# Homework #5

Release Time: 2021/05/03 (Mon.)
Due Time: 2021/05/16 (Sun.) 21:59
Contact TAs: `vegetable@csie.ntu.edu.tw`

## Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.

### Submission

- Please place your answers in the same order as the problem sheet and do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Please zip all the files, including one PDF and one xml file, name the zip file "`{your_student_id}.zip`", and submit it through NTU COOL. The zip file should not contain any other files, and the directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- security/
+-- ldif/
+-- ldap-script/
```

### Grading

- Security accounts for 100 points while LDAP accounts for 100 points. The final score is the sum of them.
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- Tidiness score: 3 bonus points, graded by TA.
- Final score = $\frac{\text{Security score}}{2} + \frac{\text{LDAP score}}{2}$ + tidiness score.

# Security

## 說明

- 請不要用任何形式干擾其他人作答，或不是以解題為目的來攻擊本作業的各項設施。經舉發查證屬實者，將會受到非常嚴厲的懲罰。
- Security 的所有題目分數加總是 150 分，但超過 100 分會以 100 分計。
  你可以斟酌不作答某些題目。
- 對於所有標記 (*CTF*) 的題目，請至 Google 表單 上傳 flag。
  所有題目的 flag 的格式都是 `HW5{XXX}`。
- 如果你有寫了 script 或程式來進行解題，請在作業的 zip 中附上檔案，放在 security 資料夾底下，並在 report 中提及。
- 動手操作的題目都需要詳細說明自己是如何做到的。請說服批改助教「你是真的有自己想過」還有「你是真的懂」。
- 即便沒解出來也請儘量作答，可以寫下錯誤的嘗試或是網路上搜尋到的資料。批改的助教將會依照方向與距離答案多遠來給予部份分數。
- 只要不是抄襲或作弊，非常歡迎你嘗試非預期解。

## 1. Threat Modeling (15 points)

老師在上課時教了大家什麼是 Threat Modeling，也提供了一些例子讓大家可以來練習。以下的題目會提出許多不同的系統 (system) 與安全需求 (security requirement)，你需要提出不超過 4 個合理的假設 (assumption) 與 2 種不同的 threat model，每種 threat model 都需要提供一個應對措施。不同題目間的 threat model 不能太相似，否則批改者會認定你是偷懶而斟酌扣分。

### 例題

- system: 系上網路列印服務
- security requirement: 同學們可以使用網路列印功能，在送出請求的三分鐘之內取得列印完成的印刷品

### 參考解答

- assumption:
  1. 電子設備的電子元件皆狀態良好
- threat model:

| Threat Model | Countermeasure |
|---|---|
| 有人嘗試利用網路列印頁面的網頁漏洞來攻擊服務 | 定期將 server 更新至最新版本 |
| 有人透過大量列印來耗盡印表機的資源（紙張或碳粉匣） | 在資源剩餘量低落時，限制每個人的使用量，並通知管理員補充列印資源 |
| 有人對印表機進行物理破壞 | 將印表機置於上鎖的機房，牆上開一個孔讓印完的紙滑出來 |

**題目 (3 points per problem)**

(1)
- system: 船運
- security requirement: 要讓貨物平安抵達目的地

(2)
- system: 吃到飽餐廳
- security requirement: 不能讓人吃霸王餐

(3)
- system: 在 204 舉辦的程式競賽
- security requirement: 所有參賽者都不能作弊、所有參賽者都不能影響其他參賽者進行比賽

(4)
- system: 系館門禁
- security requirement: 在非上課時間，只允許門禁卡的擁有者進入系館

(5)
- system: 個人筆電
- security requirement: 沒有被擁有者允許的人不能使用

**Hint**

- 上課投影片說的：“Think about how to make it fail instead of how to make it work!”
- NASA 的名稱裡面有個 “Administration” 在，有些問題也許不見得一定要用技術來解決，可以往管理層面來思考。

## 2. Proof of Work & DoS (31 points)

Sophia 學姐是一位神祕的強者，沒有人知道他真正的名字。每每有人談論起他時，都會用「那位 Sophia 學姐」來指稱。

有人說，Sophia 學姐從不懈怠，說不定是個不需要睡覺的人。曾經有 24 位系上的年輕人為了探查此事，組成了一個偵察小隊，一人負責每天的一個小時，輪流監測 Sophia 學姐的社群網站帳號。他們連續觀察了 774 十 9 天，結果發現 Sophia 學姐的帳號永遠是在線的狀態。此消息一出，在當時驚動了許多系上大佬，還有大佬感受到威脅而發了聲明稿，呼籲 Sophia 學姐一定要睡覺。然而，這些外界的臆測也沒有得到任何回應，到今天還是沒有人知道 Sophia 學姐有沒有睡覺。

除了努力工作，Sophia 學姐也很喜歡在社群媒體上分享他的生活。但，畢竟被稱為神祕的強者，Sophia 學姐的貼文總是令人難以捉摸。他經常發一些「今天在校園裡遇到柴魚」、「我～是柴魚，我好可愛」之類的文章，有時候甚至貼文內只有一個「柴」字，真的非常神祕。根據我們一位蛋研社朋友 (化名 chi) 的內線消息，上次 Sophia 在系館遇到 chi 時，直接衝上去指著 chi 的鼻子說：「我要柴魚麻咔籠！」chi 受到相當大的驚嚇，不小心就「喵」了出來。霎時間，Sophia 學姐大叫：「啊！你們都欺負我！我以後都不ㄍ你們一起吃了！」然後就一溜煙地跑走了。真的很神祕吧？

- 本題需要用到的……
  - 檔案：`server.py`
  - 連線：`nc linux[x].csie.ntu.edu.tw 13087`
    - `[x]` 可填入 7, 8, 9
- 要回答第 (3) 到 (5) 小題，請先讀懂 `server.py`。
- 要回答第 (3) 到 (5) 小題，可以參考這份 `example.py`。

(1) (4%) DoS (denial-of-service), DDoS (distributed denial-of-service) 是兩種常被搞混的攻擊手法，請簡述他們是什麼以及他們的差別。

(2) (4%) PoW (proof of work) 是一種防禦 DDoS attack 的手法。請簡述 PoW 的防禦原理，並簡介另外一種 proof of XXX 的方法。

(3) (8%) (*CTF*) Sophia 學姐人很好，人家還在痛苦地學習 DSA 時，他早就做完一個 sorting service 供大家使用了。請用上面提供的資訊連上 server，解決 PoW (md5 hash 問題) 之後，輸入選項 1。請設計適當的 input data 來達到 DoS 的效果。

(4) (8%) (*CTF*) Sophia 學姐其實覺得自己很可愛。為了過濾仰慕者的郵件，他寫了一個小函數來過濾掉不符合格式的郵件。請用上面提供的資訊連上 server，解決 PoW (md5 hash 問題) 之後，輸入選項 2。請設計適當的郵件，來達到 DoS 的效果。(hint: what is ReDoS?)

(5) (7%) (*CTF*) Sophia 學姐太愛工作了。。。你也要跟他一樣愛工作！請用上面提供的資訊連上 server，解決 PoW (md5 hash 問題) 之後，輸入選項 3。請快速地解決 10 份 PoW，並將 server 給你的 certificate 寫在作業 report 當中。

## 3. SA 知識問答 (25 points)

(1) (5%) 在 Linux 檔案權限中，有兩種特別的檔案權限叫作 SUID 跟 SGID，請說明這兩種權限的功能和有可能造成的安全問題。

(2) (5%) 如果你有一台暴露在網際網路上的 server，就會發現每次 ssh 上去時，shell 顯示自從你上次登入以來有很多 login failure。請找到這些登入嘗試的 log 被放在哪個檔案，並說明那個檔案裡存了哪些資訊。

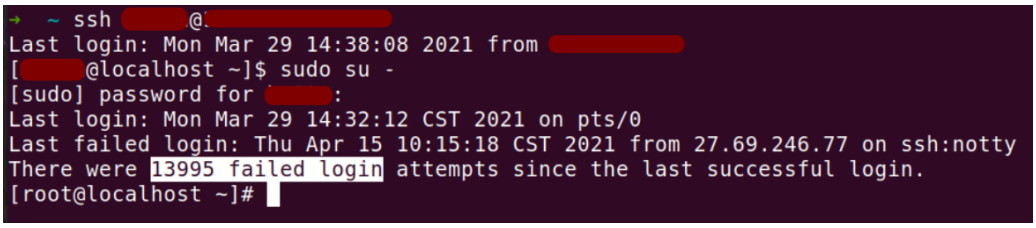


Figure 1: 很多人來敲門

(3) (5%) 當你在工作站上執行 sudo 指令時，會出現一行 "... is not in the sudoers file. This incident will be reported." 請問，這個 incident 會怎麼被 reported 呢？(hint: 被記錄在哪個 log 檔裡)

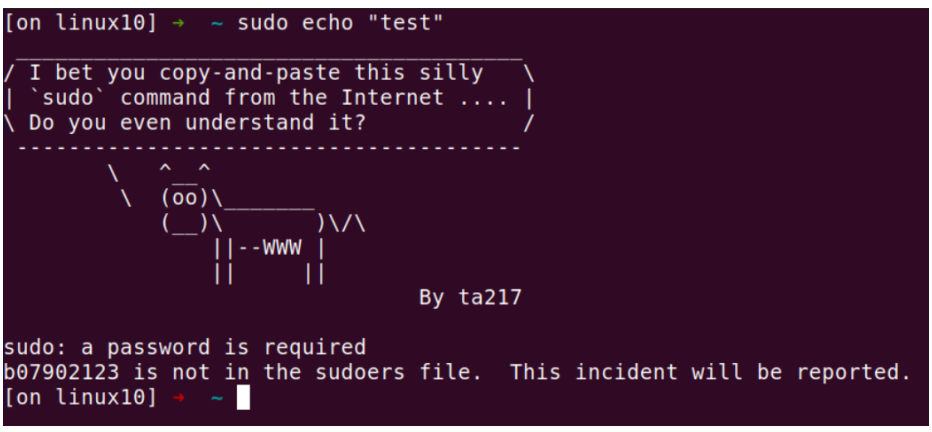


Figure 2: 調皮的嘗試

(4) (5%) 在一台 Linux 電腦上，存在著非常多我們從來就不知道的使用者，不信的話連上工作站執行 `cat /etc/passwd` 就可以看到了。例如說 http 這個使用者，就是用來處理跟網頁伺服器有關的工作；systemd-network 這個使用者，就是用來處理跟電腦網路有關的工作。請說明為什麼這些工作需要額外創建專門的使用者來處理，並舉出如果全部都用 root 使用者來執行的話會有什麼安全問題。

(5) (5%) 你知道嗎？GitHub 即將在 2021/08/13 開始，不再允許 git 指令的 password authentication。另外，許多教學文章也都建議使用 ssh 不要用 password 來登入，而是使用 ssh key 來登入。請比較 password authentication 和 token-based authentication 這兩者的優缺點。

## 4. 弱密碼 (44 points)

近期在資工系流行起一股「大意」風潮，不管是去吃個飯或只是去上個廁所，不管是大剌剌地把螢幕打開或是把螢幕亮度調到最低，只要螢幕忘了上鎖，就有可能在回到電腦時發現自己的 Facebook 多了一則「大意」貼文。也許你沒有注意到，「大意」倒過來念會變成「意大」，多念幾次就是「意大意大」。是的，你也發現了，就是「意大意大 i da i dai dai dai 代一代一代」。沒錯，這樣的教訓真是痛，痛的日文就是「一代一」。

傳聞這種行為早在數年前就已在資訊年會圈出現。聽說如果當時你在會場使用電腦，暫時離開電腦卻沒有將螢幕上鎖，就會遭到無情發文，在自己的動態牆上發現多了一則新貼文，內容是「我下次離開座位會記得鎖螢幕」，或「我下次用別人的電腦會記得登出」之類的。

但，你知道嗎？真正恐怖的不是你忘了將螢幕上鎖，而是就算你把螢幕上鎖、把電腦關機，有心人士還是有機會可以破解你的密碼、幫你登入電腦，再幫你發文。

資安的學習路上，我們一直被告知：「不知攻，焉知防？」在這個大題，我們要練習的就是進行這樣的攻擊。然而，作為具有技術的知識份子，我們更應該要擁有一顆具有道德倫理的心。學習這些攻擊技術，不是為了要拿來獲利或做不法行為，或是去讓你沒有大意的同學「大意」，而是要了解真正的壞人能做到什麼程度。

連結 展示了針對 Mac 電腦的攻擊手法，請利用相同的原理來嘗試解出以下 Ubuntu 和 Windows 電腦的密碼。

再次提醒，中華民國刑法 妨害電腦使用罪：

- 第 358 條
  無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
- 第 359 條
  無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

請大家帶著嚴肅與戒慎恐懼的心來完成這大題。

### 題目

(1) 請使用 Hank's Ubuntu 來進行測試。請至 這裡 下載 ova 檔，然後：

- (15%) 破解出 Hank 的密碼。
- (5%) (*CTF*) 登入 Hank 的使用者之後找到桌面上的 flag。

(2) 請使用 howhow's Windows 來進行測試。請至 這裡 下載 ova 檔，然後：

- (15%) 破解出 howhow 的密碼。

- (5%) (*CTF*) 登入 howhow 的使用者之後找到桌面上的 flag。

(3) (4%) 請提出針對這種攻擊手法可能的防禦手段至少兩種。

**Hint**

- 如果你的電腦沒有那麼多 CPU，記得去 VMWare/VirtualBox 調整設定 (ova 檔預設是 8 顆)。
- 什麼是 live USB (live CD)？
- Ubuntu 跟 Windows 分別是把密碼放存哪個檔案？
- 有可能有用（也可能沒用）的 password list
- Ubuntu 的密碼似乎不太適合用暴力破解，key space 太大…也許 Hank 用的是常見的密碼？
- 上次看到 howhow 輸入密碼時，好像沒有看到他按 shift 鍵，而且他第一個按的字母是 a

## 5. WiFi Hacking (35 points)

本來想寫一個精彩的故事來介紹 Lisa 學姐和 WannaLisa 的微笑，但發現太難寫了，所以就不寫了。

(1) (15%) 軒爺是一位學士淵博的學者，近期來到敝系訪察，令德田商旅蓬蓽生輝。為了接待這位學者，敝系決定用最高級的房間來接待 - Room 217。但是，這個最高級的房間因為長期沒有夠格的人可以入住，已經長了不少灰塵。聽說前些日子還有一隻怪怪的蟲子住在裡面，請你調查一下這件事。

- 請在德田館 217 實驗室外面的走廊進行解題。
- 本題的目標是破解 “Palace of Joe Tsai” 這個 WiFi 的密碼，並連上這個 WiFi。
- WiFi 密碼的格式似乎是某人的手機號碼…？
- 如果一點頭緒也沒有，可以嘗試搜尋 “WPA2 PSK cracking” 或類似的關鍵字…

(2) (10%) (*CTF*) 你靠近一看，被那隻蟲子給嚇了一跳。那蟲子又大又肥，身上爬了滿滿的三格空白、tab 字元和各種亂放的大括號，嘴角不停流下加滿鹽巴的義大利麵，還躺在一堆看起來一模一樣的輪子上。仔細一看，你發現了大蟲子的身後有一條細細的不起眼的光絲，沿著牆腳延伸向窗戶，最終通向未知的遠方。這光絲，似乎流動著一股神祕的力量…

- 請在完成第一小題之後再解這題。
- 本題的目標是找出哪個可疑的 IP 位址連上了 “Palace of Joe Tsai”，並破解這個 IP 位址正在進行的 TCP 連線內容。
- 如果一點頭緒也沒有的話，可以嘗試搜尋 “decrypt 802.11 traffic” 或類似的關鍵字…

```
int func (int x1, int x2)
    { return x1 + x2;
}
```

Figure 3: 亂放的大括號

(3) (10%) (*CTF*) 你心想：「要接待軒爺這種人物的地方，怎麼容忍得了任何一絲的不潔！軒爺的世界絕對容不下任何一隻蟲的存在！」於是，你決定成為屠蟲勇者，斬除眼前的噁心的怪物。你使勁全力地攻擊臭蟲，但它卻絲毫沒有受到動搖，被劃開的傷口也迅速癒合，似乎宣示著要住在 Room 217 千秋萬世。幸好，眼尖的你很快就發現，那縷細細的光絲，總在臭蟲受傷時閃耀著詭異的光芒。「該不會…」你猜那條光絲就是這臭蟲的生命力來源，所以決定嘗試將這連結打斷，看能不能一舉讓這臭蟲回歸塵土！

- 請在完成第一小題之後再解這題。
- 本題的目標是讓上一題的可疑 IP 位址無法穩定連上 “Palace of Joe Tsai” 連續 40 秒。
- 若要查看當前狀態，請在 217 實驗室外面連上 “battle-field” 這個 WiFi，並透過 “battle-field” 連上 這個網址 來確認解題進度和獲取 flag。
  - 上述網址只有在連上 “battle-field” 之後才能查看。
  - “battle-field” 的 WiFi 密碼和 “Palace of Joe Tsai” 的密碼相同。
- 如果一點頭緒也沒有的話，可以嘗試搜尋 “wifi deauthentication” 或類似的關鍵字…

(4) (0%) 你的猜測是對的。在切斷那臭蟲的生命力來源之後，你的攻擊逐漸奏效，臭蟲愈來愈扁、愈來愈小，最後連同那些流落在地上的義大利麵和輪子全都煙消雲散，彷彿不曾存在過。後來，軒爺果然住進了 Room 217，並且對於德田館讚譽有佳。這一切，都要感謝你的默默付出。

…但這題沒有任何分數，厂。

# LDAP

你聽過 giver 嗎？傳聞 giver 是 DSA 以及 NASA 兩門課程中下手最狠的一位助教，由於他出的作業實在是太難太神了，在同學的要求下，giver 開設了專門為 DSA 以及 NASA 設計的衝刺班。由於學生眾多，giver 決定使用 LDAP 來管理所有學生以及教材的資訊。

在下面的問題中，請你幫 giver 逐步完成 LDAP 的設置。請在繳交的作業中詳細記錄下完整指定目標所需的重要指令，並以截圖的方式來證明你的設定真的有達到 giver 的要求。如果作答過程中有使用到內容較多的 LDIF 檔案，可以將檔案放到 `ldif` 這個資料夾內，並在報告中提到檔名即可。為了統一格式，如果你沒有要將 LDIF 檔放在報告外，請也創造一個 `ldif` 資料夾並留空即可。

所有的小題都會給視作答的情況給部分分數，所以就算沒有達成最後的要求，也請在作業中附上你的進度。

## 1. Basic Setup (15 points)

請參考 Lab 9 投影片中的步驟，安裝一台 CentOS 7 的 VM，並在上面設置 LDAP Server。為了之後題目的需求，請為這台 VM 設定一張橋接網卡。

LDAP Server 的設定請按照下列的要求：

- `olcSuffix` 請設為 `dc=giver,dc=csie,dc=ntu`
- `olcRootDN` 請設為 `cn=giver,dc=giver,dc=csie,dc=ntu`，並設定一組 `olcRootPW`
- 設置 `dc=giver,dc=csie,dc=ntu` 的節點，並在下面設置 root (giver) 以及 `people`, `group` 兩個 OU

請附上 `ldapsearch` 所有 `dc=giver,dc=csie,dc=ntu` 下資訊的結果。

## 2. Client (20 points)

當然，參加衝刺班的學生需要一台工作站來完成課程的作業。所以，giver 請你安裝一台 Arch Linux 的 VM 當作工作站，並與 server 一樣設置橋接網卡。

在工作站上，請安裝 LDAP client 所需的工具，並先確認可以透過 `ldapsearch -x` 來查詢 server 上 `dc=giver,dc=csie,dc=ntu` 下的資訊。確認完成後，請安裝並設置 SSSD ，使得 LDAP 上的使用者可以用 LDAP server 上的密碼來登入，並在第一次登入時自動新增家目錄。

再來，於 LDAP server 上新增兩個群組 `student` 以及 `ta`，其中 `student` 是給修課學生使用、而 `ta` 是給助教的。最後，在 client 上設定所有在 `ta` 群組中的使用者都可以在不用輸入密碼的情況下執行 `sudo` 。注意 client 上的 `root` 使用者仍然要是使用本機的 `root`。

請新增兩個使用者，一個在 `student` 群組、一個在 `ta` 群組，並在作業中附上以上的截圖：

- 用 SSH 登入這兩個使用者（初次登入），並且展示在 `ta` 群組中的使用者可以在不打密碼的情況下執行 `sudo`
- 比較並說明 `cat /etc/passwd` 與 `getent passwd` 的差別

## 3. Schema (10 points)

除了學生資訊之外，giver 也想要用 LDAP 來管理他所出的題目。請新增一個名為 `giverProblem` 的 object class ，包含以下的 attribute：

- `problemName`：題目名稱
- `problemDescription`：題目敘述
- `problemVisibility`：題目是否為公開
- `problemSolution`：題目解答

一個 `giverProblem` 必須要有前三個 attribute，而第四個為可有可無。四個 attribute 都是字串，其中 visibility 用 `public` 或 `private` 來區分。

此外，請新增 `ou=problem,dc=giver,dc=csie,dc=ntu` 來存放問題。

請新增兩個測試題目，一個為 `public` 一個為 `private` ，其中 `public` 的題目請另外加上 `problemSolution`，並附上 `ldapsearch` 新增的 `ou=problem,dc=giver,dc=csie,dc=ntu` 下資訊的截圖。

## 4. Access Control (20 points)

請於 server 上設定權限管制，達到以下的目的：

- 使用者只能更改自己**除了家目錄、UID、GID 以外**的資訊，如 `loginShell`
- 使用者（包含 `anonymous` ）可以查訊到其他使用者**除了密碼以外的資訊**
- 只有在 LDAP server 本機上才能查詢到題目的 `problemSolution`
- 使用者在 client 上只可以查詢到 `problemVisibility` 為 `public` 的題目資訊
- 只允許來自 LDAP server 本機或是工作站（client）的 IP 的操作

注意，由於 giver 想要的權限設定可能有時候會更動，請確保你的設定可以在不重新啟動 `slapd` 的情況下做改動。

## 5. Multiple LDAP Servers (15 points)

giver 的名氣實在是太大了，因此，來自世界各地的學生都想要參加這個衝刺班。所以，giver 決定設定第二個 LDAP server。

請再安裝一台 CentOS 7 的 VM，一樣使用橋接網卡，並安裝 LDAP 相關的套件。安裝好之後，將原本 server 中的 config 以及 `{2}hdb` 資料庫中的內容複製到新的 server 上。注意參加衝刺班的學生很多，所以請不要一筆一筆的慢慢搬。

將兩台 server 上的資料設置為相同之後，請再進一步將兩台 server 設為同步的狀態。也就是說，在任何一台的新增或改動都必須即時反映到另一台上，隨時維持兩邊的資料相同。

## 6. Scripting (20 points)

使用 LDIF 以及 `ldapadd`、`ldapmodify` 來新增資料實在是太麻煩了，所以 giver 請你用 Python 實作一個基於 `python-ldap`[1] 這個套件的腳本。你的腳本需要有以下的功能：

- (10 points) 新增使用者：輸入使用者名稱以及該使用者是否是 TA，新增該使用者並將其加入正確的群組以及設定其家目錄為 `/home/<username>`。請為該使用者設定一個還沒有被用過的 UID。

[1] https://www.python-ldap.org/en/python-ldap-3.3.0/

- (5 points) 封鎖/解封使用者：指定使用者名稱，鎖該使用者使其無法當入工作站（不能刪除該使用者的 LDAP 資訊）。
- (5 points) 修改使用者名稱：使用者可以於 client 上執行此腳本，在輸入密碼後更改自己的 `givenName`。

請將這些腳本放在名為 `ldap-script` 的資料夾。以上的腳本都沒有限制格式以及使用方法，請自行設計並在繳交的作業中簡單說明要怎麼使用。