Homework #8 - LDAP

Due Time: 2024/04/28 (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.

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 script, ldif... 等檔案，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：

```
- b12902000
    - report.pdf
    - ldif
        - base.ldif
        - user.ldif
        - ...
    - scripts
        - add_user.py
        - ...
    - ...
```

- 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

VM Setup

請在工作站上執行 `/tmp2/aoaaceai/publish/setup_ldap.sh`。這個指令會在 `/tmp2/[你的學號]/ldap` 中生成此題所需要的虛擬機環境。完成後，請 `cd` 至該資料夾，並執行裡面的 `run.sh`。
接下來你應該會看到如下的畫面：

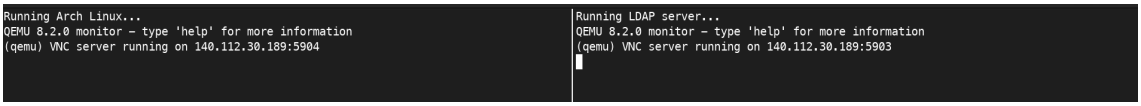

Figure 1: 執行 `run.sh` 後的結果

請在兩個子視窗中都執行 `change vnc password` 來設定連線密碼。
注意：每次執行 `run.sh` 都必須重設密碼，否則無法連線！

接下來，請使用任意一種 VNC client，分別連線至 `run.sh` 提及的兩個 IP 及 port。輸入先前的密碼後，你會看到 Arch Linux 以及 Debian 的登入畫面。或者，你也可以在執行 `run.sh` 之前，先執行 `export ARCH_SSH_PORT=${PORT_NUM}` 以及 `export DEBIAN_SSH_PORT=${PORT_NUM}`，如此一來，執行完 `run.sh` 後就可以以 `ssh` 來存取機器了。在接下來的題目中，我們會利用這台 Debian VM 來作為我們的 LDAP Server、而另外一台 Arch Linux 作為我們的工作站。
你可以使用以下帳號來登入這兩台機器，並開始進行後續的題目！

- 帳號：`root`
- 密碼：`nasa2024`

Tasks

1. Server Setup (10 points)

(a) 請依照下列的要求，架設一個 LDAP Server：

- `olcSuffix` 設爲 `dc=nasa,dc=csie,dc=ntu`
- `olcRootDN` 設爲 `cn=admin,dc=nasa,dc=csie,dc=ntu`，並設定一組 `olcRootPW`
- 設定 `dc=nasa,dc=csie,dc=ntu` 的節點，並在下面設置 root(admin) 以及 people, group 兩個 ou

新

新

請附上 `ldapsearch` 所有 `dc=nasa,dc=csie,dc=ntu` 下資訊的結果。

(b) 請替 LDAP Server 增加安全性 – TLS/SSL:

- 請爲你的 LDAP Server 啓用 TLS 及 LDAPS (LDAP over SSL)。
- 附上成功執行 `ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu` 的結果。
- 附上成功執行 `ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu` 的結果。

2. **Client Setup (20 points)**

   (a) 在你的工作站安裝 LDAP client 所需的工具，並透過 `ldapsearch` 查詢 server 上 `dc=nasa,dc=csie,dc=ntu` 下資訊的結果。

   (b) 請調整設定，讓 client 只能用 StartTLS 或 SSL 連線到 server。完成後，請在 client 上嘗試用未加密的方法向 server 連線，並截圖失敗的結果。

   (c) 在工作站上安裝 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。

   (d) 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. **Access Control Lists (5 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家目錄、UID、GID 以外的資訊，如 `loginShell`。

   (c) 使用者（包含 anonymous）可以存取其他使用者除了密碼以外的資訊。

4. **Scripts (15 points)**[3]

   接下來我們希望可以利用一些 Scripts 來讓我們的 LDAP Server 更加易於管理，請使用 Python 3.11.2 (就是直接 `apt install` 會得到的版本) 或是 Shell Script (Bash or Zsh) 在 LDAP Server 寫幾份腳本來提供以下的功能：

   (a) `add_user`：admin 執行該腳本後，會輸入兩行，第一行為使用者名稱，第二行則為密碼，請根據使用者名稱以及密碼在 LDAP Server 新增使用者，並依據使用者名稱來設定其家目錄的位置。
   其中，保證新增的使用者名稱滿足 `[0-9a-z]{1,10}`，密碼則滿足 `\w{1,10}`，且不會重複新增相同的使用者名稱。

   (b) `del_user`：admin 執行該腳本後，會輸入一行，代表使用者名稱，請根據使用者名稱在 LDAP Server 刪除使用者。
   其中，保證刪除的使用者名稱滿足 `[0-9a-z]{1,10}`，且使用者必定原本存在。

   你可以假設可以存取以及執行此腳本的都是管理員身份的使用者。若你有其他相關假設，請清楚寫在 report 當中。

   hint1: OpenLDAP 不會自動產生新的 `uidNumber`，必須由我們指定一個沒被用過的 `uidNumber`，其中一種（效率不高）的作法是選擇所有 `uidNumber` 的最大值再加一。
   hint2: 可以參考下面的連結，裡面有一些關於 python-ldap 的範例與說明。

[2] https://en.wikipedia.org/wiki/System_Security_Services_Daemon
[3] https://www.python-ldap.org/en/python-ldap-3.4.3/index.html