**COMP 9337 Securing Wireless Networks T1, 2019**

**Project 1**

***Portable Penetration Testing Station for Wi-Fi Networks***

Group: SWN19 AI

Wanze LIU (z5137189), Zhou JIANG (z5146092)

School of Computer Science and Engineering

UNSW Sydney

**Task 1**

In this task , firstly ,we install the kali linux system in the raspberry Pi, after that we turn on the raspberry pi and open the terminal typing `ifconfig` command it shows there is no connection with internet in wlan1 which means no ipv4 address been allocated to this machine we are using, and then we initialize the connection to the WIFI , we input the command again, it show the allocated ipv4 address in wlan1

**Task2**

In task 2, in the beginning, we create the fake AP which the name is same as the victim connected to, after that, we force the target to disconnect from the original AP and connect to our fake AP, this is because the SSID of the original AP is same as the fake one, when the victim machine find out it can not connect the real AP, it will try to connect the fake one which because the SSID is same as the real one.

**Task3**

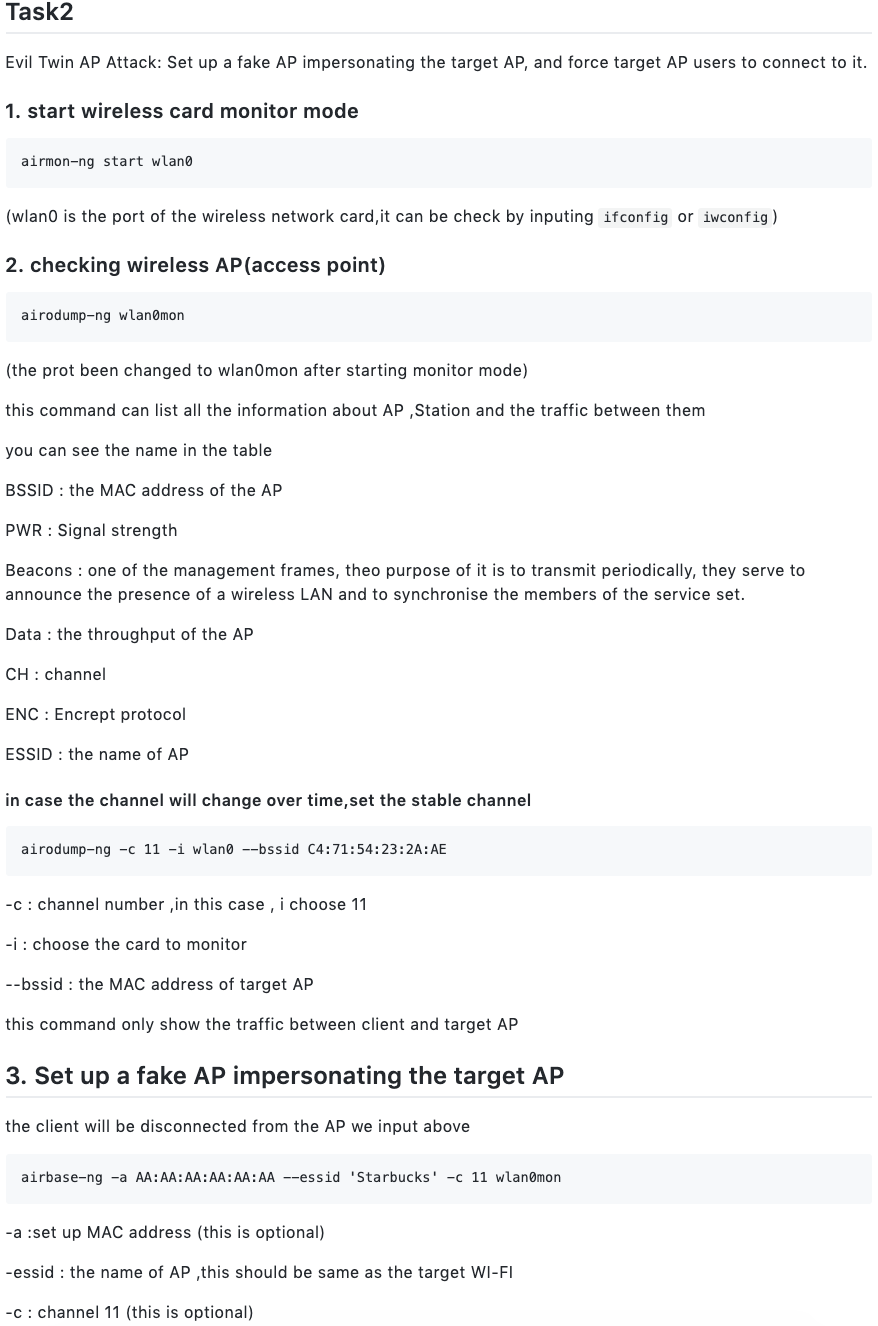
In task 2 , the victim have alreadly connect to the fake AP, in this situation, as long as victim machine try to browsing the web, the fake login webpage will show in front of the victim and misguide them to enter the username and password, this confidential information will capture in the backend of the raspberry Pi

**Task1**

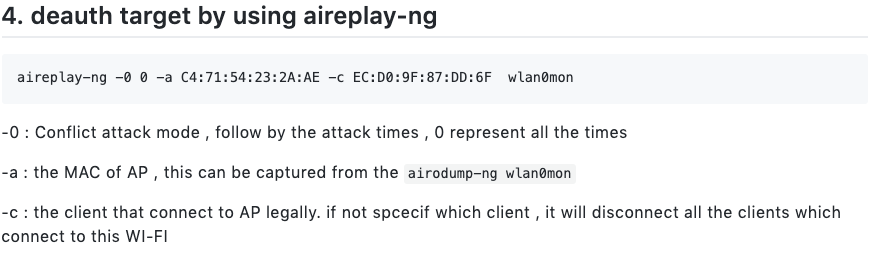
we downland the image of kali linux and using balenaEtcher to install the OS into the raspberry Pi, after it turn on, we open the terminal and input `ifconfig` to check whether the internet card connect to the internet before and after we connect to the internet.

**Task2**

The first step we done in this task is to create the fake AP, we have already plugin the ALFA adaptor,and following step will be:



After the fake AP created, now we can deauth the victim by using aireplay-ng



We write the shell script to execute

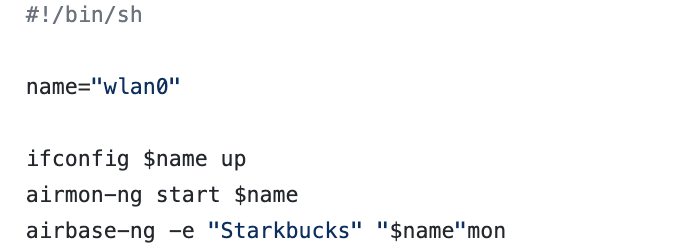
As we have described functionality of command above,

the script for setup fake AP will be

```

sh twinstart.sh

```



The script for deauthencating (force victim to disconnect to real AP)

```

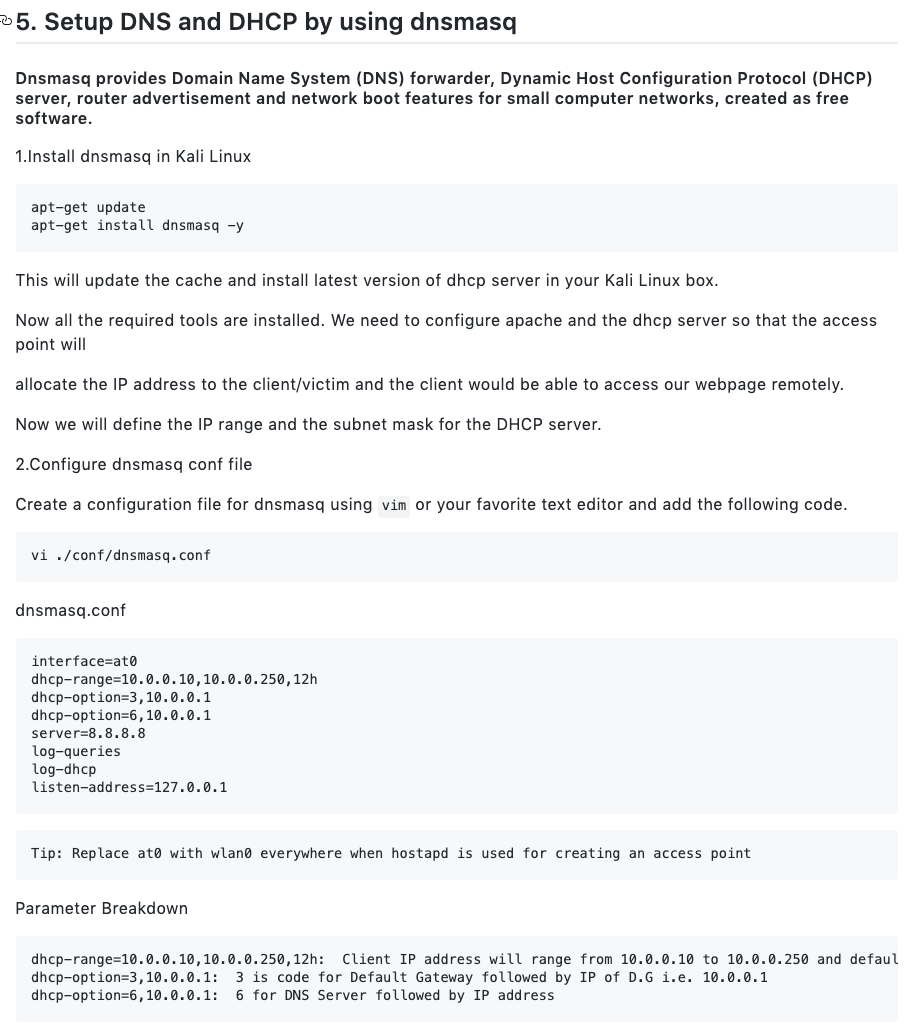
sh deauth.sh victimMAC APMAC

```



**Task3**

We first install dnsmasq in the kali, and configure the conf file according below



And execute the shell script to launch the dnsmsaq (dns server and dhcp server)

```

sh setting.sh

```



And then we create the fake login page and turn on the flask server on kali(we assume this is similar as the real page which victim using)

when victim enter the password and click the submit the chrome will execute the js script sending the password to the flask server we build in the kali trough port 5000 and api will automatic generate the file for password captured.

In this situation, the evil twin AP is hard to detect as it is also a legitimate AP , for defencing against attacks performed, we can apply some detect system that can find the evil twin AP, for example , we can use e wireless intrusion prevention systems (WIPS) to detect the presence of an evil twin AP and prevent any managed corporate clients from connecting to them.

And also using a VPN is also a good way to prevent an evil twin attack and protect users, but it will not necessarily stop users from connecting to the rogue access point. we could disable the option to connect to unapproved wireless networks, but this could be a significant limitation for users

Weekly log

|  |  |
| --- | --- |
| Week1 | LIU: find how to install the kali linux into raspberry Pi and record the screen record of task 1  JIANG :install the kali linux on the raspberry |
| Week2 | LIU : build the backend and frontend to capture the password  JIANG: configure the dnsmasq in kali |
| Week3 |  |
| Week4 |  |