Homework #0

Due Time: **2025/02/18 (Tue.) 23:59**
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** problem you have to specify the references (the URL of the website you consulted or the people you discussed with) on the first page of your solution to that problem.
- You may use large language models or other AI tools to help with answering the questions. However, your answer should not be copied from the output of these tools and should be written **in your own words**. The grading TA will check your answers against outputs of common tools.
- Some problems may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.
- Announcement will be updated on here. Please visit the page at least once a day.

Submission

- Put all answers **in one single PDF file**, in the same order as the problem sheet. Do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Submit through this google form: Form link.
- If you need to update your submission, please create another submission. We'll use your latest submission as your final submission.

Grading

- Both NA and SA account for 50 points. The final score is the total of them.
- It is possible that you do not get full points even if you provide a correct answer. You should show how you get the answers step by step and list the references.
- There is also a 3% *tidiness score*. You are encouraged to improve the readability of your document so that TA can easily grade more than 100 homework submissions.
  - Please list your answers in the same order as the problem set. You should type your answers and use a proper typesetting.
  - Please use `monospace fonts` when writing commands and codes in your answer sheet.
  - Screenshots of your terminal outputs are allowed. Please crop the screenshots and zoom them to a proper size that we can easily read your terminal outputs.

  As a sweet note, we recommend you to try out *hackmd*, *typora* and other markdown applications if you don't know how to make a proper typesetting. They should be pretty easy to the beginners.
- You can get at most $50 + 50 + 3 = 103$ points. However, we cannot guarantee the minimum score to be admitted into the course.

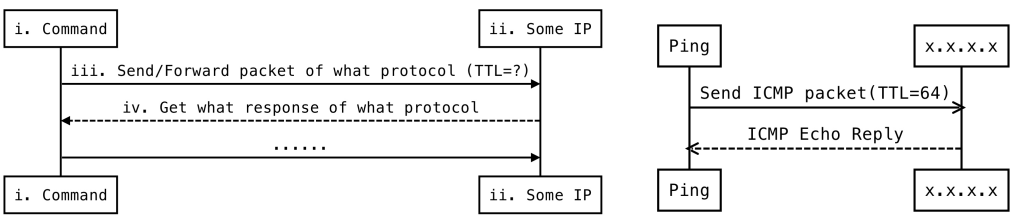
Network Administration

1. Short Answer (10pt)

1. 請根據最廣泛使用的 TCP/IP 模型（共 5 層），列出每一層的名稱、簡述其功能，並提供每層實際應用服務的例子。(1pt)
2. 網路設備與常見問題解析
   (a) 請簡單介紹什麼是 VLAN。(1pt)
   (b) 請簡單說明 Switch（交換器）和 Router（路由器）的功能與用途，並比較它們在 TCP/IP 五層架構中扮演的角色和主要差異。(1pt)
   (c) Broadcast Storm 和 Switching Loop 是兩個網路中常見的問題，請簡單說明並比較它們有什麼不同和相似之處，以及如何防範這些問題。(1pt)
3. 我們現在使用的網路協定有 IPv4 和 IPv6。為什麼 IPv4 要換成 IPv6？那以後有可能會需要從 IPv6 換成其他的嗎？這兩個版本有什麼差別？既然有 IPv6 為什麼還要用 IPv4？(1pt)
4. 關於 UDP 以及 TCP 兩種協定，它們是如何運作的？有哪些相同處以及相異處？什麼時候會傾向於使用其中一種？(1pt)
5. 系上 NA 有使用一種簡稱 EFK 的好東西來幫助大家。什麼是 EFK? 它有什麼優點，而適合系上使用? 它有什麼缺點，你覺得可能會造成什麼問題嗎？(2pt)
6. 什麼是 Multiplexing？Multiplexing 有很多種類，請列舉 3 種並簡單說明。我們系上的 Wi-Fi 運用到了哪幾種 Multiplexing? 為什麼這麼想？(2pt)

2. Command Line Utilities (14pt)

1. 請對 speed.ntu.edu.tw trace route，並回答下列問題：
   在本題中，請使用 NTU SSL VPN 完成作答。依照你的系統，你可以自由選擇使用 `traceroute` 或 `tracert`，惟請確保作答前後一致。
   (a) 請寫下所執行的指令並截圖你的執行結果，其必須要順利找到目的地。(1pt)
   (b) 當你進行 `traceroute`/`tracert` 時，指令會同時顯示 speed.ntu.edu.tw 的 IP 位址，請另外提供至少兩個查詢特定 domain name 所對應的 IP 位址的方法，並截圖透過他們查詢 `speed.ntu.edu.tw` 的結果。(1pt)
   (c) 請辨別 a 小題執行結果中各個節點的 IP，哪些是屬於 private network、哪些是 public network；請說明你的判斷理由。(1pt)
   (d) 說明執行結果中，每列的三個時間代表的意思；請問越下面的結果一定比上面大嗎？是或否皆請說明原因。(1pt)
   (e) 依據你在 a 小題的執行結果以及指令的原理繪製循序圖，說明你的指令是如何達成該題執行結果；循序圖的範例如下圖左（2pt）：



上圖右便是對某個直接可到達的節點 `x.x.x.x` 進行 `ping` 的循序圖，更具體而言：

i. 循序圖中最左邊的縱軸是你的指令，請標示上你在 a 小題使用的指令
ii. 右軸則是收到封包的節點，請以其 IP 標示；注意在整個過程中可能會牽涉不只一個接收的節點，亦即可能會有多個縱軸
iii. 請用實線箭頭表示「發出」或「轉發」了封包，並加註該封包所使用的**協議**以及該封包的 **Time-to-Live 欄位**所具的值
iv. 若該節點收到封包後會回應，請用虛線箭頭表示回應，並註明該回應使用的**協議**及其**回應的種類**

2. 接下來的問題請針對 140.112.91.2 這台伺服器進行回答：
對於題目中需要附上指令的部分，若你的指令有使用到任何參數，請列出你認為解題所需**最簡短的參數組合**，可以附上必須使用這個參數的原因作為輔助說明。

(a) 我們想先使用 `ping` 這個指令來確認伺服器有沒有開機，請問：(1) `ping` 發送的請求與回應的訊息名稱 (2) 請附上執行 `ping 140.112.91.2` 指令後的結果。(1pt)

(b) 接下來請改成使用 `nmap` 這個指令對這台伺服器做「ping scan」（**注意！請不要進行 port scan !**）請附上執行的完整指令與結果，並與上一題 ping 的結果比較。如果有不同，請說明你的 `nmap` 指令發送了哪些請求才得到回應。(1pt)

(c) 我們在這台伺服器上開了一些服務，請使用 nmap 這個指令找出 (1) 開在 port 80 的服務名稱以及版本，並簡單描述一下這個服務是什麼 (2) 另外，請附上你執行的 `nmap` 完整指令。(1pt)

(d) 接下來，請你使用任意指令跟 port 80 建立連線，並對 / 這個路徑發送 HTTP POST 請求。最後，根據伺服器提供給你的提示找到隱藏的另一個服務，並接收這個服務傳給你的訊息。請列出所有你執行的指令與執行結果。(1pt)

3. DNS record
請附上解每題的指令和答案。

(a) **小孤獨的行蹤**
原本約好放學後來樂團練習的小孤獨 (Bocchi) 突然悄無聲息的缺席了。妳是她的知心好友喜多，心急如焚，於是啟用了偷偷放在她身上秘密追蹤器。這個追蹤器的名稱是 `Bocchi-Tracker.csie.ntu.edu.tw`，請依據它提供的線索，找到 Bocchi 的所在位置 (IP)。(1pt)

(b) **神秘地址的名稱**
透過追蹤器，妳剛才獲取了一組神秘的地址，但不知道這個地址所對應的名稱。請幫助她解析這組地址，確認這是什麼場所 (Domain Name)。(1pt)

(c) **吉他的線索**
來到該場所後，妳找到了小孤獨，卻發現她將吉他忘在了這裡。在尋找吉他的過程中，妳注意到此場所留有一張**字條** (TXT)，似乎和 Bocchi 的吉他有關係。請揭開字條上的內容，告訴她吉他放哪裡。(1pt)

(d) **小孤獨不為人知的一面**
小孤獨最近常常一個人對著手機傻笑，妳隱約偷瞄到她有經營一個頻道，但不知道她的名稱。現在，請根據域名 `Bocchi.csie.ntu.edu.tw` 的線索，找出她的**別名** (CNAME)，揭開她的另一個身份。(1pt)

3. Basic Wireshark (11pt)

請下載 Wireshark 及題目檔案，分析 `p1.pcapng` 以及 `p2.cap` 的內容，並且回答問題。

1. 請以 Wirshark 分析 `p1.pcapng`

(a) 根據檔案內容，請辨識作為伺服器的機器，給出其所使用的 port。(1pt)

(b) 請解釋上題你的判斷依據。(1pt)

(c) 請使用 Wireshark 內部的工具繪製流量表（I/O throughput graph），並且調整單位為 bytes/1 sec 之後截圖。(1pt)

(d) 請問最高的傳輸速度是多少（bytes/1 sec)？是發生在哪個時刻呢？(1pt)

(e) 請問在 `p1.pcapng` 中出現了多少個 HTTP GET 的 request？請說明你如何計算出這個數量。(1pt)

(f) 在這題的封包中，用戶端新增了一筆發票資訊（invoices）到伺服器上。請找出更新資訊中，`customer ID` 欄位的值。(2pt)

2. 請以 Wirshark 分析 `p2.cap`

(a) 如果你有私鑰，wireshark 能夠幫你解碼以 SSL 加密的封包內容。請以本題所附上的 `p2_private.key` 檔案，解密封包內容，並詳細說明你如何做到。(2pt)

(b) 在 `p2.cap` 檔案中，有傳送了一張 Apache 的官方圖片，請回答是第幾個封包內包含了此圖片，並且附上此圖。(2pt)

4. Cryptography (5pt)

Act I: 三角初華的祕密委託

身為在 NASA 工作的資安專家，你精通各種密碼學系統的運作原理與攻擊手段，包含被廣泛利用的公開金鑰加密 (public-key encryption) 演算法: RSA(Rivest–Shamir–Adleman)。一天，當紅樂團 Ave Mujica 的主唱兼吉他手——三角初華——找上了解 RSA 的你，打算委託一個 RSA 相關的祕密任務。為了防止其他人竊聽這項祕密任務的內容，她打算使用你提供的 RSA public key 加密任務內容，再將加密後的內容傳給你。這樣一來，只有持有 RSA private key 的你能夠解開這個加密訊息，進而防止其他人得知初華委託了什麼給你。

初華執行的程式為 `uika.py`，其原始碼可以在這裡下載。在 `uika.py` 中將會用到 `MISSION` 這個變數，其內容即為初華要傳輸給你的訊息內容，但這個變數定義在 `secret.py` 中，而你無法存取 `secret.py` 的內容。初華在 `140.112.91.1:48763` 等著你，你可以透過 `nc 140.112.91.1 48763` 來聯繫她，其中 `nc` 是 netcat 的指令，用於建立 TCP 連線。

請接收並解開初華所傳給你的加密訊息，以接下她所委託的祕密任務 (**無須完成任務**)。為了證明你有正確收到她委託的任務，請找出包含於任務內容的 flag，此 flag 的格式為 `NASA_HW0{...}`。答案只須包含你找到的 **flag** 與你的**解題過程**。此外，若你在解題過程中有使用指令或程式，也須將它一併附於答案中。

附上一些你可能會需要的資源：

- Python packages:
  - PyCryptodome `Crypto.Util.number` 裡面的 `getPrime(n)` 能生成 n-bit 質數，而 `long_to_bytes` 能將 integer 轉換成 byte string
  - Pwntools: 若只想學會完成本題所需要的 Pwntools 基本用法，GPT(或其他 LLM) 是可以讓你快速上手的好老師
- RSA:
  - A Graduate Course in Applied Cryptography §10.3: A Trapdoor Permutation Scheme Based on RSA
  - Wikipedia

在接下祕密任務後，你驚訝地得知：竟有人膽敢欺騙另一支樂團的吉他手兼溝通大師——千早愛音，導致她誤用糟糕的 RSA public key 來加密她的私密資料！聰明的你能夠在之後的作業幫助三角初華，解開主謀的身份嗎？

HW11 待續.....

5. 為什麼簽不了憑證 ??? (10pt)

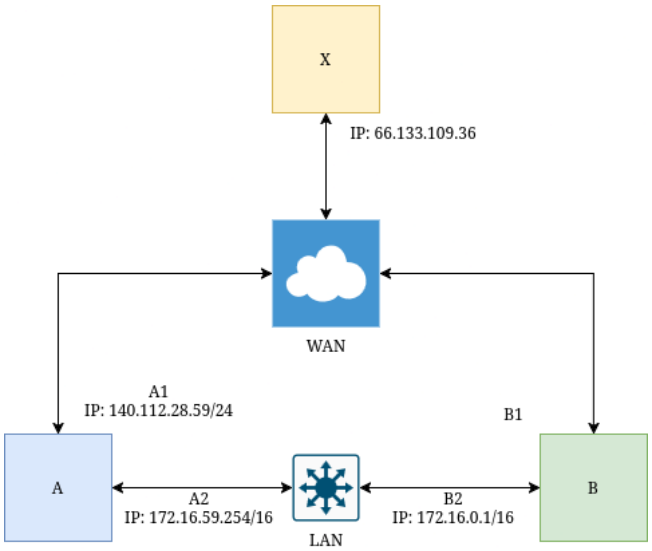
以下題目改編自令人痛苦的真人真機器真事。

題目背景

修完了 NASA 1234（?）階的你成為了程式解題社的網管，負責社團系統的大小事。某天你想幫社團網站簽憑證的時候，發現居然簽不動！

社團和系上的網路系統架構圖（簡化後）如下。有三臺重要的機器：

- 機器 A 是社團的機器，有兩個網路介面：
  - 第一個介面 A1 的 IP 是 140.112.28.59/24（WAN）
  - 第二個介面 A2 的 IP 是 172.16.59.254/16（LAN）
  - A 的 default gateway IP 設定為 172.16.0.1。
- 機器 B 是系上防火牆，有兩個網路介面：
  - 第一個介面 B1 連接 WAN（IP 不重要）。
  - 第二個介面 B2 的 IP 是 172.16.0.1/16（LAN）
- 機器 X 是 Let's Encrypt （簽憑證用）的機器，IP 是 66.133.109.36。



為了簡化問題，我們假設 WAN 是一個可靠的通訊管道，不會掉封包或弄壞封包。

題目

本大題是問答題，請在保持答案完整的前提下，儘可能簡短的回答。
所有題目應該都可以在兩句話內回答完整。

1. 什麼是 subnet？(1pt)
2. 什麼是 gateway？(1pt)
3. 給定架構圖，如果 X 想要送一個封包到 A1 的 IP，會經由什麼樣的路徑到 A1？(1pt)
4. 給定架構圖，如果 A 想要送一個封包到 X，會從哪個介面（A1 或 A2）、經由什麼樣的路徑到 X（例：A1 -> WAN -> X）？(1pt)
5. 我們（應該）都知道防火牆可以擋住可疑的封包。請問 stateful 和 stateless 的防火牆差在哪？哪一種比較可能擋住 TCP ACK without SYN？(1pt)
6. 簽憑證的（簡略）過程如下：
   - 第一步：A 和 X 說「我要幫 A1 的 IP 簽憑證」。
   - 第二步：X 發一個 HTTP request 的封包到 A1 檢查。
   - 第三步：A 發一個 HTTP response 的封包回答 X 的檢查。

   根據 debug log 顯示 A 沒有收到 X 第二步的封包。

   已知 B 是一臺 stateful 的防火牆，在所有連線都正整常運作的情形下，請問可能原因為何？(3pt)
   - 提示一：你可以用 這些封包記錄 來驗證你想的是否正確！
   - 提示二：TCP 和 HTTP 是不同東西，要先建立 TCP 連線才可以發送 HTTP request！
   - 提示三：A 用 A1 的 IP 發送的封包不一定是從 A1 出去……？

(以下問題沒有標準答案，給出合理的回答才有分)

7. 測試系統、更換憑證時通常需要讓系統下線、停止服務，因此需要把停止服務的時間公告給使用者。請估計需要花的時間，並且簡略說明原因（例如每項工作預估所需時間）。(1pt)
8. 請提出一個讓 Let's Encrypt 可以正常運作、順利簽到憑證的解決方案。(1pt)
9. 以上是 NA 可能會遇到的情境模擬。你準備好加入 NASA，解決這些奇怪的問題了嗎？(0pt)

System Administration

6. btw I use arch（15pt）

在 SA 部分題目的一開始，請先安裝一台 Arch 發行版的 Linux 作業系統作為基礎技能的練習，可以採用雙系統、虛擬機等任意形式。系統設定需求如下：

- 為了避免系統差異，請使用我們提供的安裝檔作答
- Partition Layout

Mount Point	Format	Size
/	ext4	約 15G
/home	ext4	約 5G
SWAP	swap	請跟據你的記憶體配置選擇適當的參數
其他必要的分割	-	-

- boot loader: grub
- 你需要可以在開機時自動掛載前面提到的所有分割區，並啟用 SWAP
- 新增使用者：帳號與密碼皆為 nasa
- 其他沒指定的設定可任意調整，請在作答時說明即可。

附上一些你可能會需要的資源：

- 安裝檔下載：
  - link: https://drive.google.com/file/d/12K2puYQmNDLbrV4WvJa52YpDlL0ef8If/view?usp=sharing
  - or `/tmp2/b10902001/` on `ws5`
  - `/tmp/hw0` on 公用電腦
  - sha256 checksum: `74b109b4b36d20bef8f4203e30b8d223e0ab297a09d1a1213a02894472aa530a`
- 安裝教學：https://wiki.archlinux.org/title/Installation_guide

6-0. (0pt)

請敘述你安裝的流程，如果流程有重大瑕疵或是沒有完成本小題的話，將酌扣本大題的分數。

6-1. (5pt)

請將主機的 host name 改成你的學號，並截圖繳交（如果你是雙系統則可以用拍照的）。

6-2. (5pt)

請使用指令來印出機器中各分割的 uuid，以及磁碟空間分配，並截圖繳交。

6-3. (5pt)

請使用指令查詢你所使用的 Linux Distribution 以及 kernel 版本，並截圖繳交。

7. Flag Hunting（25pt）

請使用以下的虛擬機來完成以下的題目（帳號與密碼皆為 nasa），找出題目中隱藏的 FLAG，並敘述作答的過程。

- `/tmp2/rabhunter/nasahw0-flag.qcow2` on `ws5`
- `/tmp/hw0/nasahw0-flag.qcow2` on 公用電腦
- sha256 checksum: `92dc99a084447b27ac6e99833b0fb5161aa4fca8819b4e7ca4f3bf562301562a`

前言

後續會有許多地方會需要用到虛擬機，這裡簡單說明要如何使用 qemu 開啟虛擬機。

1. 第一步就是去安裝 qemu，請根據自己的發行版來安裝。
2. 接下來，輸入以下指令：`qemu-system-x86_64 -m 4G -vnc :3 nasahw0-flag.qcow2`
3. 研究一下前面的指令的參數，並請根據你的需求進行調整。
4. 接下來使用 vnc viewer 進行連線（推薦 tigervnc），如果你是在本地端進行架設，對 localhost 的 5903 port 進行連線即可；若是在工作站上的話，則需要對工作站機器的 5903 port 進行連線才能連線到你的虛擬機喔！這裡 port 的選擇與前面指令的 `vnc` 參數有關，請自行研究。

正文

1. history（6pt）
   打開虛擬機後，你第一個念頭就是想找出助教出題時使用的指令歷史紀錄，然而，你卻發現 history 早就已經被助教動過手腳了，現在的你並不知道真正的 history 被紀錄在哪個檔案中，幸運的是，你發現粗心的助教並沒有把舊的 bash history（bash 的預設 history file）紀錄檔清乾淨...。
   (a) 請找到目前存放 bash history 的檔案位置？(2pt)
   (b) 請找到哪邊可以設定當前 bash session 可以暫存的歷史指令數。(1pt)
   (c) 請找到哪邊可以設定 history file 中可以記錄的指令數大小上限？(1pt)
   (d) 請從原本預設 history file 中找到真正的 flag 的位置相關線索後，到新的 history file 中尋找真正的 flag，flag 的格式必定為 NASA...，且裡面的內容看起來會像是有意義的文字。(2pt)
2. 寶藏箱（/home/nasa/treasure）(5pt)：
   你發現了一個很酷的寶藏箱，不過裡面似乎有點亂...。你能找到藏在其中的 FLAG 嗎?

(執行/home/nasa/treasure 並在執行結束後依照指示在 treasure-chest 目錄底下尋找 FLAG，FLAG 的長度不超過 100，而且裡面的文字是有意義的。FLAG 後面沒有意義的亂碼不是 FLAG 的一部份，而如果你找到的 FLAG 是沒有意義的亂碼的話，那可能不是正確的...)

3. 魔物（/home/nasa/boss）(5pt)：
   你遇到了一個很強大的魔物，而且他似乎握有 FLAG 的資訊，他在一瞬間生出了好多個分身! 只要在 3 秒內擊敗本體以外的所有分身，或許他就會知道你的厲害並告訴你 FLAG 了...

4. 通關密語（/home/nasa/chal）(5pt)：
   前陣子小明送了小奕一個沒有超過 40 個可識字元的 FLAG，小奕怕麻 FLAG 被偷走，所以把 FLAG 藏在 chal 中，只有在執行檔案時使用正確的通關密語才能看到 FLAG，而且為了防止 FLAG 被爆破出來，他還特地設了很多錯誤的通關密語來混淆視聽。

   現在由於一些原因，他想要存取這個 FLAG，可是健忘的他卻忘記正確的通關密語了，於是小奕跑來向你求助，畢竟你是他最信任的人。他偷偷和你分享一個分辨真假通關密語的關鍵：只有正確的通關密語同時含有 486 和re02 這兩個子字串。

   請幫小奕找回他的 FLAG（FLAG 的格式必為 NASA2025{...}）。

   Hint: 原始碼中的字串經過編譯後常常會原封不動的殘留在 binary 中...

5. tmux (本題沒有 flag) (4pt)
   tmux 是個相當方便的指令，可以讓你自由的切換工作，他的 detatch 功能也可以讓你再也不擔心作業寫到一半斷線！請嘗試在我們提供的虛擬機中，使用 tmux 製作出如下的 layout，並附上製作流程：

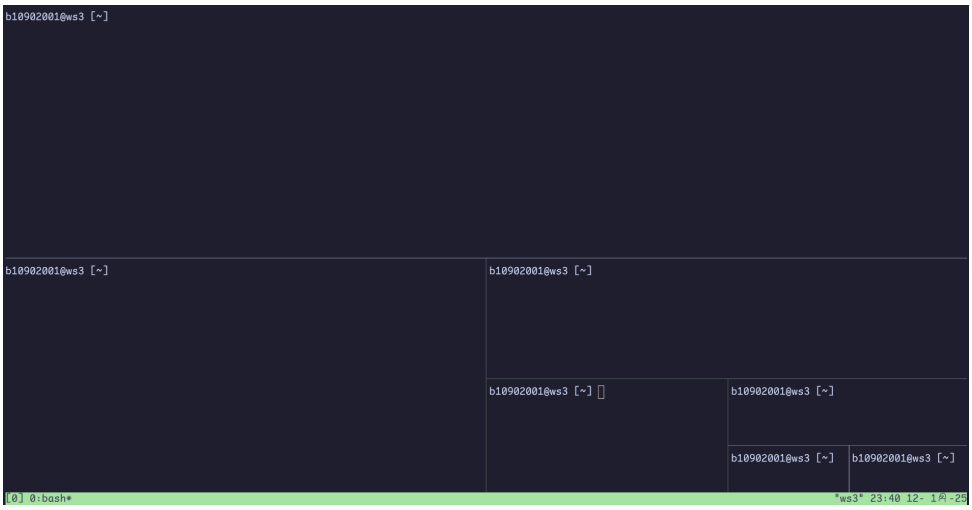


Figure 1: 示意圖

Hint: 有注意到預設的 Prefix 按鍵 Ctrl+b 沒有作用嗎？這會是為甚麼呢？

8. NASA 國的大危機（10pt）

在遙遠的 NASA 國度，黑暗勢力正步步逼近，揚言將在某天派出殺手暗殺國王。傳說中，只有喚醒「神奇聖杯」的超強預言能力，才能預知黑暗勢力的行動日期，拯救國家於危難之中。

國內典籍記載，喚醒聖杯（Docker Container）需要閱讀古老卷軸（Dockerfile）所述的咒語，並為容器注入正確的魔法元素。然而即使成功喚醒，還有一群神秘傳令兵，正在偷偷從某個位置傳送極機密的暗號。如果能找到這些暗號，就能知道殺手在哪一天入侵！

8-0. 準備

- VM 的 qcow2 如下，請參考前一題的教學來開啟 vm。
  - 網址
  - or `/tmp2/rabhunter/nasahw0-pickle.qcow2` on `ws5`
  - or `/tmp/hw0/nasahw0-pickle.qcow2` on 公用電腦
  - sha256 checksum: `c5af3166092080c7cbb42d8ef6e73af18fc2aea054c00f859a1f05c3a35af9cc`
- 本題的 VM 在工作站啟用時並不會有對外的網路，我們認為 VM 中已有足夠的工具可以完成此題（我們安裝了不只一種）。若是你真的想裝 VM 中沒有的工具的話，請自行修好 VM 的網路。
- 帳號：nasa
- 密碼：nasa2025

8-1. 解讀古老卷軸（3pt）

在 mystic-cup 目錄裡，你會發現一份古老卷軸——Dockerfile。請詳細說明：這個 Dockerfile 裡面到底寫了什麼？每一段指令（FROM、RUN、COPY、CMD）在做哪些事？

8-2. 啟動聖杯（3pt）

請嘗試正常啟動虛擬機裡面唯一的 docker image，並想辦法成功喚醒它。

提示：

- 或許你可以使用 docker images 查看目前存在的 image，並嘗試正常啟動。
- 詳細閱讀 Dockerfile，破解的線索就在其中！

8-3. 神秘訊息（4pt）

成功喚醒聖杯後，神秘的影像在容器中顯現。你會注意到 docker container 中有一個不斷在進行的資料傳送行為。（傳令兵正在不斷地偷偷傳遞訊息，似乎是跟殺手入侵的日期有關），發揮你的網路技能，設法找出這內部到底哪裡有封包在傳送！

找到之後，請解讀封包，並回答殺手入侵的日期（你找到的封包內容應該類似於 flag[...]。）