

Ans:

```
gateway { ip : 10.0.2.1    , mac : 52:54:00:12:35:00 }
```

victim arp table screenshot:

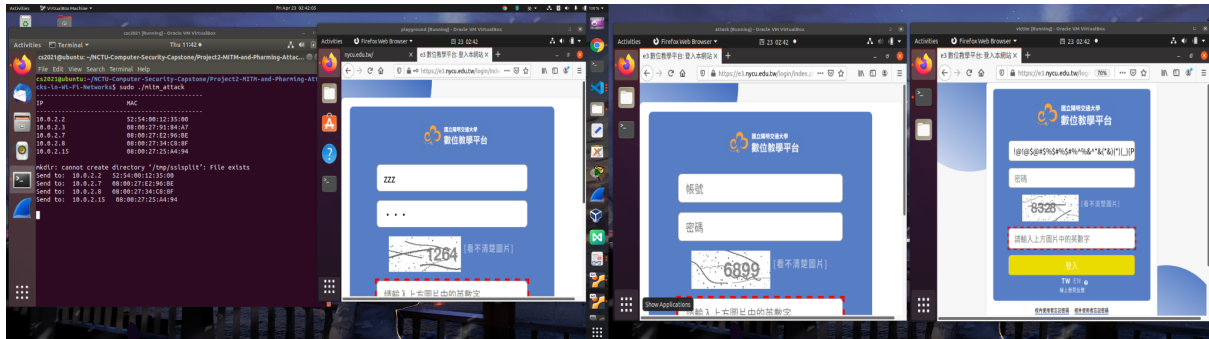
```
user@ubuntu:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.15        ether    08:00:27:75:37:fe  C           enp0s3
_gateway         ether    08:00:27:75:37:fe  C           enp0s3
```

attacker wireshark screenshot:

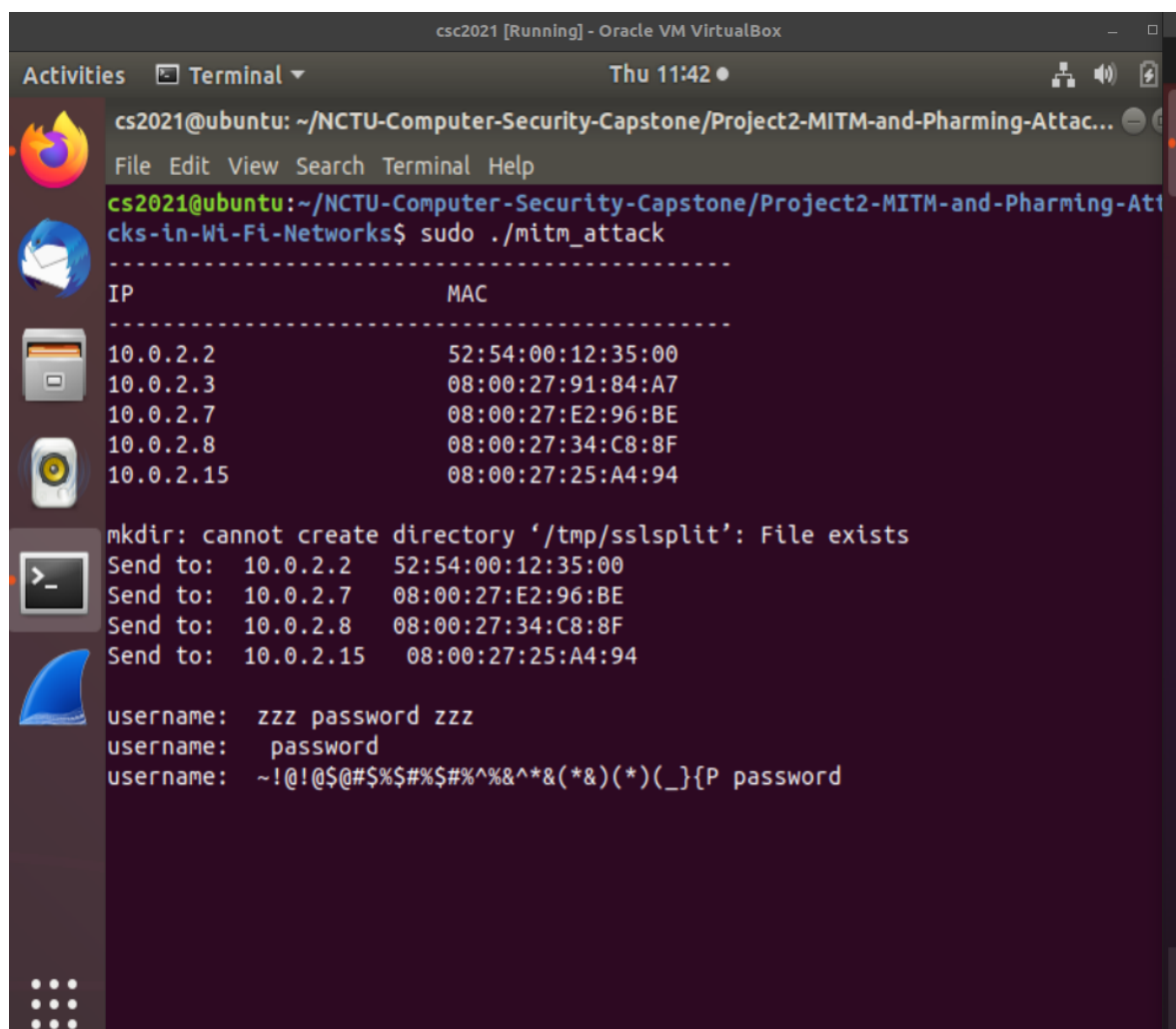
529	13.803594720	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=64
530	13.803633260	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=63
531	13.807764405	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=58
532	13.807784731	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=57
▶ Frame 529: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0						
▼ Ethernet II, Src: PcsCompu_46:b0:ca (08:00:27:46:b0:ca), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)						
		Destination: PcsCompu_75:37:fe (08:00:27:75:37:fe)		victim -> attacker		
		Source: PcsCompu_46:b0:ca (08:00:27:46:b0:ca)				
		Type: IPv4 (0x0800)				
529	13.803594720	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=64
530	13.803633260	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=63
531	13.807764405	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=58
532	13.807784731	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=57
▶ Frame 530: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0						
▼ Ethernet II, Src: PcsCompu_75:37:fe (08:00:27:75:37:fe), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)						
		Destination: RealtekU_12:35:00 (52:54:00:12:35:00)		attacker -> AP		
		Source: PcsCompu_75:37:fe (08:00:27:75:37:fe)				
		Type: IPv4 (0x0800)				
529	13.803594720	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=64
530	13.803633260	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=63
531	13.807764405	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=58
532	13.807784731	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=57
▶ Frame 531: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0						
▼ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_75:37:fe (08:00:27:75:37:fe)						
		Destination: PcsCompu_75:37:fe (08:00:27:75:37:fe)		AP -> victim		
		Source: RealtekU_12:35:00 (52:54:00:12:35:00)				
		Type: IPv4 (0x0800)				
529	13.803594720	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=64
530	13.803633260	10.0.2.4	8.8.8.8	ICMP	98 Echo (ping) request	id=0x0ebf, seq=1/256, ttl=63
531	13.807764405	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=58
532	13.807784731	8.8.8.8	10.0.2.4	ICMP	98 Echo (ping) reply	id=0x0ebf, seq=1/256, ttl=57
▶ Frame 532: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0						
▼ Ethernet II, Src: PcsCompu_75:37:fe (08:00:27:75:37:fe), Dst: PcsCompu_46:b0:ca (08:00:27:46:b0:ca)						
		Destination: PcsCompu_46:b0:ca (08:00:27:46:b0:ca)		attacker -> victim		
		Source: PcsCompu_75:37:fe (08:00:27:75:37:fe)				
		Type: IPv4 (0x0800)				

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 :

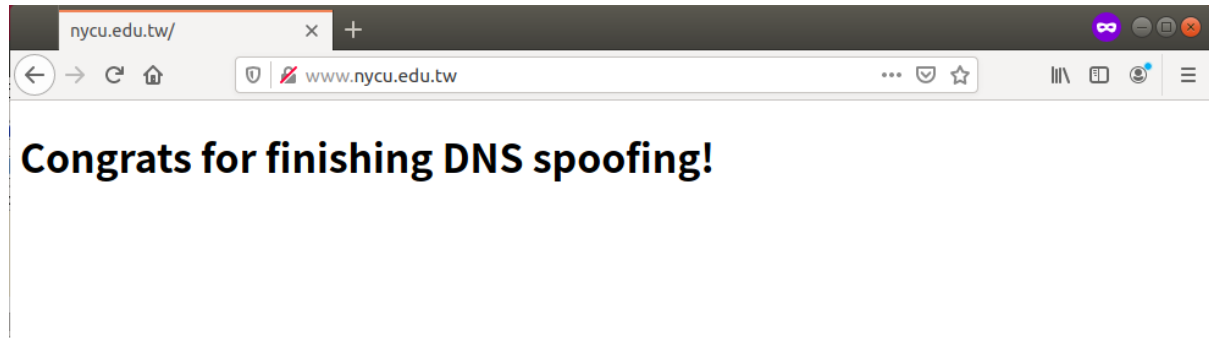


Item 2 (5%): please give evidence that you have finished the phishing attack

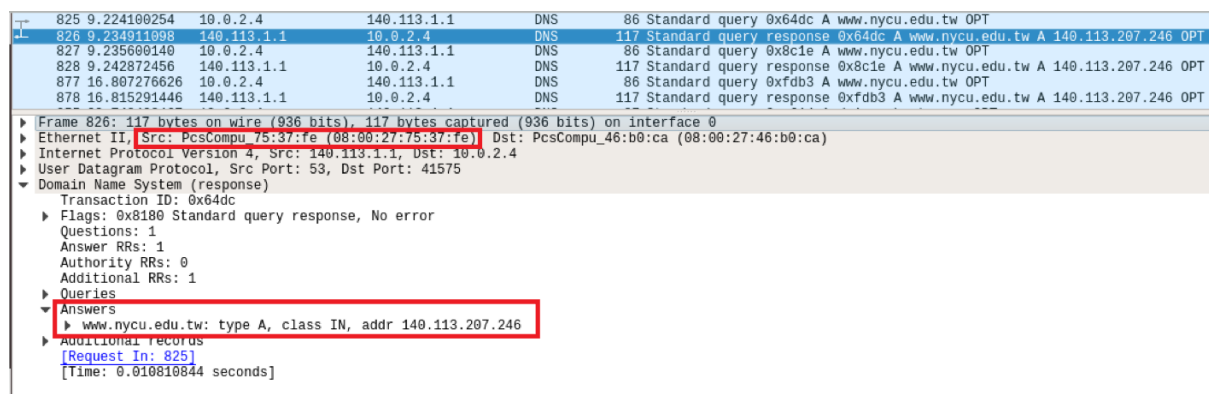
Ans:

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.