資訊處
Office of Information Technology

資安宣導

如何防範暴力攻擊法破解密碼

中華民國112年9月

編號：025

大綱

一、什麼是暴力攻擊法？如何防範？
二、良好的密碼使用習慣
三、提高密碼複雜度的方法
四、絕對不要使用這樣的密碼
五、資安相關法規議題
六、參考資料

一、什麼是暴力攻擊法？

- 暴力攻擊是一種反覆試驗的方法，用來解密機密資料。暴力密碼攻擊通常藉由針對網站登入頁面的指令碼或傀儡程式來進行。
- 暴力攻擊法又稱為窮舉法，駭客利用字典檔或字元排列組合兩種方式，逐一嘗試登入系統直到成功為止。
  - ✓字典檔：駭客使用的字典檔除了收錄一般英文單字之外，通常也會收錄一些常見的弱密碼，藉此進行嘗試攻擊。
  - ✓排列組合：由1碼、2碼、3碼...漸次增加長度，逐一嘗試各種英文大小寫字母、數字及特殊符號等字元的排列組合加以嘗試，直到成功為止。

一、如何防範暴力攻擊法？

- 避免使用英文單字及常見的弱密碼, 例如：

密碼	原因	密碼	原因
international	英文單字	university	英文單字
1234	懶人密碼	abcde	懶人密碼
abc123	懶人密碼	111111	懶人密碼
1234567890	懶人密碼	susan	常見人名
JoeBiden	知名人物	monkey	常見動物
rover	常見寵物名稱	Taiwan	地名
asdf	鍵盤組合	qwerty	鍵盤組合
aaaaa	鍵盤組合	80/01/01	日期
admin	常用預設密碼	administrator	常用密碼
password	常用密碼	p@$$\/\/0rd	常用密碼

一、如何防範暴力攻擊法？

- 增加排列組合複雜度，提高破解時間的不可行性
  - ✓ 使用英文大小寫字母、數字及特殊符號組合
  - ✓ 密碼長度至少應設為8碼
  - ✓ 各種排列組合複雜度情況下，破解密碼所需時間：

密碼長度	英文字母 (26字元)	英文字母+數字 (26+10字元)	英文字母大小寫 (52字元)	含特殊符號字元 (96字元)
4	0	0	1分鐘	13分鐘
5	0	10分鐘	1小時	22小時
6	50分鐘	6小時	2.2天	3個月
7	22小時	9天	4個月	23年
8	24天	10.5個月	17年	2287年
9	21個月	32.6年	881年	21萬9000年
10	45年	1159年	45838年	2100萬年

大綱

一、什麼是暴力攻擊法？如何防範？
二、良好的密碼使用習慣
三、提高密碼複雜度的方法
四、絕對不要使用這樣的密碼
五、資安相關法規議題
六、參考資料

二、良好的密碼使用習慣

➢七不

- ✓不使用設備的預設密碼
- ✓不使用與帳號相同的密碼
- ✓不使用太常見的密碼
- ✓不要使用常見名詞、單字
- ✓不使用個資相關密碼
- ✓不要全部使用數字，或全部為英文
- ✓不使用相同的密碼

大綱

一、什麼是暴力攻擊法？如何防範？
二、良好的密碼使用習慣
三、提高密碼複雜度的方法
四、絕對不要使用這樣的密碼
五、資安相關法規議題
六、參考資料

三、提高密碼複雜度的方法

- 無論使用任何方法，密碼絕對不可以少於8碼。
- 中文碼對映法
  - ✓中文碼對應鍵盤字元是一種易記難猜的有效策略。
  - ✓例如「芝蘇開門」注音碼對映鍵為 5 a86 d9 ap6。
- 留頭去尾法
  - ✓ 以自己喜歡的一段話，取各單字字首組合成長密碼，大小寫字母交替使用效果更好。
  - ✓ 例如：Never put off till tomorrow what you can do today，可以取 nPottwycdT 做為密碼。
- 單字組合法
  - ✓ 將幾個英文單字連結起來，組合成容易記憶的長密碼。
  - ✓ 例如：利用 chick、Fly、dog、Jump 四個單字組合成長密碼chickFlydogJump。

大綱

一、什麼是暴力攻擊法？如何防範？
二、良好的密碼使用習慣
三、提高密碼複雜度的方法
四、絕對不要使用這樣的密碼
五、資安相關法規議題
六、參考資料

四、絕對不要使用這樣的密碼

- 暴力攻擊法幾乎可以秒殺的密碼：
  - ✓空白（未設密碼）
  - ✓常見的預設密碼（如：admin、1234、0000）
  - ✓常見的懶人密碼（通常已被收錄於駭客字典檔）
  - ✓英文單字或專有名詞（如：national、YMCA）
  - ✓系統管理相關名詞（如：administrator、password）
- 知道你個人相關資訊的有心人士可能會嘗試：
  - ✓個資資訊（如：英文名字、生日、手機/車牌號碼）
  - ✓職務相關資訊（如：機關或部門縮寫、電話或分機號碼）

大綱

一、什麼是暴力攻擊法？如何防範？
二、良好的密碼使用習慣
三、提高密碼複雜度的方法
四、絕對不要使用這樣的密碼
五、資安相關法規議題
六、參考資料

五、資安相關法規議題

- 資通訊設備(如個人電腦、伺服器主機及網通設備等)密碼之設定，應符合政府組態基準(GCB)規範之規定：
  - ✓通行碼長度8碼以上
  - ✓通行碼複雜度應包含英文大寫、小寫、特殊符號或數字三種以上
  - ✓使用者每90天應更換一次通行碼
  - ✓使用者通行碼最短需使用1天，最長使用期限為90天，且通行碼需保留三次歷史紀錄不得相同

五、資安相關法規議題

- 各單位建置資訊系統(含網站後台)時，應遵守資通系統防護基準之規範：
  - ✓ 只允許特定IP或網段登入，遠端存取均應先取得授權
  - ✓ 應具備唯一識別及鑑別使用者，禁止使用共用帳號
  - ✓ 設置驗證碼機制，防範自動化程式之登入或密碼嘗試
  - ✓ 使用預設密碼登入時，應於登入後要求立即變更密碼
  - ✓ 身分驗證相關資訊不以明文傳輸
  - ✓ 帳號登入失敗達三次後，至少十五分鐘內不允許繼續嘗試登入
  - ✓ 應強制最低密碼複雜度，並強制密碼最短及最長之效期限制
  - ✓ 使用者更換密碼時，至少不可以與前三次使用過之密碼相同

※ 以上僅列出與系統登入有關之重點，各單位開發系統時，應完整參考資通系統防護基準。

大綱

一、什麼是暴力攻擊法？如何防範？
二、良好的密碼使用習慣
三、提高密碼複雜度的方法
四、絕對不要使用這樣的密碼
五、資安相關法規議題
六、參考資料

六、參考資料

- 資通安全責任等級分級辦法
  - (附表十　資通系統防護基準)
- 政府組態基準(GCB)
- 密碼強度
- 密碼安全設定
- 密碼設定與使用原則
- 密碼的安全設定原則
- 設定高強度密碼並強化帳戶安全性

資訊處
Office of Information Technology

感謝閱讀