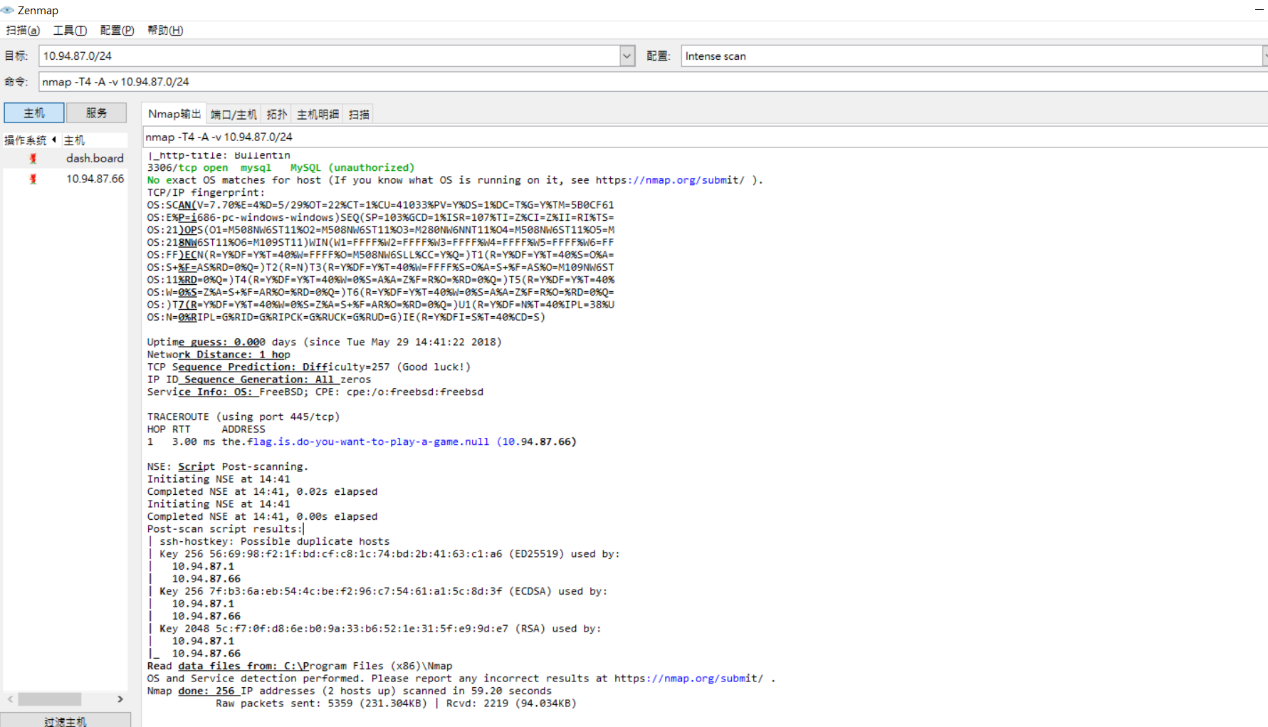
0516208 黃郁恬

Dashboard上的名稱: 0516208\_v2

(因為忘記密碼~所以開了一個新的)

1. Challenge1

用nmap找到第一個flag



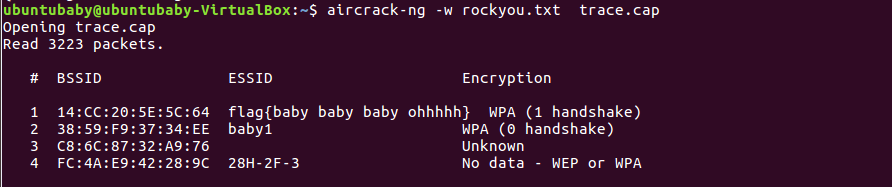
2. Challenge2

(wireshark, aircrack-ng)

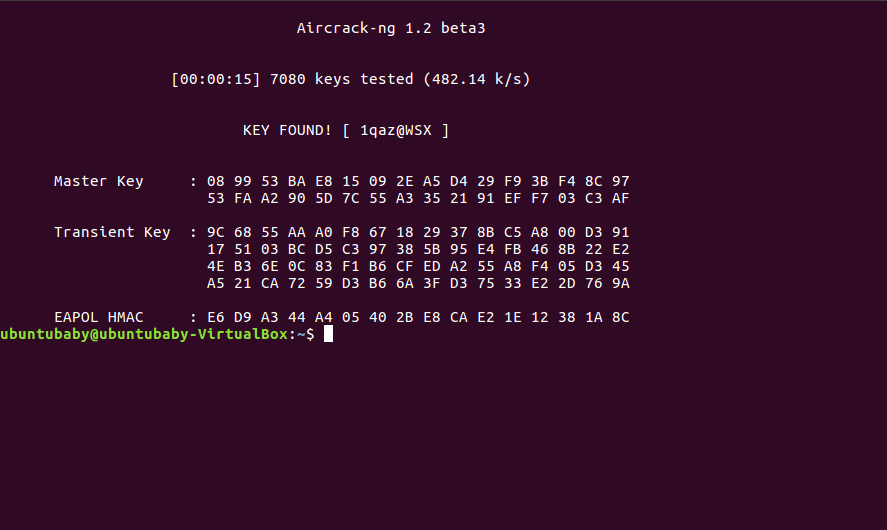
利用wireshark和aircrack-ng找到baby baby baby ohhhhh這個flag

接著，下載rockyou.txt(網路上很多人用+推薦)

* 利用字典破解法找到密碼(passphrase):

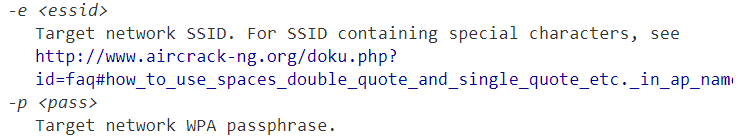


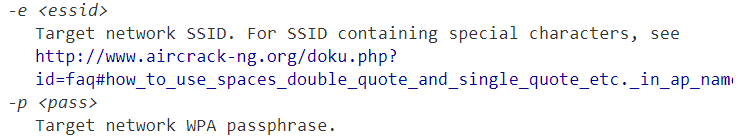
找到密碼: 1qaz@WSX



用airdecap-ng來對檔案進行解密:

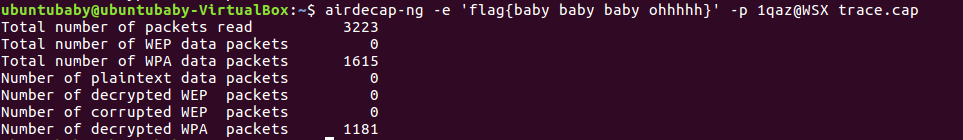
(airdecap-ng 可以對從 WEP/WPA/WPA2 擷取的檔案進行解密作業)





-e 該SSID的名字，也就是flag{baby baby baby ohhhhh}

-p 密碼，前面利用rockyou.txt找到的1qaz@WSX



* dec.cap:
* 找到flag

