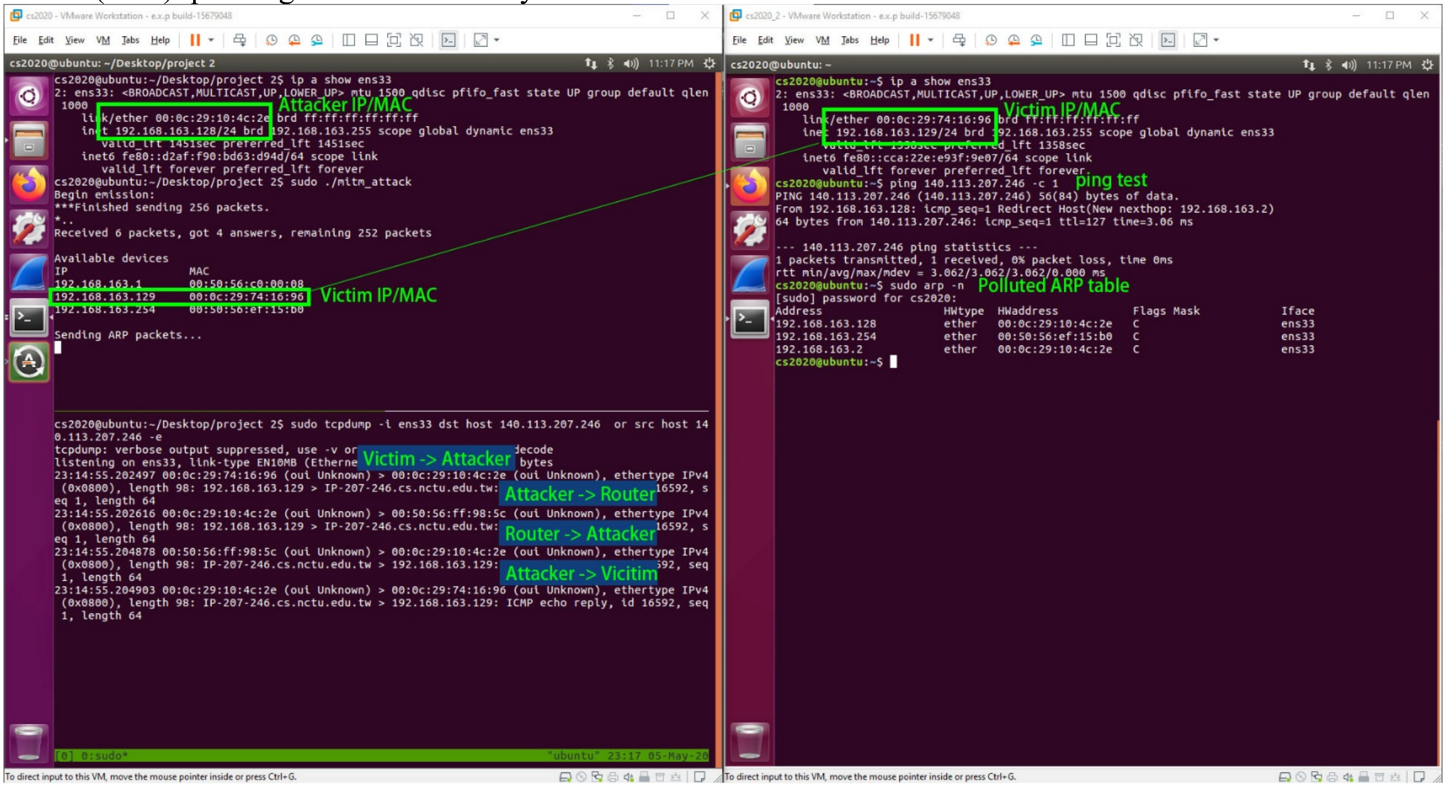
All testing is done under test scenario 2

Item 1 (10%): please give evidence that you have finished the MitM attack



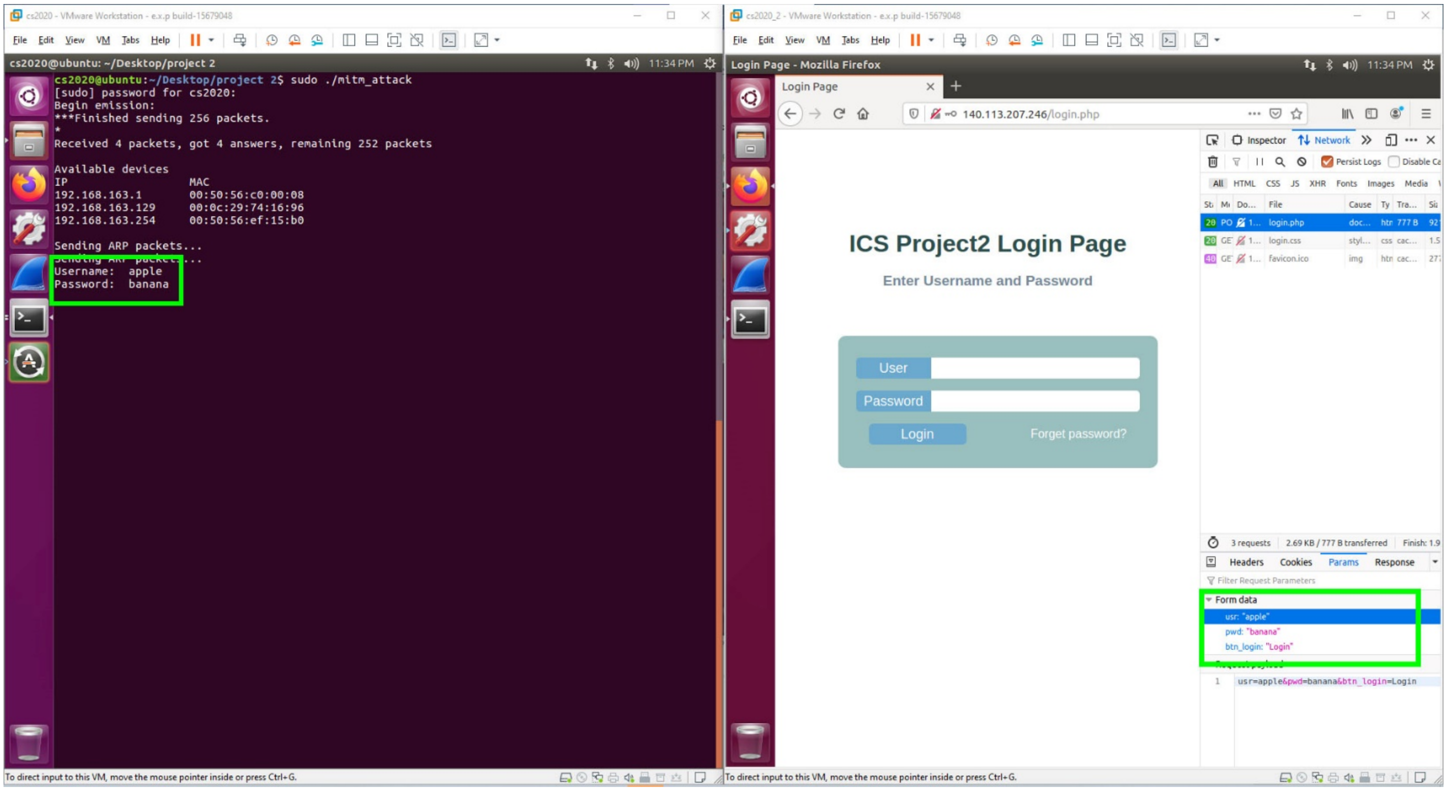
cs2020 - VMware Workstation - e.x.p build-15679048
File Edit View VM Tabs Help
cs2020@ubuntu: ~/Desktop/project 2
11:17 PM
Attacker IP/MAC
Victim IP/MAC
Victim -> Attacker
Attacker -> Router
Router -> Attacker
Attacker -> Vicitim
cs2020_2 - VMware Workstation - e.x.p build-15679048
cs2020@ubuntu: ~
Victim IP/MAC
ping test
Polluted ARP table
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
cs2020@ubuntu:~/Desktop/project 2$ ip a show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
 1000
    link/ether 00:0c:29:10:4c:2e brd ff:ff:ff:ff:ff:ff
    inet 192.168.163.128/24 brd 192.168.163.255 scope global dynamic ens33
       valid_lft 1451sec preferred_lft 1451sec
    inet6 fe80::d2af:f90:bd63:d94d/64 scope link
       valid_lft forever preferred_lft forever
cs2020@ubuntu:~/Desktop/project 2$ sudo ./mitm_attack
Begin emission:
***Finished sending 256 packets.
*..
Received 6 packets, got 4 answers, remaining 252 packets

Available devices
IP                  MAC
192.168.163.1       00:50:56:c0:00:08
192.168.163.129     00:0c:29:74:16:96
192.168.163.254     00:50:56:ef:15:b0

Sending ARP packets...
```

```
cs2020@ubuntu:~/Desktop/project 2$ sudo tcpdump -i ens33 dst host 140.113.207.246  or src host 14
0.113.207.246 -e
tcpdump: verbose output suppressed, use -v or                  decode
listening on ens33, link-type EN10MB (Etherne                  bytes
23:14:55.202497 00:0c:29:74:16:96 (oui Unknown) > 00:0c:29:10:4c:2e (oui Unknown), ethertype IPv4
 (0x0800), length 98: 192.168.163.129 > IP-207-246.cs.nctu.edu.tw:                    16592, s
eq 1, length 64
23:14:55.202616 00:0c:29:10:4c:2e (oui Unknown) > 00:50:56:ff:98:5c (oui Unknown), ethertype IPv4
 (0x0800), length 98: 192.168.163.129 > IP-207-246.cs.nctu.edu.tw:                    16592, s
eq 1, length 64
23:14:55.204878 00:50:56:ff:98:5c (oui Unknown) > 00:0c:29:10:4c:2e (oui Unknown), ethertype IPv4
 (0x0800), length 98: IP-207-246.cs.nctu.edu.tw > 192.168.163.129:                    592, seq
 1, length 64
23:14:55.204903 00:0c:29:10:4c:2e (oui Unknown) > 00:0c:29:74:16:96 (oui Unknown), ethertype IPv4
 (0x0800), length 98: IP-207-246.cs.nctu.edu.tw > 192.168.163.129: ICMP echo reply, id 16592, seq
 1, length 64
[0] 0:sudo*                                                          "ubuntu" 23:17 05-May-20
```

```
cs2020@ubuntu:~$ ip a show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
 1000
    link/ether 00:0c:29:74:16:96 brd ff:ff:ff:ff:ff:ff
    inet 192.168.163.129/24 brd 192.168.163.255 scope global dynamic ens33
       valid_lft 1358sec preferred_lft 1358sec
    inet6 fe80::cca:22e:e93f:9e07/64 scope link
       valid_lft forever preferred_lft forever
cs2020@ubuntu:~$ ping 140.113.207.246 -c 1
PING 140.113.207.246 (140.113.207.246) 56(84) bytes of data.
From 192.168.163.128: icmp_seq=1 Redirect Host(New nexthop: 192.168.163.2)
64 bytes from 140.113.207.246: icmp_seq=1 ttl=127 time=3.06 ms

--- 140.113.207.246 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.062/3.062/3.062/0.000 ms
cs2020@ubuntu:~$ sudo arp -n
[sudo] password for cs2020:
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.163.128          ether   00:0c:29:10:4c:2e   C                     ens33
192.168.163.254          ether   00:50:56:ef:15:b0   C                     ens33
192.168.163.2            ether   00:0c:29:10:4c:2e   C                     ens33
cs2020@ubuntu:~$
```

As shown in the picture, I am able to print out local clients and pollute their ARP table, therefore, the ping request is routed to the attacker instead of directly to the router.



cs2020 - VMware Workstation - e.x.p build-15679048
File Edit View VM Tabs Help
cs2020@ubuntu: ~/Desktop/project 2
11:34 PM
cs2020_2 - VMware Workstation - e.x.p build-15679048
Login Page - Mozilla Firefox
Login Page
140.113.207.246/login.php
ICS Project2 Login Page
Enter Username and Password
User
Password
Login
Forget password?
Inspector
Network
Persist Logs
Disable Ca
All HTML CSS JS XHR Fonts Images Media
Headers Cookies Params Response
Filter Request Parameters
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
cs2020@ubuntu:~/Desktop/project 2$ sudo ./mitm_attack
[sudo] password for cs2020:
Begin emission:
***Finished sending 256 packets.
*
Received 4 packets, got 4 answers, remaining 252 packets

Available devices
IP                  MAC
192.168.163.1       00:50:56:c0:00:08
192.168.163.129     00:0c:29:74:16:96
192.168.163.254     00:50:56:ef:15:b0

Sending ARP packets...
Sending ARP packets...
Username:  apple
Password:  banana
```

St	M	Do...	File	Cause	Ty	Tra...	Si
20	PO	1...	login.php	doc...	htr	777 B	92
20	GE	1...	login.css	styl...	css	cac...	1.5
40	GE	1...	favicon.ico	img	htr	cac...	27

3 requests 2.69 KB / 777 B transferred Finish: 1.9

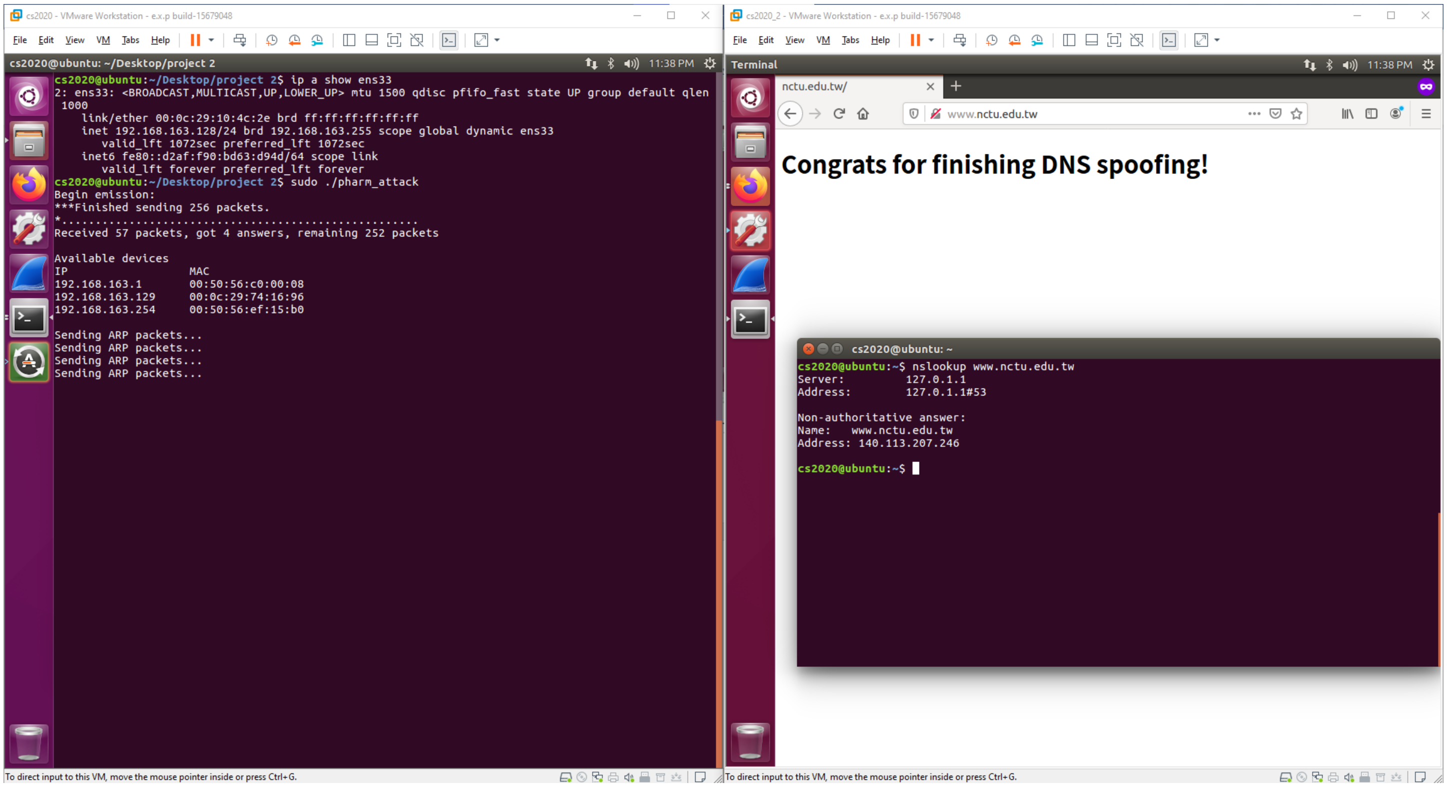
Form data
usr: "apple"
pwd: "banana"
btn_login: "Login"

Request payload

```
usr=apple&pwd=banana&btn_login=Login
```

Also, the program can print out login data sent to 140.113.207.246.

Item 2 (10%): please give evidence that you have finished the pharming attack


cs2020 - VMware Workstation - e.x.p build-15679048
File Edit View VM Tabs Help
cs2020@ubuntu: ~/Desktop/project 2
11:38 PM

```
cs2020@ubuntu:~/Desktop/project 2$ ip a show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
 1000
    link/ether 00:0c:29:10:4c:2e brd ff:ff:ff:ff:ff:ff
    inet 192.168.163.128/24 brd 192.168.163.255 scope global dynamic ens33
       valid_lft 1072sec preferred_lft 1072sec
    inet6 fe80::d2af:f90:bd63:d94d/64 scope link
       valid_lft forever preferred_lft forever
cs2020@ubuntu:~/Desktop/project 2$ sudo ./pharm_attack
Begin emission:
***Finished sending 256 packets.
*.....................................................
Received 57 packets, got 4 answers, remaining 252 packets

Available devices
IP                  MAC
192.168.163.1       00:50:56:c0:00:08
192.168.163.129     00:0c:29:74:16:96
192.168.163.254     00:50:56:ef:15:b0

Sending ARP packets...
Sending ARP packets...
Sending ARP packets...
Sending ARP packets...
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
cs2020_2 - VMware Workstation - e.x.p build-15679048
File Edit View VM Tabs Help
Terminal
11:38 PM
nctu.edu.tw/
www.nctu.edu.tw

Congrats for finishing DNS spoofing!

```
cs2020@ubuntu:~$ nslookup www.nctu.edu.tw
Server:         127.0.1.1
Address:        127.0.1.1#53

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

cs2020@ubuntu:~$ 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

As shown above, the victim is redirected to a fake website when it connects www.nctu.edu.tw.

Item 3 (10%): please propose a solution that can defend against the ARP spoofing attack

Whenever a client receives an ARP response, it can verify it by sending another request. For example, if a client receives an ARP packet that claims 192.168.0.1 is AA-BB-CC-DD-EE-FF, it can send another packet asking who is 192.168.0.1 and if the client receives conflicting responses, it will know that its network might be under attack. We can also encrypt all connections so the middleman cannot modify or read anything. For instance, using DNS over TLS will render our second attack useless.