、筆記型電腦請事先了解安裝那些軟體、服務，並確認系統及軟體均已更新至最新
  - ✓個人電腦、筆記型電腦安全設定請參閱本處作業指引
  - ✓連結:https://isms.ccu.edu.tw/p/426-1044-8.php?Lang=zh-tw
- 物聯網設備(如印表機、無線分享器、網路監視攝影機…等)，請確保韌體均更新至最新，且完成安全性設定
  - ✓物聯網設備安全使用請參閱本處作業指引
  - ✓連結:https://isms.ccu.edu.tw/p/426-1044-13.php?Lang=zh-tw

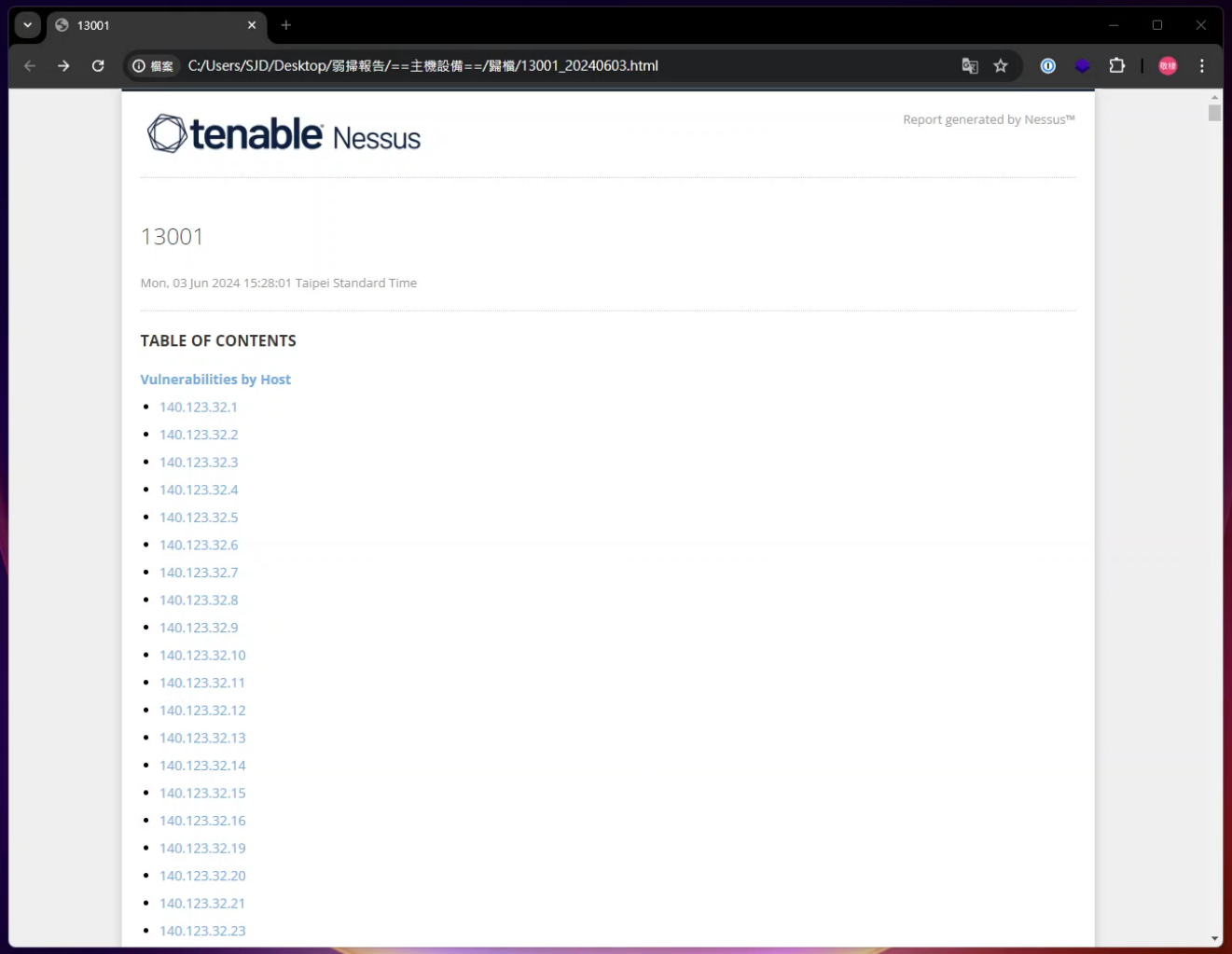
物聯網設備

- 物聯網設備修補常見特殊狀況：
  - ✓設備老舊且原廠已不提供維護
    - 更換新設備
  - ✓沒有經費購買新設備
    - 限制連線
  - ✓設備本身做不到限制連線設定
    - 使用私人網段
    - 單機作業
    - 設備下架不使用

資訊處
Office of Information Technology

如何閱讀報告

提供html格式，方便閱讀



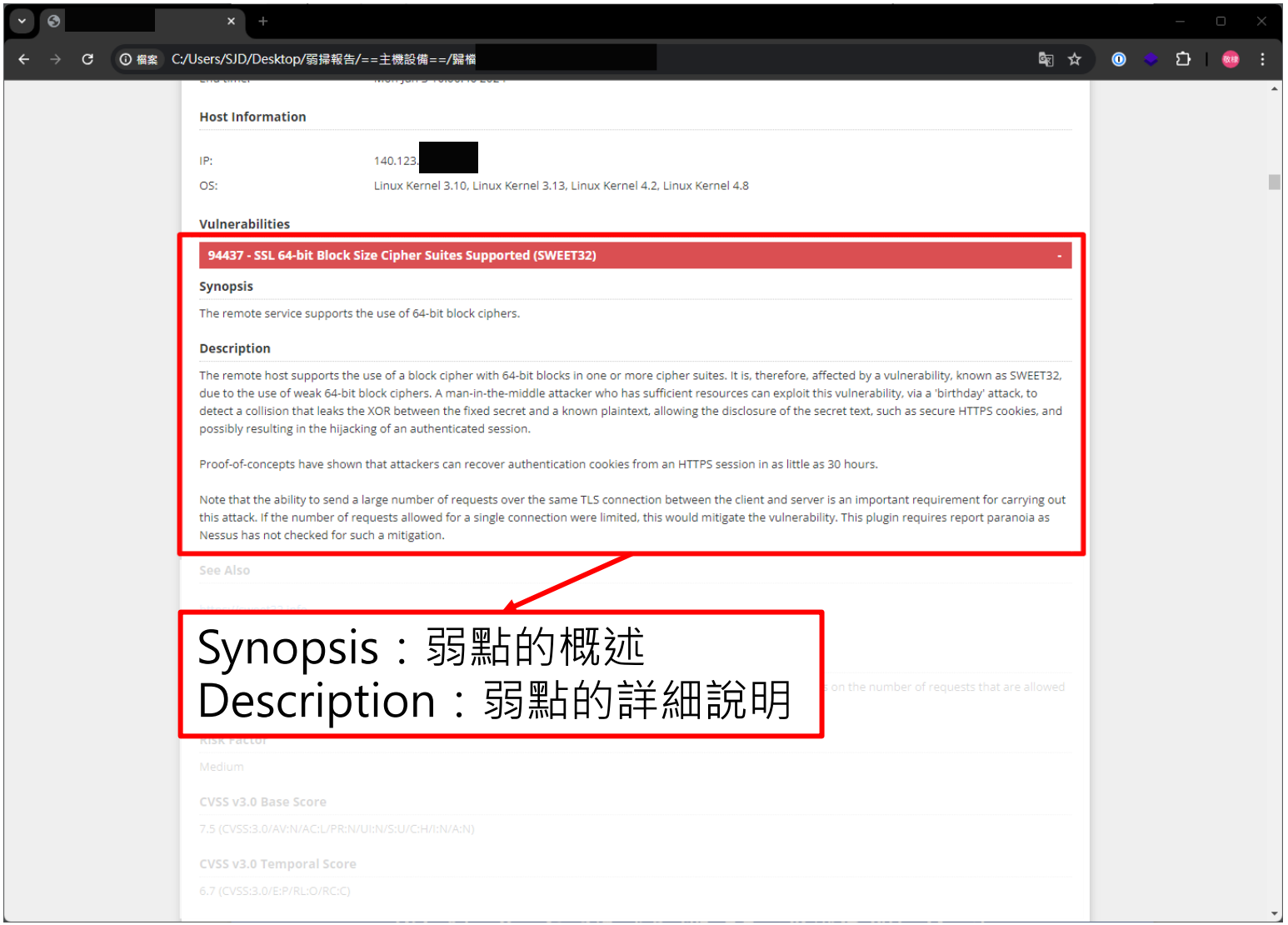
風險數統計

統計使用該IP設備的弱點數與取得的資訊數

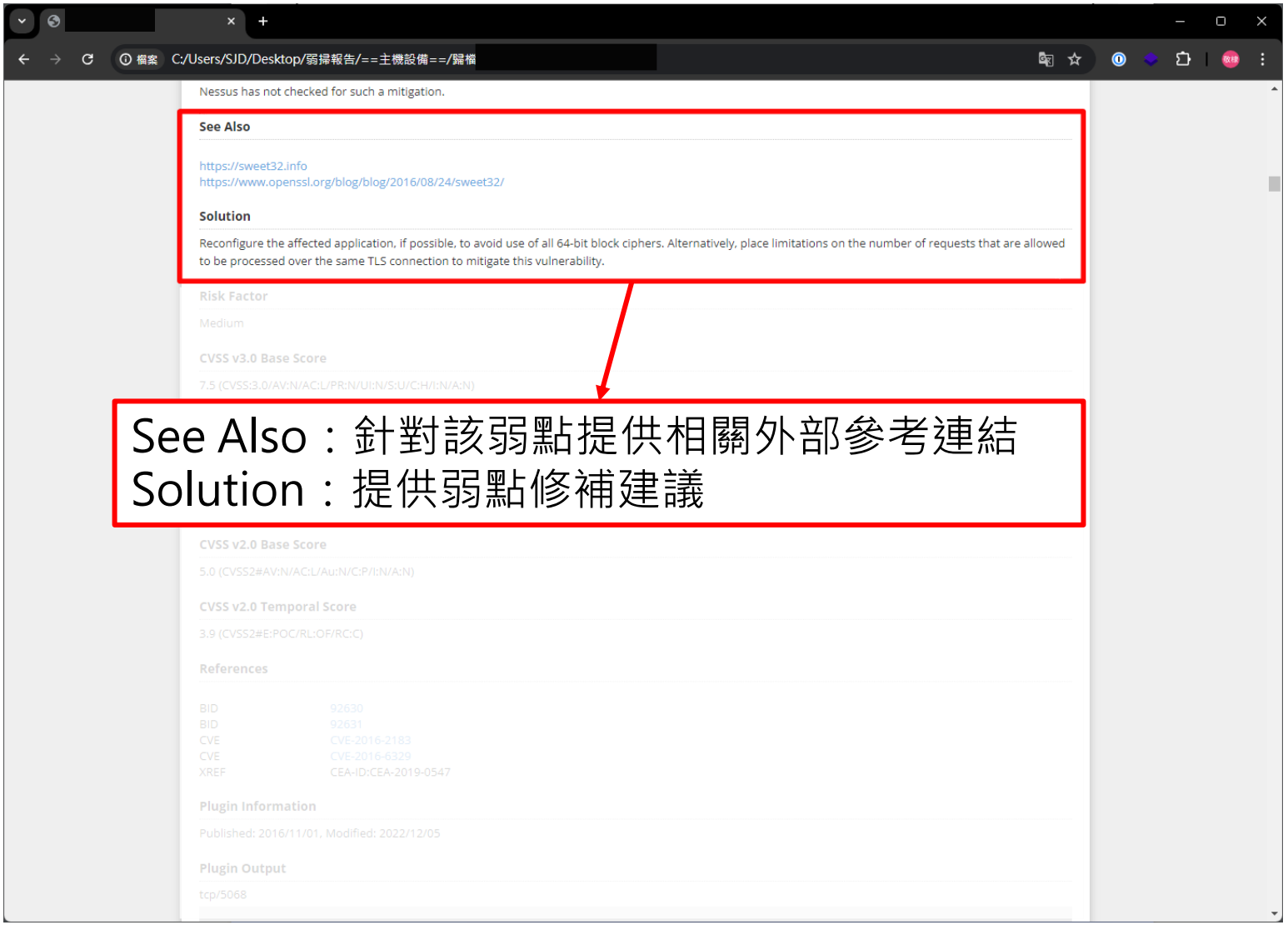
1. 存在Critical(嚴重)、High(高)、Medium(中)弱點須盡速修補
2. 存在Low(低)為建議修補
3. Info(資訊)為弱掃過程中取得的資訊

※中以上風險(含中風險)都必須修補

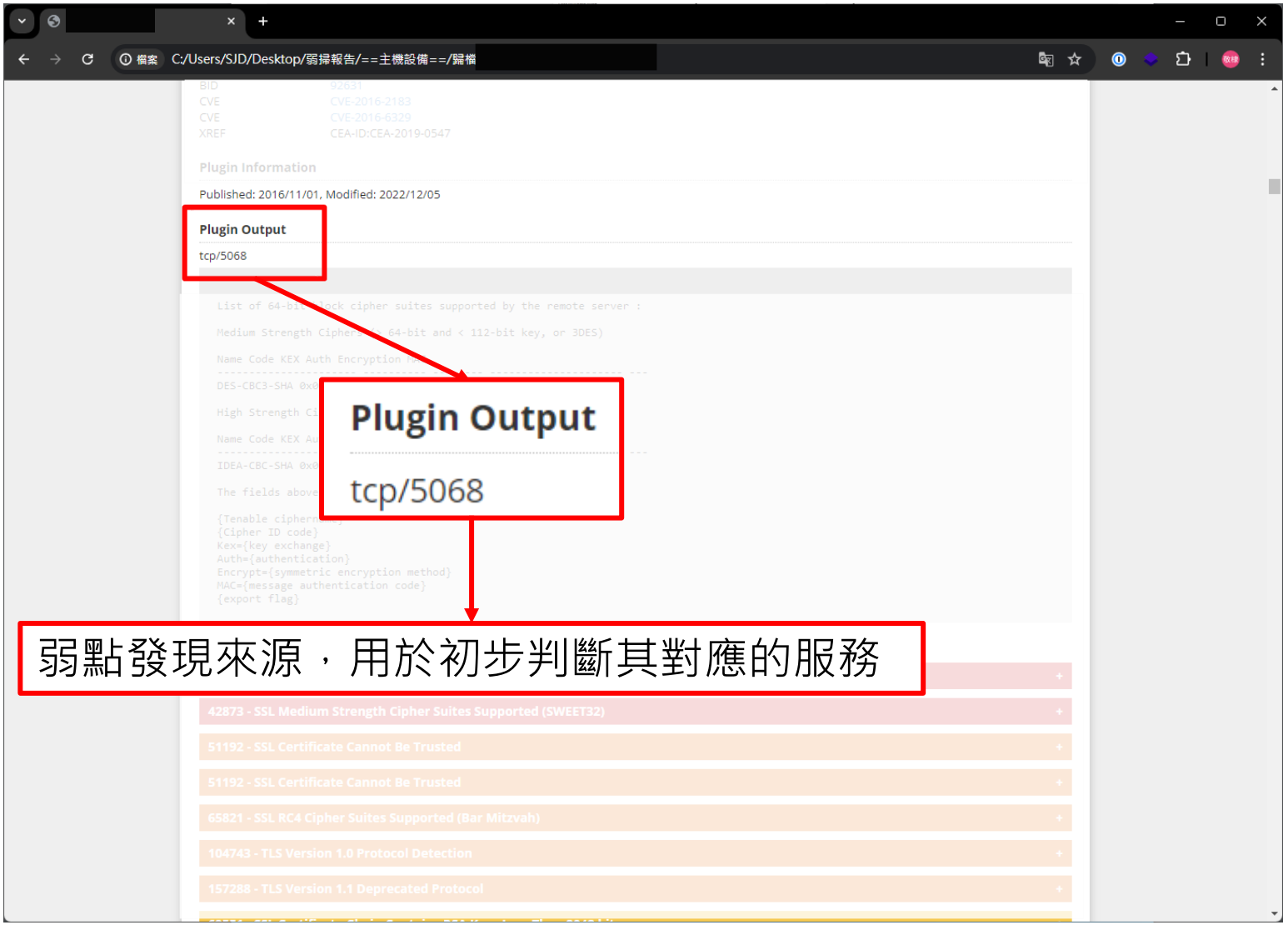
弱點名稱與說明


C:/Users/SJD/Desktop/弱掃報告/==主機設備==/歸檔
Host Information
IP: 140.123.[redacted]
OS: Linux Kernel 3.10, Linux Kernel 3.13, Linux Kernel 4.2, Linux Kernel 4.8
Vulnerabilities
94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Synopsis
The remote service supports the use of 64-bit block ciphers.
Description
The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.
Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. This plugin requires report paranoia as Nessus has not checked for such a mitigation.
See Also
Synopsis：弱點的概述
Description：弱點的詳細說明
Medium
CVSS v3.0 Base Score
7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVSS v3.0 Temporal Score
6.7 (CVSS:3.0/E:P/RL:O/RC:C)

外部參考連結與建議修補方式



弱點的發現來源


C:/Users/SJD/Desktop/弱掃報告/==主機設備==/報檔
BID 92631
CVE CVE-2016-2183
CVE CVE-2016-6329
XREF CEA-ID:CEA-2019-0547
Plugin Information
Published: 2016/11/01, Modified: 2022/12/05
Plugin Output
tcp/5068
Plugin Output
tcp/5068
弱點發現來源，用於初步判斷其對應的服務
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
51192 - SSL Certificate Cannot Be Trusted
51192 - SSL Certificate Cannot Be Trusted
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
104743 - TLS Version 1.0 Protocol Detection
157288 - TLS Version 1.1 Deprecated Protocol

常見通訊埠

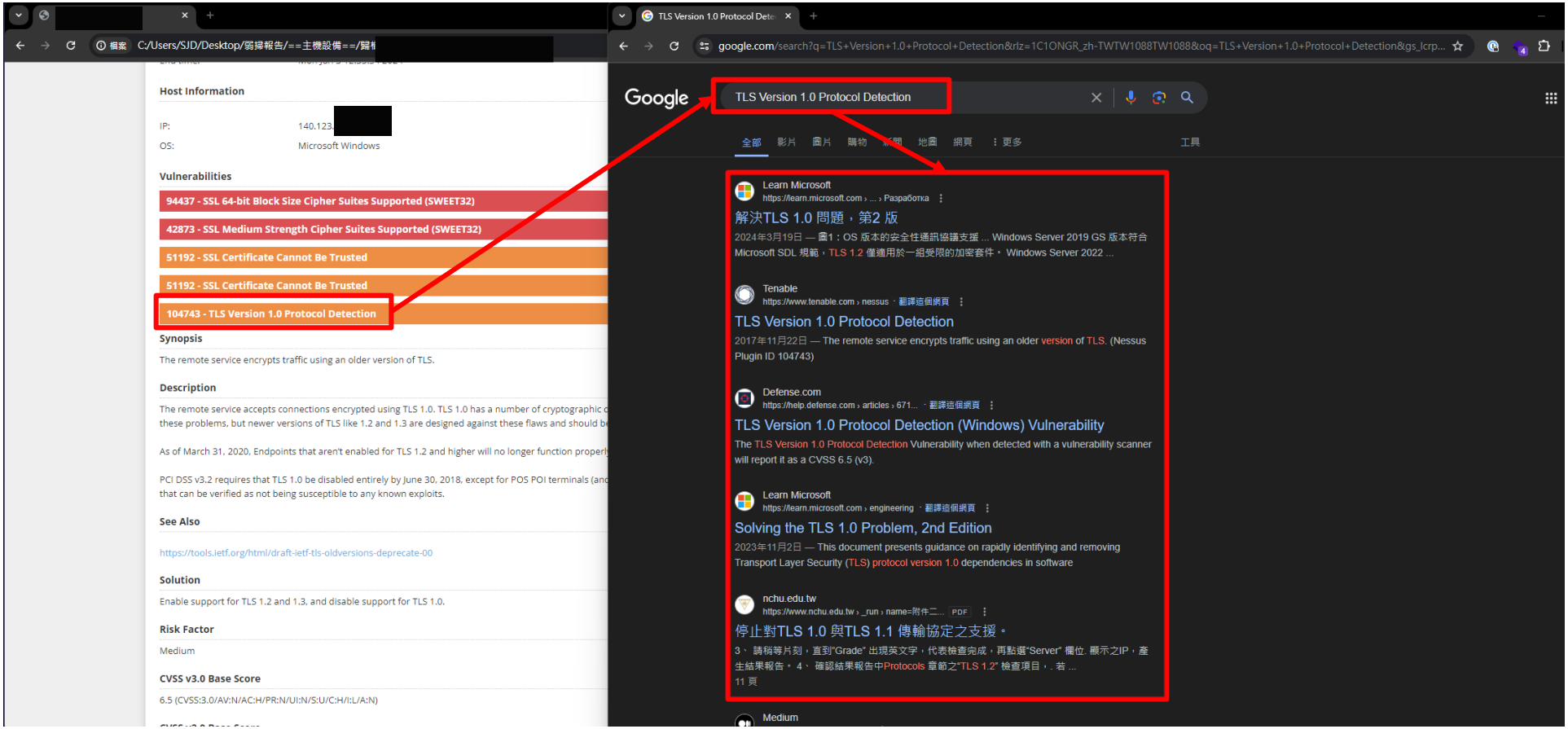
port	用途
21	FTP，檔案傳輸協定，用於傳輸檔案使用
22	SSH、SFTP(FTP使用SSH加密驗證，所以也走這個port)
25	SMTP，郵件傳輸協定，通常是mail server會使用
80	WEB SERVER常用，資料傳遞沒有經過SSL加密，HTTP
135	RPC，容易被惡意利用
139	SMB，常用於網路芳鄰共享文件或印表機共享掃描檔案，常見的服務為Samba，容易被惡意利用
udp/161	snmp協定，常見於印表機、交換機等網通設備，用於監控管理
443	WEB SERVER常用，資料傳遞有經過SSL加密，HTTPS
445	功能同port 139，容易被惡意利用
1433	MSSQL的預設port
3306	MySQL的預設port，有些使用者可能會改到port 3307、3308
3389	Microsoft的遠端桌面連線RDP

常見通訊埠(僅列TCP Port)

port	用途
5000	群輝(synology)管理介面預設http port
5001	群輝(synology)管理介面預設https port
5432	PostgreSQL的預設port
7777	健保卡驗證元件
8080	常用於WEB SERVER的proxy port，HTTP
8443	常用於WEB SERVER的proxy port，HTTPS
10443	FortiVPN常用port
14665	帝緯公文系統公文製作元件
17500	DropBox
21112	Apex One的listener，client端憑證名稱為ofcsslagent
39021	中華郵政網路ATM元件
56306	ServiSign多憑證元件，可能用於需要自然人憑證、健保卡、銀行金融卡等的系統

報告會看了，但還是不會修…

- 打開瀏覽器搜尋弱點名稱，大部分常見狀況都能找到修補教學

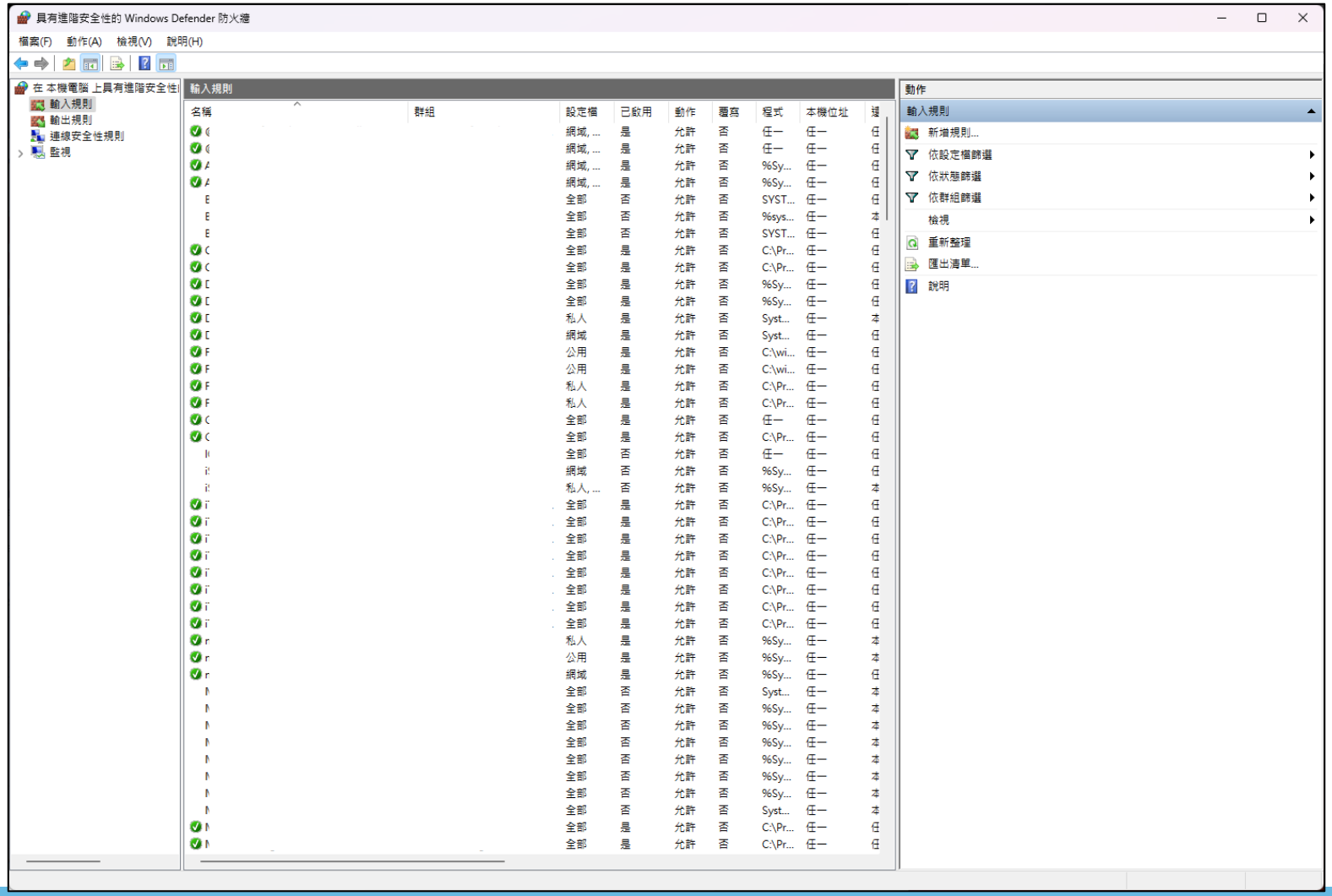


搜尋後還是找不到解決方法…

- 個人電腦、筆記型電腦：
  - ✓請盤點電腦內安裝的軟體，移除不常使用的軟體或服務
  - ✓若無法解決問題，可以考慮重灌設備，一台重灌後未安裝任何軟體也未進行過任何設定的電腦，基本上不會有任何弱點。
    - 提醒windows 10在2025年10月14日終止支援安全性更新，近期單位如有電腦重灌需求建議一律重灌為windows 11
- 物聯網設備：
  - ✓請見P3說明

其他解決方法…

- 從本機防火牆限制連線



資訊處
Office of Information Technology

尋找弱點來源的服務

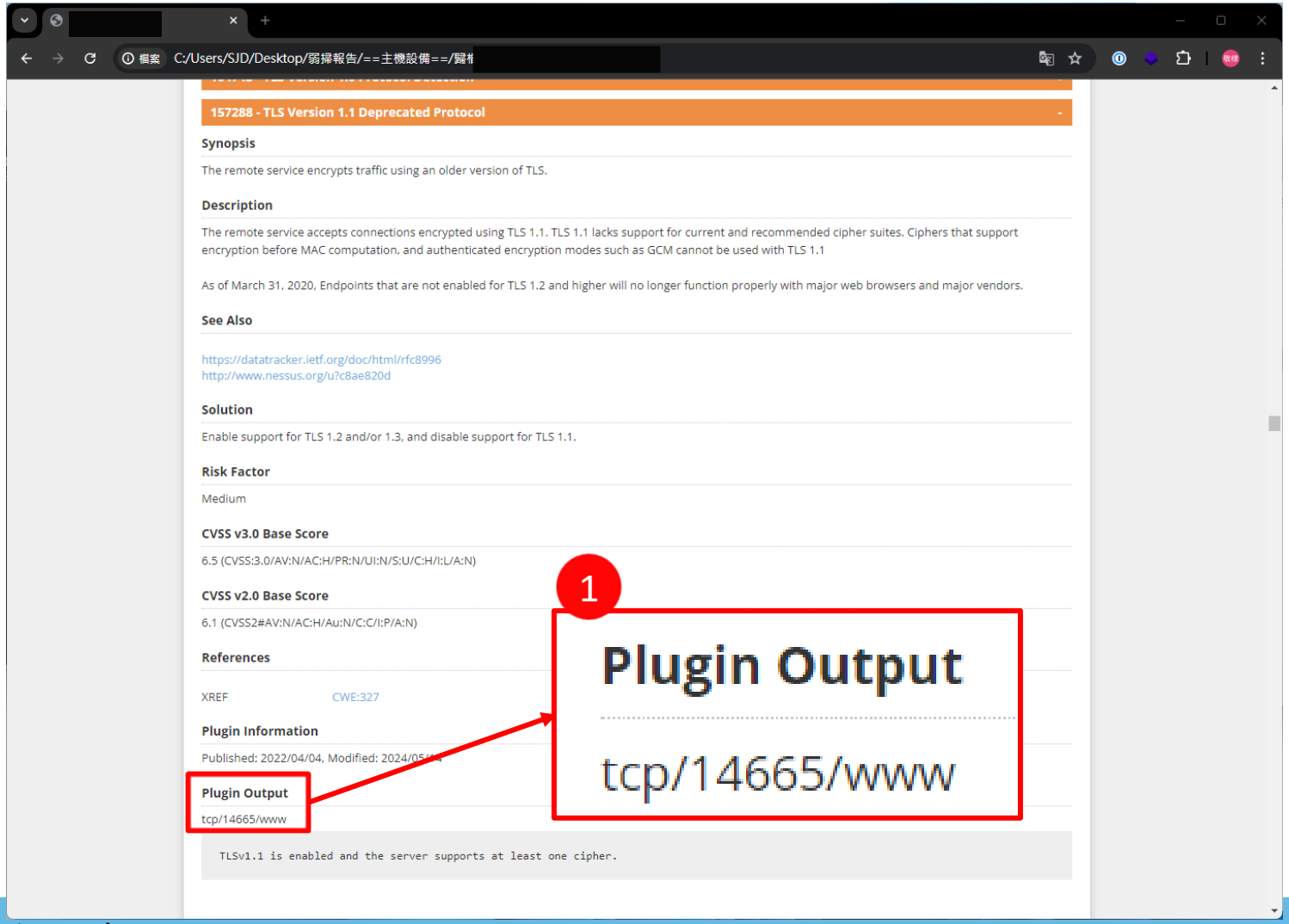
常見系統預設通訊埠(僅列TCP Port)

- 範圍通常在port 1~1023

port	用途
21	FTP，檔案傳輸協定，用於傳輸檔案使用
22	SSH、SFTP(FTP使用SSH加密驗證，所以也走這個port)
25	SMTP，郵件傳輸協定，通常是mail server會使用
80	WEB SERVER常用，資料傳遞沒有經過SSL加密，HTTP
135	RPC，容易被惡意利用
139	SMB，常用於網路芳鄰共享文件或印表機共享掃描檔案，常見的服務為Samba，容易被惡意利用
443	WEB SERVER常用，資料傳遞有經過SSL加密，HTTPS
445	功能同port 139，容易被惡意利用

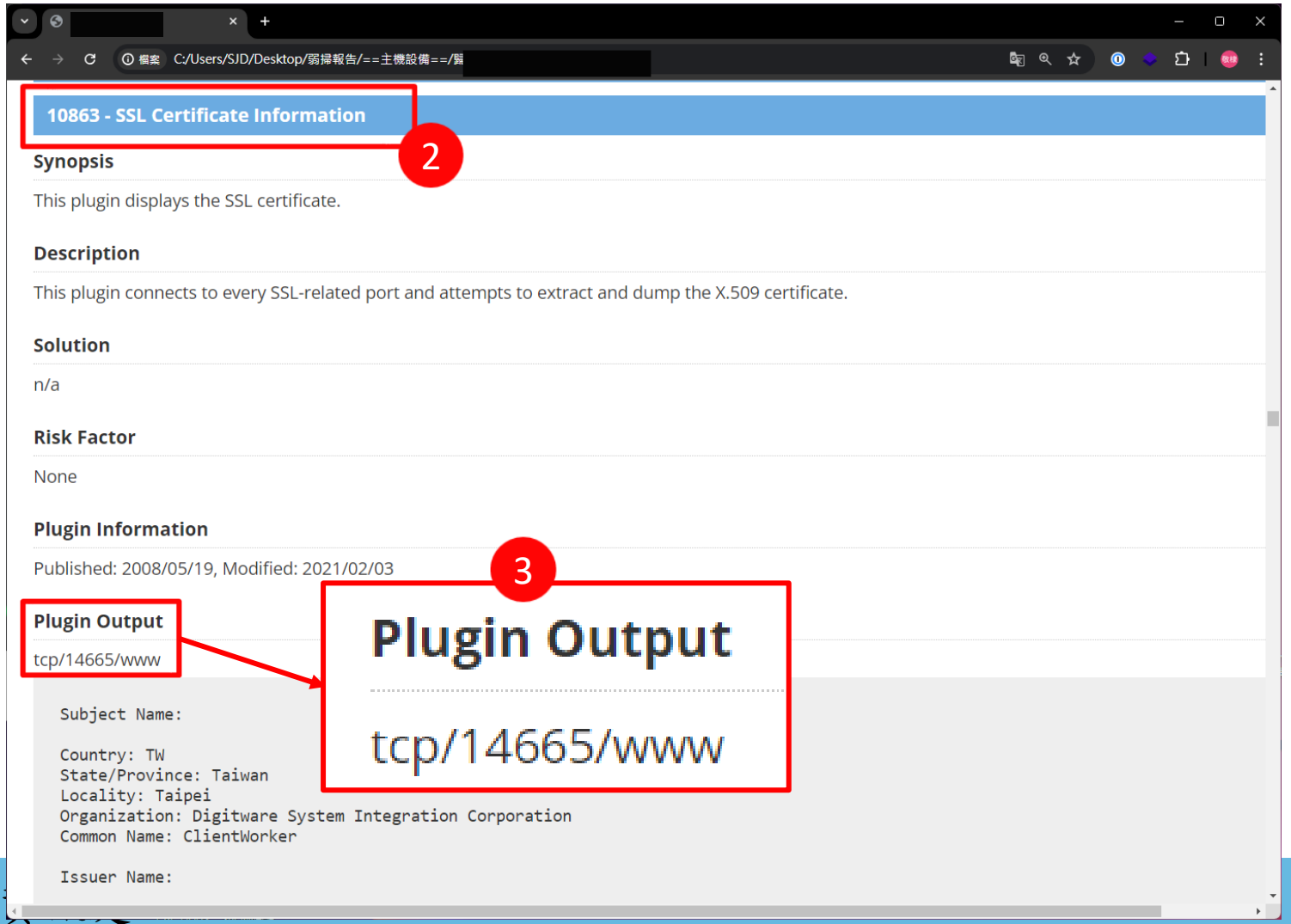
從憑證判斷程式或服務

- 發現一項弱點，先看「plugin output」，找到通訊埠為tcp 14665



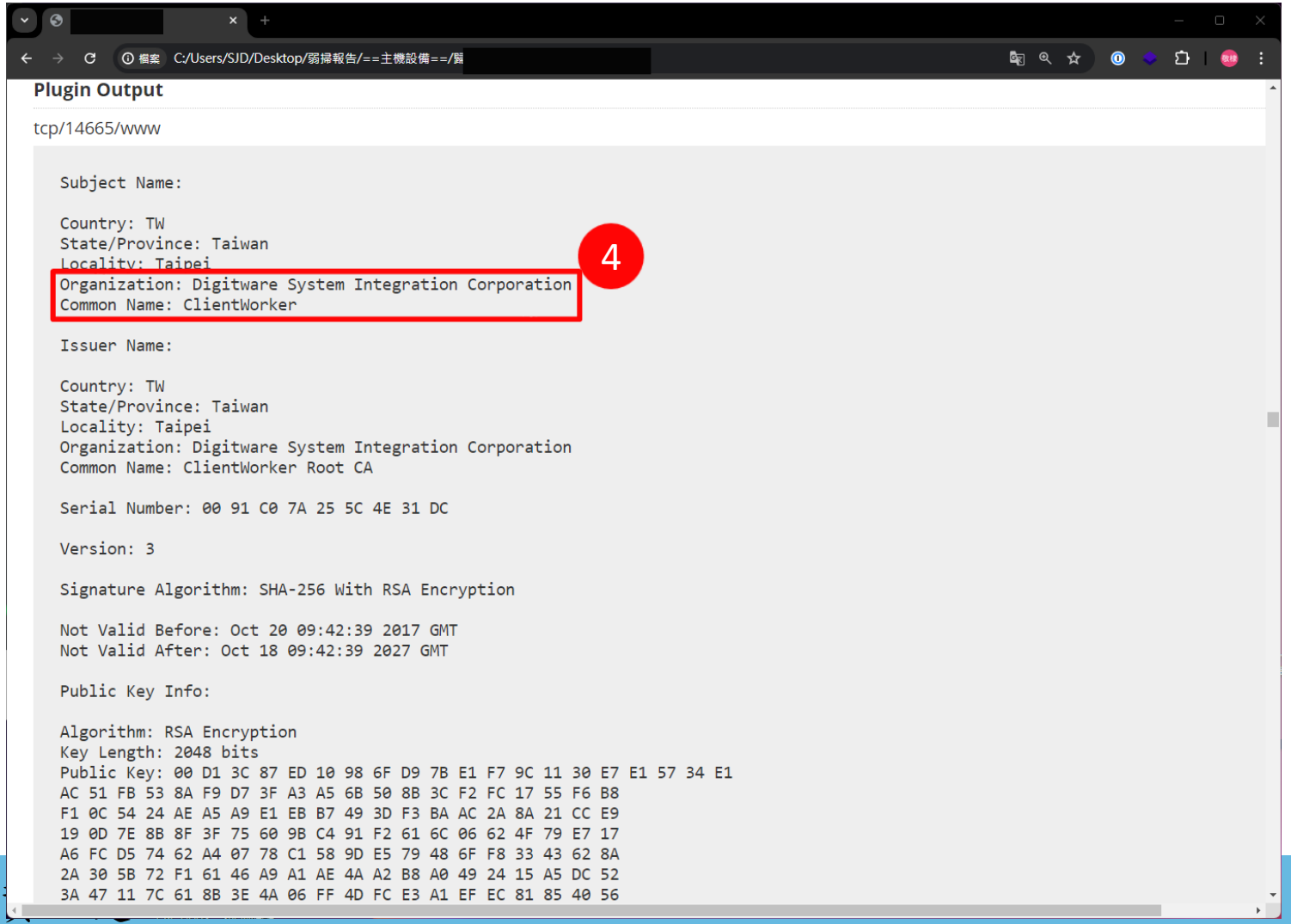
從憑證判斷程式或服務

- 找到「10863 - SSL Certificate Information」資訊，確認通訊埠一樣為tcp 14665



從憑證判斷程式或服務

- 檢視其憑證詳細內容，可以看「Organization」及「Common Name」資訊



從憑證判斷程式或服務

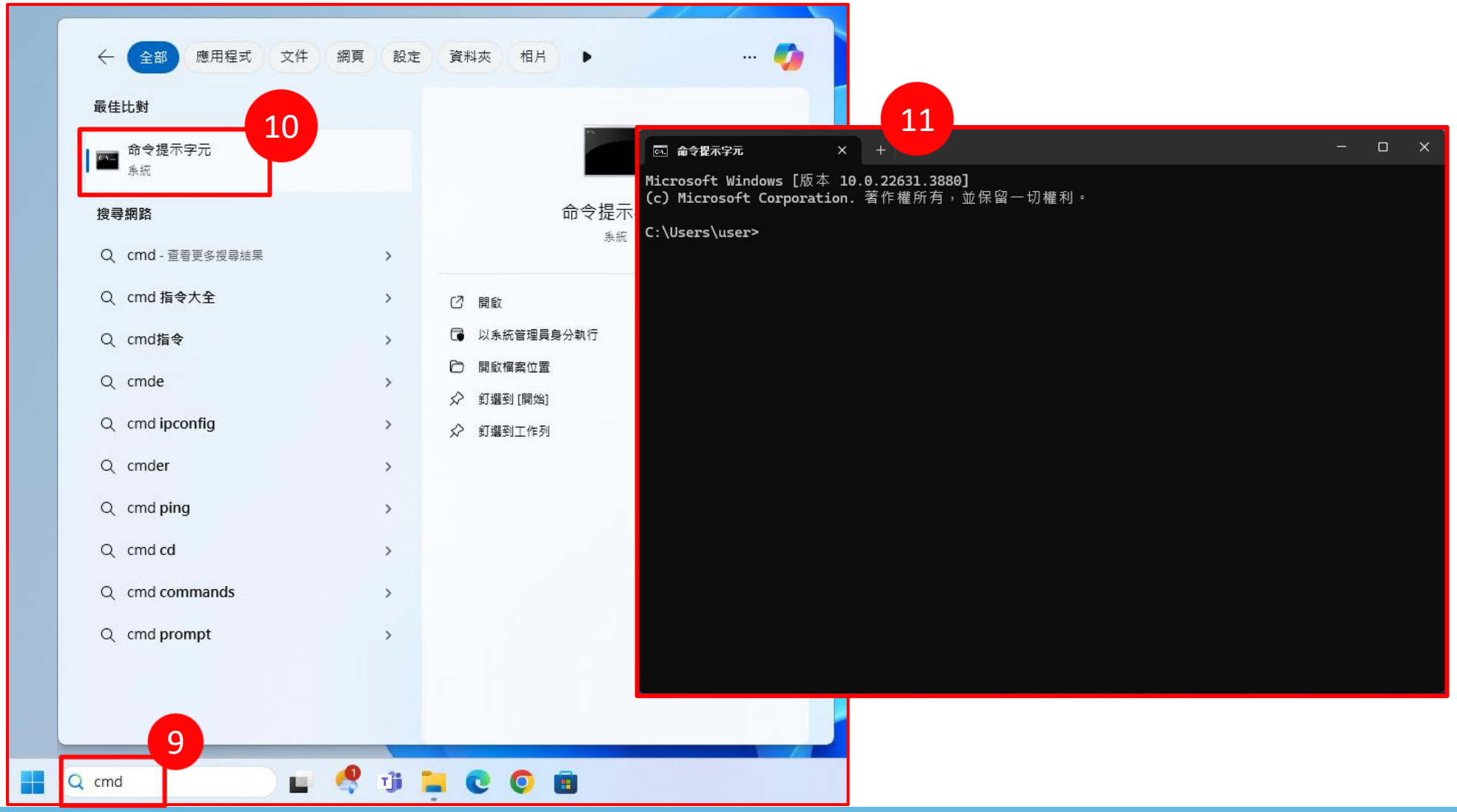
- 打開瀏覽器搜尋組織名稱或憑證通用名稱，以本案為例查到帝緯公司，推測可能是帝緯公司提供的服務

從憑證判斷程式或服務

- 組織加憑證通用名稱查詢，得到疑似是公文系統相關服務，後續針對該服務實施修補措施(更新程式…等)

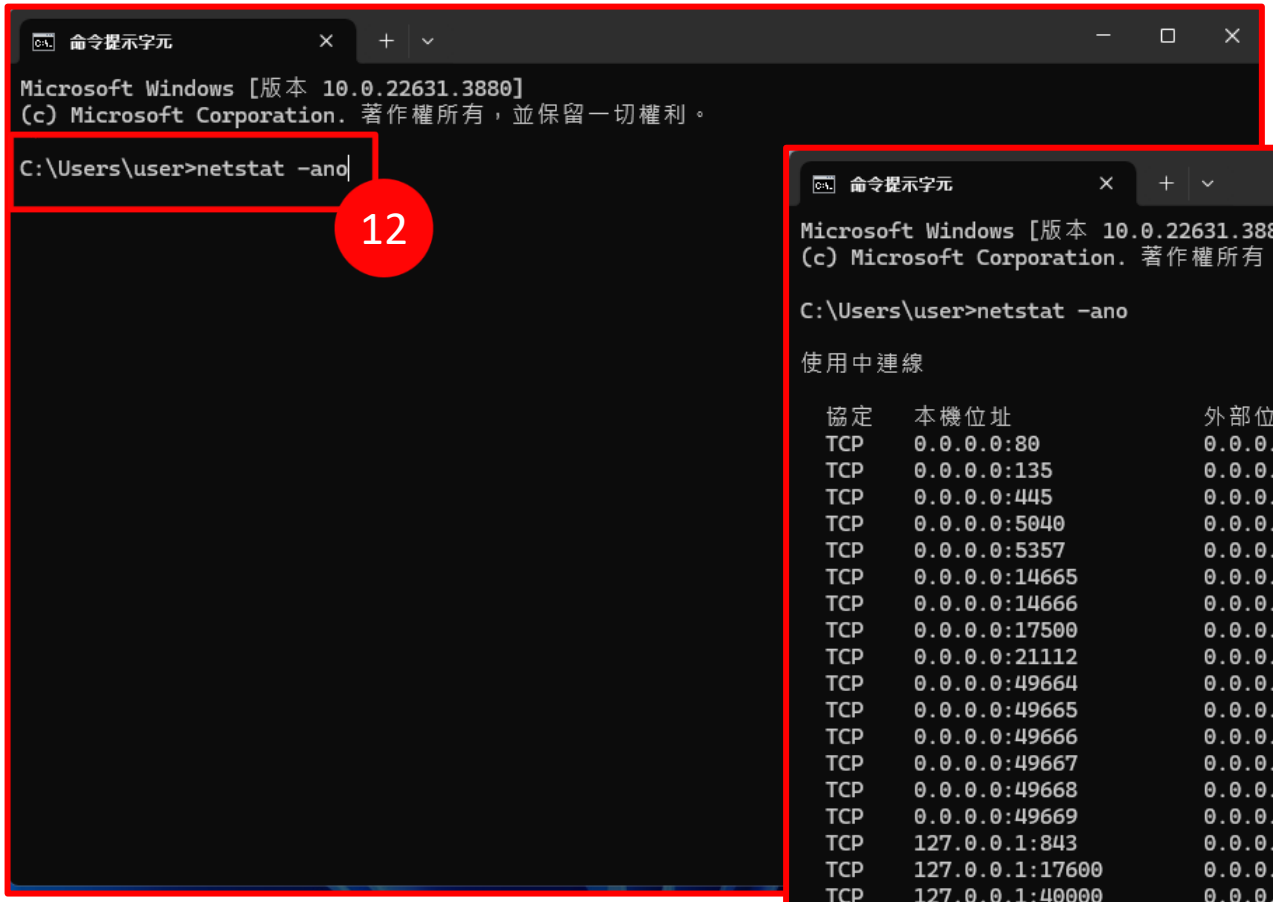
從系統工作程序找服務

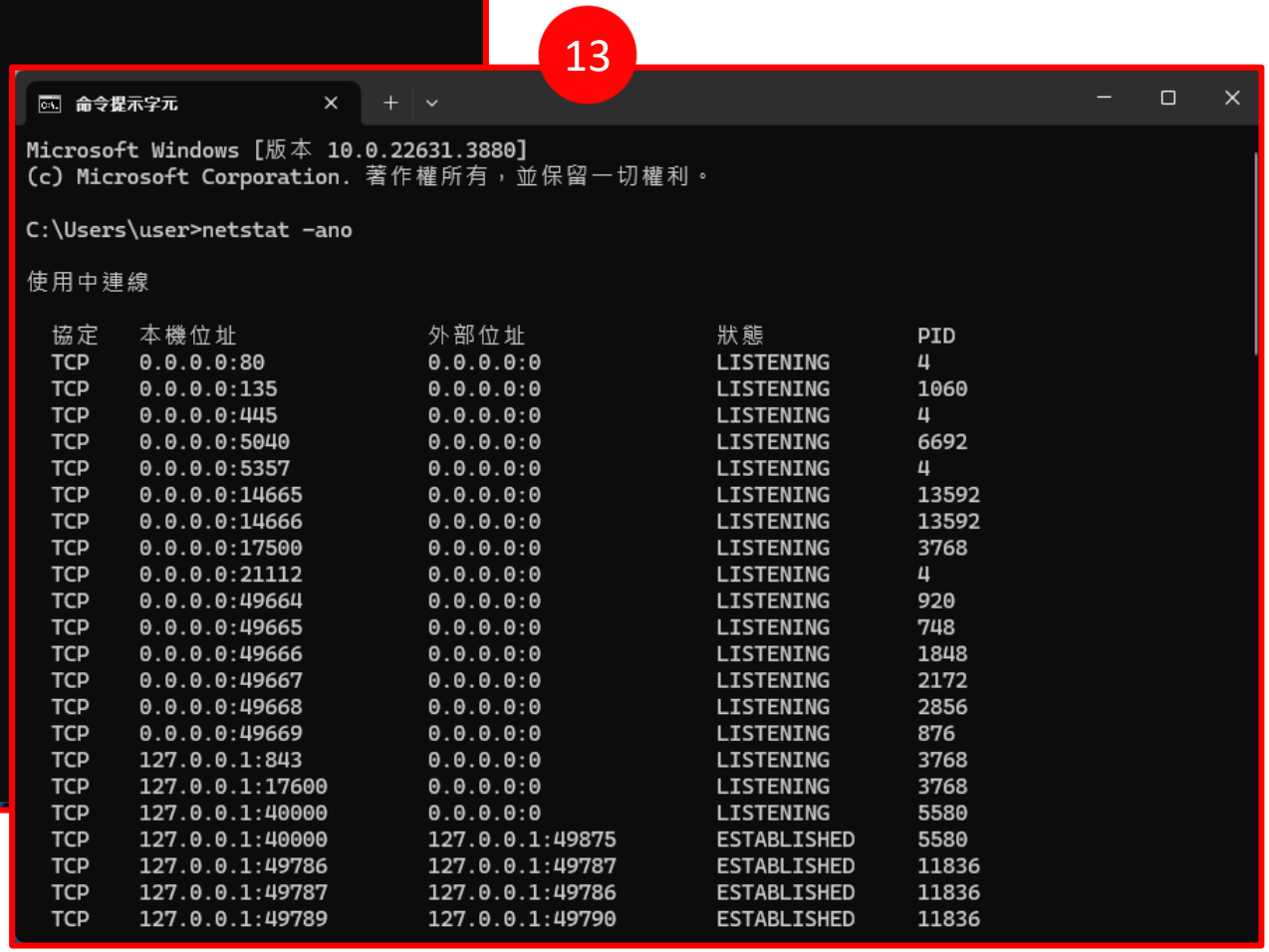
➢ 工作列搜尋「cmd」，點擊開啟「命令提示字元」



netstat指令

➢ 輸入指令「netstat -ano」，按鍵盤「Enter」執行指令





netstat 指令參數說明

➢netstat + 參數

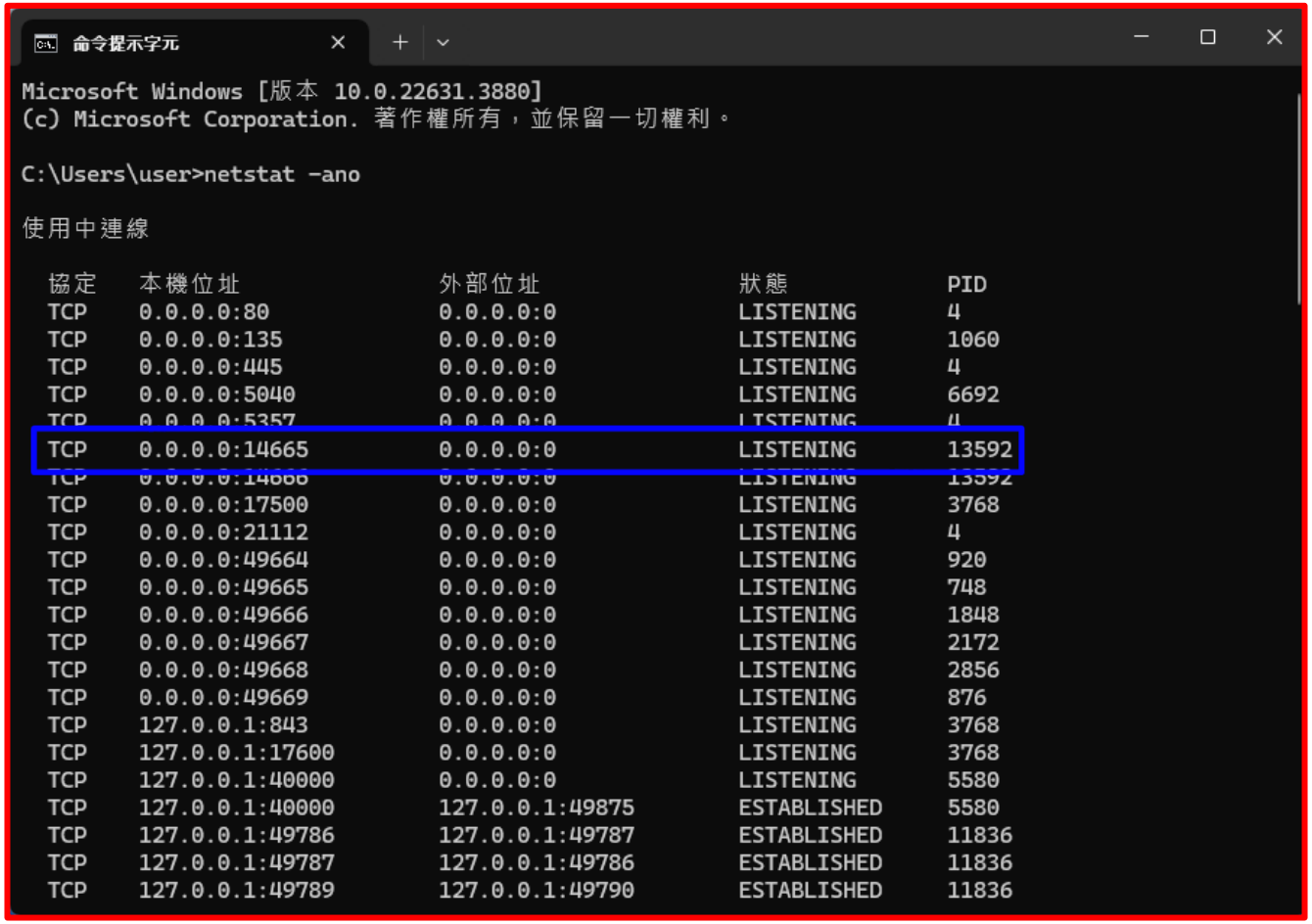
參數	說明
-a	顯示系統中所有正在活動中與監聽的tcp、udp埠，來源及目的地如果具有域名則會顯示域名
-n	連線的來源及目的不解析域名(只顯示IP)，因為不解析域名，指令執行動作會較快完成
-o	顯示所有活動的進程ID(PID)
-p	查詢指定通訊協定，如tcp、udp、icmp等，使用指令時需要指定通訊協定
-s	顯示通訊協定的統計資訊，可以搭配-p使用，不指定就是全部列出

➢使用範例

指令	說明
netstat -an	顯示系統中所有正在活動中與監聽的tcp、udp埠，以IP顯示來源及目的地
netstat -ano	顯示系統中所有正在活動中與監聽的tcp、udp埠，以IP顯示來源及目的地、顯示所有活動的PID
netstat -anop tcp	顯示系統中所有正在活動中與監聽的tcp埠，以IP顯示來源及目的地、顯示所有活動的PID

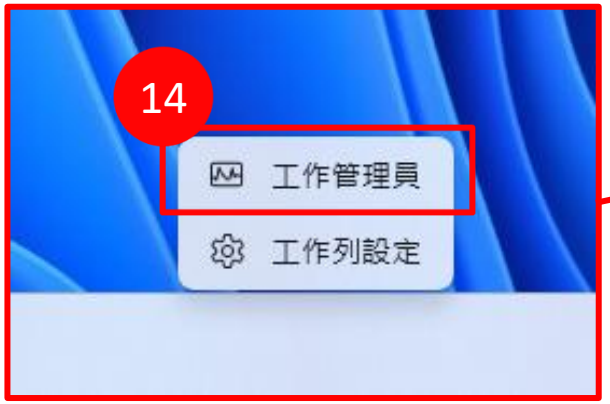
查找系統進程PID

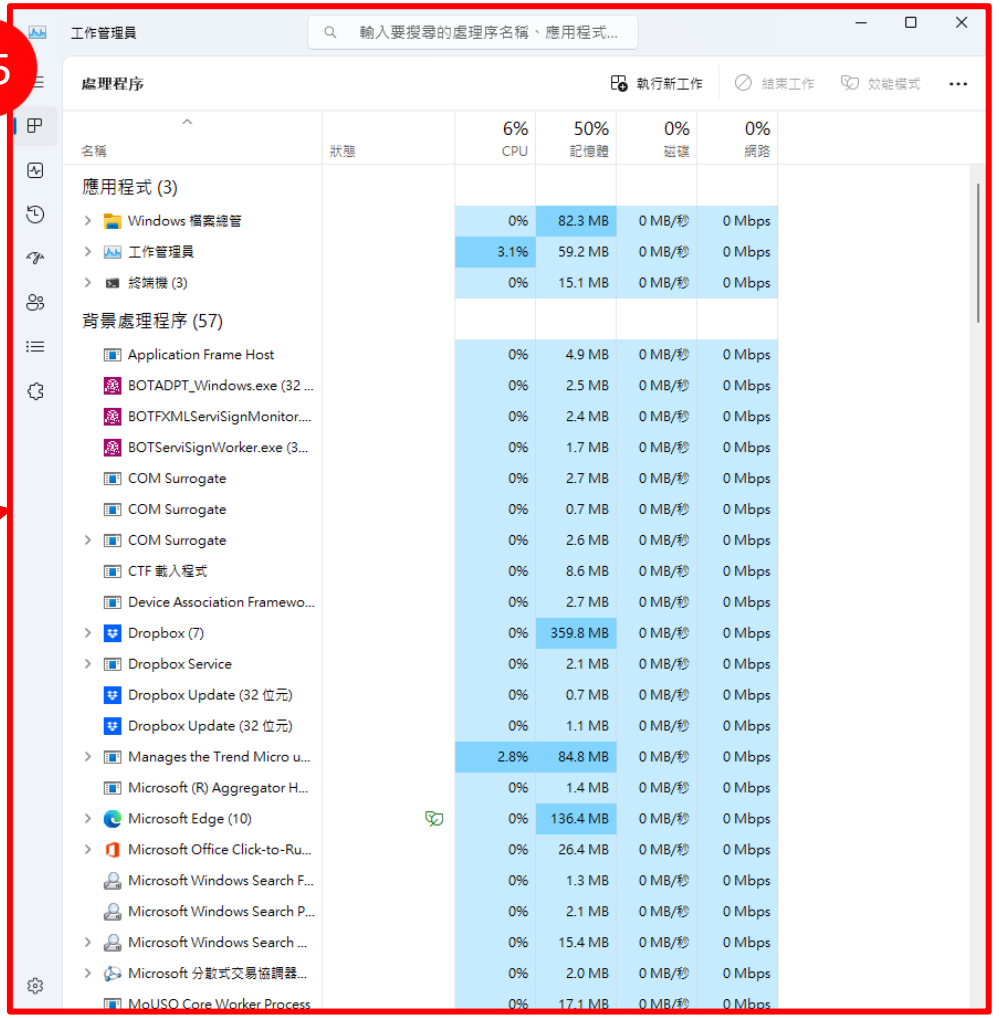
- 依報告找到TCP 14665的項目
- 找到對應的進程ID(PID)，以本案為例PID為「13592」



依PID查找對應服務

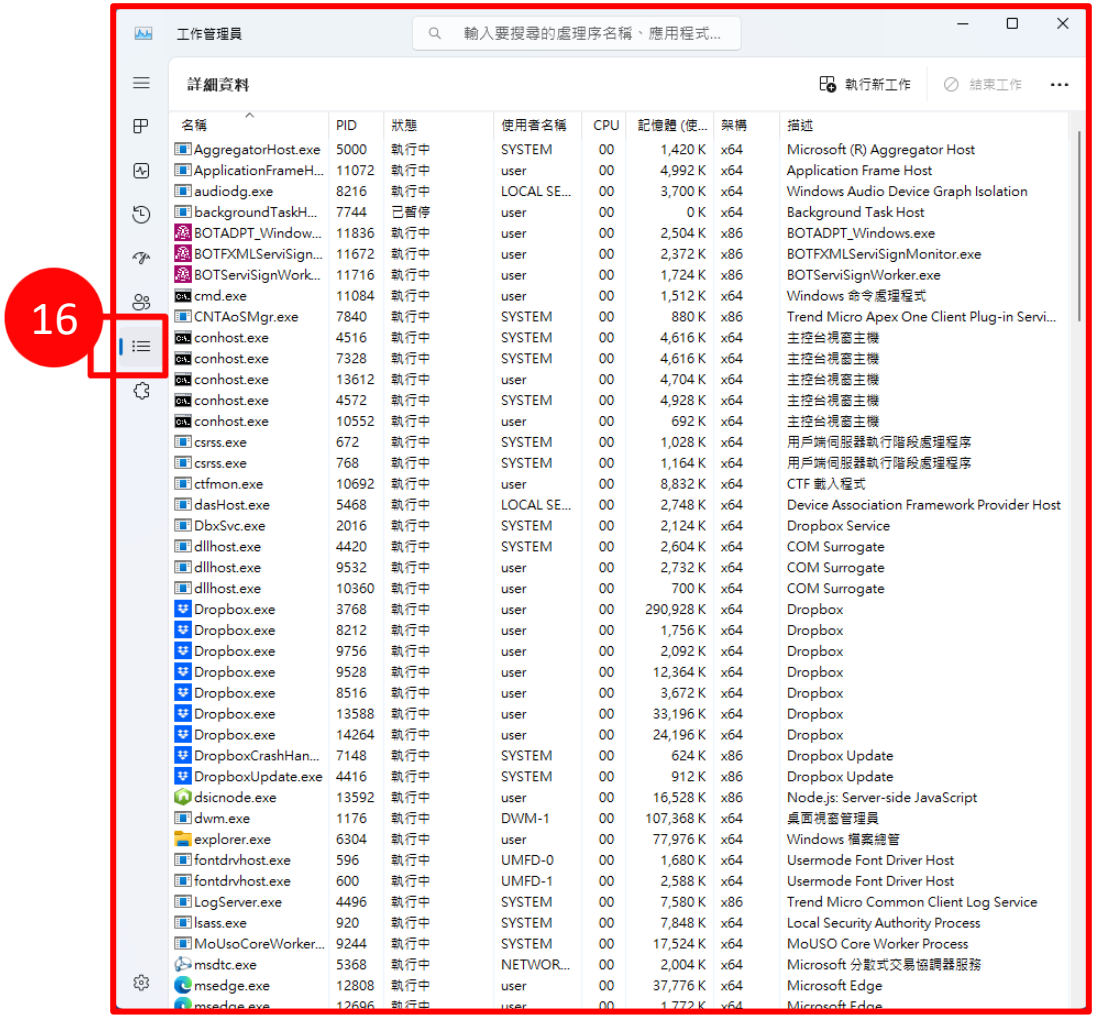
➢工作列空白處「右鍵」，點擊開啟「工作管理員」





依PID查找對應服務

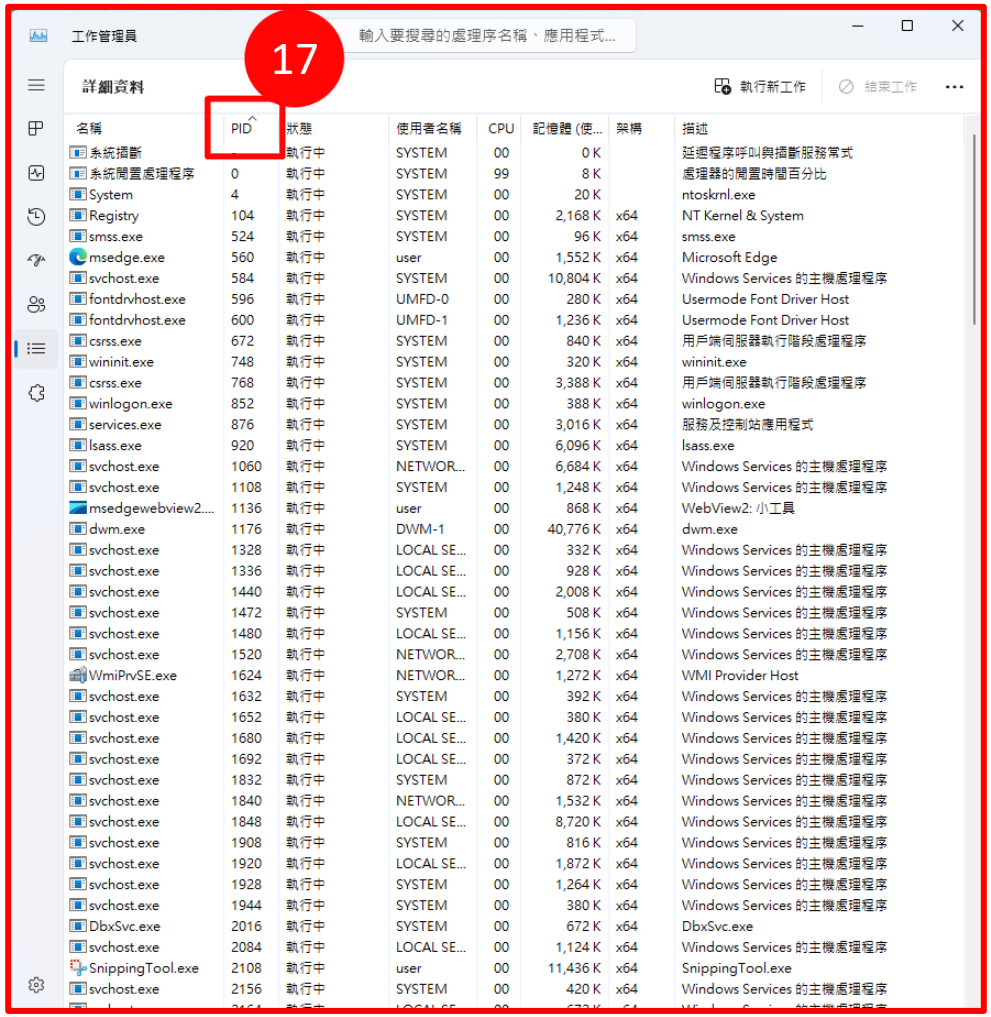
- 切換到「詳細資料」頁簽



名稱	PID	狀態	使用者名稱	CPU	記憶體 (使...	架構	描述
AggregatorHost.exe	5000	執行中	SYSTEM	00	1,420 K	x64	Microsoft (R) Aggregator Host
ApplicationFrameH...	11072	執行中	user	00	4,992 K	x64	Application Frame Host
audiodg.exe	8216	執行中	LOCAL SE...	00	3,700 K	x64	Windows Audio Device Graph Isolation
backgroundTaskH...	7744	已暫停	user	00	0 K	x64	Background Task Host
BOTADPT_Window...	11836	執行中	user	00	2,504 K	x86	BOTADPT_Windows.exe
BOTFXMLServiSign...	11672	執行中	user	00	2,372 K	x86	BOTFXMLServiSignMonitor.exe
BOTServiSignWork...	11716	執行中	user	00	1,724 K	x86	BOTServiSignWorker.exe
cmd.exe	11084	執行中	user	00	1,512 K	x64	Windows 命令處理程式
CNTAoSMgr.exe	7840	執行中	SYSTEM	00	880 K	x86	Trend Micro Apex One Client Plug-in Servi...
conhost.exe	4516	執行中	SYSTEM	00	4,616 K	x64	主控台視窗主機
conhost.exe	7328	執行中	SYSTEM	00	4,616 K	x64	主控台視窗主機
conhost.exe	13612	執行中	user	00	4,704 K	x64	主控台視窗主機
conhost.exe	4572	執行中	SYSTEM	00	4,928 K	x64	主控台視窗主機
conhost.exe	10552	執行中	user	00	692 K	x64	主控台視窗主機
csrss.exe	672	執行中	SYSTEM	00	1,028 K	x64	用戶端伺服器執行階段處理程序
csrss.exe	768	執行中	SYSTEM	00	1,164 K	x64	用戶端伺服器執行階段處理程序
ctfmon.exe	10692	執行中	user	00	8,832 K	x64	CTF 載入程式
dasHost.exe	5468	執行中	LOCAL SE...	00	2,748 K	x64	Device Association Framework Provider Host
DbxSvc.exe	2016	執行中	SYSTEM	00	2,124 K	x64	Dropbox Service
dllhost.exe	4420	執行中	SYSTEM	00	2,604 K	x64	COM Surrogate
dllhost.exe	9532	執行中	user	00	2,732 K	x64	COM Surrogate
dllhost.exe	10360	執行中	user	00	700 K	x64	COM Surrogate
Dropbox.exe	3768	執行中	user	00	290,928 K	x64	Dropbox
Dropbox.exe	8212	執行中	user	00	1,756 K	x64	Dropbox
Dropbox.exe	9756	執行中	user	00	2,092 K	x64	Dropbox
Dropbox.exe	9528	執行中	user	00	12,364 K	x64	Dropbox
Dropbox.exe	8516	執行中	user	00	3,672 K	x64	Dropbox
Dropbox.exe	13588	執行中	user	00	33,196 K	x64	Dropbox
Dropbox.exe	14264	執行中	user	00	24,196 K	x64	Dropbox
DropboxCrashHan...	7148	執行中	SYSTEM	00	624 K	x86	Dropbox Update
DropboxUpdate.exe	4416	執行中	SYSTEM	00	912 K	x86	Dropbox Update
dsicnode.exe	13592	執行中	user	00	16,528 K	x86	Node.js: Server-side JavaScript
dwm.exe	1176	執行中	DWM-1	00	107,368 K	x64	桌面視窗管理員
explorer.exe	6304	執行中	user	00	77,976 K	x64	Windows 檔案總管
fontdrvhost.exe	596	執行中	UMFD-0	00	1,680 K	x64	Usermode Font Driver Host
fontdrvhost.exe	600	執行中	UMFD-1	00	2,588 K	x64	Usermode Font Driver Host
LogServer.exe	4496	執行中	SYSTEM	00	7,580 K	x86	Trend Micro Common Client Log Service
lsass.exe	920	執行中	SYSTEM	00	7,848 K	x64	Local Security Authority Process
MoUsoCoreWorker...	9244	執行中	SYSTEM	00	17,524 K	x64	MoUSO Core Worker Process
msdtc.exe	5368	執行中	NETWOR...	00	2,004 K	x64	Microsoft 分散式交易協調器服務
msedge.exe	12808	執行中	user	00	37,776 K	x64	Microsoft Edge
msedge.exe	12696	執行中	user	00	1,772 K	x64	Microsoft Edge

依PID查找對應服務

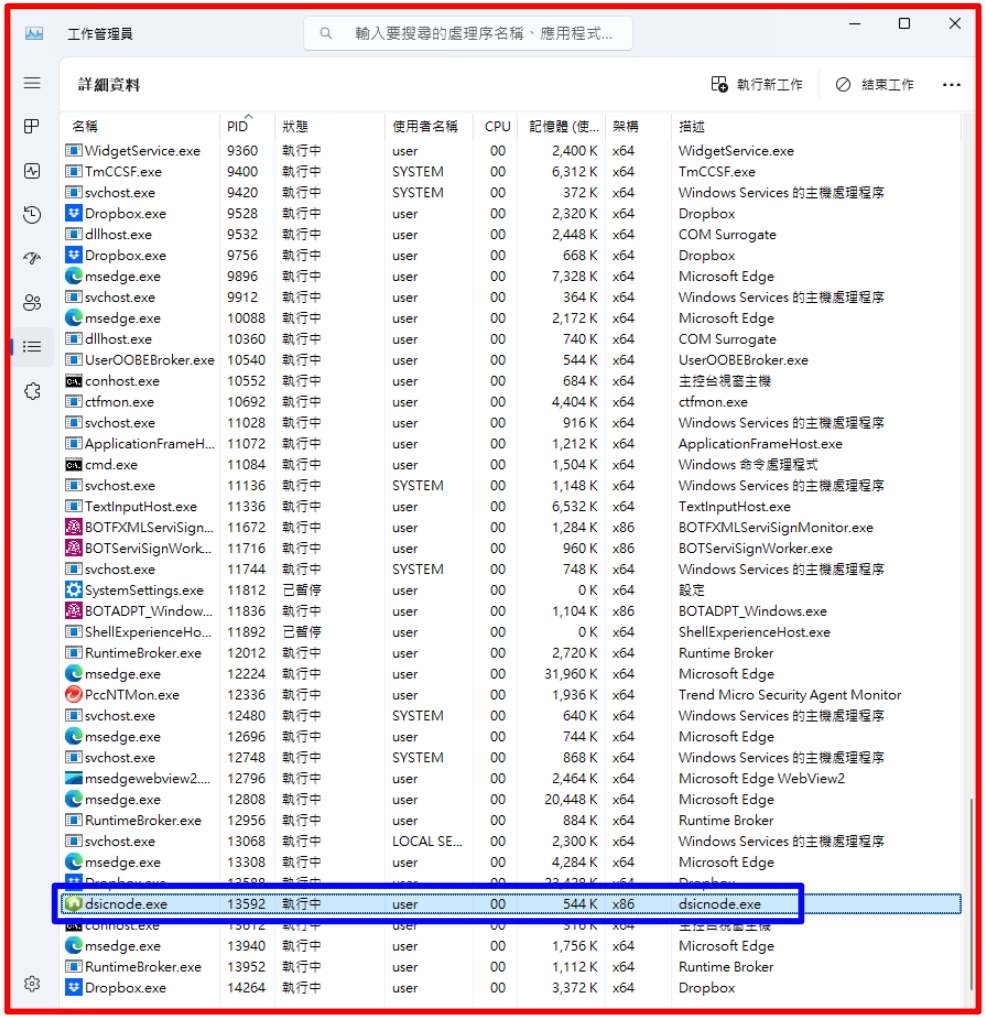
- 點擊PID欄位，依數字由小到大排序



名稱	PID	狀態	使用者名稱	CPU	記憶體 (使...	架構	描述
系統擷斷		執行中	SYSTEM	00	0 K		延遲程序呼叫與擷斷服務常式
系統閒置處理程序	0	執行中	SYSTEM	99	8 K		處理器的閒置時間百分比
System	4	執行中	SYSTEM	00	20 K		ntoskrnl.exe
Registry	104	執行中	SYSTEM	00	2,168 K	x64	NT Kernel & System
smss.exe	524	執行中	SYSTEM	00	96 K	x64	smss.exe
msedge.exe	560	執行中	user	00	1,552 K	x64	Microsoft Edge
svchost.exe	584	執行中	SYSTEM	00	10,804 K	x64	Windows Services 的主機處理程序
fontdrvhost.exe	596	執行中	UMFD-0	00	280 K	x64	Usermode Font Driver Host
fontdrvhost.exe	600	執行中	UMFD-1	00	1,236 K	x64	Usermode Font Driver Host
csrss.exe	672	執行中	SYSTEM	00	840 K	x64	用戶端伺服器執行階段處理程序
wininit.exe	748	執行中	SYSTEM	00	320 K	x64	wininit.exe
csrss.exe	768	執行中	SYSTEM	00	3,388 K	x64	用戶端伺服器執行階段處理程序
winlogon.exe	852	執行中	SYSTEM	00	388 K	x64	winlogon.exe
services.exe	876	執行中	SYSTEM	00	3,016 K	x64	服務及控制站應用程式
lsass.exe	920	執行中	SYSTEM	00	6,096 K	x64	lsass.exe
svchost.exe	1060	執行中	NETWOR...	00	6,684 K	x64	Windows Services 的主機處理程序
svchost.exe	1108	執行中	SYSTEM	00	1,248 K	x64	Windows Services 的主機處理程序
msedgewebview2....	1136	執行中	user	00	868 K	x64	WebView2: 小工具
dwm.exe	1176	執行中	DWM-1	00	40,776 K	x64	dwm.exe
svchost.exe	1328	執行中	LOCAL SE...	00	332 K	x64	Windows Services 的主機處理程序
svchost.exe	1336	執行中	LOCAL SE...	00	928 K	x64	Windows Services 的主機處理程序
svchost.exe	1440	執行中	LOCAL SE...	00	2,008 K	x64	Windows Services 的主機處理程序
svchost.exe	1472	執行中	SYSTEM	00	508 K	x64	Windows Services 的主機處理程序
svchost.exe	1480	執行中	LOCAL SE...	00	1,156 K	x64	Windows Services 的主機處理程序
svchost.exe	1520	執行中	NETWOR...	00	2,708 K	x64	Windows Services 的主機處理程序
WmiPrvSE.exe	1624	執行中	NETWOR...	00	1,272 K	x64	WMI Provider Host
svchost.exe	1632	執行中	SYSTEM	00	392 K	x64	Windows Services 的主機處理程序
svchost.exe	1652	執行中	LOCAL SE...	00	380 K	x64	Windows Services 的主機處理程序
svchost.exe	1680	執行中	LOCAL SE...	00	1,420 K	x64	Windows Services 的主機處理程序
svchost.exe	1692	執行中	LOCAL SE...	00	372 K	x64	Windows Services 的主機處理程序
svchost.exe	1832	執行中	SYSTEM	00	872 K	x64	Windows Services 的主機處理程序
svchost.exe	1840	執行中	NETWOR...	00	1,532 K	x64	Windows Services 的主機處理程序
svchost.exe	1848	執行中	LOCAL SE...	00	8,720 K	x64	Windows Services 的主機處理程序
svchost.exe	1908	執行中	SYSTEM	00	816 K	x64	Windows Services 的主機處理程序
svchost.exe	1920	執行中	LOCAL SE...	00	1,872 K	x64	Windows Services 的主機處理程序
svchost.exe	1928	執行中	SYSTEM	00	1,264 K	x64	Windows Services 的主機處理程序
svchost.exe	1944	執行中	SYSTEM	00	380 K	x64	Windows Services 的主機處理程序
DbxSvc.exe	2016	執行中	SYSTEM	00	672 K	x64	DbxSvc.exe
svchost.exe	2084	執行中	LOCAL SE...	00	1,124 K	x64	Windows Services 的主機處理程序
SnippingTool.exe	2108	執行中	user	00	11,436 K	x64	SnippingTool.exe
svchost.exe	2156	執行中	SYSTEM	00	420 K	x64	Windows Services 的主機處理程序

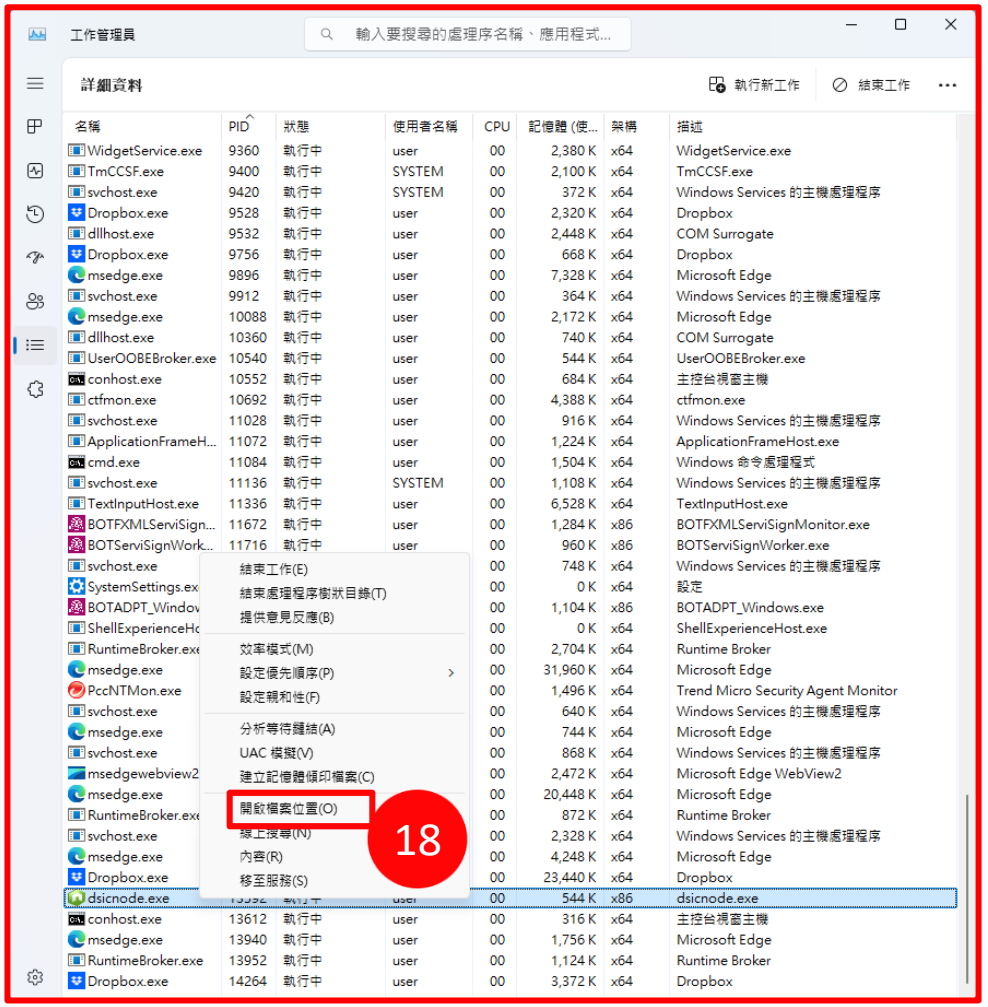
依PID查找對應服務

- 找到PID為「13592」的執行程序



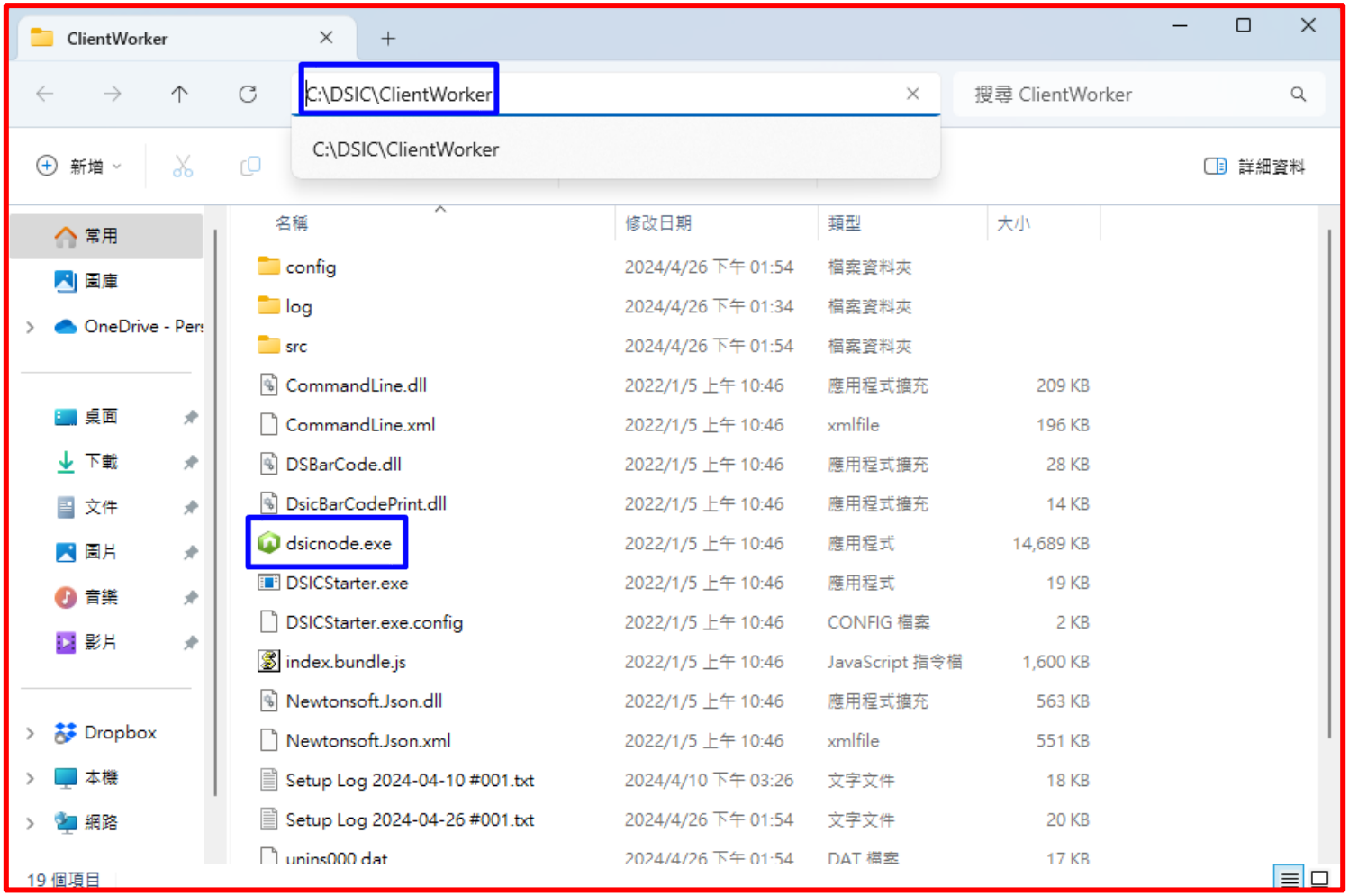
查找服務安裝目錄

➢ 對執行程序點「右鍵」，點選「開啟檔案位置」



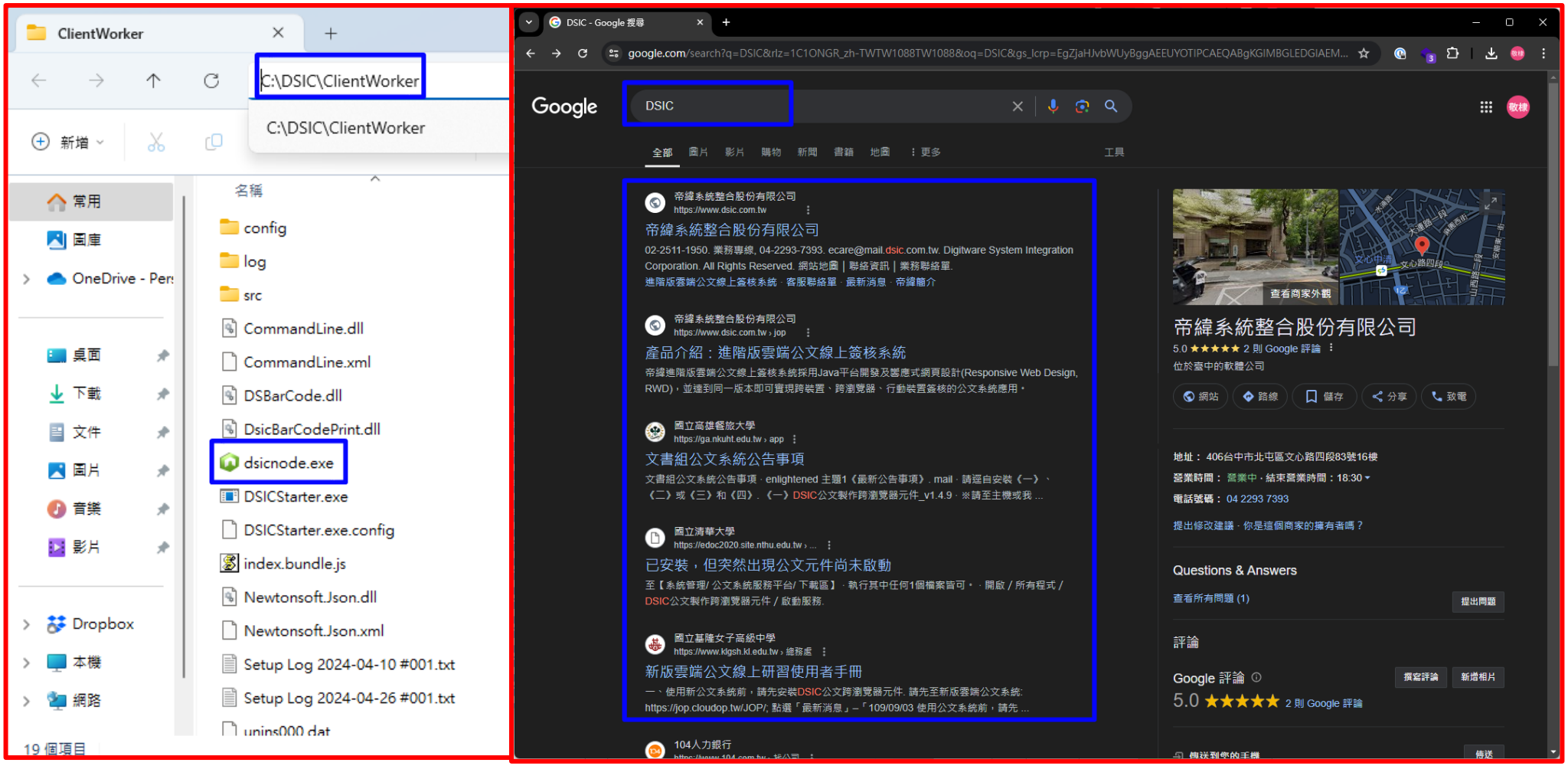
查找服務安裝目錄

- 開啟該執行程序安裝的位置，可以從目錄路徑或程式名稱判斷服務



已經找到安裝路徑了，還是看不出服務

- 把安裝路徑或程式名稱丟到瀏覽器查詢…

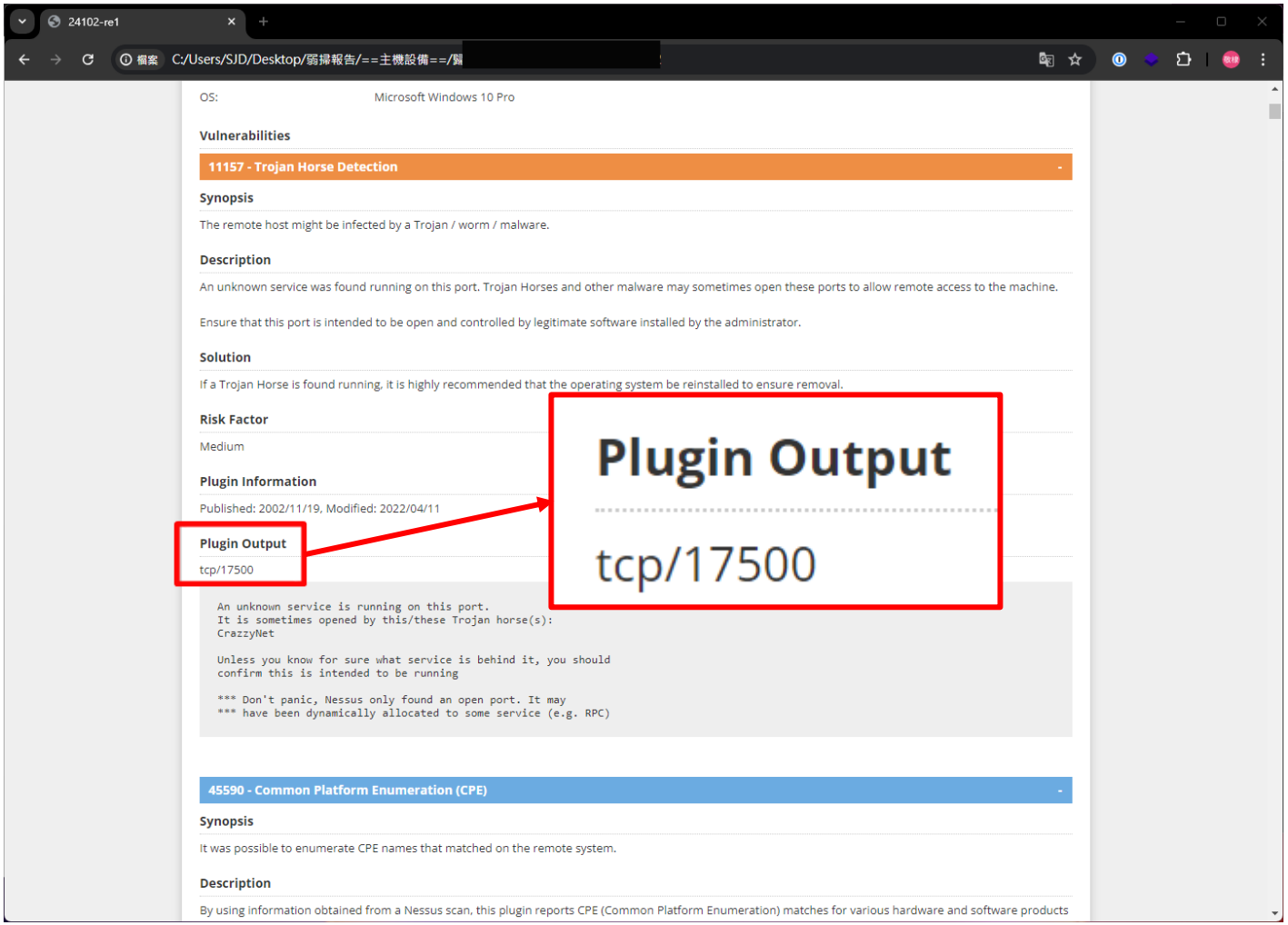


結論

- 看SSL憑證，初步先判斷弱點出現在哪個服務
- 從系統工作程序再次確認是哪個服務
  - ✓如果目標程式當下不是運作中，用這個方法可能會找不到服務
  - ✓如果查到PID為4，表示該服務以系統層級運行，可以從本機防火牆找對應通訊埠的規則再判斷該規則套用的服務是哪個

11157 - Trojan Horse Detection

- 先看「plugin output」，找到通訊埠為tcp 17500

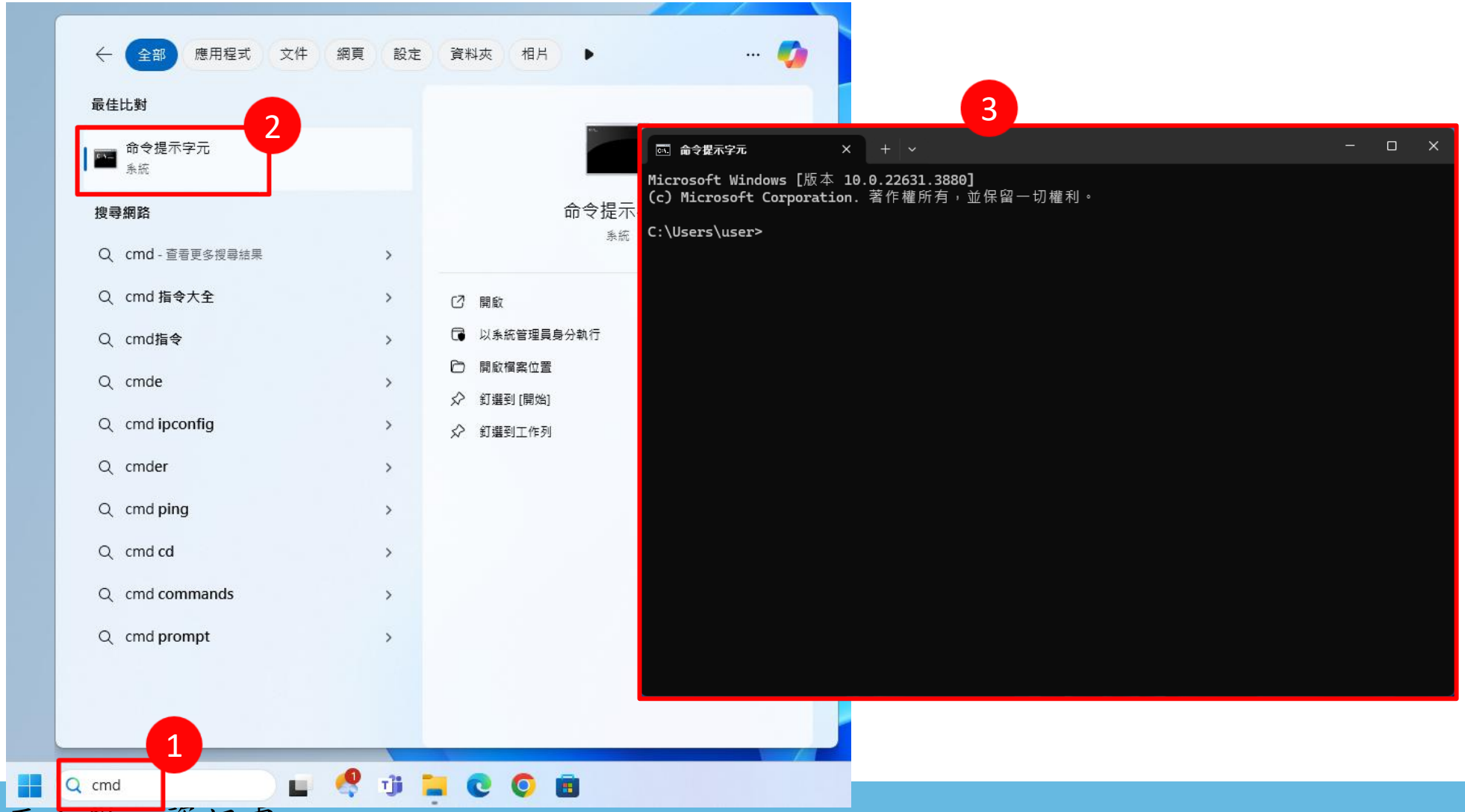


11157 - Trojan Horse Detection

- 這一項弱點原因是找不到SSL憑證，弱掃工具判斷可能是惡意植入的程式或服務
- 從系統工作程序找看看

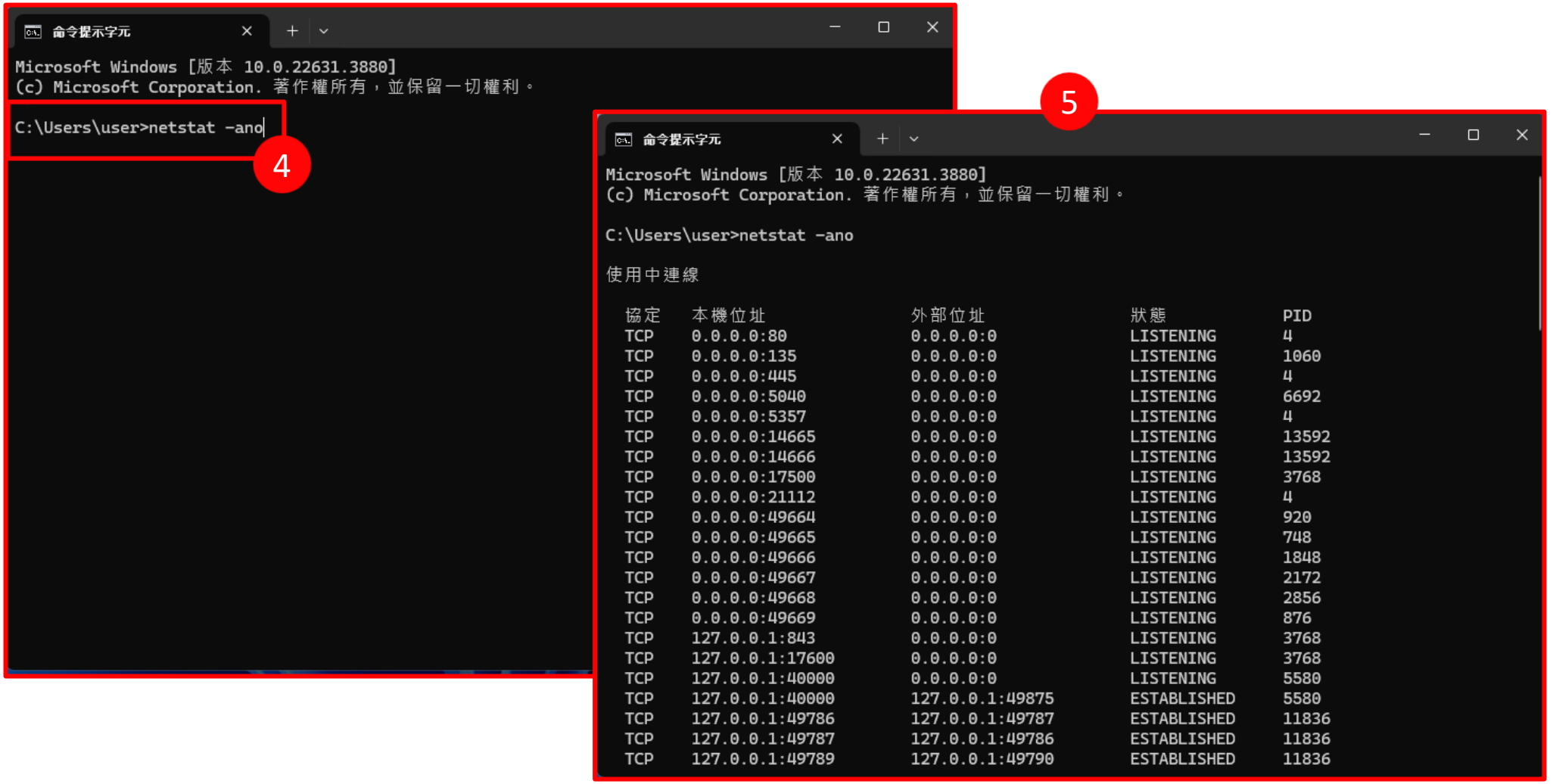
從系統工作程序找服務

➢ 工作列搜尋「cmd」，點擊開啟「命令提示字元」



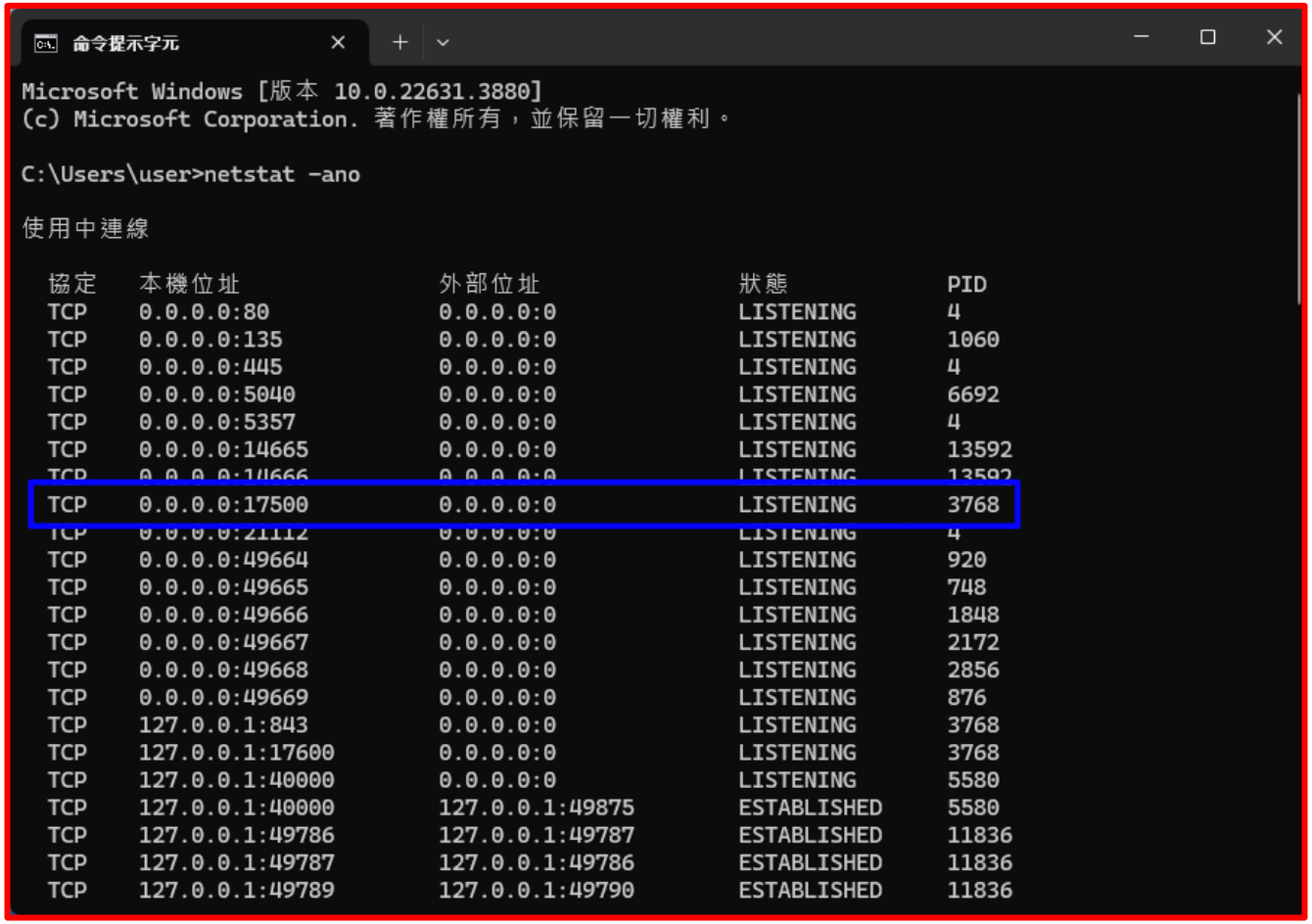
netstat指令

➢ 輸入指令「netstat -ano」，按鍵盤「Enter」執行指令



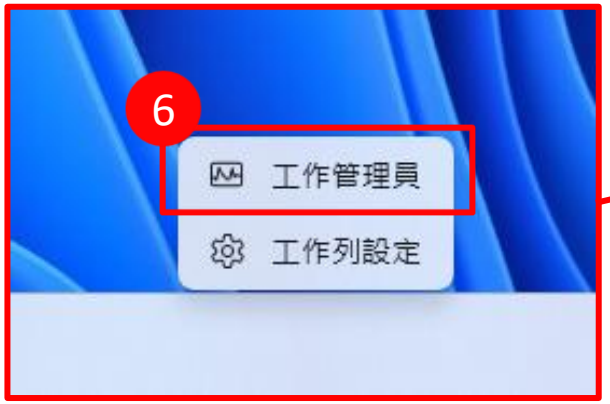
查找系統進程識別碼PID

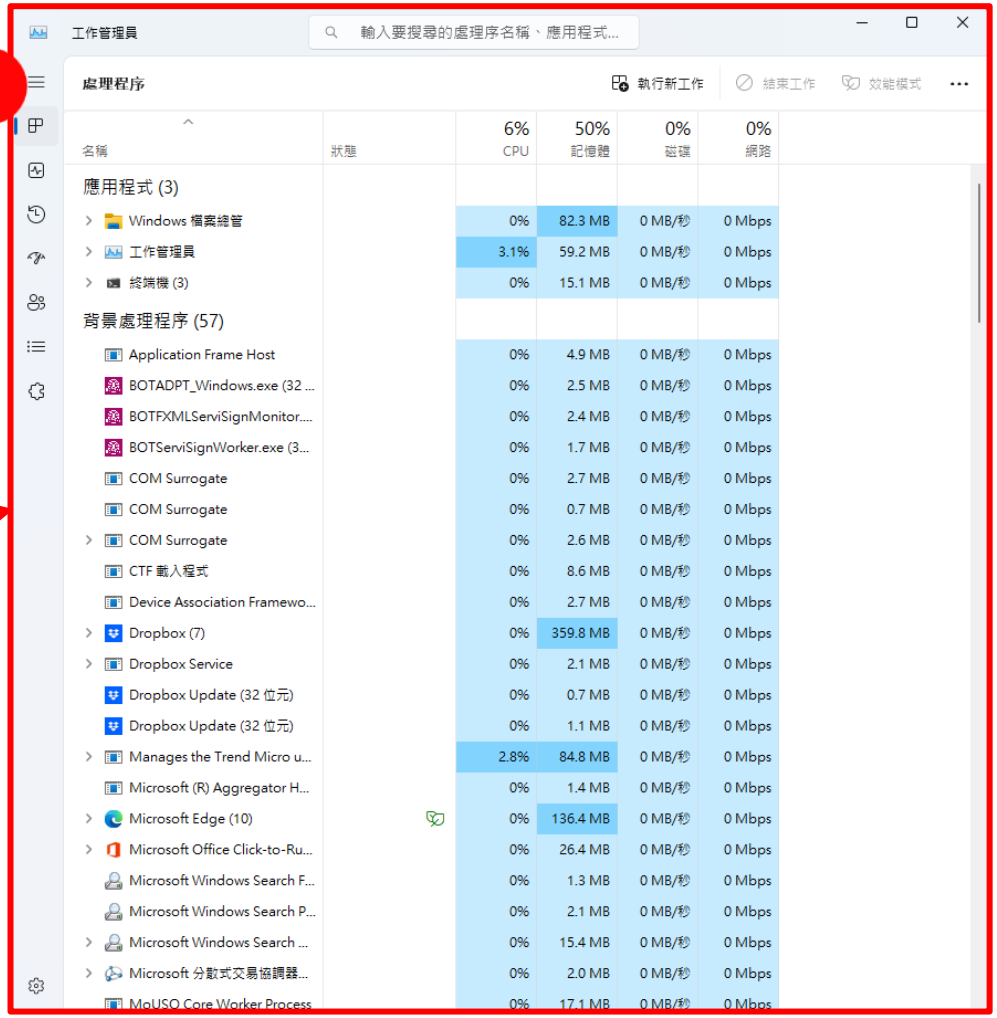
- 依報告找到TCP 17500的項目
- 找到對應的PID ，以本案為例PID為「3768」



依PID查找對應服務

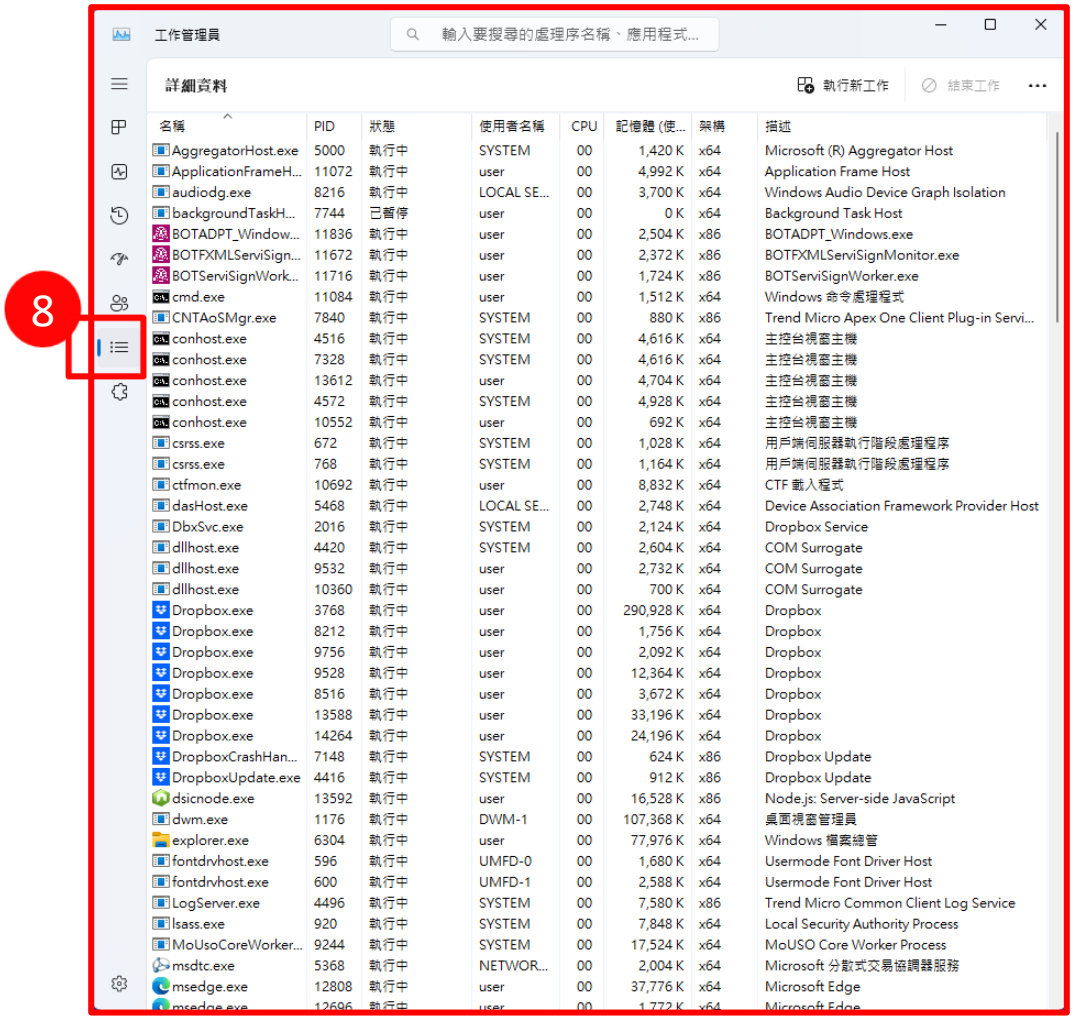
➢工作列空白處「右鍵」，點擊開啟「工作管理員」





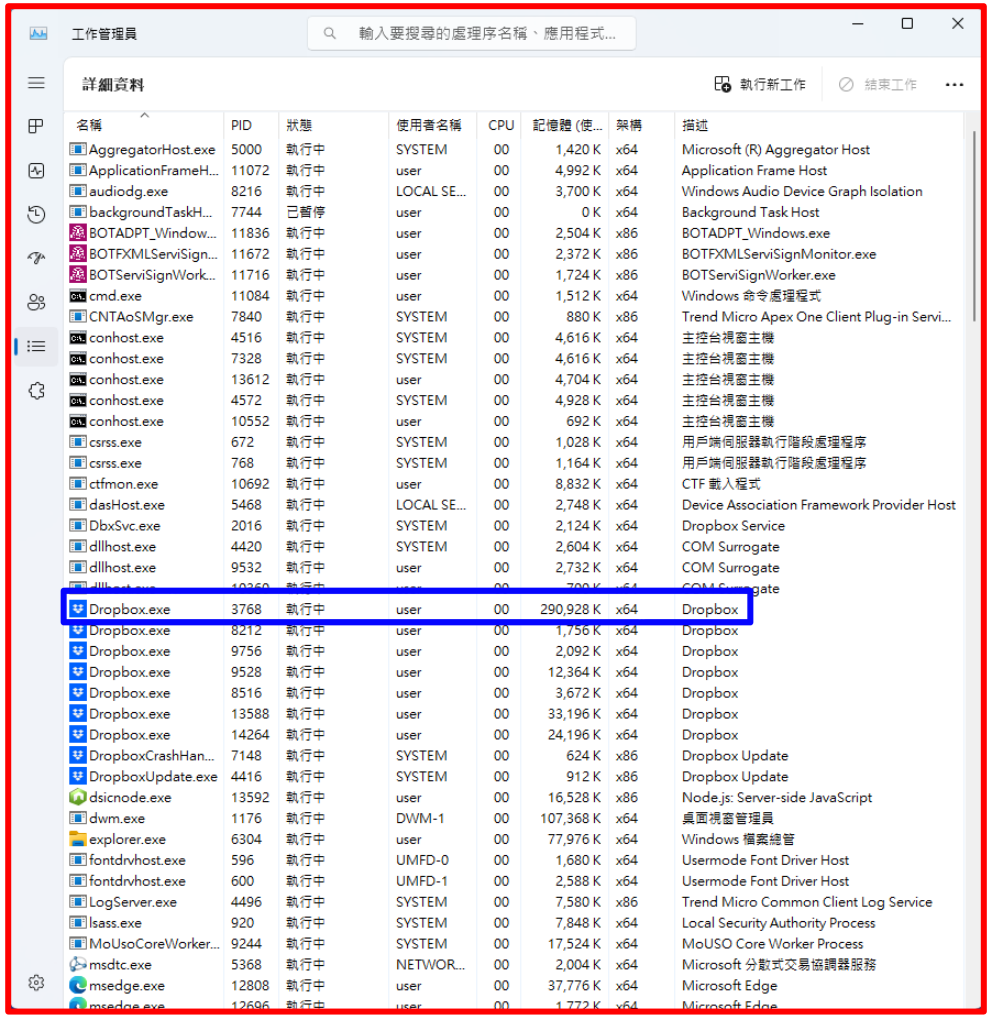
依PID查找對應服務

- 切換到「詳細資料」頁簽



依PID查找對應服務

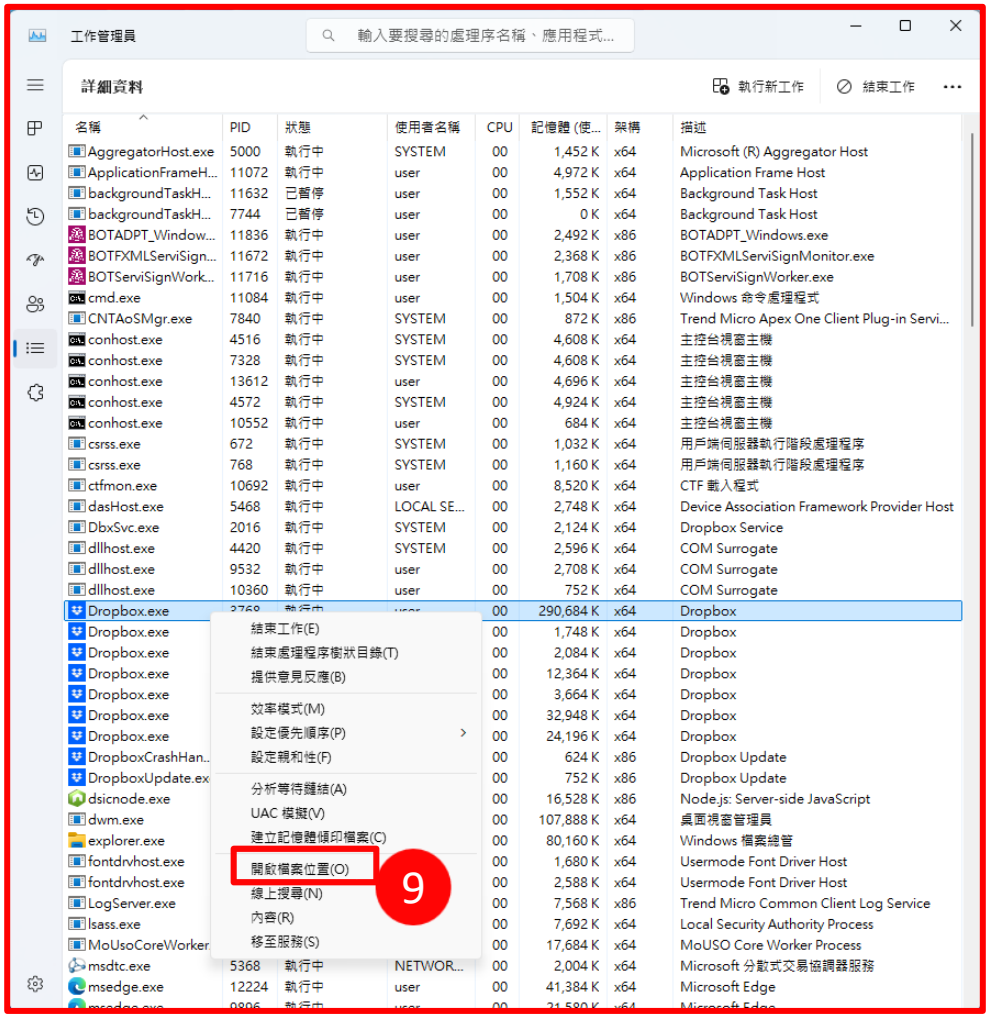
- 找到PID為「3768」的執行程序



名稱	PID	狀態	使用者名稱	CPU	記憶體 (使...	架構	描述
AggregatorHost.exe	5000	執行中	SYSTEM	00	1,420 K	x64	Microsoft (R) Aggregator Host
ApplicationFrameH...	11072	執行中	user	00	4,992 K	x64	Application Frame Host
audiodg.exe	8216	執行中	LOCAL SE...	00	3,700 K	x64	Windows Audio Device Graph Isolation
backgroundTaskH...	7744	已暫停	user	00	0 K	x64	Background Task Host
BOTADPT_Window...	11836	執行中	user	00	2,504 K	x86	BOTADPT_Windows.exe
BOTFXMLServiSign...	11672	執行中	user	00	2,372 K	x86	BOTFXMLServiSignMonitor.exe
BOTServiSignWork...	11716	執行中	user	00	1,724 K	x86	BOTServiSignWorker.exe
cmd.exe	11084	執行中	user	00	1,512 K	x64	Windows 命令處理程式
CNTAoSMgr.exe	7840	執行中	SYSTEM	00	880 K	x86	Trend Micro Apex One Client Plug-in Servi...
conhost.exe	4516	執行中	SYSTEM	00	4,616 K	x64	主控台視窗主機
conhost.exe	7328	執行中	SYSTEM	00	4,616 K	x64	主控台視窗主機
conhost.exe	13612	執行中	user	00	4,704 K	x64	主控台視窗主機
conhost.exe	4572	執行中	SYSTEM	00	4,928 K	x64	主控台視窗主機
conhost.exe	10552	執行中	user	00	692 K	x64	主控台視窗主機
csrss.exe	672	執行中	SYSTEM	00	1,028 K	x64	用戶端伺服器執行階段處理程序
csrss.exe	768	執行中	SYSTEM	00	1,164 K	x64	用戶端伺服器執行階段處理程序
ctfmon.exe	10692	執行中	user	00	8,832 K	x64	CTF 載入程式
dasHost.exe	5468	執行中	LOCAL SE...	00	2,748 K	x64	Device Association Framework Provider Host
DbxSvc.exe	2016	執行中	SYSTEM	00	2,124 K	x64	Dropbox Service
dllhost.exe	4420	執行中	SYSTEM	00	2,604 K	x64	COM Surrogate
dllhost.exe	9532	執行中	user	00	2,732 K	x64	COM Surrogate
Dropbox.exe	3768	執行中	user	00	290,928 K	x64	Dropbox
Dropbox.exe	8212	執行中	user	00	1,756 K	x64	Dropbox
Dropbox.exe	9756	執行中	user	00	2,092 K	x64	Dropbox
Dropbox.exe	9528	執行中	user	00	12,364 K	x64	Dropbox
Dropbox.exe	8516	執行中	user	00	3,672 K	x64	Dropbox
Dropbox.exe	13588	執行中	user	00	33,196 K	x64	Dropbox
Dropbox.exe	14264	執行中	user	00	24,196 K	x64	Dropbox
DropboxCrashHan...	7148	執行中	SYSTEM	00	624 K	x86	Dropbox Update
DropboxUpdate.exe	4416	執行中	SYSTEM	00	912 K	x86	Dropbox Update
dsicnode.exe	13592	執行中	user	00	16,528 K	x86	Node.js: Server-side JavaScript
dwm.exe	1176	執行中	DWM-1	00	107,368 K	x64	桌面視窗管理員
explorer.exe	6304	執行中	user	00	77,976 K	x64	Windows 檔案總管
fontdrvhost.exe	596	執行中	UMFD-0	00	1,680 K	x64	Usermode Font Driver Host
fontdrvhost.exe	600	執行中	UMFD-1	00	2,588 K	x64	Usermode Font Driver Host
LogServer.exe	4496	執行中	SYSTEM	00	7,580 K	x86	Trend Micro Common Client Log Service
lsass.exe	920	執行中	SYSTEM	00	7,848 K	x64	Local Security Authority Process
MoUsoCoreWorker...	9244	執行中	SYSTEM	00	17,524 K	x64	MoUSO Core Worker Process
msdtc.exe	5368	執行中	NETWOR...	00	2,004 K	x64	Microsoft 分散式交易協調器服務
msedge.exe	12808	執行中	user	00	37,776 K	x64	Microsoft Edge

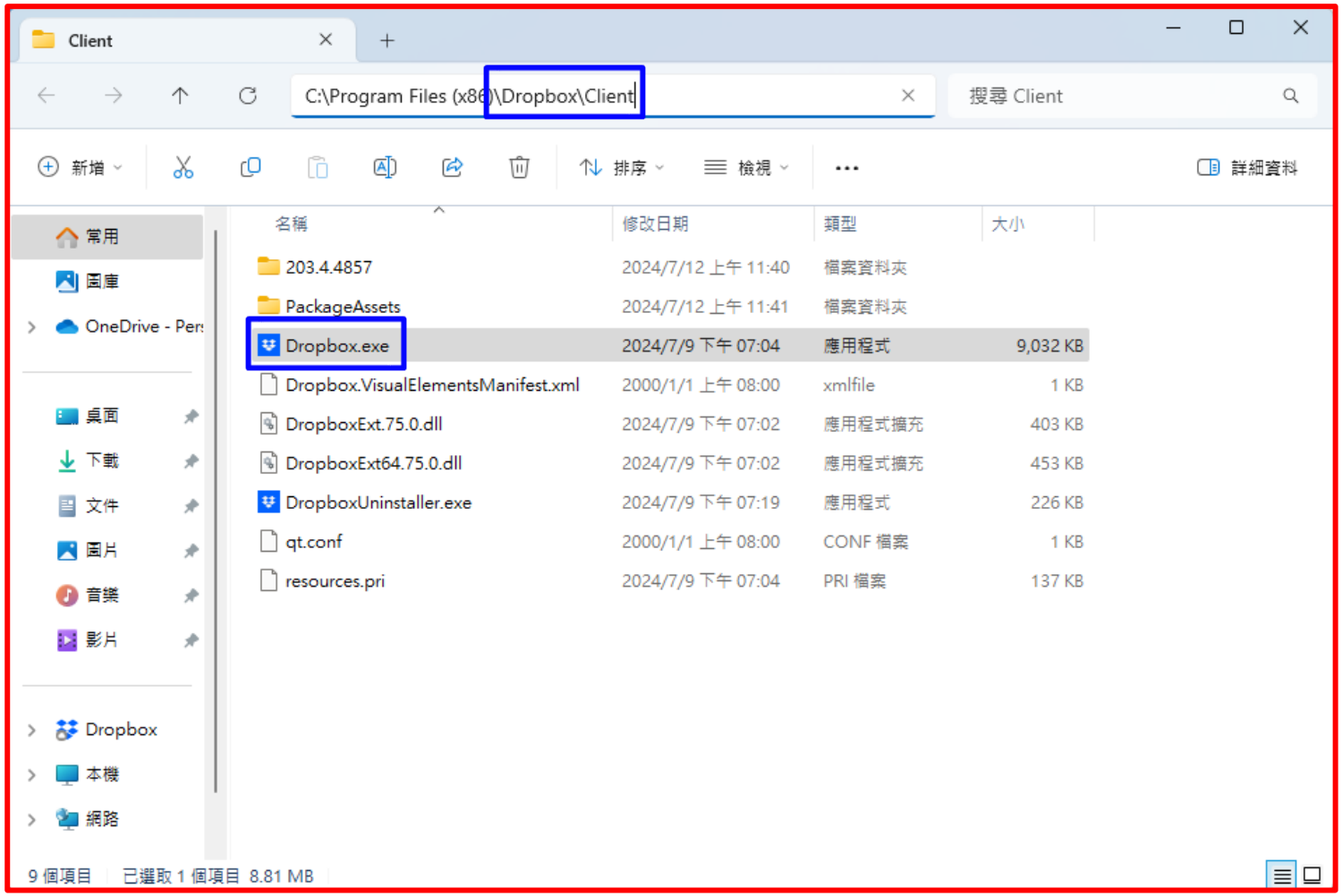
查找服務安裝目錄

- 對執行程序點「右鍵」，點選「開啟檔案位置」



查找服務安裝目錄

- 開啟該執行程序安裝的位置，可以從目錄路徑或程式名稱判斷服務
- 判斷port 17500為Dropbox使用，非惡意程式或服務，弱點11157可以列為誤判



補充說明

- 這個方法有可能因為當下程式未啟動執行或程式自動更換連接埠等因素導致後續查找時找不到
- 建議再複測一次確認結果是否仍相同

資訊處
Office of Information Technology

常見弱點修補建議

套件、韌體版本不足

- Apache、Tomcat、OpenSSL、MariaDB、Mysql、PHP……等
  - ✓ 153583 - Apache < 2.4.49 Multiple Vulnerabilities
  - ✓ 161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
  - ✓ 48255 - Apache Tomcat 6.0 < 6.0.28 Multiple Vulnerabilities
  - ✓ 160480 - OpenSSL 1.0.2 < 1.0.2ze Vulnerability
  - ✓ 164027 - MariaDB 10.8.0 < 10.8.4 Multiple Vulnerabilities
  - ✓ ……
  - ✓ 更新相對應的套件至最新

- 物聯網設備韌體
  - ✓ DLink DIR-859 < 1.07B03 Information Disclosure
  - ✓ DLink DIR-859 1.05 & 1.06B01 Multiple Vulnerabilities (RCE)
  - ✓ ……
  - ✓ 更新設備韌體至最新

SSL憑證加密與TLS協定相關

- 94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
- 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
- 104743 - TLS Version 1.0 Protocol Detection
- 157288 - TLS Version 1.1 Deprecated Protocol
- 在windows系統上，部分系統內建或使用者安裝的程式，其服務會透過windows Schannel建立安全通道，而系統預設的TLS protocal及SSL ciphers suite可能有啟用不安全的版本
  - ✓ 以 Windows 10 系統及 Apex One 防毒軟體為例，Apex One 僅支援 TLS 1.2 或以上版本的協定，並採用 AES-128、AES-256 或更高安全性的加密演算法。然而，由於 Windows 10 的 Schannel 預設啟用 TLS 1.0、TLS 1.1 協定及 3DES 加密演算法，導致工具檢測顯示 Apex One 防毒軟體有使用 TLS 1.0、TLS 1.1 及 3DES 等不安全的通訊協定及加密演算法。
  - ✓ 簡而言之，即使程式本身僅使用安全的通訊協定與加密演算法，由於 Schannel 啟用了不安全的協定與加密，檢測結果仍會判定程式使用了不安全的協定與加密。
- 解決方法：
  - ✓ 修改登錄檔(regedit)，將Schannel停用不安全的通訊協定及加密演算法(建議的方法)。
  - ✓ 作業系統更新(需等官方釋出相關patch，時間未知。目前windows11 Schannel預設已停用3des，但有仍啟用TLS1.0、TLS1.1)。

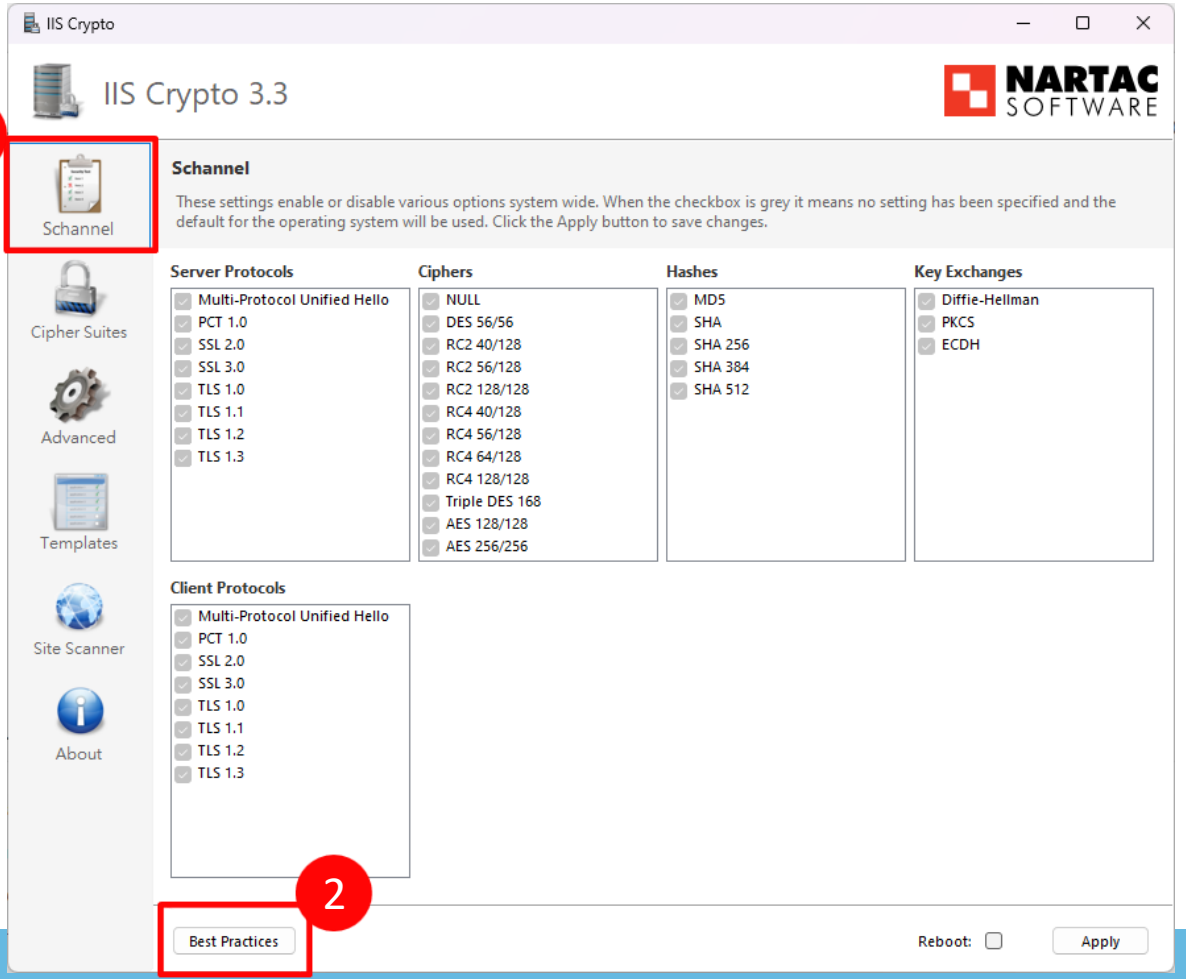
IIS Crypto

- 請下載「IIS Crypto」
- 連結：https://www.nartac.com/Downloads/IISCrypto/IISCrypto.exe

IIS Crypto

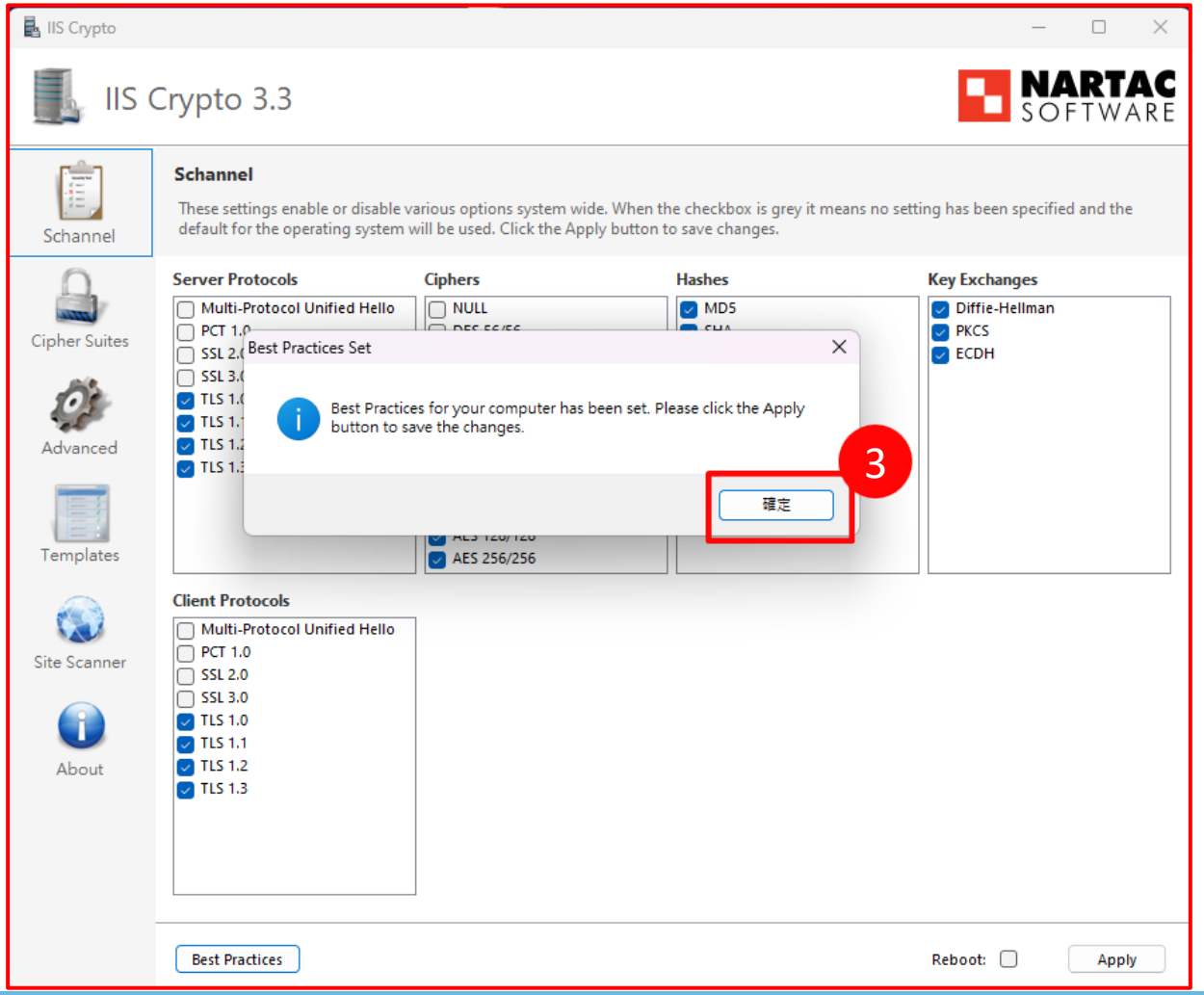
- 點擊 

打開程式
- 在「Schannel」分頁，點選「Best Practices」



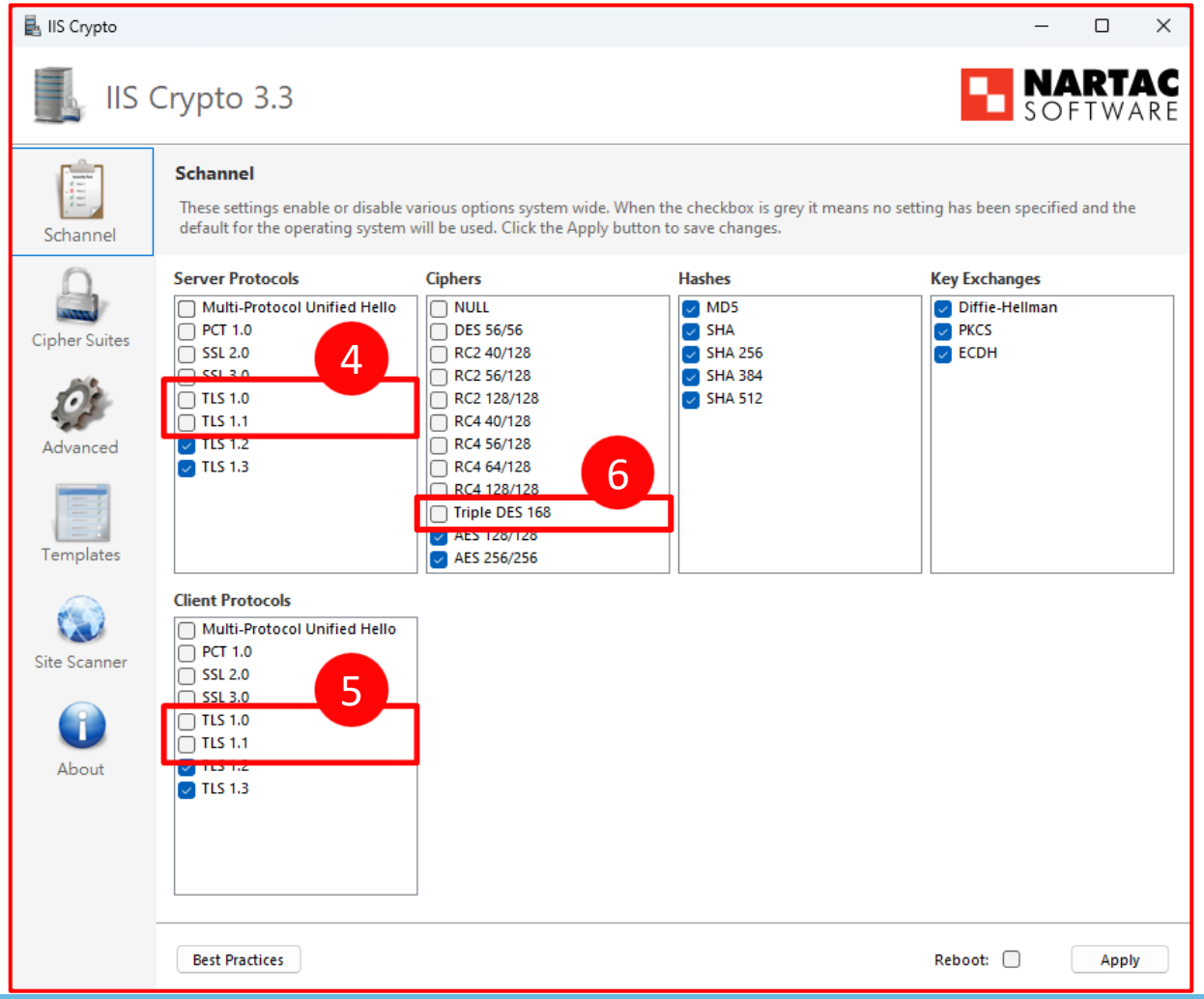
IIS Crypto

➢跳出提示告知已完成設定，點擊「確定」



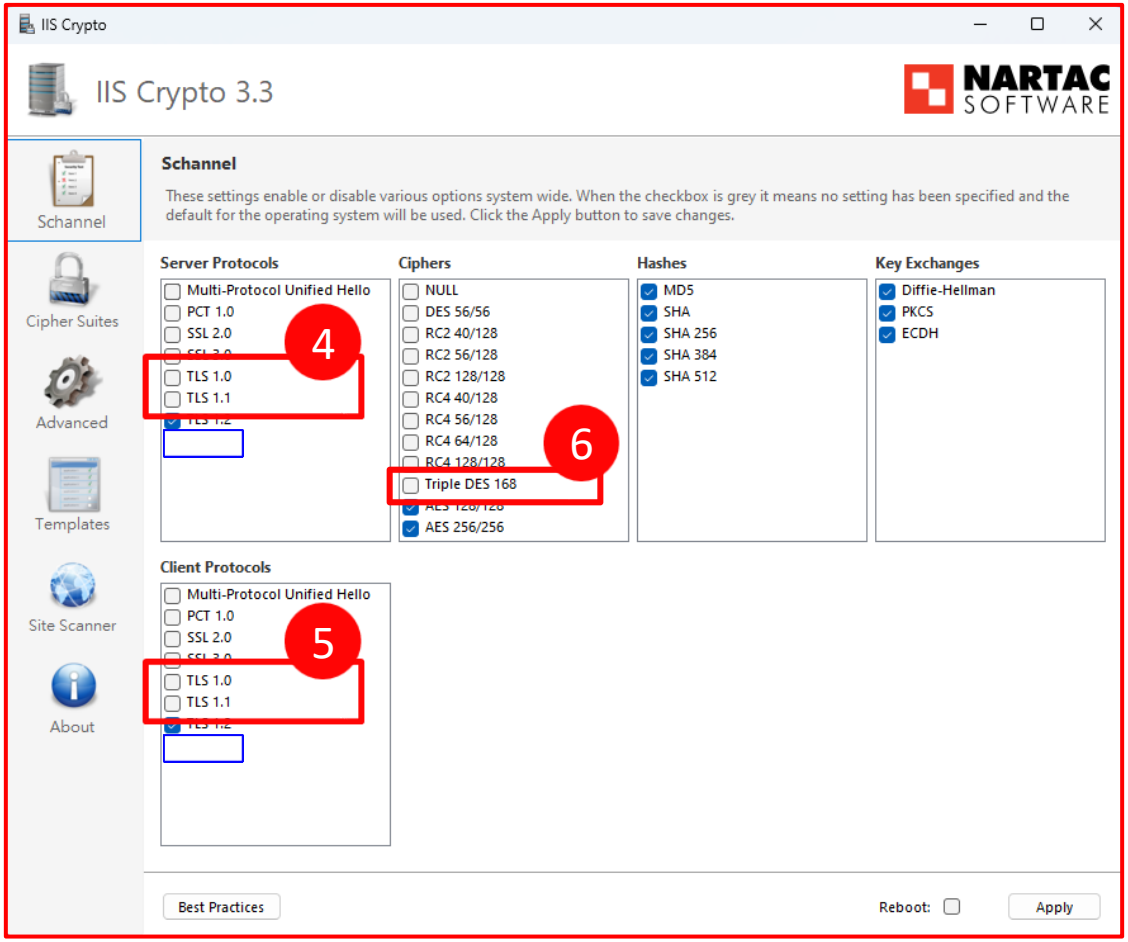
IIS Crypto - win11

- 反勾選TLS1.0、TLS1.1及Triple DES 168



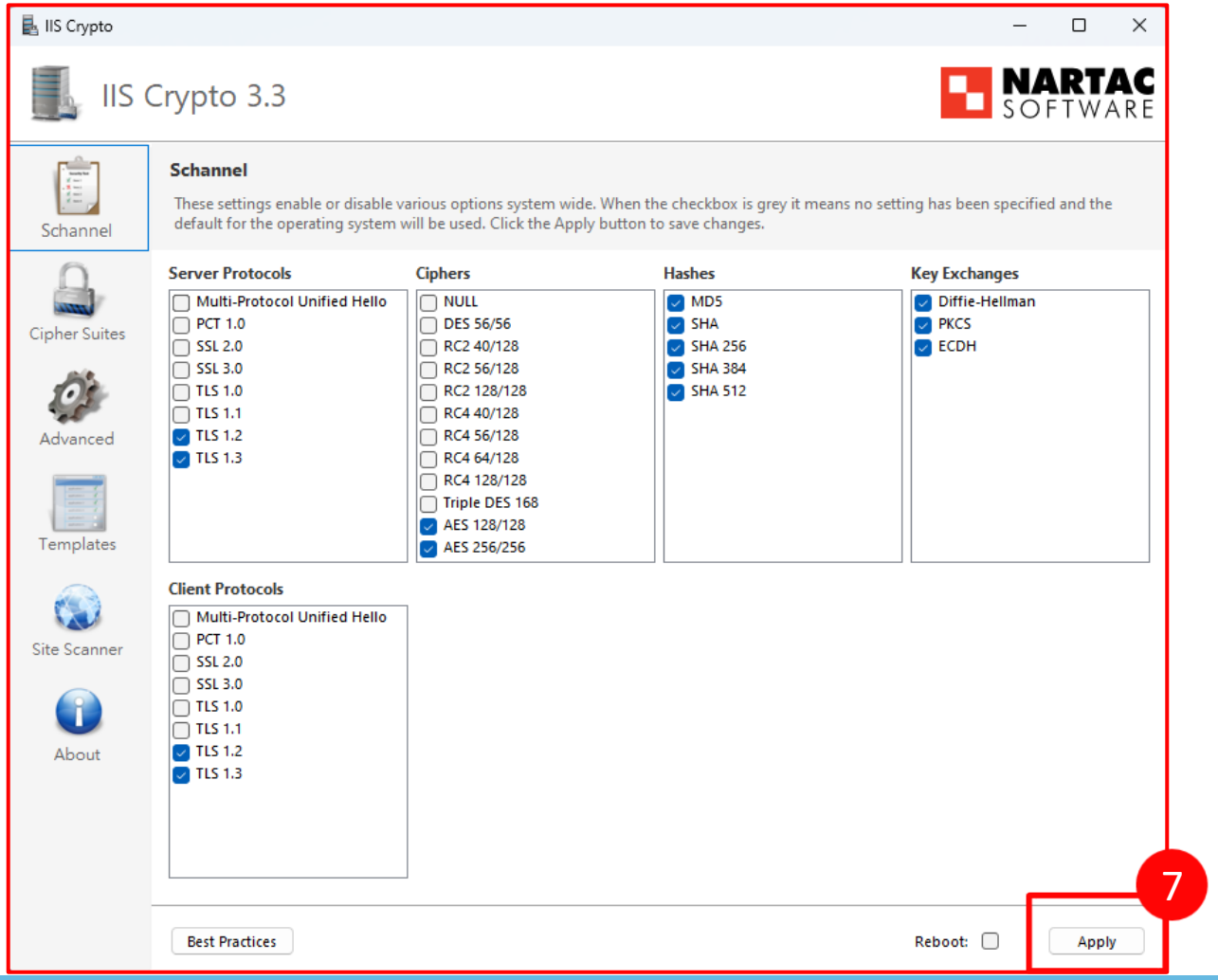
IIS Crypto - win10

- 因作業系統不同，win10可能沒有TLS1.3的選項，但一樣將TLS1.0、TLS1.1及Triple DES 168反勾選



IIS Crypto

➢點擊「Apply」保存，並重新啟動電腦讓設定生效



同時解決與Schannel有關的弱點

- 此方法僅適用作業系統為windows或windows server的電腦與主機
- 其他相關弱點也能一併解決：
  - ✓60108 - SSL Certificate Chain Contains Weak RSA Keys
  - ✓42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
  - ✓65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
  - ✓20007 - SSL Version 2 and 3 Protocol Detection
  - ✓26928 - SSL Weak Cipher Suites Supported
  - ✓104743 - TLS Version 1.0 Protocol Detection
  - ✓157288 - TLS Version 1.1 Protocol Deprecated

非透過Schannel執行的程式

- 以下幾項服務用修補後可能還是會掃到相同弱點(只列出弱掃常見的項目)
- 這幾項元件類的程式因本身有定義TLS協定及加密演算法，沒有透過Schannel執行，僅能從程式本身去修正。因非使用者可以自行修補的項目，若為公務必須，建議元件嘗試更新至最新；若非公務必須，請自行評估使用

port	用途
7777	健保卡驗證元件
14665	帝緯公文系統公文製作元件 (本校元件已於113.04.26更新，新元件弱掃後未發現相關弱點)
39021	中華郵政網路ATM元件
56306	ServiSign多憑證元件，可能用於需要自然人憑證、健保卡、銀行金融卡等的系統

微軟遠端桌面(RDP)相關

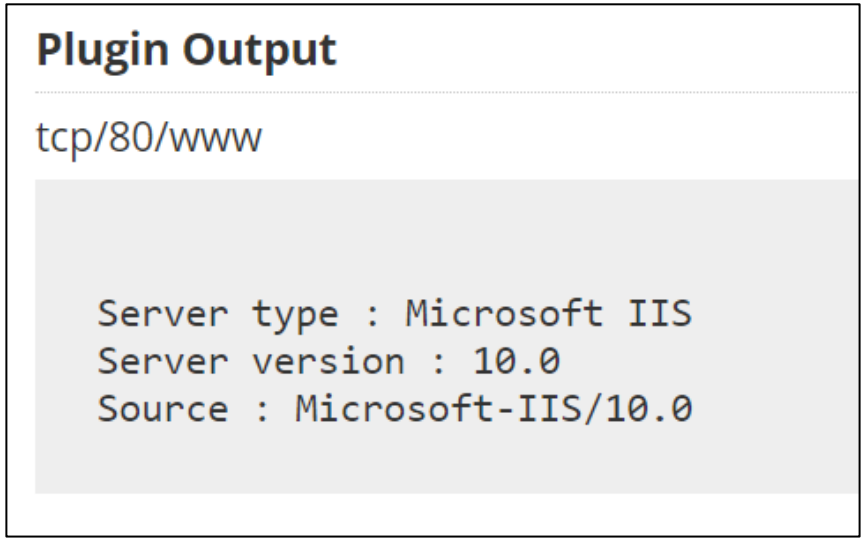
- 42873 - Medium Strength Cipher Suites Supported (SWEET32)
- 94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
- 104743 - TLS Version 1.0 Protocol Detection
- 157288 - TLS Version 1.1 Protocol Deprecated
  - ✓ 以上幾項都可以用IISCrypto處理
- 18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness
  - ✓ 請檢查遠端連線設定是否有啟用「要求裝置使用網路層級進行連線(建議)」

微軟遠端桌面(RDP)相關

- 遠端連線建議限定特定IP或範圍
- 參閱本處手冊P7~P17
  - ✓連結：https://it.ccu.edu.tw/var/file/9/1009/img/1856/186640335.pdf

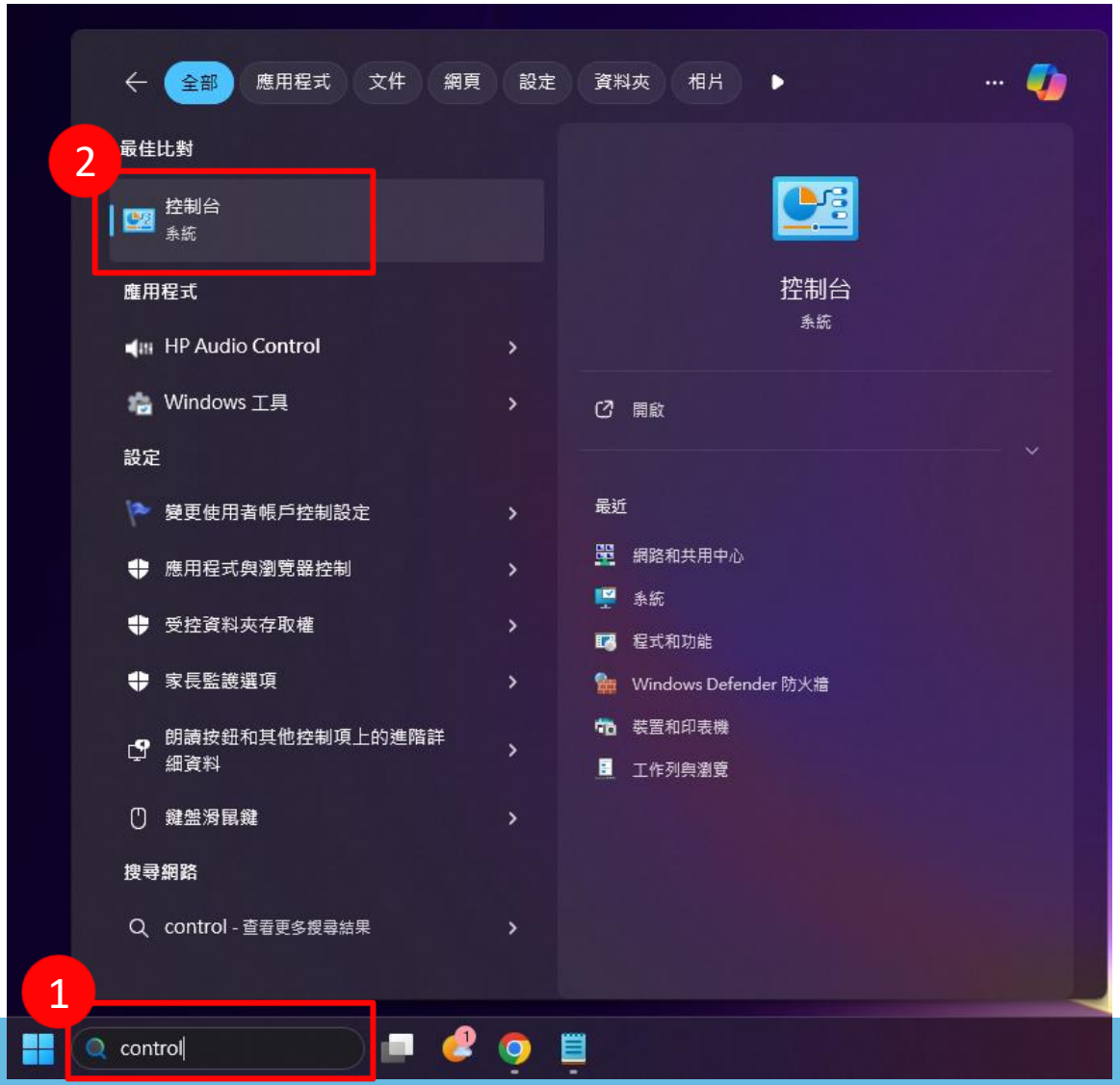
微軟IIS服務

- 106609 - Microsoft Windows IIS Default Index Page
- 88099 - Web Server HTTP Header Information Disclosure
  - ✓部分單位弱掃發現有開啟IIS相關功能但使用者不知情
  - ✓請先確認有發現這個弱點的設備是否作為「網頁伺服器」使用
    - 是，請針對弱點處理，將預設頁面移除(或停用預設站點)、移除Header的伺服器資訊
    - 否，請依操作進行確認與關閉服務，操作以windows11環境做示範，windows10的操作邏輯相同



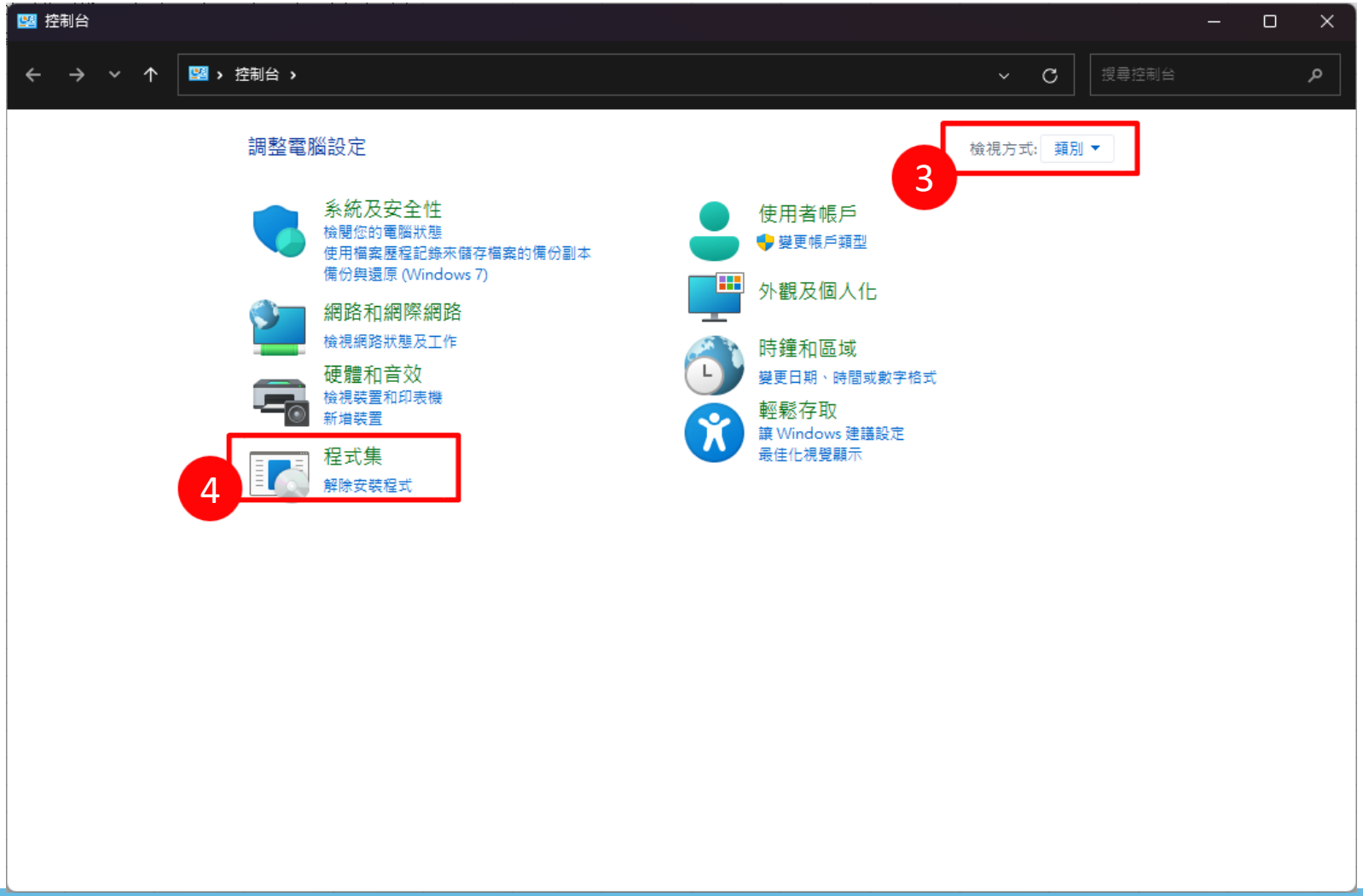
關閉微軟IIS服務

- 工作列搜尋欄輸入「control」，點擊「控制台」



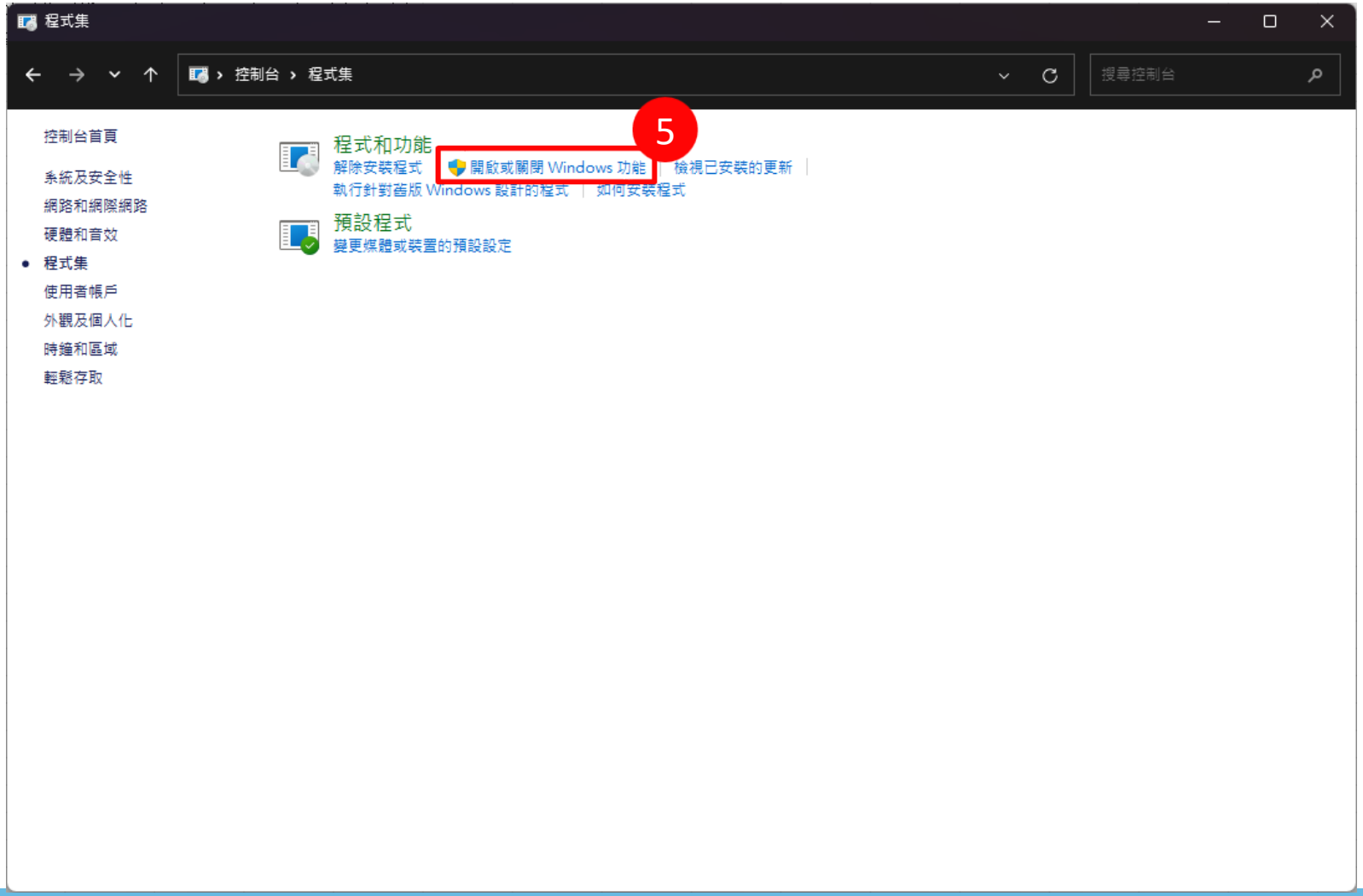
關閉微軟IIS服務

➢切換檢視方式為「類別」，點選「程式集」



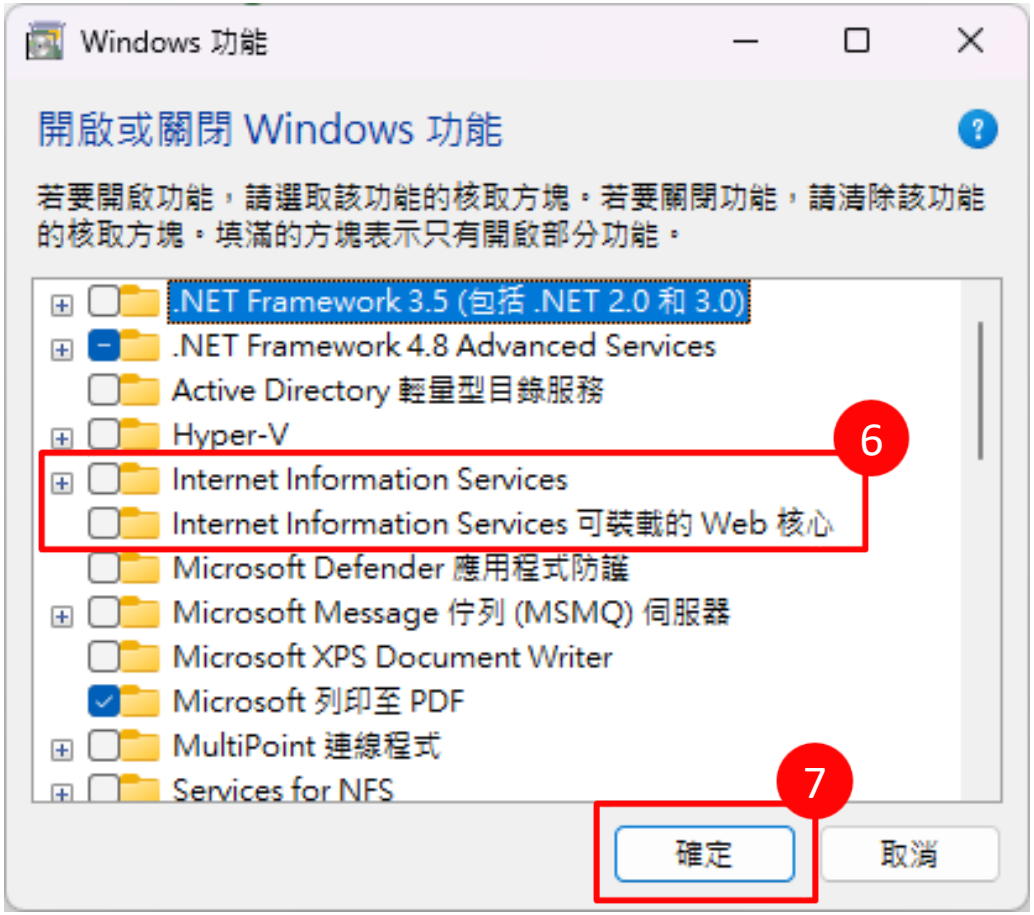
關閉微軟IIS服務

➢點選「開啟或關閉windows功能」



關閉微軟IIS服務

- 檢查「Internet Information Services」與「Internet Information Services可裝載的Web核心」，請確認這兩項為非勾選狀態(與下圖相同)
- 取消勾選後點「確定」，並重新啟動電腦



類似的弱點

- 12085 - Apache Tomcat Default Files
- 106374 - Default nginx HTTP Server Settings
- 112351 - Apache Default Index Page
- 處理邏輯相同，將預設的頁面、預設文件等的伺服器架設時的預設檔案移除

網頁伺服器相關安全性設定(apache為例)

- 10297 - Web Server Directory Traversal Arbitrary File Access

```
<Directory "網頁根目錄">
    AllowOverride All
    Options -Index FollowSymLinks
    Require all granted
</Directory>
```

或不加Index

```
<Directory "網頁根目錄">
    AllowOverride All
    Options FollowSymLinks
    Require all granted
</Directory>
```

網頁伺服器相關安全性設定(apache為例)

- 106232 - Apache ServerTokens Information Disclosure
- 88490 - Web Server Error Page Information Disclosure
- 88099 - Web Server HTTP Header Information Disclosure

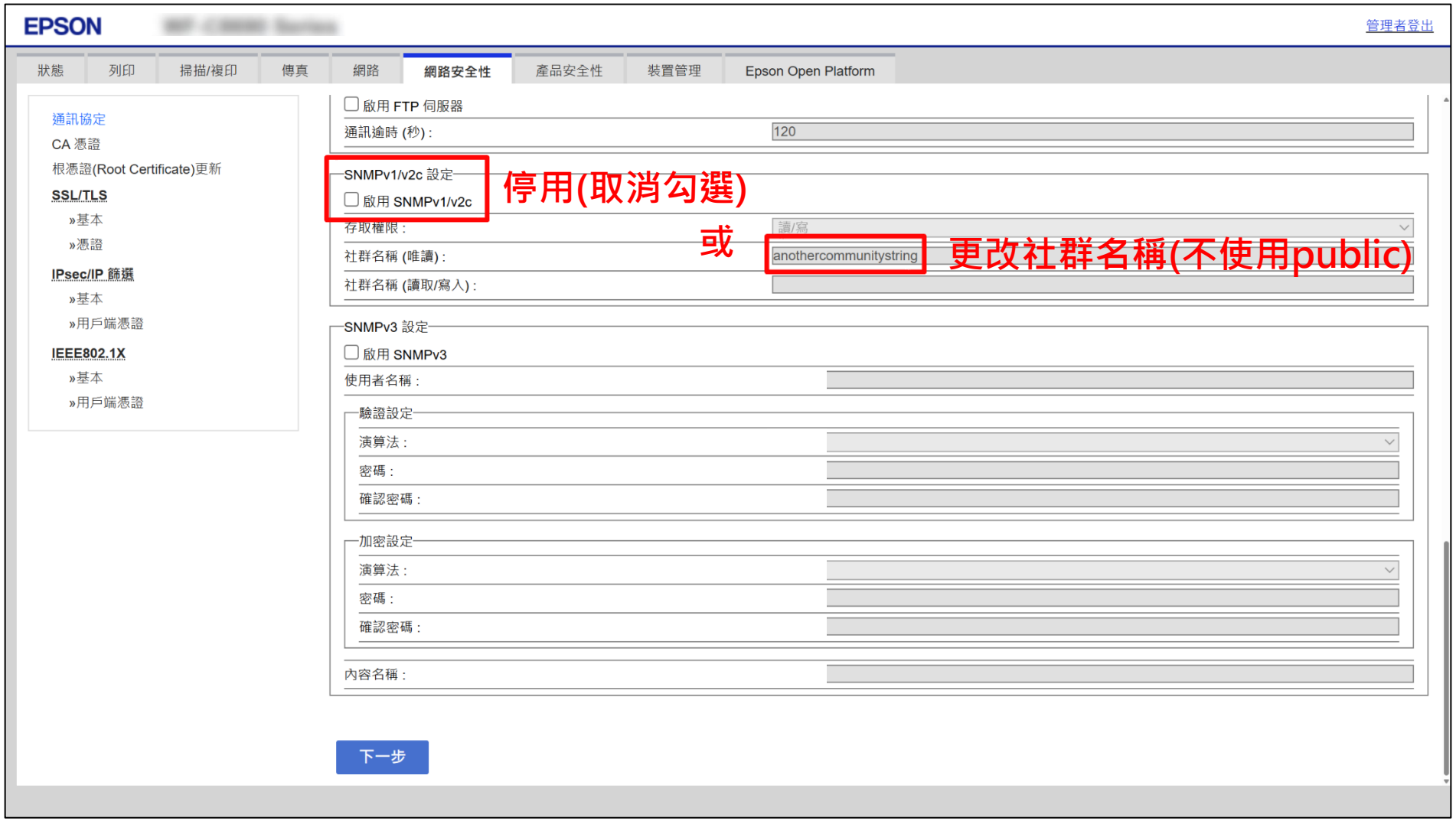
```
#Directory   ../apache2/security.conf
#錯誤頁面資訊量顯示多寡
ServerTokens Prod      建議    #Apache
ServerTokens Major             #Apache/2
ServerTokens Minor             #Apache/2.4
ServerTokens Minimal           #Apache/2.4.41
ServerTokens OS                #Apache/2.4.41 (Unix)
ServerTokens Full              #Apache/2.4.41 (Unix) PHP/4.2.2

#錯誤頁面是否顯示以上資訊
ServerSignature Off    建議    #不顯示
ServerSignature On             #顯示
```

印表機或其他物聯網設備snmp協定

- 41028 - SNMP Agent Default Community Name (public)
- 76474 - SNMP 'GETBULK' Reflection DDoS
- snmp協定主要用於監控及管理連網設備，對於一般使用者來說不太可能會用到，但幾次弱掃下來發現校內大部分印表機都有開啟這個協定且社群名稱皆為預設的public
  - ✓任何未授權的使用者只要知道設備IP加上預設的社群名稱，都可以取得該設備的情資並加以利用
- 解決方法：
  - ✓停用snmp
  - ✓更改社群名稱，不要使用public或其他很好猜的名稱
  - ✓設定限制為只有特定IP可以透過snmp取得資訊

印表機或其他物聯網設備snmp協定(範例)



資訊處
Office of Information Technology

可以排除的項目

SSL憑證相關

- 51192 - SSL Certificate Cannot Be Trusted
- 57582 - SSL Self-Signed Certificate
  - ✓物聯網設備大部分都會有這兩項，指的是對弱掃工具而言，套用的憑證為自簽憑證及無法信任
  - ✓因為設備憑證通常都是廠商憑證，原則上只要是非對外服務設備就可以排除
  - ✓個人電腦部分服務也會有(常見如微軟遠端程式RDP)，同理只要是非對外提供服務就可以排除
- 補充：對外服務泛指在校外或校內任何非授權使用者都可以連到這台設備取得並使用設備提供的功能或服務
  - ✓例如：行政、學術單位網站，屬於對外服務的範疇
  - ✓例如：單位業務印表機，通常只有單位內成員或特定人士可以使用，屬於非對外服務

SSL憑證相關

- 對外服務(常見為網站系統)如果有掃出這兩項弱點
  - ✓請確認是否使用有效的憑證
  - ✓例如：TWCA、Let's Encrypt(每3個月要更新一次)等

- 對外服務憑證請保持有效且安全
  - ✓相關弱點：
    - 35291 - SSL Certificate Signed Using Weak Hashing Algorithm
    - 31705 - SSL Anonymous Cipher Suites Supported
    - 51192 - SSL Certificate Cannot Be Trusted
    - 15901 - SSL Certificate Expiry
    - 45411 - SSL Certificate with Wrong Hostname
    - 57582 - SSL Self-Signed Certificate

資訊處
Office of Information Technology

感謝閱讀