Set up hotspot

1. 教學

<https://wiki.archlinux.org/index.php/Software_access_point>

1. hotspost 軟體教學

<https://wireless.wiki.kernel.org/en/users/Documentation/hostapd>

1. 缺失netlink library補救

<https://askubuntu.com/questions/277803/how-to-install-update-libnl-1-0pre8-or-later>

1. 缺失openssl library 補救

<https://stackoverflow.com/questions/17915098/openssl-ssl-h-no-such-file-or-directory-during-installation-of-git>

1. 缺失 nl-genl-3 library 補救

<https://askubuntu.com/questions/861742/getting-error-cannot-find-lnl-genl-3-while-running-make/861744>

1. 架設NAT

<https://wiki.archlinux.org/index.php/Software_access_point>

1. Iptables指令教學

<https://wiki.archlinux.org/index.php/Iptables>

how to set up bridge

1. Wiki explan what is bridge

<https://en.wikipedia.org/wiki/Bridging_(networking)>

1. Teach how to set up

<https://wiki.archlinux.org/index.php/Network_bridge>

what is tx power of wifi?

<https://www.quora.com/What-is-TX-Power-in-Wi-Fi-terminology>

rtl8812 5.3.4 driver problem 無法改變 txpower

<https://github.com/aircrack-ng/rtl8812au/issues/180>

this problem can be solved by downloading the 5.2.20 version driver

git clone –b v5.2.20 https://github.com/aircrack-ng/rtl8812au.git

如何利用python對ap其內部的設定網頁登入認證做字典攻擊

此例中利用python2版本

WF2412 netis 型號的ap其192.168.1.1的網站登入認證是利用http header裡的basic access authentication且其http 方式為get

Wiki basic access authentication 解說

<https://en.wikipedia.org/wiki/Basic_access_authentication>

python requests 模組解說

<https://realpython.com/python-requests/>

python base64 function 解說

<https://docs.python.org/2/library/base64.html>

第二種利用竊取封包將其之中的http authrization 中的base64字串轉回ascii將可得到帳號與密碼(帳號與密碼之間用冒號隔開)

ex. Account:password

先用字典攻擊其帳號如果此帳號沒有存在，回傳的http封包裏會顯示此帳號不存在，如果存在會顯示密碼錯誤