# Homework #5

Due Time: 2022/05/15 (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 name your PDF "`{your_student_id}.pdf`", and submit it through NTU COOL.

### Grading

- NA accounts for 50 points while SA accounts for 50 points. The final score is the sum between 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 = NA score + SA score + tidiness score.

# DNS & DHCP

## 1. Build DNS and DHCP server(30 points)

本題希望同學們自己練習架設 DNS & DHCP server。請同學們事先準備一個 CentOS 8 的 VM 作為 DNS & DHCP server，以及一個 Ubuntu server 的 VM 作為 client，再根據以下要求完成此題。除了如何開這兩個 VM 外，同學們需要將自己架設的過程一步一步完整解釋清楚 (或許搭配一些截圖來進行解釋)，方能拿到滿分。

1. Server VM:
   (a) IP 固定為 192.168.5.254
   (b) server 有兩個 interface，一個對內 (向內提供 DNS 和 DHCP 服務) 一個對外。
   (c) DNS settings:
      i. 新增一個 zone：[your_student_ID].com
      ii. 新增 A record：www.[your_student_ID].com 指向 1.2.3.4
      iii. 新增 PTR record：使 1.2.3.4 可以反查回 www.[your_student_ID].com
      iv. 當 client 查詢非自己負責的 zone 時，要能再去向其他 DNS recursive query 直到查詢到結果
   (d) DHCP settings:
      i. subnet：192.168.5.0/24
      ii. range: 192.168.5.100-192.168.5.200
      iii. dns server: 192.168.5.254
      iv. route/gateway: 192.168.5.254
2. Client VM:
   (a) 透過 DHCP server 拿到 IP (18 points)
   (b) dig www.[your_student_ID].com, google.com, 跟 dig -x 1.2.3.4，並截圖 (各 4 points, 共 12 points)

## 2. Short Answers (20 points)

1. 請簡單說明什麼是 DNS-over-HTTPS？並列出 DNS-over-HTTPS 的一個優點和一個缺點。(4 points)
2. 請簡單描述 amplification attack？(4 points)
3. 什麼是 DNS cache poisoning attack，並提出一個防禦的方法。(6 points)
4. 什麼是 Kaminsky attack，請說明為何這是一種比 DNS cache poisoning attack 更難防禦的攻擊。(6 points)

# NFS & Fix VM

## Fix VM (20%)

- 對於 Root Password 及 Cannot SSH? 兩題，請下載 VM 檔案:
  - CSIE Workstation: http://linux7.csie.ntu.edu.tw:17718
- Account:
  - Username : `nasa`
  - Password : `nasa2022`
- 建議使用工作站的 QEMU 來完成本次作業
  - 首先在工作站上使用 `curl http://linux7.csie.ntu.edu.tw:17718/init.sh | bash`
  - 前述步驟將會把所有檔案下載到/tmp2/[YOUR-STUDENT-ID]/NASAHW5 的目錄下
  - 建議使用 tmux 或是 screen，並執行 `bash /tmp2/[YOUR-STUDENT-ID]/NASAHW5/run.sh [YOUR-SSH-PORT-NUM] [YOUR-VNC-PORT-NUM]`
  - 使用 VNC 連線到 `host:[5900+YOUR-VNC-PORT-NUM]`

1. **Root Password (10%)**

   在成功使用你的使用者帳號登入 VM 之後，你發現你沒有用 sudo 拿到 root 權限的機會 (因為你不是 sudoer)。但是，修了 NASA 的你卻發現這台 VM 裡有些檔案的權限似乎有點奇怪... 有一些本來不應該有 SUID 的檔案竟然有 SUID，或許你可以從中著手，想辦法利用它找到 root 的密碼。並使用找出的密碼登入 root 帳號並截圖。

   - Hint:
     - 找出 Vim Swap File，並從中得到 root 的密碼的 hash
     - 獲得 Hash 後，可以利用 hashcat,john the ripper 等工具破解 root 密碼

2. **Cannot SSH? (10%)**

   你一直以來都習慣用 SSH 連入 VM，但是今天你卻碰到這台沒辦法使用 ssh 登入的 VM(編按：也就是輸入正確密碼之後還是無法登入)，讓你覺得十分不舒服。因此請想辦法解決這個問題，並附上解決此問題的所有步驟。

   - SSH 連入方式 (On CSIE Workstations):
     - `ssh nasa@localhost -p [YOUR-SSH-PORT-NUM]`

## PXE boot using NFS (30%)

- 這題請從下面的 URL 下載 host.qcow2 作為 PXE server(你應該使用 qemu).
  - CSIE Workstation: http://linux7.csie.ntu.edu.tw:17718
- Account
  - Username: root
  - Password: nasa2022

1. 請簡述一下什麼是 PXE boot，並說明它的使用情境以及優點 (8%)
2. 建立 PXE server 並用於開機：(12%)
   - 請用 host.qcow2 建立 VM
   - 下載最新的 Arch Linux iso 在 VM 上 (應該是 2022.04.05 的那個)
   - 用下載好的 iso 在 VM 上面架設一個 Arch Linux 的 PXE server
   - PXE server 有很多不同方法來傳送資料，請你使用 NFS
   - 自行建立一個 clinet machine 使其能用你的 PXE server PXE 開機。
   - 請寫下做到以上幾步驟所需的詳細指令並在 client 開機後截一張 client 的圖
3. 安裝 Arch Linux 於 client 上：(10%)
   - 請在剛剛用 PXE boot 的 client 上安裝 Arch Linux
   - 請在安裝完畢後新增一個 User，username 是你的學號，password 任意
   - 請寫下做到以上幾步驟所需的詳細指令並在 client 開機後截一張你成功用新創 user 登入的圖