# Homework #0

Due Time: 2022/02/16 (Wed.) 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** 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.
- 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 https://hackmd.io/@uqzWTXyyTk6IYTBwcPwnoA/SklJTh0aF. 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: https://forms.gle/cu6AXw9fvFsLGWhF6.
- If you need to update your submission, please create another submission. We'll use your latest submission as your final submission.

### Grading

- NA accounts for 100 points while SA accounts for 100 points. The final score is the average 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 a *7% early-bird bonus* points in HW0. It decays linearly since *2022/02/07 10:00*.
- 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.
  - Please choose a friendly font and adequate font size for your main content. Also, please do not use a weird background color or text color.
  - *Tidiness score* is not limited to the above rules. If your document has other factors which makes it hard to read, you will not get full points of *tidiness score*.

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 $\frac{100+100}{2} + 7 + 3 = 110$ points. However, we cannot guarantee the minimum score to take the class.

# Network Administration

## 1. True/False (40 points)

針對每一個問題，請回答該敘述是否為真，並簡單說明原因，每題 4 分。

1. 現在新聞中常聽到得 4G 和 5G，都是指網路的傳輸速度。
2. 每一個裝置 (e.g. 筆電) 都只有一個 **MAC address**。
3. 因為 NAT，私有網路中不同機器發出的封包，外部網路看到的 Source IP 會是一樣的。
4. 當使用 **VPN** 時，從使用者的裝置發出的封包內 Source IP 的值會直接被修改。
5. 在 **intranet** 中, 所有封包的傳輸都必須經過 gateway。
6. 假設你發送了一個 request 到 DNS server 8.8.8.8，若 server 中並未擁有該 request 的答案，你只會收到一個"no corresponding domain" 的回覆。
7. 若是 DHCP、DNS 以及 NAT 不存在，我們就沒有辦法連到網路中一個已知 IP 的 server。
8. 若一個裝置從 DHCP 拿到了 IP，則從這一刻開始，任何由此裝置送出的封包都會經過該 DHCP server。
9. 如果我們使用 HTTP protocol 發出封包，任何收到此封包的人都可以很輕易地獲得 Source IP、Destination IP、訊息內容等資訊。
10. 使用 RSA 加密演算法時，若選擇越長的密鑰長度，安全性也會越高。

## 2. Short Answer (35 points)

回答問題，每題 7 分

1. 簡單解釋下列名詞，並說明其用處。
   (a) MAC address
   (b) Switch
   (c) broadcast storm
2. 說明何謂 **subnet mask**，並選出與 192.168.0.1/23 在相同 subnet 的 IP address。
   (a) 192.167.0.1
   (b) 192.168.0.0
   (c) 192.168.1.0
   (d) 193.168.0.1
3. 在學習網路運作原理的時，**five-layer internet protocol stack** 是我們第一步要先學會的。請列出 five layers 分別為何 (2%)，簡述每層 layer 在做的事 (3%)，並舉出每一層 layer 提供的服務的例子。(2%)。
4. 簡短說明何謂 TCP 及 UDP(3%)，兩者互相比較之下的優點與缺點 (2%)，並分別舉出一應用或是情境，我們會選用 TCP/UDP 而非另一種 (2%)。
5. 網路攻擊事件已經變得越來越常發生，請簡單敘述下列攻擊如何運作，以及如何防範它們。
   (a) DoS
   (b) DDoS
   (c) Man in the middle attacks

## 3. Command Line Utilities (25 points)

針對下列問題，若在回答時有用到 command line，請在答案中提供所有使用到的所有指令。

1. 找出對應的 IP address

   (a) www.ntu.edu.tw
   (b) csie.ntu.edu.tw

   找出對應的 domain name

   (a) 140.112.30.32
   (b) 140.112.161.178

2. **NTU VPN**

   以下問題會需要連到台大的 VPN 請參考下列網址。

   **Usage of NTU SSL VPN**: https://ccnet.ntu.edu.tw/vpn/
   For Windows: https://ccnet.ntu.edu.tw/vpn/for-windows.html
   For Linux: https://ccnet.ntu.edu.tw/vpn/for-ubuntu.html
   For Mac OS: https://ccnet.ntu.edu.tw/vpn/for-macosx.html

   請連到台大的 VPN server 並回答以下問題

   (a) 你獲得的 IP Address 為何？(3%)
   (b) 當你送出 `csie.ntu.edu.tw` 的 domain name request 至 DNS server 時，該 DNS server 的 IP 為何？此外，請提供此 query 至 root name servers 的 deleagation path。(3%)
   (c) 現在，請中斷連結 VPN，並送出 `csie.ntu.edu.tw` 的 domain name request 至 DNS server 時，此時 DNS server 的 IP 為何，請說明為何與 (b) 結果不同。(3%)
   (d) 接續 (c)，請提供從你的 device 到 (c) 中該 DNS server 的 routing path。(4%)

# System Administration

## 1. Capture The Flag (100 points)

### 環境與規則說明

1. VM 下載網址: http://linux15.csie.ntu.edu.tw:10001/
   - 請下載 tar 檔後並取出打包中的檔案（包含三個檔案：虛擬機硬碟、虛擬機資訊、SHA256 校驗和）
   - 使用者：nasa，密碼：nasa2022hw0
   - VMware 使用者可以直接 import ovf 檔來開啟 VM
   - Virtual Box 使用者一樣可以直接 import ovf 檔，但務必將 “作業系統” 設成 “ArchLinux(64-bit)”，且網路設定使用 NAT 的須至 VM 網路設定的進階選項中新增一條 port forwarding 到 VM port 22 的規則
   - Qemu 使用者請先用 qemu−img convert nasahw0−disk1.vmdk −O qcow2 nasahw0.qcow2 轉換硬碟檔型態後便可使用 qemu−system−x86_64 來開啟硬碟檔 “nasahw0.qcow2”
2. 網址中要下載的檔案與解開打包後的 vm 皆有提供 sha 校驗和，建議在下載後比較一下得到檔案的校驗和是否正確以確保檔案的正確性與完整性
3. VM 在開機時就會開啟 ssh server，建議可以使用 ssh 來操作 VM （以及拿到第 1 題的 flag）
4. 本題中的所有題目皆為 CTF 形式，請按照題目說明與線索來操作 VM 並達成要求來獲得 flag
5. 你們有此台 VM 的網路與 root 權限 (sudo 群組)，因此你們擁有任意操作 VM 的權限也可以下載額外的套件來幫助解題（不過現有的套件足以解出所有題目），但請小心使用 root 權限，在不需要時盡量使用原使用者權限
6. 對於你有做出來的題目，請在 report 中寫下得到的 flag 以及得到 flag 所使用的方法與指令
7. 基本上所以題目只要能得到 flag 就好，沒有特別限制作法或指令，但請不要使用太 hacky 的方法（e.g. 逆向工程、在整台 VM 嘗試搜所有 flag 等），否則可能視情況不給分
8. 本題中所有的 flag 格式皆為 NASA{P<id>_<content>} ，其中 <id> 是題號（1-1, 2, ...），而 <content> 如題目沒有特別說明，則是任意可視字元所組成的字串。此外有幾個 flag 的難度提示為 HARD ，代表是屬於比較額外的範圍或是實務中遇到比較難找出解法的題目（但不一定真的比較難做或很麻煩）
9. 建議在操作中隨時 snapshot VM 以免做出不可回復的修改後只能重開一台 VM
10. 題目中所給的大多檢查執行檔請在執行檔所在的資料夾執行，以免因為相對路徑不同而判斷失敗拿不到 flag
11. 在你們拿到 flag 後，請將 flag 使用 nc linux11. csie .ntu.edu.tw 45454 指令上傳作為紀錄與方便批改，同時也可以驗證你們的 flag 的正確性（雖然除了 typo 外應該不太會有錯）。未上傳只寫在 report 的 flag 可能會酌扣一些分數。

### 題目敘述

1. (3 pts) 歡迎來到 NASA CTF 的世界，請在將 VM 打開後使用 SSH 登入進 VM 中，並找出你是誰、你自己的簡介、以及你在哪。(本題有 3 個 flags，每個 1 分)

2. (2 pts) 在 arch linux 中有個重要的人叫 “pacman”，請找出他的介紹。[1]（本題有 1 個 flag，每個 2 分）

3. (2 pts) 在家目錄中有份給新手的包裹，請將它拆開到你的家目錄中，裡面有著後續的題目（本題之後的題目大多不分順序可以任意跳題做）。此外若你不小心弄壞了給定的檔案，你可以將家目錄中的其他檔案刪掉後重新解開本題的包裹。(本題有 1 個 flag，每個 2 分）

4. (3 pts) 我們在 p4/ 中找到了大量散落的檔案們，其中藏著一個正確的 flag ，請在這之中找到它。(本題的 flag 格式為 NASA{P4_<content>}，其中 <content> 只包含大小寫英文數字與底線，且 flag 的總長度是 35)。(本題有 1 個 flag，每個 3 分）

5. (6 pts) 在 p5/ 裡有個從 Windows 送來的壓縮檔，然而 Windows 中沒有 linux 的檔案權限，因此所有的檔案與資料夾權限竟都變成了 777！請你幫忙把權限改回正常的狀態（對於資料夾請設成權限 755，而對於一般檔案請設成 644。(本題有 2 個 flags，每個 3 分，最後一個難度為 HARD）

6. (8 pts) 在 p6/ 中有個人正在像神明禱告但神明卻聽不到。你能幫他把他禱告的話轉達給神明嗎？為了方便理解內容，神明想要分別聽 1. 他想說的話 2. 他所犯的錯 3. 完整的禱告內容。(本題有 4 個 flags，每個 2 分）

7. (3 pts) 快來看！在 p7/ 裡有一本有趣的故事書！在這本書中藏有一個 flag，請把他找出來吧！然而這個偷藏 flag 的人為了避免 flag 輕易洩漏，因此將 flag 做了簡單的加密：他將 flag 中的這些字元 xfP7Xng_paSF@}izoJIMhQbVYyH8KL4m!G01RwA6uNBed{qWrlsC3U5TtDEkv9 依序換成了以下這些字元 qHyUMf6QXlOR18SbjsIk7PWYoC3chpgx94wirt0uenNKm5AdDTvEFZ2BJzGLVa 並在中間塞了很多非英文數字的字元。請找到 flag 後並嘗試解密還原出原本的 flag 吧！不過由於這個故事太長的讀起來太花時間了，他還偷偷告訴了你如果拿掉所有非大小寫英文數字的話，flag 就藏在鬱金香根的附近（tulip roots)。(本題有 1 個 flag，每個 3 分）

8. (4 pts) 有個壞小孩住在 p8/ 中，他的身上藏有 2 個 flag 可是卻不想乖乖告訴你，請嘗試跟他溝通並找出他偷藏的 flag 。(本題有 2 個 flags，每個 2 分）

9. (6 pts) 在 /mnt/p9 中有個拿來備份文件的特殊空間。然而在這些文件中有幾個特別胖的檔案快把空間都佔滿了令我很困擾，你可以幫我找出它們並把它們刪掉釋放出空間嗎？不過要注意請不要動到我的其他檔案們，它們是很重要的。(本題有 3 個 flags，每個 2 分，最後一個難度為 HARD）

10. (6 pts) 有人想在 /mnt/p10 中製造一些大檔案，他想在裡面放置 10 個檔名分別為 0 9 且大小都至少 1MB 的檔案，你能幫他完成這件事嗎？(本題有 3 個 flags 分別是用不同方法完成的，每個 2 分）

11. (9 pts) 我們發現在 p12/ 中有好幾隻怪物，為了避免他們亂跑到處破壞，我們在 p11/ 建造了一個籠子希望可以把他們引進去並擊殺他們。然而這個籠子沒有附使用說明書，請想辦法找出應該要怎麼使用他[2]。此外你發現在這個籠子裡有些缺少的零件，請把它們補齊，你可以通過籠子裡的 root/check 來檢查是否有完成。
此外，在做籠子的檢查時，你意外的發現竟然有人誤闖進了籠子中待在 root/train，並吵著說想要看彩色小火車[3]，你能達成他的願望讓他乖乖離開嗎？(本題有 3 個 flags ，每個 3 分，最後一個難度為 HARD）

12. (8 pts) 在找出第 11 題的籠子用法後，我們要正式把 p12/ 中的這些怪物放進去一一擊殺了，你把他們放到籠子裡並一一打敗他們吧！(本題有 4 個 flags，其中 “monster” 有不同解法的兩個 flag，而 “monster_revenge” 和 “clone_monster” 各有一個 flag，每個 2 分）

[1] 這題所用的指令非常重要，善用它可能可以幫助你完成後面的很多題目
[2] Hint: 不知道你有沒有覺得這個籠子的結構似曾相似？
[3] 彩色小火車可以通過 sl | lolcat 指令來產生

13. (12 pts) 在 p13/ 中有著一群在網路[4]中討論東西的人們，請嘗試從中找出祕密資訊。(本題有 4 個 flags，每個 3 分，最後一個難度為 HARD)（你需要執行他們代表他們上線開始討論，每個人的操作間隔約為 10 秒）

    (a) Alice 和 Bob 是好朋友，他們在網路中討論著一個 flag。

    (b) Carlos 想找人和他做朋友，因此他藏著一個 flag。他每一段時間就會到一個固定的地方找找看有沒有人願意和他做朋友，如果有的話他就會就會慢慢的依序給你 flag 的內容，來希望你能跟他玩久一點。

    (c) Charlie 正在等待他的朋友們上線，而他們之間有偷偷達成一個共識來驗證身份。而 Eve 雖然不是他的朋友中的一員，他卻偷偷找出了他們的驗證協定了，但他需要你幫他建立能跟 Charlie 溝通的網路連線，你能跟他合作找出 Charlie 在哪裡並幫 Eve 建立連線來得到 flag 嗎？

    (d) Faythe 是這個網路平台的管理者，他平常會聽著 port 30002 看有沒有人需要幫忙。今天 Dave 有事想找 Faythe ，但是他卻記錯了 port 跑到 40002 去了，你能幫他導正讓他能順利的找到 Faythe 嗎？

14. (8 pts) p14/ 中有個人正在整理近期收到的信件，並將信件們全部存成一個檔案 “mails” ，然而在處理完後，他發現了幾個問題：

    - 他希望把信件中 “Received: by” 欄位的 “linux1.” 部份去掉，只保留 “csie.ntu.edu.tw”
    - 他每封信件的 header 不小心漏複製了兩條資料：“MIME-Version: 1.0” 和 “Content-Type: text/plain; charset=ascii”，因此希望把這兩條加到每封信 header 的最後

    一封信修改前與期望修改後的範例如 sample_original 和 sample_correct 檔案內容，請你幫幫他把所有的信都照著修改成應有的樣子。值得注意的是，他的所有信件都長的非常相似，收計件地址與標題內容雖然略有不同但全部都有一樣的長度，所有信也都有完全相同的格式[5]。除此之外，他在整理信件時還發現了有另一封信件中有一個附加檔案 flag.jpg 在裡面，由於信中沒有任何說明與介紹，擁有資訊安全素養的他不敢隨意打開來路不明的檔案，因此他將檔案交給了很電的您，請幫他看看這個附加檔案到底是什麼東西。
    在處理完信件後，他準備要來一一回信了，然而就在他寫完一封信正要回復時，突然發現機器上的郵件伺服器（postfix）竟然沒有啟動服務，請將他把服務開起來，並且為了避免之後再遇到相同的問題，請順便將這個服務設定成開機會自動啟動。你可以通過 p14/check_postfix 來檢查是否有完成。
    最後，雖然服務升起來了，他卻在寄送時又遇到了另一個問題：郵件伺服器竟然警告他的服務的 TLS 憑證簽署單位不認識無法驗證，有可能是自簽憑證有危險性。然而在看了這段訊息後，對 TLS 協定沒有任何概念的他不知道該怎麼辦，你能幫他看看憑證的內容有沒有什麼問題嗎？[6][7]（本題有 4 個 flags，每個 2 分，最後一個難度為 HARD）

15. (20 pts) CSIE 最近正在舉辦 “SA 知識小問答，百萬獎金等你拿” 活動，只要成功答對所有的題目就能立刻搖身一變成為 CSIE 百萬富翁！得知了這個消息的你還不快來參加這個活動挑戰看看嗎？不過當然的，獎品這麼好的活動當然也會有嚴格的檢查以免有人偷作弊來獲勝。因此，請在 report 中**簡單**寫下你所答對的問題的解釋[8]，否則主辦方將會懷疑你作弊並沒收你的獎品們。(本題有 1 個 flag，每個 20 分)

[4]為了討論內容的隱私性，他們只在 VM 的 localhost 網域中討論以避免資料外洩，因此 VM 沒有連外網也可以做本題
[5]因此，或許你可以考慮把所有信件切開再對每封信做相同的修改可能會比較容易
[6]本題與服務內容無關，因此你不需要去看服務的設定
[7]Hint: 成功連上 TLS 服務後交換憑證階段自然就會有憑證內容了
[8]盡量以簡單一句話或一行指令等方式說明即可不用很詳細