Web Application Hacking - Denial of Service Attacks

Objectives

- Review lecture
- Complete lab DoS

Lecture

Slow HTTP attacks are denial-of-service (DoS) attacks in which the attacker sends HTTP requests in pieces slowly, one at a time to a Web server. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. When the server's concurrent connection pool reaches its maximum, this creates a DoS. Slow HTTP attacks are easy to execute because they require only minimal resources from the attacker.

Lab

NOTE DO NOT USE THIS AGAINST LIVE SITES. A DENIAL-OF-SERVICE ATTACK CAN LAND YOU IN PRISON. At the very best case, it can end your security career before it ever begins.

Attacking Apache with the OWASP HTTP DoS Tool

Requirements

You will need two machines--they can be physical or virtual, but they must be on the same LAN:

- A Linux machine (I recommend an Ubuntu VM) This is theTarget
- A Windows attacker (any version is OK, I used Windows XP in this example)

Starting the Apache Web Server

Start the Linux machine and log in. Open a Terminal window. Ping ubuntu.com and make sure you are getting replies. If you are not, you need to fix your networking before you can proceed.

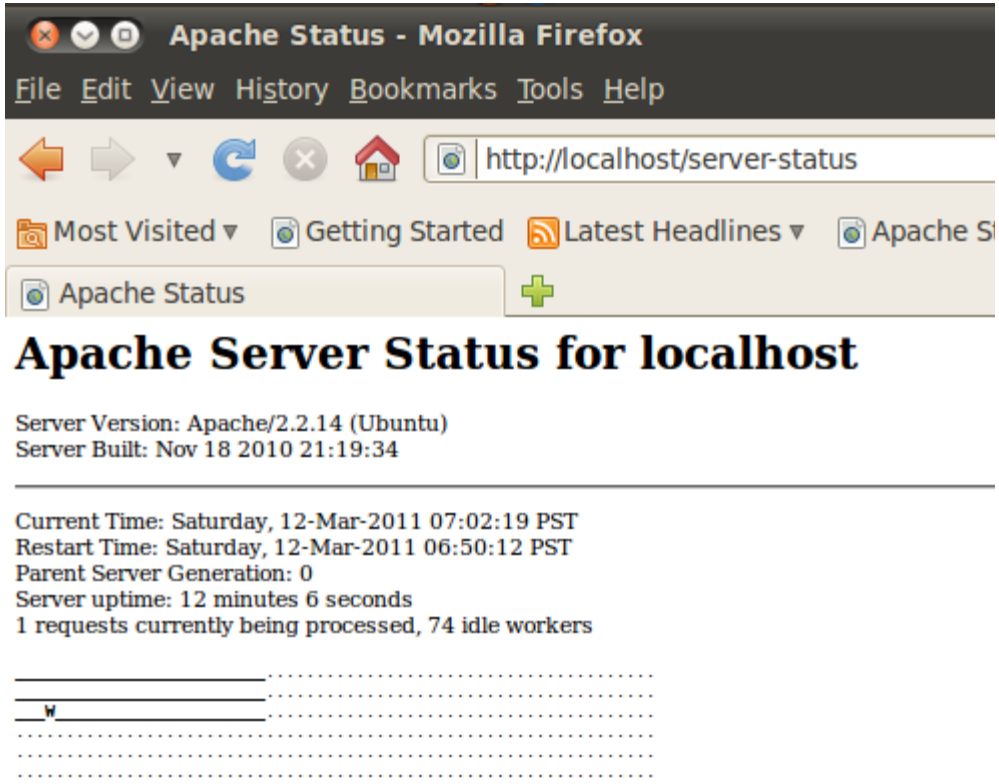
In the Terminal window, execute this command:

/etc/init.d/apache2 start

Viewing the Apache Server Status

In the Linux machine, open Firefox. Enter this address: **http:///localhost/server-status**

You should see only one letter in the grid, indicating that only one client is being served at the moment, as shown below on this page.



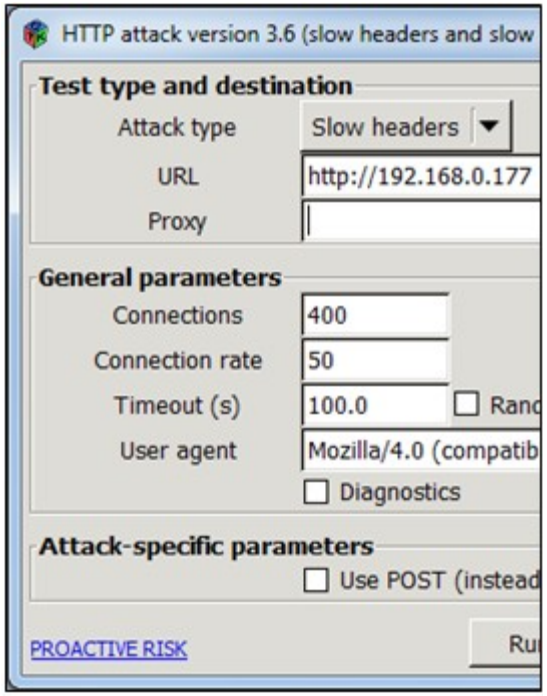
Getting the OWASP HTTP DoS Tool

On the Windows machine, open a browser and go to http://code.google.com/p/owasp-dos-http-post

Click **Downloads**. Click **HttpDosTool3.6.zip**. Download the file and unzip it.

Attacking Apache with the OWASP HTTP DoS Tool

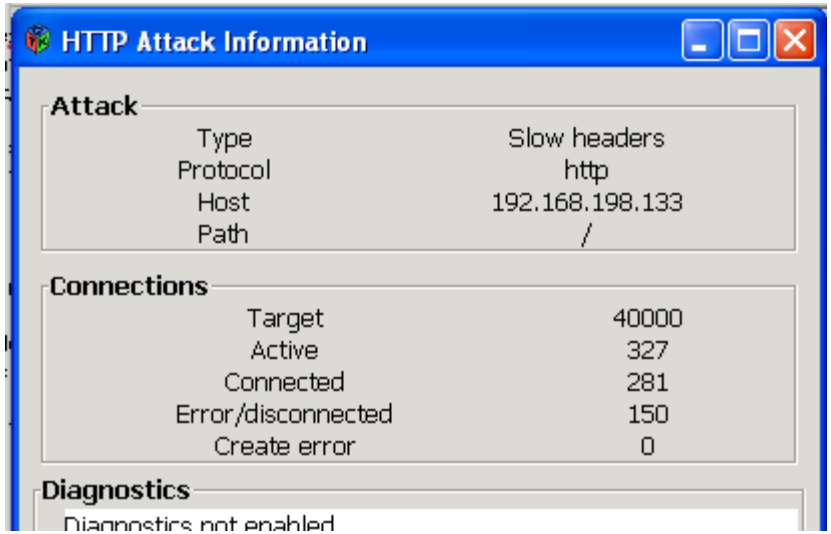
When you unzipped the file, a folder named HttpDosTool appears. Double-click it to open it. Double-click the gui.exe file. The "HTTP attack" window opens, as shown below.



In the URL box, enter **http://** followed by the IP address of your Linux Apache server.
Start with these parameters, which are sufficient to bring Apache to a total stop:

- Attack Type: **Slow headers**
- Connections: **40000**
- Connection rate: **50**
- Timeout(s): **100**

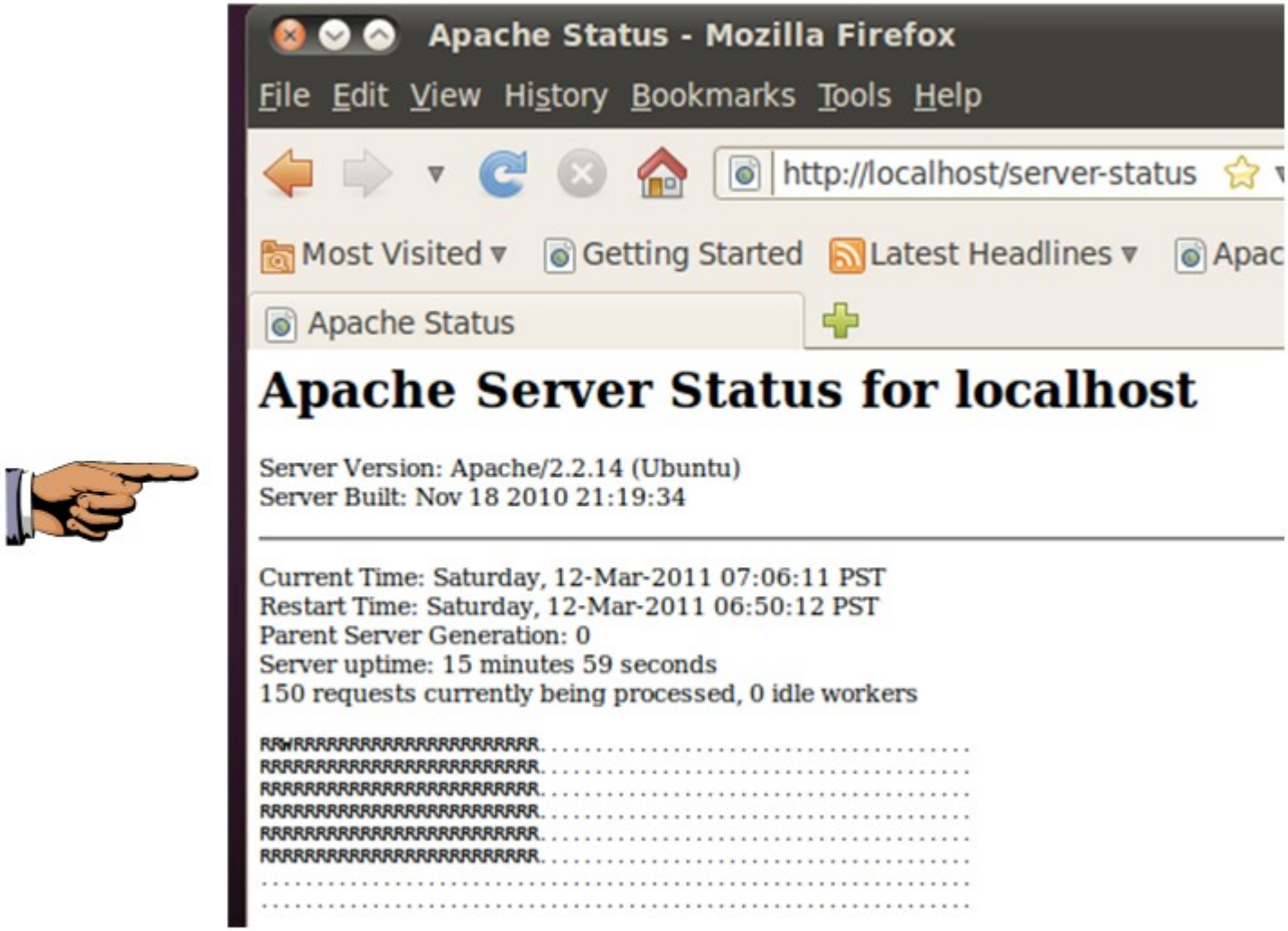
Click the "Run attack" button. You should see the "HTTP Attack information" box, as shown below on this page.



Viewing the Apache Server Status

In the Linux machine, in Firefox, click the Refresh button. If the page does not load, you may have to stop the attack briefly to get the session started, and then restart the attack, and then refresh the Firefox page.

You should see the grid full of letters, indicating that all possible connections are in use, as shown below on this page.



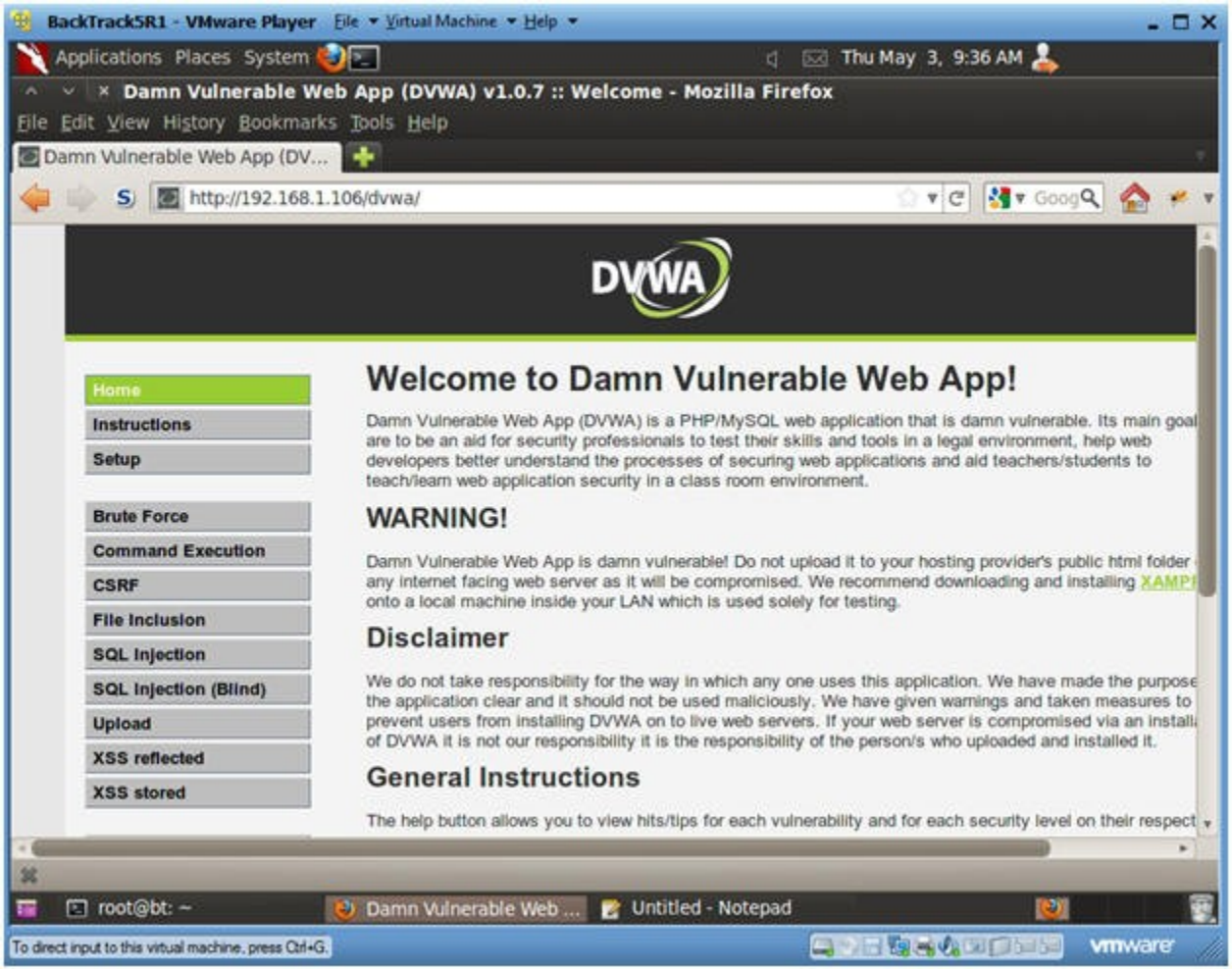
Saving the Screen Image

Make sure you can see the status grid filled with letters, as shown in the image above on this page. Save a screen image with the filename **Proj 16 from Your Name**.

Stopping the Attack

In the Windows machine, in the "HTTP Attack information" box, click the "Cancel attack" button.

Turning in Your Project



-

Proof of Lab

1. Proof of Lab
    1. Do a <PrtScn>
    2. Paste into a word document
    3. Upload to TeamBox
    -

Questions:

1. Explain in you own words what the HTTP DoS is?
2. Does this type of DoS require much resources? Why or why not?
3. Google and List some ways to protect against this