Homework #7

Due Time: 2024/04/07 (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 name your PDF "`{your_student_id}.pdf`", and submit it through Gradescope.

Grading

- 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.

DNS

1. Do you know what is DNS ? (20 points)

以下問題請用十句以內的句子回答，言簡意賅即可。

1. 請解釋 DNS 是什麼？(5 points)
2. 請解釋 DDNS 是什麼？(5 points)
3. 請問目前全世界共有幾臺 root name servers（不包括 mirrors，即每個不同的 ip 算一臺）？(5 points)
4. 請問 TXT records 除了作為註解外，還有什麼樣的實際應用？請任舉一例，並簡述該服務的用途或目的。(5 points)

2. Do you know how to reach CSIE DNS? (10 points)

請找出從任一 root name server 到 www.csie.ntu.edu.tw 的任何一條 query path，列出所有經過的 name servers 所管轄之網域及 ip，並列出所使用的指令及截圖。

範例：root name server 到 www.nasa.com

```
ulin@nasa:/$ //Some command that I used to find out the delegation path.
```

Domain Name	IP	Zone
g.root-servers.net	192.112.36.4	root zone
a.gtld-servers.net	192.5.6.30	*.com
ns1.parkingcrew.net	13.248.158.159	*.nasa.com
www.nasa.com	185.53.177.52	

Table 1: name server list

3. Do you know how to design a DNS architecture? (30 points)

假設你是 NTU CSIE 的網管，要幫系上的 *.csie.ntu.edu.tw 網域設計 DNS 架構，請問你會如何設計呢？答案可能包括且不限於：硬體、軟體、地理位置、網路架構……。你不需要將詳細的配置步驟及細節寫出來，只需要提供一個大方向即可。

你可能需要考慮以下問題：

- 如果今天其中一台伺服器壞掉了怎麼辦？
- 如果今天系館停電導致所有機房下線怎麼辦？
- 如果因為某些原因導致伺服器上的 DNS records 不見了怎麼辦？
- 有些實驗室想要擁有自己的 subdomain，該如何實現？
- 如何應對 DNS flooding attack？
- 如何應對 DNS amplification attack？
- 如何確保對 *.csie.ntu.edu.tw 的 query response 不會被攻擊者竄改成 malicious ip 呢？

評分標準：

- 基本 DNS server setup 得 9 分。
- 每解決上述的一個問題得 3 分。

示範問答：

- Q：如何設置 DHCP 系統？
- A：在與 clients 相同的網路裡面，開一台 server，並在上面跑 dnsmasq。

4. The Power of DNS (40 points)

目前系上的 DNS server 使用 BIND，然而現在其實有許多開源的 DNS 軟體可供選擇，PowerDNS 便是其中之一。

相信大家在做 Lab 的時候，應該或多或少都有覺得「好麻煩喔，BIND 怎麼加個 record 要改這邊又要改那邊」的時刻吧—(我們也是)—，因此我們未來的目標之一就是把管理 DNS 的任務簡化，並且 PowerDNS 還支援各式各樣的功能，例如我們需要監控 DNS server 是不是有正常運作，在 BIND 的話需要額外寫 script 去做，在 PowerDNS 則可以由他內建的 metrics API 來達成監控的目的；又如 DDNS，BIND 需要更複雜的設定，PowerDNS 則有預設支援。而 PowerDNS 除了這些功能，如果再搭配上適當的前端管理頁面，則可以將管理 DNS 的任務大幅簡化！

舉例來說：目前的 BIND server，如果要在 *.csie.ntu.edu.tw 網域內修改 record，我們需要先進入 DNS server，然後找到 BIND 的 zone file，在 zone file 內找到對應的 record 進行修改，最後再重新簽署 DNSSEC，整個過程大約需要 3 至 5 分鐘。然而若使用 PowerDNS + PowerDNS-Admin ，只需要在 GUI 內點幾下便可完成，30 秒內便可完成。

因此，NASA DNS 團隊的終極目標便是把陽春的 BIND 換成厲害的瑞士刀 PowerDNS。

不過天下沒有白吃的午餐，架設 PowerDNS 的過程比較繁瑣，因此這一題要請你架設 PowerDNS + PowerDNS-Admin stack。

(請紀錄下所有步驟，要讓助教批改時可以依照你文件上的步驟完成任務，若有每一步的截圖更好！)

1. 架設 PowerDNS。請在你的機器上架設 PowerDNS，**請注意，後端限定使用 SQLite** 。(20 points)
2. 架設 PowerDNS-Admin。請在同一台機器上跑 PowerDNS-Admin，記得確認 PowerDNS-Admin 有連接到你的 PowerDNS 服務（提示：跟 API 有關）。(10 points)
3. 透過 PowerDNS-Admin 新增 records。請根據以下故事新增 DNS records，並附上 dig 後的截圖（提示：應該包含 TXT、NS、A 共三種 records）。(10 points)

   > 您好：
   >
   > 我們是臺灣的秘密網路管理組織———納沙，在此誠摯邀請您加入我們的團隊！
   >
   > 由於我們團隊只招收有經驗的網管，我們想要先確認您有管理網路的經驗，聽聞您負責管理 nasa.csie.tw 網域，請您新增一個 TXT record，讓我們在查詢 verification.nasa.csie.tw 時可以看到："I LOVE NASA" 的文字訊息，如此一來我們才能確認您真的擁有這個網域。

另外，我們團隊之前在德田館撿到一臺 ip 為 10.1.6.88 的伺服器，據說是 *.sub.nasa.csie.tw 的 authoritative server，因此希望您能將所有詢問 *.sub.nasa.csie.tw 的 query 引導到這臺伺服器上。具體流程如下：

(a) 如果有人詢問任何屬於 *.sub.nasa.csie.tw 的 domain name，您回應中的 authority section 應該要包含 subns.nasa.csie.tw，以告訴他應該要去哪裡詢問這個 domain name。
(b) 接下來那個人會詢問您的 DNS server：「subns.nasa.csie.tw 的 ip 是什麼？」，此時您的伺服器應該要在 answer section 回覆「10.1.6.88」。
(c) 再來那個人會自己去詢問 10.1.6.88，與您的伺服器無關了。

感謝您撥冗閱讀這封信件，希望您能順利加入我們團隊！

納沙團隊 敬上