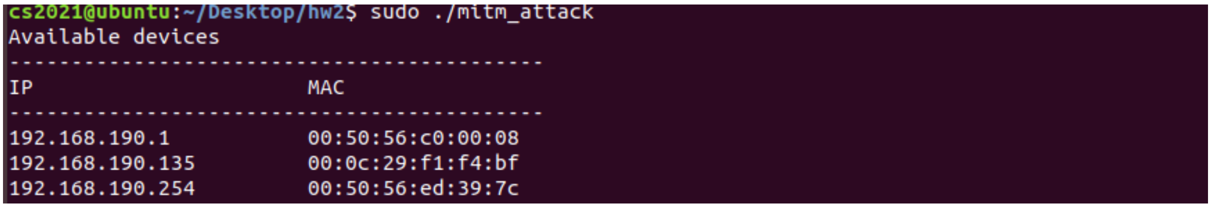
Computer Security Capstone Homework2 Report

- Part 1: MITM attack

  Test scenario: II

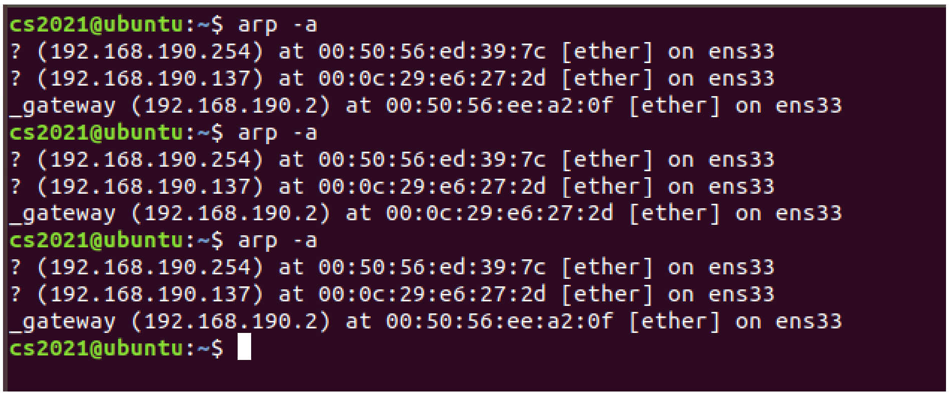
  Task 1:



```
cs2021@ubuntu:~/Desktop/hw2$ sudo ./mitm_attack
Available devices
------------------------------------------
IP                      MAC
------------------------------------------
192.168.190.1           00:50:56:c0:00:08
192.168.190.135         00:0c:29:f1:f4:bf
192.168.190.254         00:50:56:ed:39:7c
```

The figure above is task 1: listing all the available devices. 192.168.190.135 is the victim.

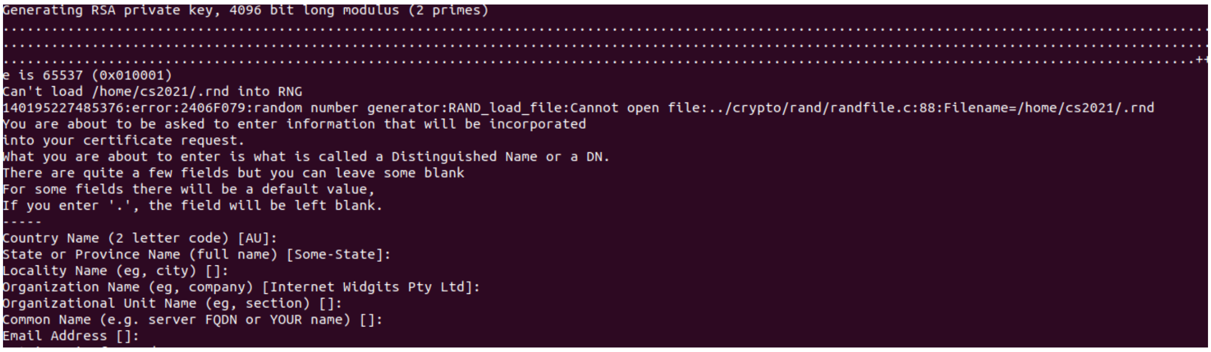
Task 2:



```
cs2021@ubuntu:~$ arp -a
? (192.168.190.254) at 00:50:56:ed:39:7c [ether] on ens33
? (192.168.190.137) at 00:0c:29:e6:27:2d [ether] on ens33
_gateway (192.168.190.2) at 00:50:56:ee:a2:0f [ether] on ens33
cs2021@ubuntu:~$ arp -a
? (192.168.190.254) at 00:50:56:ed:39:7c [ether] on ens33
? (192.168.190.137) at 00:0c:29:e6:27:2d [ether] on ens33
_gateway (192.168.190.2) at 00:0c:29:e6:27:2d [ether] on ens33
cs2021@ubuntu:~$ arp -a
? (192.168.190.254) at 00:50:56:ed:39:7c [ether] on ens33
? (192.168.190.137) at 00:0c:29:e6:27:2d [ether] on ens33
_gateway (192.168.190.2) at 00:50:56:ee:a2:0f [ether] on ens33
cs2021@ubuntu:~$
```

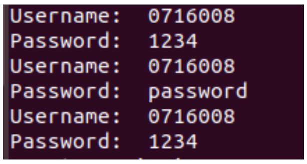
The picture above shows that the Mac address of the gateway indeed will be tampered to that of the attacker during the attack.

Task 3:



```
Generating RSA private key, 4096 bit long modulus (2 primes)
.........................................................................................................................
.........................................................................................................................
.......................................................................................................................++
e is 65537 (0x010001)
Can't load /home/cs2021/.rnd into RNG
140195227485376:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/home/cs2021/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

The figure above is the process of generating the certificate.

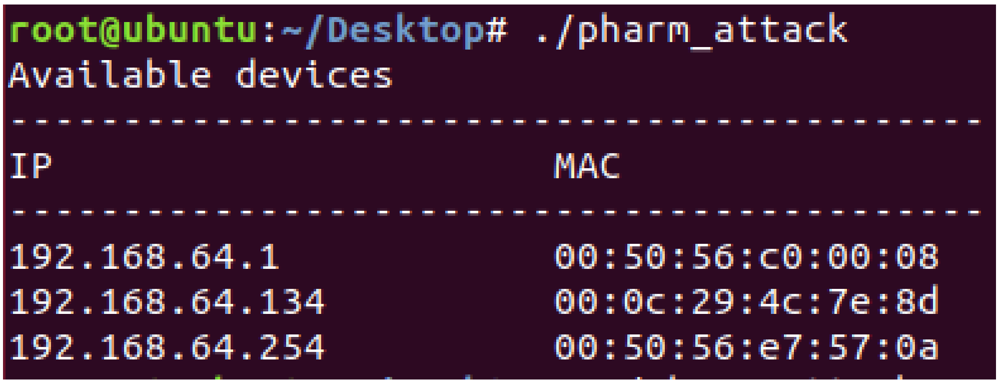


```
Username:  0716008
Password:  1234
Username:  0716008
Password:  password
Username:  0716008
Password:  1234
```

The acquired username and password on e3 by using sslsplit.

- Part 2: Pharming attack
  Test scenario: II

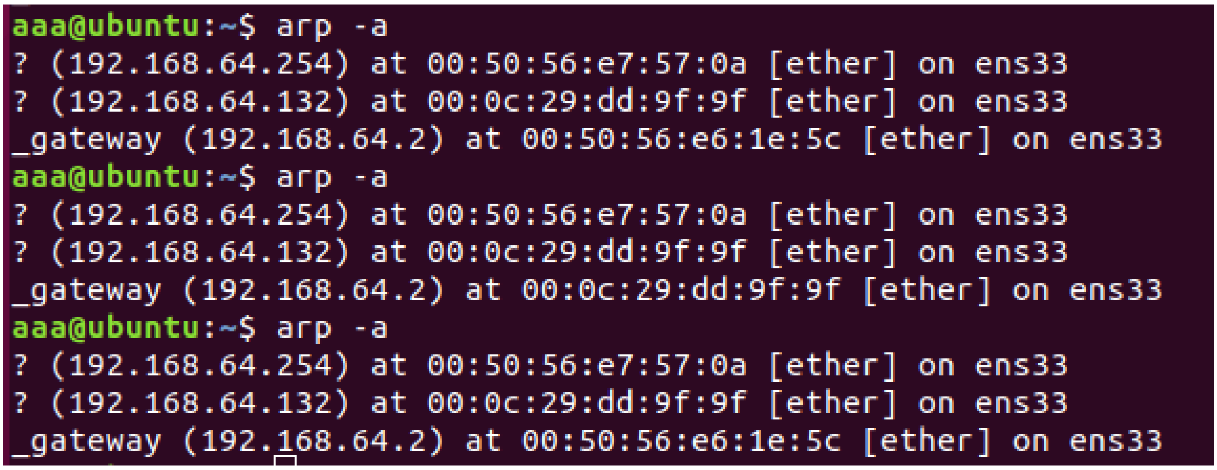
  Task1:



```
root@ubuntu:~/Desktop# ./pharm_attack
Available devices
-------------------------------------------
IP                     MAC
-------------------------------------------
192.168.64.1           00:50:56:c0:00:08
192.168.64.134         00:0c:29:4c:7e:8d
192.168.64.254         00:50:56:e7:57:0a
```

The figure above is task 1: listing all the available devices. 192.168.190.134 is the victim.

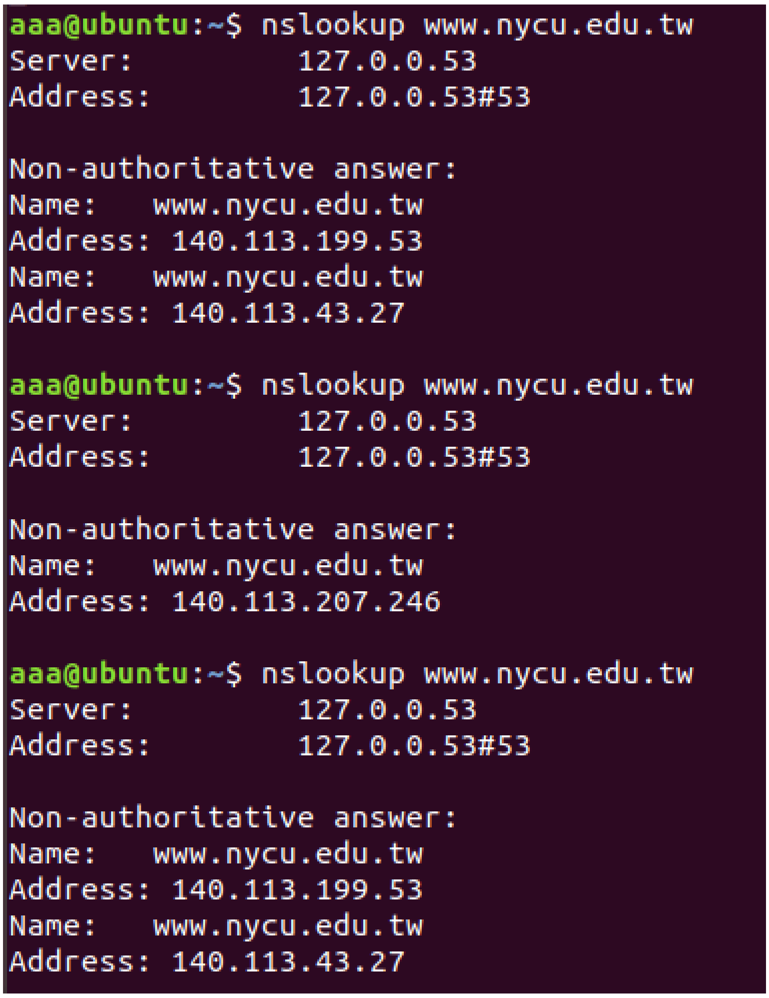
Task2:



```
aaa@ubuntu:~$ arp -a
? (192.168.64.254) at 00:50:56:e7:57:0a [ether] on ens33
? (192.168.64.132) at 00:0c:29:dd:9f:9f [ether] on ens33
_gateway (192.168.64.2) at 00:50:56:e6:1e:5c [ether] on ens33
aaa@ubuntu:~$ arp -a
? (192.168.64.254) at 00:50:56:e7:57:0a [ether] on ens33
? (192.168.64.132) at 00:0c:29:dd:9f:9f [ether] on ens33
_gateway (192.168.64.2) at 00:0c:29:dd:9f:9f [ether] on ens33
aaa@ubuntu:~$ arp -a
? (192.168.64.254) at 00:50:56:e7:57:0a [ether] on ens33
? (192.168.64.132) at 00:0c:29:dd:9f:9f [ether] on ens33
_gateway (192.168.64.2) at 00:50:56:e6:1e:5c [ether] on ens33
```

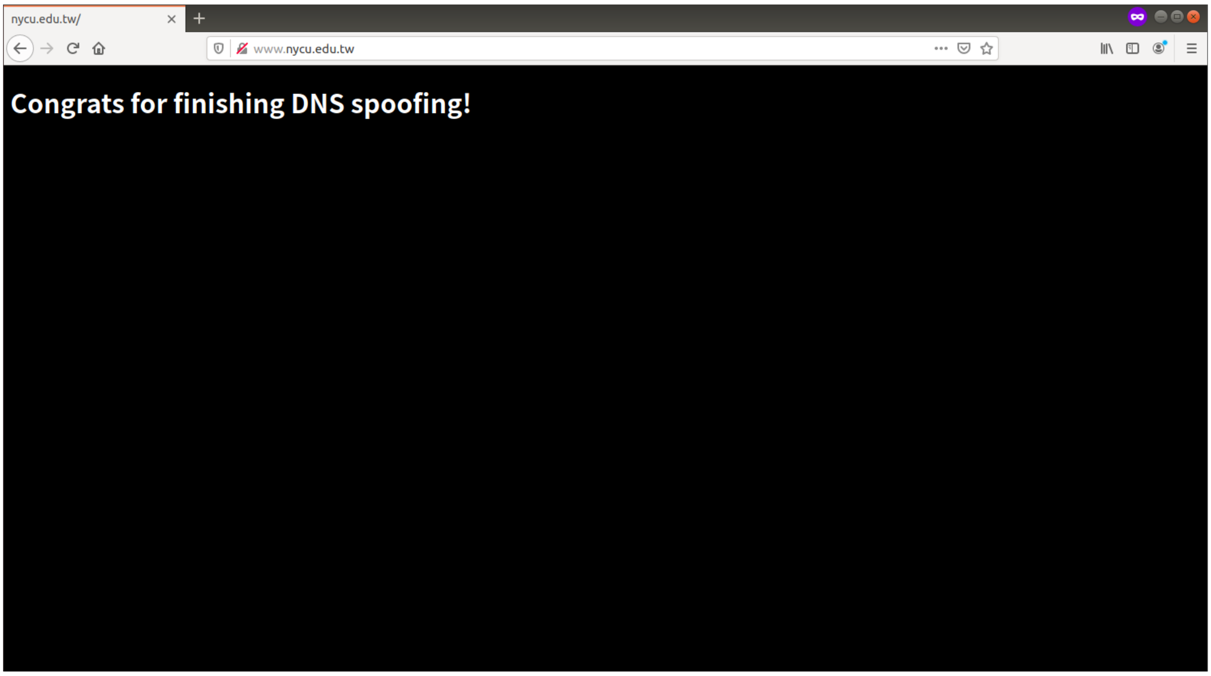
The picture above shows that the Mac address of the gateway indeed will be tampered to that of the attacker during the attack.

Task 3:



```
aaa@ubuntu:~$ nslookup www.nycu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.nycu.edu.tw
Address: 140.113.199.53
Name:   www.nycu.edu.tw
Address: 140.113.43.27

aaa@ubuntu:~$ nslookup www.nycu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.nycu.edu.tw
Address: 140.113.207.246

aaa@ubuntu:~$ nslookup www.nycu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.nycu.edu.tw
Address: 140.113.199.53
Name:   www.nycu.edu.tw
Address: 140.113.43.27
```

The figure above shows that the address is redirected to the attack server(140.113.207.246) while doing DNS spoofing.



Congrats for finishing DNS spoofing!

The figure above shows that the phishing webpage is shown to the victim.

- Part 3: Prevention of ARP spoofing
    - Use static ARP
      Since the victim’s ARP is dynamic in this homework, we consider setting the ARP of a PC static a feasible way to prevent ARP spoofing. The ARP protocol will prevent devices from listening on ARP responses for an address once the address was binded with a static ARP entry.

    - Use VPN
      Since VPN will encrypt all the communication from devices to the Internet, this makes ARP spoofing infeasible (not in the case when the victim has the attacker’s certificate).

    - Packet filtering
      We can stop the packet before they reach the devices on our network by checking whether there exists paradox in the source information. For instance, the mac of gateway is 00:50:56:ee:a2:0f at first, if it becomes 00:0c:29:e6:27:2d later, we shall block the packet.