Homework #8

Due Time: 2025/04/27 (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 zip all the files, name it "`{your_student_id}.zip`", and submit it through NTU COOL.

Grading

- The total score for the correctness and completeness of your answer is 100 points.
- 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 = correctness score + tidiness score.

LDAP

LDAP (Lightweight Directory Access Protocol)[1]，作爲一個輕量的目錄服務協定能有效幫助我們管理眾多的使用者帳號。你知道嗎？我們平日系內使用的工作站、CSIE Wi-Fi、以及 CSIE Mail 等服務皆都需要透過 LDAP 來進行驗證及獲取使用者的相關資訊。接下來在這份作業中，你將會學習使用 LDAP 來管理你的使用者資訊。

共通的規定

本次作業的作答內容請統一放在一個以學號為名的目錄中，並包含報告以及作答會需要的 ldif 檔案，壓縮成 `[你的學號].zip` 後上傳至 NTU Cool，解壓縮後的格式範例如下：

```
- b13902000
    - report.pdf
    - ldif
        - base.ldif
        - user.ldif
        - ...
    - ...
```

- 在報告中，請同學詳細列出回答題目的完整過程（例如輸入的指令），以及你所使用的參考資料。我們也鼓勵你寫出你遇到的問題，及如何解決該問題。所有的小題都會視作答給予部分分數，所以即使你沒有完成最後的要求，也請同學儘量附上你的進度。
- 由於接下來的題目會涉及較多的 LDIF 檔案，同學可以選擇統一印在報告內，或者將檔案放在名為 ldif 資料夾內（如同上面的範例），在報告中提到檔名即可。
- 在完成 TLS/SSL 小題後，請同學使用 StartTLS 或者 SSL 的方式與 LDAP 連線。

[1] https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

I. 前置作業

請在 `nasaws*` 執行 `/tmp2/hw8/run-vm.sh [你的學號]`，可以看到以下的結果，這個指令會在 `/tmp2/[你的學號]/hw8` 中生成此題所需要的虛擬機環境。完成後，請 cd 至該資料夾。

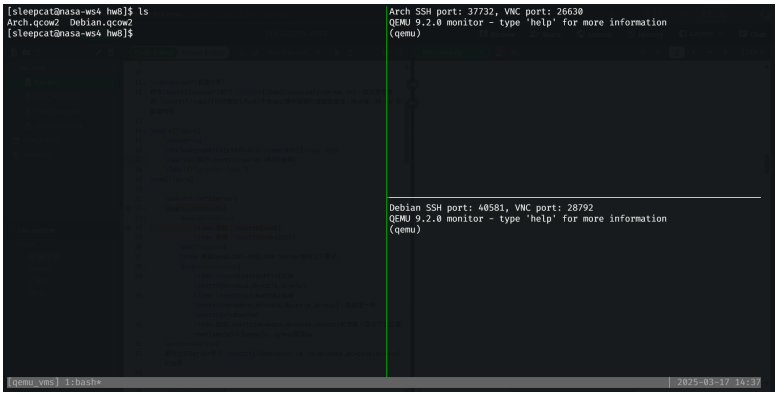

Figure 1: 執行 `run-vm.sh` 後的結果

可以看到右邊有兩台用 QEMU 打開的 VM，同學可以使用 `SSH port` 或 `VNC port` 連線至 VM。在接下來的題目中，我們會使用 Debian 當作我們的 LDAP Server、Arch 當作我們的工作站 (LDAP Client)。你可以使用以下帳號來登入兩台 VM:

- 帳號：`root`
- 密碼：`nasa2025`

注意：每次執行 `run-vm.sh` 可能會產生不同的 port number!

1. Server (5 points)

架設 OpenLDAP，你的 LDAP Server 需有以下要求:

1. `olcSuffix` 設 `dc=nasa,dc=csie,dc=ntu`
2. `olcRootDN` 設 `cn=admin,dc=nasa,dc=csie,dc=ntu`，並設定一組 `olcRootPW`
3. 設定 `dc=nasa,dc=csie,dc=ntu` 的節點，並在下面設 root(admin) 以及 people, group 兩個 ou

請附上在 Server 執行 `ldapsearch -x -b dc=nasa,dc=csie,dc=ntu` 的結果。

2. Client (5 points)

安裝 LDAP 環境，附上在 Client 透過 `ldapsearch` 查詢 Server 上 `dc=nasa,dc=csie,dc=ntu` 的結果

II. Task

1. **LDAPS (LDAP over SSL) (30 points)**
   - 請為你的 LDAP Server 啓用 TLS 服務
   - 附上在 Server 成功執行 `ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu` 的結果
   - 附上在 Server 成功執行 `ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu` 的結果
   - 請調整設定，讓 Client 只能用 StartTLS 或 SSL 連線到 Server。
   - 附上在 Client 上成功使用 `ldaps` 查詢 Server 上 `dc=nasa,dc=csie,dc=ntu` 的結果
   - 附上在 Client 上嘗試用未加密的方法向 Server 連線，並截圖失敗的結果。

2. **SSSD (20 points)**

   在 Client 上安裝 SSSD[2](System Security Services Daemon, 系統安全服務背景服務程式)，使得 LDAP 上使用者可以使用 LDAP server 上的密碼透過 SSH 登入，並在第一次登入時自動新增家目錄。接下來，請完成下列步驟：
   - 在 LDAP 新增兩個群組 ta 及 student，並設置 ta group 的使用者有 sudo 的權限，而 student group 的使用者則沒有。
   - 添加兩個新的使用者，一個在 ta 群組，一個在 student 群組。
   - 最後附上兩位使用者透過 SSH 初次登入的截圖（包含自動新增家目錄的提示），以及各自展示使用 sudo 的結果（e.g., `sudo echo Hello World`）。

3. **ACL (Access Control Lists) (20 points)**

   接下來你要爲你的工作站使用者設置權限管控，請於 LDAP Server 上設置以下訪問控制權限：

   (a) 使用者不可以修改其他使用者的資料，如其他使用者的 `userPassword`。
   (b) 使用者只可以更改除了 cn、uid、gid 和家目錄以外的資訊，如 `loginShell`。
   (c) 使用者（包含 anonymous）可以存取其他使用者密碼以外的資訊。

4. **LDAP Schema Extension (20 points)**

   在 LDAP 中，objectClass 定義了一個 entry 可以擁有的屬性（Attributes）。例如：
   - organizationalUnit 定義了 entry 的 `ou` 屬性。
   - organizationalRole 定義了 entry 的 `cn` 屬性。

   現在，請你透過 Schema Extension，客製化不同的 ObjectClass 和屬性。在開始之前，建議可以先把目前的狀態做備份，設定錯誤可能會造成不可逆的結果。接著請達成以下需求:

   (a) 定義兩個新的屬性: `studentName`、`examGroupID`
   (b) 定義一個新的 objectClass: `StudentInformation`
   (c) 在 `StudentInformation` 底下新增兩個屬性:`studentName`、`examGroupID`。
   其中，請設定 `studentName` 和 `examGroupID` 為必填欄位。
   (d) 新增一個 group 在 student 使用者，此使用者必須有 `StudentInformation` 的 objectClass，並指派 `studentName` 和 `examGroupID` 兩個屬性

   請附上使用 LDAP 查詢此使用者的結果。

[2] https://en.wikipedia.org/wiki/System_Security_Services_Daemon