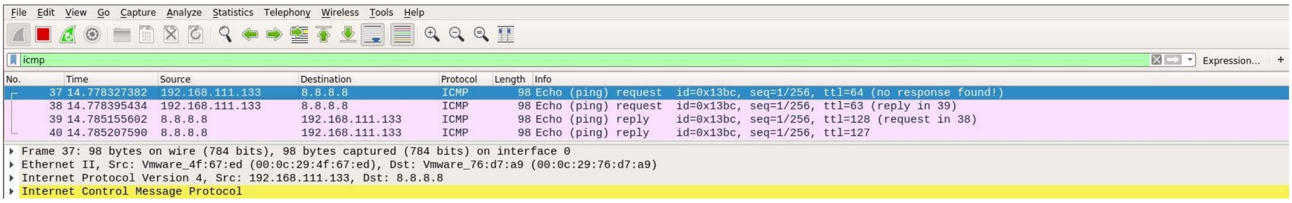
CSC-project2

0711529 陳冠儒

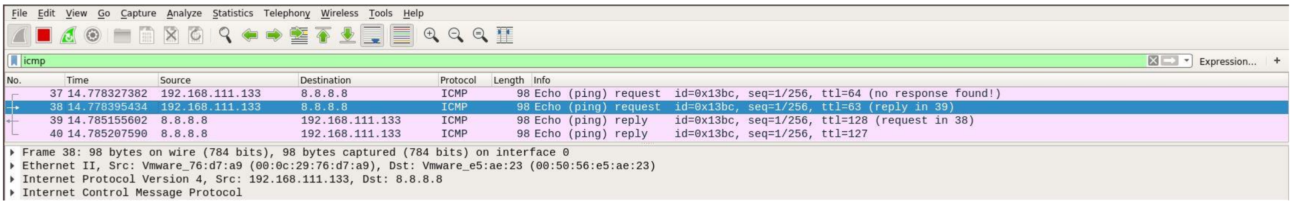
- Item 1 (5%): please give evidence that you have finished the MITM attack Specify your scenario (I or II) and Illustrate your results based on some snapshots

  I use the Scenario II that use two VM and NAT mode to do the MITM attack. The following pictures are the ARP spoofing evidence.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression… +

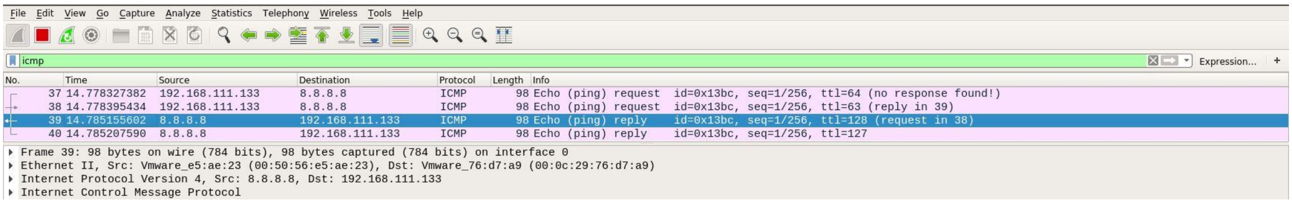
```
No.  Time           Source           Destination      Protocol Length Info
  37 14.778327382   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=64 (no response found!)
  38 14.778395434   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=63 (reply in 39)
  39 14.785155602   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=128 (request in 38)
  40 14.785207590   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=127
▸ Frame 37: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_4f:67:ed (00:0c:29:4f:67:ed), Dst: Vmware_76:d7:a9 (00:0c:29:76:d7:a9)
▸ Internet Protocol Version 4, Src: 192.168.111.133, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```

Figure 1. Victim to Attacker


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression… +

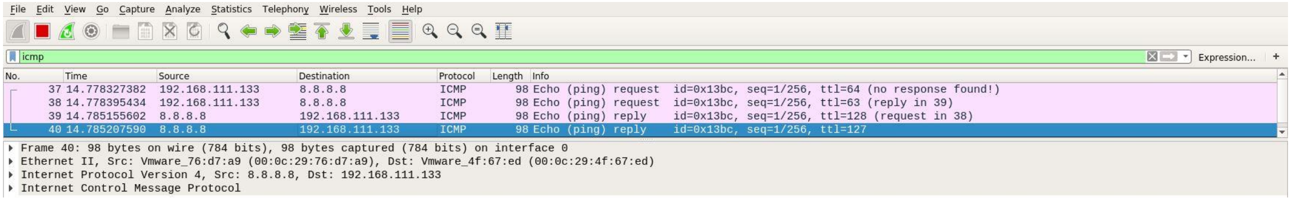
```
No.  Time           Source           Destination      Protocol Length Info
  37 14.778327382   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=64 (no response found!)
  38 14.778395434   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=63 (reply in 39)
  39 14.785155602   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=128 (request in 38)
  40 14.785207590   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=127
▸ Frame 38: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_76:d7:a9 (00:0c:29:76:d7:a9), Dst: Vmware_e5:ae:23 (00:50:56:e5:ae:23)
▸ Internet Protocol Version 4, Src: 192.168.111.133, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```

Figure 2. Attacker to AP


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression… +

```
No.  Time           Source           Destination      Protocol Length Info
  37 14.778327382   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=64 (no response found!)
  38 14.778395434   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=63 (reply in 39)
  39 14.785155602   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=128 (request in 38)
  40 14.785207590   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=127
▸ Frame 39: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_e5:ae:23 (00:50:56:e5:ae:23), Dst: Vmware_76:d7:a9 (00:0c:29:76:d7:a9)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.111.133
▸ Internet Control Message Protocol
```

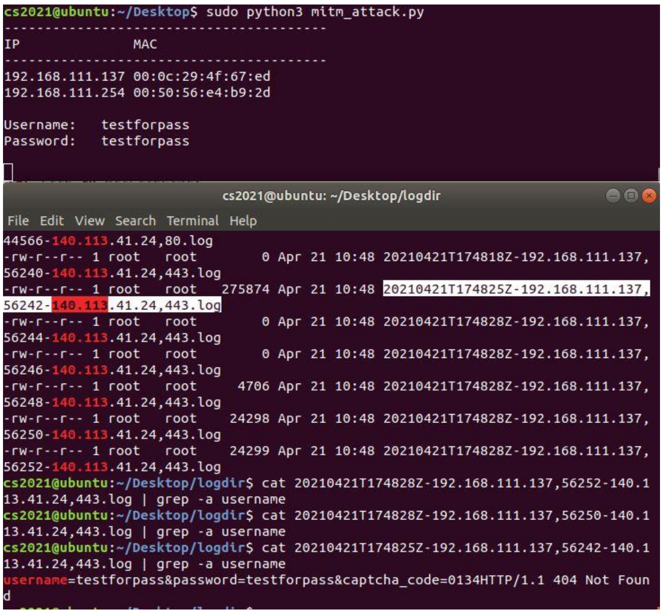
Figure 3. AP to Attacker


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression… +

```
No.  Time           Source           Destination      Protocol Length Info
  37 14.778327382   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=64 (no response found!)
  38 14.778395434   192.168.111.133  8.8.8.8          ICMP     98 Echo (ping) request  id=0x13bc, seq=1/256, ttl=63 (reply in 39)
  39 14.785155602   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=128 (request in 38)
  40 14.785207590   8.8.8.8          192.168.111.133  ICMP     98 Echo (ping) reply    id=0x13bc, seq=1/256, ttl=127
▸ Frame 40: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_76:d7:a9 (00:0c:29:76:d7:a9), Dst: Vmware_4f:67:ed (00:0c:29:4f:67:ed)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.111.133
▸ Internet Control Message Protocol
```

Figure 4. Attacker to Victim

Above is the ARP Spoofing evidence. Next is the MITM attack evidence. It shows that I successfully get the username and password from 140.113.41.24(https://e3.nycu.edu.tw/login/index.php), and the mitm_attack program can scan through the log file and print out the username and password to the console window.



cs2021@ubuntu: ~/Desktop/logdir
File Edit View Search Terminal Help

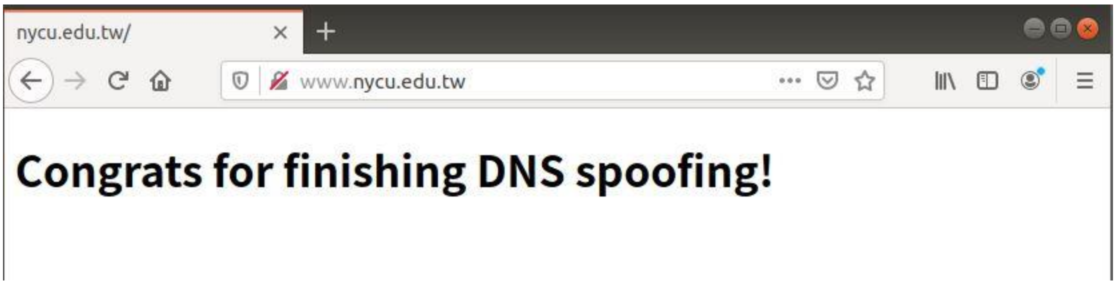
```
cs2021@ubuntu:~/Desktop$ sudo python3 mitm_attack.py
----------------------------------------
IP              MAC
----------------------------------------
192.168.111.137 00:0c:29:4f:67:ed
192.168.111.254 00:50:56:e4:b9:2d

Username:   testforpass
Password:   testforpass
```

```
44566-140.113.41.24,80.log
-rw-r--r-- 1 root   root        0 Apr 21 10:48 20210421T174818Z-192.168.111.137,
56240-140.113.41.24,443.log
-rw-r--r-- 1 root   root   275874 Apr 21 10:48 20210421T174825Z-192.168.111.137,
56242-140.113.41.24,443.log
-rw-r--r-- 1 root   root        0 Apr 21 10:48 20210421T174828Z-192.168.111.137,
56244-140.113.41.24,443.log
-rw-r--r-- 1 root   root        0 Apr 21 10:48 20210421T174828Z-192.168.111.137,
56246-140.113.41.24,443.log
-rw-r--r-- 1 root   root     4706 Apr 21 10:48 20210421T174828Z-192.168.111.137,
56248-140.113.41.24,443.log
-rw-r--r-- 1 root   root    24298 Apr 21 10:48 20210421T174828Z-192.168.111.137,
56250-140.113.41.24,443.log
-rw-r--r-- 1 root   root    24299 Apr 21 10:48 20210421T174828Z-192.168.111.137,
56252-140.113.41.24,443.log
cs2021@ubuntu:~/Desktop/logdir$ cat 20210421T174828Z-192.168.111.137,56252-140.1
13.41.24,443.log | grep -a username
cs2021@ubuntu:~/Desktop/logdir$ cat 20210421T174828Z-192.168.111.137,56250-140.1
13.41.24,443.log | grep -a username
cs2021@ubuntu:~/Desktop/logdir$ cat 20210421T174825Z-192.168.111.137,56242-140.1
13.41.24,443.log | grep -a username
username=testforpass&password=testforpass&captcha_code=0134HTTP/1.1 404 Not Foun
d
```

Figure 5. MITM attack evidence

- Item 2 (5%): please give evidence that you have finished the pharming attack Specify your scenario (I or II) and Illustrate your results based on some snapshots

  I use the Scenario II that use two VM and NAT mode to do the MITM attack. The following pictures are the pharming attack evidence.



Congrats for finishing DNS spoofing!

Figure 6. Pharming Attack Evidence

The evidence shows that when I what to go to http://www.nycu.edu.tw this website, the query will be modify by the attacker and redirect to a fake phishing web page.

- Item 3 (10%): please propose a solution that can defend against the ARP spoofing attack. No more than 200 English words

  We can use the DAI(Dynamic ARP Inspection) protection mechanism to defend against the ARP spoofing attack. To do this mechanism, we should build a table on switch which stores the correspondence between the IP address and the MAC address of the end host. The table can be built by DHCP snooping mechanism, which can prevent the illegal DHCP Server from causing incorrect client IP configuration information.

In this way, when the end host sends an ARP response which is difference with the record in the table, it means that this ARP response message is illegal. The switch will directly interrupt the connection between the attacker and switch, so that the other users network connection won't be interrupt. It ensures the normal use of the whole network.

Besides the above solution, there are still some other solutions. For example, we can build a static ARP table, but this method is more likely to do in a small network; Or we can set it that if I haven't send the ARP query, but I got an ARP response, then this response is probability sent by attacker so we ignore it.