Security

說明

- 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}`。
- 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」。

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 points) 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 points) 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。

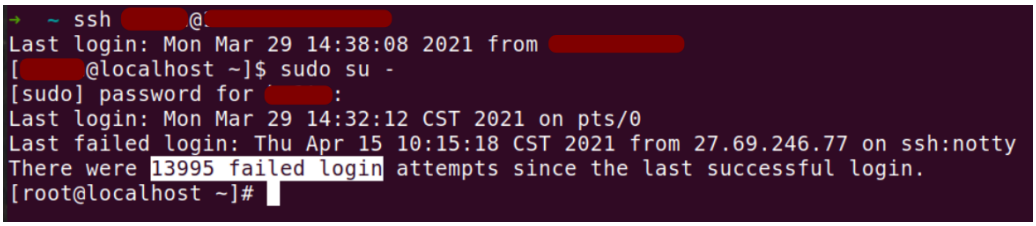

Figure 1: 很多人來敲門

(3) (5 points) 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)

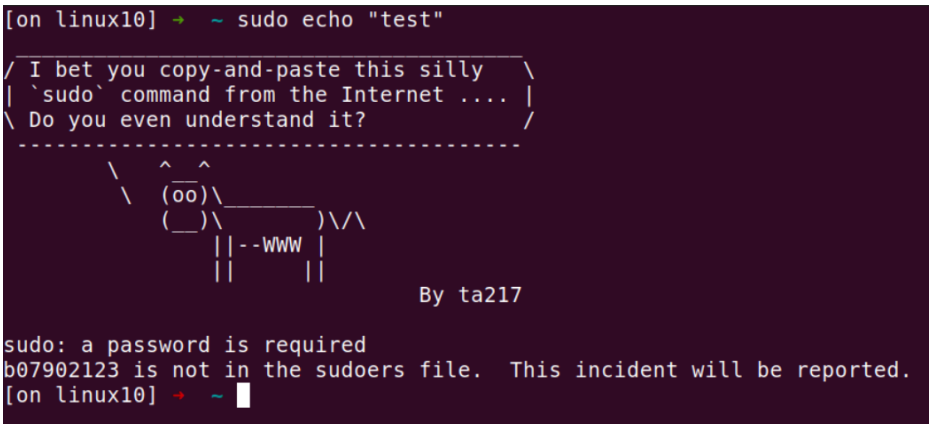

Figure 2: 調皮的嘗試

(4) (5 points) 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 points) 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 points) 破解出 Hank 的密碼。
- (5 points) (*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 points) 破解出 howhow 的密碼。
- (5 points) (*CTF*) 登入 howhow 的使用者之後找到桌面上的 flag。

(3) (4 points) 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. (35 points)

(Lisa 學姐穿工地背心施工中)