Homework #0

Due Time: **2025/09/04 (Thu.) 23:59**
Contact TAs: `nasa@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 here. Please visit this 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

- NA is 50 points and SA is 55 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 points *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 $50 + 55 + 3 = 108$ points. However, we cannot guarantee the minimum score to be admitted into the course.

Network Administration

I. Short Answer (22 points)

†請根據最廣泛使用的 TCP/IP 模型（共 5 層；可參考 Kurose 與 Ross 撰寫的課本與錄製的線上影片），列出每一層的名稱、簡述其功能，並提供一個每層實際應用服務的例子。(2 points) 網路設備與常見問題解析

2. (a) 請簡單介紹什麼是 VLAN。(1 points)
   (b) 請簡單介紹什麼是 Gateway。(1 points)
   (c) 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。(1 points)
   (d) 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。(1 points)

3. 請解釋 NAT 並舉例其兩個應用。(2 points)

4. 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？(2 points)

5. 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？請至少給一個例子。(2 points)

6. 臺灣大學資訊工程學系有著自己的無線網路，你認為架設一個完整的無線網路可能需要什麼設備，這些設備的功能是什麼？(4 points)

7. 你有一台伺服器，安裝了兩張網卡：

   - 外網介面 (`eno0`)
     - Subnet: 140.112.30.0/24
     - Gateway: 140.112.30.254
   - 內網介面 (`eno1`)
     - Subnet: 172.16.0.0/16
     - Gateway: 172.16.0.1

   目標：讓伺服器同時擁有一個外網的 public IP，以及一個能存取內網機器的 private IP。假設伺服器外網 IP 是 140.112.30.1，則其他機器在有連上網路的環境下可以 ping 到 140.112.30.1，並且伺服器本身可以 ping 到 8.8.8.8, 172.16.0.2, 10.0.0.1 等其他機器（假設他們存在）。

   注意：內網機器不一定會在同一個 private IP 網段，要分開設定。

   請問你會如何設定這台伺服器的 IP 路由？文字敘述或是給 netplan 設定檔皆可。(2 points)

8. 你有一台伺服器，只有一個網路孔，但需要同時連接到三個不同的網段。為了達成目標，你購買了一台可支援 VLAN 的 switch。現在網路線的連接如下：伺服器的網路孔連到 switch 的 port 1，三條網路線來自三個不同網段，並分別連接到 switch 的 Port 2、Port 3、Port 4。注意：這三個網段原本是沒有 vlan 的。

   (a) 請解釋 switch 的 trunk/access 模式他們的功能，這兩個設定在 vlan 設定上有什麼不同。(1 points)

(b) 請問你會如何設定 switch？VLAN ID 可以自由選擇。請填入以下表格。(2 points)

Port	Mode (trunk/access)	Native VLAN	Tagged VLAN(s)
1			
2			
3			
4			

(c) 請問你會如何設定伺服器的網路介面，文字簡要敘述即可，routing 部分可忽略。(1 points)

II. Command Line Utilities (8 points)

1. 找出對應的 IP address
   (a) www.ntu.edu.tw (2 points)
   (b) csie.ntu.edu.tw (2 points)
2. 找出對應的 domain name
   (a) 140.112.30.56 (2 points)
   (b) 140.112.2.142 (2 points)

III. 網路連線與 WireShark (20 points)

1. TCP 封包
   (a) 請簡述 TCP 封包的用途，以及它在傳輸層所扮演的角色。(1 points)
   (b) 請列出並解釋 TCP Header 中五個主要欄位的功能（例如：Source Port、Destination Port 等）。回答時請具體描述用途。(1 points)

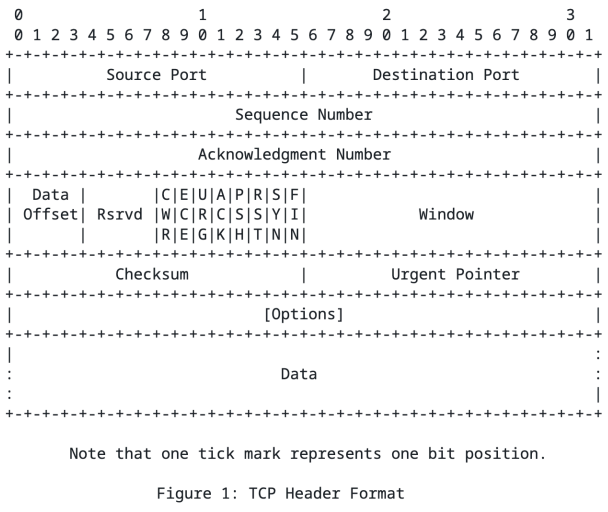

Figure 1: TCP Header Format (取自 https://datatracker.ietf.org/doc/html/rfc9293)

(c) 請解釋為什麼 TCP 需要三向交握（Three-way Handshake），並清楚描述三個封包的內容（如 SYN、SYN+ACK、ACK）以及雙方確認的資訊。回答時請注意不要只寫縮寫，請具體說明它們各自確認了什麼。(2 points)

2. ICMP

   (a) 請說明 ICMP 的主要功能，以及它和 TCP/UDP 在傳輸方式上的差異。(1 points)

   (b) 請舉出三種常見的 ICMP 訊息類型，並說明其用途。回答時請寫出完整名稱（例如 Echo Request）。(1 points)

   (c) 在 Linux 系統上，指令 `ping` 會使用 ICMP 來測試網路連線狀態，請解釋其運作原理（例如，如何利用 Echo Request 與 Echo Reply 進行測試）。(1 points)

   Wireshark 是一個開源的網路封包分析器，可即時從網路介面擷取封包中的資料。可以從這個連結去找到下載網址：https://www.wireshark.org/download.html

3. Wireshark：SSL 解密

   (a) 請簡述 SSL/TLS 的用途，並說明它如何確保傳輸的安全性。(1 points)

   (b) 請解釋什麼是 pre-master secret key，以及為什麼在使用 Wireshark 來解密 SSL/TLS 封包需要用到。回答時請提到它與會話金鑰（session key）的關連。(1 points)

   (c) 請比較 HTTP 與 HTTPS 的差異，並具體說明在傳輸過程中資料是如何受到保護的。(1 points)

   (d) 使用提供的 pre-master secret key log 以及 `pcapng` 檔案，以 Wireshark 來解密這段 HTTPS 封包，並回答以下問題。回答時詳細描述你找到該段查詢內容的過程，並指出是在哪一個封包（編號）中出現。

   這題所需檔案在以下連結：https://drive.google.com/drive/folders/1Uf3PDd9LZRuZ7oJ8QDOt-9J7ckSZ-ygt?usp=sharing

      i. 在解密後的封包中，有連上一個臺大的網站，請說明是哪個網站，並指出你在 Wireshark 中是在哪個欄位（field）看到的。請具體寫出欄位名稱。(2 points)

      ii. 在解密後的封包中，可以發現使用者在該網站搜尋了一段內容，請寫出該查詢內容（為四個中文字），並說明你是如何找到的。(2 points)

4. Wireshark：封包擷取

   (a) 請使用 Wireshark 擷取 `ping` 指令的 ICMP 封包，並附上一張截圖，必須顯示至少一個 Echo Request 與一個 Echo Reply，並且請標出 `ping` 的目標 IP（例如 `8.8.8.8`）。(1 points)

   (b) 經過前面的討論，你知道 HTTP 很不安全！聰明的你，發現網站 http://neverssl.com/ 並沒有使用 SSL 加密，於是你打算開啟 wireshark 來看看能不能偷看到封包內容。

   - 請使用 Wireshark 擷取封包，並使用瀏覽器連線至 http://neverssl.com/
   - 請在 Wireshark 中找到對應的 HTTP 封包，並附上有包含連線資訊的顯示封包截圖。(如：HTTP Host, HTTP Connection 資訊等)
   - 請說明你是如何找到的（用了什麼 wireshark 的指令或是在 wireshark 的哪個欄位）。

   (5 points)

System Administration

I. 想變強的捷兔 (15 points)

捷兔自從在龜兔賽跑慘遭烏龜打敗之後就一心一意地想要成為全宇宙的最強，不過要成為最強並沒有這麼簡單。需要經過層層的歷練，要先有辦法理解何謂『最強』，了解之後才有辦法到強者的聖地進行訓練，並在過程中領悟真理並在強者的路上邁進。

在強之前還有一道牆

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。(若使用 NASA 課程公用工作站或是資訊系工作站則不需這一步)
2. 下載要開啟的 qcow2 檔案後，輸入以下指令：

   ```
   qemu-system-x86_64 -m 4G -vnc :3 nasahw0-tddy.qcow2
   ```

3. 若有需要，請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， `-vnc : d` 表示會連到 `port 5900+d` 。

- Hint1：推薦使用 `tmux` 來開 VM ，即使終端機關掉仍可以維持 VM 運作。
- Hint2：執行上述啟動 VM 的指令後，如果沒有出現錯誤訊息而只是停在那裡，這是正常的，表示 VM 正在運作，可以直接進行下一步。
- Hint3：若使用工作站，port forwarding 可以查查看 `ssh -L` 的相關用法。
- Hint4：VM 開機需要一小段時間。

底下會有兩種方式可以開啟虛擬機，分別是從雲端下載在本地端執行，或從資訊系工作站上指定目錄複製檔案後執行 (速度較快不需下載)，資訊系工作站的使用方式可以參考：ssh 使用方式, 資訊系工作站使用規範, 資訊系工作站使用小技巧。(tl;dr : 在 terminal 輸入 `ssh < 學號 >@ws6.csie.org` 詳細說明皆在上面網址內)。

破牆而入

- VM 的 qcow 檔案連結如下，請參考上面教學開啟虛擬機：
  - qcow Link （檔案較大，約 3GB，若下載一直失敗可嘗試使用 gdown 下載)
  - 另一個下載點：/tmp2/nasahw0-vm/nasahw0-tddy.qcow2 on ws6（請先複製到自己的目錄再進行操作)
  - sha256 checksum : ff772ac007c378bb1e85f5cd83211e3182f0f3be40b0bed9e9ca915a16672cba
- 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。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：nasa

何謂最強

進到虛擬機的/home/nasa 目錄底下後會發現一份強者留下來的體悟————Dockerfile。請詳細說明：

1. Dockerfile 裡面到底寫了什麼？每一段指令(FROM、WORKDIR、COPY、RUN、ENTRYPOINT)在做什麼事？
2. 如果把 RUN 執行的指令合併到 ENTRYPOINT 一起執行可能會發生什麼事情？可以這樣做嗎？
3. 可以把 ENTRYPOINT 換成 CMD 嗎，為什麼？請簡述 ENTRYPOINT 跟 CMD 的關係 (若同時有 ENTRYPOINT 跟 CMD 會發生什麼事)？

強者的聖地

在領悟完『強』之後終於可以前往聖地了。你可以透過某些指令查看目前虛擬機內所有的 docker image，請試著啟動唯一的 docker image 並進入到聖地裡（docker 裡面的 shell)。為了確保你進入聖地以後可以在裡面的 shell 互動，你在需要使用特定的參數啟動它。請簡述找到並且啟動 docker image 的指令，並且將進入 docker 裡面 shell 的畫面截圖下來。

Figure 2: 進入 Docker Shell 的示意圖

成為最強

到了聖地之後你發現雖然勤勞練習努力是變強的重要要素，但就如同古人所說的一樣“休息是為了走更遠的路”對於強者更是如此，尤其是對捷兔來說休息跟假期是成為強者不可或缺的最後要素，畢竟

Nothing beats a 捷兔 holiday!

不過要擁有假期也不是這麼容易，請幫捷兔在茫茫強者聖地中找假期吧！(請在 docker container 裡面的 shell，透過輸入某些指令找到 holiday.txt 並且從中得到 flag (FLAG 的形式 `FLAG{...}`)。)
找到之後請把回答 flag 的內容並簡單描述使用了哪些指令得到 holiday.txt 並且如何得到 flag。

II. RSA (10 points)

RSA 是現今被廣泛使用的非對稱加密演算法之一。演算法需要使用兩個金鑰：公鑰和私鑰，兩者相互對應，私鑰由使用者保密，公鑰則可以任意公佈。我們可以使用公鑰將**明文**加密，得到**密文**，而密文只有相對應的私鑰可以解開。請閱讀 RSA Operation，了解其數學原理。

本大題需要使用的檔案在這裡下載。

1. `rsa.py` 裡面包含一組私鑰 (N, d)，以及一則密文。明文是一則字串，將明文字串透過 ASCII 編碼為 hex string (十六進位字串)，然後再透過十六進制轉換為整數 m 後，對整數 m 進行加密操作得到整數 c，最後將 c 透過十六進制轉換為 hex string，並將 hex string 編碼為 Base64 字串，即為檔案中的 cipher。請撰寫程式，將密文解密得到明文，並將得到的明文寫在你的回答中。

   Hint1：明文的形式為 `FLAG{...}`。

   Hint2：你可能會想使用 PyCryptodome 提供的 `bytes_to_long()` 和 `long_to_bytes()` 來幫助你轉換資料型式。

2. `private.pem` 是一把由 PKCS#8 定義的格式儲存的 RSA 私鑰。雖然實際上使用私鑰加解密時只需要 N, d 兩個整數，但按照文件的定義，我們實際上使用的 RSA 私鑰儲存了 N, p, q, e, d 等關於金鑰的完整資訊，因此我們可以從中提取出 RSA 公鑰。請使用 openssl 命令列工具，從 `private.pem` 取得對應的公鑰，並附上使用指令以及產生的公鑰文件內容的截圖。

   Hint：公鑰文件內容的開頭處應該會寫著“`-----BEGIN PUBLIC KEY-----`”。

3. 請找出 `private.pem` 私鑰中的 N 為多少，並附上解題工具的截圖。由於該數很大，請提供 N 在十六進位中最低 8 位的數字。

   Hint：PKCS 幾乎都使用 ASN.1 這種資料描述語言來定義物件。

III. The Web (15 points)

全球資訊網（World Wide Web，常簡稱為 WWW 或 the Web）最初由英國電腦科學家 Tim Berners-Lee，於 1989 年在歐洲核子研究組織（CERN）工作期間發明，並於 1993 年將其程式碼釋出至公有領域，開放任何人免費使用，間接促成了 WWW 的蓬勃發展。時至今日，WWW 又歷經了 Web 2.0、甚至 Web 3.0 的革命，一步步地造就了我們現今熟悉的網路體驗。

1. **核心技術**

   當時為了實現 WWW 的構想，Berners-Lee 先後開發了三大核心技術，即今日為人熟知的 HTTP、HTML、URL。請回答：這三項名詞分別是什麼？他們的用途為何？

2. **終端機瀏覽器**

   (a) 請在終端機中執行 `curl -v http://www.csie.ntu.edu.tw/`，截圖附上執行結果，也請將內容填入下表：

欄位	**內容**
請求方法（Request method） 請求目標路徑（Request target） 請求使用的 HTTP 協定版本 請求標頭（Request headers，全部列出）	
回應狀態碼與訊息（Response status code and message） 回應使用的 HTTP 協定版本 回應標頭（Response headers，全部列出） 回應主體（Response body，列出一兩行即可）	

   (b) 乘上題，我們看到這個特定的回應狀態碼與訊息代表什麼意義？其中又會用到哪個回應標頭的資訊？那個標頭代表什麼意義？

   題外話：可以去看看 HTTP Cats。

(c) 如果再執行 `curl -v http://www.inm.ntu.edu.tw/`，我們會驚訝地發現，他和 `www.csie.ntu.edu.tw` 是連到同一個 IP 位址，卻是兩個截然不同的網站。
請問這是使用了什麼技術？伺服器要如何得知我們是想連到哪個網站？
題外話：Cloudflare 提供的服務與此息息相關。

3. **捷兔的優惠**

捷兔在成功找到假期後，又接獲到神秘情報，得知有個假期優惠碼隱藏在系上的某台伺服器中：

- 情報中說道：「旗者，虛實交錯之境也。」
- 虛：網址顯示為 `jet2holidays.csie.ntu.edu.tw` 之 `/discount`。
- 實：實際服務卻藏在 `ws6.csie.ntu.edu.tw` 之 21080 port。

輸了龜兔賽跑的捷兔賠光了一生積蓄，家徒四壁的他亟需此優惠。然而面對這謎語般的情報，他卻不知從何下手，因此找到了精通 NASA 的你。請你幫忙捷兔找出優惠碼(格式為 `FLAG{...}`)，並附上找出優惠碼的詳細流程（如指令、設定檔等）。

- 提示 1：「虛」與「實」指涉 TCP/IP 模型不同層的內容，其中「虛」與 2.(c) 高度相關。
- 提示 2：這題不需使用到瀏覽器，請以終端機作答。
- 提示 3：可以先試著直接造訪 `ws6.csie.ntu.edu.tw:21080/discount` 觀察，再試著手動鑄造一個在現實中不合理的請求，而這至少有 2 種方法。

題外話：I'm a teapot

4. **安全？連線**

(a) 請連線至 `https://www.csie.ntu.edu.tw/`，並將該連線的 TLS 相關資訊填入下表：

欄位	內容
TLS 版本	
Cipher suite	
憑證主體（Subject）	
憑證發行者（Issuer）	
憑證到期日	

也請附上得到資訊的截圖或指令。

(b) 請問憑證在 TLS 中扮演的功能為何？

(c) 請問 TLS 1.3 相較於 TLS 1.2 的改進有哪些？試舉出 2 項。

(d) Google Chrome 於 117 版將網址列的鎖頭圖示換為「調整設定」圖示，因為 HTTPS 在今日已是常態，使用鎖頭圖示反而容易誤導使用者。在前面連結的文章中，其明確指出“For example: we know that the lock icon does not indicate *website trustworthiness*.”。請試著舉出一種「即使有 HTTPS 也未必安全（可信任）」的情境，並說明其背後的原因。

IV. Unix (15 points)

傳說有一位跑得比光還快的喵王——FLASHPAW。捷兔為了尋求變快的秘密，他必須找到喵王，請你幫助捷兔尋找喵王的秘密。

- VM 的 qcow 檔案連結如下，請參考「I. 想變強的捷兔」中的教學開啟虛擬機：
  - qcow Link （檔案較大，約 4GB，若下載一直失敗可嘗試使用 gdown 下載）

  - 另一個下載點：`ws6:/tmp2/nasahw0-vm/nasahw0-vm2.qcow2`(請先複製到自己的目錄再進行操作)
  - SHA256 checksum : df743d46d9ea85ecbcb843c1445b732f1a473bd492f02f2078f2c1bfdfccd712

- 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。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：nasa

進入喵王神殿

捷兔終於來到傳說中的「喵王神殿」，但大門上鎖，必須輸入通關密語才能進入。就在門口，捷兔撿到一個真空壓縮袋，裡面有一張神秘的圖片。請你幫助捷兔打開神殿吧！

- 可以嘗試先把壓縮檔（bag.zip）解開，看看裡面有什麼東西。
- 圖片看起來很普通，但也許有辦法能從檔案中「直接讀出我們想要的隱藏文字」。(Hint: 不要使用 `cat` 指令！如果手癢用了這個指令，可以考慮耐心等 30 秒讓它噴完亂碼你就會回到正常的終端機介面可以用了。)
- 通關密語的格式為 `FLAG{...}`。

喵王的房間

捷兔走進了神殿，發現裡面有許多大房間，每個大房間裡又有許多小房間，而小房間裡還有迷你房間。在每個迷你房間裡，都擺放著一個名叫 statue.sh 的檔案。現在捷兔擁有的線索是：真正喵王雕像的「大小」比其他的假雕像還大。請透過你的聰明才智，幫助捷兔找到真正的喵王房間。

- 想要進入神殿，請直接輸入上一題得到的「`FLAG{...}`」(包含 FLAG 和大括號）來解壓縮 temple.zip，並進入 temple 資料夾。
- 想一想，要怎麼快速找出目錄中「最大的檔案」?
- 當你找到真正的雕像時，請執行它 (./statue.sh)，它會告訴你你是否找對了！

召喚喵王

執行雕像後，雕像對捷兔說：「召喚我的方法，早已刻在神殿的石牆之中，只是被刻得非常淺……想見我，先偽裝成彩色貓咪，再使用彩虹之聲讓貓咪大聲喊出咒語 !」

按照雕像的說法，喵王房間內似乎藏有隱藏且加密後的召喚咒語，可以請你幫助捷兔尋找隱藏的召喚咒語並成功召喚喵王嗎?

- 在真正雕像所在的資料夾下，嘗試查看房間內的「隱藏檔案」，找到刻在石牆上的咒語。
- 咒語似乎經過一種名為 ROT13 的加密方法，經過加密後才刻在石牆上，請先將它解密回原本的文字。
- 讓咒語由「貓咪」念出來，並搭配「彩色效果」輸出。(Hint: 不需要自己繪製 ASCII art 喔，想想有什麼指令 ?)

- 請將輸出截圖下來，並且記錄所使用的指令，讓我們知道你已經成功召喚喵王！請注意：如果你不小心召喚到神龍、GNU 牛羚、或者是 Linux 企鵝的話都是不合格的噢。
- 以下為召喚喵王示意圖，裡頭的「summon spell」請替換成實際要輸出的咒語。

Figure 3: 召喚喵王示意圖