10. Session Hijacking

Practical 1: Session Hijacking using Hamster/Ferret in Kali Linux

Note: This method will work only within intranet environment. We use Kali Linux as attacker and Lubuntu 16.04 as a victim machine. Before starting, make sure to clear all the browser history from Kali and Ubuntu so all previous sessions should get terminated.

1. In Kali Linux, start the terminal and enter command:

```
cd /usr/bin/
```

2. Next enter following command:

```
rm hamster.txt
```

This will clear previously captured data.

3. Now enter command:

```
hamster
```

4. Start the Mozilla Firefox browser in Kali and go to Preferences ==> Advanced ==> Network ==> Connection ==> Settings
There select Manual and provide IP address as 127.0.0.1 i.e localhost and provide a port number 1234. Make sure to check the box “Use this proxy server for all protocols”. Afterwards clear the box that says “No proxy for”.

5. Once this is done, in URL enter:

http://hamster

6. Once you get the hamster page, on the top click on Adapter. Provide your adapter name submit it. Then head back to terminal window and confirm if the Ferret automatically started. At the end it should show “Traffic seen”.

7. Now go to your victim’s system and in browser enter some website which could be vulnerable for session hijacking

http://www.timesjobs.com
http://www.altoromutual.com

get logged in with your account.

8. Return back to Kali Linux and refresh the hamster page from browser.

9.You should notice the victim machine's IP address. If you click on that, in left side pane it will show all cloned URL from victim's browser.

10. You can start a new tab and open the same website which victim is browsing. And you should notice that you will be in his/her account. So that means you can do all activities from his/her account.

Note: Session Hijacking only works if victim's session is alive so it will be just a temporary access.

Practical 2: Session Hijacking using Cookies Manager+ addon

1. Make sure to clear all the browsing history from Kali and Lubuntu.

2. Open Wireshark in Kali Linux and start capturing the packets.

3. Go to victim's system and get logged in to http://www.altoromutual.com

4. Then return back to Kali and check wireshark. Apply a display filter "http.cookie" to get all that packets.

5. Analyse and find a right packet that contains session ID values. Right click on that packet, and select copy ==> As printable text. Paste copied data in a leafpad to see it. You should see some session ID values.

6. Now open Mozilla Firefox in Kali Linux and browse the website http://www.altoromutual.com then go to Tools ==> Cookies Manager+ and click on Search:www.altoromutual.com. It will show all the session ID tokens that you got.

7. Now replace the tokens you got with the one's from victim's captured. And then refresh the page.

8. On refreshing the page you should notice you gets access to victim's account.