編號:

專題名稱：資安輔助工具

校名與科系:淡江資訊管理學系

指導老師：廖賀田老師

團員成員:陳韋彤、杜哲言、莊皓鈞、曾善梓

1. 前言

「資安輔助工具」專題所設計之系統，係針對近年重大資安問題，大多是因為企業內部電腦及資訊環境遭駭客利用各種入侵手法植入惡意程式或勒索軟體所致，並且一而再地發生，同時根據事後調查，員工個人電腦幾乎都是被入侵的管道。因此，除了企業在既有的基本資安防護及加強員工資安意識之外，專題提出最小預算及人力成本的解決方案，資訊人員利用Windows系統內建功能，自行撰寫工具程式，設定使用者登入電腦時自動執行，發出用戶端自我防護通知，使用者每次登入可自行簡易的檢視及修正電腦安全狀況，工具程式同時蒐集用戶端資訊至資料庫，開發網頁程式呈現資料庫之資料，提供管理者查詢分析記錄，在駭客未成功發動攻擊之前，儘早發現異常並立即進行處置。

二、創意描述

市售的防毒軟體，這些專業防毒軟體功能強大且複雜，需付出相當龐大的金錢及維護人力等資源，使用上雖然方便，但使用者其實對具體狀況一無所知，只能被動地看到電腦處於危險、普通、安全等等狀態，因此我們 開發讓使用者也能參與其中的資安工具，藉此讓使用者更了解電腦的狀況，以此降低被駭客入侵的風險。

三、系統功能簡介

用戶端使用者登入電腦後，自動跳出自我防護工具程式通知主視窗畫面，讓使用者很明顯清楚的看到系統資訊。視窗內共有四個檢視項目，一、使用者上次登入電腦時間；二、Windows Update系統更新狀態；三、Windows安全性狀態；四、Windows備份狀態。這四個項目是用戶端可以協助管理者維護資安而自行檢視的重要項目，工具程式並設計[一鍵管理]按紐，讓不熟悉操作管理電腦的一般使用者，能夠快速輕易地直接開啟各管理設定項目之介面而進行簡單的操作，同時按紐下方提供官網連結，讓使用者能夠暸解及學習更多相關執行操作的細節。

四、系統特色

1. 市面上的防毒軟體多半沒有提供讓使用者簡易自行檢視安全及一鍵管理的介面，使用者無法很容易的協助或減少系統管理者之負擔，進而造成資安破口。因此，本系統撰寫用戶端工具程式，提供簡易的界面給使用者操作。
2. 管理工作常常會因為繁忙疏忽或是不熟操作，而百密一疏致組織遭受危害。因此，本系專題撰寫伺服器端網頁程式，提供簡易的重要監控記錄給管理者使用。
3. 利用本專題系統之自我防護工具程式及簡易紀錄分析網頁，輕鬆的將員工更融入資安防護工作，藉以提升企業之整體資安。

五、系統開發工具與技術

1. 系統分析工具說明：Word 2016。
2. 程式開發工具說明：VBScript、ASP.NET C#、Notepad++、[Visual Studio Community 2019](https://visualstudio.microsoft.com/zh-hant/vs/community/)。
3. 系統使用對象

本系統可應用於一般中小型企業或組織，在資訊預算及人力有限的情況下，使能簡單的結合所有內部人員做到最佳資安防護，以避免影響資訊系統正常運作，或被駭客做為攻擊他人的跳板。

1. 系統使用環境
2. 硬體環境：專題使用之筆電硬體規格為8Core CPU、16G記憶體、512G SSD硬碟及Windows 10專業版作業系統，啟用Hyper-V虛擬化服務，建置虛擬架構運作環境如下：
3. Windows 10個人電腦虛擬機3台，電腦名稱為ooo-c1、ooo-c2、ooo-c3。
4. Windows Server 2019伺服器虛擬機1台，ooo-s1。
5. 網路環境：
6. Windows Server 2019伺服器虛擬機啟用Active Directory網域服務，設定成為AD伺服器，建置Windows網域環境，網域名稱為ooo。
7. Windows 10個人電腦虛擬機3台皆加入網域，設定成為AD網域用戶端電腦。
8. 新增3個網域使用者帳號，t001、t002、t003。
9. 軟體環境：
10. 使用者登入AD用戶端電腦後，將自動執行AD伺服器端GPO (Group Policy Object,群組派送原則)所設定之登入VBScript程式，發出訊息通知，並蒐集用戶端相關資訊回傳資料庫。
11. AD伺服器虛擬機安裝SQL Server資料庫軟體，負責儲存從用戶端蒐集之系統相關資訊，資料庫管理工具SSMS 2019、資料庫名稱為maintain。
12. AD伺服器虛擬機啟用IIS網頁伺服器及ASP.NET功能，開發設計C#程式，擷取SQL資料庫內容並呈現資料分析結果網頁，提供系統管理員瞭解用戶端資安狀況。

八、結語

本專題提供可讓使用者簡易自行檢視安全及一鍵管理的介面、簡易的重要監控記錄給管理者使用，以最簡單最明瞭且有效的方式來提升資訊安全，希望在資安領域進一份心力。

以下是我們希望將來系統能更進一步完成的功能：

1. 目前工具程式於用戶端登入時僅顯示安全性通知使用者，自行檢視後手動執行安全性修正，未來可對必要的安全性，開發程式使自動強制執行安全性修正，例如密碼3個月強制變更；安全性更新超過1個月未更新則自動安裝更新等，以確保企業資訊作業安全。
2. 系統發現異常時，可主動以電子郵件或簡訊方式，即時通知管理者，而不須等到管理者開啟網頁查詢分析記錄。
3. 系統可增加簡易的視覺化圖表，提供經營階層容易暸解資安管理工作的內容，進而重視資訊部門的發展。