Homework #8

Due Time: 2025/11/11 (Tue.) 23:59
Contact TAs: `vegetable@csie.ntu.edu.tw / 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 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]是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。事實上，我們平日系上的 CSIE 工作站、CSIE Wi-Fi、CSIE Mail 等服務，都需要透過 LDAP 進行驗證或是取得使用者的資訊。接下來在這份作業中，你將會學習使用 LDAP 管理使用者資訊。

共通規定

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，其中包含報告的 PDF 檔以及各題答案的 LDIF 檔，並將此目錄壓縮成 `[你的學號].zip` 後上傳至 NTU COOL。解壓縮後的格式範例如下：

```
b14902000
|- report.pdf
|- ldif
   |- base.ldif
   |- user.ldif
   |- ...
```

- 在報告中，請詳細列出作答的完整過程，例如執行的指令、使用到的 LDIF 檔案、以及閱讀的參考資料。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 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，往後的題目請一律使用 StartTLS 或者 LADPS（LDAP over SSL）的方式與伺服器連線。

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

前置作業

本次作業的檔案位於 `nasaws{1,2,3}` 的 `/tmp2/hw8`，內容如下：

```
/tmp2/hw8
|-- client.qcow2
|-- run_vm
|-- server.qcow2
```

- `server.qcow2`：一台全新安裝好的 Debian 13 VM，作為 LDAP server，對內 IP 位址為 `192.168.8.1/24`。
- `client.qcow2`：一台全新安裝好的 Arch Linux VM，作為 LDAP client，對內 IP 位址為 `192.168.8.2/24`。
- `run_vm`：執行 VM 的腳本，會創建一個新的 tmux session，並將 window 分割為左右兩半，分別執行 server 與 client 的 VM。

請將 `/tmp2/hw8` 複製到自己習慣的工作目錄，並修改 `run_vm` 中的 `SERVER_SSH_PORT` 與 `CLIENT_SSH_PORT` 變數，才可用 SSH 連進 VM。出於資安考量，VM 的 SSH 只接受來自 host 的連線，因此連線方式為**在開 VM 的 nasaws 上執行** `ssh -p SSH_PORT root@localhost`。
兩台 VM 的帳密皆為：

- 帳號：`root`
- 密碼：`nasa2025`

Tasks

1. Server setup (5 points)

   架設 OpenLDAP 伺服器，並滿足以下設定：

   - `olcSuffix` 為 `dc=nasa,dc=csie,dc=ntu`。
   - `olcRootDN` 為 `cn=admin,dc=nasa,dc=csie,dc=ntu`，並設定一組 `olcRootPW`。
   - 新增節點 `dc=nasa,dc=csie,dc=ntu`，並在其之下新增 people、group 兩個 organizational unit。

   請附上在 server 執行 `ldapsearch -x -H ldapi:/// -b dc=nasa,dc=csie,dc=ntu` 的結果。

2. Client setup (5 points)

   - 在 client 上安裝 LDAP 客戶端相關套件，並調整相關設定，使得執行 `ldapsearch -x` 即可正確查詢到 server 上 `dc=nasa,dc=csie,dc=ntu` 底下的所有目錄資訊。
   - 附上在 client 上執行 `ldapsearch -x` 的結果。

3. LDAPS (LDAP over SSL) (30 points)
   (a) 調整設定，為 LDAP server 啟用 SSL/TLS。
   (b) 附上在 server 成功執行 `ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu` 的結果。
   (c) 附上在 server 成功執行 `ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu` 的結果。
   (d) 調整設定，讓 client 只能用 StartTLS 或 LDAPS 連線到 server。
   (e) 附上在 client 上成功使用 LDAPS 查詢 server 上 `dc=nasa,dc=csie,dc=ntu` 的結果。
   (f) 附上在 client 上嘗試用未加密的方法向 server 連線並失敗的結果。

4. SSSD and Sudo (20 points)
   (a) 在 client 上安裝 SSSD[2]，使得 LDAP 上的使用者可以使用儲存於 LDAP 的密碼透過 SSH 登入，並在第一次登入時自動新增家目錄。
   (b) 在 LDAP 新增兩個群組 ta 及 student，並設置 ta 群組的使用者有 sudo 的權限，而 student 群組的使用者則沒有。
   (c) 添加兩個新的使用者，一個在 ta 群組，一個在 student 群組。
   (d) 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，以及各自使用 sudo 的結果（如 `sudo echo Hello World`）。

5. ACL (Access Control Lists) (20 points)
   請於 LDAP server 上設定以下訪問控制權限：
   (a) 使用者不得修改其他使用者的任何屬性。
   (b) 使用者可以修改自己的任意屬性，除了 `cn`、`uid`、`uidNumber`、`gidNumber`、`homeDirectory` 以外，如 `loginShell`、`userPassword` 等。
   (c) 使用者（包含 anonymous）可以讀取其他使用者的任意屬性，除了 `userPassword` 以外。

   各子題請都附上足以證明 ACL 符合預期的 `ldapsearch` 或 `ldapmodify` 指令結果。(b) 中不得修改的屬性舉其一為例即可。

6. LDAP Schema Extension (20 points)
   開始寫這題之前，建議可備份當前的 VM 或資料庫狀態，因為設定錯誤可能會造成不可逆的結果。

   在 LDAP 中，objectClass 定義了一個 entry 可以擁有的屬性（attributes），例如 organizationalUnit 定義了 `ou` 屬性，inetOrgPerson 定義了 `givenName`、`mail` 等屬性。事實上，我們也可以自定義一些 objectClass 與屬性，以符合特定應用的需求。

   現在我們來設計一個代表台大學生的 objectClass：
   (a) 定義三個新的屬性：`studentEntryMethod`(入學管道)、`studentAdvisor`(導師)、`studentClub`(社團)。
   (b) 定義一個新的 objectClass：`ntuStudent`。
   (c) 在 `ntuStudent` 中新增 (a) 定義的三個屬性，並將 `studentEntryMethod` 和 `studentAdvisor` 設定為必要，`studentClub` 設定為非必要。
   (d) 新增一個 student 群組的使用者，此使用者必須有 `ntuStudent` 的 objectClass，以及至少有 `studentEntryMethod` 和 `studentAdvisor` 這兩個屬性。
   (e) 附上使用 `ldapsearch` 查詢此使用者的結果。

[2]System Security Services Daemon, 系統安全服務背景服務程式