Homework #4

Release Time: 2021/03/29 (Mon.)
Last Update: 2021/04/14 (Wed.) 01:27
Due Time: 2021/04/25 (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 zip all the files, including one PDF and one xml file, name the zip file "`{your_student_id}.zip`", and submit it through NTU COOL. The zip file should not contain any other files, and the directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- {your_student_id}.xml
```

Grading

- NA accounts for 50 points while SA accounts for 50 points. The final score is the sum of 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 - Firewall

Short Answers (13 points)

1. (4%) 在 pfSense 防火牆 rule 的設定中，對封包的處置有 Block 跟 Reject 可以選擇。請說明兩者的差別，還有各自在什麼情況下較適合使用。
2. (4%) 在 pfSense 防火牆 rule 的設定中，Source 跟 Destination 選擇 “interface net” 和 “interface address” 的差別是什麼？
3. (5%) **4/14 Updated.** lab6 設定防火牆 rule 時，為了要允許 VLAN99 的機器可以 ping 到 VLAN5 的機器，我們只在 VLAN99 設了允許 ICMP 的 rule。仔細想想，當 echo request 從 VLAN99 到 VLAN5 時，會被我們設的 rule 給通過，但從 VLAN5 回到 VLAN99 的 echo reply 卻沒有 rule 來允許它通過。可是 ping 還是好好運作的啊，為什麼？(hint: what does “stateful firewall” means?)

pfSense (37 points)

安裝 pfSense 並設定他有兩個 VLAN interface: VLAN5, VLAN99。對於每一小題，請寫下你詳細的設定步驟。如果需要的話，你可以自己開其他虛擬機 (Ubuntu, Alpine, ...) 來做測試。

1. (4%) 設定 10.5.0.0/16, 192.168.99.0/24 給 VLAN5 和 VLAN99。
   - pfSense 作為這兩個 interface 的 DHCP server。
   - DHCP lease 需包含 8.8.8.8 和 8.8.4.4 這兩個 DNS server。
2. (5%) 設定以下的 alias：

Alias Name	Value
`GOOGLE_DNS`	8.8.8.8, 8.8.4.4
`ADMIN_PORTS`	22, 80, 443
`CSIE_WORKSTATIONS`	linux1.csie.org, linux2.csie.org, linux3.csie.org, linux4.csie.org, linux5.csie.org

3. (5%) 打開 pfSense 的 SSH 功能。設定只有 VLAN99 的機器可以透過 ADMIN_PORTS 連到 pfSense。
4. (5%) VLAN99 的機器只能存取以下的位址（或機器）：
   - `Google_DNS`。
   - 這台 pfSense。
   - VLAN5 的機器。
   - `CSIE_WORKSTATIONS`。
5. (5%) 所有非 VLAN99 的位址都不能連到 VLAN99 的位址。
6. (5%) 在 2021/05/11 整天，VLAN5 這個 interface 不能通過任何的封包。
7. (4%) 除了上述的 rule 之外，VLAN5 的機器可以連到所有位址。
8. (4%) 到 `Diagnostics > Backup & Restore` 中，點選 Download Configuration as XML 下載 config.xml，將檔名依照你的學號改成如 `b07902075.xml` 的檔名，連同作業 PDF 一起繳交。

入侵防火牆 (0 points)

防火牆身為我們私有網路的第一道防線，一定要謹慎地來進行設定，否則一旦被入侵，內部的網路就會受到相當大的威脅。在這部份，我們沒有要教你怎麼使用 Windows 7 作業系統的命令提示字元來入侵防火牆。

請自行參照 教學影片 來學習。

Figure 1: 破解防火牆需要一些時間

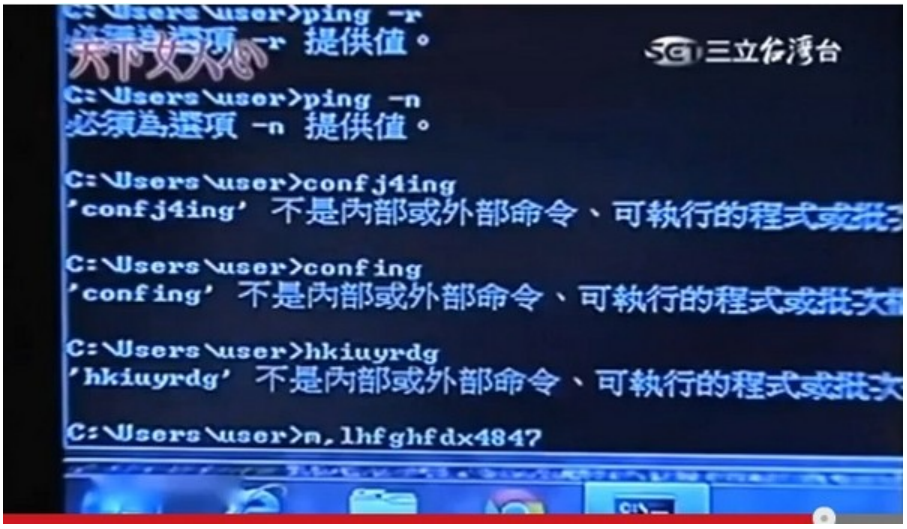

Figure 2: 宇宙的奧祕

Firewall TA: Good luck on midtern :)

System Administration

夢夢最近手頭吃緊，想要出租夢夢貼補家用。身為 NASA 的修課學生，夢夢很驕傲的在履歷上寫下夢夢是 NASA 一階的中堅份子，可以出租夢夢在系統管理方面的才能。這個漂亮的履歷也為夢夢找到一份薪水不錯的國小家教工作。然而開始上課後，夢夢發現這個小學生竟然正在學 Docker，他問的問題讓夢夢快要招架不住了。夢夢現在需要你的支援！

注意事項

- 夢夢需要知道你所有的步驟，你還要寫下使用的指令以及解釋。除非特別註明，未解釋者將扣部分分數。
- 請事先在自己的機器安裝 Docker，可以參考 https://docs.docker.com/get-started/
- 請在 Dockerhub 註冊一個帳號。

1. 關於 Container (8%)

1. 請列出：4 個使用 Container 的時機 (1%) 3 個使用 VM 而非 Container 的時機 (1%)
2. 何為 OCI(Open Container Initiative) 與 CRI(Container Runtime Interface)？它們與 Docker 之間的關係是什麼？(2%)
3. 承上題，請介紹一種 Docker 以外的 Container Runtime，並列出 3 個他們的不同之處與 3 個他們的共通點 (2%)
4. 承上題，請在你的電腦安裝你所選的 Container Runtime，並執行一個使用 nginx:1.19.2 這個 image 的 container。請附上指令、解釋與成功的截圖 (2%)

2. Docker Basics (8%)

以下作答記得附上指令與解釋。

1. 用一個指令停下所有的 container (1%)
2. 用一個指令刪除所有的 image (1%)
3. 用一個指令刪除所有未被使用的資源，包含 containers, networks, images 與 volume (1%)
4. 用一個指令列出一個 container 的 IP (假設 Container ID 為 5b0f1ed0dcb8) (1%)
5. 即時查看當前所有 Container 的 CPU 與 Memory (1%)
6. 使用 docker run 在背景執行一個使用 nginx:1.19.2 這個 image 的 container，並將其命名為 nginx-1。另外，你必須可以從本機的 port 5678 訪問到此 container。請附上指令、解釋與成功的截圖 (1%) (Hint: port-forward)
7. 承上題，請使用 Docker 的指令登入 nginx-1 的 terminal，並附上指令、解釋與成功的截圖 (1%)
8. 承上題，請問如何使用 Docker 的指令，在不登入 nginx-1 的 terminal 的前提下查看位於 /etc/nginx/nginx.conf 的檔案內容？請附上指令、解釋與成功的截圖 (1%)

3. Docker Network (5%)

1. 請問 Docker 預設有哪幾種 Network 模式？請解釋每種模式的特性與給出各一個使用時機 (2%)
2. 上一大題中你啟動了一個叫做 nginx-1 的 container，現在請你啟動另一個使用同樣 image 但名為 nginx-2 的 container，接著使用 bridge 模式創造一個名為 nasa-net 的 network，最後將 nasa-1 與 nasa-2 都連接到這個 network 上。請附上指令的步驟與解釋，並各別在 nasa-1 與 nasa-2 內 ping 對方，最後將成功的畫面截圖 (總共兩張截圖) (2%)

   Note: 在連接 network 時，不得停止 nginx-1，而 nginx-2 則沒有這個限制。
3. 請找出在 Docker engine 的網路中 Host machine 的 IP。請附上指令與解釋 (1%)

4. Build Application (updated: 04/08) (9%)

1. 撰寫 Dockerfile 時，我們需要為程式設定進入點。請列出 3 個使用 ENTRYPOINT 與 CMD 的差異，並舉一個同時使用它們兩者的例子。你的答案必須附上一個完整的 Dockerfile (2%)
2. 什麼是 Docker-Compose？它與 Docker 的差別為何？(1%)
3. 現在有以下兩個用 docker run 執行的服務：

```
dreamdream@nasa [~] docker run -p 3000:3000 \
>   -w /app -v ${PWD}:/app \
>   --network nasa-net \
>   -e MYSQL_HOST=mysql \
>   -e MYSQL_USER=root \
>   -e MYSQL_PASSWORD=secret \
>   node:12-alpine \
>   sh -c "echo helloworld"
dreamdream@nasa [~] docker run \
>   --network nasa-net \
>   -v mysql-data:/var/lib/mysql \
>   -e MYSQL_ROOT_PASSWORD=secret \
>   mysql:5.7
```

   請解釋上述兩個指令的參數各別代表的意思，接著使用一個 docker-compose 檔封裝兩個服務並執行它們。答案需要附上完整的 docker-compose 檔案與執行結果的截圖 (3%)
4. 請給出以下 docker-compose 相關操作的指令 (3%)
   (a) 在背景啟動所有服務 (1%)
   (b) 暫停所有服務 (1%)
   (c) 刪除所有服務、network 與 volume (1%)

5. Docker in Docker (8%)

Docker 裡面可以執行另一個 Docker，這在 CI (Continuous Integration) 環境十分常見。請幫助夢夢完成以下任務：

1. 以 ubuntu:18.04 為 base image 撰寫一個 Dockerfile，其中需包含安裝 Docker 與其相關套件的指令，並使用 docker run hello-world 作為進入點 (4%)
2. 承上題，請使用 docker build 打包你的程式，並附上你的指令與解釋 (1%)
3. 承上題，請使用 docker run 啟動你打包好的程式，並附上指令、解釋與成功的截圖 (1%)
4. 承上題，請將你的 image 發布到 Dockerhub 上，image 取名為 dind-nasa-hw4，且必須附上 v1.0.0 的版本號。請附上指令、解釋與成功發布到 Dockerhub 上的截圖 (2%)

6. Docker & Distributed System (12%)

由於需要管理出租夢夢的粉專、回覆留言、宣揚社工價值與讚美他人，夢夢決定自行開發一個後台管理兼募資平台。然而蜂擁而至的捐款讓網站的流量激增，夢夢快要受不了了！請幫助夢夢水平擴展他的網站，將單機的 Docker 服務分布到多台機器上，以分散龐大的流量。

1. Docker 的 swarm mode 可以讓一群運行著 Docker 的機器互相溝通，構成一個運算叢集。這讓一個服務可以 scale 到多台機器上，達到負載均衡與高可用的效果。請畫一張系統架構圖簡述 Docker Swarm 的架構，並說明每一種 node 角色的作用、node 之間如何保持高可用、以及服務之間是如何找到彼此的 (關鍵字：service discovery) (5%)
2. 請依照下列步驟建立一個 3 個 node 的 Docker Swarm 叢集，並運行服務 (7%)
   (a) 建立三台網路互通的 linux VM，並分別在上面安裝與運行 Docker (0%)
   (b) 建立 Docker Swarm 叢集，請設定其中一台為 manager node，另外兩台為 worker node。請提供你的指令步驟與解釋，並截圖最後的 cluster node 狀態 (Hint：docker node ls) (2%)
   (c) 將一台 node 加上一個名為 db 的 label，其他兩台則加上 web 的 label。請使用 docker node inspect 指令列出各 node 的 label，並將結果截圖 (1%)
   (d) 按照以下規則撰寫一個 docker-compose 檔，並以 docker stack 指令部署服務。請提供你部署服務的完整指令，最後用 docker stack 列出所有成功執行的服務並截圖 (4%)
      i. 部署一個 mysql:5.7 到有 db label 的 node 上，並將 mysql 的 /var/lib/mysql 資料夾掛載到該 node 的 /data 下
      ii. 部署兩個 nginx:1.19.2 的 replicas 到有 web label 的 node 上