Lab2 : TLS MITM Attack

This lab is related to Transport Layer Security Protocol and Man in the Middle Attacks. Transport Layer Security protocol gives data integrity and privacy between two application which communicate with each other. It provides message authentication and is utilised for web browsers and similar application which need secret trading of information over a network which can be message exchanging or file sharing.

Address Resolution Protocol spoofing is also a kind of an attack where an attacker sends on LAN fake messages which can lead to link the MAC address of the attacker with the correct server‘s IP address on the same network. The attacker then start receiving the messages that are actually for the IP address of the original system which is the victim here.This allows the adversaries to modify , stop and read the data that are exchanged on the network.

A MITM attack is a man in the middle attack which happens when a communication between two systems is caught by an external entity. Secure Socket Layer strip is a type of man in the middle attack where the browser of a victim is forced to communicate with an attacker using plain text (HTTP). It takes place by using the proxy designed by attacker. Secure Socket Layer certificates errors are not displayed by the browser in case of SSL stripping and victim will never know about the attack which takes place. Therefore, when a connection is by the browser of the victim is brought down from HTTPS to HTTP, then it is known as HTTP downgrading attacks. This lab is related to the same attacks where we use three machine which as as a server, attacker and victim.

Server is the external router machine, Kali machine is the attacker and Windows XP machine is the victim. The Secure Socket Layer stripping is started on the Kali machine which is the attacker and then, the victim tries to access the URL http://fakebook.vlab.local. The browser of victim and the attacker are connected to each other and is continuously waiting for a reply from the server. Further, the attacker sends the request of the victim and then waits for a response from the server. All communication happens using a Secure Socket Layer tunnel and therefore, there is a secure connection established between victim and server. After there is a reply from the server, the login page is seen on the browser. Attacker has now the access and can modify the responses it receives from the server and converts https to http. The attacker can easily access the log in webpage which is the reply from server and change the server response from HTTPS to HTTP. The web page can now browse the login

Archit Goyal
Ag6288
N17398125

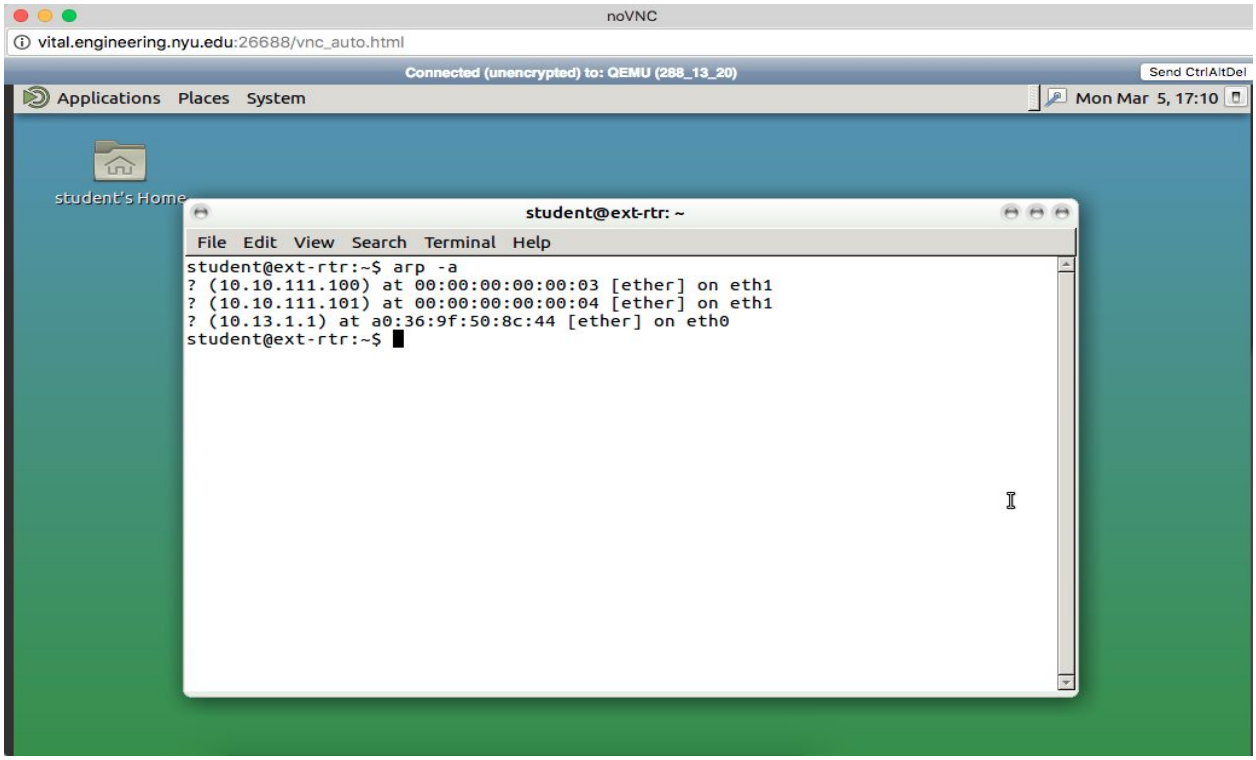
webpage but the connection established is not secure because of which all the requests from the victim's machine now is passed as a plain text which can be easily modified and also access the credential which is collected in the SSLstrip log file.

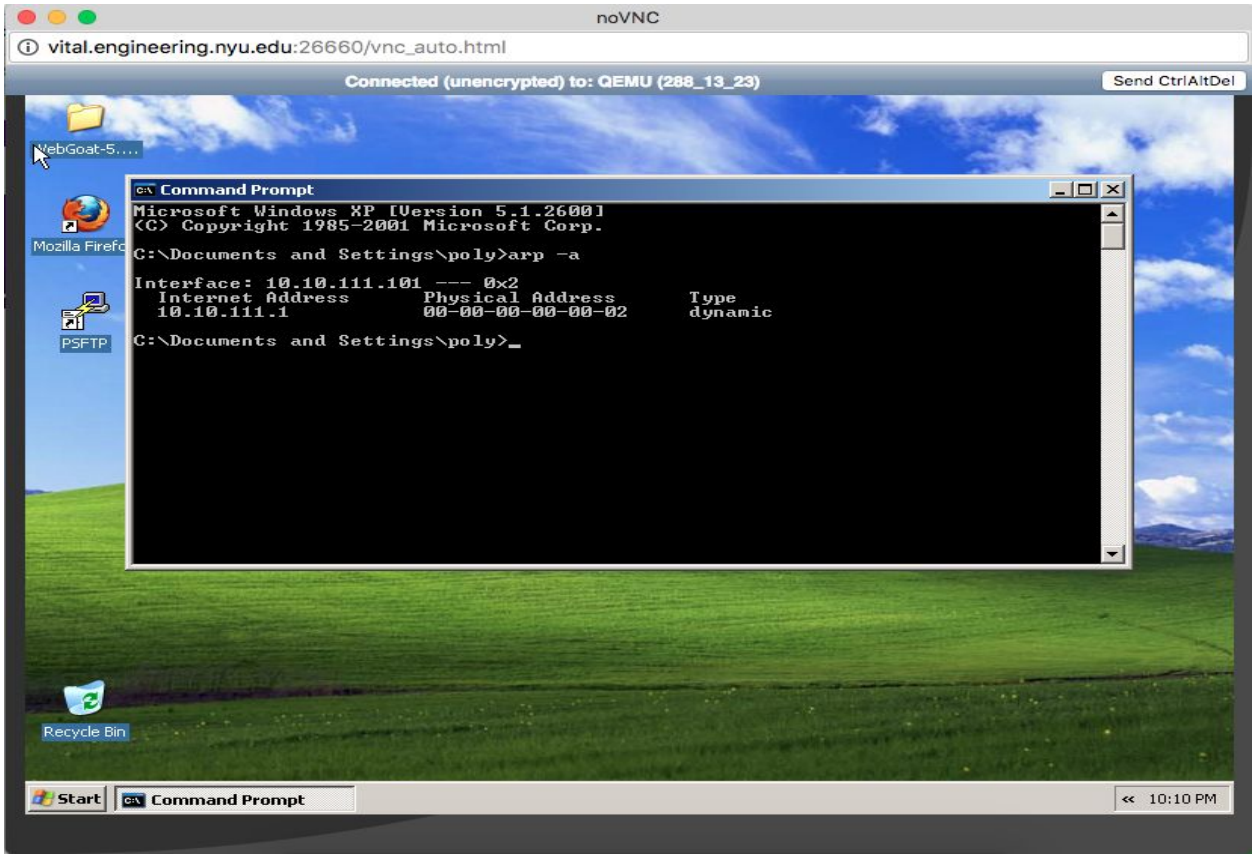
Steps to perform the attack :

1. Start the external router, Kali and Windows xp machine in order and then try to access the url http:fakebook.vlab.local on the Kali machine.

2. Run command **arp -a** on the Windows xp and external router machine so that we can get the information. MAC address of adversary is **00:00:00:00:00:03.**

Archit Goyal
Ag6288
N17398125





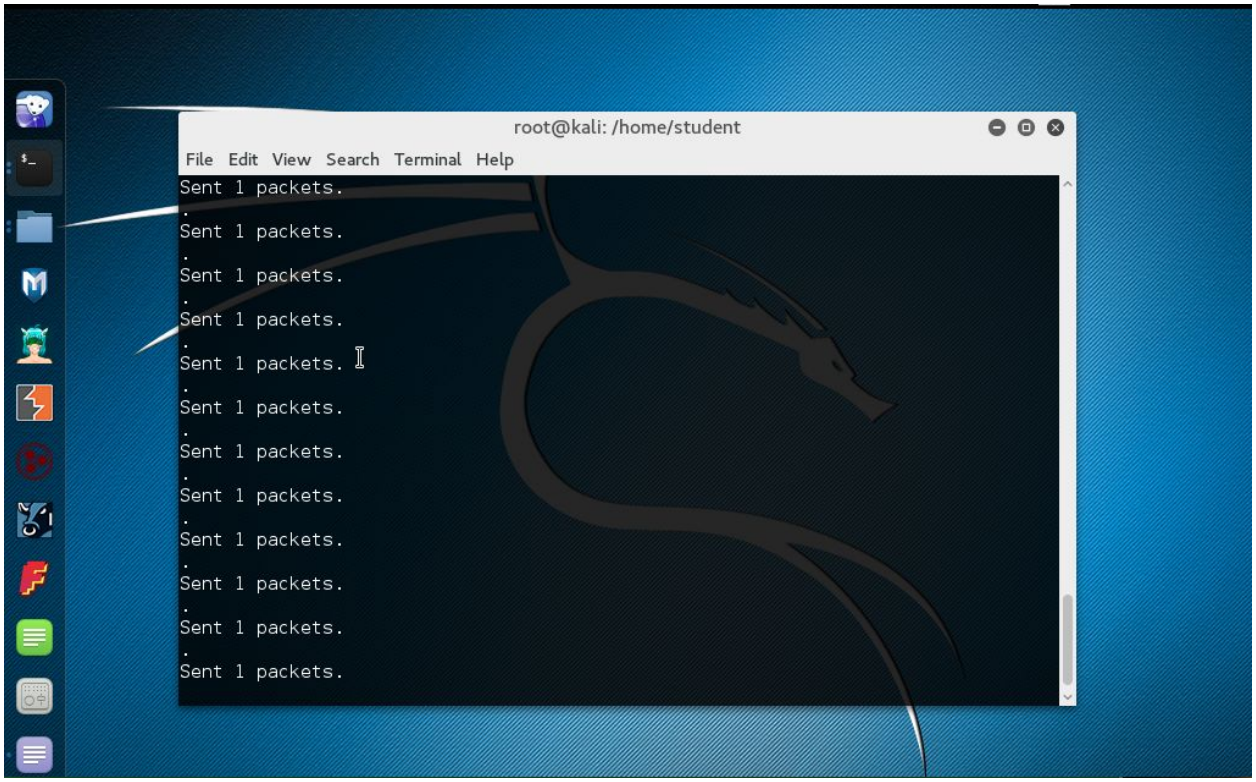
Archit Goyal
Ag6288
N17398125

3. Run the following commands one by one

- **sudo su**
- **echo “1” > /proc/sys/net/ipv4/ip_forward**
- **iptables -t nat -A PREROUTING -p tcp --destination-port 80 - j REDIRECT --to-port 8080**

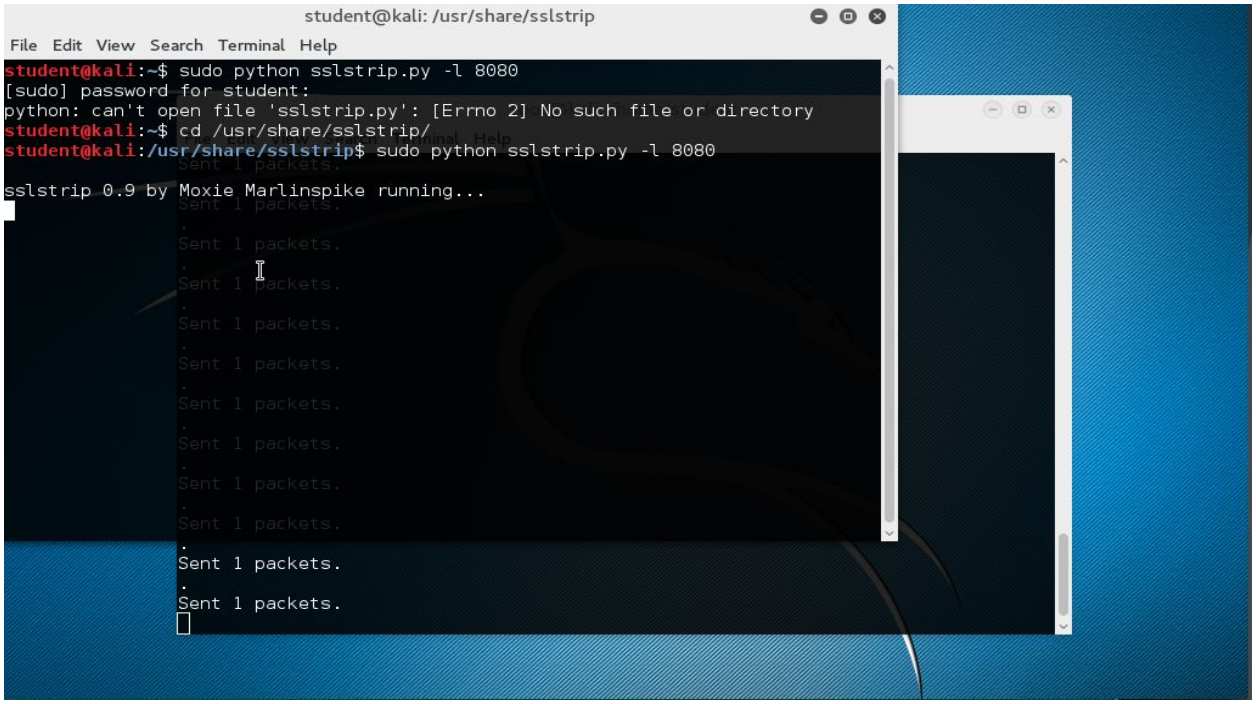
The first command is used to give root privileges. The second command is used to accept the inbound packets and then send it out and the other way round. The third commanda helps in modifying the IP table. All the traffic will now be redirected to the 8080 port address.

4. Then we write a python script to which sends gratuitous ARP messages from Kali to both the Windows XP machine and the external router machine and then the program is run on the Kali machine. ARP spoofing attack is completed in this step.

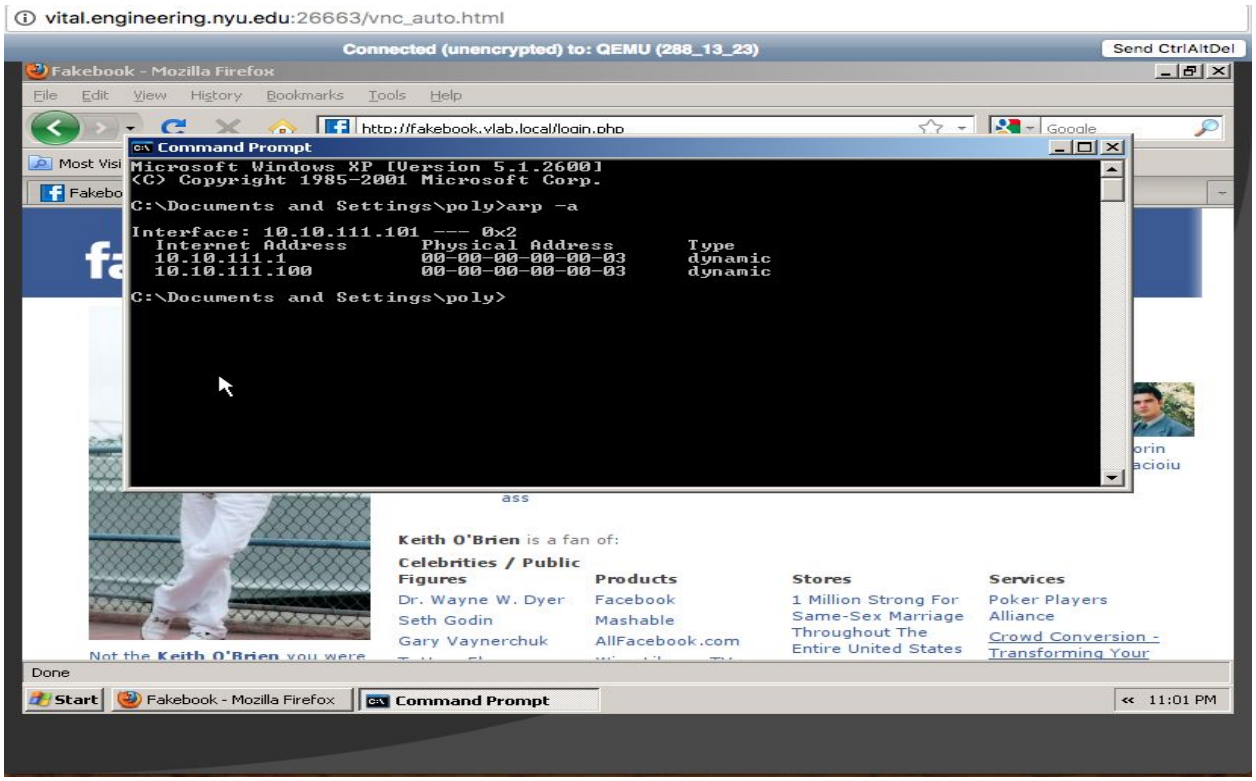


5. On the Kali machine, a new terminal is opened and then we use it for the SSL Stripping using the command **python sslstrip.py -l 8080** at the location **/usr/share/sslstrip**. This is the SSL strip attack and it hijacks the HTTP traffic on the

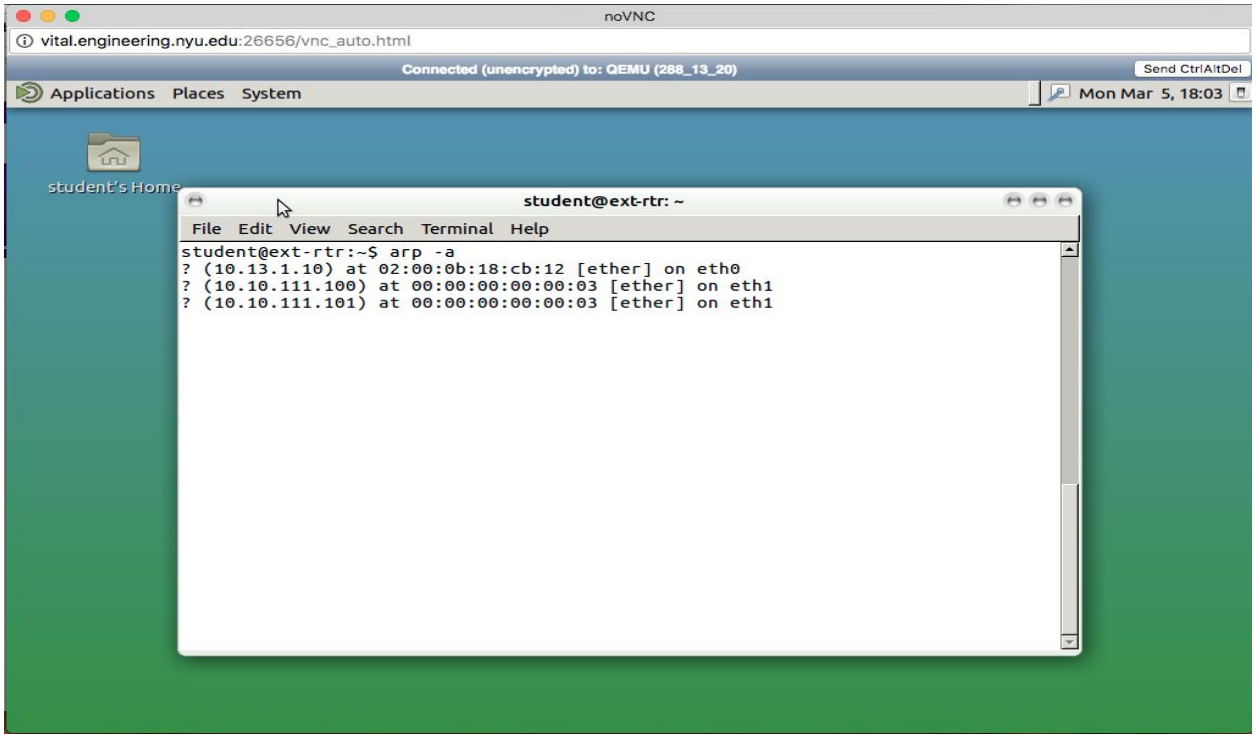
network. All the traffic is redirected to 8080.



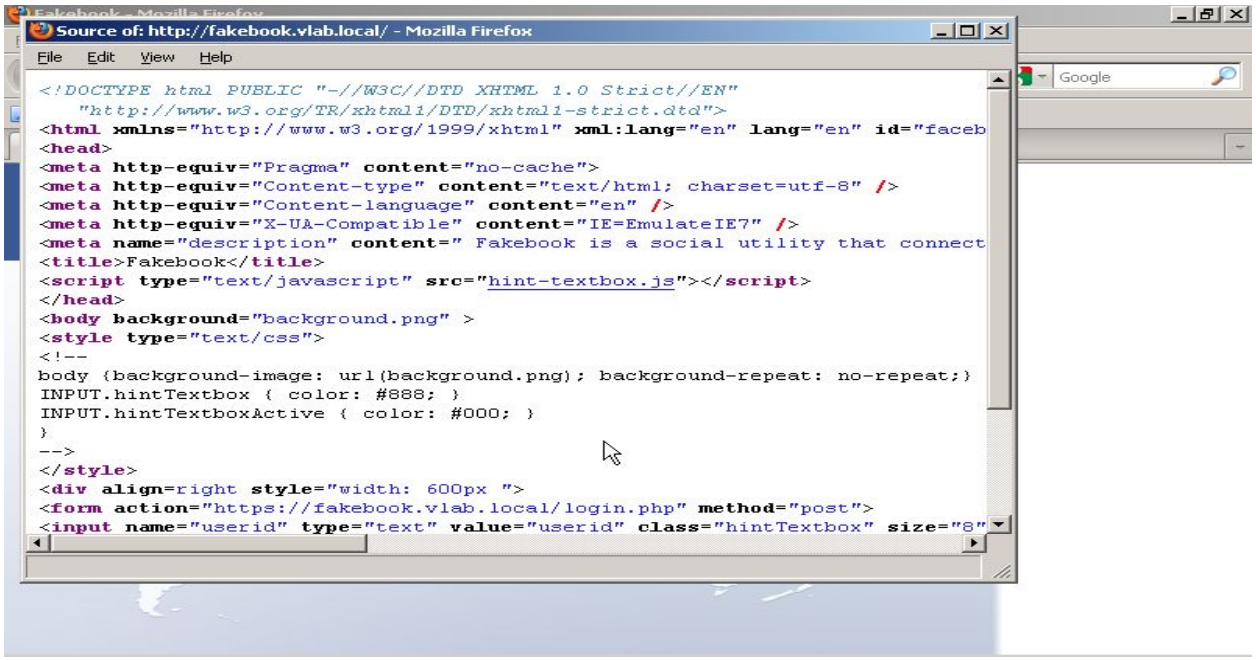
6. Check for the ARP entries after the attack and the Physical address is changed to the one of the Kali machine which is the attacker for both the Windows machine and the external router. We see that the Physical address in the entries is the same as MAC address of the adversary which is **00:00:00:00:00:03** in both router and client machine.



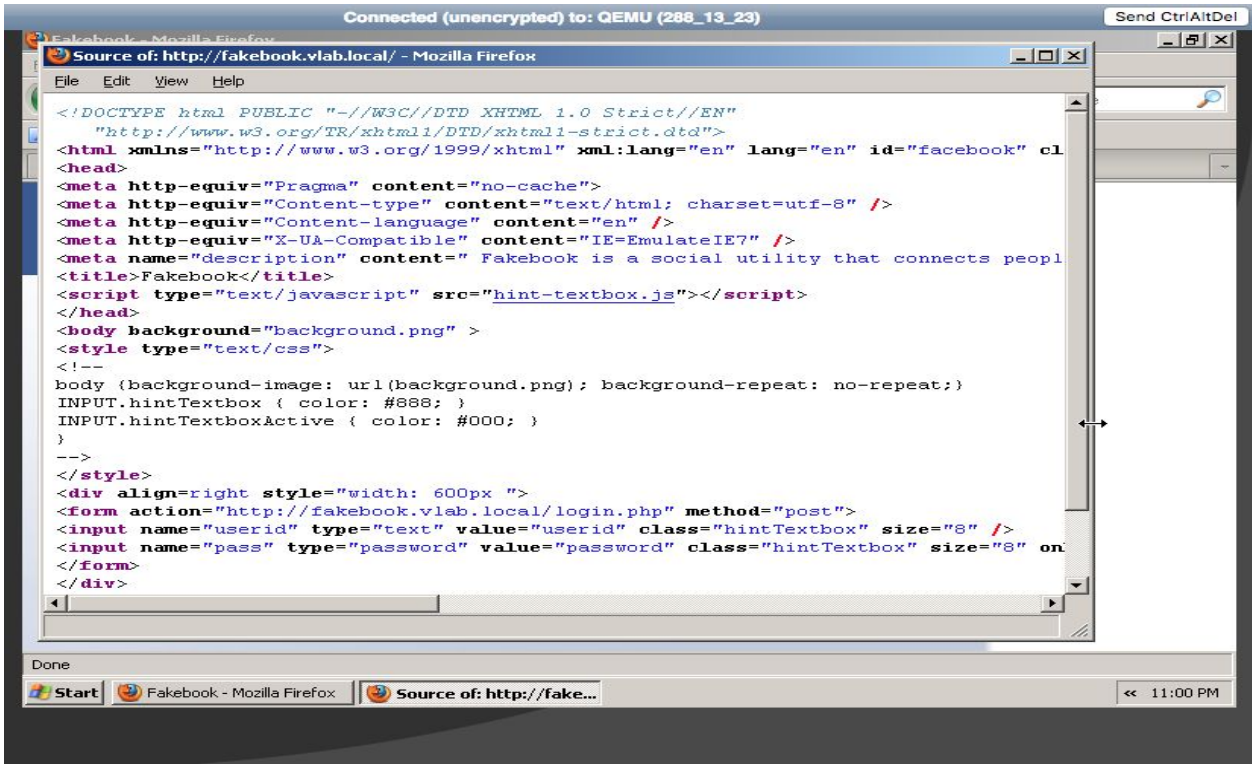
Archit Goyal
Ag6288
N17398125

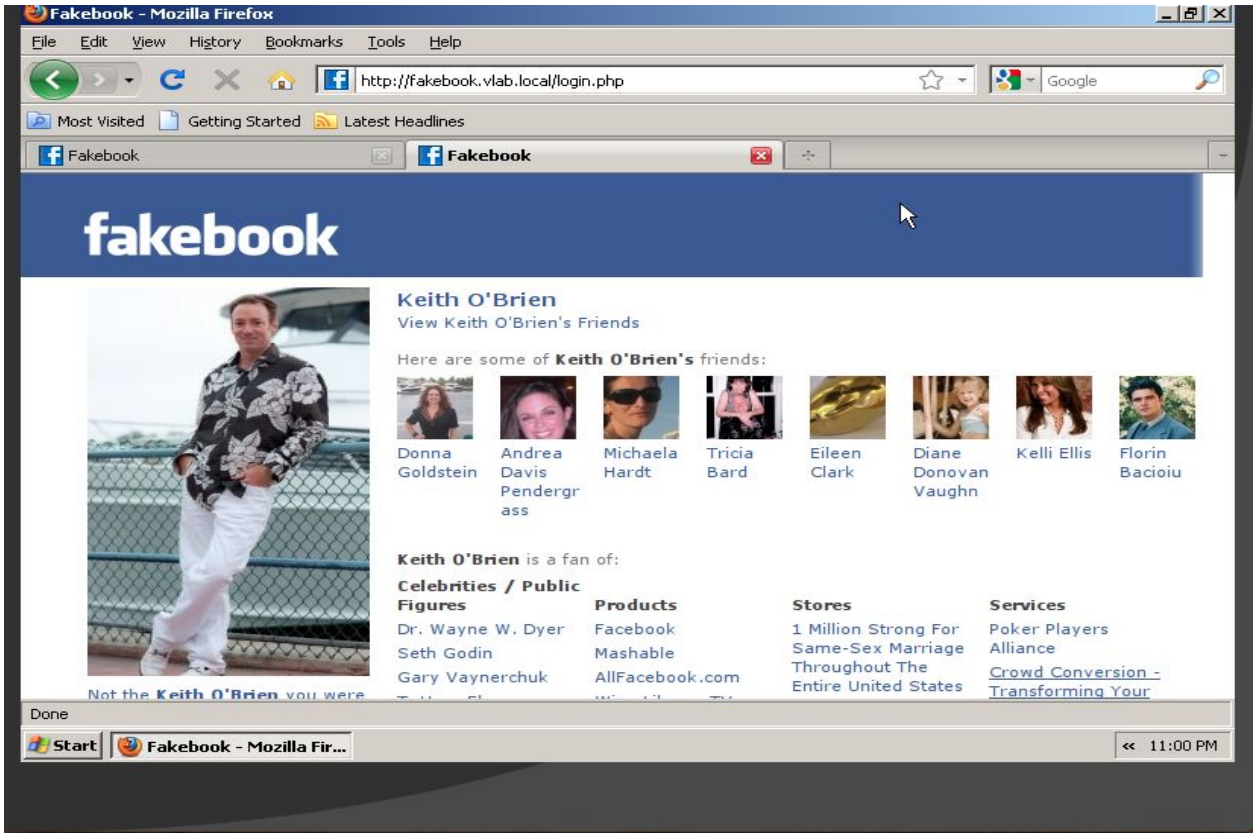


7.We then try to access the login page using the url http://fakebook.vlab/local . We then check the page source of it and then search for the form section and find that it has been changed from https to http. We can also see in the SSLstrip.log file the entries of the id password which was used to access login the webpage. Screenshot of the page source before and after the attack have been attached below along with the SSLstrip log which can show us the log in entries clearly in form of plain text.

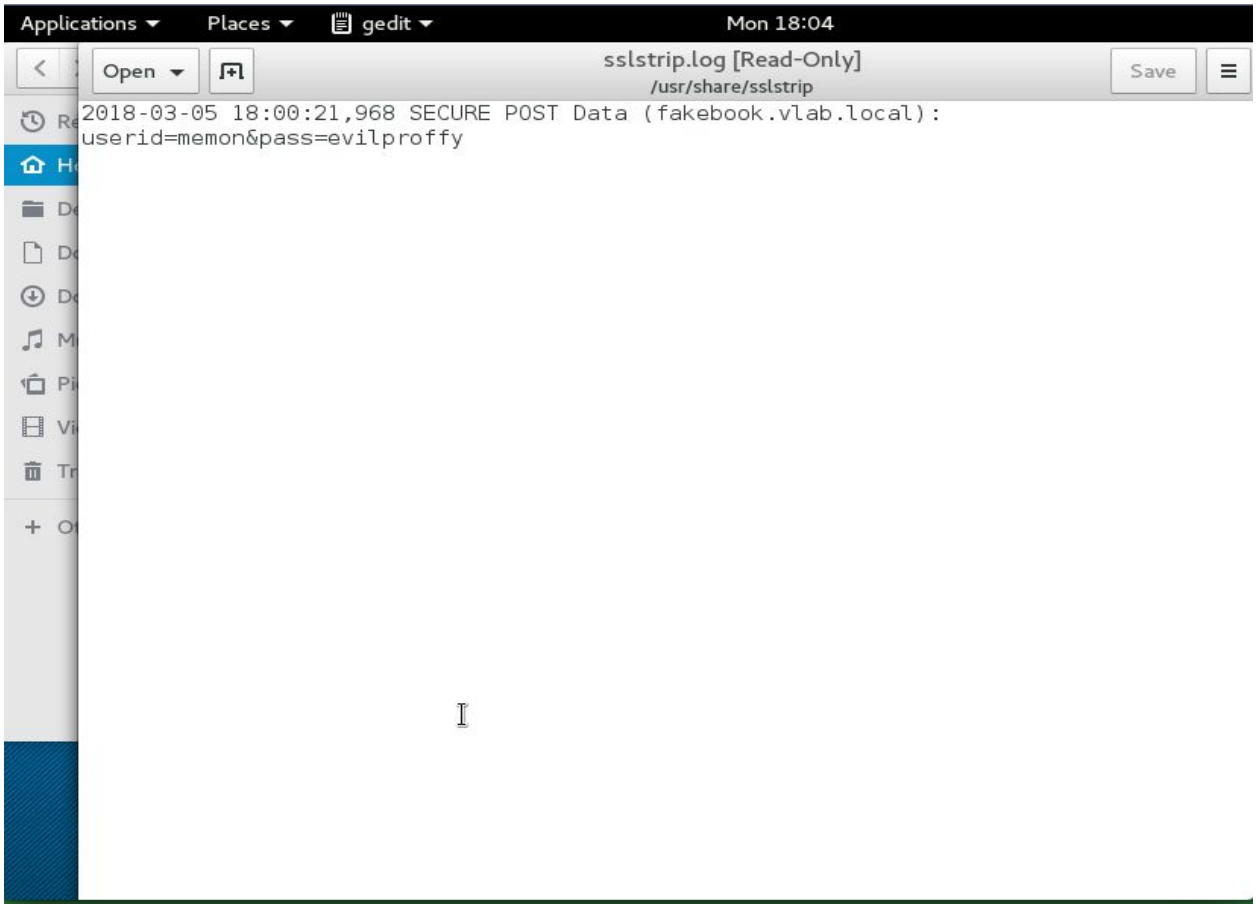


Archit Goyal
Ag6288
N17398125





Archit Goyal
Ag6288
N17398125



Therefore, it is clear from the above screenshot that the attack changed the form from HTTPS to HTTP and also, the attack was successful and we could easily see the entry which was added to the log file and it contained the id password which was used to login to the system.

Screenshot for the code is :

```
from scapy.all import *
from time import sleep

#This code sends gratuitous ARPs to XP and rtr so that Kali is in the middle of the communication between external router machine and Windows machine XP.

source1 = '10.10.111.1'   #External Router IP as source
source2 = '10.10.111.101' #Windows machine IP as source
dest1 = '10.10.111.101' #Windows machine IP as destination
dest2 = '10.10.111.1' #External Router IP as destination
hw1 = '00:00:00:00:00:04' #Windows XP physical address
hw2 = '00:00:00:00:00:02' #External router physical address

def startSpoof():
    while(True):
        #There are three parameters in order external router IP, Windows machine IP and Window machine physical address
        #op value 2 is for reply
        send(ARP(op=2,psrc=source1,pdst=dest1,hwdst=hw1))
        #There are three parameters in order Windows machine IP, external router IP and External router machine physical address
        send(ARP(op=2,psrc=source2,pdst=dest2,hwdst=hw2))
        time.sleep(2) #Sleep for some time waiting for the next packet

startSpoof() #Start spoofing
```

Archit Goyal
Ag6288
N17398125

We send two ARP with the op value as 2 which is for the reply. In one packet we have source as the ip of the external router and the destination is Windows XP machine which is the victim. The hardware physical address of the destination machine which is the windows physical address. The second ARP also is a reply with op value as 2 and has now source as ip of windows XP machine and the destination as the external router machine. The physical address is of the external router machine. Then we make the code sleep for some time before the next packet is sent. This code goes in an infinite process where packet is sent continuously on regular intervals and sends gratuitous ARPs to XP and rtr so that Kali is in the middle of the communication between external router machine and Windows machine XP. This code is run on the Kali machine.

Archit Goyal
Ag6288
N17398125