實作練習:配置無線環境

## 實作目的

建立之後可以使用的工作環境。

## 實作配備

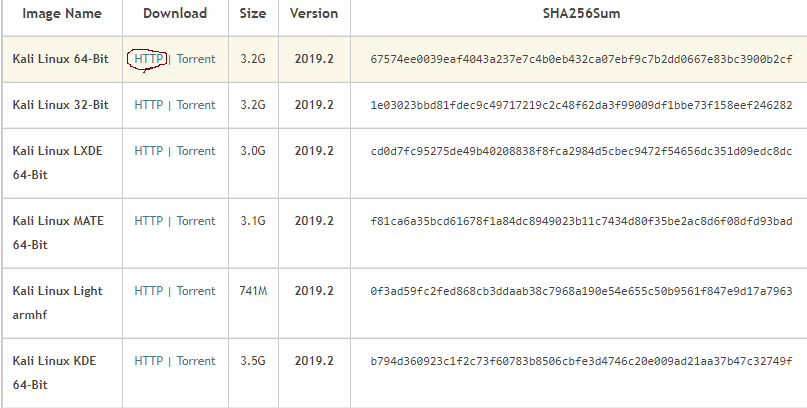
1台電腦

1張無線網卡

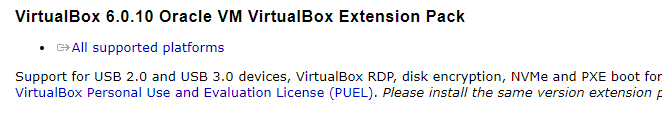
## 實作步驟

Step1:去網路上把我們需要的資源下載下來

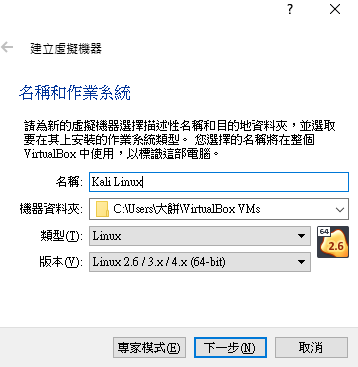
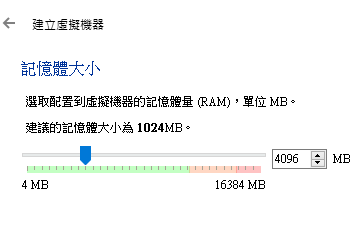
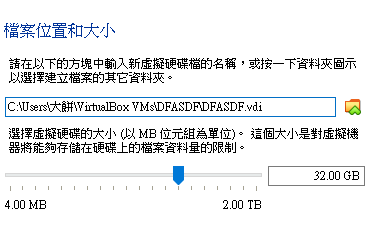
* 去Kali Linux官網下載Kali Linux的ISO檔



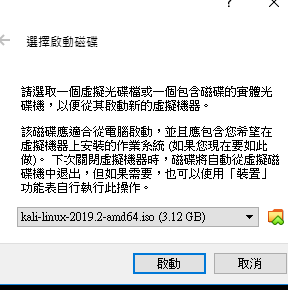
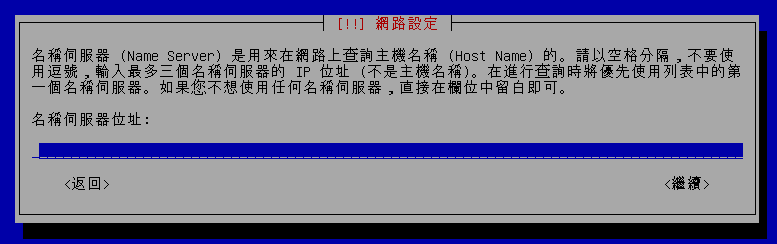
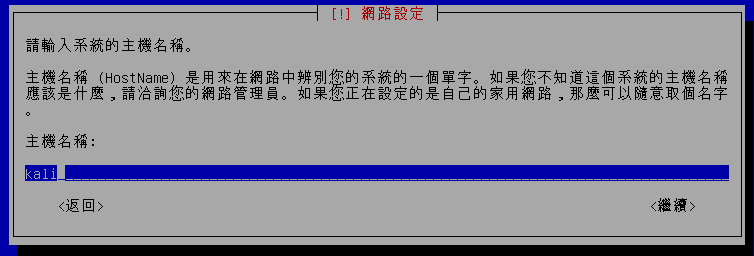
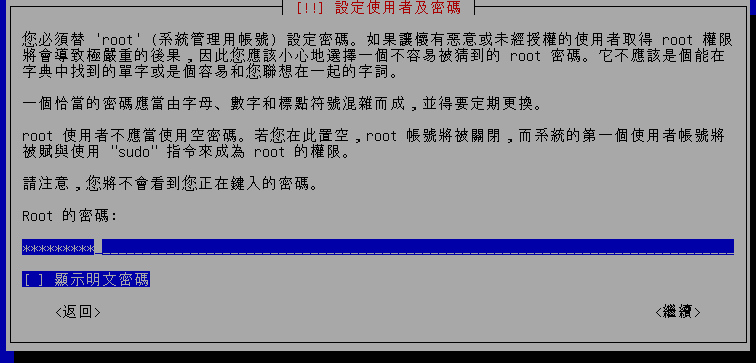
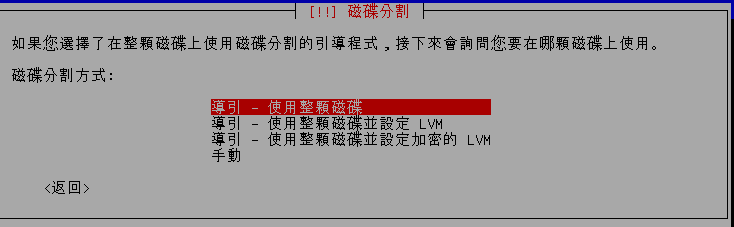
* 去Oracle VM VirtualBox下載虛擬機
* 之後往下拉下載Extension Pack，這樣我們網卡才能使用

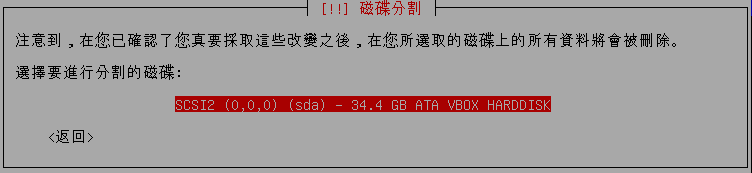
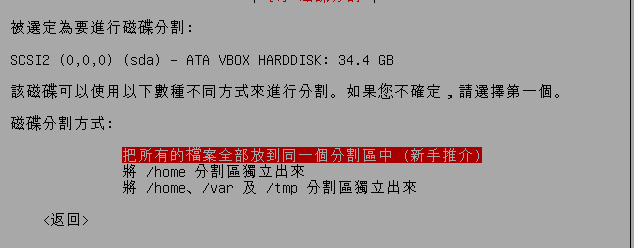


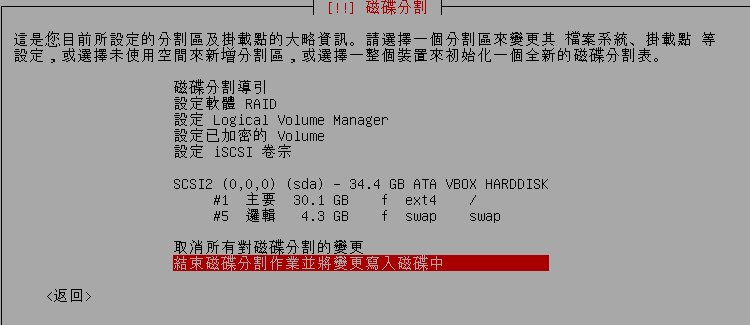
Step2:安裝虛擬主機

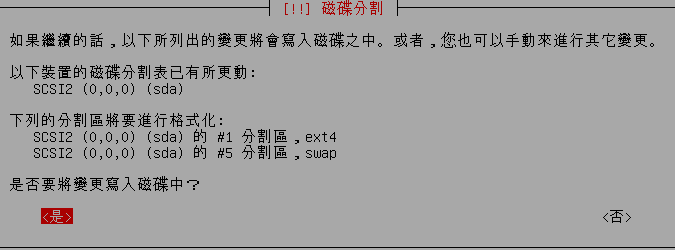
* 先設定名稱  
  
* 記憶體大小攻擊機至少3G靶機至少1G  
  
* 硬碟大小大約給個32G，太小作業系統會裝不進去  
  
* 點設定->USB把無線網卡用進去  
  

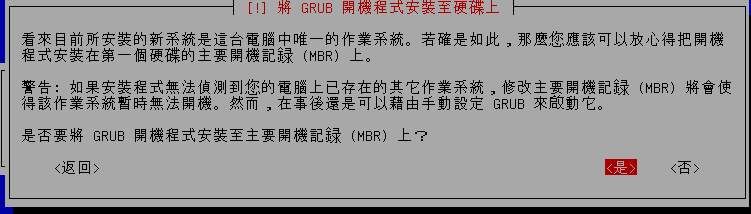
Step3:安裝Kali Linux

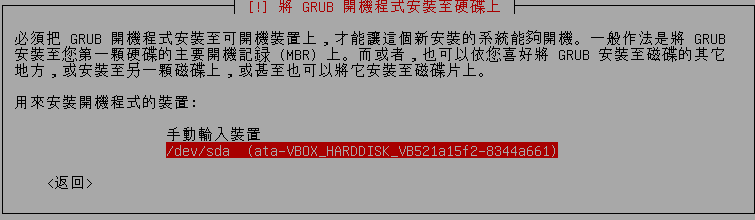
* 選擇剛剛下載的Kali Linux的iso檔案  
  
* 選擇安裝  
  
* 選擇語言完後，這網路設定可以留白  
  
* 設定使用者名稱  
  
* 設定最高權限者(root)的密碼  
  
* 之後是分割磁碟，如果不會跟著導引走就行  
  

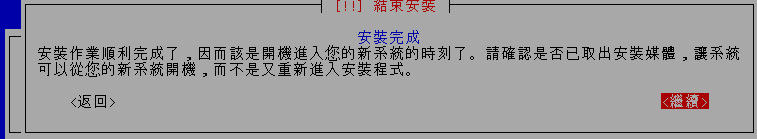
  




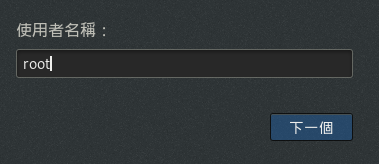




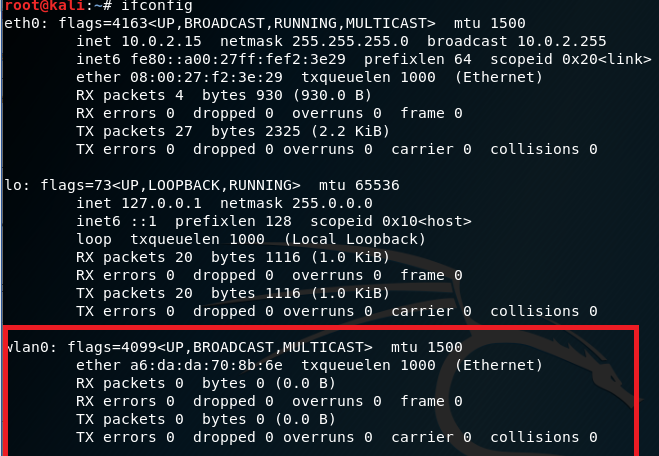




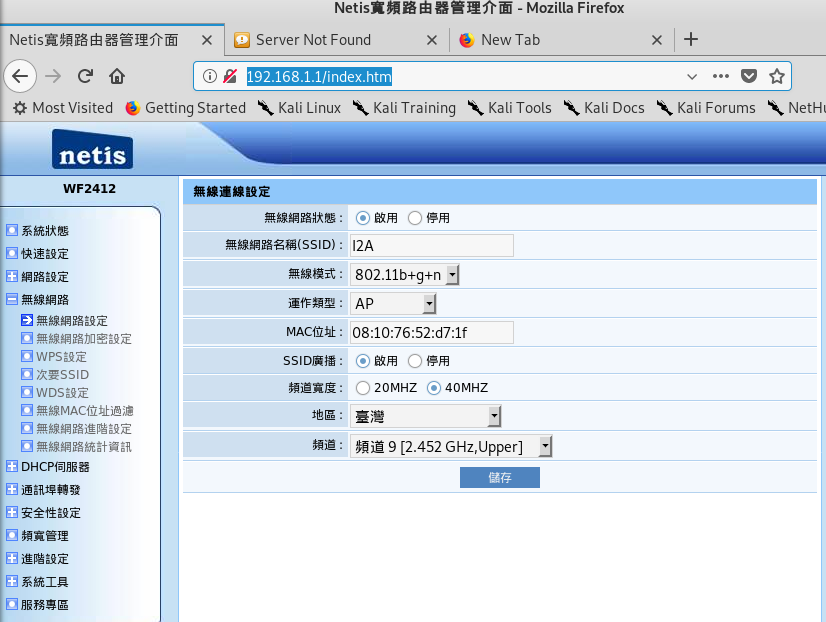
到了這步驟就是安裝完成了!

* 接著登入虛擬機，先使用root帳號進入，密碼是剛剛設定的。  
  
* 進入畫面成功會是這樣  
  

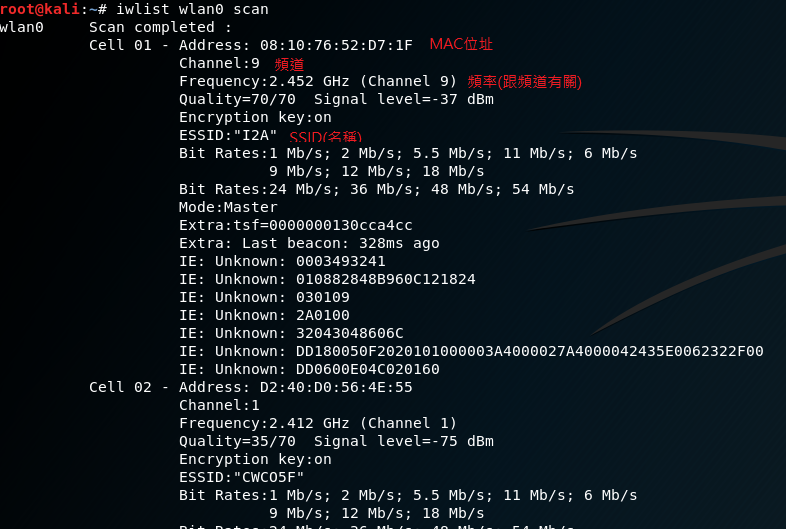
Step4:確認無線網卡是否有成功安裝

* 接著打ifconfig看看網卡有沒有成功安裝，沒有的話打ifconfig wlan0 up開啟

Step5:設定AP

* 先連上我們設定的WIFI，並且點開(Kali Linux的瀏覽器)，並且打192.168.1.1。SSID為WIFI名稱，之後幾次攻擊會使用到，現在可以先更改，之後再用手機看有沒有把名稱更改。  
  

Step6:將我們的裝置連線到無線網路

* 先使用iwlist wlan0 scan尋找我們要的wifi 
* 接著連到網路打nmcli dev wifi connect 網路名稱 password 密碼，如果沒有密碼可以把password之後不打。接著看到右上有 這樣就完成了。

## 結語

第一次做的話可能會很挫折，虛擬機部分可能會有點問題，如果做照做還是不能的話多插拔網卡的話就可以用了。

# 問題與解答

Q1.

無線網卡沒抓到

A1.

以筆者的經驗可以分成下面幾種。

1. kali啟動時未將此網卡開啟

利用ifconfig此指令將想要的網卡開啟

Ex. Ifconfig <網卡介面名稱> up

2. 開機後將網卡拔開之後裝上又或者是跟開機後才將網卡插上

則跟A1的1解答一樣

3. 沒有裝網卡的驅動程式

在本次實驗中，筆者只接觸了AWUS036NH與AWUS036ACH這兩款可以用作側錄周遭無線網路環境中的封包，而在這次的實驗中， KALI本身就有AWUS036NH的驅動程式但是沒有AWUS036ACH的驅動程式，所以就要自行去網路上找此裝置相對應作業系統的驅動程式。如果讀者們所持有的網卡是後者的話，可以照著下面的步驟做。

Step1. 前往<https://store.rokland.com/>此網站點擊圖1中的support，如果沒有support的話則有可能是頁面縮小的原因(筆者所遇到的情況

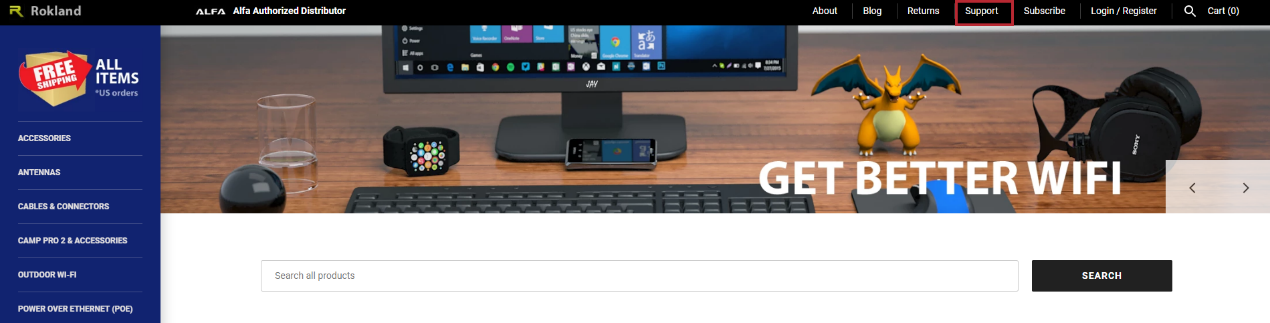


圖1

Step2. 點擊圖2中所框起來的

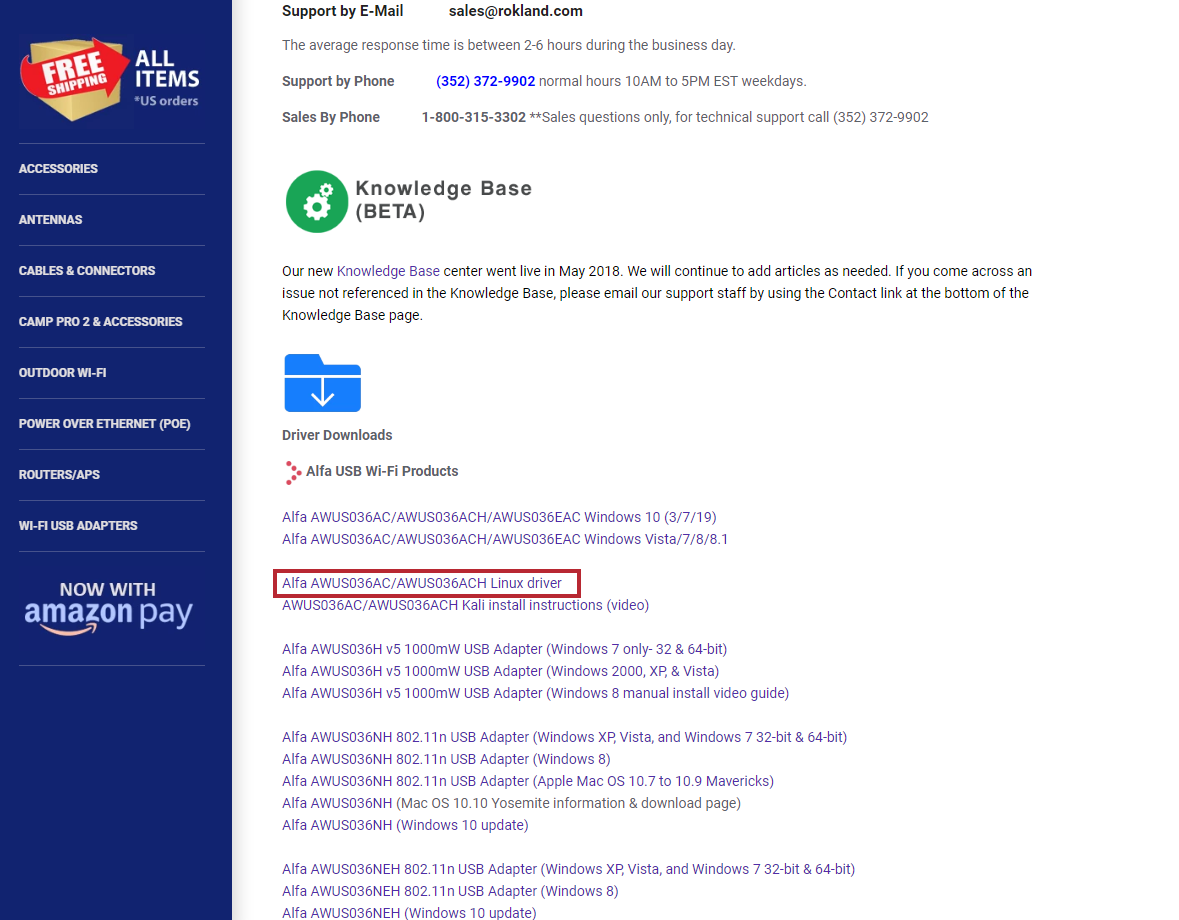


圖2

Step3. 圖3為驅動程式所在的網頁，而這網頁之中的所有資料，則是一個資料庫，我們則是要將此資料庫下載下來。

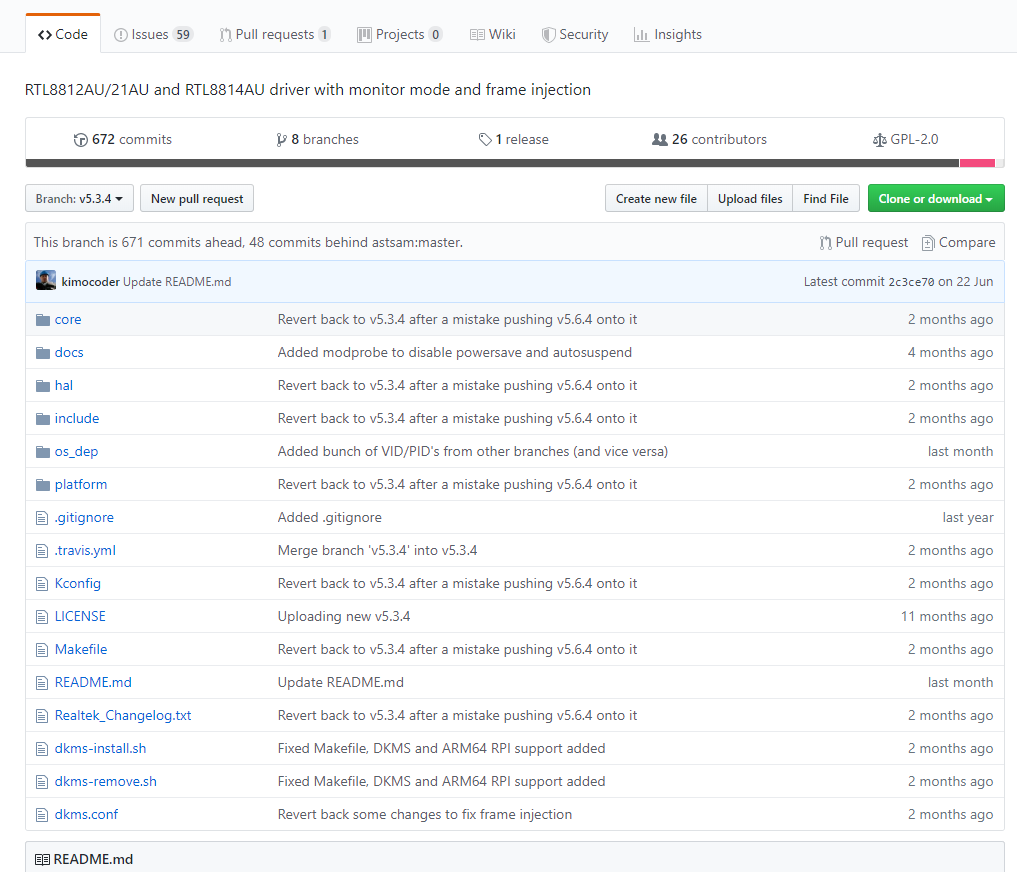


圖3

在這裡筆者提供兩種方法

1. 利用git 指令將此資料庫下載下來 (如果讀者沒有git指令的話可以參閱Q2來下載git)

* 點擊圖4中紅框的地方
* 在kali的terminal上打git clone <網址> 這裡的網址就是點擊後出現的網址
* 完整指令為 git clone https://github.com/aircrack-ng/rtl8812au

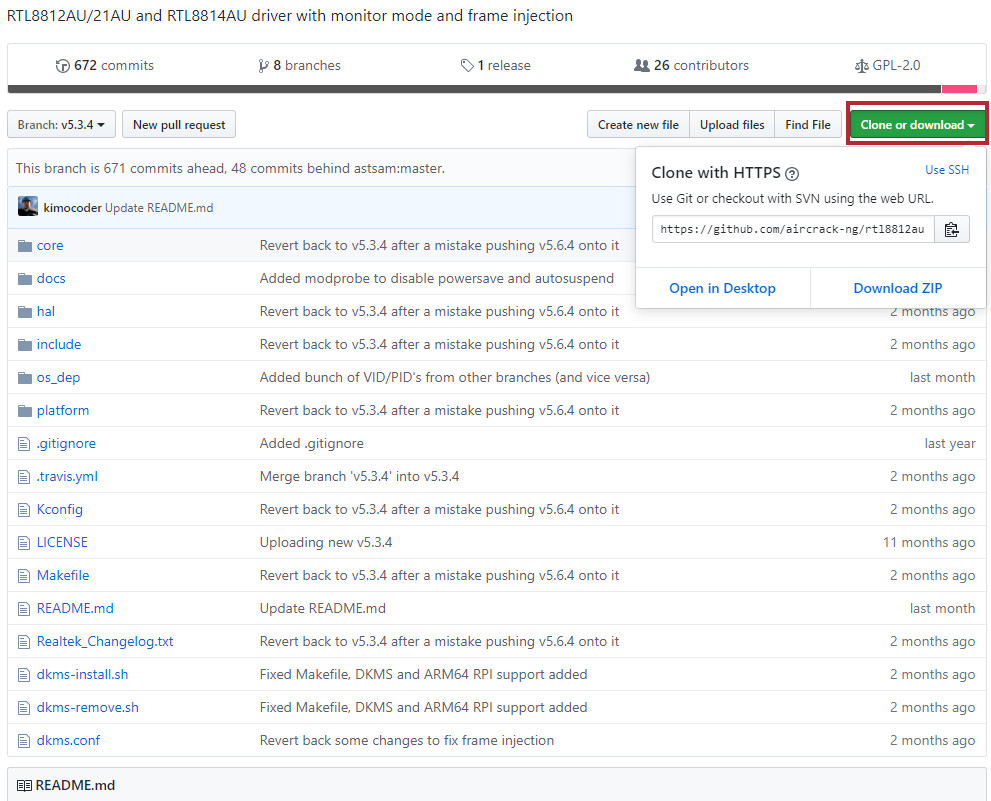


圖4

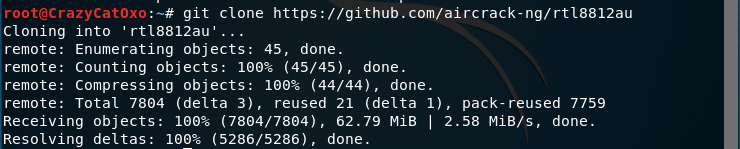


圖5

* 圖5為成功將驅動程式所在的資料庫下載下來，在圖5中的的2行可以看到我們所下載下來的資料庫其資料夾的名稱為rtl8812au



圖6

1. 直接開啟KALI的瀏覽器登入到圖4中的網頁



圖7

* 點擊圖7中所標示的圖示，此為本次KALI附有的瀏覽器(如果讀者無法上網的話請參閱Q3)

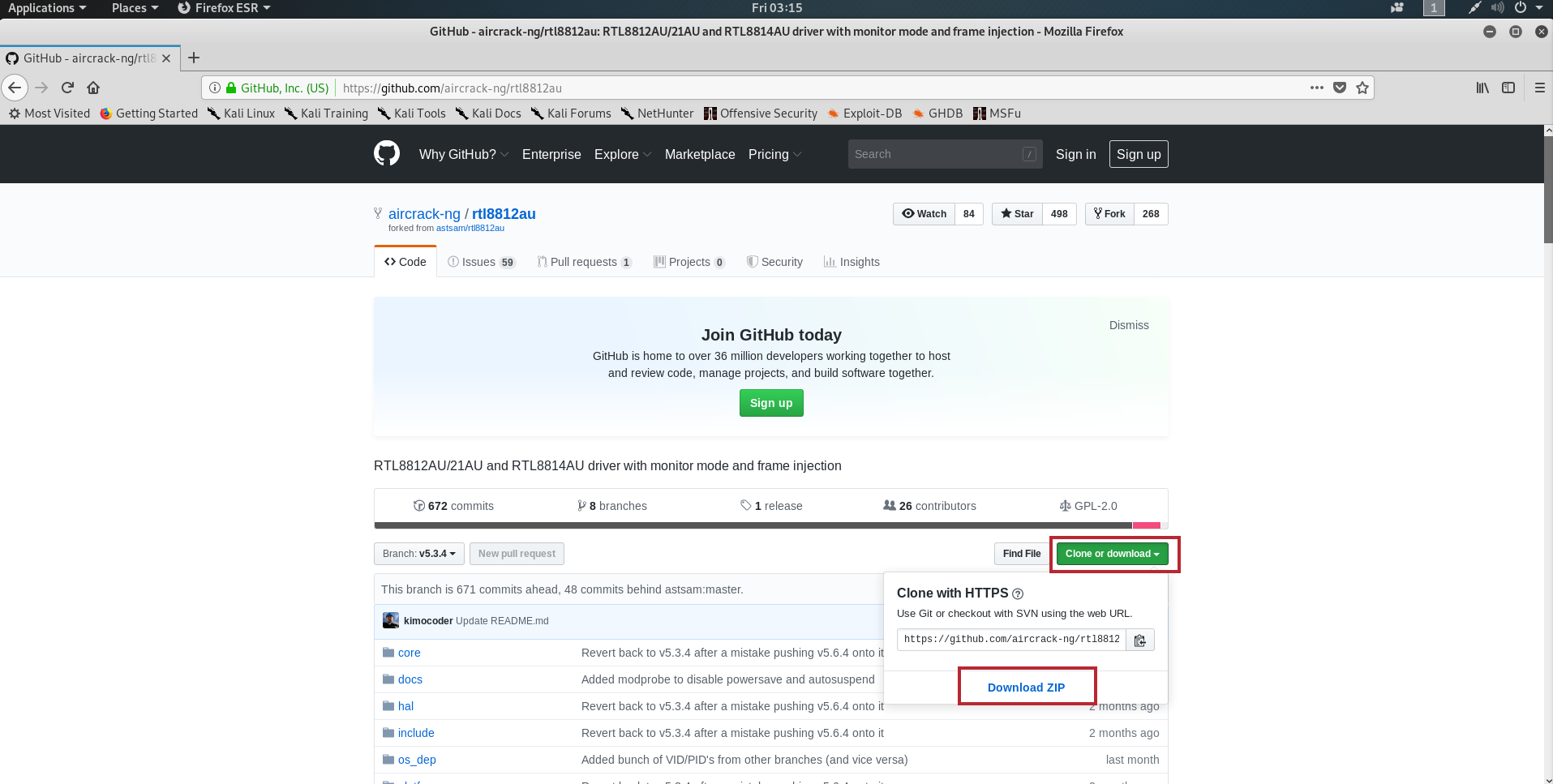


圖8

* 到達目的地網站後點擊圖8的Clone or download，之後再點擊Download ZIP

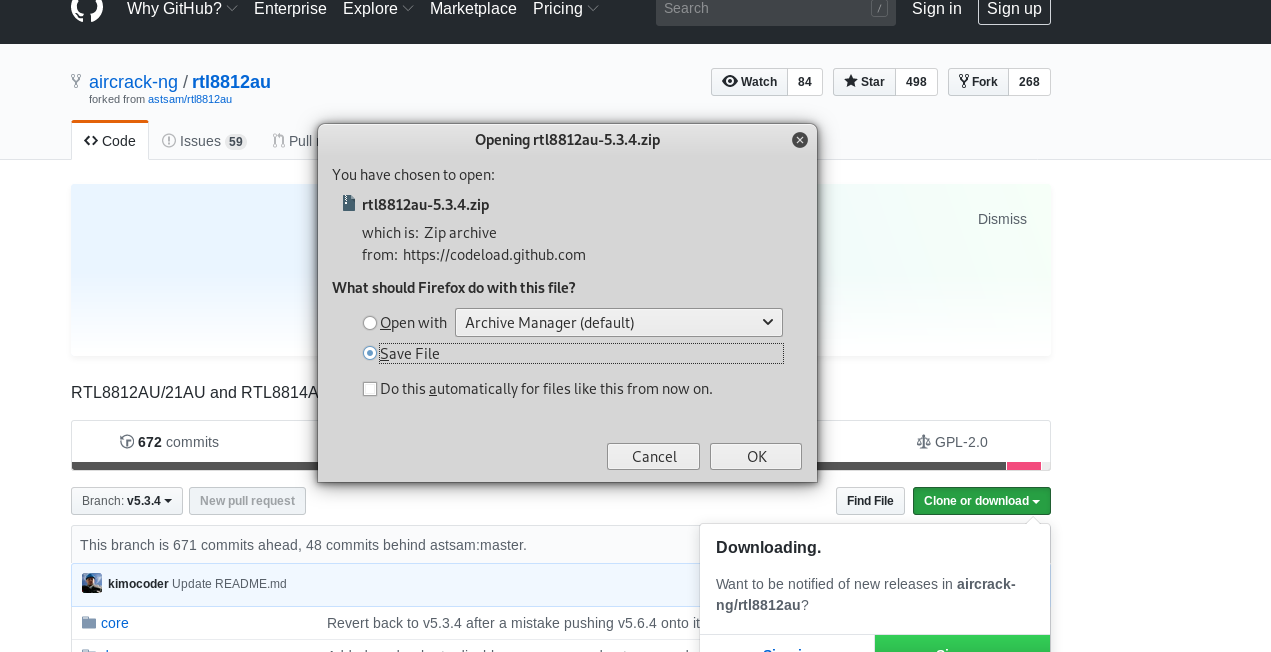


圖9

* 之後會跳出圖9的訊息視窗，然後點Save File再來點OK。
* 下載好後，會預設將下載的檔案放到使用者其家目錄中的的Downloads資料夾。
* 筆者目前在KALI中所用的帳號為root (root預設上為擁有最大權限的帳號)，root的家目錄會在/root這個絕對路徑上，

如果是之後新創的帳號，其家目錄預設上則會在/home/<你的帳號>這個絕對路徑上。

* 如果讀者不知道自己的所在位置可以打 pwd，顯示目前的所在位置。

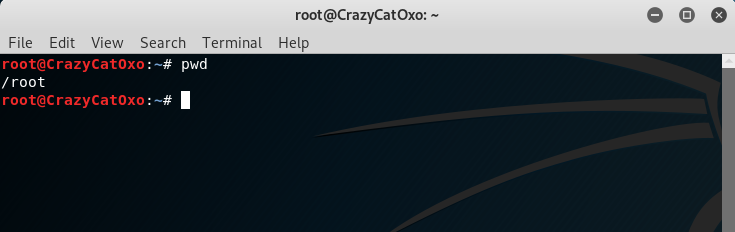


圖10

* 如果讀者所在的位置不在自己的家目錄的話可以打 cd ~ 到自己的家目錄。(這裡的~是一個變數，此變數儲存著目前帳號家目錄的絕對路徑，cd 則是change directory的縮寫，此指令用來改變目前所在的位置)

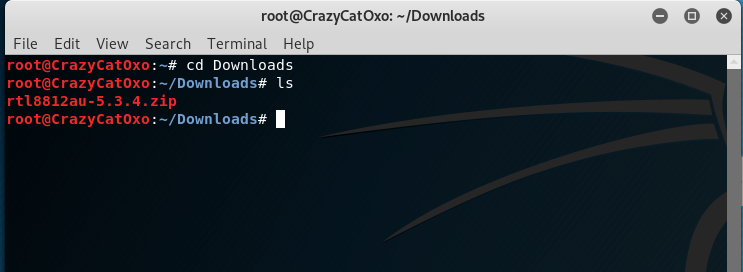


圖11

* 筆者在灌KALI時，設定的語言為英文所以筆者的資料夾都會是以英文來顯示，如果讀者所選的語言跟筆者的不一樣，就以讀者目前的語言進去家目錄中的下載這個資料夾。
* 進入到Downloads這個資料夾可以發現我們所下載的資料庫檔案，檔名後面的.zip為利用zip此軟體所壓縮的附檔名，我們要利用相對應的軟體來解壓縮此檔案，在此我們利用unzip此指令來解壓縮。
* 打上unzip rtl8812au-5.3.4.zip，之後就會顯示解壓縮過程中所產生的檔案。

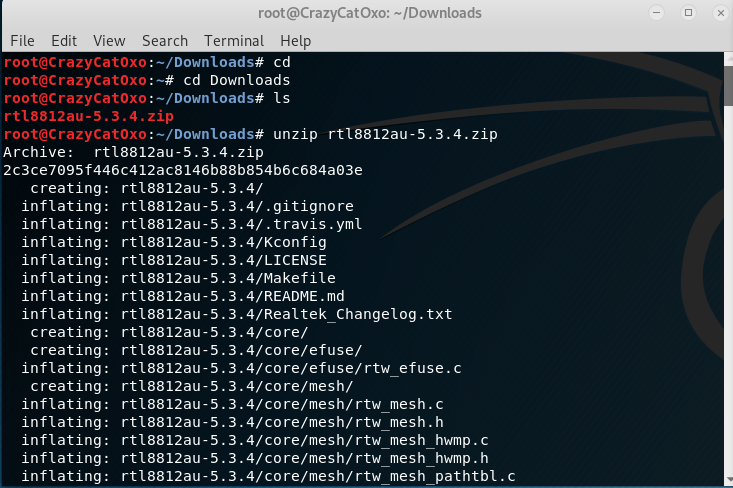


圖12

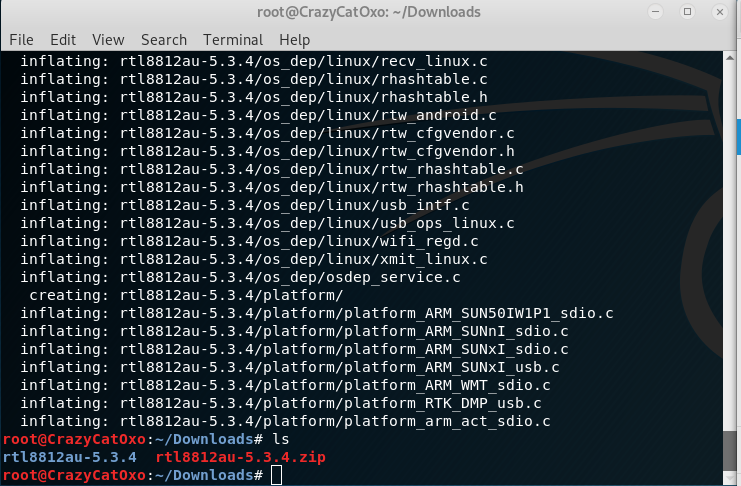


圖13

* 解壓縮完成後可以發現多了一個目錄為 rtl8812au-5.3.4

Step4. 根據自己所選的下載方法，其所產生出的資料夾其名稱，打 cd rtl8812au-5.3.4 或 cd rtl8812au。

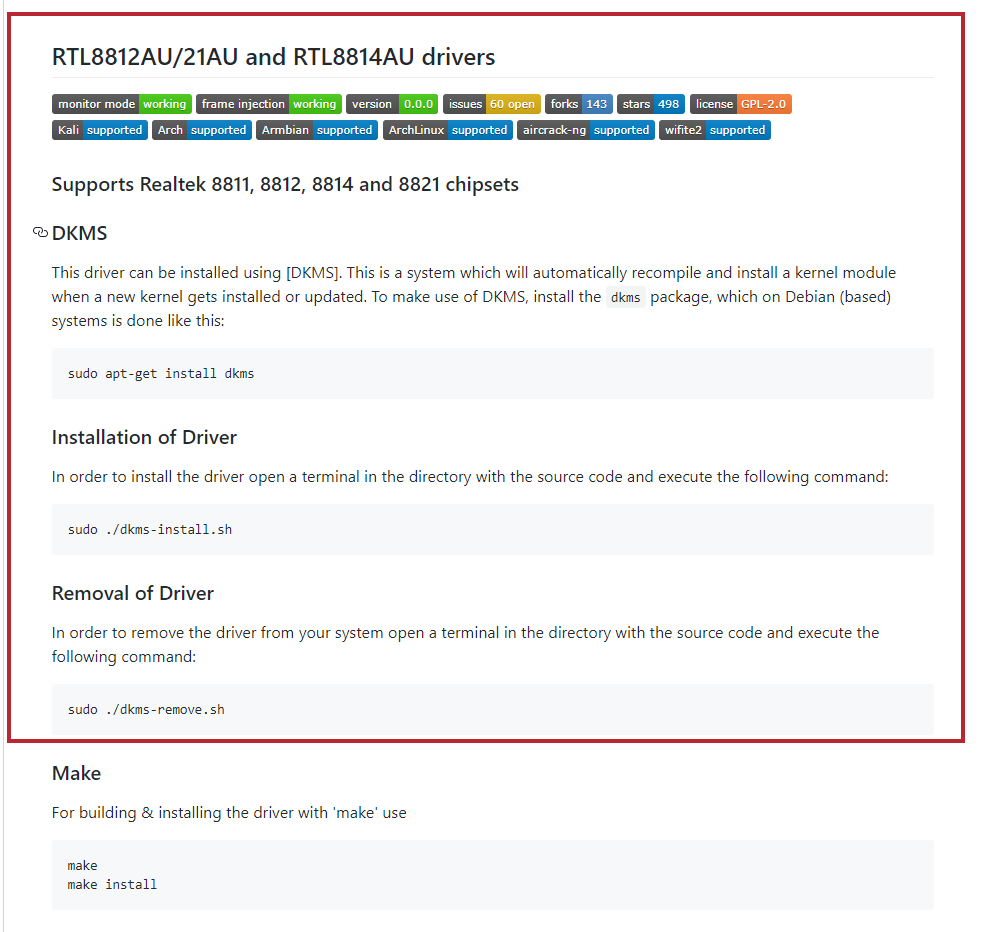


圖14

Step5. 在圖8中的網頁中，往下拖拉可以看到圖14的內容，此內容為教我們如何灌它們所提供的驅動程式。

Step6. 根據圖14的圖中的步驟，先打上apt-get install dkms (由於筆者在這本書都會使用root這個帳號，而root帳號的權限預設是很大的，可以把它想像成KALI裡的管理者，而圖14中會在指令最前面加上sudo 的原因為，有些指令及操作是不允許一般的使用者來執行，由於一般使用者的權限較低，權限上的設定是可以做到的，但在此筆者並不對其有過多的討論，而sudo這個指令為利用其他帳號的權限來執行後面的指令，如果沒有特定帳號則是root這個帳號)，下載dkms這個軟體。

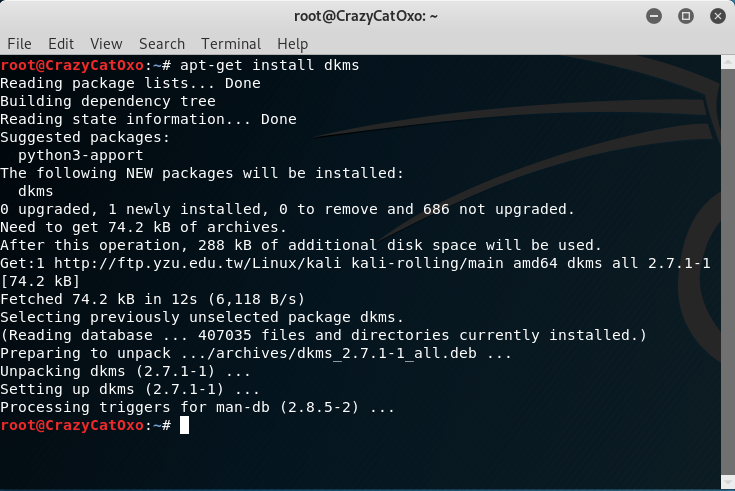


圖15

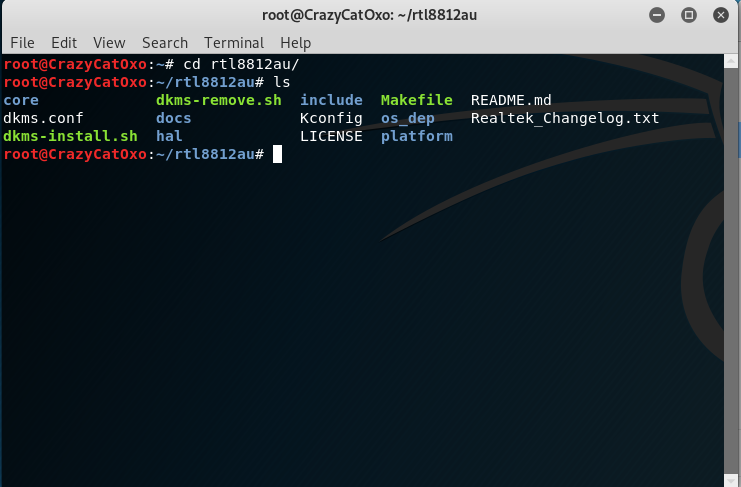


圖16

Step6. 透過Step4.我們的所在位置會在rtl8812au 或者 rtl8812au-5.3.4 資料夾內，可以發現資料夾內有其他檔案，根據圖14中的內容，打上 ./dkms-install.sh 的指令就可將 AWUS036ACH的驅動程式安裝完成。

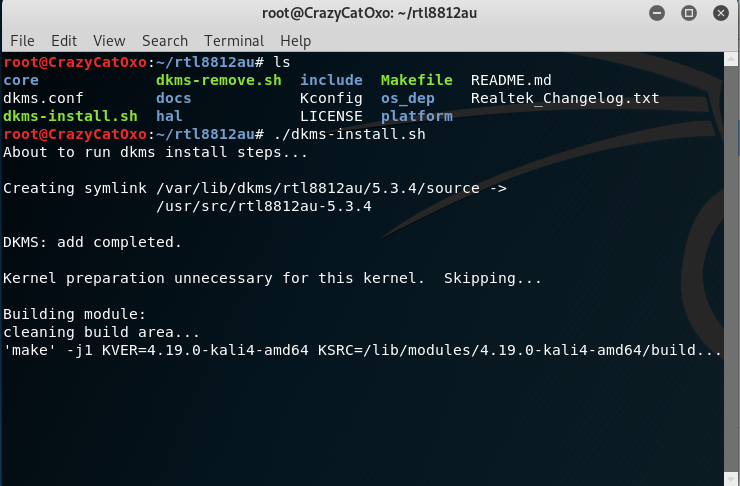


圖17

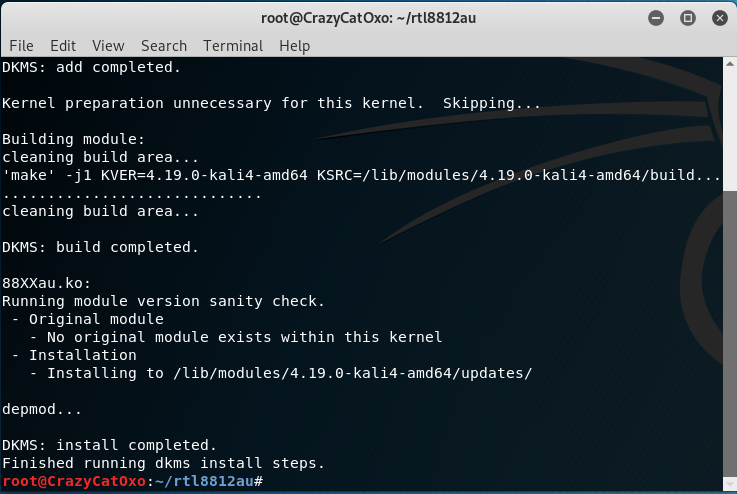


圖18

Final Step. 到這裡我們就可以查看AWUS036ACH這個網卡是否抓到，如果沒抓到的話，請參閱Q1中其他的解答，如果讀者是使用虛擬主機來跑KALI的話請參閱Q4

如果讀者想要將其他其他的網路卡裝上的話，請到製作其網卡的公司官方網站查詢此網路卡是否支援LINUX，如果可以的話，筆者在此道歉關於用其他方式灌驅動程式這方面的筆者不太熟悉，所以只能請讀者自尋上網尋找教學。

Q2.

apt-get無法下載或者顯示unable to locate packge 的訊息

A2.

1./etc/apt/sources.list 沒設定好

Step1. 在<https://docs.kali.org/general-use/kali-linux-sources-list-repositories> 這個網頁有提供kali 所提供的資料庫，apt-get 此指令

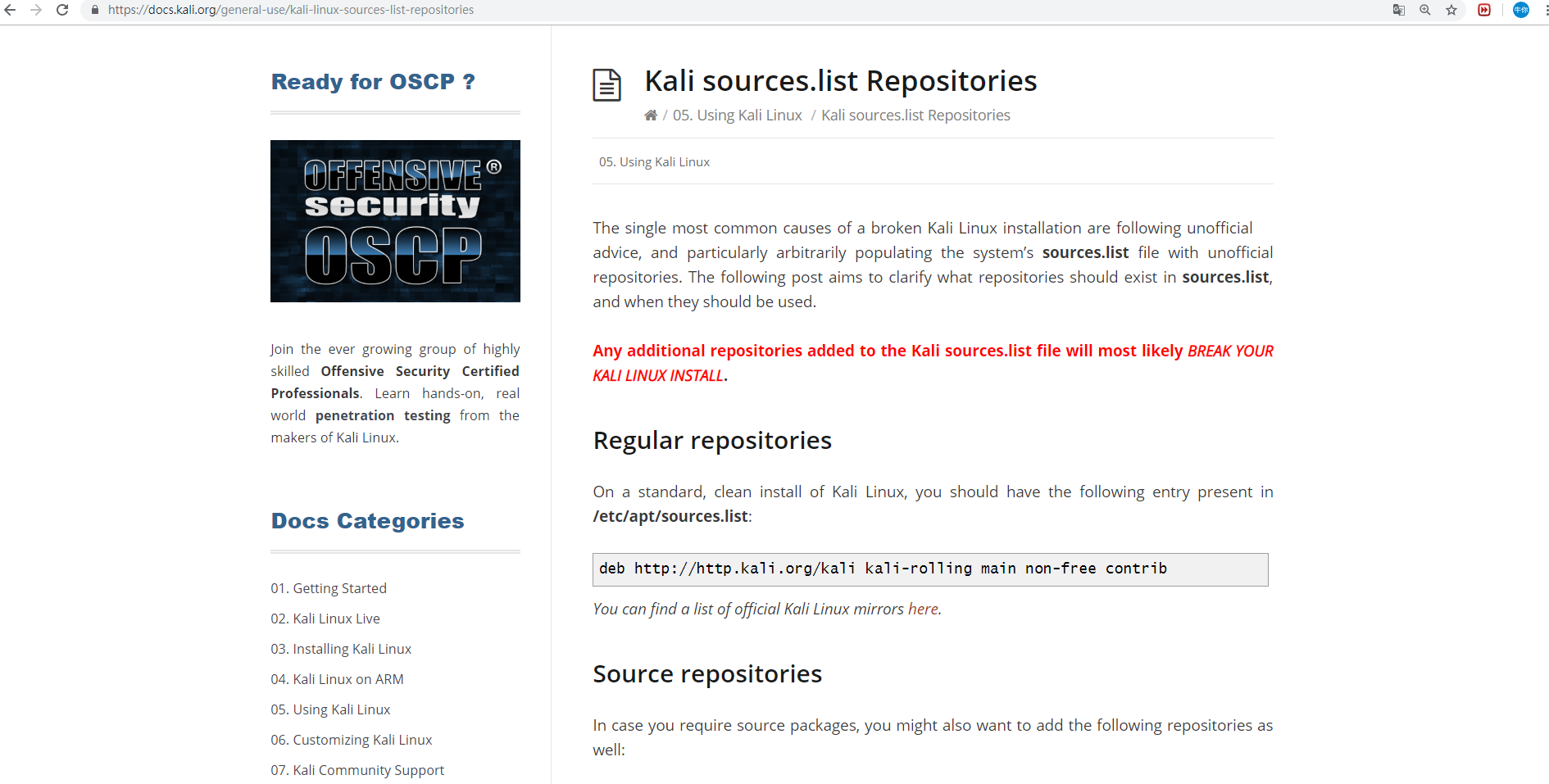


圖19

Q3.

有配置網卡但是無法上網

A3.

Q4.

有關虛擬主機會遇到的問題

A4.

# 參考資料

1. Oracle的virtual box 下載點

<https://www.virtualbox.org/>

1. Kali linux下載點

<https://www.kali.org/downloads/>

1. AWUS036ACH網卡驅動程式下載網站

<https://store.rokland.com/>

1. Kali 提供的資料庫

<https://docs.kali.org/general-use/kali-linux-sources-list-repositories>