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:

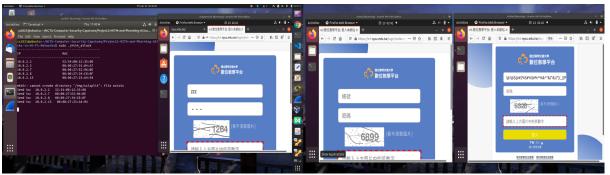
user@ubuntu:~\$ arp				
Address	HWtype	HWaddress	Flags Mask	Iface
10.0.2.15	ether	08:00:27:75:37:fe	C	enp0s3
_gateway _	ether	08:00:27:75:37:fe	С	enp0s3

attacker wireshark screenshot:

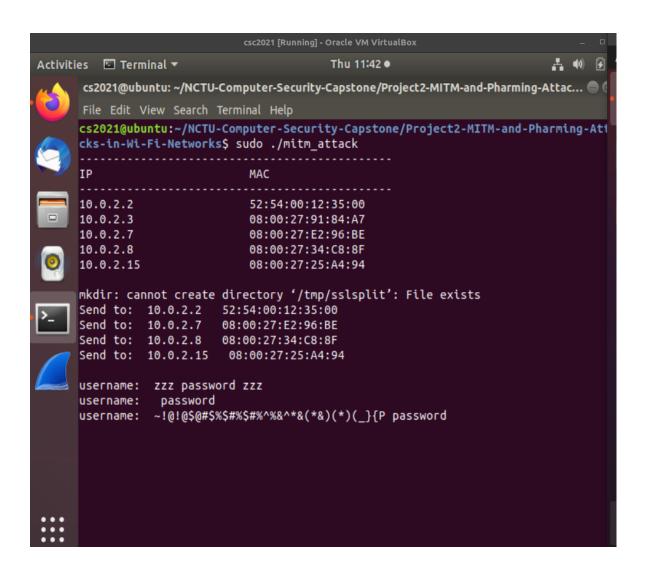
_	529 13.803	594720	10.0.2.4	8.8.8.8	ICMP	98 Echo				seq=1/256,				
	530 13.803		10.0.2.4	8.8.8.8	ICMP			request						
	531 13.807			10.0.2.4	ICMP	98 Echo				seq=1/256,				
	532 13.807	784731	8.8.8.8	10.0.2.4	ICMP	98 Echo	(ping)	reply	id=0x0ebf,	seq=1/256,	tt1=57			
▶ Frame 529: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0														
	Ethernet II. Src: PcsCompu 46:b0:ca (08:00:27:46:b0:ca), Dst: PcsCompu 75:37:fe (08:00:27:75:37:fe)													
Destination, DesCompy 75:07:50 (00:00:07:75:07:50)														
				08:00:27:46:b0:ca)	victim -> a	attack	er							
Type: 1994 (0X0800)														
		•			TOUR					4 (050				
	529 13.803			8.8.8.8	ICMP				id=0x0ebf,					
+•	530 13.803		10.0.2.4	8.8.8.8	ICMP				id=0x0ebf,					
-	531 13.807			10.0.2.4	ICMP	98 Echo				seq=1/256,				
	532 13.807	/84/31	8.8.8.8	10.0.2.4	ICMP	98 Echo	(ping)	reply	ld=⊎x⊍ebT,	seq=1/256,	tt1=5/			
▶ E	rame 530: 9	8 bytes	on wire (7	84 bits), 98 bytes capture	ed (784 bits) on	interface	0							
				37:fe (08:00:27:75:37:fe),				0:12:35:	00)					
				.00 (50.54.00.40.05.00)	_	,			,					
				08:00:27:75:37:fe)	attacker -:	> AP								
	Type: IPv	4 (0x08	JU)											
	529 13.803	-		8.8.8.8	ICMP	08 Echo	(ning)	request	id-OvOohf	seq=1/256,	t+1-64			
П.	530 13.803		10.0.2.4	8.8.8.8	ICMP			request		seq=1/256,				
	531 13.807		8.8.8.8	10.0.2.4	ICMP	98 Echo				sea=1/256.				
	532 13.807			10.0.2.4	ICMP	98 Echo				seg=1/256,				
<u> </u>								, cpr)	20 0/100017	554 17 2557				
				84 bits), 98 bytes capture										
				35:00 (52:54:00:12:35:00),	, Dst: PcsCompu_7	5:37:fe (08:00:2	7:75:37:	te)					
				:fe (08:00:27:75:37:fe)	AP -> atta	ckor								
				52:54:00:12:35:00)	Ar -> alla	ickei								
	Type: IPV													
Г	529 13.803			8.8.8	ICMP			request		seq=1/256,				
	530 13.803			8.8.8.8	ICMP			request		seq=1/256,				
	531 13.807			10.0.2.4	ICMP	98 Echo				seq=1/256,				
	532 13.807	784731	8.8.8.8	10.0.2.4	ICMP	98 Echo	(ping)	reply	id=0x0ebf,	seq=1/256,	tt1=57			
b E	rame 532: 9	8 bytes	on wire (7	84 bits), 98 bytes capture	ed (784 bits) on	interface	0							
								7:46:b0:	ca)					
	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)													
> bestination: PcsCompu_46:09:26 (08:09:27:46:09:ca) attacker -> victim														
Type: 1PV4 (exb80e)														
		_ `												

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:

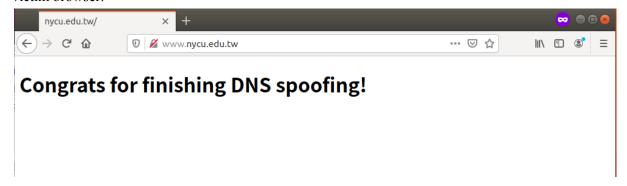


Item 2 (5%): please give evidence that you have finished the pharming attack

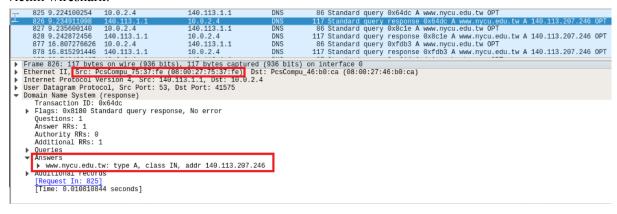
Ans:

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.