Item 1 (5%): please give evidence that you have finished the MITM attack

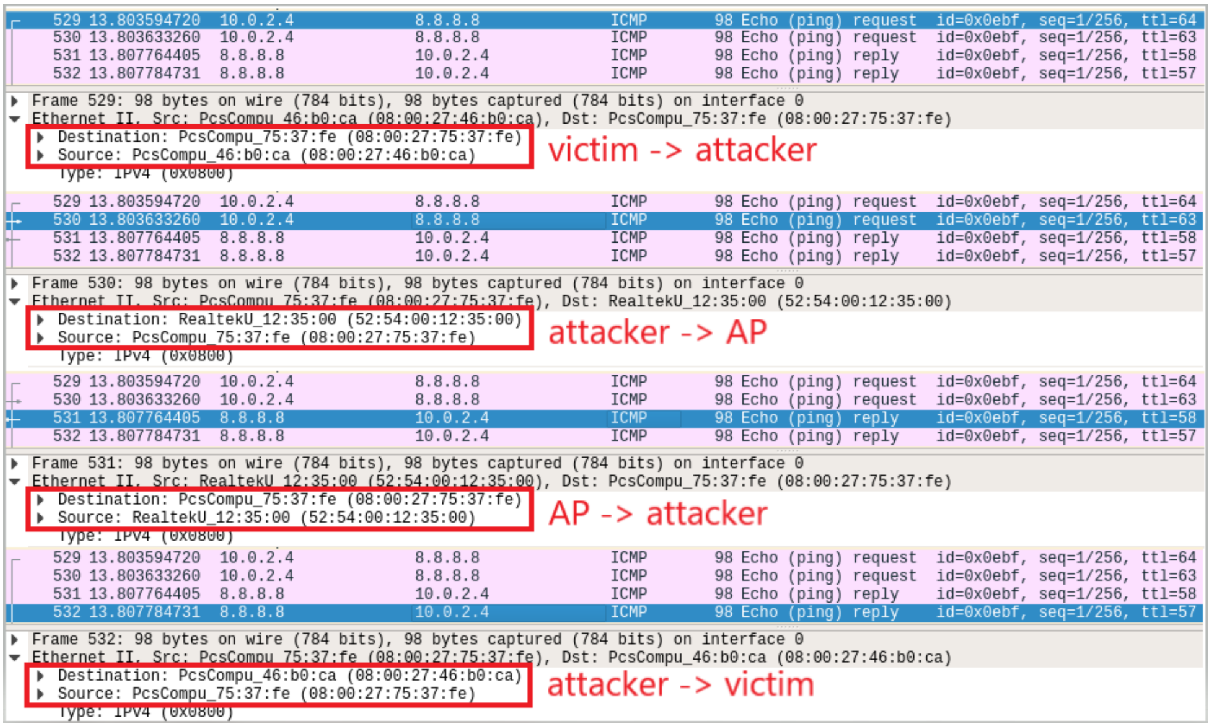
Ans:

scenario (II)
attacker { ip : 10.0.2.15 , mac : 08:00:27:75:37:fe }
vitim { ip : 10.0.2.4 , mac : 08:00:27:46:b0:ca }
gateway { ip : 10.0.2.1 , mac : 52:54:00:12:35:00 }

victim arp table screenshot:

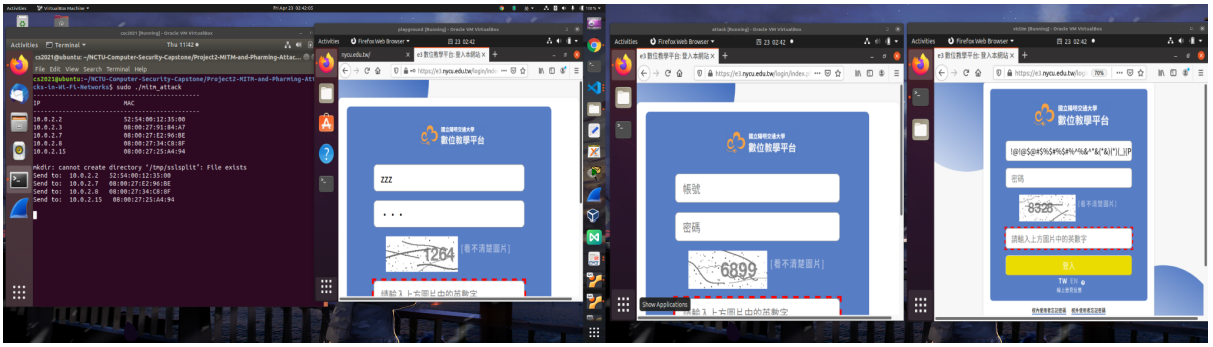
```
user@ubuntu:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.15                ether   08:00:27:75:37:fe   C                     enp0s3
_gateway                 ether   08:00:27:75:37:fe   C                     enp0s3
```

attacker wireshark screenshot:

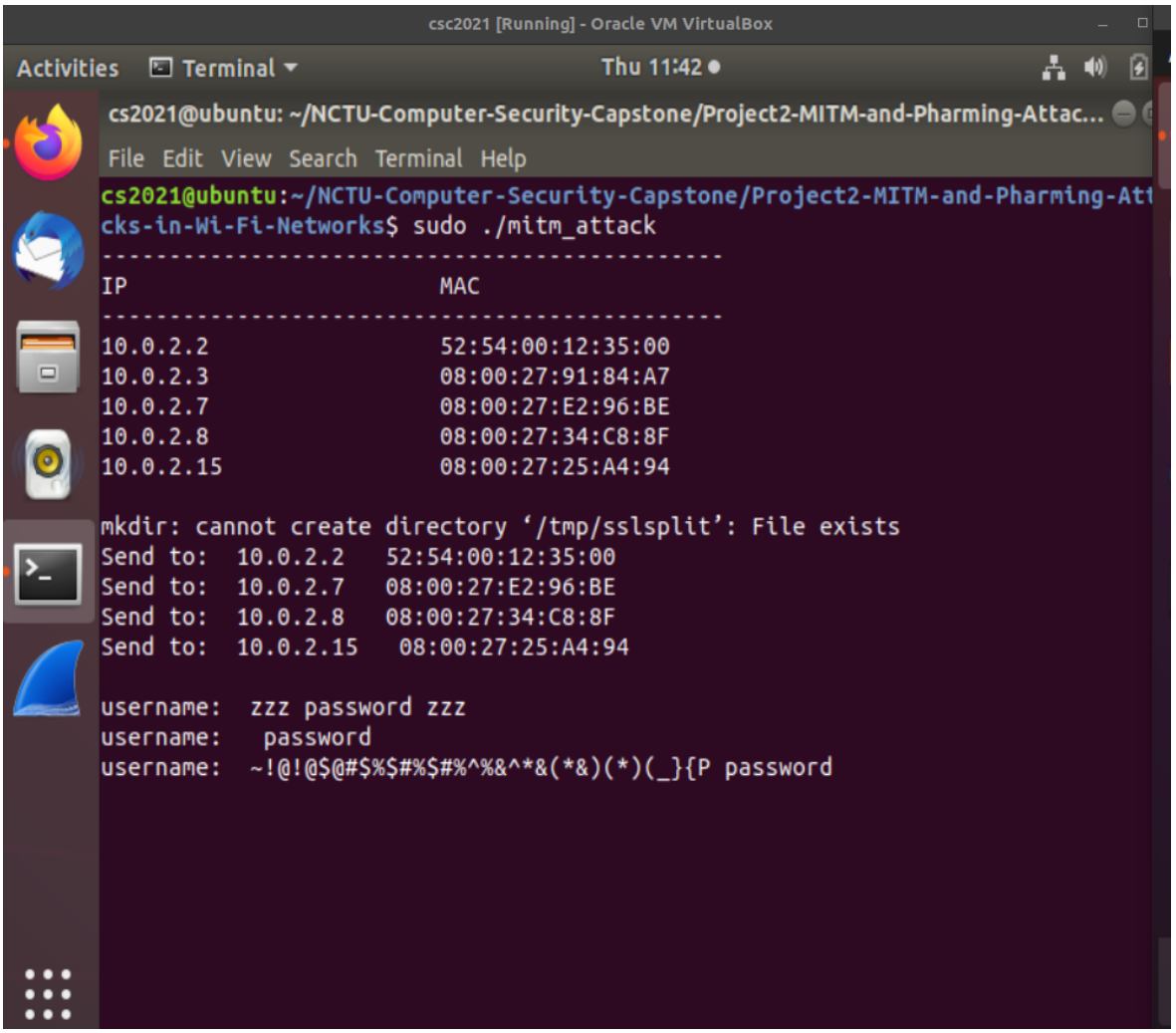


Print out the username and password which a user submits to the website:

We prepared three VMs for testing, the left one using normal password just consisting of letters. The middle one will submit an empty username and password. The right one will submit a username consisting of many complex symbols and without password.



The result is correct :

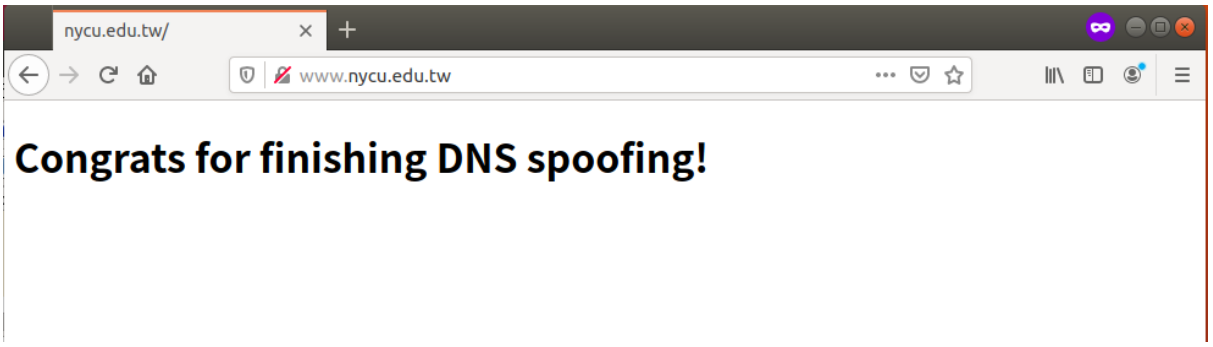


Item 2 (5%): please give evidence that you have finished the pharming attack

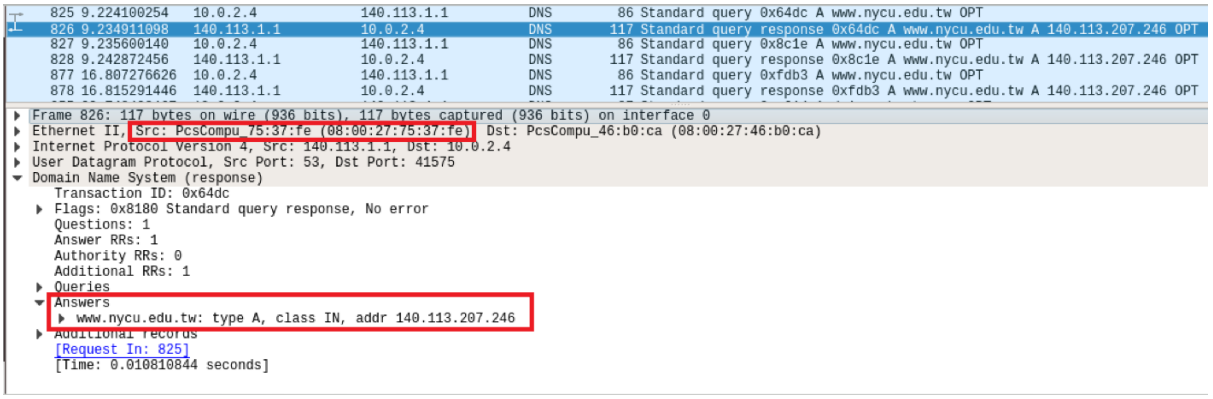
Ans:

scenario (II)

victim browser:



victim wireshark:



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

Ans:

We can use DHCP snooping to prevent from ARP spoofing attack. DHCP snooping is a series of techniques applied to improve the security of a DHCP infrastructure, in particular, it listens on packet through the authorized DHCP server and construct DHCP binding table, which in each record include an IP with a corresponding MAC address, and thus results in denial of ARP spoofing attack.