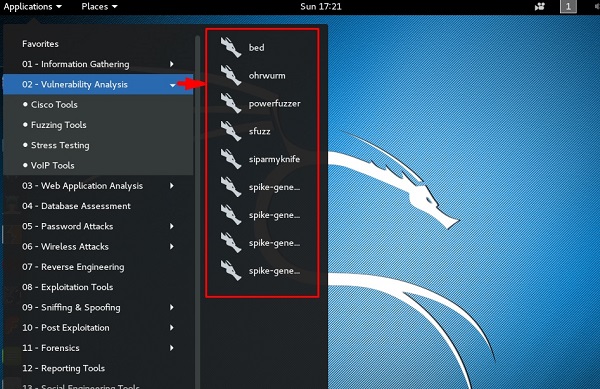
Stressing tools are used to create DoS attacks or to create the stress test for different applications so as take appropriate measures for the future.

All the Stress testing tools are found in Applications → 02-Vulnerability Analysis → Stress testing.



All Stress testing test will be done on metsploitable machine which has IP of 192.168.1.102

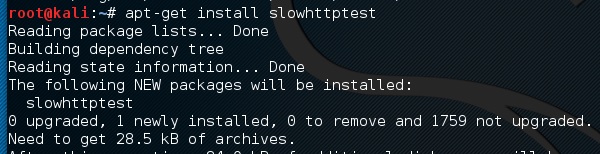
Stress Testing

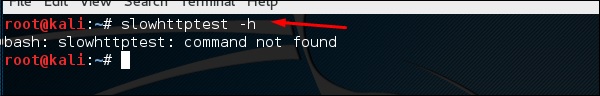
Slowhttptest

Slowhttptest is one of the DoS attacking tools. It especially uses HTTP protocol to connect with the server and to keep the resources busy such as CPU and RAM. Let’s see in detail how to use it and explain its functions.

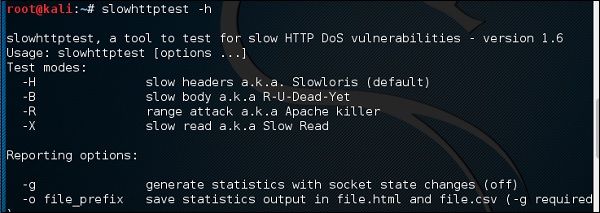
To open slowhttptest, first open the terminal and type **“slowhttptest –parameters”**.

You can type “slowhttptest –h” to see all the paramenters that you need to use. In case you receive an output, ‘Command not found’ you have to first type **“apt-get install slowhttptest”**.





Then after installation, again type **slowhttptest –h**



Type the following command −

slowhttptest -c 500 -H -g -o outputfile -i 10 -r 200 -t GET –u

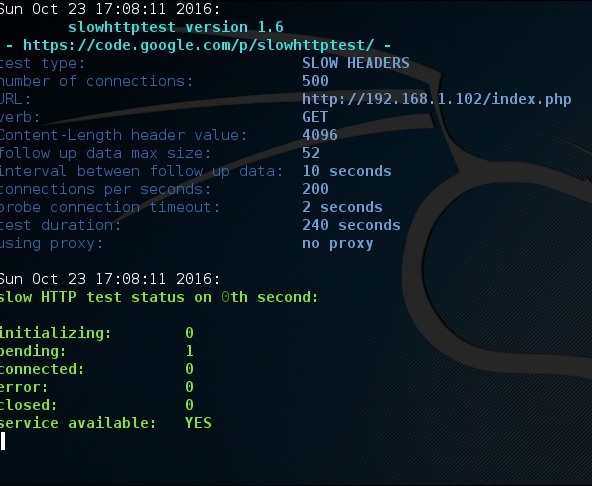
http://192.168.1.202/index.php -x 24 -p 2

Where,

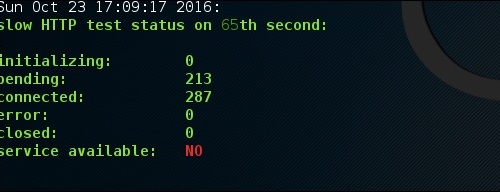
* **(-c 500) = 500** connections
* **(-H)** = Slowloris mode
* **-g** = Generate statistics
* **-o outputfile** = Output file name
* **-i 10** = Use 10 seconds to wait for data
* **-r 200** = 200 connections with -t GET = GET requests
* **-u http://192.168.1.202/index.php** = target URL
* **-x 24** = maximum of length of 24 bytes
* **-p 2** = 2-second timeout

Time Seconds

Once the test starts, the output will be as shown in the following screenshot, where you can notice that the service is available.



After a while, at the 287 connection the service goes down. This means that the server can handle a maximum of 287 HTTP connections.

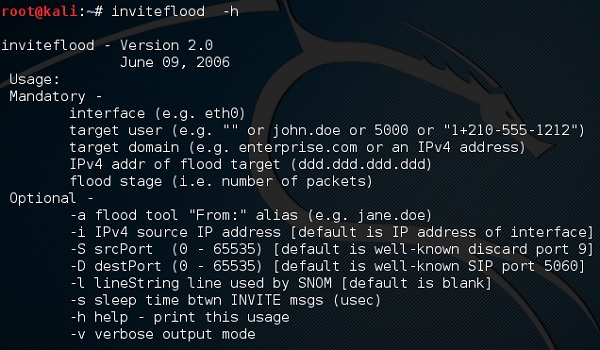


Inviteflood

Inviteflood is a SIP/SDP INVITE message flooding over UDP/IP. It executes on a variety of Linux distributions. It carries out DoS (Denial of Service) attacks against SIP devices by sending multiple INVITE requests.

To open Inviteflood, first open the terminal and type **“inviteflood –parameters”**

For help, you can use **“inviteflood –h”**

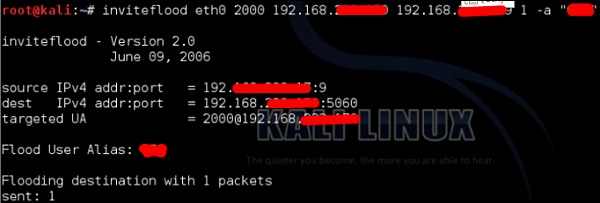


Next, you can use the following command −

inviteflood eth0 target\_extension target\_domain target\_ip number\_of\_packets

Where,

* **target\_extension** is 2000
* **target\_domain** is 192.168.x.x
* **target\_ip** is 192.168.x.x
* **number\_of\_packets** is 1
* **-a** is alias of SIP account



Iaxflood

Iaxflood is a VoIP DoS tool. To open it, type **“iaxflood sourcename destinationname numpackets”** in the terminal.

To know how to use, type **“iaxflood –h”**

Iaxflood

thc-ssl-dos

THC-SSL-DOS is a tool to verify the performance of SSL. Establishing a secure SSL connection requires 15x more processing power on the server than on the client. THCSSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet.

Following is the command −

thc-ssl-dos victimIP httpsport –accept

In this example, it will be −

thc-ssl-dos 192.168.1.1 443 –accept

Its output would be as follows −

