Homework #7

Due Time: 2018/6/17 (Sun.) 22:00

Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Compress all your files into a file named **HW7_[studentID].zip** (e.g. `HW7_bxx902xxx.zip`), which contains two folders named **[studentID]_NA** and **[studentID]_SA**.
- There should be a **na.pdf** in **Folder [studentID]_NA** containing all your answers in *Network Administration*.
- There should be a **sa.pdf** in **Folder [studentID]_SA** containing all your answers in *System Administration*.
- Submit your zip file to Ceiba.

Instructions and Announcements

- 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.
- Problems below will be related to the materials taught in the class and may be far beyond that. Try to search for additional information on the Internet and give a reasonable answer.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.
- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**

Network Administration

For each of the following task, your goal is to get the flag in the format of `NASA{flag_is_here}`. You'll have to provide:

1. The flag.
2. An explanation of how you have done it.
3. Your script (if you have one).

NOTE: **The files provided can be found here.**

1. Cryptolocker (10%)

My file was encrypted by cryptolocker...QAQ
Please help me to recover them!!!

- Decrypt `flag.encrypted` to get the flag.
- You can safely assume that `AESCipher.py` is secure, so focus on the implementation of `crytolocker.py`

2. 2AES (15%)

Here is a new cipher called `DoubleAES`, which encrypts the plaintext twice using 2 different keys. Since the key space is `2**46`, you'll not be able to break it unless you're super rich and have super powerful computer.

- Your goal is to find ??? of 2aes.txt
- You'll have to have `pycrypto` installed, use `pip install pycrypto` to install if you haven't.

Hint: You've probably heard of DES and 3DES, but have you ever wonder why there is no 2DES?

3. Man in the Middle 2 (25%)

You MitM me once. But you can't MitM me twice.
Service in on `linux13.csie.org:7122`. You can connect to it using `nc linux13.csie.org 7122`

- *Hint: Can we somehow guess the password?*

System Administration

1 Lab

在 docker 的實驗課時, 我們也曾在 centos 的環境下使用了 nginx, 並修改了它的 config 以實現 reverse proxy (e.g. localhost:8081 為 reverse proxy1)，使 curl localhost:8081/NASA/ 顯示了 http://web-app1/index.html 的內容。以此為前提，請回答以下問題。

1.1 概念解釋 (15%)

Note: 注意篇幅剪裁

1. 請解釋 proxy server 與 reverse proxy，並簡單舉例它們的用途。
2. 試比較 nginx 與 apache 兩種 web server 的優缺，並說明你認為何者更適用於 reverse proxy。

1.2 Apache (20% - 35%)

同樣在 centos 下，若以 apache 取代 nginx 作為 reverse proxy 所使用的 web server，請嘗試新增/修改 apache 的 config，以達成相同的效果。

Note:

1. 因應大家都辛苦撐到了期末，本題將實作當成 bonus，請視個人狀況完成。可以僅回答下方列出之 task，保證與 docker 完全無關。但完成 bonus 與否將有差別，請自行評估是否完成。
2. 若對以下兩點擇一實作並附上流程 (step by step) 都會視回答情況提供 bonus。
   - 使用 docker：在 docker 中 build 一個 image 作為使用 apache 的 reverse proxy，並達成與當時的 curl 一樣的成果
   - 使用本次上課之 vm: 題目略為改變, 需 copy 兩個 vm 分別模擬 reverse proxy1 與 web-app1, 並達成與當時的 curl 一樣的成果。
   - 補充：若可以的話請注意網路設定，展示主機無法直接碰到 web-app1，而要透過 reverse proxy1。
3. 為方便回答，對於沒有實作 bonus 的人，apache 假設與本次實驗課時產生之 `/etc/httpd` 一樣, 可藉此說明新增/修改了哪些部分；實作 bonus 的人若有不同則以實際情況為準。
4. 題目背景可參考 4/16 docker 講義 p11,23,25，若有需要可再自行參考其他頁數。

Task:

1. reverse proxy 會使用到 mod_proxy 與相關 module，無論預設環境是否有做好這件事，請明確寫出以保證你能使用到這些 module。作為提示，可在 `/etc/httpd` 之下找到相關的 conf。

2. 請描述新增/修改的部分，並解釋所使用到的 directive。

3. 將修改的內容成功套用到 apache 上。

2 Directive (15%)

```
Listen 80
<VirtualHost *:80>
    ServerName www.example.com
    # other directives
</VirtualHost>
```

上面為 Apache config 中 VirtualHost 的雛形，請使用適當的 directive 完成以下操作:

1. 將 `/var/www/html` 對應至網址中的 `http://www.example.com/`

2. 將 `/var/www/html/nasa` 這個 directory 設定為僅允許 `192.168.1.105` 存取，拒絕其他 ip (請避免使用舊版 apache 2.2 的 Allow, Deny)

3. 為了安全網站啓用了 https，需將 http 的使用者導向 `https://www.example.com/`