CSC Project2 Report 0712223-0712254

ScenarioII		
VM1(Attacker)	IP= 192.168.79.132	MAC= 00:0c:29:09:2c:d8
VM2(Victim)	IP= 192.168.79.133	MAC= 00:0c:29:cc:75:5d
AP	IP= 192.168.79.2	MAC= 00:50:56:f9:1b:be

- **Item1 : please give evidence that you have finished the MITM attack**
  - **ARP spoofing (victim's aspect)**

```
cs2021@ubuntu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.79.254           ether   00:50:56:fd:e3:40   C                     ens33
192.168.79.132           ether   00:0c:29:09:2c:d8   C                     ens33
_gateway                 ether   00:50:56:f9:1b:be   C                     ens33
cs2021@ubuntu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.79.254           ether   00:50:56:fd:e3:40   C                     ens33
192.168.79.132           ether   00:0c:29:09:2c:d8   C                     ens33
_gateway                 ether   00:0c:29:09:2c:d8   C                     ens33
```

(before)

(after)

  - **victim: ping 8.8.8.8 (attacker's Wireshark aspect)**

request : victim→attacker

```
    3 0.257038… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/1
    4 0.258105… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/1
    5 0.263872… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/1
    6 0.264739… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/1
▸ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_cc:75:5d (00:0c:29:cc:75:5d), Dst: Vmware_09:2c:d8 (00:0c:29:09:2c:d8)
▸ Internet Protocol Version 4, Src: 192.168.79.133, Dst: 8.8.8.8
```

request : attacker→AP

```
    3 0.257038… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/
    4 0.258105… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/
    5 0.263872… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/
    6 0.264739… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/
▸ Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_09:2c:d8 (00:0c:29:09:2c:d8), Dst: Vmware_f9:1b:be (00:50:56:f9:1b:be)
▸ Internet Protocol Version 4, Src: 192.168.79.133, Dst: 8.8.8.8
```

reply : AP→attacker

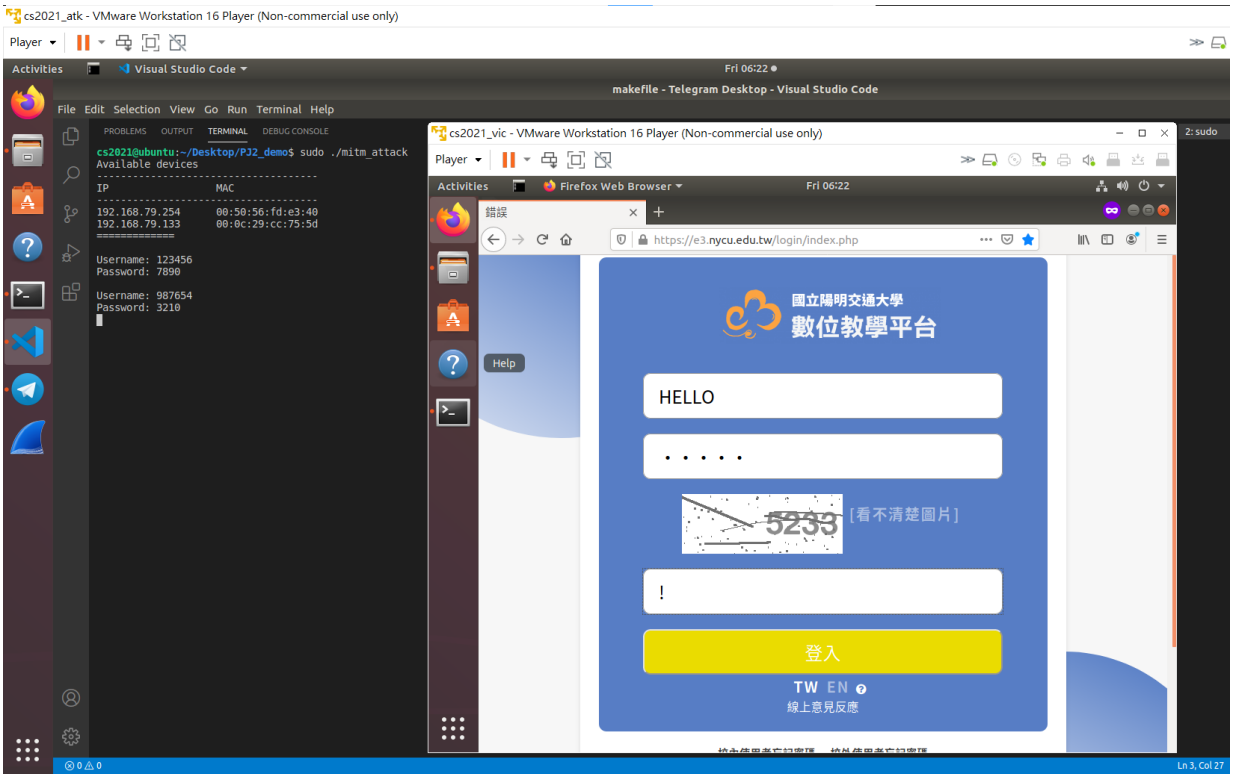
```
    3 0.257038… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/
    4 0.258105… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/
    5 0.263872… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/
    6 0.264739… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/
▸ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_f9:1b:be (00:50:56:f9:1b:be), Dst: Vmware_09:2c:d8 (00:0c:29:09:2c:d8)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.79.133
```

reply : attacker→victim

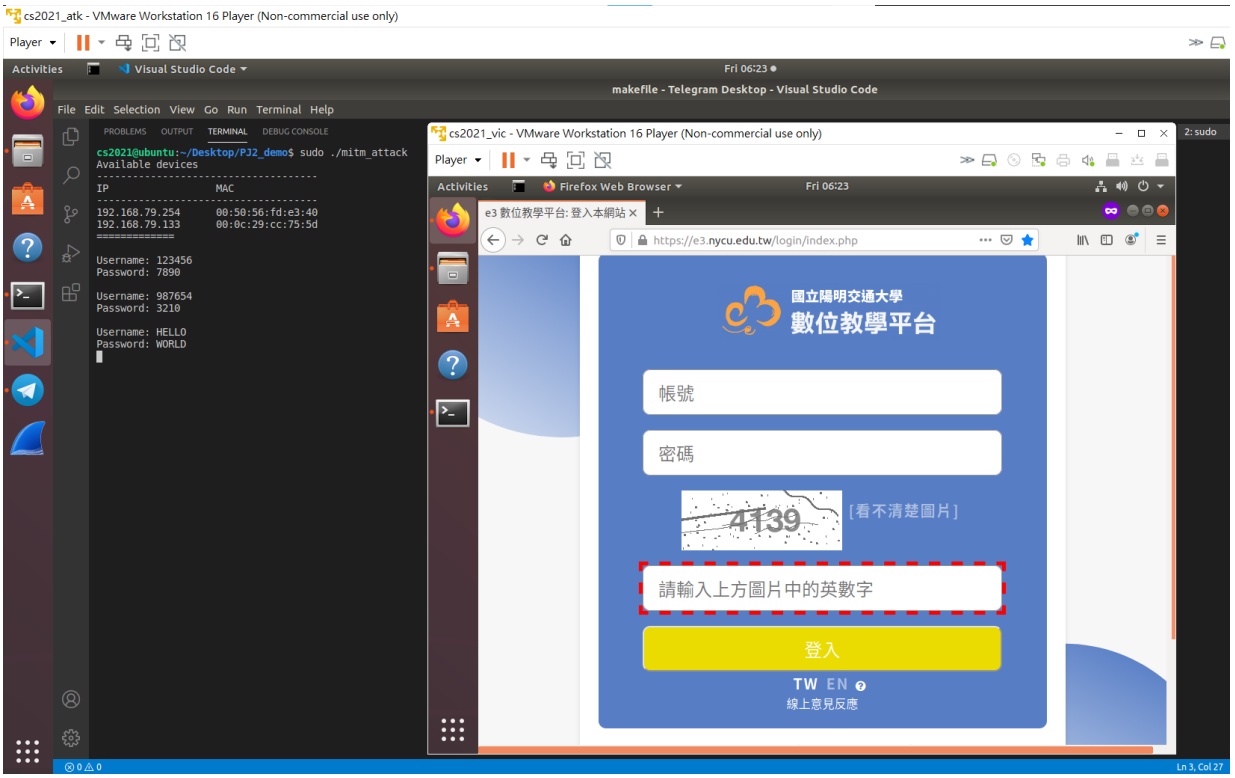
```
    3 0.257038… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/
    4 0.258105… 192.168.79.133  8.8.8.8          ICMP    98 Echo (ping) request  id=0x1034, seq=67/
    5 0.263872… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/
    6 0.264739… 8.8.8.8         192.168.79.133  ICMP    98 Echo (ping) reply    id=0x1034, seq=67/
▸ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_09:2c:d8 (00:0c:29:09:2c:d8), Dst: Vmware_cc:75:5d (00:0c:29:cc:75:5d)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.79.133
```

- **SSL Split on Encrypted Connections**

  Attacker uses the command ‘sslsplit’ to sniff connections.



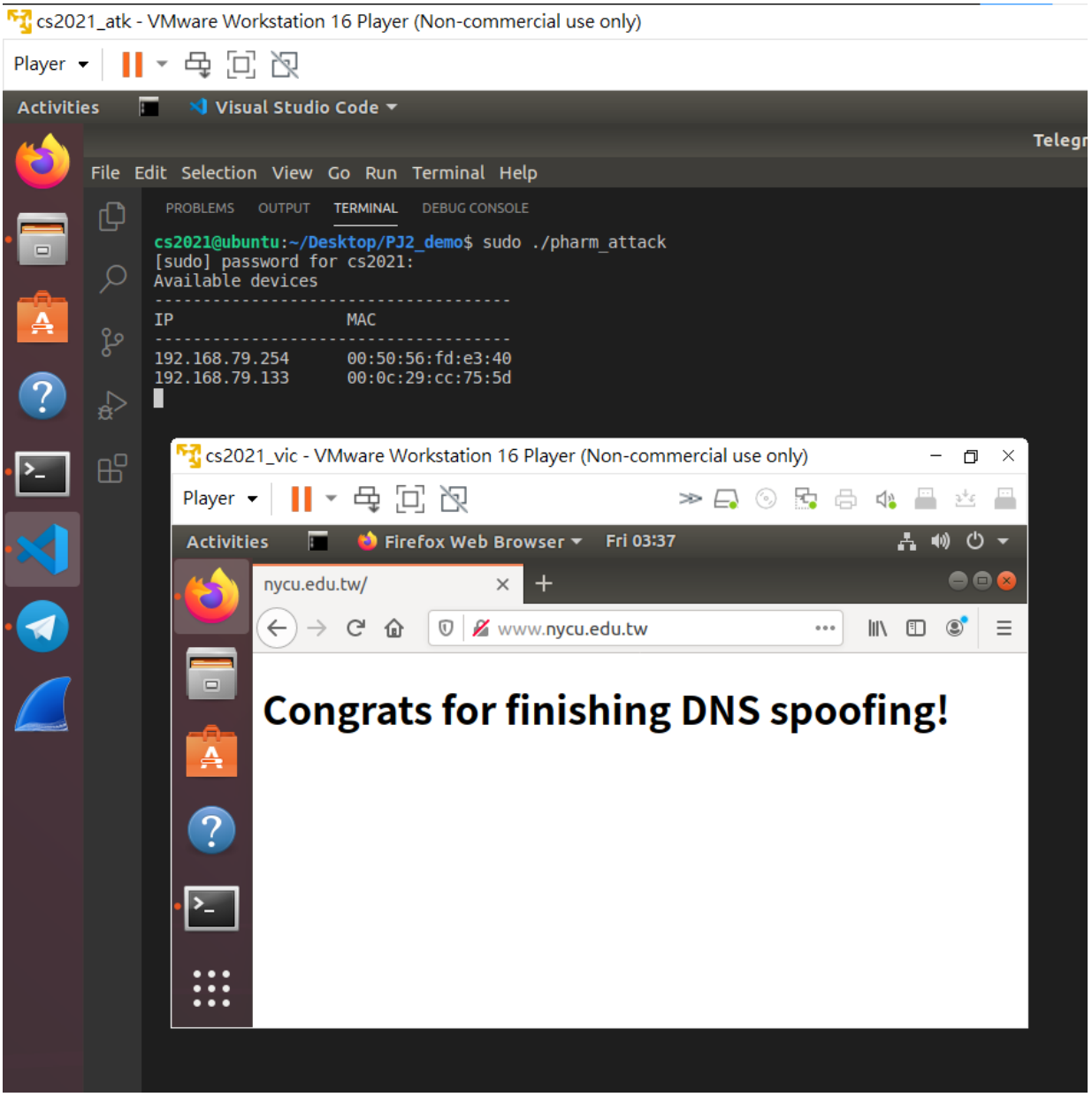
Victim logs into the website, then the attacker gets the information.



- **Item2 : please give evidence that you have finished the pharming attack**

  Attacker's terminal launches the pharming attack.

  Victim's browser(Firefox) shows the phishing web.



- **Item3 : please propose a solution that can defend against the ARP spoofing attack**
  - Use spoofing detection software to monitor ARP traffic and look for mapping inconsistencies.
  - Use encrypted and authenticated protocols to authenticate the application or device to which you're connecting, and encrypt data in transit.