Network Administration and System Administration

Final Examination

Time: 2024/06/03 09:10 - 12:10

Instructions and Announcements

- 考試時間共三小時，三人一組考試。分組連結及簽到結果。
- 考試期間禁止使用手機、電話、任何通訊軟體等與同組成員外任何人聯繫，也禁止組與組之間**一切討論與合作**，如被發現視為作弊行為，**期末考 0 分**，並依校規懲處。
- 考試期間禁止使用生成式模型 (包含但不限於 ChatGPT, Gemini, LLaMA, Copilot 等等) 直接作答或間接輔助作答，如被發現同樣視為作弊行為，**期末考 0 分**，並依校規懲處。
- 作答過程中請自行斟酌備份，避免電腦發生意外，損失過多進度，可考慮準備隨身碟或雲端空間備份進度。
- 為避免發生重大意外，請自行注意 VM 用量，同時開啟過多 VM 可能導致電腦當機，我們恕不負責。
- 每組會領到一組筆電 (包含筆電、滑鼠、充電線)，並且在考試結束後交回。
- 第九題的 Task4 會需要實體操作 switch，每組會有 20 分鐘時間可以操作。請確定你有完成第九題的 Task1 之後填寫這個表單預約時間，並在這裡確認你是不是有預約成功。
- 線上考試的 announcement 將會更新在 https://docs.google.com/document/d/1waY5nZVeIoNgj02V2MVT4CSltrqENXP_fzWsho54gkw/edit?usp=sharing。
- 題目檔案請至 雲端硬碟下載 (考試開始後公開) 。也可以在考試開始前先下載加密過的壓縮檔 (ws2:/tmp2/NASA-Final-Exam)，解壓縮密碼將會在考試開始後公佈。
- 完成題目時請至 Submission Form 上傳作答內容，每組每個 subtask **最多上傳 3 次**。
- 計分板連結 Scoreboard。
- 各題後面黑色星號數目代表我們估計的難度。請參考，可用來決定解題順序。
- 題目可能難免有疏誤之處。若發現有解不開題目、題敘不清的狀況，請盡快跟助教或老師反應，或斟酌時間先解別的題目。
- 滿分為 100 pts。

1 Red Team Revenge ★★ ~ ★★★ (13 points)

Resources

- Visit http://ws1.csie.ntu.edu.tw:51190
- Backup site: http://ws6.csie.ntu.edu.tw:51190

Description

你在黑市遊蕩的時候，某個駭客突然拍了你的肩膀並給了你已經存在已久的網路服務的網址，同時也附上了該網路服務**更新前**的程式碼。他告訴你若要成為他們的夥伴，你必須試著找尋並利用這個網路服務的漏洞，完成下面所描述的工作。

Tasks

1. Login Again ★★ (4 points)

   存取上面的網址可看到一個登入系統。經過了 Lab 以及作業的洗禮，相信你明白 SOP 是什麼吧？

   - 請登入 `admin` 帳號，並且取得 `flag1`
   - Note: `home.php` 中的 `flag` 不是最新的 flag，你仍需要登入才能得到真正的 `flag1`
   - Hint 1: 資料庫的表格 (table) 名稱: `users`
   - Hint 2: 資料庫的欄位 (column) 名稱: `id, username, password`

2. Under Construction...? ★★★ (5 points)

   登入後你發現網頁卻顯示正在維修中... 身為資安高手的你依然嗅到有漏洞的味道。

   - 請讀取 `/flag` 得到 `flag2`
   - Hint 1: 該網路服務使用的 Web Server 是什麼呢？
   - Hint 2: 登入後的主頁寫了什麼？
   - Hint 3: 照片可愛吧！
   - Hint 4: Alias LFI Misconfiguration

3. Secret Service ★★ (4 points)

   當你正在努力解題目時，突然一通電話打來，並說了其實有一個神秘的網路服務正在運行，但卻不告訴你該 `endpoint` [1]是什麼。

   - 請讀取在 Server 上**存在於某個 directory** 底下的 `final_flag`，得到 `flag3`
   - Note: `secret.php` 中的 `endpoint` 不是最新的 `endpoint`，你仍需要透過某種方式才能得知正確的 `endpoint` 並存取該神秘的服務
   - Hint 1: 該網路服務使用的 Web Server 是什麼呢？
   - Hint 2: 該 Web Server 的預設設定檔位置或許有幫助。

Submission

- 找助教 demo。

[1]不知道 Endpoint 是什麼意思的話，可以參閱這裡。基本上是一個可以用 HTTP 或 HTTPS 存取的 URL。

2 Web Server ~~(Docker revenge)~~ ★ ~ ★★★ (16 points)

Resources

1. vm.qcow2
   - user name: user
   - user password: nasa2024
   - root password: nasa2024
   - 虛擬機是用以下指令安裝 Debian-12.5.0。
     (a) 'qemu-img create -f qcow2 vm.qcow2 8G'
     (b) 'qemu-system-x86_64 -m 4G –enable-kvm –hda vm.qcow2 -cdrom debian-12.5.0-amd64-netinst.iso'
     (c) 已開啟的重要服務包含，standard system utilities, GNOME, SSH server。
   - 欲在工作站上以無 GUI 方式開啟此虛擬機可用以下指令，'qemu-system-x86_64 -m 4G –enable-kvm –hda vm.qcow2 -net nic -net user,hostfwd=tcp::[port]-:22 -nographic'。並用 'ssh user@127.0.0.1 -p [port]' 連線至虛擬機中。注意開啟虛擬機後需等待作業系統開啟 sshd，故若依開啟後未能連上，可等一下子再重新連線，
   - 欲以有 GUI 方式開啟此虛擬機可用以下指令，'qemu-system-x86_64 -m 4G –enable-kvm –hda vm.qcow2'。可利用 ssh X11 forwarding 的功能將虛擬機的 GUI 從工作站發送至本地，亦可直接在本地端執行指令。

Tasks

以下四小題為同一題組。

1. Basic setups (2 points)
   - 開啟並登入虛擬機，vm.qcow2，中，並依照 Docker 官網 的指示，利用 apt 安裝 Docker。
   - 利用 docker 指令開啟一個運行 Nginx 1.25.5 的容器，請將容器的 80 埠映射到虛擬機的 8080 埠
   - 可利用 curl http://localhost:8080 檢查服務是否開啟。
2. Access log (2 points)
   - 為了方便接下來的設定 nginx 的方便，並在唯讀的模式下，掛載虛擬機中的 /home/user/Documents/nginx.conf 到 /etc/nginx/nginx.conf 中。
   - 為了紀錄 web server 的連線狀況，請將 access log 建立並保存在 container 的 /var/log/nginx/new-access.log 中。
   - 同時為了在本機中也可以看到這份紀錄以及持久化的儲存紀錄，將虛擬機中的 /home/user/Documents/log/ 掛載到容器的 /var/log/nginx/。
   - 可利用 curl http://localhost:8080 存取網頁內容，並檢查 /home/user/Documents/log/new-access.log 的內容。
3. Directory and redirection (3 points)
   - 接續上一小題，設定 Nginx 符合下列要求。
   - 在虛擬機中建立一個 HTML 檔 index.html，並掛載到容器的 /var/www/index.html。並設定 Nginx server，當連上 http:/localhost:8080/index.html 時，需要回傳 /var/www/index.html 的內容。

- 可用 curl http://localhost:8080/index.html 檢查期內容是否為 index.html。
- 除此之外，當連上 http://localhost:8080/ntu-csie/[path] 時，會被 redirect 到 https://www.csie.ntu.edu
  當中 [path] 為任意非空字串。
- 可用 curl -L http://localhost:8080/ntu-csie/[path] 檢查是否有成功 redirect 到 https://www.csie.ntu.edu

4. Permission and error pages (3 points)

   - 接續上一小題，設定 Nginx 符合下列要求。
   - 在虛擬機中建立一個資料夾 /home/user/Documents/secret/，並掛載到容器的 /var/www/secret/，設定 Nginx server 任何嘗試連線到這個資料夾的，都會回傳 403 Error response。
   - 自行撰寫一個 HTML 檔，並將其映射到容器中的 /var/www/403.html，同時將 403 Error response 的頁面設定成 /var/www/403.html。
   - 可用 curl http://localhost:8080/secret/ 檢查。

以下三小題為同一題組。

5. Reverse proxy (2 points)

   - 在 /home/user/Documents/reverse-proxy 底下已經有一個設定到一半的 Docker Compose，請設定當中的 nginx.conf 以使得 reverse proxy 可以如下面設定的條件正常運作。
   - 當使用者訪問 http://localhost:7080/web 內容時，會利用 reverse proxy 的技術 forward 請求到 http://web0:5000/web 並將 web0 的回應回傳給使用者。
   - 執行 Docker Compose 啟動對應的容器，可以用 curl http://localhost:7080/web 檢查內容。

6. Load balance (2 points)

   - 接續上一小題，設定 Nginx 符合下列要求，以達成 load balance。
   - 在 Nginx 的設定中，將 web0 和 web1 成立同一個 group，並以 round robin 的方式來達到 load-balancing。
   - 當使用者訪問 http://localhost:7080/web 內容時，會利用 reverse proxy forward 請求到前面建立的 group 中的一個容器，並將 web0 或 web1 的回應回傳給使用者。
   - 連線至 http://localhost:7080/web 會依照 round robin 的方式詢問不同容器，可多連線幾次觀察變化。

7. Self-signed certificate (2 points)

   - 接續上一小題，請設定 Nginx 和 Docker Compose 符合下列要求。
   - 利用 OpenSSL 自己簽一個 SSL 的簽證，私鑰使用 RSA 演算法，長度為 4096 位元，私鑰不需要加密，證書有效日期為 365 天。
   - 更改 docker-compose.yaml，將 nginx 容器的 443 埠映射到虛擬機的 7443 埠，同時將簽章與私鑰放入 nginx 容器中。
   - 修改 nginx.conf，使其除了 HTTP 外，還可利用 HTTPS 連上伺服器。
   - 可用 curl https://localhost:7443/web 和 curl -k https://localhost:7443/web 測試結果。

Submission

- 全部小題都請找助教 demo。

3 Wireless Network ★ ∼ ★★★ (12 points)

Resources

- example_radius_log.json
- example_answer.txt
- radius_log.json

Tasks

1. **Wireless QA ★ ∼ ★★ (2 points)**

   (a) (1 points) 我們在 lab 中簡單介紹過系上 Wi-Fi 的架構，請說明當一個使用者使用行動裝置登入 csie 這個 SSID，接著在完成驗證並開始使用網路後傳送封包到 google.com 這個網域的這個過程中，依序會使用或經過以下的哪些服務或機器？請先從以下的服務或機器中選出有使用到的，接著依照第一次使用到該服務的順序依序排出。

   - LDAP Server
   - VPN Server
   - CSIE Firewall
   - AP Controller
   - Mail Server
   - DHCP Server
   - RADIUS Server
   - Access Point (AP)

   (b) (1 points) 當你使用電腦第一次連線到系上的 Wi-Fi 並登入時，系統可能會詢問你是否信任以下的這個憑證，請你說明為什麼連線及使用系上的 Wi-Fi 時我們會需要這個憑證？請說明為什麼檢查這個憑證是否合法是重要的。

Figure 1: 一個系上與 Wi-Fi 相關的憑證

2. **RADIUS Accounting Log is so fun! ★ ∼ ★★★ (8.5 points)**

在 Lab 中我們介紹過 RADIUS 在無線網路中負責的是 AAA 服務，其中一個 A 代表的是 accounting，也就是統計使用者的使用資訊。而在這題中，我們會提供某段期間內實際在系館的無線網路系統中所搜集到的 RADIUS accounting log。為了保護系上成員及同學的隱私，我們已經把使用者名稱欄位換成亂數的學號。在我們提供的 log 中，可以依據 StatusType 欄位共分為 3 種類別：Start, Interim-Update, Stop。其中，Start 代表開始統計使用者 session 的使用資訊 log，Interim-Update 則是在 session 連線過程中 RADIUS 定時紀錄的中途用量，Stop 則是該 session 完成之後統計的總使用量。以下則是這題中可能會使用到的欄位說明：

- User：使用者名稱
- InputPackets：使用者下載的封包數
- OutputPackets：使用者上傳的封包數
- InputOctets：使用者下載的 byte 數
- OuputOctets：使用者上傳的 byte 數
- UserEndRSSI：該使用者最後觀測到的 RSSI 值，是 AP 廠商訂定的分數，沒有特定單位
- @timestamp：該筆 log 的時間戳記，形式為 ISO 8601 格式的 UTC 日期與時間字串

請使用提供的 log 檔 (radius_log.json) 並根據以下題目的要求回答問題。此外，(b) 至 (e) 小題部分，為了方便同學 debug 及理解題目，我們額外提供了範例測資 (example_radius_log.json) 及其對應的答案 (example_answer.txt) 供同學參考。

(Hint: 你可以使用 Python 內建的 json package 處理 json 檔，及使用 datetime package 處理時間戳記；或是使用 Javascript 也可以方便處理 json 檔及時間戳記)

(a) (1 points) 請將 log 檔打開，你會看到除了以上的欄位之外，在每一筆 log 中都還有一個欄位叫做 CalledStationId。請依照課堂上所學到的知識，說明這個欄位可能指的是什麼？並回答其內容所代表的意義為何？

(b) (2 points) 通常，我們會關注使用者的網路使用量，因此我們可以從 Stop log 中計算出使用者的總使用量。因此，在這題中，請先從提供的 log 檔中篩選出符合以下條件的 log：

- StatusType 欄位為 Stop 的 log
- InputOctets, OutputOctets, InputPackets, OutputPackets 四個欄位中至少一個欄位不為 0 的 log
- 時間戳記範圍在 2024-05-21T12:02:45.00+08:00 至 2024-05-21T13:08:13.00+08:00 內的 log

然後請回答篩選完成之後的 log 總共有多少筆？

(c) (1 points) 承 (b) 小題，請從上一題篩選出來的 log 中，找出在這些 log 之中出現次數最多的 CalledStationId 為何？

(d) (1.5 points, 0.5 points each) 承 (b) 小題，在篩選完成並只留下 Stop log 之後，接著我們就可以計算每個使用者的總用量了，同時請注意**同一個使用者可能會出現在很多筆 log 中，所以請將所有屬於該使用者的 log 的流量一起加總計算**。請從上一題整理好的 log 中，計算以下幾位使用者各自總共使用了多少的流量，並計算以下幾位使用者各使用了多少個不同的 CalledStationId？在這裡，我們將流量定義為 InputOctets 及 OutputOctets 的總和。(請記得每個小題都要回答該使用者在所有 log 中的總流量，及該使用者使用了多少個不同的 CalledStationId，兩個答案都對才給分)
(本題之範例測資所求的使用者為 b68902238，非以下三個使用者)

a. r42922959
b. b55902658

c. r46944072

請注意此題的以上三個小題之繳交次數合併計算，建議同時繳交以上各小題的答案以免浪費繳交次數！

(e) (3 points, 1.5 points for each user) 承 (b) 小題，現在我們想要分別找到上傳及下載使用量最多的使用者。因此，請從第 (b) 小題篩選出來的 log 中，先找出 InputOctets 總和最大的使用者及 OutputOctets 總和最大的使用者，接著針對這兩位使用者各自所有 log 的使用量總和回答以下的內容：

- 使用者名稱
- 該使用者所有 log 的 Input 封包平均大小
- 該使用者所有 log 的 Output 封包平均大小

請注意不需要提供這兩個使用者使用的 InputOctets 或 OutputOctets 總和，只需要回答以上三個項目即可，並且每位使用者之以上三個項目都回答正確才給分。此題中的所有 log 的平均封包大小定義為該使用者在其所有 log 中所傳輸的總 byte 數除以該使用者在其所有 log 中傳輸的總封包數，請四捨五入到小數點後第二位。

請注意此題的兩個使用者之繳交次數合併計算，建議同時繳交答案以免浪費繳交次數！

3. **Easy, Fun, Kool ★ (1.5 points)**

上一題中用到 RADIUS Accounting 的 log，你好奇我們是怎麼得到這些資料的嗎？事實上，系館的 logging 是使用 Elasticsearch、Fluentd、Kibana 組成的系統，簡稱 EFK。請你搜尋關於他們的資訊，了解他們在做什麼之後，回答以下的問題：

請注意 (a) 及 (b) 小題各自都只能回答一次！

(a) (0.5 point) RADIUS 的 log 會儲存在哪裡？(複選題)
   (1) Elasticsearch
   (2) Fluentd
   (3) Kibana

(b) (0.5 point) 當我們想要尋找 RADIUS accounting log 的時候，可以去哪裡搜尋？(複選題)
   (1) Elasticsearch
   (2) Fluentd
   (3) Kibana

(c) (0.5 points) 為什麼我們需要使用 EFK 來蒐集 log？(Hint: 如果我們單獨在一台機器上架設 RADIUS，他的 log 會儲存在哪裡？)

Submission

- 所有題目皆請透過 Google Forms 上傳文字回答。
- 除了 2(d), 2(e), 3(a) 及 3(b) 外，其餘 tasks 的所有子題及小題皆可以分開上傳，並且次數分開計算。
- 2(d) 及 2(e) 的子題繳交次數合併計算。
- 3(a) 及 3(b) 僅能上傳一次。

4 (Cisco Switch) NASA is my GOAL !!! 劇場版 ★★ (10 points)

Resources

- kaisou.pka
- Packet Tracer 8.2.0 安裝檔
- Packet Tracer account: cisco.packet.tracer@yopmail.com
- Packet Tracer password: Cisco.packet.tracer0
- 劇場版還沒上映，所以這次就沒有故事咯

為了讓大家更好地銜接劇場版，我們決定幫大家複習一下前面的劇情前面的概念。

Chapter 6: 回層浮 ★★ (10 points)

- 目標：完成 `kaisou.pka`
- 題目：請直接參考 `kaisou.pka` 內的說明
- 注意：本題沒有 Activity Check，需自行檢查設定結果

Submission

- 請上傳完成後的 `.pka` 檔

5 Why DNS again? ★ ∼ ★★★★★ (12 points)

Resources

1. debian.ova
    - user name: nasa
    - user password: nasa2024
    - root password: nasa2024
    - OS: debian-12.1.0
    - 裡面什麼都沒有，是 fresh installed Debian。
    - 若需要 qcow2 檔案（例如 ova import 時因為相容性問題失敗），可以搜尋如何將 ova 檔案中的 vmdk 檔案轉成 qcow2 檔案。
2. logs.py
    - 用來模擬產生大量 logs 的程式

Tasks

1. Prerequisite (0 points)
   - 請安裝兩臺 Linux 機器，一臺作為 DNS server，另一臺為 DNS client。你可以選擇自己找 distro 來裝，也可以直接 import 附上的 Debian。
   - 這兩臺 VM 應該要能互相碰到對方。
   - 強烈建議使用 VirtualBox 來使用 VM，否則請自行解決網路拓樸。
   - 系統裝好後請安裝以下 package：
     - curl
2. Do Not Search - Part I ★ (2 points)

   系上不斷收到計中寄來資安示警的信，說我們的 DNS 有些奇怪的動作，經過排查發現某些網域有問題，請你幫助我們將這些網域列入黑名單吧！(BTW, 這是真實案件喔，如果你可以完成的話，表示你跟 NASA 團隊一樣厲害了！)
   - 本題請在 DNS client 作答及 demo。
   - 請修改系統中的某個檔案，使得這臺機器無法使用 `curl <url>` 連線至以下**網址**：
     - adsweu.com
     - shoeonlineblog.com
     - scriptsmysql.com
     - anxmalls.com
   - 請確保其他網址不受影響。
   - Hint: When resolving domains, the system will first look in /etc/*****?
3. Do Not Search - Part II ★★★ (4 points)

   經過 Part I 的處理後，我們已經可以讓某一臺機器無法連線到那些奇怪的網址了，不過計中說這樣還不夠，機器仍然可以連線到 *.<domain>.com，因此這題需要請你把這些**網域**都封鎖掉，且不影響到其他網域的連線。
   - 本題請在 DNS server 作答及 demo。
   - 請使用任意方式，使得這臺機器無法使用 `curl <url>` 連線至以下**網域**（也就是任何結尾為以下網域的網址皆需無法連線）：
     - adsweu.com
     - shoeonlineblog.com
     - scriptsmysql.com
     - anxmalls.com
   - 請確保其他網域不受影響。
   - Hint: dnsmasq is a light-weight DNS software.
4. Do Not Search - Part III ★ (2 points)

   經過 Part I, II 的處理後，我們已經可以讓某一臺機器無法連線到那些奇怪的網域了，不過如果要讓系上所有電腦都無法連線至這些網域的話，一臺一臺設定太花時間了。因此，這題假設系上所有電腦都已經設定好指向你架設的 DNS server ，透過更改這台 DNS Server 的設定來一勞永逸地阻止所有系上的電腦連線到奇怪的網域。
   - 本題請在 DNS server, client 作答及 demo。

- 請將 DNS server 及 DNS client 設定好，使 client 無法透過 `curl <url>` 的方式連線至以下網域。
  - adsweu.com
  - shoeonlineblog.com
  - scriptsmysql.com
  - anxmalls.com
- 請確保其他網域不受影響。
- Note: 中國國家防火牆也有用到這個概念喔！

5. Dangerous if No remote Storage ★★★★ (2 points)

   如同在 HW7 簡答題所問的問題，如果擔心存著 DNS records 的伺服器壞掉導致所有 records 消失不見，我們平時就要做好備份，而且要備份到不同機器上，~~可以的話備份到美國去更好~~。這題要請你幫忙實作「定時把某個檔案備份到另一臺機器的功能」。

   - 本題請在 DNS server, DNS client 作答及 demo。
   - 請用任何自動化的方式，**每分鐘**將 DNS Server 上面某一特定目錄下的所有檔案及目錄，使用下面的方法打包成 tar 檔案。將此 tar 檔案複製一份到 DNS Client 上面給定的一個路徑。Server 上的原始目錄以及 Client 上面複製後儲存的檔案位置可以自己任意選，請在 Demo 時向助教說明。)
   - 複製之前，請先將檔案以 `tar` 工具打包，並將打包檔命名為
     `backup-{YYYY}-{MM}-{DD}_{hh}:{mm}:{ss}.tar`
     其中時間為執行備份當下的時間。
   - 複製到另一台機器的檔案並非原檔，而是上一步打包完成後的 `.tar` 檔案。
   - 複製過去後，請將打包檔從 server 端刪除。

6. Does Not have enough Space ★★★★★ (2 points)

   DNS 系統因為需要頻繁回覆各種 queries，因此如果我們把 query logs 存下來，很容易把硬碟塞爆。這題請你提出一套解決方案來達成「維持 log 檔案大小不超過 1 MB」

   - 本題請在 DNS server 作答及 demo。
   - 執行 `python3 logs.py` 會建立一個檔案 `logs.log`，並且每秒寫入約 10000 筆長度約為 40 字元的 logs (也就是說，每秒約 400 KB 的資料)，持續 10 秒。
   - 請使用 `logrotate` 及 shell script，使 `logrotate` **每秒**都會檢查 `logs.log` 是否大於 1000 KB，若超過，則進行 log rotation；若未超過，則不做任何事。
   - Log rotation 的定義為：
     - 將 `logs.log` 重新命名為 `logs.log.1`，並將 `logs.log` 中的內容清空，以利後續 logging 繼續進行。
     - 若在重新命名時，`logs.log.{n}` 已經存在，則先將 `logs.log.{n}` 重新命名為 `logs.log.{n+1}`。
   - 請注意，某些服務（包含 logs.py）可能不支援 logrotate 中 create 新檔案的模式，因此在將目前的 log 存好並重新命名後，僅能將 `logs.log` 的內容「清空」，而非建立一個新的 `logs.log` 檔案來繼續存 log。這個做法確實有可能在「清空」檔案時影響到 logging 服務，使部分 logs 沒被 rotate 到，不過在這題，你可以無視這樣的情形。
   - Note 1: 結合 `logrotate` 及 Dangerous if No remote Storage 那題的做法就可以讓跑服務的機器不會因為硬碟被塞爆而壞掉。
   - Note 2: 一般來說 logrotate 會搭配 crontab 使用，且通常一天 rotate 一次就差不多了。

Submission

- 找助教 demo。
- 第六題（Does Not have enough Space）可以參考以下 shell script 進行 demo。即先跑 logs.py 後，每一秒執行你的指令，共 10 秒，logs.py 也僅會在這 10 秒內持續寫入 logs，10 秒後會自動停止：

```
#! /usr/bin/env bash

python3 logs.py &

sleep 1

for i in {1..10}; do
    # Put your commands here.
    sleep 1
done

wait
```

6 (NFS) Nasa's Fragile System ★ ∼ ★★ (10 points)

Resources

- NFS server:
  - 使用 `ssh sana@ws[4-6].csie.ntu.edu.tw -p 221XX` 登入
  - 對內網卡 IP: 192.168.30.1
- NFS client:
  - 使用 `ssh sana@ws[4-6].csie.ntu.edu.tw -p 222XX` 登入
  - 對內網卡 IP: 192.168.30.2
- 上述的 `XX` 請填入自己的組別編號。
- 登入密碼為考試前發放給各組的 password。

Description

還記得 HW9 中 Nasa, Sana 和 Asan 的故事嗎？在那之後，Nasa 因為嫌麻煩，最後仍然沒有使用 RPCSEC_GSS 機制來保護 NFS 的安全性。因此 Sana 決定以行動來告訴 Nasa 使用安全機制的重要性，請你來協助她。

- 你可以登入 NFS server 和 client 上的 `sana` 帳號，此帳號沒有 sudo 權限。
- Server 和 client 上的 `nasa` 帳號有 sudo 權限，密碼不公開，兩台的密碼不相同。
- 本題為 CTF 形式，flag 的格式皆為 `NASA{...}`。
- 請從 ws4, ws5, ws6 選一台使用，若需要重置可以換一台使用。
- 在開始解題之前，請先確認 client 上面有正確掛載 NFS 目錄 (`/mnt/nfs-share`)。如果 NFS server 和 client 之間的網路通訊有問題，請立即跟助教反應。

Tasks

1. ★ (3 points) 在 client 機器上，Nasa 固定每一分鐘都會把自己的家目錄中的 `flag1.txt` 檔案 (`/home/nasa/flag1.txt`) 備份到 NFS 目錄 (`/mnt/nfs-share`) 中。請設法取得 flag1.txt 的檔案內容。
   - Hint 1: 在 client 上有 tcpdump 這個工具可以使用。
   - Hint 2: 沒事備份一個 flag 做什麼呢？原來 flag1 中底線 `'_'` 之後的字元 (不含大括號 `'}'`) 就是 Nasa 在 client 機器上的密碼！取得 *flag* 之後，你就可以在 *client* 登入 `nasa` 來取得 *sudo* 權限了。這在後面的小題會需要使用到。
2. ★ (3 points) Server 還有分享一個目前沒有 mount 的 NFS 目錄，請設法讀取其中的 `flag2.txt`。
   - Hint: 這個目錄的完整 NFS 參數如下: `sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,root_squash,no_all_squash`
3. ★★ (4 points) 請讀取 server 上 Nasa 的家目錄中的 `flag3.txt` (`/home/nasa/flag3.txt`)。
   - 這題會需要在 NFS 目錄中製作一個 setuid 的執行檔。

Submission

- 請將 flag 上傳至 Submission Form。

7 LDAP ★★ ∼ ★★★ (13 points)

Resources

請在工作站上執行 `/tmp2/aoaaceai/publish/setup_ldap_final.sh`，這會在`/tmp2/<your id>/ldap_final/`目錄下放置 qcow2 檔案及 run.sh。請用這個目錄下的 `run.sh` 開機。兩台機器登入方式如下：

1. ldap1
   - olcSuffix: `dc=nasa,dc=csie,dc=ntu`
   - olcRootDN: `cn=admin,dc=nasa,dc=csie,dc=ntu`
   - olcRootPW: `nasa2024`
   - username: `root`
   - password: `nasa2024`
2. ldap2
   - username: `root`
   - password: `nasa2024`

Description

如果要使用 SSH 連線，請選擇好兩台機器的 SSH port，並執行以下指令：
`LDAP1_SSH_PORT=12345 LDAP2_SSH_PORT=23456 ./run.sh`

Tasks

0. Initialization (0 points)
   - `ldap1` 已經有先存放一些基本資訊，進度大概在 LDAP Lab 做完的程度。
   - `ldap2` 則是剛安裝完系統的狀態。與 LDAP 相關的 package 都有預先裝好。
   - `ldap1` 與 `ldap2` 可以經由內網互連。在兩台機器上執行 `ping ldap1` 與 `ping ldap2` 應該都會有結果。
1. SSL Certificate Generation (4 points)
   - 至 `ldap1` 上創建 `/etc/ssl/ldap/` 資料夾。
   - 創造一個 CA Certificate，命名為 `ca.pem`，憑證內容全部自訂。
   - 利用剛剛創好的 CA，簽署兩個 Certificate。Common Name 分別是 `ldap1` 與 `ldap2`。
   - 將屬於 `ldap2` 的 Certificate 與 Key 移動至 `ldap2` 的 `/etc/ssl/ldap/` 底下，命名為 `ldap.pem` 與 `ldap.key`。
   - 將 CA Certificate 複製至 `ldap2`，命名為 `/etc/ssl/ldap/ca.pem`。
   - 將屬於 `ldap1` 的 Certificate 與 Key 重新命名為 `ldap.pem` 與 `ldap.key`。
2. LDAP TLS Setup (5 points)
   - 請設定兩台 LDAP Server，使得 `ldapwhoami -ZZ -x -H ldap://ldap1` 與 `ldapsearch -ZZ -x -H ldap://ldap2` 可以正常運作。`TLS_REQCERT` **請設定為 demand**。
3. Syncprov (4 points)
   - 請微調 Debian Wiki 的作法，完成 `olcDatabase={1}mdb` 的 syncprov 設定。
   - 完成後，對兩邊進行 `ldapsearch` 的結果應該會一樣，而且 `ldapmodify` 的結果會同時出現在兩台機器中。

Submission

- 找助教 demo。

8 NTU COOL Video Storage ★★ ~ ★★★★ (7 points)

在 2022 年底時，COOL 的影片儲存面臨到很大的挑戰。主要的問題有三：(1) 原本用以儲存影片的傳統硬碟陣列的 I/O 容量不足，新的影片系統是儲存小檔案，因此造成 random access 的存取模式，是傳統硬碟比較不擅長的。(2) 磁碟陣列中的硬碟大多在 2018 年前後採購，因此逐漸進入高損壞率的使用時間。(3) 影片儲存容量不足。全校使用 NTU COOL 後，每學期產生約 70 TB 的影片。

NTU COOL 的影片儲存系統主要是利用minio這套分散式物件儲存系統。在當時的系統配置中，總共有 9 台 minio 主機，每一台主機使用 iSCSI 協定掛載了 NAS 上面的 4 顆 14 TB 或 16 TB 的傳統硬碟，共使用了 36 顆傳統硬碟。NAS 並非直接把整顆硬碟以 iSCSI 供 minio 系統使用，而是以檔案方式儲存 iSCSI 的 Logical Unit of Storage (LUN) ，可視為一個 raw 格式的磁碟映像檔。詳細說明請見下方題目。

本題讓大家可以操作當時 NTU COOL 團隊解決這些問題時所想出來的解決方案。不過，為了節省時間，不會牽涉到 iSCSI 部分，另外也將原本 14 TB 的磁碟大小，改以約 1.4 GB 來模擬。

使用於 COOL 影片儲存系統的 NAS，在每一顆使用的硬碟上會建立三個 partition，而已知其中第三個 partition 會用來建立一個 Linux RAID，這個 RAID paritition 中有一個 ext4 的檔案系統，

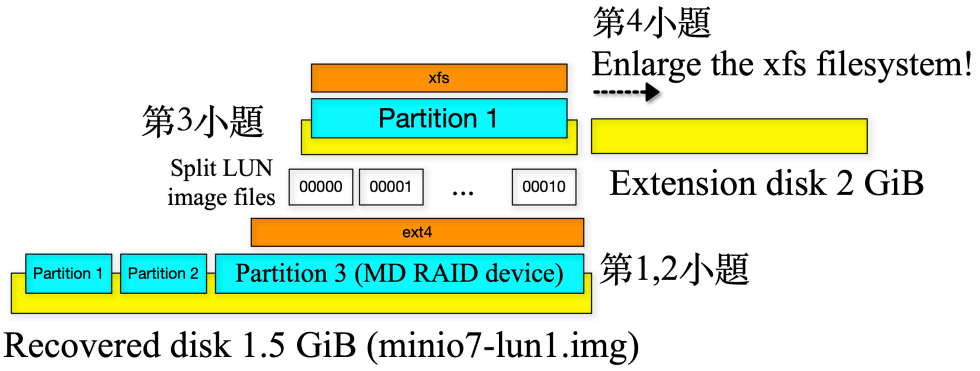

Figure 2: 本題儲存架構示意圖

其中儲存了 LUN 的許多檔案。Partition table 的摘要如下（執行 `fdisk -l /dev/<dev name>` 的結果）：

```
Disk /dev/vdb: 1.5 GiB, 1610612736 bytes, 3145728 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 1AAC488B-85F6-3B4E-8410-40470E3B836C

Device       Start     End Sectors  Size Type
/dev/vdb1     2048  206847  204800  100M Linux RAID
/dev/vdb2   206848  411647  204800  100M Linux RAID
/dev/vdb3   411648 3145694 2734047  1.3G Linux RAID
```

數日前，NAS 上的其中一顆硬碟 (minio7-lun1) 產生損壞警示，因此目前團隊已經將其取下，並且以ddrescue拷貝到了一顆健康的硬碟上。請將 minio7-lun1.img 掛載在你的虛擬機，模擬這顆健康的硬碟。

本題的一些條件設定：

- 需要直接在 minio7-lun1.img 上面操作，而不可以將包含於其中的檔案系統拷貝出來。這是因為在真實的環境裡面，硬碟的大小為 14 TB 或 16 TB，將整個檔案系統拷貝出來所需要的時間超過一天，大幅延遲系統上線時間。
- 可以使用任何你所熟悉的 Linux 作業系統來處理這題的工作。

Resources

- minio7-lun1.img

Tasks

1. (1 points) ★★
   在將硬碟從 NAS 卸除下來時，NAS 的作業系統固定會將硬碟第三個 partition 的 md RAID superblock 移除。因此，目前沒有辦法讓 Linux 作業系統直接偵測到這個 RAID partition，也

沒有辦法掛載。由於過去團隊也有碰過這樣的狀況，過去曾經利用 `mdadm --examine` 指令，將這個 RAID partition 的 meta data 記錄下來，如下：

```
/dev/vdb3:
          Magic : a92b4efc
        Version : 1.2
    Feature Map : 0x0
     Array UUID : 007e55f0:32b982f3:70e64d14:2b9c41d2
           Name : RS3617RPxs_3:4
  Creation Time : Mon Mar 25 23:44:09 2024
     Raid Level : raid1
   Raid Devices : 1

 Avail Dev Size : 2731999 sectors (1333.98 MiB 1398.78 MB)
     Array Size : 1365952 KiB (1333.94 MiB 1398.73 MB)
  Used Dev Size : 2731904 sectors (1333.94 MiB 1398.73 MB)
    Data Offset : 2048 sectors
   Super Offset : 8 sectors
   Unused Space : before=1968 sectors, after=95 sectors
          State : clean
    Device UUID : d2480bf3:33997cf6:b562897b:ba7400cd

    Update Time : Tue Mar 26 08:17:44 2024
  Bad Block Log : 512 entries available at offset 16 sectors
       Checksum : 2be80c68 - correct
         Events : 2


   Device Role : Active device 0
   Array State : A ('A' == active, '.' == missing, 'R' == replacing)
```

在本題中，請在不重建 md superblock 的狀況下，直接掛載第三個 partiion 上的 ext4 檔案系統。請在掛載的目錄下，執行 tree 指令，並繳交輸出的文字檔。(理論上會需要用 fsck 來修復在 RAID partition 中的 ext4 檔案系統，不過在這題裡面，我們就不做這個步驟)

提示：請注意上方 meta data 中的 Data Offset 的數值。

2. (1 points) ★★
請重建 mdadm 的 superblock 在第三個 partition，並且使得 RAID 使用原本的 RAID level、Array UUID、Name、meta data 版本（請使用 1.2）、Data Offset (非常重要!)，且不可損壞原本存在於 parition 中的資料。完成後請讓作業系統啟動此一 md device，並且繳交：

   (a) `mdadm --detail /dev/<md device>` 的文字顯示結果

   (b) `mdadm --examine /dev/<3rd partition device>` 的文字顯示結果

3. (3 points) ★★★★
在第三個 partition 中的檔案系統中，儲存著紀錄 iSCSI 內容的映像檔。請參見 Figure 2。首先，其中有一個 iscsi_lun.conf 檔案，其格式如下

```
[LUN_00ee11d8-f6b6-412a-a34e-03c8101f2315]
        lid=9
```

```
pre_alloc=yes
devtype=1
rootpath=/volume2
restored_time=0
uuid=00ee11d8-f6b6-412a-a34e-03c8101f2315
vpd_unit_serial=00ee11d8-f6b6-412a-a34e-03c8101f2315
dev_attribs=emulate_3pc:0,
  emulate_tpws:0,emulate_caw:0,emulate_tpu:0,can_snapshot:0
bytes=1153433600
name=minio7-lun1
bkp_obj=0
vaai_support=no
```

在檔案系統中存在一個 `00ee11d8-f6b6-412a-a34e-03c8101f2315/`的目錄（即 iscsi_lun.conf 中的 uuid 屬性作為目錄名稱），其中包含著被切分為數個每個約 100 MB 的映像檔（真實的系統上是切分成每個 1 TB 的映像檔）。這些映像檔的檔名為 `minio7-lun1_00000`, `minio7-lun1_00001`, `...`, `minio7-lun1_00010`（minio7-lun1 為 iscsi_lun.conf 中的 name 屬性）。

在連接好所有磁碟映像檔案後，可以發現映像檔有如下的 partition table：

```
Disk /dev/<virtual dev>: 1.07 GiB, 1153433600 bytes, 2252800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: EBA250C7-6112-834A-B6BF-EEC0986617DD

Device                     Start     End Sectors  Size Type
/dev/<virtual dev>p1  2048 2252766 2250719  1.1G Linux filesystem
```

在這個 partition 底下，有一個 XFS 檔案系統，其中放置了 minio 系統所使用的檔案。

請撰寫一個 Bash shell script, 可以依照 iscsi_lun.conf 的檔案內容取得 uuid 和 name，並依照切分後的映像檔案數量，將所有映像檔連接起來，並且掛載其中的檔案系統。在掛載的目錄下執行 tree，並繳交 shell script 及文字執行結果。(若無法撰寫可以完成掛載指令的 shell script，而僅以手動方式完成掛載，可獲得一半分數)

提示：請使用 losetup、dmsetup、kpartx 等工具完成此題。使用 dmsetup 線性連接多個裝置的方式，可參考dm-linear 說明以及這篇 serverfault 上的文章。

4. (2 points) ★★★
不久之後，果然硬碟容量開始不足了（上題中的 XFS 檔案系統已使用 88%）。請在你的虛擬機中增加一個大小為 2 GiB 的空硬碟，想辦法將前一題產生用來掛載 XFS 的裝置與這個新的空硬碟串接在一起，並且將上面的 partition 和 XFS 檔案系統都擴充到可利用整個新硬碟。請繳交 `lsblk -f <expanded dev>` 的文字輸出結果。

提示：和前一題類似，使用 dmsetup 來將兩個裝置合併成一個裝置。接著，使用 parted 修改 partition table，使用 xfs_growfs 來將檔案系統的大小擴大。

9 Fix PC ★ ~ ★★★★ (7 points)

Resources

1. 一台筆電
   - nvme0n1p1 EFI 開機磁區，與本題無關，勿動。
   - nvme0n1p2 LUKS 磁區，password: 未知，之後會告訴你
   - nvme0n1p3 LUKS 磁區，是加密過的 boot partition，password: nasa2024
   - nvme0n1p4 LUKS 磁區，是加密過的 root partition，password: 不提供，由 nvme0n1p3 自動解密
   - linux username: root
   - linux password: nasa2024
2. 一台 switch (共用)
   - ip: 192.168.1.1 (可用瀏覽器連線)
   - username: nasa
   - password: nasa2024
   - 此帳號只有唯讀權限，無法更改任何設定
   - port 1 為 uplink，可以連接外網
   - port 2-3 留給助教使用
   - port 4-8 供解題使用

Description

還記得考試開始時發給你的筆電嗎？你的同學小明趁你不在的時候，對它惡搞了一番，現在它連開機都開不了了。請修好它吧！

Notes

這題是實體題，而且部份題目需要到其他地方接網路線解題。Task 1 為離線題目。Task 4 需要接網路線，請依助教的指示輪流使用。其餘題目請自行判斷。
如果你不小心搞砸了，可以向助教申請 reset。每組只有**一次** reset 機會。
在開機時，如果 grub 一直顯示 decryption failure，請在打密碼之前先按一次 Esc 鍵。

Tasks

1. **Booting The System ★★★★**
   - (1 points) 小明執行了 ‘dd if=/dev/zero of=/dev/nvme0n1p4 count=4096 bsize=4096‘，導致現在無法開機。不過，你早就把那個區域的資訊備份在 ‘/dev/nvme0n1p2‘ 磁區裡了。請到 這個 Hackmd 表單中取得密碼，解鎖磁區後將電腦修復至可以成功開機的狀態。
2. **Filesystem Debugging ★**
   - (1 points) 執行 ‘lsblk‘ 後，你會發現 nvme0n1p2 磁區明明佔了 128M 的大小，但是連 80M 的檔案都塞不下 ?! 請找出原因並修復它。

3. **VM Debugging ★★★**

   - (1 points) 執行 '/root/vm/run.sh' 時，發現它好像會出現錯誤。請找出原因並修復它。VM 的開機時間請控制在 10 秒以內。

4. **Network Debugging ★★★**

   (a) (2 points) 因為某些未知的原因，現在電腦沒辦法連上網路。請修復到可以正常 DHCP 取得 IP，並能 'ping 8.8.8.8' 的程度。

   (b) (1 points) 請修復電腦到可以正常 'curl https://example.com' 的程度。請注意設定的方式必須要和 DHCP 可以配合。

5. **Shell Debugging?! ★★**

   - (1 points) 你平常會用 shellcheck 來檢查 shell script 的潛藏問題。不過，現在執行 'shellcheck myscript' 的時候好像會出錯。請找出原因並修復它。

Submission

- Task 1: 請找助教 demo。
- Task 2: 請至 Google 表單回答出問題的原因，以及你所用的指令們。
- Task 3: 請找助教 demo。
- Task 4: 請找助教 demo。
- Task 5: 請至 Google 表單回答出問題的原因，以及你所用的指令們。