Homework #6

Due Time: 2021/05/30 (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 name your PDF "`{your_student_id}.pdf`", and submit it through NTU COOL.

Grading

- NA accounts for 50 points while SA 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.

Network Administration

1 DNS & DHCP (30%)

此題目是希望同學們練習架設 DNS server 以及 DHCP server，為了方便，此次題目中的 DNS server 以跟 DHCP server 只需架設在同一台 VM(建議使用 CentOS or Ubuntu server)，然後再另外架設一台 client VM 來測試並使用兩 server 提供的服務。同學們需要將自己架設的過程一步一步完整解釋清楚 (或許搭配一些截圖來進行解釋)，方能拿到滿分。

以下是 server 與 client 的要求：

1. server VM:
   (a) 設定 server 固定 ip 為 192.168.5.254
   (b) server 要有兩個 network interface, 一個對內 (以向內網提供 DNS 以及 DHCP 服務), 一個對外
   (c) DHCP setting:
      i. subnet : 192.168.5.0/24
      ii. range: 192.168.5.100-192.168.5.200
      iii. dns server: 192.168.5.254
      iv. route/gateway: 192.168.5.254
   (d) DNS setting:
      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. allow recursion: 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
2. client VM:
   (a) 透過 DHCP server 拿到 IP，並截圖 (18%)
   (b) 分別 dig www.[your_student_ID].com, google.com, 跟 dig -x 1.2.3.4，並都截圖 (各 4%, 共 12%)

2 Short answer (20%)

Cache 在 DNS 的架構中是扮演著相當重要的角色，但他好像也帶來了一些問題....

1. 請先解釋 DNS record 中的 TTL 是什麼 (2%)？說明其與 DNS propagation time 的關係 (2%)，並說明長的 TTL 跟短的 TTL 各有什麼好處 (1%)。
2. 請解釋 DNS 架構中是如何使用 cache(3%)？並且以 authoritative servers 的視角來說明 cache 的重要性 (2%)。
3. Cache 帶來許多好處，但也給予了一些攻擊的漏洞。請解釋什麼是 DNS cache poisoning attack(3%)，並提出一個防禦的方法 (2%)。
4. 當你研究完 DNS cache poisoning attack 後會發現，其實它要能成功的條件蠻嚴苛的，而且你剛剛也提出了一些可行防禦的方式，因此後來又出現了 Kaminsky attack！(其實提出者 Dan Kaminsky 是研究人員不是壞人。) 請你說明為什麼 Kaminsky attack 是一個比 DNS cache poisoning attack 更難防禦的攻擊 (3%)，並提出一個防禦方法 (2%)。

System Administration

1 This Problem Is Not For Sale (20%)

1.1 Using a Saddle? Shame on You! (4%)

> The only people who never tumble are those who never mount the high wire.

在系上內網有一臺 IP address 為 `10.217.44.112` 的 NFS server，可以從工作站存取。請掛載 `10.217.44.112:/e/NASA_flag` 這個資料夾以取得 flag，並寫下取得 flag 的方式和過程。

1.2 Failing Successfully (6%)

> He who blinded by ambition, raises himself to a position whence he cannot mount higher, must thereafter fall with the greatest loss.

你可能已經知道工作站上的家目錄是在 NFS 上的。(詳情可以參考 `/etc/autofs/auto.nfs` 這個檔案。) 請說明為什麼，你身為一個普通使用者，無法使用如前一題的方式掛載家目錄並存取他人的檔案。(當然，如果你有辦法做到這件事，也請務必告訴我們 :))

Hint `man 5 exports`

1.3 Notice My Files, Senpai (7%)

> I do hope his eyes gaze upon me, and that my allegiance is recognized! I dunno... Notice me senpai! Notice me!

請在你的家目錄下放一個名為 `.nasa-is-an-awesome-course` 的檔案，並確保只有你和使用者 `wp`[1] 能存取這個檔案。另外，也請附上該檔案的絕對路徑以及寫下設定的過程和使用的指令。

1.4 RIP=RELEASE (3%)

> Nice boat!

在 NASA 工作站組，我們同時使用了 NFS 和 iSCSI 兩種技術/協議。請簡述這兩者的異同，並舉例說明兩者適合的使用情境。

2 Getting Your Fix of VMs (25%)

在以下問題中，我們會提供數個壞掉的虛擬機器映像檔請你修復，並請詳細地寫下修復的步驟。另外請注意**不要將整個系統重灌**。若你不確定你進行的操作是否算作重灌，也歡迎來信詢問。

2.1 Does It Boot? (Baka Mitai) (10%)

> There's a snake in my boot!

[1] 或許還有 `root`，不過不重要？

本題使用的映像檔可於 `linux2` 上的 `/tmp2/haha.qcow2` 或是 https://tinyurl.com/pxbp4frp 找到，`b2sum` 為

```
753691c35a3f63314fc3e165e72c73b7cc65c6b6683579cc20396944d7f20a9057356a78556e5a49
05490bcb034848ca9393d10fc1c366fb32e2b6821f0438d2
```

（以下內容皆為虛構，若有雷同純屬巧合。）

在某個小島上，曾經有位不負責任的 NASA 助教，遠端改了自己位於糕熊市的機器的設定，卻沒有好好測試。不幸的是，南部的假牙業非常發達，使用了非常多的電力，造成民生用電經常停擺。而這位助教的機器，也在某次興達電廠跳電之後無法開機了。無助的他只好打電話求助朋友去他家幫他修復……唯一的問題是他沒有朋友。沒辦法了，只好藉職務之便壓迫 `^H^H` 請身為修課學生的你幫他修了。

講了那麼久的故事，只是要說倉促被趕到他家的你手上什麼都沒有（對，連 `root` 密碼都沒有），所以這題**請不要使用任何的 live CD 或 installation ISO 等工具**[2]。

2.2 Is It Wrong To Try to Recycle Midterm Problems? (15%)

> I roll my eyes. "I'm not asking you to take your clothes off, baby. I just want to peek at your midterm."

本題使用的映像檔可於 `linux2` 上的 `/tmp2/hahaha.qcow2` 或是 https://tinyurl.com/2zy9zfr3 找到，`root` 密碼為 `h44CH4m4`，而 `b2sum` 為

```
ea4a7955370904828cfdc3c5c3cb05bb06d8fa9144cd35a17c9c903d2e0e9fc829b90f14e7e61a0b
edd5cd101e1e738f2ca45bbd506239b64c190b8fbbd1fb3b
```

2.2.1 Vanilla (9%)

還記得期中考的 "By the way, I use Arch" 題目嗎？認真的你旁邊的同學在完成前二小題後，發現他的虛擬機無法開機了！果然天下沒有白吃的午餐，TANSTAAFL，第三小題的分數不是白給的！於是他來尋求你的協助，請你幫他修復這個問題。

Note 你不需要再寫一支重灌腳本，將修復的過程寫下就足夠了。

Note 實際上因為我們只有一顆硬碟，所以磁碟代號可能會和期中考題目有些出入。

2.2.2 Raid, Shadow Legends (6%)

除了期中考題目指定的分區，其實你旁邊的同學還使用 `mdadm` RAID1 建立了 `/dev/md1` 這個裝置，據說裡面放了很多有趣的資料 (°ʖ°) 。不過這個 RAID 底下似乎有個分割區壞掉了。請修復這個 RAID 裝置，使其不再處於 degraded mode。

3 PAC-Man 2024 (5%)

> I like to think of innovation as upgrading your current self. This upgrade helps you to more effectively deal with changes happening around you and to be able to think in a more complex manner than before.

[2]當然，你在測試的時候偷偷用是沒人知道 `^H^H^H^H` 沒問題的，但最後的解請不要用到這類的工具。

你的朋友剛開始使用 Arch Linux。他聽說 pandoc 是個可以用來將 Markdown 轉成 PDF 的有用工具[3]，於是便迫不及待地用以下的指令安裝：

```
$ pacman -Sy pandoc
```

不幸的是，在執行 pandoc 時他很快地遇到以下的錯誤：

```
$ pandoc
pandoc: error while loading shared libraries:
libHStexmath-0.12.2-9PrjeHGF0WjK1H3ULy1SzS-ghc8.10.4.so:
cannot open shared object file: No such file or directory
```

你知道為什麼會發生這個問題嗎？又，如果你是你的朋友，要如何避免這個問題呢？

[3]事實上，它的用途不僅於此。