**資訊安全報告**

**作業一、後門程式**

**組別 : 第二組**

**組員 :**

B10217004 葉冠麟

B10217025 邱宇勳

B10217027 賴政瑋

B10217036 黃子羿

B10217057 趙威筑

**目 錄**

1. **題目功能解決辦法**
2. **程式碼解說**
3. **功能展示**
4. **心得報告**
   1. **題目功能解決辦法**

原本的Backdoor程式只有開啟後門的功能，並且開啟後會跑出小黑窗。連接成功時也會跳出小黑窗，且只有一個使用者能成功連接。實作將Backdoor開啟時改為無畫面跳出、連接成功時將小黑窗改為在背景執行、可供多個使用者成功連接。增加Client端的使用程式。

|  |  |
| --- | --- |
| **功能** | **實作方法** |
| 建立有視窗的Client | 使用C#製作視窗、並使用TCPclient的方式連接backdoor |
| Backdoor 不要顯示視窗 | 在CreateProcessA的function中更改參數的引用 |
| Backdoor 多人連線 | 在listen之後的程式包入無限迴圈中  使得socket能一直被連接 |

**2、程式碼解說**

**Backdoor程式解說**

|  |  |
| --- | --- |
|  | 將原本的Main的宣告改為視窗化的模式，但下方程式並沒有將視窗顯示出來。  因此，  開啟Backdoor時  使用者並不會看到任何視窗 |
|  | Backdoor程式原本並沒有while，增加while迴圈在listen之後將可以使程式一直停留在accept階段，因此可以一直接收client端得連線 |

|  |  |
| --- | --- |
|  | 將creatProcess中dwcreationflags的參數改為CREATE\_NO\_WINDOW  將可以讓連線之後跑出的小黑窗改為在背景執行 |
| **更改後的程式** | |

**Client程式解說**

程式使用C#來編寫

|  |
| --- |
|  |

Client端程式畫面

|  |  |
| --- | --- |
|  | 按下連線後的function  跑出messagebox讓使用者輸入IP  Port預設為10000  開啟TcpClient連線的功能  定義資料傳輸的通道目標  使用多執行緒執行傳輸的function |
|  | 在多執行緒裡執行的function  在無限迴圈裡持續讀取sever傳回來的資料並存在字串s  讀取使用者輸入的指令並傳入sever端 |

|  |  |
| --- | --- |
|  | 使用timer固定1秒讀取接收到的資料並輸出至richtextbox中。 |
| 程式中剩餘按鈕的功能程式碼:  只要將指令存入cmdin中即可將指令傳入backdoor中 | |

**3、功能展示**

使用一台主機及兩台虛擬機電腦做測試

|  |
| --- |
| 開啟Backdoor的虛擬機IP資訊    開啟Backdoor後10000Port打開且下方並無程式跑出 |

|  |
| --- |
| Client端點選建立連線後顯示輸入ip的對話窗    連線成功後可以看到已經接收到小黑窗的開頭資訊    點選IP資訊後接收到的資料 |

|  |
| --- |
| 點選CMD指令輸入的對話窗，點選OK即可發送指令 |

|  |
| --- |
| 兩台Client端同時連線的畫面，左方位於虛擬機  右方則是主機的畫面，兩者可同時使用。 |

1. **心得**

這應該是我們第一次使用後門程式，之前對於資訊安全這方面都只是紙上談兵，都只知道個資很重要，但是知道就只是想法並沒有去實作過，這次的作也讓我們可以實際動手去體驗資訊安全的操作，後門程式是第一次使用，真的很有趣，簡單透過命令提示字元下個指令就可以操控別人的電腦，感覺真的很新鮮，但也親至體驗到後門程式的威力，沒想到入侵別人電腦是那麼的簡單，也體會到保護電腦資料的重要性。也讓我更加了解網路程式連接的機制和結構是如何運作的，透過telnet的方式可以連線到主機，然後開啟命令提示字元就可以提供client端做指令操作。雖然之前對網路程式只略懂皮毛，但是透過這次作業可以實際完成一個簡單的連接過程操作，對於網路的程式架構有更深入的學習和了解，學習到更多網路程式兩端的溝通方法，完成這次作業。