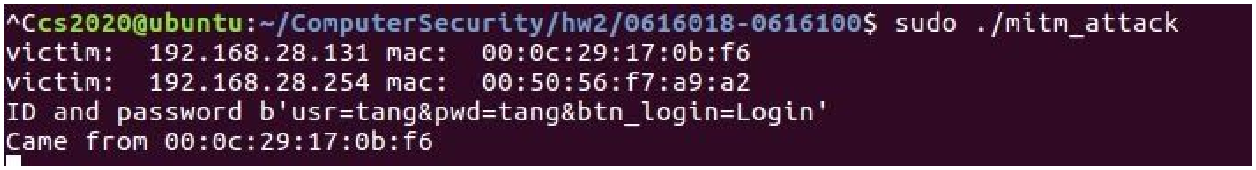
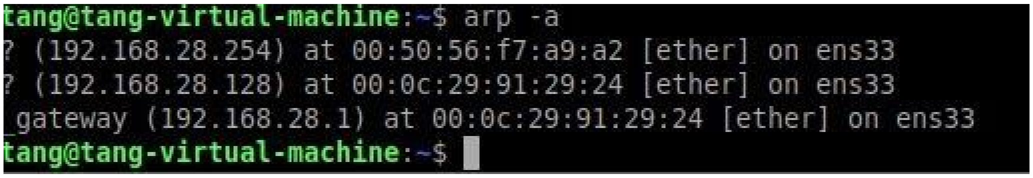
please give evidence that you have finished the MitM attack

Attacker Side:



```
^Ccs2020@ubuntu:~/ComputerSecurity/hw2/0616018-0616100$ sudo ./mitm_attack
victim:  192.168.28.131 mac:  00:0c:29:17:0b:f6
victim:  192.168.28.254 mac:  00:50:56:f7:a9:a2
ID and password b'usr=tang&pwd=tang&btn_login=Login'
Came from 00:0c:29:17:0b:f6
```

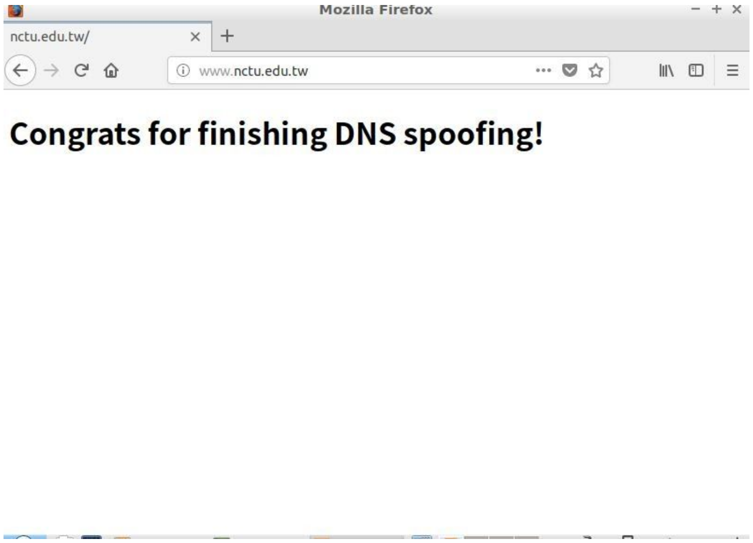
Victim Side:



```
tang@tang-virtual-machine:~$ arp -a
? (192.168.28.254) at 00:50:56:f7:a9:a2 [ether] on ens33
? (192.168.28.128) at 00:0c:29:91:29:24 [ether] on ens33
_gateway (192.168.28.1) at 00:0c:29:91:29:24 [ether] on ens33
tang@tang-virtual-machine:~$
```

please give evidence that you have finished the pharming attack

Victim Side:



Congrats for finishing DNS spoofing!

please propose a solution that can defend against the ARP spoofing attack

1. Use static arp table which can not be modified by unauthenticated attacker to prevent the attacker to do arp spoofing.

2. Use DHCP snooping which can preserve all devices' MAC addresses and it is able to detect the fake packet.

3. Monitor the arp response and notify administration when there is any abnormal change of arp table.