Linux鑑識分析

|  |  |  |
| --- | --- | --- |
| 題目描述 | 某機關制定資安政策來規範員工，本案例是針對可疑的使用者活動違背機關資安政策的鑑識情境。 | |
| 目的 | 熟悉Linux 鑑識分析技術 | |
| 對象 | 學員 | |
| 先備知識 | Linux作業系統 | |
| 範圍 | 第五單元(Linux系統鑑識實務) | |
| 時數 | 50分鐘 | |
| 實作流程 | 講師說明 | 5分鐘 |
| 學員實作練習 | 35分鐘 |
| 講師總結 | 10分鐘 |

### 2.6.1.實作內容：

* 鑑識問題:
  + 問題1:這台機器上使用的是哪個 Linux 發行版？
  + 問題2: apache access.log 的 MD5 值是什麼？
  + 問題3:根據專家經驗有可能已經下載了憑證轉儲(credential dumping )工具？下載的檔案名稱是什麼？
  + 問題4:使用者創建了一個 supersecret.txt，此檔案的絕對路徑是什麼？
  + 問題5:在執行過程中哪個程式使用了 didyouthinkwedmakeiteasy.jpg？
  + 問題6:這台機器似乎被用來攻擊另一台機器，什麼文件可以證明這一點？
  + 問題7:有一位使用者在 11:26 多次 su root。他是誰？

### 

### 測試樣本:

### Hocrux.E01 來自Def Con 2019 (Linux Forensics)

### 檔案下載:

### <https://www.dropbox.com/sh/4qfk1miauqbvqst/AAAVCI1G8Sc8xMoqK_TtmSbia?dl=0>

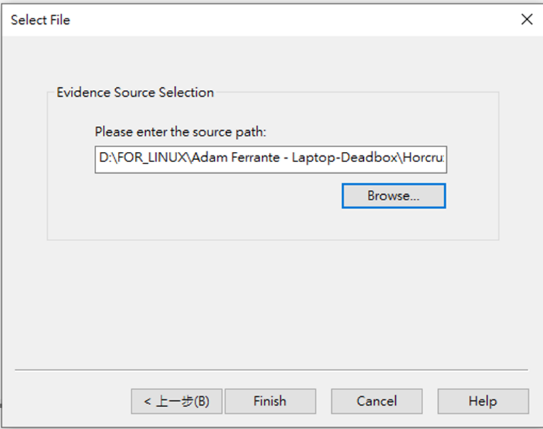
### 鑑識工具:FTK Imager

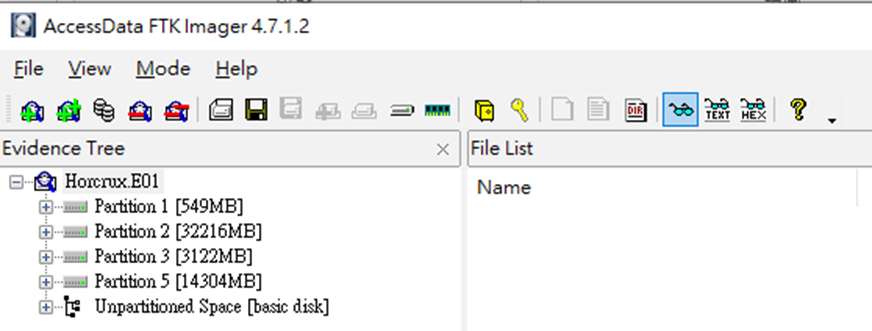
### 參考解答: <https://www.jaiminton.com/Defcon/DFIR-2019/#category-linux-forensics>

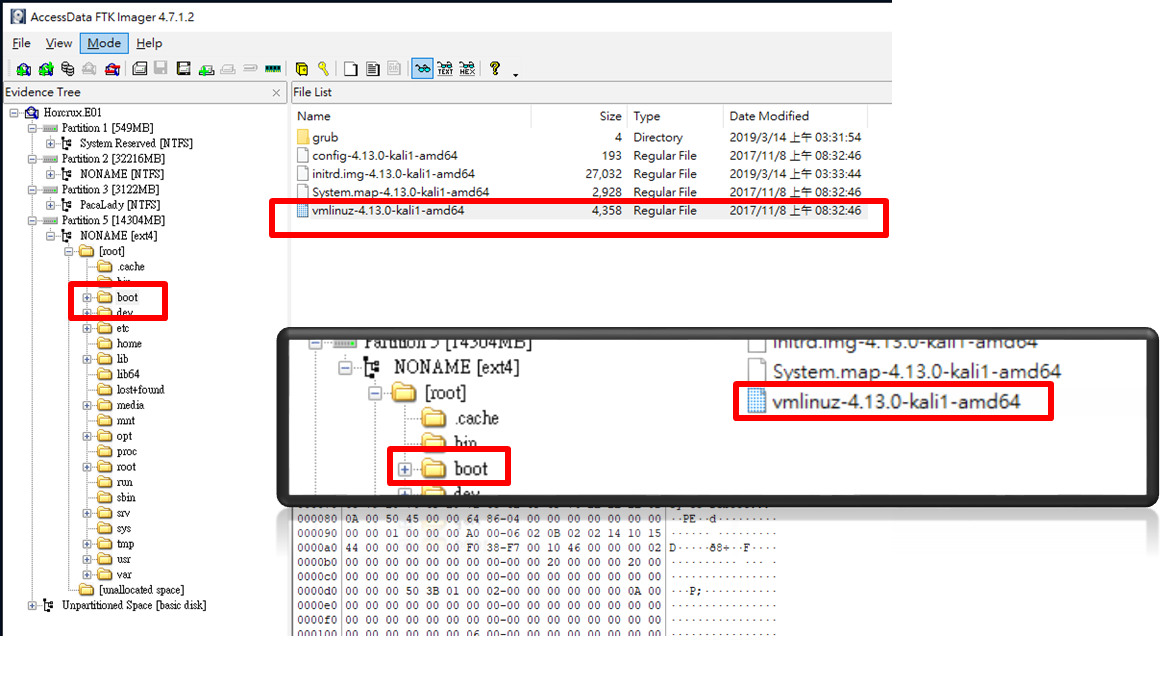
### 鑑識分析:

### 步驟1: 開啟FTK Imager，點選Add Evidence Item

### 步驟2:在Select Source 點選Image File

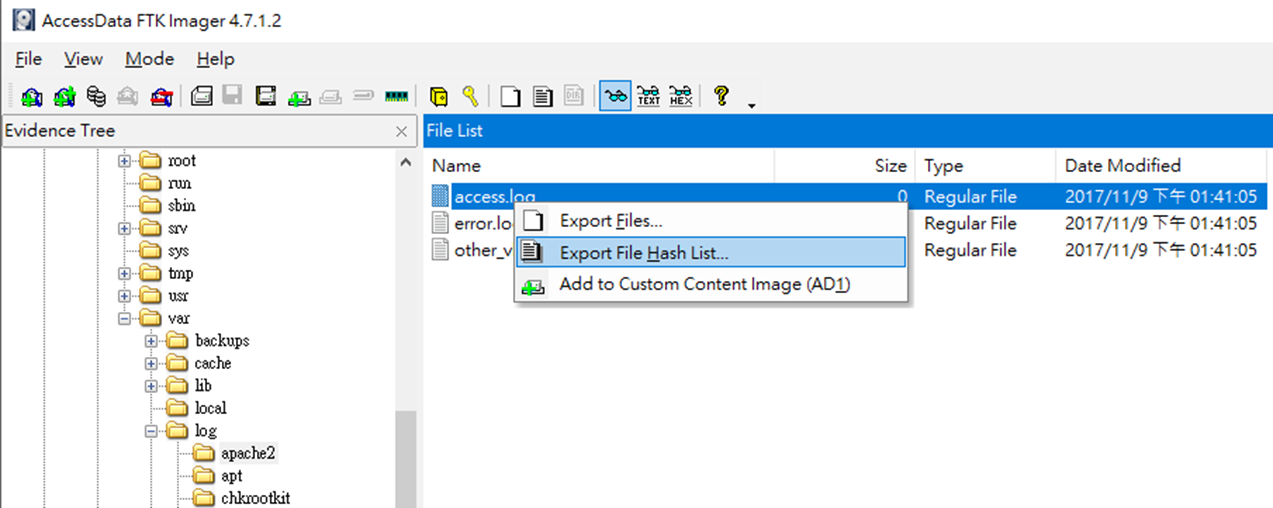
* + 步驟3: 在Select File點選Browse將檔案載入

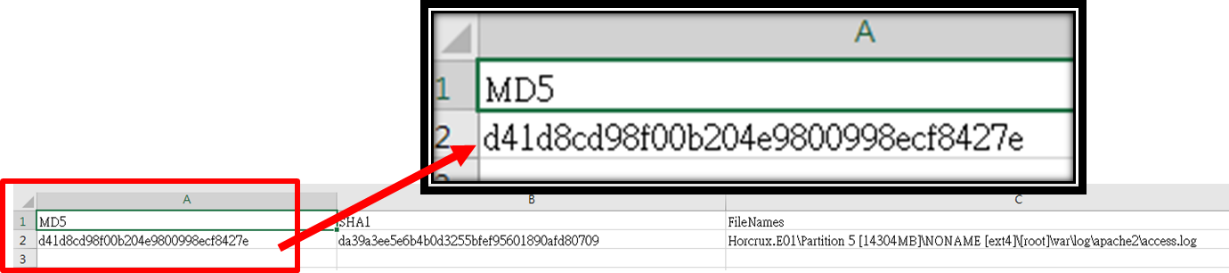
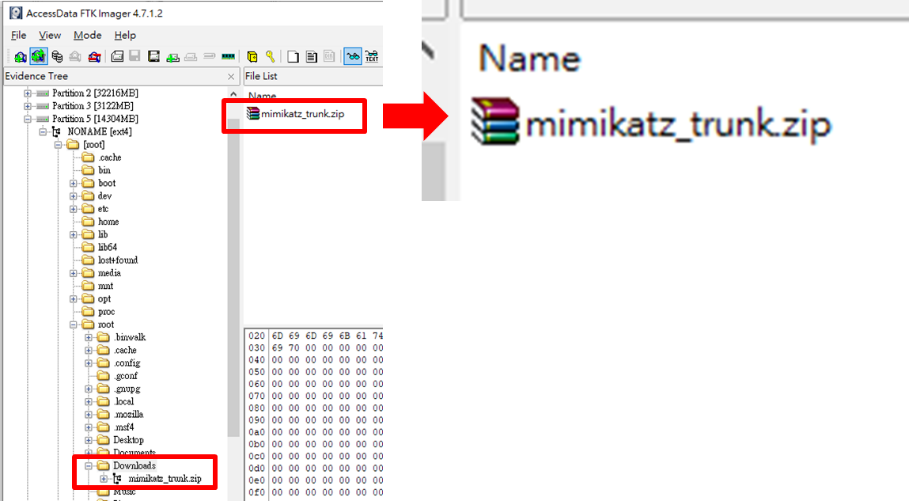
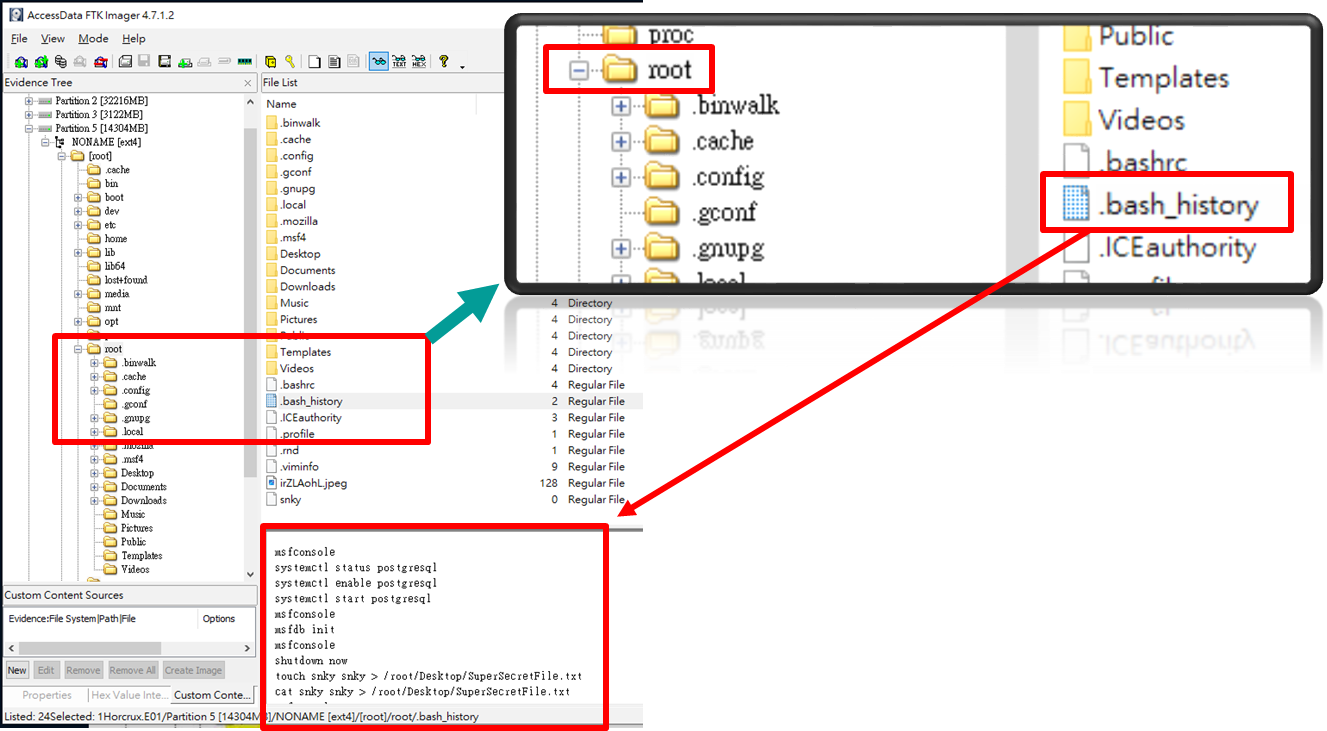
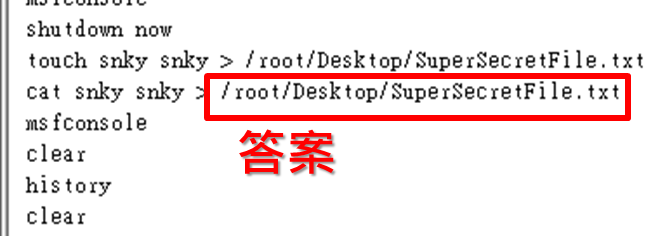


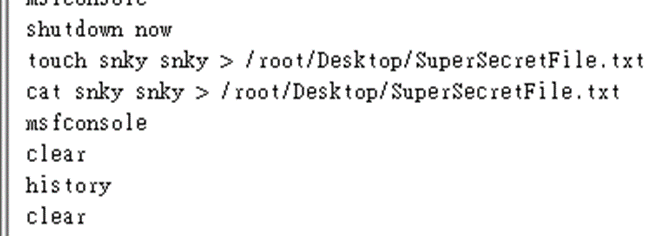
* 問題1:這台機器上使用的是哪個 Linux 發行版？
  + 使用FTK Imager可看到Partition 5是一個Linux Partition，再從boot部分顯示示它是Kali Linux

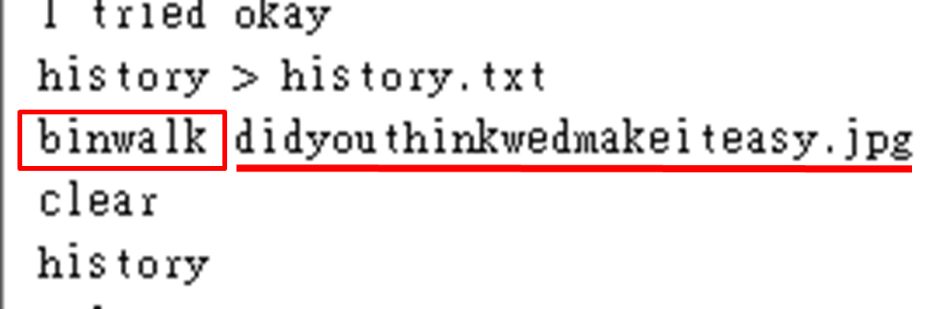
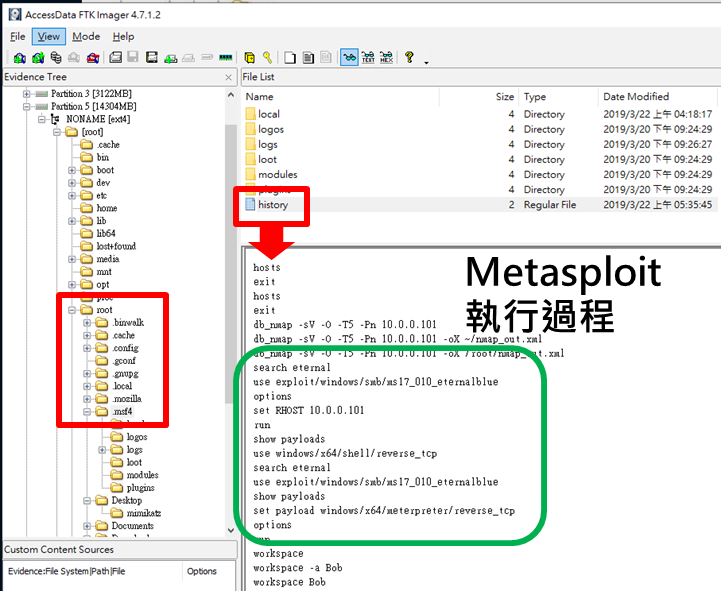
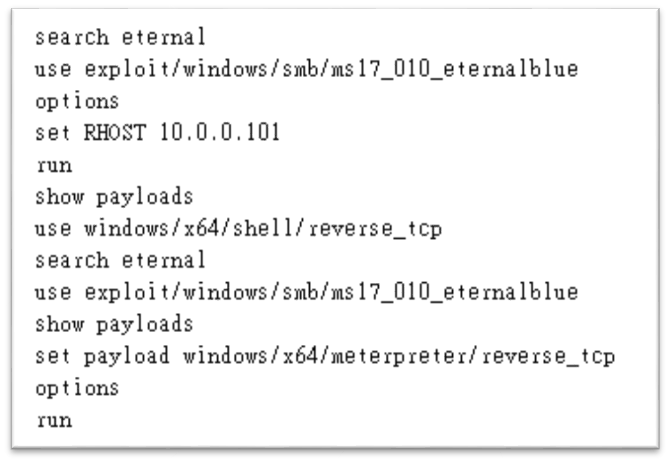
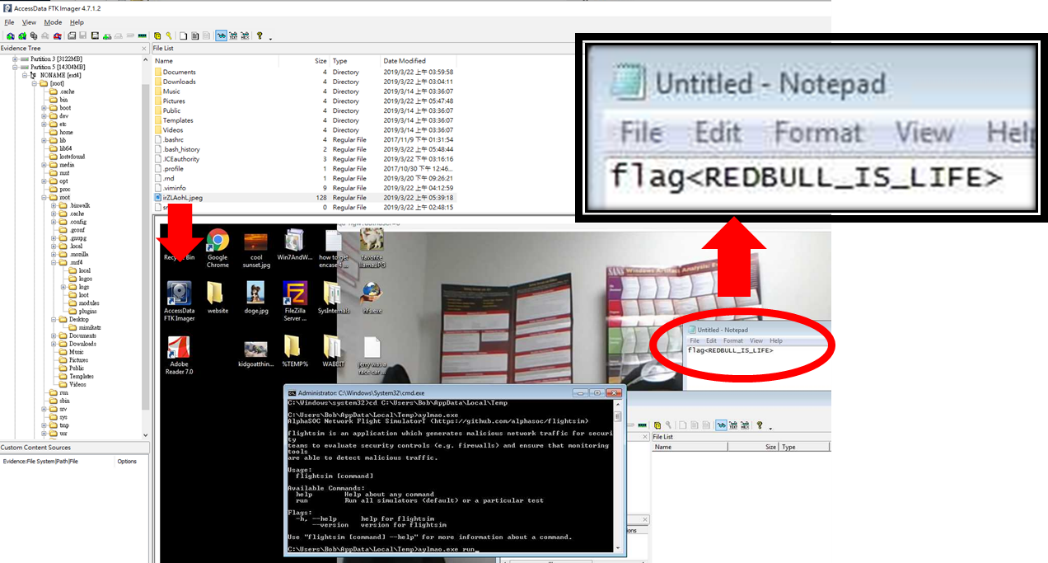
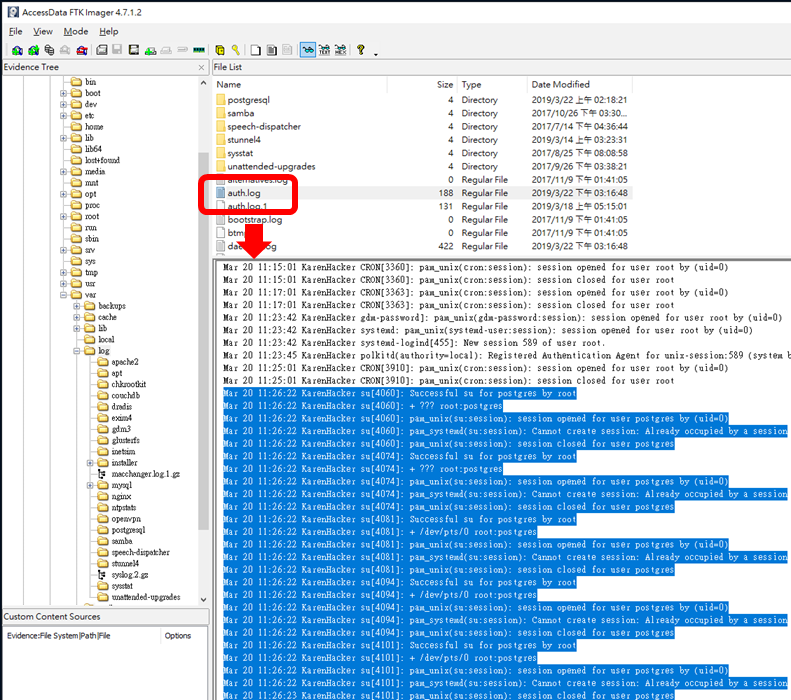
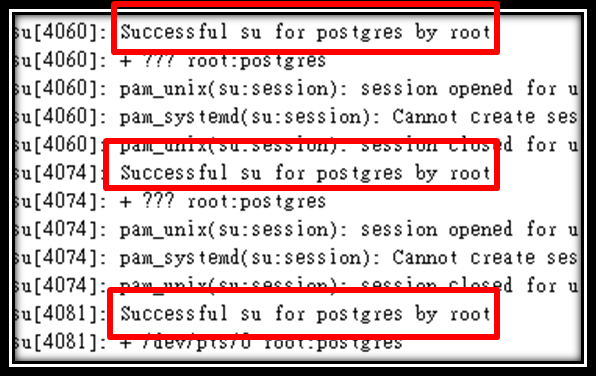
答案: Kali Linux

* 問題2: apache access.log 的 MD5 值是什麼？
  + apache access.log位於 /var/log/apache2/access.log



* + 在檔案按滑鼠右鍵並選擇 Export File Hash List1(將檔案存成hash.csv)
  + 打開此hash.csv檔案即可見到MD5值
* 問題3:根據專家經驗有可能已經下載了憑證轉儲(credential dumping )工具？下載的檔案名稱是什麼？
  + 檢視Kali | root | Downloads
  + 答案:mimikatz\_trunk.zip
* 問題4: 使用者創建了一個 supersecret.txt，此檔案的絕對路徑是什麼？
  + 建立檔案的動作會記錄在root/.bash\_history
  + 檢視root/.bash\_history會發現
  + 仔細往下查看即可發現到答案



* 問題5:在執行過程中哪個程式使用了 didyouthinkwedmakeiteasy.jpg？
  + 同上題作法:持續檢查root/.bash\_history會發現是binwalk
  + 答案:binwalk
* 問題6:這台機器似乎被用來攻擊另一台機器，什麼文件可以證明這一點？
  + Kali Linux最著名的攻擊框架是Metasploit
  + 檢查Metasploit 執行歷史== > root/.msf4/history
  + 這是針對Windows作業系統著名的ms17-010攻擊(EeternalBlue攻擊)
  + 上述的分析有可能被駭客竄改,無法明確斷定 !
  + 所以另找其他佐證資料:
  + 發現root目錄底下有一jpeg檔案(irZLAohL.jpeg)是螢幕截圖 可找到
  + 答案: irZLAohL.jpeg
  + 註:此練習是改自CTF競賽，因此是根據部分暗示(題目會提示有一檔案有flag)來解題
* 問題7:有一位使用者在 11:26 多次 su root。他是誰？
  + su root 會記錄在/var/log/auth.log
  + 仔細檢視就會發現
  + 答案:postgres