Homework #5

Red Correction Date: 2025/03/28

Due Time: 2025/03/30 (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 put the pdf file and all three configuration files for PowerDNS, Recursor, and dnsdist as-is after completing all the problem sets into a directory named after your student ID, zip it, name the zip file "`{your_student_id}.zip`", and submit it via NTU COOL. If you modified or created additional **config files** for the three services during the process, please attach them in the zipped directory as well. Config files for other services, such as nginx, do not have to be attached as files. The directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- pdns.conf
+-- recursor.conf
+-- dnsdist.conf
+-- [any other .conf/.lua/.yml files modified/created(*), if any]
```

  * Edit: In addition to `.conf` and `.lua` listed originally, modified or created `.yml` config files should also be attached, if you used such format over others.

- As a friendly reminder, the zip file should contain a directory, not just the files. If you are unsure, `zipinfo` or similar programs may help.

Grading

- The total score for the correctness and completeness of your answer is 100 points.
- 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 = correctness score + tidiness score.

回顧在 lab 中，我們學習了如何安裝及操作 BIND 這個 DNS 服務，事實上，這也是目前系上真實使用中的服務。然而現在其實有更多開源的 DNS 軟體可供選擇，我們現在便將試著上手另一套常被運用的 DNS 服務－－ PowerDNS。

ＣＳ貓是個經營水果買賣的大型電商，店裡專門販售高級客製的水果；這天老闆辦了一讚折一元的活動，沒想到引來上萬人按讚，正逢活動，結果居然有駭客把老闆的 DNS Server 搞沒了，害大家沒辦法透過網址進到老闆的商店，天啊！老闆趕緊提前截止活動，請到了 NASA 團隊的你來幫他重建 DNS Server，找回水果店往日的光彩，你能擔起這個任務嗎？

在這份作業中，凡是需要操作的題目你都需要對各個步驟清楚列出過程讓 NASA 團隊的其他成員還有ＣＳ貓老闆可以重現你的過程，若允許，請盡量多加截圖讓我們能更好理解！

1 Setting up PowerDNS (48 pts)

首先，請你先試著架設 PowerDNS 與 PowerDNS Admin！

1. 請建立一個 Debian 12 的虛擬機，在你的機器上的 port 5301 架設 PowerDNS **4.9+**，請使用 MariaDB 做為後端，最後請附上可以對這個伺服器成功進行 `dig @[server ip] -p 5301` 查詢之截圖、以及 `pdns_control version` 之截圖（16 pts，需提供安裝及設定過程）。

2. 在同一台虛擬機上將 PowerDNS-Admin 架設在其預設的 port 9191。記得確認 PowerDNS-Admin 有連接到你的 PowerDNS 服務，最後須以學號為帳號的 First Name 註冊帳號、用瀏覽器登入後截圖帶有該名稱的任意頁面（16 pts）。

3. 利用 Nginx 將 PowerDNS-Admin 設置為反向代理服務，並且將 `[student-id].com` 設定為 domain name，最後請附上從瀏覽器使用 domain name 且不帶指定 port 直接瀏覽管理介面的截圖（7 pts，不限制解析該 domain 之方式）。

4. 作為 cscat.tw 的管理者，請根據以下需求**使用 PowerDNS-Admin** 新增 DNS records，並附上 PowerDNS-Admin 裡顯示 `cscat.tw` 這個 zone 全部 records 的頁面、以及 `dig` 敘述中所有 records 的截圖（7 pts，Hint：應該包含 NS、A、CNAME、AAAA、MX、TXT 共六種七項 records）：

   - 老闆希望當顧客輸入 `www.cscat.tw` 時，能夠自動導向到 `cscat.tw`，而 `cscat.tw` 的主機在 `192.0.2.1`。
   - 目前，ＣＳ貓發送訂單通知與促銷郵件時，部分郵件會被標記為詐騙郵件，原因是缺少正式的郵件交換設定。請確保當其他郵件伺服器查詢 `cscat.tw` 的郵件交換資訊時，可以知道應該將郵件發送到 `mail.cscat.tw`，優先值請設為 `10`。
   - 另外，為了幫助外部郵件伺服器確認這台郵件伺服器是合法的。請新增適當 **TXT** 記錄，讓查詢 `cscat.tw` 時，可以看到 `"v=spf1 mx -all"`，以防止詐騙郵件偽造公司域名。(按：這份作業中只要練習新增即可，但若有興趣可以在網路上認識 SPF 這類別 record)
   - 開發團隊最近設置了一個新的 API 伺服器，並將其部署在 IPv4：`192.0.2.4` 和 IPv6：`2001:db8::50` 上，他們希望能透過 `api.cscat.tw` 訪問這些服務，而不需要記憶 IP 地址。請確保此網域可解析到正確的伺服器。
   - 由於業務拓展，老闆決定將子公司的服務 `store2.cscat.tw` 交由他們自行管理，而他們使用自己的 DNS 伺服器 `dns2.cscat.tw` 來處理所有 `store2.cscat.tw` 的查詢。請適當設定 DNS，將該子網域的解析權限委託給他們。

5. 請解釋 DNSSEC 的基本原理與目的，接著請為 `cscat.tw` 這個 zone 開啟 DNSSEC；現階段你只需要確保可以查到 DNSKEY 即可，不需要確保其可驗證，並且，請附上 `dig @[server ip] -p 5301 cscat.tw DNSKEY` 的截圖（2 pts）。

2 PowerDNS Recursor (25 pts)

0 Basic

然而，一整套完整的 DNS 服務只有 authoritive server 可能是不夠的，當想要問其他問題的時候，我們總不能什麼都不做吧！這時我們便可另外設置 recursive resolver 來進行 recursive DNS query。

1. 前面，我們做的是建立一個 authoritive server。請說明什麼是 authoritive server（1 pt）。
2. 請解釋 recursive DNS query 和 iterative DNS query 分別是什麼，並比較兩者（1 pt）。

1 Setting up PowerDNS Recursor

1. 請依據以下需求在 port 10053 另外設置 PowerDNS Recursor 服務，為求精簡，在同一台虛擬機上安裝即可（6 pts，需提供安裝及設定過程）。
   - 將快取的 TTL 設定成 300 seconds.
   - 用 `forward-zones-file` 將 `cscat.tw` 重新導向到你剛建立好的 Authoritative Server，其餘則轉給 Google DNS（`8.8.8.8`）。
   - 它會驗證 record 的 DNSSEC。
2. 請提供針對這個 Recursor 服務查詢 `google.com` 的截圖（1 pts）。
3. 請提供針對這個 Recursor 服務查詢 `cscat.tw` 的截圖（1 pts）。讓我們回到真實的角度，請說明為什麼這個服務可以正確回應 `google.com`，面對 `cscat.tw` 卻會是 `SERVFAIL` 呢（2 pts，提示：考慮 DNSSEC）？
4. 調整相關設定以令 Recursor 得以**驗證** `cscat.tw`（不可關閉或不驗證 DNSSEC），並附上調整後成功查詢 `cscat.tw` 的截圖（5 pts）。
5. 請問將快取的 TTL 設定過高或過低分別會有什麼問題（1 pts）？
6. DNS 快取有個相當經典的攻擊手法被稱為 cache poisoning，請用 10 句話以內描述一個可能**汙染整個 zone** 的攻擊過程，若需要也可搭配最多一張示意圖回答。汙染整個 zone 就是指其他人不管查 zone 的任何記錄，都會改為回覆攻擊者所指定的答案，而不是真實 zone 紀錄中正確的資訊（3 pts）。

2 Security

為了確保安全性，就像我們在 LAB 做的，我們應該設定 DNS 伺服器，使得 Recursive Query 只允許可信任的 IP 進行查詢。

1. 請問為什麼需要有這樣的要求？如果允許 Recursive Query 讓非信任的裝置使用，將會造成什麼額外風險？請用 10 句話以內解釋原因並舉例一個可能的具體攻擊過程，若需要也可搭配最多一張示意圖回答（3 pts）。
2. 雖然大多數 DNS 伺服器預設都會限制 Recursive Query 不可供任意 IP 使用，但為了確保安全性，在這題中請明確將 Recursive Query 設定為僅讓內網 IP 查詢。內網 IP 的定義，可以依據你對 VM 的網路配置選擇一個適當的網段作為代表（請列出步驟，1 pts）。

3 dnsdist（18 pts）

畢竟是大幅折價，大家迫不及待想購買便宜的水果而瘋狂人肉 DDoS ＣＳ貓的服務，若太多人使用而讓 DNS 服務卡住或壞掉害大家沒辦法買折價水果可不好，因此只有一台 DNS server 是不夠的！

dnsdist 正如其名，負責 **dist**ribute DNS 的 query，在這個小節中，我們將試著從頭架設一次 dnsdist 的服務。

1 Setting up dnsdist

1. 請在 port 53 設定 dnsdist ，將 query 自動（不限規則）分發至你的 PowerDNS Recursor 伺服器與 `8.8.8.8`，同樣只需安裝在同一台虛擬機即可（6 pts，需提供安裝及設定過程，最後請附上一張 `dig` 的截圖，說明他在 port 53 正常運作；按：通常我們會新增兩個自己的 Authoritive DNS 伺服器，但作為操作練習我們就設 Google DNS 作為第二台）。
2. DNS 有時會被拿來傳輸原先設計之外的資料，稱之為 DNS tunneling。這樣的做法有時是很好的變通方式，有時卻被用於惡意攻擊。老闆就懷疑競爭對手ＣＳ狗可能想透過 DNS tunneling 竊取公司機密，請針對以下三個需求，分別在 dnsdist 設立對應的規則來阻止攻擊（3 pts）：
   - 針對總長度超過 70 的 TXT record 進行過濾，超過則丟棄查詢不予回應。
   - 限制每個 IP 最多每秒可查詢 20 次，超過則丟棄查詢不予回應。
   - 針對所有對 `*.csdog.tw` 的 query 都丟棄查詢而不回應。

2 DNS-over-TLS

完成了基本的設定後，我們要為 dnsdist 設定 DNS-over-TLS。

1. 為什麼要設定 DNS-over-TLS 呢？請說明 DNS-over-TLS 解決了無加密的 DNS 的什麼問題（1 pts）？並且，請比較 DNS-over-HTTPS 與 DNS-over-TLS 在加密機制、效能、安全性的區別（1 pts）。
2. 接著，請你為你的 dnsdist 設定 DNS-over-TLS（DoT）（6 pts，需提供安裝及設定過程）。
   - **只**在 port 853 啟用 DoT。
   - 用 `openssl` 自己簽你的 TLS。
3. 請透過 `dig` 以 DoT 查詢 `cscat.tw` 來確認是否已正確設定（請提供截圖，1 pts）。

4 Master and Slave (9 pts)

從 load balancing 出發，你可能開始意識到了「備援」的重要性。從高可用性（High Availability）的角度，我們該如何確保服務的穩定性？

現在，帶著你幫ＣＳ貓的經驗回到 NASA，假設你成為 NTU CSIE 的網管，為系上管理 DNS 伺服器以及 `*.csie.ntu.edu.tw`，你可以如何整合我們在前面設定的各個服務建立一個完整、有備援機制的架構？

考慮你**可以**將多個服務重複設置在不同機器、這些機器**可以**被設置在不同地理位置，需要架設的服務包括 PowerDNS Authoritive、MariaDB、PowerDNS Admin、Recursor、dnsdist，但請依要求決定需要備援之範疇。我們不會依你提出的架構之真實可行性 (如各個地點是不是真的有辦法讓你裝服務等等) 決定評分，但請盡可能依你對系上和學校的認識進行發想。

1. 請用文字、表格或繪圖描述你的架構，該架構需達成在以下各個情況下都仍然能維持**所有人都能正常查詢系上各網站、系上師生都能用你的 DNS 往外搜尋**，並分項說明你的架構為何可以解決下列狀況（架構合理 2.5 pts、每個狀況之說明 1.5 pts）

   - 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？

2. 請描述 AXFR 與 IXFR 的差異，以及在前述架構中什麼時候要使用哪一種方法 (2pts)。