CSC Project 2 Report

Attacker's IP and MAC:

```
cs2021@ubuntu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.171.138  netmask 255.255.255.0  broadcast 192.168.171.255
        inet6 fe80::5cf9:2e5b:797e:6f9c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:dd:f5:5b  txqueuelen 1000  (Ethernet)
        RX packets 2611  bytes 1520054 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3572  bytes 899619 (899.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 176  bytes 14192 (14.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 176  bytes 14192 (14.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Item 1: Using scenario 2

In attacker:

```
cs2021@ubuntu:~/Desktop$ sudo ./mitm_attack
MAC                IP
-------------------------
00:50:56:fb:54:e2   192.168.171.2
00:0c:29:90:10:e8   192.168.171.137
00:50:56:fc:e7:54   192.168.171.254

0: ('00:50:56:fb:54:e2', '192.168.171.2')
1: ('00:0c:29:90:10:e8', '192.168.171.137')
2: ('00:50:56:fc:e7:54', '192.168.171.254')
choose victim device: 1
Using ('00:0c:29:90:10:e8', '192.168.171.137')

username=aaa   password=bbb
```

In victim:

Attacker's MAC and gateway's MAC are the same.

```
cs2021@ubuntu:~/Desktop$ arp -a
? (192.168.171.138) at 00:0c:29:dd:f5:5b [ether] on ens33
_gateway (192.168.171.2) at 00:0c:29:dd:f5:5b [ether] on ens33
? (192.168.171.254) at 00:50:56:fc:e7:54 [ether] on ens33
cs2021@ubuntu:~/Desktop$
```

In login page, input username aaa, password bbb. Then they will display on attacker (first picture).

Item 2: Using scenario 2

In attacker:

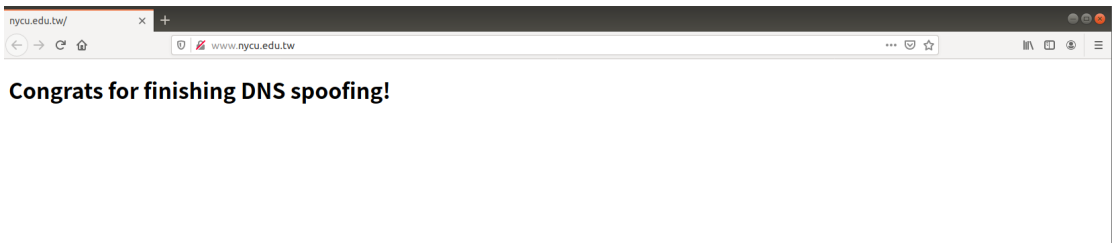
```
cs2021@ubuntu:~/Desktop$ sudo ./pharm_attack
[sudo] password for cs2021:
MAC                IP
-------------------------
00:50:56:fb:54:e2   192.168.171.2
00:0c:29:90:10:e8   192.168.171.137
00:50:56:fc:e7:54   192.168.171.254

0: ('00:50:56:fb:54:e2', '192.168.171.2')
1: ('00:0c:29:90:10:e8', '192.168.171.137')
2: ('00:50:56:fc:e7:54', '192.168.171.254')
choose victim device: 1
Using ('00:0c:29:90:10:e8', '192.168.171.137')
```

In victim:

Attacker's MAC and gateway's MAC are the same.

```
cs2021@ubuntu:~/Desktop$ arp -a
? (192.168.171.138) at 00:0c:29:dd:f5:5b [ether] on ens33
_gateway (192.168.171.2) at 00:0c:29:dd:f5:5b [ether] on ens33
? (192.168.171.254) at 00:50:56:fc:e7:54 [ether] on ens33
cs2021@ubuntu:~/Desktop$
```

Open webpage http://www.nycu.edu.tw. It will be redirected to 140.113.207.246.



Item 3:

To defend against ARP spoofing attack, we can enable DAI (Dynamic ARP Inspection) on switch. First, We have to generate a table on switch that saved all devices' correct IP and MAC. Then if a host send a ARP message, the switch can compare whether the packet's source IP and MAC matches with the table. If not, then it will be seen as a spoof packet. The switch will drop it.