Homework #4

Due Time: 2023/05/07 (Sun.) 22:00
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, including one PDF, the security folder and the ldap folder. Name the zip file "`{your_student_id}.zip`", and submit it through NTU COOL. The zip file should not contain any other files, and the directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- ldap/
+---- {ldif file}
+---- ...
```

Grading

- DNS accounts for 50 points while LDAP 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)

你知道你幾乎每天都會用到 DNS 和 DHCP Service 嗎？本題希望同學們練習架設 DNS & DHCP server。請同學們使用一個 Debian 11 的 VM 作為 DNS & DHCP server，以及一個 Ubuntu 20 的 VM 作為 client，再根據以下要求完成此題。請列出架設 VM 的所有過程及解釋（可搭配截圖說明），方能拿到滿分。

1. Server VM:
   (a) IP 固定為 192.168.5.1
   (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: 192.168.5.1
      iv. route/gateway: 192.168.5.1
2. Client VM:
   (a) 透過 DHCP server 拿到 IP。請附上 `ip -a` 的截圖 (18 points)
   (b) `dig www.[your\_student\_ID].com`、`google.com`，跟 `dig -x 1.2.3.4`，每個都要附上有 & 無指定 192.168.5.1 為 server 的截圖 (各 4 points，共 12 points)

2. Short Answers (20 points)

1. 先前上課同學們已使用過 Docker (但還是附個工作站安裝連結)，這題請同學下載資料夾，在 `nasahw4/` 中執行 `./build.sh` 建立一個叫做 dns-server container，進入後執行 `./run-dnsperf` 觀察輸出並回答下列問題。
   - dnsperf 這個工具可以用來測試 DNS 的效能，`./run-dnsperf` 的輸出為「對這台**剛建好**的 DNS server **連續**執行指令 `dnsperf -s 127.0.0.1 -d queryfile -l 10 -c 1 -Q 100` 三次」後，每次的結果。針對 Average Latency 欄位，描述你觀察到的現象，並推測造成其變化的可能原因。(3 points)
   - 承上，說明此機制在 DNS 架構中可能受到的攻擊 (2 points) 及防禦方法 (2 points)。
2. 請解釋何謂 DNS propagation time。(2 points) 並說明長的 TTL 跟短的 TTL 對 DNS server 各有什麼優缺點 (2 points)。
3. 請簡單說明什麼是 DNS-over-HTTPS？(2 points) 並列出 DNS-over-HTTPS 的一個優點和一個缺點。(2 points)
4. 我們知道 DHCP 在 transportation layer 是使用 UDP 進行傳輸，請問在配置時是否能把 DHCP server 和 client 放在不同的 subnet？請說明原因。如果可以，請提出具體的實踐方法。(3 points)

5. 什麼是 DHCP Snooping？它可以用來預防什麼攻擊？(2 points)

LDAP

LDAP (Lightweight Directory Access Protocol)[1]，作爲一個輕量的目綠服務協定能有效幫助我們管理衆多的使用者賬號。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

- 在接下來的每項問題中，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，然後將資料夾留空，或者將檔案放在 ldif 資料夾內，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。

Basic Setup (15 points)

1. Prequisites:
   - 請安裝一臺 Debian 11 的虛擬機器，並在上面架設 OpenLDAP[2]
     - vcpus: 2
     - memory: 1GB or 2GB or more
     - disk: 10G or more
     - network: bridged
2. 你的 LDAP server 請依照下列的要求：
   - `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

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

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

Client (20 points)

1. Prerequisites:
   - 請安裝一臺 Arch Linux 的虛擬機器，作爲你的工作站
     - vcpus: 2
     - memory: 1GB or 2GB or more
     - disk: 10G or more
     - network: bridged
2. 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。
3. 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。
4. 在工作站上安裝 SSSD[3](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。
5. 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`）。

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：

1. 使用者不可以修改其他使用者的資料，如其他使用者的 `userPassword`。
2. 使用者只可以更改除了家目錄、UID、GID 以外的資訊，如 `loginShell`。
3. 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. 僅允許 LDAP Server 及 client 的 IP 端的連線。

Backup && Restoration && Replication (10 points)

1. 請如 Basic Setup Prerequisites 再架設一臺 Debian 11 的虛擬機器，一樣使用 bridged network, 並且安裝 LDAP server 相關套件。
2. 接下來，請備份你原本的 LDAP server 中的 configuration 及 database 並搬到新的 server。注意請不要一筆一筆地搬動資料。
3. 最後當兩臺 server 的資料一致之後，將兩臺 server 設爲同步狀態，當一臺 server 對 LDAP 操作時都會反映到另一臺 server 上。
4. 完成後，請在其中一台機器上更改某些資料，並在另一台機器用 `ldapsearch` 檢查更改是否成功。

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